Les données de paiement, entre DSP 2 et RGPD

Pierre Storrer
Avocat à la Cour,
Kramer Levin LLP

1. L'articulation entre la deuxième directive sur les services de paiement (DSP 2[1]) et le règlement général sur les données personnelles (RGPD[2]) constituera un enjeu majeur des années à venir, 2018 représentant à cet égard, sans doute, une « *année charnière* »[3], ne serait-ce que parce que ces deux grands textes y entrent successivement en application (13 janvier dernier pour l'un, 25 mai prochain pour l'autre).

2. S'il est commun de souligner que les prestataires de services financiers, les banques en particulier, devraient se livrer à une « bataille de la donnée » – qui n'est jamais qu'une bataille de la connaissance client (connaissance positive et non subie du fameux *KYC* de la lutte anti-blanchiment), une bataille pour garder le lien d'intermédiation –, il l'est un peu moins d'observer que les données ont fait leur entrée, de plain-pied, dans le droit des services de paiement avec la DSP 2[4].

3. La considération des données à caractère personnel est désormais une réalité pour les prestataires de services de paiement (PSP), tenus de recueillir le consentement exprès de leurs clients : « *Les prestataires de services de paiement n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement exprès de l'utilisateur de services de paiement* » (CMF, art. L. 521-5). Une sorte de permission légale leur est même octroyée pour combattre la fraude[5]. Quant à la Commission nationale de l'informatique et des libertés, compétence dérogatoire lui est accordée pour mettre en œuvre le RGPD et recevoir, notamment, toute plainte en la matière (cf. CMF, art. L. 521-7).

4. Le vocabulaire du droit des services de paiement s'enrichit par ailleurs de deux nouvelles catégories de données qui, par nature, devraient être à caractère personnel : les données de sécurité personnalisées ou « *données personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification* » (CMF, art. L. 133-4, a), ainsi que les données de paiement sensibles, très (trop) approximativement entendues comme « *des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude* » (CMF, art. L. 133-4, g). L'impératif de protection de ces dernières se retrouve parmi les conditions nouvelles d'obtention de l'agrément d'établissement de paiement (ou de monnaie électronique), puisque doivent être fournies à l'Autorité de contrôle prudentiel et de résolution (ACPR) une description du processus pour enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles et en garder la trace, de même qu'une description des mesures de maîtrise et d'atténuation des risques décelés en matière de sécurité, dont l'utilisation illicite de données sensibles ou à caractère personnel[6]. De manière générale, la délivrance de l'agrément suppose « *des dispositifs à même d'assurer la sécurité des services de paiement fournis, ainsi que la protection des données de paiement sensibles* » (CMF, art. L. 522-6, II). Sachant que les normes techniques de réglementation concernant l'authentification et la communication, que vient enfin d'adopter la Commission[7], sont destinées, entre autres, à « *garantir la sécurité des fonds et des données à caractère personnel des utilisateurs de services de paiement* » (DSP 2, art. 98, 2, b).

5. Et puis, et surtout, la promotion de l'*open banking* par la DSP 2, autrement dit l'ouverture des comptes de paiement à ceux qui ne les gèrent pas, place les données (de sécurité personnalisées, de paiement sensibles ou à caractère personnel) au cœur de la problématique d'interaction avec le RGPD. Ce n'est pas tellement le nouveau service 7° d'initiation de paiement[8], pas davantage l'accès aux comptes donné aux émetteurs d'instruments de paiement liés à une carte (cf. CMF, art. L. 133-39), mais bien le 8° : celui d'information sur les comptes, ce « *service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de*

1 - Dir. (UE) 2015/2366, 25 nov. 2015, concernant les services de paiement dans le marché intérieur.

2 - Règl. (UE) 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

3 - ACPR, Étude sur la révolution numérique dans le secteur bancaire français, Analyses et Synthèses, n° 88, mars 2018, p. 20. *Adde*, N. Beaudemoulin, « Les enjeux liés à l'exploitation responsable des données par les établissements financiers », Revue Banque n° 810, juill.-août 2017, p. 28.

4 - Voir toutefois A. Banck, « Données personnelles : la difficile articulation des dispositions de la Directive sur les Services de paiement 2 et du Règlement général sur la protection des données », Rev. dr. banc. et fin. n° 1, janv. 2018, étude 1.

5 - Cf. CMF, art. L. 525-6 : « *Les systèmes de paiement et les prestataires de services de paiement peuvent mettre en œuvre des traitements de données à caractère personnel lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le règlement (CE) 45/2001 du Parlement européen et du Conseil* ».

6 - Arr. 29 oct. 2009 portant sur la réglementation prudentielle des établissements de paiement, art. 2, 7° et 10°. *Adde*, Arr. 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique.

7 - Règl. Délégué (UE) 2018/389, 27 nov. 2017, complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

8 - Cf. CMF, art. D. 314-2, 6° : « *Service d'initiation de paiement, un service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement* ».

services de paiement » (CMF, art. D. 314-2, 7°), qui retient à l'évidence l'attention.

6. Car ce service, communément appelé d'« agrégation de données », est davantage un service de la société de l'information qu'un service de paiement ; point d'exécution d'opérations de paiement, mais accès et traitement, pour consolidation, des données de compte. Avec lui, l'impératif de protection des données à caractère personnel, d'autant plus convoitées qu'elles révèlent, en tout ou partie[9], la situation financière du titulaire du compte, prend tout son sens en droit des paiements. Car une brèche est ouverte par la DSP 2, qui laisse s'échapper les données de compte, peut-être toutes les données de compte… Mais, après tout, l'accès au compte de paiement n'est jamais qu'un droit conféré à l'utilisateur de services de paiement[10]. Où l'on retrouve, à l'article L. 133-41 du Code monétaire et financier, siège du régime de l'information sur les comptes, les principes majeurs du traitement des données à caractère personnel selon le RGPD[11] : consentement exprès du titulaire du compte, finalité déterminée, minimisation des données[12], etc. Étant observé, en passant, que les données de compte recueillies par les agrégateurs servent d'ores et déjà à bien d'autres choses qu'à la seule fourniture du service expressément demandée par l'utilisateur de services de paiement, mais c'est un sujet à part entière…

7. Cette question, pour terminer : le droit (des services de paiement) à l'information sur les comptes pourrait-il être relayé, voire dépassé car sans les limites imposées par la DSP 2, par le droit à la portabilité des données consacré par l'article 20 du RGPD (et les articles L. 224-42-1 et suivants du Code de la consommation) ? Les conditions de ce texte paraissent remplies (consentement, procédés automatisés) et l'on peut même penser que la mise en place future des interfaces de communication (API) entre prestataires de services de paiement, gestionnaires de comptes et prestataires sans compte rende possible une transmission directe des données des uns aux autres. Nul doute, en conséquence, que le sujet de l'interaction entre DSP 2 (PSD2 en anglais) et RGPD (ou GDPR) ne nous préoccupe à l'avenir. À telle enseigne, au demeurant, que l'Autorité bancaire européenne (ABE ou EBA) l'a inscrit dans sa "Fintech roadmap" : "*the EBA will monitor potential clarifications that may be provided by the European Parliament, the Council of the EU, the Commission or other EU authorities on the interaction between PSD2 and the GDPR, in order to assess what, if any, implications such clarifications may have on the EBA, national authorities, consumers and/or payment service providers*"[13]. Il est heureux que des clarifications soient apportées sur l'articulation entre deux textes majeurs.

9 - À l'heure où nous terminons la rédaction de cette note, le Sénat vient d'adopter, en 1re lecture, le projet de loi de ratification de l'ordonnance de transposition de la DSP 2, où l'on découvre avec une certaine stupeur, qu'un article L.522-7-1 du CMF permettrait l'accès, non plus aux seuls comptes de paiement (ce que permet seulement la DSP 2, pour cette raison simple que son champ d'application n'est que le paiement), mais aussi aux comptes sur livret, comptes à terme, comptes-titres, comptes d'épargne, de crédit, etc.

10 - Voir P. Storrer, « Du droit de donner libre accès à son compte de paiement », *in* Le futur du paiement, Hors-série Banque & Droit, juill.-août 2016, p. 14.

11 - Comp. DSP 2, cons. 89 : « *En particulier, lorsque des données à caractère personnel font l'objet d'un traitement aux fins de la présente directive, la finalité devrait être précisée, la base juridique pertinente devrait être visée et les exigences de sécurité applicables de la directive 95/46/CE satisfaites, et les principes de nécessité, de proportionnalité, de limitation de la finalité et de la durée proportionnée de conservation devraient être respectés. De même, la protection des données dès la conception et la protection des données par défaut devraient être intégrées dans tous les systèmes de traitement des données développés et utilisés dans le cadre de la présente directive* ».

12 - Comp. ABE, Orientation finales sur la sécurité des paiements sur internet, 19 déc. 2014, 4.4 : « *Lorsqu'ils conçoivent, élaborent et maintiennent des services de paiement sur internet, les PSP doivent veiller à ce que la minimisation des données soit une composante essentielle de la fonctionnalité principale: la collecte, l'acheminement, le traitement, le stockage et/ou l'archivage, et la visualisation de données sensibles de paiement doivent être maintenus au strict minimum* ».

13 - The EBA's Fintech Roadmap – Conclusions from the consultation on the EBA's approach to financial technology (Fintech), 15 mars 2018, n° 87. Voir encore EBA, Report on innovative uses of consumer data by financial institutions, 28 june 2017; et, en dernier lieu, ESMA, EBA and EIOPA, Joint Committee Final Report on Biga Data, 15 march 2018.