Lecture croisée de la Directive sur les services de paiement et du Règlement sur la protection des données personnelles

VALÉRIE POZZO DI BORGO
Directeur
Associée EY

Dans un contexte d'innovation et de concurrence, l'exploitation et la protection des données personnelles de paiement deviennent un enjeu central. Cet enjeu se retrouve au cœur des préoccupations de deux nouvelles réglementations européennes qui entreront en application en 2018, le Règlement sur la protection des données personnelles et la 2e Directive sur les services de paiement. Ces textes prévoient des dispositions visant à protéger le consentement des clients et à assurer la sécurité de leurs données personnelles de paiement.

L'ordonnance n° 2017-1252 du 9 août 2017[1] achevant la transposition de la Directive n° 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (ci-après « DSP 2 » ou la « Directive ») a récemment été publiée[2] et entrera en vigueur le 13 janvier 2018[3].

Comme le souligne le Rapport au président de la République relatif à cette ordonnance[4], la Directive sur les services de paiement comporte des dispositions relatives à quatre grandes thématiques, dont « *les exigences de sécurité renforcées pour les paiements électroniques et la protection des données des utilisateurs de services de paiement* ».

Cette thématique n'est pas sans interpeller lorsque l'on sait l'entrée en application, à quelques mois d'intervalle, du Règlement européen 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 personnelles, ci-après « RGPD » ou le « Règlement »)[5].

Ces deux réglementations s'inscrivent en réalité dans une dynamique commune, portée par des textes épars mais sous-tendus par une logique identique. Il s'agit de favoriser l'innovation et la concurrence entre opérateurs économiques en facilitant la circulation des données personnelles des clients, tout en renforçant le droit fondamental de ces derniers de conserver la maîtrise desdites données.

Outre la mobilité bancaire instituée par la Loi Macron[6], les deux textes « phares » en matière d'ouverture et de circulation des données personnelles sont la DSP 2 et le RGPD. La première procède à une petite révolution en obligeant les établissements gestionnaires de comptes à ouvrir l'accès aux données de paiement de leurs clients[7].

Cette obligation vise à permettre à deux nouveaux types de prestataires de services de paiement d'initier des paiements au nom et pour le compte du client[8] et/ou de fournir à ce dernier des informations consolidées concernant ses comptes de paiement ouverts auprès d'établissements gestionnaires de comptes différents[9].

Quant au RGDP, son entrée en application le 25 mai 2018 marquera celle du droit à la portabilité[10], c'est-à-dire le droit pour les personnes concernées de « *recevoir les données à caractère personnel [...] qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine* » et « *le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* ».

1. J. Lasserre Capdeville, « Nouvelle réforme des services de paiement : la DSP2 est transposée – À propos de l'ordonnance n° 2017-1252 du 9 août 2017 », *JCP* éd. G., n° 37, 11 septembre 2017, 923.
2. *JORF* n° 0186 du 10 août 2017, texte n° 26.
3. Article 34 - I de l'ordonnance.
4. *JORF* n° 0186 du 10 août 2017, texte n° 25.
5. Règlement (UE) 2016/679 du 27 avril 2016 qui entrera en application le 25 mai 2018.
6. Loi du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques. Cette loi vise à faciliter le changement d'établissement bancaire en instituant l'obligation de proposer au client, gratuitement et sans condition, un changement automatisé des domiciliations bancaires, des prélèvements valides et virements récurrents.
7. P. Storrer (coord.) « DSP2 : le futur du paiement », Banque et Droit, Hors-série, juill.-août 2016.
8. Les prestataires de service d'initiation de paiement définis par l'article 4 – 15° de la Directive.
9. Les prestataires de service d'information sur les comptes définis par l'article 4 – 16° de la Directive.
10. Article 20 du RGPD.

Bien entendu, cette ouverture des données personnelles ne doit pas se faire au détriment des droits des individus d'en conserver la maîtrise et de bénéficier de garanties de sécurité adéquates quant à leur utilisation.

À cet égard, la Loi pour la République numérique a frappé un coup symbolique : elle a complété l'article 1er de la Loi informatique et libertés du 6 janvier 1978 par l'affirmation selon laquelle « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ».

Dans un contexte d'innovation et de concurrence, la protection des données personnelles devient ainsi un enjeu majeur, que l'on retrouve là encore au cœur des préoccupations tant du RGPD que de la DSP 2. Chacun de ces textes prévoit des dispositions importantes visant à protéger le consentement des clients (1.) et à assurer la sécurité de leurs données de paiement (2.).

Ces dispositions sont cumulativement applicables dès lors que les données concernées revêtent un caractère personnel, ce qui implique d'analyser les deux textes de manière croisée et de les articuler dans leur mise en œuvre.

1. La protection du consentement des utilisateurs des nouveaux services de paiement

Comme déjà évoqué, les nouveaux services de paiement institués par la DSP 2 – l'initiation de paiement et l'information sur les comptes – reposent sur le nécessaire accès par tiers aux comptes de paiement du client et, par là même, à ses données d'authentification et de paiement.

Bien que ces données ne constituent pas des données sensibles au sens du RGPD, elles sont qualifiées comme telles par la DSP 2, qui définit « *les données de paiement sensibles* » comme « *les données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude* »[11].

C'est la raison pour laquelle la Directive encadre très strictement les conditions dans lesquelles le prestataire recueille le consentement du client afin de pouvoir lui fournir ces nouveaux services. En effet, pour chacun d'eux, la Directive prévoit l'obligation de recueillir le consentement explicite du client et précise que le prestataire ne pourra avoir accès qu'aux données nécessaires à la fourniture du service spécifiquement consenti.

De ce point de vue, les dispositions de la Directive sont pleinement conformes aux exigences du RGPD qui prévoit l'obligation de recueillir le consentement exprès de la personne concernée afin de pouvoir traiter ses données[12], et à son corollaire le principe de minimisation, en vertu duquel les données collectées doivent être limitées à ce qui est nécessaire au regard des finalités consenties[13].

Toutefois, le respect de ces exigences ne suffit pas à remplir l'ensemble des conditions nécessaires pour obtenir le consentement libre et éclairé également requis par le RGPD.

Ainsi, les prestataires des nouveaux services de paiement devront intégrer dans la convention conclue avec le client l'ensemble des autres informations prévues par l'article 13 du RGPD afin de garantir un consentement donné en toute connaissance de cause : informations sur le responsable de traitement, possibilité de demander la rectification ou l'effacement des données, le cas échéant, les destinataires ou catégories de destinataires, le transfert des données vers un pays tiers, l'existence d'une prise de décision automatisée, et bien sûr la durée de conservation des données, qui devra elle-même être combinée, pour les initiateurs de paiement, avec l'interdiction qui leur est faite de stocker des données de paiement sensibles.

L'articulation des deux textes devient plus délicate concernant l'utilisation des données par les nouveaux prestataires à d'autres fins que celles prévues par la DSP2.

En effet, la Directive semble proscrire avec force une telle réutilisation : il est expressément interdit, tant aux initiateurs de paiement[14] qu'aux prestataires de services d'information[15], d'utiliser, de consulter ou de stocker des données à des fins autres que la fourniture du service d'initiation ou d'information expressément demandé par le payeur.

La solution pourrait être à rechercher dans le RGPD, qui permet toute utilisation licite des données personnelles dès lors que le consentement a été explicitement recueilli pour chacune des finalités de traitement envisagées et que toutes les informations prévues par l'article 13 pour chacune de ces finalités ont été préalablement communiquées à la personne concernée.

Enfin, les nouveaux prestataires de services de paiement devront garantir à leurs clients l'ensemble des autres droits prévus par le RGPD, dont le droit d'accès et le droit à l'effacement de leurs données personnelles, avec les lourds développements informatiques que cela implique.

2. La sécurité des données relatives aux services de paiement

L'autre grande préoccupation commune à la DSP2 et au RGPD concerne la sécurité des données personnelles de paiement.

À cet égard, il est particulièrement intéressant de constater que la DSP2 intègre le principe du *privacy by design*[16] institué par le RGPD, en obligeant désormais les prestataires de services de paiement à intégrer dans leur dossier d'agrément différents documents relatifs à la sécurité des données[17], attestant, si besoin en était, de la place primordiale prise par la protection des données personnelles dans le secteur financier.

11. Article 4. e) de la Directive.
12. Par une déclaration ou un acte positif clair (Article 4.11). Le consentement de la personne concernée n'est cependant pas requis dans tous les cas, par exemple si le traitement est fondé sur une obligation légale ou un intérêt légitime.
13. Article 5.1 c).
14. Article 66.3. g) de la Directive.
15. Article 67.2. f) de la Directive.
16. Qui impose de déterminer dès la conception du produit ou du service les mesures techniques et organisationnelles permettant de protéger les données personnelles (Article 25 du RGPD).
17. Article 5 de la Directive.

Parmi ces documents, figure un document relatif à la politique de sécurité, qui devrait ainsi inclure les mesures de sécurité propres aux données personnelles prévues par l'article 32 du RGPD. Ces mesures incluent notamment, selon les besoins, la pseudonymisation et le chiffrement des données à caractère personnel, ou encore les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

La DSP2 précise également que le document relatif aux mesures de sécurité devra comprendre une analyse détaillée des risques en ce qui concerne les services de paiement proposés et une description des mesures de maîtrise et d'atténuation prises pour protéger les clients de façon adéquate contre les risques décelés en matière de sécurité, y compris la fraude et l'utilisation illicite de données sensibles ou à caractère personnel[18].

Ce document correspond, dans ses grandes lignes, à l'analyse d'impact prévue par l'article 35 du RGPD, qui doit être réalisée lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

De même, l'exigence d'authentification forte du client lors de l'utilisation de services de paiement en ligne[19], ou bien la mise en place de mesures de communication sécurisées entre les gestionnaires de compte et les prestataires tiers[20], sont autant d'exigences qui rejoignent les impératifs de sécurité prônés par le RGPD.

C'est d'ailleurs notamment au nom de la protection des données personnelles de leurs clients que les banques tentent pour l'heure d'obtenir l'interdiction de la technique du *web-scraping* par les initiateurs de paiement et agrégateurs de comptes, au profit de la création « *d'interfaces dédiées* » (API)[21].

On le voit, dans cette matière, sécurité des services de paiement et sécurité des données personnelles sont étroitement imbriquées et l'une ne peut être envisagée sans l'autre.

Cette étroite imbrication, voire cette confusion, entre les exigences respectives des deux textes, se retrouve s'agissant des procédures de notification en cas de failles de sécurité. Chaque texte impose d'avoir une procédure spécifique de notification auprès du régulateur compétent pour superviser sa mise en œuvre ainsi, que dans, certains une procédure de notification du client.

Dès lors que les données de paiement constituent également des données personnelles, une même faille de sécurité sera donc susceptible de donner lieu à pas moins de quatre notifications distinctes, d'où l'intérêt de mutualiser ces procédures.

Dans le secteur financier, la sécurité des données personnelles des clients n'est ainsi plus l'apanage de la CNIL. Cette dernière a d'ailleurs rejoint le pôle Fintech Innovation, créé par l'AMF et l'ACPR, témoignant de l'étroite imbrication des problématiques posées par l'utilisation innovante des données personnelles dans le secteur financier. Cette double compétence devra notamment s'articuler au regard du principe *non bis in idem*, en vertu duquel on ne peut être sanctionné deux fois pour des mêmes faits.

En toute hypothèse, la problématique de la protection des données personnelles ne peut plus être contemplée de manière isolée. La nécessité d'instituer une culture globale de la donnée, permettant de gérer de manière efficace et sécurisée les données collectées par les établissements financiers, que ce soit sur la base de leurs obligations ou à des fins commerciales, apparaît plus que jamais nécessaire. ■

18. Article 5.1. j) de la Directive.
19. Article 97 de la Directive.
20. Article 98 de la Directive.
21. Cf. communiqué de presse de la Fédération européenne bancaire du 16 mai 2017.