Agence de la consommation en matière financière du Canada
Financial Consumer Agency of Canada

Les paiements mobiles et la protection des consommateurs
Examen de la situation à l'échelle internationale

Charles Gibney, Steve Trites, Nicole Ufoegbune, Bruno Lévesque

Division de la recherche, Agence de la consommation en matière financière du Canada

Janvier 2015

La Division de la recherche de l'Agence de la consommation en matière financière du Canada (ACFC) est chargée de la surveillance et de l'évaluation des tendances et des nouveaux enjeux qui pourraient avoir une incidence sur les consommateurs de produits et services financiers. Les documents de recherche de l'ACFC sont le produit d'études théoriques ou empiriques en cours. Les opinions exprimées dans le présent document sont celles des auteurs, et elles ne doivent pas être attribuées à l'ACFC.

Remerciements

De nombreux collègues et organisations ont contribué à la préparation du présent rapport de recherche. Les auteurs tiennent à remercier tout particulièrement :

- le US Consumer Financial Protection Bureau;
- l'Organisation de coopération et de développement économiques;
- le Groupe consultatif d'assistance aux pauvres.

Résumé

Les paiements mobiles sont un élément important des services bancaires mobiles, un type de services financiers de détail qui connaît une expansion rapide à l'échelle internationale (Continie, Crowe, Merritt, Oliver et Mott, 2011; Dapp, Stobbe et Wruuck, 2012; Commission européenne 2012). Les consommateurs canadiens délaissent de plus en plus les opérations bancaires en succursale pour adopter les services bancaires mobiles et en ligne. Les études indiquent que le marché canadien est sur le point de connaître une croissance très importante du volume des opérations de paiement mobile (Association canadienne des paiements, 2013; Trichur, 2013).

Le présent examen portera sur les faits nouveaux relativement à la réglementation des paiements mobiles à l'échelle de l'économie mondiale. Il met l'accent sur la protection des consommateurs. Nous avons effectué des analyses secondaires sur des marchés semblables à celui du Canada et sur des marchés où l'écosystème de paiement mobile est bien développé et où les organismes de réglementation possèdent une expérience de la supervision. Nous nous sommes penchés sur les problèmes constatés et les efforts déployés pour les régler. Nous examinons de grands enjeux stratégiques, tels que la coordination entre organismes, ainsi que l'objet et la portée de la réglementation. Nous examinons aussi comment des conditions particulières du marché influencent l'évolution des écosystèmes de paiement mobile. Le but premier du présent rapport est d'éclairer les décideurs, les organismes de réglementation et de surveillance, et les autres chercheurs et de leur donner une compréhension approfondie des questions liées à la protection des consommateurs (p. ex. la confidentialité des données, la divulgation, les recours, la fraude et la sécurité) et des initiatives réglementaires qui sont mises en œuvre à l'étranger au fur et à mesure de l'évolution des paiements mobiles.

La situation actuelle de la réglementation internationale sur les paiements mobiles

Réserve et réglementation

À l'heure actuelle, la plupart des organismes de réglementation font preuve de prudence et hésitent à créer de nouveaux règlements visant à protéger les consommateurs qui ont commencé à effectuer des paiements à l'aide d'un appareil mobile. La croissance du volume d'opérations de paiement mobile est constante, mais plus lente que prévu. La plupart sont d'avis que la technologie liée aux paiements mobiles n'en est qu'aux premières étapes de son développement. Les modèles d'entreprise ne remontent qu'à un ou deux ans. Pour ces raisons, les décideurs de l'UE et des É.-U. procèdent avec prudence. Ils veulent, semble-t-il, éviter la création de règlements qui pourraient décourager les entreprises novatrices de développer la voie du paiement mobile. Ils veulent aussi éviter de modifier les règles existantes de façon à favoriser un type d'intervenant de l'industrie ou un modèle d'entreprise au détriment des autres. On s'inquiète de ce que les nouvelles lois pourraient aller à l'encontre des règles existantes ou décourager la conformité en créant une complexité extrême.

Il y a néanmoins plusieurs faits nouveaux importants dans les pays industrialisés et en voie de développement : nouvelle réglementation, modifications apportées aux règles existantes, projets de

recherche et politiques qui cherchent à répondre aux préoccupations concernant les paiements mobiles. Malgré un climat général de prudence et de réserve, les organismes de réglementation ont adopté une approche à deux volets : premièrement, des groupes de travail de l'industrie ont été constitués en vue de conclure des ententes concernant les pratiques exemplaires, les engagements publics et les lignes directrices de conformité volontaire; deuxièmement, de nouvelles directives, de nouvelles lois et de nouveaux règlements ont été adoptés pour répondre à des préoccupations particulières liées aux paiements mobiles.

L'autoréglementation : innovation et interopérabilité

Les organismes de réglementation ont contribué à la mise sur pied de « groupes de travail » afin de faciliter le dialogue et la coopération entre les intervenants de l'industrie. Également connu sous le nom de « voie » ou d'« écosystème », le système permettant les paiements par appareil mobile est complexe et comprend une vaste gamme d'intervenants de l'industrie (p. ex. les exploitants de réseaux mobiles, les concepteurs d'applications logicielles, les fabricants d'appareils mobiles, les exploitants de réseaux de cartes de crédit et de débit, les institutions financières et les fournisseurs de services de paiement).

Les écosystèmes de paiement mobile sont fondés à la fois sur des technologies « interopérables » (p. ex. services de messages courts ou SMC), qui ont des protocoles communs pour permettre l'interaction entre les systèmes informatiques, et les technologies propriétaires, telles que l'application logicielle Google Wallet ou le système d'exploitation d'un appareil mobile (p. ex. iOS 7). Pour pouvoir développer l'écosystème de paiement mobile, les organismes de réglementation doivent faciliter les partenariats stratégiques entre les secteurs et promouvoir la concurrence entre les entreprises.

Pour trouver le juste équilibre entre concurrence et collaboration, la Réserve fédérale américaine a créé le Mobile Payments Industry Workgroup (MPIW, groupe de travail de l'industrie du paiement mobile); la Banque centrale européenne a constitué le Conseil européen des paiements et la commission coréenne des communications a mis sur pied la Grand NFC Korea Alliance (grande alliance coréenne de la communication en champ proche). Ces groupes de travail mettent en commun des études de marché, des pratiques exemplaires et des idées sur l'interopérabilité. Ils œuvrent en vue d'élaborer des principes qui permettront à l'industrie des paiements mobiles de se superviser sur une base volontaire avec l'aide des organismes de réglementation. Ces initiatives ne se sont pas déroulées sans susciter la controverse. Dans l'Union européenne, certains ont accusé des intervenants de l'industrie, en particulier de grandes banques, de dominer l'ordre du jour des groupes de travail au détriment d'intervenants moins puissants, comme les petits détaillants (Commission européenne, 2012a).

Directives réglementaires : institutions non bancaires, collecte de données et protection des renseignements personnels

Les décideurs ont préparé des modifications et adopté une série de dispositions impératives qui visent des problèmes de protection des consommateurs, qui ont vu le jour à la suite de la croissance des paiements mobiles, des opérations bancaires mobiles et du commerce électronique.

Notre examen révèle deux types d'outils réglementaires. Premièrement, même si les banques ont joué le rôle de gardiens du système de paiement de détail, il est manifeste que les institutions non bancaires, les fournisseurs de services de paiement, les fournisseurs de services de confiance et les nouvelles entreprises

tierces et nouveaux tiers entrepreneurs auront un rôle prépondérant à jouer dans l'écosystème de paiement mobile. Les banques seront peut-être exposées à de nouveaux risques systémiques lorsqu'elles concluent des ententes stratégiques avec des institutions non bancaires pour la prestation et le règlement des opérations de paiement mobile. La sécurité de l'écosystème de paiement mobile se mesurera à celle de son maillon le plus faible. Les organismes de surveillance éprouveront peut-être de la difficulté à trouver, pour les institutions non bancaires, un fardeau réglementaire proportionnel aux risques systémiques qu'elles posent, qui n'est pas trop contraignant et encourage donc les nouveaux arrivants innovateurs sur le marché. Du point de vue des consommateurs, la vaste gamme d'intervenants participant à la voie du paiement mobile peut créer de la confusion lorsque des problèmes surgissent. Les consommateurs peuvent éprouver de la difficulté à déterminer à quelle entreprise il incombe, en fin de compte, de régler les opérations litigieuses. Dans le présent rapport, nous examinons les démarches entreprises pour superviser les institutions non bancaires dans plusieurs pays. Le *Electronic Financial Transactions Act* (2007) de la Corée du Sud semble avoir les règles les plus détaillées quant à la responsabilité des banques et des institutions non bancaires d'offrir des mécanismes de recours aux consommateurs aux prises avec des difficultés. Deuxièmement, il semble que plusieurs pays aient décidé que leur cadre réglementaire ne protégera pas de façon adéquate la confidentialité des données générées par les consommateurs lors des opérations de paiement mobile. La plupart des opérations de commerce électronique produisent un ensemble de données sur le consommateur concernant les habitudes de navigation, les habitudes de consommation et les caractéristiques démographiques. Cependant, lorsque les consommateurs font des achats au détail à l'aide d'un appareil mobile, ces données courantes de commerce électronique peuvent être recueillies en même temps que de nouveaux renseignements sur la géolocalisation des consommateurs, leurs habitudes de déplacement, l'historique de leurs appels, leur abonnement de téléphone portable et leur historique de facturation. Qui plus est, les consommateurs entreposent habituellement leurs contacts personnels, photos, messages et itinéraires sur leurs appareils mobiles.

Grâce aux nouvelles technologies « intelligentes », il sera possible de récolter, de fusionner et de traiter les renseignements personnels identifiables ainsi que des données anonymes. De cette façon, les annonceurs pourront créer des profils individuels détaillés des consommateurs. Les profils peuvent servir à adapter les stratégies de marketing en fonction des données récoltées au sujet des consommateurs. La « publicité ciblée comportementale » atteint les consommateurs directement, au fur et à mesure de leurs activités quotidiennes. Elle vise à prédire et à moduler le comportement des consommateurs. Ce nouveau type de marketing peut être relativement inoffensif dans certains cas, mais il pourrait aussi donner lieu à de nouveaux problèmes sur le plan de la protection des consommateurs.

Il semble probable que la récolte de données en vue de faciliter de nouveaux types de marketing sera un élément essentiel des modèles opérationnels des grandes entreprises de paiement mobile. Google ne fait pas payer les consommateurs pour effectuer des opérations ou pour télécharger son portefeuille mobile. Il semble que Google assumera ces coûts opérationnels en échange d'une part de marché et de données sur les consommateurs, ce qui lui permettra d'augmenter ses revenus de publicité.

Les organismes de réglementation tentent de trouver un juste équilibre entre la nécessité d'encourager la croissance de la technologie de paiement mobile et l'obligation de protéger les consommateurs des

nouveaux problèmes qui pourraient se poser. Le paiement mobile améliore l'éventail de choix des consommateurs. Il permet aux annonceurs d'envoyer des annonces adaptées aux goûts et aux préférences du consommateur, au moment le plus propice. La publicité ciblée pourrait être un attrait essentiel pour les entreprises. L'une des façons qui ont permis aux organismes de réglementation de trouver un juste équilibre est de permettre aux consommateurs de décider dans quelle mesure ils veulent participer au marketing ciblé. Il est possible de donner aux consommateurs la possibilité de choisir, en exigeant des entreprises qu'elles obtiennent leur consentement éclairé; cela signifie que les entreprises doivent énoncer clairement les modalités contractuelles et donner l'occasion aux consommateurs de refuser ou d'accepter le contrat avant de s'engager.

Des experts ont applaudi l'adoption des règles de protection des consommateurs énoncées dans les directives de l'Union européenne sur la protection des données et la protection de la vie privée dans le secteur des communications électroniques. Les directives sont fondées sur des principes, sont neutres sur le plan technologique, et sont souples et adaptatives. Elles permettent aux gens de divulguer des données personnelles lorsque cela est dans leur intérêt, tout en faisant en sorte que la récolte et le traitement de leurs données se font de façon légale et équitable. Toutefois, les observateurs préviennent que ces directives pourraient ne pas suffire au fur et à mesure de l'évolution du commerce électronique et des paiements mobiles (Robinson, Graux, Botterman et Valeri, 2009).

Table des matières

1. Introduction

Le présent rapport fournit un résumé des développements à l'échelle internationale dans le domaine des paiements mobiles et de la protection des consommateurs. Les paiements mobiles constituent un élément important des services bancaires mobiles, lesquels sont un type de services financiers de détail qui connaît une expansion rapide à l'échelle internationale (Continie, Crowe, Merritt, Oliver et Mott, 2011; Dapp, Stobbe et Wruuck, 2012; Commission européenne, 2012). Les études indiquent que les consommateurs canadiens délaissent de plus en plus les opérations bancaires en succursale pour adopter les services bancaires mobiles et en ligne. En 2010, 19 p. 100 des Canadiens interrogés utilisaient des services bancaires mobiles. La proportion de consommateurs financiers qui utilisent des services bancaires en succursale a diminué de 30 p. 100 depuis 2000 et s'établit aujourd'hui à seulement 17 p. 100 (Association des banquiers canadiens, 2012). Selon les observations des experts, le marché canadien est sur le point de connaître une croissance très importante du volume d'opérations de paiements mobiles dans un proche avenir (Association canadienne des paiements, 2013; Trichur, 2013).

Le présent examen a pour objet d'informer les responsables gouvernementaux de la réglementation, les décideurs, les chercheurs, les intervenants de l'industrie et les consommateurs financiers au sujet des questions réglementaires qui ont surgi avec l'émergence des paiements mobiles. Il met l'accent sur les répercussions possibles dans le domaine de la protection des consommateurs. Nous avons effectué des recherches sur des marchés semblables à celui du Canada et sur des marchés où les paiements mobiles sont bien établis et où les organismes de réglementation possèdent une expérience de la supervision. Nous avons réalisé une recherche de synthèse sur les problèmes constatés par les organismes de réglementation et les efforts déployés par ces derniers pour les régler. En raison du potentiel qu'ont les paiements mobiles et les services bancaires mobiles de transformer les services financiers de détail, la recherche effectuée pour la préparation du présent rapport s'est faite dans une perspective étendue. Nous examinons de grands enjeux stratégiques, tels que la coordination entre organismes, l'objet et la portée de la réglementation sur les paiements mobiles ainsi que les efforts déployés pour régler les questions touchant à la protection des consommateurs comme la fraude et la protection des renseignements personnels.

La première partie concerne la réglementation sur les paiements mobiles aux États-Unis. La situation aux États-Unis est semblable à celle que l'on observe au Canada, en ce sens que les spécialistes voient un grand potentiel dans les paiements mobiles et pourtant la croissance de ce type de paiements a été plus lente que prévu. Face à cette situation, les décideurs aux États-Unis sont de l'avis qu'il est prématuré, à ce stade, d'adopter une loi visant les paiements mobiles. Les responsables de la réglementation ont entrepris des démarches en vue de modifier les règles existantes et ils continuent de surveiller plusieurs questions. Certains spécialistes décrivent le cadre réglementaire actuel comme étant trop complexe, ce qui peut poser des défis étant donné que l'écosystème de paiement mobile est également extrêmement complexe. Il faudra faire appel à un grand nombre d'organismes de réglementation pour superviser les intervenants de l'industrie qui offrent des services de paiement mobile. Il existe une certaine controverse sur la question de déterminer quels éléments de la technologie liée aux paiements mobiles devraient être des ressources partagées et quels éléments devraient faire l'objet d'une propriété exclusive, ainsi que sur

la question de savoir si les responsables de la réglementation ont un rôle à jouer dans la création de règlements sur l'interopérabilité. Le degré auquel la technologie sur les paiements mobiles est partagée, ou est interopérable, aura des répercussions sur les règles qui seront nécessaires pour assurer la sécurité des données créées lors des paiements mobiles. Enfin, il y a également des questions non résolues liées à la protection de la confidentialité des données fournies par les consommateurs qui utilisent les services de paiement mobile ou des données générées à leur sujet.

La deuxième partie fait état des faits nouveaux dans l'Union européenne (UE). Les spécialistes prévoient une croissance rapide de l'utilisation des paiements mobiles dans l'UE en raison de la tendance vers des modes de paiement électroniques ainsi que des taux de pénétration des téléphones cellulaires et d'adoption des services bancaires mobiles (Dapp, Stobbe et Wruuck, 2012). Toutefois, on observe cet état de préparation du marché depuis plus d'une décennie. La croissance du volume d'opérations de paiements mobiles a été constante, mais plus lente que prévu (Commission européenne, 2012). L'UE et les États-Unis ont de nombreux points en commun pour ce qui est des possibilités non réalisées du marché et du taux relativement élevé de satisfaction des consommateurs à l'égard des modalités existantes de paiement de détail, qui sont fiables, bien connues et sûres. L'UE a introduit une réglementation importante en matière de paiements mobiles et de services bancaires mobiles. Nous examinerons comment l'UE envisage de se servir des paiements mobiles comme outil pour harmoniser davantage le mouvement des personnes, des marchandises et du capital au sein du « marché unique ». C'est pour cette raison que les responsables de la réglementation se sont demandé si les frais perçus sur les opérations électroniques de détail nécessiteront de nouveaux types de réglementation. Notre examen porte également sur la façon dont l'UE a abordé les questions de confidentialité des données et le rôle des institutions non financières dans l'écosystème de paiement électronique.

La troisième partie porte sur les paiements mobiles et la protection des consommateurs en Corée du Sud et au Japon. Les deux marchés sont des chefs de file mondiaux pour ce qui est du taux d'adoption des paiements mobiles par les consommateurs et du volume de ces paiements (OCDE, 2012; KPMG International, 2007; Dapp, Stobbe et Wruuck, 2012). Les organismes de surveillance ont adopté une approche prudente à l'égard de l'élaboration de nouveaux règlements et de la modification du cadre existant. Nous examinons la stratégie adoptée par la Corée du Sud pour établir un juste équilibre entre la promotion des services bancaires mobiles et la protection des consommateurs des risques associés aux paiements mobiles dans la *Electronic Financial Transaction Act* (loi sur les opérations financières électroniques) et la *E-commerce Consumer Protection Act* (loi sur la protection des consommateurs en matière de commerce en ligne).

Enfin, dans la quatrième partie, nous décrivons la réponse des organismes de réglementation face à la croissance des services monétaires mobiles dans le monde en développement. Nous examinons le service M-PESA de Safaricom. Lancé au Kenya en 2007, M-PESA est devenu un modèle extrêmement réussi dans le domaine des services bancaires mobiles dans les pays en développement. Actuellement, la réglementation du secteur financier dans les pays en développement est très limitée, surtout en ce qui concerne la protection des consommateurs. L'émergence des services monétaires mobiles contribue à combler les lacunes dans la disponibilité des services financiers. La croissance des services monétaires

mobiles a donné l'impulsion à l'élaboration d'un cadre réglementaire plus étendu. Notre examen suit l'émergence de plusieurs nouvelles initiatives visant la protection des consommateurs.

2. Les États-Unis

Les États-Unis sont considérés comme l'un des chefs de file, sinon *le* chef de file, de l'innovation dans le domaine des paiements mobiles (Dapp, Stobbe et Wruuck, 2012). Néanmoins, on estime que la technologie de paiement mobile aux États-Unis en est toujours à ses balbutiements. Les marchés des paiements mobiles aux États-Unis et au Canada présentent plusieurs caractéristiques communes importantes, comme la tendance vers les modes de paiement électroniques, la grande satisfaction des consommateurs à l'égard des cartes de crédit et de débit, ainsi que le taux élevé d'adoption des téléphones cellulaires et des services bancaires mobiles (Board of Governors of the Federal Reserve System, mars 2012; Quorus Consulting Group, 2012). Voilà pourquoi l'expérience des organismes de réglementation des États-Unis peut être une source précieuse de renseignements sur les difficultés que pourraient présenter les paiements mobiles en matière de protection des consommateurs au Canada.

2.1. Réserve des organismes réglementaires

À l'heure actuelle, les organismes de réglementation américains estiment qu'il n'est pas nécessaire d'établir de nouvelles règles dans l'immédiat pour protéger les consommateurs qui effectuent des paiements mobiles (Crowe, Kepler et Merritt, 2012). Les données disponibles semblent indiquer que les consommateurs seront beaucoup plus nombreux à recourir aux paiements mobiles pour acheter des produits et des services au cours des cinq à dix prochaines années[1]. Cependant, tout le monde semble s'entendre pour dire que la technologie de paiement mobile continue d'évoluer rapidement. Les organismes de réglementation américains veulent éviter d'éventuellement freiner l'innovation en adoptant de nouvelles règles au moment où l'industrie met au point la technologie et crée des entreprises. Cette position est fondée sur la perception que le marché américain n'a pas adopté les paiements mobiles aussi rapidement que prévu. Les paiements mobiles pourraient améliorer l'efficacité du système de paiement. Les intervenants de l'industrie s'emploient à convaincre les marchands et les consommateurs de délaisser les modes de paiement traditionnels. Des observateurs ont fait remarquer que la réglementation hâtive des réseaux de paiement par carte de débit avait freiné l'innovation dans ce domaine (Montgomery, 2012)[2]. Enfin, les organismes de réglementation ont tenu compte des arguments selon lesquels même si les paiements mobiles ouvrent de nouvelles voies pour la réalisation, la compensation et le règlement des paiements, les principales sources des fonds qui sous-tendent les paiements mobiles (p. ex. les sources accessibles par cartes de débit et de crédit) sont adéquatement régies par la réglementation existante sur les opérations électroniques (Crowe, Kepler et Merritt, 2012).

Les organismes de réglementation ont choisi d'adapter graduellement les règles portant sur les paiements mobiles en prévision des nouvelles difficultés qui se présenteront à mesure que la technologie évolue. Le Consumer Financial Protection Bureau (CFPB) s'est chargé de ce processus. Les lois fédérales sur la

[1] Selon un récent sondage réalisé par la Réserve fédérale américaine, les gens utilisent de plus en plus leur téléphone cellulaire pour effectuer leurs opérations bancaires et leurs paiements, gérer leur budget et faire des achats. Cette réalité est particulièrement avérée chez les jeunes (de 18 à 24 ans) et chez les consommateurs non bancarisés ou sous-bancarisés. Cette dernière catégorie comprend aussi un nombre disproportionné de jeunes (Board of Governors of the Federal Reserve System, mars 2012).

[2] Le 29 mars 2012, lors d'un échange à la première séance du comité sénatorial des banques, les sénateurs Mark Warner et Richard Shelby sont convenus que le Congrès avait employé la méthode « brutale » lorsqu'il a imposé des plafonds aux frais de transaction par carte de débit, qui ont peut-être limité l'innovation et la croissance, et que l'adoption d'une réglementation immédiate ou « musclée » pourrait avoir un effet similaire sur les paiements mobiles (Wack, 2012).

protection des consommateurs de produits et services financiers relèvent du CFPB depuis 2011. Le CFPB a adapté le règlement E de l'*Electronic Fund Transfers Act*, en partie en raison de l'essor des opérations bancaires mobiles et des paiements mobiles. L'examen suivant de la réglementation et des paiements mobiles aux États-Unis porte sur trois questions essentielles : la complexité de la réglementation, l'interopérabilité et la protection des renseignements personnels.

2.2. Complexité de la réglementation

La première difficulté liée à la réglementation des paiements mobiles est sa complexité. Les paiements mobiles touchent une grande diversité d'intervenants de l'industrie (p. ex. exploitants de réseaux mobiles, banques et institutions financières non bancaires, fabricants de téléphones cellulaires et concepteurs d'applications logicielles), de marchands, de consommateurs et d'organismes de réglementation. Le cadre réglementaire régissant les opérations financières aux États-Unis est déjà complexe. Il fait intervenir un grand nombre d'organismes et de multiples ordres de gouvernement. Certains experts estiment qu'il est trop complexe ou fragmenté (Brown, 2012). Avec l'essor des paiements mobiles arrivent sur le marché des entreprises qui en sont à leurs premières armes dans le secteur financier et possèdent peu d'expérience pour composer avec un environnement réglementaire complexe. Ces nouveaux arrivants sur le marché sont déjà régis par un ensemble de règles liées à leurs activités principales. Certains observateurs ont avancé que la convergence de l'industrie entraînée par l'essor des paiements mobiles rendra nécessaire la convergence de la réglementation (Katz, 2012). En d'autres termes, il pourrait être souhaitable d'essayer de simplifier le cadre réglementaire régissant les opérations financières pour tenir compte des nouveaux arrivants sur le marché qui proposent des services novateurs comme les paiements mobiles. Selon les experts, trois principales difficultés peuvent se poser relativement à la complexité de la réglementation sur les paiements mobiles et aux efforts à consacrer pour réglementer ces derniers : le risque d'ambiguïtés et de lacunes; les obstacles à l'application de la réglementation, à la conformité aux exigences réglementaires et à l'entrée sur le marché; ainsi que les règlements contradictoires. Pour surmonter ces difficultés, les États-Unis ont centralisé le pouvoir de réglementation fédéral en matière de protection des consommateurs de produits et services financiers, pouvoir qu'il a conféré au Consumer Financial Protection Bureau.

2.2.1. Risque d'ambiguïtés et de lacunes

Tout d'abord, des experts ont fait remarquer que l'essor des paiements mobiles pourrait faire apparaître des ambiguïtés et des lacunes dans le cadre de protection des consommateurs. L'étendue des pouvoirs des organismes, c'est-à-dire là où ces pouvoirs commencent et là où ils arrêtent, pourrait prêter à interprétation. Ces ambiguïtés peuvent rendre difficile la réglementation des nouvelles technologies. Par exemple, la Federal Trade Commission (FTC) a compétence sur bon nombre des entreprises qui interviennent dans les paiements mobiles (comme les fabricants de matériel, les annonceurs, les gestionnaires de données et les concepteurs d'applications logicielles). La FTC a compétence principale pour ce qui est de protéger les consommateurs de la fraude, de la tromperie ou des pratiques déloyales et compte 15 ans d'expérience dans la surveillance des règles visant la protection des consommateurs en matière de technologie mobile. La FTC s'est dite intéressée par la question de l'absence de lignes directrices sur la protection des renseignements personnels dans le cas des applications mobiles qui ciblent les enfants (Crowe, Kepler et Merritt, 2012). Cependant, la FTC ne semble avoir compétence qu'à

l'égard de certains types de paiements mobiles, comme la facturation directe par l'entreprise de télécommunications[3].

La Federal Communications Commission (FCC) est l'organe de supervision de l'utilisation des services à large bande. Elle est directement concernée par la sollicitation croissante des réseaux mobiles par les paiements mobiles. La possibilité d'envoyer de la publicité sur les appareils mobiles des consommateurs semble occuper une place importante dans le modèle d'affaires des entreprises qui offrent des services de paiement mobile. La demande induite par cette publicité et imposée à la technologie sans fil à large bande utilisée pour donner accès à Internet sur les appareils mobiles revêtira un intérêt pour la FCC. Quoi qu'il en soit, certains experts soulignent que la FCC n'a pas l'autorité pour réglementer les sources sous-jacentes de paiement, quelles qu'elles soient. Une incertitude demeure quant à la mesure dans laquelle les paiements mobiles présentent un intérêt pour la FCC et quant à l'autorité dont elle dispose à leur égard.

Le Financial Crimes Enforcement Network (FinCEN) du département du Trésor des États-Unis pourrait trouver que la surveillance des paiements mobiles de personne à personne présente un intérêt, étant donné que ces paiements pourraient servir au blanchiment d'argent, au trafic de stupéfiants ou au financement d'organisations terroristes. Le département de la Justice pourrait aussi intervenir dans la surveillance des paiements mobiles. L'intérêt de ce département réside dans les lois régissant la collecte de renseignements sur les consommateurs par des tiers (Brown, 2012).

Le Consumer Financial Protection Bureau (CFPB) a le pouvoir de s'assurer que toute entreprise qui fournit des services financiers respecte les directives, les règles et les lois fédérales sur la protection des consommateurs. Comme il a été mentionné précédemment, le fait de centraliser cette protection sous l'autorité du CFPB devrait aider à surmonter certaines des difficultés liées à la complexité de la réglementation. Il semble que le CFPB ait pris l'initiative de surveiller si la réglementation actuelle était adéquate et de l'adapter à mesure que la technologie fait évoluer l'expérience client (Crowe, Kepler et Merritt, 2012). De manière générale, le CFPB a élargi le champ d'application des définitions prévues dans le règlement E pour prendre en compte les paiements mobiles dans le cadre actuel. Désormais, selon ce règlement, « institution financière » s'entend de toute entité qui fournit un « dispositif d'accès » (*access device*), ce qui comprend les appareils mobiles utilisés pour effectuer des paiements mobiles (*Regulation E*, 2011 : 1005.2). Certains observateurs ont fait valoir que le fait d'élargir la définition de termes clés ne dissipera pas l'ambiguïté à l'égard des pouvoirs des organismes de réglementation. Ces observateurs souhaiteraient que la définition d'*access device* prévue par la loi soit plus précise et que les téléphones cellulaires y soient désignés expressément (Crowe, Kepler et Merritt, 2012).

Un autre problème qui se pose est que les paiements mobiles sont régis par des règles différentes selon la source sous-jacente des fonds utilisés par le consommateur. Par exemple, les sources des fonds dans

[3] Le type de paiement mobile dépend de la source sous-jacente des fonds utilisés au cours de l'opération. La facturation directe par l'entreprise de télécommunications est l'une des façons dont les consommateurs peuvent effectuer un paiement mobile. Ce type de facturation a lieu lorsque les consommateurs utilisent leur compte chez leur fournisseur de réseaux mobiles comme source de fonds pour effectuer une opération.

le cas des opérations par carte de débit sont régies par la *Truth in Lending Act* (le règlement Z). Ainsi, une certaine ambiguïté pourrait exister à l'égard de la protection des consommateurs pour divers types d'opérations de paiement mobile, même si un seul organisme est responsable de l'application de la loi fédérale. En résumé, à cause de la complexité relative du cadre réglementaire, les experts ne savent pas trop au juste comment les consommateurs seront protégés.

La complexité de la réglementation pourrait aussi entraîner des lacunes dans le cadre de protection des consommateurs. Contrairement aux cartes de débit ou de crédit, les cartes prépayées polyvalentes rechargeables ont été assujetties uniquement à des normes volontaires de l'industrie. Ces cartes semblent être la source de fonds privilégiée par les consommateurs non bancarisés dans le cadre des paiements mobiles (Board of Governors of the Federal Reserve System, mars 2012; Braunstein, 29 mars 2012). À part les jeunes âgés de 18 à 24 ans, les consommateurs non bancarisés ou sous-bancarisés ont été les premiers à adopter la technologie de paiement mobile, et ces deux segments de la population se chevauchent beaucoup. Les cartes prépayées peuvent être une option intéressante pour les consommateurs, bancarisés ou non, qui souhaitent gérer leurs dépenses et éviter de recourir au crédit. Les groupes de défense des droits des consommateurs ont dit s'inquiéter de la prolifération des cartes prépayées polyvalentes rechargeables. Ces cartes ciblent surtout ceux qui n'ont pas d'antécédents en matière de crédit ou qui ont une mauvaise cote de crédit; or ces personnes possèdent peu d'expérience et de connaissances et sont moins en mesure de se protéger contre des conditions d'utilisation abusives, notamment en ce qui concerne les frais de transaction, de consultation de solde, d'inactivité, d'activation, de refus et de découvert, lesquels peuvent faire l'objet d'une information trompeuse (Susswein, 2012). Comme la popularité des paiements mobiles se confirme, il pourrait être nécessaire d'essayer d'améliorer la littératie financière des consommateurs non bancarisés pour qu'ils connaissent les risques et les avantages de ces cartes. Le CFPB envisage d'étendre aux cartes prépayées polyvalentes rechargeables l'application des règles prévues au règlement E concernant la protection des consommateurs, ce qui pourrait être une mesure efficace pour combler cette lacune du cadre de réglementation.

2.2.2. Obstacles à l'application de la réglementation, à la conformité aux exigences réglementaires et à l'entrée sur le marché

Le deuxième problème mis en lumière dans la littérature est le risque que la complexité croissante de la réglementation crée des obstacles à la conformité aux exigences réglementaires, à l'application de la réglementation et à l'entrée sur le marché. Alors que les organismes de réglementation prennent des mesures pour régler les questions soulevées par les paiements mobiles, certains observateurs ont soulevé trois préoccupations précises : a) plutôt que de protéger les consommateurs, la réglementation – dont l'application est déjà difficile – pourrait devenir encore plus difficile à appliquer; b) la complexité accrue de la réglementation pourrait peser sur les nouvelles et les petites entreprises, qui pourraient ne pas avoir les connaissances ou les ressources financières requises pour s'y conformer; c) une nouvelle réglementation pourrait créer des obstacles à l'entrée des entreprises sur le marché des paiements mobiles ou avantager certaines entreprises plutôt que d'autres, ce qui pourrait freiner l'innovation et le développement (Brown, 2012). Ces préoccupations expliquent probablement la prudence dont on fait preuve aux États-Unis à l'égard de la réforme de la réglementation.

Les entreprises les plus sensibles à la complexité de la réglementation semblent être les concepteurs d'applications logicielles et les jeunes entreprises qui créent bon nombre des nouvelles plateformes de paiement mobile. Ces entreprises souvent n'ont pas d'expérience en matière de conformité aux règles de protection des consommateurs de produits et services financiers. Souvent, elles n'ont pas non plus l'habitude de faire affaire avec les organismes de réglementation du gouvernement fédéral et des États. De manière générale, les concepteurs d'applications logicielles qui souhaitent se lancer sur le marché des paiements ont deux choix : a) créer un partenariat stratégique avec une institution financière, ce qui allège le fardeau réglementaire, mais signifie partager les recettes ou b) obtenir la supervision directe par les organismes de réglementation pertinents et investir beaucoup de temps et d'argent dans l'acquisition et le maintien des droits de permis dans les 50 États (Brown, 2012). Dans les deux cas, les sommes en jeu sont importantes, ce qui explique pourquoi de nombreuses jeunes entreprises ne parviennent même pas à se lancer. D'autres font faillite à cause du fardeau que représente le maintien des droits de permis ou le partage des recettes. Certaines autres ne réussiront vraisemblablement pas à acquérir les permis dans les 50 États ou à se conformer entièrement à toute la réglementation fédérale pertinente (Crowe, Kepler et Merritt, 2012).

Selon les observateurs, ce qu'il faut retenir, c'est qu'il ne semble y avoir aucune raison valable d'accroître la complexité de la réglementation, mais que le faire entraîne une série de coûts (Brown, 2012). Les obstacles à l'entrée sur le marché des concepteurs et des jeunes entreprises pourraient freiner l'innovation et réduire la concurrence. Si le niveau de conformité des intervenants de l'industrie à la réglementation diffère d'un État à l'autre, il pourrait en être de même du niveau de protection des consommateurs. Certaines sources de paiement pourraient être acceptées dans certains États, mais pas dans d'autres. Si les intervenants de l'industrie ne réussissent pas à se conformer à la réglementation ou à obtenir les permis requis, la réglementation existante pourrait par conséquent être plus difficile à appliquer. Cela pourrait aussi faire en sorte que la protection des consommateurs varie en fonction des États, de la technologie de paiement mobile ou du type de fournisseur de services financiers.

2.2.3. Règlements contradictoires

Le troisième problème soulevé par les observateurs tient au risque que les principes directeurs adoptés par divers organismes se contredisent. Un exemple pourrait être les nouvelles règles visant les transferts d'argent de personne à personne. Il se peut que ces transferts deviennent une catégorie importante de paiement mobile. La technologie mobile pourrait stimuler la concurrence, ce qui pourrait faire baisser les frais de transaction assez élevés imposés actuellement sur les envois d'argent. Ces frais n'ont toujours pas diminué, mais grâce à cette nouvelle possibilité de transférer de l'argent avec un appareil mobile, les consommateurs disposent toutefois d'un mode de transfert de fonds moins risqué que l'argent comptant, qui peut être facilement volé, endommagé ou perdu (Richard, 2012). Les organismes de réglementation souhaitent encourager l'essor des transferts mobiles. En 2009, au Sommet du G8 de L'Aquila, les chefs d'État ont donné leur aval à l'objectif du « 5 en 5 », soit de faire passer le coût moyen des transferts de fonds à 5 p. 100 d'ici cinq ans, contre 10 p. 100 à l'heure actuelle, en favorisant la diffusion d'information, la transparence, la concurrence et la collaboration entre partenaires (Cirasino et Ratha, 2009). Les organismes de réglementation sont aussi conscients du fait que les transferts de fonds de personne à personne pourraient intéresser ceux qui souhaitent effectuer des transferts illicites. Enfin, les règles

adoptées pour surveiller les transferts mobiles illicites pourraient être en contradiction avec les lois sur la protection de la vie privée.

L'évolution des paiements mobiles de personne à personne présente un intérêt pour le FinCEN parce que ceux-ci pourraient servir au blanchiment d'argent, au trafic de stupéfiants ou d'armes ou encore au financement d'organisations terroristes. Les paiements mobiles accélèrent et facilitent beaucoup les transferts de fonds. Les paiements mobiles de personne à personne permettent une « désintermédiation » plus sophistiquée, c'est-à-dire la répartition des transferts entre plusieurs personnes et dans plusieurs territoires. La désintermédiation pourrait attirer ceux qui se livrent à des opérations financières criminelles. Il est déjà difficile de surveiller les transferts d'argent illicites. Il est probable que la désintermédiation rende plus difficiles encore la détection et la surveillance de ces transferts d'argent, étant donné qu'ils ne sont plus rattachés aux marchés locaux (Hughes, 10 juillet 2012).

Par ailleurs, les transferts mobiles de personne à personne pourraient être plus faciles à surveiller que les transferts traditionnels. Les paiements mobiles laisseront en effet beaucoup de traces électroniques. Ces traces pourraient être utilisées pour améliorer la surveillance des opérations et l'application de la loi. Les efforts du CFPB pour modifier la réglementation sur les transferts de fonds visaient à rapprocher les États-Unis de l'objectif de faire passer le coût des transferts à 5 p. 100 d'ici cinq ans). La future réglementation sur les paiements mobiles de personne à personne devra établir un juste équilibre entre la nécessité de divulguer et de conserver adéquatement les renseignements et la possibilité d'effectuer des transferts plus efficaces et plus économiques pour favoriser le développement mondial, ainsi que la nécessité de protéger les renseignements personnels des utilisateurs. Force est de constater que ces objectifs ne sont pas nécessairement compatibles entre eux. Selon les experts, les nouvelles règles du CFPB sur les transferts de fonds internationaux établissent un juste équilibre entre la surveillance des opérations et la protection de la vie privée, mais il se peut qu'elles n'entraînent pas une baisse des frais de transaction étant donné que le fardeau réglementaire est plus important, ce qui pourrait réduire la concurrence et accroître les coûts administratifs (Richard, 2012).

2.3. Interopérabilité

L'interopérabilité s'entend de la capacité des organisations de collaborer et de la capacité des systèmes de fonctionner ensemble. Il y a interopérabilité lorsque les règles, les normes ou les pratiques au point d'interaction entre les systèmes (p. ex. interfaces informatiques) ou les organisations sont comprises et convenues de telle sorte que ces systèmes ou organisations fonctionnent ou travaillent ensemble de façon relativement harmonieuse. L'interopérabilité peut se manifester à divers niveaux. Les appareils mobiles sont interopérables d'un certain nombre de façons. Par exemple, tous respectent les protocoles de communications régissant les services de courrier électronique et de messagerie texte. Ils ne sont pas interopérables à d'autres égards, notamment lorsque les systèmes d'exploitation sont différents (p. ex. BlackBerry 10 OS, iOS d'Apple et Android de Google).

Le marché des paiements mobiles compte une grande diversité d'entreprises : fabricants d'appareils mobiles, entreprises de télécommunications ou exploitants de réseaux mobiles, banques et fournisseurs de services financiers, fournisseurs de services de gestion de données ou gestionnaires de services de confiance (« trusted service managers »), grandes sociétés Internet (p. ex. Google) et concepteurs

d'applications logicielles. Ces entreprises ont des intérêts divergents et n'ont que peu collaboré entre elles, mais chacune joue un rôle important dans le bon fonctionnement des systèmes de paiement mobile.

Les organismes de réglementation des États-Unis essaient de trouver un juste équilibre entre stimuler la concurrence et faciliter la collaboration. Cela nécessite entre autres de déterminer le niveau d'interopérabilité que devraient avoir les systèmes de paiement mobile. Une interopérabilité accrue pourrait améliorer l'expérience client en multipliant les endroits où les consommateurs pourraient acheter des produits et services avec leur appareil mobile et en standardisant la technologie dont les consommateurs ont besoin pour effectuer des paiements mobiles. En revanche, une interopérabilité moindre pourrait accroître l'essor des technologies propriétaires, ce qui pourrait stimuler la concurrence et l'innovation et offrir plus de choix aux consommateurs.

Vu l'évolution rapide de la technologie de paiement mobile, les organismes de réglementation ont facilité la mise sur pied du Mobile Payments Industry Workgroup (MPIW, groupe de travail de l'industrie du paiement mobile), en vue de mettre au point les règles, les normes et les pratiques qui constitueront le fondement de l'interopérabilité. Le MPIW est formé d'un grand nombre d'intervenants, représentatifs des principaux acteurs de l'industrie, comme AT&T, la Bank of America, First Data Corporation, Google, PayPal, Visa et Walmart, qui ont été rassemblés par les succursales de la Banque fédérale de réserve de Boston et d'Atlanta. Une assez grande proportion des intervenants de l'industrie s'entendent pour dire que l'interopérabilité au point de vente est souhaitable. La communication en champ proche est une série de protocoles communs qui permettent aux appareils mobiles de transmettre de l'information aux terminaux des marchands pour faciliter les opérations de paiement mobile. Les opinions semblent toutefois diverger davantage sur d'autres aspects de la technologie de paiement mobile, comme le stockage des données et la sécurité.

2.3.1. Point de vente

Le MPIW a recommandé que les organismes de réglementation participent au processus de mise au point d'un système ouvert de paiement mobile. Il propose l'application de règles communes et l'utilisation de plateformes ouvertes dans la mesure nécessaire pour permettre une expérience client intégrée (Continie, Crowe, Merritt, Oliver et Mott, 2011). Dans un monde idéal, selon le MPIW, l'interopérabilité des systèmes de paiement mobile ressemblerait beaucoup à celle des réseaux actuels de cartes de crédit dans le monde. Pour y arriver, il faudrait adopter une série de normes communes pour permettre une communication intégrée entre les diverses sources de paiement (p. ex. cartes de crédit, cartes de débit, cartes prépayées), les plateformes de paiement mobile (p. ex. Google Wallet), les chambres de compensation automatisée, les gestionnaires de données ou gestionnaires de services de confiance, les exploitants de réseaux mobiles et les terminaux de point de vente. En ce qui concerne la protection des consommateurs, pour atteindre cet objectif, il faudra harmoniser le cadre réglementaire régissant les diverses sources de paiement qui sont intégrées sur les plateformes de paiement mobile. Des normes communes seront aussi nécessaires pour la gestion sécuritaire des renseignements personnels et la sécurité des opérations aux points de vente (Continie, Crowe, Merritt, Oliver et Mott, 2011). Toutefois, les membres du MPIW s'accordent généralement pour dire que les lignes directrices de la réglementation devraient pour l'instant se limiter à l'interopérabilité au point de vente.

Pour accroître la sécurité des paiements mobiles, le MPIW affirme qu'il est important de rendre la technologie interopérable au point de vente. Cela est particulièrement vrai dans le cas des paiements mobiles par communication en champ proche, qui ont connu la croissance la plus rapide et ont été au centre des recommandations du MPIW. Au début, il y avait lieu de croire que les paiements par carte de crédit effectués par communication en champ proche, sans contact, étaient moins sûrs que ceux faits à l'aide de la technologie à puce et authentifiés ensuite par la signature du consommateur ou un numéro d'identification personnel (Wack, 2012a). Ce risque perçu était compensé par la valeur maximale relativement faible des opérations sans contact. Comme il est désormais possible d'effectuer des paiements sans contact avec des appareils mobiles dont les capacités s'apparentent à celles des ordinateurs portatifs, les paiements mobiles permettent aux points de vente des niveaux de sécurité que ne peuvent égaler les autres formes de paiement. La sécurité des paiements mobiles peut être assurée par la vérification des signatures électroniques dans d'immenses bases de données, la vérification dynamique, la biométrie et les reçus électroniques (Andrei, Rusu, Diaconescu et Dinescu, 2011; Oosting, 2012). Il faut tenir les appareils mobiles à 10 cm des terminaux, et un code chiffré temporaire est généré pour chaque opération, à la fin de laquelle il expire. Bref, les paiements mobiles peuvent être très sécuritaires. Toutefois, certains observateurs avancent qu'il faut, pour que ce soit possible, clarifier les responsabilités qu'ont les organismes de réglementation, les autorités de surveillance, les intervenants de l'industrie et les marchands les uns envers les autres ainsi qu'envers les consommateurs.

2.3.3. Éléments sécurisés

Il a été plus difficile de faire l'unanimité au sujet de l'interopérabilité de la technologie utilisée pour stocker les données des consommateurs. Les paiements mobiles nécessitent et génèrent des renseignements sur les consommateurs. Les plateformes de paiement mobile par communication en champ proche recourent à des puces de chiffrement appelées *éléments sécurisés*. L'élément sécurisé est une puce inviolable qui stocke les renseignements de l'utilisateur (p. ex. numéros d'identification personnels, justificatifs d'identité des cartes et des comptes, historiques des transactions). L'élément sécurisé est distinct du système d'exploitation, du matériel et de la mémoire du téléphone mobile et est conçu pour ne permettre qu'aux applications de confiance (p. ex. Google Wallet) d'accéder aux données de l'utilisateur du téléphone cellulaire (Ghag et Hegde, 2012). L'élément sécurisé peut essentiellement se présenter sous trois formes : a) il peut être « intégré » dans le matériel de l'appareil mobile; b) il peut être stocké sur la carte SIM de l'appareil mobile; c) il peut être stocké dans certaines cartes mémoire (p. ex microSD), qui contiennent aussi des antennes de communication en champ proche et qui peuvent être achetées et insérées dans les appareils mobiles. Les trois conceptions comportent certains avantages et certains risques au chapitre de la sécurité. Par ailleurs, selon les experts, il importe tout autant que les organismes de réglementation examinent de quelle manière ces différentes options de sécurité tendent à favoriser des intervenants de l'industrie différents (Ghag et Hegde, 2012).

Il semble que l'entreprise qui contrôle l'élément sécurisé contrôlera aussi les données générées portant sur les achats et sur les historiques des opérations, ce qui pourrait lui faire bénéficier des meilleurs taux de rendement. Ce n'est pas toujours le cas des fabricants d'appareils mobiles. Ces derniers sont séduits par l'intégration des éléments sécurisés dans le matériel des appareils mobiles, du fait qu'il y a alors une forte incitation pour les propriétaires des appareils à acheter des modèles plus récents pour pouvoir

bénéficier des améliorations apportées aux plateformes de paiement mobile. Les banques et les institutions financières, quant à elles, préfèrent que les éléments sécurisés se trouvent dans les cartes mémoire (p. ex. microSD) parce qu'ainsi elles pourraient remettre à leurs clients des cartes propriétaires des succursales, puis collecter et gérer les données produites par les paiements mobiles. Les concepteurs d'applications logicielles, comme Google, penchent plutôt pour l'intégration de l'élément sécurisé dans le téléphone; en effet, de cette façon, ils peuvent avoir prise sur les traces électroniques laissées par les consommateurs, lesquelles révèlent les habitudes de consommation de ces derniers dans les historiques d'opérations (Ghag et Hegde, 2012). Les exploitants de réseaux mobiles, en revanche, sont favorables à l'installation de l'élément sécurisé dans la carte SIM. Les principaux avantages techniques de cette conception sont que les exploitants de réseaux mobiles peuvent assurer la sécurité des utilisateurs par voie hertzienne (« over the air ») grâce à leur puissante technologie et qu'il leur est possible, dans le cas d'appareils perdus ou volés, de verrouiller ou de déverrouiller à distance les cartes SIM lorsque le propriétaire les avertit de la perte ou du vol (Ghag et Hegde, 2012). Le revers de la médaille en ce qui concerne cette conception, c'est qu'elle permet à un seul type d'intervenant, les exploitants de réseaux mobiles, d'avoir une emprise extraordinaire sur les données des consommateurs. Comme nous le verrons ci-après, il semble que certains exploitants de réseaux mobiles souhaitent user de leur poids pour empêcher les abonnés d'avoir accès aux plateformes de paiement mobile proposées par des concurrents.

2.3.4. Dans quelle mesure les portefeuilles électroniques sont-ils sécuritaires?

Tout comme les fabricants d'appareils mobiles, certains intervenants de l'industrie comme Google sont plutôt favorables à l'intégration de l'élément sécurisé dans l'appareil mobile. L'avantage de cette conception pour la sécurité, d'un point de vue objectif, est que les données des consommateurs sont protégées par chiffrement en tout temps, sur le support de stockage et lorsqu'elles sont en traitement. Toutefois, selon les spécialistes de la sécurité, les appareils mobiles n'ont qu'une capacité relativement limitée en matière de chiffrements complexes (Hoog, 2011). La puissance de traitement des appareils est limitée et la capacité de stockage des éléments sécurisés est négligeable (Hoog, 2011). Voilà pourquoi le Google Wallet stocke à l'extérieur de l'élément sécurisé les historiques d'opérations, les soldes de compte, le crédit disponible, les dates d'expiration – presque tout sauf le NIP et les 12 premiers chiffres de la carte de crédit. Le risque de vol de données personnelles en est ainsi accru (Hoog, 2011).

Android est le système d'exploitation qui fait fonctionner la majorité des appareils mobiles. Par conséquent, il est devenu la cible de choix pour les applications malveillantes, les virus et les chevaux de Troie qui peuvent être installés par des tiers dans les appareils mobiles pour voler des données, endommager l'appareil ou l'utiliser à des fins non autorisées (p. ex. des achats frauduleux). Une étude de portée limitée a permis de recueillir 1 200 échantillons d'applications Android malveillantes entre août 2010 (au lancement d'une nouvelle version du système d'exploitation) et octobre 2011. Les auteurs de cette étude estiment que les applications malveillantes pour appareils mobiles ciblent Android dans une proportion d'environ 46 %. Le meilleur logiciel de sécurité mobile a détecté seulement 79,6 % des applications malveillantes, tandis que le pire n'en a détecté que 20,2 % (Zhou et Jiang, 2012).

Les cartes prépayées Google Wallet se sont révélées vulnérables : leur utilisation non autorisée était possible sans les routeurs, tout comme l'installation d'applications malveillantes. Des spécialistes de la sécurité ont montré que lorsque les données sont effacées à partir du menu des paramètres du

portefeuille électronique, quiconque l'utilise par la suite se fait demander d'entrer un nouveau NIP. Ce défaut de conception a rendu très vulnérables à la fraude les fonds stockés sur la carte prépayée Google Wallet (Ghag et Hegde, 2012). L'antenne de communication en champ proche donne aussi étonnamment prise aux « attaques de proximité ». S'ils se trouvent dans un rayon de 10 cm, les pirates informatiques peuvent s'introduire dans l'interface poste-à-poste et récupérer l'historique de navigation, les fichiers et les documents de l'utilisateur du téléphone cellulaire (Miller, 2012).

Google a répondu à ces menaces à la sécurité d'un certain nombre de façons. La carte prépayée Google Wallet a cessé d'être offerte en octobre 2012 lorsque le défaut de conception susmentionné a été rendu public. La menace d'attaques de proximité est réduite du fait que l'antenne de communication en champ proche est éteinte lorsque l'écran est éteint. Il faut entrer un NIP de quatre chiffres pour voir les cartes dans le portefeuille électronique de Google lorsque l'application est verrouillée, et le verrouillage est automatique après une courte période d'inutilisation. Si l'appareil mobile est volé, l'utilisateur peut désactiver à distance (en ligne) l'application Google Wallet pour empêcher son utilisation pour des achats frauduleux. De plus, la dernière version du Google Wallet a une conception hybride faisant appel au nuage informatique et à l'élément sécurisé : les justificatifs d'identité des cartes de crédit et de débit sont stockés sur les serveurs Internet de Google plutôt que dans l'appareil, à l'extérieur de l'élément sécurisé. Seuls les numéros d'identification de la carte prépayée et du portefeuille électronique sont stockés dans le téléphone, tous deux dans l'élément sécurisé. De manière générale, la sécurité de la plateforme de paiement mobile de Google, sur le plan technique (point de vue objectif), est en réalité assez élevée. Les possibles menaces à la sécurité examinées ci-dessus ont diminué la sécurité perçue (point de vue subjectif) à l'égard du Google Wallet. Certains critiques ont exhorté Google à réagir au fait qu'elle est perçue comme une grande société avec une mentalité d'entreprise « en démarrage » qui ne prend pas assez au sérieux la sécurité de ses utilisateurs. Même configuré adéquatement, le Google Wallet demeure vulnérable aux attaques par des personnes qui connaissent le propriétaire et qui peuvent ainsi soit récupérer le NIP de ce dernier, soit accéder à l'appareil mobile au moment où il est déverrouillé (Ghag et Hegde, 2012).

Initialement, Verizon Wireless ne permettait pas à ces clients de télécharger les mises à jour du système d'exploitation Android requises pour utiliser le Google Wallet. Verizon a invoqué les problèmes de sécurité susmentionnés, mais des observateurs de l'industrie ont soupçonné que deux préoccupations plus importantes étaient en cause. Tout d'abord, Verizon est partie à une coentreprise appelée « Isis Mobile Wallet » avec AT&T Mobility et T-Mobile USA. Le portefeuille électronique Isis a été annoncé avant le Google Wallet, mais la plateforme Isis n'a été lancée sur les marchés-tests d'Austin et de Salt Lake City qu'en octobre 2012 (Olivarez-Giles, 2012). C'est plutôt Google qui a été la première à proposer son portefeuille électronique sur le marché américain. En septembre 2011, le Google Wallet a été lancé sur un seul modèle de téléphone, le Sprint Nexus S 4G, qui fonctionnait sous le système d'exploitation de Google (Android) et n'était offert que chez Sprint. Deuxièmement, la concurrence s'est dite préoccupée de la façon dont Google utilise une technologie propriétaire pour traiter les données de l'utilisateur du portefeuille. Grâce à cette technologie, Google aurait la mainmise sur les données. Des observateurs de l'industrie ont supposé que le retard de Verizon à permettre le Google Wallet sur ses réseaux était motivé par le fait que la société n'avait pas réussi à conclure une entente convenable de partage des revenus et des données, étant donné qu'AT&T et T-Mobile permettaient le Google Wallet sans avoir soulevé les

mêmes préoccupations à l'égard de sa sécurité. Verizon a depuis changé sa position et permet désormais les mises à jour requises du système d'exploitation Android sur les appareils mobiles sur son réseau. Cet exemple montre comment la sécurité et l'interopérabilité sont liées.

2.4. Protection des renseignements personnels : collecte des données et protection des consommateurs

De toutes les questions soulevées par les paiements mobiles relativement au cadre existant des règles de protection des consommateurs, la question de la protection des renseignements personnels est sans doute la plus complexe. Pour les intervenants de l'industrie, les revenus des plateformes de paiement mobile proviennent essentiellement de trois sources : a) la vente de logiciels d'application ou de plateformes de paiement mobile; b) les frais de transaction pour le traitement des paiements mobiles; c) la collecte de données et la publicité. Comme des options de paiement sécuritaires, efficaces et fiables sont bien établies aux États-Unis, les recettes générées par la collecte de données et la publicité ciblée devraient être un élément important des modèles d'affaires des fournisseurs de services de paiement mobile (Hughes, 10 juillet 2012). La croissance de nouvelles formes de publicité et de traitement des données pourrait poser des difficultés aux organismes de réglementation chargés de la protection des consommateurs de produits et services financiers.

Google, par exemple, permet actuellement aux consommateurs de télécharger son portefeuille gratuitement. La société n'impose pas de frais aux consommateurs pour traiter leurs paiements (Google, 2013). Son modèle d'affaires semble conçu pour gagner des parts de marché. Il donne aussi à penser qu'il permet de générer des revenus importants grâce à la collecte de données sur les consommateurs effectuant des paiements mobiles. Les données peuvent être utilisées pour envoyer de la publicité personnalisée aux consommateurs directement sur leur appareil mobile. Google compte réaliser des profits dans la voie du paiement mobile grâce à la collecte de données et à la publicité. Ce modèle est assez prometteur pour que cette société soit disposée à renoncer pour le moment aux revenus qu'elle pourrait tirer des frais de transaction et de la vente de leur application logicielle.

Les problèmes de protection des renseignements personnels liés aux paiements mobiles sont complexes. Les organismes de réglementation des États-Unis semblent vouloir trouver un juste équilibre entre deux responsabilités. Premièrement, il est de leur devoir de protéger le droit des consommateurs de refuser la collecte de leurs données et d'être informés adéquatement de la façon dont leurs données sont collectées, traitées et utilisées. D'autre part, les organismes de réglementation estiment qu'ils sont responsables de faciliter le développement de l'écosystème de paiement mobile et de donner aux consommateurs plus de choix en permettant aux intervenants de l'industrie de se disputer les bénéfices commerciaux. Du point de vue des consommateurs, la publicité personnalisée ou « intelligente » (p. ex. publicité ciblée comportementale) facilitée par la collecte de données peut être vue comme un avantage que possèdent les paiements mobiles par rapport aux modes de paiement traditionnels. Certains consommateurs seront attirés par les paiements mobiles parce qu'ils trouveront pratique de recevoir de la publicité adaptée à leurs goûts et à leurs préférences. Certains observateurs ont fait remarquer que, pour protéger les consommateurs tout en leur permettant de participer à ce nouveau type de marketing, il pourrait s'avérer nécessaire de modifier les règles sur la protection et la divulgation

des renseignements personnels. Adapter le cadre réglementaire actuel ou mettre au point de nouvelles règles sur la protection des renseignements personnels sera une tâche exigeante. De nombreux intervenants de l'industrie, organismes de réglementation, voies de transmission des données et dépôts de données doivent être pris en considération. En outre, il existe différentes façons de collecter, de traiter et d'utiliser les données destinées à des applications commerciales et publicitaires. Une réforme du cadre réglementaire actuel pourrait ne pas suffire. Certains font valoir qu'un nouveau code pourrait être nécessaire pour protéger adéquatement les renseignements personnels des consommateurs (King et Jessen, 2010).

2.4.1. Collecte de données et publicité ciblée comportementale

Pour comprendre les difficultés que pourraient poser les paiements mobiles pour les organismes de réglementation des États-Unis, il est crucial d'examiner brièvement en quoi diffèrent les études de marché sur des segments de consommateurs et le profilage des consommateurs. Les annonceurs recourent depuis longtemps aux analyses statistiques et aux études de marché pour cibler des segments précis de la population. Toutefois, King et Jessen (2010) ont constaté quatre changements importants dans les analyses de la consommation et le marketing de consommation. Ensemble, ces changements représentent un nouveau paradigme, appelé « publicité ciblée comportementale », qui prendra de l'importance à mesure que progressera la technologie de paiement mobile.

Premièrement, les paiements mobiles permettent aux intervenants de l'industrie de collecter de nouveaux types de données et de les conjuguer à des renseignements conventionnels recueillis sur les consommateurs. Habituellement, lorsque les consommateurs utilisent Internet, ils laissent des traces électroniques qui révèlent leur comportement de navigation, leurs habitudes de consommation et leurs caractéristiques démographiques (p. ex. nom, adresse postale, numéro de téléphone). Les appareils mobiles peuvent générer d'autres renseignements personnels au sujet de la géolocalisation, des déplacements, des abonnements à la téléphonie mobile, de la facturation et de l'historique des appels. De plus, les gens gardent dans leur appareil mobile leurs contacts, messages, itinéraires et photos ainsi que divers biens de consommation, comme de la musique. Bref, les paiements mobiles généreront un éventail beaucoup plus large de données sur les consommateurs, données qui peuvent être combinées à des données collectées de manière conventionnelle, pour les besoins des études de marché et de la publicité (King et Jessen, 2010).

Deuxièmement, les nouvelles technologies dites « intelligentes » seront utilisées pour tirer ces renseignements des dépôts de données. L'analyse des données sera effectuée par ordinateur automatiquement, ou presque automatiquement, avec une intervention humaine limitée. Le profilage des consommateurs ne dépend pas de l'intelligence humaine, mais plutôt de programmes informatiques conçus pour extraire automatiquement des données des dépôts. Ces programmes peuvent mettre en lumière des corrélations inattendues entre les données sur les caractéristiques des consommateurs et les types de comportement de consommation (King et Jessen, 2010).

Troisièmement, ces analyses informatisées peuvent permettre d'établir des profils de consommation très personnalisés, ce qui pourrait faire s'estomper la distinction entre renseignements personnels identifiables et données anonymes. Selon la loi américaine sur la protection de la vie privée, les

renseignements personnels identifiables s'entendent de données qui peuvent être utilisées pour identifier, trouver ou contacter une personne donnée. Les données anonymes ne permettent pas l'identification. L'analyse des données basée sur le profilage des consommateurs est beaucoup plus personnalisée que celle basée sur les études de marché sur des segments de consommateurs. Le volume de données très précises collectées à partir des appareils mobiles est plus important, et des techniques plus poussées sont utilisées pour extraire ces données des dépôts. Le profilage fondé sur les données de paiement mobile permet de cibler la publicité pour des personnes précises en fonction de leurs caractéristiques personnelles particulières. Les études de marché sur des segments de consommateurs permettent de développer les connaissances sur de grandes catégories de consommateurs. Le profilage de consommateurs, quant à lui, permet d'établir de manière plus précise les comportements, les préférences, les goûts et les attitudes des personnes faisant l'objet du profilage. Il est alors possible de dégager des corrélations entre les caractéristiques et le comportement d'un consommateur et le profil d'autres consommateurs pour créer des catégories de marché plus subtiles. Toutefois, l'unité de base de la publicité ciblée rendue possible par les paiements mobiles sera les profils individuels des consommateurs, non pas les catégories de marché. La publicité faite à l'aide de la technologie de paiement mobile ciblera des personnes en particulier plutôt qu'un type de personne (King et Jessen, 2010).

Quatrièmement, le profilage des consommateurs basé sur les opérations de paiement mobile ne sera pas limité à l'analyse descriptive. Le but de la publicité ciblée comportementale est de prédire et de moduler le comportement de consommateurs individuels en temps réel. Les sites Web qui affichent de la publicité installent souvent des « témoins » sur l'ordinateur des utilisateurs pour créer un profil de leurs habitudes de navigation. Ce profil est utilisé pour générer de la publicité encore plus convaincante. La principale innovation rendue possible par les paiements mobiles est le fait que les annonceurs peuvent joindre les consommateurs directement au moment où ils effectuent des achats ou pensent à le faire. Ce type de publicité comportementale en temps réel pourrait véritablement influencer les consommateurs alors qu'ils s'apprêtent à faire un choix (King et Jessen, 2010). En voici un exemple anodin : un après-midi, au moment où il prend sa pause, un travailleur remarque dans son téléphone cellulaire qu'un bon de réduction lui a été envoyé pour un nouveau produit proposé au café du coin, bon qu'il peut utiliser s'il fait son achat habituel. Il s'agirait d'un exemple moins anodin si la publicité portait sur des produits controversés, comme des aliments prêts à manger, et ciblait des consommateurs souffrant d'une maladie chronique comme le diabète de type 2. Pour résumer, la croissance des paiements mobiles rendra possible l'essor de la publicité ciblée comportementale. Ce nouveau type de publicité table sur la collecte d'un grand éventail de données sur les consommateurs, des technologies informatiques automatisées qui extraient et analysent ces données et l'établissement de profils de consommation très personnalisés, et vise à prédire et à moduler le comportement des consommateurs ciblés.

2.4.2. Protection des données et autonomie et liberté personnelles

Les paiements mobiles et la publicité ciblée comportementale soulèvent deux questions liées à la protection des renseignements personnels et de la vie privée des consommateurs : a) la protection des données, b) l'autonomie et la liberté personnelles (King et Jessen, 2010). En ce qui concerne la protection des données, la plupart des inquiétudes concernent la collecte et la divulgation des renseignements

personnels identifiables, c'est-à-dire les données qui permettent d'identifier, de contacter ou de trouver une personne donnée. Les consommateurs doivent être avisés adéquatement de la collecte de leurs renseignements personnels identifiables à des fins commerciales pour pouvoir y consentir en toute connaissance de cause ou la refuser. La publicité ciblée comportementale expose aussi les personnes à de nouveaux risques liés au vol d'identité et à la sécurité générale de leurs renseignements personnels identifiables. Le profilage rendu possible par les paiements mobiles pourrait entraîner la création d'un réseau de surveillance envahissant et pas du tout transparent, à mesure que le comportement des consommateurs est de plus en plus suivi et surveillé et les données s'y rapportant sont traitées. Enfin, les consommateurs risquent d'être exposés à des pratiques commerciales injustes ou trompeuses (p. ex. prix discriminatoires), alors que les annonceurs tentent de moduler les choix des consommateurs au moment où ils s'apprêtent à les faire (King et Jessen, 2010).

Les paiements mobiles pourraient poser des difficultés aux organismes de réglementation responsables de la protection de l'autonomie personnelle. Ces difficultés sont en partie attribuables au fait que la publicité ciblée comportementale peut créer une asymétrie de l'information entre les annonceurs et les consommateurs. Le risque est plus grand que les consommateurs soient manipulés s'ils ne savent pas quels renseignements sur eux sont collectés, quelles entreprises les recueillent et comment elles les utilisent. Par exemple, ce type de publicité pourrait être utilisé pour cibler des populations vulnérables en leur proposant des aliments malsains, des médicaments ou des prêts personnels à taux d'intérêt élevé (King et Jessen, 2010). Les consommateurs ont besoin de savoir pourquoi ils reçoivent ces nouvelles publicités pour pouvoir prendre des décisions éclairées et responsables.

2.4.3. Le cadre réglementaire visant la protection de la vie privée des consommateurs

La législation américaine reconnaît la protection de la vie privée au sens large de l'identité individuelle, ainsi que le droit fondamental d'être protégé contre les intrusions commerciales ou gouvernementales dans la vie privée. Cependant, certains experts ont avancé qu'il n'existait pas de cadre réglementaire exhaustif qui protège les consommateurs pour ce qui est de la collecte de leurs renseignements personnels, de la publicité ciblée comportementale ou des pratiques commerciales manipulatrices. Selon certains observateurs, la complexité du cadre réglementaire posera un problème au moment d'adapter les règles sur la protection des renseignements personnels et de la vie privée pour qu'elles tiennent compte des paiements mobiles (Brown, 2012; King et Jessen, 2010). Les États-Unis n'ont pas d'organisme unique qui disposerait des pleins pouvoirs pour la surveillance et l'application de la législation sur la protection des renseignements personnels. Les règlements applicables varient en fonction de l'intervenant de l'industrie, du type de données, de la façon dont les données sont entreposées et de l'utilisation qui est faite des renseignements (Brown, 2012). La Federal Trade Commission (FTC) dispose de la plupart des pouvoirs de supervision relativement aux règles visant à protéger la confidentialité des données sur les consommateurs. Ces règles sont complexes. Par exemple, la *Children's Online Privacy Protection Act* (COPPA, 1998) prévoit des normes minimales dans le cas de la collecte de données sur les enfants de moins de 13 ans. La collecte de données sur les consommateurs est régie par la *Gramm-Leach-Bliley Act* (*Financial Services Modernization Act of 1999*). Les données collectées par les agences d'évaluation du crédit à propos des antécédents des consommateurs en matière de crédit doivent être gérées en conformité avec la *Fair Credit Reporting Act* (FCRA, 1970) et la *Fair and Accurate*

Credit Transactions Act (FACTA, 2003). L'application de ces quatre lois est surveillée par la FTC. Toutefois, les règles visant les données collectées par les fournisseurs de soins de santé sont prévues au titre II de la *Health Insurance Portability and Accountability Act* (HIPAA, 1996) et désignées comme les dispositions de « simplification administrative »; ces dispositions sont appliquées par l'Office for Civil Rights du département de la Santé et des Services sociaux.

Les lois des États ajoutent à la complexité de la situation, tout comme les liens entre les lois fédérales et celles des États. Quarante-six États ont adopté des lois qui exigent que les consommateurs soient avisés lorsque des renseignements les concernant sont transmis à des tiers. Il se peut que le département de la Justice ait aussi compétence pour l'application des lois visant la divulgation des données sur les consommateurs à des tiers. En Californie, la définition des renseignements personnels identifiables est plus large et cet État interdit aux commerçants d'exiger ou de demander de tels renseignements personnels au point de vente. Le CFPB a intérêt, dans une certaine mesure, à surveiller les lois sur la protection des renseignements personnels du fait que les règlements Z et E sont maintenant de son ressort. Enfin, certaines sociétés comme Visa et MasterCard ont leurs propres règles interdisant aux marchands de divulguer à des tiers non inscrits certains renseignements sur les opérations (Brown, 2012). Si un principe général guide le cadre réglementaire actuel, c'est celui selon lequel les consommateurs doivent savoir quels renseignements les concernant sont collectés à des fins commerciales et avoir un droit de regard à ce sujet (Brown, 2012).

2.4.4. La loi protégera-t-elle les renseignements personnels des consommateurs dans la voie du paiement mobile?

La complexité des règles peut rendre difficile la protection des renseignements personnels des consommateurs. Par exemple, la *Telecommunications Act* (1996) donne à la Federal Communications Commission (FCC) le pouvoir de protéger les consommateurs lorsque les exploitants de réseaux mobiles collectent leurs données, comme les historiques d'appels sortants et la géolocalisation. Les données collectées par les exploitants de réseaux mobiles au sujet des appels téléphoniques d'un consommateur (p. ex. l'heure, la date, le destinataire et la durée), l'information concernant l'abonnement au réseau du consommateur et les renseignements qui figurent habituellement sur la facture de téléphone de ce dernier sont stockées dans le dépôt de renseignements exclusifs sur les consommateurs des réseaux (*Customer Proprietary Network Information*). Ces renseignements exclusifs sont régis par la FCC. Toutefois, la définition des données personnelles prévue par la loi exclut le numéro de téléphone, l'adresse et le nom des abonnés aux services mobiles, ce qui signifie que ces renseignements sont très peu protégés. En outre, les entreprises autres que les exploitants de réseaux mobiles, les annonceurs et les sites Web qui extraient des données du dépôt de renseignements exclusifs sur les consommateurs des réseaux ne sont pas surveillés par la FCC à l'heure actuelle (King et Jessen, 2010). Il s'agit là d'une grave lacune dans le cadre existant de protection des consommateurs.

Certains observateurs ont aussi fait valoir que l'autoréglementation pourrait décourager les intervenants de l'industrie d'adopter des politiques détaillées visant la protection des renseignements personnels des consommateurs. De manière générale, aux États-Unis, les entreprises ont le droit de commercialiser leurs produits comme bon leur semblent, pourvu qu'elles ne se livrent pas à des pratiques commerciales trompeuses et n'nfreignent pas la loi (King et Jessen, 2010). C'est la Federal Trade Commission (FTC) qui

a compétence sur les pratiques commerciales trompeuses. Elle n'a pas défini le profilage des consommateurs ni la publicité ciblée comportementale comme étant injustes ou trompeurs. Elle n'a pas non plus demandé aux entreprises qui font du profilage d'adopter un ensemble circonscrit de politiques sur la protection des renseignements personnels et de la vie privée. Ainsi, pour les entreprises, le meilleur moyen de réduire au minimum les risques d'être poursuivies en justice consiste à ne pas adopter de politiques pour la protection des renseignements personnels et de la vie privée, avec des règles détaillées sur le profilage des consommateurs ou sur la publicité ciblée. Si les entreprises décident d'adopter de telles politiques, elles seront certes portées à veiller à ce que le libellé leur accorde une grande latitude pour générer et partager des données, créer des profils et faire de la publicité ciblée comportementale. Selon certains observateurs, cette orientation pourrait nuire à la protection des renseignements personnels et de la vie privée des consommateurs (King et Jessen, 2010).

3. L'Union européenne

Les taux d'adoption du paiement mobile dans l'Union européenne (UE) n'ont pas atteint les sommets prévus par les experts. L'évolution vers le commerce électronique, les paiements virtuels et les appareils mobiles intelligents a créé les conditions optimales dans le marché pour que le recours aux paiements mobiles se répande (Ondrus, Lyytinen et Pigneur, 2009). En 2010, seulement 7,1 millions de personnes avaient recours aux paiements mobiles en Europe de l'Ouest par rapport à 62,8 millions dans la région Asie-Pacifique (Commission européenne, 2012).

Quatre grands points seront examinés ici. Premièrement, les organismes de réglementation souhaitent faciliter la croissance des paiements mobiles, car ils y voient un moyen de faire progresser l'harmonisation du marché des paiements au détail dans l'UE. Deuxièmement, le travail d'harmonisation des produits de paiement, des spécifications techniques, des normes d'interopérabilité et de l'infrastructure de paiement mobile présente des difficultés. Ce défi a été relevé grâce à l'autoréglementation volontaire des intervenants dans le cadre du projet de l'espace unique de paiements en euros (Single Euro Payments Area, SEPA). Troisièmement, des lois contraignantes, relativement exhaustives, ont été adoptées pour assurer le respect de la vie privée des consommateurs et la protection des renseignements personnels, parallèlement à la directive sur la protection des données personnelles et à la directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après « directive sur la vie privée et les communications électroniques »). Enfin, on examinera la directive sur les services de paiement, qui établit le cadre juridique servant à déterminer quelles entités peuvent offrir des services de paiement et à fixer leur conduite.

3.1. Objectifs réglementaires : propager le paiement mobile pour créer un « marché unique » des paiements de détail

Après plus de dix ans d'essais et de projets pilotes, le principal enjeu pour les organismes de réglementation demeure la façon de favoriser une adoption accrue des paiements sans espèces et des paiements électroniques dans l'UE. Les organismes de réglementation veulent savoir comment stimuler la croissance de l'écosystème de paiement mobile. La Commission européenne a pour but de créer un « marché unique » intégré pour les paiements de détail dans l'UE. Elle veut que les paiements de détail puissent se faire au-delà des frontières politiques des pays aussi facilement que les gens et les entreprises traversent ces mêmes frontières. Parallèlement, les observateurs ont fait remarquer que les règles en place sont déjà assez complexes. On craint que l'adoption d'une nouvelle réglementation sur les paiements mobiles accroisse la complexité des règles sans en améliorer l'efficacité. La nouvelle réglementation pourrait aussi étouffer l'innovation ou favoriser indûment un type d'intervenants du secteur aux dépens des autres. (Commission européenne, 2012a).

Les objectifs des organismes de réglementation qui supervisent les paiements mobiles dans l'UE et les difficultés que ces organismes doivent surmonter sont semblables à celles de leurs contreparties aux États-Unis. Il existe cependant d'importantes différences. L'UE a réalisé des progrès en vue de l'harmonisation des paiements de détail en créant un cadre réglementaire contraignant et détaillé pour protéger les consommateurs qui utilisent le mode de paiement mobile. L'UE a aussi précisé le statut et les obligations des fournisseurs de services de paiement non bancaires, qui sont d'importants acteurs dans

la prestation des services de paiement mobile. Les organismes de réglementation de l'UE désirent encourager la croissance des paiements mobiles, car ils estiment que ce travail contribuera à l'atteinte de l'objectif plus large qu'est la création d'un marché unique des paiements de détail dans toute l'UE.

3.2. Harmonisation : le SEPA, l'autoréglementation et les frais de transaction

3.2.1. Le SEPA

Pour tenter d'harmoniser la réglementation sur les paiements de détail, l'UE a opté pour un système d'autoréglementation volontaire du commerce électronique et des voies de paiement mobile. Le projet du SEPA (espace unique de paiements en euros) en vue d'améliorer l'autoréglementation est dirigé par le secteur bancaire européen par l'intermédiaire du Conseil européen des paiements et de la Banque centrale européenne (Banque centrale européenne, 2006). L'objectif du SEPA est la création d'un ensemble de règles et de lignes directrices concernant les normes techniques, l'interopérabilité et la sécurité. Ces règles seront ensuite adaptées et adoptées par les gouvernements nationaux dans le but de créer un « marché unique » sûr et efficace pour les paiements de détail. Les progrès dans la poursuite de ce but ont été inégaux.

Il existe quatre cadres établis pour le projet SEPA qui se rapportent à l'autoréglementation des paiements mobiles. Le SEPA a présenté un cadre réglementaire paneuropéen pour les transferts de fonds (le SEPA Credit Transfert) en 2008 ainsi qu'un cadre visant les modalités de paiement par débit direct (le SEPA Direct Debit) en 2009. Le Parlement européen a adopté ces cadres en février 2012 (Conseil européen des paiements, 2012).[4] Dans les cas où la source des fonds servant aux paiements mobiles est une carte de crédit ou de débit, ces paiements seront régis par le cadre du SEPA visant les paiements par carte (le SEPA Cards Framework), qui a été présenté pour la première fois par le Conseil en 2006. La plupart des intervenants du secteur sont d'avis que le SEPA Credit Transfert, le SEPA Direct Debit et le SEPA Cards Framework suffisent à la réglementation des paiements mobiles (Commission européenne, 2012a). Toutefois, l'Union européenne a adopté un nouvel instrument visant expressément les paiements mobiles. Les Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines (MCP IIG) ont été publiées en novembre 2011. Elles visent à faciliter et à favoriser l'élaboration de normes communes et l'adoption de pratiques exemplaires communes pour les intervenants du secteur. À ce jour, le taux d'observation volontaire du SEPA Cards Framework et des lignes directrices (MCP IIG) n'est pas à la hauteur du niveau de conformité du secteur au SEPA Credit Transfert et au SEPA Direct Debit (Commission européenne, 2012; Jones, 2009).

3.2.2. Autoréglementation

Les cadres du SEPA visent à donner aux intervenants du secteur les outils pour se réglementer eux-mêmes (Conseil européen des paiements, 2012). Les MCP IIG recommandent des engagements à prendre sur le

[4] Le SEPA Direct Debit et le SEPA Credit Transfert ont été adoptés par l'UE en février 2012 par la prise du règlement (UE) n° 260/2012 et du règlement d'exécution (CE) n° 924/2012. Les 27 États membres avaient jusqu'au 1er février 2014 pour rendre leurs normes nationales conformes au SEPA Credit Transfert et au SEPA Direct Debit. Les États qui ne sont pas membres de l'UE, mais qui adhèrent au SEPA (c.-à-d. la Suisse, Monaco, Mayotte et Saint-Pierre et Miquelon) ont jusqu'au 1er mars 2016 pour rendre leurs lois nationales conformes aux deux cadres (Conseil européen des paiements, 2012).

plan de l'interopérabilité et des normes techniques. L'adhésion à ces lignes directrices se fait sur une base volontaire pour les émetteurs de cartes, les banques acquéreuses et les gestionnaires de services de confiance, et pour ce qui concerne les modalités de paiement par carte. La priorité est de simplifier les paiements par carte et de les rendre plus sûrs pour les consommateurs et les commerçants. Les organismes de réglementation veulent également faciliter la concurrence et la collaboration entre les intervenants du secteur. En vue d'atteindre ces objectifs, les lignes directrices du SEPA visant les paiements mobiles sont très semblables à la « feuille de route » présentée par le Mobile Payments Industry Workgroup aux États-Unis. Les deux documents préconisent des normes ouvertes et l'interopérabilité au lieu de solutions de paiement mobile « fermées » en propriété exclusive. L'une des différences est que le SEPA ne recommande pas l'interopérabilité sur le plan de l'élément sécurisé. On préfère établir des normes communes à l'échelle de l'application logicielle se trouvant sur l'appareil mobile du consommateur. Autrement dit, les consommateurs devraient pouvoir avoir accès à l'ensemble de leurs services de paiement mobile sur un seul appareil mobile (Conseil européen des paiements, 2012).

Selon les observateurs, il existe plusieurs difficultés liées aux initiatives du projet SEPA. Tout d'abord, les mesures de protection ainsi que les procédures que doivent suivre les consommateurs et les commerçants qui procèdent à des opérations de détail sans utiliser d'argent comptant varient au sein de l'UE. L'adaptation des lignes directrices du SEPA par les différents pays a empêché l'harmonisation complète. Une certaine ambiguïté persiste quant au sens à donner à la conformité. Ainsi, le niveau de conformité du secteur demeure inégal (Jones, 2009). Il existe aussi une possibilité que les consommateurs ignorent ou comprennent mal les droits et les protections dont ils jouissent lorsqu'ils effectuent des paiements de détail dans un autre pays de l'UE. Le premier point de contact dans le cas d'une opération autorisée peut varier en fonction de la plateforme de paiement mobile, du fournisseur de services de paiement, de la banque émettrice ou acquéreuse et de la réglementation du pays au point de vente.

Des experts ont indiqué qu'il est aussi possible que la complexité de la réglementation ait nui à la réalisation de l'objectif premier du Conseil européen des paiements, à savoir la création d'un « marché unique » intégré pour les paiements de détail. À l'heure actuelle, il est plus facile pour les gens et les entreprises de traverser les frontières au sein de l'UE que pour les paiements de détail par carte de se faire au-delà des frontières d'un pays. Malgré l'existence de directives, de normes et de pratiques exemplaires à l'échelle de l'Europe, l'intégration du marché des paiements sans espèces accuse un retard. Les cartes de débit, par exemple, ne sont généralement pas acceptées comme mode de paiement pour l'achat de biens et de services à l'extérieur de l'État membre dans lequel se trouve l'institution financière du consommateur.

La très grande majorité des intervenants de l'industrie qui ont répondu au livre vert de la Commission européenne sur la réglementation des paiements mobiles avançaient que le manque d'intégration n'est pas attribuable à un manque de collaboration entre les entreprises (Commission européenne, 2012a). Certaines banques ont affirmé que les lois sur la concurrence n'étaient pas compatibles avec les lignes directrices du SEPA sur l'interopérabilité. La plupart des fournisseurs de services de paiement soutiennent que l'intégration du système de paiement de détail a été ralentie par le nombre important de différences dans les règles d'un pays à l'autre. Les membres de l'UE ont des normes, des règles, des protocoles de règlement et de compensation, des exigences en matière de traitement et des spécifications techniques

pour les terminaux qui différent, ainsi que des systèmes de cartes, des permis, des applications et des ententes bilatérales sur les frais d'interchange qui sont différents (Commission européenne, 2012a). Même si l'harmonisation obligatoire ne remporte que peu de soutien, il semble évident que les instruments d'autoréglementation n'ont pas encore permis de créer un marché intégré pour les consommateurs.

Troisièmement, la complexité du paysage réglementaire signifie que le taux d'utilisation frauduleuse des cartes de paiement demeure relativement élevé, en particulier dans le cas des paiements mobiles à distance (Commission européenne, 2012). Étant donné que les cartes de crédit servent de source de fonds pour une grande partie des paiements mobiles, le fait que le contexte actuel permet la persistance d'un taux relativement élevé de fraude par carte de crédit est une préoccupation importante.

Enfin, même si la plupart des acteurs conviennent que le secteur devrait se réglementer lui-même, l'absence d'un organe décisionnel indépendant pour superviser l'élaboration des cadres du SEPA a été largement critiquée. La plupart des intervenants du secteur ont dit craindre que le SEPA favorise indûment les intérêts et les priorités des banques (Commission européenne, 2012a). Certains des nouveaux fournisseurs de services de paiement ont avancé que les fournisseurs déjà établis interdisaient l'accès à l'infrastructure de règlement des opérations. Les nouveaux joueurs sont plus enclins à favoriser une réglementation contraignante, une harmonisation obligatoire et des niveaux supérieurs d'interopérabilité (Commission européenne, 2012a). Les gouvernements nationaux et les banques de moindre envergure ont dit craindre que les réseaux nationaux de paiement par débit, de faible coût, soient expulsés du marché par les deux réseaux dominants de cartes de crédit. Autrement dit, Visa et MasterCard pourraient en pratique exercer un duopole sur les paiements de détail, si l'harmonisation des règles ne tient pas compte des intérêts de tous les intervenants du secteur. Les commerçants veulent pouvoir choisir leur banque acquéreuse dans le réseau de cartes ou veulent que le SEPA serve à créer une banque acquéreuse centrale (Commission européenne, 2012a). Les consommateurs, les commerçants et les concepteurs de logiciels ont soutenu que la structure de gouvernance du SEPA devrait être modifiée. Ils veulent que l'autorité suprême soit confiée à la Commission européenne et à la Banque centrale européenne plutôt qu'au Conseil européen des paiements, qui, selon eux, favorise les intérêts des banques. Les sociétés émettrices de cartes de crédit et les fournisseurs de services de paiement ont fait valoir que la participation des intervenants devrait être mieux équilibrée et qu'ils devraient être mieux représentés.

3.2.3. Frais de transaction

L'une des raisons qui explique le retard de l'adoption du SEPA Cards Framework est la controverse entourant la nécessité de réglementer les frais de transaction, en particulier les commissions d'interchange. Chaque fois qu'un consommateur paie à l'aide d'une carte – à moins que ladite carte ne fasse partie du « réseau fermé » de cartes prépayées du commerçant – une série de frais de transaction sont échangés entre le titulaire de la carte, le commerçant, la banque et l'exploitant du réseau de cartes de paiement.

La plupart des réseaux de cartes de paiement mettent en jeu quatre parties (Borestam et Schmiedel, 2011). Il y a quatre types de frais dans ce système. Tout d'abord, le consommateur qui est titulaire de la carte versera des paiements mensuels à sa banque émettrice ainsi que des intérêts sur tout solde en

souffrance et, dans certains cas, des frais annuels. Ensuite, le commerçant qui accepte le paiement par carte du consommateur paie des frais appelés frais de service du commerçant à sa banque acquéreuse[5]. Troisièmement, lorsque la banque émettrice règle l'achat du titulaire de la carte en envoyant le paiement à la banque acquéreuse du commerçant, la banque émettrice reçoit une commission d'interchange de la banque acquéreuse[6]. Quatrièmement, l'exploitant du réseau de cartes de paiement perçoit des « frais de commutation » ou « cotisations » auprès de la banque acquéreuse et de la banque émettrice (Borestam et Schmiedel, 2011).

Les frais prélevés sur les opérations dans les réseaux de cartes de paiement sont devenus controversés dans l'UE pour un certain nombre de raisons. Comme les consommateurs optent de plus en plus pour les paiements électroniques par carte, les revenus que tirent les banques et les exploitants de réseaux de cartes de paiement des frais de transaction ont connu une croissance marquée, ce qui a attiré plus d'attention. On note aussi certaines préoccupations quant à la concurrence, car les grilles tarifaires sont généralement établies par les exploitants de réseaux de cartes de paiement et le marché est dominé par deux acteurs (c.-à-d. Visa et MasterCard) (Martin, 2010).

Ce sont les commissions d'interchange qui ont fait l'objet de l'attention la plus grande. Pareille attention est partiellement attribuable aux importantes différences dans les commissions d'interchange d'un pays à l'autre. Les décideurs de l'UE sont aussi préoccupés par le fait que les commissions d'interchange prélevées sur les opérations sont plus élevées lorsque la banque émettrice et la banque acquéreuse ne se trouvent pas dans le même pays. Les décideurs voient ces différences et ces frais supplémentaires comme des obstacles à la création d'un « marché unique » intégré des paiements de détail (Commission européenne, 2012). Pour leur part, les exploitants de réseaux de cartes de paiement affirment que ces écarts et ces frais supplémentaires s'expliquent par les coûts de règlement des opérations à l'intérieur d'un même pays et entre deux pays différents (Commission européenne, 2012a; Haas, 2012). La Cour générale de l'UE a décidé en mai 2012 de fixer les commissions d'interchange sur les règlements transfrontaliers à 0,2 p. 100 dans le cas des opérations par cartes de débit et à 0,3 p. 100 dans celui des paiements par carte de crédit (Commission européenne, 2012c).

Le débat concernant la réglementation des commissions d'interchange est aussi lié aux questions de protection des consommateurs et de paiement mobile pour d'autres raisons. Tout d'abord, les spécialistes ont constaté que le système de cartes de paiement à quatre parties peut faire grimper les commissions d'interchange ainsi que les frais de service imposés aux commerçants lorsque le niveau de concurrence augmente. Les exploitants de réseaux de cartes de paiement cherchent souvent à attirer les consommateurs et à les convaincre d'utiliser leurs cartes en offrant des programmes de récompenses de plus en plus généreux. Étant donné que ce sont les exploitants de réseaux de cartes de paiement qui fixent la grille tarifaire pour les frais de transaction, ils peuvent récupérer les coûts des programmes de

[5] Étant donné que la banque acquéreuse débitera les frais de service du commerçant de la somme totale de l'achat au moment de rembourser le commerçant, ces frais sont souvent appelés « taux d'escompte du commerçant ».
[6] La commission d'interchange est aussi appelée « commission d'interchange multilatérale » lorsque la grille tarifaire est établie par les exploitants de réseaux de cartes de paiement pour un ensemble de banques acquéreuses et émettrices différentes. Si la grille tarifaire est établie dans un contrat entre une banque émettrice et une banque acquéreuse, on l'appelle « commission d'interchange bilatérale ».

récompenses généreux en haussant les frais que paient les commerçants pour faire assurer le règlement des paiements par carte. Les commissions d'interchange et les frais de commutation sont en fin de compte tirés des frais de service des commerçants. Les contrats entre les commerçants, les banques acquéreuses et les exploitants de réseaux de cartes de paiement interdisent généralement aux commerçants d'établir une distinction entre les cartes de crédit haut de gamme au coût plus élevé et les cartes de base d'un même réseau. En se concurrençant pour attirer davantage de consommateurs, les réseaux de cartes peuvent faire grimper les coûts liés à l'acceptation des paiements électroniques par carte pour les commerçants (Evans et Mateus, 2011; Hayashi et Weiner, 2005). Étant donné que la concurrence dans le marché des cartes de paiement a généralement mené à une hausse des commissions d'interchange et des frais de service imposés aux commerçants, il est possible que les frais augmentent également en raison de la lutte que se livrent les fournisseurs de services de paiement mobile pour attirer les consommateurs vers une nouvelle plateforme de paiement.

Les commerçants ont présenté de nombreuses plaintes quant à l'équité des frais de transactions (Evans, 2011). Dans l'UE, des groupes de défense des consommateurs et des associations de commerçants ont soutenu que les tarifs imposés sur les opérations ne peuvent être justifiés en raison du faible coût d'entretien et d'exploitation du réseau servant à régler les opérations de débit et les opérations par carte de crédit. Il est important de reconnaître que ce type d'interfinancement qui fait en sorte que les commerçants financent les coûts du mode de paiement choisi par le consommateur est représentatif des marchés bilatéraux. Même si le marché des cartes de crédit est concentré, les exploitants doivent toujours concurrencer d'autres formes de paiement (p. ex. les paiements en espèces ainsi que les paiements par carte de débit, par carte en circuit fermé et par carte prépayée). La nécessité de faire en sorte que les commerçants continuent d'accepter les cartes de crédit pourrait aussi exercer une pression à la baisse sur les frais de transaction. Néanmoins, il est important de tenir compte du fait que la concurrence sur le marché entraînée par l'arrivée des services de paiement mobile ne débouchera pas nécessairement sur des frais de transaction moindres pour les commerçants. L'augmentation des frais de transaction peut aussi se traduire par des prix plus élevés pour les consommateurs, dans la mesure où les commerçants peuvent leur transférer les coûts croissants liés aux frais de service qui leur sont imposés. Ce transfert n'est pas particulièrement transparent, car bon nombre de consommateurs ignorent les frais de transaction liés aux différentes cartes de paiement et l'effet que ces frais peuvent avoir sur les prix (Haas, 2012). Il peut aussi y avoir interfinancement entre diverses catégories de consommateurs, étant donné que seuls les titulaires de cartes de paiement haut de gamme profiteront de l'amélioration des programmes de récompenses, mais que les commerçants majorent les prix pour tous les consommateurs (Bergevin et Zywicki, 2012). Ce phénomène a été interprété comme un transfert régressif de richesse. En effet, les consommateurs qui ont un revenu inférieur et qui paient en espèces, par carte de débit ou à l'aide d'une carte de crédit ordinaire financent les récompenses plus généreuses qu'obtiennent les titulaires de cartes haut de gamme; or ces derniers satisfont aux critères d'obtention des cartes offrant des récompenses, qui, dans la plupart des cas, exigent un revenu supérieur. Les organismes de réglementation pourraient souhaiter être attentifs à ces phénomènes d'interfinancement au fur et à mesure que les paiements mobiles gagnent en popularité.

Enfin, on craint de plus en plus que les commissions d'interchange et les contrats qui fixent les grilles tarifaires constituent des obstacles à l'entrée sur le marché de fournisseurs de services plus petits et plus novateurs, arrivés récemment sur le marché. Cela pourrait réduire la concurrence sur le marché des services de paiement et ainsi nuire aux commerçants, aux consommateurs et à l'économie en général. Les obstacles à l'entrée peuvent également réduire l'innovation. Les paiements électroniques ne sont pas seulement importants pour faire progresser l'harmonisation. Les décideurs de l'UE estiment aussi qu'il s'agit d'un moyen plus efficace de faire circuler l'argent dans l'économie. Des poursuites pour pratiques monopolistiques ont été intentées aux États-Unis contre des exploitants de réseaux de cartes de paiement pour le compte de gros détaillants. Les responsables de la réglementation antitrust de l'UE ont fait enquête sur les grilles des commissions d'interchange de Visa pendant plus de quatre ans et ont déposé un avis d'opposition préliminaire en juillet 2012. La Commission européenne soutient que les commissions d'interchange multilatérales de Visa limitent la concurrence entre les banques et contreviennent aux règles de l'UE interdisant les cartels (Commission européenne, 2012b). On a avancé que les obstacles à l'entrée sur le marché nuiraient à l'expansion des paiements mobiles, tandis que les pratiques monopolistiques pourraient empêcher les modes de paiement mobile d'offrir au consommateur un choix à faible coût. D'un autre côté, la participation de Visa et de MasterCard pourrait aussi favoriser l'adoption des paiements mobiles par les consommateurs, car ces exploitants de réseaux de cartes de paiement ont acquis une réputation en matière de sécurité et de fiabilité.

3.3. Protection des données et des renseignements personnels

La collecte et le traitement des données sur les consommateurs et leurs opérations font partie intégrante de la prestation des services de paiement mobile. La réglementation juridique sur la protection des données et les droits à la vie privée dans l'UE est très détaillée. Le cadre de l'UE est un peu plus strict que les lignes directrices de l'OCDE (Greenleaf, 2012). Deux directives protègent les données personnelles des consommateurs dans le cas des paiements mobiles : la directive sur la protection des données personnelles et la directive sur la vie privée et les communications électroniques. Toutes deux doivent être enchâssées par les États membres dans leurs lois nationales (King et Jessen, 2010). En outre, la plupart des membres de l'UE ont aussi signé la Convention 108, un traité international sur la protection des données (Conseil de l'Europe, 1981). L'article 8 de la *Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales* (Convention de sauvegarde) accorde aux individus d'autres droits quant au respect de la vie privée, sauf si l'ingérence est nécessaire à la sécurité nationale, à la sécurité publique ou au bien-être économique (Convention de sauvegarde, 2010). Enfin, la *Charte des droits fondamentaux de l'Union européenne* (Charte de l'UE) précise à l'article 8 que « [t]oute personne a droit à la protection des données à caractère personnel la concernant », que « [c]es données doivent être traitées loyalement » et que « [t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ». (Charte de l'UE, 2000). Ces traités guident les travaux actuels de modernisation de la protection de la vie privée et des données. Le présent examen portera surtout sur la directive sur la protection des données personnelles et la directive sur la vie privée et les communications électroniques en raison de leur niveau de précision et de leur pertinence en ce qui concerne la stratégie de l'UE pour protéger les consommateurs qui ont commencé à faire des paiements mobiles.

La directive sur la protection des données personnelles est un cadre réglementaire fondé sur des principes que les pays de l'UE sont tenus d'adopter, mais qu'ils peuvent adapter dans une certaine mesure (Directive 95/46/EC). La directive est constituée de huit principes de base. Le premier principe, qui est aussi le principe directeur, englobe les notions de respect de la loi et de loyauté. Si le premier terme est explicite, la loyauté est interprétée comme signifiant que les entités qui recueillent, traitent et contrôlent les données personnelles (c.-à-d. les « responsables des données ») doivent tenir compte de l'intérêt de la personne (c.-à-d. la « personne concernée ») sur laquelle des données sont recueillies. Les notions de respect de la loi et de loyauté ont préséance sur les principes qui suivent (Bygrave, 2000).

Le second principe est celui du « respect des finalités »; il signifie que les données personnelles peuvent seulement être recueillies à des fins légitimes. La raison de la collecte doit être déterminée et rendue explicite. Les données ne peuvent être utilisées que d'une manière compatible avec le but énoncé. (King et Jessen, 2010). Le troisième principe est celui de la « juste mesure » ou de la « proportionnalité », ce qui signifie que la somme de données recueillies doit être limitée à ce qui est nécessaire pour atteindre le but initial de la collecte. Au quatrième rang, on trouve le principe de la « qualité de l'information », selon lequel les données recueillies et traitées doivent être raisonnablement exactes, à jour et valables en regard de ce qu'elles sont censées représenter. Le principe de « qualité » plaide aussi en faveur d'un système de contrôle périodique de la validité des données. Le cinquième principe se rapporte au droit de « participation et de contrôle » d'une personne relativement aux données qui sont recueillies à son sujet. Il existe deux types de dispositions. D'une part, il existe des règles obligeant les responsables des données à rendre disponibles aux autorités de surveillance compétentes des renseignements de base sur leurs modes de collecte et de traitement des données, ainsi que des règles qui obligent les organismes de réglementation à verser ces renseignements dans un registre public. D'autre part, il existe des lignes directrices qui obligent les responsables des données à communiquer directement avec les personnes concernées pour les informer des procédures de collecte et de traitement des données les concernant et obtenir leur consentement éclairé avant d'aller de l'avant. Le sixième principe indique que les responsables des données ne peuvent divulguer des données à des tiers que dans des circonstances très précises. Au strict minimum, le consentement éclairé de la personne concernée est nécessaire avant que les données la concernant puissent être divulguées à de tierces parties. Le septième principe exige des responsables des données qu'ils prennent toutes les mesures nécessaires et raisonnables pour garantir la sécurité des données en prévenant leur destruction accidentelle, leur consultation non autorisée ou leur altération. Enfin, le huitième principe concerne le « caractère délicat » des données et oblige les responsables des données à prendre des mesures exceptionnelles pour veiller le plus rigoureusement possible à la sécurité des données particulièrement délicates (Bygrave 2000; King et Jessen, 2010).

Le principal cadre réglementaire de protection de la confidentialité des renseignements transmis par voie électronique dans l'UE est la directive sur la vie privée et les communications électroniques (2002/58/EC). Cet instrument élargit les mesures de protection offertes par la directive sur la protection des données personnelles (95/46/EC). La directive sur la vie privée et les communications électroniques vise principalement les exploitants de réseaux mobiles et les fournisseurs d'accès Internet. Elle les oblige à se conformer à tous les principes fondamentaux applicables de la directive sur la protection des données personnelles, comme celui du « consentement éclairé ». Plus précisément, la directive vise à faire en sorte

que les annonceurs obtiennent le consentement éclairé des consommateurs avant de leur envoyer des publicités non sollicitées sur leurs appareils mobiles. La définition que donne la directive des renseignements permettant l'identification d'une personne englobe les données recueillies sur les appareils mobiles des consommateurs se rapportant au trafic Internet, à l'historique de navigation et à la géolocalisation. Pour pouvoir s'en servir, les exploitants de réseaux mobiles et les fournisseurs d'accès Internet doivent transformer les données concernant le trafic et la géolocalisation en données anonymes, aviser les consommateurs que ces données sont recueillies et traitées, et obtenir leur consentement éclairé. Enfin, la directive donne aux consommateurs le droit de refuser l'installation sur leurs appareils mobiles de témoins HTTP, de logiciels de suivi et d'autres dispositifs qui peuvent y être placés pour recueillir des données sur leurs activités sur les réseaux des exploitants de réseaux mobiles et des fournisseurs d'accès Internet.

Des lacunes ont été repérées dans la directive sur la vie privée et les communications électroniques. Par exemple, elle n'aborde pas certaines formes de marketing de personne à personne. Les publicités envoyées indirectement par l'intermédiaire de personnes physiques ou morales plutôt que directement aux consommateurs seront probablement exclues des règles sur la protection de la vie privée. La directive ne s'appliquera pas aux personnes qui envoient des communications électroniques à d'autres consommateurs pour leur vendre des biens ou des services qu'ils possèdent ou qu'ils ont achetés auparavant (King et Jessen, 2010). Cette exclusion pourrait ouvrir la voie à de la publicité non sollicitée de tierces parties, un type de marketing qui s'est répandu récemment. La publicité envoyée indirectement par les consommateurs qui utilisent les fonctions « J'aime » ou « Recommander à un ami » sur le populaire site de média social Facebook serait exclue. Il existe aussi une certaine ambiguïté quant à la forme que prendrait l'application conjointe de la directive sur la protection des données personnelles et de la directive sur la vie privée et les communications électroniques à des questions comme les « identificateurs secondaires », les protocoles Internet et les témoins HTTP.

3.4. La directive sur les services de paiement, les institutions non bancaires et les établissements de paiement

La directive sur les services de paiement (2007/64/EC) est une initiative de réglementation de la direction générale Marché intérieur et services de la Commission européenne. La directive a deux grands objectifs. Tout d'abord, elle est conçue pour faciliter la création d'un marché unique pour les paiements de détail électroniques dans l'ensemble de l'UE. En vue d'atteindre cet objectif, la directive élimine les obstacles à l'entrée sur le marché et garantit aux nouveaux fournisseurs de services de paiement (p. ex. les détaillants, les exploitants de réseaux mobiles et les expéditeurs de fonds) un accès équitable au marché. Pour y parvenir, elle vise l'harmonisation du contexte réglementaire dans les 27 États membres.

La directive crée une autorisation de portée générale pour les établissements de paiement, nouveau terme utilisé pour désigner les intervenants de l'industrie sur le marché des paiements mobiles lorsqu'ils font l'objet d'une supervision et d'une réglementation. Les établissements de paiement doivent respecter les lignes directrices concernant les fonds propres et la gestion des risques, et présenter une demande d'autorisation dans les États membres de l'UE où ils comptent offrir des services de paiement. Après s'être acquittés de ces obligations, ils peuvent exercer leurs activités dans tous les pays de l'Union européenne

sans autre autorisation d'un organisme de surveillance. Il existe trois types d'établissements dans l'écosystème de paiement mobile qui sont visés par le nouveau cadre régissant les établissements de paiement : i) les expéditeurs de fonds, ii) les exploitants de réseaux mobiles et iii) les fournisseurs de services complets en matière de paiement, tels les systèmes de cartes de crédit. Les établissements de paiement ont le droit d'exercer trois activités principales : i) fournir des services de change; ii) exercer des activités en tant que fiduciaires des fonds en dépôt et iii) exploiter les systèmes de paiement (directive sur les services de paiement, 2007).

Les banques jouaient par le passé le rôle de gardiennes du système de règlement des paiements. Aujourd'hui, dans de nombreux cas, ce sont des institutions non bancaires qui gèrent les réseaux et l'infrastructure servant au traitement et au règlement des opérations. (Weiner, Bardford, Hayashi, Sullivan, Wang et Rosati, 2007). Actuellement, ce sont les institutions non bancaires qui jouent le rôle le plus important dans le traitement des opérations par carte, mais on s'attend à ce qu'elles occupent encore plus de place dans le marché des paiements de détail à mesure que le commerce électronique et les paiements mobiles prennent leur essor. L'importance croissante d'instruments comme les paiements mobiles – qui sont caractérisés par une phase presque entièrement automatisée avant la réalisation des opérations, le traitement des opérations en ligne et l'autorisation des paiements en temps réel – complexifiera la chaîne de traitement des paiements. Les banques et les institutions non bancaires devront coordonner leurs activités à de nombreuses étapes de cette chaîne. Des données personnelles de nature délicate seront transmises. La sécurité de la chaîne de traitement des opérations se mesurera à celle de son maillon le plus faible. Des observateurs préviennent que les banques pourraient être exposées à de nouveaux risques. Elles pourraient être tenues responsables de fraudes relatives aux paiements, même si les données compromises qui ont servi à commettre le crime ont été acquises à une étape de la chaîne contrôlée par une institution non bancaire (Weiner et al., 2007).

Le rôle croissant des institutions non bancaires dans le système dominant de règlement à quatre parties pourrait aussi exposer les banques à des risques d'un genre nouveau (Weiner et al., 2007). Les banques sont assujetties à des règlements stricts. Elles ont fait la preuve qu'elles pouvaient réduire au minimum les risques opérationnels et prévenir la fraude, la contrefaçon et les atteintes à la protection des données. Weiner et ses collègues font remarquer qu'il ne serait peut-être pas souhaitable d'assujettir les institutions non bancaires à un régime de réglementation aussi rigide, qui pourrait réduire les incitatifs économiques qui stimulent la concurrence et l'innovation dans le secteur des paiements électroniques de détail. Les institutions non bancaires disposent de la technologie et de l'expertise opérationnelle capables d'accroître la sécurité (Weiner et al., 2007). La directive crée une autorisation de portée générale pour les établissements de paiement pour trois raisons. Les organismes de réglementation veulent établir un juste équilibre entre la nécessité d'accroître la participation des institutions non bancaires, celle de rendre les communications plus efficaces entre les banques et les institutions non bancaires et celle d'améliorer la gestion prudentielle parmi les institutions non bancaires.

Le deuxième objectif principal de la directive est la simplification des règles concernant les droits et les obligations des utilisateurs et des fournisseurs de services de paiement (EUbusiness, 2007). La directive vise à établir un juste équilibre entre la responsabilité des commerçants et celle des consommateurs.

Des lignes directrices sur le droit des utilisateurs de refuser de payer pour des opérations frauduleuses y sont énoncées. La directive précise les conditions de remboursement des utilisateurs ainsi que le délai accordé au fournisseur de services de paiement pour y procéder. Par exemple, le « principe du montant total » définit la mesure dans laquelle les consommateurs ont le droit de se faire immédiatement rembourser la totalité de la somme en cause s'ils signalent à leur fournisseur de services de paiement une opération électronique non autorisée dans un délai de 13 mois (OCDE, 2012). La directive établit des principes de transparence selon lesquels il faut que les frais de transaction facturés par le fournisseur de services de paiement soient indiqués séparément et clairement et ne soient pas compris dans le prix des biens ou des services achetés. Les fournisseurs de services de paiement doivent aussi transmettre ou rendre accessible aux consommateurs un relevé mensuel de leurs opérations. Une autre disposition importante de la directive est celle dite du jour ouvrable suivant, qui stipule que toutes les opérations de paiement doivent avoir été réglées et conclues au plus tard le jour ouvrable suivant. Même si leurs heures d'activité peuvent varier, les fournisseurs de services de paiement doivent indiquer clairement dans leurs contrats à quel moment les ordres de paiement doivent avoir été reçus pour que la banque du destinataire du paiement puisse se faire créditer les fonds le jour ouvrable suivant (Turing, 2011).

4. La Corée du Sud et le Japon

4.1. Introduction

En ce qui concerne le taux d'adoption par les consommateurs et le volume des opérations, la Corée du Sud et le Japon sont des chefs de file à l'échelle internationale en matière de paiements mobiles (Dapp, Stobbe et Wruuk, 2012; KPMG International, 2007; OCDE, 2012). Au Japon, les transferts d'argent effectués au moyen du paiement mobile comptaient en mars 2009 pour 11,5 p. 100 du volume total des transferts électroniques d'argent. Dans ce pays, certaines banques sont autorisées à émettre de l'« argent électronique », lequel équivaut à de l'argent comptant, mais est stocké sur des « cartes à puce intelligentes », des appareils électroniques ou des serveurs à distance. Le volume des opérations faites au moyen d'argent électronique connaît une croissance rapide. En 2008, il a dépassé le nombre d'opérations faites au moyen d'une carte de débit, pour atteindre une valeur de deux mille milliards de yens en 2011. Au Japon, la vente d'appareils mobiles dotés de la technologie de communication en champ proche, nécessaire pour effectuer un paiement mobile sans contact, a atteint 64 millions d'appareils en 2009 (OCDE, 2012). À la fin août 2010, la plus importante plateforme de paiement mobile au Japon – la marque « iD » de l'exploitant de réseau mobile NTT Docomo – comptait, selon les affirmations de l'exploitant, plus de 15 millions d'abonnés (NTT Docomo, 2010).

La Corée du Sud, quant à elle, est depuis le début à l'avant-poste de l'adoption des technologies numériques. Dans toute la région Asie-Pacifique, on observe attentivement l'évolution du paiement mobile dans ce pays, où l'argent électronique est en train de devenir rapidement le principal mode de paiement dans les opérations de détail. En 2008, plus de 22,8 mille milliards de wons ont été échangés par voie électronique (KPMG International, 2007)[7]. Déjà en 2009, plus de quatre millions de personnes utilisaient chaque mois leur appareil mobile pour payer des laissez-passer de transport en commun, l'abonnement à un journal ou à un centre de conditionnement physique, de la musique et des jeux vidéo, ou encore des achats dans divers commerces. Le total de ces achats se chiffrait alors à 1,7 mille milliards de wons, soit 1,4 milliard de dollars US. Cependant, le pourcentage du volume total d'opérations en argent électronique alors effectuées au moyen d'appareils mobiles n'atteignait même pas 1 p. 100 (Sang-Hun, 2009). Comparativement à ce qui se passe dans le reste du monde, les voies de paiement mobile sont très développées en Corée du Sud et au Japon. Les organismes de réglementation ont adopté une approche prudente en ce qui concerne l'élaboration de nouveaux règlements en matière de paiements mobiles. La priorité est de favoriser l'innovation et l'entrée sur le marché de nouveaux joueurs, de même que la croissance de l'utilisation du paiement mobile.

[7] Les observateurs de l'industrie s'attendent à ce que, en Corée du Sud, les ventes d'appareils mobiles dotés de la technologie de communication en champ proche atteignent 20 millions d'appareils en 2012. Cela représenterait, à l'échelle mondiale, le plus important déploiement d'appareils mobiles dotés d'un système interopérable (c'est-à-dire non exclusif) destiné à permettre les paiements mobiles sans contact dans les points de vente (Balaban, 2012). Même si au Japon on trouve plus d'appareils dotés de la technologie de communication en champ proche en circulation sur le marché qu'en Corée (60 millions d'appareils), tous ces appareils fonctionnent sous le système « FeliCa », une technologie appartenant à Sony qui n'est pas compatible avec les appareils mobiles ni avec les lecteurs dotés de la technologie de communication en champ proche habituellement utilisés (Balaban, 2012).

La position adoptée par les organismes de réglementation au Japon et en Corée du Sud est semblable à celle adoptée aux États-Unis et dans l'Union européenne. Même si le taux d'adoption et le volume d'opérations sont plus élevés dans les deux premiers pays, on considère tout de même que le paiement mobile n'en est qu'aux premières étapes de son développement. Les organismes de réglementation semblent vouloir éviter de ralentir ce développement en imposant trop rapidement de nouveaux règlements. Récemment, la commission coréenne des communications a plutôt décidé de réunir les fournisseurs de passerelles de paiement[8], les exploitants de réseaux mobiles, les fabricants d'appareils mobiles, les exploitants de réseaux de cartes de paiement et les fabricants de terminaux de point de vente afin de créer un consortium d'intervenants de l'industrie, la Grand NFC Korea Alliance (grande alliance coréenne de la communication en champ proche). L'alliance mène ses activités en vue d'atteindre des objectifs communs comme l'augmentation du taux d'adoption des appareils dotés de la technologie de communication en champ proche et du nombre de terminaux de point de vente conçus pour les opérations mobiles, ainsi que l'accroissement de l'interopérabilité en matière de paiement mobile (Balaban, 2012). La composition et les objectifs de l'alliance sont similaires à ceux du Mobile Payment Industry Workgroup (groupe de travail de l'industrie du paiement mobile) aux États-Unis et du groupe de l'initiative SEPA (espace unique de paiement en euros) de l'Union européenne.

4.2. Paiement mobile et populations sous-bancarisées

Le développement du paiement mobile au Japon et en Corée du Sud a grandement été influencé par les besoins des personnes sous-bancarisées. Selon des études de marché menées aux États-Unis, les jeunes adultes (de 18 à 24 ans) et les populations sous-bancarisées sont ceux qui ont le plus de chances d'être parmi les premiers à adopter la technologie du paiement mobile. Il y a d'ailleurs un important chevauchement entre ces deux groupes (Braunstein, 29 mars 2012). Cependant, les caractéristiques des populations sous-bancarisées semblent varier en fonction des conditions économiques. L'industrie s'adapte donc en conséquence et cherche à répondre aux besoins de ces populations de diverses manières, tout en respectant les limites du cadre réglementaire (Board of Governors of the Federal Reserve System, mars 2012). La réglementation et l'histoire économique respectives du Japon et de la Corée du Sud ont créé des lacunes particulières en ce qui concerne la fourniture de services financiers. Les entreprises de paiement mobile qui connaissent le plus de succès sont celles qui répondent d'abord aux besoins des consommateurs sous-bancarisés.

Dans les études publiées, deux facteurs sont reconnus comme ayant façonné le développement du paiement mobile au Japon. Premièrement, les grandes banques privées jouaient traditionnellement un rôle important dans le fonctionnement des « keiretsu », c'est-à-dire les groupes d'entreprises

[8] Les fournisseurs de passerelles de paiement sont des fournisseurs de services qui offrent des applications de commerce électronique et de paiement mobile permettant d'autoriser le paiement à un marchand. Les passerelles de paiement chiffrent les données sensibles (p. ex. les renseignements de carte de crédit) afin que les renseignements puissent être transférés de manière sécuritaire du client au marchand et au responsable du traitement du paiement.

interdépendantes qui ont généralement dominé l'économie du Japon durant la seconde moitié du vingtième siècle. Deuxièmement, l'État a imposé des limites strictes quant à l'offre de crédit à court terme aux consommateurs, et ce, dans le but d'encourager les ménages à économiser. Pour ce qui est des keiretsu, de grandes banques privées sont au cœur de la structure de chacun des six plus importants. Même si l'influence des keiretsu a commencé à décliner, environ la moitié des actifs financiers personnels de la population sont toujours détenus sous forme de dépôts bancaires, le salaire de la très grande majorité des Japonais est déposé directement dans leur compte bancaire, et la plupart d'entre eux paient leurs factures au moyen du prélèvement automatique (Dapp, Stobbe et Wruuck, 2012). Autrement dit, les grandes banques privées demeurent au cœur de l'économie du Japon et de son système de règlement. Il aurait donc pu sembler logique de penser que ces banques étaient bien placées pour jouer un rôle prédominant parmi les différentes entreprises qui ont convergé vers le marché du paiement mobile. Toutefois, d'après les observateurs, les limites strictes imposées relativement à l'offre de crédit renouvelable par les banques ont fait en sorte d'empêcher ces dernières de jouer un rôle important dans l'écosystème de paiement mobile. Au Japon, les cartes de crédit fonctionnent essentiellement de la même manière que les cartes de débit en Amérique du Nord, à la différence que le solde de la carte n'est déduit automatiquement du compte bancaire du client qu'à la fin de chaque mois. Les personnes ayant besoin de crédit à court terme sont donc généralement sous-bancarisées, ou à tout le moins mal desservies par les institutions financières accréditées, ce qui pousse parfois des consommateurs solvables à se tourner vers le marché noir ou même des usuriers (KPMG International, 2007). Ce manque d'accès à un crédit à court terme sécuritaire, pratique et légal constitue l'un des principaux facteurs à l'origine de l'essor du paiement mobile. En effet, lorsque le gouvernement japonais a assoupli les restrictions liées au crédit renouvelable par l'État japonais a mené à l'apparition de nouvelles institutions financières prêtes à répondre aux besoins des clients par le biais de l'argent électronique.

Au Japon, sept entreprises dominent le marché de l'argent électronique : Waon, Nanaco, Rakuten Edy, Suica, Pasmo, ICOCA et iD (Dapp, Stobbe et Wruuck, 2012). Ces « banques itinérantes » appartiennent généralement à des compagnies de chemin de fer, des détaillants, des supermarchés et des exploitants de centres commerciaux. Elles émettent à leurs clients des cartes à puce intelligentes, ainsi que des cartes de débit ou de crédit. Toutefois, le paiement mobile sans contact se fait pratiquement juste au moyen de cartes à puce intelligentes, puisque la plupart des cartes de crédit ne sont pas « sans contact » et que les cartes de débit ne le sont pas non plus. Les exploitants de réseaux mobiles offrent généralement une fonction permettant aux cartes à puce intelligentes d'être utilisées sur les appareils mobiles. Le plus important exploitant de réseau mobile japonais est NTT Docomo. L'entreprise offre la carte à puce intelligente iD, laquelle est associée à la banque électronique iD. Il s'agit de loin de la plus importante plateforme de paiement mobile au Japon; en fait, elle jouit d'un monopole presque total sur le marché du paiement mobile au Japon. NTT Docomo réclame aux banques électroniques qui émettent les cartes à puce intelligentes iD des frais de location pour l'utilisation de la plateforme de paiement mobile. Elle prélève aussi une part des frais de transaction facturés au marchand. Ces derniers doivent également payer à l'entreprise des frais de location pour le lecteur de cartes à puce intelligentes (c'est-à-dire le terminal). Enfin, la quasi-totalité des appareils mobiles dotés de la technologie de communication en champ proche au Japon fonctionnent grâce au système FeliCa, une technologie exclusive à Sony Corporation (Balaban, 2012). Comme le paiement moyen effectué à l'aide d'une carte à puce intelligente

s'élève à 800 yens, ou 10 dollars US, ce type de carte ne rivalise pas vraiment avec les cartes de crédit émises par les banques ou encore avec les services de transfert d'argent. Néanmoins, les opérations mobiles surpassent déjà les opérations faites au moyen d'une carte de débit et sont en train de rapidement remplacer l'argent comme principale mode de paiement pour les petits achats de tous les jours dans les supermarchés, les restaurants, les dépanneurs et les terminaux de transport en commun (Dapp, Stobbe et Wruuck, 2012).

Le système japonais est unique en son genre, en ce que la quasi-totalité des paiements mobiles se fait selon un seul modèle de fonctionnement : une carte à puce intelligente émise par une banque électronique permet d'effectuer de petites opérations dans des commerces de détail par l'intermédiaire d'une plateforme de paiement mobile gérée par un exploitant de réseaux mobiles (KPMG International, 2007). D'après les spécialistes, en raison de ce système unique, le cadre réglementaire au Japon est plutôt simple. Le paiement mobile relève du ministère de l'Économie, du Commerce et de l'Industrie et la plateforme de paiement iD, appartenant à NTT Docomo, est assujettie à la réglementation sur les prêts personnels. Des limites sont par ailleurs imposées sur le montant total pouvant être accordé à un consommateur ainsi que sur le taux d'intérêt pouvant être imposé sur le crédit renouvelable consenti par l'intermédiaire du système de paiement mobile.

En Corée du Sud, le paiement mobile a connu une évolution différente. Dans les années 1990 et au début des années 2000, des exploitants de réseaux mobiles et des banques ont tenté de s'associer pour offrir des services mobiles, mais ces tentatives n'ont pas été très fructueuses. Les banques privées du pays n'occupent pas dans l'économie un rôle aussi central qu'au Japon. Selon les observateurs, la concurrence et le manque de confiance ont nui aux premiers partenariats entre institutions financières et exploitants de réseaux mobiles. Ce sont plutôt des tiers, les fournisseurs de passerelles de paiement (p. ex. Danal, Mobilans, Infohub et Inicis), qui ont été les principaux responsables du développement du système de paiement mobile (KPMG International, 2007). En Corée du Sud, c'est le segment sous-bancarisé de la population qui a été à l'origine de l'essor de cette technologie. Les jeunes désiraient avoir accès à un moyen autre que l'argent pour acheter de la musique, des vidéos, des jeux informatisés, des applications logicielles, etc. Le fonctionnement de la passerelle de paiement est plutôt simple : l'utilisateur transfère des fonds sur une carte prépayée qui est ensuite insérée dans son appareil mobile (KPMG International, 2007).

En Corée du Sud, le marché du paiement mobile est très concurrentiel. La ville de Séoul, LG CNS et la Korean Credit Card Union ont lancé la carte à puce intelligente « T-Money », qui peut être utilisée dans le système de transport en commun, les distributeurs automatiques et les dépanneurs des environs, ainsi que dans les taxis de la ville. À plus grande échelle, des exploitants de réseaux mobiles comme SKT et KT Freetel se sont associés à des exploitants de réseaux de cartes de crédit afin d'offrir un autre type de système de paiement mobile. Par exemple, SKT et Visa ont lancé un service de paiement mobile appelé « SKT Moneta ». Néanmoins, autant dans le modèle d'affaires fondé sur la passerelle que dans celui créé par l'association d'un exploitant de réseau mobile et d'un exploitant de réseau de cartes de crédit, les revenus proviennent des frais de service imposés lors des opérations. Pour les services comme SKT Moneta, des frais de 3,5 p. 100 sont ajoutés à chaque opération. Dans le cas des passerelles de paiement comme Danal, les frais de transaction sont considérablement plus élevés. En effet, pour chaque opération,

le fournisseur de la passerelle de paiement exige des frais de 3 p. 100, auxquels s'ajoutent des frais de 5 p. 100 imposés par l'exploitant de réseau mobile. Malgré cet écart, les passerelles font directement concurrence à SKT Moneta et au service de paiement mobile MasterCard offert par KT Freetel. Les fournisseurs de passerelles de paiement continuent de cibler et d'attirer principalement les jeunes, qui représentent un segment de la population qui est sous-bancarisé et mal desservi par les institutions financières traditionnelles et les réseaux de cartes de crédit (KPMG International, 2007). Contrairement au marché japonais, le marché sud-coréen du paiement mobile est diversifié et son cadre réglementaire mérite d'être examiné en détail, puisque l'objet de la réglementation dans ce pays est assez semblable au système complexe de paiement mobile qui se développe en Amérique du Nord et dans l'Union européenne.

4.3. Cadre réglementaire des paiements mobiles en Corée du Sud

En Corée du Sud, les paiements mobiles sont assujettis à deux lois. La première version de la *E-commerce Consumer Protection Act* (loi sur la protection des consommateurs en matière de commerce électronique) a été adoptée en 2002. En 2005, elle a fait l'objet d'une révision approfondie, et la nouvelle loi est entrée en vigueur le 1er avril 2006 (Blythe, 2006). Cette loi a été rédigée à la suite d'une période durant laquelle la fraude par carte de crédit était particulièrement fréquente, c'est-à-dire au lendemain de la crise économique asiatique de 1997 (KPMG International, 2007). Durant la décennie qui a suivi la crise, une stratégie nationale a été élaborée qui visait à promouvoir le commerce électronique, notamment en fournissant à l'industrie des renseignements permettant de clarifier la réglementation en matière de protection des consommateurs. En ce qui concerne les paiements mobiles, la loi sur la protection des consommateurs en matière de commerce électronique définit trois obligations. Premièrement, le consommateur doit avoir accès à tous les renseignements nécessaires à propos du vendeur ou du commerçant et, le cas échéant, à propos du fournisseur de services de paiement. Ces renseignements doivent être accessibles sur le site Web du commerçant. Le consommateur doit également avoir accès à tous les renseignements concernant la procédure de règlement des différends. Deuxièmement, le commerçant ou le fournisseur de services de paiement doit fournir au consommateur un « formulaire de confirmation de la commande », qui donne au consommateur des renseignements détaillés concernant l'achat et lui permet soit de confirmer cet achat ou de modifier la commande avant que celle-ci ne soit autorisée. Troisièmement, les renseignements communiqués par le consommateur durant l'opération doivent être protégés à la fois par le commerçant et par le fournisseur de services de paiement (OCDE, 2012).

La *Electronic Financial Transactions Act* (loi sur les opérations financières électroniques) a été adoptée en 2007. Parmi les dispositions les plus intéressantes de la loi, notons que celle-ci prévoit que la responsabilité de redresser la situation lorsqu'un client subit une perte, notamment en raison de fraude, d'opérations non autorisées, de falsification ou de commandes non complétées, incombe à l'institution financière. Essentiellement, selon la loi, l'institution financière qui fournit le service de règlement est responsable de résoudre les problèmes créés en aval par les exploitants de réseaux mobiles, les gestionnaires de services de confiance, les fournisseurs de passerelles de paiement, les fournisseurs de services de paiement, les marchands ou les vendeurs. L'expérience acquise dans le domaine a permis aux

organismes de réglementation sud-coréens de conclure qu'il était très difficile pour un consommateur de prouver la nature de la responsabilité, de l'intention ou de la négligence dans le système de paiement mobile. En effet, le système est très complexe : les opérations sont instantanées et souvent automatisées, et le système est commandé à distance. Les organismes de réglementation ont donc décidé qu'il était préférable qu'il revienne à l'institution financière d'indemniser le consommateur floué. Par la suite, l'institution financière peut utiliser son expertise et ses ressources pour trouver l'intervenant coupable et exiger une indemnisation en fonction des conditions du contrat. Cependant, même si la loi prévoit que, dans la plupart des cas, cette procédure est la meilleure, les « exploitants de services financiers électroniques » (p. ex. les exploitants de réseaux mobiles, les fournisseurs de passerelles de paiement et les exploitants de réseaux de cartes de crédit) ont la responsabilité de dédommager les consommateurs et de chercher les intervenants responsables lorsqu'une institution financière accréditée n'est pas partie prenante (Chung, 2012). Enfin, toute réclamation faite par le consommateur à un fournisseur de services de paiement secondaire doit être considérée comme un avis à l'institution financière et aux exploitants de services financiers électroniques. Le consommateur n'a pas nécessairement à savoir que l'institution financière représente le point de référence ultime. L'institution financière a donc la responsabilité d'établir une voie de communication efficace avec les divers intervenants.

Deuxièmement, afin de garantir que les paiements mobiles sont traités de manière sûre et fiable, la loi prévoit que la commission des services financiers doit jouer un rôle de surveillance vis-à-vis des institutions financières, des exploitants de services financiers électroniques, des auxiliaires et des fournisseurs tiers. La commission procède à des examens afin de s'assurer que les divers intervenants respectent les normes de sécurité prévues par la loi en matière de paiement mobile et de commerce électronique (p. ex. en ce qui concerne les technologies de l'information, la main-d'œuvre, les installations et le matériel électronique) (Chung, 2012). Les intervenants de l'industrie doivent également présenter à la commission des rapports de rendement.

Troisièmement, la loi oblige les institutions financières et les exploitants de services financiers électroniques à créer, à mettre à jour et à conserver de manière sécuritaire un registre détaillé de tous les paiements mobiles et de toutes les opérations électroniques effectués, et ce, durant une période d'au moins cinq ans. Les données du registre doivent aussi être accessibles aux intervenants, aux organismes de réglementation et aux consommateurs à des fins d'enquête ou de vérification de leur exactitude, ou encore dans le but de retracer des erreurs et de les corriger ou de repérer les cas de fraude et de rectifier la situation (Chung, 2012).

Quatrièmement, en ce qui a trait au respect de la vie privée et à la communication des renseignements, la loi impose à tous les intervenants de l'industrie d'obtenir le consentement éclairé du consommateur avant de communiquer des renseignements personnels liés à l'identité de la personne ou des détails concernant les opérations ou les comptes de cette dernière à une tierce partie qui n'a pas joué de rôle direct dans l'opération qui a généré les données en question. En outre, les intervenants ayant joué un rôle direct dans l'opération doivent aussi obtenir le consentement éclairé du consommateur avant d'utiliser les données à des fins qui ne sont pas liées directement au traitement de l'opération en question (Chung, 2012).

Finalement, la loi oblige les institutions financières et les exploitants de services financiers électroniques à tenir une comptabilité distincte pour chaque activité financière afin de faciliter et de rendre plus efficace le processus de vérification réglementaire. La loi prévoit aussi certaines exigences prudentielles (p. ex. le ratio de dépôts bancaires par rapport au crédit accordé par le truchement des passerelles de paiement pour les consommateurs qui n'ont pas l'obligation de régler leurs comptes immédiatement). La commission coréenne de la concurrence (Korean Fair Trade Commission) a accordé aux autorités municipales et provinciales le pouvoir de surveiller les fournisseurs de services de paiement et de veiller à ce que ces derniers n'usent pas de leur position de manière anticoncurrentielle. La *Telecommunications Business Act* (loi sur les services de télécommunications) oblige les exploitants de cybermarché à obtenir un permis de « fournisseur de services à valeur ajoutée » et à présenter des rapports au ministère de l'Information et de la Communication (KPMG International, 2007).

5. Le Kenya et les pays en développement

5.1. Systèmes financiers sous-développés et réseaux d'argent mobile très développés

Contrairement aux pays développés, où les paiements mobiles permettent d'accéder à des sources de paiement existantes par le biais de nouvelles technologies, les paiements mobiles jouent un rôle important dans la transformation des produits et services financiers dans les pays en développement. Le terme « argent mobile » est celui utilisé dans la plupart des pays en développement pour désigner la notion d'argent électronique. L'argent mobile est maintenant accessible aux consommateurs qui désirent effectuer des opérations au moyen de leur appareil mobile. Cet argent, enregistré de manière électronique, peut aussi être échangé contre de l'argent comptant (Castri, 2013). L'argent mobile renvoie à une grande variété de services comme les paiements mobiles, les services financiers mobiles (p. ex. les produits d'assurance) et les services bancaires mobiles (Klein et Mayer, 2011; Ndiwalana et Popov, 2008; Banque mondiale, 2012).

Dans les pays en développement, on trouve deux modèles de services financiers mobiles. Dans le premier modèle, la banque joue un rôle central, c'est-à-dire que le consommateur a une relation contractuelle directe avec une institution financière autorisée et soumise à une surveillance. Dans certains cas, le consommateur est titulaire d'un compte dans cette institution financière, alors que dans d'autres, il ne fait affaire avec l'institution que pour une seule opération. Par la suite, le consommateur peut traiter exclusivement avec un intermédiaire qui s'occupera de gérer les communications avec l'institution financière (Sultana, 2009). Ce modèle est généralement considéré comme un moyen pour les institutions financières existantes d'offrir de nouveaux services à leurs clients (Lachaal et Zhang, 2012).

Le deuxième modèle est celui axé sur les exploitants de réseaux mobiles. Ce modèle a connu une croissance plus rapide. Il est reconnu pour avoir joué un rôle de transformation, car il permet à des populations non bancarisées ou sous-bancarisées d'avoir accès à des services financiers (Klein et Mayer, 2011; Lachaal et Zhang, 2012; Sultana, 2009). Lancé au Kenya, M-PESA est l'une des marques d'argent mobile les plus populaires dans le monde. Safaricom est le plus grand exploitant de réseau mobile du Kenya, où il contrôle environ 80 p. 100 du marché (Jack et Suri, 2011). En 2007, Safaricom a lancé M-PESA pour permettre aux Kényans vivant en milieu urbain d'envoyer de l'argent à leur famille vivant dans les régions rurales. Ce type de transfert de milieu urbain à milieu rural était alors difficile, car les institutions financières l'avaient négligé dans le passé (Veniard et Goss, 2012). Essentiellement, Safaricom a répandu une pratique qui était déjà courante. La plupart des exploitants de réseaux mobiles permettaient aux personnes d'acheter du crédit prépayé pour l'utilisation de leur téléphone cellulaire. Safaricom a permis à ses clients d'envoyer ce crédit à d'autres utilisateurs par messagerie texte. Ces utilisateurs pouvaient alors le « revendre » à un agent local en échange d'argent comptant, de biens ou de services (Jack et Suri, 2011). Selon Jack et Suri (2011), le système M-PESA fonctionne de la façon suivante : les clients enregistrés font des dépôts (aussi appelés « liquidités électroniques ») auprès d'agents M-PESA au moyen de leur appareil mobile et d'une carte SIM Safaricom. M-PESA assure le maintien et la gestion des comptes des clients, et permet à ceux-ci de reporter un solde de liquidités électroniques. Des frais sont exigés pour le

retrait de fonds, mais les dépôts sont effectués gratuitement. Il est possible de transférer des liquidités électroniques à une autre personne par messagerie texte moyennant des frais forfaitaires minimes. La personne qui reçoit les fonds se voit imposer des frais uniquement lorsqu'elle fait un retrait. Les agents M-PESA conservent les soldes de liquidités électroniques sur leur appareil mobile et sont tenus de conserver une certaine somme d'argent sur place. Ces soldes sont alors achetés auprès de Safaricom ou d'autres clients par l'entremise d'agents (Jack et Suri, 2011). Au départ, le système M-PESA était un service d'envoi de fonds. Il a ensuite évolué rapidement pour devenir un outil permettant d'effectuer une grande variété de paiements. En avril 2011, Safaricom a déclaré que M-PESA comptait près de 14 millions de clients et 28 000 points de service où travaillent des agents (Safaricom, 2011).

L'approche M-PESA est largement considérée comme un modèle à suivre dans d'autres pays en développement (Jack et Suri, 2011; Lachaal et Zhang, 2012). Comme dans le cas des paiements mobiles en Corée du Sud, ce sont les consommateurs sous-bancarisés et non bancarisés du Kenya qui ont été les premiers en général à adopter l'argent mobile. Le Kenya compte environ 40 millions d'habitants. La population vit majoritairement en milieu rural, où les services financiers sont limités. Seulement 4,23 p. 100 des adultes ont un compte dans une institution financière (Banque mondiale, 2012). Cependant, le taux de pénétration des appareils mobiles est supérieur à 75 p. 100 (iHub Research; Research Solutions Africa, 2012). Dans les pays en développement, les gens peuvent plus facilement avoir accès à des réseaux de téléphonie mobile qu'à des services financiers de base. Dans la région de l'Asie orientale et du Pacifique, 34,5 p. 100 des personnes de 15 ans et plus ont une carte de débit, comparativement à 9,1 p. 100 au Moyen-Orient et à 7,2 p. 100 en Afrique du Nord (Banque mondiale, 2012). Toutefois, on compte près de 5 milliards d'abonnements de téléphonie mobile dans les pays en développement, ce qui représente environ 83 p. 100 de tous les abonnements de téléphonie mobile dans le monde (Banque mondiale, 2012). En raison du succès de M-PESA, les offres d'argent mobile se multiplient rapidement dans les pays en développement.

L'émergence de l'argent mobile peut être considérée comme une solution à l'exclusion financière. Les collectivités obtiennent l'accès à des services financiers par l'entremise d'une infrastructure mobile et virtuelle comprenant des mécanismes souvent supérieurs à ceux des institutions financières (Klein et Mayer, 2011). La multiplication des options en matière d'argent mobile dans les économies en développement prouve qu'il existe une forte demande pour des services bancaires et des solutions de paiement. Si l'on tient compte à la fois de la prévalence des appareils mobiles et de la propension des consommateurs à adopter les applications mobiles, il est possible de conclure que les services financiers mobiles servent finalement à promouvoir l'inclusion financière et à favoriser le développement économique (di Castri, 2013; Klein et Mayer, 2011; Agence suédoise de coopération au développement international, 2010; Banque mondiale, 2012).

5.2. Réglementation prudentielle

À l'heure actuelle, les organismes de réglementation semblent surtout se préoccuper de la solidité de la structure des entreprises offrant des services financiers mobiles. L'écosystème des services financiers mobiles est complexe et englobe divers intervenants, parties, contrats et ententes de services. Des observateurs ont souligné que la surveillance des opérations financières mobiles nécessitait la

coopération et la coordination entre différentes structures de gouvernance (p. ex. organismes de réglementation et décideurs), les représentants de l'industrie (p. ex. exploitants de réseaux mobiles, institutions financières, agents de la vente au détail, tiers fournisseurs de services de contenu, fabricants d'équipement) et les utilisateurs finaux (Klein et Mayer, 2011; Ndiwalana et Popov, 2008). Par conséquent, les organismes de réglementation de différents secteurs régissent habituellement des questions qui se chevauchent.

L'émergence d'exploitants de réseaux mobiles agissant à titre d'institutions financières a poussé les organismes de réglementation à se concentrer initialement sur la réglementation prudentielle des institutions financières non bancaires. Comme l'ont souligné Klein et Mayer (2011), les décideurs et les organismes de réglementation de pays aussi divers que la Namibie, l'Indonésie, le Mexique, les Philippines, le Kenya et le Pakistan rédigent des règlements adaptés à l'ère des services financiers mobiles; ils s'efforcent d'adapter la réglementation visant les services bancaires aux services bancaires mobiles. De nouvelles exigences prudentielles sont établies pour maintenir l'intégrité du capital des institutions et un certain niveau de liquidité. Ces exigences visent entre autres des ratios de capital minimum, des systèmes de mesure de la suffisance des fonds propres et des réserves obligatoires (Castri, 2013). Par exemple, dans le cas du service M-PESA offert au Kenya, Safaricom n'utilise pas les dépôts pour octroyer du crédit. Safaricom agit comme un encaisseur de dépôts responsable de conserver et de transférer l'argent (Klein et Mayer, 2011). Les agents qui échangent l'argent dématérialisé sont des entreprises indépendantes qui n'effectuent pas d'investissement pouvant mettre en danger l'argent des clients (Klein et Mayer, 2011). Par conséquent, il est difficile d'appliquer la réglementation prudentielle déjà en vigueur à des services non conventionnels qui diffèrent des services offerts par les institutions financières réglementées.

Parmi les méthodes utilisées, mentionnons la décomposition fonctionnelle, qui est une forme de réglementation établie en fonction des services ou des produits offerts plutôt qu'en fonction du type d'entreprise offrant ces services ou produits. Dans le cadre de la décomposition fonctionnelle, les agents responsables de la surveillance doivent déterminer le type de réglementation approprié pour chaque type de service (Klein et Mayer, 2011). Le système des services financiers mobiles a permis de faire ressortir la différence entre diverses composantes des services financiers et la décomposition fonctionnelle aide à déterminer quelle devrait être l'orientation de la réglementation (Klein et Mayer, 2011). Cette méthode contribue également à déterminer si la prestation de services financiers mobiles modifie ou accroît les risques auxquels les consommateurs sont généralement exposés lorsqu'ils utilisent des services traditionnels (Sotomayor, 2012). Les organismes de réglementation évaluent les risques éventuels et les avantages prévus pour chaque type d'institution, d'activité, de produit ou de service et élaborent les mesures de surveillance de sorte que le fardeau réglementaire soit adapté (Lauer, Dias, et Tarazi, 2011).

Comme il n'existe pas de règles prudentielles établies, les organismes de réglementation et les entreprises qui fournissent des services financiers mobiles appliquent continuellement de nouvelles solutions pour tenter de suivre l'évolution de l'industrie des télécommunications et du système financier, qui est rapide. Dans le cas de M-PESA, la Banque centrale du Kenya exige au fournisseur de services d'investir les dépôts nets provenant des opérations des clients dans des banques réglementées pour en assurer la sécurité et pour les garder en lieu sûr. Aux Philippines, où le contexte réglementaire est reconnu pour être flexible et favoriser l'innovation, Globe Telecommunications a créé une filiale, G-Xchange, pour gérer les aspects

financiers de son application de services financiers mobiles, « G-Cash ». Cette filiale est alors réglementée par la Banque centrale des Philippines, qui a établi un groupe central de surveillance des technologies de l'information pour accroître sa capacité à réglementer le secteur des services financiers mobiles (Ndiwalana et Popov, 2008).

Dans l'ensemble, il semble nécessaire d'accroître la coordination entre les intervenants (Ndiwalana et Popov, 2008). Les observateurs conseillent vivement aux organismes de réglementation d'examiner les politiques nationales et le contexte juridique, d'accroître leur capacité et de favoriser la collaboration entre les organismes responsables de la surveillance et le secteur privé (Kimenyi et Ndung'u, 2009; Ndiwalana et Popov, 2008). Les décideurs s'efforcent d'établir un cadre de réglementation flexible qui créera un marché ouvert et équitable favorisant la concurrence et l'innovation, mettant à profit la valeur de l'offre des fournisseurs bancaires et non bancaires, attirant l'investissement et permettant aux fournisseurs de se concentrer sur le perfectionnement des activités et la promotion de l'adoption par les clients (di Castri, 2013; Ndiwalana et Popov, 2008). En outre, les entreprises offrant des services financiers mobiles explorent les exigences réglementaires de différents secteurs pour veiller à ce que leurs services les respectent entièrement.

5.3. Cadres de réglementation et protection des consommateurs

Les préoccupations et les risques liés à l'utilisation des services financiers mobiles sont semblables dans tous les pays en développement. Cependant, on note certaines différences importantes qui découlent de conditions économiques particulières. De nombreux pays viennent tout juste d'adopter des cadres de protection des consommateurs dans le secteur financier. Peu d'entre eux disposent de règlements concernant l'argent mobile ou l'offre de services financiers mobiles par les exploitants de réseaux mobiles. Dernièrement, lorsque le Groupe consultatif d'assistance aux pauvres a analysé la protection offerte aux consommateurs dans le secteur financier dans la région de l'Europe-Asie centrale (c.-à-d. Albanie, Arménie, Azerbaïdjan, Bosnie, Géorgie, Kazakhstan, Kosovo, République kirghize, Macédoine, Russie, Serbie et Tadjikistan), il a conclu que la plupart de ces pays avaient commencé à élaborer des règles seulement en 2008 (Groupe consultatif d'assistance aux pauvres, 2012). Ces règlements établissent généralement des principes fondamentaux en matière de protection des consommateurs, comme la transparence et la communication, le traitement équitable et les mécanismes de recours relativement à l'utilisation des produits bancaires, comme les prêts et les dépôts (Groupe consultatif d'assistance aux pauvres, 2012). Cependant, comme les règlements ne s'appliquent généralement pas aux fournisseurs de services financiers non bancaires, la protection offerte aux consommateurs varie en fonction de la source des fonds servant à faire le paiement. Les paragraphes suivants résument les approches de réglementation et les mesures de protection des consommateurs actuellement en vigueur au Kenya, au Bangladesh et en Inde.

5.3.1. Le Kenya

M-PESA a été lancé en mars 2007 au Kenya, un pays qui ne disposait pas de loi, de règlement ni de politique régissant directement les opérations effectuées au moyen de l'argent électronique (Sultana, 2009). Par conséquent, les services financiers mobiles ont évolué rapidement, dans un contexte réglementaire essentiellement indéfini (Flaming et al., 2011). Dans le but d'assurer le respect des pratiques bancaires habituelles, Safaricom a consulté la Banque centrale du Kenya en août 2006. Depuis

lors, la Banque centrale continue de mener des activités de surveillance et de fournir des conseils (Flaming et al., 2011). Grâce à la collaboration et à des mesures novatrices, la Banque centrale et Safaricom ont réglé de nouvelles difficultés liées au lancement de nouveaux services financiers mobiles et d'initiatives de protection des consommateurs (Flaming et al., 2011). Par exemple, après un examen approfondi des pratiques, la Banque centrale a conclu que M-PESA n'était pas une entreprise bancaire aux termes de la *Banking Act* (loi sur les banques) étant donné que l'argent échangé pour sa valeur électronique n'était pas remboursé à échéance ni prêté dans l'objectif de réaliser d'autres activités ou un revenu d'intérêt (Sultana, 2009). Par la suite, Safaricom a été invité à préparer et à présenter une stratégie détaillée d'atténuation des risques et a été autorisé à mettre en œuvre M-PESA peu après l'approbation de cette stratégie (Sultana, 2009). Safaricom a également mis au point sa propre approche en matière de communication d'information, de pratiques équitables et de règlement des différends, et a bénéficié pour ce faire des conseils explicites mais non officiels de la Banque centrale (Flaming et al., 2011). Sans doute grâce à cette relation de travail efficace entre Safaricom et la Banque centrale, des politiques favorables aux consommateurs ont été adoptées dans le cadre du système M-PESA, même en l'absence de lois sur la protection des consommateurs (Dias et McKee, 2010).

Depuis la mise en œuvre de M-PESA, la Banque centrale du Kenya a apporté certains changements au cadre de réglementation des services financiers mobiles. En 2010, elle a adopté des lignes directrices sur les agents bancaires (*Guidelines on Agent Banking*) qui établissent la façon dont les agents (p. ex. agents fournissant des services financiers mobiles) devraient exercer leurs activités au Kenya, de façon à assurer la surveillance, la sécurité et la solidité du secteur bancaire (Université de Boston, 2013; Banque centrale du Kenya, 2010). En 2011, la Banque centrale a adopté la *National Payment System Act* (loi nationale sur les systèmes de paiement) pour surveiller les systèmes de paiement et pour établir clairement quelles entreprises sont visées par la définition de fournisseur de services de paiement et doivent être réglementées en conséquence (Banque centrale du Kenya, 2011). Grâce à la *National Payment System Act*, un cadre général de réglementation et de protection des consommateurs dans l'industrie des services financiers mobiles commence à prendre forme au Kenya.

5.3.2. Le Bangladesh

Le Bangladesh compte cinq entreprises actives offrant des services financiers mobiles. La Banque (centrale) du Bangladesh a appliqué des mesures visant à réglementer les services de paiement électronique et à protéger les consommateurs. En 2009, elle a adopté le *Payment and Settlement Systems Regulations* (règlement sur les systèmes de paiement et de règlement) afin d'officialiser son pouvoir d'accorder des permis pour les systèmes de paiement, les exploitants de systèmes de paiement et les fournisseurs de services de paiement (Sultana, 2009). Ainsi, la Banque centrale a le pouvoir de classifier les nouveaux produits et services financiers (p. ex. l'argent électronique) comme instruments de paiement désignés (Sultana, 2009). Lorsque la Banque centrale détermine que des services constituent des instruments de paiement, les entreprises qui offrent ces services sont tenues de respecter différentes lignes directrices applicables.

Dans le but d'atténuer les risques posés par les partenariats intersectoriels dans lesquels interviennent les banques, seules les entités ayant obtenu l'autorisation de la Banque centrale à cette fin peuvent émettre de l'argent électronique. Le règlement accorde une exemption aux banques et aux institutions

financières déjà en activité, de sorte qu'elles n'ont pas à obtenir de permis. Avant de pouvoir passer des ententes de services avec les consommateurs, les fournisseurs de comptes autorisés doivent faire preuve de diligence raisonnable en suivant un processus visant à leur faire connaître leur client. Afin de surveiller la masse monétaire et de protéger les consommateurs en assurant l'intégrité, la sécurité et la fiabilité des systèmes de paiement, les fournisseurs de comptes doivent aussi respecter la *Money Laundering Prevention Act* (loi sur la prévention du blanchiment d'argent) de 2002 et interdire les transferts d'argent transfrontaliers (Sultana, 2009; Klein et Mayer, 2011).

5.3.3. L'Inde

Dans le but d'atténuer les difficultés associées à la surveillance des nouveaux fournisseurs de services financiers mobiles, la Reserve Bank of India a publié des lignes directrices sur les opérations des banques (*Operative Guidelines for Banks*) en 2008. Elles portent sur la mise en œuvre de nouveaux règlements de contrôle des devises. Selon ces lignes directrices, pour offrir des services financiers mobiles aux résidents, les banques doivent être titulaires d'un permis, faire l'objet d'une surveillance et être physiquement présentes en Inde (Reserve Bank of India, 2009). Il est désormais interdit aux institutions financières non bancaires d'émettre de l'argent électronique. Aux termes de ces lignes directrices, les services devraient être limités aux comptes bancaires et aux comptes de carte de crédit en Inde qui sont conformes aux exigences en matière de connaissance des clients et de lutte contre le blanchiment d'argent. En outre, ces lignes directrices prévoient que seuls des services utilisant des roupies (c.-à-d. la devise indienne) devraient être offerts (Reserve Bank of India, 2009). Par conséquent, les transferts d'argent transfrontaliers sont strictement interdits en application du nouveau règlement. Les fournisseurs de comptes doivent également respecter la *Prevention of Money Laundering Act* de 2002 et la *Consumer Protection Act* (loi sur la protection des consommateurs) de 1986.

6. Conclusion

6.1. Les États-Unis

Notre examen de la situation aux États-Unis a porté sur les avis des spécialistes sur les problèmes que présente pour la réglementation la croissance des paiements mobiles. Pour résumer, l'émergence des paiements mobiles a exercé des contraintes sur le cadre réglementaire assez complexe des États-Unis. Le marché des paiements mobiles fait intervenir un grand nombre d'entreprises d'industries différentes. Il faut sans délai clarifier les responsabilités de chaque organisme à l'égard des divers aspects de ce nouveau mode de paiement. L'adoption d'une nouvelle réglementation n'est peut-être pas nécessaire. Toutefois, la complexité du cadre réglementaire peut créer des ambiguïtés à propos des pouvoirs en matière de surveillance. La complexité pourrait aussi faire ressortir des lacunes dans le cadre de protection des consommateurs.

Les observateurs soulignent que des résultats prometteurs ont été obtenus grâce à la *Dodd-Frank Wall Street Reform and Consumer Protection Act* (2010), où il est prévu au titre X que le pouvoir de réglementation fédéral en matière de protection des consommateurs soit centralisé et conféré au Consumer Financial Protection Bureau (CFPB). Avant ce transfert de pouvoir en 2011, les paiements mobiles auraient relevé de cinq organismes de réglementation fédéraux. Le fait que le CFPB soit devenu l'unique organe de supervision des paiements mobiles a grandement simplifié la situation. Par ailleurs, la réforme a créé un organisme fédéral unique ayant un intérêt marqué dans la réforme du cadre réglementaire et disposant du pouvoir d'améliorer la protection des consommateurs à mesure qu'évoluent les produits et services financiers.

La question de savoir quelles technologies de paiement mobile devraient être ouvertes et partagées et quelles technologies devraient être fermées et exclusives ne fait pas l'unanimité, tout comme la question de savoir si les organismes de réglementation devraient jouer un rôle dans l'établissement des règles d'interopérabilité. La majorité des intervenants de l'industrie s'entendent pour dire que la technologie de paiement mobile devrait être interopérable au point de vente, ce qui faciliterait le développement d'un système de paiement mobile intégré pour les consommateurs, comparable à celui des cartes de débit et de crédit.

On ne s'entend pas toutefois sur l'interopérabilité des paiements mobiles à plus grande échelle, par exemple par l'établissement de normes communes sur les éléments sécurisés. Généralement, l'entreprise qui contrôle l'élément sécurisé est aussi celle qui régit les précieuses données sur le consommateur qui sont générées lorsque sont effectués des paiements mobiles. Les organismes de réglementation doivent trouver un juste équilibre entre la protection de la sécurité des données des consommateurs et la nécessité de proposer des incitatifs économiques aux entreprises se livrant concurrence pour la mise au point de la technologie de paiement mobile.

Le différend très médiatisé opposant Google et Verizon montre comment la sécurité et l'interopérabilité sont liées. Google a pris des mesures pour renforcer la sécurité de son portefeuille électronique, d'un point de vue objectif. Néanmoins, comme la conception hybride (nuage informatique et élément sécurisé) de sa solution est propriétaire, les concurrents de Google ne cessent de l'exhorter à fournir d'autres

preuves que la sécurité de sa technologie de paiement mobile est adéquate. Derrière ces préoccupations soulevées à l'égard de la sécurité des données des consommateurs se cachent d'importants intérêts commerciaux liés à l'accès aux nouvelles données générées par les paiements mobiles. L'intervenant de l'industrie qui possède ou régit les données sur les consommateurs qui font des paiements mobiles jouit d'un avantage stratégique. Le règlement ultérieur du différend entre Google et Verizon montre aussi la volonté des intervenants de l'industrie de s'entendre et de conclure des contrats commerciaux mutuellement avantageux sans l'intervention des organismes de réglementation.

Pour les organismes de réglementation chargés de surveiller la protection des consommateurs, la question pourrait être de savoir si ces contrats protègent suffisamment les droits et les renseignements personnels des consommateurs. Certains spécialistes font valoir que les difficultés entourant l'interopérabilité trouveraient le mieux leur résolution par l'application des lois antitrust en vigueur et des règles existantes régissant la propriété intellectuelle et la concurrence (Brown, 2012). Cette position est étayée également par l'hypothèse selon laquelle la complexité de l'écosystème de paiement mobile fait en sorte que les solutions universelles ne sont pas souhaitables. Il pourrait plutôt être préférable de permettre aux acteurs de l'industrie de négocier des contrats stipulant le niveau d'interopérabilité, le partage des revenus, la propriété des données sur les consommateurs, la responsabilité d'assurer la sécurité des utilisateurs et les procédures de recours (Brown, 2012).

Le Mobile Payments Industry Workgroup (MPIW) a fait valoir, au contraire, que le mandat des organismes de réglementation devrait être élargi pour faire appliquer des règles précises ou encore mener les intervenants de l'industrie à accepter que l'interopérabilité se fasse au niveau de l'élément sécurisé. Le MPIW propose comme solution de donner la responsabilité de la gestion des éléments sécurisés à des gestionnaires de services de confiance qui superviseraient la production de ces éléments, le règlement des opérations de paiement et la gestion sécuritaire des données sur les consommateurs. Le fait de transférer la responsabilité des éléments sécurisés aux gestionnaires de services de confiance faciliterait la coordination entre les intervenants de l'industrie, en permettant l'échange de données dans le cadre de contrats commerciaux conclus avec les gestionnaires de services de confiance plutôt que l'exercice d'un monopole sur ces données par le truchement d'une technologie propriétaire (Continie, Crowe, Merritt, Oliver et Mott, 2011). À l'heure actuelle, cette solution pose problème du fait qu'aucun gestionnaire de services de confiance ne dispose de ressources et d'une expertise comparables à celles des géants d'Internet comme Google. Ce qui semble plutôt se produire, c'est que les exploitants de réseaux mobiles forment des coentreprises pour créer des gestionnaires de services de confiance, tandis que Google ne déroge pas de son intention de gérer les données sur les consommateurs dans ses propres serveurs Internet (p. ex. conception hybride de la plus récente plateforme du Google Wallet faisant appel au nuage informatique et à l'élément sécurisé).

Enfin, selon la littérature, le cadre réglementaire visant la protection de la vie privée des consommateurs aux États-Unis présente des lacunes, tant à l'égard de la protection des données sur les consommateurs que de celle, plus large, de l'autonomie des consommateurs. L'écosystème de paiement mobile reposera vraisemblablement sur la collecte de données sur les consommateurs et l'établissement de profils très personnalisés de consommateurs, ce qui permettra ensuite de joindre directement les consommateurs avec de nouvelles formes de publicité ciblée. Il semble que le cadre actuel ne puisse pas permettre aux

consommateurs d'être informés de la publicité comportementale les ciblant ou de décider de la refuser. On reproche aussi aux règles actuelles de ne pas habiliter les consommateurs à utiliser les profils établis à leur sujet pour prendre des décisions éclairées à l'égard de ce type de publicité. Tout effort visant à réformer le cadre réglementaire existant ou à proposer une nouvelle réglementation doit tout d'abord prendre en compte la complexité du paysage réglementaire actuel. Cette complexité signifie que l'adoption de nouvelles lignes directrices pourrait nuire à l'essor des paiements mobiles ou aller à contresens de règlements régis par d'autres organismes (p. ex. une nouvelle réglementation visant à protéger les renseignements personnels des consommateurs pourrait contredire une autre réglementation exigeant de divulguer des renseignements pour permettre la surveillance des opérations bancaires afin de cibler celles qui sont illicites).

6.2. L'Union européenne

Le principal enjeu pour les responsables des politiques de l'UE est l'harmonisation. Les experts font remarquer qu'il est beaucoup plus facile actuellement pour les gens et les entreprises de traverser les frontières politiques au sein de l'UE que pour les paiements de détail de se faire au-delà des frontières d'un pays. La Commission européenne voit les paiements mobiles comme un outil permettant de poursuivre la réalisation d'un marché unique intégré comprenant tous les états membres de l'UE. Les résultats ont été mitigés.

Certains ont soutenu que la fragmentation réglementaire a nui à la réalisation de l'objectif premier du Conseil européen des paiements, à savoir la création d'un « marché unique » intégré pour les paiements de détail pour tous les États membres. Le Conseil et la Banque centrale européenne anticipent que la croissance des paiements mobiles contribuera à amener les intervenants de l'industrie et les organismes de réglementation nationaux à se conformer aux cadres du SEPA (espace unique de paiement en euros). Toutefois, les consommateurs et les commerçants ne seront pas nombreux à adopter les paiements mobiles tant que cette façon de faire ne s'avérera pas plus pratique, sécuritaire et efficace que les autres modes de paiement déjà en place. Les organismes de réglementation sont actuellement confrontés à un cercle vicieux : une plus grande harmonisation du cadre réglementaire est nécessaire pour permettre le développement du système de paiement mobile, mais le développement de la voie du paiement mobile est nécessaire pour amener l'industrie à se conformer à la réglementation harmonisée.

Le débat entre les intervenants du secteur sur les frais de transaction témoigne des multiples défis associés à l'utilisation d'instruments à caractère non obligatoire par l'UE pour gérer l'écosystème de paiement mobile. Les commissions d'interchange sont devenues un problème pour les organismes de réglementation, car les frais varient de façon importante d'un pays à l'autre et des frais supplémentaires sont prélevés sur les opérations réglées entre des banques émettrices et des banques acquéreuses de différents pays. Les commissions d'interchange sont perçues comme un obstacle à l'harmonisation.

La question de savoir si les commissions d'interchange constituent aussi un problème en matière de protection des consommateurs fait l'objet d'un débat. Des experts de l'industrie soutiennent que les frais de transaction augmentent malgré la forte concurrence. Les banques émettrices attirent les détenteurs de cartes en leur offrant des programmes de récompenses plus généreux, qui sont financés à même des

commissions d'interchange plus élevées. Les banques acquéreuses payent les commissions d'interchange avec le revenu que leur procurent les frais de service imposés aux commerçants. Les commerçants augmentent les prix de détail pour tous les consommateurs, quel que soit le mode de paiement que ceux-ci utilisent, pour couvrir les dépenses que représentent les frais de service qui leur sont imposés. Actuellement, les consommateurs ne peuvent pas éviter de payer des prix de détail plus élevés en choisissant d'effectuer leur paiement au comptant ou en utilisant leur carte de débit. Les consommateurs qui payent comptant se trouvent donc à subventionner le coût des opérations effectuées par les consommateurs qui détiennent des cartes de crédit privilèges. L'interfinancement est très répandu dans les économies modernes, mais les systèmes de paiement se distinguent du fait qu'ils jouent un rôle essentiel pour faciliter le commerce. La décision prise récemment par l'UE de réglementer les commissions d'interchange pourrait influer sur l'évolution des frais de transaction dans l'écosystème des paiements mobiles.

La directive sur la protection des données personnelles de l'UE est l'un des cadres de réglementation les plus avancés à l'échelle mondiale. On a fait l'éloge de ses huit principes de base et de la directive dans son ensemble, laquelle est perçue comme un pas dans la bonne direction, vers une protection plus adéquate des données des consommateurs, alors qu'ils se tournent vers le commerce électronique et les paiements mobiles (Robinson, Graux, Botterman et Valeri, 2009). Parmi ses forces figurent le langage et les définitions utilisés, qui sont neutres sur le plan technologique, ainsi que son cadre de règles souple et adaptatif fondé sur des principes. La directive offre une façon efficace d'établir un juste équilibre entre la volonté d'un individu de se laisser persuader de divulguer ses données personnelles, lorsqu'il en va de son intérêt, et l'assurance que la collecte et le traitement de ces données personnelles seront licites et équitables. Il est toujours possible que la directive devienne inadéquate, étant donné l'évolution rapide du commerce électronique et des voies de paiement mobile.

L'un des problèmes perçus relativement au cadre tient à l'adoption, à l'adaptation et à l'application inégales qui en sont faites dans les différents pays de l'UE. Par exemple, Bygrave (2000) a fait remarquer que la définition de données « délicates », figurant dans le principe huit, variait de façon importante d'un pays à l'autre, selon l'adoption qui était faite de la directive. Dans la plupart des pays, on définit la race et les origines ethniques, les opinions politiques, l'orientation sexuelle et les renseignements sur la santé comme des données « délicates ». Cependant, la définition s'appliquant à l'appartenance à un groupe, à une association ou à un syndicat varie, tout comme les protections offertes pour les données concernant l'allocation sociale. Robinson et ses collègues, quant à eux, font observer qu'étant donné la portée mondiale de la collecte et du traitement des données personnelles, la directive, dans son approche de la supervision des données, devra avoir un champ d'application qui s'étend au-delà des frontières de l'UE (Robinson et al., 2009). Des règlements compatibles ont été adoptés dans 39 pays à l'extérieur de l'Europe, alors que 50 pays européens ont déjà adopté la directive, mais les États-Unis et la Chine, qui sont des partenaires commerciaux extrêmement importants, ne se sont toujours pas décidés à l'adopter (Greenleaf, 2012). Selon Greenleaf (2012), on n'insistera jamais assez sur l'importance de la Chine et des États-Unis. Des mesures s'imposent pour harmoniser les règlements entre ces deux entités politiques et l'UE. Une autre faiblesse cruciale est la définition simpliste et statique de « contrôleurs de données », qui

renvoie aux entreprises qui recueillent et traitent les données sur les consommateurs (Robinson et al., 2009).

King et Jessen (2010) ont fait remarquer que les plus importantes lacunes réglementaires concernant la voie du paiement mobile pourraient bien être les ambiguïtés entourant la définition des renseignements personnels identifiables. La portée de la directive se limite principalement à ces renseignements, ce qui a eu comme conséquence non souhaitée de créer une forte incitation économique, chez les contrôleurs de données, à définir les données qu'ils collectent et traitent comme « données anonymes » ou « renseignements ne permettant pas l'identification » afin de contourner la réglementation. Par exemple, l'ambiguïté persiste autour de la question de savoir si les « identificateurs secondaires » comme les adresses de protocole Internet (adresses IP) et les témoins HTTP devraient constituer des renseignements personnels identifiables. Les adresses IP « dynamiques », qui changent au fur et à mesure que les utilisateurs d'appareils mobiles ouvrent et ferment des sessions dans Internet et sur les réseaux des exploitants de réseaux mobiles, et les témoins HTTP, qui sont des données peu volumineuses automatiquement téléchargées des sites Web avant d'être stockées sur les navigateurs Web, sont tous deux utilisés par les entreprises qui collectent et traitent les données pour suivre l'activité en ligne des utilisateurs d'appareils mobiles et générer leurs profils de consommateur. Le statut de ces profils, à savoir s'il s'agit de renseignements personnels identifiables ou de données anonymes, n'est pas clair, ce qui veut dire que le statut des droits des consommateurs en lien avec la participation et le contrôle, le consentement éclairé et la divulgation à un tiers, tel qu'il est indiqué dans la directive, est lui aussi incertain.

King et Jesson (2010) font valoir que des règles plus claires pourraient s'avérer nécessaires pour s'assurer qu'on ne puisse pas établir de correspondance entre les renseignements personnels identifiables et les identificateurs secondaires lorsque ces derniers sont classés comme des renseignements ne permettant pas l'identification. L'UE a formé un groupe de travail en vue de considérer ces lacunes; leur recommandation préliminaire est d'appliquer une espèce de « principe de précaution ». Cela voudrait dire que les adresses IP dynamiques seraient considérées comme des renseignements personnels identifiables, à moins que les contrôleurs de données ne soient en mesure de prouver le contraire. L'hypothèse sera donc qu'il est possible de relier les adresses IP dynamiques à des renseignements personnels identifiables ou d'utiliser les adresses IP dynamiques pour en générer; par conséquent, il incombera aux contrôleurs de données de prouver l'anonymat de leurs données afin qu'elles soient exemptées des exigences de la directive (King et Jessen, 2010).

6.3. La Corée du Sud et le Japon

Il y a deux leçons fondamentales à retenir des expériences du Japon et de la Corée du Sud. D'abord, l'évolution des paiements mobiles dans ces pays a été profondément marquée par les besoins des personnes sous-bancarisées, qui, dans l'ensemble, ont adopté cette technologie dès le début. Pour les consommateurs japonais, l'accès au crédit renouvelable à court terme était limité, si bien que les fournisseurs de paiements mobiles ont été parmi les premières entreprises à tirer profit de la libéralisation du commerce. En Corée du Sud, les jeunes — qui ont adopté les appareils mobiles dans une grande proportion, mais qui n'ont qu'un accès limité au crédit et disposent de peu de façons d'effectuer des opérations électroniques — ont été les premiers à s'inscrire aux services de paiement mobile. Ce point

est important pour les organismes de surveillance, car cela donne à penser que la protection des consommateurs dans la voie du paiement mobile nécessitera la mise en œuvre de programmes permettant de joindre les personnes sous-bancarisées et d'améliorer leur niveau de littératie financière.

Deuxièmement, alors que les organismes de réglementation de la Corée du Sud se préoccupent de ne pas nuire à l'évolution des paiements mobiles en faisant adopter une réglementation indûment contraignante, les législateurs ont, en 2007, mis en place deux cadres relativement approfondis et détaillés visant à protéger les consommateurs dans la voie du paiement mobile (OCDE, 2012). D'une certaine manière, la Corée du Sud montre de quelle façon la réglementation peut servir à stimuler le développement des paiements mobiles en instaurant davantage de certitude pour l'industrie.

Dans ce pays, le cadre réglementaire, très élaboré, vaut la peine qu'on s'y attarde. Même s'il est l'un des cadres réglementaires les plus avancés dans le genre, la *E-commerce Consumer Protection Act* (loi sur la protection des consommateurs en matière de commerce électronique) était toujours considérée comme inadéquate pour encadrer la multitude de nouvelles questions de nature juridique qui ont fait surface avec la croissance des services bancaires mobiles, du commerce électronique et des paiements mobiles. L'un des problèmes était le langage utilisé dans la loi, qui était neutre sur le plan technologique (Chung, 2012). Pour s'attaquer à ces lacunes, les organismes de réglementation ont fait l'ébauche de la *Electronic Financial Transactions Act* (loi sur les opérations financières électroniques), qu'ils ont fait adopter en 2007. Le champ d'application de cette loi permet d'étendre la supervision afin qu'elle englobe les fournisseurs de services de paiement tiers (c.-à-d. les fournisseurs de passerelles de paiement) ainsi que les exploitants de réseaux mobiles et les institutions financières. Elle délimite précisément les obligations des différents intervenants les uns envers les autres, ainsi qu'envers les consommateurs et les commerçants. Des critiques ont fait valoir que la *Electronic Financial Transactions Act* risquait aussi de s'avérer inadéquate au fil de la croissance et de l'évolution des paiements mobiles.

6.4. Le Kenya et les pays en développement

La croissance des transferts d'argent mobile, dans les pays en développement, est fulgurante. Des entreprises novatrices comme Safaricom profitent du taux relativement élevé de pénétration du téléphone cellulaire pour mettre en place des services financiers répondant aux besoins de nombreux consommateurs qui sont non bancarisés ou sous-bancarisés. À la suite du succès considérable du service M-PESA de Safaricom au Kenya, on observe partout aujourd'hui dans les pays en développement l'adoption de modèles d'entreprises centrés sur un exploitant de réseaux mobiles. Dans un avenir prévisible, il y a de fortes chances que la tendance se maintienne étant donné que les services financiers mobiles peuvent servir d'outil d'accès aux services financiers de base et de développement économique. Toutefois, le fait que les lois et règlements n'aient pas suivi le rythme de l'innovation dans le domaine de l'argent mobile constitue un problème (Ndiwalana et Popov, 2008). Les observateurs encouragent les organismes de réglementation, les responsables des politiques, les fournisseurs de services et les autres parties à continuer à se pencher sur la question des risques, particulièrement dans le domaine de la protection des consommateurs. En outre, il est selon eux nécessaire que les fournisseurs de services élargissent leur offre de produits pour répondre aux nouveaux besoins. Enfin, on encourage les organismes de réglementation à offrir aux consommateurs des outils d'éducation et à les informer au sujet des avantages et des risques de l'argent mobile.

.

7. Bibliographie

About the European Payments Council (EPC), extrait tiré du site du Conseil européen des paiements [http://www.europeanpaymentscouncil.eu/content.cfm?page=what_is_epc] (consulté le 2 mars 2013)

Agence suédoise de coopération au développement international. *The Innovative Use of Mobile Applications in East Africa,* Edita Publishing, Helsinki, 2010.

Andrei, V., Rusu, S. M., Diaconescu, S. et Dinescu, A. « Securing On-Line Payment Using Dynamic Signature », *Journal of System and Management Science*, *1* (1), 2011

Association des banquiers canadiens. *Les Canadiens et leurs services* bancaires, Toronto, 2012.

Association canadienne des paiements. *Examen des méthodes de paiement et des tendances des paiements au Canada,* Ottawa, 2013

Balaban, D. « South Korea Takes Lead Globally in NFC Rollouts with Millions of Phones and SIMs », *NFC Times*, 12 janvier 2012.

Banque centrale européenne. *Vers un espace unique de paiement en euros : objectifs et échéances (4e apport d'étape),* BCE, Frankfurt am Main, 2006.

Banque mondiale. *Information and Communications for Development: Maximizing Mobile*, Washington, 2012.

Banque mondiale. *The Little Data Book on Financial Inclusion*, Washington, 2012.

Bergevin, P. et Zywicki, T. *Debit, Credit, and Cell: Making Canada a Leader in the Way We Pay,* C.D. Howe Institute, Toronto, 2012.

Black, J. « Forms and paradoxes of principles-based regulation », *Capital Markets Law Journal*, *3* (4), p. 425-457, 2008.

Blythe, S. E. « The tiger on the Peninsula is digitized: Korean E-Commerce Law as a driving force in the world's most computer-savvy nation », *Houston Journal of International Law,* 28 (3), 2006.

Board of Governors of the Federal Reserve System. *Consumers and Mobile Financial Services*, sondage, Washington, DC, mars 2012.

Borestam, A. et Schmiedel « Interchange Fees in Card Payments », *European Central Bank: Occasional Paper Series*, 131, 2011.

Boston University Center for Finance, Law & Policy, extrait tiré de *Laws under Consumer Protection* [http://www.bu.edu/bucflp/laws/by-type/consumer-protection/] (consulté le 2 mars 2013)

Braunstein, S. F. *Statement to the Senate Hearing on Mobile Payments*, Committee on Banking, Housing, and Urban Affairs, Sénat des États-Unis, Washington, DC, 29 mars 2012.

Brown, T. P. *Statement to the Senate Hearing on Mobile Payments,* Committee on Banking, Housing, and Urban Affairs, Sénat des États-Unis, Washington, DC, 2012.

Bureau of Consumer Financial Protection. *Advanced Notice of Proposed Rulemaking, Regulation E, GPR cards*, Docket No. CFPB-2012-0019, Washington, 2012.

Bygrave, L. A. « Core principles of data protection », *Privacy Law and Policy Reporter*, *6* (8), 2000.

Central Bank of Kenya, extrait tiré du *Guideline on Agent Banking*, CBK/PG/15, 2010. Site du Boston University Center for Finance, Law & Policy.
[http://www.bu.edu/bucflp/files/2012/01/Guideline-on-Agent-Banking-CBKPG15.pdf]

Central Bank of Kenya, extrait tiré du *National Payment System Act*, National Council for Law Reporting, 2011.
[http://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf]

Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, Convention européenne, 7 décembre 2000.

Children's Online Privacy Protection Act, 6501-6506 (Pub.L. 105-277, 112 Stat. 2581-728), Federal Trade Commission, 21 octobre 1998.

Chung, C. H. « Liability Issues Arising from Mobile Finance », *Banking and Finance Law Review,* 27 (2), 2012.

Cirasino, M. et Ratha, D. « The Activities of the Global Remittances Working Group », *G8 International Conference on Remittances* (p. 1-22), Banque mondiale, Rome, 2009.

Commission européenne (2012a). *Livre vert : Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile,* Bruxelles, CE, 2012.

Commission européenne (2012b). *Antitrust : la Commission adresse une communication des griefs complémentaire à Visa (Ref : IP/12/871),* Bruxelles, Europa, 2012.

Commission européenne (2012c). *Antitrust : Commission welcomes General Court Judgment in MasterCard case (Ref : Memo/12/377)*, communiqué de presse, Europa, Bruxelles, 2012.

Conseil européen des paiements. *White Paper: Mobile Payments,* Version 4.0 (EPC492-09), EPC*,* Bruxelles, 2012.

Consultative Group to Assist the Poor. *Financial Consumer Protection Regulation in Europe/Central Asia.* CGAP, 2012.

Continie, D., Crowe, M., Merritt, C., Oliver, R. et Mott, S. *Mobile Payments in the United States: Mapping the Road Ahead,* Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, BetterBuyDesign, Boston, MA, 2011.

Convention européenne des droits de l'homme, protocole n° 14, Cour européenne des droits de l'homme, Conseil de l'Europe, 1er juin 2010.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens, n° 108, Conseil de l'Europe, 28 janvier 1981.

Crowe, M., Kepler, M. et Merritt, C. *The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators,* Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, Boston, MA, 2012.

Cunningham, L. A. « A Prescription to Retire the Rhetoric of "Principles-Based Systems" in Corporate Law, Securities Regulation and Accounting », *Boston College Law School Faculty Papers*, paper 195, 2007.

Dapp, T. F., Stobbe, A. et Wruuck, P. *The future of (mobile) payments: New (online) players competing with banks*, Deutsche Bank Research, Frankfurt am Main, Allemagne, 2012.

di Castri, S. *Mobile money: Enabling regulatory solutions,* GSM Association, Londres, 2013.

Dias, D. et McKee, K. « Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options », *Focus Note* (64), 2010

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, Parlement européen et Conseil, 12 juillet 2002.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Parlement européen et Conseil, 23 novembre 1995.

Directive sur les services de paiement, 2007/64/CE, Commission européenne, 5 décembre 2007.

Electronic Fund Transfers Act (Regulation E), 12 CFR part 1005.76 FR 81019, Bureau of Consumer Financial Protection, 30 décembre 2011.

EUbusiness. *Payment Services Directive: Frequently Asked Questions*, 24 avril 2007, extrait tiré de EUbusines [http://www.eubusiness.com/topics/finance/payment-services-qa/] (consulté le 15 mars 2013)

Evans, D. S. « Interchange Fees: The Economics and regulation of What Merchants Pay for Cards », *Competition Policy International*, 2011.

Evans, D. S. et Mateus, A. *How Changes in Payment card Interchange Fees Affect Consumers Fees and Merchant Prices,* Social Sciences Research Network, Londres, 2011.

Fair and Accurate Credit Transactions Act, Pub.L. 108-159, 108e Congrès des États-Unis, 22 novembre 2003.

Fair Credit Reporting Act, Title VI, Pub.L. 91-508 (84 Stat. 1114), 91e Congrès des États-Unis, 26 octobre 1970.

Financial Services Modernization Act, Pub.L. 106-102, 113 Stat. 1338, 106e Congrès des États-Unis, 12 novembre 1999.

Flaming, M. et al. *Consumer Protection Diagnostic Study - Kenya*, Financial Sector Deepening Kenya, Nairobi, 2011.

Ghag, O. et Hegde, S. « A comprehensive Study of *Google Wallet* as an NFC Application *»*, *International Journal of Computer Applications*, *58* (16), p. 37-42, 2012.

Google, extrait tiré de *Google Wallet FAQ* [http://www.google.ca/wallet/faq.html#general-in-store] (consulté le 23 février 2013)

Greenleaf, G. « The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108? », *Edinburgh School of Law Research Paper Series*, p. 1-36, Université d'Édimbourg, 2012.

Haas, M. *Réponse à la Commission européenne – Consultation sur le livre vert intitulé « Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile »,* PayPal, Bureau de liaison pour l'UE, 2012.

Hayashi, F. et Weiner, S. *Competition and Credit and Debit Card Interchange Fees: A Cross-Country Analysis,* Federal Reserve Bank de Kansas City, 2005.

Health Insurance Portability and Accountability Act, Pub.L. 104-191 (110 Stat. 1936), 104e Congrès des États-Unis, 21 août 1996.

Hoog, A. *Forensic Security Analysis of Google Wallet,* viaForensics, San Francisco, 2011.

Hughes, S. J. *Statement to the Senate Hearing on Mobile Payments*, Committee on Baking, Housing, and Urban Affairs, Sénat des États-Unis, Washington, DC, 10 juillet 2012.

iHub Research. *Mobile Phone Usage at the Kenyan Base of the Pyramid,* Research Solutions Africa, 2012.

Jack, W. et Suri, T. *Mobile Money: The Economics of M-PESA,* The National Bureau of Economic Research, 2011.

Jones, P. « Rethinking the European Cards Harmonization Framework », *n-genuity Magazine*, printemps 2009.

Juniper Research. *Whitepaper: Mobile Money Goes Mainstream,* Hampshire, Royaume-Uni, 2011.

Katz, M. L. *Statement to the Senate, Developing a Framework for Safe and Efficient Mobile Payments – Part 2*, Committee on Banking, Housing, and Urban Affairs, Sénat des États-Unis, Washington, DC, 2012.

Kimenyi, M. S. et Ndung'u, N. S. *Expanding the Financial Services Frontier: Lessons From Mobile Phone Banking in Kenya,* Brookings, Washington, 2009.

King, N. J. et Jessen, P. W. « Profiling the mobile customer - Privacy concerns when behavioural marketers target mobile phones - Part I », *Computer Law and Security Review*, *26*, p. 455-478, 2010.

Klein, M. et Mayer, C. *Mobile Banking and Financial Inclusion: Regulatory Lessons,* Banque mondiale, Washington, 2011.

KPMG International. *Mobile payments in Asia Pacific,* Hong Kong, 2007.

Lachaal, L. et Zhang, J. « Mobile Money Services, Regulation and Creating an Enabling Environment in Africa », *Africa Capacity Development Brief*, 3 (2), 2012.

Lauer, K., Dias, D. et Tarazi. *Bank Agents: Risk Management, Mitigation, and Supervision,* Consultative Group to Assist the Poor (CGAP), Washington, 2011.

Martin, A. « How Visa, Using Card Fees, Dominates the Market », *The New York Times*, 4 janvier 2010.

Miller, C., *Exploring the NFC Attack Surface*, Accuvant Labs, Denver, 2012.

Mobile Money Tracker, extrait tiré de GSM Association [http://www.mobileworldlive.com/mobile-money-tracker] (consulté le 2 mars 2013)

Montgomery, K. C. *Statement to the Senate Hearing on Mobile Payments,* Committee on Banking, Housing, and Urban Affairs, Sénat des États-Unis, Washington, DC, 2012.

Ndiwalana, A. et Popov, O. « Mobile Payments: A Comparison between Philippine and Ugandan Contexts », *IST-Africa 2008 Conference Proceedings*, p. 10, IST-Africa, Windhoek, 2008.

NTT Docomo, *Press Release: Subscriptions to iD Mobile Credit Payment Services Top 15 Million,* NTT Docomo, Tokyo, 2010.

OCDE, *Rapport sur la protection des consommateurs dans les paiements en ligne et mobiles,* Direction de la science, de la technologie et de l'industrie, Comité sur la politique des consommateurs, Paris, 2012.

Olivarez-Giles, N. « Isis Mobile Payments Set for Oct. 22 Launch in Salt Lake City, Austin », *Wired*, p. 1., 17 octobre 2012.

Ondrus, J., Lyytinen, K. et Pigneur, Y. « Why Mobile Payments Fail? Towards a Dynamic and Multi-perspective Explanation », *System Sciences HCISS 42nd International Conference on Computing and Processing,* IEEE, Hawaii, 2009.

Oosting, I. « How mobile POS and payment systems prevent fraud », *Mobile Payments Today*, p. 1, 7 septembre 2012.

PricewaterhouseCoopers. *Mobile payments: Is trust the key to consumer uptake?*, Banking and Capital Markets, PwC Canada Foundation, Toronto, 2013.

Quorus Consulting Group. *2012 Cell Phone Consumer Attitudes,* Ottawa, 2012.

Reserve Bank of India. *Mobile Payment in India: Operative Guidelines for Banks.* Extrait de la Reserve Bank of India, 2009 [http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365]

Richard, C. C. « Mobile Remittances and Dodd-Frank: Reviewing the Effects of the CFPB Regulations », *Pittsburgh Journal of Technology Law et Policy*, *12* (6), p. 1-24, 2012.

Robinson, N., Graux, H., Botterman, M. et Valeri, L. *Review of the European Data Protection Directive,* RAND Europe, Cambridge, Royaume-Uni, 2009.

Rockefeller IV, J. D. *Statement to the Senate, Consumer Protection in the Mobile Marketplace, C*ommittee on Commerce, Science, and Transportation; Subcommittee on Consumer Protection, Product Safety, and Insurance; Sénat des États-Unis, Washington, DC, 19 mai 2011.

Safaricom, *M-PESA Customer Agent Numbers*, 6 mai 2011, extrait tiré de Safaricom [www.safaricom.co.ke] (consulté le 18 mars 2013)

Sang-Hun, C. « In South Korea, All Life is Mobile », *The New York Times*, 24 mars 2009.

Sotomayor, N. L. *Guideline for Consumer Protection in Mobile Financial Services*, Alliance for Financial Inclusion, Bangkok, Thaïlande, septembre 2012.

Sultana, R. *Mobile banking: Overview of Regulatory framework in emerging markets,* Grameenphone Ltd, Bangladesh, 2009.

Surowieki, J. « Parsing Paulson », *The New Yorker*, 28 avril 2008.

Susswein, R. *Petition to CFPB Re: Reloadable Prepaid Cards*, Docket No. CFPB-20120019, RIN 3170-AA22, *C*onsumer Action, Washington, 2012.

Telecommunications Act, Pub.L. 104-104 (110 Stat. 56), 104e Congrès des États-Unis, 3 janvier 1996.

Trichur, R. « Rogers boosts smartphone offerings in mobile-payment push », *The Globe and Mail*, 20 mars 2013.

Turing, D.*Payment Services Directive Delayed Onset: Getting Ready for 'D+1',* Conseil européen des paiements, Bruxelles, 2011.

Veniard, C. et Goss, S. « Mobile Payments in the Philippines: Future Opportunities for Growth », *Lydian Journal* (8), 2012.

Wack, K. 2012a, « Lawmakers Begin to Explore Mobile-Payments Security », *Payments Source*, p. 1, 23 mars 2012.

Wack, K. « Senate Takes Up Mobile Payments Consumer Protections », *Payments Source* , p. 1, 30 mars 2012

Weiner, S. E. et al. « Nonbanks and Risk in Retail Payments », *Join ECB-Bank of England Conference on Payment Systems and Financial Stability,* Frankfurt, 2007.

Zhou, Y. et Jiang, X. « Dissecting Android Malware: Characterization and Evolution », *2012 IEEE Symposium on Security and Privacy,* p. 95-109, IEEE Computer Society, 2012.