Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Protection des données à caractère personnel en matière de services de paiement et de crédit

Jacquemin, Herve; Limbree, Pauline

Published in:
Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.)

Publication date:
2020

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Jacquemin, H & Limbree, P 2020, Protection des données à caractère personnel en matière de services de paiement et de crédit. Dans H Jacquemin (Ed.), *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.): premières applications et analyse sectorielle.* Commission Université-Palais, Numéro 195, Anthemis, Liège, p. 227-280.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 25. Apr. 2024

5

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN MATIÈRE DE SERVICES DE PAIEMENT ET DE CRÉDIT

Hervé JACQUEMIN
professeur à l'UNamur
(Centre de Recherche Information, Droit et Société – CRIDS, membre du NaDI)
avocat au barreau de Bruxelles

Pauline LIMBRÉE
assistante à l'UNamur
(Centre de Recherche Information, Droit et Société – CRIDS, membre du NaDI)
avocate au barreau de Liège

Sommaire

Introduction 228

Section 1
Protection des données à caractère personnel en matière de services de paiement 230

Section 2
Protection des données à caractère personnel en matière de crédit 251

Section 3
Focus sur certaines questions spécifiques posées par le *big data* et l'intelligence artificielle 267

Conclusion 279

Introduction

1. Données à caractère personnel et services financiers. Dans le secteur financier, les traitements de données à caractère personnel sont nombreux, spécialement en matière de services de paiement et de crédit.

Pour octroyer un crédit à un consommateur, le prêteur doit préalablement évaluer sa solvabilité. Aussi sera-t-il amené à examiner la situation financière et les facultés de remboursement de celui-ci, sur la base des informations fournies par le consommateur lui-même (données d'identification, profession, revenus, charges, situation familiale, autres crédits en cours, etc.), recueillies auprès d'une base de données centralisée, comme la Centrale des crédits aux particuliers (ci-après, « C.C.P. ») ou, le cas échéant, tirées de l'historique de leur relation contractuelle (si le consommateur était déjà un client du prêteur). Ces renseignements constituent normalement des données à caractère personnel. Elles peuvent d'ailleurs présenter un caractère sensible dans le chef du consommateur : on songe, par exemple, à un défaut de paiement à la suite duquel le consommateur aura été fiché dans le volet négatif de la C.C.P.

Les prestataires de services de paiement traitent également les données à caractère personnel de leurs utilisateurs, à l'occasion des opérations effectuées par leur intermédiaire (consultation des comptes, virement, paiement par carte de crédit ou de débit, etc.). Les informations recueillies sont diverses et variées : identité des parties à la transaction, objet, montant, communication éventuelle, etc.

L'analyse pourrait se poursuivre dans d'autres secteurs, comme l'assurance ou le conseil en investissement (nous ne les examinerons toutefois pas dans la présente contribution).

Dans de nombreuses hypothèses, les traitements de données à caractère personnel sont nécessaires à la fourniture du service financier en tant que tel (octroi d'un crédit, exécution d'une opération de paiement, etc.). Très souvent, ils sont d'ailleurs imposés de manière expresse par une disposition légale ou réglementaire (voy. *infra*, n° 36). Les professionnels du secteur ont d'ailleurs l'obligation d'identifier leurs clients (et de vérifier cette identité), conformément aux dispositions de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces[1].

En complément aux opérations ressortissant aux métiers classiques de la banque et du crédit, les prestataires peuvent également être intéressés à exploiter les données pour des finalités plus périphériques (mais néanmoins capitales d'un point de vue *business*), par exemple pour mener des campagnes de marketing ciblées ou établir des modèles prédictifs (pour évaluer la solvabilité de leurs clients, par exemple).

1 *M.B.*, 6 octobre 2017. Voy. spéc. art. 21 et s. de la loi.

2. Traitements de données dans l'environnement numérique. Avec le numérique, les professionnels du secteur financier sont en mesure d'offrir de nouveaux services à valeur ajoutée à leurs clients : dématérialisation – quasi intégrale – du processus d'octroi du crédit, informations bancaires en temps réels, transferts d'argent instantanés par *smartphone*, internet[2] et mobile *banking*[3], etc. Ces opérations offrent généralement des gains de temps, de pertinence et d'efficacité, dans l'intérêt de toutes les parties impliquées. Elles s'accompagnent toutefois de certains risques, en termes d'atteintes à la vie privée ou de fraude, notamment, que des mesures techniques et organisationnelles devront combattre.

Pour les prêteurs ou les prestataires de services de paiement, le numérique ouvre également des perspectives intéressantes, spécialement dans un contexte d'économie de la donnée (*data economy*). En tirant habilement avantage du *big data*, combiné aux outils d'intelligence artificielle sans cesse plus performants, les professionnels peuvent automatiser de nombreuses opérations (exécutées, dans certains cas, sans intervention humaine) ou mieux connaître leurs clients (et dès lors, leur offrir des produits personnalisés qui répondent très précisément à leurs besoins, augmentant ainsi leur « expérience client »).

3. Plan et limites de la présente contribution. Les traitements de données à caractère personnel sont principalement régis par le Règlement général sur la protection des données[4] (ci-après, « R.G.P.D. ») et, le cas échéant, la législation complémentaire adoptée en Belgique (principalement la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[5], ci-après, « loi du 30 juillet 2018 »).

En principe, ces textes s'appliquent également aux données de paiement et aux données de crédit. Toutefois, comme on le verra, dans ces secteurs spécifiques, le législateur a adopté des règles en matière de protection des données, qu'il convient d'articuler avec les dispositions du R.G.P.D.

2 En effet, aujourd'hui, il y a, en Belgique, environ 13 millions d'abonnements à la banque en ligne. Voy. dashboard.febelfin.be, consulté le 12 novembre 2019.

3 De même, il y a plus de 7 millions d'abonnements à la banque mobile. Voy. dashboard.febelfin.be, consulté le 12 novembre 2019.

4 Règlement (UE) n° 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, *J.O.U.E.*, L 119/1 du 4 mai 2016. Sur ce règlement, on consultera notamment C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, pp. 5 et s.; É. DEGRAVE, « La protection des données à caractère personnel enfin réformée », *J.D.E.*, 2016, pp. 136 et s.; K. JANSSENS et M. NUYTTEN, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk – Le Règlement général sur la Protection des Données : de la théorie à la pratique », *R.D.C.*, 2018, pp. 401 et s.; C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. du CRIDS, Bruxelles, Larcier, 2018. Voy. également le commentaire article par article réalisé par Th. LÉONARD et D. CHAUMONT et disponible sur le site www.GDPR-expert.eu.

5 *M.B.*, 5 septembre 2018.

Cette articulation n'est pas sans poser de questions, spécialement lorsque les règles sectorielles ont été prises plusieurs années avant l'entrée en application du R.G.P.D., et n'ont plus fait l'objet de modification depuis lors.

Nous examinons successivement la protection des données à caractère personnel en matière de services de paiement (section 1) et de crédit (section 2).

Dans ces deux domaines, le phénomène du *big data*, combiné à des applications d'intelligence artificielle, offre de nouveaux outils aux entreprises du secteur. Encore faut-il s'assurer de la conformité des procédures envisagées, à l'aune des exigences posées par le R.G.P.D. (section 3).

Section 1

Protection des données à caractère personnel en matière de services de paiement

4. Plan de la section 1. Des données à caractère personnel sont nécessairement traitées dans le cadre des opérations de paiement. Elles sont soumises au R.G.P.D. et à la législation spécifique sur les paiements, qui figure principalement dans le livre VII du Code de droit économique. Les données bancaires et de paiement sont ainsi soumises à deux réglementations, qui semblent aller à contre-courant, l'une tendant à favoriser les transferts de données, alors que l'autre entend les encadrer strictement[6].

Après un rappel du cadre normatif et de son champ d'application (A), on analyse l'articulation entre les dispositions du livre VII en matière de services de paiement et celles du R.G.P.D. (B).

A. Cadre normatif applicable aux services de paiement

1. Textes européens et belges

5. La D.S.P. II. La directive 2015/2366/UE concernant les services de paiement dans le marché intérieur[7] (ci-après, « D.S.P. II ») – qui abroge et remplace la D.S.P. I[8] – a modifié de manière importante le cadre juridique applicable aux services de paiement[9]. En effet, conscient des nouveaux défis suscités par l'innovation technologique, le législateur européen a souhaité mettre à jour les règles en vigueur en ouvrant la voie à l'*Open Banking*. Celle-ci implique l'ouverture des systèmes d'information des banques et le partage des données de leurs clients à des tiers[10].

Ainsi, le texte de 2015 poursuit l'objectif de promouvoir la concurrence dans le domaine des paiements électroniques, tout en garantissant la sécurité de ceux-ci et en assurant un niveau élevé de protection aux consommateurs[11]. Pour atteindre cet objectif, le législateur européen mise sur le renforcement de la sécurité et de la transparence du processus de paiement[12].

6. Les lois de transposition belges. La Belgique a opté pour une transposition en deux volets de la D.S.P. II[13].

Le législateur a d'abord adopté la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement[14] (ci-après, « loi du 11 mars 2018 »), entrée en vigueur le 28 mars 2018, à l'exception de certaines dispositions[15]. Cette loi règle principalement les aspects institutionnels de la matière. Elle établit notamment la liste des prestataires de services de paiement (à laquelle sont ajoutés deux nouveaux acteurs, sur l'activité desquels nous reviendrons, *infra*, n° 8)[16], modifie l'accès au statut d'établissement de paiement[17] et impose des normes de sécurité plus strictes pour les

6 S. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », disponible sur www.twobirds.com, février 2019 ; Covington & Burling LLP, « European Data Protection Board Provides Clarification On PSD 2 », disponible sur www.covfinancialservices.com, 25 juillet 2018.

7 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, *J.O.U.E.*, L 337/35 du 23 décembre 2015. Pour des analyses détaillées de ce texte, voy. D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *in* J.-P. Buyle *et al.* (dir.), *Actualités en droit commercial et bancaire*, Bruxelles, Larcier, 2017, pp. 455 à 477 ; Th. Bonneau, « La directive sur les services de paiement "2" : révolution ou évolution ? », *J.D.E.*, 2016/6, n° 230, pp. 214-217 ; Th. Bonneau, *Régulation bancaire et financière européenne et internationale*, Bruxelles, Bruylant, 2018, pp. 763-775.

8 Directive (UE) 2007/64 du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, *J.O.U.E.*, L 319/1 du 5 décembre 2007.

9 G. Hennard, « La loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique », *D.B.F.*, 2019/1, p. 25.

10 J. Moldonato, « Les banques à l'heure de l'*Open Banking*. Comment se développer dans un univers incertain ? », disponible sur www2.deloitte.com, consulté le 3 décembre 2019.

11 Cons. 6 de la D.S.P. II ; D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *op. cit.*, p. 456.

12 C. Bourguignon, « L'utilisateur dans la nouvelle loi sur les services de paiement : entre protection et responsabilisation », *in* H. Jacquemin et B. Michaux (dir.), *Actualités en droit du numérique*, Limal, Anthemis, 2019, p. 157.

13 Précisons que l'article 115 de la D.S.P. II imposait aux États membres de transposer les nouvelles dispositions de la directive avant le 13 janvier 2018.

14 Loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, *M.B.*, 26 mars 2018.

15 Cette loi remplace la loi du 21 décembre 2009 relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement, *M.B.*, 19 janvier 2010.

16 Art. 5 et s. de la loi du 11 mars 2018.

17 Art. 9 et s. de la loi du 11 mars 2018.

paiements en ligne[18]. Un arrêté royal du 3 juin 2018 a été adopté en exécution de cette nouvelle législation[19].

Il faut ensuite avoir égard à la loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique[20], entrée en vigueur le 9 août 2018. Cette loi modifie principalement le titre 3 du livre VII du Code de droit économique relatif aux services de paiement.

2. Champ d'application des dispositions du livre VII du Code de droit économique en matière de services de paiement

a) Notions clés du livre VII du Code de droit économique[21]

7. Champ d'application matériel. Du point de vue matériel, le livre VII du Code de droit économique s'applique aux « services de paiement » listés à l'article I.9, 1°, du Code de droit économique.

Cette disposition dénombre huit types de services susceptibles d'être qualifiés comme tels, pour autant qu'ils soient livrés dans le cadre d'une activité professionnelle. Outre les services traditionnels, relèvent notamment de cette notion l'*internet banking*, le *mobile banking* ainsi que de nouveaux services fournis par les *FinTechs*[22] qui étaient, jusqu'alors, dans la zone grise du droit : les services d'initiation de paiement et les services d'information sur les comptes. Cette extension du champ d'application matériel est l'une des avancées majeures de la D.S.P. II[23].

18 Art. 50 et s. de la loi du 11 mars 2018.

19 Arrêté royal du 3 juin 2018 portant exécution de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, en ce qui concerne les établissements de paiement limités et les établissements de monnaie électronique limités, *M.B.*, 19 juin 2018.

20 Loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique, *M.B.*, 30 juillet 2018.

21 Nous ne développerons pas, dans le cadre de la présente contribution, les règles relatives au champ d'application territorial de la D.S.P. II. À cet égard, voy. G. Hennard, « La loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique », *op. cit.*, pp. 36 à 41.

22 « On peut décrire une *Fintech* comme une start-up qui est construite sur un modèle opérationnel ou économique disruptif, visant à traiter de manière innovante des produits ou des services financiers de l'industrie traditionnelle ou à offrir des services financiers nouveaux en utilisant les possibilités offertes par les nouvelles technologies », voy. C. Houssa et L. Standaert (dir.), « La "Nouvelle frontière" de la finance », *in Le droit des affaires en évolution : l'économie du futur, le futur de l'économie*, Bruxelles, Bruylant, 2016, p. 155.

23 P. Berger, I. Van Biesen et S. Liebaert, « De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt », *R.D.C.*, 2017/2, p. 126 ; C. Bourguignon, « L'utilisateur dans la nouvelle loi sur les services de paiement : entre protection et responsabilisation », *op. cit.*, p. 156.

8. Nouveaux services en lien avec la stratégie d'*Open Banking*. Le « service d'initiation de paiement » vise le « 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 »[24].

En d'autres termes, l'initiateur est un tiers qui s'interpose entre la plateforme de l'entreprise (vendeur de biens ou fournisseur de services) et celle de l'établissement bancaire du payeur, afin de donner à ce dernier une instruction de paiement[25]. Pour que celle-ci soit exécutée, il suffit que l'établissement en question confirme la disponibilité du montant nécessaire à l'opération de paiement sur le compte concerné[26]. Dans ce scénario, ce n'est donc pas l'utilisateur qui ordonne à sa banque de payer le créancier mais bien le prestataire intermédiaire, ce qui libère l'utilisateur de l'exigence de disposer d'une carte de paiement. Cette solution à faible coût, qui simplifie le processus de paiement et diminue le nombre d'intermédiaires, présente un intérêt pratique, tant pour le consommateur que pour l'entreprise[27]. Malheureusement, l'action d'« initier » n'est pas définie, ce qui est susceptible de créer des difficultés, notamment quant à la question de savoir si les fournisseurs de portefeuilles numériques (p. ex., *PayPal*) relèvent de cette notion[28].

Le « service d'information sur les comptes » se rapporte quant à lui au « 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 »[29]. En d'autres termes, ce service permet à l'utilisateur d'obtenir, en temps réel, un aperçu global de sa situation financière via une interface unique (peu importe que les comptes dont il dispose soient ouverts dans des établissements bancaires distincts)[30]. C'est d'ailleurs pour cette raison qu'on surnomme les prestataires de ce service « agrégateurs de comptes »[31]. Ceux-ci rejoignent la catégorie des applications de gestion

24 Art. 1.9.33/14°, C.D.E. ; art. 4, 18), de la D.S.P. II.

25 A.-P. André-Dumont, « Les services de paiement à l'épreuve des évolutions technologiques », *in* J.-A. Delcorde (dir.), *La révolution digitale et les start-ups*, Bruxelles, Larcier, 2016, p. 96 ; cons. 27 de la D.S.P. II.

26 Cette confirmation est censée inviter l'entreprise à livrer le bien ou à fournir le service promptement.

27 P. Berger, I. Van Biesen et S. Liebaert, « De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt », *op. cit.*, p. 126 ; H. Toupin-Trinckvel, « L'assujettissement des services PSIC et PSIP à la législation anti-blanchiment : axes de réflexion », *B.E.R.*, 2019, n° 3, pp. 264 et 269 ; Th. Bonneau, « La directive sur les services de paiement "2" : révolution ou évolution ? », *op. cit.*, p. 216 ; *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 10.

28 P. Berger, I. Van Biesen et S. Liebaert, « De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt », *op. cit.*, p. 126.

29 Art. 1.9.33/12°, C.D.E. ; art. 4, 19), de la D.S.P. II.

30 P. Berger, I. Van Biesen et S. Liebaert, « De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt », *op. cit.*, p. 126 ; H. Toupin-Trinckvel, « L'assujettissement des services PSIC et PSIP à la législation anti-blanchiment : axes de réflexion », *op. cit.*, p. 263 ; cons. 28 de la D.S.P. II.

31 Cette expression est d'ailleurs reprise dans la loi du 11 mars 2018.

de budgets vu qu'ils offrent à leurs utilisateurs une vision consolidée de leurs comptes (soldes et opérations réalisées), et, *a fortiori*, une possibilité de les gérer de manière optimale[32].

L'*Open Banking*, encouragé par la D.S.P. II, se matérialise par l'ouverture des données de paiement des utilisateurs, au bénéfice de tiers que sont les prestataires de services d'initiation de paiement et d'information sur les comptes. L'idée est de permettre à l'utilisateur d'accéder à ses comptes ou d'ordonner des paiements sans être contraint de passer par ses applications bancaires classiques[33]. Dans cette optique, les banques traditionnelles sont tenues de mettre à la disposition de ces *FinTechs* un canal de communication[34] par lequel celles-ci peuvent s'identifier et prélever toutes les informations sur les comptes, nécessaires à la livraison de leurs services[35]. Pour ce faire, il suffit que le compte concerné soit accessible en ligne, c'est-à-dire soit « un compte qui offre à l'utilisateur une interface en ligne »[36 37]. Cette nouvelle prérogative implique des exigences supplémentaires à charge des prestataires de services d'initiation de paiement et d'information sur les comptes.

Conformément aux définitions des services d'initiation de paiement et des services d'information sur les comptes, il est manifeste que l'accès offert aux nouveaux prestataires concerne uniquement le compte de paiement de l'utilisateur, c'est-à-dire « un compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et qui est utilisé aux fins de l'exécution d'opérations de paiement »[38]. *A contrario*, les comptes d'épargne ou de crédit ne sont pas ouverts aux nouveaux prestataires[39]. Pourtant, certains agrégateurs de comptes veulent fournir à l'utilisateur des fonctionnalités plus vastes que celles qui sont fondées sur les données des seuls comptes de paiement. Le fait que le législateur européen ait uniquement précisé les règles relatives à l'ouverture

32 P. Berger, I. Van Biesen et S. Liebaert, « De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt », *op. cit.*, p. 126 ; H. Toupin-Trinckvel, « L'assujettissement des services PSIC et PSIP à la législation anti-blanchiment : axes de réflexion », *op. cit.*, p. 263.

33 G. Richard, « Nouveau droit d'accès aux comptes et aux données des comptes », *R.B.*, 27 mars 2019, p. 1.

34 Plus précisément, les banques traditionnelles sont tenues de créer des interfaces de partages de données sécurisées et standardisées (Application Programming Interface – API) et de les mettre à disposition des nouveaux prestataires de paiement. De ce fait, ces derniers doivent abandonner leur technique de *web scraping*, qui permet de récupérer le contenu d'un site web pour l'intégrer dans un autre.

35 D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *op. cit.*, p. 458.

36 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-2896/001, p. 77.

37 Cons. 30 de la D.S.P. II ; art. 35 de la D.S.P. II.

38 Art. I.9, 8°, C.D.E. ; art. 4, 12), de la D.S.P. II.

39 À cet égard, voy., p. ex., la police vie privée de C.B.C., qui précise que, « conformément à la loi (PSD 2), C.B.C. en tant que banque a l'obligation de fournir l'accès aux informations relatives aux soldes et aux transactions des *comptes de paiement* de ses clients, dans la mesure où le client a installé une application en ligne » ; par ailleurs, le règlement de son application C.B.C. *Mobile* indique que « le service d'infocomptes permet au contractant de consulter, par l'intermédiaire de la banque, les infocomptes d'un ou de plusieurs comptes de paiement ou d'épargne indiqués par lui, qui sont consultables en ligne et que l'utilisateur détient auprès d'une ou plusieurs autres banques », voy. multimediafiles.kbcgroup.eu.

des comptes de paiement signifie-t-il que ce dernier souhaitait interdire l'accès à tout autre type de comptes ou, au contraire, qu'il tenait à le laisser libre[40] ? Nous sommes d'avis que la première branche de l'alternative doit être privilégiée : le libre accès aux données issues de comptes d'épargne ou de crédit est, à notre sens, contraire aux objectifs de sécurité des opérations de paiement et de protection du consommateur contre les risques de fraude, poursuivis par la D.S.P. II[41]. Cependant, la thèse de l'interdiction totale a pour effet de réduire drastiquement l'intérêt des services d'information sur les comptes[42]. Dans l'attente de précisions à cet égard, les agrégateurs de comptes se maintiennent dans la zone grise pré-D.S.P. II concernant leurs services hors comptes de paiement.

9. Champ d'application personnel. S'agissant du champ d'application personnel du titre 3 du livre VII du Code de droit économique, il y a lieu de distinguer le prestataire de services de paiement et l'utilisateur.

Le « prestataire de services de paiement » est la personne morale qui fournit le service à un utilisateur et qui répond aux caractéristiques imposées par l'article I.9, 2°, du Code de droit économique. Par ailleurs, le prestataire de services de paiement peut également, suivant les services fournis, être qualifié de gestionnaire de comptes[43], d'initiateur de paiement[44] et/ou d'agrégateur de comptes[45].

Quant à l'« utilisateur de services de paiement », il est défini comme la « personne physique ou morale qui utilise un service de paiement en qualité de payeur, de bénéficiaire ou les deux »[46]. Cette notion est double dès lors qu'elle vise indifféremment le payeur et le bénéficiaire de l'opération de paiement, étant entendu que ceux-ci peuvent être, ou pas, des consommateurs[47].

b) Qualification des éléments-clés du service de paiement au sens du R.G.P.D.

10. Données nécessaires à l'exécution de l'opération de paiement. La notion de donnée à caractère personnel vise toute information se rapportant à une personne physique identifiée ou identifiable, désignée sous l'expression de personne concernée[48]. En tant que clé de voûte de la réglementation, cette

40 G. Richard, « Nouveau droit d'accès aux comptes et aux données des comptes », *op. cit.*, p. 2.

41 *Ibid.*, p. 2.

42 À titre d'exemple, mentionnons la *FinTech* Bankin dont le fondateur a précisé que « 80 % des comptes concernés par nos services ne sont pas des comptes de paiement ». À cet égard, voy. S. Lebouchier, « Agrégateurs et banques : comment vont-ils s'échanger les données des comptes ? », *R.B.*, 15 décembre 2017, p. 2.

43 Art. I.9, 33/13°, C.D.E.

44 Art. I.9, 33/14°, C.D.E.

45 Art. I.9, 33/15°, C.D.E.

46 Art. I.9, 5°, C.D.E.

47 Voy. art. I.1, 2°, C.D.E. selon lequel est un consommateur « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ».

48 Art. 4.1) R.G.P.D.

notion est à mettre en lien avec celles de responsable du traitement et de sous-traitant (voy. *infra*, n° 11). En effet, la qualification dépend intrinsèquement de la manière dont l'acteur traite les données à caractère personnel et, en ce qui concerne plus précisément l'hypothèse étudiée, les données de paiement.

La majorité des données de paiement sont des données à caractère personnel. En effet, le numéro de compte d'un client, ses identifiants, l'historique de ses opérations bancaires ou de ses bénéficiaires habituels sont des données qui permettent d'identifier, directement ou indirectement, ledit client[49].

Parmi ces informations, certaines peuvent par ailleurs bénéficier d'une protection renforcée aux termes de l'article 9 du R.G.P.D. Cette disposition dresse une liste de données dites particulières sur laquelle ne figurent pas expressément les données bancaires[50]. Cependant, celles-ci peuvent, dans certains cas, bénéficier par ricochet de la protection renforcée des données particulières, notamment lorsqu'un utilisateur effectue un virement au profit d'une organisation syndicale ou d'une paroisse. Par ailleurs, le Groupe de travail « article 29 » a indiqué que les données de paiement étaient « à caractère hautement personnel »[51] dans la mesure où leur violation est susceptible d'avoir des incidences graves sur la vie privée des personnes concernées[52].

Quant à la D.S.P. II, elle établit une classification parmi les données bancaires. Elle identifie tout d'abord les données de sécurité personnalisées, qui sont des « caractéristiques personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification »[53]. Il s'agit concrètement des codes PIN, mots de passe ou numéros d'identification uniques fournis à l'utilisateur par sa banque[54]. La D.S.P. II consacre ensuite la notion de données de paiement sensibles, qu'elle définit comme des « données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude »[55] [56]. Ces données doivent être distinguées

49 Th. Bonneau, « L'accès aux données bancaires au regard du respect de la vie privée », *R.B.*, novembre-décembre 2018, p. 1.

50 A. Banck, « La DSP 2 et le R.G.P.D. sont-ils alignés ou orthogonaux ? », *Banque & Stratégie*, n° 379, avril 2019.

51 Groupe de travail « article 29 », « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679 », WP 248 rév.01, 4 avril 2017.

52 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 », *R.B.*, janvier-février 2018, p. 17.

53 Art. I.9, 33/17, C.D.E. ; art. 4, 31), de la D.S.P. II. Bien que la D.S.P. II fasse mention de « données personnalisées », le législateur belge a préféré, eu égard aux termes utilisés dans les versions anglaise et néerlandaise, la notion de « caractéristiques personnalisées », ce qui permet d'éviter toute confusion avec la terminologie de la directive 95/46/CE ; voy. *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 11.

54 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 12 ; notons que le numéro de carte et la date d'échéance apposés sur celle-ci de manière apparente ne relèvent pas de la notion de données de sécurité personnalisées.

55 Art. I.9, 33/18, C.D.E. ; art. 4, 32), de la D.S.P. II.

56 Notons que le nom du titulaire de compte et le numéro de compte ne relèvent pas de cette notion pour ce qui concerne les services d'initiation de paiement et d'information sur les comptes.

des données sensibles au sens de la directive 95/46/CE (rebaptisées « données particulières » par le R.G.P.D.).

11. Qualification des intervenants à un service de paiement. La dichotomie prestataire de services de paiement/utilisateur de services de paiement trouve un écho dans le R.G.P.D., qui distingue les acteurs du traitement (responsable du traitement[57] et sous-traitant[58]) de la personne qui voit ses données traitées (personne concernée[59]).

Le Groupe de travail « article 29 » a rendu un avis[60] concernant les notions de responsable du traitement et de sous-traitant. À cette occasion, il précise que le concept de responsable du traitement est fonctionnel, car il vise à attribuer une responsabilité aux personnes qui exercent une influence de fait dans l'opération de traitement. Par conséquent, il convient de procéder à une analyse factuelle propre pour chacun des prestataires visés par la D.S.P. II afin de déterminer leur rôle respectif au sens du R.G.P.D.

Tout d'abord, la banque traditionnelle, dont le rôle de base est notamment d'exécuter un ordre de paiement, peut, normalement, être qualifiée de responsable du traitement puisque c'est elle qui détermine les moyens et les finalités du traitement opéré. Notons que cette position est à retenir, peu importe que cette banque agisse comme émetteur de l'opération de paiement ou comme destinataire de celle-ci. L'entreprise bénéficiaire du paiement ne devrait pas, quant à elle, être qualifiée de responsable du traitement même si, dans les faits, l'opération de paiement peut être effectuée pour son compte, en particulier lorsque la transaction est réalisée au moyen d'un terminal de paiement qu'elle met à la disposition des clients dans son magasin ou son *e-shop*. En effet, selon les critères dégagés par le Groupe de travail « article 29 », la qualité de responsable du traitement impose soit d'avoir déterminé les finalités du traitement, soit d'avoir déterminé les questions sensibles fondamentales pour la licéité du traitement[61]. Or, en l'espèce, aucune de ces prérogatives n'est exercée par l'entreprise bénéficiaire du paiement.

Le payeur et le bénéficiaire doivent par ailleurs être qualifiés de personnes concernées pour autant qu'il s'agisse de personnes physiques.

La banque traditionnelle, de même qu'une *FinTech*, peuvent aussi proposer de centraliser les données de paiement des différents comptes d'un utilisateur afin de les réunir sur une seule interface (dans le cadre du nouveau service

57 Art. 4.7) R.G.P.D.

58 Art. 4.8) R.G.P.D.

59 Art. 4.1) R.G.P.D.

60 Groupe de travail « article 29 », « Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" », 16 février 2010, WP 169 et A. Delforge, « Titre 8 – Les obligations générales du responsable du traitement et la place du sous-traitant », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, *op. cit.*, pp. 373 et s.

61 Groupe de travail « article 29 », « Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" », *op. cit.*, p. 16.

d'information sur les comptes – défini *supra*, n° 8). Dans cette hypothèse, le prestataire peut, en principe, être qualifié de responsable du traitement puisqu'il a la maîtrise des données bancaires de l'utilisateur (ses numéros de compte, ses historiques de virements, la liste de ses bénéficiaires habituels, etc.). Par ailleurs, il fixe la finalité du traitement opéré sur ces dernières (agrégation des données) et il détermine les éléments essentiels de l'opération, tels que les catégories de données traitées, leur durée de conservation ou encore leurs modalités d'accès[62].

Par ailleurs, la banque traditionnelle ou la *FinTech* peut initier un paiement sur instruction d'un utilisateur qui, par exemple, souhaite effectuer un achat en ligne (*cf.* le nouveau service d'initiation de paiement, défini *supra*, n° 8). Dans ce scénario, il est plus délicat d'attribuer de manière catégorique les rôles du traitement dès lors que plusieurs prestataires de services interviennent de manière quasi simultanée. En effet, le prestataire de services d'initiation de paiement demande à la banque gestionnaire de comptes de confirmer la disponibilité du montant nécessaire à la transaction afin d'exécuter l'opération de paiement. Dans ce cas de figure, l'initiateur devrait revêtir la qualité de responsable du traitement puisqu'il traite les données afin de fournir son service intermédiaire. Quant à la banque traditionnelle, son rôle est plus délicat à déterminer. Celle-ci pose manifestement un acte de traitement sur les données de son client lorsqu'elle vérifie la disponibilité de ses fonds ; cependant, en détermine-t-elle les moyens et les finalités ? Le Groupe de travail « article 29 » nous aiguille à cet égard en indiquant les critères à prendre en compte, parmi lesquels figurent notamment l'initiative du traitement, l'autonomie du prestataire, le degré de contrôle exercé, l'influence de fait, le degré de précision dans la détermination des moyens et des finalités et l'expertise des parties. Ce dernier critère est également relevé par l'Autorité de protection des données belge[63]. Dans l'hypothèse étudiée, il est indubitable que la banque gestionnaire fait preuve d'expertise dans le traitement qu'elle opère. Cependant, il n'est pas contesté que l'initiative du traitement ne lui appartient pas. Il reste donc à établir si la banque gestionnaire de comptes bénéficie d'une autonomie accrue dans ce cadre, et plus important encore, si elle détermine les moyens essentiels de ce traitement.

62 F. Chen et B. Joanides, « Les prestataires de services de paiement face au nouveau règlement général européen sur la protection des données, *R.B.*, 22 décembre 2016, p. 1 ; Groupe de travail « article 29 », « Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" », *op. cit.*, p. 15.

63 Autorité de protection des données belge, « Le point sur les notions de responsable de traitement/sous-traitant au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats », disponible sur www.autoritédeprotectiondesdonnées.be.

B. Articulation des dispositions du livre VII du Code de droit économique et du R.G.P.D. en matière de services de paiement

12. D.S.P. II et Code de droit économique. La D.S.P. II impose le respect des droits fondamentaux, et notamment, du droit au respect de la vie privée et du droit à la protection des données[64]. À cet égard, elle mentionne expressément la directive 95/46/CE relative à la protection des données à caractère personnel[65] [66]. Ce texte ayant été abrogé, il convient de renvoyer aux dispositions du R.G.P.D.

En particulier, le considérant 89 de la D.S.P. II impose le respect des principes de finalité, de licéité, de nécessité, de proportionnalité, ainsi que des exigences liées à la conservation et à la sécurité des données. Les principes de protection des données « par défaut »[67] et « par *design* »[68] sont également mentionnés, alors même qu'ils étaient absents de la directive de 1995[69].

L'article 94 de la D.S.P. II règle spécifiquement les traitements de données à caractère personnel. Il est transposé à l'article VII.63 du Code de droit économique, sur lequel nous reviendrons par la suite (*infra*, n°s 18 et s.).

13. Focus sur certaines questions spécifiques en matière de protection des données à caractère personnel. Dans le cadre de la présente contribution, on examine certaines questions spécifiques posées par l'application des règles relatives aux traitements de données à caractère personnel dans le contexte des services de paiement.

On se penche d'abord sur les exigences de transparence et de sécurité, qui sont prescrites tant par la législation en matière de services de paiement que par le R.G.P.D. et la loi du 30 juillet 2018 (1).

On analyse ensuite les dispositions du livre VII du C.D.E. qui traitent spécifiquement de la protection des données en matière de services de paiement (2).

64 Cons. 46 et 90 de la D.S.P. II.

65 Directive (UE) 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, L 281 du 23 novembre 1995.

66 Cons. 89 et art. 94 de la D.S.P. II.

67 Le principe de protection des données « par défaut » implique que, par défaut, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement sont traitées ; cons. 78 et art. 25, al. 2, R.G.P.D. ; voy. E.D.P.B., « Guidelines 4/2019 on Art. 25 Data Protection by Design and by Default », disponible sur edpb.europa.eu, 13 novembre 2019 (adopted for public consultation), pp. 6 à 10.

68 Le principe de protection des données « par *design* » impose au responsable du traitement, lors de de la détermination des finalités du traitement ainsi que pendant l'opération de traitement, d'adopter les mesures et les garanties qui sont de nature à mettre en œuvre les principes de protection des données ; cons. 78 et art. 25, § 1er, du R.G.P.D. ; voy. aussi E.D.P.B., « Guidelines 4/2019 on Article 25 Data Protection by Design and by Default », disponible sur edpb.europa.eu, 13 novembre 2019 (adopted for public consultation), pp. 10 à 23.

69 A. Banck, « La DSP 2 et le R.G.P.D. sont-ils alignés ou orthogonaux ? », *op. cit.*

1. Transparence et sécurité

14. Transparence. Diverses obligations d'information sont imposées au prestataire de services de paiement par la D.S.P. II et le livre VII du Code de droit économique. Sur ce point, une distinction est d'ailleurs faite suivant qu'il s'agit d'une opération de paiement isolée[70] ou d'opérations couvertes par un contrat-cadre[71].

Par ailleurs, comme tout responsable du traitement, le prestataire de services de paiement devra respecter les articles 12 et suivants du R.G.P.D. relatifs à l'information de la personne concernée[72].

En vertu de ces dispositions, le responsable du traitement est tenu d'informer de manière détaillée la personne concernée au sujet du traitement équitable de ses données[73]. Cette information, dont le contenu diffère en fonction de l'origine des données collectées, doit être « aisément accessible »[74] et se faire « de façon concise et transparente »[75], c'est-à-dire, de manière efficace et succincte afin d'éviter de « noyer » la personne concernée[76]. À cet égard, le Groupe de travail « article 29 » conseille, pour ce qui concerne l'environnement numérique, de diviser en plusieurs niveaux la déclaration de confidentialité[77]. De cette manière, il n'est pas nécessaire, pour la personne concernée, de faire défiler de grandes quantités de texte avant de trouver l'information recherchée. Par ailleurs, il appartient au responsable du traitement, en vertu de l'article 12 du R.G.P.D., de *fournir* ces informations, c'est-à-dire de les communiquer de manière active ou, à tout le moins, de diriger activement les personnes concernées vers celles-ci[78]. Cette exigence découle également du critère « aisément accessible », selon lequel la personne doit accéder directement aux renseignements concernant ses données[79]. Ainsi, l'obligation d'information active est respectée par le responsable du traitement lorsqu'il renvoie vers l'emplacement de la déclaration de confidentialité au moyen d'un lien direct ou d'un code Q.R. En outre, le Groupe de travail « article 29 » recommande, à titre de bonne

70 Art. VII.13 et s. C.D.E.

71 Art. VII.20 et s. C.D.E.

72 Ces dispositions traitent du contenu de l'obligation d'information, du mode de communication et du moment où il faut transmettre les informations.

73 L'identité du responsable du traitement et de son délégué à la protection des données, les finalités du traitement opéré, les destinataires de ces traitements, la durée de conservation ou les droits de la personne concernée devront notamment être précisés. Concernant le contenu des informations à fournir, voy. Groupe de travail « article 29 », « Lignes directrices sur le consentement au sens du Règlement 2016/679 », 28 novembre 2017, WP 259 rév. 01, pp. 16 à 27.

74 Art. 12 R.G.P.D.

75 Art. 12 R.G.P.D.

76 Groupe de travail « article 29 », « Lignes directrices sur la transparence au sens du Règlement 2016/679 », 29 novembre 2017, WP 260 rév. 01, p. 7.

77 Groupe de travail « article 29 », « Lignes directrices sur la transparence au sens du Règlement 2016/679 », *op. cit.*, pp. 7, 16 et 22.

78 *Ibid.*, p. 21.

79 *Ibid.*, pp. 8 et 9.

pratique, de fournir le lien vers la police vie privée au moment et à l'endroit de la collecte des données à caractère personnel. Dans le cadre des nouveaux services de paiement, cette recommandation pourrait être mise en œuvre à travers des notifications de type *push*, c'est-à-dire des informations envoyées « juste à temps », via une bannière sur leur application par exemple, et des notifications de type *pull* qui facilitent l'accès à l'information à des moments pertinents[80].

Le prestataire de services de paiement devra, lorsqu'il collecte les données bancaires de l'utilisateur, veiller à mentionner le lien à partir duquel ce dernier pourra prendre connaissance de la politique de confidentialité. En d'autres termes, il appartient au prestataire de services de paiement de renvoyer vers sa police vie privée dès le premier contact[81] qu'il tisse avec son utilisateur, même si ce contact ne débouche ni sur l'exécution d'une opération de paiement, ni sur la conclusion d'un contrat-cadre.

15. Sécurité des opérations de paiement. Cette dernière décennie, les opérations de paiement vont croissant, en nombre et en complexité[82]. Cette mutation s'accompagne d'une augmentation des risques de sécurité tels que la perte – classique – de la carte de banque ou, depuis peu, l'interception de données bancaires lors d'un paiement sans contact[83]. Compte tenu de ces risques, de la faiblesse supposée des utilisateurs, de leur manque de confiance corrélatif dans les services de paiement et des objectifs poursuivis par la D.S.P. II, les législateurs, européen puis belge, ont dicté des mesures destinées à garantir la sécurité recherchée[84]. Cela passe notamment par l'adoption de mesures techniques et organisationnelles.

Systèmes de chiffrement de données (par le biais, p. ex., de mots de passe à usage unique), intervention de tiers de confiance, obligations de confidentialité, systèmes de détection de programmes malveillants, organisation interne de gouvernance de la donnée, tels sont des exemples de mesures techniques et organisationnelles à mettre en œuvre par les prestataires afin de sécuriser leurs services de paiement[85]. Plus précisément, les travaux préparatoires de la loi du 11 mars 2018 indiquent que « les mesures de sécurité devraient être compa-

80 *Ibid.*, pp. 24 et 25.

81 Notons, cependant, que si le prestataire n'a pas collecté directement les données de l'utilisateur auprès de celui-ci, il dispose, en vertu de l'article 14, paragraphe 3, point a), d'un délai maximal d'un mois pour fournir les informations exigées.

82 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 4.

83 A.-P. ANDRÉ-DUMONT, « Les services de paiement à l'épreuve des évolutions technologiques », *op. cit.*, p. 99.

84 Par ailleurs, l'Autorité bancaire européenne (A.B.E.) a élaboré des normes techniques et réglementaires (R.T.S.), adoptées par la Commission européenne le 27 novembre 2017 et entrées en application le 14 septembre 2019, voy. règlement délégué (UE) n° 2018/389 du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication, *J.O.U.E.*, L 69/23 du 13 mars 2018.

85 A. CHATELIER-CHAMOULAND, « Avantages et difficultés lors de la mise en œuvre du R.G.P.D. », *R.B.*, 27 mars 2019, p. 1.

tibles avec le niveau de risque associé au service de paiement »[86]. À cet égard, la D.S.P. II impose aux prestataires de services de paiement de mettre en place une politique de sécurité et d'intégrer, dans leurs systèmes de traitement des données, les principes de protection des données dès la conception et par défaut[87]. Ce point correspond au principe de sécurité et de confidentialité des données[88] et applique l'article 25 du R.G.P.D. selon lequel le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées afin de respecter les principes relatifs à la protection des données de façon effective.

Le prestataire de services de paiement, tenu de part et d'autre par des exigences de sécurité strictes, est donc incité à s'y conformer à plus d'un titre. En pratique, beaucoup de *FinTechs* recourent au *cloud computing*. Cette solution, qui présente l'avantage de s'adapter aisément à leur croissance, apporte de nouveaux risques de sécurité qu'il convient d'endiguer, notamment par la conclusion d'un contrat solide de sous-traitance avec le prestataire de *cloud*[89].

Lorsque l'opération de paiement non autorisée relève d'un incident opérationnel ou de sécurité majeur, il appartient au prestataire de services de paiement d'en informer sans retard la Banque nationale de Belgique[90] (ci-après, « B.N.B. »). Tel est le cas lorsque les infrastructures du prestataire font l'objet d'une *cyberattaque* ou présentent une faille de sécurité importante. À cette occasion, il appartient au prestataire de déterminer si l'incident rencontré est « majeur » au moyen des critères définis par l'Autorité bancaire européenne[91]. Par ailleurs, celui-ci devra vraisemblablement informer l'Autorité de protection des données, conformément aux obligations qui lui incombent en vertu du R.G.P.D., dès lors que ce type d'incidents (caractérisés par l'atteinte à l'intégrité, à la disponibilité ou à la confidentialité des données nécessaires au service de paiement) constitue généralement une violation de données à caractère personnel[92] [93]. Cependant, comme le précise le Groupe de travail « article 29 », un incident de sécurité ne constitue une violation de données que dans la mesure où les données violées sont à caractère personnel[94].

En conséquence, le prestataire de services de paiement dont le système subit un incident majeur, impliquant des données à caractère personnel, devra respecter une double procédure de notification. Or, les procédures ne sont pas

86 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 47.

87 D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *op. cit.*, p. 470.

88 Art. 5, § 1er, f), R.G.P.D.

89 N. Beaudemoulin, « Les enjeux liés à l'exploitation responsable des données par les établissements financiers », *R.B.*, 28 juin 2017, p. 1.

90 Art. 53 de la loi du 11 mars 2018 ; art. 96 D.S.P. II.

91 E.B.A., « Guidelines on major incidents reporting under directive (EU) 2015/2366 », EBA/GL/2017/10, disponible sur eba.europa.eu, 27 juillet 2017.

92 Voy. la définition de l'article 4.12 du R.G.P.D.

93 A. Banck, « La DSP 2 et le R.G.P.D. sont-ils alignés ou orthogonaux ? », *op. cit.*

94 Groupe de travail « article 29 », « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement 2016/679 », 3 octobre 2017, WP 250 rév. 01, p. 13.

les mêmes. À titre d'exemple, mentionnons le délai de notification : en matière de services de paiement, l'article 53 de la loi du 11 mars 2018 prévoit une notification sans retard (4 heures suivant les *Guidelines* de l'A.E.B.)[95], alors qu'un délai de 72 heures[96] est offert au responsable du traitement (à partir du moment où il en a pris connaissance)[97]. Il appartient donc au prestataire d'être attentif à ces différentes obligations de notification, d'autant plus que l'autorité à qui s'adresser, le contenu des informations à lui communiquer ou encore le canal à utiliser sont différents selon la réglementation concernée[98]. Dans ce contexte, la mise en place d'un guichet unique serait le bienvenu[99].

Le prestataire de services de paiement est également tenu de contacter ses utilisateurs si l'incident rencontré est susceptible d'avoir un impact sur leurs intérêts financiers. À cette occasion, il lui appartient de leur communiquer les mesures qu'ils peuvent adopter pour atténuer les effets dommageables dudit incident[100]. Cette information devra par ailleurs respecter l'article 34 du R.G.P.D. si l'incident rencontré est susceptible d'engendrer des risques pour les droits et libertés des personnes concernées. Cette disposition prévoit que la communication à la personne concernée « décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel » et doit, au minimum, indiquer le nom et les coordonnées du délégué à la protection des données, décrire les conséquences probables de la violation ainsi que les mesures que le responsable du traitement a prises ou envisage de prendre pour y remédier.

2. Traitements de données spécifiquement encadrés par la législation sur les paiements

16. Exigence du consentement explicite dans trois hypothèses. Le consentement explicite de l'utilisateur de services de paiement est exigé dans trois cas particuliers. Tout d'abord, tout prestataire de services de paiement doit obtenir le consentement explicite de l'utilisateur afin de traiter ses données, nécessaires à la fourniture du service de paiement[101]. Le consentement est éga-

95 E.B.A., « Guidelines on major incidents reporting under directive (EU) 2015/2366 », *op. cit.*

96 S. McInnes, « The EBA's Final Guidelines on Major Incident Reporting under PSD 2 », octobre 2017, disponible sur www.dataguidance.com, consulté le 4 décembre 2019, p. 18 ; R. Frajman et Th. Leblond, « DSP 2, RTS : comment démontrer sa conformité ? », *R.B.*, 26 mars 2019, p. 3.

97 S. McInnes, « The EBA's Final Guidelines on Major Incident Reporting under PSD 2 », *op. cit.*, p. 18. Art. 33 du R.G.P.D.

98 En ce qui concerne l'obligation de notification de violations de données à caractère personnel, voy. Groupe de travail « article 29 », « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement 2016/679 », *op. cit.*

99 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 », *op. cit.*, p. 4.

100 Art. 92 de la D.S.P. II.

101 Art. VII.63, al. 3, C.D.E. ; art. 94, § 2, de la D.S.P. II.

lement requis pour le service d'initiation de paiement[102] et le service d'information sur les comptes[103].

L'application des dispositions concernées suscite des questions d'interprétation. À ce stade, seul le Comité européen de la protection des données (ci-après, « C.E.P.D. »[104]) s'est penché sur certaines d'entre elles, après avoir été interpellé par la députée européenne Sophie in't Veld. L'organe européen a répondu à cette interpellation par une lettre datée du 5 juillet 2018[105]. Bien que ce type de document n'ait qu'une valeur d'interprétation, on peut s'y référer dans l'attente de lignes directrices du C.E.P.D. à ce sujet (annoncées pour l'année 2019-2020[106]).

17. Le consentement (explicite) en vertu du R.G.P.D. L'article 6 du R.G.P.D. énumère six fondements légitimes[107] susceptibles de justifier le traitement de données, parmi lesquels figure le consentement de la personne concernée. En d'autres termes, il suffit au responsable du traitement de collecter le consentement de l'individu pour respecter le principe de licéité consacré par le R.G.P.D. Il convient toutefois d'apporter une nuance importante à ce principe : le traitement ne sera licite que si le consentement de la personne concernée est libre, spécifique, éclairé et univoque[108].

En premier lieu, le consentement doit être libre, ce qui implique que la personne concernée se voit offrir un choix réel concernant le traitement envisagé de ses données[109]. *A contrario*, l'individu qui ne peut refuser son consentement sans subir de préjudice ne peut consentir valablement au traitement. C'est par exemple le cas lorsque la fourniture d'un service dépend du consentement au traitement de données, alors même que ce traitement n'est pas nécessaire à l'exécution dudit contrat[110].

Par ailleurs, la personne concernée doit être informée de la possibilité de retirer son accord à tout moment, sans justification aucune et d'une façon aussi simple que celle par laquelle elle l'a donné[111].

102 Art. 48, § 1er, 3°, de la loi du 11 mars 2018 ; art. 67, 2, a), D.S.P. II.

103 Art. 98, § 3, 6°, de la loi du 11 mars 2018 ; art. 66, 3, c).

104 Le Comité européen de la protection des données (anciennement, le Groupe de travail « article 29 ») est un groupe de travail européen indépendant, institué par l'article 68 du R.G.P.D., traitant de questions de protection des données à caractère personnel et de la vie privée. Il est doté de la personnalité juridique et peut prendre des décisions contraignantes.

105 C.E.P.D., EDPB-84-2018, Bruxelles, disponible sur edpb.europa.eu, 5 juillet 2018.

106 E.D.P.B., « Work program 2019/2020 », disponible sur edpb.europa.eu, 12 février 2019.

107 Outre le consentement de la personne concernée, le traitement de données à caractère personnel peut être nécessaire à l'exécution d'un contrat ou à l'exécution d'une mission relevant de l'exercice de l'autorité publique, au respect d'une obligation légale, aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ou pour protéger les intérêts fondamentaux de la personne concernée.

108 Art. 4, 11, R.G.P.D.

109 Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, « Manuel de droit européen en matière de protection des données », Luxembourg, édition 2018, p. 163.

110 Cons. 42 et art. 7 R.G.P.D.

111 Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *op. cit.*, p. 167.

En deuxième lieu, la personne concernée doit consentir de manière éclairée au traitement de ses données, ce qui signifie qu'elle doit disposer de suffisamment d'informations avant de prendre sa décision. Le R.G.P.D. précise à cet égard que « la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel »[112].

En troisième lieu, le consentement de la personne concernée doit être spécifique à la finalité du traitement, ce qui implique, d'une part, que celle-ci soit exprimée en des termes clairs et non équivoques, d'autre part, que dans l'hypothèse de finalités multiples, le consentement soit collecté pour chacune d'elles[113].

En dernier lieu, il est requis que la personne concernée consente de manière univoque ce qui signifie qu'« il ne doit pas exister de doute raisonnable quant au fait que la personne concernée souhaitait donner son accord au traitement de ses données »[114 115]. De cette exigence découle l'obligation de collecter le consentement via une déclaration ou une action affirmative de la personne concernée.

Outre ces quatre exigences, le consentement devra dans certains cas être explicite, notamment si les données qui font l'objet du traitement sont des données particulières au sens du R.G.P.D. Dans cette hypothèse, il est nécessaire de disposer d'une déclaration expresse de la part de la personne concernée.

18. Le consentement explicite en vertu de l'article VII.63 du Code de droit économique. L'article VII.63 du Code de droit économique dispose 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 explicite de l'utilisateur de services de paiement ».

Cette disposition, lue à la lumière du R.G.P.D., implique que le consentement requis soit, comme nous venons de l'exposer, libre, éclairé, spécifique, univoque et explicite, c'est-à-dire affirmé par une déclaration expresse de la partie concernée.

Cette lecture de l'article VII.63 du Code de droit économique débouche sur des difficultés pratiques de poids, notamment quant au caractère libre du consentement et à la question de son retrait.

Tout d'abord, l'utilisateur d'un service de paiement bénéficie-t-il effectivement d'une liberté de choix concernant le traitement de ses données de paiement ? On peut légitimement répondre par la négative dès lors que, dans

112 Cons. 49 R.G.P.D.

113 Cons. 32 R.G.P.D.

114 Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *op. cit.*, p. 166.

115 Art. 4.11 R.G.P.D.

l'hypothèse d'un refus de sa part, le service de paiement ne pourra tout simplement être fourni[116].

Ensuite, *quid* si, dans un premier temps, l'utilisateur consent au traitement de ses données puis, soudainement, décide de retirer son accord ? Il semble que ce retrait entrainerait la rupture de la convention, le prestataire n'étant plus en mesure de livrer son service.

Ces difficultés pratiques illustrent le problème fondamental de l'article VII.63 du Code de droit économique lorsqu'il est interprété à la lumière du R.G.P.D. : cette disposition semble mettre en lien le consentement de l'utilisateur et la fourniture du service de paiement[117]. Or, nous l'avons déjà souligné, le R.G.P.D. interdit strictement ce lien lorsque le traitement n'est pas nécessaire à l'exécution du contrat.

Par ailleurs, interpréter l'exigence de consentement explicite au regard de la législation relative à la protection des données revient à donner à l'article VII.63 du Code de droit économique un caractère de *lex specialis* par rapport au R.G.P.D.[118]. En effet, selon cette lecture, le consentement explicite de l'utilisateur de services de paiement concernant le traitement de ses données serait exigé alors même que ce traitement pourrait être, en vertu du R.G.P.D., fondé sur une autre base de licéité (par exemple, les intérêts légitimes du responsable du traitement)[119].

19. Le consentement explicite en vertu de l'article VII.63 du Code de droit économique interprété par le C.E.P.D. Le C.E.P.D. s'est prononcé sur l'interprétation qu'il convient de donner à l'article 94 de la D.S.P. II (et, partant, à l'article VII.63 du Code de droit économique, qui le transpose en droit belge).

Dans sa lettre du 5 juillet 2018, il précise que le consentement explicite exigé par la législation sur les services de paiement est de nature contractuelle, ce qui le distingue du consentement explicite du R.G.P.D. À cet égard, l'organe européen renvoie au considérant 87 de la D.S.P. II, selon lequel cette directive ne devrait concerner que des obligations contractuelles, c'est-à-dire des opérations de paiement sous-tendues par un contrat.

Or, l'existence d'une convention entre le prestataire de services de paiement et l'utilisateur justifie, au sens du R.G.P.D., le traitement par le premier

116 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 », *op. cit.*, p. 17.

117 *Ibid.*, p. 18.

118 S. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », *op. cit.* ; notons que la position du C.E.P.D. est confirmée par l'avis de l'A.B.E. du 13 juin 2018 sur la mise en œuvre des R.T.S., voy. G. Koliferah, « Les données à l'épreuve de la DSP 2 et du R.G.P.D. », *R.B.*, 27 mars 2019, p. 1.

119 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 65.

des données du second[120]. En d'autres termes, le traitement des données de l'utilisateur se fonde sur l'exécution du contrat de prestation de services et non sur le consentement de ce dernier.

Par conséquent, l'exigence de consentement explicite de la D.S.P. II ne vise pas à fonder le traitement en vertu du R.G.P.D., mais s'inscrit plutôt dans le cadre du principe de transparence[121] : la personne concernée doit être pleinement consciente des finalités pour lesquelles ses données sont traitées et doit être en mesure de déterminer la portée et les conséquences du traitement opéré[122].

À cet égard, le Comité indique que les clauses d'information relatives aux traitements de données à caractère personnel doivent être « *clearly distinguishable* »[123], ce qui renvoie à l'exigence de consentement éclairé. Il ne précise toutefois pas la manière dont il convient de séparer ces clauses du reste du contrat de prestation de services de paiement. Quoi qu'il en soit, il ne peut être considéré que l'utilisateur donne son consentement explicite au traitement de ses données lorsqu'il accepte les conditions générales de la banque[124]. En revanche, selon l'Autorité de protection des données hollandaise, celui-ci pourrait être recueilli, dans l'environnement numérique, via une fenêtre séparée (un *pop-up* p. ex.)[125]. Cette position rejoint la recommandation du Groupe de travail « article 29 » selon laquelle il est possible, pour fournir des informations sur la transparence, d'avoir recours à des notifications de type *push*, données « juste à temps »[126]. Le législateur belge, quant à lui, considère que l'utilisateur partie à un contrat-cadre consent au traitement de ses données aux fins des opérations de paiement visées par ledit contrat lorsqu'il consent à l'exécution des opérations de paiement en question[127].

Quant au traitement de données pour d'autres finalités que celles nécessaires à l'exécution du contrat, le C.E.P.D. précise qu'il peut être opéré, pour autant que le prestataire ait collecté le consentement de l'utilisateur concernant ces autres finalités[128]. On émet toutefois une réserve sur ce point concernant

120 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 », *op. cit.*, p. 2.

121 Voy. cons. 39 R.G.P.D. selon lequel « [l]e principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples ».

122 Groupe de travail « article 29 », « Lignes directrices sur la transparence au sens du Règlement 2016/679 », *op. cit.*, p. 8.

123 C.E.P.D., EDPB-84-2018, Bruxelles, disponible sur edpb.europa.eu, 5 juillet 2018.

124 Clifford Chance, « PSD 2 – innovation and GDPR – protection : a fintech balancing act. Part one : Consent », accessible sur talkingtech.cliffordchance.com, 6 novembre 2019.

125 X, « The Netherlands tackles uncertainties around PSD2 consent and GDPR », disponible sur www.medium.com, 20 novembre 2018.

126 Groupe de travail « article 29 », « Lignes directrices sur la transparence au sens du Règlement 2016/679 », *op. cit.*, p. 8.

127 *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3131/001, p. 66.

128 Concernant les conditions auxquelles le consentement collecté doit satisfaire, voy. Groupe de travail « article 29 », « Lignes directrices sur le consentement au sens du Règlement 2016/679 », *op. cit.*

les prestataires de services d'initiation de paiement et d'information sur les comptes[129].

En conséquence, en vertu de l'article VII.63 du Code de droit économique, l'utilisateur de services de paiement est amené à consentir explicitement (c'est-à-dire sur la base d'une information préalable spécifique et séparée) aux traitements opérés sur ses données, qui sont nécessaires, au sens du R.G.P.D., à l'exécution du contrat de prestation de services de paiement.

20. Traitement des données dans le cadre des services d'initiation de paiement et d'information sur les comptes. En ce qui concerne le prestataire de services d'initiation de paiement, il y a lieu de se référer à l'article 48 de la loi du 11 mars 2018[130] qui traite de la protection de certaines données. En vertu de cette disposition, l'établissement initiateur de paiement veille à garantir la confidentialité des données de sécurité personnalisées, c'est-à-dire des identifiants et mots de passe de l'utilisateur émis d'ordinaire par sa banque traditionnelle. En effet, ces données ne peuvent être accessibles qu'à l'utilisateur et ladite banque et ne doivent être transmises qu'au moyen de canaux sûrs et efficaces. Par ailleurs, elles ne peuvent être conservées par le prestataire étant donné leur qualité de données de paiement sensibles[131].

Les autres données de l'utilisateur nécessaires au service d'initiation de paiement ne peuvent être communiquées qu'au bénéficiaire et uniquement avec le consentement explicite du premier. La D.S.P. II se montre donc plus contraignante que le R.G.P.D. concernant l'usage des données relatives à l'utilisateur, celles-ci ne pouvant être traitées en dehors du service d'initiation de paiement alors même que le prestataire disposerait d'un fondement légal pour le traitement envisagé.

Quant au prestataire de services d'information sur les comptes, il y a lieu de se référer à l'article 98 de la loi du 11 mars 2018[132]. Cette disposition est relativement similaire à l'article VII.63 du Code de droit économique, qui s'applique à tout prestataire de services de paiement, sauf en ce qui concerne les données auxquelles l'agrégateur de comptes peut avoir accès, et qui sont limitées aux informations provenant des comptes de paiement désignés, à l'exclusion des données de paiement sensibles.

Aux termes de l'article 98, § 3, de la loi du 11 mars 2018, « l'établissement de paiement agrégateur de comptes n'utilise, ne consulte et ne conserve des données à des fins autres que la fourniture du service d'information sur les comptes expressément demandé par l'utilisateur de services de paiement,

129 *Infra*, n° 20.

130 Art. 66 de la D.S.P. II.

131 Rappelons qu'en ce qui concerne les prestataires de services d'initiation de paiement et d'information sur les comptes, la notion de données de paiement sensibles ne recouvre pas le nom du titulaire du compte NI le numéro de compte.

132 Art. 67 de la D.S.P. II.

conformément aux dispositions légales et réglementaires, le cas échéant de droit étranger, régissant la protection des données à caractère personnel ».

Cette formulation, en ce qu'elle fait référence aux principes encadrant la protection des données à caractère personnel, peut être interprétée de deux façons radicalement opposées. Soit, on comprend que les données ne peuvent tout simplement pas être traitées à des fins autres que la fourniture du service d'information sur les comptes expressément demandé par l'utilisateur. Soit, on comprend que, contrairement au prestataire de services d'initiation de paiement, l'agrégateur de comptes peut traiter les données collectées à des fins autres que le service d'information sur les comptes, pour autant que ce traitement respecte le R.G.P.D. (par exemple, après avoir obtenu le consentement de l'utilisateur concernant ces nouvelles finalités)[133].

À notre connaissance, aucune autorité compétente (que ce soit l'Autorité bancaire européenne[134], la Commission ou encore le Comité européen de protection des données) ne s'est encore penchée sur cette question[135]. Le C.E.P.D. a toutefois précisé, dans le cadre de sa lettre du 5 juillet 2018, que les traitements effectués sur les données de tiers à l'occasion de services d'initiation de paiement ou d'information sur les comptes ne peuvent être opérés à des fins étrangères à celles pour lesquelles ces données ont été collectées. Cette position peut-elle être défendue *mutatis mutandis* dans le cadre de traitements ultérieurs des données de l'utilisateur personne concernée ? Cela aurait pour conséquence de remettre en doute la pertinence du modèle économique de ces nouveaux acteurs qui, dans la majorité des cas, ne se limitent pas à communiquer à l'utilisateur ses soldes et ses listes d'opérations de paiement mais, au contraire, lui proposent un arsenal de fonctionnalités complémentaires[136].

Dans l'attente d'un avis précis sur cette question[137], les prestataires doivent se montrer vigilants concernant les traitements ultérieurs qu'ils envisageraient d'opérer. Notons que certains semblent plus catégoriques et interdisent tout traitement ultérieur, comme la Banque centrale de Hongrie ou la France qui n'a tout simplement pas repris, dans sa loi de transposition[138], la référence aux principes encadrant la protection des données[139].

133 L. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », *op. cit.*

134 Qui est notamment chargée de veiller à la convergence des pratiques réglementaires autour de la D.S.P. II.

135 L. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », *op. cit.*

136 G. Richard, « Nouveau droit d'accès aux comptes et aux données des comptes », *op. cit.*, p. 5.

137 Qui devrait, selon le programme du C.E.P.D., être adopté au cours de l'année 2020 dans le cadre de lignes directrices concernant l'articulation de la D.S.P. II et du R.G.P.D.

138 Art. L. 133-41, 6°, C. mon. et fin. Notons, toutefois, que certains auteurs français plaident pour une lecture nuancée de cette disposition. À cet égard, voy. G. Richard, « Nouveau droit d'accès aux comptes et aux données des comptes », *op. cit.*, p. 5.

139 L. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », *op. cit.* ; 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 », *op. cit.*, p. 3.

21. Le traitement des *silent parties data*. Tout service de paiement nécessite d'opérer des traitements sur les données de tiers. En effet, l'exécution ou l'initiation d'une opération de paiement à l'attention d'un particulier nécessite de collecter certaines données de cette tierce partie (notamment son numéro de compte). De même, l'agrégation des données bancaires d'un utilisateur commande de recueillir des informations sur ses transactions bancaires, dont certaines concernent ses bénéficiaires. Ces exemples renvoient à la problématique du traitement des données des *silent parties* : comment justifier, au sens du R.G.P.D., les traitements effectués sur les données de tiers à l'opération de paiement qui, par hypothèse, ne sont liés, au prestataire de services, par aucun contrat ?

En présence des nouveaux prestataires de services, ces traitements sont de deux ordres.

Tout d'abord, la banque gestionnaire de comptes est tenue, en vertu de l'objectif d'*Open Banking* poursuivi par la D.S.P. II, de rendre les données de tiers accessibles au prestataire de services d'initiation de paiement ou d'information sur les comptes. S'agissant d'une obligation légale, le traitement en question est justifié au sens du R.G.P.D.

Ensuite, les données de tiers sont traitées par le prestataire de services d'initiation de paiement/d'information sur les comptes, lui-même, en vue de la fourniture de son service. Le C.E.P.D. a considéré, dans sa lettre du 5 juillet 2018, que le traitement opéré sur les données de tiers peut se baser, compte tenu de l'absence de contrat, sur le fondement des intérêts légitimes poursuivis par une partie tierce[140]. En effet, dans le cadre d'un service d'initiation de paiement, le bénéficiaire a, en toute logique, un intérêt à voir se réaliser l'opération de paiement.

Quant au service d'information sur les comptes, les intérêts légitimes du titulaire du compte à obtenir la centralisation de ses informations de paiement justifient le traitement des données de tiers. Le C.E.P.D. précise toutefois qu'à son sens, les données de tiers collectées dans le cadre de l'un de ces nouveaux services ne peuvent être traitées à des fins autres que celles nécessaires auxdits services. Par ailleurs, il rappelle également les balises posées par le R.G.P.D. que sont notamment les principes de transparence, de minimisation des données et de proportionnalité. Ce dernier principe empêche le prestataire de services d'information sur les comptes[141] de se fonder systématiquement sur les intérêts légitimes de son utilisateur dès lors qu'en vertu de l'article 6 du R.G.P.D., une pondération des intérêts en présence doit être réalisée[142]. En d'autres termes, l'agrégateur de comptes peut traiter les données des tiers mentionnées dans les

140 Hogan Lovells, « EDPD clarifies interaction between PSD 2 and the GDPR – but does it go far enough? », disponible sur www.lexology.com, 30 juillet 2018.

141 À la différence du prestataire de services d'initiation de paiement puisque son traitement est précisément justifié par les intérêts légitimes de la personne concernée.

142 L. McInnes et L. Sampedro, « EU : The interplay of PSD 2 and GDPR – Some select issues », *op. cit.*

différents comptes de paiement de son utilisateur, pour autant que l'intérêt de ce dernier à voir l'ensemble de ses données de paiement agrégées est supérieur à l'atteinte occasionnée aux droits et libertés des personnes visées par certaines de ces données.

Section 2
Protection des données à caractère personnel en matière de crédit

22. Plan de la section 2. La présente section examine les principales règles applicables aux traitements de données à caractère personnel dans le domaine du crédit[143]. Après un bref rappel du cadre normatif, on se penche sur les règles spécifiques prévues par le titre 4 du livre VII du Code de droit économique, relatives à la transmission des données à des tiers, à la consultation de la Centrale des crédits aux particuliers et à d'autres questions ponctuelles régies par ces dispositions (en matière de conservation des données ou de base de licéité p. ex.).

A. Cadre normatif

23. Dispositions spécifiques dans le livre VII du Code de droit économique. Dans le titre 4 du livre VII du Code de droit économique, relatif aux contrats de crédits, des dispositions spécifiques encadrent les traitements de données à caractère personnel.

Il faut ainsi avoir égard aux articles VII.116 et suivants (crédit à la consommation), VII.147/32 et suivants (crédit hypothécaire) et VII.148 et suivants (Centrale des crédits aux particuliers, pour les crédits à la consommation et hypothécaires).

Deux arrêtés royaux sont également pertinents dans l'hypothèse qui nous occupe :

- l'A.R. du 23 mars 2017 réglementant la Centrale des crédits aux particuliers[144] (ci-après, « l'A.R. du 23 mars 2017 ») ;
- l'A.R. du 20 novembre 1992 relatif au traitement des données à caractère personnel en matière de crédit à la consommation[145] (ci-après, « l'A.R. du 20 novembre 1992 »).

143 À cet égard, voy. Y. Poullet et A. Lefebvre, « Vie privée et crédit à la consommation, protéger le consommateur ou sa vie privée : un choix difficile », *Le crédit à la consommation*, Bruxelles, Éd. du Jeune Barreau, 1997, pp. 103 et s. ; Th. Léonard et A. Mention, « Crédit à la consommation et protection des données à caractère personnel : un aperçu des règles protectrices », *Handboek consumentenkrediet*, Bruges, la Charte, 2007, pp. 449 et s.

144 *M.B.*, 31 mars 2017.

145 *M.B.*, 11 décembre 1992. Cet arrêté royal a été pris en exécution de la loi du 12 juin 1991 relative au crédit à la consommation (à laquelle il est d'ailleurs fait référence à l'article 1, 1°, de l'A.R. du 20 novembre

24. Articulation du R.G.P.D. et des dispositions du livre VII du Code de droit économique. Les dispositions spécifiques aux traitements des données à caractère personnel, qui figurent actuellement dans le livre VII du Code de droit économique (titre 4 sur les contrats de crédit), ont été adoptées lorsque la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[146] était d'application.

Cette loi de 1992 est désormais abrogée[147], de même que la directive 95/46/CE, dont elle assurait la transposition en droit belge. Aucune modification n'a par contre été apportée aux dispositions du titre 4 du livre VII. Aussi faut-il lire les références aux dispositions de la loi du 8 décembre 1992 comme des renvois aux dispositions correspondantes de la loi du 30 juillet 2018 ou du R.G.P.D.[148].

Sans révolutionner le droit à la protection des données, le R.G.P.D. apporte diverses modifications qui tendent à renforcer le niveau de protection dont bénéficient les personnes concernées (avec, corrélativement, des obligations supplémentaires dans le chef du responsable du traitement et du sous-traitant).

S'agissant d'un règlement européen, il est directement applicable dans les États membres et, en cas de contradiction ou d'incohérence avec une disposition de droit national, cette dernière doit s'effacer pour permettre l'application pleine et entière du règlement. Cette primauté du droit de l'Union ne prive toutefois pas les États membres d'une certaine marge de manœuvre, pour certaines questions spécifiques.

L'article 23 du R.G.P.D. autorise ainsi les États membres à «limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22». Plusieurs conditions doivent néanmoins être observées. Il doit s'agir de mesures législatives, et la limitation éventuelle doit respecter «l'essence des libertés et droits

1992). Cette loi a été abrogée par la loi du 19 avril 2014 portant insertion du livre VII «Services de paiement et de crédit» dans le Code de droit économique, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres Ier et XV du Code de droit économique, et portant diverses autres dispositions. L'article 54, § 1er, de cette loi du 19 avril 2014 énonce que «les dispositions réglementaires prises en exécution de la loi du 12 juin 1991 relative au crédit à la consommation, de la loi du 4 août 1992 relative au crédit hypothécaire, de la loi du 10 août 2001 relative à la Centrale des crédits aux particuliers et de la loi du 24 mars 2003 instaurant un service bancaire de base demeurent en vigueur jusqu'à leur abrogation». L'A.R. du 20 novembre 1992 reste donc applicable, et concernant les références aux dispositions de la loi du 12 juin 1991, il faut avoir égard aux «dispositions équivalentes du Code de droit économique» (art. 55 de la loi du 19 avril 2014).

146 Cette loi avait d'ailleurs été modifiée en 1998 en vue de transposer la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée par l'article 94 du R.G.P.D., avec effet au 25 mai 2018.

147 Art. 280 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

148 Voy. art. 253 de la loi du 30 juillet 2018.

fondamentaux», tout en constituant une mesure «nécessaire et proportionnée dans une société démocratique» pour garantir certains objectifs énumérés de manière limitative. Parmi ceux-ci, on trouve notamment «les objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale» (*littera* e) ou «la protection de la personne concernée ou des droits et libertés d'autrui» (*littera* i). S'agissant de la marge de manœuvre laissée aux États membres, on peut également avoir égard à l'article 6, § 2, du R.G.P.D., aux termes duquel «les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX»[149].

Dans son code annoté, le S.P.F. Économie n'exclut pas qu'une éventuelle incompatibilité puisse exister. On lit en effet que «le R.G.P.D. prévaut donc sur les dispositions relatives aux traitements de données intégrées dans le C.D.E. Si les dispositions réglementaires contraires ou incompatibles ne sont pas adaptées, elles ne peuvent plus être appliquées. Les dispositions relatives au traitement des données dans le C.D.E., restent donc d'application pour les dispositions additionnelles qui ne sont pas contraires au R.G.P.D. et qui ne seraient pas remplacées par des dispositions identiques du R.G.P.D.»[150]. Les prêteurs sont par conséquent dans une situation délicate, source d'insécurité juridique, puisqu'ils peuvent être amenés à appliquer de manière concurrente des dispositions légales potentiellement incompatibles entre elles. Aussi regrette-t-on vivement que le législateur belge n'ait pas procédé à l'analyse encadrée par l'article 23 ou l'article 6, §§ 2 et 3, du R.G.P.D., pour confirmer la conformité des dispositions spécifiques du livre VII (ou, à défaut, pour les abroger ou les amender en conséquence).

B. Acteurs et rôle au sens du R.G.P.D.

25. Acteurs impliqués, directement ou indirectement, dans un crédit à la consommation ou un crédit hypothécaire. Plusieurs acteurs

149 Comme le prévoit l'article 6, § 3, du R.G.P.D., les dérogations peuvent concerner «les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX».

150 S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees#definition.

sont généralement impliqués dans l'octroi et la gestion d'un contrat de crédit à la consommation. Eu égard à la manière dont les concepts sont définis par la loi, le « crédit à la consommation »[151] ou le « crédit hypothécaire »[152] supposent en tout cas la conclusion d'un contrat entre un « prêteur »[153] et un « consommateur »[154].

Le cas échéant, un « intermédiaire de crédit »[155], intervenant comme « agent lié »[156] ou « courtier »[157], peut également jouer un rôle. L'intermédiation en crédit est ainsi définie comme l'« activité consistant à : a) présenter ou proposer des contrats de crédit aux consommateurs ; b) assister les consommateurs en réalisant pour des contrats de crédit des travaux préparatoires autres que ceux visés au a) ; ou c) conclure des contrats de crédit avec des consommateurs pour le compte d'un prêteur ou pour compte propre lorsque l'activité est exercée par un prêteur qui ne fait pas appel à un intermédiaire de crédit »[158].

Par ailleurs, les prêteurs peuvent faire appel à un assureur-crédit, en vue de couvrir le risque engendré par le manquement du consommateur à ses obligations (de remboursement du crédit).

Des autorités publiques peuvent également être amenées à intervenir, comme B.N.B. (qui gère notamment la Centrale des crédits aux particuliers), la F.S.M.A. ou le S.P.F. Économie, dans le cadre de leurs missions respectives.

S'agissant spécialement de la consultation de la Centrale des crédits aux particuliers, qui constitue une obligation légale dans le chef des prêteurs (voy. *infra*, n° 36), un mandat pourrait être donné à certains tiers (un assureur-crédit ou un autre prêteur, par exemple), dans les conditions de l'article 14 de l'A.R. du 23 mars 2017.

26. Qualification des principaux acteurs, au sens du R.G.P.D. Les principales obligations prescrites par le R.G.P.D. doivent être observées par le « responsable du traitement » et, dans une moindre mesure, par le « sous-traitant ». Aussi faut-il déterminer si les acteurs impliqués dans le contrat de crédit interviennent en qualité de responsable (ou de coresponsable), de sous-traitant ou de tiers (tels que définis par le R.G.P.D.[159]).

Il paraît difficilement contestable que le prêteur agit comme responsable du traitement : c'est lui, en effet, qui détermine les moyens et les finalités du traitement[160]. Quant au consommateur, il s'agit de la personne concernée.

151 Tel que défini à l'article I.9, 54°, C.D.E.
152 Tel que défini à l'article I.9, 53/3, C.D.E.
153 Tel que défini à l'article I.9, 34°, C.D.E.
154 Tel que défini à l'article I.1, 2°, C.D.E.
155 Tel que défini à l'article I.9, 35°, C.D.E.
156 Tel que défini à l'article I.9, 36°, C.D.E.
157 Tel que défini à l'article I.9, 37°, C.D.E.
158 Art. I.9, 94°, C.D.E.
159 Voy. la contribution de C. DE TERWANGNE, dans le présent ouvrage, pour l'analyse de ces notions.
160 Voy., p. ex., Civ. Bruxelles, 15 octobre 2003, *J.T.*, 2004, p. 140.

Lorsque l'assureur-crédit intervient *qualitate qua*, il doit également être vu comme le responsable du traitement. Des difficultés devront à cet égard être surmontées, notamment en ce qui concerne le respect des obligations d'information au bénéfice de la personne concernée puisqu'en pratique, il n'a pas de relation directe avec celle-ci.

S'agissant de l'intermédiaire de crédit, comme le courtier, une réponse plus nuancée s'impose. D'une part, il peut être vu comme un sous-traitant du prêteur, pour les missions exécutées pour le compte de ce dernier, spécialement la transmission des informations dans le cadre de l'octroi du crédit, par exemple. Les exigences de l'article 28 du R.G.P.D. doivent par conséquent être respectées (et, notamment, la conclusion d'une convention *ad hoc*). D'autre part, l'intermédiaire intervient en qualité de responsable du traitement pour les finalités liées au développement de la relation commerciale à l'égard de la clientèle, et pour laquelle il détermine les finalités et les moyens du traitement.

Pour les données de la C.C.P., c'est la B.N.B. qui est normalement le responsable du traitement[161]. Il lui incombe en effet d'enregistrer dans la C.C.P. les données communiquées par les prêteurs (ou toute autre personne débitrice d'une obligation de communication), tout en permettant aux personnes limitativement énumérées de la consulter.

On rappelle encore que les qualifications précitées sont relatives, au sens où elles s'appliquent dans le cadre de traitements de données précisément circonscrits.

27. Notion de « tiers » utilisée dans le livre VII du C.D.E. Les dispositions spécifiques du livre VII du Code de droit économique encadrent des aspects déterminés des traitements de données à caractère personnel et, en particulier, leur transmission à certains destinataires.

La transmission à des tiers n'est en effet possible que conformément aux conditions des articles VII.116 et suivants du Code de droit économique (pour le crédit à la consommation)[162].

Comme on le verra (*infra*, n° 29), cette transmission n'est possible que pour atteindre les finalités énumérées à l'article VII.117 du C.D.E. et pour les seules données visées à l'article VII.118 du C.D.E. En outre, l'article VII.119 du C.D.E. énumère les personnes susceptibles d'être les destinataires de ces informations (et au nombre desquelles les intermédiaires de crédit ont été délibérément exclus).

Dans son code annoté des crédits aux consommateurs, le S.P.F. Économie considère que le « tiers » visé par ces dispositions (et notamment l'article VII.116

161 Voy. à cet égard Civ. Bruxelles, 15 octobre 2003, *J.T.*, 2004, p. 140.
162 Voy. art. VII.147/32 et s. C.D.E. pour le crédit hypothécaire.

du C.D.E.) doit être compris au sens du R.G.P.D.[163]. Il s'agit donc d'une « personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel »[164]. D'un point de vue légistique, il est évidemment souhaitable qu'un terme donné (comme celui de « tiers ») soit défini de manière uniforme dans un même contexte spécifique (comme celui de la protection des données). En l'occurrence, on peut toutefois se demander si le législateur n'ouvre pas la porte à un possible contournement des objectifs poursuivis. En effet, dès lors que la notion de « tiers » exclut expressément les sous-traitants et que, pour certaines de leurs activités dans le cadre du crédit, les intermédiaires pourraient être considérés comme tels, cela signifie qu'en cette qualité de « sous-traitant » (au sens de la protection des données), ils échappent aux restrictions établies aux articles VII.116 et suivants du Code de droit économique. Certes, dans ce rôle, les traitements susceptibles d'être réalisés par les intermédiaires sont limités et précisément encadrés (puisqu'ils doivent agir au nom et pour le compte du responsable du traitement, et sur la base d'une instruction documentée de ce dernier) ; le risque existe cependant que certains intermédiaires ne distinguent pas les deux fonctions.

C. Règles spécialement applicables aux consommateurs de crédits

28. Focus sur certaines questions. Lorsque des données à caractère personnel sont traitées dans le cadre de la gestion et de l'octroi d'un crédit à la consommation ou d'un crédit hypothécaire, le responsable du traitement – prêteur, assureur-crédit, B.N.B., intermédiaire de crédit, etc. – doit respecter les exigences prescrites par le R.G.P.D. et, le cas échéant, la loi du 30 juillet 2018.

Aussi doit-il s'assurer que les traitements sont conformes aux principes établis à l'article 5 du R.G.P.D., qu'ils soient fondés sur l'une des bases de licéité de l'article 6, dans le respect des droits de la personne concernée (art. 12 et s. R.G.P.D.) et des autres obligations spécifiques du règlement (exigence de sécurité, analyse d'impact, transfert éventuel vers des pays tiers, etc.).

Dans le cadre de la présente contribution, on peut difficilement reprendre chacune de ces exigences, pour les appliquer au contexte du crédit[165]. Du reste, elles ne sont pas forcément propres à ce secteur. Aussi mettons-nous l'accent sur

163 S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees/transmission-des-donnees-collectees-pour-un-credit-2/vii-119-vii-147-35-tiers-autorises.

164 Art. 4, 10°, du R.G.P.D.

165 Pour une telle analyse, voy. S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees#le-rgpd-le-cadre-general.

les exigences spécifiques qui figurent dans le livre VII du Code de droit économique, pour les présenter à la lumière des obligations générales du R.G.P.D.

On examine la transmission des données à caractère personnel à un tiers (1), les traitements effectués en lien avec la C.C.P. (2) et d'autres questions réglées par le livre VII en matière de traitements de données, comme la base de licéité ou la conservation des données (3).

1. Transmission des données à caractère personnel à un tiers

29. Transmission de données à caractère personnel précisément encadrée. Le livre VII du Code de droit économique encadre précisément les traitements à l'occasion desquels des données à caractère personnel du consommateur (ou de la personne qui constitue une sûreté) sont transmises, par le responsable du traitement, à des tiers.

Pour le crédit à la consommation[166], l'article VII.116 du Code de droit économique impose en effet que les conditions cumulatives de la sous-section 1re soient respectées. Ces conditions ont trait aux destinataires autorisés, aux finalités poursuivies et aux données traitées. Il s'agit d'une restriction par rapport au R.G.P.D.[167].

Une distinction doit ainsi être faite entre la base de données *externes* (susceptibles d'être communiquées à d'autres personnes), pour laquelle les traitements sont limités, spécialement en ce qui concerne la transmission aux tiers, et la base de données *interne*, pour laquelle le responsable du traitement retrouve sa liberté, dans le respect du R.G.P.D. et d'autres obligations sectorielles spécifiques.

30. Tiers susceptibles de recevoir une communication des données. Le R.G.P.D. ne limite pas *a priori* les personnes auxquelles des données à caractère personnel peuvent être transmises par le responsable du traitement. Tout au plus peut-on relever une obligation d'information dans le chef de ce dernier, sur les destinataires ou les catégories de destinataires des données à caractère personnel[168].

Le livre VII du Code de droit économique est, sur ce point également, plus restrictif, puisque seules les catégories de personnes énumérées à l'article VII.119, § 1er, du Code de droit économique peuvent se voir communiquer des données[169]. Dans la liste, on trouve notamment les prêteurs (1°), les assureurs-crédits (2°), la F.S.M.A. et la B.N.B. (3°), les avocats (6°) ou les

166 Pour le crédit hypothécaire, voy. art. VII.147/32 C.D.E.

167 Suivant le Code annoté du S.P.F. Économie, cette restriction est justifiée à l'aune de l'article 6, § 3, du R.G.P.D. (S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees/transmission-des-donnees-collectees-pour-un-credit-2/vii-116-vii-147-32-prohibition-de-la-transmission-des-donnees).

168 Art. 13, § 1er, e), et 14, § 1er, e), R.G.P.D.

169 Voy. art. VII.147/35 C.D.E. pour le crédit hypothécaire.

médiateurs de dettes (7°), dans le cadre de leurs missions respectives. Le même principe s'applique, logiquement, en cas de communication ultérieure des données[170].

Dans l'hypothèse d'un contrat de crédit couvert par une assurance-crédit, le prêteur doit nécessairement transmettre certaines informations à l'assureur, pour lui permettre d'évaluer le risque (et de décider s'il accepte de le couvrir). Ultérieurement, si le consommateur fait défaut, et qu'une procédure de recouvrement doit être menée par l'assureur à son encontre, diverses informations devront nécessairement lui être transmises. Il en va de même si un médiateur de dette est appelé à intervenir. Ces hypothèses sont clairement couvertes – et autorisées – par les articles VII.116 et suivants du Code de droit économique[171].

Par contre – et c'est probablement la limite la plus importante en pratique –, les intermédiaires de crédit ne figurent pas dans la liste et ne peuvent donc pas recevoir communication des données en qualité de « tiers ».

31. Finalités. Conformément à l'article 5, § 1er, b), du R.G.P.D., les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ». Dans le respect de cette exigence (et des autres obligations du règlement, notamment en matière de licéité), le responsable du traitement est libre de déterminer les finalités poursuivies et qui peuvent inclure le marketing ou la publicité.

L'article VII.117, § 1er, du Code de droit économique déroge à cette règle, en matière de crédit à la consommation[172]. Aux termes de cette disposition, « les données à caractère personnel ne peuvent faire l'objet d'un traitement que dans le cadre de la double finalité suivante : 1° afin d'apprécier la situation financière et d'évaluer la solvabilité du consommateur ou de la personne qui constitue une sûreté ; 2° dans le cadre de l'octroi ou de la gestion des crédits ou de services de paiement visés par le présent livre susceptibles de grever le patrimoine privé d'une personne physique et dont l'exécution peut être poursuivie sur le patrimoine privé de cette personne.

En aucun cas, les données personnelles ne peuvent être utilisées à des fins de prospections commerciales ».

Il est important d'insister sur le fait que les traitements pour des finalités de marketing sont expressément interdits par cette disposition.

On rappelle que cette limitation des finalités ne vaut que pour les traitements dans le cadre desquels les données sont transmises à des tiers. En l'absence d'une telle transmission, les traitements par des prêteurs pour d'autres finalités restent possibles (pour autant, cela va de soi, que les autres obligations du R.G.P.D. soient observées).

32. Données susceptibles d'être traitées. Les données susceptibles de faire l'objet d'une transmission à un tiers sont également listées de manière limitative par l'article VII.118, § 1er, du Code de droit économique[173]. Elles sont relatives « à l'identité du consommateur ou de la personne qui constitue une sûreté, le montant et la durée des crédits, la périodicité des paiements, les facilités de paiement éventuellement octroyées, les retards de paiement, ainsi que l'identité du prêteur. Cette dernière donnée n'est communiquée qu'au responsable du traitement et au consommateur exclusivement, sauf en ce qui concerne les retards de paiement ».

Le législateur donne délégation au Roi pour déterminer le contenu desdites données. Des précisions peuvent ainsi être trouvées dans l'A.R. du 20 novembre 1992, concernant l'identité du consommateur[174], l'identité du prêteur[175] et le retard de paiement[176].

L'article VII.117, § 2, du Code de droit économique énonce aussi que les données « doivent être pertinentes, appropriées et non excessives au vu des finalités énumérées au paragraphe précédent ». Si les termes diffèrent, on trouve une exigence comparable à l'article 5, § 1er, c), du R.G.P.D., relatif au principe de minimisation des données (« données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »).

2. Enregistrement, communication et consultation des données de la Centrale des crédits aux particuliers

33. Objectif et double volet – négatif et positif. En vue de lutter contre le surendettement des consommateurs et empêcher que ceux-ci contractent des crédits alors qu'ils ont déjà connu des défauts de paiement ou que leur niveau d'endettement est trop élevé (et, partant, leur capacité de remboursement, corrélativement réduite), le législateur a créé une Centrale des crédits aux particuliers, soit une base de données centralisée, gérée par la B.N.B.[177].

Elle est composée d'un volet *positif*, où sont enregistrés les contrats de crédits conclus par les consommateurs (tels que visés par la législation applicable) et d'un volet *négatif*, qui mentionne pendant une période spécifique les défauts de paiements éventuels des consommateurs, en lien avec lesdits contrats[178].

170 Art. VII.119, § 2, C.D.E.

171 Sur la manière dont la demande de renseignement doit être faite, voy. art. VII.119, § 3, C.D.E., qui prévoit notamment, de manière pragmatique, que les demandes peuvent être regroupées, pour plusieurs consommateurs identifiés.

172 Voy. art. VII.147/33 C.D.E. pour le crédit hypothécaire.

173 Voy. art. VII.147/34 C.D.E. pour le crédit hypothécaire.

174 Art. 2 de l'A.R. du 20 novembre 1992.

175 Art. 3 de l'A.R. du 20 novembre 1992.

176 Art. 4 de l'A.R. du 20 novembre 1992.

177 Sur les objectifs de la C.C.P. et l'évolution du cadre normatif en la matière, voy. Th. Léonard et A. Mention, « Crédit à la consommation et protection des données à caractère personnel : un aperçu des règles protectrices », *Handboek consumentenkrediet*, Bruges, la Charte, 2007, pp. 456 et s.

178 Voy. art. VII.148 C.D.E.

De manière générale, la C.C.P. poursuit donc un objectif de transparence ; il est cependant encadré de manière très stricte, pour limiter strictement l'accès aux données enregistrées et empêcher qu'elles soient utilisées à d'autres fins que la lutte contre le surendettement des consommateurs (à des fins de marketing, notamment).

Les règles applicables à la Centrale des crédits aux particuliers – qu'il s'agisse d'un crédit à la consommation ou hypothécaire – figurent aux articles VII.148 et suivants du Code de droit économique[179]. Le législateur donne également délégation au Roi pour régler certains aspects spécifiques (*cf.* l'A.R. du 23 mars 2017).

34. Données enregistrées dans la C.C.P. L'article VII.149, § 2, du Code de droit économique énumère les données enregistrées dans la C.C.P. : « 1° l'identité du consommateur, du prêteur et, le cas échéant, du cessionnaire et la personne qui constitue une sûreté ; 2° les références du contrat de crédit ; 3° le type de crédit ; 4° les caractéristiques du contrat de crédit qui permettent de déterminer la situation débitrice du contrat et son évolution ; 5° le cas échéant, le motif du défaut de paiement communiqué par le consommateur ; 6° le cas échéant, les facilités de paiement accordées au consommateur ».

L'A.R. du 23 mars 2017 énumère de manière plus détaillée les données figurant dans le volet positif (art. 2 et s.) ou dans le volet négatif (art. 5 et s.), ainsi que les circonstances de nature à déclencher l'obligation de communication. S'agissant du volet négatif, c'est par exemple le cas, pour une ouverture de crédit, lorsque le « montant en capital et/ou du coût total du crédit pour le consommateur vient à échéance conformément aux conditions du contrat de crédit et n'a pas été remboursé ou l'a été incomplètement dans un délai de trois mois »[180]. Encore faut-il que le défaut de paiement porte sur une somme supérieure à 50 euros (ce montant minimal étant uniquement d'application lors du premier enregistrement d'un défaut de paiement)[181]. Le consommateur est par ailleurs informé, par la B.N.B., de l'enregistrement dont il est l'objet dans le volet négatif, et des droits qui sont les siens dans ce cadre (notamment le droit d'accès, de rectification et de suppression des données)[182].

La durée de conservation, dans le volet positif[183] ou négatif[184], est précisément indiquée. À l'issue de ces périodes, les données sont normalement[185] supprimées. Ces délais sont importants pour le consommateur, et potentiellement

179 Pour une présentation de ces exigences, voy. aussi Autorité de protection des données, « Les droits des personnes fichées à la Centrale des crédits aux particuliers de la Banque nationale », 1er juillet 2018, disponible sur www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_cr%C3%A9dit_2018.pdf.

180 Art. 5, § 1er, 2°, a), de l'A.R. du 23 mars 2017.

181 Art. 5, § 2, de l'A.R. du 23 mars 2017.

182 Art. VII.151 C.D.E.

183 Art. 4 de l'A.R. du 23 mars 2017.

184 Art. 8 de l'A.R. du 23 mars 2017.

185 Voy. toutefois l'article 8, § 3, de l'A.R. du 23 mars 2017 (« en vue du traitement pour les finalités visées à l'article VII.153, § 4, CDE, la Banque peut conserver ces données pour une durée plus longue après

lourds de conséquences : aussi longtemps qu'il reste « fiché » dans le volet négatif de la C.C.P., il lui sera quasi-impossible de contracter un nouveau crédit[186]. Le délai est ainsi de douze mois à partir de la date de la régularisation (ou dix ans maximum à partir de la date du premier défaut de paiement, avec ou sans régularisation).

35. Communication des informations à la C.C.P. L'efficacité du mécanisme mis en place repose sur la communication systématique des données relatives aux contrats de crédit (volet positif) et aux défauts de paiement (volet négatif).

L'obligation incombe aux prêteurs, ainsi qu'aux personnes désignées par le Roi[187]. L'article 9 de l'A.R. du 23 mars 2017 mentionne notamment les assureurs-crédits « à qui les droits découlant du contrat de crédit ont été cédés ou acquis en totalité ou en partie » ou les personnes exerçant une activité de recouvrement amiable de dettes.

Il importe également que la communication se fasse rapidement, pour donner aux prêteurs un tableau aussi actuel que possible de la solvabilité du consommateur. S'agissant du volet positif, le délai de communication est de deux jours ouvrables après la conclusion du contrat[188]. Il est porté à huit jours ouvrables pour les défauts de paiement ou les régularisations à enregistrer dans le volet négatif.

36. Consultation des données de la C.C.P. L'article VII.153, § 1er, du C.D.E. énumère de manière limitative les personnes auxquelles les données figurant dans la C.C.P. peuvent être communiquées par la B.N.B. Il s'agit principalement des personnes visées à l'article VII.119 ou VII.147/35 du Code de droit économique (*supra*, n° 30), le cas échéant en imposant des conditions complémentaires. Les centrales de crédit étrangères sont également mentionnées. Une transmission à tout autre tiers sera sanctionnée par les autorités compétentes. Le Code annoté du S.P.F. Économie cite ainsi un arrêt inédit de la cour d'appel de Bruxelles, rendu le 26 juin 2007, qui confirme la mesure infligée par le S.P.F. Économie à un prêteur qui avait transmis les résultats de la consultation de la C.C.P. à un autre prêteur du même groupe, mais qui ne disposait pas de l'agrément requis[189].

codage en ce qui concerne les données à caractère personnel »). Une règle similaire est prévue pour les données figurant dans le volet positif (art. 4, § 3, de l'A.R. du 23 mars 2017).

186 Art. VII.77, § 2, C.D.E. (crédit à la consommation) et art. VII.133, § 2, C.D.E. (crédit hypothécaire).

187 Art. VII.148, § 2, C.D.E. Voy. aussi Liège, 9 septembre 2003, *J.L.M.B.*, 2003, p. 1222, qui décide que « contrairement à ce que soutiennent les intimés, la communication des défauts de paiement ne constitue pas pour le prêteur une faculté mais une obligation ».

188 Art. 3 de l'A.R. du 23 mars 2017.

189 S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees/transmission-des-donnees-collectees-pour-un-credit-2/vii-119-vii-147-35-tiers-autorises#exemple-jurisprudence-et-avis-de-l-administration.

S'agissant des prêteurs, la consultation de la C.C.P. est une obligation légale dans le cadre de l'octroi d'un crédit à la consommation ou hypothécaire : aux termes de l'article VII.149, § 1er, du C.D.E., « afin d'obtenir des informations sur la situation financière et la solvabilité aussi bien du consommateur que de la personne qui constitue une sûreté personnelle, les prêteurs consultent la Centrale préalablement à la conclusion d'un contrat de crédit, à l'exception d'un dépassement, ou à la remise de l'offre de crédit visés aux articles VII.127, § 3, et VII.133 »[190]. Ils doivent également conserver la preuve du respect de cette obligation, de manière à la produire, le cas échéant, aux autorités compétentes[191]. Le non-respect de l'obligation de consultation fait l'objet de sanctions civiles[192] et pénales[193] spécifiques.

Les modalités de la consultation sont par ailleurs fixées par l'A.R. du 23 mars 2017 (et notamment les délais dans lesquels ladite consultation doit être réalisée[194]). On peut d'ailleurs regretter que soit seule visée la consultation de la C.C.P. par les prêteurs. En pratique, il paraît impossible aux autres personnes visées à l'article VII.153, § 1er, du C.D.E. d'accéder directement aux données figurant dans la C.C.P. Cette circonstance paraît particulièrement contestable, en tout cas pour les assureurs-crédits, auxquels l'information est manifestement utile au moment d'apprécier le risque de couverture (et que la loi autorise par ailleurs à fournir diverses informations aux intermédiaires de crédit – *infra*, n° 37).

Certaines données ne sont pas communiquées dans la réponse. Pour des motifs de saine concurrence sur le marché, l'article 12 de l'A.R. du 23 mars 2017 exclut ainsi le « nom du prêteur, du cessionnaire, du numéro et de la langue du contrat de crédit ». Cette disposition ajoute que « la Centrale est autorisée à fournir une réponse synthétique établie sur [la] base de tout ou partie des renseignements enregistrés. Si la consultation porte sur une personne non enregistrée dans la Centrale, il en est fait mention dans la réponse ».

Les finalités des traitements susceptibles d'être opérés sur les données sont par ailleurs limitées : les renseignements ne peuvent en effet être utilisés que « dans le cadre de l'octroi ou de la gestion de crédits ou de services de paiement, susceptibles de grever le patrimoine privé d'une personne physique et dont l'exécution peut être poursuivie sur le patrimoine privé de cette personne », et à l'exclusion de toute prospection commerciale[195]. Le cas échéant, un détournement des seules finalités pour lesquelles les données de la C.C.P. peuvent être traitées sera sévèrement sanctionné. Le Code annoté du S.P.F. Économie donne

190 Voy. également art. VII.77, § 2, C.D.E. (crédit à la consommation) et art. VII.133, § 2, C.D.E. (crédit hypothécaire).

191 Voy. J.P. Courtrai, 2 juillet 2013, *Ann. jur. crédit*, 2013, p. 40, qui sanctionne le prêteur qui n'apporte pas la preuve du respect de son obligation de consultation (conformément à l'article VII.201, 1°, du C.D.E.).

192 Art. VII.195, al. 2, C.D.E.

193 Art. XV.88 C.D.E. (sanction de niveau 4).

194 Art. 10 de l'A.R. du 23 mars 2017.

195 Art. VII.153, § 2, C.D.E.

ainsi l'exemple d'un procès-verbal de constat rédigé par l'inspection économique, concernant un prêteur, ayant également la qualité d'intermédiaire de crédit, qui interrogeait la C.C.P. pour utiliser les informations obtenues dans le cadre de cette dernière activité, de manière à proposer aux consommateurs de regrouper leurs crédits[196].

La loi impose également aux personnes ayant obtenu ces renseignements de prendre les mesures nécessaires en vue de garantir leur confidentialité[197].

La personne concernée – autrement dit, le consommateur ou la personne qui constitue une sûreté – peut également consulter les données. Sur ce point, le R.G.P.D. est par ailleurs applicable, et spécialement les articles 12 et suivants relatifs aux droits de la personne concernée[198]. L'article VII.152 du C.D.E. précise que cet accès aux données est libre et sans frais. La personne concernée peut également postuler la rectification des données erronées. Dans ce cas, suivant l'article VII.152, alinéas 2 et 3, la B.N.B. « est tenue de la transmettre à la personne visée à l'article VII.149, alinéas 1er et 3, qui a communiqué les données et qui est responsable du contenu exact. Le cas échéant, cette personne demande à la Centrale la correction des données enregistrées. En cas de rectification, la Banque est tenue de communiquer cette rectification aux personnes qui ont obtenu des renseignements de la Centrale et que la personne enregistrée indique ». La personne concernée doit justifier de son identité, étant entendu qu'un mandat peut, le cas échéant, être donné à un tiers (pour autant qu'il ne s'agisse pas d'un intermédiaire de crédit)[199]. Si la personne concernée n'est pas satisfaite des suites données à sa demande d'accès, de rectification ou de suppression, plusieurs mesures peuvent être prises, notamment auprès de l'Autorité de protection des données[200].

37. Communication des données de la C.C.P. aux intermédiaires de crédit ? Les intermédiaires de crédit, comme les courtiers, ne peuvent pas accéder aux données de la C.C.P.[201]. Ils ne figurent pas dans la liste des per-

196 S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees/centrale-des-credits-aux-particuliers.

197 Art. VII.153, § 3, C.D.E.

198 On peut observer que ni le droit à la limitation du traitement, ni le droit d'opposition ne sont expressément mentionnés, comme le relève le Code annoté, qui justifie cette restriction sur le pied de l'article 23 du R.G.P.D. pour garantir des objectifs importants d'intérêt public (S.P.F. Économie, *Code annoté des crédits aux consommateurs*, 10 mars 2019, https://credit2consumer.be/fr/traitement-des-donnees/centrale-des-credits-aux-particuliers).

199 Sur la conformité des dispositions avec le régime prévu par le R.G.P.D. pour le droit d'accès, voy. le Rapport au Roi précédant l'A.R. du 23 mars 2017.

200 Autorité de protection des données, « Les droits des personnes fichées à la Centrale des crédits aux particuliers de la Banque nationale », 1er juillet 2018, disponible sur www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_cr%C3%A9dit_2018.pdf.

201 Sur l'interdiction, pour les intermédiaires de crédit, de consulter la C.C.P., voy. F. DOMONT-NAERT, « Le crédit à la consommation », *Guide juridique de l'entreprise*, Kluwer, 2004, liv. 113.1, n° 160 ; *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1730/001, p. 41 : « la responsabilité de l'intermédiaire de crédit est ainsi clairement affirmée ; elle est fatalement moins large que celle du prêteur, lequel dispose d'autres sources

sonnes auxquelles les données peuvent être communiquées par la B.N.B.[202]. Le législateur craint en effet que ces informations soient utilement exploitées par les intermédiaires à des fins de marketing, pour encourager les consommateurs à regrouper leurs crédits ou à les refinancer à des taux préférentiels, créant ainsi un risque de surendettement dans leur chef.

La question se pose néanmoins de savoir si certaines données, tirées de la consultation de la C.C.P. par les personnes habilitées, pourraient leur être transmises.

Désormais, la réponse est positive, dans les limites strictement fixées par la loi.

Dans sa version en vigueur au 1er décembre 2016, l'article VII.153, § 2, alinéa 3, du Code de droit économique énonce en effet que « les personnes visées à l'article VII.119, § 1er, alinéa 1er, 1° et 2° [*autrement dit, les prêteurs et les assureurs-crédit*], sont, le cas échéant et sous leur responsabilité, autorisées d'informer l'intermédiaire de crédit de la réponse globalisée à la consultation dans la mesure où la consultation a eu lieu sur la base d'une demande de crédit concrète pour laquelle l'intermédiaire de crédit a posé des actes d'intermédiation de crédit. Cette réponse globalisée ne peut avoir trait que sur le nombre des contrats de crédit, la somme des montants de crédit enregistrés et, en cas de refus du crédit en vertu de l'article VII.77, § 2, alinéa 2, la mention que le refus est basé sur l'application de cette disposition. L'intermédiaire de crédit ne peut utiliser ces données qu'en vue du respect de ses obligations visées aux articles VII.69 à VII.71, VII.74 et VII.75. Une fois que le dossier de crédit a été clôturé par le prêteur, la réponse globalisée n'est plus disponible ».

Certaines informations tirées de la C.C.P. pourraient donc être communiquées à l'intermédiaire de crédit (le courtier, par exemple).

Cette possibilité a été ajoutée en 2014, lors de l'introduction des dispositions de la loi du 12 juin 1991 sur le crédit à la consommation dans le Code de droit économique[203]. Jusqu'au 1er décembre 2016, les informations susceptibles d'être fournies étaient toutefois plus limitées, notamment pour éviter que l'intermédiaire utilise cette information pour inciter le consommateur à regrouper ses crédits[204]. Le législateur voulait toutefois permettre à l'intermédiaire de disposer de davantage de données pour évaluer la solvabilité du débiteur

d'information, en particulier la consultation de la banque centrale de données de la Banque nationale de Belgique ».

202 Art. VII.153, § 1er, C.D.E., qui renvoie aux articles VII.119, § 1er, et VII.147/35 du C.D.E.

203 Loi du 19 avril 2014 portant insertion du livre VII « Services de paiement et de crédit » dans le Code de droit économique, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres Ier et XV du Code de droit économique, et portant diverses autres dispositions, *M.B.*, 28 mai 2014.

204 Voy., en ce sens, les travaux préparatoires de la loi : *Doc. parl.*, Ch. repr., sess. ord. 2013-2014, nos 53-3429/001 et 53-3430/001, p. 33.

(pour prévenir la pratique, illicite[205], consistant à demander au consommateur de consulter lui-même la C.C.P.).

La loi du 22 avril 2016 a complété la liste des informations susceptibles d'être fournies à l'intermédiaire. Dans la version antérieure de l'article VII.153, le prêteur ne pouvait pas informer l'intermédiaire sur le fait qu'en cas de refus du crédit, ce refus était basé sur le résultat de la consultation de la C.C.P. L'intermédiaire pouvait juste indiquer au consommateur que son dossier était refusé, sans autre explication (en l'enjoignant, le cas échéant, à consulter le prêteur, s'il souhaitait obtenir davantage d'informations). Or, comme le notent les travaux préparatoires, « cela peut avoir pour conséquence que tant le candidat-emprunteur que les intermédiaires concernés sont amenés à consentir des frais et des efforts inutiles qu'ils auraient pu s'épargner si, en cas de refus, une explication correcte avait pu être donnée au consommateur par l'intermédiaire de crédit. Une adaptation de la possibilité actuelle trop limitée pour le prêteur d'informer l'intermédiaire de crédit des résultats de la consultation de la C.C.P. par le prêteur s'impose donc. Cette consultation est sans préjudice des obligations dans le chef du prêteur en vertu de l'article VII.79 »[206]. L'article VII.153, § 2, du C.D.E. a ainsi été amendé et, depuis le 1er décembre 2016, l'intermédiaire peut également être informé du motif de refus du dossier résultant de la consultation de la C.C.P.

3. Autres questions réglées par le livre VII en matière de traitements de données

38. Base de licéité du traitement. L'article 6 du R.G.P.D. liste les bases de licéité des traitements de données à caractère personnel.

En l'occurrence, le prêteur peut en tout cas se prévaloir de la nécessité de se conformer à une obligation légale à laquelle il est soumis : en effet, aux termes de l'article VII.69 du Code de droit économique[207], les prêteurs doivent obligatoirement demander divers renseignements aux consommateurs qui sollicitent un crédit en vue d'évaluer leur solvabilité. On observe que plusieurs catégories de renseignement – ressortissant aux données particulières visées à l'article 9 du R.G.P.D. – ne peuvent pas être sollicitées dans ce cadre[208].

Le cas échéant, pour effectuer des traitements plus accessoires, notamment à des fins de marketing, une autre base de licéité devra être trouvée.

205 Art. VII.153, § 2, al. 4, C.D.E.

206 *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1685/001, p. 56.

207 Voy. art. VII.126 C.D.E. pour le crédit hypothécaire.

208 Art. VII.69, § 1er, al. 2, C.D.E., qui cite « la race, l'origine ethnique, la vie sexuelle, la santé, les opinions ou activités politiques, philosophiques ou religieuses ou l'appartenance syndicale ou mutualiste ».

39. Conservation des données. Le principe de « limitation de la conservation » est énoncé à l'article 5, § 1er, e), du R.G.P.D. Sauf exception[209], les données ne peuvent pas être conservées pour une durée supérieure à celle qui est nécessaire au regard des finalités du traitement. La personne concernée doit par ailleurs être informée de la durée de conservation des données ou, en tout cas, du critère utilisé pour la calculer (un délai de prescription, par exemple), pour autant que l'information soit nécessaire « pour garantir un traitement équitable et transparent »[210].

Le principe est également énoncé à l'article VII.120, § 1er, du C.D.E., qui donne délégation au Roi pour fixer les délais de conservation des données. Ceux-ci sont établis à l'article 5 de l'A.R. du 20 novembre 1992. En l'absence de facilités de paiement, les données doivent être effacées par le responsable du traitement quinze jours après l'extinction des obligations ou l'expiration du contrat de crédit. Si des facilités de paiement ont été octroyées, les données sont effacées un an après l'extinction des obligations ou l'expiration du contrat de crédit. En cas de retard de paiement, il est prévu que les données sont supprimées « 1° douze mois à partir de la date de régularisation du contrat de crédit ; 2° maximum dix ans à partir de la date du premier enregistrement d'un retard de paiement, que le contrat de crédit ait été ou non régularisé ».

L'article VII.120, § 2, du Code de droit économique ajoute que « le responsable du traitement est tenu de prendre toutes les mesures qui permettent de garantir la parfaite conservation des données à caractère personnel ». Vu la généralité des termes employés, la disposition n'apporte guère de précision (ou de restriction éventuelle) par rapport au R.G.P.D.

40. Droits de la personne concernée. De manière surabondante (et inutile), l'article VII.122, § 1er, du Code de droit économique énonce que « à l'égard des données enregistrées dans un fichier concernant sa personne ou son patrimoine, tout consommateur ou personne qui constitue une sûreté peut exercer les droits mentionnés aux articles 10 et 12 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ». Une précision est ajoutée concernant le droit de rectification : il incombe en effet au responsable du traitement d'informer les personnes auxquelles elle a communiqué des renseignements sur la personne concernée de les informer de cette rectification. La loi ajoute cependant que la personne enregistrée doit indiquer qui sont ces personnes.

209 Par exception, conformément à l'article 5, § 1er, e), du R.G.P.D., « les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée ».

210 Art. 13, § 2, a), et 14, § 2, a), R.G.P.D.

Section 3

Focus sur certaines questions spécifiques posées par le *big data* et l'intelligence artificielle

A. Contexte et enjeux principaux

41. Le phénomène du *big data*, en évolution constante. Avec l'utilisation croissante des technologies de l'information et de la communication, une quantité croissante de données sont produites, échangées, conservées et... exploitées, par les pouvoirs publics ou les entreprises, notamment à des fins économiques et commerciales.

Elles peuvent être fournies par les utilisateurs eux-mêmes ou les entreprises, volontairement ou pas, sciemment ou pas, à travers les réseaux sociaux, les sites internet transactionnels ou de partage de contenus, les jeux en ligne, etc. En réalité, toute trace laissée à l'occasion d'une activité sur l'internet ou à travers une application dédiée, sur son appareil mobile, constitue une donnée : l'historique de navigation, les pages visitées sur le site d'un marchand ou une simple recherche dans Google peuvent ainsi fournir des informations intéressantes dans le cadre du *big data*.

Une quantité exponentielle de données, structurées ou non, à caractère personnel ou pas, sont ainsi à la disposition des entreprises ou des autorités publiques. On parle de « *big data* » ou, en français, de « données massives » ou de « mégadonnées »[211] [212].

Le phénomène est rendu possible grâce aux capacités de stockage en augmentation constante, notamment dans le *cloud*, et aux infrastructures techniques permettant d'échanger les données rapidement et en grand volume. L'existence de données publiques – *open data* – mises à la disposition de tous est une autre explication du succès des *big data*.

211 Pour une description du phénomène et de ses principales caractéristiques, voy. V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data – La révolution des données est en marche*, Paris, Robert Laffont, 2014 ; A. LATREILLE et C. ZOLYNSKY, « Séance 4 : nouvelles pratiques : faut-il de nouvelles protections ? », *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Tiens Europe Expert*, Paris, Société de législation comparée, 2014, pp. 262 et s. ; M. MAIRLOT, « Big Data et vie privée : mariage possible ? », *D.B.F.*, 2015/VI, p. 446 ; A. GROSJEAN, « Le profilage : un défi pour la protection des données à caractère personnel », *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, nos 17 et s. ; P. DE FILIPPI, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, pp. 99 et s. ; E. LUTS, « Big data in de financiële sector », *Rev. banc. fin.*, 2016/2, pp. 123 et s. ; B. FRENAY, « Démystifier le machine learning », *R.D.T.I.*, 2018/70, pp. 5 et s. Voy. aussi Groupe 29, « Opinion 03/2013 on purpose limitation », 2 avril 2013, WP 203, p. 35 et pp. 45 et s. ; A. ROUVROY, « Des données et des hommes – Droits et libertés fondamentaux dans un monde de données massives », rapport rédigé pour le Conseil de l'Europe, 11 janvier 2016, T-PD-DUR (2015)09REV.

212 Les considérations de la présente section principalement tirées de l'analyse que nous avons rédigée dans H. JACQUEMIN et J.-M. VAN GYSEGHEM, « Le *big data* en matière d'assurance à l'épreuve du R.G.P.D. », *Bull. ass.*, dossier 2017, *Data Protection : l'impact du GDPR en assurances*, pp. 233 à 260.

Ce volume considérable de données ne présente de l'intérêt que s'il est possible de l'analyser efficacement, pour en tirer des enseignements utiles, notamment en termes prédictifs. Comme certains l'indiquent pertinemment, il s'agit de «laisser parler les données»[213]. Précisément, les progrès techniques permettent d'atteindre cet objectif, au moyen d'algorithmes de plus en plus sophistiqués, qui livrent des résultats généraux (en identifiant certaines tendances sur le marché p. ex.), ou plus précis (en procédant, p. ex., au profilage des personnes, de manière à leur appliquer des décisions automatisées). Comme l'a écrit le Contrôleur européen de la protection des données, «l'une des utilisations potentiellement les plus importantes des données massives est de prédire ce qui va probablement se produire, mais ne s'est pas encore produit, et ce que nous allons probablement faire, mais n'avons pas encore fait»[214]. Les progrès de l'intelligence artificielle, qui permet de traiter les données de manière automatisée, voire autonome, sans intervention humaine systématique, sont ainsi étroitement liés au *big data*[215] (voy. *infra*, n° 42).

Pour circonscrire et expliquer le phénomène du *big data*, on fait traditionnellement référence aux trois V[216]. Ils désignent le Volume massif de données – et en croissance exponentielle – à la disposition de certaines entreprises; leur Variété, puisqu'il peut s'agir de données à caractère personnel ou d'autres catégories d'informations, structurées ou pas, et sous des formats divers (texte, image, son, etc.) et la Vitesse à laquelle il est maintenant possible de les collecter et de les traiter, en temps réel dans certains cas. On pourrait y ajouter un V supplémentaire, relatif à la Valeur de ces données[217], spécialement s'il s'agit de données à caractère personnel. Elles constituent d'ailleurs l'un des éléments-clés de notre économie numérique, au point que l'on peut parler d'«économie de la donnée».

Dans le domaine financier, comme dans de nombreux secteurs d'activités, les entreprises sont soucieuses de tirer le meilleur parti des données à leur disposition. Nombre d'entre elles disposent déjà, en interne, d'un volume important de données, qui peut leur être utile moyennant l'application d'algorithmes correctement configurés. Elles sont en outre intéressées d'enrichir cette base de données, à l'aide de données disponibles librement et publiquement, de données acquises auprès de tiers, ou d'objets connectés utilisés par les personnes concernées.

213 V. Mayer-Schönberger et K. Cukier, *Big Data – La révolution des données est en marche*, Paris, Robert Laffont, 2014, pp. 14 et s.; A. Latreille et C. Zolynsky, «Séance 4: nouvelles pratiques: faut-il de nouvelles protections?», *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, *op. cit.*, p. 265.

214 E.D.P.S., «Relever les défis des données massives», avis n° 7/2015, 19 novembre 2015, p. 9.

215 Voy., à ce sujet, A. Rouvroy, «La robotisation de la vie ou la tentation de l'inséparation», *in* H. Jacquemin et A. de Streel (coord.), *L'intelligence artificielle et le droit*, coll. CRIDS, n° 41, Bruxelles, Larcier, 2017, pp. 22 et s.

216 P. De Filippi, «Gouvernance algorithmique: vie privée et autonomie individuelle à l'ère des Big Data», *Open Data & Big Data – Nouveaux défis pour la vie privée*, *op. cit.*, pp. 99 et s.; A. Latreille et C. Zolynsky, «Séance 4: nouvelles pratiques: faut-il de nouvelles protections?», *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de législation comparée, 2014, p. 263; C. Brion, H. Waem et Y. Hendricks, «The Big Cloud of Things is watching you: le droit de la vie privée et l'internet des objets», *in* J.-A. Delcorde (dir.), *La révolution digitale et les start-ups*, Bruxelles, Larcier, 2016, pp. 233 et 234.

217 A. Latreille et C. Zolynsky, «Séance 4: nouvelles pratiques: faut-il de nouvelles protections?», *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, *op. cit.*, p. 263.

D'un point de vue marketing, on comprend sans peine l'opportunité d'anticiper, en termes prédictifs, les attentes du marché pour proposer rapidement – et si possible avant les concurrents – des produits qui répondent adéquatement aux besoins des prospects ou des clients. De même, en combinant les informations recueillies au moyen de *cookies* installés sur les terminaux des consommateurs, avec d'autres informations les concernant, des publicités ciblées et personnalisées peuvent leur être envoyées.

Le secteur du crédit est également intéressé d'évaluer la solvabilité des emprunteurs potentiels en se fondant sur les données dont les prêteurs disposent déjà, de préférence enrichies d'informations complémentaires tirées du *big data*.

Des algorithmes (plus ou moins) sophistiqués peuvent également faciliter l'identification des fraudes commises, notamment dans le secteur des paiements en ligne.

En définitive, les potentialités offertes par le *big data* sont extrêmement nombreuses, et devraient d'ailleurs se multiplier à l'avenir, à mesure que la masse de données augmente, ainsi que l'efficacité d'algorithmes chargés de les «faire parler».

Si le *big data* présente des avantages indéniables, à titre individuel et collectif, ils peuvent être éclipsés par les risques corrélatifs. On peut craindre en effet que des choix biaisés, discriminatoires, illégitimes ou injustes soient faits sur la base des données analysées. Le risque existe également d'un certain conformisme, auquel les personnes pourraient être tentées de se soumettre, pour être en phase avec les critères dégagés d'une analyse *big data* (correspondant par exemple à ce que fait le plus grand nombre et qu'un algorithme a désigné comme étant la norme à suivre) et, ainsi, bénéficier de conditions tarifaires plus réduites[218]. Ce faisant, on brise les velléités d'innovation ou de choix différents, guidés par la liberté individuelle et le libre arbitre, qui pourraient pourtant être source de progrès. De manière plus générale, le *big data* pose d'évidentes questions de nature philosophique ou éthique, puisqu'on accepte désormais d'être gouverné

218 Voy. en ce sens E.D.P.S., «Relever les défis des données massives», avis n° 7/2015, 19 novembre 2015, p. 10: «la nécessité d'obtenir un prêt ou une couverture d'assurance pourrait pousser ou contraindre des individus à éviter le contact avec certaines personnes ou entreprises ou à visiter des quartiers ou les taux de criminalité sont élevés de la même manière que des personnes sont incitées à installer des "boîtes noires" qui permettent à un responsable du traitement externe de les contrôler pendant qu'elles conduisent».

par les données et les algorithmes chargés de leur donner sens. Dans la présente contribution, il nous est malheureusement difficile de développer ce point.

42. Intelligence artificielle. Dans le secteur financier, comme dans d'autres domaines (justice, santé, marketing, etc.), les entreprises ou les autorités publiques cherchent à automatiser les procédures en se fondant sur des algorithmes, plus ou moins sophistiqués. Des applications d'intelligence artificielle sont ainsi mobilisées, pour fournir des informations aux consommateurs (au moyen de *chatbot*), pour les conseiller (*robo-advisors*) ou pour évaluer leur solvabilité sans intervention humaine (avec un outil de *credit scoring* p. ex.)[219].

En l'absence de définition légale de l'intelligence artificielle ou du robot[220], en droit de l'Union[221] ou en droit belge, on peut opter pour une acception volontairement large, qui met l'accent sur les fonctions attendues du procédé[222]. L'application d'intelligence artificielle intervient de manière automatisée, voire autonome, en ce sens qu'elle est capable d'adopter un comportement déterminé, sans intervention humaine systématique lors de chaque action posée. Ce comportement est le résultat des opérations algorithmiques ou de toute autre instruction logicielle, tenant compte de l'analyse des données dont le système dispose, qu'il reçoit (dès lors qu'il est connecté) ou qu'il tire de son environnement (au moyen de capteurs, par exemple). Le système peut être doté d'une

219 Sur le recours à l'I.A. dans le secteur financier, voy. C. Houssa, P. De Prez et L. Standaert, « La finance digitale #robotisation », *in* H. Jacquemin et A. de Streel (coord.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, pp. 357 et s.

220 Dans le langage courant, le terme « robot » désigne généralement l'enveloppe physique et matérielle, capable de se mouvoir dans l'espace et d'interagir avec son environnement grâce au système d'intelligence artificielle, plus ou moins développé, dont il est muni. Il peut revêtir des apparences diverses, le cas échéant proches de celles de l'être humain.

221 Dans sa résolution du 16 février 2017, le Parlement encourage toutefois la Commission à intervenir en ce sens (Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, 2015/2103 [I.N.L.], pt 1).

222 R. Calo, « Robots in American Law », *Legal Studies Research Paper*, n° 2016-04, pp. 6 et s., et R. Calo, « Robotics and the Lessons of Cyberlaw », *California Law Review*, 2015, pp. 529 et s. (« *(1) a robot can sense its environment, (2) a robot has the capacity to process the information it senses, and (3) a robot is organized to act directly upon its environment* », renvoyant au paradigme « *sense, think, act* »). Voy. aussi *Artificial Intelligence and Life in 2030, One hundred Year Study on Artificial Intelligence*, Report of the 2015 Study Panel – Stanford University, Septembre 2016, pp. 18 et s. (https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf), p. 12, qui reprend notamment la définition de N.J. Nilsson, *The Quest of Artificial Intelligence : A History of Ideas and Achievements*, Cambridge, Cambridge University Press, 2010: « *Artificial Intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment* » ; Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, 2015/2103 (I.N.L.), principe 1, qui pointe les caractéristiques suivantes des robots intelligents : « acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données avec l'environnement (interconnectivité) et à l'échange et l'analyse de ces données ; capacité d'autoapprentissage à travers l'expérience et les interactions (critère facultatif), existence d'une enveloppe physique, même réduite ; capacité d'adaptation de son comportement et de ses actes à son environnement ; non vivant au sens biologique du terme » ; Ch. Holder, V. Khurana, F. Harisson et L. Jacobs, « Robotics and law : Key legal and regulatory implications of the robotics age (Part I of II) », *Computer Law and Security Review*, 2016, pp. 384 et 385.

faculté d'autoapprentissage (de type *machine learning*), qui lui permet, sur la base de son expérience, d'apprendre et de changer son comportement en conséquence[223]. Concrètement, cela signifie que les actions posées par le système ne découleront pas d'une instruction spécifique donnée en ce sens par l'homme, mais seront le résultat d'opérations algorithmiques effectuées par celui-ci, qui lui permettent de résoudre, de manière autonome, des problèmes complexes et d'effectuer des prédictions.

B. Focus sur certaines questions en matière de protection des données

43. Enjeux en matière de protection des données. Sur le plan strictement juridique, les questions posées par le *big data* et l'intelligence artificielle sont également nombreuses, en particulier lorsque des données à caractère personnel sont concernées (ce qui sera souvent le cas). Les traitements réalisés – potentiellement automatisés avec l'I.A. – pourraient en effet porter atteinte à la vie privée des individus[224].

Faut-il pour autant abandonner tout projet de *big data* susceptible d'être mené dans le secteur du crédit ou des paiements ? Nous ne le croyons pas. Et, manifestement, les entreprises concernées sont du même avis… Une attention particulière devra néanmoins être de mise, pour s'assurer que les principes établis par le R.G.P.D. et les règles sectorielles éventuellement applicables ont été respectés.

En l'occurrence, on se focalise sur le respect de certains principes établis à l'article 5 du R.G.P.D. (*infra*, n°s 44 et s.). Il incombe ainsi à tout responsable du traitement (un prestataire de services de paiement ou un prêteur, par exemple) de s'assurer, au cas par cas et avant de lancer un projet fondé sur des résultats *big data*, que ces principes ont été et seront dûment respectés en l'espèce. Cette démarche préalable et systématique est indispensable. On examine également à quelles conditions il est permis de prendre une décision fondée sur un traitement automatisé, conformément à l'article 22 du R.G.P.D.

D'autres questions sont évidemment pertinentes, telles que l'exercice, par la personne concernée, des droits que lui octroie le R.G.P.D. ou l'identification

223 Voy. H. Surden, « Machine Learning and Law », *Washington Law Review*, 2014, pp. 87 et s.

224 Pointant certains risques du *big data* en termes de vie privée et de traitement des données à caractère personnel, voy. M. Mairlot, « Big Data et vie privée : mariage possible ? », *D.B.F.*, 2015/VI, pp. 448 et s. ; P. De Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée*, *op. cit.*, pp. 104 et s. ; L. Merland, « L'identité civile des personnes : "Is big data beautiful?" », *R.L.D.I.*, 2015/121, pp. 37 et s. ; C. Houssa, P. De Prez et L. Standaert, « La finance digitale #robotisation », *in* H. Jacquemin et A. de Streel (coord.), *L'intelligence artificielle et le droit*, *op. cit.*, pp. 401 et s. ; A. Delforge, « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.*, 2018/70, pp. 15 et s. Voy. aussi Groupe 29, « Opinion 03/2013 on purpose limitation », 2 avril 2013, WP 203, p. 35 et pp. 45 et s. ; E.D.P.S., « Relever les défis des données massives », avis n° 7/2015, 19 novembre 2015, pp. 8 et s.

du rôle joué par chacun des acteurs. Elles ne seront toutefois pas traitées en l'espèce.

Notons encore que, pour échapper aux exigences prescrites par le R.G.P.D., la solution peut consister à anonymiser les données. Encore faut-il que la personne concernée ne soit plus identifiable de manière irréversible, ce qui pourrait faire l'objet de discussions[225]. Dans le contexte du *big data*, où le volume de données susceptible d'être utilisé est particulièrement important, le risque d'une possible (ré-)identification de la personne concernée augmente corrélativement[226]. Aussi sera-t-on très attentif au moment de décider si les données peuvent être considérées comme étant « anonymes » : la qualification est délicate pour les traitements traditionnels, et davantage encore en matière de *big data*[227] ; s'il apparaît ultérieurement que les données ne sont pas anonymes, parce qu'une personne physique peut être identifiée, il faudra gérer *a posteriori* un traitement pour lequel aucune mesure n'a été prise en vue d'en assurer la licéité (aucun consentement préalable n'ayant été obtenu de la personne concernée, par exemple) ce qui exposera très probablement l'entreprise concernée à une lourde sanction de la part des autorités de contrôle.

1. Respect des principes établis à l'article 5 du R.G.P.D.

44. Principe de limitation des finalités. Conformément à l'article 5, § 1er, b), du règlement, les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales ».

225 Le considérant 26 du R.G.P.D. apporte des précisions sur ce point : aux termes de celui-ci, « il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ».

226 C. Brion, H. Waem et Y. Hendricks, « The Big Cloud of Things is watching you : le droit de la vie privée et l'internet des objets », *in* J.-A. Delcorde (dir.), *La révolution digitale et les start-ups*, *op. cit.*, p. 234 : « l'anonymisation ne semble toutefois pas être une véritable solution dans un contexte de big data ».

227 En ce sens, voy. A. Latreille et C. Zolynsky, « Séance 4 : nouvelles pratiques : faut-il de nouvelles protections ? », *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Expert*, *op. cit.*, p. 267 : « la puissance des pratiques "big data" pourrait faire qu'un traitement de données à caractère personnel soit possible alors que, prises isolément, chaque base ne contient pas de données à caractère personnel. Le traitement "big data" peut, par croisement, conduire à des pratiques de ré-identification, notamment par le biais de techniques de zoomage permettant de passer du "big" à la "nano", et ainsi de faire parler ces données non identifiantes à des fins d'identification des personnes. [...] Nombreux considèrent alors, avec les possibilités de croisements et la logique du recoupement du traitement Big Data, que les pratiques d'anonymisation actuelle ne sauraient être efficaces ».

Il s'agit d'un principe fondamental en matière de protection des données : la personne concernée doit savoir à quelle(s) fin(s) ses données sont collectées – et ensuite traitées – par le responsable du traitement. Aussi lui incombe-t-il, par application du principe de transparence, d'informer la personne concernée sur ce point. En pratique, cet élément figurera généralement dans la politique de confidentialité ou tout autre document contractuel fourni à la personne concernée. Il faut par ailleurs s'assurer que celui-ci soit opposable à la personne concernée.

Dans le domaine du *big data*, la question du traitement ultérieur compatible avec les finalités initiales ne manquera pas de se poser. L'objectif est en effet d'exploiter utilement le volume important des données dont on dispose pour en tirer des enseignements sur la personne concernée, à des fins de marketing, pour cerner plus précisément son profil de risque ou pour évaluer sa solvabilité. Or, pour la plupart, ces données n'ont pas forcément été collectées à cette fin. La situation se complique encore sachant que les données ont pu être collectées initialement par un autre responsable du traitement, qui se ménagerait le droit de les communiquer à des tiers (transmission du prêteur à l'assureur-crédit, par exemple).

L'analyse est assurément complexe et, pour faciliter la tâche de l'interprète chargé de le mettre en œuvre, le R.G.P.D. énonce les principes à prendre en considération pour procéder à l'évaluation. Sans que la liste soit limitative, on peut ainsi tenir compte, aux termes de l'article 6, § 4, du règlement, « a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ; b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ; d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ; e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ».

Même si le responsable ne parvient pas à démontrer que le traitement ultérieur est compatible avec les finalités initiales, celui-ci ne sera pas nécessairement interdit. Le règlement confirme en effet clairement – et c'est une nouveauté – qu'un traitement ultérieur pour des finalités incompatibles avec les finalités initiales est permis, moyennant le respect de certaines conditions.

L'article 6, § 4, du R.G.P.D. l'autorise dans deux hypothèses : lorsqu'il est fondé sur « le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, § 1er ». À cet égard, on doit se rappeler que, suivant la proposition

introduite par la Commission en janvier 2012, l'autorisation des traitements ultérieurs incompatibles avec les finalités initiales était admise beaucoup plus largement : l'article 6, § 4, de la proposition indiquait en effet que, « lorsque la finalité du traitement ultérieur n'est pas compatible avec celle pour laquelle les données à caractère personnel ont été collectées le traitement doit trouver sa base juridique au moins dans l'un des motifs mentionnés au paragraphe 1, points a) à e). Ceci s'applique en particulier à toute modification des clauses et des conditions générales d'un contrat ». Plusieurs conditions de licéité – et pas seulement le consentement de la personne concernée – pouvaient donc être invoquées pour autoriser le traitement ultérieur. Dans la proposition de la Commission, seul l'intérêt légitime du responsable du traitement ou d'un tiers ne pouvait pas être invoqué (*cf. littera* f) ; le Conseil avait toutefois proposé de lever cette exclusion en autorisant une telle base de légitimation. Ce faisant, les opérations de *big data* auraient été facilitées (c'était d'ailleurs l'objectif poursuivi), mais au prix d'un affaiblissement substantiel du principe de finalité[228]. De nombreuses critiques avaient ainsi été émises, notamment par le Groupe 29[229]. Il aurait en effet été possible de corriger l'incompatibilité en identifiant une nouvelle base de légitimation. Ce faisant, on permettait de pallier la méconnaissance du principe de finalité par le respect d'une autre condition. Or, il s'agit de deux conditions distinctes et cumulatives. Le texte avait heureusement été revu pour limiter les hypothèses dans lesquelles les traitements ultérieurs pour des finalités incompatibles avec les finalités initiales sont permis.

On peut également échapper à l'interdiction d'un traitement ultérieur incompatible avec les finalités initiales si ce traitement est réalisé à des fins statistiques. Des garanties appropriées doivent toutefois être prévues. L'article 89, § 1er, du R.G.P.D. impose ainsi la mise en place de « mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière ».

45. Principe de minimisation des données. Le principe de minimisation des données est consacré à l'article 5, § 1er, c), du règlement aux termes duquel 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 ». Cette exigence de proportionnalité figurait déjà dans la directive 95/46/CE et la loi du 8 décembre 1992, qui exigeaient toutefois que les données soient « non excessives » (et pas « limitées à ce qui est nécessaire »).

228 À ce sujet, voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *op. cit.*, pp. 18 et s.

229 Groupe 29, « Opinion 03/2013 on purpose limitation », 2 avril 2013, WP 203, pp. 36 et 37.

Le considérant 39 précise que « les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens ».

Dans le contexte du *big data*, le respect de ce principe pourrait poser de réelles difficultés.

Par nature, les opérations de *big data* supposent que de grands volumes de données soient examinés, sans savoir, *a priori*, si elles se révéleront pertinentes, adéquates ou même utiles dans le cadre du traitement. C'est d'ailleurs l'élément clé du *big data* : utiliser le plus de données possible, pour espérer en tirer une information utile dans le cadre des traitements envisagés par les prêteurs (en termes de *scoring* des clients, par exemple).

Une analyse au cas par cas devra donc être effectuée par le responsable du traitement, pour s'assurer que la finalité poursuivie, à la supposer légitime et respectueuse des autres exigences applicables, ne peut pas être atteinte autrement, par des mesures plus respectueuses des droits de la personne concernée.

46. Principe d'exactitude. L'article 5, § 1er, d), du R.G.P.D. exige que les données soient « exactes et, si nécessaire, tenues à jour ». Cette disposition ajoute que « toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ».

Des difficultés sont également à prévoir dans le contexte du *big data*, qui repose sur l'analyse d'une grande quantité de données, sans se soucier, *a priori*, de leur exactitude. Les sources de la collecte sont à ce point nombreuses et variées que, sans surprise, pour certaines d'entre elles, il est permis de douter de leur conformité à la réalité (on pense, p. ex., aux données collectées sur les réseaux sociaux).

47. Principe de limitation de la conservation. Ce principe est énoncé à l'article 5, § 1er, e), du R.G.P.D., aux termes duquel les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée ».

Il semble que, pour la plupart, les données exploitées dans le cadre du *big data* ont été collectées assez récemment. À terme, le prêteur ou le prestataire de services de paiement agissant comme responsable du traitement peut toutefois être intéressé de conserver celles-ci sur une longue période, de manière à en tirer autant d'informations utiles que possible, ce qui pourrait heurter ce prin-

cipe de limitation de la conservation. Ces prestataires devront donc être attentifs à cette exigence et mettre en place des mesures techniques et organisationnelles en interne, pour s'assurer que les données soient effacées le moment venu.

La fixation de ce moment se confondra généralement avec la période de prescription applicable ou avec des délais de conservation éventuellement imposés par des législations spécifiques ressortissant au secteur financier. On sait toutefois qu'en matière d'archivage, cette question peut être source d'incertitudes et de discussions. Par prudence, le choix d'une période de conservation relativement longue (correspondant au délai de prescription le plus long) est recommandé, ce qui sera utile dans l'hypothèse du *big data*.

48. Principe de responsabilité (*accountability*). Conformément au principe de responsabilité, tel qu'énoncé à l'article 5, § 2, du R.G.P.D., il incombe au responsable du traitement de respecter les principes énoncés au paragraphe 1er, tout en étant en mesure d'en apporter la preuve. Aussi est-il recommandé de mettre en place des mesures organisationnelles, en interne, qui garantissent leur respect effectif, et de les documenter à suffisance. En cas de plainte ou de demande d'une autorité de contrôle compétente, le prestataire de services financiers pourra ainsi établir qu'il agit en parfaite conformité avec la législation applicable.

En lien avec ce principe, le R.G.P.D. impose diverses obligations qui participent de cet objectif et visent à prévenir, autant que possible, les risques engendrés par les traitements de données. En remplacement de l'obligation de notification préalable auprès des autorités de contrôle – dont l'efficacité pouvait être sérieusement questionnée, le règlement prévoit désormais l'obligation de tenir un registre des activités de traitement[230] et de procéder, dans certains cas, à une analyse d'impact[231].

Sur ce dernier point, il est prévu que, « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ». L'objectif est de s'assurer qu'en réponse à cette analyse d'impact, des mesures soient prises en vue de réduire le risque ainsi identifié et correctement circonscrit. Qu'en est-il dans le contexte du *big data* ? Il est clairement visé par le considérant 91 du règlement[232], qui mentionne l'hypothèse dans laquelle « des données à caractère

230 Art. 30 R.G.P.D.

231 Art. 35 R.G.P.D.

232 En ce sens, voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *op. cit.*, p. 30. À ce sujet, voy. aussi Groupe 29, « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk", for the purposes of Regulation 2016/679 », 4 avril 2017, WP 248.

personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données ». On mentionne aussi l'hypothèse dans laquelle « l'autorité de contrôle compétente considère que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées [...] parce qu'elles sont effectuées systématiquement à grande échelle ». Le cas échéant, les prêteurs ou les prestataires de services de paiement devront réaliser une telle analyse d'impact pour les traitements *big data* qu'ils envisagent.

2. Décisions individuelles automatisées

49. Article 22 du R.G.P.D. Conformément à l'article 22, § 1er, du R.G.P.D., « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »[233].

Cette interdiction ne s'applique pas si l'une des trois hypothèses de l'article 22, § 2, du R.G.P.D. est rencontrée, autrement dit lorsque « la décision :

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou
c) est fondée sur le consentement explicite de la personne concernée ».

Avant d'examiner ces conditions, encore faut-il s'assurer que la disposition est d'application. Tel est le cas si (i) la personne concernée fait l'objet d'une décision ; (ii) que celle-ci est fondée exclusivement sur un traitement automatisé et (iii) qu'elle produit des effets juridiques concernant ou affectant la personne concernée de manière significative de façon similaire.

L'analyse doit évidemment se faire au cas par cas, en fonction des circonstances de l'espèce. Il paraît néanmoins acquis qu'un refus de crédit constituera normalement une décision ayant des effets juridiques sur la personne concernée. La situation est sans doute plus discutable si un prestataire de services de paiement recourt à une application d'intelligence artificielle de type *chatbot* pour répondre aux questions de ses clients : en tant que telle, la personne concernée ne fait pas l'objet d'une décision automatisée, au sens où le prestataire se limite

233 Sur cette disposition, voy. Th. Tombal, « Les droits de la personne concernée dans le R.G.P.D. », *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 531 et s.

à la conseiller ou lui fournir un document utile pour ses activités, mais sans prendre de décision au sens strict.

En tout état de cause, l'entreprise pourra écarter l'application de l'article 22 en veillant à ce qu'une intervention humaine ait lieu à un moment donné du processus. Si l'application d'intelligence artificielle est utilisée comme un outil, parmi d'autres, ce sera généralement le cas. Encore faut-il, cela va de soi, que cette intervention humaine ne devienne pas artificielle (dans le seul but d'échapper à l'application de l'article 22). Dans ses lignes directrices, le Groupe 29 indique ainsi que : « le responsable du traitement ne peut pas contourner les dispositions de l'article 22 en créant une intervention humaine de toutes pièces. Par exemple, si quelqu'un applique systématiquement des profils générés automatiquement à des individus sans aucune influence réelle sur le résultat, il s'agirait quand même d'une décision fondée sur un traitement automatisé. Pour qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique. Le contrôle devrait être effectué par une personne qui a l'autorité et la compétence pour modifier la décision. Dans le cadre de l'analyse, il convient de tenir compte de toutes les données pertinentes »[234].

Avec les développements techniques et l'évolution de certaines pratiques, on ne peut toutefois pas exclure que, dans des cas spécifiques, les professionnels du crédit ou des paiements recourent intégralement à des applications d'intelligence artificielle. Dans cette hypothèse, l'interdiction devra être levée en se basant sur l'une des trois exceptions visées au paragraphe 2 de l'article 22. À cet égard, le consentement explicite est sans doute l'hypothèse la plus prometteuse : un recours exclusif au traitement automatisé pour rendre une décision ne devrait pas rencontrer l'exigence de nécessité à la conclusion du contrat, ni faire l'objet d'une disposition légale ou réglementaire qui l'autorise.

Lorsque les exceptions visées sous a) et c) sont invoquées (comme cela devrait être le cas en l'espèce), l'article 22, § 3, du R.G.P.D. exige du responsable du traitement qu'il mette en œuvre « des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision ».

On ajoute que des règles additionnelles doivent être observées si des données particulières, visées à l'article 9, § 1er, du R.G.P.D. sont traitées dans ce cadre.

234 Groupe de travail « article 29 », « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 », adoptées le 3 octobre 2017 et révisées le 6 février 2018, WP251rev.01, p. 23.

50. Transparence et liberté de choix. Des obligations d'information en cas de recours à l'I.A. figurent déjà dans le R.G.P.D., lorsque les conditions d'application de l'article 22 sont réunies.

Une information doit en effet être donnée sur « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée »[235].

Il ne s'agit donc pas de révéler des secrets d'affaires ou des informations confidentielles, voire de dire ce que l'on ignore (vu l'impossibilité technique d'expliquer le raisonnement tenu par l'I.A. dans la « *black box* », le cas échéant). L'information doit permettre au consommateur de comprendre la décision qui a été prise à son égard, pour la contester si nécessaire.

S'agissant des éléments à prendre en considération, on peut se référer au considérant 71 du R.G.P.D., suivant lequel, « afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, et sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques ».

Conclusion

51. Cadre normatif complexe. Qu'il s'agisse des services de paiement ou de crédit, il convient d'articuler les dispositions du R.G.P.D. et les règles sectorielles figurant dans le livre VII du Code de droit économique ou dans des législations annexes (comme la loi du 11 mars 2018).

Il en résulte un cadre normatif complexe. Il est manifeste que le législateur européen n'a pas rédigé de concert les textes du R.G.P.D. et de la D.S.P. II,

235 Art. 13, § 2, f), et 14, § 2, g), R.G.P.D.

malgré leur proximité temporelle[236]. Quant aux dispositions spécifiques dans le domaine du crédit, elles n'ont pas été amendées suite au R.G.P.D. et, dans certains cas, la question de leur conformité au règlement pourrait légitimement se poser.

52. Ouverture précisément encadrée. Dans les deux domaines étudiés, on constate également que, pour atteindre les objectifs poursuivis, la transparence et la transmission des données sont indispensables. C'est le cas en matière de services de paiement, pour permettre la fourniture des nouveaux services d'initiation de paiement et d'information sur les comptes. Le constat peut aussi être fait en matière de crédit, avec l'obligation de communiquer des données à la C.C.P. et de consulter celle-ci en cas de demande de crédit de la part d'un consommateur.

Parallèlement, si l'ouverture est admise sur le principe, des exigences particulièrement strictes doivent être observées par les acteurs impliqués, pour protéger la vie privée des personnes concernées et garantir un traitement loyal et équitable de leurs données à caractère personnel. L'analyse se vérifie tant en matière de services de paiement que de crédit.

En définitive, si le législateur prend un risque, il est manifestement calculé. Encore faut-il qu'en pratique, l'insécurité juridique ne soit pas exploitée par certains acteurs, qui chercheraient à contourner les objectifs de la réglementation. En matière de crédit, il ne semble pas exister de dérives importantes sur ce point. Concernant les paiements, il est plus délicat de se prononcer à ce stade, les nouveaux services n'étant encore qu'à leur balbutiement. Il faut toutefois s'attendre à ce que de nouveaux acteurs cherchent également à exploiter ces données. Aussi faut-il rester vigilant.

236 Cette complexité est source d'insécurité juridique. Certaines pratiques répandues des *FinTechs* subsistent ainsi dans une zone grise, ce qui compromet les objectifs de promotion de la concurrence et de protection du consommateur poursuivis par le législateur européen. Cela étant, l'articulation de ces deux réglementations présente l'avantage de poser les bases du régime actuel en matière de services de paiement et de traitement de données à caractère personnel, dans l'attente des lignes directrices du Comité européen de la protection des données, qui nous l'espérons, traiteront au minimum des difficultés identifiées dans les présentes lignes.