DSP 2
L'ÉPINEUSE QUESTION DE L'ACCÈS AUX DONNÉES DE PAIEMENT

Noémie Weinbaum

Of counsel

Aramis Société d'Avocats

À l'heure où les données de paiement constituent l'or de l'économie, de nouveaux acteurs font irruption pour exploiter un gisement traditionnellement réservé aux banques. Une nouvelle activité tisse sa toile, ce qui n'est pas sans soulever de vastes questions juridiques.

La question de l'accès à la donnée de paiement n'est pas sans rappeler une histoire où, dans la terrible jungle, un petit animal trouve un œuf, mais une bête toujours plus grosse affirme que l'œuf lui appartient... le plus gros animal ayant toujours le dernier mot. Quand le chef intervient enfin pour arbitrer le litige et rendre l'œuf convoité au plus petit des animaux, l'œuf se brise pour laisser apparaître un crocodile, qui n'hésite pas à avaler la petite bête. C'est un peu le cas de la donnée de paiement qui finira bien par engloutir tous ses aspirants. Car dans cette jungle, ce ne sont pas seulement les acteurs traditionnels du secteur que sont les établissements de crédit, de paiement[1] et de monnaie électronique[2] qui se battent pour obtenir des droits d'accès aux données de paiement ; sont apparus à leur côté des tiers qui ne sont pas – du moins jusqu'à la prochaine transposition de la DSP 2[3] prévue pour janvier 2018 - soumis au respect des règles prudentielles, et qui agissent à la limite de ces activités[4]. Il s'agit des prestataires de services de paiement tiers (« PSP tiers »).

Parmi ces nouveaux acteurs, on trouve deux types de prestataires :
– les facilitateurs de transactions de paiement, qui proposent des prestations d'initiation de paiement (*i. e.* lors de la validation d'un panier) telles que des services d'authentification forte, des facilités de paiement, des garanties de paiement ou encore des assurances ;
– et les prestataires spécialisés en « *push* » d'offres commerciales associées à la transaction, sur le mode par exemple d'Amazon, basées sur de l'analyse prédictive et de l'ingénierie de moteurs de recherche et sur de l'agrégation d'informations relatives aux données bancaires.
Ces nouveaux usages questionnent le maintien d'un niveau de sécurité élevé, qui demeure jusqu'à présent la référence pour les schèmes et le régulateur : le « *chip & pin* » et le faible niveau de fraude associé. Mais cette sécurité a un prix : l'agilité. Or les établissements de crédit et de paiement et les sociétés de financement ne souhaitent pas supporter la responsabilité de l'agilité de ces nouveaux acteurs, qui leur font

« Ces nouveaux usages questionnent le maintien d'un niveau de sécurité élevé, qui demeure jusqu'à présent la référence pour les schèmes et le régulateur : le « chip & pin » et le faible niveau de fraude associé. Mais cette sécurité a un prix : l'agilité. »

[1] Créés par la directive 2007/64/CE du 13 novembre 2007 « concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE » (dite la Directive « DSP »).

[2] Créés par les directives concernant la monnaie électronique dites « DME » du 18 septembre 2000 (directive 2000/46/CE « concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements) et la « DME 2 » du 16 septembre 2009 (directive 2009/110/CE « concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE »).

[3] Directive 2015/2366/UE du 25 novembre 2015 (« DSP 2 »)

[4] François Coupez, « Agrégateurs d'informations et initiateurs de paiement : des prestataires en mal de réglementation ? », *Revue Banque*, 29 sept. 2014.

concurrence. C'est l'épineuse question du « *liability shift* »[5].
Quant aux agrégateurs de données, sont-ils soumis aux mêmes règles en termes de secret professionnel, de sécurité informatique ou encore de respect des données à caractère personnel, notamment au regard du futur RGPD (règlement général sur la protection des données) ?
Si l'objectif ambivalent de la DSP 2 est d'encadrer l'activité de ces nouveaux acteurs, elle n'en salue pas moins leur arrivée sur le marché, qui doit permettre la promotion de la concurrence, l'efficience et l'innovation dans le secteur des paiements électroniques tout en garantissant des services de paiement sûrs et transparents, ainsi que la sécurité juridique et l'égalité des conditions de concurrence[6].

TROIS CATÉGORIES DE DONNÉES

À titre liminaire, précisons de quoi l'on parle exactement. Les données en question relèvent de trois catégories :
– les données issues des paiements (montant de la transaction, nom du commerçant, panier moyen, mais également des données plus atypiques comme l'orientation sexuelle, la composition du foyer, etc.) ;
– les données issues de la relation banque-client (catégorie socio-professionnelle, situation financière, sexe, âge, etc.) ;
– les données d'authentification (numéro de carte bancaire, nom, code d'accès, cryptogramme visuel).
En fonction de la nature de ces données, celles-ci peuvent être soit sensibles, soit personnelles, soit soumises au secret professionnel[7],

[5] http://francais-express.com/actualite/finance/-22385-banque-les-agregateurs-de-compte-sont-appeles-a-se-developper/.
[6] *Op. cit.*
[7] Aurélie Bank, « Données de paiement : mythes et réalités », *Revue de droit bancaire et financier* n°4, oct. 2013, étude 16.

> *« Les banques ne veulent en aucun cas assumer les conséquences – y compris financières – des choix du client ou de manquements d'un prestataire de services de paiement tiers au regard des exigences de sécurité. »*

soit protégées par le droit pénal, ou encore tout cela simultanément[8].
À qui appartiennent ces précieuses données ? À l'individu. Du moins, c'est bien lui qui est habilité à les utiliser et qui dispose des droits sur ces dernières, le terme consacré étant que l'individu est « *empowered* ». Et cet individu est bien souvent prêt à consentir à l'utilisation de ses données pour accéder à des services agiles[9]. Là où la question se complique, c'est que les bases de données où sont logées ces données appartiennent au titulaire des droits sur les bases de données. De fait, l'usufruit de ces données, leur agrégation, les interconnections qui en sont faites et qui donnent aux algorithmes tout leur sens constituent une chaîne de valeurs particulièrement complexe : la donnée de paiement appartenant à l'individu, la base de données appartenant selon la titularité des droits sur les bases de données, soit à la banque émetteur, soit à la banque acquéreur, soit au PSP tiers, soit à l'établissement de monnaie électronique, qui peut à son tour se présenter aussi bien en tant qu'intermédiaire proposant de faciliter le paiement ou comme prestataire offrant des services commerciaux supplémentaires.
Aussi, pour analyser au mieux les enjeux juridiques de ceux qui accèdent aux données bancaires, il convient de s'interroger sur l'identité de l'acteur qui porte la responsabilité de l'authentification forte (I.) et de vérifier que les règles imposées aux banques en termes de secret professionnel, de protection des données personnelles et de sécurité informatique n'entraînent pas une distorsion de la concurrence au détriment des banques (II.).

[8] *Op. cit.*
[9] Étude du 25 sept. 2014 : http://www.blogdumoderateur.com/etude-havas-media-francais-donnees-personnelles/.

I. L'authentification forte : le nerf de la guerre du « *liability shift* »

LA NOTION D'AUTHENTIFICATION FORTE

La notion d'authentification s'oppose à celle d'identification. Par exemple, lorsqu'une personne présente son passeport pour un contrôle, elle est identifiée grâce à ce document, mais elle n'est pas authentifiée pour autant : le lien entre le passeport et la personne n'est pas établi de façon indiscutable, irrévocable et reconnue par les tribunaux en cas de litige. Cette authentification doit être apportée par un tiers de confiance et par une preuve admise devant les tribunaux. Ainsi, un achat réalisé en confirmant un code reçu par SMS implique uniquement que ce SMS a été recopié sur une page Internet – le propriétaire de la ligne n'a pas été authentifié (cas du vol d'un portable et utilisation par un tiers) et aucune preuve matérielle ne permet de s'assurer de son consentement.
Les systèmes d'authentification utilisent un seul facteur (i. e. un mot de passe). Pour sécuriser l'opération, l'authentification forte utilise plusieurs facteurs de nature distincte (mot de passe, empreinte digitale,

token, carte à puce, etc.). L'authentification forte a plusieurs fonctions : le contrôle d'accès (qui y a accès) ; la confidentialité (qui peut voir) ; l'intégrité (qui peut modifier) ; la traçabilité (qui l'a fait) et l'irrévocabilité (qui peut le prouver).

L'APPORT DE LA DSP 2

Tirant les enseignements de la DSP 1[10], la DSP 2 adapte le cadre réglementaire des services de paiement aux défis posés par l'innovation et consacre le fait que les PSP tiers[11] seront en mesure de fournir les nouveaux services de paiement : initiation de paiement et agrégation d'informations. Ces derniers ne détenant pas de fonds pour le compte des utilisateurs, ils seront soumis à une procédure d'agrément et à des exigences prudentielles allégées.

La création de ces nouveaux services a conduit le législateur européen à créer un droit des utilisateurs, d'accès aux comptes de paiement tenus par les PSP gestionnaires de comptes lorsque ces comptes sont accessibles par voie électronique. Ce droit d'accès concerne les PSIP et les PSIC, mais également les PSP émetteurs d'instruments de paiement liés à une carte.

Les services proposés par les PSP tiers s'inscrivent de fait en complément de la chaîne de valeurs bancaires. Les PSP tiers prennent la forme de plateformes intermédiaires qui se couplent aux opérations bancaires classiques. D'un point de vue opérationnel, ces nouveaux acteurs ne se rémunèrent pas sur les commissions bancaires ; ils se positionnent en tant qu'intermédiaires, provoquant l'évolution du circuit des paiements vers une relation quadripartites entre banques,

> *« La DSP 2 adapte le cadre réglementaire des services de paiement aux défis posés par l'innovation. »*

clients, commerçants et PSP tiers. La FBF a été particulièrement amère lors de l'adoption du texte de la DSP 2 : « *ce texte n'apporte pas de réponses claires et à la hauteur des enjeux de responsabilité, de supervision et de sécurité. [...] Certes, le principe d'authentification forte a été introduit dans la directive et une supervision partielle de nouveaux acteurs est prévue. Mais l'ensemble est renvoyé aux textes d'application confiés à l'Autorité bancaire européenne et à la Commission. En outre, plusieurs points problématiques demeurent :*

– *les exigences de sécurité applicables aux tiers de paiement dans leurs relations avec le client et sa banque [...] restent floues ;*

– *[...] le partage de ces données n'est pas interdit ;*

– *la traçabilité des transactions afin d'identifier les responsabilités de chacun des acteurs n'est pas prévue* »[12].

Surtout « *les banques ne veulent en aucun cas assumer les conséquences, y compris financières, des choix du client ou de manquements d'un prestataire de services de paiement tiers au regard des exigences de sécurité* »[13]. C'est le fameux « *liability shift* » que l'Autorité bancaire européenne (ABE) a arbitré aux termes du *Final Draft of the Technical Standard Regulations* (RTS)[14].

LES TECHNICAL STANDARD REGULATIONS

Concrètement, les recommandations de l'ABE publiées le 23 février dernier excluent l'accès aux données dès lors qu'un tel accès pourrait permettre de perpétrer une fraude. Or, il suffit de quelques transactions bancaires pour identifier un individu. Aussi, comment déterminer ce qu'est une donnée sensible ? À ces incertitudes s'ajoute l'exigence de demander une authentification forte de l'utilisateur final, avec :

– un audit annuel ;

– pas plus de 5 erreurs d'authentification, à défaut de quoi le service doit être réinitialisé et un laps maximum de 5 minutes sans activité pour la déconnexion au service ;

– le paiement sans contact ne peut excéder 50 euros, ou 150 euros cumulés sur plus de 5 transactions consécutives ;

– les transactions sont considérées de faible valeur dès lors qu'elles sont inférieures à 30 euros, là où les projets antérieurs faisaient état de 10 euros ;

– les PSP tiers ne peuvent interroger le teneur de compte que sur demande explicite de leur client final ou, au maximum, quatre fois par jour.

Autant d'éléments qui risquent selon les PSP tiers de nuire à leur attractivité, et cela au nom de la sécurité informatique.

Néanmoins, et suite à l'important nombre de contestations de la part des différents acteurs économiques sur le principe de l'authentification forte systématique, jugé trop strict pour les paiements, l'ABE a finalement accepté d'assouplir la règle, en

[10] Directive 2007/64/CE concernant les services de paiement.

[11] À savoir les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'informations sur les comptes (PSIC)

[12] http://www.fbf.fr/fr/files/A38B29/Communique-FBF-DSP2-09102015.pdf.

[13] http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-(dsp)-et-le-projet-de-reglement-sur-les-commissions-d'interchange-pour-les-paiements-par-carte.

[14] https://www.esma.europa.eu/sites/default/files/library/jc_2016_21_final_draft_rts_priips_kid_report.pdf.

introduisant deux nouvelles exemptions à ce principe :
– la première repose sur une analyse des risques relatifs aux transactions ;
– la seconde concerne les paiements effectués sur des terminaux de paiement autonomes, en général utilisés dans les transports en commun ou dans les parkings.
À noter toutefois que l'exemption relative à l'analyse des risques d'une transaction est liée à un niveau prédéfini de fraude et est assujettie à une clause de révision, 18 mois après la date d'application des RTS.
Un des autres points faisant débat concerne la communication entre les établissements teneurs de compte et les deux nouveaux types de PSP tiers réglementés. L'ABE a conservé sa position initiale sur le sujet et l'obligation pour les établissements teneurs de compte d'offrir au moins une interface pour les AISP et PISP pour accéder aux comptes demeure. Cette décision tient au fait que la DSP 2 interdit désormais à ces acteurs l'accès direct aux comptes de leur client sans identification préalable. Toutefois, afin de répondre aux préoccupations de certains acteurs, les RTS précisent à présent que les établissements teneurs de compte proposant une interface dédiée doivent offrir le même niveau de disponibilité et de performance que sur l'interface réservée à leurs propres clients.
Enfin, il faut souligner que l'ABE a fait le choix de la neutralité technologique, en supprimant toute référence aux normes ISO et aux caractéristiques de l'authentification forte pour ne pas entraver les innovations futures. Pour cette raison, l'ABE a préféré édicter des normes à un niveau plus macro en dépit des réclamations pour un certain niveau de détail du fait des enjeux élevés de sécurité.
Notons que le projet final des RTS doit être soumis à la Commission européenne et au Parlement européen. L'ABE se réserve le droit de faire évoluer ces règles dix-huit mois après leur entrée en vigueur.
In fine, si l'on constate que l'arrivée des nouveaux acteurs est saluée par l'ABE, il n'en demeure pas moins que les RTS sont à ce stade encore relativement restrictives.
Voyons à présent si les règles imposées aux banques en termes de secret professionnel, de protection des données personnelles et de sécurité informatique entraînent une distorsion de la concurrence au détriment des banques.

II. Secret professionnel, protection des données personnelles, sécurité informatique : des éléments qui pèsent sur l'agilité des banques ?

LE SECRET PROFESSIONNEL

Le Code monétaire et financier[15] (CMF) impose aux établissements de crédit, de paiement et sociétés de financement un secret professionnel aux termes duquel ils ne peuvent communiquer des informations couvertes par un tel secret qu'au cas par cas et uniquement lorsque les personnes concernées leur ont expressément permis de le faire. À titre de dérogation, ces établissements peuvent communiquer de telles informations sans obtenir le consentement préalable des personnes concernées notamment aux personnes avec lesquelles ils négocient, concluent ou exécutent des contrats de prestations de services conclus avec un tiers en vue de lui confier des fonctions opérationnelles importantes. Cette exception n'a pas pour effet de modifier la nature et le régime auquel sont soumises les informations communiquées qui demeurent soumises au secret professionnel.

« De manière analogue aux établissements de crédit et de financement, les établissements de paiement sont également soumis au secret professionnel. Le respect de ces règles s'impose-t-il aux PSP tiers ? »

À ce stade, l'ACPR ne s'est pas penchée sur la question en matière d'agrégation de données. Néanmoins, elle a noté que « *la protection des données sensibles et personnelles, de même que le respect du secret bancaire, [est] particulièrement difficiles au sein d'infrastructures mutualisées et potentiellement accessibles aux régulateurs locaux* », et elle a identifié certaines bonnes pratiques pour garantir la sécurité et la confidentialité des données communiquées dans un nuage informatique[16]. De même, l'ACPR a également insisté sur le fait que « *le risque opérationnel lié aux insuffisances des SI est désormais pris en compte par Solvabilité II ; il est potentiellement accru avec le Big Data et notamment lorsque les activités sont externalisées dans un Cloud* »[17]. Ces bonnes pratiques « *s'inscrivent dans le cadre plus large défini pour le contrôle des prestations essentielles externalisées* ». Aussi, même si la prestation n'est pas une prestation externalisée essentielle ou importante, il convient de s'assurer du respect de l'esprit du CMF.
Notons également que de manière analogue aux établissements de crédit et de financement, les établissements de paiement sont également soumis au secret professionnel[18].

[15] Article L. 511-33-6° du CMF. Il semblerait justifié d'appliquer un raisonnement analogue aux projets d'agrégation de données des établissements de crédit et de financement, d'autant plus lorsque l'on garde à l'esprit qu'aux termes de l'article 10-r de l'arrêté du 3 novembre 2014, les prestations de service essentielles externalisées, comprennent également les opérations connexes mentionnées aux 1, 2 ,3, 7 et 8 du I de l'article L. 311-2, aux 1, 2, 5 et 6 de l'article L. 321-2 et aux articles L. 522-2 et L. 526-2 du CMF.

[16] Étude de l'ACPR, juillet 2013 : « Les risques associés au *Cloud computing* »

[17] Bruno Longet, « Les enjeux de la qualité des données », Séminaire Commission analyse des risques, Fédération Française des Assurances, 16 déc. 2016 : https://acpr.banque-france.fr/uploads/media/20161216-enjeux-qualite-donnees.pdf.

[18] Article L. 522-19 I du Code monétaire et financier. Les établissements de paiement doivent dès lors également veiller au respect de l'esprit de l'arrêté du 3 novembre 2014. Comme pour les établissements de crédit, il est recommandé pour les établissements de paiement de mettre en œuvre

Le respect de ces règles s'impose-t-il aux PSP tiers ? De prime abord, la réponse à cette question réside dans le fait que les règles prudentielles ont vocation à s'appliquer aux opérations emportant la mise à disposition de fonds. Les PSP tiers ne procédant pas à de telles opérations, leurs obligations sont de fait allégées, ce qui ne va pas sans créer un certain émoi.

Le Président de l'ACPR ne s'est d'ailleurs pas mépris sur le sujet en déclarant en novembre dernier que son « *ambition est d'être une place d'excellence tant par le niveau de sécurité que d'adaptation des réglementations, susceptible à ce titre d'attirer les meilleures initiatives en matière de FinTech et d'innovation financière* »[19]. Conscient des risques liés à la rupture digitale[20], tous s'accordent sur le fait que « *les établissements financiers comme les régulateurs et les superviseurs doivent s'adapter à la rupture digitale qui accompagne l'émergence des FinTechs, et prendre la mesure des enjeux devenus prégnants avec l'émergence des FinTechs : automatisation des processus et services financiers, usage croissant des algorithmes de calcul* ».

À ce stade, l'ABE a publié la version finale du projet de RTS qui tente d'opérer un difficile équilibre entre les parties, et dont seule l'application nous permettra de savoir s'il est efficient. De son côté, la CNIL a mis en place un pack conformité pour le secteur des assurances, mais celui concernant les banques est toujours en cours de discussion.

> *« Sous l'ère du RGPD, il ne sera plus possible pour les PSP tiers de se positionner en simples sous-traitants, et de se soustraire ainsi aux règles de protection des données à caractère personnel. »*

Pour finir ce tour d'horizons, à ce jour, l'ACPR s'est bornée à émettre une seule recommandation 2016-R-01, effective en octobre 2017, sur l'usage des médias sociaux à des fins commerciales.

LA RÉGULATION DE LA PROTECTION DES DONNÉES PERSONNELLES

En matière de protection des données personnelles, le rapport du Conseil d'État[21] sur le numérique et les droits fondamentaux était en 2014 prometteur sur le sujet. Le Conseil d'État avait souligné le fait que le cadre juridique applicable jusque-là à la protection des données personnelles avait été mis en place alors qu'aucun acteur n'avait conscience de la valeur économique de celles-ci et alors que la circulation de ces données restait limitée.

Pour limiter les risques juridiques liés aux usages actuels, tout en tentant de ne pas entraver le développement des innovations liées, le Conseil d'état avait proposé de :

– maintenir dans le Règlement européen sur la protection des données (RGPD) la liberté de réutilisation statistique des données personnelles, indépendamment de la finalité initiale de leur traitement, et dès lors que ces données sont anonymisées[22] ;

– créer, pour les catégories de traitement présentant un risque plus élevé, une obligation de certification périodique par un organisme tiers indépendant et accrédité par une autorité de contrôle[23] ;

– codifier la jurisprudence relative à la nullité des transactions portant sur des fichiers non autorisés ou non déclarés à la CNIL[24] ;

– mettre en place des outils de régulation de l'utilisation d'algorithmes de sorte à pouvoir détecter les discriminations illicites[25].

Des propositions loin d'être dénuées d'intérêt au regard des enjeux des PSP tiers. On peut considérer par ailleurs que le RGPD quant à lui, utilise le *privacy by design* pour couvrir à la fois l'anonymisation des données et la mise en place des outils de régulation d'algorithmes pour détecter les discriminations illicites. La question reste ouverte néanmoins. Quant à la jurisprudence relative à la nullité des transactions portant sur des fichiers non autorisés, on peut espérer que les sanctions prévues par le RGPD sont suffisantes pour bannir ce type de procédés ab initio, mais là aussi le RGPD ne reprend pas in concreto les propositions du Conseil d'État. Quoi qu'il soit, il est essentiel de noter que jusqu'à présent, l'article 17 de la Directive 95/46/CE s'est borné à imposer au responsable du traitement de nommer un sous-traitant présentant les mêmes garanties de conformité aux lois nationales transposées sur la base de la Directive 95/46/CE que celles applicables au responsable du traitement. Pour ce faire, un engagement écrit précisant que le sous-traitant devait agir uniquement sur instruction écrite du responsable du traitement et qu'il s'engageait à assurer la sécurité des données à caractère personnel était suffisant.

Le RGPD fait évoluer ce point en étendant le champ d'application de la protection des données personnelles. Le considérant 81 du RGPD reconnaît ainsi le rôle des sous-traitants dans la protection des données à caractère personnel. Les sous-traitants ne peuvent plus

des bonnes pratiques afin de garantir la sécurité et la confidentialité des données communiquées dans le cadre de projets impliquant des études d'analyse prédictives.

[19] François Villeroy de Galhau, Gouverneur de la Banque de France, président de l'Autorité de contrôle prudentiel et de résolution : https://acpr.banque-france.fr/lacpr/missions/pole-acpr-fintech-innovation.html.

[20] Évaluation des risques du système financier français – rapport de la Banque de France de décembre 2016 - https://www.banque-france.fr/sites/default/files/medias/documents/ers-2016-s2-evaluation-des-rsques-du-systeme-financier.pdf.

[21] Conseil d'Etat, Le numérique et les droits fondamentaux – étude annuelle 2014 – www.conseil-etat.fr.

[22] Proposition n° 12 du rapport du Conseil d'Etat, *op. cit.*

[23] Proposition n° 19 du rapport du Conseil d'Etat, *op. cit.*

[24] Proposition n° 20 du rapport du Conseil d'Etat, *op. cit.*

[25] Proposition n° 23 et n°25 du rapport du Conseil d'Etat, *op. cit.*

arguer de l'inapplicabilité des règles à leur égard puisque le responsable de traitement doit utiliser uniquement des sous-traitants fournissant des garanties suffisantes, en particulier en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement. En effet, l'article 28 du RGPD dispose que le sous-traitant se doit de mettre en place des mesures de sécurité et organisationnelles pour protéger les données à caractère personnel contre tout incident ou destruction illégale, perte, altération, divulgation non autorisée ou accès. En fonction de la nature du traitement, cela peut induire :

– le cryptage des données à caractère personnel ;
– l'examen continu des mesures de sécurité ;
– des systèmes de redondance et de secours ;
– des tests de sécurité réguliers.

Voilà qui démontre bien que le sous-traitant est responsable vis-à-vis de ceux dont il traite les données. En plus, le sous-traitant est également soumis au régime des sanctions mis en place par le RGDP.

De toutes évidences, sous l'ère du RGPD, il ne sera plus possible pour les PSP tiers de se positionner en simples sous-traitants, et de se soustraire aux règles de protection des données à caractère personnel. Le RGPD requiert des sous-traitants – y compris des PSP tiers, de développer et de mettre en place un certain nombre de procédures internes et de pratiques pour la protection des données personnelles pour garantir notamment l'anonymisation irréversible des données.

LA SÉCURITÉ INFORMATIQUE

In fine, la DSP 2 soulève aujourd'hui avant toute chose un défi majeur quant à la sécurité des données de paiement : les PSP tiers auront accès aux informations confidentielles des clients et pourront générer des paiements depuis leurs comptes. Il s'agit là d'un risque opérationnel d'autant plus important que la DSP 2 n'impose aucune obligation contractuelle entre les PSP tiers et les banques, et ce sans compter que les dispositions et responsabilités en cas de fraude ne sont pas clairement définies.

D'un point de vue technique, assurer cet accès facilité aux comptes tout en respectant les exigences d'authentification forte représente une difficulté dont les banques devront prendre toute la mesure pour déployer des dispositifs de sécurité complémentaires : évolution des systèmes d'information, renforcement des contrôles et monitoring des transactions –autant d'initiatives opérationnelles à mettre en œuvre pour se conformer à ces nouvelles dispositions[26].

Côté PSP tiers, ceux-ci devront au même titre que les banques se conformer aux standards de sécurité bancaires définis par l'ABE. À ce titre, on peut s'interroger sur la capacité des RTS à assurer la sécurité des nouveaux services de paiement et à protéger les parties contre le risque de fraude, notamment au vu de l'exemption prévue par les RTS sur l'analyse de risques.

Il va sans dire que le contenu des orientations de l'ABE risque encore d'évoluer et les normes techniques devront probablement évoluer de manière continue en considération de l'évolution des risques sécuritaires inhérents aux nouveaux services de paiement et prévenir au maximum la réalisation de fraude tout en évitant d'être un frein au développement de ces nouvelles activités.

Autant d'impacts opérationnels pour les banques qui ne doivent pas occulter les enjeux d'évolution de leur offre de service, lesquels se doivent d'ouvrir la voie à une plus forte intégration des services bancaires dans les parcours d'achat et dans les activités de gestion administrative. ■

[26] http://finance.sia-partners.com/agregateurs-dinformation-et-initiateurs-de-paiement-quels-enjeux-pour-les-banques.