RB PRESSE

Mars 2019
ISSN 1777-5752
70 euros
revue-banque.fr

BANQUE & DROIT

la pratique du droit bancaire et financier et de la conformité

HORS-SÉRIE

Les données à l'heure de la DSP2 et du RGPD

COLLOQUE AEDBF DU 9 OCTOBRE 2018

organisé en association avec le cabinet Kramer Levin

AEDBF FRANCE

Kramer Levin

RB REVUE BANQUE

Sommaire

Propos introductifs

Le colloque, dont ce numéro spécial de *Banque & Droit* fait la synthèse, a porté d'abord sur l'articulation entre DSP 2 et RGPD ; puis sur la mise en œuvre de ces textes, en incluant une intervention de la CNIL pour évoquer la position du régulateur

THIERRY BONNEAU
Agrégé des facultés de droit
Professeur
Université Panthéon-Assas (Paris 2)

1. Les textes, qu'ils soient européens ou français, peuvent être sectoriels ou transversaux. Les premiers, telle que la directive du 25 novembre 2015, dite DSP2[1], ne s'appliquent que dans un secteur d'activité – les services de paiement – alors que les seconds, illustrés par le RGDP – le règlement du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2] – s'appliquent quel que soit le secteur d'activité, ce qui oblige à les combiner sauf lorsque les dispositions des textes sectoriels sont dérogatoires aux textes transversaux.

2. RGPD est l'acronyme de l'intitulé abrégé officiel du Règlement du 27 avril 2016 : « *Règlement général sur la protection des données* ». Acronyme facile, mais un peu trompeur, car les données peuvent être de deux sortes : des données générales, par hypothèse impersonnelles, et des données à caractère personnel. Seules les secondes sont à envisager dans le cadre de ce colloque bien que son titre se réfère, comme l'intitulé abrégé du règlement du 27 avril 2016, aux « données » sans autre précision. Cette conclusion s'impose d'autant plus que la DSP 2 vise à régir, outre les établissements de paiement[3], la relation nouée entre les professionnels fournissant des services de paiement et leurs clients[4].

3. Les données à caractère personnel sont elles-mêmes diverses et variées. Elles peuvent être bancaires comme non bancaires, extrapatrimoniales comme patrimoniales. Est-ce à dire que les données à caractère personnel doivent être identifiées aux seules données extrapatrimoniales ? La réponse est assurément négative[5]. Les

1. Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.
2. Règlement (UE) 2016/678 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). V. not E. Jouffin et C. Bret, I. Falque-Pierrotin, A. Basdevant et J-P. Mignard, F. Parmentier, A. Bounfour, M. Griguer, E. A. Caprioli, G. Mathias et A. Alfer, « La donnée dans tous ses états », Hors-Série *Banque et Droit*, septembre 2018.
3. Art. 5 et s., Directive préc.
4. Art. 38 et s., Directive préc. et notamment art. 50 et s. qui régissent les contrats-cadres.
5. V. H. Claret, « Plateformes numériques et protection des données personnelles du consommateur », *Contrats-Concurrence-Consommation*, juillet 2018, Études 10, spéc. n° 6 : « *La notion même de données personnelles est entendue largement et leur nature extra-patrimoniale ou patrimoniale n'est pas précisée ; s'il paraît consacrer la première conception, la seconde n'en est pas absente.* »

données patrimoniales, tels que les types de comptes ouverts au nom des clients, la fréquence, le montant et le type des opérations qui y sont portées, l'amplitude des variations des soldes des comptes et le montant des mêmes soldes à un instant « T » sont, tout autant que les données extrapatrimoniales, des données à caractère personnel. Le confirme la définition du Règlement du 27 avril 2016[6] selon lequel l'expression « données à caractère personnel » désigne « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée")* »[7], le règlement ajoutant qu'« *est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[8]. Le confirme également l'article 2 de la loi du 6 janvier 1978[9], telle que modifiée notamment par les lois des 7 octobre 2016[10] et 20 juin 2018[11] selon lequel « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ».

4. Ces définitions, qui ne distinguent pas selon le type d'information, patrimoniale ou extrapatrimoniale, interpellent car elles ne prennent en considération que les seules personnes physiques ; les personnes morales ne sont pas visées. Ce qui n'est pas étonnant en raison de l'objet du RGDP qui est d'établir « *des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données* »[12]. Est-ce à dire que ces personnes morales sont sans protection ? La réponse est assurément négative en raison du secret bancaire[13] dont le fondement est la protection des clients, personnes physiques comme personnes morales[14].

6. Règlement(UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
7. Art. 4, point 1, Règlement préc.
8. Art. préc.
9. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
10. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
11. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. V. M. Bourgeois et M. Moine, « La nouvelle loi informatique et libertés, Une transposition du RGPD ? », *JCP* 2018, éd. E, 1417.
12. Art. 1, § 1, Règlement préc.
13. Art. L 511-33, Code monétaire et financier.
14. La Cour de cassation vise, dans ses arrêts, l'article 9 du Code civil (v. not. Cass. com. 8 juill. 2004, *Banque et Droit* n° 93, janv.-févr. 2004. 54, obs. Th. Bonneau ; Cass. com. 21 sept. 2010, *Banque et Droit* n° 134, nov.-déc. 2010. 21, obs. Th. Bonneau ; *Rev. trim. dr. com.* 2010. 761, obs. D. Legeais ; *Rev. dr. bancaire et financier*, mars-avril 2011, com. n° 35 p. 49, note F-J. Crédot et Th. Samin).

5. Les données à caractère personnel sont quotidiennement recueillies par les établissements de crédit dans le cadre de leurs activités. Cela n'est pas étonnant car ces informations sont indispensables à la bonne exécution des opérations de clientèle tels que les virements, les paiements par carte ou autres services de paiement. Et comme les établissements de crédit, comme tout professionnel, souhaitent développer leurs activités avec leurs clients, ils sont tentés de les traiter afin d'approfondir leur connaissance de leurs clients, ce qui est utile pour cerner leurs besoins, et par voie de conséquence pour déterminer les services et opérations qu'ils peuvent opportunément leur proposer.

6. D'où l'importance, pour les établissements de crédit et autres prestataires de services de paiement, du RGDP car ce règlement définit ce qui est possible et ce qui est impossible en matière de traitement des données. Étant observé qu'il pose un certain nombre de principes en matière de traitement[15] et reconnaît des droits aux personnes concernées par les données à caractère personnel : les clients ont en particulier un droit d'accès qui s'analyse en un droit de confirmation et d'information[16], un droit à la portabilité, qui est le droit de récupérer les données à caractère personnel et de les transmettre à un tiers sans avoir à obtenir l'autorisation du responsable du traitement[17], et un droit à l'oubli, et donc à l'effacement desdites données[18].

7. Le droit à la portabilité n'est pas sans interpeller, car il conduit à un partage de données par les établissements de crédit avec d'autres prestataires de services bancaires, ce qui est d'autant plus notable que ce partage de données, qui participe de l'*open banking*[19], est imposé aux établissements de crédit ; il n'est pas volontaire de leur part. Le droit à la portabilité rejoint le partage des données imposées par la DSP2 dont l'objectif est la mise en place et le renforcement, via l'accroissement de la concurrence, d'un marché unique des services de paiement. Ce qui explique que les établissements de crédit se soient vus imposer de communiquer les informations qu'ils détiennent, en particulier aux professionnels qui fournissent le service d'initiation de paiement, défini comme « *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* »[20].

8. L'accès des tiers à des informations détenues par d'autres et sans leur consentement traduit un changement de paradigme qui révèle un changement de culture, en particulier pour le monde bancaire car il impose « *de passer d'une culture du secret à une culture de l'accès aux données dans le domaine bancaire et financier* »[21]. Ce qui explique sans doute les réticences, qui sont d'autant plus grandes lorsque les informations sont communiquées à des tiers qui ne sont pas soumis aux mêmes exigences professionnelles que les personnes qui détenaient les informations – on pense en particulier aux fournisseurs informatiques en nuage – le fameux *cloud*[22] – et les difficultés d'adaptation que certains peuvent éprouver, étant observé que les textes sont complexes et que leur compréhension n'est pas aisée.

9. La difficulté n'est pas négligeable lorsque l'on prend en considération un seul texte. Aussi est-ce une évidence de dire que la difficulté est accrue lorsqu'il convient de combiner plusieurs textes. Laquelle est d'autant moins ordinaire que les objectifs des textes ne sont pas les mêmes : pour l'un, à savoir la DSP 2, organiser un marché unique des services de paiement ; pour l'autre, et donc le RGDP, protéger les libertés et droits fondamentaux des personnes physiques[23]. Et, bien sûr, si l'on ajoute des éléments d'extranéité pour envisager la protection des données dans un cadre international, la complexité semble atteindre son paroxysme.

10. C'est dire toute la difficulté du thème du présent colloque qui a été construit en deux temps. Dans un premier temps, on va essayer de voir comment la DSP 2 et le RGDP s'articulent : messieurs Richard, Storrer, Plankensteiner et Jouffin vont nous apporter leur lumière en ce qui concerne l'accès, le statut et le transfert des données à caractère personnel. Dans un second temps, c'est la mise en musique des textes qui va nous être exposée. Cette tâche est revenue à mesdames Laïdi et Chatellier-Chamoulaud. Que tous nos intervenants, sans oublier madame Nerbonne qui va évoquer la position du régulateur, soient chaleureusement remerciés pour leurs présentations qui seront assurément passionnantes. ●

15. Art. 8, Règlement préc.
16. Art. 15, Règlement préc.
17. Art. 20, Règlement préc.
18. Art. 17, Règlement préc.
19. V. Th. Bonneau, « *Open banking* et services de paiements », in *Régulation bancaire et financière européenne et internationale*, 4e éd., 2018, Bruylant, p 765 et s.
20. Art. 4, point 15, Directive préc.
21. V. G. Capelle-Blancard, R. Bellando et R. Lacroix, « L'accès aux données bancaires et financières : une misison de service public », Rapport du groupe de travail du Cnis, juillet 2015, spéc. la recommandation n° 11 : « *le groupe de travail recommande que la Banque de France formalise sa procédure d'accès aux données confidentielles et qu'elle diffuse un guide d'accès comme le font par exemple la Bundebank et la Banque d'Angleterre* ».
22. V. not. R. Perray, « L'externalisation des données des Fintech : les risques du Cloud », *rev. dr. banc. et financier*, janvier-février 2017, dossier 9.
23. Art. 1, § 2, Règlement préc.

QUALIFICATION

Statut et gouvernance de la donnée dans la DSP 2*

Dans la DSP 2, les données acquièrent un véritable « statut », même si elles sont diversement nommées (donnéers de sécurité, de paiement, à caractère personnel…) et peuvent être diversement catégorisées (nécessaires, obligées, convoitées…). Elles font également l'objet de règles de gouvernance, au travers des contrats, de la responsabilité du traitement et du contrôle interne.

PIERRE STORRER**
Avocat à la Cour

Kramer Levin Naftalis & Frankel LLP

1. Conjonction… et disjonction. Soit, d'une part, entré en application le 13 janvier 2018, un texte majeur (du moins dans son domaine) : la DSP 2[1], majeur en ceci qu'il fait entrer de plain-pied sur la scène juridique les données de compte, les données de paiement, toutes massivement à caractère personnel, sans quoi elles n'intéresseraient pas ceux qui les convoitent. Cela a un nom : l'*open banking*, la DSP 2 pouvant être considérée comme le premier grand texte de réglementation, en même temps que de consécration, de ce phénomène proprement remarquable d'ouverture des comptes de paiement, et de leurs données, à d'autres qui ne les tiennent pas, le tout à la main (faut-il l'espérer tremblante, comme elle devrait l'être avant de s'engager dans un acte grave ?) du payeur, titulaire du ou des comptes.

Soit, d'autre part, applicable à compter du 25 mai 2018, le règlement que l'on attendait depuis vingt ans : le RGPD[2], qui est de toutes les conversations – y compris Outre-Atlantique –, comme si la protection (mais n'oublions pas leur libre circulation) des données à caractère personnel était devenue le symbole de l'esprit juridique européen, sa réglementation son chef-d'œuvre[3]. À telle enseigne que l'on avait presque oublié qu'existaient aussi et encore, et même en nombre, des données non personnelles, qu'un tout petit règlement traite désormais : le règlement (UE) 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[4].

* Le présent article étant le fruit d'une conférence, il en a gardé le ton.
** Les propos de l'auteur n'engagent que celui-ci.

1. Dir. (UE) 2015/2366, 25 nov. 2015, concernant les services de paiement dans le marché intérieur, abrogeant Dir. 2007/64/CE, 13 nov. 2007 (DSP 1).
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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
3. Voir encore Ord. n° 2018-1125, 12 déc. 2018, prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
4. Cf. P. Storrer, « À l'heure du règlement européen relatif au libre flux des données à caractère non personnel », RTDF n° 4-2018, déc. 2018, p. 76

La conjonction entre DSP 2 et RGPD est ainsi un événement considérable, l'événement de l'année 2018, dont les conséquences iront bien au-delà de celle-ci, ne serait-ce que pour trouver les clés d'articulation entre la directive et le règlement. Mais, assez curieusement somme toute, disjonction aussi, dans la mesure où la DSP 2 n'est pas, faute d'un petit décalage (aurait-on pu le combler ?), « *GDPR by design* ». Presque contemporaine du RGPD, la DSP 2 se réfère en effet encore à l'antique directive de 1995, en particulier lorsque son article 94 dispose que « *la communication aux personnes d'informations sur le traitement des données à caractère personnel et le traitement de ces données à caractère personnel ainsi que tout autre traitement de données à caractère personnel aux fins de la présente directive sont effectués conformément à la directive 95/46/CE et aux règles nationales transposant ladite directive, ainsi qu'au règlement (CE) n° 45/2001* ». Et ce n'est pas l'artifice de cet autre article 94 (du RGPD cette fois : « *Les références faites à la directive abrogée s'entendent comme faites au présent règlement* ») qui permettra de réduire l'anachronisme.

2. Des difficultés d'articulation ? La question de l'articulation entre les deux textes s'est vite posée. On se souvient que, en mars 2018, dans sa *FinTech Roadmap*, l'Autorité bancaire européenne (ABE ou EBA) se préoccupait de l'interaction entre la DSP 2 (PSD2) et le RGPD (GDPR) : « *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* »[5].

> “Données d'authentification, les données de sécurité personnalisées sont naturellement au cœur du dispositif de la DSP 2.”

Difficultés d'articulation[6] ? En tout cas complexité, a répondu le nouveau European Data Protection Board (EDBP), aux termes d'une lettre (PSD2 Letter) qui n'est pas passée inaperçue parmi les professionnels et annonce d'emblée : « *The legal framework regarding the protection of personal data in the context of PSD2 is complex and developments in this regard are therefore being monitored by the EDPB*[7]. » On y reviendra.

3. Plan. Il ne fait guère de doute que la donnée acquiert un véritable « statut » dans la DSP 2, au sens étymologique qu'elle s'y « tient debout » et, ce faisant, fait l'objet de diverses règles et régimes de protection. Partant, la donnée est l'objet de règles de « gouvernance », terme ayant acquis droit de cité, notamment en matière bancaire et financière.

Statut (I.) et gouvernance (II.) de la donnée dans la DSP 2 – plutôt dans la DSP 2 telle que transposée dans notre Code monétaire et financier (CMF) – à l'heure du RGPD seront sans surprise les deux thèmes de cette contribution, qui sera loin de les épuiser.

I. STATUT DE LA DONNÉE

4. Catégorisation. La donnée ou, plutôt, les données, doit-on dire, car à lire la DSP 2, il nous est apparu que la donnée se présente sous divers aspects. Les données sont en effet diversement nommées (1.) ; il est ensuite des cas où les données apparaissent comme nécessaires ou obligées (2.) et, enfin et surtout, d'autres cas où elles sont convoitées, convoitise de l'*open banking* à l'origine de la deuxième génération de DSP (3.).

1. Données nommées

5. Données de sécurité personnalisées. On ne parle dorénavant plus de « dispositif » mais de « *données de sécurité personnalisées* », qui s'entendent « *des 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), issu de DSP 2, art. 4, 31)).

Données d'authentification, les données de sécurité personnalisées sont naturellement au cœur du dispositif de la DSP 2, non seulement pour protéger les fonds des utilisateurs de services de paiement et pour limiter les risques de fraude, mais aussi et avant tout afin d'empêcher l'accès non autorisé au compte de paiement[8]. Si bien que les nouveaux acteurs d'accès aux comptes, eux-mêmes nommés de manière inédite – prestataires de services d'initiation de paiement (PSIP) et prestataires de services d'information sur les comptes (PSIC), faisant ressortir la catégorie nouvelle des prestataires de services de paiement gestionnaires de comptes (PSPGC) – doivent spécialement veiller à ce que lesdites données ne soient pas accessibles à d'autres que leur titulaire et leur émetteur, le plus souvent PSPGC (CMF, art. L. 133-40 et L. 133-41, issus de DSP 2, art. 66 et 67).

On n'oublie pas, enfin, que la confidentialité et l'intégrité des données de sécurité personnalisées font l'objet de normes techniques de réglementation (dites « RTS ») particulières, prévues aux articles 22 et suivants du fameux règlement délégué 2018/389 du 27 novembre 2017 complétant la DSP 2 par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication, concernant tant leur création et transmission, association avec l'utilisateur, livraison, renouvellement, et destruction, désactivation et révocation.

5. *The EBA's Fintech Roadmap, Conclusion from the consultation on the EBA's approach to financial technology (Fintech)*, 15 mars 2018, n° 87.

6. Cf. 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 », *RD bancaire et fin.* 2018, étude 1 ; et « Données personnelles : articulation de la Directive sur les Services de Paiement 2 et du Règlement général sur la protection des données – Acte II : suite et fin ? », *RD bancaire et fin.* 2018, étude 20.

7. EDPB-84-2018, 5 juillet 2018.

8. Cf. DSP 2, cons. 69.

6. Données de paiement sensibles. Nous avons déjà eu l'occasion de le dire, leur définition est décevante, dans la mesure où ce sont toutes données (y compris de sécurité personnalisées) « *qui sont susceptibles d'être utilisées pour commettre une fraude* » (CMF, art. L. 133-4, g) issu de DSP 2, art. 4, 32)).

Quoi qu'il en soit, et alors même que leur occurrence, dans la DSP 2, est limitée, il faut remarquer que la protection des données de paiement sensibles fait désormais partie des exigences premières d'un dossier d'agrément de prestataire de services de paiement (PSP) : « *Pour délivrer l'agrément à un établissement de paiement, l'Autorité de contrôle prudentiel et de résolution vérifie que, compte tenu de la nécessité de garantir une gestion saine et prudente de l'établissement de paiement, celui-ci dispose pour son activité de prestation de services de paiement d'une gouvernance et d'un contrôle interne adéquat, 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, al. 1er, issu de DSP 2, art. 5,1, g))[9]. Prescription relative à la protection des données de paiement sensibles que l'on trouve détaillée dans les importantes orientations de l'ABE sur les informations à fournir pour l'agrément d'établissement de paiement (EP) et d'établissement de monnaie électronique (EME) et pour l'enregistrement de PSIC au titre de l'article 5, paragraphe 5, de la DSP 2.[10].

Les données de paiement sensibles, faut-il encore observer, sont soustraites aux PSIP et PSIC : les premiers ne peuvent les stocker (CMF, art. L. 133-40, II, 5°, issu de DSP 2, art. 66, 3, e)), les seconds les demander (CMF, art. L. 133-41, II, 5°, issu DSP 2, art. 67, 2, e)), étant précisé que, vis-à-vis des uns et des autres, dans le cadre de leur activité, le nom du titulaire du compte et le numéro du compte (IBAN) n'en constituent exceptionnellement pas.

7. Données à caractère personnel. Leur irruption, dans la DSP 2 et, par voie de conséquence, dans le CMF, est sans nul doute une affaire importante.

Jugeons sur pièces :

– un principe général, d'abord, exigeant nécessité et consentement exprès : « *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, issu de DSP 2, art. 94, 2) ;

– une permission légale, ensuite : « *Les systèmes de paiement et les prestataires de services de paiement sont autorisés à traiter des données à caractère personnel lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements.* [...] » (CMF, art. L. 521-6, issu de DSP 2, art. 94, 1) ;

– la compétence exceptionnelle (car dérogatoire à celle de l'ACPR) de la CNIL, enfin : « *Par dérogation aux dispositions de l'article L. 612-1, la Commission nationale de l'informatique et des libertés veille au respect des dispositions des articles L. 521-5 et L. 521-6 en utilisant les compétences qui lui sont reconnues par le règlement (UE) 2016/679 du Parlement européen et du Conseil. À cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives aux infractions aux dispositions des articles L. 521-5 et L. 521-6* » (CMF, art. L. 561-7).

L'observatoire de la sécurité des moyens de paiement a ainsi pu observer, dans son rapport annuel 2017, que « *le RGPD s'applique dans son intégralité aux traitements de données à caractère personnel effectués par les prestataires de services de paiement (PSP), que ces traitements relèvent ou non de la DSP 2. Par exemple, les PSP doivent se conformer aux obligations de documentation (registre et étude d'impact relative à la protection des données, le cas échéant), de pertinence des données par rapport à l'objectif poursuivi, ou encore d'information préalable quant aux caractéristiques des traitements, et enfin de respect des droits d'accès, d'opposition, etc.* » (p. 18, encadré 3).

> “La protection des données de paiement sensibles fait partie des exigences premières d'un dossier d'agrément de prestataire de services de paiement (PSP).”

2. Entre données nécessaires et données obligées

8. Données nécessaires à l'exécution des services de paiement et à la lutte contre la fraude. Nous revenons par là aux données à caractère personnel, dont le traitement, dorénavant, suppose qu'elles soient, de manière générale, nécessaires à l'exécution des services de paiement ou, particulièrement, nécessaires à la lutte contre la fraude. En observant à cet égard que l'article 96, 6 de la DSP 2 fait obligation aux PSP de fournir, au moins annuellement, à leurs autorités compétentes, des données statistiques relatives à la fraude liée aux différents moyens de paiement ; obligations que des orientations adoptées par l'ABE le 17 septembre 2018 sont venues éclairées 11.

Où l'on retrouve, non sans contradiction on le verra, l'exigence de nécessité – souvent associée à celle de proportionnalité – si chère au RGPD, lorsque par exemple le texte pose les principes relatifs au traitement des données (art. 5) ou les conditions de sa licéité (art. 6).

9. Données d'authentification (forte). On retombe ici sur les données de sécurité personnalisées, dans leur fonction d'authentification « forte », qui est l'une des grandes innovations de la DSP 2. L'exigence d'authentification forte figure au point 1 de l'emblématique article 97 de la DSP 2 : « *Les États membres veillent à ce qu'un prestataire de services de paiement applique l'authentification forte du client*

9. Pour les établissements de monnaie électronique, cf. CMF, art. L. 526-8, I, al. 1er.

10. EBA/GL/2017/09, 8 nov. 2017. Comp. Orientations de l'ABE relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liées aux services de paiement dans le cadre de la DSP 2, EBA/GL/2017/17, 12 janv. 2018, point 4.3 : « *Les PSP devraient veiller à la confidentialité, l'intégrité et la disponibilité de leurs actifs logiques et physiques critiques, ressources et données de paiement sensibles de leurs USP qu'elles soient stockées, en transit ou en cours d'utilisation* ».

11. EBA/GL/2018/05. Cf. Avis de l'ACPR de mise en œuvre des orientations du 18 décembre 2018.

lorsque le payeur : / a) accède à son compte de paiement en ligne ; / b) initie une opération de paiement électronique ; / c) exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse »[12].

Mis à part les pouvoirs publics, voire certains utilisateurs précautionneux, personne ou presque n'aime l'authentification forte – ni n'a aimé, du moins au départ, 3Dsecure – qui perturbera nécessairement le « parcours client ». D'où l'intérêt porté par marchands ou prestataires sans comptes, entre autres, aux dérogations permises par le règlement 2018/389 (art. 10 et s.). Or parmi celles-ci, il en est une générale, tirée de l'« *analyse des risques liés à l'opération* » (*risk scoring*), qui veut qu'un PSP soit autorisé à ne pas appliquer l'authentification forte du client après qu'il s'est assuré que l'opération de paiement considérée présente un faible niveau de risque (art. 18). Pourquoi la distingue-t-on des autres ? Et bien parce que, à défaut d'authentification forte, c'est une masse considérable de

> “Mis à part les pouvoirs publics, voire certains utilisateurs précautionneux, personne ou presque n'aime l'authentification forte, qui perturbera nécessairement le « parcours client ».”

données (à caractère personnel) que le PSP doit recueillir. Ainsi ne doit-il avoir décelé, à l'issue d'une « *analyse en temps réel des risques* », ni « *des dépenses anormales ou un type de comportement anormal du payeur* », ni « *une localisation anormale du payeur* » ou ni « *une localisation du bénéficiaire présentant des risques élevés* » ; et encore faut-il qu'il tienne compte des « *habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement* », de l'« *historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement* » ou de l'« *identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement* » (art. 18, 2, c), i), v) et vi), et 3, a), b) et d)).

On conviendra que de la dispense d'authentification forte est au prix d'une intrusion plus que forte dans la vie numérique des utilisateurs de services de paiement.

10. Données de LCB-FT. Nous sortons sans doute un peu de notre sujet en abordant celui de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT), qui relève évidemment d'un autre corps de règles que celui de la DSP 2.

Mais on ne peut parler de « données » dans le cadre du paiement, évoquer leur « statut », en passant sous silence cette réalité qu'elles sont, qu'il est emporté(es) par la vague irrépressible de l'identification obligée des clients, désormais formellement doublée par la vérification de celle-ci (KYC)[13]. En y ajoutant que, bientôt, l'identification électronique, au sens du règlement eIDAS[14], prévaudra certainement sur les mesures archaïques mises en œuvre aujourd'hui ; qu'il en sera bien fini des quelques parcelles d'anonymat qui demeuraient encore, qui ne peuvent résister longtemps au « *traitement invasif* » des données, pour reprendre une expression de l'ancien contrôleur européen de la protection des données (CEPD)[15].

Quoi qu'il en soit, remarquons cette originalité qu'est le « *droit d'accès indirect aux données* » de l'article L. 561-45 du CMF : « *Lorsque des données à caractère personnel font l'objet d'un traitement aux seules fins de l'application des articles L. 561-5 à L. 561-23 par une personne mentionnée à l'article L. 561-2, le droit d'accès s'exerce auprès de la Commission nationale de l'informatique et des libertés.* [...] ».

3. Données convoitées

11. Renvoi. Nous passerons rapidement sur la principale « innovation DSP 2 » qu'est l'accès aux comptes par d'autres qui ne le tiennent pas, spécialement traitée par M. Guillaume Richard dans son exposé sur les nouveaux droits d'accès aux comptes et aux données de compte, pour nous contenter de quelques observations.

12. L'accès aux comptes : un droit des utilisateurs de services de paiement. Il n'a jamais été question, à notre connaissance, de donner un droit d'accès à tel ou tel prestataire nouveau, mais bien de (re)donner pouvoir aux utilisateurs – aux payeurs en particulier – de consentir à ce que d'autres que les PSPGC puissent avoir accès aux comptes dont ils (les utilisateurs) sont titulaires. En somme, la titularité l'emporte sur la gestion, sans même évoquer la question de la propriété, hors de propos (comme pour les données à caractère personnel au demeurant).

13. L'accès aux comptes : des différentes manières d'y accéder. On le sait, les prestataires sans comptes ne sont pas deux, mais trois :

– les premiers, émetteurs d'instruments de paiement lié à une carte, peuvent bénéficier, sur consentement exprès de leurs clients payeurs donné au PSPGC et à eux-mêmes, d'un « droit d'interrogation » : interrogation du solde du compte et confirmation par ce dernier que le montant nécessaire à l'exécution de l'opération de paiement liée à une carte est disponible (CMF, art. L. 133-39, issu de DSP 2, art. 65) ;

– comme leur nom l'indique, les seconds, PSIP, se voient accorder un « droit d'initiation » de paiement à partir de comptes qu'ils ne tiennent pas, sur la foi du consentement explicite (le législateur français, même par voie d'ordonnance, aurait pu choisir entre « exprès » ou « explicite ») du payeur (CMF, art. L. 133-40, issu de DSP 2, art. 66)

– les troisièmes, les PSIC, diffèrent des deux premiers en ce que leur matière première n'est pas le paiement, mais bien les données de paiement (ou de compte) (CMF, art. L. 133-41, issu de DSP 2, art. 67) et, en cela, participent bien de cette économie de la donnée que la Commission européenne nous vend (ou nous vante) depuis quelques années déjà.

14. L'accès aux comptes : l'enjeu des données. La sécurisation des données ainsi « ouvertes à tous les vents », ou presque, est naturellement au cœur du règlement délégué 2018/389 qui, outre le sujet de l'authentification forte, traite également de la protection de la confidentialité et de l'intégrité des données de sécurité personnalisées ainsi que de la mise en place de normes ouvertes communes et sécurisées de communication entre PSPGC et PSIP et PSIC ; normes qui, à n'en pas douter, donneront naissance à une réglementation, voire un droit (et une gouvernance) des interfaces d'accès ou API.

II. GOUVERNANCE DE LA DONNÉE

15. Gouvernance ? Nous employons le terme de « gouvernance » au sens désormais admis par les textes de droit bancaire, CRD 4 bien sûr, mais désormais aussi la DSP 2 qui, au titre des conditions d'octroi de l'agrément, impose aux PSP de disposer « *d'un solide dispositif de gouvernance d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités qui soit bien défini, transparent et cohérent, des procédures efficaces de détection, de gestion, de contrôle et de déclaration des risques auxquels il est ou pourrait être exposé et des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines* »[16].

16. Modes. En nous concentrant de manière privilégiée, cette fois, sur les données à caractère personnel – sujet de ce colloque –, contrat (1.), responsabilité du traitement (2.) et, enfin, contrôle interne (3.) sont les trois modes de gouvernance que nous aborderons.

1. Contrat

17. L'hypertrophie de la clause RGPD. Il y a eu comme un phénomène de « passage à l'an 2000 du RGPD », un avant et un après 25 mai 2018, une sorte d'« hystérisation » qui a soufflé sur la mise à jour RGPD des contrats bancaires (conventions de compte, contrats-cadres de services de paiement, etc.).

Si bien que nous avons vu passer nombre de contrats de paiement où l'incorporation des règles nouvelles de la DSP 2, par nature prioritaire, avait marqué le pas face à l'hypertrophie de la clause RGPD (souvent doublée par une « politique de confidentialité » tout aussi ampoulée), tellement verbeuse qu'elle disait tout hormis les quelques mesures élémentaires de gouvernance des données à caractère personnel.

Sauf à ce que les contrats bancaires ou para-bancaires ne soient plus que des contrats de traitement de données à caractère personnel – ce qui nous étonnerait –, voilà une inversion des choses qui ne laisse pas de nous étonner.

18. Consentement et nécessité ? Faut-il que l'utilisateur de services de paiement consente expressément, ou explicitement, au traitement de ses données à caractère personnel ? Si oui, comme semble l'exiger l'article L. 521-5 du CMF, n'y-a-t-il pas une contradiction *in adjecto* à imposer, de surcroît, que l'accès auxdites données par le PSP soit nécessaire à l'exécution de leurs services de paiement ?

Car, si nous avons bien lu le RGPD et ses différents commentaires, la nécessité du traitement emporte la négation du consentement, nie toute manifestation de volonté libre

> “Si nous avons bien lu le RGPD et ses différents commentaires, la nécessité du traitement emporte la négation du consentement.”

dès lors que la personne concernée n'est plus en mesure de refuser de consentir. Tel est l'objet du curieux point 4 de l'article 7 du règlement : « *Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat* ». De sorte que le Groupe de travail « Article 29 » sur la protection des données a pu écrire : « *Si un responsable du traitement cherche à traiter des données qui sont effectivement nécessaires à l'exécution d'un contrat, le consentement n'est alors pas la base juridique appropriée*[17]. »

Nécessité et consentement ne vont pas ensemble, y compris en matière de protection des données à caractère personnel : « *Soit le traitement est nécessaire à l'exécution d'un contrat, soit un consentement (libre) doit être obtenu* »[18]. La DSP 2 aurait ainsi fait preuve d'un excès de « zèle protecteur » en doublant l'exigence de nécessité par celle d'un consentement, qui plus est explicite. Or la condition de nécessité se suffisait parfaitement à elle-même, puisque la licéité du traitement peut très bien reposer sur ceci : « *le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci* » (RGPD, art. 6, 1, b). Partant, si l'on considère que la DSP 2 n'est pas une lex specialis du RGPD, ou que l'article 94, 2 de la DSP 2 ne crée pas une base légale nouvelle mais doit être interprété à la lumière

12. Voir encore CMF, art. L. 133-44, I.

13. Voir, en dernier lieu, ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, 14 déc. 2018.

14. Règl. (UE) n° 910/2014, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dont les mesures d'identification électronique intègrent désormais IIIe CMF au titre de l'exécution des obligation de vigilance.

15. Cf. Avis 1/2017 du CEPD sur la proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE – Accès aux informations sur les bénéficiaires effectifs et conséquences sur la protection des données, 2 févr. 2017.

16. DSP 2, art. 11, 4, reprenant quasi exactement les termes de l'art. 74, 1 de CRD 4. Voir encore ABE, Orientations sur la gouvernance interne, EBA/GL/2017/11, 21 mars 2018.

17. Lignes directrices sur le consentement au sens du règlement 2016/679, adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2019, WP259 rév. 01, p. 10.

18. Groupe de travail « Article 29 » sur la protection des données, Avis 15/2011 sur la définition du consentement, adopté le 13 juillet 2011, WP 187, p. 8.

du RGPD[19], on a un problème… quoiqu'en pense l'EDBP, qui cherche à concilier, d'une main à l'autre, ce qui paraît difficile de l'être : « *The EDPB is of the view that the "explicit consent" referred to in Article 94 (2) of PSD2 is a contractual consent. Payment services are always provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of PSD2, "This Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider." In terms of the GDPR, the legal basis for the processing of personal data is Article 6 (1) (b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party. We consider that, in view of the foregoing, Article 94(2) of PSD2 should be interpreted, on the one hand, in coherence with the applicable data protection legal framework and, on the other hand, in a way that preserves its useful effect. This implies that Article 94 (2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject. The concept of explicit consent under Article 94(2) of PSD2 is therefore an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR* » [20].

2. Responsabilité du traitement

19. Qui fait quoi ? On a vu et lu, à cet égard, tout et son contraire, dès lors que le modèle contractuel faisait apparaître d'autres intervenants que seulement l'utilisateur de services de paiement et son prestataire, notamment agents (de services de paiement) et nouveaux prestataires de services d'initiation de paiement et/ou d'information sur les comptes.

Comme si, là encore, les « mots » du RGPD étaient entourés d'une sorte de vertu auto-qualificatrice, tels ou tels étaient indifféremment tantôt nommés « *responsables du traitement* », tantôt « *sous-traitant* », et inversement ; mots auto-qualificateurs qui, au final, ne qualifient plus rien. Faut-il que l'on ne sache pas, ou plus, qui sont, naturellement, les uns et les autres ? Ce n'est pas à exclure.

20. Responsabilité conjointe ? Il serait tout de même embêtant, en droit des paiements comme ailleurs, de buter sur une notion aussi prégnante de la protection des données à caractère personnel. D'autant que, si nous lisons bien les travaux en la matière, « *le rôle premier de la notion de responsable du traitement est de déterminer qui est chargé de faire respecter les règles de protection des données, et comment les personnes concernées peuvent exercer leurs droits dans la pratique. En d'autres termes, il s'agit d'attribuer les responsabilités* [21]. »

Ou alors faut-il considérer que les traitements mis en œuvre par les uns et les autres, à l'heure de l'économie de la donnée, y compris de la donnée de paiement, sont tellement imbriqués les uns aux autres, que la détermination de leurs responsables serait vaine ? On ne peut dès lors écarter l'hypothèse qu'il faille se satisfaire de la qualification, remise au goût du jour, de « *responsables conjoints du traitement* », au sens où l'article 26, 1 du RGPD nous dit que « *lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement* ». Peut-être, à condition de ne pas oublier que cette économie de qualification, en amont, se répercute, en aval, sur la nécessaire répartition contractuelle et transparente, entre responsables conjoints, de leurs obligations respectives, notamment en ce qui concerne l'exercice des droits de la personne concernée, destinataire des grandes lignes de l'accord que les responsables conjoints du traitement auront passé entre eux (RGPD, art. 26, 1, 2 et 3).

Notons, pour finir sur ce point, que l'avis précité 1/2010 sur les notions de « *responsable du traitement* » et de « *sous-traitant* » donnait cet exemple intéressant sur les « *transactions financières* » : « *Prenons maintenant l'exemple d'une banque qui a recours à un service de messagerie financière pour réaliser ses transactions financières. La banque et le service de messagerie conviennent des moyens du traitement des données financières. Le traitement des données à caractère personnel concernant les transactions financières est réalisé en premier lieu par l'établissement financier et, seulement après, par le service de messagerie financière. Cependant, même si au niveau individuel, chacune de ces entités poursuit sa propre finalité, au niveau global, les différentes phases, les finalités et les moyens du traitement sont étroitement liés. Dans cet exemple, la banque et le service de messagerie peuvent être considérés comme coresponsables* [22]. »

3. Contrôle interne

21. *Accountablity* et conformité. Ce n'est pas une révélation mais, associé à la matière bancaire et financière, le principe « cardinal » d'*accountability* (mal traduit par le terme de « responsabilité »), posé au point 2 de l'article 5 du RGPD, est potentiellement explosif : « *Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité)* » [23].

Explosif ? Nécessairement, dans la mesure où cette disposition, en apparence anodine (et curieusement non exposée dans les considérants du RGPD), fait basculer la protection des données à caractère personnel dans une logique de « conformité » (on aime à dire compliance aujourd'hui), clairement mise en œuvre aux articles 24 et suivants, à commencer par ceci : « *Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire* » (RGPD, art. 24, 1). Fichtre, ne serait-ce qu'en regard de ce seul bout de texte qui introduit les obligations générales du responsable du traitement – et sans même parler de *privacy by design*, etc. –, la tâche est immense !

22. Faut-il réécrire l'arrêté du 3 novembre 2014 ? La question se pose, nous semble-t-il, à l'égard des établissements relevant de l'arrêté du 3 novembre 2014 relatif au contrôle interne, c'est-à-dire aux entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'ACPR. Car le thème de la gouvernance (dispositifs, procédures) des données, quelles qu'elles soient (donc pas seulement celles à caractère personnel), y est évidemment absent, cependant que les impératifs de conformité (et les risques de non-conformité [24]) ne cessent de croître.

Réécrire l'arrêté de 2014, non pas en ce qui concerne, directement, les données à caractère personnel : on a vu que compétence exceptionnelle, en matière de services de paiement, a été donnée à la CNIL (cf. CMF, art. L. 521-7) ; il faudra toutefois que celle-ci se coordonne avec celle-là (ACPR), voire avec la Banque de France, elle-même nouvellement investie de s'assurer de la sécurité de « *l'accès aux comptes de paiement et à leurs informations* » dans le cadre des nouveaux services d'initiation de paiement et d'information sur les comptes (CMF, art. L. 521-8). Mais il s'agirait peut-être de réécrire l'arrêté relatif au contrôle interne à l'égard des données de sécurité personnalisées et autres données de paiement sensibles, ne serait-ce que pour y intégrer davantage le « risque informatique » et les mesures de cybersécurité propres à l'endiguer [25]. Avec cette difficulté qu'elles devraient majoritairement présenter un caractère personnel, sans quoi elles ne seraient pas convoitées. Et cette autre qu'il faudrait aussi aller voir du côté de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; du côté, encore, de la directive NIS (*Network and Information Security*)…

23. La question de l'anonymat, pour finir. Nous avions remarqué, lors de la lecture du règlement délégué 2018/389, la première phrase de son considérant 8 : « *En raison même de leur nature, les paiements effectués par l'intermédiaire d'instruments de paiement anonymes ne sont pas soumis à l'obligation d'authentification forte du client* ». « Anonyme », le mot devient rare dans la réglementation bancaire et financière.

DSP 2, RGPD : 2018 fut aussi marquée par les transpositions nationales chaotiques – la France ne fit pas exception – de la 4e directive Antiblanchiment [26] et par la publication de la 4e directive *bis* [27]. Or quel objectif immédiat poursuivent-elles ? La fin de l'anonymat des paiements et, pour cela, la chasse aux paiements en espèces, bien sûr, mais aussi en monnaie électronique ou en monnaies virtuelles ; le « requiem » même, pour reprendre les mots d'un auteur [28], de cet « anonyme », qui caractérise les sociétés du même nom (voire toutes les sociétés par actions), avec la recherche du bénéficiaire effectif ultime. Et si, en paiement comme ailleurs, nous n'avions pas besoin de préserver une petite, voire infime, part d'anonymat ? Un peu d'anonymat n'est-il pas le meilleur garant de nos données à caractère personnel [29] ? Du respect de (l'intimité de) notre vie privée ? Or autant nous pouvons faire l'économie de nous exhiber sur les réseaux sociaux, autant il devient impossible de ne pas payer à l'aide d'instruments électroniques. Nécessité et consentement, toujours et encore… ●

> « Faut-il considérer que les traitements mis en œuvre par les uns et les autres, à l'heure de l'économie de la donnée, sont tellement imbriqués les uns aux autres, que la détermination de leurs responsables serait vaine ? »

19. En ce sens, P. Silva (European Commission, DG FISMA), Interaction between PSD2 and GDPR. Adde, Observatoire de la sécurité des moyens de paiement, Rapport annuel 2017 précit., p. 18, encadré 3.
20. PS2 Letter, précit.
21. Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », adopté le 16 février 2010, WP 169, p. 4.
22. WP 169, p. 22.
23. En anglais : « *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')* ».
24. Cf. Arr. 3 nov. 2014 relatif au contrôle interne, art. art. 10, p) : « *Risque de non-conformité : le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législative ou réglementaire, nationales ou européennes directement applicables, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions des dirigeants effectifs prises notamment en application des orientations de l'organe de surveillance* ».
25. Cf. ACPR, *Le risque informatique*, Document de réflexion, mars 2018, dont l'annexe relative à la catégorisation du risque informatique.
26. Dir. (UE) 2015/849, 20 mai 2015, relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux ou du financement du terrorisme.
27. Dir. (UE) 2018/843, 30 mai 2018, modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.
28. R. Mortier, *Requiem pour l'anonymat*, Recueil Dalloz n° 36, 18 oct. 2018, 1977.
29. Comp. RGPD, cons. 26.

L'ARTICULATION DES TEXTES : UN CASSE-TÊTE RÉGLEMENTAIRE

Nouveau droit d'accès aux comptes et aux données des comptes

Le nouveau droit d'accès aux comptes et aux données de compte établi par la DSP 2 pose la question du périmètre d'application de ce dernier, des modalités d'accès à ces données et des finalités possibles pour leur utilisation par les nouveaux PSP.

GUILLAUME RICHARD
Responsable juridique
Direction des Affaires juridiques
Crédit Agricole SA

Pour comprendre le nouveau régime juridique des services d'initiation de paiement et d'information sur les comptes, il est important de revenir en quelques mots introductifs sur les objectifs et principales évolutions apportées par la DSP 2[1].

Avec ce texte, le législateur européen a souhaité étendre le champ d'application des dispositions existantes au sein de l'Union européenne, renforcer les droits des utilisateurs de services de paiement et la sécurité dans ce domaine. Il a aussi, et surtout, ouvert le marché des paiements aux « *nouveaux acteurs des paiements* ». La DSP 2 a offert un cadre légal aux nombreuses sociétés (principalement des *FinTechs*) qui fournissaient déjà depuis de nombreuses années, des services dits « d'agrégation » ou d'initiation de paiement, y compris en France.

L'Europe, qui a souhaité protéger ces entreprises, leur a ainsi permis un développement serein et sécurisé au sein de l'Union. Le marché des paiements, qui jusqu'alors était le monopole des établissements de crédit, établissements de paiement et autres Prestataires de Services de Paiement (PSP) s'est, au final, ouvert à la concurrence.

C'est l'ordonnance de transposition de la DSP 2 en droit français[2], entrée en vigueur le 13 janvier 2018, qui a introduit dans le Code monétaire et financier (CMF) ces deux nouveaux services de paiement : le service d'information sur les comptes[3] et le service d'initiation de paiement[4].

Ces deux services, qui peuvent être fournis par trois types de PSP[5] sont définis à l'article D. 314-2 du CMF.

Le service d'initiation de paiement est 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* ».

Le service d'information sur les comptes est, quant à lui, un « *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 services de paiement* ».

1. Directive 2015/2366 du 25 novembre 2015 relative aux services de paiement dans le marché intérieur.
2. Ordonnance 2017-1252 du 9 août 2017.
3. Art. L. 314-1 7°) du CMF
4. Art. L. 314-1 7°) du CMF.
5. Art. L. 521-2 du CMF : les établissements de crédit, les établissements de paiement et les prestataires de services d'information sur les comptes (PSIC).

NOUVEAU DROIT D'ACCÈS AUX COMPTES ET AUX DONNÉES DE COMPTE

Pourquoi évoquer un « *nouveau droit d'accès aux comptes et aux données de compte* » ?

Ces définitions sont claires. Il s'agit de permettre à l'utilisateur d'accéder à ses comptes et d'ordonner des paiements sans être obligé d'utiliser, exclusivement, les interfaces mis à disposition par sa banque (espaces de banque en ligne sur Internet, applications mobiles).

En imposant aux banques de traiter « *sans aucune discrimination autre que fondée sur des raisons objectives* »[6] les demandes de données ou les ordres de paiement transmis par les PSP fournissant ces deux services, et en interdisant, en parallèle, de subordonner leur fourniture à l'existence de relations contractuelles entre elles et ses PSP[7], la DSP 2 leur a également imposé d'ouvrir à ces PSP leurs systèmes d'information, allant, de fait, au-delà d'une simple possibilité offerte aux utilisateurs d'user de ces nouveaux services de paiement « intermédiés ». Et c'est ainsi que les questions d'interprétation juridique débutent...

LA BATAILLE POUR LA DONNÉE DE PAIEMENT : CHRONIQUE D'UN CASSE-TÊTE RÉGLEMENTAIRE ANNONCÉ

L'introduction de ces nouveaux services dans notre droit a sonné le commencement d'une bataille entre les banques teneurs de comptes et ces nouveaux acteurs du paiement autour du nouvel or noir qu'est la donnée de paiement.

Si nous devions nous livrer à un classement des données bancaires, on distinguerait trois catégories[8] :

– les données issues de la relation banque/client : pour simplifier, il s'agirait des données obligatoires permettant de répondre aux obligations en matière de connaissance client (identité, sexe, âge, catégorie socioprofessionnelle, situation financière, etc.) ;

– les données d'authentification : numéro de carte bancaire, nom, code d'accès, cryptogramme visuel, etc. ;

– les données issues des paiements (montant de la transaction, nom du commerçant, panier moyen) et toutes les informations sur le profil de l'utilisateur que l'on peut en déduire : composition du foyer, habitude de vie, orientation politique, sexuelle, etc.

Il est dès lors très simple de comprendre à quel point la donnée de paiement constitue une véritable manne : l'ingénierie en matière d'analyse de la donnée (autrement appelée « *data mining* ») offre des possibilités, presque illimitées, de connaissance, dans les moindres détails, de la vie privée et intime de tout à chacun.

Jusqu'à présent, les banques gestionnaires de compte disposaient d'un monopole sur la détention de cette donnée. Elles disposaient donc, seule, de cette capacité illimitée de connaissance de leurs clients et de l'opportunité d'en user pour développer leur activité (profilage, analyse comportementale, etc.).

L'arrivée de ces nouveaux acteurs de paiement n'est pas sans soulever de vastes questions juridiques sur l'exploitation de ce gisement traditionnellement réservé aux banques.

QUEL PÉRIMÈTRE POUR CE NOUVEAU DROIT D'ACCÈS ?

Il n'y a d'abord aucun doute sur le fait que la DSP 2 ne réglemente les services d'initiation de paiement et d'information sur les comptes que sur le périmètre des comptes de paiement.

La définition de ces services est, à ce titre, parfaitement univoque. Il s'agit, pour ce qui est du service d'information sur les comptes de « *fournir des informations consolidées concernant un ou plusieurs comptes de paiement* ». Il s'agit, pour ce qui est du service d'initiation de paiement, « *d'initier un ordre de paiement [...] concernant un compte de paiement* ».

Rappelons que sont des comptes de paiement, les comptes détenus au nom d'un ou de plusieurs utilisateurs de services de paiement et qui sont utilisés aux fins de l'exécution d'opérations de paiement : les comptes de dépôt à vue et les comptes ouverts par les établissements de paiement sont des comptes de paiement[9]. En revanche, les comptes d'épargne (ou de titres) ne relèvent pas de cette catégorie puisqu'ils n'ont pas pour finalité d'exécuter des opérations de paiement quotidiennes[10]. L'Ordonnance qui a transposé la DSP 2 au sein du Code Monétaire et Financier est conforme à ce périmètre[11].

Notons, par ailleurs, que le Code monétaire et financier impose désormais aux PSP proposant ces nouveaux services de paiement de respecter des conditions strictes pour leur exercice : des formalités préalables à réaliser auprès de l'ACPR (demandes d'agrément simplifié pour la fourniture du service d'initiation de paiement ; enregistrement pour les PSPIC fournissant uniquement le service d'information sur les comptes 12), des mesures strictes à mettre en place pour garantir la sécurité des données des utilisateurs[13] et des modes de communication sécurisés entre les PSP[14].

6. Art. L. 133-40 III et L. 133-41 III du CMF.
7. Art. L. 133-40 III et L. 133-41 III du CMF.
8. « Données. De quelques notions sur la propriété des données de paiement », *Revue Banque*, novembre 2017.
9. Art. 4 12 DSP 2, art. L. 314-1 CMF, art. L. 522-4 du CMF.
10. On notera que certains types de compte d'épargne, tel que le livret A, peuvent toutefois permettre de façon accessoire et limitative, l'exécution d'opération de paiement sans pour autant recevoir la qualification de compte de paiement au sens du CMF puisque leur finalité n'est pas, exclusivement, l'exécution d'opérations de paiement : Pierre Storrer, « Brèves remarques sur le compte de paiement », *Revue Banque* n° 788 du 13 oct. 2015.
11. Rappelons que la DSP 2 étant une directive d'harmonisation maximale, les textes de transposition ne pouvaient pas aller au-delà du seul périmètre prévu par la DSP 2.
12. Art. L. 522-11-2 du CMF.
13. Art. L. 133-40 II et L. 133-41 II du CMF.
14. Canaux sécurisés des art. L. 133-40 II 4° et L. 133-41 II 3° du CMF.

Qu'en est-il, dès lors, d'un service « d'agrégation » qui serait rendu hors du périmètre « compte de paiement » ? Cette question n'est aucunement théorique puisque ces services, bien avant d'être encadrés par la réglementation, s'exerçaient, sans distinction sur l'ensemble du périmètre des produits et services détenus par les clients dans les livres de leur banque.

Devons-nous considérer qu'en l'absence de texte spécial, tant européen que français, régulant ou interdisant ces services sur ce périmètre, ils peuvent être fournis librement, sans aucune règle ou obligation ? Ou devons-nous, à l'inverse, considérer que l'accès aux autres informations et types de comptes est désormais interdit (ce qui aurait pour conséquence de réduire drastiquement l'intérêt de ces services...) ? En l'absence de contraintes particulières sur le périmètre des comptes de placement, la technique dite du « *webscrapping* », dont on sait qu'elle est loin d'assurer un niveau de sécurité pour les utilisateurs, peut-elle continuer à perdurer ?

Avoir d'une part, un cadre juridique très contraignant pour l'accès aux données issues des comptes de paiement (tant pour les teneurs de comptes que pour les PSP fournissant ces services) et, d'autre part, une absence totale de texte spécial, tant européen que français, encadrant l'accès aux données issues des autres produits et services bancaires accessibles en ligne, est source d'une grande insécurité juridique et semble, qui plus est, en contradiction avec les objectifs de la DSP 2 qui entendait « *garantir la sécurité des opérations de paiement et la protection des consommateurs contre les risques de fraude* »[15].

L'analyse qui consisterait à considérer qu'en l'absence de textes régulant l'accès aux données hors comptes de paiement, ces services peuvent être fournis librement semble discutable. Comment, en effet, concevoir que, pour une même typologie d'activité (un service visant à restituer des informations issues de produits et services accessibles depuis un service de banque en ligne) mettant en relation les mêmes parties (teneurs de compte, clients et tiers de paiement), on assujettisse, lorsqu'elle est fournie sur le périmètre des comptes de paiement, les prestataires et la fourniture de ce service à des conditions strictes d'accès à cette activité et on permette, à l'inverse et lorsque cette même activité serait fournie sur des comptes d'épargne (ou sur des données issues d'autres types de produits ou services financiers, tel que le crédit), un accès totalement libre à ces données sans aucune contrainte, de sécurité ou prudentielle ?

De surcroît, cette absence de cadre légal et de dispositifs techniques imposés par les normes européennes sur le périmètre hors « comptes de paiement » pourrait poser d'autres questions pour les établissements teneurs de compte. Quid du respect de leurs obligations en matière de secret professionnel/bancaire[16] ? Quid du respect de leurs obligations en matière de protection des données personnelles[17] ? Quid du respect des contrats conclus avec leurs clients qui interdisent, pour la plupart, la communication à des tiers des identifiants fournis pour la connexion aux espaces de banque en ligne ?

La cohérence et la sécurité juridique devraient donc conduire à considérer qu'en l'absence de textes spéciaux, ces services ne peuvent pas être légalement fournis sur les données hors comptes de paiement et ne pourront l'être que dans un cadre légal et réglementaire spécial et adapté.

Néanmoins, cette question de l'accès aux données hors comptes de paiement étant non régulée, il n'est pas certain que le superviseur bancaire se déclare compétente et se prononce de façon ferme sur la question. Notons toutefois que l'ACPR a déjà indiqué que, « *s'agissant de la réglementation française, à défaut de modification du cadre réglementaire qui leur est applicable, les conditions d'accessibilité des comptes utilisés à des fins autres que l'exécution d'opérations de paiement ne devraient pas être modifiées par la transposition de la DSP 2. Ainsi, à défaut de dispositions contraires, les prestataires gestionnaires de compte n'auront aucune obligation d'ouvrir l'accès à ces comptes et les PSIC n'auront aucun droit de l'exiger*[18]. » En d'autres termes, le Superviseur semble considérer que, sur ce périmètre non réglementé (i) les teneurs de compte n'auraient, contrairement au périmètre couvrant les comptes de paiement, aucune obligation d'ouvrir les accès et pourraient imposer une contractualisation avec les tiers de paiement et (ii) les tiers de paiement n'auraient aucun droit d'imposer l'ouverture de ces accès.

QUELLES MODALITÉS POUR ACCÉDER AUX COMPTES ?

La deuxième problématique juridique porte sur les modalités d'accès aux comptes et aux conditions de licéité des traitements des données (de paiement) mis en place à l'occasion de la fourniture de ces deux nouveaux services.

Les termes employés par les articles du CMF introduits à l'occasion de la transposition de la DSP 2 peuvent en effet laisser perplexes et ne sont pas sans poser certaines difficultés d'application.

Les paramètres de l'équation sont les suivants :

– (1) l'article L. 133-40 I du CMF, dans la liste des conditions devant être respectées pour la fourniture du service d'initiation de paiement, dispose que le payeur doit « *donner son consentement explicite à l'exécution d'un paiement* ». L'article L. 133-41 I, relatif quant à lui aux conditions de fourniture du service d'information sur les comptes, prescrit que le PSP fournissant le service « *1° Recueille le consentement exprès de l'utilisateur de services de paiement* ». En parallèle, le nouvel article L. 521-5 du CMF, qui s'applique à tous les PSP quel que soit le service de paiement qu'ils fournissent, dispose désormais que « *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* » ;

– (2) le RGPD[19] prescrit quant à lui qu'un traitement de données personnelles, pour qu'il soit licite, soit fondé sur un des fondements juridiques prescrits par son article 6[20].

Le RGPD a significativement renforcé la place du consentement en matière de traitement de données et ses conditions de recueil. Le consentement est défini, dans son article 4.11, comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement.* » Le RGPD dispose, en outre, dans son article 7, que « *la personne concernée a le droit de retirer son consentement à tout moment.* »

Doit-on dès lors considérer que le consentement cité par les articles L. 521-5, L. 133-40 et 41 du CMF correspond au consentement requis par l'article 6.1.a) du RGPD et qu'il impose ainsi le consentement comme seule base juridique possible aux traitements de données sous-jacents aux services d'initiation de paiement et d'information sur les comptes ? Une réponse affirmative pourrait complexifier de façon significative les modalités de souscription et de fourniture de ces services afin d'être en conformité avec les conditions fixées par les dispositions du RGPD en la matière. Si les dispositions de l'article L. 521-5 du CMF, qui cite explicitement les notions « *d'accès, de traitement et de conservation* » des données à caractère personnel, semblent limpides, une telle conclusion pourrait être trop hâtive.

Il apparaît d'abord très discutable de considérer que le recueil d'un consentement dans le cadre de la conclusion d'un contrat cadre de service de paiement puisse l'être librement de la part de son utilisateur. Les données personnelles collectées à l'occasion d'un tel contrat sont, en théorie, nécessaires à l'exécution même du service de paiement concerné[21]. Dès lors, si un utilisateur venait à refuser la collecte et le traitement de ces données personnelles dans ce contexte, l'adhésion à ce service lui serait obligatoirement refusé par le PSP. L'utilisateur est-il, dans ces conditions, en mesure d'exprimer librement son consentement ? Les lignes directrices du G29 en matière de consentement[22] sont, sur ce point, claires puisqu'elles précisent que « *l'adjectif "libre" implique un choix et un contrôle réel pour la personne concernée. En règle générale, le RGPD dispose que si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives si elle ne donne pas son consentement, le consentement n'est pas valable. Si le consentement est présenté comme une partie non négociable des conditions générales, l'on considère qu'il n'a pas été donné librement. Le consentement ne sera par conséquent pas considéré comme étant donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.* »

Il apparaît tout aussi discutable de considérer qu'un utilisateur de service de paiement puisse retirer à tout moment son consentement aux traitements de données nécessaires à l'exécution du contrat comme le prescrit l'article 7 du RGPD. En effet, dans un tel cas, comment un PSP serait-il en mesure de respecter ses obligations en matière de lutte contre le blanchiment sur les opérations réalisées avant le retrait de ce consentement, alors même que le CMF, dans son article L. 521-6, permet également de traiter les données pour « *garantir la prévention, la recherche et la détection des fraudes en matière de paiement* » ?

Il semble, en réalité, que conclure de la sorte reviendrait à lier intrinsèquement le consentement donné par l'utilisateur au contrat de prestation de service et le consentement que ce même utilisateur donnerait pour le traitement de ses données à caractère personnel, ce qui apparaît contraire à la volonté du RGPD[23].

> “Le RGPD a significativement renforcé la place du consentement en matière de traitement de données et ses conditions de recueil.”

Quoi qu'il en soit, le débat pourrait avoir été tranché par le « Comité européen de la protection des données » (EDPB) dans une lettre en réponse adressée le 5 juillet dernier à une parlementaire européenne[24] sur ce sujet. Le consentement visé par le Code monétaire et financier ferait ainsi référence, non pas au consentement requis par le RGPD pour fonder le traitement des données, mais uniquement au consentement donné par l'utilisateur dans le cadre de la contractualisation du service, laissant ainsi le soin au PSP fournissant le service de fonder lesdits traitements sur les autres bases juridiques listés par le RGPD (l'exécution du contrat ou le respect de ses obligations légales).

QUELLES FINALITÉS POSSIBLES POUR L'UTILISATION DES DONNÉES DE PAIEMENT ?

La troisième et dernière problématique juridique (la principale ?) qui nous occupera est relative aux finalités qu'il est possible de mettre en place pour l'utilisation

15. Considérant n° 33 de la DSP 2.
16. Cette pratique du *webscrapping* met en effet, par nature, les établissements dans l'impossibilité de recueillir un accord express et spécifique de leurs clients pour lever le secret professionnel au profit des prestataires proposant ces services.
17. Notamment les obligations de sécurité prescrites par l'art. 32 du RGPD.
18. Propos recueillis par la société SYRTALS auprès de Jean-Claude Huyssen, directeur de la direction des agréments, des autorisations et de la réglementation de l'ACPR et publiés dans un rapport de novembre 2016.
19. Règlement n° 2016/679 du Parlement européen et du Conseil 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.
20. Exécution d'un contrat, respect d'une obligation légale, intérêt légitime du responsable de traitement, sauvegarde des intérêts vitaux de la personne, exécution d'une mission d'intérêt public, le consentement de la personne concernée.
21. Ce que précise d'ailleurs ce même art. L. 521-5 du CMF.
22. Lignes directrices 17/FR - WP259 rév.01 révisées et adoptées le 10 avril 2018.
23. Considérant 43 du RGPD et Lignes directrices 17/FR-WP259 rév.01 révisées et adoptées le 10 avril 2018.
24. Mme Sophie in't Veld.

des données de paiement auxquelles ont accès ces nouveaux acteurs.

Les dispositions du CMF ne prohibent pas expressément l'utilisation des données de paiement à des fins commerciales (profilage, prospection ciblée sur l'analyse comportementale des clients). Il est toutefois précisé dans les articles L. 133-40 II 7° et L. 133-41 II 6° que lorsqu'ils fournissent leurs services [d'initiation de paiement ou d'information sur les comptes], « *le prestataire de services de paiement [...] n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par le payeur qu'aux seuls fins de la fourniture du service d'information sur les comptes expressément demandée par l'utilisateur de services de paiement* ».

> “Les dispositions du CMF ne prohibent pas expressément l'utilisation des données de paiement à des fins commerciales.”

Doit-on dès lors considérer que ces articles limitent pour le PSP, purement et simplement, l'utilisation des données à la seule finalité de fourniture du service considéré, quelle que soit la finalité complémentaire que ce PSP souhaiterait mettre en place (à des fins commerciales ou autres) ?

Comme pour la problématique précédente, on pourrait s'arrêter à une lecture stricte de ces articles qui, textuellement, semblent être parfaitement clairs. Néanmoins, et comme pour la problématique précédente, une réponse plus nuancée s'impose.

Avant même de parler de la volonté de mettre en place des traitements à des fins commerciales avec les données de paiement collectées à l'occasion de la fourniture des services d'initiation ou d'information sur les comptes, on ne peut ignorer que les acteurs qui fournissent ces services depuis plusieurs années ne se contentent pas de restituer à leurs utilisateurs des soldes et des listes d'opérations de paiement. Le service d'information sur les comptes est presque systématiquement accompagné d'une panoplie de fonctionnalités « accessoires » : catégorisation d'opérations, calculs prévisionnels de solde, assistants budgétaires, aides et conseils pour la gestion de ses finances personnelles.

D'un point de vue strictement juridique, ces fonctionnalités n'entrent pas dans le champ de la définition du service d'information sur les comptes qui, selon l'article D. 314-2 du Code monétaire et financier, ne consiste qu'à « *fournir des informations consolidées concernant un ou plusieurs comptes de paiement* ».

Considérer que les articles L. 133-40 et L. 133-41 du CMF prohibent purement et simplement les traitements de données dès lors qu'ils n'auraient pas pour finalité la stricte fourniture des services d'initiation ou d'information devrait, en conséquence, conduire à prohiber la fourniture de ses fonctionnalités complémentaires par ces acteurs.

Peut-être faut-il davantage chercher dans les formulations employées par le Code monétaire et financier une réaffirmation du principe de « minimisation » édictée par l'article 5.1.c) du RGPD[25]. Le CMF précise au demeurant : « *Lorsqu'il fournit* » [le service d'initiation de paiement/d'information sur les comptes], ce qui ne semble nullement interdire aux PSP fournissant ces services de fournir, par ailleurs, d'autres services (de paiement ou d'autres sortes) et pourquoi pas des fonctionnalités dont la finalité serait, précisément, la connaissance des besoins des utilisateurs et la fourniture de propositions commerciales adaptées à leur profil, leurs habitudes de vie, etc.

Rappelons, en complément, que l'article L. 521-6 du CMF précise que les PSP peuvent mettre en place d'autres traitements de données que ceux servant strictement à la fourniture de leurs services de paiement et que ceux-ci doivent être mis en place conformément aux dispositions du RGPD[26].

REPLACER LE CONSOMMATEUR AU CENTRE DES SERVICES DE PAIEMENT

Ces questions juridiques mettent en évidence une certaine imprécision rédactionnelle de la DSP 2 et de ses textes de transposition. Au-delà, cette situation reste source d'insécurité juridique et pourrait porter préjudice aux intérêts des consommateurs dont la protection était, pourtant, un des objectifs de la DPS2.

Sans renier l'intérêt intellectuel que présente la poursuite des réflexions autour de ces questionnements, un nouveau cadre légal a été créé : il présente certes des imperfections, mais il pose les bases et conditions d'exercice de services régulés et sécurisés.

Les acteurs en présence ne sont que les dépositaires des données de paiement et en aucun cas les propriétaires. Il ne nous reste dès lors qu'à espérer que la bataille pour la donnée de paiement se gagne par l'inventivité dont l'ensemble de la profession saura faire preuve pour proposer de nouveaux services simples, performants et innovants plutôt que par la défense d'un monopole ou d'un pré carré. ●

25. « *Les données à caractère personnel doivent être [...] adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).* »

26. « *[...] le traitement de ces données à caractère personnel ainsi que tout autre traitement de données à caractère personnel sont effectués conformément aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil et du règlement (CE) 45/2001 du Parlement européen et du Conseil.* »

TRANSFERTS SUBIS

Cloud Act: nouvelle manifestation de l'extraterritorialité des textes US et réponse européenne

Adopté en mars 2018, le *Cloud Act* permet aux autorités américaines d'obtenir des données stockées par des entreprises américaines en dehors des États-Unis, dans le cadre d'enquêtes judiciaires criminelles. La Commission européenne a publié en avril 2018 le paquet « *e-evidence* », sous forme d'une proposition d'une directive et d'un règlement qui permettent d'envisager une réciprocité dans la collecte d'information.

BLANDINE EGGRICKX
Analyses stratégiques et réglementation européenne

EMMANUEL JOUFFIN
Docteur en droit
Responsable juridique de banque

Adopté le 23 mars 2018, le *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) est une loi fédérale des États-Unis amendant la loi *Stored Communications Act* (SCA) de 1986[1]. Le *Cloud Act* permet aux autorités américaines, s'agissant d'enquêtes judiciaires criminelles, d'obtenir des données stockées par des entreprises américaines[2] en dehors des États-Unis, sans avoir recours à des Traités d'entraide judiciaire (TEJ).

I. PÉRIMÈTRE D'APPLICATION DU *CLOUD ACT*

Les données demandées doivent concerner des « US *persons* »[3], c'est-à-dire des citoyens ou ressortissants des États-Unis, des étrangers légalement admis en tant que résident permanent, ou encore des sociétés incorporées aux États-Unis. On doit toutefois souligner que des « non US *persons* » peuvent être visées par des demandes.

Dans ce cas, c'est au prestataire d'élever une contestation dans un délai de 14 jours de la réception de la demande[4] s'il remplit deux conditions cumulatives : la divulgation des données reviendrait à enfreindre les lois[5] d'un gouvernement étranger « *qualifié* »[6] et la personne visée n'est pas une « US person » et ne réside pas États-Unis. Cependant, pour être un gouvernement étranger « *qualifié* », il faut avoir conclu au préalable un accord bilatéral avec les États-Unis qui encadre les demandes d'accès directes des autorités américaines et de permettre la réciprocité.

On soulignera, le *Cloud Act* permet la conclusion d'accords bilatéraux entre les États-Unis et des États étrangers afin d'encadrer les demandes d'accès directes des autorités américaines et de permettre la réciprocité. Ces accords ne conditionnent pas l'entrée en vigueur du *Cloud Act*, mais ils sont toutefois une condition de recevabilité des recours des prestataires.

1. La SCA a été codifiée au Chapitre 18 du US Code traitant notamment de la divulgation de communications sur support électronique détenues par des fournisseurs de services.
2. Sont visés des fournisseurs de services de communications électroniques (les opérateurs de communications électroniques et les fournisseurs d'un accès à un service de communication) mais aussi les prestataires d'informatique en nuage et les fournisseurs d'accès à un service informatique à distance.
3. *Cloud Act* § 2523. *Executive agreements on access to data by foreign governments* – (a) DEFINITIONS. Voir Tableau.
4. *Cloud Act* § 2713 (h) (2) (A) al. 2.
5. Le risque auquel s'expose le prestataire qui, se pliant au *Cloud Act*, violerait le droit local, ne doit pas être uniquement théorique. Il faut envisager la probabilité de sanctions importantes.
6. « *Qualifying Foreign Government* » (QFG).

On notera que le 5 février 2019, sous l'impulsion du Conseil, la Commission européenne a publié une recommandation[7], afin qu'elle soit autorisée à négocier, au nom de l'Union, un accord avec les États-Unis sur l'accès transfrontalier des autorités judiciaires aux preuves électroniques. Les négociations porteront sur l'accès en temps utile aux preuves électroniques, la résolution des différends juridiques notamment en clarifiant les obligations juridiques et en garantissant des droits réciproques à toutes les parties et, enfin, l'existence de garanties solides en ce qui concerne la protection des données et de la vie privée, des droits fondamentaux, notamment au regard des principes de nécessité et de proportionnalité.

II. QUELLES RÉPONSES DE LA FRANCE ET DE L'EUROPE ?

1. La France

La préoccupation des pouvoirs publics au sujet de l'extraterritorialité de la législation américaine est réelle[8], autant que celle des ministères de l'Intérieur de l'Économie et des Finances. En 2017, le ministère de l'Intérieur[9] alertait déjà sur la portée extraterritoriale de certaines législations et préconisait de « *préférer des prestataires français, ou à défaut européens, dont les serveurs sont situés dans l'Hexagone ou dans un pays membre de l'Union européenne* ». Cette recommandation a été formulée à nouveau par le ministère de l'Économie, notamment dans le cadre de la stratégie cloud de la France[10] et l'opportunité de créer un cloud hébergeant les données des autorités françaises. À ce jour, la CNIL ne s'est pas prononcée sur la question de la cohabitation du *Cloud Act* avec les principes du RGPD. Toutefois, seule une réponse concertée au niveau européen semble être à la mesure des enjeux.

2. L'Europe : proposition d'un Paquet « *e-evidence* » par la Commission européenne

Le 17 avril 2018, la Commission européenne a publié un paquet de mesures destinées à permettre aux autorités policières et judiciaires d'obtenir plus rapidement les preuves électroniques détenues par des prestataires de services établis dans un autre État membre ou en dehors de l'Union européenne.

Le Paquet « *e-evidence* » contient ainsi deux mesures complémentaires, sous la forme d'une directive et d'un règlement. Deux remarques s'imposent. Tout d'abord, à ce jour, aucun calendrier n'a été annoncé par le Parlement européen[11], bien que la Présidence autrichienne ait affirmé que l'adoption de ces propositions soit une priorité[12]. Par ailleurs, si ces propositions permettent d'envisager une réciprocité dans la collecte d'information, elles n'apportent aucune réponse, en termes de protection, s'agissant des demandes présentées sous l'égide du *Cloud Act*.

2.1. La proposition de directive sur la désignation des représentants légaux

La proposition Directive[13] a pour objet d'établir des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale[14]. Cette harmonisation devrait se traduire par la désignation d'un représentant légal dans l'Union en charge d'assurer la réception et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres. Seraient concernés les fournisseurs de services de communications électroniques (traditionnels et les nouveaux services basés sur l'internet comme les messageries instantanées, et les services de messagerie électronique), les prestataires de services détenant des données pour les besoins de la prestation qu'ils fournissent (réseaux sociaux, *marketplaces*), les prestataires de services d'hébergement et, enfin, les fournisseurs de noms de domaine ou de services d'adressage[15]. On notera que le texte exige un lien suffisant entre le prestataire et l'Union européenne[16].

2.2. Proposition de règlement[17] relatif aux injonctions européennes de production et de conservation

Cette proposition de règlement a pour but de créer des injonctions européennes de production et de conservation des preuves électroniques.

L'injonction européenne de production permettra à une autorité judiciaire d'un État membre de demander des preuves électroniques directement auprès d'un prestataire[18] offrant des services[19] dans l'Union, indépendamment de la localisation des données. L'injonction européenne de conservation permettra quant à elle à une autorité judiciaire d'un État membre de contraindre le prestataire à conserver certaines données afin que ladite autorité puisse en demander communication ultérieurement, par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production.

Ces deux injonctions devront être émises ou validées par une autorité judiciaire d'un État membre pour obte-

Les principales notions du *Cloud Act*, en bref

Thèmes	Commentaires
Les sociétés concernées	La rédaction du § 2713 du *Cloud Act* est compréhensive en ce qu'elle vise les « *providers of electronic communications services or remote computing services* »[1] et vise les données qui sont en dehors des USA et « *in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States* ». Les sociétés pouvant être l'objet d'une demande sous le visa du *Cloud Act* sont les fournisseurs de services de communications électroniques (les opérateurs de communications électroniques et les fournisseurs d'un accès à un service de communication), mais aussi les prestataires d'informatique en nuage et les fournisseurs d'accès à un service informatique à distance. Ces sociétés devront relever de la juridiction des États-Unis pour recevoir des demandes au titre du *Cloud Act*[2]. Le fait qu'une « *entreprise non américaine offre depuis l'étranger des services électroniques ciblés vers le marché américain (par exemple en ayant recours à de la publicité sur des sites américains* [...] *les autorités pourraient la considérer comme étant "within the United States"* »[3].
Les infractions	***Serious crime*** Le *Cloud Act* vise spécifiquement les « *serious crime, including terrorism* »[4], ainsi que la notion de « *threat of death or serious bodily harm to any person* »[5]. À titre d'exemple, l'article 37 du CFR (*United States Code of Federal Regulations*) donne la définition suivante : « *– Any criminal offense classified as a felony*[6] *under the laws of the United States, any state or any foreign country where the crime occurred; or* *– Any crime a necessary element of which, as determined by the statutory or common law definition of such crime in the jurisdiction where the crime occurred, includes interference with the administration of justice, false swearing, misrepresentation, fraud, willful failure to file income tax returns, deceit, bribery, extortion, misappropriation, theft, or an attempt or a conspiracy or solicitation of another to commit a serious crime.* » **Atteinte à la « *public safety* »** La notion de « *serious crime* » n'apparaît que s'agissant des demandes de communication tournées vers les États-Unis[7]. Il s'ensuit que les autorités US pourraient adresser des demandes de communication au sujet d'infractions très variées, relevant de la notion floue « *sécurité publique* ».
Les données[8]	Ces données peuvent aussi bien être des contenus, e-mails, des documents électroniques, que des métadonnées. Les données à caractère personnel sont bien entendu visées.
Les « *Qualifying Foreign Government* » – QFG	La signature d'un accord avec un « *qualifying foreign government* » (QFG) n'est pas une condition de mise en application du *Cloud Act*. mais l'une des deux conditions cumulatives nécessaires pour qu'un fournisseur de services puisse s'opposer à une demande de communication de données. Pour être QFG, un état devra satisfaire à un ensemble d'exigences très détaillées visées au § 2523 du *Cloud Act ((b) Executive agreement requirements*), lesquelles sont satisfaites par application du RGPD. Au titre des critères permettant de soumettre au Congrès américain un accord exécutif avec un État étranger, l'*Attorney General* devra fournir un certain nombre d'éléments justificatifs, portant notamment sur le niveau des garanties en matière de vie privée, de collecte de données et de respect d'un certain nombre de droits[9]. En l'absence d'*executive agreement* avec les États-Unis, il faudra alors recourir aux « *common law standards governing the availability or application of comity analysis* » c'est-à-dire, à la « *courtoisie internationale* » liée aux intérêts respectifs des États-Unis et de l'État où sont localisées les données, de l'importance et l'effectivité du risque contentieux qui pèse sur le fournisseur de services s'il exécute l'injonction et des liens tant du fournisseur de services que du titulaire des données avec les États-Unis ou encore à la possibilité d'accéder à ces données par d'autres moyens.

1. Définis par l'*Electronic Communications Privacy Act* de 1986 ; cf. l'*United States Code*, titre 18, § 2510(12) et 2711(2). Concerne les opérateurs de communications électroniques dont l'offre d'accès wifi publics, mais aussi les opérateurs des *cloud computing*.
2. L'exposé des motifs du *Cloud Act* fait référence aux prestataires « *subject to the jurisdiction of the United States* », il n'est donc pas impossible que soient concernées les sociétés ayant une filiale aux États-Unis et elles qui ont des activités ciblant le marché américain.
3. C.F.R. §515.329(d) et 31 C.F.R. §515.330(a)(2) cité par R. Bismuth, « *Every Cloud Has a Silver Lining* - Une analyse contextualisée de l'extraterritorialité du *Cloud Act* », JCP éd. E, n° 40, 4 oct. 2018, 1497 spéc. § 25.
4. "§ 2523. *Executive agreements on access to data by foreign governments* - DEFINITIONS.—In this section, spec. D.
5. *Idem* G.
6. De manière générale, infraction passible d'une peine d'emprisonnement supérieure à un an.
7. Cf. section 5 -3- D et les commentaires de P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières. - Remarques sur l'application du droit dans l'espace numérique à la lumière du *Cloud Act* », *Cahiers de droit de l'entreprise*, juill. 2018, du 1er juillet 2018.
8. § 2713 du *Cloud Act*.
9. Notamment : le respect de l'État de droit et du principe de non-discrimination, le respect des droits de l'homme, la protection contre les interceptions arbitraires ; le droit à un procès équitable ; la prohibition des arrestations arbitraires ; la prohibition de la torture ; des règles claires d'accès judiciaire aux données…

7. http://europa.eu/rapid/press-release_IP-19-843_fr.htm.
8. Rapport d'information fait au nom de la Commission des affaires européennes sur l'extraterritorialité des sanctions américaines, Par M. Philippe Bonnecarrère, 4 octobre 2018 ; Rapport par la Commission des affaires étrangères et la Commission des finances en conclusion des travaux d'une mission d'information constituée le 3 février 2016 sur l'extraterritorialité de la législation américaine, rapporteure Mme Karine Berger et enfin le 11 juillet 2018, le député Raphaël Gauvain, conjointement avec Christophe-André Frassa, a été missionné par le Premier ministre au sujet de la « loi de blocage » et les conséquences de la promulgation du *Cloud Act*.
9. Flash ingérence économique : https://www.economie.gouv.fr/files/dgsi-special-cybersecurite.pdf page 17.
10. Annoncée le 3 juillet 2018 par Mounir Mahjoubi. Cette stratégie s'appuie sur le développement de trois solutions « *cloud* » en fonction des usages et de la sensibilité des données avec un « *cloud* interne », hébergé par l'administration pour des données sensibles, un « *cloud* dédié » pour des données de sensibilité moindre, et un « *cloud* externe ».
11. La Commission parlementaire saisie au fond est « libertés civiles, justice et affaires intérieures » (LIBE).
12. La Présidence autrichienne a présenté une approche générale sur le Paquet lors de la réunion du Conseil « Justice et Affaires intérieures » des 6 et 7 décembre 2018 (document du Conseil : 10497/18). Par ailleurs, la Commission a également publié, le 23 octobre 2018, son programme de travail pour 2019. Les propositions de textes « e-evidence » sont listées dans l'annexe III « Les propositions prioritaires en attente » COM(2018) 800 final.
13. Proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale COM/2018/226 final - 2018/0107 (COD).
14. Peu importe si le prestataire est établi dans l'Union européenne s'il fournit des services dans un État membre.
15. Il s'agit ici des « prestataires de services » visés par le texte et définis à l'article 2 § 2 de la proposition de directive
16. Selon l'article 2 § 3, et le considérant 13 de la proposition de directive, l'existence de ce lien suffisant ou « lien étroit » correspond non seulement au fait que des utilisateurs aient accès au service dans l'État membre mais aussi l'existence d'un ciblage des activités du prestataire sur cet État membre. Ce ciblage est établi sur la base d'un ensemble de circonstances pertinentes (l'utilisation de la langue, de la devise de l'État membre, ou la possibilité de commander des biens et services)
17. Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD).
18. Selon l'article 7 sur les destinataires des injonctions, elles sont directement adressées au représentant légal désigné par le fournisseur de services (dans les conditions définies par la proposition de directive)
19. Le projet d'approche générale du Conseil du 30 novembre 2018 (15020/18), approuvée par les ministres européens de la Justice le vendredi 7 décembre 2018, exclut du champ d'application du règlement les services financiers visés à l'article 2, paragraphe 2, point b), de la directive 2006/123/CE. Cette précision apparaît à l'article 2 paragraphe 3 qui définit un fournisseur de service. Cette exclusion des services financiers du périmètre n'est cependant pas définitive puisqu'elle devra être également approuvée par le Parlement européen et la Commission lors des discussions en trilogue.

nir des données qui devront servir de preuves dans le cadre d'enquêtes judiciaires ou de procédures pénales 20. Dans le cas d'une injonction de production, les données doivent être transmises directement aux autorités de l'État membre[21] qui émet la demande sans passer par les autorités de l'État membre où est établi le fournisseur de services. Les prestataires concernés[22] sont les mêmes que pour la proposition de Directive sur la désignation de représentant légal.

Les données visées[23] sont catégorisées selon qu'il s'agisse de données « *hors contenus* », c'est-à-dire les données relatives à l'accès[24], les données relatives aux abonnés[25] et les données relatives aux transactions[26] et, d'autre part, les données de contenus.

Éléments de calendrier en relation avec le *Cloud Act*

23 mars 2018 : publication du *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*)

17 avril 2018 : publication par la Commission européenne du Paquet « *e-evidence* »

5 février 2019 : publication de la recommandation de la Commission européenne pour négocier un accord entre l'Union européenne et les États-Unis

18 février 2019 : inauguration du 8e *datacenter* d'Equinix par Bruno Le Maire, ministre de l'Économie et des Finances, lequel prend position sur le *Cloud Act* : « *nous voulons donner un mandat clair et ambitieux à la Commission européenne pour négocier avec les États-Unis* » et annonce une solution concrète : « *D'ici la fin de l'année 2019, nous souhaitons, avec le Premier ministre et avec le président de la République, disposer de premières propositions de mise en place d'un* cloud *sécurisé.* »

25 février 2019 : publication des lignes directrices de l'EBA en matière d'externalisation (*outsourcing*) remplaçant la recommandation 2017/03 de décembre 2017 sur les fournisseurs de *cloud*, en vigueur depuis juillet 2018.

Les droits des personnes concernées[27] comprennent, la possibilité de contester la légalité, la nécessité ou bien encore, la proportionnalité de l'injonction. Les personnes dont les données sont requises sont informées par l'autorité d'émission de l'existence d'une injonction européenne de production et des recours dont elles disposent. Néanmoins, il convient de noter que ces possibilités de recours ne concernent que l'injonction européenne de production. Aucun recours n'existe pour l'injonction européenne de conservation.

Pour ce qui concerne le prestataire, pour qu'une injonction soit valide, il faudra la confronter au droit de l'État membre destinataire, notamment si les données requises ou les fournisseurs de services sont protégés par une immunité[28] dans l'État concerné. Il conviendra également de tenir compte des éventuelles conséquences sur les intérêts fondamentaux de l'État membre comme la sécurité nationale et la défense, mais aussi de tenir compte de la nécessité de protéger les droits fondamentaux des individus. Ainsi, la proposition de règlement prévoit une procédure de réexamen de l'injonction européenne de production si celle-ci entraînait une violation d'une ou plusieurs lois d'un pays tiers pour l'un des motifs exprimé précédemment[29].

Concernant la procédure[30], les injonctions doivent faire figurer des informations précises pour que le fournisseur de services identifie et produise les données requises, ainsi qu'un raisonnement motivé sur la nécessité de la mesure. Les injonctions sont mises en œuvre au moyen d'un certificat d'injonction européenne de production (EPOC) ou de conservation (EPOC-PR) qui contiennent toutes les informations nécessaires, sauf le plein raisonnement sur la nécessité de la mesure. Ce sont les destinataires (représentants légaux des fournisseurs de services) qui reçoivent ces certificats et veillent à ce que les données soient transmises. En cas de non-respect de ces injonctions, la proposition met en place des mécanismes d'assistance entre États membres[31].

Les États membres fixeront des sanctions[32] pécuniaires effectives, proportionnées et dissuasives qui pourraient être imposées aux prestataires.

La question de principe que pose tout ceci est de savoir si la réponse à une situation clairement issue d'un rapport de force économique peut trouver sa solution dans des instruments juridiques. Il ne faut toutefois pas désespérer de l'effet « *soft power* » que peut représenter une réglementation telle que celle du RGPD, ce dernier semblant être en passe de devenir un standard international de protection des données, alors même que l'Europe ne dispose d'aucun mastodonte dans le domaine de la data. ●

20. L'article 4 revient sur les autorités compétentes pour émettre des injonctions européennes de production et de conservation. Ensuite, les articles 5 et 6 reviennent en détail sur les conditions d'émission générales des deux injonctions
21. Article 9 § 1 de la proposition de règlement.
22. La définition de fournisseur de services est la même que pour la proposition de directive. Cf. article 2 § 3 de la proposition de règlement.
23. Ces données sont définies dans l'article 2 paragraphes 7, 8, 9 et 10 de la proposition de règlement.
24. Données relatives au début et à la fin d'une session d'accès utilisateur à un service, y compris l'adresse IP, les données sur l'interface utilisée par l'utilisateur, l'identifiant de l'utilisateur, et les métadonnées de communications électroniques.
25. Données relatives à l'identité d'un client telles que le nom, la date de naissance, l'adresse postale, les données de paiement ; ainsi que les données sur le type de service, et sa durée.
26. Données qui servent à fournir des informations contextuelles ou supplémentaires sur le service, dont la source et la destination d'un message, les données sur l'emplacement du dispositif, la date, l'heure, le routage, le format, les métadonnées de communications électroniques
27. L'article 17 de la proposition de règlement revient sur les recours possibles des personnes qui sont directement suspectées et accusées mais aussi pour les personnes dont les données ont été obtenues mais qui ne sont ni suspectées, ni accusées.
28. L'article 18 de la proposition de règlement revient sur la garantie des privilèges et des immunités.
29. L'article 15 de la proposition de règlement décrit cette procédure de réexamen en cas d'obligations contradictoires basées sur les droits fondamentaux ou les intérêts fondamentaux d'un pays tiers. À l'article 16, il est également prévu une procédure de réexamen en cas d'obligations contradictoires basées sur d'autres motifs que ceux visés par l'article 15.
30. La procédure de mise en œuvre est décrite à l'article 8 de la proposition de règlement qui porte sur les certificats des injonctions européennes de production et de conservation. Les informations concernant leur exécution sont décrites aux articles 9 et 10.
31. Article 14 de la proposition de règlement.
32. Article 13 de la proposition de règlement.

TRANSFERTS VOULUS

L'encadrement des transferts internationaux des données

Le RGPD a consacré un principe général d'autorisation sous condition de transferts de données personnelles vers un pays tiers. L'article présente les règles régissant ces transferts internationaux, qu'il s'agisse de transferts de droit ou de transferts soumis à des conditions spécifiques.

MARCO PLANKENSTEINER
Partner, Speaker
Kramer Levin Naftalis & Frankel LLP

Alors que le droit positif avait pendant longtemps maintenu un principe général d'interdiction des transferts de données personnelles vers un pays tiers, le Règlement (UE) 2016/679 relatif à la protection des données personnelles (ci-après « RGPD » ou « Règlement ») est venu consacrer un principe général d'autorisation sous condition de tels transferts, prévus au Chapitre V du RGPD, qu'ils soient fondés sur une décision d'adéquation, réalisés moyennant des garanties appropriées, opérés dans le cadre de règles d'entreprise contraignantes, requis sur décision judiciaire ou administrative fondée sur un accord international, ou encore réalisés sur le fondement de dérogations pour des situations particulières.

Il s'agit dès lors de présenter les règles régissant les transferts internationaux de données « voulus », c'est-à-dire volontairement consentis par les intervenants dans le traitement des données. Seront d'abord évoqués les transferts de droit, puis les transferts soumis à des conditions spécifiques.

I. LES TRANSFERTS HORS UNION EUROPÉENNE DE DROIT

Les transferts de droit peuvent être réalisés soit sur le fondement d'une décision d'adéquation (1.), soit par le biais de clauses contractuelles types (2.). Il convient de noter d'emblée, que les différentes modalités de transferts de données hors Union européenne s'appliquent alternativement ou plus précisément en cascade, de telle sorte que la mise en place des garanties appropriées prévues à l'article 46 du RGPD, telle l'adoption de règles d'entreprises contraignantes, par exemple, ne s'impose que si le pays vers lequel les données personnelles sont transférées ne bénéficie pas d'une décision d'adéquation au sens de l'article 45 du RGPD.

1. Les transferts fondés sur une décision d'adéquation

Il existe un nombre réduit de situations pour lesquelles une décision d'adéquation permet de réaliser de droit un transfert. La liste des pays dits « adéquats » comprend, en l'état, Andorre, l'Argentine, le Canada, les États-Unis d'Amérique (partiellement), Guernesey, les Îles

Féroé, l'Île de Man, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay et bientôt le Japon[1]. Les décisions d'adéquation, adoptées par la Commission européenne sur le fondement de l'article 45 du RGPD, consistent en la reconnaissance que le pays tiers « *assure un niveau de protection adéquat.* » Trois séries de critères gouvernent l'appréciation de la Commission européenne : la législation du pays tiers, notamment en matière de protection des droits de l'homme et des libertés fondamentales, de sécurité publique, d'accès des autorités publiques aux données personnelles, de droits de la défense des personnes concernées, ainsi que le caractère effectif de leur recours ; l'existence d'une autorité de contrôle indépendante ; et les engagements internationaux en matière de protection des données personnelles.

Une fois la décision d'adéquation adoptée par la Commission européenne, le transfert des données est de droit, sans nécessiter d'autorisation préalable ou être assujetti à d'autres conditions. Cependant, l'admission au bénéfice de ce régime n'est pas définitive : l'adéquation doit être réévaluée par la Commission européenne au moins tous les quatre ans et la décision abrogée si le pays tiers n'assure plus un niveau de protection adéquat.

Par ailleurs, l'adéquation peut n'être que partielle pour un pays donné. Tel est notamment le cas de l'accord liant les États-Unis d'Amérique et l'Union européenne, couramment dénommé *Privacy Shield*. Celui-ci est entré en vigueur au 1er août 2016 pour remplacer l'accord dénommé *Safe Harbor*, invalidé par la Cour de Justice de l'Union européenne (CJUE) dans son arrêt *Schrems* du 6 octobre 2015[2]. Le mécanisme institué par le *Privacy Shield* est reconnu par la Commission européenne comme ayant un niveau de protection « *essentiellement équivalent* » aux exigences européennes. Il consiste en une auto-certification par les entreprises américaines soumises au pouvoir de la FTC (Commission fédérale américaine du commerce) ou du DoT (Département des transports américains). Il n'est donc pas applicable aux entreprises ne relevant pas du contrôle desdits organismes, ce qui exclut du bénéfice du *Privacy Shield* précisément les banques américaines, qui sont soumises au contrôle de la SEC. Cette circonstance n'exclut évidemment pas des transferts sur le fondement d'autres dispositifs prévus par le RGPD.

En pratique, pour pouvoir invoquer le bénéfice du *Privacy Shield*, le responsable des données doit accomplir certaines diligences avant tout transfert vers les États-Unis : vérifier que la société américaine dispose d'une certification active pour le type de données à transférer, cette certification étant réexaminée tous les ans ; informer la personne concernée du destinataire de ses données personnelles ; enfin, vérifier que l'utilisation des données est compatible avec les principes énumérés dans la réglementation européenne.

> “Les décisions d'adéquation adoptées par la Commission européenne consistent en la reconnaissance que le pays tiers « assure un niveau de protection adéquat ».”

Ce nouveau mécanisme a, lui aussi, fait l'objet de vives critiques. Une association irlandaise a formé un recours en annulation de la décision de la Commission européenne reconnaissant l'adéquation du *Privacy Shield* devant le Tribunal de l'Union, recours rejeté pour défaut d'un intérêt à agir de ladite association en sa qualité de personne morale ne bénéficiant pas de la protection des données personnelles[3]. Le Parlement européen a adopté récemment une résolution aux termes de laquelle il considère que « *l'actuel bouclier de protection des données n'offre pas le niveau de protection adéquat requis par le droit de l'Union en matière de protection des données et par la charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la Cour de Justice de l'Union européenne* »[4]. Affaire à suivre donc, car il n'est pas impossible que le futur réserve au *Privacy Shield* un sort analogue à son prédécesseur, le *Safe Harbour*.

2. Les transferts fondés sur des clauses contractuelles types (CCT)

En l'absence de décision d'adéquation au sens de l'article 45 du RGPD, un transfert vers un pays tiers pourra être réalisé moyennant les garanties appropriées prévues à l'article 46 du RGPD, qui se déclinent en différents dispositifs pouvant être utilisés par les responsables du traitement ou les sous-traitants selon les situations spécifiques dans lesquelles le transfert doit avoir lieu.

Les clauses contractuelles types (CCT) sont, sans doute, l'un des dispositifs les plus connus et employés par la pratique. Il s'agit des clauses types de protection des données adoptées soit par la Commission européenne, soit par une autorité de contrôle et approuvées par la Commission européenne. Jusqu'à présent, deux jeux de clauses ont été adoptés par la Commission européenne : les CCT encadrant les transferts entre responsables de traitement (2001 et 2004) et celles encadrant le transfert entre un responsable de traitement et un sous-traitant (2010)[5]. Elles définissent, en substance, les droits des personnes concernées (notamment les droits d'information et de recours à la médiation en cas de litige), les détails du transfert de données (catégorie de données, finalité, durée de conservation) et la responsabilité de l'exportateur et de l'importateur des données.

Les CCT préexistaient donc au RGPD, de sorte que, aujourd'hui, un décalage s'opère parfois entre les CCT existantes et les nouvelles dispositions du Règlement qui consacrent de nouveaux concepts comme le mécanisme d'autocontrôle (l'*accountability*) ou l'exigence de protection dès la conception, la *Privacy by design*. Aussi, une attention particulière doit être portée à l'adéquation des anciennes CCT avec le RGPD, d'autant que la Cour de Justice devra bientôt répondre à une question préjudicielle portant sur la conformité de celles-ci avec les exigences de la Charte des droits fondamentaux de l'Union[6]. Enfin, les entreprises peuvent toujours prévoir des clauses contractuelles spécifiques entre les différents intervenants (responsable de traitement, sous-traitant, destinataire des données), qui devront toutefois faire l'objet d'une autorisation préalable de l'autorité de contrôle compétente, donc de la CNIL.

Le transfert peut être réalisé également sur le fondement d'un code de conduite, prévu aux articles 40 et 41 du RGPD, élaboré par les associations et organismes représentant un secteur d'activité. Ce code doit être approuvé par les autorités nationales de contrôle, voire la Commission européenne pour une application générale au sein de l'Union européenne. Il encadre le traitement loyal et transparent des données et des informations communiquées, l'exercice des droits des personnes concernées, le transfert des données hors de l'Union, ainsi que les procédures de règlement des litiges, et ce au regard de la spécificité du secteur d'activité. Il peut être appliqué par des responsables de traitement non soumis au RGPD, au moyen d'un engagement contraignant et exécutoire afin de fournir des garanties appropriées en cas de transfert de données hors de l'Union européenne.

Autre dispositif prévu par l'article 46 du RGPD, un mécanisme de certification permettant d'établir que les traitements réalisés par l'entreprise respectent le RGPD. La certification est délivrée et, le cas échéant, retirée par des organismes agréés par l'autorité nationale de contrôle dans les conditions prévues à l'article 42 du Règlement. Ce mécanisme peut lui aussi être adopté par des responsables de traitement non soumis au RGPD, afin de fournir des garanties appropriées pour le transfert de données hors de l'Union européenne, par un engagement contraignant et exécutoire.

II. LES TRANSFERTS HORS UNION EUROPÉENNE SOUS CONDITIONS

Le RGPD a prévu d'autres possibilités pour les transferts de données hors l'Union européenne, notamment les *Binding Corporate Rules* (1.), le consentement explicite de la personne concernée (2.) et une série de situations pouvant justifier un transfert de données à titre dérogatoire (3.).

1. Les *Binding Corporate Rules*

Les *Binding Corporate Rules* (règles d'entreprise contraignantes) constituent, sans doute, le dispositif le plus adapté aux transferts des données au sein des multinationales. Prévu par l'article 46, paragraphe 2, point b) du Règlement, ce dispositif consiste en un code de conduite interne applicable à toutes les entités du groupe, qu'elles soient responsables de traitement ou sous-traitant, par tout dans le monde. Les principaux avantages de ce mécanisme sont, d'une part, l'uniformisation des pratiques en matière de transfert au sein du groupe et, d'autre part, l'économie de la conclusion de clause contractuelles types pour les différents transferts intragroupe.

L'article 47, paragraphe 2, du RGPD donne une liste exhaustive des points qui doivent être obligatoirement couverts par les *Binding Corporate Rules*, incluant notamment le respect des principes généraux en matière de données personnelles, la formation du personnel, la responsabilité de l'entreprise, les procédures de réclamation ou encore les audits sur la protection des données. Plus généralement, ces règles doivent répondre aux exigences générales concernant la finalité du traitement, la limitation des données transférées au strict nécessaire et la durée de conservation, ainsi qu'en matière de protection des données et de base juridique du traitement.

> “Le transfert peut être réalisé également sur le fondement d'un code de conduite, élaboré par les associations et organismes représentant un secteur d'activité.”

Toutefois, la mise en place de transfert de données intragroupe sur la base de *Binding Corporate Rules* est conditionnée à l'approbation préalable desdites règles par une autorité de contrôle. À cet égard, les entreprises multinationales sont libres de choisir une autorité de contrôle chef de file pour la procédure d'approbation de leurs *Binding Corporate Rules*. Elle sera ainsi l'unique interlocutrice du groupe en Europe en matière de protection de données personnelles.

2. Le consentement explicite

En l'absence de décision d'adéquation ou de garanties appropriées, un transfert de données à caractère personnel vers un pays tiers pourra toujours avoir lieu avec le consentement de la personne concernée, y compris lorsque ledit transfert ne répond pas à l'une des finalités prévues à l'article 49, paragraphe 1, points b) à g) du RGPD.

1. Le processus d'adoption d'une décision d'adéquation a été lancé par la Commission européenne le 5 septembre 2018 à la suite de la conclusion des pourparlers entre l'UE et le Japon concernant l'adéquation réciproque le 17 juillet 2018 en vertu desquels les parties sont convenues de reconnaître comme adéquats leurs systèmes respectifs de protection des données.
2. CJUE 6 octobre 2015, *Maximilian Schrems c/ Data Protection Commissioner*, C-362/14.
3. Trib. UE, Ord. 22 novembre 2017, *Digital Rights Ireland Ltd c/ Commission européenne*, T-670/16
4. Résolution du Parlement européen du 5 juillet 2018 sur l'adéquation de la protection assure par le bouclier de protection des données EU-États-Unis, 2018/245 RSP, § 34.
5. https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commission-europeenne.
6. CJUE, Demande préjudicielle, 29 juin 2018, Facebook Ireland & Schrems, C-311/18.

Aux termes de l'article 49, paragraphe 1, point a) du Règlement, il doit toutefois s'agir d'un « *consentement explicite au transfert envisagé* », donné par la personne concernée après avoir été informée des risques que ce transfert peut comporter pour elle en raison de l'absence d'adéquation et de garanties appropriées. Ce consentement ne peut être valable que s'il a été exprimé librement par la personne concernée, constituant ainsi, conformément au principe général de l'article 4, paragraphe 11, du RGPD, une « *manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* », et donc d'un transfert vers un pays tiers ne bénéficiant pas d'une décision d'adéquation et ce sans garanties appropriées. L'obligation d'informer précisément la personne concernée des risques du transfert constitue indéniablement un renforcement de la protection par rapport à ce qui prévoyait la Directive n° 96/46/CE.

> "L'article 49 du RGPD prévoit également une série de situations particulières justifiant un transfert des données vers un pays hors Union européenne."

3. Les dérogations pour des situations particulières

En l'absence de décision d'adéquation ou de garanties appropriées, l'article 49 du RGPD prévoit également une série de situations particulières justifiant un transfert des données vers un pays hors Union européenne, même sans le consentement explicite de la personne concernée[7].

Pour l'essentiel, la liste des dérogations est identique à celle de la Directive n° 95/46/CE. Ces dérogations couvrent les transferts nécessaires à l'exécution d'un contrat ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ou nécessaires à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée ; les transferts nécessaires pour des motifs d'intérêts publics ou à la constatation, l'exercice et la défense de droits en justice ; ou encore ceux nécessaires à la sauvegarde des intérêts vitaux de la personne concernée, mais aussi « d'autres personnes » (nouveauté par rapport au régime de la Directive n° 96/46/CE), lorsque la personne concernée est dans l'incapacité physique ou juridique de donner son consentement. Sont également autorisés à ce titre les transferts des données personnelles au départ de registres publics, c'est-à-dire ouverts à la consultation du public ou de toute personne justifiant d'un intérêt légitime. Concernant plus particulièrement la dérogation pour les transferts nécessaires en raison de motifs importants d'intérêt public, l'intérêt public doit être reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable de traitement est soumis.

Enfin, même lorsqu'aucune dérogation spécifique prévue à l'article 49 (1) du RGPD n'est applicable, un transfert de données vers un pays tiers peut avoir lieu, à titre exceptionnel en quelque sorte, si le transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées et est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. À ces conditions très restrictives s'ajoute l'obligation pour le responsable du traitement d'évaluer toutes les circonstances entourant le transfert de données et d'offrir, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel, ainsi que celle d'informer à la fois l'autorité de contrôle du transfert et la personne concernée du transfert et des intérêts impérieux qu'il poursuit. À cet égard, seuls les intérêts qui peuvent être reconnus comme « *impérieux* » sont pertinents en l'espèce. Le champ d'application de la dérogation est donc sensiblement restreint puisqu'il ne couvre pas tous les « *intérêts légitimes* » concevables en vertu de l'article 6 (1) point f) du RGPD. Selon les Lignes directrices adoptées par le Comité européen de la protection des données, il doit s'agir d'un intérêt essentiel pour le responsable du traitement, comme par exemple dans le cas où le responsable du traitement est tenu de transférer les données à caractère personnel afin de protéger son organisation ou ses systèmes d'un préjudice immédiat grave ou d'une sanction sévère qui affecterait gravement son entreprise.

En conclusion, le régime issu du RGPD ouvre, notamment aux établissements bancaires, des nouvelles voies pour gérer le transfert des données personnelles hors Union européenne, en introduisant des dispositifs, tels les codes de conduite, qui pourraient être mis à profit pour dessiner des règles sectorielles sur mesure qui prennent mieux en compte les spécificités de ce secteur. Pour l'heure, l'assimilation de ce nouveau cadre réglementaire n'est pas encore suffisamment aboutie pour permettre aux acteurs économiques de profiter pleinement de toutes les possibilités qu'il offre en matière de transfert des données personnelles. Parions donc sur le fait que le RGPD ne sera bientôt plus perçu comme un casse-tête, mais comme un cadre favorable, offrant aux entreprises des nouvelles perspectives en matière de gestion des données personnelles. ●

7. Voir notamment EBPB, « Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679 », adoptées le 25 mai 2018.

LA DSP 2 VUE DE BRUXELLES

Les mesures de niveaux 2 et 3 de la DSP 2 concernant les API

Le règlement délégué n° 2018/389, pierre maîtresse des API de la DSP 2, commande une concertation entre acteurs publics et privés pour la définition de ces API au niveau européen comme au niveau de chaque État membre. Ont été créés à cet effet l'*API Evaluation Group* à Bruxelles et le groupe de travail « Interface DSP 2 d'accès aux comptes de paiement » dans le cadre du Comité National des Paiements Scripturaux en France.*

LOUISE LAIDI
Juriste
BPCE
Membre du *Legal Support Group* de l'EPC

Dans le cadre de la deuxième Directive sur les Services de Paiement (DSP 2), un Prestataire de Service de Paiement Gestionnaires de Compte (PSPGC) doit s'équiper, d'ici le 14 septembre 2019, d'une interface dédiée d'accès aux comptes de paiement accessible en ligne pour permettre une identification et un échange sécurisé entre l'utilisateur de paiement, les Prestataires de Services d'Initiation de Paiement, les Prestataires de Services d'Information sur les Comptes et les prestataires de services de paiement émetteur d'instrument de paiement lié à des cartes (TPP).

· À cette fin, un PSPGC doit :
– déterminer l'interface de programmation (API) sur la base de laquelle il construira son interface dédiée ;
– avoir sollicité et obtenu de son Autorité Nationale Compétente (ANC) une exemption de solution de repli en cas de défaillance de son interface dédiée ; et
– avoir mis un dispositif d'essai de cette interface dédiée à la disposition des TPP d'ici le 14 mars 2019.

* Cet article est la transcription de l'intervention de l'auteur lors du colloque AEDBF du 9 octobre 2018.

1. LES 3 NIVEAUX (*LEVELS*) DU CADRE RÉGLEMENTAIRE EUROPÉEN

1.1 Le niveau 1 : la DSP 2

Pour mémoire, la DSP 2 a été adoptée le 25 novembre 2015 et est entrée en vigueur le 13 janvier 2018.

L'article 98 de la directive donne mandat à l'Autorité Bancaire Européenne (ABE) pour soumettre à la Commission un Projet de Normes Techniques (RTS) relatif à l'authentification forte et à la communication sécurisée en vue de leur adoption sous forme de règlement délégué.

1.2 Le niveau 2 : le règlement délégué 2018/389, pierre maîtresse des API

Les principales dispositions du règlement délégué 2018/389

L'article 30 dispose que les PSPGC doivent mettre à disposition des TPP, le 14 mars 2019, un dispositif d'essai pour permettre aux TPP de tester les logiciels et appli-

cations qu'ils utiliseront pour proposer des services de paiement aux utilisateurs de services de paiement à partir du 14 septembre en lien avec les API.

Commentaire sur l'article 30 : ce dispositif d'essai implique des échanges entre PSPGC et TPP.

L'article 31 dispose que le PSPGC doit mettre à disposition soit, une interface dédiée, soit permettre l'utilisation par les TPP des interfaces servant à l'authentification et à la communication entre l'utilisateur de services de paiement et son PSPGC.

Commentaire sur l'article 31 : les PSPGC optent plutôt en pratique pour l'interface dédiée d'accès aux comptes de paiement.

L'article 32 dispose que les PSPGC qui mettent en place une interface dédiée doivent veiller à ce que cette interface n'entrave pas les prestations des services d'initiation de paiement et d'information sur les comptes.

Commentaire sur l'article 32 : volonté du législateur européen de favoriser le développement des TPP face aux acteurs traditionnels.

L'article 33 stipule que le PSPGC doit concevoir son interface dédiée avec une « solution de repli » (*fall-back solution*), c'est-à-dire des mesures d'urgence au cas où l'interface ne fonctionnerait pas conformément à l'article 32, ou serait indisponible de façon imprévue.

Le PSPG peut toutefois être exempté de construire cette solution de repli par son ANC si son interface dédiée remplit les quatre conditions suivantes :
– elle est conforme aux obligations prévues à l'article 32 ;
– elle est conçue et testée conformément à l'article 30,

1. REPÈRES

La genèse du règlement délégué 2018/389

22 février 2017 : publication du 1er projet de RTS rédigé par l'ABE.

27 novembre 2017 : la Commission adopte un projet final de RTS et le transmet pour adoption au Parlement et au Conseil qui ont un droit de veto pendant 3 mois.

26 janvier 2018 : l'ABE estime que le processus législatif n'a pas été respecté, car la Commission ne l'a pas consultée sur tous les amendements apportés à son 1er projet.

13 mars 2018 : publication du règlement délégué 2018/389 au JOUE.

14 septembre 2019 : entrée en vigueur du règlement délégué.

c'est-à-dire à la satisfaction des TPP qui l'ont testée ;
– largement testée par des TPP ; et
– tout problème lié à l'interface est résolu sans retard injustifié.

L'article 33 organise par ailleurs une concertation entre l'ABE et les ANC des États membres pour garantir une harmonisation au niveau européen des conditions d'exemption de « solution de repli » des interfaces dédiées.

Commentaire sur l'article 33 : volonté du législateur européen d'organiser une concertation entre l'ABE et les ANC sur les conditions que les interfaces dédiées doivent remplir pour être conformes au règlement délégué 2018/389.

1.3 Le niveau 3 : l'avis de l'ABE du 13 juin 2018 sur la mise en œuvre de l'authentification forte et la communication sécurisée

2. L'API EVALUATION GROUP (API EG) : UN EXERCICE D'AUTORÉGLEMENTATION VOULU PAR LA COMMISSION

En laissant volontairement une marge d'interprétation du règlement délégué 2018/389 aux autorités publiques et acteurs privés pour l'élaboration des API et interfaces dédiées, il a fallût prévoir l'harmonisation future de ces interprétations.

Cela a été rendu possible par la mise en place :
– d'abord au niveau européen, sous l'impulsion de la Commission européenne, de l'API EG
– puis par la mise en place au niveau de chaque État membre, sous l'impulsion de l'ABE, de groupes de travail nationaux rassemblant autorités publiques et acteurs nationaux. En France un GT « Interface DSP 2 d'accès aux comptes de paiement » a été mis en place le cadre du Comité National des Paiements Scripturaux.

2.1 L'API EG

L'API EG a pour objectif d'évaluer les initiatives d'API qui serviront de base aux interfaces dédiées des PSPGC, au regard des fonctionnalités requises par la DSP 2.

Les trois associations bancaires européennes (FBE, EACB et ESBG), des représentants de TPP, des consommateurs et commerçants participent à l'API EG.

La Commission européenne, la Banque Centrale Européenne et l'ABE font office d'observateurs. Son secrétariat est assuré par « European Payments Council » (EPC).

L'API EG a dû répondre à des questions juridiques indispensables à la conception des API, concernant notamment le consentement que le PSU doit donner lorsqu'il utilise une interface dédiée.

2.2 Question juridique sur le « consentement explicite » du PSU lors de l'intervention d'un TPP

L'expression « consentement explicite » existe à la fois dans la DPS2 et le RGPD qui lui est postérieur.

L'article 94.2 de la DSP 2 relatif à la protection des données stipule que les TPP « *n'ont accès à des données à caractère personnel nécessaire à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement explicite de l'utilisateur de services de paiement* ».

La question est de savoir si cette expression a le même usage dans les deux textes d'une part et si le PSPGC doit ou non vérifier que l'utilisateur du service de paiement a effectivement donné son consentement pour l'intervention d'un TPP d'autre part.

La position de la Commission :
– le terme consentement explicite de l'article 94.2 de la DSP 2 ne doit pas être rapproché de l'usage de ce terme dans le RGPD ;
– s'agissant des rapports entre le TPP et l'utilisateur de service de paiement, qui par hypothèse sont régis par un contrat, le traitement des données est licite parce qu'il est nécessaire à l'exécution du contrat conclu entre eux. Le consentement de l'utilisateur repose sur le contrat conclu entre eux => fondement de l'article 6.1 b du RGPD ;
– s'agissant des rapports entre le PSPGC et le TPP, qui par hypothèse ne sont régis par aucun contrat puisque la fourniture de services de paiement n'est pas subordonnée à l'existence de relations contractuelles entre eux, la transmission de données entre le PSPGC et le TPP est licite car il s'agit d'une obligation légale résultant de la DSP 2 => fondement de l'article 6.1 c du RGPD ;
– le PSPGC ne doit pas vérifier si l'utilisateur de service de paiement a donné son consentement au TPP.

Cette position de la Commission a été confirmée tout à la fois pas par le Comité Européen de la Protection des Données (Lettre 05/07/2018 Sophie in't Veld) et par L'avis de l'ABE du 13 juin 2018 sur la mise en œuvre des RTS.

2. GROUPE DE TRAVAIL DE L'*API EVALUATION GROUP*

Les principales conditions des interfaces dédiées et les API

Conditions	Article
Permettre aux PSIC, PSIP et PSEIPC [1] d'avoir accès aux données nécessaires des comptes de paiement accessibles en ligne	Articles 65, 66 et 67 de la DSP 2 Article 30 du règlement délégué
Conformité aux standards (largement utilisés) de communication émis par des organisations qualifiées européennes ou internationales	Article 30(3) du règlement délégué
Permettre aux utilisateurs de services de paiement d'autoriser et consentir à une transaction de paiement via un PISP	Articles 64 (2) de la DSP 2 Article 30 (1) du règlement délégué

[1] Prestataires de services de paiement émetteur d'instrument de paiement lié à des cartes.

L'API EG s'inspire des préconisations publiées par l'ABE le 13 juin 2018, dans un avis relatif à la mise en œuvre des RTS sur l'authentification forte et la communication sécurisée.

L'avis de l'ABE comporte notamment un tableau des principales conditions devant être remplies par les interfaces dédiées et les API (voir tableau 2).

Enfin, des réunions de l'API EG ont été programmées jusqu'en fin 2018 pour permettre la convergence des initiatives nationales d'API.

2.3. Les fonctionnalités des API et interfaces dédiées

L'API EG travaille sur un document recensant :
– les fonctionnalités que doivent remplir les initiatives d'API pour servir de base à des interfaces dédiées qui puissent être conformes à la DSP 2 ;
– les fonctionnalités que doivent remplir les interfaces dédiées elles-mêmes, pour obtenir de leur ANC une exemption de solution de repli, étant précisé que chaque PSGC est libre de retenir une partie seulement des fonctionnalités offertes par l'API dont il se sert.

3. LES TRAVAUX DU GT « INTERFACE DSP 2 D'ACCÈS AUX COMPTES DE PAIEMENT » DANS LE CADRE DU COMITÉ NATIONAL DES PAIEMENTS SCRIPTURAUX EN FRANCE

Objectif du GT : définir les fonctionnalités d'une API de place répondant aux exigences de la DSP 2 et ayant vocation à établir un consensus entre les PSPGC, les PSIC et les PSIP, en s'appuyant sur l'initiative française d'API de STET.

Il est coprésidé par la Banque de France et la Direction Générale du Trésor.

Il rassemble les acteurs concernés par les projets d'interfaces d'accès DSP 2, du côté des PSPGC, PSIC et PSEIPC. ●

(R)ÉVOLUTION EN PROTECTION DES DONNÉES

Avantages et difficultés lors de la mise en œuvre du RGPD

Le RGPD a remis la protection des données sur le devant de la scène. Cela a-t-il pour autant engendré une révolution dans l'organisation des banques ? L'exemple de BNP Paribas.

AGNÈS CHATELLIER-CHAMOULAUD
Responsable juridique,
Regulatory Digital
BNP Paribas

La protection des données personnelles est multidisciplinaire, au cœur de la relation des banques avec leurs clients. En effet, ces dernières recueillent et traitent une quantité importante de données personnelles pour exercer leurs activités, que ce soit au titre du respect de nombreuses réglementations ou pour répondre aux attentes de leurs clients et améliorer sans cesse la relation avec eux.

La protection des données constitue un avantage compétitif qui peut renforcer la réputation de chaque banque. C'est en effet une composante essentielle de la confiance des clients. Mais c'est aussi un facteur déterminant de la transformation digitale et une opportunité pour développer l'innovation.

Le règlement général pour la protection des données (RGPD) entré en application en Europe le 25 mai 2018, a mis – ou plutôt remis – la protection des données sur le devant de la scène. Cela a-t-il pour autant engendré une révolution dans l'organisation des banques ?

Le droit de la protection des données personnelles n'est pas nouveau. En France, la loi « Informatique et Libertés » du 6 janvier 1978 a fêté ses 41 ans. Par ailleurs, le secteur bancaire a toujours été fortement réglementé. La confidentialité des données fait historiquement partie de la culture des banques qui ont développé un savoir-faire en matière de sécurité et de protection de celle-ci.

Le RGPD ne constitue donc pas pour BNP Paribas une révolution, mais il a généré une réelle évolution de son organisation concernant la protection des données personnelles.

RGPD : QUELS DÉFIS ?

Le défi majeur pour les banques est probablement la mise en place d'une gouvernance de la donnée qu'elle soit personnelle ou non.

La nécessité pour les banques de respecter les standards BCBS 239 du Comité de Bâle[1] en matière de qualité des données de *reporting* risque, a déjà poussé celles-ci à mieux structurer leur organisation afin d'appréhender les données dans leur ensemble.

Ainsi, au sein de BNP Paribas, a été mis en place un réseau de *Chief Data Officers* (CDO) chargé d'assurer dans chaque métier ou entité le respect des mesures concernant la qualité et l'intégrité des données. Pour coordonner ce réseau, une équipe centrale partage l'information tout en établissant les normes, principes, méthodologie, *guidelines*, déclinés ensuite par les CDO en fonction du contexte local.

1. Le BCBS 239 (Basel Committee on Banking Supervision's standard n° 239), publié le 9 janvier 2013 par le Comité de Bâle, pose des principes visant à améliorer les capacités des banques en matière d'agrégation de données de risques financiers, afin de les aider à produire des *reportings* réglementaires plus fiables en améliorant la qualité de ces données risques.

L'implémentation du RGPD s'est inscrite dans la continuité. La décision a été prise de profiter des structures et comités déjà en place et l'équipe centrale s'est fortement étoffée pour réunir des acteurs des fonctions Juridique, Conformité, Risque, Informatique, mais aussi des métiers.

Un autre défi pour les banques est de transformer l'organisation sans totalement bouleverser les structures en place pour installer durablement une culture de la donnée personnelle.

Avec le RGPD, tous les établissements doivent pouvoir démontrer à tout moment leur conformité aux principes de protection des données. Cela implique entre autres :

– de cartographier/documenter les traitements existants ;
– d'analyser les processus opérationnels pour déterminer si des données personnelles sont manipulées ;
– de vérifier que ne sont traitées que les données personnelles nécessaires au regard de chaque finalité ;
– de prendre en compte les principes de protection des données dès la conception d'un nouveau produit ou service mais aussi pendant toute la durée des traitements ;
– de gérer les violations de données (procédure de gestion de crise) ;
– d'aménager les contrats avec les prestataires/sous-traitants.

BNP Paribas a souhaité pour cela accroître l'implication de tous dans la mise en place des initiatives assurant la protection des données personnelles en favorisant une coopération active des acteurs de différents horizons : opérationnels, juridiques, finance, risque, IT, conformité.

L'objectif, essentiel, est de casser les silos pour aller vers une collaboration transversale effective entre les pays, les entités, les métiers et les fonctions, et ainsi pouvoir assurer la cohérence des interprétations communes et faciliter leur implémentation opérationnelle en proposant des solutions pragmatiques adaptées aux structures existantes.

La mise en place d'un réseau de délégués à la protection des données (en anglais, *Data Protection Officer* – DPO) accompagnés de correspondants données personnelles, réseau coordonné par un DPO Groupe, permet de faciliter cette transversalité.

Par ailleurs, les rôles et responsabilités de chacun des acteurs de BNP Paribas en matière de protection des données ont été définis, ainsi que les processus de contrôle pour veiller au respect des règles internes établies.

Enfin, la sensibilisation des collaborateurs à tous les niveaux a été développée, à travers des *eLearning* obligatoires pour tous les collaborateurs en Europe sur les fondamentaux de la protection des données, des formations spécifiques et une forte montée en compétence des juristes spécialisés sur les questions digitales.

RGPD : QUELS AVANTAGES ?

BNP Paribas a toujours placé ses clients au cœur de sa stratégie en se positionnant vis-à-vis d'eux comme un tiers de confiance dans le cadre de la construction et du maintien d'une relation client forte.

La protection des données est un facteur clé dans cette relation de confiance et BNP Paribas veille au quotidien à la sécurité de ses systèmes pour garantir l'intégrité, la qualité et la confidentialité des données personnelles qui lui ont été confiées.

Le RGPD permet de renforcer cette démarche qualité en mettant l'accent sur les personnes et leurs données.

BNP Paribas a développé la transparence auprès de ses clients en leur communiquant, dans l'ensemble de son Groupe en Europe, une Notice protection des données et une Charte de confidentialité des données personnelles[2].

Elle a aussi amélioré le processus de réponse aux requêtes des clients.

Mais c'est probablement la mise en place d'une gouvernance sur la Protection des données personnelles avec responsabilisation de l'ensemble des acteurs de la Banque qui constitue l'apport essentiel de la mise en œuvre du RGPD au sein de BNP Paribas.

Les piliers de cette gouvernance sont le réseau de DPO, la transversalité des positions et interprétations liées à cette réglementation, ainsi que la standardisation des procédures, processus et documentation, notamment en ce qui concerne l'information des personnes, le développement du principe de *Privacy by Design*, ou la création d'une méthodologie pour réaliser l'analyse d'impact sur les données personnelles des personnes physiques ou clients de la Banque.

RGPD : QUELS ENJEUX ?

L'enjeu principal est constitué par la nécessité d'inscrire dans la durée les efforts actuels pour mettre en place une telle gouvernance de la donnée personnelle dans le Groupe en Europe, voire au-delà.

Notamment, dans un Groupe international, la multiplicité des entités et le multiculturalisme doivent être pris en compte.

Un autre enjeu est lié à l'articulation du RGPD avec d'autres textes, comme notamment le futur règlement *ePrivacy*, la DSP 2, la directive NIS, le *Cloud Act*, etc., qui créent de nombreuses interactions et impliquent d'assurer le respect et la coexistence de règles parfois antinomiques.

Enfin, ne doit pas être oubliée la hausse des demandes de communication de données par les régulateurs, autorités ou institutions juridictionnelles de tous pays – dans le cadre de leurs activités de supervision, d'investigation, ou de *discovery* –, qui nécessite d'analyser le fondement de cette communication et son contenu.

Le RGPD n'a donc pas totalement fini de faire parler de lui ! ●

2. Ces documents sont aussi accessibles sur ses sites internet ou sur les espaces privés des banques en ligne.

RGPD

La Cnil accompagne les professionnels dans leur mise en conformité

Le RGPD instaure une nouvelle gouvernance européenne qui implique les autorités de contrôle de chaque État membre. En France, la Cnil doit s'adapter à cette nouvelle configuration et à ses nouvelles missions pour accompagner les professionnels dans la mise en conformité aux obligations réglementaires RGPD. En aura-t-elle les moyens ?*

SOPHIE NERBONNE
Directrice chargée de co-régulation économique
Commission Nationale de l'Informatique et des Libertés (Cnil)

■ De nombreuses incertitudes existent avec la mise en place du RGPD

La prise de conscience généralisée par les professionnels des obligations issues de ce texte fondant la protection des données du XXIe siècle a provoqué une vague d'inquiétude à laquelle la Cnil a répondu par un discours apaisant et de nombreux outils d'aide à la mise en conformité, disponibles sur son site. Responsable de traitement et sous-traitant doivent penser leur mise en conformité en prenant en compte :

– les actions de conformité immédiates : registre (cf. le modèle simplifié) et dispositions contractuelles (cf. guide sous-traitant) ;

– le rôle central du nouvel acteur qu'est le délégué à la protection des données (DPO) ;

– la maîtrise progressive des nouveaux outils, obligatoires ou facultatifs, de conformité : analyses d'impact (cf. guide méthodologique et logiciel téléchargeable), certification, codes de conduite...

Régulateur pragmatique, la Cnil considère que les obligations s'apprécient en fonction de la taille de l'entreprise et de la sensibilité des traitements. Elle a également entrepris la transformation de son patrimoine normatif afin d'apporter de la sécurité juridique aux acteurs. De même, elle a publié la liste des traitements devant faire l'objet d'une analyse d'impact ainsi que des lignes directrices synthétiques permettant aux responsables de traitement concernés de savoir plus précisément s'ils sont ou non soumis à cette obligation. Elle suit les travaux relatifs à une dizaine de codes de conduite, portant notamment sur la recherche médicale et les infrastructures dites de *cloud* et a développé un MOOC pour se familiariser avec les principes fondamentaux du RGPD, qui sera prochainement accessible.

■ Une gouvernance européenne

Pour les traitements transfrontaliers de données, la Cnil fait en effet désormais partie d'un mécanisme de prise de décision européenne. Il s'agit d'un modèle novateur, participatif et distribué et non pas centralisé à Bruxelles, qui implique toutes les autorités de contrôle concernées. L'autorité chef de file propose une décision en matière de traitements transfrontaliers qui est analysée par ses pairs. En l'absence de consensus, le comité européen peut émettre un avis contraignant.

Face à ces nouveaux enjeux, les moyens dont dispose la Cnil restent sous-dimensionnés au regard du nombre d'acteurs concernés, à savoir toutes les entreprises, collectivités territoriales, organismes publics, associations... C'est également vrai au regard des moyens dont disposent ses homologues : 200 personnes dans les services de la Cnil, plus de 600 pour l'Autorité britannique.

■ Une nouvelle mission de certification

La certification succède à la labellisation que la Cnil a pratiquée ces dernières années en matière de formation, de gouvernance « informatique et libertés », d'audit de traitement et de coffre-fort électronique. Elle a adapté au RGPD les deux premiers référentiels et pourrait les transformer en référentiels de certification. En la matière, ce seront des tiers certificateurs qui délivreront les certifications. Le premier référentiel adopté par la Cnil porte sur la certification des compétences des DPO, ce qui intéresse de nombreux organismes dont l'International Association of Privacy Professionals (IAPP), une structure à l'origine américaine s'installant dans l'Union européenne.

Le marché de la certification pourra prendre en compte le besoin des acteurs et développer par exemple des offres de coffres-forts numériques combinés avec d'autres services, des mécanismes d'anonymisation ou de limitation de la durée de conservation des données.

■ Qu'en est-il des suites législatives post-RGPD ?

Le RGPD est un règlement européen, texte d'application directe, contrairement à la précédente directive de 1995. Pour autant, le législateur national est intervenu pour que la loi du 6 janvier 1978 permette d'opérer les « raccords » entre le règlement et les procédures nationales, en matière de mesures répressives notamment. Cette loi a aussi permis l'utilisation, modérée, des marges de manœuvre nationales spécifiques laissées aux États membres par le RGPD et transpose la directive « police-justice » relative aux traitements régaliens. Une ordonnance est venue boucler ce dispositif, quasi complet en attendant la sortie du décret d'application.

■ Le recueil des besoins des professionnels

Le passage au RGPD a multiplié les demandes d'accompagnement venant d'opérateurs ou de collectifs professionnels présentant des niveaux de maturité variables en matière d'appropriation du règlement, parfois peu informés ou souhaitant au contraire d'emblée se saisir pleinement de toutes les potentialités des nouveaux outils de conformité. Afin de répondre à la prise de conscience massive par les entreprises de la nécessité d'intégrer la protection des données personnelles dans leurs chantiers numériques, la Cnil a complété son dispositif d'accompagnement des acteurs économiques.

Elle met systématiquement en consultation ses projets de référentiels. Elle déploie une stratégie dite des « têtes de réseaux », qui sont des interlocuteurs de référence capables de lui remonter les problématiques spécifiques des acteurs concernés et de relayer ses recommandations auprès d'eux dans un processus continu et évolutif. Elle facilite la montée en compétence desdites « têtes des réseaux » et la mutualisation des bonnes pratiques dans les secteurs où elle n'existe pas encore.

■ Le délégué à la protection des données (DPO), un nouvel acteur de la protection des données

La sortie des lignes directrices européennes sur le DPO n'a pas épuisé les questions susceptibles de se poser, sur son statut et ses missions et les interactions des professionnels avec le service des DPO ont progressé pour y répondre ou faire remonter au niveau européen les cas les plus délicats. En février 2019, plus de 45 000 organismes ont déclaré via le téléservice de la Cnil, un DPO.

Pour le secteur public, il y a une obligation de désignation d'un DPO, qui peut être mutualisé pour plusieurs entités, ce qui est particulièrement utile pour les petites structures homogènes (notaires, huissiers de justice, municipalités...). L'obligation de désignation ne vaut dans le secteur privé que pour les traitements à large échelle soit de données sensibles soit s'il s'agit d'un suivi systématique et régulier des personnes, ce qui est le cas des banques ou sociétés d'assurance par exemple.

L'ensemble des Cnil européennes recommande en toutes hypothèses de désigner un DPO, bonne pratique permettant de disposer d'un pilote de la conformité RGPD, gage tout à la fois de confiance mais aussi de compétitivité économique car il s'agit de développer un modèle d'innovation responsable, embarquant dès la conception des produits ou services, la protection des droits des personnes concernées.

> “C'est un pari unique d'envisager un règlement européen d'application directe.”

■ Le consentement dans le cadre du RGPD

Il a été beaucoup question du consentement des personnes concernées par la collecte de leurs données, alors que le consentement constitue une base légale du traitement parmi d'autres, telles que l'obligation légale (pour les traitements de lutte antiblanchiment par exemple) ou l'intérêt légitime du responsable de traitement (pour les traitements de lutte contre la fraude ou de prospection commerciale). Afin que le consentement soit valable, les modalités de son recueil doivent garantir qu'il est libre, éclairé et spécifique. Cela signifie qu'il ne peut être mélangé avec l'acceptation des conditions générales d'utilisation d'un site ou résulter d'une case précochée, par exemple. À côté du cadre général posé par le RGPD, s'applique la directive « *ePrivacy* » transposée dans le code des communications électroniques qui fixe le principe du consentement pour certains *cookies* et fait l'objet de travaux européens à l'échéance assez peu claire.

■ S'adapter rapidement aux changements

Les acteurs économiques ont réalisé que le principe de « responsabilisation » mis en avant par le RGPD, à savoir être en mesure de démontrer qu'ils respectent leurs obligations, s'avère au final plus lourd que les formalités préalables qui ont quasiment disparu, sauf dans la recherche médicale. Cette nouvelle logique garantit pourtant une application effective du RGPD, au bénéfice du respect des règles du jeu par tous les acteurs économiques, qu'ils soient situés en Europe ou non. C'est au final le respect des droits et libertés de chacun d'entre nous qui se trouve ainsi mieux protégé.

La Cnil entend dès lors offrir un accompagnement renouvelé de cette trajectoire des acteurs au moyen d'un

* Cet article s'appuie sur les propos tenus lors du colloque AEDBF du 9 octobre 2018. L'auteur tient à remercier l'AEDBF, son président Pierre Minor, et le cabinet Kramer Levin de l'avoir invitée à ce colloque.

premier niveau de service de sensibilisation sur la conformité RGPD et sur toute la gamme d'instruments de corégulation disponible (référentiels, codes de conduite, mécanismes de certification, etc.), amorcer un dialogue sectoriel structuré avec l'ensemble des secteurs économiques (corégulation) et davantage articuler, dans un souci de lisibilité pour les acteurs économiques, les différents corpus normatifs avec les autres régulateurs économiques (interrégulation). Un guide AFA Cnil « protection des données et lutte anticorruption » devrait ainsi prochainement sortir.

■ ***Quid* du droit à la portabilité ? Gadget inutile ou véritable atout ?**

Il s'agit là d'un droit nouveau qui devrait constituer un double atout. Ce droit à la portabilité a été voulu par le législateur européen pour éviter aux individus d'être dépendants des plates-formes ou entités disposant de leurs données numériques, qu'ils souhaiteraient basculer chez un autre opérateur. Il a aussi été instauré dans l'optique de stimuler la concurrence et l'innovation technologique. Son utilisation devrait mener à la création de nouveaux services, démontrant ainsi que la réglementation peut être à la source d'innovations.

En conclusion, je souhaitais souligner le déploiement de la stratégie de la Cnil à destination des « têtes de réseaux » économiques. Il s'agit de créer une nouvelle dynamique avec les collectifs, de quelque nature qu'ils soient, représentatifs des secteurs d'activité, professions, thématiques, pour répondre à leurs besoins et produire un travail de régulation plus opérationnel. Il s'agit aussi de réussir le passage à l'échelle, avec un effet levier permettant de démultiplier les actions de conformité. La construction de liens permettant une étroite collaboration avec le secteur financier remonte déjà à plusieurs années et cette dernière devrait se trouver régénérée par cette nouvelle approche. ●

PROPOS CONCLUSIFS

Les données à l'épreuve de la DSP 2 et du RGPD

Le droit à la portabilité prévu par le RGPD conduit à un partage des données par les établissements de crédit avec d'autres prestataires de services bancaires. Il rejoint ainsi le partage des données imposé par la DSP 2.

GILLES KOLIFRATH
Avocat, associé
Kramer Levin Naftalis & Frankel LLP

Comme nous l'avons vu, la DSP 2[1] et le RGPD[2] sont complexes et leur compréhension n'est pas aisée ! De surcroît, leurs objectifs ne sont pas les mêmes !

Si ces deux textes peuvent présenter des imperfections, ils posent néanmoins les bases de la réglementation actuelle en matière de service de paiement et de protection des données des personnes physiques.

LE DROIT À LA PORTABILITÉ : UNE IDÉE DONT LA MISE EN PLACE EST DIFFICILE

Plus particulièrement, le RGPD traite de la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et de la libre circulation des données. Il pose un certain nombre de principes en matière de traitement et reconnaît des droits aux personnes concernées par les données à caractère personnel. Les clients ont en particulier un droit d'accès qui s'analyse en un droit de confirmation et d'information, un droit de portabilité (qui permet de transmettre les données à un tiers sans avoir à obtenir l'autorisation du responsable de traitement) et un droit à l'oubli (donc à l'effacement des données).

Ce droit à la portabilité n'est pas sans interpeller. Il conduit en effet à un partage des données par les établissements de crédit avec d'autres prestataires de services bancaires. Ce droit rejoint le partage des données imposé par la DSP 2 dont l'un des objectifs est la mise en place d'un marché unique des services de paiement.

Puisqu'il y a une obligation de transmettre certaines données relatives au paiement[3] et que l'article 44 du RGPD pose le principe général d'autorisation sous conditions des transferts de données vers un pays tiers, il va s'avérer nécessaire de déterminer l'interface de programmation applicative (en anglais, *Application Programming Interface* – API) sur la base de laquelle un Prestataire de services de paiement gestionnaire de comptes (PSPGC) (une banque ou établissement de crédit) construira son interface dédiée pour permettre d'ici au 14 septembre 2019 une identification et un échange sécurisé de données entre un utilisateur de paiement, un agrégateur (PSIC 4), un initiateur (PSIP[5]) ou un prestataire de services de paiement émetteur d'instrument de paiement (en anglais, *Third Party Provider* – TPP) lié à une carte par exemple.

1. Directive (UE) 2015/2366 du Parlement européen et du Conseil, du 25 novembre 2015, concernant les services de paiement dans le marché intérieur.
2. Règlement (UE) 2016/679 de Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
3. Art. L. 133-40 III du Code monétaire et financier pour les données relatives au service d'initiation de paiement et L. 133-41 III du Code monétaire et financier pour le service d'information sur les comptes.
4. Prestataire de services d'informations sur les comptes.
5. Prestataire de services d'initiation de paiement.

Notons qu'il y a plusieurs initiatives d'API en Europe, STET en France, Berlin Group en Allemagne, *open banking* au Royaume-Uni.

Or les choses ne sont pas simples, car la transmission de données personnelles relatives à un utilisateur de services de paiement lors de l'intervention d'un TPP doit respecter tout à la fois la DSP 2 et le RGPD. En effet, l'article 94-2 de la DSP 2 relatif à la protection des données a été adopté par le Parlement européen en 2015, alors que le RGPD était encore en cours de discussion.

Cet article stipule que les TPP « *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 explicite de l'utilisateur de service de paiement* ».

> “La protection des données représente pour les banques un avantage compétitif qui peut renforcer leur réputation.”

Les intervenants du colloque comme les juristes de la place se sont interrogés sur le fait de savoir si le « *consentement explicite* » de la DSP 2 doit être rapproché de l'usage de ce terme dans le RGPD ?

La Commission a donné une position informelle devant l'API EG [6] sur le fait que le terme de consentement explicite visé à l'article 94-2 de la DSP 2 ne doit pas être rapproché de l'usage de ce terme dans le RGPD. L'avis de l'ABE du 13 juin 2018 [7] sur la mise en œuvre des RTS est venu confirmer cette position.

UNE SÉCURITÉ ACCRUE POUR UN RENFORCEMENT DE LA COMPÉTITIVITÉ ?

Le RGPD avait identifié que les différences dans le niveau de protection des droits et libertés des personnes physiques, en particulier le droit à la protection des données à caractère personnel à l'égard du traitement des données dans les États membres peuvent empêcher le libre flux de ces données dans l'ensemble de l'Union. Ces différences peuvent dès lors constituer un obstacle à l'exercice des activités économiques au niveau de l'Union, fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union.

Comme nous l'a confirmé une grande banque Française lors de notre colloque, « *la protection des données personnelles est multidisciplinaire, au cœur de la relation de la banque avec ses clients, car le groupe recueille, stocke et utilise une grande quantité de données personnelles dans le cadre de ses activités quotidiennes* » [8].

La protection des données représente donc pour les banques un avantage compétitif qui peut renforcer leur réputation et une opportunité pour développer l'innovation, tout en renforçant la confiance des clients, mais représente aussi un facteur de risque.

On pourra constater que les banques, comme les assureurs d'ailleurs, ont mis en place des équipes dédiées pour gérer le projet RGPD. Ces établissements réglementés ont une culture historique visant à gérer la relation confidentielle avec leurs clients et avaient développé un fort savoir-faire en la matière.

Ces établissements ont très souvent capitalisé sur les structures et les comités déjà en place autour de leurs réseaux de *Chief Data Officers*, afin de s'assurer du respect concernant la qualité et l'intégrité des données.

Mais il a fallu transformer les organisations pour créer un maillage dans les correspondants gérant les données personnelles qui accompagnent les DPO (*Data Protection Officers*), avec un DPO groupe pour coordonner leur travail.

Ce travail s'est fait main dans la main avec les équipes de la conformité. Il a fallu également gérer les prestataires/sous-traitants et clarifier les obligations de chacun. Enfin, en sus de la gestion des failles de sécurité, il a fallu notamment former les collaborateurs à tous les niveaux, jusqu'au plus élevé.

On peut penser que la banque qui place ses clients au cœur de sa stratégie a pu tirer d'une contrainte un avantage. La banque peut profiter en effet de son rôle « centralisateur » en se positionnant comme un tiers de confiance vis-à-vis de ses clients. La protection des données est clé dans la relation de confiance entre le client et la banque. En travaillant sur le principe du secret bancaire, la banque a pu de longue date garantir l'intégrité, la qualité et la confidentialité des données qu'elle détient.

Elle a pu ainsi développer de nouveaux applicatifs pour instaurer une plus grande transparence sur la gestion des données et mettre en place de nouvelles chartes de protection des données personnelles. Cela a été également l'occasion de mieux mettre en œuvre le suivi et l'implémentation des données utilisées par les différents métiers. En d'autres termes, les systèmes de *reporting* et de traçabilité des données ont été revus et améliorés. On est entré dans l'aire du *privacy by design* [9], où on vient intégrer les principes du RGPD dès la conception d'un projet, d'un service ou de tout outil lié à la manipulation de données personnelles...

6. L'API Evaluation Group (API EG) a été proposé par la Commission pour faire partie du *Euro Retail Payments Board* (ERPB) *Working Group on Payment Initiation Services* (PIS), ce qui a été accepté par l'ERPB en novembre 2017 (API EG 002-18 Version A.3 *dated 4 September 2018*).
7. Avis de l'ABE (l'Autorité bancaire européenne) sur la mise en œuvre de l'authentification forte et de la communication sécurisée, 13 juin 2018.
8. Agnès Chatellier-Chamoulaud, *Head of Regulatory Digital*.
9. Le *privacy by design* est né aux États-Unis à la fin des années 1990 suite à l'initiative d'Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'État d'Ontario. Elle consistait à imposer que chaque nouvelle technologie destinée à traiter les données personnelles soit conçue de manière à offrir un haut niveau de protection des données.

SI LES AVANTAGES PEUVENT S'AVÉRER NOMBREUX, LES CONTRAINTES DEMEURENT...

Il est clair que la nouvelle donne qui s'impose aux traitements des données qu'elles soient de paiement ou autres, nécessite une agilité et une rigueur de premier plan. Les interactions entre les équipes ont été accrues et la coordination doit se faire au quotidien.

Comme nous l'avons vu, la mise en musique de la DSP 2 et du RGPD n'est pas simple ! Mais ce ne sont pas les seuls textes applicables en matière de traitement des données. On citera pêle mêle et de manière non exhaustive : la proposition de Règlement *ePrivacy* [10] à venir, la directive NIS [11], le *Cloud Act* [12]. Ces textes nécessitent donc une mise en perspective qui ne simplifie pas toujours les choses.

Mais c'est surtout l'application de ces nouveaux textes à l'international qui risque de poser question à l'avenir pour les grands groupes internationaux qui sont actifs dans de nombreux pays, en Europe comme hors d'Europe. En effet, il faudra pouvoir déterminer à quel régulateur parler ! La maison mère peut-elle être l'autorité chef de file pour toutes ses entités ? Ou y aura-t-il plusieurs autorités chefs de file ? C'est clairement une question qui a été soulevée lors de notre colloque.

LA CNIL : LA POSITION DU RÉGULATEUR

Le droit de l'Union, réformant le droit de la protection des données à caractère personnel, a imposé aux États membres de repenser les missions des autorités de régulation, largement étendues dans le RGPD, or la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que réformée [13] ne traduit pas toujours un tel élargissement [14].

Madame Sophie Nerbonne, directrice de la conformité de la Commission nationale informatique et libertés (CNIL) qui nous a fait l'honneur de participer au colloque, nous a rappelé que les « données » étaient le pétrole de l'économie numérique... et que celles-ci étaient créatrices de valeur pour l'entreprise. Nous sommes entrés dans la quatrième révolution industrielle, sans forcément s'en être rendu compte [15] !

En sus de son rôle de régulateur des données personnelles, la CNIL accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

C'est dans cette perspective que la CNIL intervient comme facilitateur de la transition numérique avec pour mission :

– de comprendre les besoins des acteurs professionnels ;
– d'être au service des personnes concernées par les traitements ;
– d'élaborer des outils de régulation agiles ;
– de porter la réglementation au niveau européen ;
– de construire une innovation durable et responsable.

On pourra illustrer la quatrième révolution industrielle avec le domaine de l'automobile : la voiture roule seule, sans l'assistance humaine. Mais ce n'est pas le seul domaine dans lequel l'utilisation de la donnée a bouleversé notre vie. On pourra citer tout aussi bien la médecine, les objets connectés...

La CNIL nous a indiqué qu'elle n'est d'ailleurs pas la seule à intervenir en la matière et qu'on est plutôt entré dans une aire de co-régulation qui se double d'une inter-régulation. On est aussi passé au « droit souple », avec l'idée de pouvoir « rectifier », plutôt que de nécessairement sanctionner.

> “Le droit à la portabilité pose lui aussi des questions, notamment quant au consentement qu'il convient d'y apporter.”

De nombreuses questions se posent sur le responsable des traitements.

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne (physique ou morale), l'autorité publique, le service ou l'organisme qui (seul ou conjointement) détermine ses finalités et ses moyens [16].

Comme indiqué, plusieurs personnes peuvent être désignées responsables d'un seul et même traitement de données. Dans ce cas, leur responsabilité est conjointe [17]. Les personnes dont les données font l'objet du traitement géré conjointement doivent se voir communiquer les grandes lignes de l'accord répartissant les obligations de chaque responsable.

10. Proposition de Règlement du Parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques COM/2017010 final-2017/03 (COD).
11. Directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
12. Adopté le 23 mars 2018, le *Clarifying Lawful Overseas Use of Data Act* ou *Cloud Act*, est une loi fédérale des États-Unis amendant la loi Stored Communications Act (SCA) de 1986.
13. Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
14. Nathalie Martial-Braz, « Droit de la protection des données à caractère personnel issu de l'ordonnance n° 2018-1125 du 12 décembre 2018 », *La Semaine du Droit – Édition générale*, n° 1-2, 14 janvier 2019.
15. La première révolution industrielle est liée à l'utilisation de la machine à vapeur, la deuxième est liée à l'utilisation du pétrole et de l'électricité, la troisième est liée au développement de l'informatique.
16. Voir Art. 1 du RGPD.
17. L'article 26 du RGPD souligne qu'il leur incombe de définir leurs obligations respectives par un accord conclu entre eux.

Une entreprise peut demander à un sous-traitant la mise en œuvre d'un traitement de données personnelles pour son compte. Le responsable du traitement est toujours rattaché à l'entreprise mais c'est le sous-traitant qui est chargé de réaliser le traitement[18]. C'est toutefois le responsable du traitement initial qui reste le premier à mettre sa crédibilité en jeu. Un sous-traitant ne peut être qualifié de responsable du traitement que dans le cas où il définirait lui-même les finalités et moyens du traitement mis en œuvre.

Enfin, et nous n'y reviendrons pas, le droit à la portabilité pose lui aussi des questions, notamment quant au consentement qu'il convient d'y apporter[19].

Finalement, quelles réflexions en tirer pour l'avenir ?

Le considérant 9 du RGPD avait mis en lumière que « *si elle demeure satisfaisante en ce qui concerne ses objectifs et ses principes, la directive 95/46/CE*[20] *n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique ou le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne* ». Le RGPD va-t-il répondre de manière satisfaite à cette préoccupation ?

Le Cloud Act américain ne risque-t-il pas de permettre aux autorités américaines d'obtenir des données stockées par des entreprises américaines en dehors des États-Unis, sans passer par les Traités d'entraide judiciaire ?

Selon l'article 9 du Code civil, auquel font écho la Convention européenne des droits de l'homme (article 8, § 1) et la Charte des droits fondamentaux de l'Union européenne (article 7), « *chacun a droit au respect de sa vie privée* ». Toute personne a donc le droit de garder confidentielles les informations la concernant, et par conséquent à ce que ces informations ne soient pas communiquées, ce qui implique une interdiction d'accès à ces données, notamment à celles détenues par les établissements de crédit[21]. Et c'est peut-être là que le bât blesse ! En effet, il existe de nombreux cas où nous communiquons des données à caractère personnel en acceptant que la personne à qui on les communique puisse les utiliser, *i.e.* en renonçant en quelque sorte au respect de notre vie privée et en acceptant que le bénéficiaire en devienne propriétaire… Il est clair qu'il devient alors plus compliqué de reprocher à ce bénéficiaire l'utilisation de « ses » données !

> “La plupart des observateurs voient dans le *Big Data* des enjeux majeurs pour l'avenir, tant en termes d'opportunités commerciales que de bouleversements sociopolitiques.”

On pourra noter également que la donnée étant parfois « vraiment » publique, son utilisation ne semble pas poser de problème particulier. C'est sans compter le phénomène du *Big Data*[22]. En effet, les évolutions qui caractérisent le *Big Data* (et ses algorithmes) sont en partie cachées (notamment au sein des services de renseignement de grands États) et si rapides et potentiellement profondes que peu de prospectivistes se risquent à pronostiquer son devenir à moyen ou long terme. Mais la plupart des observateurs y voient des enjeux majeurs pour l'avenir, tant en termes d'opportunités commerciales que de bouleversements sociopolitiques, avec le risque de voir émerger des systèmes capables de fortement contrôler, surveiller et/ou influencer les individus et groupes…

En conclusion, « *le Web est devenu une machine produisant de l'injustice et de la division, influencée par des forces puissantes qui l'utilisent pour imposer leur propre agenda* », comme le constatait Sir Tim Berners-Lee, l'un des deux inventeurs du Web. Dévasté par les récents scandales sur la vie privée impliquant les géants du Web, comme Facebook, ce dernier a décidé de diminuer son rôle au sein du World Wide Web Consortium (W3C), l'organisme chargé d'élaborer les standards du Web, pour se consacrer à un nouveau projet. Celui-ci vise à développer une communauté de développeurs autour d'une nouvelle architecture *open source*, « Solid », qui inverse « *le modèle actuel où les utilisateurs donnent leurs données personnelles à des géants du numérique* ». L'idée est que chacun garde le contrôle sur ses contacts, ses photos, ses données bancaires, ou sa santé. Chaque individu les conservera dans un ou plusieurs portefeuilles numériques (*pods*) et choisira de les stocker, soit sur ses terminaux, soit sur le serveur d'un fournisseur, en choisissant à quelles applications il donnera accès… Gageons que cette fois-ci, le service ne sera plus gratuit comme lors de la création du Web ! Mais, comme on dit, « *s'il n'y a pas de prix, c'est que c'est vous le prix* » !

Ainsi, en matière de « données », rien n'est jamais définitif ! Et tout est toujours surprenant… ●

18. Dans un tel cas, l'article 28 du RGPD indique qu'un contrat doit nécessairement régir le traitement effectué par un sous-traitant.
19. Aurélie Banck, « Données personnelles : articulation de la DSP 2 sur les services de Paiement et du RGPD sur la protection des données – Acte II : suite et fin ? », RDBF n° 6, novembre-décembre 2018.
20. Directive 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.
21. Thierry Bonneau, « L'accès aux données bancaires au regard du respect à la vie privée », RDBF n° 6, novembre-décembre 2018, précitée.
22. Il n'y a pas de définition officielle, mais on peut traduire *Big Data* par « mégadonnées », qui désigne des ensembles de données très volumineuses qui dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données ou de l'information.

Des solutions sur mesure à vos problématiques juridiques françaises et internationales

En choisissant Kramer Levin, vous bénéficiez :

- d'une équipe capitalisant sur une connaissance approfondie du monde des affaires, animée notamment par d'anciens directeurs juridiques aujourd'hui avocats
- de solutions proactives, créatives et pragmatiques en réponse aux problématiques juridiques les plus complexes
- de la forte implication des associés dans le traitement quotidien de vos dossiers
- d'une équipe pérenne de cultures et nationalités diverses
- d'une collaboration étroite avec les bureaux de New York et Silicon Valley, ainsi qu'un réseau mondial de « best friends »
- de l'indépendance du bureau de Paris, assurant optimisation et transparence des coûts

L'offre de notre équipe Banque & Finance :

- Opérations bancaires (financements bancaires, projets, actifs, acquisition, immobiliers, exports)
- Opérations de marchés de capitaux (Dette / Equity)
- Réglementation et conformité bancaires et financières
- Monétique (services de paiement, monnaie électronique)
- Contentieux boursiers, bancaires, disciplinaires, commerciaux et pénal financier
- Investigations et enquêtes internationales
- Procédure collectives

Votre contact : Gilles Kolifrath

Notre équipe en droit bancaire

Conseil

Gilles Kolifrath
Associé
Conformité bancaire, financière et assurancielle, Lutte anti-blanchiment, anti-corruption, sanctions internationales

Pierre Storrer
Counsel
Moyens & services de paiement

Conseil / Contentieux

Hugues Bouchetemble
Associé
Contentieux bancaire et financier, Conseil - Réglementation et conformité bancaires et financières

Marie-Christine Fournier-Gille
Associée
Contentieux bancaire et financier, Restructuring

Consultant

Wadie Sanbar
Counsel
Réglementation et conformité bancaires et financières

Thierry Bonneau
Professeur agrégé des Facultés de droit, Consultant
Réglementation et conformité bancaires et financières

Dominique Penin
Associé
Contentieux bancaire et financier, Droit pénal des affaires

Marco Plankensteiner
Associé
Contentieux bancaire et financier

Kramer Levin

Kramer Levin Naftalis & Frankel LLP
47 avenue Hoche – 75008 Paris
T: +33 (0)1 44 09 46 00

Métro : Charles-de-Gaulle Etoile
Parking : Indigo, 18 avenue Hoche
www.kramerlevin.com