Université de Lausanne

École de Droit
Faculté de droit, des sciences criminelles
et d'administration publique

MÉMOIRE DE MASTER

LE DROIT EUROPÉEN DE LA PROTECTION DES DONNÉES ET L'*OPEN BANKING*

Présenté

par

Christof Cardinaux

sous la direction du

Professeur Sylvain Métille

Lausanne, le 15 avril 2021

Table des matières

Bibliographie

BASEL COMMITTEE ON BANKING SUPERVISION, *Customer due diligence for banks,* 2001 (cité BASEL COMMITTEE, *CUSTOMER DUE DILIGENCE*)

BASEL COMMITTEE ON BANKING SUPERVISION, *Report on open banking and application programming interfaces, 2019 (*cité BASEL COMMITTEE, REPORT ON OPEN BANKING)

BENOUSSAN ALAIN, *Règlement Européen sur la protection des données : Textes, commentaires et orientations pratiques*, 2e édition, Bruxelles, 2016, pp. 159-163

BRODSKY LAURA / OAKES LIZ, *Data sharing and open banking*, McKinsey on Payments, juillet 2017 (cité BRODSKY/OAKES)

BÜHLMANN LUKAS / REINLE MICHAEL, *Extraterritoriale Wirkung der DSGVO,* 2017, pp. 8-12 (cité BÜHLMANN / REINLE)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Le droit à la portabilité en question*, disponible sous : https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite (Dernière consultation le : 10 avril 2021) (cité CNIL)

DOYLE MARGARET / RAHUL SHARMA / ROSS CHRISTOPHER / VISHWANATH SONNAD, *How to flourish in an uncertain future: Open Banking and PSD2*, Deloitte, 2017 (cité DOYLE ET AL.)

ESSEBIER JANA / BOURGEOIS JANIQUE, *Open-Banking – Der Zahlungsverkehr im Umbruch*, Zurich, 2018, pp.116-128 (cité ESSEBIER/BOURGEOIS)

EUROPEAN BANKING ASSOCIATION, *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC, EBA/OP/2020/10,* 4 juin 2020 (cité EBA)

EUROPEAN BANKING FEDERATION, *EBF response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR, EBF_042474*, 16 septembre 2020 (cité EBF, *Response to EDPB interplay consultation*)

EUROPEAN BANKING FEDERATION, *European Banking Federation's comments to the Working Party 29 Guidelines on the right to data portability, EBF_025448E*, 15 février 2017 (cité EBF, *Comments on WP29 Portability Guidelines*)

EUROPEAN BANKING FEDERATION, *Guidance for implementation of the revised Payment Services Directive, PSD2 guidance*, 20 décembre 2019 (cité EBF, *Guidance*)

EUROPEAN COMMISSION, COMMISSION, *Staff working document, Impact assessment, accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions, SWD(2013) 288 final, Volume 1/2*, adopté le 24 juillet 2013 (cité EUROPEAN COMMISSION, *Volume 1/2*)

EUROPEAN COMMISSION, COMMISSION, *Staff working document, Impact assessment, accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions, SWD(2013) 288 final, Volume 2/2*, adopté le 24 juillet 2013 (cité EUROPEAN COMMISSION, *Volume 2/2*)

EUROPEAN DATA PROTECTION BOARD, *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, 2ème version*, adopté le 15 décembre 2020 (cité EDPB, *Interplay*)

EUROPEAN DATA PROTECTION BOARD, *Letter to Ms in't Veld,* EDPB-84-2018, le 5 juillet 2018 (cité EDPB, *Letter)*

FINANCIAL CONDUCT AUTHORITY, *Call for Input: Open finance*, décembre 2019 (cité FCA, *OPEN FINANCE*)

FINANCIAL CONDUCT AUTHORITY, *Implementation of the revised Payment Services Directive (PSD2): Approach Document and final Handbook changes*, septembre 2017

FOLCIA MARCO / CASCINELLI FABRIZIO / ZANETTI GIANMARCO / MARCOZZI SARA, *PSD2 in a nutshell 3 – The main regulatory changes introduced*, PricewaterhouseCoopers, 2016 (cité FOLCIA ET AL.)

GAWRONSKI MACIEJ, *Guide to the GDPR,* Alphen aan den Rijn, 2019, pp. 160 ss

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Lignes directrices relatives au droit à la portabilité des données – 16/FR, WP 242 rév.01*, révisée et adoptée le 5 avril 2017 (cité GR29, *WP242*)

HERBST THOMAS, *Art. 20 Recht auf Datenübertragbarkeit*, in: Kühling / Buchner (édit.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, München, 2018, pp. 478-492, (cité HERBST)

HAAS GÉRARD, *Le RGPD expliqué à mon boss,* Bluffy, 2017, pp. 99-101

INFORMATION COMMISSIONER'S OFFICE, *Right to data portability*, Disponible sous: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability (Dernière consultation le : 10 avril 2021)

INSURANCE EUROPE, *Insurance Europe response to EC data strategy consultation, COB-TECH-20-033*, 31 mai 2020 (cité INSURANCE EUROPE)

KERN ALEXANDER, *Principles of Banking Regulation,* Cambridge, 2019, pp. 332-337 (cité KERN)

LYNSKEY ORLA, *Article 20 Right to data portability*, in: Christopher Kuner / Lee A. Bygrave / Christopher Docksey /Laura Drechsler (édit.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 409-507 (cité LYNSKEY)

MALLICK AMIT / WOJIK EWA / MCFARLANE ANDREW, *Power plays for monetizing Open Banking APIs: Turning Open Banking into an opportunity to drive growth and profitability*, Accenture, 2020 (cité MALLICK ET AL.)

MILSHINA ANASTASYIA / DANKERT MARLOES / KITS PETER / VAN DUIJVENBODE MARIA, *PSD2 and GDPR: An awkward match?*, Deloitte NL, 2018 (cité MILSHINA ET AL.)

METILLE SYLVAIN / ACKERMANN ANNELISE, *Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen / Le Règlement général sur la protection des données (RPDG) : portée et premières expériences*, 2020, pp. 77-97 (cité MÉTILLE / ACKERMANN)

REICHLIN JEREMY, *Le droit à la portabilité des données sous le RGPD*, in : Molin-Kränzlin / Schneuwly / Stojanovic (édit.), Digitalisierung – Gesellschaft – Recht, pp. 401 ss (cité REICHLIN)

SCHREY JOACHIM, *New European General Data Protection Regulation: A Practitioner's Guide: ensuring compliant corporate practic*e, in: Rücker Daniel / Kugler Tobias, Munich, 2018, pp. 144-147 (cité SCHREY)

SIX GROUP, b.Link of SIX, The Pioneering Link to Open Banking, 2020

SIX GROUP, *b.Link, Frequently Asked Questions: "What does the participation in b.Link cost?"*, disponible sous : https://www.six-group.com/en/products-services/banking-services/blink.html#what_does_the_participationinblinkcost (Dernière consultation le : 10 avril 2021) (cité SIX, *FAQ*)

STENGEL CORNELIA / WEBER THOMAS, *Digitale und mobile Zahlungssysteme : Technologie, Vertträge und Regulation von Kreditkarten, Wallets und E-Geld*, Zurich, 2016, PP. 228-232

SYDOW GERNOT, *Europäische Datenschutzgrundverordnung*, Handkommentar, Münster, 2017, pp. 529-537, (cité SYDOW)

VAN DER KROFT JEROEN / KUIJSTEN PIETER, *How banks can balance GDPR and PSD2*, disponible sous : https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2 (Dernière consultation le : 11 avril 2021) (cité VAN DER KROFT / KUIJSTEN)

Table des abréviations

API	*Application Programming Interface*
Cf.	confer
ch.	chapitre
CNIL	Commission nationale de l'informatique & des libertés (France)
éd.	Édition
ibid	ibidem locution latine signifiant « même endroit »
in	dans
let.	lettre
n°	numéro
p.	page
PSD II	*Payment Services Directive II* ou 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
GR29	Groupe de travail « article 29 »
RGPD	Règlement (UE) 2015/679 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
RTS	*Regulatory Technical Standard* ou Règlement délégué (UE) 2018/389 de la Commission 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

INTRODUCTION

A. Généralités

L'*Open Banking* est un changement profond du mode de fonctionnement du secteur bancaire tel qu'on le connaît. L'ouverture d'un accès à certaines données bancaires des clients a poussé les différents acteurs à redéfinir le rôle qu'ils souhaitent adopter dans ce nouveau modèle. Ce nouveau mode de fonctionner soulève certaines questions et inquiétudes de la part des banques sur les opportunités et les risques que ce changement peut comporter[1].

De plus, l'*Open Banking* se situe au croisement entre le monde de la protection des données et celui de la réglementation bancaire[2]. En effet, tant le Règlement Européen sur la Protection des Données[3], que la Directive sur les services de paiement II (ci-après « PSD II »)[4] comportent des éléments qui vont permettre à l'utilisateur d'exiger de la banque que celle-ci donne un accès à un prestataire tiers à ses données.

Nous allons donc, dans un premier temps, étudier les deux mécanismes régissant l'ouverture des données bancaires à un tiers. Le premier mécanisme est celui issu de la PSD II. Cette directive autorise les utilisateurs à requérir de leur banque de transmettre les informations relatives à leur compte bancaire à un tiers. Elle permet également d'exiger de la banque qu'elle exécute des ordres de paiements transmis par le biais dudit tiers et à ce que celle-ci exécute des ordres de paiements transmis par le biais de ce tiers[5]. Quant au second mécanisme que nous allons traiter dans cette analyse, il s'agit du droit à la portabilité des données, soit le mécanisme prévu dans le RGPD. Ce mécanisme permet à un utilisateur de demander de recevoir ou de transmettre à un tiers les données que le responsable de traitement détient à son propos[6]. L'objectif de cette étude sera ainsi de définir les conditions et l'étendue de ces droits découlant des deux instruments précités, mais également de déterminer plus précisément comment ils peuvent être utilisés dans le contexte de l'*Open Banking*.

Dans un deuxième temps, nous traiterons plus spécifiquement de deux questions en relation avec l'application concrète de l'*Open Banking* et des normes que nous aurons analysées. Nous essayerons dès lors de déterminer quelles règles doivent s'appliquer à une demande de portabilité des données servant à exécuter des services relevant de la PSD II. Finalement, nous traiterons du modèle économique des banques et plus particulièrement de la question de savoir si celles-ci peuvent demander une rémunération aux prestataires tiers pour la mise à disposition d'un accès aux données du client.

B. Contexte

Le secteur bancaire a subi, au long de son histoire, un grand nombre de changements encouragés par le développement frénétique des nouvelles technologies. Comme les banques offrent des

---

[1] BASEL COMMITTEE, *Report on Open Banking*, pp.5-7.

[2] *Ibid.* p.5.

[3] 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 (cité PSD II).

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données, (cité RGPD).

[5] *Cf. infra* Partie I, Chapitre 1, D.

[6] *Cf. infra* Partie I, Chapitre 2, D.

services essentiels au bon fonctionnement de nos sociétés, elles se doivent de suivre avec attention les opportunités et les risques que ces nouvelles technologies représentent. Les innovations dans le secteur bancaire et financier ne sont donc pas rares et les exemples de *fintechs* offrant de nouveaux services aux clients ne manquent pas[7]. Nous pouvons, à cet égard, mentionner les « *Challenger Bank* » qui – en offrant des solutions bancaires orientées vers une clientèle jeune et en se tournant vers des produits digitaux attrayants – ont connu un certain succès. En parallèle, certains législateurs, notamment en Europe, ont commencé à mieux saisir l'étendue des pouvoirs que confère la collecte et l'agrégation massive de données. Les législateurs ont donc eu une volonté croissante de limiter ces pouvoirs et de redonner aux consommateurs le contrôle sur leurs données. C'est dans ce contexte que l'*Open Banking* s'est développé. Comme nous allons le voir, l'*Open Banking* permet au client de la banque de faire un usage plus libre de ses données et d'intégrer les innovations technologiques développées par les *fintechs* dans le système financier actuel. En contrepartie, les banques peuvent éviter ou, du moins, contenir la possible fuite de leurs clients vers d'autres sociétés plus novatrices. Cependant, ce changement de modèle économique ne peut se faire sans l'émergence de risques. En effet, en laissant entrer sur le marché d'autres acteurs et en leur ouvrant leurs systèmes informatiques, les banques risquent de perdre une partie de la relation qui les lie aux clients et, ainsi, de perdre des revenus[8].

C. Définition de l'*Open Banking*

Afin de déterminer les contours exacts de l'*Open Banking*, nous utiliserons la définition suivante proposée par le Comité de Bâle sur le contrôle bancaire dans un rapport de 2019[9] :

> *"Open banking – the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities.* "

L'*Open Banking* se rapporte donc au partage par la banque de données bancaires que le client souhaite voir être transmises à un prestataire tiers afin que celui-ci puisse lui offrir certains services. Ces services peuvent notamment être de nature à offrir des paiements facilités ou un meilleur contrôle sur les comptes du client. Cependant, la liste citée ci-dessus n'est pas exhaustive et tout service qui se fondera sur l'accès au compte du client rentrera dans le cadre de l'*Open Banking.* Par ailleurs, nous pouvons noter que les services couverts par la PSD II[10] ne correspondent pas à l'entier des situations qui se rapportent à l'*Open Banking*[11].

Les modalités techniques exactes du partage des données ne sont pas clairement définies. Cependant, l'utilisation d'une interface de programmation ou, en anglais, d'« *Application Programing Interface »* (ci-après : « *API »*) semble être la solution favorite[12]. Cette solution vise à construire des standards communs afin de faciliter la communication sécurisée entre deux programmes informatiques[13]. La banque développera donc un programme qui ira chercher les

[7] DOYLE ET AL., p.2.
[8] KERN, p.337.
[9] BASEL COMMITTEE, *Report on Open Banking,* p. 19.
[10] *Cf. infra* Partie I, Chapitre 1, D.
[11] *Ibid.*, p.5.
[12] KERN, p. 334.
[13] *Ibid.* p.19.

données dans les serveurs internes de l'entreprise conformément aux demandes reçues par le programme informatique du prestataire tiers.

Nous pouvons également relever que les données relatives à d'autres services qu'offre la banque – tel que les activités de gestion de fortune et de banque d'investissement – ne seront pas à inclure dans le champ d'application de l'*Open Banking* comme nous le comprenons dans le cadre de cette étude. En effet, ces activités relèvent plutôt de l'*Open Finance*[14]. Seuls les comptes d'épargnes, les comptes courants et les informations rattachées à une ligne de crédits sont alors concernés par l'*Open Banking*[15].

D. Exemple de services possibles

Comme les services que les prestataires tiers pourraient offrir dans le cadre de l'*Open Banking* sont nombreux, nous allons ici citer quelques exemples illustratifs.

La possibilité de demander à la banque d'exécuter des paiements exécutés par un tiers va permettre aux prestataires externes d'offrir des solutions de paiements en ligne qui ne requièrent pas de détenir une carte de paiement[16].

Ensuite, il y a lieu de mentionner les services qui pourraient émaner d'une analyse de ces données. Ceux-ci comprennent notamment les *robo-advisor* et *personal finance manager* qui visent à aider les clients à mieux gérer leurs dépenses.

Nous pouvons également supposer que des services plus spécialisés vont bénéficier des avantages de l'*Open Banking*. Par exemple, en ayant accès aux données du client, il sera plus facile d'évaluer sa solvabilité (ci-après : « *credit scoring »)* ou encore d'offrir des services visant à aider les personnes concernées à effectuer leur déclaration d'impôt.

Finalement, l'*Open Banking* peut également ouvrir de nouvelles solutions dans le domaine du marketing, notamment par le biais de programmes de fidélités rattachés aux informations de transactions du compte[17].

E. Quelques définitions clés

Avant de procéder davantage à une analyse plus détaillée, il y a lieu de définir quelques notions et la manière dont elles sont utilisées dans le cadre de ce travail.

Premièrement, dans le contexte de l'*Open Banking,* nous avons et allons à plusieurs reprises mentionner la notion de « banque ». Cette notion est à comprendre de manière large et renvoie à toute entreprise qui propose et gère des comptes de paiements aux clients. Ceci comprend donc les établissements de crédits mais également toute autre entreprise pertinente.

Ensuite, la PSD II utilise la notion de « prestataire de services de paiement gestionnaire de compte » pour faire référence au prestataire de services de paiement qui gère le compte duquel l'ordre de paiement sera effectué. Afin de faciliter la compréhension de ce travail, nous avons simplifié la notion précitée en utilisant en lieu et place le terme de « gestionnaire de compte ».

---

[14] "Open finance refers to the extension of *Open Banking*-like data sharing and third-party access to a wider range of financial sectors and products." Voir : FCA, OPEN FINANCE, p.3.

[15] EDPB, *Interplay,* p. 22.

[16] Dans le contexte Suisse, les services proposés par la société Twint AG sont un exemple de cette application de l'*Open Banking*.

[17] BASEL COMMITTEE, *Report on Open Banking,* pp. 8-9.

Par ailleurs, il sied de préciser que la notion d'« *API* » n'est pas clairement définie, ni dans le RGPD, ni dans la PSD II et ses réglementations d'application. Nous utiliserons donc la définition suivante telle que proposée par le Comité de Bâle sur le contrôle bancaire[18] :

« a set of rules and specifications for software programs to communicate with each other, that forms an interface between different programs to facilitate their interaction. »

PARTIE I : NORMES ET PRINCIPES APPLICABLES

CHAPITRE 1 : LA DIRECTIVE SUR LES SERVICES DE PAIEMENT II

A. Généralités

La PSD II a ouvert la porte au développement de l'*Open Banking* en Europe. En effet, cette directive a introduit une obligation pour les gestionnaires d'un compte de paiement de fournir à des prestataires tiers un accès audit compte afin que ces derniers effectuent les services souhaités par l'utilisateur du compte. C'est donc une législation particulièrement relevante dans le domaine de l'*Open Banking*. Il convient de préciser cependant que, en tant que directive européenne, la PSD II appelle à ce que les États membres de l'Union Européenne adoptent des législations de mise en application et n'est donc pas directement applicable. Les États membres avaient un délai au 13 janvier 2018 pour mettre en œuvre de droit européen dans leur législation nationale ; délai qui a été respecté par la plupart desdits États.

B. Champ d'application territorial

En vertu de l'article 2 PSD II, tout service de paiement fourni au sein de l'Union Européenne est soumis à la directive. Par ailleurs, le titre III de la PSD II est également appliqué lorsque les deux prestataires de paiement impliqués dans une opération de paiement sont situés à l'intérieur de l'Union, indépendamment de l'endroit où sont fournis les services. De plus, si l'opération de paiement a lieu dans une devise de l'État membre, le titre IV sera également applicable[19].

C. Champ d'application matériel

1. Services concernés

Premièrement, en vertu de l'article 4 par. 1 point 3 PSD II, sont des services de paiements les huit services mentionnés dans l'Annexe I. Ceux-ci comprennent les retraits ou versements d'espèces[20] sur un compte de paiement, les débits d'un compte de paiement, les transactions liées à une ligne de crédit, l'émission de cartes de paiement, le transfert d'argent, les services d'initiation de paiements et, enfin, les services d'information sur les comptes. L'article 4 point 15 PSD II précise que les services d'initiation de paiement correspondent à la situation dans laquelle un ordre de paiement est initié – à la demande du client – par un autre prestataire que

[18] BASEL COMMITTEE, *Report on Open Banking,* p.19.

[19] EBF, *Guidance,* pp.8-16.

[20] A noter que les services de distributeurs de billets indépendants, qui n'offrent pas d'autres services relevant du champ d'application de la PSD II, sont exclus du champ d'application de celle-ci en vertu de l'article 3 par. 1 let. o) PSD II.

celui qui détient le compte d'où le paiement sera exécuté[21]. Les services d'informations sur les comptes, quant à eux, correspondent, en vertu de l'article 4 point 16 PSD II, aux services visant à offrir aux clients des informations consolidées sur un ou plusieurs de leurs comptes[22]. Le but des services d'information sur les comptes étant de permettre à l'utilisateur de mieux apprécier sa situation financière, ils pourront comprendre des éléments tels que la catégorisation des dépenses, ou encore la gestion budgétaire[23]. Ne sont donc pas compris dans le champ d'application de la PSD II les services d'évaluation de solvabilité et les services d'audits[24].

Ensuite, afin de rentrer dans le champ d'application matériel de la PSD II, les services mentionnés ci-dessus doivent être fournis à titre professionnel. Cela exclut tant les services effectués de manière accessoire par des personnes privées, que ceux également proposés dans le cadre d'activité caritative ou à but non-lucratif[25].

Finalement, l'article 3 PSD II comprend d'autres exceptions visant à exclure spécifiquement certains services du champ d'application de la directive. L'exception la plus notable est l'exclusion des moyens de paiements effectués par le biais d'un support papier, notamment le chèque papier.

Dans le contexte de l'*Open Banking*, seuls les services d'initiation de paiement et d'information sur les comptes sont pertinents. En effet, les autres services mentionnés dans la PSD II se rapportent à des opérations internes à l'entreprise et ne nécessitent pas un partage de données avec des tiers.

2. Données concernées

Premièrement, compte tenu des services qui rentrent dans le champ d'application de la PSD II, seules les informations relatives à un compte de paiement seront concernées par cette directive. Les données relatives à un compte d'épargne ou à un compte d'investissement ne seront pas inclues dans le champ d'application de la PSD II[26].

Ensuite, il y a lieu de préciser que les données de compte de paiements en question ne se limitent pas à des données de comptes de consommateur[27], c'est-à-dire une personne privée utilisant le compte pour ses besoins personnels. En effet, les entreprises et les personnes avec une activité commerciale disposant d'un compte de paiement pourront donc également utiliser les services régis par cette directive.[28] Cet élément constitue une différence majeure avec le droit à la portabilité des données dont seules des personnes privées peuvent être titulaires[29].

---

[21] A noter que lorsque le paiement est initié par l'utilisation d'une carte de paiement, des règles spécifiques sont applicables. Voir : EBF, *Guidance*, pp. 58-59.

[22] EDPB, *Interplay*,p.5 ; DOYLE ET AL., p. 7.

[23] Sont visés ici principalement les services de *Personal Finance Manager,* Voir : ESSEBIER/BOURGEOIS, p.119.

[24] EDPB, *Interplay*, p. 7.

[25] Article 3 par. 1 let. d) PSD II.

[26] EDPB, *Interplay*,pp. 7-8 ; EBF, Response to EDPB interplay consultation, p. 4.; Cela découle également du principe de minimisation des données, Voir : *Cf. infra* Partie I, Chapitre 1, D, ch.5.5.

[27] Voir définition article 4 point 20 PSD II.

[28] Lorsque le détenteur du compte n'est pas un consommateur, les parties peuvent plus librement déroger aux règles de la PSD II. Voir notamment articles 38 et 61 PSD II.

[29] *Cf. infra* Partie I, Chapitre 2, C., ch. 1.1.

3. Prestataires de services concernés

En vertu de l'article 37 PSD II, seules certaines catégories de prestataires de services peuvent fournir des services de paiement.

Dans un premier temps, il convient de mentionner les catégories de prestataires qui rentrent dans le champ d'application sans avoir dû suivre un processus d'autorisation, c'est-à-dire les établissements de crédits[30], les établissements de monnaie électronique[31], les offices de chèques postaux, les Banques centrales ainsi que les États membres eux-mêmes. Conformément aux articles 1er, 4, 11 et 37 PSD II, ceux-ci peuvent donc pleinement offrir des services de paiement sans avoir à requérir d'autorisation auprès de l'autorité compétente.

Ensuite, il y a lieu de mentionner « les établissements de paiement[32] », qui constituent une catégorie spéciale de prestataires de paiement. Conformément à l'article 4 par. 1 point 4 PSD II, les établissements de paiements sont des entreprises qui ont été agréées en vertu de l'article 11 PSD II et qui fournissent des services de paiements. Pour être agréées, les entreprises devront suivre un processus d'autorisation régi aux articles 5 et suivants PSD II, qui comprend, entre autres, des conditions portant notamment sur le capital social, la structure interne de l'entreprise, l'état de leurs comptes, le système d'évaluation des risques ainsi que d'autres aspects organisationnels. De plus, l'entreprise qui souhaite obtenir une autorisation devra être établie au sein d'un État membre[33] et disposer d'une assurance responsabilité civile professionnelle[34].

Toutefois, en vertu de l'article 33 PSD II, les entreprises qui ne souhaitent n'offrir que des services d'informations sur les comptes sont soumis à un processus d'autorisation allégé car ils ne disposent pas de moyens pouvant porter atteintes aux fonds des utilisateurs.

Finalement, les États membres ont la possibilité d'exempter de tout ou partie de la procédure d'autorisation les entreprises qui répondent aux conditions de l'article 32 PSD II[35].

4. Conclusion intermédiaire

Au vu de ce qui a été établi ci-dessus, pour relever du champ d'application matériel de la PSD II, trois conditions doivent être remplies. Premièrement, seuls les services de paiements électroniques, d'initiation de paiement et d'information sur les comptes fournis de manière professionnelle seront compris dans le champ d'application matériel de la PSD II. Ensuite, seules les données issues de comptes de paiements seront concernées. Finalement, la PSD II ne s'applique qu'aux prestataires de services qui doivent – à moins d'être une catégorie spéciale de l'article premier PSD II – avoir été autorisés à procéder à des opérations de paiements. Ne relèvent donc pas de la PSD II, les services d'évaluation de solvabilité, d'audit, les programmes de fidélités, ainsi que les services fondés sur des informations détenues dans un compte d'épargne.

[30] Tels que définis dans le règlement (UE) no 575/2013.
[31] Tels que définis dans la directive 2009/110/CE.
[32] Article 1er par. 1 let. d) PSD II.
[33] Article 11 par. 1 *in fine* PSD II.
[34] Article 5 par. 2,3,4 PSD II
[35] Certains États membres ont fait usage de ce droit, notamment la France, l'Italie et les Royaume-Unis.

D. Règles relatives à l'accès au compte par un prestataire tiers

1. Généralités

Comme expliqué ci-dessus[36], l'analyse sera concentrée sur deux des services qui rentrent dans le champ d'application de la PSD II. En effet, ce travail aspirant à donner une vue d'ensemble des règles s'appliquant spécifiquement à l'*Open Banking,* il y a lieu de ne traiter que des services qui donnent à un prestataire tiers un accès au compte de l'utilisateur.

2. Services d'initiation de paiement

2.1. Conditions spécifiques

En vertu de l'article 66 par. 1 et 2 PSD II, deux conditions doivent être réunies pour que l'utilisateur ait le droit d'exiger du gestionnaire de compte d'exécuter un ordre de paiement initié par l'intermédiaire d'un prestataire tiers.

Conformément à l'article 66 par 1. PSD II, la première condition requiert que le compte duquel un paiement doit être exécuté soit accessible en ligne. Nous pouvons supposer que cette condition sera remplie, notamment, lorsque le gestionnaire de compte a mis à disposition de l'utilisateur une interface en ligne pour accéder à son compte telle qu'une plateforme d'*Ebanking*.

La seconde condition découle de l'article 66 par. 2 PSD II, en vertu duquel l'utilisateur doit consentir explicitement[37] à l'exécution du paiement en lui-même. Conformément aux conditions fixées à l'article 64 PSD II, le consentement doit être fourni avant l'exécution du paiement, à moins que le prestataire et l'utilisateur n'aient prévu autre chose. Le choix de la procédure et la forme du consentement sont laissés libres au prestataire de paiement et à l'utilisateur. Il convient de préciser, qu'une fois donné, le consentement de l'utilisateur ne peut être retiré, conformément à l'article 80 par. 2 PSD II.

2.2. Obligations incombant au prestataire de services d'initiation de paiement

L'article 66 par. 3 PSD II délimite plus précisément quels sont les actes qui doivent être effectués par le prestataire de services d'initiation de paiement.

Ainsi, dans un premier temps, il incombe au prestataire de services d'initiation de paiement de s'identifier auprès du gestionnaire du compte et de lui indiquer de qui émane la demande de paiement, le montant exact à transférer – sans l'avoir modifié – et à qui il convient de transférer les fonds[38]. Le prestataire tiers doit s'assurer que le moyen de communication utilisé pour transférer ces informations est sécurisé[39].

Ensuite, dans le cadre de l'exécution du paiement, le prestataire de service d'initiation de paiement peut collecter les informations nécessaires à la fourniture de ses prestations. Il ne peut cependant pas consulter ou obtenir – soit de la part de l'utilisateur directement, soit auprès du gestionnaire du compte – d'autres informations que celles requises pour fournir les services d'initiation de paiement. L'article 66 par. 3 let e) PSD II précise également que le prestataire

[36] *Cf. supra* Partie I, Chapitre 1, A. ch. 1.

[37] La notion de consentement « explicite » de la PSD II diffère de la notion homonyme du RGPD, *Cf. infra* Partie I, Chapitre 1, D., ch.5.2.

[38] L'article 66 PSD II parle à cet égard de « Payeur » et de « Bénéficiaire » pour désigner respectivement l'utilisateur du service qui désire effectuer un paiement et la personne à qui les fonds sont transmis.

[39] *Cf. infra* Partie I, Chapitre 1, D, ch. 4.2.

ne peut pas stocker les données de paiement sensibles de l'utilisateur. La notion de « données de paiements sensibles » renvoie aux données pouvant être utilisées pour commettre des fraudes, tels que les identifiants et mots de passe de l'utilisateur[40].

Notons également que le prestataire de services d'initiation de paiement n'est pas autorisé à détenir lui-même les fonds qui seront transférés.

Finalement, il se peut que le bénéficiaire du paiement reçoive d'autres informations relatives à l'utilisateur dans le cadre de l'exécution du paiement. Le prestataire de services d'initiation de paiement doit s'assurer que ces données ne soient pas communiquées à un tiers autre que le bénéficiaire. Il devra également s'assurer que l'utilisateur ait explicitement consenti à ce que ces informations soient transmises au bénéficiaire.

2.3. Obligations incombant au gestionnaire du compte

Le gestionnaire du compte, de son côté devra, conformément à l'article 66 par. 4 PSD II, exécuter l'ordre de paiement transmis par le prestataire de services d'initiation de paiement, sans discrimination par rapport aux ordres de paiements qu'il reçoit de l'utilisateur directement. Il ne peut donc pas imposer, sans raison objective de délai ou de frais[41] supplémentaires.

De plus, conformément à l'article 66 par. 4 let. b) PSD II, le prestataire de paiement gestionnaire de compte devra fournir au prestataire tiers toutes les informations qui sont à sa disposition et qui sont nécessaires à l'exécution des services d'initiation de paiement.

Pour finir, comme nous l'avons vu ci-dessus, le gestionnaire de compte et le prestataire de services d'initiation de paiement doivent communiquer de manière sécurisée[42].

3. Services d'information sur les comptes

3.1. Conditions spécifiques

Les conditions relatives à la fourniture de services d'information sur les comptes sont allégées par rapport aux conditions requises afin d'offrir des services d'initiation de paiement[43].

La première condition requiert que le compte auquel le prestataire de services d'information sur les comptes souhaite accéder soit en ligne. En ce sens, cette exigence est similaire que celle prévue à l'article 66 par. 1 PSD II.

Ensuite, en vertu de l'article 67 par. 2 let. a) PSD II, l'utilisateur doit consentir explicitement à la fourniture des services. Il sied de relever que le consentement porte ici sur la fourniture des services et non sur le traitement des données[44]. Cette notion se distingue donc du consentement requis de par l'article 94 par. 2 PSD II[45].

3.2. Obligations incombant au prestataire de service d'information sur les comptes

[40] Cette notion se distingue de la notion de « données sensibles » de l'article 9 RPGD. Voir : EDPB, *Interplay*, p. 18.
[41] *Cf. infra* Partie II, Chapitre 2, C.
[42] *Cf. supra* Partie I, Chapitre 1, D., 2.3.
[43] *Cf. supra* Partie I, Chapitre 1, D., 2.2.
[44] EDPB, *Interplay*, p.14.
[45] *Cf. supra* Partie I, Chapitre 1, D., 5.2.

Les obligations incombant au prestataire de services d'information sur les comptes sont comparables à celles qui échoient au prestataire de services d'initiation de paiement[46].

En effet, le prestataire tiers doit également s'identifier auprès du gestionnaire de compte et ne peut accéder à d'avantage de données que celles qui s'avèrent nécessaires pour l'exécution des services en question. Ainsi, les informations qu'il peut obtenir sont uniquement celles relatives aux comptes de paiement désignées par l'utilisateur des services et l'historique des transactions sur la période souhaitée[47].

Cependant, contrairement au prestataire de services d'initiation de paiement, dans la présente situation, le prestataire n'a pas le droit de demander les données de paiement sensibles[48]. Cette obligation dépasse donc la simple interdiction de stockage de ces données.

Finalement, l'article 67 par. 2 let. f) PSD II, indique que le prestataire ne peut utiliser les données auxquelles il a accès pour un autre but que celui de fournir les services d'information sur les comptes expressément requis par l'utilisateur. Il sied de préciser que – contrairement à 66 par. 3 let. g) PSD II – le texte mentionne ici expressément le respect des règles relatives à la protection des données.

3.3. Obligations incombant au gestionnaire du compte

Les obligations incombant au gestionnaire de compte se limitent à l'interdiction de la discrimination et à la mise en place d'une communication sécurisée avec le prestataire tiers. Ces conditions étant similaires à celles qui découlent de l'article 66 PSD II[49], il y est ici expressément renvoyé.

4. Modalités techniques

La PSD II en elle-même ne fixe pas précisément les modalités techniques qui doivent être mises en place par le gestionnaire du compte pour permettre la fourniture des services de paiements par les tiers.

Cependant, la Commission a adopté des normes techniques de réglementations[50] qui visent à établir les principes liés à l'authentification et les normes relatives aux moyens de communication à utiliser dans le cadre de la PSD II. Ce règlement apporte des éléments de réponses sur les moyens techniques qui seront choisies par les gestionnaires de compte lors de l'implémentation de la PSD II.

4.1. Authentification forte du client

En vertu de l'article 97 PSD II, l'authentification forte du client est requise lorsqu'il accède à son compte, lorsqu'il initie un paiement ou encore lorsqu'il effectue une action qui comporte un risque important de fraude. A noter que, conformément aux articles 10 et suivant RTS, l'obligation ici mentionnée comporte de nombreuses dérogations, notamment lorsque les informations consultées portent uniquement sur le solde du compte ou sur l'historique des

[46] *Cf. supra,* Partie I, Chapitre 1, D, ch. 2.2.

[47] *Cf. supra,* Partie I, Chapitre 1, D., 5.5.

[48] Article 67 par. 2 let. e) PSD II.

[49] *Cf. supra,* Partie I, Chapitre 1, D, ch. 2.3.

[50] Règlement délégué (UE) 2018/389 de la Commission 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 fore du client et à des normes ouvertes communes et sécurisées de communication (cité : « RTS »).

opérations de paiements de moins de nonante jours. Néanmoins, la première fois que l'utilisateur utilise le service ou lorsqu'il ne l'a plus utilisé depuis nonante jours, il devra tout de même suivre la procédure classique d'authentification renforcée.

Selon l'article 4 point 30 PSD II, la procédure d'authentification forte du client se caractérise par l'utilisation de deux éléments au moins qui permettent la vérification de l'identité d'un utilisateur. Ces éléments de vérification doivent relever de deux catégories différentes parmi les trois suivantes : les éléments qui sont de la connaissance de l'utilisateur, ceux qui sont en sa possession et finalement ceux qui sont inhérent à sa personne. Les articles 4 à 6 RTS définissent plus précisément de quelle manière ces moyens peuvent être utilisés dans le cadre de l'authentification forte du client.

Il convient également de noter que, en vertu de l'article 30 point 3 RTS, lorsqu'une banque prévoit une interface dédiée aux obligations lui incombant en vertu de la PSD II, elle ne peut faire entrave aux prestations offertes par les tiers. Tel sera notamment le cas lorsqu'un utilisateur est redirigé vers une autre interface que celle du prestataire tiers afin de procéder à son authentification. En pratique, ce point a soulevé de nombreuses questions de la part des prestataires de services de paiements et d'information sur les comptes ceux-ci étant régulièrement confrontés à des processus d'authentification faisant obstacle aux services qu'ils proposent. Le 4 juin 2020, l'*European Banking Association* a donc émis un document apportant quelques précisions au sujet. Ainsi, elle a notamment clarifié que le fait de renvoyer un utilisateur vers une application installée sur son téléphone dans le but de procéder à son authentification ne constitue pas un obstacle. En effet, l'application installée doit être considérée comme étant un élément en la possession de l'utilisateur conformément à l'article 7 RTS, de sorte qu'elle n'est donc pas une redirection au sens de l'article 30 point 3 RTS. En revanche, l'*European Banking Association* a estimé qu'il y a notamment entrave lorsque le gestionnaire de compte ne met pas à la disposition des prestataires tiers tous les moyens d'authentification qu'il utilise pour ses propres services[51]. Enfin, le document précise que si l'authentification repose sur l'utilisation de facteurs biométriques, l'évaluation desdits facteurs doit avoir lieu au sein de l'interface du prestataire tiers et ne peut faire l'objet d'une redirection de l'utilisateur vers une interface du gestionnaire du compte[52].

4.2. Normes ouvertes communes et sécurisées de communication

Les articles 28 à 36 RTS traitent des obligations qui doivent être respectées concernant la communication de données ayant lieu dans le cadre de la fourniture de services d'initiation de paiement et d'information sur les comptes. Le gestionnaire du compte doit, en vertu de l'article 30 RTS, mettre en place une interface qui doit au moins permettre aux prestataires tiers de s'identifier, de demander et de recevoir les données dont ils ont besoin et, le cas échéant, d'initier un paiement. Pour ce faire, le gestionnaire pourra choisir parmi deux moyens de transmission ; il peut soit développer une interface dédiée à ce transfert de données, soit permettre aux prestataires tiers de se servir de l'interface qui est mise à disposition de l'utilisateur pour accéder lui-même aux données de son compte.

La première option permet de mieux sécuriser l'accès aux données mais aura, cependant, des coûts plus importants pour le gestionnaire. De plus, s'il choisit la première option, le gestionnaire devra s'assurer que l'interface dédiée soit tout autant performante et disponible

[51] EBA, p.4.
[52] *Ibid.*

que l'interface mise à disposition du client[53], ce qui représente des complications supplémentaires.

Dans la deuxième option l'utilisateur se connecte via l'interface qu'il utilise habituellement, par exemple via la plateforme *Ebanking.* Une fois que l'utilisateur s'est connecté, le prestataire tiers pourra y extraire les informations dont il a besoin et y initier un paiement. Cette solution a l'avantage que le gestionnaire de compte n'a pas à développer une nouvelle interface. Néanmoins, dite solution peut poser des problèmes de sécurité[54]. Cette option peut également être contraire au principe de minimisation des données[55] car le prestataire a accès à plus de données qu'il a besoin pour l'exécution de ses services.

5. Respect de la protection des données

L'article 94 PSD II[56] précise que tout traitement de données à caractère personnel qui a lieu dans le cadre de la directive doit être conforme au RGPD.

Le prestataire de services doit donc veiller à respecter les principes du RGPD, notamment les principes de licéité, de bonne foi, de responsabilité, de transparence et de minimisation[57].

Dans le cadre de ce travail, nous nous limiteront à l'analyse de quelques problématiques spécifiques pouvant survenir lors de la fourniture de services de paiement par des tiers.

5.1. Licéité du traitement

En premier lieu, il convient de déterminer sur quel motif de l'article 6 par. 1 RGPD se fonde le prestataire de paiement tiers pour traiter les données de l'utilisateur. Dans le cadre de l'exécution de services de paiement par un tiers, le client souhaite obtenir une prestation qui requiert que ses données soient communiquées et traitées par le prestataire. Le traitement de données s'inscrit donc dans une relation contractuelle[58] entre le prestataire externe et l'utilisateur. Ce traitement est nécessaire à l'exécution dudit contrat car le prestataire de services d'initiation de paiement ou de services d'information sur les comptes ne peut vraisemblablement pas offrir ses services sans pouvoir accéder aux données, respectivement les traiter[59]. Le traitement de données opéré par le prestataire tiers qui a lieu dans le cadre de la PSD II se fonde sur l'article 6 par. 1 let. b) RGPD[60].

En outre, l'article 94 par. 1 PSD II mentionne la nécessité pour les États membres d'adopter une législation autorisant un traitement de données à des fins de préventions des fraudes dans le domaine des paiements. Un traitement supplémentaire qui est fondé non pas sur les besoins liés à l'exécution d'un contrat mais sur les obligations légales en matière de prévention des fraudes est donc possible.

---

[53] Article 32 RTS.

[54] VAN DER KROFT / KUIJSTEN

[55] EBF, *Guidance* p.85; EBF, *Response to EDPB interplay consultation*, pp. 14-15; ESSEBIER/BOURGEOIS, p. 120.

[56] A noter qu'en vertu de l'article 33 PSD II, l'article 94 ne s'applique pas aux services d'information sur les comptes.

[57] EDPB, *Interplay*, pp. 21-26.

[58] Voir Considérant n° 87 PSD II.

[59] EDPB, *Interplay*, pp. 9-10; Avis contraire : EBF, Response to EDPB interplay consultation, pp. 5-7.

[60] Le prestataire tiers qui souhaiterait effectuer un traitement qui dépasse les besoins issus de la fourniture des services tels que compris dans le contrat pourra le faire qu'avec le consentement de l'utilisateur ou de par une obligation légale. De plus, les articles 66 par. 3 let. g) et 67 par. 2 let. f) PSD II empêche le prestataire tiers d'effectuer un traitement qui s'éloigne du but initial. Voir: EDPB, *Interplay*, pp.11-12.

Finalement, s'agissant du fondement sur lequel s'appuie le gestionnaire du compte pour transférer les données du client au prestataire tiers, il y a lieu de rappeler que les article 66 et 67 PSD II imposent au premier nommé de donner au prestataire tiers l'accès aux données du compte si l'utilisateur le demande. Les États membres se doivent d'ailleurs d'adopter des législations concrétisant ces principes. Le transfert de données n'est donc pas issu d'une relation contractuelle ou du consentement de l'utilisateur mais d'une obligation légale, en vertu de l'article 6 par. 1 let. c) RGPD[61].

5.2. Consentement explicite de l'article 94 PSD II

L'article 94 par. 2 *in fine* PSD II établit également que l'utilisateur doit consentir explicitement à ce que le prestataire de paiement ait accès, traite et enregistre les données personnelles nécessaires à l'exécution des services de paiements. La notion de « consentement explicite » se distingue de la notion homonyme du RGPD[62]. En effet, comme nous l'avons vu[63], le traitement de données est fondé sur le fait qu'il est nécessaire à l'exécution d'un contrat, conformément à l'article 6 par 1 let. b) RGPD[64]. Le consentement explicite ici mentionné s'inscrit donc dans le cadre d'une relation contractuelle et ne porte ainsi pas sur le même objet que le consentement explicite de l'article 9 RGPD[65]. Il doit donc être interprété de manière indépendante[66]. Il y a lieu de noter que la PSD II ne détermine pas clairement quels sont les conditions à remplir pour exprimer un consentement explicite. Nous pouvant cependant supposer que la personne devra, au moins, être renseignée sur le fait que le prestataire puisse accéder à ses données bancaires, sur la nature exacte des données auxquelles il a accès, lesquels il compte collecter et sur l'usage qui en sera fait[67].

5.3. Traitement portant sur des catégories spéciales de données

Il y a ensuite lieu d'analyser brièvement la question des catégories spéciales de données[68] qui peuvent être traitées dans le cadre de la PSD II. En effet, certaines transactions peuvent révéler une certaine opinion politique, une orientation sexuelle, des informations sur la santé de la personne ou encore l'appartenance à un syndicat[69]. Tel est notamment le cas lorsque la personne effectue certains achats, un paiement à destination d'un parti politique ou encore à un médecin spécialisé dans certaines maladies[70]. Dans de pareilles circonstances, le gestionnaire du compte et le prestataire tiers sont donc amenés à traiter des données à caractères sensibles. Il sied de préciser que la nécessité d'exécuter un contrat n'est cependant pas un motif de licéité d'un tel traitement selon l'article 9 RGPD[71] ; un autre motif doit donc être trouvé.

Parmi les autres motifs envisageables, nous pouvons mentionner que, en vertu de l'article 9 par. 2 let. a) RGPD, la personne concernée peut donner son consentement explicite au traitement de

---

[61] EDPB, *Interplay*, p. 12.

[62] EDPB, *Interplay*, pp. 14-15; EDPB, *Letter* pp. 3-4; Avis contraire : EBF, *Response to EDPB interplay consultation*, pp. 7-8.

[63] *Cf. supra* Partie I, Chapitre 1, D, ch. 5.1.

[64] *Ibid*.

[65] *Ibid*.

[66] *Ibid*.

[67] *Ibid*.

[68] A noter que nous ne traitons pas ici des « données de paiement sensibles » lesquelles ont été discutées plus haut. *Cf. supra* Partie I, Chapitre 1, D, ch. 2.2.

[69] EDPB, *Interplay*, p 18.

[70] *Ibid*.

[71] *Ibid*.

ses données sensibles[72]. Contrairement à l'article 94 PSD II, le consentement ici mentionné devra remplir les conditions du RGPD[73]. L'utilisateur devra donc être libre de consentir au traitement ou non et devra avoir reçu les informations nécessaires à la formation de son opinion[74]. De plus, le consentement devra porter précisément sur le traitement de données à caractère sensible. Il pourra, par ailleurs, retirer son consentement à tout moment[75].

En outre, le prestataire de paiement pourra se fonder sur un intérêt public important en vertu de l'article 9 par. 2 let. g) RGPD[76]. Cependant, ce motif exige que l'État membre dont le responsable de traitement dépend adopte une législation dérogeant à l'article 9 RGPD. Il devra y être démontré en quoi le traitement est nécessaire et proportionné afin de protéger un intérêt public avec une importance systémique[77]. Dans les cas visés par la PSD II, nous pouvons soutenir que la prévention des fraudes de paiements est un intérêt suffisant pour que le prestataire soit autorisé à traiter des données à caractère sensible[78].

5.4. Traitement de données concernant des tiers

Lors du transfert de données qui a lieu dans le cadre de services d'initiation de paiement et d'information sur les comptes, se pose également la question du traitement de données de tiers. En effet, dans le cadre d'un paiement effectué entre deux personnes, les informations qui sont traitées pour l'un, comprennent également les données personnelles de l'autre, qui doit donc être considéré comme un tiers au traitement[79]. Il y a donc lieu de déterminer sur quelle base ce traitement se fera et quel usage pourra en être fait par le prestataire tiers.

Aucune relation contractuelle n'existe entre le tiers et le prestataire de service dans l'hypothèse précitée[80]. Néanmoins, ce dernier dispose d'un intérêt légitime à traiter ces données puisqu'il désire pouvoir offrir ses services à l'utilisateur[81]. Conformément à l'article 6 par. 2 let. f) RGPD, même si justifié par un intérêt légitime, le traitement ne doit pas résulter en une atteinte pour la personne concernée[82]. Or, comme la PSD II émet des règles strictes visant à protéger les consommateurs d'un usage excessif de leurs données, le tiers n'a que peu de risque de subir une telle atteinte[83]. En effet, le prestataire tiers ne pourra, selon la PSD II, de toute manière pas utiliser les données pour un autre motif que celui de fournir les services de paiement à l'utilisateur[84].

---

[72] EDPB, *Interplay*, pp. 19-20.
[73] *Ibid.*
[74] Article 7 RGPD.
[75] EDPB, *Interplay*, p.24.
[76] EDPB, *Interplay*, p 19.
[77] *Ibid.*
[78] *Ibid.;* Avis contraire : EBF, *Response to EDPB interplay consultation*, p.10.
[79] EDPB, *Interplay*, p.16; EDPB, *Letter*, pp.2-3.
[80] *Ibid.*
[81] *Ibid*.
[82] *Ibid.*
[83] *Ibid.*
[84] *Cf. supra* Partie I, Chapitre 1, D., ch.2-3

5.5. Principe de minimisation des données

Le prestataire tiers devant respecter le principe de minimisation des données de l'article 5 par. 1 let. c) RGPD, il sied de déterminer plus précisément son étendue dans le contexte de l'Open Banking[85].

Tout d'abord, le principe de minimisation des données est respecté lorsqu'un responsable de traitement ne traite pas plus de données que ce qui est nécessaire pour atteindre le but recherché[86]. En combinaison avec les principes de *Privacy by Design* et de *Privacy by Default,* tous deux découlant de l'article 25 RGPD, cela implique que le responsable du traitement doit minimiser les traitements qu'il effectue dès la collecte des données[87].

Dans le cadre de la PSD II, le prestataire de services externe ne doit extraire que les données qui sont essentielles à l'exécution des services qu'il propose[88]. À moins que cela soit ne soit nécessaire, il ne peut ainsi ni collecter les données relatives à des tiers qui ne sont pas pertinentes[89], ni obtenir les descriptions détaillées de paiement, ni demander des données trop anciennes pour être utiles[90]. De plus, il doit s'assurer que les données ne sont pas conservées sur une trop longue période[91].

Pour veiller au respect de ce qui précède, *le Comité Européen de la Protection des Données* a suggéré que le gestionnaire de compte adopte des outils digitaux assurant que les prestataires tiers se limite à n'extraire que les données qui leurs sont indispensables[92]. Cette proposition a été critiquée par l'*European Banking Federation* qui l'estime contraire à la PSD II. En effet selon elle, l'instrument précité n'attribue aucune responsabilité au gestionnaire de compte de mettre en œuvre une surveillance des données transmises au tiers ou, le cas échéant, de refuser un accès aux données qui soit contraire au principe de minimisation[93].

E. Conclusion intermédiaire

La PSD II relève d'une importance majeure dans le contexte de l'*Open Banking* car elle permet à un client de partager les données de son compte de paiement avec un tiers et d'exiger l'exécution d'un paiement initié par un prestataire tiers. De plus, les banques sont encouragées à adopter des interfaces dédiées comme moyen de transmission des données. Cela implique que les banques vont probablement développer des *API* afin de remplir leurs obligations, ce qui va grandement contribuer au développement de l'*Open Banking.* En effet, les banques qui choisissent de développer une infrastructure dédiée à l'ouverture du compte sera plus encline à l'utiliser dans les cas qui ne relèvent pas de la PSD II. Selon nous, la PSD II a donc grandement aidé l'adoption de l'*Open Banking* comme nouveau modèle économique.

Cependant, comme nous l'avons vu[94], le champ d'application de la PSD II est limité à la fourniture de deux services spécifiques liés à l'exécution de paiements et ne garantit que l'accès aux données portant sur un compte de paiement, excluant ainsi les informations relatives à un

---

[85] EDPB, *Interplay,* p.21-22.
[86] *Ibid.*
[87] *Ibid.*
[88] *Ibid.*
[89] *Cf. supra* Partie 1, Chapitre 1, D., ch.5.4.
[90] *Ibid.*
[91] *Ibid.*
[92] *Ibid.*
[93] EBF, *Response to EDPB interplay consultation*, p.13.
[94] *Cf. supra* Partie I, Chapitre 1, C., ch. 1.

compte d'épargne. Il en résulte que la PSD II ne s'applique pas à un bon nombre de services et innovations issues du développement de *l'Open Banking*. À titre d'exemple, nous pouvons imaginer une société offrant un service de *credit scoring* grâce à l'accès direct aux informations bancaires du client. N'entrant pas dans le champ d'application de la PSD II, un tel prestataire se verrait refuser l'accès aux données du client, quand bien même celui-ci y consent. Cet exemple illustre les raisons pour lesquelles la PSD II ne saurait être l'unique fondement juridique à l'*Open Banking.*

CHAPITRE 2 : LE DROIT A LA PORTABILITE DES DONNEES

A. Généralités

La PSD II ne couvrant pas l'intégralité des services nécessitant un accès aux données bancaires de l'utilisateur, il sied d'analyser plus précisément le droit à la portabilité des données régi à l'article 20 RGPD, qui – dans le contexte de *l'Open Banking* – peut être un fondement pour à l'utilisateur afin d'exiger de sa banque qu'elle transmette des données à un prestataire externe. En effet, le droit à la portabilité permettant à un utilisateur d'exiger d'un responsable de traitement de lui transmettre ou de transmettre à un tiers les données le concernant, il y a lieu d'analyser dans quelle mesure ce droit peut être utilisé, quelles en sont les limites et, en dernier lieu, de déterminer plus précisément sa portée dans le contexte de l'*Open Banking.*

B. Champ d'application territorial

La portabilité des données étant un droit issu du RGPD, il y a lieu de rappeler les situations dans lesquelles le règlement est applicable. Ce point ne soulevant que peu de problèmes dans la pratique, nous le traiterons de manière succincte.

En vertu de son article 3, le RGPD s'applique premièrement en raison du lieu auquel un responsable du traitement ou un sous-traitant est rattaché. En effet, toute personne, qui traite des données personnelles, établie sur le territoire de l'Union Européenne est soumise au RGPD[95]. Ensuite, une application extraterritoriale du règlement peut être reconnue aux responsables de traitement qui visent le marché de l'Union, soit car ils offrent des produits et des services à des personnes concernées se trouvant sur le territoire de l'UE, soit car ils analysent le comportement de ces personnes[96].

Dans le cadre de l'*Open Banking*, le RGPD est applicable dans les deux hypothèses suivantes. D'une part, lorsqu'une personne située en dehors des frontières de l'UE souhaite accéder à des informations détenues par un gestionnaire de compte établi au sein du territoire de l'Union. D'autre part, lorsqu'une personne concernée se trouve dans l'UE souhaite accéder aux informations détenues par un gestionnaire de compte se situant en dehors des frontières de l'Union[97].

[95] MÉTILLE/ACKERMANN, p.80.

[96] MÉTILLE/ACKERMANN, p.82-88, BÜHLMANN / REINLE, pp. 8-10.

[97] A noter que le lieu d'où le prestataire de service tiers opère importe peu dans le contexte de la portabilité des données car il n'est pas le titulaire du droit. En effet, la personne concernée pourra recevoir ses données et les transmettre à un prestataire tiers, indépendamment du fait que celui-ci soit soumis au RGPD ou non.

C. Champ d'application matériel

1. Données concernées

1.1. Données à caractère personnelle portant sur la personne concernée

En vertu de l'article 20 par. 1 RGPD, le droit à la portabilité ne peut que porter sur des données à caractère personnel qui se rapportent à la personne concernée.

La notion de « données à caractère personnel » renvoie à l'article 4 par. 1 point 1 RGPD qui fixe le champ d'application matériel du Règlement. Une donnée revêt un caractère personnel lorsqu'elle porte sur une personne physique identifiée ou identifiable[98]. Les données anonymisée ainsi que les données relatives aux personnes morales ne peuvent ainsi pas faire l'objet d'une demande de portabilité[99].

Dans le contexte de *l'Open Banking* et au vu de ce qui précède, il est possible de considérer les informations de comptes des personnes privées comme des données à caractère personnel. Cependant, les données de personnes morales ne rentrent pas dans le champ d'application du RGPD et ne peuvent pas– selon nous –être transférées au prestataire de service sur la base du droit à la portabilité des données. Cet élément est une différence majeure avec la PSD II, qui, elle, inclut dans son champ d'application les données des personnes morales[100].

L'article 20 par. 1 RGPD précise ensuite que les données ne doivent porter que sur la personne qui fait la demande de portabilité. Cependant, il n'est pas rare qu'un fichier de données sur la personne faisant la demande contienne également des données de tiers. Le GR29 a précisé que lorsque les données de tiers concernent également la personne concernée, elles peuvent être comprises dans les données à transférer[101]. En revanche, les données sont ensuite transmises à un autre responsable de traitement, celui-ci ne pourra utiliser les données des tiers en portant atteinte à leurs droits, à moins de détenir un intérêt prépondérant justifiant un tel traitement[102].

Ce dernier point relève d'une importance particulière pour la mise en œuvre de l'*Open Banking*. En effet, il est difficile d'imaginer une quelconque utilité pour un client de recevoir l'historique de ses transactions, sans que le fichier ne fasse mention des personnes physiques ou morales à qui ce dernier a effectué des paiements.

En conclusion, les données concernées par le droit à la portabilité sont celles qui porte sur la personne physique identifiée ou identifiable qui en fait la demande, mais également celles de tiers, dans la mesure où elles sont pertinentes.

1.2. Données fournies par la personne concernée

Conformément à l'article 20 par. 1 RGPD, afin de faire l'objet du droit à la portabilité, les données doivent avoir été « fournies » au responsable du traitement par la personne concernée[103].

L'étendue exacte de cette notion n'est cependant pas clairement définie. Une interprétation stricte du terme « fournies » exclurait toute donnée qui n'aurait pas été transmise directement

[98] Considérant n°26 RGPD.
[99] GR29, *WP242*, p. 11.
[100] *Cf. supra* Partie I, Chapitre 1, C, ch 2.
[101] GR29, *WP242*, p. 11.
[102] *Ibid*., *Cf. supra* Partie I, Chapitre 2, C, ch. 1.3.
[103] SYDOW, p. 534., HERBST p.484.

et activement par la personne concernée. Or, un grand nombre de données traitées par les responsables de traitement résultent de l'observation du comportement de la personne concernée. Tel est notamment le cas des historiques de connexions ou encore des registres d'activités[104]. C'est pourquoi le GR29 a opté pour une interprétation plus large qui comprend également les données issues de l'observation de l'utilisateur[105]. Néanmoins, les informations qui sont déduites ou dérivées de l'analyse de ce comportement ne sont, quant à elles, pas incluses dans le droit à la portabilité[106]. Cette distinction entre les données observées et analysées peut se révéler difficile et devra faire l'objet d'une analyse au cas par cas[107].

Dans le contexte bancaire, les données fournies par le client rentrent donc dans le cercle des données concernées par le droit à la portabilité. Cela inclut, selon nous, les ordres de paiement ou les informations d'identification, telles que l'adresse, une copie de sa carte d'identité, son adresse *email* ou encore son numéro de téléphone. L'historique des transactions, qui, quant à lui, est issu de l'observation du comportement de la personne concernée, est également inclus dans le champ d'application des personnes concernées, alors que les informations relatives à l'évaluation de la solvabilité du client, par exemple, résultent de l'analyse de son comportement et sont donc à exclure[108].

Nous pouvons cependant nous demander si la catégorisation et la description des opérations de paiement[109] relèvent d'une observation ou d'une analyse des données du client. Afin de répondre à cette question, il y a lieu de distinguer deux situations. Selon nous, si – lors du paiement – le client peut choisir une catégorie, il faut comprendre que celle-ci a été fournie au responsable du traitement car elle résulte d'une action prise par la personne concernée. Cependant, si la catégorisation est opérée entièrement par le responsable du traitement, notamment lors de paiements effectués avec une carte de paiement, nous sommes d'avis que la catégorisation dépasse la simple observation du comportement de l'utilisateur car une valeur supplémentaire est ajoutée à la donnée. La catégorie rattachée à la transaction résulte d'une analyse et ne saurait ainsi rentrer dans le champ d'application du droit à la portabilité des données.

De plus, l'*European Banking Federation* a soulevé la question de la surveillance des données liée à la lutte contre le blanchiment d'argent (ci-après « *AML* ») et de la lutte contre les fraudes[110]. Lors de cette surveillance, la banque va observer, notamment, le flux des transactions et détecter les opérations suspectes. Les informations qui résultent de cette surveillance résultent d'une analyse qui dépasse la simple observation d'un comportement. Elles ne sont donc pas à inclure lors d'un transfert de données fondé sur le droit à la portabilité[111].

En conclusion, le droit à la portabilité se limite aux données fournies activement par la personne concernée ou qui résultent de l'observation de son comportement. Les informations issues d'une analyse sont, quant à elles exclues. Le cercle des données à transmettre comprend donc les informations sur le compte, les ordres de paiement et l'historique des transactions.

---

[104] GR29, *WP242* p.12.

[105] GR29, *WP242*, pp. 11-12, Avis contraire : EBF, *Comments on WP29 Portability Guidelines*, pp. 3-5.

[106] *Ibid*.

[107] REICHLIN, p.406.

[108] GR29, *WP242* p.12.

[109] Nous faisons référence ici aux services d'analyse des dépenses, plus communément appelés « *Personal finance manager* » (ou « PFM ») que certaines banques proposent. Ceux-ci reposent sur la catégorisation des dépenses sous différentes rubriques, telles que « loisir », « ménage » ou encore « transport ».

[110] EBF, *Comments on WP29 Guidelines*, p.4.

[111] GR29, *WP242*, p. 12.

1.3. Données dont le transfert ne porte pas atteinte aux droits et libertés de tiers

En vertu de l'article 20 par. 4 RGPD, le droit à la portabilité ne peux nuire aux droits et libertés de tiers[112]. Or, comme mentionné précédemment, il se peut que les données transmises dans le cadre d'une demande de portabilité portent également sur un tiers[113]. Il faudra donc s'assurer que le nouveau responsable traite les données du tiers en respectant l'article 6 RGPD. A cet égard, il est admis que le responsable de traitement a un intérêt légitime, conformément à l'article 6 par. 2 let. f) RGPD, à traiter les données du tiers dans le but d'offrir un service à l'utilisateur initial[114]. S'il souhaite traiter les données du tiers pour d'autres motifs, par exemple à des fins marketing, il devra soit obtenir le consentement de la personne, soit se fonder sur un autre motif de l'article 6 RGPD. De plus, les autres droits du tiers – tel que le droit d'accès issu de l'article 13 RGPD – doivent également être respectés[115].

Finalement, nous pouvons mentionner les droits de la propriété intellectuelle et des secrets d'affaires de tiers, lesquels pourraient également être atteints lors d'un transfert de données fondé sur une demande de portabilité[116].

Dans le contexte de l'*Open Banking*, l'historique des transactions d'un compte comprend des informations relatives au tiers avec qui l'utilisateur a interagi. Il faudra donc s'assurer que le prestataire tiers n'utilise pas ces données pour un autre but que celui d'offrir les services souhaités par l'utilisateur. Le GR29 a cependant estimé que le risque d'atteinte dans le cadre des données de tiers liées à un compte en banque est faible[117].

2. Traitements concernés

2.1. Traitement de données fondé sur consentement de la personne concernée ou nécessaire à l'exécution d'un contrat

Le cercle des données pouvant faire l'objet de la demande de portabilité n'est pas seulement déterminé par la nature de celles-ci mais également par le traitement dont elles ont fait l'objet[118].

L'article 20 par. 1 let. b) RGPD précise que seules les données qui ont fait l'objet d'un traitement fondé, soit sur le consentement de l'utilisateur (article 6 par. 1 let. a) RGPD), soit sur la nécessité du traitement pour l'exécution d'un contrat (article 6 par. 1 let. b) RGPD), rentrent dans le champ d'application du RGPD. Les données traitées sur la base des autres motifs justificatifs des articles 6 RGPD, notamment l'accomplissement d'une tâche publique, la poursuite d'un intérêt légitime et le respect d'une obligation légale, sont donc exclus du droit à la portabilité des donnée[119]s. A noter également que, selon nous, les données relevant d'une catégorie spéciale doivent avoir été traitées sur la base du consentement explicite, conformément à l'article 9 par. 2 let. a) RGPD, de l'utilisateur pour rentrer dans le champ d'application du droit à la portabilité, car la nécessité du traitement pour l'exécution d'un contrat ne fait pas partie des dérogations de l'article 9 RGPD[120]. Les informations médicales

---

[112] SYDOW, p. 535, HERBST p.486.
[113] *Cf. supra* Partie I, Chapitre 2, C, ch. 1.2.
[114] GR29, *WP242*, pp. 13-14; REICHLIN, p.406; EBF, *Comments on WP29 Portability Guidelines*, p. 7.
[115] *Ibid.*
[116] GR29, *WP242*, p. 15.
[117] *Ibid.*, p. 14.
[118] A noter que nous traitons ici non pas du traitement dont elles feront l'objet à la suite du transfert à la personne concernée mais bien du traitement qui leur sont appliquées par le responsable de traitement initial.
[119] SYDOW, p. 534., HERBST p.485.
[120] *Cf. supra* Partie I, Chapitre 1, D., 5.3.

fournies à un médecin, par exemple, qui n'auraient pas fait l'objet d'un consentement explicite ne peuvent rentrer dans le champ d'application du droit à la portabilité, alors que les informations fournies à un fiduciaire qui ont été traitées sur la base d'un contrat le peuvent.

Dans le contexte bancaire, cette condition soulève la question des données traitées dans le cadre des obligations réglementaires qui incombent aux banques. Le traitement d'informations qui seront traitées afin de répondre à ces obligations, notamment les informations relatives à la lutte contre le blanchiment d'argent, sera fondé sur le respect d'une obligation légale (article 6 par. 1 let. c) RGPD) et ne seront ainsi pas comprises dans le champ d'application du droit à la portabilité.

Ensuite, les données bancaires qui portent sur la religion, les opinions politiques, l'appartenance syndicale, l'orientation sexuelle ou encore des données relatives à la santé de la personne concernée[121] et qui ont été traitées sur la base du consentement explicite de l'utilisateur, conformément à l'article 9 RGPD, peuvent être inclues dans le droit à la portabilité.

Finalement, la condition posée par l'article 20 par. 1 let. b) RGPD ne fait pas obstacles aux autres informations usuellement comprises dans l'*Open Banking*, c'est-à-dire les informations sur le compte et l'historique des transactions car celles-ci ont été transmises dans le cadre de l'exécution du contrat ou sur la base du consentement de l'utilisateur.

En conclusion, le droit à la portabilité des données inclut les données transmises sur la base du consentement de la personne concernée et celles transmises afin d'exécuter un contrat. Sont alors exclues, sur la base de cette condition, les données traitées dans le but de respecter les nombreuses réglementations bancaires.

2.2.Traitement automatisé

La deuxième et dernière condition limitant le champ d'application du droit à la portabilité a trait à la forme du traitement qui est opéré.

En vertu de l'article 20 par. 1 let. b), ne sont comprises dans le droit à la portabilité que les données qui ont fait l'objet d'un traitement à l'aide d'un procédé automatisé[122]. Il n'est pas clairement défini dans le RGDP ce que constitue un « procédé automatisé » ou non[123]. Nous pouvons cependant supposer que cela se réfère à un traitement informatisé[124]. Les traitements qui résultent d'un travail manuel effectué par une personne physique sont donc exclus, de sorte que les fichiers papiers ou les documents contenus sur une clé USB, par exemple, ne pourront pas faire l'objet d'une demande de portabilité[125]. Il y a lieu de préciser que la terminologie ici utilisée ne doit pas être confondue avec la notion de « décision automatisée » également traitée par le RGPD.

Quoi qu'il en soit, cette condition relative à l'automatisation du traitement ne fera que rarement obstacle à l'Open Banking car la plupart des données bancaires font l'objet d'un traitement automatisé.

---

[121] *Ibid.*

[122] GR29, *WP242*, p. 11, REICHLIN, p.407, SYDOW, p. 534., HERBST p.485.

[123] SCHREY, p.144.

[124] REICHLIN, p.407.

[125] *Ibid*.

3. Conclusion intermédiaire

Au vu de ce qui précède, nous pouvons définir que le cercle des données à inclure dans le champ d'application du droit à la portabilité comprend les données qui portent sur la personne physique concernée et qui ont été fournies par cette dernière ou doivent résulter de l'observation de son comportement. De plus, le transfert desdites données ne doit pas porter atteinte à des tiers et elles doivent avoir fait l'objet d'un traitement automatisé qui soit fondé sur le consentement de la personne concernée ou qui soit nécessaire à l'exécution d'un contrat. Ainsi, les données qui résultent d'une analyse faite par le responsable du traitement, celles qui ont été traitées sur la base d'une obligation légale ou qui se fondent sur un intérêt légitime du responsable de traitement, les données qui sont détenues sur un document papier ou une clé USB et enfin, les données de personnes morales ne rentrent donc pas dans le champ d'application du droit à la portabilité des données.

Dans le contexte de l'*Open Banking,* le tableau récapitulatif ci-dessous tend à offrir une vue d'ensemble des données qui seront à inclure dans le cadre d'une demande de portabilité :

Figure 1 - Champ d'application du droit à la portabilité

	Portant sur la personne physique concernée	Fournie par la personne concernée ou observée	Transfert ne portant pas atteinte aux droits de tiers	Traitement fondé sur le consentement ou un contrat	Traitement automatisé	Rentre dans le champ s'application du droit à la portabilité
Données d'identifications (nom, IBAN, etc.)	✓	✓	✓	✓	✓	✓
Solde du compte	✓	✓	✓	✓	✓	✓
Historique des transactions	✓	✓	✓	✓	✓	✓
Ordre de paiements permanent	✓	✓	✓	✓	✓	✓
Informations KYC, due diligence & AML	✓	✗	✓	✗	✓	✗
Catégorisation des paiement (PFM)	✓	✗	✓	✓	✓	✗

Les données d'identification – tels que le nom, le prénom, et l'adresse – le solde du compte, l'historique des transactions et les ordres de paiements permanents initiés par la personne concernée remplissent les conditions requises pour rentrer dans le champ d'application du droit à la portabilité. Cependant, les données qui sont traitées dans le cadre des obligations réglementaires qui incombent aux banques, notamment mais pas exclusivement les informations relatives au *KYC,* due diligence et au système de lutte contre le blanchiment d'argent sont exclues du champ d'application du droit à la portabilité car, d'une part, leur traitement se fonde sur des obligations légales et, d'autre part, elles résultent d'une analyse de la banque qui est opéré issues d'une analyse de la part de la banque. Ensuite, la catégorisation des paiements effectués par la banque ne sont pas incluses dans le droit à la portabilité car elles ne sont, sauf exception, pas fournies par la personne concernée. Enfin, les comptes détenus par des personnes morales ne peuvent également pas faire l'objet d'une demande de portabilité fondé sur l'article 20 RGPD.

D. Contenu du droit à la portabilité des données

1. Droit de recevoir les données

Le droit à la portabilité des données se sépare en deux droits distincts ; le droit de recevoir ses données et le droit de les faire transmettre à un tiers.

Conformément à l'article 20 par. 1 RGPD, la personne concernée a le droit de recevoir de la part du responsable du traitement – dans un format structuré, couramment utilisé et lisible par une machine – les données rentrant dans le champ d'application de la portabilité[126]. Le considérant n° 68 RGPD précise, notamment, que le droit à la portabilité tend à ce que la personne concernée puisse garder le contrôle sur les données la concernant qui ont été transmises à un responsable de traitement[127]. En ayant le droit de recevoir une copie de ses données, elle pourra ainsi les conserver et les utiliser comme bon lui semble. À la suite de la réception de ses données, la personne concernée doit donc être libre d'en faire un usage privé, de les transmettre à un tiers ou d'en faire tout autre usage qui lui semblerait opportun[128].

Bien que ce droit se rapproche du droit d'accès de l'article 15 RGPD, le champ d'application matériel, la nature des deux droits et le format utilisé pour transmettre les données diffèrent[129]. Le droit d'accès a trait à informer la personne concernée des traitements qui sont opérés alors que le droit à la portabilité a pour but qu'une personne puisse utiliser librement ses propres données. A noter également que le droit à la portabilité n'a pas d'effet sur le droit à l'effacement de l'article 17 RGPD[130].

2. Droit de demander la transmission des données à un tiers

La personne concernée peut également demander au responsable du traitement de transférer ses données directement à un autre responsable de traitement[131].

Prévu par l'article 20 par. 2 RGPD, le droit de voir ses données transmises à un tiers comporte cependant une condition supplémentaire par rapport au droit de recevoir ses données, tel qu'il a été analysé au sous-chapitre précédent. En effet, l'article 20 par. 2 RGPD stipule que le droit de voir ses données transmises à un tiers existe uniquement lorsque cela est techniquement possible. La notion « techniquement possible » n'ayant pas de définition légale claire, il y aura lieu de déterminer au cas par cas, si cette condition est remplie, notamment en effectuant une analyse des moyens techniques usuellement utilisés dans le secteur d'activité du responsable en question[132]. Cependant, le responsable de traitement ne pouvant faire volontairement obstacle[133] au droit à la portabilité, un refus dont le fondement repose sur une impossibilité technique de satisfaire la demande ne doit être admis que de manière restrictive[134].

Par ailleurs, il convient de préciser que la demande de portabilité peut tout à fait être effectuée par le prestataire tiers au nom et pour le compte de la personne concernée[135]. Bien que la

---

[126] GR29, *WP242*, p. 4; REICHLIN, p. 403, SYDOW, p. 533-534., HERBST p.487-488.
[127] *Ibid*.
[128] GR29, *WP242*, p. 5; REICHLIN, p.404.
[129] GR29, *WP242*, p. 5; REICHLIN, p.405.
[130] GR29, *WP242*, pp. 8-9; REICHLIN, p.413.
[131] SYDOW, p. 534., HERBST p.489-490.
[132] GR29, *WP242*, p.19; REICHLIN, p.410.
[133] *Cf. infra* Partie I, Chapitre 2, E, ch. 3.
[134] REICHLIN, p.411.
[135] GR29, *WP242*, p. 23.

titularité du droit reste en main de l'utilisateur des services, ce moyen de faire peut faciliter la mise en œuvre des demandes, tant pour l'utilisateur que pour les responsables de traitement[136].

Dans le contexte de l'*Open Banking,* c'est sur la base de ce droit que l'utilisateur va demander à la banque de transmettre les données de son compte à un prestataire tiers. Au vu de l'informatisation des données bancaires, nous sommes d'avis qu'il sera difficile, voire insoutenable, pour la banque de démontrer qu'un transfert à un tiers est techniquement impossible.

E. Modalités du transfert de données

1. Devoir d'information

Le droit à la portabilité étant un droit de la personne concernée, les règles de l'article 12 RGPD sont applicables. Celles-ci comprennent notamment le devoir d'information.

Ainsi, en vertu de l'article 12 RGPD, le responsable du traitement devra indiquer à la personne concernée l'existence du droit à la portabilité, les modalités à respecter pour son exercice, ainsi que la différence entre le droit à la portabilité et le droit d'accès[137]. En effet, une distinction claire entre le droit à la portabilité et les autres droits de la personne concernée doit être faite[138], puisque le cercle des données rentrant dans le champ d'application de la portabilité étant plus restreint que les autres droits, le responsable du traitement ne peut faire l'économie de cette distinction. Ensuite, les informations transmises doivent être exprimées de façon concise, transparente, compréhensible, accessible et en des termes clairs et simples pour la personne concernée[139]. Les informations doivent être transmises au moment de la collecte de données si celles-ci sont collectées directement auprès de la personne concernée[140]. Cela vaut aussi pour les données dites « observées[141] ». En revanche, lorsque les données sont collectées auprès d'une autre personne, le devoir d'information doit être rempli au plus tard dans le mois qui suit la collecte[142]. Finalement, le GR29 encourage les responsables de traitement à fournir une nouvelle fois les informations relatives au droit de la portabilité lorsque la personne concernée ferme son compte[143].

Au vu de ce qui a été exposé ci-dessus, les banques doivent indiquer à leurs utilisateurs quelles données seront comprises dans le droit à la portabilité et sous quel format elles seront transmises.

2. Format structuré, couramment utilisé et lisible par machine

Afin de répondre de manière satisfaisante à une demande de portabilité, un responsable du traitement doit fournir les données dans un format structuré, couramment utilisé et lisible par

---

[136] Il y a lieu de préciser que, selon nous, la situation dans laquelle des données sont transmises à un tiers alors que la personne concernée n'était pas à l'origine de la demande de portabilité constitue une fuite de donnée. Le responsable de traitement doit donc s'assurer de la volonté réelle de la personne concernée et l'authentifier correctement.

[137] GR29, *WP242*, pp. 15-16; REICHLIN, p.409.

[138] *Ibid*.

[139] *Ibid*.

[140] *Ibid*.

[141] *Cf. supra* Partie I, Chapitre 2, C, ch. 1.2.

[142] GR29, *WP242*, pp. 15-16; REICHLIN, p.409.

[143] *Ibid*.

machine. Ces conditions cumulatives n'étant pas clairement définies par l'article 20 RGPD, il sied d'y apporter quelques précisions.

Tout d'abord, un fichier répondra à l'exigence d'un « format structuré » lorsque celui-ci permet d'identifier les données que l'on souhaite utiliser et que l'on puisse les extraire les données qu'il contient[144].

Ensuite, conformément à l'article 20 par. 1 RGPD, le format du fichier devra être « couramment utilisé »[145]. Cette notion juridique indéterminée doit être interprétée au cas par cas. En effet, un format peut être couramment utilisé dans une industrie mais pas dans une autre. La portée exacte de cette condition sera donc différente selon le contexte dans lequel le responsable du traitement s'inscrit[146]. Cependant, le GR29 a établi que, dans les cas où aucune pratique courante s'impose, les données devront être transmise dans un format ouvert, tel que les fichiers XML, JSON ou CSV[147]. Les données devront également être accompagnées des métadonnées pertinentes[148]. Le GR29 recommande également aux différents secteurs économiques d'adopter des standards communs afin de faciliter les transferts[149].

Finalement, le format choisi devra être « lisible par machine[150] », c'est-à-dire qui permet à une application logicielle d'identifier, de reconnaître et d'extraire les données souhaitées[151].

En cas de doute sur le format à adopter en vue de satisfaire à ces conditions, les responsables de traitement doivent choisir le format qui permet au mieux à l'utilisateur de réutiliser les données qui lui sont transmises[152].

Le GR29 a suggéré deux moyens techniques qui remplissent les exigences fixées par les conditions précitées[153]. Ainsi le responsable du traitement peut, soit transmettre directement l'intégralité des données dans un format permettant d'extraire celles qui sont recherchées, soit mettre en place un mécanisme automatisé qui permet à la personne concernée d'extraire uniquement les données qu'elle juge pertinentes[154]. Cette deuxième solution vise à faciliter l'exécution d'une demande de portabilité tant lorsqu'elle concerne une quantité importante de données que lors d'un transfert à un responsable de traitement tiers[155].

Il convient cependant de préciser qu'il n'existe aucune obligation pour les responsables de traitement d'adopter des systèmes compatibles ou interopérables[156]. C'est-à-dire que le responsable du traitement transférant n'a pas l'obligation d'adopter un système informatique ayant la capacité de fonctionner avec le système informatique du destinataire. En effet, le considérant n° 68 se limite à encourager les responsables de traitement à adopter de tels systèmes[157]. Un responsable du traitement pourra donc choisir de simplement transmettre les

---

144 GR29, *WP242*, p.21; REICHLIN, p.411.
145 *Ibid*.
146 GR29, *WP242*, p.21; REICHLIN, P.412.
147 *Ibid*.
148 GR29, *WP242*, p.21.
149 *Ibid*.
150 *Ibid*.
151 *Cf. Considérant n° 21 de la directive 2013/37/EU du 26 juin 2013 ;* GR29, *WP242*, p.20-21; REICHLIN, p.411-412.
152 *Ibid*.
153 GR29, *WP242*, p.19-20; REICHLIN, p.412.
154 *Ibid.*
155 *Ibid.*
156 REICHLIN, p.408.
157 *Ibid.*

données requises à la personne concernée ou à un tiers sous la forme de son choix, sans avoir à offrir un accès à son service informatique ou sous la forme souhaitée. Les données peuvent donc être transmises, par exemple, au moyen d'un DVD, d'une clé USB ou par courriel alors que le destinataire des données utilise une application web pour les exploiter[158].

Finalement, il y a lieu de relever que – bien qu'il soit libre de choisir le format de son choix – le responsable du traitement ne peut pas volontairement faire obstacle au droit de la portabilité[159]. Le choix d'un format qui viserait à restreindre la possibilité pour le client d'en faire l'usage qu'il souhaite ou à en ralentir le transfert pourrait ainsi être considéré comme un obstacle au droit à la portabilité[160].

Comme nous l'avons vu[161], en ce qui concerne l'*Open Banking*, les prestataires de services tiers souhaitent obtenir un accès direct aux données bancaires du client. Or, conformément aux principes discutés ci-dessus, il n'existe pas d'obligation légale pour le responsable du traitement d'offrir un tel accès. Une banque pourrait alors, *a priori*, transmettre les données au client dans le format de son choix. Elle pourrait ainsi choisir, par exemple, de transmettre les données de la personne concernée en lui envoyant un fichier par courriel. Ce point est une des différences majeures avec les droits contenus dans la PSD II[162] et rend peu adaptée l'utilisation du droit à la portabilité comme fondement de l'*Open Banking*.

3. Interdiction de faire obstacle au droit à la portabilité

L'article 20 par. 1 RGPD précise également que le responsable du traitement ne peut pas faire obstacle au transfert de données.

Selon le GR29, les obstacles au droit à la portabilité des données se définissent comme toute action de nature technique, juridique ou financière visant à restreindre ou ralentir l'accès aux données, leur transfert ou la possibilité de les réutiliser[163]. Le responsable du traitement ne peut ainsi pas imposer, par exemple, un délai d'une longueur inexplicable pour le transfert des données, un paiement de frais ou encore le recours à un format volontairement inadéquat. Les motifs qui peuvent cependant justifier l'existence d'obstacles, sont, notamment, ceux concernant la sécurité du système informatique du responsable. Si de tels motifs devaient exister, il incomberait au responsable du traitement de prouver leur légitimité[164].

Il y a donc lieu de se demander si le refus d'une banque d'offrir un accès à l'infrastructure *API* mise en place dans le cadre de la PSD II au tiers à qui elle doit transmettre des données sur la base d'une demande de portabilité constitue un obstacle au sens de l'article 20 par. 1 RGPD. Cette question sera cependant traitée au Chapitre 2 de la deuxième partie de ce travail[165].

4. Délai pour transférer les données

La question du délai du droit à la portabilité est régie à l'article 12 par. 3 RGPD. Cet article stipule que le responsable du traitement devra fournir des informations sur les actions prises pour répondre à la demande « dans les meilleurs délais, mais au plus tard un mois après la

[158] GR29, *WP242*, p.17; REICHLIN, p.412.
[159] *Cf. infra* Partie I, Chapitre 2, E, ch. 3.
[160] *Cf. infra* Partie I, Chapitre 2, E, ch. 3.
[161] *Cf. supra* Partie I, Introduction, C.
[162] *Cf. supra* Partie I, Chapitre 1, D., ch.4.2.
[163] GR29, *WP242*, pp.18-19; REICHLIN, p.410.
[164] *Ibid*.
[165] *Cf. infra* Partie II, Chapitre 2, B.

réception de la demande ». Ce délai d'un mois pourra être étendu à trois mois lorsque la demande est particulièrement complexe ou qu'il y a de multiples demandes[166].

Néanmoins, il sied de rappeler qu'un retard injustifié dans la réponse faite à la demande de portabilité peut être constitutif d'un obstacle au sens de l'article 20 par. 1 *in fine* RGPD[167]. Le responsable du traitement devra donc répondre à la demande sans prendre plus de temps que ce qu'il lui est réellement nécessaire au vu des outils techniques dont il dispose.

Dans le cadre de *l'Open Banking*, l'utilisateur ou le prestataire de services tiers pourra recevoir les données au plus tard un mois après la demande, sauf si celle-ci est particulièrement complexe. Néanmoins, comme nous l'avons vu, la banque pourrait se voir reprocher de faire obstacle au droit de la portabilité si elle retarde volontairement le transfert de données. Tel pourrait notamment être le cas si elle dispose d'une infrastructure lui permettant de répondre à la demande immédiatement[168].

5. Sécurité des données

Conformément à l'article 5 par. 1 let. f) RGPD, le responsable du traitement doit s'assurer en tout temps que les données traitées sont correctement sécurisées et protégées contre les traitements illicites[169]. Ce principe doit être respecté même lors d'un transfert de données fondé sur le droit à la portabilité[170]. Dès lors, ce chapitre portera sur l'identification des risques éventuels et l'évaluation des mesures pouvant être prises pour les minimiser.

Il convient, à cet égard, de mentionner deux risques principaux. Le premier consiste en ce que les données ne parviennent pas à la personne concernée. Cela peut résulter soit d'un problème d'identification de cette dernière, soit de l'utilisation d'un moyen de communication pas sécurisé[171]. Dans la première hypothèse, le responsable du traitement peut minimiser le risque en mettant en place des systèmes d'authentification renforcés lors de la demande de portabilité[172]. La deuxième situation, quant à elle, peut être évitée en utilisant un chiffrement des données de bout en bout lors de la communication[173]. Le deuxième risque qui sera abordé dans la présente analyse, porte sur l'éventualité que les données – une fois transmises à la personne concernée ou au tiers – ne soient pas détenues dans un environnement sécurisé. Bien qu'il soit de la responsabilité de la personne concernée de s'assurer que ses données soient en sécurité, le responsable du traitement devra attirer l'attention de cette dernière sur le fait qu'il n'est plus lui responsable de la sécurité des données transférées[174].

Il y a lieu de mentionner que les mesures de sécurités adoptées par le responsable du traitement – notamment concernant la méthode d'authentification choisie – ne doivent faire obstacle de manière excessive au droit de la portabilité des données, notamment concernant la méthode d'authentification choisie.

---

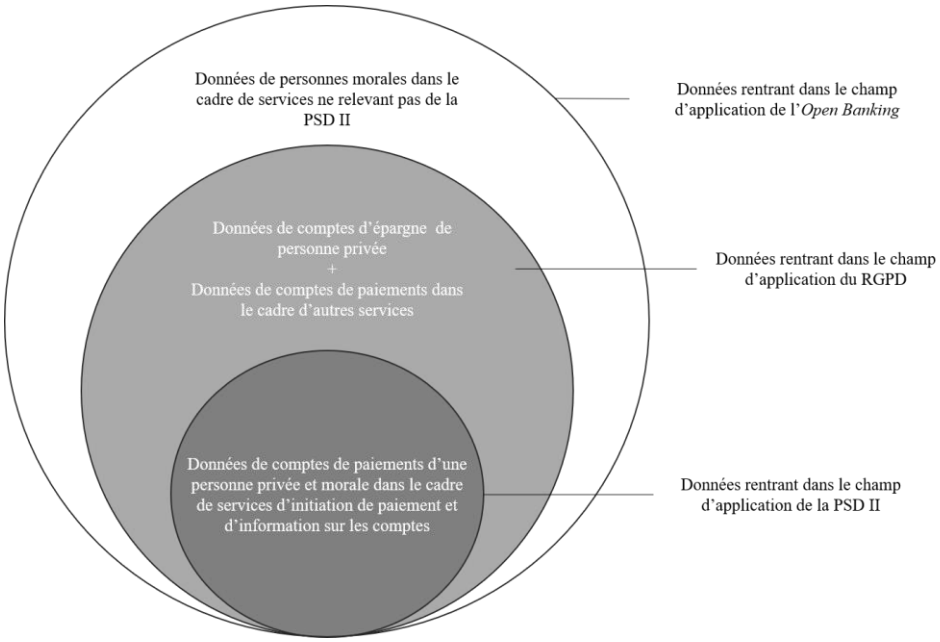
166 GR29, *WP242*, pp.17-18; REICHLIN, pp. 409-410.
167 GR29, *WP242*, p.20.
168 Ce point sera analysé dans la deuxième partie de ce travail. *Cf. Infra* Partie II, Chapitre 2, B, ch. 3.
169 GR29, *WP242*, pp.23-24; REICHLIN, p. 412; EBF, *Comments on WP29 Portability Guidelines,* p. 8.
170 *Ibid.*
171 GR29, *WP242*, pp.23-24; REICHLIN, p. 412.
172 *Ibid.*
173 *Ibid.*
174 *Ibid.;* Avis contraire: EBF, *Comments on WP29 Portability Guidelines,* pp. 8-9.

Concernant le secteur bancaire, l'*European Banking Federation,* a fait part de ses inquiétudes relatives à la sécurité des données dans le cadre de l'exercice du droit à la portabilité[175]. En effet, les données bancaires étant particulièrement sensibles, il existe une crainte que des acteurs mal intentionnés profitent de ce transfert pour s'introduire dans les systèmes informatiques de la banque et mettent à mal les données des autres utilisateurs[176]. Le secteur bancaire souhaiterait ainsi appliquer les standards de sécurité usuels pour le domaine. Or, des mesures de sécurités trop strictes pourraient être vues comme un obstacle au droit à la portabilité.

CONCLUSION INTERMEDIAIRE

Dans de cette partie nous avons pu déterminer que l'*Open Banking* se fonde principalement sur deux institutions issues du droit Européen. Le champ d'application de chaque loi peut être résumé de la manière suivante :

Figure 2 - Champ d'applications de la PSD II et du droit à la portabilité



D'une part la PSD II permet à un client de demander que ses données bancaires soient partagées avec un prestataire tiers et d'exiger de la banque qu'elle exécute des paiements qui émanent de ceux-ci. L'accès sera fourni au prestataire externe sous la forme d'une interface dédiée ou en l'autorisant à utiliser la plateforme généralement utilisée par les clients. Cependant, la PSD II ne s'applique que dans le cadre de services d'initiation de paiement et d'information sur les comptes, ne couvrant ainsi pas l'ensemble des services rentrant dans la définition de l'*Open Banking*.

D'autre part, le droit à la portabilité des données permet de demander à la banque de transmettre ses données de comptes d'épargne et de comptes de paiement à un prestataire tiers. Le choix du format de transmission est laissé libre au responsable de traitement, mais il ne pourra pas

[175] *Ibid.*
[176] *Ibid.*

volontairement faire obstacle au droit de l'utilisateur dans sa réponse. Par ailleurs, le droit à la portabilité ne peut être utilisé que par des personnes physiques.

Notons également que les droits issus de la PSD II sont plus adaptés dans le contexte de l'*Open Banking* – notamment grâce au fait qu'une interface *API* est recommandée et qu'il est possible d'exiger de la banque d'exécuter des paiements. Néanmoins, le droit à la portabilité peut se révéler fort pratique, notamment pour les cas qui ne tombent pas dans le champ d'application de la PSD II.

PARTIE II : ANALYSE DE QUESTIONS CHOISIES

CHAPITRE 1 : DEMANDE DE PORTABILITE RELEVANT DU CHAMP D'APPLICATION DE LA PSD II : APPLICATION DE QUELLES REGLES ?

A. Délimitation de la problématique

Dans le cadre de l'*Open Banking*, il se peut qu'une demande de portabilité fondée sur le RGPD relève également du champ d'application de la PSD II[177].

Cette problématique peut causer une difficulté en pratique puisque, sous le régime de la directive précitée, le prestataire tiers est soumis à des règles plus strictes que celles découlant du règlement européen. L'obligation d'avoir été agréé par l'autorité compétente d'un État membre[178] et l'utilisation qui peut être faite des données[179] sont des exemples types de cette dualité de règles inégales. Il convient donc de déterminer si le prestataire tiers confronté à une telle situation devra respecter les règles issues de la PSD II ou celles issues du droit à la portabilité[180].

B. Application de quelles règles ?

La première étape afin d'établir à quel instrument il convient d'avoir recours consiste à déterminer s'il demeure possible d'effectuer une demande de portabilité des données conformément aux dispositions du RGPD dans les cas rentrant dans le champ d'application de la PSD II. A cet égard, le GR29 a précisé que l'exercice du droit à la portabilité n'empêche pas l'utilisateur d'exercer d'autres droits qui sont à sa disposition, notamment les droits qui comportent des éléments similaires au droit à la portabilité[181]. Cependant, s'il est clairement défini que l'intention de l'utilisateur était d'exercer son droit à la portabilité des données, les règles du RGPD seront applicables à la demande[182]. Il conviendra cependant de déterminer au cas par cas dans quelle mesure les principes régissant les droits similaires au droit à la portabilité des données doivent, tout de même, être appliqués à la demande[183]. En revanche, lorsqu'il est clair que l'intention de l'utilisateur consistait à exercer un autre droit que celui de la portabilité,

---

[177] MILSHINA ET AL., p. 2.

[178] *Cf. supra* Partie I, Chapitre 1, C, ch.3.

[179] *Cf. supra* Partie I, Chapitre 1, D, ch.3.2.

[180] A noter que cette situation n'est cependant possible que dans le cadre de services d'information sur les comptes car le droit à la portabilité des données ne comprend pas l'obligation pour le gestionnaire du compte de modifier les données. Les prestataires de services d'initiation de paiement ne pourront donc pas demander l'exécution d'un ordre de paiement sur la base du droit à la portabilité.

[181] GR29, WP242, p.9; EBF, *Comments on WP29 Portability Guideline*s, p. 10.

[182] *Ibid.*

[183] *Ibid.*

les règles applicables à cet autre droit doivent primer[184]. Le GR29 a, par ailleurs, eu recours aux services d'information sur les comptes et la PSD II pour illustrer ce principe[185]. Lorsqu'un utilisateur demande qu'un accès à son compte soit donné à un prestataire tiers offrant des services relevant du champ d'application de la PSD II, les responsables de traitement doivent donc appliquer les règles y-relatives. Les principes du droit à la portabilité des données tels que régis dans le RGPD devront ainsi s'effacer au profit des règles de la PSD II.

Nonobstant l'exposé qui précède, il existe des cas pour lesquels il est difficile de déterminer quel droit l'utilisateur voulait utiliser, notamment lorsque le destinataire des données offre plusieurs services, dont une partie seulement relève de la PSD II. Pour illustrer cela, il peut être fait référence à la situation d'une entreprise qui offre à ses clients une vue d'ensemble sur leurs comptes et, en parallèle, évalue leur solvabilité afin de les mettre en relation avec une société tierce proposant des crédits à la consommation. Il est regrettable que le GR29 n'apporte pas d'indications claires pour de tels cas. En effet, les banques ne disposent ainsi pas des éléments nécessaires pour décider quel droit appliquer lorsqu'il leur est difficile d'interpréter l'intention réelle de l'utilisateur.

Selon nous, face à une telle situation d'incertitude, il serait préférable que le gestionnaire du compte demande à la personne concernée quel droit elle souhaite voir être appliqué. Bien qu'une telle solution puisse conduire à un traitement plus lent de la demande, les banques ne peuvent unilatéralement décider du régime qu'elles souhaitent appliquer. Cela pourrait, premièrement, amener à des abus de leur part car elles pourraient, par exemple, systématiquement choisir d'appliquer la PSD II et, ainsi, exclure les prestataires qui n'auraient pu obtenir une autorisation[186]. De plus, si les banques décidaient seules du droit applicable, il pourrait leurs être reproché d'avoir choisi le mauvais droit et elles en engageraient ainsi leur responsabilité.

C. A qui incombe la responsabilité de déterminer le droit applicable ?

Ce sous-chapitre tend à désigner qui est responsable de déterminer si la demande de l'utilisateur doit être traitée par le RGPD ou la PSD II. Cette question ne trouve pas de réponse claire et explicite dans les lignes directrices émises par le GR29, mais il y est laissé entendre que cela relèverait de la responsabilité du responsable de traitement.[187].

De notre point de vue, ce raisonnement prête le flanc à la critique. En effet, dans une telle hypothèse, il incomberait au responsable du traitement d'apprécier la nature de chacun des services qui sont offerts par le destinataire des données. Or, contrairement aux demandes régies explicitement par la PSD II[188], le prestataire tiers ne doit pas s'identifier auprès du responsable de traitement. Celui-ci ne disposerait donc pas, au moment de la demande, des éléments nécessaires pour déterminer si les services proposés par le prestataire tiers relèvent de la PSD II ou non.

Nous pouvons cependant admettre qu'il incombe au responsable de traitement de demander à la personne concernée quel droit doit être appliqué à la demande. Dans une telle hypothèse, il ne pourrait pas lui être reproché d'avoir appliqué le mauvais droit. Le seul grief qui pourrait ici

[184] *Ibid.*
[185] *Ibid.*
[186] Cf. supra Partie I, Chapitre 1, C, ch. 3.
[187] *Ibid*.
[188] *Cf. supra* Partie I, Chapitre 1, D., ch.2.2.

être fait à la banque serait de n'avoir pas entrepris les démarches nécessaires pour déterminer la volonté réelle de l'utilisateur.

Nous regrettons également que le GR29 n'ait pas précisé quelles mesures doivent être prises par le responsable du traitement afin de garantir la sécurité des données lors de leur transfert à un tiers dans le cadre d'une demande de portabilité. Par ailleurs, il a été précisé qu'il n'était pas de la responsabilité du responsable de traitement de s'assurer que celles-ci soient conservées de manière sécurisée lorsque la personne concernée les reçoit directement. Il n'est cependant pas clair si le même principe doit être appliqué lors de la transmission des données à un tiers. Nous soutenons cependant que le responsable initial n'a pas à s'assurer que le prestataire tiers recevant les données n'opère pas de traitement illicite, car, n'étant pas partie à la relation liant ce dernier à la personne concernée, il ne dispose pas des moyens nécessaires pour le faire.

Compte tenu de ce qui précède, nous soutenons qu'il serait préférable qu'il soit de la responsabilité de l'utilisateur – respectivement du prestataire tiers lorsqu'il effectue la demande au nom de l'utilisateur – de communiquer clairement sur quel fondement il souhaite transmettre ses données au tiers. À défaut d'une communication claire, la banque devra demander des précisions sur le droit qui doit être appliqué à la demande de l'utilisateur. Il ne pourra ainsi uniquement être reproché au gestionnaire du compte de n'avoir pas entrepris les démarches nécessaires auprès de la personne concernée.

D. Conclusion intermédiaire

En conclusion, lorsqu'il est possible de déterminer clairement que l'utilisateur souhaite donner à un tiers un accès à ses données sur la base de la PSD II, les règles y-relatives s'appliqueront, à l'exclusion de celles découlant du droit à la portabilité. En revanche, en présence d'une demande de portabilité qui ne permet pas de déterminer de manière suffisamment certaine quel est son fondement – notamment en présence de services mixtes – nous sommes d'avis que la banque doit demander à la personne concernée quel droit doit être appliqué.

Il n'est donc selon nous, pas de la responsabilité de la banque de déterminer seule du droit applicable. L'unique responsabilité de la banque est donc d'entreprendre les démarches auprès de la personne concernée afin que celle-ci puisse se déterminer sur le droit qu'elle souhaite voir appliquer à sa demande.

CHAPITRE 2 : LA COMMERCIALISATION DE L'ACCES AUX DONNEES PAR LA BANQUE : CONFORMITE AVEC LE RGPD ET LA PSD II ?

A. Délimitation de la problématique

Le développement de l'*Open Banking* a amené les banques à repenser leur modèle économique. Un modèle qui s'est particulièrement dégagé est le modèle dit de « *Banking-as-a-Platform* », dans lequel la banque met en relation – via l'interface qu'elle a développé– ses clients et les prestataires de services avec qui elles ont un partenariat[189]. Pour ce faire, elle pourrait, par exemple, demander au prestataire tiers de payer des frais mensuels pour avoir le droit d'utiliser l'*API* donnant accès aux données du client[190]. De plus, les banques considèrent qu'obtenir ces données est le résultat d'un grand investissement que les prestataires tiers n'auraient pas besoin

[189] BRODSKY/OAKES, p.8; Mallick et Al., p.8.

[190] Ce modèle est celui qu'ont choisi les banques suisses avec la plate-forme « b.Link », Voir : SIX, *FAQ*.

d'effectuer[191]. Il serait donc justifié de demander une rémunération pour l'accès qu'elles leur donnent[192].

En outre, ce modèle soulève un certain nombre de questions tant en droit européen de la protection des données que par rapport à la PSD II. Nous tenterons donc de déterminer s'il est possible pour la banque de commercialiser l'accès aux données de ses clients.

B. Conformité avec le RGPD

1. Généralités

S'agissant du droit à la portabilité des données, la question de la commercialisation de l'accès aux données est particulièrement intéressante car sa réponse aura une implication, non seulement sur le secteur bancaire, mais également dans tout secteur qui choisira la voie d'une innovation passant par l'ouverture des données à des prestataires tiers[193]. Pour illustrer, nous pouvons mentionner le secteur des assurances qui étudie actuellement la possibilité d'adopter un modèle similaire à celui choisi par le secteur bancaire[194].

Afin de déterminer si la commercialisation de l'accès aux données est conforme au RGPD, nous centrerons notre analyse autour de deux questions distinctes. Premièrement, nous déterminerons l'étendue du principe de gratuité de l'article 12 par. 5 RGPD et si celui-ci s'étend également aux paiements demandés aux prestataires tiers. Deuxièmement, nous chercherons à déterminer si le fait d'offrir au prestataire tiers un accès aux données du client sous la forme d'une *API* excède les obligations qui incombent à la banque, constituant ainsi une prestation pouvant être rémunérée.

2. Paiement demandé aux tiers : contraire au principe de gratuité ?

En vertu de l'article 12 par. 5 RGPD, le droit à la portabilité doit être fourni sans demander de paiement, sauf s'il est exercé de manière infondée ou excessive, notamment de par le nombre important de demandes qui sont effectuées[195]. Dans un tel cas, des frais ne dépassant pas les coûts supportés pour satisfaire la demande peuvent être exigés[196]. Cependant, si le responsable du traitement dispose d'un système informatique automatisé lui permettant de répondre facilement à des demandes répétées, il ne subira quasiment aucun frais[197]. Celui-ci ne serait ainsi pas légitimé à exiger un paiement de la part de la personne concernée. De plus, les responsables de traitement ne peuvent pas mettre à la charge de cette dernière les frais qu'ils ont dû supporter pour la mise en place de l'infrastructure globale requise pour répondre au droit de la portabilité[198].

Dans le contexte de l'*Open Banking*, la personne concernée va effectuer une demande de portabilité à chaque fois qu'elle désirera obtenir les services du prestataire tiers. Le nombre de demande va donc grandement varier selon les services qui sont offerts. Nous pouvons cependant

---

[191] EBF, *Comments on WP29 Portability Guidelines*, p.6.

[192] *Ibid*.

[193] Par ailleurs, le nouveau droit suisse de la protection des données introduisant le droit à la portabilité des données dans sa révision entrant en vigueur en 2022, les principes que nous explorons ici pourraient également être utiles à l'interprétation des normes suisses.

[194] INSURANCE EUROPE.

[195] GR29, *WP242*, p.18; REICHLIN, p.410.

[196] *Ibid*.

[197] *Ibid.*

[198] GR29, *WP242*, p.18.

imaginer que certains services auront besoin d'un accès constant et répété[199]. Dans cette hypothèse, nous pourrions donc admettre que les demandes de la personne concernée seraient excessives, conformément à l'article 12 par. 5 RGPD. Des frais pourraient ainsi, *a priori,* être envisagés. Cependant, si le responsable du traitement dispose d'un système automatisé lui permettant de faire face à ces demandes répétées, il ne subira pratiquement aucun coût supplémentaire et ne pourra ainsi pas demander de rémunération à la personne concernée. Or, les banques se trouvent précisément dans ce cas puisqu'elles disposent déjà d'un tel système pour satisfaire leurs exigences relatives aux transferts de données fondés sur la PSD II. Il leur est de ce fait aisé, soit de transférer à un tiers les mêmes données que celles couvertes par la PSD II mais pour des services qui ne rentrent pas dans son champ d'application, soit d'utiliser le système automatisé développé dans le cadre de la PSD II pour traiter les demandes de portabilité de données ne relevant pas de la PSD II. En de pareilles circonstances, il serait difficile pour la banque de démontrer que les demandes répétées de l'utilisateur leur ont créés un coût tel qu'il serait justifié de faire porter des frais à la charge de la personne concernée. Dès lors, nous soutenons donc que l'exercice du droit à la portabilité dans le cadre de l'*Open Banking* devra se faire gratuitement.

Ensuite, il n'est pas clairement défini si l'interdiction de l'article 12 RGPD ne porte que sur les paiements qui seraient demandés à la personne concernée ou si elle s'étend également aux frais mis à la charge du tiers recevant les données. Il y a donc lieu de déterminer la volonté du législateur et de déterminer la portée exacte de cette notion. A cet égard, il sied de rappeler que le but du droit à la portabilité des données est de donner un libre contrôle sur ses données à la personne concernée[200]. Le législateur a en effet souhaité lutter contre les situations de « *lock-in*», dans lesquelles les consommateurs peuvent se retrouver[201]. En conséquence, la personne concernée doit pouvoir exiger de recevoir ses données ou de demander leurs transferts sans que cela ne lui coûte. Or, s'il était admis que le responsable du traitement puisse demander une rémunération de la part du prestataire de services tiers, nous sommes d'avis qu'il y'aurait un risque que la personne concernée en supporte la charge de manière indirecte. En effet, pour pouvoir absorber les coûts supplémentaires imposés par la banque, le prestataire de services va soit augmenter le prix de ses services, soit diminuer leur qualité. La personne concernée, en ayant fait exercice de son droit à la portabilité, aurait ainsi à subir un désavantage qui ne saurait être conforme à la volonté du législateur. Au vu de ce qui précède, nous sommes d'avis qu'il faut interpréter cette notion de manière large et y inclure les paiements exigés aux prestataires tiers. Par conséquent, nous pouvons considérer que le principe de gratuité s'applique tant à la personne concernée qu'au tiers recevant les données.

Finalement, nous pouvons arguer qu'en exigeant un paiement de la part de la personne tierce recevant les données, le responsable de traitement fait obstacle à l'exercice du droit à la portabilité. En effet, conformément à l'article 20 par 1 *in fine* RGPD, le responsable du traitement ne peut volontairement ajouter des barrières juridiques, techniques ou financières afin de rendre l'exercice du droit à la portabilité moins attrayant pour la personne concernée[202]. Or, il est à craindre que de tels frais – si admis – pourraient être utilisés pour décourager les utilisateurs à utiliser les services de tiers. Bien que des entraves au droit de la portabilité puissent être tolérés, notamment afin de protéger des tiers ou de sécuriser ses systèmes informatiques, il

[199] Nous pouvons ici mentionner, à titre d'exemple, les programmes de « *Cashback* » qui visent à fidéliser les clients de certaines entreprises en leur offrant des rabais selon en fonction des dépenses qu'ils ont effectués auprès de celles-ci. De tels programmes peuvent se fonder sur le droit à la portabilité pour accéder aux données des clients de manière répétée et ainsi pouvoir déterminer leurs dépenses effectives.

[200] *Cf. supra* Partie I, Chapitre 2, D., ch. 1.

[201] *Cf. supra* Partie I, Chapitre 2, D., ch. 1.

[202] GR29, *WP242*, p.19.

incombe au responsable de traitement de démontrer en quoi elles sont justifiées. En l'espèce, nous pouvons raisonnablement douter que le responsable du traitement parvienne à justifier un intérêt supérieur à imposer une contribution financière au prestataire tiers. Nous sommes donc d'avis qu'exiger du tiers le paiement de frais constitue une barrière au droit à la portabilité des données, laquelle est contraire à l'article 20 RGPD.

3. Transmission des données via une *API :* un service supplémentaire ?

Dans cette section, il sera plus spécifiquement traité de l'utilisation d'une interface de programmation d'application permettant l'accès aux données de la personne concernée.

Il ne serait pas surprenant que les banques soutiennent qu'offrir un accès constant, instantané et permanent aux données du client au moyen d'une *API* outrepasse les simples obligations découlant du droit à la portabilité et constitue ainsi un service supplémentaire. Dans un tel cas, une banque pourrait alors demander un paiement fondé sur un contrat qu'elle aurait conclu avec le prestataire de service pour qu'il puisse avoir accès à cette interface[203].

Un tel modèle n'est cependant pertinent que si la fourniture d'un accès sous la forme d'une *API* ne relève pas de l'exécution normale du droit à la portabilité. En effet, bien que le droit à la portabilité des données appartienne à la personne concernée et non au prestataire tiers, nous pouvons imaginer que celui-ci préfèrerait demander à cette dernière qu'elle fasse usage de son droit plutôt que de devoir payer des frais. Partant, il convient de déterminer si la fourniture d'une interface de programmation d'application permettant d'accéder aux données constitue un service supplémentaire ou si elle s'il s'agit d'une composante du droit à la portabilité des données.

A cet égard, il y a lieu de rappeler que le considérant n°68 du RGPD ne fait qu'encourager les responsables de traitement à adopter des moyens de transmission interopérable[204]. Le législateur n'a donc pas souhaité imposer une obligation de développer des interfaces dédiées à la transmission des données qui a lieu dans le cadre du droit à la portabilité, contrairement au choix qui a été fait dans le cadre de la PSD II. En effet, concernant l'accès donné aux prestataires de services d'initiation de paiement et d'information sur les comptes, le législateur a clairement indiqué que les gestionnaires du compte devaient développer une interface dédiée ou laisser la possibilité au tiers d'utiliser l'interface mise à disposition des clients[205]. Or, un tel choix n'a pas été fait dans le cadre du droit à la portabilité. Le responsable du traitement est donc libre d'honorer ses obligations découlant du droit à la portabilité avec le mode de transmission de son choix. De plus, il n'existe aucune obligation pour le responsable du traitement de répondre de manière instantanée à la demande de portabilité. Un délai pour répondre allant jusqu'à trente jours est ainsi toléré[206]. Ses obligations se limitant à la transmission des données dans un format « lisible par une machine » et exécutée dans un délai raisonnable, il est possible d'arguer que le responsable du traitement ne sera pas obligé de fournir une interface dédiée à la transmission des données qui a lieu dans le cadre du droit à la portabilité.

De plus, se prévaloir du droit à la portabilité des données afin d'obtenir un accès constant et permanent aux données pourrait être constitutif d'un abus de droit. En effet, en introduisant le droit à la portabilité, le législateur a souhaité permettre aux utilisateurs d'un service utilisant leurs données personnelles de changer de fournisseur, sans avoir à subir de désavantages

[203] A noter que dans un tel cas, la banque devra vraisemblablement obtenir le consentement de l'utilisateur ou démontrer un intérêt prépondérant pour justifier le transfert de données, en vertu de l'article 6 RGPD.
[204] *Cf. supra* Partie I, Chapitre 2, E, Ch. 2.
[205] *Cf. supra* Partie I, Chapitre 1, D, Ch. 4.2.
[206] *Cf. supra* Partie I, Chapitre 2, E, Ch. 4.

majeurs[207]. Il n'a donc nullement été prévu que la personne concernée puisse obtenir des services de tiers fondés sur l'accès à ses données, lesquelles ont été maintenues auprès du fournisseur initial. Le droit à la portabilité a donc été pensé de manière que l'utilisateur puisse obtenir du responsable du traitement de lui transmettre ses données un nombre limité de fois. On ne saurait ainsi admettre qu'un droit à un accès « dynamique » et permanent aux données soit inféré du droit à la portabilité, faute de quoi la volonté du législateur serait détournée de manière inacceptable.

Nonobstant les éléments qui précèdent, il sied de rappeler que le responsable du traitement ne peut, conformément à l'article 20 par. 1 RGPD, créer volontairement des barrières visant à ralentir ou restreindre l'exercice du droit à la portabilité. Or, en utilisant un autre format de transmission que l'*API* déjà existant, le responsable du traitement choisit volontairement un moyen technique moins rapide et moins pratique pour le prestataire tiers. Cette situation a, par ailleurs, été expressément citée comme exemple d'obstacle au droit à la portabilité des données par le GR29[208]. Il y a donc lieu de différencier la situation où le responsable du traitement dispose des moyens techniques nécessaires pour répondre à la demande de portabilité sans délais et dans un format interopérable de la situation où aucun moyen technique n'existe. En effet, dans la deuxième hypothèse, conformément aux éléments détaillés ci-dessus, il ne saurait être exigé du responsable du traitement de développer un système interopérable. Cependant, si – comme dans la première hypothèse – un tel système est déjà en place, nous sommes d'avis qu'il devra l'utiliser et ne pourra favoriser un autre moyen de transmission, faute de quoi il ferait barrage au droit à la portabilité.

Quant à la question d'un éventuel abus de droit, les arguments précités ne sauraient, selon nous, résister à un examen plus approfondi de la volonté du législateur. En effet, bien que l'hypothèse d'un accès « dynamique » aux données n'ait pas été expressément prévue par le législateur, nul ne peut ignorer que celui-ci souhaitait avant tout donner à l'utilisateur la possibilité d'avoir un certain contrôle sur ses données[209]. La personne concernée doit donc être libre de décider comment ses données sont traitées et doit ainsi pouvoir faire appel au prestataire de services de son choix. De plus, il y a lieu de rappeler que le droit à la portabilité vise également à éviter qu'un responsable de traitement puisse garder les personnes concernées en tant que clients pour la seule raison qu'il dispose de données importantes sur elles. Le droit à la portabilité des données comporte ainsi également d'une dimension anticoncurrentielle[210]. Il n'est donc pas incompatible avec la volonté du législateur qu'elles puissent maintenir leurs données auprès d'un responsable de traitement, tout en donnant un accès à celles-ci à un tiers.

Ainsi, il ne saurait être admis que le transfert de données exécuté grâce une *API* soit constitutif d'un service excédant les obligations qui incombent aux banques. Un tel accès ne constitue également pas, selon nous, un abus de droit. Les prestataires de paiement doivent ainsi pouvoir obtenir un accès aux données des clients via une *API* en demandant à ces derniers d'effectuer une demande de portabilité.

4. Conclusion intermédiaire

En conclusion, l'article 12 par. 5 RGPD implique qu'aucun paiement ne peut être demandé de la part du responsable de traitement pour l'exécution d'une demande de portabilité. Il y a lieu d'étendre cette interdiction également aux paiements qui émaneraient du tiers recevant les

[207] *Cf. supra* Partie II, Chapitre 2, B, Ch. 2.
[208] *Ibid*.
[209] Cette volonté du législateur ressort notamment du considérant n°7 du RGPD.
[210] SYDOW, p.531

données, faute de quoi l'utilisateur devrait en assumer les coûts indirects. De plus, dans le cadre de l'*Open Banking,* la banque ne subit aucun coût supplémentaire provenant de demandes répétées de l'utilisateur car elle dispose déjà, par leurs obligations découlant de la PSD II, d'une infrastructure apte à faire face à ces demandes à moindre coût. Finalement, si – lorsqu'elles répondent à une demande de portabilité – les banques favorisent un format de transmission volontairement plus lent qu'un autre à leur disposition, il leur sera reproché de faire obstacle au droit de l'utilisateur.

Pour tous ces motifs, nous concluons que les banques ne pourront commercialiser l'accès aux données qui peuvent faire l'objet d'une demande de portabilité.

C. Conformité avec la PSD II

Si la PSD II établit des règles claires concernant les frais qui peuvent être requis à l'utilisateur d'un service de paiement, tel n'est pas le cas pour les frais qui peuvent être mis à la charge des prestataires de services d'initiation de paiement et d'information sur les comptes[211]. Le considérant n°65 *in fine* PSD II mentionne que « les dispositions concernant (…) les frais prélevés n'ont aucun effet direct sur les tarifs appliqués entre les prestataires de services de paiement ou les autres intermédiaires ». Il serait donc légitime de penser que des frais peuvent être requis de la part du gestionnaire de compte à l'égard des prestataires de services tiers.

Cependant, pour que le gestionnaire de compte puisse prélever des frais auprès du prestataire tiers, une base contractuelle est requise, puisque cela ne découle pas de la loi. Or, il ressort des articles 66 par 5. PSD II et 67 par. 4 PSD II que les services d'initiation de paiement et d'information sur les comptes doivent pouvoir être fournis – indépendamment de l'existence d'une quelconque relation contractuelle entre le prestataire de services et le gestionnaire de compte. Ainsi, un utilisateur qui souhaiterait bénéficier des services d'un prestataire tiers doit se voir accorder cette possibilité, en dépit de tout contrat – convenant d'un paiement de frais – passé entre ce dernier et le gestionnaire du compte.

En outre, ce point avait été soulevé dans le cadre de l'analyse d'impact préalable à l'adoption de la directive menée par le Parlement européen[212]. En effet, au moment de choisir le modèle législatif autorisant l'accès aux données bancaires des clients, plusieurs options ont été discutées, dont une qui aurait laissé les gestionnaires de comptes et les prestataires de services régir leur relation dans le cadre d'un contrat. Si cette option n'a finalement pas été retenue, c'est précisément parce que les banques auraient alors pu fixer des frais importants, limitant ainsi la possibilité pour un prestataire tiers d'offrir des services de paiement.

De plus, selon les articles 66 par. 4 let. c) et 67 par. 3 let. b) PSD II, le gestionnaire du compte ne peut effectuer, sans raison objective, de différence de traitement entre les demandes faites par l'intermédiaire d'un prestataire tiers et celles faites dans le cadre des services que lui-même propose[213]. Or, en demandant une rémunération aux prestataires de services d'initiation de paiement ou d'information sur les comptes, le gestionnaire de compte traite de manière moins favorable les demandes effectuées en utilisant les services d'un prestataire tiers que celles issues de ses propres services. Partant, nous sommes d'avis le gestionnaire de compte ne peut pas – en vertu des dispositions précitées sur l'interdiction de la discrimination – demander au prestataire tiers un paiement pour la fourniture d'un accès aux données du client. C'est

[211] FOLCIA ET AL., p.5; EB
F, *Guidance,* pp.43-44.
[212] EUROPEAN COMMISSION, *Volume 1/2,* p. 64; EUROPEAN COMMISSION, *Volume 2/2,* p.137.
[213] *Cf. supra* Partie I, Chapitre 1, D., ch. 3.3.

également l'opinion du Comité de Bâle sur le contrôle bancaire dans son rapport de novembre 2019 portant sur l'*Open Banking* et les *APIs*[214].

En somme, les services doivent être fournis malgré l'absence de toute relation contractuelle entre les parties et que les gestionnaires de compte ne peuvent pas traiter de manière discriminatoire les demandes faites par l'intermédiaire d'un prestataire tiers.

Au vu de ce qui précède, nous soutenons donc que les banques ne pourront pas exiger de paiement de la part des prestataires de services d'initiation de paiement et d'information sur les comptes pour l'accès aux informations de compte et pour l'exécution d'ordres de paiement.

D. Propositions de services conformes au RGPD et à la PSD II

Nous allons ici brièvement explorer les différents services qui peuvent être offerts contre rémunération de manière conforme au RGPD et à la PSD II dans le cadre de l'*Open Banking.*

Premièrement, les banques peuvent tout à fait commercialiser l'accès aux données de personnes morales qui ne relèvent pas de la PSD II. En effet, les données de personnes morales ne relevant pas du champ d'application du RGPD, elles ne peuvent donc pas faire l'objet d'une demande de portabilité[215]. Une transmission de ces données à un prestataire tiers devra donc, selon nous, se faire sur la base d'un contrat. De plus, les banques disposant déjà de l'infrastructure technique permettant le transfert sécurisé de données bancaires, il leur sera aisé d'y inclure les données de personnes morales[216]. À titre d'exemple, des entreprises pourraient souhaiter ouvrir leurs données bancaires à des services de comptabilité d'entreprise, de gestion des factures ou encore à des fiduciaires. Dans de tels cas, nous sommes d'avis qu'il serait possible pour la banque de demander une rémunération auxdits prestataires tiers.

Ensuite, la banque peut commercialiser une analyse issue de données du client. Il lui sera par exemple possible de vendre aux prestataires de paiements tiers des informations relatives à la solvabilité de la personne concernée ou encore des informations qui résulteraient de son programme de détection des fraudes. Cependant, l'analyse en elle-même ainsi que sa communication à des tiers devront être légitimés par un des motifs de l'article 6 RGPD.

CONCLUSION FINALE

L'*Open Banking* vise à permettre à un prestataire externe d'offrir des services grâce à un accès aux données du compte en banque de ses clients. Cela représente un changement majeur du modèle économique du secteur bancaire car le rôle des banques n'est plus le même et elles n'ont ainsi plus la même relation qu'auparavant avec les clients. Tel que cela ressort de la présente étude, ce changement comporte son lot de questions et de difficultés.

En Europe, l'*Open Banking* a été encouragé par l'adoption de la PSD II. En effet, la directive précitée a introduit un droit pour l'utilisateur d'exiger de sa banque qu'elle donne un accès à des prestataires tiers et qu'elle collabore avec ceux-ci dans l'exécution de paiements. De cette manière, la PSD II offre une garantie aux prestataires tiers de pouvoir offrir aux utilisateurs les services souhaités. De plus, la réglementation technique de mise en œuvre de cette directive encourage l'utilisation d'une api. Pour ces motifs, la PSD II a grandement contribué au développement de l'*Open Banking* en Europe.

---

[214] BASEL COMMITTEE, *Report on Open Banking*, pp.16-17.

[215] *Cf. supra* Partie I, Chapitre 2, C, ch. 1.1.

[216] A noter qu'il y aura cependant lieu de respecter les autres normes qui pourraient s'appliquer.

Néanmoins, cette législation ne couvre pas l'entier des opportunités émanant de l'*Open Banking*, de telle sorte qu'il convient d'avoir recours aux règles relatives au droit à la portabilité issues du RGPD. Celles-ci permettant ainsi à un utilisateur de demander à une banque de transmettre que les données personnelles le concernant soit transmises à un tiers, même dans les cas ne rentrant pas dans le champ d'application de la PSD II. Ces règles sont, cependant, moins adéquates car elles ne permettent pas l'exécution de paiements et ne peuvent être utilisées par des personnes morales.

Par ailleurs, contrairement aux droits issus de la PSD II, le droit à la portabilité n'a pas été conçu pour une transmission en continu des données, de sorte qu'il ne prescrit pas l'utilisation d'une api. En outre, tel que cela ressort de l'analyse faite dans le cadre de ce travail, les banques ne peuvent pas volontairement faire obstacle au droit à la portabilité. Dès lors, comme elles disposent en principe déjà d'une infrastructure apte à transmettre les données instantanément, nous sommes d'avis qu'elles doivent utiliser pour répondre aux demandes de portabilité, faute de quoi il pourra leur être reproché de ralentir volontairement la transmission des données.

De plus, il ressort de notre étude que le droit à la portabilité doit être exempt de tout frais, tant pour la personne concernée que pour le tiers recevant les données. Les banques ne peuvent donc pas générer des revenus en mettant leur infrastructure *API* à disposition des tiers. Il en est de même dans le cadre de la PSD II, car les données doivent pouvoir être transmises à tout prestataire tiers, sans discrimination, indépendamment de toute conclusion de contrat avec le gestionnaire du compte.

Ensuite, nous avons pu analyser dans le cadre de cette étude la relation entre le droit à la portabilité et les règles issues de la PSD II. Il ressort de cette analyse que lorsqu'un utilisateur a clairement eu l'intention d'utiliser l'un ou l'autre des droits précités, il y aura lieu d'appliquer les normes qui en découlent. Cependant, la situation est moins claire lorsque l'intention de l'utilisateur n'est pas déterminée, notamment lorsque le prestataire tiers offre des services qui ne relèvent que partiellement de la PSD II. Dans une telle hypothèse, nous sommes d'avis qu'il est préférable d'appliquer les règles du droit à la portabilité car elles permettent de respecter au mieux la volonté de l'utilisateur. En outre, il serait souhaitable, selon nous, que le Comité Européen de la Protection des Données précise à qui incombe la responsabilité de déterminer quel droit voulait être appliqué par l'utilisateur.

Finalement, il sied de mentionner que, bien que les règles que nous avons pu analyser ci-dessus ne soient pas toujours favorables pour les banques – notamment concernant le principe de gratuité – l'*Open Banking* a, sans doute, permis d'éviter une fuite des capitaux vers de nouveaux acteurs du monde de la finance. Ce faisant, l'activité dite « traditionnelle » de la banque, c'est-à-dire de prêter de l'argent déposé par des tiers, a pu être protégée. De plus, les innovations qui vont pouvoir émaner de ce modèle vont, selon nous, permettre d'offrir de bien meilleurs services aux clients, qui n'en seront que plus satisfaits. Partant, nous sommes d'avis que l'*Open Banking*, malgré ses quelques désavantages, représente une grande opportunité pour le secteur bancaire qui peut ainsi mieux intégrer les nouveaux acteurs de l'innovation et, par conséquent, ouvrir une nouvelle page de son histoire.