

**Faculté de droit et de criminologie**

# **Les situations de conflits de lois entre Etats membres dans le cadre du RGPD**

Une analyse à la lumière de l'exemple du  
consentement du mineur au traitement de ses  
données à caractère personnel

Auteur : Anastasia-Angeliki KOUTRA  
Promotrice : Stéphanie FRANCO  
Année académique 2018-2019  
Master en droit - Finalité droit de l'entreprise



## **Plagiat et erreur méthodologique grave**

---

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation\*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

\* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

## Remerciements

---

Je tiens à remercier sincèrement ma promotrice, Pr. S. FRANCO, pour sa disponibilité et ses conseils avisés tout au long de cette étude, ainsi que pour avoir éveillé en moi l'intérêt du sujet des conflits de lois dans le nouveau Règlement général sur la protection des données personnelles, me poussant ainsi à élargir mes horizons et mettre en avant mon esprit critique.

Je remercie également M. CLOTUCHE, B. ROELENS ainsi que ma mère, P. MATENOPOULOU, pour le temps et l'attention qu'ils ont consacrés à la relecture orthographique et syntaxique du présent mémoire.

Enfin, je souhaite remercier ma famille et chacun de mes amis pour leurs encouragements quotidiens au cours de cette réflexion et, plus généralement, leur soutien durant ces cinq années de formation académique.

## Table des matières

<b>Introduction</b> .....	1
<b>Chapitre 1. Remarques préliminaires : un cadre juridique global définissant son applicabilité</b> .....	4
<b>Section I. Une nouvelle base juridique</b> .....	4
§1. <i>Choix de l'instrument juridique approprié</i> .....	4
§2. <i>Champs d'application matériel et personnel du RGPD</i> .....	6
1. Les données à caractère personnel .....	6
2. Le traitement .....	7
3. Les personnes concernées .....	8
4. Les responsables de traitement et les sous-traitants .....	8
<b>Section II. Les caractéristiques principales du droit à la protection des données personnelles</b> .....	10
§1. <i>Nature juridique du droit</i> .....	10
§2. <i>Difficulté de rattachement à un seul territoire</i> .....	10
<b>Section III. Les caractéristiques de l'article 3 du règlement</b> .....	11
§1. <i>Analyse préalable : état des lieux de l'article 4 de la directive</i> .....	11
1. Présentation de l'article .....	11
2. La notion d'établissement telle qu'interprétée par la Cour de justice .....	12
§2. <i>Champ d'application territorial du RGPD</i> .....	13
§3. <i>Absence de règle de conflit de lois</i> .....	14
<b>Chapitre 2. Les conflits de lois dans les relations intra-européennes : les scénarios</b> .....	15
<b>Section I. Les limites à l'uniformisation</b> .....	15
§1. <i>Présentation du caractère original du règlement</i> .....	16
§2. <i>Marges de manœuvre laissées aux législateurs nationaux</i> .....	17
1. Actions requises de la part des Etats membres en vertu du RGPD .....	17
2. Actions possibles des Etats membres en vertu du RGPD .....	18
§3. <i>Silence du règlement</i> .....	18
<b>Section II. Les lois nationales exécutant le RGPD : Analyse au regard d'un exemple concret : l'âge du consentement du mineur à travers les lois belge et française</b> .....	19
§1. <i>Présentation de l'article 8 du RGPD</i> .....	19
§2. <i>Cas pratique de départ</i> .....	21
§3. <i>La législation belge d'exécution du RGPD</i> .....	22

1. Champ d'application territorial .....	22
2. Exécution de l'article 8 §1 du règlement .....	23
<b>§4. La législation française d'exécution du RGPD.....</b>	<b>23</b>
1. Champ d'application territorial .....	23
2. Exécution de l'article 8 §1 du règlement .....	24
<b>§5. Conclusion intermédiaire : quelle législation retenir ? .....</b>	<b>25</b>
<b>Chapitre 3. Les règles classiques de droit international privé européen .....</b>	<b>25</b>
<b>Section I. Raisonnement au départ des règles classiques de droit international privé européen : précautions introductives .....</b>	<b>25</b>
<b>§1. La matière « civile et commerciale » .....</b>	<b>26</b>
1. Définition et contextualisation .....	26
2. Les données à caractère personnel peuvent-elles être incluses dans cette notion ? .....	27
<b>§2. L'objet du consentement .....</b>	<b>28</b>
<b>Section II. Détermination de la loi applicable au contrat via le règlement Rome I : une société établie en Belgique traitant avec un mineur résidant en France .....</b>	<b>30</b>
<b>§1. Retour sur le champ d'application matériel du règlement.....</b>	<b>31</b>
1. La notion d' « obligations contractuelles » .....	31
2. Exclusions du champ d'application de Rome I : l'état et la capacité .....	32
2.1.) L'exclusion en tant que telle .....	32
2.2.) L'exclusion au regard du cas pratique.....	33
2.3.) Quelques réflexions supplémentaires : une question de catégorie de rattachement ?	34
<b>§2. La personne concernée par le traitement est-elle un consommateur ? .....</b>	<b>35</b>
1. Le champ d'application personnel de l'article 6 du règlement Rome I tel que défini par la jurisprudence européenne .....	36
1.1) Le consommateur.....	36
1.2.) Le professionnel .....	38
2. Le droit applicable en vertu de l'article 6 du règlement Rome I.....	39
3. Application au cas pratique du mineur.....	39
<b>§3. Autres règles prévues par le règlement Rome I : fondements classiques de rattachement .....</b>	<b>40</b>
<b>§4. Fais du casus inversés : une société établie en France .....</b>	<b>41</b>
1. Mineur de nationalité belge résidant en Belgique.....	41
1.1.) Droit applicable à la question du consentement .....	41
1.2.) Droit applicable pour les autres questions .....	42
2. Mineur de nationalité française résidant en Belgique .....	42
2.1.) Droit applicable à la question du consentement .....	42
2.2.) Droit applicable pour les autres questions .....	43

<b>Section III. Les relations extracontractuelles .....</b>	<b>43</b>
§1. <i>Le droit à la vie privée et le droit à la protection des données .....</i>	43
§2. <i>Etat des lieux sur le règlement Rome II .....</i>	45
§3. <i>La possibilité d'introduire une nouvelle clause dans Rome II ? .....</i>	47
<b>Chapitre 4. Bilan des questions envisagées dans le cadre de cette étude au regard du droit international privé et autres pistes de réflexion.....</b>	<b>48</b>
<b>Section I. L'absence de solution satisfaisante dans les règles de droit commun.....</b>	<b>49</b>
§1. <i>Hypothèses de « cumul » et de « lacune » suite à l'adoption du RGPD .....</i>	49
§2. <i>Argument de la « lex specialis » .....</i>	52
1. <i>Le règlement Rome I peut-il forcer l'application d'une loi nationale à des situations qu'elle ne vise pas ? Raisonement à partir du phénomène de l'autolimitation .....</i>	52
1.1.) <i>Contextualisation théorique .....</i>	52
1.2.) <i>Qu'en est-il des lois d'exécution nationales du RGPD?.....</i>	53
2. <i>L'article 23 du règlement Rome I .....</i>	54
<b>Section II. Quelques pistes de réflexions supplémentaires quant à la détermination du droit applicable .....</b>	<b>55</b>
§1. <i>Les lois nationales en tant que lois de police ?.....</i>	56
1. <i>Définition et critères au départ de l'article 9 du règlement Rome I.....</i>	56
2. <i>Remarques relatives aux lois d'exécution du RGPD .....</i>	57
§2. <i>L'autorité chef de file et le mécanisme du « guichet unique » : un indice donné par le RGPD ? .....</i>	59
<b>Conclusion.....</b>	<b>61</b>
<b>Bibliographie .....</b>	<b>64</b>



## Introduction

« RGPD »: ces quatre lettres qui suscitent, depuis plus de trois ans, un engouement hors du commun, une multitude de débats et une agitation invraisemblable des deux côtés de l'Atlantique. Il s'agit du Règlement général sur la protection des données à caractère personnel 2016/679, entré en vigueur le 25 mai 2018<sup>1</sup>. Après plus de 20 ans d'existence de la directive 95/46/CE<sup>2</sup>, ce règlement apparaît comme une construction juridique inédite, portée par la nécessité grandissante de faire face aux défis découlant de la société de l'information. Le développement conjoint d'internet, du *Big Data*, et de l'informatique en nuage façonnent une autre économie, faisant dire à certains que les données constituent le « nouvel or noir », le carburant de l'économie numérique<sup>3</sup>. Des publicités comportementales aux appareils de géolocalisation, en passant par les voitures autonomes, les polices d'assurance et les profilages politiques, les traitements de données personnelles sont aujourd'hui incontournables. Le législateur européen l'a bien saisi : « *les nouvelles technologies permettent tant aux entreprises privées qu'aux pouvoirs publics d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde* »<sup>4</sup>. Toutefois, l'utilisation de ces données suscite une opposition d'intérêts entre le profit et la protection. En effet, elle génère des préoccupations mais également des innovations. Dans ce contexte, le règlement intervient comme un instrument juridique ayant l'ambition de poursuivre, voire d'étendre, la protection des données à caractère personnel, tout en favorisant leur circulation dans l'espace économique européen. A cet égard, l'Union européenne rappelle que « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* »<sup>5</sup>.

Les discussions et commentaires autour du RGPD se focalisent principalement sur les nouvelles notions et nouveaux principes qui y sont intégrés ou encore sur l'expansion de son champ d'application territorial ainsi que sur les amendes administratives conséquentes susceptibles de pouvoir être imposées en cas de violation de ses dispositions. La plupart des règles contenues dans ce règlement sont pensées sur base de l'extrême volatilité et vélocité des données à caractère personnel. Ces dernières sont non seulement un bien immatériel mais aussi un bien non-rival. Par leur nature même donc, les données ne s'entendent pas par rapport à un territoire donné. Elles sont appelées à traverser les frontières et à circuler dans le monde entier.

---

<sup>1</sup> Règlement (UE) n° 2016/679 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 (règlement général sur la protection des données), art. 99 §2. , *J.O.U.E.*, 4 mai 2016, L 119, p. 1 (ci-après « RGPD »).

<sup>2</sup> Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, 23 novembre 1995, L 281, p. 31 (ci-après « directive 95/46/CE »).

<sup>3</sup> « *Data is the new oil* » (2006), phrase du mathématicien anglais Clive Humby; Voy. aussi l'article paru dans le journal *The Economist* du 6 mai 2017, « *Regulating the internet giants. The world's most valuable resource is no longer oil, but data* », <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (consulté le 22 juillet 2019).

<sup>4</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), C.O.M. (2012) 011, final, p. 1.

<sup>5</sup> Considérant 4, du RGPD.

Partant, il est surprenant que le règlement n'aborde précisément pas l'ensemble des modalités pratiques de cette volatilité, dans le cadre de la réalisation du marché intérieur qu'il poursuit. Étonnamment, peu d'attention est accordée à l'interaction entre le RGPD et les nouvelles lois des Etats membres de l'Union, qui ont été adoptées en réponse à celui-ci<sup>6</sup>. En effet, l'étude seule de ce règlement ne permet pas d'appréhender les contours juridiques nécessaires pour que son contenu soit pleinement efficace et intelligible<sup>7</sup>. Cet instrument juridique, de ce fait, ne se suffit pas entièrement à lui-même. Comme son nom l'indique, il s'agit d'un règlement « général », ce qui implique que certains points n'y sont pas traités ou qu'ils mériteraient d'être précisés, dans des textes qui pourraient ainsi être qualifiés de « spéciaux ». C'est que, pour certaines questions précises, il accorde une latitude plus ou moins grande aux Etats membres, contraignante ou facultative selon les cas.

En théorie, un règlement européen qui accorde une possibilité d'intervention aux législateurs nationaux semble être signe de compromis positif entre l'uniformisation du droit, dans le but de protéger un droit fondamental, et la reconnaissance de certaines particularités des Etats membres. En pratique, il est nécessaire de départager clairement les situations entre les ordres juridiques nationaux potentiellement impliqués. Toutes les personnes ou entités concernées par les articles du RGPD ont besoin de savoir comment le droit européen trouve une harmonie avec les droits nationaux des Etats, afin de connaître leurs droits et obligations. Toutefois, le règlement ne donne aucune indication, en tout cas explicite, à cet égard. Quel est le droit applicable ? Quelles sont les conséquences pratiques des renvois aux législateurs nationaux ? Quand une situation relèverait-elle du droit d'un Etat membre plutôt que de celui d'un autre ? Sur base de quel(s) critère(s) ? Comment le règlement prend-il ou non en compte ces implications par rapport à son prédécesseur ? Quel(s) indice(s) donnerait éventuellement le règlement ou encore d'autres instruments juridiques par rapport à ces « conflits de lois » qui peuvent se poser ?

Le présent mémoire propose une étude de ces questions. Elle se décline en quatre chapitres.

Le premier chapitre contextualisera l'adoption du nouveau règlement et donnera certaines clés de lecture essentielles à toute analyse de la matière des données à caractère personnel. Outre des définitions inhérentes à ce domaine, ce droit présente des caractéristiques propres qui sont à la source de notre raisonnement sur le droit international privé et, plus particulièrement, sur le droit applicable. En outre, cette mise en contexte ne pourrait être complète sans une comparaison entre l'ancienne directive qui prévoyait une règle de conflit de lois, compte tenu des différentes lois de transposition, et le nouveau règlement qui reste silencieux à cet égard. En effet, il ne prévoit aucune règle de conflit de lois.

Un deuxième chapitre étudiera les différents scénarios d'intervention législative prévus par le RGPD. Il s'agit d'un règlement européen qui accorde une possibilité, voire une obligation dans certains

---

<sup>6</sup> K. NOLAN, « GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law », *Berkeley Technology Law Journal*, 2018, <http://btjl.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/> (consulté le 20 juillet 2019).

<sup>7</sup>V. VERBRUGGEN, « Titre 1. RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne, in *Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Bruxelles, Larcier, 2018, p. 26.

cas, d'exécution de la part des Etats membres. Il en résulte que le droit en la matière n'est pas totalement uniformisé au niveau de l'Union européenne, pouvant ainsi mener à des situations où des lois sont en conflit. Afin d'appréhender les éventuels conflits de lois, la présente étude propose d'analyser, plus précisément, comment l'article 8 du RGPD sur le consentement du mineur au traitement de ses données a été exécuté en droit belge et en droit français. La protection des enfants sur Internet est, de fait, devenue un enjeu majeur pour l'Union. A travers cet article, les implications pratiques des implémentations des Etats membres seront révélées. Celles-ci seront étudiées au départ de l'évocation d'un « *casus* », imaginaire bien entendu. Cette façon de faire permettra au lecteur d'avoir une approche concrète.

Dans un troisième chapitre, nous procéderons à un exercice d'identification du droit applicable par rapport au cas pratique précité, impliquant un mineur, en partant des règles de conflits de lois de droit commun, qui se trouvent dans les instruments européens de droit international privé. Il s'agit de la solution la plus logique pour envisager l'interaction entre les différentes lois nationales d'exécution ainsi que la résolution des conflits de loi. Une première section se concentrera sur les relations contractuelles, tandis qu'une seconde se focalisera sur les relations extracontractuelles. Chacune s'efforcera de suivre le raisonnement conflictuel traditionnel, afin d'établir dans quelle mesure il peut s'appliquer ou non, de manière cohérente, à la réglementation relative à la protection des données personnelles.

Enfin, un quatrième chapitre proposera une explication, par des concepts de droit international privé, des constats établis par l'intermédiaire du *casus*. Il essaiera de montrer comment le fait même d'avoir une liberté, en tant que législateur, dans l'élaboration du champ d'application spatial de sa loi mène à des impasses que seule la pratique peut révéler. En effet, dans certains cas, les mineurs ou les responsables du traitement ne savent pas quelle loi d'exécution nationale respecter, aussi bien pour vérifier la validité du consentement de l'enfant que pour les autres questions où le droit national est pertinent. Ce chapitre se présentera alors comme un bilan des problématiques identifiées, ainsi qu'une occasion de proposer quelques pistes de réflexion. La méthode conflictuelle classique n'étant pas toujours satisfaisante, il peut s'avérer nécessaire de raisonner à partir d'autres mécanismes.

Nous voudrions ici prévenir le lecteur. La présente étude a l'ambition d'effectuer un travail d'identification de certaines hypothèses de conflits de lois qui peuvent se poser suite à l'adoption du RGPD, sans prétendre en élucider tous les mystères. Ne souhaitant pas entamer une critique vis-à-vis du travail du législateur européen, ce mémoire a simplement pour but de présenter et de clarifier une lacune du règlement qu'il a élaboré ; lacune qui ne paraît pas évidente à sa seule lecture. Même identifiée, celle-ci a pu paraître « insignifiante » aux yeux de certains. Ainsi donc l'ambition de la présente étude est de montrer, par un cas pratique, les conséquences, pourtant considérables, de l'absence de règle de conflits de lois, dans un instrument juridique qui laisse une ample place à la « subjectivité » de chaque législateur. Le mémoire aspire à dépasser les aspects théoriques de cette coexistence entre règlement – supranational – et lois nationales, afin de se plonger dans la pratique et de révéler, concrètement, les problèmes qui se posent. Ce n'est qu'une fois que l'on parvient à identifier ces derniers, qu'on peut nourrir l'espoir de les comprendre et, éventuellement, de les résoudre...

## **Chapitre 1. Remarques préliminaires : un cadre juridique global définissant son applicabilité**

Le cadre législatif européen sur la protection des données personnelles à caractère personnel a été modifié avec l'entrée en vigueur du RGPD. La réglementation des données a été amenée à évoluer avec le temps, notamment à la suite de l'adoption du Traité de Lisbonne, tout en maintenant un champ d'application personnel et matériel en continuité avec cet historique (Section I).

Une telle évolution n'a pu se faire sans prendre en considération les caractéristiques principales de ce droit. Il est, en effet, caractérisé par sa nature juridique « hybride » ainsi que son caractère habituellement transnational, particulièrement dans un monde numérique sans frontières, qui ne cesse d'être le résultat de nombreux progrès technologiques (Section II). Dans ce contexte, le règlement prend le soin de délimiter son champ d'application dans l'espace, aussi bien en ce qui concerne les relations intra-européennes qu'extra-européennes (Section III). Le règlement s'inspire, sur certains points, de son prédécesseur mais innove par rapport à d'autres, suscitant alors toute une série de questions pratiques, pouvant perturber cette volonté d'innovation dans la protection dont il se prétend garant.

### **Section I. Une nouvelle base juridique**

Tout acte juridique s'inscrit dans un contexte et dans des discussions ayant précédé son élaboration. Le législateur européen a posé un choix quant à la forme juridique la mieux adaptée pour la protection des données personnelles au vingt-et-unième siècle. La protection, jusque-là assurée par une directive, l'est désormais au moyen d'un règlement (§ 1), avec tout ce que cela engendre comme conséquences logiques et implications, que nous analyserons par la suite.

Par ailleurs, toute analyse de la matière des données personnelles implique une certaine terminologie, sans laquelle des confusions existeraient sur ce qui serait inclus dans le champ d'application du nouveau règlement et ce qui ne le serait pas. Une brève analyse de celle-ci s'avère donc nécessaire pour aborder la matière (§ 2).

#### **§1. Choix de l'instrument juridique approprié**

La volonté du législateur de réglementer par un seul instrument le droit européen de la protection des données a été animée par le constat d'un environnement juridique fragmenté suite aux vingt-sept lois de transpositions de la directive 95/46/CE . En effet, bien que l'objectif de la directive ait été de mettre en œuvre un niveau équivalent de protection des données, en pratique, des exigences différentes existaient entre Etats membres quant aux règles mises en œuvre, menant ainsi à une grande insécurité juridique<sup>8</sup>. Ces disparités étaient notamment dues à la trop large marge de manœuvre laissée dans certains

---

<sup>8</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données (...), *op. cit.*, p. 2.

domaines aux Etats lors de la transposition ainsi qu'aux définitions générales de la directive interprétées différemment par ceux-ci<sup>9</sup>. Le besoin s'est donc fait sentir d'adopter un cadre harmonisé et cohérent, qui tiendrait également compte des évolutions technologiques. En effet, « *la nécessité d'une harmonisation repose sur un constat d'inefficacité, de carence ou de contradiction des règles existantes. A cet égard, l'absence comme la multiplicité des règles peuvent constituer des indices de l'utilité éventuelle de l'intervention* »<sup>10</sup>.

Un des facteurs qui a permis la révision de la directive 95/46/CE a été l'entrée en vigueur du Traité de Lisbonne, marquant le point de départ d'« *une nouvelle ère pour la protection des données* »<sup>11</sup>. Jusque-là, l'Union européenne avait établi ses législations par secteur, en raison de sa structure en piliers<sup>12</sup>. Les trois piliers caractérisaient, jusqu'en 2007, le paysage institutionnel de l'Union européenne : le premier pilier était le pilier communautaire ; le second était relatif à la politique étrangère et la sécurité commune ; le troisième pilier concernait la coopération dans les domaines de la justice et des affaires intérieures<sup>13</sup>. Plus précisément, pour la matière des données personnelles, il avait opté pour la directive 95/46/CE pour légiférer dans le domaine du marché intérieur (matière commerciale), tandis que, pour la coopération policière et judiciaire en matière pénale, l'instrument juridique retenu avait été celui de la décision-cadre 2008/977/JAI<sup>14</sup>. Toutefois, la pratique avait révélé qu'un stockage de données relevant de la matière commerciale (ex-premier pilier) pouvait être utile pour répondre à des « *préoccupations sécuritaires de l'ex-troisième pilier* »<sup>15</sup>. En vue de lutter contre cette fragmentation de la mise en œuvre de la protection des données personnelles, l'Union européenne a choisi d'opter pour une approche globale et intelligible de la matière par l'abolition de la structure en piliers dans le cadre du Traité de Lisbonne<sup>16</sup>. En premier lieu, les article 8 de la Charte des droits fondamentaux<sup>17</sup> et article 16 §1<sup>er</sup> du Traité sur le fonctionnement de l'Union européenne<sup>18</sup> (ci-après « TFUE ») reconnaissent le droit, pour toute personne, à la protection de ses données personnelles<sup>19</sup>. En deuxième lieu, l'article 16 §2 TFUE fournit une nouvelle base juridique complète pour l'adoption d'un cadre législatif en matière de protection des données personnelles au niveau de l'Union, indépendamment des matières concernées<sup>20</sup>, selon la procédure législative ordinaire<sup>21</sup>.

---

<sup>9</sup> S. PEYROU, « Un nouveau cadre juridique général pour la protection des données au sein de l'Union européenne : une réforme législative ambitieuse », *R.A.E. – L.E.A.*, 2012, p. 153.

<sup>10</sup> V.L. BENABOU, « Faut-il une harmonisation minimale du droit », in *Le droit international de l'internet* (sous la dir. de G. CHATILLON), Bruxelles, Bruylant, 2002, p. 180.

<sup>11</sup> Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée — « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », adopté le 14 janvier 2011, p. 3, point 16.

<sup>12</sup> S. PEYROU, « Un nouveau cadre juridique général pour la protection des données (...) », *op. cit.*, p. 152.

<sup>13</sup> *Ibid.* ; S. VAN RAEPENBUSCH, « La réforme institutionnelle du traité de Lisbonne : l'émergence juridique de l'Union européenne », *C.D.E.*, 2007, pp. 578 et s.

<sup>14</sup> Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.*, 30 décembre 2008, L 350, p. 60.

<sup>15</sup> S. PEYROU, « Un nouveau cadre juridique général pour la protection des données (...) », *op. cit.*, p.154.

<sup>16</sup> Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions. Protection de la vie privée dans un monde en réseau Un cadre européen relatif à la protection des données, adapté aux défis du 21<sup>e</sup> siècle, adoptée le 25 janvier 2012, COM (2012) 9 final, p. 3.

<sup>17</sup> Charte des droits fondamentaux de l'Union européenne, art. 8, *J.O.U.E.*, 26 octobre 2012, C 326.

<sup>18</sup> Traité sur l'Union européenne (version consolidée), art. 16 §1, *J.O.U.E.*, 26 octobre 2012, C 326. (ci-après « TUE »).

<sup>19</sup> Avis du Contrôleur Européen de la Protection des données (...), *op. cit.*, adopté le 14 janvier 2011, p. 3, point 18.

<sup>20</sup> S. PEYROU, « Un nouveau cadre juridique général pour la protection des données (...) », *op. cit.*, p.154.

<sup>21</sup> L'article 16 §2 du TFUE énonce que « *Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les Etats membres dans l'exercice d'activités qui*

L'article 16 TFUE est, en d'autres termes, devenu la base juridique pour l'adoption de règles en matière de protection de données<sup>22</sup>.

La Commission aurait pu soumettre un instrument unique, mais elle n'a pas exploité cette possibilité prévue par l'article 16 TFUE, poursuivant ainsi la pilariséation entre les matières pénale et commerciale en termes d'instruments juridiques relatifs à la matière des données personnelles<sup>23</sup>. Par conséquent, la proposition législative a pris la forme d'un règlement en matière de protection des données personnelles et d'une directive concernant le domaine de la coopération policière et judiciaire en matière pénale<sup>24</sup>.

Il n'en demeure pas moins que le passage d'une directive à un règlement pour la protection des données à caractère personnel est, en soi, révolutionnaire. Tout comme la directive, le but de ce règlement est double, à savoir de garantir le droit fondamental des individus à la protection des données ainsi que de créer un véritable marché intérieur, afin de faciliter le transfert de ces données. De plus, par son applicabilité directe ainsi que par son caractère obligatoire, le règlement permettrait de « *réduire la fragmentation juridique et d'apporter une plus grande sécurité juridique* »<sup>25</sup>. Dès sa proposition initiale, la Commission européenne avait l'intention de proposer « a single set of rules »<sup>26</sup>. Il y a là l'idée prometteuse d'un seul corps de règles sur les données personnelles, dans un marché intérieur.

## **§2. Champs d'application matériel et personnel du RGPD**

Certains termes spécifiques à la matière des données personnelles méritent d'être expliqués brièvement, afin de mieux comprendre les développements qui vont suivre. Il s'agit des quelques notions récurrentes, qui déclenchent, en grande partie, l'application du règlement.

### 1. Les données à caractère personnel

Une donnée à caractère personnel est définie par le règlement comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable* »<sup>27</sup>. Tous les éléments de la définition de ces termes sont repris de la directive 95/46/CE. Tous types d'informations y sont visés : aussi bien privées

---

*relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes ».*

<sup>22</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données (...), *op. cit.*, p. 6.

<sup>23</sup> C. GAYREL, R. ROBERT, « Proposition de règlement sur la protection des données – Premiers commentaires », *J.D.E.*, 2012, pp. 173-174.

<sup>24</sup> Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, 4 mai 2016, L 119, p. 89.

<sup>25</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données(...), *op. cit.*, p. 6.

<sup>26</sup> European Commission – Press release : «Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses», 25 janvier 2012, [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm](http://europa.eu/rapid/press-release_IP-12-46_en.htm) (consulté le 7 avril 2018).

<sup>27</sup> Art. 4, 1), du RGPD.

que publiques mais encore celles de nature commerciale ou professionnelle<sup>28</sup>. Les informations peuvent, par ailleurs, être exactes ou inexactes, objectives ou subjectives, sous la forme d'avis ou d'appréciations<sup>29</sup>.

Selon la jurisprudence de la Cour de justice de l'Union (ci-après également « CJUE » ou « Cour de justice »), même des informations ayant été diffusées notamment sur Internet, dans les médias ou la presse à un public indéfini en nombre peuvent être considérées comme « données à caractère personnel » et, dès lors, être protégées<sup>30</sup>. Ainsi donc, le critère principal pour établir si une donnée est personnelle, consiste à déterminer qu'elle se rapporte directement ou indirectement à une personne concernée, à savoir une personne identifiée ou identifiable, peu importe qu'elle concerne ou non la vie privée et familiale de celle-ci<sup>31</sup>. Une information sera également qualifiée de donnée à caractère personnel lorsqu'elle ne se suffit pas à elle-même pour identifier une personne ou que des éléments détenus par un tiers sont nécessaires pour son identification complète<sup>32</sup>. Ces termes sont donc interprétés de manière très large<sup>33</sup>.

## 2. Le traitement

Il s'agit de la deuxième notion importante en la matière. Un traitement est défini comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel »<sup>34</sup>. Aux termes de l'article 4 §2 du RGPD, des exemples d'opérations particulièrement variées sont citées comme traitements ; ainsi : « la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ». Il peut s'agir d'une opération unique ou d'une succession d'opérations effectuées dans la poursuite d'un même but<sup>35</sup>. Le traitement des données à caractère personnel visé peut, en outre, aussi bien être totalement ou partiellement automatisé que non automatisé s'il rassemble les données dans un fichier<sup>36</sup>. Notons, toutefois, que pour qu'un traitement manuel entre dans le champ d'application du RGPD, il est nécessaire que les données à caractère personnel soient structurées dans un fichier et accessibles selon des critères déterminés<sup>37</sup>.

---

<sup>28</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie* (sous la dir. de C. DE TERWANGNE et K. ROSIER), Bruxelles, Larcier, 2018, pp. 60-61.

<sup>29</sup> Arrêt Peter Nowak/Data Protection Commissioner, C-434/16, EU:C:2017:994, point 34.

<sup>30</sup> Arrêt Tietosuoja/valtuutettu/ Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, EU:C:2008:727, points 48-49.

<sup>31</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *op. cit.*, p. 61.

<sup>32</sup> B. DOCQUIR, *Droit du numérique : contrats, innovation, données et sécurité*, Bruxelles, Larcier, 2018, p. 382.

<sup>33</sup> Voy. également Arrêt Peter Nowak/Data Protection Commissioner, *op. cit.* qui prévoit dans son dispositif que les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examineur relatives à ces réponses constituent des données à caractère personnel au sens de l'article 2, sous a), de la directive 95/46.

<sup>34</sup> A. BEELEN, , *Guide pratique du RGPD : fiches de guidance*, Bruxelles, Bruylant, 2018, p. 21.

<sup>35</sup> B. DOCQUIR, *Droit du numérique : contrats, innovation, données et sécurité*, *op. cit.*, pp. 392-393.

<sup>36</sup> Art. 2, du RGPD. ; [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing\\_fr](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_fr) (consulté le 22 juin 2019).

<sup>37</sup> Art. 4, 6), du RGPD.

### 3. Les personnes concernées

Les données à caractère personnel doivent se rapporter à une personne physique. *A contrario*, elles ne peuvent être liées à des personnes morales ou à des personnes décédées<sup>38</sup>. Il faut, en outre, que ces données « concernent » la personne, sans qu'une définition de la nature ou de l'intensité de ce lien entre l'information et la personne ne soit établie par le règlement<sup>39</sup>. Les informations doivent permettre d'identifier une personne, « *directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »<sup>40</sup>. La Cour de justice de l'Union précise, à cet égard, que la personne est concernée « *lorsque, en raison de son contenu, sa finalité ou son effet, l'information est liée à une personne déterminée* »<sup>41</sup>. Il s'agit là de critères alternatifs<sup>42</sup>. La personne doit ainsi être identifiée ou identifiable. Ce dernier terme renvoie à une personne qui, quoique non encore identifiée par une information à elle seule, pourrait l'être suite à une combinaison d'informations<sup>43</sup>. Si un tel lien entre une ou plusieurs données et une personne n'est pas établi, les données seront qualifiées d'anonymes et seront, par conséquent, exclues du champ d'application du règlement<sup>44</sup>.

### 4. Les responsables de traitement et les sous-traitants

Le responsable de traitement joue un rôle primordial à travers le règlement, puisque c'est à lui qu'incombe la majeure partie des obligations qui y sont prévues en faveur de la protection des personnes concernées par les données faisant l'objet du traitement. En vertu de l'article 4 §7 du RGPD, un responsable de traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Il s'agit là d'une notion communautaire. Cette qualification peut soit découler directement ou indirectement d'un texte législatif soit d'une analyse des faits de l'espèce, selon les cas<sup>45</sup>. Afin de démontrer cette approche factuelle, le Groupe de Travail « Article 29 » (ci-après GT art. 29)<sup>46</sup>, remplacé dorénavant par le Comité européen de la protection des données (ci-après CEPD)<sup>47</sup>, explique qu'une entité devient responsable de traitement, lorsqu'elle décide de traiter des données à caractère personnel pour des

---

<sup>38</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *op. cit.*, p. 63.

<sup>39</sup> B. DOCQUIR, *Droit du numérique : contrats, innovation, données et sécurité*, *op. cit.*, p. 385.

<sup>40</sup> Art. 4, 1), du RGPD.

<sup>41</sup> Arrêt Peter Nowak/Data Protection Commissioner, *op. cit.*, point 35.

<sup>42</sup> N. MICHAÏL « Le domaine d'application du GDPR : de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *R.D.C.*, 2019, p. 56.

<sup>43</sup> *Ibid.*, p. 57 ; voy. également l'Arrêt Patrick Breyer/Bundesrepublik Deutschland, C-582/14, EU:C:2016:779 développé dans cet article.

<sup>44</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *op. cit.*, p. 64.

<sup>45</sup> Avis 1/2010 du Groupe de Travail « Article 29 » sur les notions de « responsable du traitement » et de « sous-traitant » (WP 169), adopté le 16 février 2010, p. 9.

<sup>46</sup> Il s'agit du groupe de travail européen indépendant qui traitait les questions relatives à la protection des données personnelles et de la vie privée jusqu'à l'entrée en vigueur du RGPD, à savoir le 25 mai 2018, [https://edpb.europa.eu/our-work-tools/article-29-working-party\\_fr](https://edpb.europa.eu/our-work-tools/article-29-working-party_fr) (consulté le 28 juin 2019).

<sup>47</sup> Voy. art. 68 et s., du RGPD ; <https://edpb.europa.eu> (consulté le 28 juin 2019).

finalités qui lui sont propres<sup>48</sup>. Ainsi, l'importance de cette notion repose sur l'influence exercée par l'opérateur soit sur les moyens soit sur les finalités du traitement, ou encore sur les deux, et pas nécessairement sur le traitement en tant que tel effectué par ce même opérateur<sup>49</sup>. Cela doit donc être vérifié au cas par cas, en fonction notamment des opérations de traitement entreprises et de la personne qui les détermine avec un pouvoir de décision<sup>50</sup>.

La Cour de justice de l'UE semble étendre davantage cette interprétation dans un arrêt récent relatif à la collecte et aux traitements ultérieurs de données à caractère personnel effectués par des membres d'une communauté religieuse dans le cadre d'une activité de prédication de porte-à-porte<sup>51</sup>. Elle a, de fait, considéré qu'« *une personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et participe de ce fait à la détermination des finalités et des moyens de ce traitement, peut être considérée comme étant responsable du traitement* »<sup>52</sup>. L'influence sur le traitement en tant que tel semble devenir également un critère déterminant<sup>53</sup>. Un autre arrêt récent vient également perturber le paysage juridique en la matière, en incluant dans la qualification de responsable de traitement les administrateurs de pages Facebook, au même titre que Facebook<sup>54</sup>.

Le sous-traitant, quant à lui, est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ». Il s'agit donc d'une personne distincte du responsable du traitement<sup>55</sup>. Depuis l'adoption du RGPD, les sous-traitants ont vu leur rôle s'élargir et se retrouvent directement soumis à certaines obligations nouvelles<sup>56</sup>. Ils peuvent, dès lors, être sanctionnés par des autorités de contrôle en cas de non-respect de celles-ci, même s'ils ne déterminent pas les moyens ou les finalités du traitement<sup>57</sup>. Une même personne peut être responsable de traitement pour une opération et sous-traitant dans le cadre d'une autre<sup>58</sup>.

Notons que les aspects de droit international privé du contrat ou acte juridique entre le responsable de traitement et le sous-traitant seront régis par le droit international privé commun en matière contractuelle, à défaut de disposition expresse dans le règlement<sup>59</sup>.

---

<sup>48</sup> Avis 1/2010 du Groupe de Travail « Article 29 » sur les notions de « responsable du traitement » et de « sous-traitant », *op. cit.*, p. 9.

<sup>49</sup> N. MICHAIL « Le domaine d'application du GDPR : (...) », *op. cit.*, p. 59.

<sup>50</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *op. cit.* p. 68 ; B. DOCQUIR, *Droit du numérique : contrats, innovation, données et sécurité*, *op. cit.*, p. 400.

<sup>51</sup> Arrêt *Jehovan todistajat – uskonnollinen yhdyksunta*, C-25/17, EU:C:2018:551, point 21.

<sup>52</sup> *Ibid.*, point 28.

<sup>53</sup> Pour un bref commentaire sur cet arrêt voy. N. MICHAIL « Le domaine d'application du GDPR : (...) », *op. cit.*, p. 59.

<sup>54</sup> *Ibid.*, pp. 60-61.

<sup>55</sup> Avis 1/2010 du Groupe de Travail « Article 29 » sur les notions de « responsable du traitement » et de « sous-traitant », *op. cit.*, p. 1.

<sup>56</sup> Voy. par exemple le considérant 82 du RGPD qui prévoit que le sous-traitant, tout comme le responsable de traitement, devrait tenir des registres pour les activités de traitement relevant de sa responsabilité ou encore l'obligation de désigner un délégué à la protection des données dans les cas prévus à l'article 37 §1<sup>er</sup> du RGPD.

<sup>57</sup> A. BEELEN, *op. cit.*, p. 121.

<sup>58</sup> C. DE TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *op. cit.*, p. 69.

<sup>59</sup> N. MICHAIL « Le domaine d'application du GDPR : (...) », *op. cit.*, p. 64.

## Section II. Les caractéristiques principales du droit à la protection des données personnelles

Une réflexion sur le droit applicable ne peut être menée sans avoir conscience de certains éléments inhérents à la protection des données, qui pourraient avoir un impact sur la détermination de celui-ci.

### §1. Nature juridique du droit

Tout d'abord, le droit à la protection des données personnelles est un droit qui contient des caractéristiques de plusieurs branches du droit, notamment du droit de la protection du consommateur, des droits de l'homme, du droit public et du droit civil<sup>60</sup>. Il s'agit donc d'un droit de nature hybride<sup>61</sup>.

L'identification du domaine du droit concerné peut avoir des implications sur le droit applicable. En effet, en fonction du secteur du droit en question, il existe un ou plusieurs critères de rattachement établissant un lien pertinent avec la loi d'un pays qui doit être appliquée. Souvent, les questions liées à la protection des données relèveront de plusieurs branches différentes. Ainsi, le droit à la protection des données personnelles peut contenir des aspects de nature publique pour tout ce qui concerne les décisions et devoirs d'une autorité publique qui traite des données personnelles, mais également des aspects de droit civil pour des questions liées à la responsabilité quant à une violation de données<sup>62</sup>. Il semble, par conséquent, préférable de prendre en considération l'activité ou la question concrète en cause pour la qualification du droit et non de conclure, *a priori*, sur la nature uniquement publique ou privée du droit à la protection des données à caractère personnel<sup>63</sup>.

### §2. Difficulté de rattachement à un seul territoire

Deuxièmement, le nombre croissant d'activités transfrontières dans l'ère du numérique rendent la limite entre compétence territoriale et extraterritoriale plus floue qu'auparavant<sup>64</sup>. En effet, il y a quelques années, la localisation d'un traitement de données ne suscitait pas de questions, sachant que, généralement, tant le responsable de traitement, les personnes concernées que les moyens utilisés pour le traitement étaient facilement rattachables à un seul pays<sup>65</sup>. C'est dans ce contexte-là que la directive 95/46/CE avait été adoptée dans les années 90. Toutefois, avec le développement de la société de l'information, l'expansion de l'Internet et, plus généralement, les progrès technologiques, la réalité de la

---

<sup>60</sup> D. COOPER, C. KUNER, « Data Protection Law and International Dispute Resolution », *Académie de Droit international 382 Recueil des Cours*, 2017, pp. 57-58.

<sup>61</sup> *Ibid.*, p. 57.

<sup>62</sup> J. BING, « Data Protection, Jurisdiction and the Choice of Law », 21st International Conference on Privacy and Personal Data Protection, Office of the Privacy Commissioner for Personal Data, Hong Kong 1999. p. 2.

<sup>63</sup> C. KUNER, « Data Protection Law and International Jurisdiction on the Internet (Part 1) », *I.J.L.I.T.*, 2010, p. 185.

<sup>64</sup> M. GÖNMANN, « The new territorial scope of EU data protection law: deconstructing a revolutionary achievement », *C.M.L. Rev.*, 2017, p. 568.

<sup>65</sup> P. DE HERT, M. CZERNIAWSKI, « Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context », *I.D.P.L.*, 2016, p. 230.

protection des données personnelles est devenue une affaire transnationale<sup>66</sup>. Les données des résidents de l'UE sont désormais non seulement traitées dans l'UE mais également en dehors de l'UE. L'idée de territorialité ne tient plus<sup>67</sup>. C'est la raison pour laquelle certains auteurs parlent de l'effet « extraterritorial » de la protection des données, puisqu'une loi peut, par exemple, s'appliquer à des responsables de traitement ou des traitements en tant que tels situés hors du pays qui l'a promulguée<sup>68</sup>.

La localisation des données n'est donc plus si évidente. La société du numérique implique qu'en permanence des données sont générées via internet et envoyées à un opérateur quelque part dans le monde pour être traitées. Les critères liant alors un événement précis à un territoire perdent ainsi leur pertinence<sup>69</sup>. Dans ce contexte, les questions de droit applicable à une situation ne font que se complexifier et présentent un réel enjeu pour les législateurs nationaux.

### **Section III. Les caractéristiques de l'article 3 du règlement**

Pour comprendre les nouveautés apportées par le Règlement général sur la protection des données à caractère personnel en matière d'applicabilité, il est intéressant de revenir sur l'instrument juridique qui l'a précédé, à savoir la directive 95/46/CE (§ 1). Ainsi, le contenu et les apports du nouvel article 3 du RGPD pourront être mieux compris (§ 2). C'est, en outre, précisément sur la modification de cet article que trouve son fondement notre réflexion sur les conflits de lois entre Etats membres, cet article ne contenant plus de règle relative au droit applicable (§ 3).

#### **§1. Analyse préalable : état des lieux de l'article 4 de la directive**

##### 1. Présentation de l'article

L'article 4 de la directive 95/46/CE prévoyait la détermination de la loi applicable en matière de protection des données à caractère personnel au niveau de l'Union européenne. Il s'agissait du premier instrument international en matière de protection des données optant pour une règle de conflits de lois<sup>70</sup>. En effet, cet article apportait une solution à deux types de problèmes : d'une part, quand la loi d'un Etat membre serait-elle applicable par opposition à une loi étrangère et, d'autre part, quelle loi de transposition faudrait-il appliquer en particulier à l'intérieur de l'Union européenne.<sup>71</sup>

---

<sup>66</sup> P. DE HERT, M. CZERNIAWSKI, *op. cit.*, pp. 230-231.

<sup>67</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Le règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé », *D.*, 2016, p. 1875.

<sup>68</sup> D. COOPER, C. KUNER, *op. cit.*, pp. 69-70.

<sup>69</sup> J. BING, *op. cit.*, p. 3.

<sup>70</sup> L. A. BYGRAVE, « European data protection. Determining applicable law pursuant to European data protection legislation », *Computer Law & Security Report*, 2000, pp. 252-253.

<sup>71</sup> M. BRKAN, « Data Protection and Conflict-of-laws: A Challenging Relationship », *E.D.P.L.*, 2016, p. 326 ; Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable (WP 179), adopté le 16 décembre 2010, p. 6.

Cet article était rédigé comme suit :

« 1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable;

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même ».

Cet article était nécessaire dans le cadre d'une directive appelée à être transposée par les 28 Etats membres concernés lors de son adoption, et présentait le mérite de donner une base de lignes directrices pour résoudre les questions de conflits de lois qui pouvaient se poser. Toutefois, en raison des disparités dans la mise en œuvre de ce corps de règles par les Etats membres, la fragmentation dans le niveau de protection du droit à la protection des données à caractère personnel n'en était qu'accrochée<sup>72</sup>. Par conséquent, le libre flux de ces données à travers l'Union était impacté et cela suscitait, en outre, la tentation de procéder à du *forum shopping* dans le choix du lieu d'établissement du responsable du traitement, afin d'obtenir l'application d'une loi plus protectrice<sup>73</sup>. A cet égard, la Commission européenne a émis, en 2010, une communication intitulée « une approche globale sur la protection des données à caractère personnel dans l'Union européenne ». A travers cette dernière, elle insiste notamment sur la nécessité de clarifier les règles relatives au droit applicable, ainsi que de déterminer « *quel est l'Etat membre responsable de l'application des règles en matière de protection des données et, en définitive, d'assurer le même niveau de protection à tous les résidents de l'Union concernés, indépendamment du lieu d'établissement du responsable du traitement* »<sup>74</sup>.

## 2. La notion d'établissement telle qu'interprétée par la Cour de justice

Suite à l'intervention de la Cour de justice, cet article a été également amené à régler le champ d'application dans l'espace de la directive. Comme le définit l'auteur P. Mayer, « *le domaine d'application d'une règle dans l'espace est déterminé par un critère spatial incorporé dans le présupposé de la règle et qui constitue l'une des conditions du déclenchement de son effet juridique* »<sup>75</sup>.

<sup>72</sup> Considérant 9, du RGPD. ; B. CUSTERS, F. DECHESNE, A. M. SEARS, T. TANI, S. VAN DER HOF, « A comparison of data protection legislation and policies across the EU », *C.L.S.R.*, 2018, pp. 241-242.

<sup>73</sup> F. JAULT-SESEKE, « La portée extraterritoriale ou a-territoriale du RGPD », *R.A.E.-L.E.A.*, 2018, p. 45.

<sup>74</sup> Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », adoptée le 4 novembre 2010, COM (2010) 609 final, pp. 12-13.

<sup>75</sup> P. MAYER, « Les lois de polices étrangères », *J.D.I.*, 1981, p. 282.

La règle initialement vouée à déterminer la loi applicable a ainsi également eu la fonction de règle d'applicabilité<sup>76</sup>. La CJUE a notamment interprété la notion d'établissement du responsable de traitement, qui était le critère principal pour déterminer la loi applicable en vertu de l'article 4 §1<sup>er</sup> point (a), mais n'était pourtant pas défini par le texte. La Cour comprend largement le champ d'application territorial de la directive 95/46/CE, en s'appuyant en particulier sur son considérant 19<sup>77</sup>, qui prévoyait que l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité – même minime<sup>78</sup> – au moyen d'une installation stable, indépendamment de la forme juridique adoptée par cet établissement<sup>79</sup>. Par conséquent, des responsables de traitement basés hors de l'UE pouvaient être forcés à se conformer à la législation européenne en matière de données personnelles par le simple fait qu'ils avaient un certain niveau de présence dans l'UE, par une filiale ou une succursale par exemple<sup>80</sup>. Il s'agit d'une interprétation téléologique de l'article, en vue d'assurer une protection effective des droits fondamentaux des individus<sup>81</sup>. Elle s'écarte donc d'une interprétation rigide de la notion, selon laquelle les entreprises seraient établies uniquement dans l'Etat où elles sont enregistrées, mais favorise, à la place, la recherche de la réalité de l'exercice des activités<sup>82</sup>. Après avoir établi si le responsable de traitement possède un établissement dans ou en dehors de l'Union, la Cour considère qu'il importe, dans un deuxième temps, de déterminer si le traitement a lieu « dans le cadre » des activités de l'établissement et non s'il a lieu « par » l'établissement<sup>83</sup>. Elle opte, de cette façon, encore une fois pour une interprétation souple de la notion.

## **§2. Champ d'application territorial du RGPD**

L'article 3 du RGPD définit le champ d'application dans l'espace du règlement, afin d'élargir la protection offerte aux individus dont les données sont traitées. Le RGPD s'applique, en premier lieu, au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement sur le territoire de l'Union, quel que soit le lieu où le traitement est effectué, aussi bien dans l'Union qu'en dehors<sup>84</sup>. Il s'agit là d'une reprise du critère du premier paragraphe de l'article 4 de la directive, à la différence qu'il s'étend désormais non seulement à l'établissement du responsable du traitement, mais également à celui du sous-traitant<sup>85</sup>. L'interprétation de la notion par la CJUE reste donc pertinente. Le considérant 22 du règlement<sup>86</sup> est, par ailleurs, rédigé dans des termes similaires au considérant 19 mentionné ci-dessus, marquant ainsi une certaine continuité entre les deux textes européens concernant leur territorialité<sup>87</sup>.

---

<sup>76</sup> F. JAULT-SESEKE, *op. cit.*, p. 46.

<sup>77</sup> Arrêt Google Spain SL (...), *op. cit.*, point 48. ; Arrêt Weltimmo (...), *op. cit.*, point 28.

<sup>78</sup> Arrêt Weltimmo (...), *op. cit.*, point 31.

<sup>79</sup> Considérant 19, de la directive 95/46/CE.

<sup>80</sup> P. DE HERT, M. CZERNIAWSKI, *op. cit.*, p. 233.

<sup>81</sup> M. GÖMANN, *op. cit.*, p. 571.

<sup>82</sup> *Ibid.*; Arrêt Weltimmo (...), *op. cit.*, point 29.

<sup>83</sup> Arrêt Google Spain SL (...), *op. cit.*, point 52. ; Arrêt Weltimmo (...), *op. cit.*, points 34-35.

<sup>84</sup> Art. 3, §1<sup>er</sup>, du RGPD.

<sup>85</sup> S. PEYROU, « Un nouveau cadre juridique général pour la protection des données ... », *op. cit.*, p. 149.

<sup>86</sup> Le considérant 22 du RGPD est rédigé dans les termes suivants : « *Tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même ait lieu ou non dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.* ».

<sup>87</sup> M. GÖMANN, *op. cit.*, p. 575.

Lorsque les opérateurs ne possèdent pas d'établissement sur le territoire de l'Union<sup>88</sup>, le règlement s'applique au traitement de données relatives à des personnes qui se trouvent sur le territoire de l'Union, lorsque les activités de traitement sont soit liées à l'offre de biens ou de services à ces personnes concernées, soit au suivi de leur comportement<sup>89</sup>. Le règlement s'applique, enfin, lorsque le responsable du traitement est établi dans un lieu où le droit d'un État membre s'applique en vertu du droit international public<sup>90</sup>. Le critère subsidiaire d'application du règlement a donc changé pour rendre l'application de celui-ci plus efficace<sup>91</sup>. En effet, les responsables du traitement établis hors de l'UE ne seront plus concernés par la législation européenne en fonction de leur recours à des « moyens situés sur le territoire d'un Etat membre », mais s'ils ciblent des individus dans l'Union<sup>92</sup>.

### **§3. Absence de règle de conflit de lois**

La grande différence entre l'article précité de la directive et celui du nouveau règlement est que le législateur semble avoir estimé qu'il n'était pas nécessaire de réitérer – en tout cas par écrit – une règle de conflits de lois. Il est compréhensible qu'à première vue, l'enjeu des conflits de lois soit de moindre importance. La protection des données personnelles, jusque-là assurée par une directive, l'est désormais par un règlement, par nature d'application directe en droit interne<sup>93</sup>. Nous passons donc de 28 versions nationales différentes d'une source législative commune à un texte unique qui est automatiquement juridiquement contraignant dans les différents Etats membres et ne nécessite, en théorie, pas de transposition<sup>94</sup>. Le RGPD s'insère dans les ordres juridiques nationaux. Une grande partie des disparités entre législations nationales sont ainsi supposées être gommées<sup>95</sup>. Les dispositions sont, dès lors, vouées à s'appliquer uniformément sur le territoire de l'UE. Cela peut, par exemple, être illustré par le fait que la référence « au territoire d'un Etat Membre » dans l'article 4 §1<sup>er</sup> de la directive sur les données personnelles a été remplacée dans l'article 3 §1<sup>er</sup> du règlement par « le territoire de l'Union ».

La question du droit national applicable ne serait pas un problème si le règlement se suffisait à lui-même et mettait fin à la nécessité de lois nationales sur la protection des données personnelles<sup>96</sup>. Toujours est-il que le règlement ne procède pas à une uniformisation complète du droit en la matière, puisqu'il permet aux Etats d'avoir une marge de manœuvre sur certains points, pour ce qui les concerne<sup>97</sup>. Les lois

---

<sup>88</sup> Notons, à cet égard, que le G. art. 29 a considéré dans le cadre de la directive que doivent être compris comme établis hors de l'UE aussi bien les responsable de traitement qui ne disposent pas d'installation sur le territoire de l'Union pouvant être qualifiée d'établissement au sens de l'article 4.1.a) que les responsables qui possèdent un tel établissement mais que ce dernier n'est pas pertinent au regard du traitement ou des activités considérés. Voy. Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable, *op. cit.*, pp. 21-22.

<sup>89</sup> Art. 3, §2, du RGPD.

<sup>90</sup> Art. 3, §3, du RGPD.

<sup>91</sup> Voy. notamment sur le sujet Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable, *op. cit.*, pp. 23-24.

<sup>92</sup> C. GAYREL, R. ROBERT, « Proposition de règlement sur la protection des données – Premiers commentaires », *J.D.E.*, 2012, p. 174

<sup>93</sup> R. SCHÜTZE, *European Constitutional Law*, Cambridge, Cambridge university press, 2016, 91.

<sup>94</sup> Cfr. art. 288 §2, du TFUE

<sup>95</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Le règlement 2016/679/UE relatif (...), *op. cit.*, p. 1875.

<sup>96</sup> J. CHEN, «How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation», *I.D.P.L.*, 2016, p. 312.

<sup>97</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Le règlement 2016/679/UE relatif (...), *op. cit.*, p. 1876.

nationales demeurent pertinentes, alors même que le règlement ne prévoit pas de règle de conflits de lois. Pourtant, ces derniers sont toujours susceptibles de se poser, particulièrement dans les cas où les lois nationales d'exécution optent pour un contenu différent.

Se pose évidemment la question de savoir à quel point cette « imprévision » du législateur européen, en n'insérant pas de règle de conflit de lois, est volontaire ou involontaire. Une possibilité pourrait être de dire qu'il était naturel, selon lui, d'inférer du nouveau règlement sur la protection des données une règle de conflit inspirée de la directive. Peut-être encore cette absence de règle reflète-t-elle simplement un oubli de sa part et faut-il interpréter l'esprit du règlement. En tout état de cause, une analyse du cadre juridique, tel qu'il se présente actuellement, mérite d'être menée, afin de comprendre toutes les implications de ce changement législatif du point de vue des relations entre Etats membres.

## **Chapitre 2. Les conflits de lois dans les relations intra-européennes : les scénarios**

Le règlement permet donc, dans certaines de ses dispositions, une intervention des législateurs nationaux. Le droit des données à caractère personnel n'est pas entièrement uniformisé. Une analyse des principaux scénarios prévus par le règlement laissant place à une exécution normative du RGPD semble nécessaire, afin d'appréhender les éventuels conflits de lois qui peuvent se poser par la suite (Section I). Une fois ces dispositions identifiées, le RGPD n'est plus concerné et nous nous focaliserons sur les lois nationales et leurs champs d'application respectifs en nous basant sur un exemple, l'article 8 du règlement relatif conditions applicables au consentement des enfants (Section II).

### **Section I. Les limites à l'uniformisation**

Le législateur européen a opté pour un instrument juridique d'application directe, tout en permettant une intervention législative de la part des parlements nationaux. Or, il s'agit là d'une caractéristique non inhérente à la nature même des règlements européens, qui se distinguent en principe sur ce point des directives (§ 1).

Trois types de marges de manœuvres résultant du règlement sont à distinguer. Dans le texte même du RGPD, certaines dispositions obligent les législateurs nationaux à procéder à une exécution normative, tandis que d'autres offrent simplement la possibilité de compléter, d'adapter ou de déroger, sous certaines conditions, à la disposition concernée (§ 2). Enfin, la question du droit applicable se pose naturellement pour les questions non évoquées par le règlement (§ 3).

## §1. Présentation du caractère original du règlement

Le RGPD a vocation à mettre en place un niveau de protection des droits et libertés « équivalent dans tous les Etats membres »<sup>98</sup>. Pourtant, il n'assure pas une uniformisation complète de la protection des données à caractère personnel, puisqu'il délègue explicitement aux Etats membres la compétence pour adopter des mesures d'exécution normative des dispositions qui le prévoient<sup>99</sup>. Les personnes, entreprises ou Etats concernés auront donc affaire non seulement au texte du RGPD, mais également aux 28 (ou 27 après la sortie du Royaume-Uni de l'Union européenne) législations des Etats<sup>100</sup>. Les réglementations nationales ne pourraient, cependant, pas affaiblir le niveau général de protection des données à caractère personnel tel que mis en place par le règlement, ni apporter des entraves non permises par le règlement lui-même à la libre circulation des données dans l'Union<sup>101</sup>.

La question mérite d'être posée : comment se fait-il qu'un règlement, qui est une source directe de droits et d'obligations pour les Etats membres ou les individus concernés en vertu du droit européen, nécessite une implémentation ? En réalité, ce phénomène n'est pas si exceptionnel<sup>102</sup>. Tout d'abord, les Etats peuvent être amenés à modifier leur cadre législatif existant, dans le but d'être en conformité avec le règlement. Ils adoptent donc des mesures d'exécution pour modifier ou supprimer les dispositions de droit national qui étaient incompatibles avec le RGPD<sup>103</sup>. De plus, il arrive assez fréquemment que le législateur européen invite les Etats membres à adopter des législations implémentant les dispositions des règlements, en général pour les compléter ou y déroger dans les limites prévues par ceux-ci. A titre d'exemple, citons l'article 8 §1<sup>er</sup> alinéa 2 du RGPD relatif au consentement du mineur, qui sera analysé ci-dessous, qui prévoit que « *Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans* »<sup>104</sup>.

L'explication s'appuie sur la distinction entre « application directe » et « effet direct »<sup>105</sup>. La première notion signifie qu'aucun acte national de réception du texte n'est requis pour que le droit européen produise pleinement ses effets dans les ordres juridiques nationaux<sup>106</sup>. Les règlements européens sont d'application directe. Néanmoins, toutes leurs dispositions n'ont pas nécessairement effet direct<sup>107</sup>. En d'autres termes, bien que le principe soit que ces dernières ont un effet immédiat dans l'ordre interne, sans mesure d'implémentation nécessaire, il arrive que certaines dispositions nécessitent

---

<sup>98</sup> Condiérant 10, du RGPD.

<sup>99</sup> N. MICHAIL, « Le domaine d'application du GDPR : (...) », *op. cit.*, p. 75 ; A. THYSEN, « Titre préliminaire. L'application du droit communautaire : un aspect essentiel de sa « mise en œuvre » », in *L'application et le contrôle de l'application du droit communautaire par les administrations belges*, Gent, Academia press, p. 17.

<sup>100</sup> K. NOLAN, *op. cit.*, <http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/> (consulté le 5 juillet 2019).

<sup>101</sup> B. DOCQUIR, « Introduction générale », in *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 18.

<sup>102</sup> R. KRAL, « National normative implementation of EC regulations. An exceptional or rather common matter? », *E.L.R.*, 2008, p. 243.

<sup>103</sup> *Ibid.*, pp. 247-248.

<sup>104</sup> Art. 8, §1, al. 2, du RGPD.

<sup>105</sup> R. SCHÜTZE, *op. cit.*, p. 91.

<sup>106</sup> R. KRAL, *op. cit.*, p. 243.

<sup>107</sup> R. SCHÜTZE, *op. cit.*, pp. 91-92.

l'adoption de mesures d'exécution par les Etats, mesures sans lesquelles les individus ne peuvent se prévaloir des droits visés par les articles en question<sup>108</sup>.

Un tel constat perturbe la distinction entre directives et règlements européens, puisqu'il semble être possible d'implémenter les deux types d'actes. En quoi le passage d'une directive à un règlement européen serait-il alors tellement révolutionnaire dans la protection des données personnelles ? Ce qui change principalement avec le choix d'un règlement est qu'une transposition des termes de celui-ci est, en principe, interdite<sup>109</sup>. Les règlements intègrent directement les ordres juridiques nationaux, indépendamment d'une mesure de réception, de reproduction ou de reformulation en droit interne. Ils sont directement applicables et préservent ainsi leur « caractère communautaire »<sup>110</sup>. Il est uniquement requis d'adopter les mesures *nécessaires* à l'effectivité de leur contenu<sup>111</sup>. Au contraire, les directives doivent voir leur contenu intégralement transposé dans du droit national et reçoivent ainsi un « caractère national »<sup>112</sup>.

## **§2. Marges de manœuvre laissées aux législateurs nationaux**

Comme mentionné ci-dessus, deux catégories d'interventions législatives sont prévues par le règlement. Le RGPD exige, dans certains cas, des Etats membres de légiférer en complément du RGPD (point 1), tandis que pour d'autres aspects, il leur offre simplement la possibilité de le faire (point 2). Il s'agit ici uniquement d'un exercice, non exhaustif, d'identification de ces hypothèses qui créent une insécurité juridique, étant donné que le règlement ne définit pas quel sera le critère de rattachement dans ces cas pour départager la compétence des lois nationales<sup>113</sup>.

### 1. Actions requises de la part des Etats membres en vertu du RGPD

Nous pouvons reconnaître les hypothèses où une intervention des législateurs nationaux est obligatoire par l'utilisation du verbe « *shall* »<sup>114</sup> en anglais<sup>115</sup>. Dans la version en français, ces dispositions sont identifiées notamment par des mots tels que « veille à » ou « concilie par la loi »<sup>116</sup>. Citons, par exemple, l'article 54 du règlement qui prévoit notamment l'obligation pour les Etats d'assurer, « *par une loi* », « *la création d'une autorité de contrôle* »<sup>117</sup> ou encore l'article 84 §1<sup>er</sup>, selon lequel les « *États*

<sup>108</sup> Arrêt Azienda Agricola Monte Arcosu Srl/Regione Autonoma della Sardegna, C-403/98, EU:C:2001:6, points 26-28.

<sup>109</sup> K. NOLAN, op. cit., <http://btli.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/> (consulté le 5 juillet 2019).

<sup>110</sup> R. KRAL, op. cit., p. 248.

<sup>111</sup> *Ibid.*, p. 249.

<sup>112</sup> *Ibid.* De plus, tel qu'expliqué par l'auteur R. KRAL, bien que ce ne soit pas le cas pour le RGPD, les règlements *peuvent* requérir une mesure d'exécution normative alors que celle-ci est toujours requise dans le cadre d'une directive.

<sup>113</sup> C. DE TERWANGNE, K. ROSIER, B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, p. 14.

<sup>114</sup> Ce mot se traduit littéralement par « devoir » et indique plus généralement l'existence d'une obligation, voy. <https://www.merriam-webster.com/dictionary/shall> (consulté le 6 juillet 2019)

<sup>115</sup> M. FAZLIOGLU, « What the GDPR Requires of and Leaves to the Member States », *International Association of Privacy Professionals (IAPP)*, 2018, [https://iapp.org/media/pdf/resource\\_center/GDPR-Derogations-Whitepaper-FINAL.pdf](https://iapp.org/media/pdf/resource_center/GDPR-Derogations-Whitepaper-FINAL.pdf) (consulté le 6 juillet 2019).

<sup>116</sup> V. VERBRUGGEN, « Titre 1 – RGPD : cœur du puzzle de l'encadrement de la protection des données (...) », op. cit., p. 39.

<sup>117</sup> Art. 54, du RGPD.

membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives »<sup>118</sup>.

## 2. Actions possibles des Etats membres en vertu du RGPD

Nombreux sont également les exemples de dispositions qui laissent une faculté aux Etats membres d'exécuter le règlement sur un point précis. Il s'agit d'« *open clauses* » ou de dispositions ouvertes<sup>119</sup>. Elles sont généralement identifiées par l'utilisation du verbe « may » en anglais ou « pouvoir » en français. Mis à part l'article 8 qui sera analysé dans la section II du présent chapitre, nous pouvons citer comme autre exemple l'article 49 §5 du RGPD qui prévoit qu'« *en l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres notifient de telles dispositions à la Commission* »<sup>120</sup>. L'article 23 §1<sup>er</sup> du règlement permet, quant à lui, aux Etats de limiter la portée de certains droits et obligations prévus par le texte, à condition qu'une « *telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la défense nationale, la sécurité nationale, [...]* »<sup>121</sup>.

Nous constatons donc que le législateur européen accorde souvent une large marge de manœuvre aux législateurs nationaux, tout en établissant certaines conditions pour la mise en œuvre de celle-ci. De plus, des références au droit national des Etats sont faites tout au long du règlement, laissant entendre que son contenu est également à prendre en considération pour l'un ou l'autre domaine du droit, peu importe la substance effective de celui-ci<sup>122</sup>. Un tel renvoi général résulte de l'application par nature transversale de la protection des données à caractère personnel<sup>123</sup>.

### **§3. Silence du règlement**

La question du droit applicable à un traitement de données personnelles se posera également pour tout ce qui n'est pas visé par le RGPD. Il y a, en effet, une série de questions à propos desquelles le règlement est silencieux, comme certaines questions relatives à la validité du contrat (par exemple, le dol ou la nullité) ou encore aux modalités de rupture. Il s'agit de certains aspects matériels qui ne rentrent pas

---

<sup>118</sup> Art. 84, §1, du RGPD.

<sup>119</sup> V. VERBRUGGEN, « Titre 1 – RGPD : cœur du puzzle de l'encadrement de la protection des données (...) », *op. cit.*, p. 44.

<sup>120</sup> Art. 49, §5, du RGPD.

<sup>121</sup> Art. 23, §1, du RGPD.

<sup>122</sup> Voy. par exemple l'article 38, § 5 du RGPD qui précise que « *Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres* ».

<sup>123</sup> V. VERBRUGGEN, « Titre 1 – RGPD : cœur du puzzle de l'encadrement de la protection des données (...) », *op. cit.*, p. 39.

dans le domaine du règlement. Sur ces questions, il faudra de toute façon déterminer la loi applicable au contrat.

Cette question se posera également pour tout ce qui n'est pas visé en détail par le règlement. A titre exemplatif, l'article 82 du RGPD est relatif à la réparation qui peut être demandée par la personne concernée par le traitement en cas de préjudice matériel ou moral subi en raison de la violation du règlement, en particulier en cas de traitement illicite<sup>124</sup>. Bien que l'article précise certaines circonstances de responsabilité, des Etats membres ont probablement des règles de droit civil différentes, plus ou moins favorables sur l'évaluation du dommage ou sur l'établissement du lien causal. En l'absence de règle de conflits de lois, les parties pourraient procéder à du *forum shopping* en fonction des régimes juridiques prévus par les Etats (voy. *infra*).<sup>125</sup>

## **Section II. Les lois nationales exécutant le RGPD : Analyse au regard d'un exemple concret : l'âge du consentement du mineur à travers les lois belge et française**

Une fois qu'une situation entre bien dans le champ d'application territorial et matériel du règlement (cfr. exposé ci-dessus), le raisonnement n'est pas d'office clos pour ce qui est du cadre législatif applicable. Il peut s'agir soit d'une question entièrement traitée par le RGPD et, dans ce cas, la situation concernée est traitée uniformément, à travers les Etats-membres, par une disposition européenne. Il se peut, cependant, aussi que la disposition en cause du RGPD renvoie aux législations nationales qui ont exécuté le règlement, comme le prévoit l'article 8 à propos de l'âge du consentement du mineur au traitement de ces données (§ 1). Dans ce dernier cas, la question se pose de savoir comment déterminer la loi nationale applicable si plusieurs Etats membres sont potentiellement impliqués dans la situation. Il faudra, en tout cas, identifier les législations concernées et analyser leur champ d'application également. A cette fin, nous proposons de raisonner à partir d'un exemple concret, afin de saisir ultérieurement les enjeux pratiques qu'engendre l'absence de règle de conflits de lois dans le règlement (§ 2). Nous analyserons, dans ce cadre, le contenu des lois belge (§ 3) et française (§ 4).

### **§1. Présentation de l'article 8 du RGPD**

L'article 8 du RGPD est sans doute un des scénarios le plus illustratif des conséquences de la marge de manœuvre laissée aux Etats membres au niveau des conflits de lois pouvant se poser. Cet article traite des conditions applicables pour l'obtention du consentement des enfants en ce qui concerne les services de la société d'information<sup>126</sup>. La protection des mineurs et de leurs données à caractère personnel accessibles via leur utilisation d'Internet est devenue un enjeu majeur pour l'Union

---

<sup>124</sup> Art. 82, du RGPD.

<sup>125</sup> M. BRKAN, « Data Protection and Conflict-of-laws: (...) », *op. cit.*, pp. 336-337.

<sup>126</sup> Article 8, §3, du RGPD. ; Par « services de la société d'information », il faut entendre les services tels que définis par la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.U.E.*, 17 juillet 2000, L 178, p. 1.

européenne<sup>127</sup>. Le considérant 38 du règlement précise, en effet, que « *les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel* »<sup>128</sup>.

Cet article accorde une certaine flexibilité aux Etats membres quant à l'âge auquel un mineur pourrait consentir au traitement de ses données à caractère personnel<sup>129</sup>. L'article prévoit, plus particulièrement, une règle par défaut selon laquelle « *le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale [à savoir ses parents ou personnes disposant de la tutelle légale] à l'égard de l'enfant* »<sup>130</sup>. Cependant, l'article poursuit en habilitant les Etats membres à prévoir par voie législative un âge inférieur, pour autant que celui-ci ne soit pas inférieur à l'âge de 13 ans<sup>131</sup>. La limite pour consentir valablement seul en tant que mineur ne sera donc de 16 ans qu'à défaut de disposition contraire prévue par chaque législateur national. Par ailleurs, ce même article affirme qu'il ne porte pas atteinte au droit général des contrats des Etats membres.

Un responsable de traitement pourrait, dès lors, en fonction de l'étendue territoriale de ses activités, être potentiellement soumis à plusieurs lois nationales d'exécution différentes, si les Etats ont utilisé cette marge d'appréciation sur cette question. La question du droit national applicable se posera nécessairement chaque fois qu'un complément national est permis par le RGPD<sup>132</sup>. De fait, il convient de noter qu'un responsable de traitement qui fournit un service transfrontalier ne peut pas toujours se fonder sur le seul respect de la législation de l'État membre dans lequel il a son établissement principal, mais peut être tenu de respecter les législations nationales respectives de chaque État membre où il offre le ou les services de la société de l'information. Il faudra, dans chaque cas, vérifier le champ d'application des lois nationales concernées<sup>133</sup>. Certaines visent le lieu d'établissement principal du responsable du traitement comme point de référence de leur applicabilité alors que d'autres ont choisi le lieu de résidence de la personne concernée, pour ne citer que ces critères-ci.

Cet article 8 du règlement a une raison d'être assez pragmatique. La détermination de l'âge auquel une personne peut consentir provient d'un consensus politique et social au sein d'un Etat<sup>134</sup>. Il variera donc d'un Etat à l'autre, d'une culture à une autre. C'est précisément pour prendre en compte cette diversité au sein de l'Union que, notamment pour cet article, le législateur européen a fini par laisser une

---

<sup>127</sup> S. PEYROU, « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », *R.A.E. – L.E.A.*, 2016, p. 105.

<sup>128</sup> Considérant 38, du RGPD.

<sup>129</sup> J. CHEN, *op. cit.*, p. 316.

<sup>130</sup> Art. 8, §1, al. 1, du RGPD.

<sup>131</sup> Article 8, §1, al. 2, du RGPD.

<sup>132</sup> V. VERBRUGGEN, « Titre 1 – RGPD : cœur du puzzle de l'encadrement de la protection des données... », *op. cit.*, p. 48.

<sup>133</sup> Lignes directrices du Groupe de Travail « Article 29 » sur le consentement au sens du règlement 2016/679 (WP 259), adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018, p. 29.

<sup>134</sup> J. CHEN, *op. cit.*, p. 320.

discrétion aux Etats membres, tout en définissant un cadre général<sup>135</sup>. Se pose alors la question de savoir comment concilier cette autonomie nationale avec l'incertitude qui en découle au niveau des champs d'application territoriaux des lois nationales qui en résultent<sup>136</sup>. En effet, leur applicabilité spatiale peut potentiellement rentrer en conflit.

## **§2. Cas pratique de départ**

Afin d'envisager et de comprendre les impacts de cette habilitation, il est utile de raisonner à partir d'un exemple concret qui sera utilisé tout au long de la présente étude, avec certaines variantes. Nous nous concentrerons sur les lois nationales françaises et belges d'exécution.

Supposons qu'une société établie en Belgique vende des biens sur mesure en ligne, notamment à des clients résidant en France. Nous nous intéressons à une situation transnationale, impliquant deux Etats membres de l'Union – la Belgique et la France. Dans le cadre du contrat de vente impliquant les deux pays, la société est naturellement amenée à traiter des données à caractère personnel de ses clients, d'autant plus qu'elle doit prendre en compte les spécificités demandées par ceux-ci dans le cadre de la vente. Elle collecte donc des données personnelles avec le consentement de ses clients. Parmi ces derniers, il y a également des enfants<sup>137</sup>. Toutefois, il s'avère par la suite que la société vend les données collectées à une société tierce sans l'accord des personnes concernées. Il s'agit *a priori* d'un transfert de données non autorisé, ayant une finalité différente du transfert initial et n'ayant pas de fondement légal. Les parents d'un client de moins de 18 ans demandent devant les tribunaux de sa résidence (la France), que prenne fin le comportement consistant en la vente de ses données personnelles. Ils demandent, par ailleurs, des dommages et intérêts au titre d'indemnisation du préjudice subi. Étant donné que la partie demanderesse est un mineur, se pose en premier lieu la question de savoir si le contrat a été conclu entre personnes capables juridiquement. En d'autres termes, est-ce que le consentement d'un mineur de *14 ans accomplis* au traitement de ses données personnelles est licite ? Il s'agit d'une question de validité du contrat qui dépend du droit applicable à celui-ci. En fonction de la réponse à cette question, il sera possible ou non de demander des dommages et intérêts pour le traitement illégal de données.

Pour déterminer le droit applicable en matière de données à caractère personnel au niveau de l'Union, deux questions intimement liées méritent d'être posées. Dans un premier temps, il faut déterminer si le droit européen de la protection des données à caractère personnel s'applique au cas énoncé<sup>138</sup>. En l'occurrence, tout traitement de données à caractère personnel est désormais soumis au nouveau Règlement 2016/679, s'il entre dans le prescrit de l'article 3 de celui-ci (voy. *supra*). L'article pertinent du règlement pour apprécier la validité du consentement est l'article 8 précité. Toutefois, pour savoir l'âge à prendre en considération dans un traitement transnational, le droit européen renvoie à du droit national. Il

---

<sup>135</sup> J. CHEN, *op. cit.*, p. 317.

<sup>136</sup> *Ibid.*

<sup>137</sup> Chaque Etat fixe, en principe, le seuil de la majorité civile. En droit belge, l'article 909 du Code civil prévoit que « *La majorité est fixée à dix-huit ans accomplis ; à cet âge, on est capable de tous les actes de la vie civile* ».

<sup>138</sup> J. CHEN, *op. cit.*, p. 320.

s'agit donc de la deuxième étape de raisonnement, à savoir une fois que le droit européen des données personnelles s'applique, il convient de chercher le droit national pertinent. Tant la Belgique que la France ont modifié leur cadre légal concernant la protection des données à caractère personnel. Chaque pays a prévu un champ d'application territorial qui lui est propre ainsi que des règles matérielles différentes.

### **§3. La législation belge d'exécution du RGPD**

#### **1. Champ d'application territorial**

La Belgique a adopté une loi du 30 juillet 2018<sup>139</sup> ayant notamment pour objectif de mettre en œuvre, pour les clauses ouvertes, le RGPD<sup>140</sup>. Le critère principal d'application spatiale utilisé par cette loi est que le traitement soit effectué dans le cadre des activités d'un établissement sur le territoire belge, qu'il s'agisse d'un responsable du traitement ou d'un sous-traitant, indépendamment du lieu du traitement<sup>141</sup>. Elle n'utilise la situation des personnes concernées sur le territoire belge comme facteur de rattachement à sa loi que pour un traitement effectué par un responsable du traitement étant établi hors de l'Union européenne<sup>142</sup>.

Le législateur belge est conscient qu'un tel critère d'applicabilité pourrait aboutir à un conflit de lois intra-européen, dans les cas où il existe une marge d'appréciation pour l'exécution du RGPD, notamment concernant l'âge de l'enfant<sup>143</sup>. Il mentionne expressément ce risque dans l'Exposé des motifs de la loi, sans pour autant donner l'impression d'y apporter une quelconque solution pratique.

Notons tout de même que le législateur a tenté de résoudre un conflit de lois en particulier, concernant la situation d'un responsable de traitement établi sur le territoire d'un État membre de l'UE et faisant appel à un sous-traitant belge<sup>144</sup>. Dans ce cas, si le traitement est réalisé sur le territoire de cet État membre où le responsable est établi, le droit de cet État s'applique également au sous-traitant et non le droit belge<sup>145</sup>. Toutefois, si le traitement a lieu, soit en Belgique, soit dans un autre État membre, la loi du 30 juillet 2018 s'applique bien au sous-traitant et il existe alors toujours un conflit législatif selon l'Autorité de protection des données<sup>146</sup>. Cette dernière considère en effet que le critère du lieu du traitement est inadéquat<sup>147</sup>.

---

<sup>139</sup> Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616 (ci-après, « loi belge du 30 juillet 2018 »).

<sup>140</sup> Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 3.

<sup>141</sup> Art. 4, §1, de la loi belge du 30 juillet 2018.

<sup>142</sup> Art. 4, §2, de la loi belge du 30 juillet 2018.

<sup>143</sup> Projet de loi relatif à la protection des personnes physiques à l'égard des traitements (...), *op. cit.*, 16.

<sup>144</sup> *Ibid.* ; Avis 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (CO-A-2018-026), points 76-83.

<sup>145</sup> Art. 4, §3, de la loi belge du 30 juillet 2018.

<sup>146</sup> Avis n°52/2018 du 22 juin 2018 de l'Autorité de protection des données relatif à l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), pp. 8-9, point 32.

<sup>147</sup> *Ibid.*, p. 9, point 33.

## 2. Exécution de l'article 8 §1 du règlement

Le législateur a fixé la licéité du consentement au traitement des données à caractère personnel relatif aux enfants à l'âge de 13 ans, en mentionnant que cette règle est adoptée conformément au RGPD. Cela concerne l'offre directe de services de la société d'information aux enfants<sup>148</sup>. En dessous de cet âge, le consentement doit être donné par un représentant légal du mineur<sup>149</sup>. Il s'agit d'un choix politique relevant de la compétence de l'autorité fédérale, même si les différentes communautés du pays ont été consultées pour avis sur la question<sup>150</sup>.

Cette intervention législative du parlement national confirme ce qui a été expliqué ci-dessus à propos du champ d'application territorial de la loi. En effet, à travers les travaux parlementaires, le législateur reconnaît que cette marge de manœuvre crée une « discordance de la loi applicable au sein même de l'Union européenne », la loi belge n'étant pas applicable lorsque le traitement des données à caractère personnel a lieu via un responsable de traitement établi dans un autre pays de l'Union que la Belgique<sup>151</sup>.

### **§4. La législation française d'exécution du RGPD**

#### 1. Champ d'application territorial

Le législateur français a également adopté une loi datée du 20 juin 2018 relative à la protection des données personnelles<sup>152</sup> transposant le Règlement 2016/679 et la Directive 2016/680 et adaptant ainsi au droit de l'Union européenne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés<sup>153</sup>.

La loi du 20 juin 2018 adopte un critère d'applicabilité dans l'espace différent de celui choisi par le législateur belge. En vertu de l'article 5-1 alinéa premier de la loi de 1978, telle que modifiée par la loi précitée de 2018, les règles nationales françaises prises sur le fondement du RGPD s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France<sup>154</sup>. Le critère est donc celui de la résidence de la personne<sup>155</sup> et non celui de l'établissement du responsable de traitement ou du sous-traitant. C'est ainsi que le législateur français a

---

<sup>148</sup> Art. 7, al. 1., de la loi belge du 30 juillet 2018.

<sup>149</sup> Art. 7, al. 2., de la loi belge du 30 juillet 2018.

<sup>150</sup> Projet de loi relatif à la protection des personnes physiques à l'égard des traitements (...), *op. cit.*, pp. 18-19.

<sup>151</sup> Projet de loi relatif à la protection des personnes physiques à l'égard des traitements (...), *op. cit.*, p. 20.

<sup>152</sup> Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, *J.O.R.F.*, 21 juin 2018.

<sup>153</sup> Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.R.F.*, 7 janvier 1978 (ci-après « loi française n° 78-17 du 6 janvier 1978 »).

<sup>154</sup> Toutefois, une exception existe dans le cadre de traitements à des fins journalistiques mentionnés au §2 de l'article 85 du RGPD. Dans ce cas, il y a lieu d'appliquer les règles nationales dont relève le responsable de traitement qui est établi dans l'Union (art. 5-1 alinéa 2, de la loi française n° 78-17 du 6 janvier 1978).

<sup>155</sup> Notons que le législateur français parle d'une personne qui *réside* sur le territoire français et non une personne qui se *trouve* sur ce territoire, tel qu'il aurait pu le faire par analogie à l'article 3, §2 du règlement.

voulu traiter les possibles divergences de législations entre Etats membres, liées au soin qui leur a été donné d'adapter ou de compléter certains droits et obligations prévus par le règlement<sup>156</sup>.

Toujours est-il qu'au 1<sup>er</sup> juin 2019, cet article 5-1 a été abrogé et son contenu entièrement intégré dans un nouvel article 3 de la loi du 6 janvier 1978<sup>157</sup>. Ce dernier précise donc le champ d'application territorial de la loi. En plus du maintien du critère de la résidence pour régler les questions de droit applicable dans les hypothèses d'exécution des marges de manœuvre du RGPD, le nouvel article « assure enfin la cohérence des dispositions nationales avec celles de l'article 3 du règlement (UE) 2016/679 »<sup>158</sup>. A cette fin, il prévoit que « sans préjudice, en ce qui concerne les traitements entrant dans le champ du règlement (UE) 2016/679 du 27 avril 2016, des critères prévus par l'article 3 de ce règlement, l'ensemble des dispositions de la présente loi s'appliquent aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France »<sup>159</sup>. Cet alinéa semblerait donc également consacrer le critère de l'établissement du responsable du traitement. A cet égard, la Commission Nationale de l'informatique et libertés (dénommée également « CNIL ») s'interrogeait sur la bonne lisibilité de l'articulation entre le champ d'application territorial de la loi du 6 janvier 1978 et celui du Règlement lui-même<sup>160</sup>.

## 2. Exécution de l'article 8 §1 du règlement

Dans le projet de loi initialement déposé par l'Assemblée Nationale, le Gouvernement avait fait le choix de ne pas faire usage de la latitude permise dans le cadre de l'article 8 du RGPD<sup>161</sup>. Nous remarquons cependant que le législateur a finalement usé du pouvoir qui lui était accordé pour fixer l'âge minimum à 15 ans, en vue de permettre au mineur, à compter de cet âge, de consentir seul au traitement de ses données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information<sup>162</sup>.

---

<sup>156</sup> Projet de loi relatif à la protection des données personnelles, n°490, Assemblée nationale, déposé le 13 décembre 2017, p. 11.

<sup>157</sup> Art. 3, de la loi française n° 78-17 du 6 janvier 1978, tel que modifié par l'Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *J.O.R.F.*, 13 décembre 2018.

<sup>158</sup> Rapport au Président de la République relatif à l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *J.O.R.F.*, 13 décembre 2018.

<sup>159</sup> Art. 3, I. de la loi française n° 78-17 du 6 janvier 1978, tel que modifié par l'Ordonnance n° 2018-1125 (...), *op. cit.*

<sup>160</sup> Délibération n° 2018-349 du 15 novembre 2018 portant avis sur un projet d'ordonnance prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions relatives à la protection des données personnelles (saisine n° AV 18022142), p. 4.

<sup>161</sup> Projet de loi relatif à la protection des données personnelles, n°490, Assemblée nationale, déposé le 13 décembre 2017, p. 7.

<sup>162</sup> Art. 45, de la loi française n° 78-17 du 6 janvier 1978, tel qu'en vigueur au 1<sup>er</sup> juin 2019 (avant cette date, art. 7-1 de ladite loi).

### **§5. Conclusion intermédiaire : quelle législation retenir ?**

Suite à cette analyse, nous remarquons donc que le fait que les champs d'application territoriaux des lois nationales puissent varier autant pourrait avoir un effet contreproductif sur la protection effective offerte par cet article du RGPD aux mineurs ou à leurs parents dans une situation transfrontalière. Dans un tel contexte, les personnes concernées éprouvent des difficultés à percevoir quel est le droit applicable à leur situation, tant à l'égard de leurs droits que de leurs obligations, et ne savent pas comment se comporter en conséquence. Cela rajoute donc également des coûts pour les individus ainsi que pour les entreprises pour déterminer par quel régime juridique ils sont concernés<sup>163</sup>.

Se pose alors la question de savoir laquelle de ces législations sera applicable au traitement des données dans le cadre du contrat mentionné ci-dessus, afin d'apprécier la validité de celui-ci. En raison du nombre de jeunes actifs sur Internet, ce problème pourrait être beaucoup plus important qu'il n'y paraît à première vue. Certains estiment que les entreprises se conformeront simplement à l'âge le plus élevé prévu par le règlement, à savoir 16 ans, afin de s'assurer de ne violer aucune loi nationale<sup>164</sup>. Cela reste encore à voir dans la pratique, mais une telle situation risquerait cependant de ne pas être avantageuse pour ces entreprises, perdant potentiellement ainsi plusieurs transactions.

Une autre solution afin de déterminer le droit applicable, en l'absence d'indications dans le RGPD en lui-même, plus réaliste – sans doute – et fidèle à la logique inhérente au droit international privé, pourrait consister en l'application des règles classiques de droit international privé européen.

### **Chapitre 3. Les règles classiques de droit international privé européen**

Une solution naturellement envisageable pour résoudre les conflits de lois précités qui peuvent être soulevés dans la pratique des relations intra-européennes serait de déterminer la loi applicable en vertu des règles de conflits de lois de droit commun. Nous pensons bien sûr au règlement Rome I pour la matière contractuelle (Section II) et au règlement Rome II pour la matière extracontractuelle (Section III). Toujours est-il que l'application de ces règlements présuppose quelques remarques générales qui méritent d'être mentionnées préalablement à toute analyse au regard des règles de droit international privé européen prévues respectivement par ceux-ci (Section I).

#### **Section I. Raisonnement au départ des règles classiques de droit international privé européen : précautions introductives**

La nature « hybride » du droit à la protection des données à caractère personnel peut avoir un impact sur sa relation avec d'autres instruments juridiques. Les règlements européens de droit commun

---

<sup>163</sup> J. CHEN, *op. cit.*, p. 317.

<sup>164</sup> Đ. KRIVOKAPIĆ, J. ADAMOVIĆ, « Impact of General Data Protection Regulation on Children's Rights in Digital Environment », *Belgrade Law Review*, Year LXIV, 2016, p. 209.

en droit international privé suscitent, à cet égard, des débats autour de questions de qualification<sup>165</sup>. Partant, il convient de se demander dans quelle mesure les considérations relatives à la protection de ce droit relèvent de la notion de « matière civile et commerciale », composante inhérente des champs d'application des règlements Rome I et Rome II (§ 1). Ensuite, plus spécifiquement par rapport au droit international privé des relations contractuelles, il y a lieu de distinguer le consentement des cocontractants sur l'objet principal du contrat du consentement de la personne concernée au traitement de ses données, qui peut être lié à ce contrat (§ 2).

## **§1. La matière « civile et commerciale »**

### 1. Définition et contextualisation

En effet, les instruments de droit international privé bilatéraux ou multilatéraux<sup>166</sup> identifient souvent leur champ d'application matériel par rapport à la « matière civile et commerciale », accompagné ensuite par une liste d'exclusions du champ d'application et de définitions<sup>167</sup>. Tel est notamment le cas, en droit européen, du Règlement 1215/2012 sur la compétence judiciaire, la reconnaissance et l'exécution des décisions (aussi appelé « Bruxelles I bis »)<sup>168</sup>, le Règlement 593/2008 du 17 juin 2008 sur la loi applicable aux obligations contractuelles (ci-après « règlement Rome I »)<sup>169</sup> et le Règlement 864/2007 sur la loi applicable aux obligations non contractuelles (ci-après « règlement Rome II »)<sup>170</sup>. Cette délimitation du champ d'application vise à exclure généralement, et à titre d'exemple, tout ce qui concerne le droit pénal et la procédure pénale ou encore des considérations fiscales<sup>171</sup>. Elle s'appliquerait, au contraire, aux affaires traitant de relations contractuelles ou non-contractuelles privées, dans lesquelles du droit civil ou commercial est en cause<sup>172</sup>.

En droit européen, cette notion doit recevoir une interprétation autonome, c'est-à-dire indépendante de celle donnée par les Etats membres en fonction des objectifs respectifs des règlements<sup>173</sup>. La Cour de justice de l'Union européenne a interprété cette notion, notamment dans le

<sup>165</sup> N. MICHAIL, « Le domaine d'application du GDPR: (...) », *op. cit.*, p. 78.

<sup>166</sup> B. HESS, C. ORO MARTINES, « Civil and commercial matters », in *Encyclopedia of Private International Law/ edited by Jurgen Basedow, Giesela Ruhl, Franco Ferrari e.a.*, Cheltenham, Edward Elgar Publishing, 2017, p. 346.

<sup>167</sup> « Protection of privacy in private international and procedural law », *International Law Association, Sydney Conference (2018)*, p.5, [https://www.mpi.lu/fileadmin/mpi/medien/research/ILA\\_Committee\\_Protection\\_Privacy\\_Private\\_International\\_and\\_Procedural\\_Law/ILA\\_Committee\\_Privacy\\_Interim\\_Report\\_Sydney\\_REVISSED\\_FINAL.pdf](https://www.mpi.lu/fileadmin/mpi/medien/research/ILA_Committee_Protection_Privacy_Private_International_and_Procedural_Law/ILA_Committee_Privacy_Interim_Report_Sydney_REVISSED_FINAL.pdf) (consulté le 8 février 2019).

<sup>168</sup> Règlement (UE) n°1215/2012 du Parlement européen et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, art. 1 §1, *J.O.U.E.*, 20 décembre 2012, L 351, p. 1 (ci-après, « règlement Bruxelles Ibis »).

<sup>169</sup> Règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), art. 1 §1, *J.O.U.E.*, 4 avril 2008, L 177, p. 6.

<sup>170</sup> Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II), art. 1 §1, *J.O.U.E.*, 31 juillet 2007, L 199, p. 40.

<sup>171</sup> « Protection of privacy in private international and procedural law », *International Law Association, op. cit.*, p. 5. ; notons que dans des pays de Common Law, cette affirmation n'est que partiellement vraie. Le « civil law » est surtout utilisé par opposition au droit pénal mais inclut les matières fiscales par exemple (voy. P. SCHLOSSER, « Rapport sur la convention relative à l'adhésion du royaume de Danemark, de l'Irlande et du Royaume-Uni de Grande-Bretagne et de l'Irlande du Nord à la convention de Bruxelles » (Schlosser Report), *J.O.C.E.*, C 59, 5 mars 1979, pp. 82-83, §24).

<sup>172</sup> B. HESS, C. ORO MARTINES, *op. cit.*, p. 347.

<sup>173</sup> C. KESSEDJIAN, *Droit du commerce international*, Paris, PUF, 2013, pp. 521-522.

cadre de la Convention de Bruxelles I<sup>174</sup>, en affirmant que doit être exclue du champ d'application de ces textes toute décision opposant une autorité publique et une personne privée, lorsque cette autorité manifeste des prérogatives de puissance publique et exerce des pouvoirs exorbitants<sup>175</sup>. Cette interprétation des termes est transposable aux règlements sur la loi applicable<sup>176</sup>. L'attention doit donc être portée sur l'objet du litige et non sur la qualité des parties, de telle sorte qu'il ne soit pas automatiquement en dehors du champ d'application matériel de l'instrument juridique par le simple fait qu'une des parties soit une autorité publique<sup>177</sup>.

## 2. Les données à caractère personnel peuvent-elles être incluses dans cette notion ?

Ce raisonnement est intéressant pour la matière des données à caractère personnel qui impliquent souvent un Etat ou une autorité de protection des données. Ces autorités sont des organismes publics indépendants chargés de surveiller la correcte application du RGPD et de faire appliquer la loi à l'égard des responsables du traitement<sup>178</sup>. Leur caractère public est affirmé de manière claire par le RGPD<sup>179</sup> qui leur donne, entre autres, le pouvoir d'imposer des amendes administratives<sup>180</sup>. Pour savoir si les règlements Rome I et Rome II s'appliquent, il faut donc déterminer, dans un premier temps, s'il s'agit d'une « matière civile » ou d'une matière administrative<sup>181</sup>. Il est, dès lors, nécessaire d'apprécier, au cas par cas, si une autorité de contrôle est impliquée et, dans l'affirmative, si elle agit dans le cadre de ses pouvoirs publics ou non. Autrement dit, il ne faut pas que l'autorité publique fasse usage de prérogatives qui sont les siennes allant au-delà de celles existant pour les relations entre personnes physiques ou morales « privées »<sup>182</sup>. Il est, par conséquent, non souhaitable d'établir *a priori* une réponse de principe, selon laquelle les litiges sur les données à caractère personnel impliquant une autorité de contrôle sont compris dans le champ d'application desdits règlements, mais tel pourra en être le cas après une analyse précise des faits de l'espèce<sup>183</sup>.

En tout état de cause, il semblerait, à titre d'exemple, qu'une action intentée par une partie privée pourrait être considérée comme une sorte de « private enforcement » du droit à la protection des données et, dès lors, être assimilée à une matière civile<sup>184</sup>. En effet, cela implique que la personne concernée par le traitement invoque ses droits ou cherche indemnisation pour son propre compte.

---

<sup>174</sup> Convention de Bruxelles de 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, *J.O.C.E.*, L 299, 31 décembre 1972, p. 32.

<sup>175</sup> Voy. par exemple Arrêt LTU Luftransportunternehmen GmbH & Co. KG/Eurocontrol, C-29/76, EU:C:1976:137, point 4 ; Arrêt Eirini Lechouritou et Autres/Dimosio tis Omospondiakis Dimokratias tis Germanias, C-292/05, EU:C:2007:102, points 33-36.

<sup>176</sup> Voy. considérants 7 du règlement Rome I et du règlement Rome II.

<sup>177</sup> B. HESS, C. ORO MARTINES, *op. cit.*, p. 353.

<sup>178</sup> M. BRKAN, « Data Protection and European Private International Law: Observing a Bull in a China Stop », *I.D.P.L.*, 2015, p. 262.

<sup>179</sup> Art. 4, 21), du RGPD ; art. 51, du RGPD.

<sup>180</sup> Considérant 150, du RGPD.

<sup>181</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 260.

<sup>182</sup> B. HESS, C. ORO MARTINES, *op. cit.*, p. 353.

<sup>183</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 262 ; M. BRKAN, « Data Protection and Conflict-of-laws: (...) », *op. cit.*, p. 331.

<sup>184</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 260. Cette auteur propose de s'inspirer du « private enforcement » existant en matière de droit de la concurrence européen où ce concept fait référence à l'action en dommages et intérêts à l'initiative de parties privées victimes de pratiques anticoncurrentielles sur base des règles européennes applicables en la matière (voy. également J. LEONARD, « Le droit de la concurrence entre-t-il dans l'ère du private enforcement ? La loi sur l'action en dommages et intérêts pour les infractions au droit de la concurrence », *Competitio*, 2018, p. 4).

Il faut également déterminer s'il s'agit d'une matière civile « et commerciale » pour que les instruments européens sur le droit applicable puissent être utilisés. Cette notion vise souvent à montrer que l'instrument juridique a également un but de facilitation du commerce transnational<sup>185</sup>. Certaines juridictions considèrent que la notion de relations commerciales est incluse dans celle de la matière civile, tandis que d'autres estiment qu'il y a lieu de les distinguer<sup>186</sup>. En matière de données personnelles, serait, par exemple, considéré comme litige commercial un différend entre un responsable du traitement et un sous-traitant ou encore entre un exportateur de données personnelles et un importateur de celles-ci<sup>187</sup>.

Notons enfin que certains auteurs estiment que, par la nature même du droit à la protection des données à caractère personnel, impliquant une classification incertaine de celui-ci dans une des branches classiques du droit, il ne rentre pas dans le champ d'application des instruments bilatéraux de droit international privé<sup>188</sup>. En effet, ces auteurs affirment que ce droit ne peut être compris comme faisant partie de la « matière civile et commerciale ». Ils estiment que le droit applicable doit, en priorité, être déterminé sur base de règles européennes spécifiques en matière de droit à la protection des données personnelles ou de droits fondamentaux et non par des textes de droit international privé<sup>189</sup>. Un tel raisonnement, quoique sans doute fondé du temps de la directive 95/46/CE qui adressait directement les questions de droit applicable, apportant ainsi une solution concrète aux conflits de lois, se suffisant à elle-même<sup>190</sup>, ne semble plus pouvoir être suivi aujourd'hui. En l'absence d'une clause similaire dans le RGPD, le recours aux instruments de droit international privé de droit commun sur le droit applicable semble être – si pas nécessaire – en tout cas à envisager.

## **§2. L'objet du consentement**

L'application des normes de protection des données à caractère personnel ne peut être considérée comme une simple question contractuelle pouvant, en toute hypothèse, être librement négociée entre parties<sup>191</sup>. De plus, le non-respect du droit à la protection des données ne résulte pas nécessairement d'un manquement à un contrat<sup>192</sup>. Il y a lieu de distinguer, conceptuellement au moins, le consentement au contrat de vente ou de prestation de services et le consentement au traitement des données personnelles.

Nous nous attardons ici sur le deuxième point, à savoir le consentement au traitement. Le RGPD prévoit, en son article 6 §1<sup>er</sup>, point a), que le consentement est l'une des six bases juridiques permettant

---

<sup>185</sup> « Protection of privacy in private international and procedural law », *International Law Association*, *op. cit.*, p. 5.

<sup>186</sup> *Ibid.*, p. 4.

<sup>187</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 264.

<sup>188</sup> M. BRKAN « Data Protection and Conflict-of-laws: (...) », *op. cit.*, p. 330. ; D. COOPER, C. KUNER, *op. cit.*, p. 113.

<sup>189</sup> D. COOPER, C. KUNER, *op.cit.*, p. 114. Voy. également Document de travail du Groupe de Travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE (WP 56), adopté le 30 mai 2002, pp. 6-8.

<sup>190</sup> D. COOPER, C. KUNER, *op. cit.*, p. 80

<sup>191</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 266.

<sup>192</sup> *Ibid.*

de justifier valablement une collecte ainsi qu'un traitement de données à caractère personnel pour une ou plusieurs finalités spécifiques<sup>193</sup>. En effet, pour tout traitement de données, il faut s'interroger sur le fondement juridique approprié pour le traitement envisagé<sup>194</sup>. Le consentement doit émaner de la personne concernée par le traitement. Tel que défini par le règlement lui-même, il s'agit de « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »<sup>195</sup>. Selon le GT art. 29 sur la protection des données, le consentement ne peut constituer une base légale appropriée que si la personne concernée se voit offrir le contrôle ainsi qu'un véritable choix quant à l'acceptation ou au refus des conditions proposées, ou à leur refus sans préjudice<sup>196</sup>. Ne peuvent, dès lors, constituer un consentement licite le consentement tacite basé sur le silence, le consentement passif basé sur l'inactivité<sup>197</sup> ou encore sur des cases cochées par défaut<sup>198</sup>.

L'article 7 du RGPD prévoit les conditions pour la validité du consentement en tant que fondement juridique d'un traitement licite. Cet article prévoit par ailleurs que la personne a le droit de retirer son consentement à tout moment<sup>199</sup>. Ainsi, en théorie, l'on pourrait imaginer des situations où une personne a consenti à un contrat de vente ou de services, mais ne souhaite plus que certaines de ses données soient traitées dans le cadre de celui-ci. Elle retire son consentement sur ce point, sans que cela affecte nécessairement la prestation caractéristique du contrat liant les parties. Inversement, un manquement au niveau de l'objet principal du contrat n'impactera pas spécialement le traitement subséquent des données qui en est fait dans ce cadre. Par conséquent, même si le traitement de données est généralement lié à un contrat, il y a lieu de les distinguer d'un point de vue purement théorique.

Toujours est-il que le droit applicable à un contrat tel que déterminé par le règlement Rome I peut s'avérer pertinent dans un contexte de protection des données personnelles, lorsqu'un régime de protection de telles données fait partie intégrante de clauses contractuelles<sup>200</sup>. Un contrat de vente ou de services inclut souvent une dimension sur la vie privée et la protection des données à caractère personnel. Une telle constatation est particulièrement d'actualité, compte tenu du fait que les responsables du traitement des données ont aujourd'hui largement recours à des arrangements contractuels pour le traitement des données et fournissent par ailleurs des informations sur les méthodes de traitement<sup>201</sup>. Le consentement au traitement fonctionne alors comme un contrat. A cet égard, un tribunal allemand sur une affaire Facebook<sup>202</sup> antérieure à l'adoption du RGPD aurait considéré que le règlement Rome I pourrait

---

<sup>193</sup> A. BEELEN, *op.cit.*, p. 43.

<sup>194</sup> Lignes directrices du Groupe de Travail « Article 29 » sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 5.

<sup>195</sup> Article 4, 11), du RGPD ; considérants 32, 42 et 43, du RGPD.

<sup>196</sup> Lignes directrices du Groupe de Travail « Article 29 » sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 6.

<sup>197</sup> A. BENSOUSSAN, J.-F. HENROTTE, M. GALLARDO, S. FANTI, *General Data Protection Regulation: texts, commentaries and practical guidelines* (sous la dir. de A. BENSOUSSAN), Mechelen, Kluwer, 2017, p. 92 ; Lignes directrices du Groupe de Travail « Article 29 » sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 16.

<sup>198</sup> B. DOCQUIR, « Consentement et intérêt légitime dans le secteur privé », in *Data Protection & Privacy – Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2016, p. 30.

<sup>199</sup> Art. 7, du RGPD.

<sup>200</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 266.

<sup>201</sup> J. CHEN, *op. cit.*, p. 318.

<sup>202</sup> Facebook Ireland Ltd/ Facebook Inc. c. Independent Data Protection Authority of Schleswig-Holstein, Allemagne, 13 février 2013.

être pertinent, en raison du fait qu'il existe un contrat entre la société Facebook et ses utilisateurs qui prévoit notamment l'application de la loi allemande de protection des données personnelles dans le cadre de leur relation<sup>203</sup>. Il serait applicable alors en raison de la nature civile de la relation entre les deux parties contractantes (voy. *supra*)<sup>204</sup>. Notons que, dans un tel cas, l'application du règlement sur le droit applicable en matière contractuelle serait suscitée par le non-respect des clauses du contrat par le responsable de traitement et non directement par le non-respect des instruments juridiques en matière de protection des données personnelles<sup>205</sup>. Le tribunal affirme également qu'étant donné que la protection des données personnelles constitue une partie du contrat, elle est, par conséquent, sujette à la législation sur les clauses abusives basée sur le droit de la consommation<sup>206</sup>.

Dans le cadre de la présente étude, nous ne nous intéressons qu'aux hypothèses où le consentement au traitement des données personnelles fait partie ou est lié au contrat de vente ou de services sous-jacent entre les parties contractantes.

## **Section II. Détermination de la loi applicable au contrat via le règlement Rome I : une société établie en Belgique traitant avec un mineur résidant en France**

Suite à ces remarques, il est important de faire l'exercice complet de résolution effective des conflits de lois en matière de données personnelles à partir du cas pratique qui a été exposé dans le second chapitre de la présente étude. Les faits restent simples : il s'agit de la relation contractuelle entre une société dont l'établissement est situé en Belgique et un mineur de quatorze ans résidant en France, aux termes de laquelle les données personnelles de ce dernier sont traitées. Ces parties se demandent, dans le cadre d'un litige qui survient entre elles concernant les données à caractère personnel traitées, quel est le droit applicable à ce traitement, partant du postulat – pour des facilités de raisonnement – que leur contrat ne prévoit pas de clause de choix de loi. Dans une telle situation, il est probable que les tribunaux français soient saisis et, à partir de là, commence la recherche du droit applicable.

Dans un premier temps, il faut s'assurer que les différentes composantes du cas pratique énoncé sont bien incluses dans le champ d'application matériel du règlement Rome I, notamment au regard des exclusions prévues par ce dernier. A cette fin, il y aura, plus particulièrement, lieu de traiter séparément la question de la capacité du mineur à consentir au traitement de ses données et les autres questions de droit applicable qui peuvent être suscitées (§ 1). Une fois la question du consentement étudiée, nous retombons, dans un second temps, dans la méthode conflictuelle classique du règlement Rome I. Sans s'intéresser à ce stade à l'un des facteurs perturbateurs du raisonnement classique de conflits de lois qu'est la loi de police (voy. *infra*), l'analyse sera poursuivie en appliquant les règles liées aux contrats de

---

<sup>203</sup> M. BRKAN « Data Protection and Conflict-of-laws: (...) », *op. cit.*, p. 335.

<sup>204</sup> *Ibid.*

<sup>205</sup> M. BRKAN, « Data Protection and European Private International Law: (...) », *op. cit.*, p. 266.

<sup>206</sup> J. CHEN, *op. cit.*, p. 318.

consommation (§ 2). Les facteurs classiques de rattachement seront, en outre, mentionnés pour information (§ 3).

Enfin, les constats de l'exercice d'identification de la loi d'exécution applicable pourraient s'avérer moins convaincants si les rattachements territoriaux n'étaient examinés que dans un sens. Il convient alors d'explorer à quel point les conclusions tirées jusque-là différeraient si les faits du casus étaient inversés, à savoir si le contrat liait le responsable de traitement dont le principal établissement se trouve en France et des mineurs résidant sur le territoire belge (§ 4).

## **§1. Retour sur le champ d'application matériel du règlement**

### 1. La notion d' « obligations contractuelles »

Le règlement Rome I vise la matière civile et commerciale pour délimiter son champ d'application matériel (voy. *supra*). Il traite de ces matières dans le cadre d' « obligations contractuelles », mais ne définit pas ce qu'il faut entendre par cette expression<sup>207</sup>. Le soin a alors été laissé à la jurisprudence européenne de la préciser. Certains arrêts ont d'abord tenté de distinguer les obligations contractuelles des obligations délictuelles<sup>208</sup>. C'est ainsi que l'arrêt *Kalfelis* affirme le caractère résiduel de la matière délictuelle par rapport à la matière contractuelle<sup>209</sup>. L'affaire *Brogstetter*, toujours par rapport à cette distinction, précise que la qualification contractuelle doit l'emporter « *si le comportement reproché peut être considéré comme un manquement aux obligations contractuelles, telles que déterminées compte tenu de l'objet du contrat* »<sup>210</sup>. Il a fallu attendre la jurisprudence *Handte* pour une définition générale et abstraite du contrat<sup>211</sup>. La Cour de justice a ainsi indiqué que la matière contractuelle suppose « *un engagement librement assumé d'une partie envers une autre* »<sup>212</sup>. La jurisprudence est restée constante quant à cette définition, le critère ayant été légèrement affiné au fil du temps, afin de viser « *une obligation juridique librement assumée par une personne à l'égard d'une autre* »<sup>213</sup>. La Cour a néanmoins récemment ajouté une précision par rapport à cette notion. Dans un arrêt *Flightright* du 7 mars 2018, elle considère que l'obligation librement assumée qui doit exister peut être invoquée par une personne qui n'est pas impliquée dans le contrat sur lequel elle appuie son action<sup>214</sup>. En effet, pour savoir si l'inexécution alléguée par le demandeur est bien de nature contractuelle, il y a lieu de s'intéresser à la cause de l'action et non à l'identité des parties<sup>215</sup>. Selon les termes de la Cour, relèvent de la matière contractuelle « *toutes les obligations qui trouvent leur source dans le contrat dont l'inexécution est invoquée* »<sup>216</sup>.

---

<sup>207</sup> G. LARDEUX, *Droit international privé des obligations contractuelles*, Bruxelles, Larcier, 2016, p. 18.

<sup>208</sup> *Ibid.*, p. 20.

<sup>209</sup> Arrêt Athanasios Kalfelis/Banque Schröder, Münchmeyer, Hengst et Cie, et autres, C-189/87, EU:C:1988:459, point 17.

<sup>210</sup> Arrêt Marc Brogstetter/Fabrication de Montres Normandes EURL et Karsten Fräßdorf, C-548/12, EU:C:2014:148, points 16 et 24.

<sup>211</sup> G. LARDEUX, *op. cit.*, p. 23.

<sup>212</sup> *Ibid.* ; Arrêt Jakob Handte & Co. GmbH/Traitements mécano-chimiques des surfaces SA, C-26/91, EU:C:1992:268, point 15.

<sup>213</sup> Arrêt Harald Kolassa/ Barclays Bank plc, C-375/13, EU:C:2015:37, point 39 ; A. NUYS, « Droit international privé européen », *J.D.E.*, 2018, p. 402.

<sup>214</sup> *Ibid.*, p. 402.

<sup>215</sup> Arrêt Flightright GmbH/Air Nostrum, LÍneas Aéreas del Mediterráneo SA, C-274/16, Roland Becker/Hainan Airlines Co. Ltd, C-447/16, Mohamed Barkan et autres/ Air Nostrum, LÍneas Aéreas del Mediterráneo SA (C-448/16), EU:C:2018:160, point 61.

<sup>216</sup> *Ibid.*, point 59.

## 2. Exclusions du champ d'application de Rome I : l'état et la capacité

Pour revenir à notre cas pratique énoncé ci-dessus, eu égard à la jurisprudence européenne, la commande d'un bien par une personne, fût-elle un mineur, à une société ne fait aucun doute quant à la qualification contractuelle ainsi qu'à l'applicabilité du règlement Rome I<sup>217</sup>. La personne concernée a, en outre, dans le cadre de ce contrat, consenti au traitement de ses données personnelles. Dans l'exemple toutefois, la première question qui nous intéresse est de savoir si le mineur a pu valablement conclure le contrat, sachant que le responsable de traitement avait connaissance de cette incapacité. En d'autres termes, nous nous demandons quel est l'âge auquel l'enfant peut valablement consentir, pour savoir ce qu'il advient du contrat.

### *2.1.) L'exclusion en tant que telle*

La capacité, en tant que qualité de la personne, est exclue des conventions européennes ou internationales de droit international privé<sup>218</sup>. Tel est le cas du règlement Rome I sur la loi applicable aux obligations contractuelles qui exclut « l'état et la capacité juridique des personnes physiques » aux termes de son article 1<sup>er</sup>, § 2, point a)<sup>219</sup>. Il en va de même, par exemple, de la Convention de la Haye 1996 sur la compétence et la loi applicable en matière de protection des mineurs<sup>220</sup>. Tout ce qui concerne la capacité d'un mineur et sa représentation est considéré comme une question de statut personnel régie par sa loi nationale<sup>221</sup>. Il s'agit du droit commun applicable indépendamment du droit conventionnel<sup>222</sup>. Ce qui est visé est l'incapacité générale d'exercice affectant un individu, en l'occurrence le mineur, en raison de considérations tirées de sa personne et non les incapacités spéciales visant certaines catégories d'actes<sup>223</sup>. Il y a donc une certitude de rattachement à la loi « personnelle » en la matière, ce qui permet d'éviter toute concurrence normative ou des discussions sur la détermination de la loi applicable<sup>224</sup>. Le rattachement par la nationalité permet en outre de favoriser une certaine permanence<sup>225</sup>. C'est, par exemple, à la loi nationale du mineur qu'il faut se référer pour savoir quel est l'âge de la majorité ou les pouvoirs des représentants<sup>226</sup>.

---

<sup>217</sup> G. LARDEUX, *op. cit.*, p. 26.

<sup>218</sup> H. PEROZ, « La gestions des biens de la personne », in *Droit International Privé Patrimonial de la famille*, Paris, LexisNexis, 2017, p. 91.

<sup>219</sup> L'article 1, §2, petit a) du règlement Rome I dispose que : « 2. Sont exclus du champ d'application du présent règlement: a) l'état et la capacité juridique des personnes physiques, sous réserve de l'article 13 ». L'article 13 dudit règlement prévoit que « Dans un contrat conclu entre personnes se trouvant dans un même pays, une personne physique qui serait capable selon la loi de ce pays ne peut invoquer son incapacité résultant de la loi d'un autre pays que si, au moment de la conclusion du contrat, le cocontractant a connu cette incapacité ou ne l'a ignorée qu'en raison d'une imprudence de sa part ».

<sup>220</sup> Convention concernant la compétence, la loi applicable, la reconnaissance, l'exécution et la coopération en matière de responsabilité parentale et de mesure de protection des enfants, signée à la Haye le 19 octobre 1996, approuvée par la loi du 25 mai 2014, *M.B.*, 22 août 2014, 63560.

<sup>221</sup> M. REVILLARD, *Droit International Privé et Communautaire : Pratique notariale*, Paris, Défrenois Lextenso éditions, 2010, p. 291.

<sup>222</sup> *Ibid.* ; T. VIGNAL, *Droit international privé*, Paris, Sirey, 2011, p. 148. ; B. AUDIT, L. D'AVOUT, *Droit international privé*, Paris, Librairie générale de droit et de jurisprudence, 2018, p. 619.

<sup>223</sup> T. VIGNAL, *op. cit.*, p. 143.

<sup>224</sup> *Ibid.*

<sup>225</sup> S. CLAVEL, *Droit international privé* (sous la dir. de D. CHAGNOLLAUD et S. GUINCHARD), Paris, Editions Dalloz, 2016, p. 388.

<sup>226</sup> M. REVILLARD, *op. cit.*, p. 292.

En fonction du pays dans lequel le juge est saisi, la base légale renvoyant à la loi nationale sera différente. En Belgique, il faut consulter l'article 34 du Code de droit international privé<sup>227</sup> pour prendre connaissance de cette règle, tandis qu'en France, il s'agit de l'article 3 du Code civil français qui soumet la capacité des nationaux à la loi française<sup>228</sup>.

## 2.2.) L'exclusion au regard du cas pratique

Concernant la marge de manœuvre précise de l'article 8 du RGPD, les Etats sont amenés à légiférer sur une question renvoyant à la capacité du mineur, alors même qu'ils utilisent un critère de rattachement souvent autre que celui qui veut qu'on applique à la capacité la loi de la nationalité. Une telle solution n'est pas sans susciter débats et incertitudes. En pratique, l'on serait amenés à constater que les lois sur les données à caractère personnel concernées ne seraient utiles, afin d'établir la capacité, que s'il s'agit de la loi de la nationalité de l'individu visé. Pour cette question en particulier, et pour revenir à notre cas pratique, le rattachement à la résidence de la personne concernée prévu par la loi française ne serait donc pas directement pertinent. En effet, les tribunaux français probablement saisis devraient distinguer si le mineur est de nationalité française ou s'il ne l'est pas. Dans le premier cas de figure, à savoir si le mineur résidant en France est de nationalité française, la loi de 1978 serait pleinement applicable et les deux critères de rattachement coïncideraient. Il faut alors vérifier ce que prévoit la loi de 1978 comme âge valable de consentement en son article 45 (voy. *supra*). Le contrat serait donc probablement réputé nul s'il a consenti seul, alors qu'il n'avait pas atteint l'âge de 15 ans accomplis.

Toutefois, le mineur pourrait résider en France et donc entrer dans le champ d'application de la loi française précitée, mais avoir une nationalité différente. Il faudrait alors appliquer la loi de sa nationalité pour les questions relevant de son statut personnel. Une analyse au cas par cas risque donc d'être nécessaire en fonction de la personne concernée. Toutefois, dès lors que la loi nationale est ciblée par le juge français, celle-ci prévoit un critère de rattachement qui lui est propre et qui doit, partant, être vérifié. Si le mineur est de nationalité belge par exemple, la loi applicable serait la loi belge précitée du 30 juillet 2018 (voy. *supra*). Cette loi prévoit son champ d'application dans l'espace par rapport à l'établissement du responsable de traitement. Le mineur belge pourrait donc se voir appliquer la loi de sa nationalité par rapport à la capacité lors du consentement à un traitement de données personnelles que dans le cas où l'établissement qui traiterait ses données est situé en Belgique. Or, la loi nationale est censée s'appliquer dans un but de protection des individus quant à leur statut personnel et, faire dépendre celle-ci de l'application d'un critère factuel, tel que l'établissement du responsable de traitement, peut être source de grande insécurité juridique pour les personnes concernées.

Nous constatons donc que si l'entreprise dont l'établissement principal est situé en Belgique traite avec un mineur de 14 ans de nationalité belge, le consentement ainsi donné respecte la loi belge et est

---

<sup>227</sup> Codip, art. 34.

<sup>228</sup> C.civ. français, art. 3.

donc licite, tandis que si le mineur, de même âge, est de nationalité française, la validité du contrat sera affectée.

En fonction du lieu où se situe l'établissement de l'entreprise avec laquelle le mineur belge qui réside en France contracte, il peut se trouver dans une situation où il ne serait pas protégé parce qu'aucune loi nationale d'exécution ne s'appliquerait à lui, ne rentrant pas dans le champ d'application de la loi belge, et la loi française ne s'appliquant pas pour cette question. Il serait alors dans une situation différente sur ce point très précis et, dès lors, déséquilibrée, par rapport à un mineur français résidant lui aussi en France.

En outre, cette situation pourrait probablement créer une difficulté pour les entreprises qui contractent avec des personnes résidant en France dans notre exemple. Pour s'assurer de la validité du consentement des personnes avec lesquelles elles sont liées par un contrat, en plus de respecter la loi du pays qui les institue, ces entreprises devraient vérifier la nationalité des personnes concernées par le traitement, lorsque celles-ci sont des mineurs, afin d'établir le droit applicable pour le consentement. Une telle constatation ne semble pas évidente à la lecture du Règlement ou des lois d'exécution et génère de l'insécurité juridique aussi bien pour les responsables de traitement que pour les personnes concernées quant au droit applicable.

### 2.3.) *Quelques réflexions supplémentaires : une question de catégorie de rattachement ?*

Face à ce constat de lois nationales qui prétendent régler la question de la capacité à consentir au traitement de données avec un facteur de rattachement autre que celui de la nationalité du mineur, nous pouvons nous demander comment caractériser ou qualifier la question de la capacité au sens du RGPD. En effet, traiter la capacité en ce qui concerne les données à caractère personnel comme ne relevant pas du champ d'application dans l'espace prévu par chaque législateur national, comme une question pour laquelle il se serait « trompé » et qu'il faudrait rattacher à un autre critère (celui de la nationalité) semble apporter de la confusion, sans doute non voulue par le législateur européen. Il s'agirait alors d'un problème de qualification à donner à cette capacité dans ce secteur juridique en particulier. En d'autres termes, « *lorsqu'une question de droit soulève un conflit de lois et qu'on veut le résoudre au moyen d'une règle de conflit, la première question qui se pose est de rapporter cette question à une catégorie de rattachement donnée ; c'est une opération de qualification ou classification qui, le cas échéant, soulève un conflit de catégories* »<sup>229</sup>. Il s'agit donc d'un exercice de segmentation de la matière du droit en catégories de rattachement (le type de situation juridique) avec une loi qui leur est propre, désignée au moyen d'un facteur de rattachement (l'élément caractéristique)<sup>230</sup>.

C'est sur cette base qu'est suscitée notre réflexion : il se peut que le consentement dans le domaine des données personnelles ne relève pas de la loi applicable en matière de statut personnel, mais

---

<sup>229</sup> B. AUDIT, L. D'AVOUT, *op. cit.*, 2018, p. 239.

<sup>230</sup> J.-L. VAN BOXTAEL, « Division du droit en catégories », *Rép. Not.*, Tome XVIII, Droit international privé, Livre 0, Code DIP – Premiers commentaires, Bruxelles, Larcier, 2018, p. 211. ; B. AUDIT, L. D'AVOUT, *Droit international privé*, Paris, Economica, 2013, p. 146.

d'une autre catégorie de rattachement, une catégorie qui serait alors propre à ce droit fondamental. Ce consentement précis s'éloignerait ainsi du noyau central de la catégorie « statut personnel »<sup>231</sup>, l'incapacité générale du mineur n'ayant pas d'impact en matière de données personnelles, puisqu'elle affecterait un de leurs droits propres en tant que mineurs. En effet, une certaine doctrine soutient que même l'âge par défaut de 16 ans prévu par le RGPD serait trop élevé, eu égard aux droits de l'enfant garantis par la Convention des Nations Unies de 1989<sup>232</sup>. En vertu de cette dernière, les enfants ont, entre autres, le droit d'apprendre, la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières<sup>233</sup>. Or, cela est de nos jours grandement favorisé par le monde numérique. Selon cette doctrine donc, l'article 8 §1<sup>er</sup> du RGPD interdirait ainsi aux enfants de moins de 16 ans de participer activement à de nombreuses activités sur Internet, dont la plupart sont des moyens valables pour communiquer et s'instruire, même si elles comportent certains risques en matière de protection des données<sup>234</sup>.

Une telle argumentation justifierait alors que chaque législateur national s'en prévale et choisisse que la question de la capacité à consentir de ce qu'il advient de nos données personnelles, pour son ordre juridique, soit déterminée soit par la résidence de la personne, soit par l'établissement du responsable de traitement ou par un autre critère qu'il aurait adopté pour l'applicabilité spatiale sa législation d'exécution.

Notons que cette réflexion, quoiqu'ayant le mérite de justifier l'inclusion de l'article 8 du RGPD parmi les marges de manœuvres et de faciliter l'analyse des conflits de lois du règlement dans son ensemble, reste assez théorique à ce stade. Elle pourrait, selon nous, assurément servir de source d'inspiration pour les cours et tribunaux qui souhaiteraient opter pour une interprétation uniforme du champ d'application des lois nationales, sans devoir systématiquement segmenter celui-ci pour la question du consentement du mineur.

Inversement, les juridictions pourraient trouver plus logique que cette disposition du RGPD reste absorbée par les règles de rattachement générales sur l'état et la capacité. Dans ce dernier cas, il pourrait être utile, afin de faire œuvre de clarté, de préciser directement dans chaque loi d'exécution que pour cette marge de manœuvre du RGPD, il y a lieu de se référer directement à la loi de la nationalité du mineur.

## **§2. La personne concernée par le traitement est-elle un consommateur ?**

Nous supposons dans le cadre de cette étude que le mineur est de nationalité belge mais réside en France et que, par conséquent, le contrat est valable. A défaut de choix de loi, pour savoir quel droit s'applique au contrat de vente noué entre la société française et le mineur belge et ainsi au traitement des données, il faut déterminer quel article du règlement Rome I est pertinent en l'espèce. Il contient quatre

---

<sup>231</sup> Voy. raisonnement suivi par les auteurs B. AUDIT, L. D'AVOUT, *op. cit.*, 2018, p. 240.

<sup>232</sup> Convention relative aux droits de l'enfant, signée à New York le 20 novembre 1989, approuvée par une loi du 25 novembre 1991, *M.B.*, 17 janvier 1992, p. 803 ; Đ. KRIVOKAPIĆ, J. ADAMOVIĆ, *op. cit.*, p. 209.

<sup>233</sup> Convention relative aux droits de l'enfant, signée à New York le 20 novembre 1989, *op. cit.*, art. 13.

<sup>234</sup> Đ. KRIVOKAPIĆ, J. ADAMOVIĆ, *op. cit.*, p. 210.

dispositions spéciales sur des contrats conclus avec une partie réputée faible<sup>235</sup>, à savoir le passager dans un contrat de transport<sup>236</sup>, le consommateur dans un contrat de consommation<sup>237</sup>, le souscripteur d'assurance dans certains contrats d'assurances<sup>238</sup> et le travailleur dans un contrat individuel de travail<sup>239</sup>. Le but de ces dispositions est de prévoir un niveau de protection équilibré, par le droit international privé dans des relations par nature déséquilibrées<sup>240</sup>, où la liberté de choix de la loi applicable ne manquerait pas d'être utilisée au détriment des cocontractants concernés<sup>241</sup>.

### 1. Le champ d'application personnel de l'article 6 du règlement Rome I tel que défini par la jurisprudence européenne

Le régime qui nous intéresse ici concerne les consommateurs et la question de savoir si le contrat issu du cas pratique peut être considéré comme un contrat de consommation. S'agissant de ces contrats, un parallèle est fait par le législateur européen entre les textes relatifs aux conflits de juridictions et ceux propres aux conflits de lois<sup>242</sup>. Une identité d'interprétation est également opérée par la jurisprudence européenne qui a rendu de nombreux arrêts dans le cadre des conflits de juridiction qui sont transposables aux questions de loi applicable<sup>243</sup>. En effet, comme nous l'avons évoqué également par rapport à la matière civile et commerciale ou par rapport aux obligations contractuelles (voy. *supra*), les champs d'application respectifs des règlements se fondent sur des notions similaires<sup>244</sup>. Un tel rapprochement paraît d'autant plus avantageux, lorsqu'il s'agit d'assurer une cohérence entre les dispositions, afin d'apporter des solutions avantageuses à des plus « petites » demandes, telles que celles de consommateurs<sup>245</sup>.

#### 1.1) *Le consommateur*

La Cour de justice retient une interprétation stricte de la notion de consommateur<sup>246</sup>. Elle considère qu'il s'agit de la personne qui conclut un contrat à des fins privées, par lequel elle ne s'engage pas « dans des activités professionnelles ou commerciales »<sup>247</sup>. Dans le prolongement de cette définition, la Cour a affirmé qu'une personne contractant en vue d'une activité professionnelle future ne pouvait être qualifiée de consommateur qui aurait noué un contrat de consommation<sup>248</sup>. De plus, dans l'affaire *Gruber*, le juge européen a précisé que, s'agissant des contrats conclus dans un but mixte, c'est-à-dire dans un but revêtant à la fois un caractère privé et professionnel, il ne s'agira pas de contrats de consommation « *sauf si l'usage professionnel est marginal au point d'avoir un rôle négligeable dans le contexte global de*

<sup>235</sup> Đ. KRIVOKAPIĆ, J. ADAMOVIĆ, *op. cit.*, p. 130.

<sup>236</sup> Article 5, §2, du règlement Rome I.

<sup>237</sup> Article 6, du règlement Rome I.

<sup>238</sup> Article 7, § 3, du règlement Rome I.

<sup>239</sup> Article 8, du règlement Rome I.

<sup>240</sup> F. RAGNO, « The Law Applicable to Consumer Contracts under the Rome I Regulation », in *Rome I Regulation. The Law Applicable to Contractual Obligations in Europe*, Munich, Sellier, p. 129.

<sup>241</sup> B. AUDIT, L. D'AVOUT, *op. cit.*, p. 870.

<sup>242</sup> G. LARDEUX, *op. cit.*, p. 266.

<sup>243</sup> *Ibid.*, p. 268.

<sup>244</sup> G. LARDEUX, *op. cit.*, p. 268.

<sup>245</sup> F. RAGNO, *op. cit.*, p.136.

<sup>246</sup> P. WAUTELET, « Le consommateur, le réseau social et l'action collective », *J.D.E.*, 2018, p. 261.

<sup>247</sup> Arrêt Bertrand/Paul Ott KG., C-150/77, EU:C:1978:137, point 21.

<sup>248</sup> Arrêt Francesco Benincasa/Dentalkit Srl., C-269/95, EU:C:1997:337, points 18-19.

*l'opération en cause, le fait que l'aspect extraprofessionnel prédomine étant sans incidence à cet égard* »<sup>249</sup>. Les règles protectrices telles que délimitées par la jurisprudence européenne sont incontestablement source de sécurité juridique<sup>250</sup>. Deux conditions doivent donc être respectées pour que les dispositions étudiées s'appliquent à un contrat mixte : d'une part, celui qui se prétend être consommateur doit prouver que la partie professionnelle est non négligeable et, d'autre part, le cocontractant du consommateur ne doit pas avoir légitimement ignoré la finalité extraprofessionnelle de l'opération<sup>251</sup>. Il appartient au juge saisi de vérifier, au cas par cas, si ces conditions sont réunies et, notamment, le rôle signifiant ou insignifiant de l'usage professionnel<sup>252</sup>. Cette appréciation se prendra en considération des éléments de fait pertinents, sans « *tenir compte de circonstances ou d'éléments dont le cocontractant aurait pu avoir connaissance lors de la conclusion du contrat, sauf si la personne qui invoque la qualité de consommateur s'est comportée de manière telle qu'elle a légitimement pu faire naître l'impression, dans le chef de l'autre partie au contrat, qu'elle agissait à des fins professionnelles* »<sup>253</sup>. Dans ce dernier cas, elle ne pourra pas se prévaloir des règles de conflits de lois sur les contrats de consommation<sup>254</sup>.

Le règlement Rome I, en son article 6 §1<sup>er</sup>, prévoit, en outre, que la personne concernée doit être une personne physique<sup>255</sup>. Cette dernière doit donc invoquer une prétention individuelle. Il s'infère que ce régime de protection du consommateur en droit international privé ne peut pas être invoqué par une association de consommateurs<sup>256</sup>. La Cour européenne a estimé qu'une telle action doit alors être qualifiée d'extracontractuelle<sup>257</sup>.

Récemment, la Cour de justice a rendu un arrêt *Schrems II*<sup>258</sup> qui vient préciser l'importance de la qualité de consommateur dans un monde fonctionnant, en permanence, à travers des communications électroniques. Bien que la question principale concernée par cet arrêt soit relative au for compétent pour des infractions aux droits autrichien, irlandais et de l'Union en matière de protection de la vie privée et des données personnelles, elle n'est intéressante suite à l'entrée en vigueur du RGPD que pour ce qui concerne la loi applicable<sup>259</sup>. Les règles favorables sur la compétence juridictionnelle en matière de contrats de consommation prévues par le règlement Bruxelles I *bis*<sup>260</sup> ne sont, en effet, plus utiles pour les litiges contre un responsable de traitement ou un sous-traitant, puisque l'article 79 du RGPD prévoit un droit à un recours juridictionnel effectif de la personne concernée, notamment devant les juridictions de

---

<sup>249</sup> Arrêt Johann Gruber/Bay Wa AG., C-464/01, EU:C:2005:32, point 54.

<sup>250</sup> G. LARDEUX, *op. cit.*, p. 268.

<sup>251</sup> Arrêt Johann Gruber (...), *op. cit.*, points 51 et s. ; J. TORO, « DIP, protection des consommateurs et contrats », in *Contrats et protection des consommateurs* (sous la dir. de C. VERDURE), Limal, Anthemis, 2016, p. 102.

<sup>252</sup> Arrêt Johann Gruber (...), *op. cit.*, point 47.

<sup>253</sup> *Ibid.*, point 54.

<sup>254</sup> F. RAGNO, *op. cit.*, p. 135.

<sup>255</sup> G. LARDEUX, *op. cit.*, p. 268.

<sup>256</sup> *Ibid.*, p. 269.

<sup>257</sup> Arrêt Verein für Konsumenteninformation/Karl Heinz Henkel, C-167/00, EU:C:2002:555, points 40 et 41.

<sup>258</sup> Arrêt Maximilian Schrems/Facebook Ireland Limited, C-498/16, EU:C:2018:37.

<sup>259</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Shrems II accès au juge en matière de protection des données : une solution en demi-teinte potentiellement remise en cause par le RGPD », *D.*, 2018, p. 2002.

<sup>260</sup> Section 4, du règlement Bruxelles *Ibis*.

l'Etat membre où il a sa résidence habituelle<sup>261</sup>. La Cour, dans son arrêt, commence à rappeler sa jurisprudence antérieure<sup>262</sup>. Elle adopte, ensuite, une interprétation plus souple de la notion de consommateur, en faveur des utilisateurs des réseaux sociaux, tels que Facebook<sup>263</sup>. Elle affirme, de fait, qu' « *il y a notamment lieu de tenir compte, s'agissant de services d'un réseau social numérique ayant vocation à être utilisés pendant une longue durée, de l'évolution ultérieure de l'usage qui est fait de ces services* »<sup>264</sup>. Un utilisateur de réseau social peut donc développer en parallèle une activité professionnelle sur ce réseau et garder la qualification de consommateur, à condition que l'activité demeure marginale<sup>265</sup>. Cette interprétation « diachronique » mise en avant par la Cour permet donc de prendre en compte les évolutions dans l'utilisation qui est faite d'un réseau social, afin de déterminer la qualité de consommateur ou non de la personne concernée, dans la détermination de la loi applicable<sup>266</sup>.

### 1.2.) Le professionnel

Outre la conclusion d'un contrat de consommation, pour que l'application de l'article 6 du règlement soit enclenchée, il est nécessaire que le cocontractant du consommateur soit une personne qui agisse dans le cadre de son activité professionnelle<sup>267</sup>. Une méthode indiciaire est alors suivie, afin de conclure le degré de connexion entre la direction des activités du professionnel et l'Etat du domicile du consommateur<sup>268</sup>. Le professionnel peut exercer son activité professionnelle directement dans le pays concerné ou peut diriger cette activité vers cet Etat, sans y être présent physiquement<sup>269</sup>. Dans ce deuxième cas, l'intention du professionnel de diriger ses activités vers tel pays pour entrer en relations commerciales avec les consommateurs sera déterminante, et non le simple fait que ses biens ou services soient accessibles depuis l'étranger via un site internet par exemple<sup>270</sup>. A cet égard, une série d'indices énumérés de manière non exhaustive par la Cour de Justice doivent être pris en considération afin de s'orienter vers une protection du consommateur ou du professionnel<sup>271</sup>. A titre exemplatif, la langue du site ne constitue pas un élément pertinent pour démontrer la volonté du professionnel de diriger ses activités vers l'Etat membre du domicile du consommateur<sup>272</sup>. La Cour énonce d'autres indices, pouvant être éventuellement combinés les uns aux autres, qui, au contraire, apporteront une telle preuve, notamment « *la nature internationale de l'activité en cause [...], la mention de coordonnées téléphoniques*

---

<sup>261</sup> L'article 79 § 2, du RGPD est rédigé comme suit : « *Toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'Etat membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. Une telle action peut aussi être intentée devant les juridictions de l'Etat membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un Etat membre agissant dans l'exercice de ses prérogatives de puissance publique* ».

<sup>262</sup> Arrêt Maximilian Schrems (...), *op. cit.*, points 27 à 32.

<sup>263</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Shrems II accès au juge en matière de protection des données : (...) », *op. cit.*, p. 2001.

<sup>264</sup> Arrêt Maximilian Schrems (...), *op. cit.*, point 37.

<sup>265</sup> P. WAUTELET, *op. cit.*, p. 261.

<sup>266</sup> F. JAULT-SESEKE, C. ZOLYNSKI, « Shrems II accès au juge en matière de protection des données : (...) », *op. cit.*, p. 2001.

<sup>267</sup> V. MARQUETTE, « Le Règlement "Rome I" sur la loi applicable aux contrats internationaux », *R.D.C.-T.B.H.*, 2009, p. 530.

<sup>268</sup> J. DE MEYER, « International jurisdiction and conflict of law rules for consumer claims: a survey of European legislation », *R.E.D.C.*, 2009, p. 641.

<sup>269</sup> N. MICHAIL, « Entre le RGPD et le Règlement Bruxelles Ibis : quel juge pour protéger nos données personnelles ? », *D.C.C.R.*, 2019, p. 179.

<sup>270</sup> V. MARQUETTE, *op. cit.*, p. 531.

<sup>271</sup> E. ALVAREZ ARMAS, M. DECHAMPS, « Arrêt Pammer et Hotel Alpenhof : L'équilibre entre consommateurs et professionnels dans l'e-commerce », *R.E.D.C.*, 2011, p. 450.

<sup>272</sup> G. LARDEUX, *op. cit.*, p. 275.

avec l'indication du préfixe international, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État membre où le commerçant est établi [...] »<sup>273</sup>.

## 2. Le droit applicable en vertu de l'article 6 du règlement Rome I

Le règlement Rome I prévoit deux règles principales de protection des consommateurs<sup>274</sup>. Premièrement, en l'absence de clause de choix de loi insérée par les parties, le droit applicable par défaut est le droit du pays de la résidence habituelle du consommateur<sup>275</sup>. Deuxièmement, si les parties ont choisi le droit applicable à leur contrat, ce choix ne peut cependant avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions auxquelles il ne peut être dérogé par un accord en vertu de la loi de sa résidence principale<sup>276</sup>. Cela sera vérifié par le juge<sup>277</sup>. Le consommateur bénéficie ainsi de l'applicabilité d'un système de droit qu'il connaît bien et il ne se heurte pas aux aléas des systèmes étrangers qui pourraient l'étonner<sup>278</sup>. Il s'agit d'un système hybride qui tente de concilier le principe de l'autonomie de la volonté des parties avec le besoin de protéger le consommateur qui se trouve, par sa nature, dans une position déséquilibrée par rapport à son cocontractant, en définissant une règle de rattachement personnelle et exclusive<sup>279</sup>.

## 3. Application au cas pratique du mineur

Il n'y a aucun doute sur le fait que le mineur, dans notre exemple, n'agit pas en tant que professionnel et recevra donc la qualité de consommateur. En faisant jouer les règles de droit commun pour les questions du litige autres que sa capacité (cfr. *supra*), le mineur bénéficie ainsi des règles protectrices en vigueur dans l'Etat de sa résidence, à savoir les règles françaises. Le droit applicable à cette relation sera donc le droit français, ce qui pourrait, en outre, paralyser une éventuelle clause de choix de loi qui figurerait dans les conditions générales du contrat<sup>280</sup>.

Dans ce cas précis, le droit international privé européen renvoie vers le droit national de la résidence habituelle, aussi bien pour les questions non traitées par le RGPD que pour les questions laissant une marge de manœuvre au législateur français. Ainsi, comme nous l'avons étudié, ce dernier a précisément utilisé le critère de la résidence de la personne concernée par le traitement pour déterminer le champ d'application dans l'espace des règles exécutant le RGPD. L'utilisation de ce critère de rattachement par le législateur français marque, en dépit de la question du consentement du mineur, une

---

<sup>273</sup> Arrêt Peter Pammer/Reederei Karl Schlüter GmbH & Co. KG, C-585/08, Hotel Alpenhof GesmbH/Oliver Heller, C-144/09, EU:C:2010:740, point 83.

<sup>274</sup> L. BEIL, « Reconciling private international law with European consumer law: where to start consumer protection in the context of e-commerce? », in *Boundaries of European Private International Law. Les frontières du droit international privé européen. Las fronteras del derecho internacional privado europeo*, Bruxelles, Bruylant, 2015, p. 544.

<sup>275</sup> Art. 6, §1, du règlement Rome I.

<sup>276</sup> Art. 6, §2, du règlement Rome I.

<sup>277</sup> D. P. FERNANDEZ ARROYO, « Consumer protection in international private relations », in *Consumer Protection in International Private Relationships. La protection des consommateurs dans les relations privées internationales*, Asunción, CEDEP, 2010, p. 680. ; J.-P. MOINY, B. DE GROOTE, « "Cyberconsommation" et droit international privé », *R.D.T.I.*, 2009, p. 20.

<sup>278</sup> C. BISPING, « Mandatorily Protected : The Consumer in the European Conflicts of Laws », *E.R.P.L.*, 2014, p. 514.

<sup>279</sup> F. FERRARI, F. RAGNO, « European Union », in *Consumer Protection in International Private Relationships. La protection des consommateurs dans les relations privées internationales*, op.cit., p. 596.

<sup>280</sup> JAULT-SESEKE, C. ZOLYNSKI, « Shrems II accès au juge en matière de protection des données : (...) », op. cit., p. 2002.

cohérence dans le système et est en continuité avec les règles de droit commun des conflits de lois pour tous les cas où la personne concernée aurait effectivement la qualité de consommateur.

### **§3. Autres règles prévues par le règlement Rome I : fondements classiques de rattachement**

L'article 4 du règlement détermine le droit applicable à une relation contractuelle à défaut de choix de loi<sup>281</sup>. Cet article est appliqué, par ailleurs, sans préjudice notamment de l'article 6 précité, qui prévoit des règles spéciales pour les contrats de consommation<sup>282</sup>. Le premier paragraphe de l'article 4 du règlement Rome I prévoit une règle fixe pour le facteur de localisation en fonction du type du contrat concerné<sup>283</sup>. Il s'agit des contrats les plus usuels. Pour un contrat de vente de biens, par exemple, le droit applicable sera celui de la résidence habituelle du vendeur, alors que pour un contrat de prestations de services, ce sera la loi du pays où le prestataire a sa résidence habituelle<sup>284</sup>. Lorsque le contrat correspond à plusieurs contrats visés par cette disposition ou à aucun de ceux-ci, est applicable la loi de la résidence habituelle du débiteur de la prestation caractéristique, en vertu de l'article 4 §2 du règlement<sup>285</sup>. A titre illustratif, la prestation caractéristique dans un contrat de vente allié à la prestation de certains services serait celle du vendeur, tandis que dans un contrat d'assurance, ce serait celle de l'assureur<sup>286</sup>. Si celle-ci ne peut être identifiée ou si un contrat présente des liens plus étroits avec un autre pays, le droit de ce dernier devra régir le contrat<sup>287</sup>.

L'analyse de l'application concrète de cet article à un mineur qui se voit reconnaître la qualité de consommateur presque naturellement dans notre casus ne présente pas beaucoup d'intérêt. Néanmoins, des conflits de lois risquent de se poser au même titre s'agissant des domaines dans lesquels les législateurs nationaux exécutent ou complètent le règlement. Ces conflits sont suscités par l'absence de règle de conflit de loi dans le règlement et la multitude de critères de rattachement potentiellement choisis respectivement dans chaque loi nationale. A partir du moment où ces derniers diffèrent de ceux de l'article 4 du règlement Rome I, des discordances dans leur applicabilité peuvent se présenter (voy. *supra*). Imaginons, à titre illustratif, la situation où une entreprise française vend des logiciels à une entreprise située sur le territoire belge. Dans le cadre de cette relation contractuelle, des données sont traitées. Pour identifier la loi nationale qui doit être appliquée afin de déterminer les sanctions pénales pouvant être infligées par exemple, le règlement Rome I mènerait à l'application de la loi française d'exécution, puisqu'il s'agit de la loi du pays où le débiteur de la prestation caractéristique a sa résidence habituelle. Cependant, cette loi prévoit que, pour les règles implémentant le RGPD, elle s'applique « *dès lors que la personne concernée réside en France* »<sup>288</sup>. Or, dans ce cas « la personne concernée » ne renvoie non seulement

<sup>281</sup> A. SAVIN, *EU Internet Law*, Cheltenham, Elgar, 2017, p. 93.

<sup>282</sup> R. PLENDER, M. WILDERSPIN, *The European Private International Law of Obligations*, London, Sweet & Maxwell, 2009, p. 176.

<sup>283</sup> S. FRANCO, « Le règlement "Rome I" sur la loi applicable aux obligations contractuelles », *J.D.I.*, 2008, p. 5.

<sup>284</sup> Article 4 §1, points a) et b), du règlement Rome I.

<sup>285</sup> A. NUYTS, « II. – Obligations contractuelles », in *Actualités en droit international privé*, Bruxelles, Bruylant, 2013, p. 142.

<sup>286</sup> R. PLENDER, M. WILDERSPIN, *op. cit.*, pp. 187-188.

<sup>287</sup> *Ibid.*, pp. 196-197. ; article 4, §3, du règlement Rome I. `

<sup>288</sup> Art. 3, II. de la loi française n° 78-17 du 6 janvier 1978.

pas à une personne morale<sup>289</sup>, mais surtout vise la personne dont les données sont traitées et non le responsable du traitement.

#### **§4. Fais du casus inversés : une société établie en France**

Nous avons pris l'exemple d'une société établie en Belgique traitant notamment avec des mineurs, résidant en France. Dans une telle hypothèse, si l'un des mineurs est de nationalité belge, cela permet à l'entreprise de traiter ses données personnelles dans le cadre de leur contrat, le mineur ayant atteint l'âge de 13 ans accomplis lorsqu'il consent au traitement. Il se peut, comme nous l'avons expliqué, que le mineur ne soit pas de nationalité belge ou encore qu'il ne réside pas en France. Nous avons brièvement mentionné quelles seraient alors les conséquences de tels éléments d'extranéité dans la relation contractuelle du point de vue du droit international privé.

Pensons maintenant au scénario inverse, celui d'une entreprise établie en France qui traite les données de ses cocontractants mineurs résidant en Belgique.

##### 1. Mineur de nationalité belge résidant en Belgique

###### *1.1.) Droit applicable à la question du consentement*

Comme mentionné ci-dessus, l'état et la capacité des personnes physiques sont exclues du champ d'application matériel du règlement Rome I. Afin de déterminer la licéité du traitement des données à caractère personnel d'un mineur de moins de 16 ans, il faut alors se tourner vers le droit de la nationalité du mineur, sachant que la question relève de la catégorie « statut personnel » (sous-réserve des considérations énoncées *supra*).

Si le mineur qui réside en Belgique dans notre casus est de nationalité belge, la loi belge est d'application. Le consentement en matière de données personnelles est déterminé par la loi d'exécution du RGPD du 30 juillet 2018. Cette loi prévoit, en son article 7, que le consentement au traitement des données est licite lorsqu'il a été donné par des enfants âgés de 13 ans ou plus<sup>290</sup>. Nous serions donc facilement tentés d'arriver à la conclusion que le mineur, par rapport à notre exemple, étant âgé de 14 ans, a respecté ce prescrit juridique. Toutefois, une telle conclusion peut être perturbée par l'applicabilité spatiale de cette loi d'exécution, en vertu de son article 4 §1<sup>er</sup>, déterminée par le traitement dans le cadre des activités d'un établissement du responsable de traitement localisé sur le territoire belge<sup>291</sup>. Le responsable de traitement étant ici établi en France, le traitement visé ne rentre, en principe, pas dans le champ d'application de la loi belge.

---

<sup>289</sup> Voy. art. 4, 1), du RGPD.

<sup>290</sup> Art. 7, al. 1, de la loi belge du 30 juillet 2018.

<sup>291</sup> Art. 4, §1, de la loi belge du 30 juillet 2018.

Le consentement du mineur de nationalité belge ne serait-il, par conséquent, pas protégé par la loi belge ou faudrait-il quand même lui appliquer cet article en vertu du respect des règles sur son statut personnel ? Il serait probable que la deuxième solution soit adoptée en pratique, par souci de simplicité et afin de s'assurer la détermination la plus aisée du seuil de l'âge pour le consentement. Toutefois, la situation reste problématique au regard du raisonnement classique du droit international privé et il n'est pas possible d'identifier une solution claire.

### *1.2.) Droit applicable pour les autres questions*

Pour les questions autres que le consentement, des conflits de lois subsistent. Partant du postulat que le contrat en cause est un contrat de consommation, l'article 6 du règlement Rome I indique qu'un tel contrat est régi par la loi du pays dans lequel le consommateur a sa résidence habituelle. Il s'agit également du droit belge. A cet égard, il faut opérer une distinction entre les conflits de lois concernant les questions non traitées par le règlement et les conflits concernant les dispositions qui laissent une marge de manœuvre aux législateurs nationaux (voy. *supra*). Dans la première hypothèse, les règles du droit belge sont pleinement applicables. Nous pouvons notamment penser au droit civil.

Pour la deuxième hypothèse néanmoins, nous sommes confrontés encore une fois à une impasse, la relation contractuelle concernée n'étant pas visée par le champ d'application dans l'espace de la loi d'exécution du RGPD en son article 4 §1<sup>er</sup> précité. Le règlement Rome I mène donc à l'application d'une loi qui ne prévoit pas qu'elle s'applique dans une telle situation, à savoir en présence d'un établissement situé dans l'Union européenne, mais en dehors de la Belgique.

Faudrait-il ignorer la volonté d'application de la loi belge désignée par le règlement Rome I et l'appliquer, afin de préserver la protection que prétend offrir ce dernier ? A défaut, comment déterminer la compétence éventuelle d'un autre ordre juridique ? Le RGPD et les lois nationales ne prévoyant pas les balises nécessaires pour répondre à ces questionnements, la solution sera laissée à l'appréciation des juges et autres praticiens.

## 2. Mineur de nationalité française résidant en Belgique

### *2.1.) Droit applicable à la question du consentement*

Pour déterminer si le consentement du mineur de nationalité française est licite, il y a lieu d'appliquer sa loi nationale, à savoir le droit français et, pour le traitement des données à caractère personnel, les dispositions adoptées comme mesure d'exécution du RGPD. Le droit français prévoit que le seuil d'âge est de 15 ans pour valablement consentir au traitement de données<sup>292</sup>. Toutefois, le même

---

<sup>292</sup> Art. 45, de la loi française n° 78-17 du 6 janvier 1978.

problème au regard du champ d'application dans l'espace se pose ici également. Le mineur français n'est pas résident français et n'est donc a priori pas concerné par la loi d'exécution française.

Quelle loi doit alors être prise en compte pour conclure à la validité ou non du contrat ? La loi française s'applique-t-elle à toute personne ayant la nationalité française, au moins pour les questions de capacité et abstention faite du critère de rattachement choisi par le législateur ? Les interrogations sont ici encore nombreuses et ne permettent donc pas aux individus de savoir quel droit ils doivent à respecter, alors même qu'il s'agit de relations ou transactions courantes.

## 2.2.) Droit applicable pour les autres questions

Les considérations évoquées au point 1.2) du §4 de la présente section sont pertinentes à l'identique dans ce cas de figure. En effet, la nationalité de la personne n'impacte nullement les règles de conflits de lois prévues par le règlement Rome I. Elle n'est, en outre, pas prévue comme critère de rattachement dans les deux lois d'exécution qui font l'objet de l'analyse dans la présente étude. L'article 6 du règlement Rome I désignerait, dans ce cas, la loi belge, avec toutes les conséquences que cela implique (voy. *supra*).

## Section III. Les relations extracontractuelles

La différence entre le droit à la vie privée et la protection des données à caractère personnel ne semble pas toujours évidente et a souvent fait l'objet de débats<sup>293</sup>. Ces derniers portent sur la question de savoir si le droit à la protection des données peut être considéré comme autonome par rapport au droit à la vie privée ou bien s'il s'agit d'un aspect de ce dernier<sup>294</sup> (§ 1). Cette question peut avoir des implications pratiques importantes, notamment du point de vue du droit international privé, quant à l'application de certains instruments juridiques, tels que le règlement Rome II sur la loi applicable aux obligations non contractuelles (§ 2). Ce règlement ne régit pas la loi applicable aux violations de vie privée et aux droits de la personnalité, de telle sorte que la question d'une révision de celui-ci soit particulièrement pertinente suite à l'entrée en vigueur du RGPD (§ 3).

### §1. Le droit à la vie privée et le droit à la protection des données

Selon D. Cooper et C. Kuner, la meilleure manière de comprendre ces deux droits consiste à dire que la protection des données est liée à la vie privée, mais que ces deux notions ne sont pas des synonymes<sup>295</sup>. La protection des données à caractère personnel concerne le contrôle de la collecte et de l'utilisation qui s'ensuit, contrôle qui vise à protéger la vie privée de la personne à laquelle les données se

<sup>293</sup> M. BRKAN, « Data Protection and Conflict-of-laws: (...) », *op. cit.*, p. 331.

<sup>294</sup> M. TZANOU, « Is Data Protection the same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures », *J.I.L.*, 2013, p. 26.

<sup>295</sup> D. COOPER., C. KUNER, *op. cit.*, p. 60.

rapportent<sup>296</sup>. La vie privée serait donc un concept plus large que la protection des données<sup>297</sup>. Elle est à comprendre « *comme faculté d'autodétermination, d'autonomie, capacité de l'individu à effectuer des choix essentiels* »<sup>298</sup>. Cette notion engloberait le respect d'autres questions que celles strictement liées à la protection des données, comme par exemple la non-ingérence dans les affaires privées, le droit d'être laissé seul dans son intimité ou l'identité individuelle<sup>299</sup>. De la même manière, toutes les informations sur une personne identifiée ou identifiable considérées comme données personnelles ne rentrent pas nécessairement dans la sphère de la vie privée<sup>300</sup>. En ce sens, la protection des données personnelles couvre des informations entrant dans un champ plus large que celui de la vie privée<sup>301</sup>. Par ailleurs, les données à caractère personnel sont protégées non seulement pour garantir le respect de la vie privée, mais aussi celui d'autres droits fondamentaux comme le droit à la non-discrimination<sup>302</sup>. Ainsi, la violation de l'une d'elles n'impliquerait pas nécessairement la violation de l'autre.

Les différents champs d'application de ces droits peuvent, en outre, être déduits des deux articles différents de la Charte des droits fondamentaux de l'Union européenne<sup>303</sup>. L'article 7 de cette Charte prévoit que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications<sup>304</sup>. Il existe un article différent, à savoir l'article 8 de ladite Charte, qui traite spécifiquement du droit fondamental à la protection des données à caractère personnel<sup>305</sup>. Cette approche peut être soutenue par le fait que la Cour de justice mentionne habituellement les deux droits dans sa jurisprudence, même si elle les analyse souvent de concert ou de manière entremêlée<sup>306</sup>.

Une autre tentative de dissocier le droit à la protection des données personnelles du droit à la vie privée, sans toutefois nier leur lien, vient de la formulation et de la terminologie utilisées dans le RGPD. Contrairement à la directive 95/46/CE<sup>307</sup> qui le précédait, le règlement ne semble, en réalité, pas accorder une place plus importante au droit à la vie privée par rapport aux autres droits et libertés fondamentaux<sup>308</sup>. La vie privée est uniquement mentionnée dans son considérant 4, parmi d'autres droits fondamentaux à être respectés par le règlement et est ainsi explicitement distinguée du droit à la protection des données par le règlement<sup>309</sup>.

---

<sup>296</sup> D. COOPER., C. KUNER, *op. cit.*, pp. 60-61.

<sup>297</sup> Arrêt *The Bavarian Lager Co. Ltd/Commission des Communautés européennes*, T-194/04, EU:T:2007:334, point 118.

<sup>298</sup> C. DE TERWANGNE, « Chapitre 9 – Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, p. 329.

<sup>299</sup> M. TZANOU, *op. cit.*, p. 26.

<sup>300</sup> D. COOPER., C. KUNER, *op. cit.*, p. 60.

<sup>301</sup> J. KOKOTT, C. SOBOTTA, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *I.D.P.L.*, 2013, p. 225; M. TZANOU, *op. cit.*, p. 26.

<sup>302</sup> CEPD – Contrôleur européen de la protection des données, « Accès du public aux documents et protection des données », Documents de référence, Juillet 2005, p. 15, [https://edps.europa.eu/sites/edp/files/publication/05-07\\_bp\\_accesstodocuments\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_fr.pdf) (consulté le 22 avril 2019).

<sup>303</sup> J. KOKOTT, C. SOBOTTA, *op. cit.*, p. 223.

<sup>304</sup> Charte des droits fondamentaux de l'Union européenne, art. 7, *J.O.U.E.*, 26 octobre 2012, C 326.

<sup>305</sup> *Ibid.*, art. 8.

<sup>306</sup> M. BRKAN, « Data protection and Conflict-of-laws: (...) », *op. cit.*, p. 331; C. DE TERWANGNE, « Chapitre 9 – Internet et la protection de la vie privée (...) », *op. cit.*, p. 332. ; Arrêt *Google Spain SL (...)*, *op. cit.*, point 80; Arrêt *Digital Rights Ireland Ltd/ Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande, The Attorney General*, C-293/12 et C-594/12, EU:C:2014:238, point 47.

<sup>307</sup> Voy. notamment considérants 8 et 9, de la directive 95/46/CE.

<sup>308</sup> M. CLEMENT-FONTAINE, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Legicom*, 2017, p. 64.

<sup>309</sup> Considérant 4, du RGPD.

## §2. Etat des lieux sur le règlement Rome II

Pour revenir au casus de départ, le mineur pourrait vouloir également tenter une action en réparation contre l'entreprise qui a frauduleusement reçu et traité ses données, alors même qu'ils ne sont pas liés par un contrat. En ce qui concerne les relations non-contractuelles ou les aspects extracontractuels d'un litige, le règlement prévoit le droit à la réparation du préjudice moral ou matériel subi<sup>310</sup>. Sont également prévues quelques règles spécifiques sur les responsabilités qui peuvent être engagées<sup>311</sup>. Toutefois, il n'harmonise pas certaines questions comme celle du calcul des dommages et intérêts, par exemple. Il faut alors passer par le droit international privé général pour déterminer le droit applicable à ces questions. Nous quittons, dès lors, la sphère du règlement Rome I pour nous intéresser au règlement Rome II sur la loi applicable aux obligations non contractuelles<sup>312</sup>. Ce dernier ne définit pas ce qu'il faut entendre par « obligations non-contractuelles ». Selon la jurisprudence de la Cour de justice de l'Union, il faut comprendre cette notion comme « toute demande qui vise à mettre en jeu la responsabilité d'un défendeur et qui ne se rattache pas à la « matière contractuelle » » (voy. *supra*)<sup>313</sup>. Le concept est donc défini négativement, par rapport à ce qu'il ne concerne pas. Les champs d'application des règlements Rome I et Rome II doivent ainsi être interprétés conjointement, de telle sorte que le champ de l'un exclue celui de l'autre<sup>314</sup>.

Toutefois, le rôle du règlement Rome II en matière de protection des données personnelles est controversé et souvent exclu. En effet, en vertu de son article 1<sup>er</sup> §2, sont exclues du champ d'application du règlement, notamment « les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité, y compris la diffamation »<sup>315</sup>. C'est face à cette exclusion que le débat sur la distinction entre le droit à la vie privée et le droit à la protection des données mentionné ci-dessus devient intéressant. Il n'est en effet, pas évident de savoir si, dans le contexte de ce règlement, la qualification de vie privée inclut les considérations en matière de données personnelles<sup>316</sup>. Sans nier tout ce que ces deux droits ont en commun, certains auteurs s'appuient sur le fait que ces deux droits ne sont pas équivalents et sont garantis par deux articles différents dans la Charte des droits fondamentaux de l'UE pour affirmer que les questions de protection des données peuvent tomber dans le champ d'application de Rome II<sup>317</sup>. De plus, nous avons expliqué que toutes les questions de données personnelles ne sont pas nécessairement liées à la sphère de la vie privée.

---

<sup>310</sup> Art. 82, du RGPD.

<sup>311</sup> R. ROBERT, C. PONSART, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, p. 438.

<sup>312</sup> Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II), *J.O.U.E.*, 31 juillet 2007, L 199, p. 40.

<sup>313</sup> Arrêt Athanasios Kalfelis (...), *op. cit.*, points 17-18.

<sup>314</sup> A. SCOTT, « The Scope of "Non-Contractual Obligations" », in *The Rome II Regulation on the Law Applicable to Non-Contractual Obligations : A New International Litigation Regime*, Leiden, Nijhoff, 2009, p. 61.

<sup>315</sup> Art. 1 § 2, g), du règlement Rome II.

<sup>316</sup> M. BRKAN, « Data protection and Conflict-of-laws: (...) », *op. cit.*, p. 331.

<sup>317</sup> J. CHEN, *op. cit.*, p. 318 ; J. KOKOTT, C. SOBOTTA, *op.cit.*, p. 223.

Toujours est-il que l'exclusion visée par le règlement avait, aux yeux du législateur, sans doute pour but de s'étendre également aux actions civiles impliquant des responsables de traitement suite à une utilisation ou divulgation illicite de données à caractère personnel. Initialement, la Commission avait proposé de ne pas exclure les obligations non-contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité. Un article dans le règlement y était consacré<sup>318</sup>. Ensuite, le Parlement européen, tant dans son premier<sup>319</sup> que dans son second rapport<sup>320</sup>, a proposé une modification du contenu de cet article, en y incluant notamment un libellé se rapportant spécialement « à la violation de la vie privée ou des droits de la personnalité dans le cadre du traitement des données personnelles »<sup>321</sup>. Toutefois, aucun accord n'a pu être trouvé concernant le facteur de rattachement et l'article, y compris avec les amendements proposés par le Parlement européen, n'a tout simplement pas été inclus dans la version finale du règlement<sup>322</sup>. Si une approche téléologique est adoptée dans l'interprétation de cette exclusion, il semble donc plus probable que les atteintes à la protection des données personnelles soient hors du champ d'application du règlement, au même titre que celles à la vie privée<sup>323</sup>. Il serait, de fait, difficile en pratique d'établir une ligne de démarcation claire entre ces deux types d'atteintes et, par conséquent, de déterminer le droit applicable, si la vie privée était exclue et pas la protection des données<sup>324</sup>.

Le règlement Rome II excluant les obligations non contractuelles découlant d'atteintes à la vie privée et aux autres droits de la personnalité, il faut se référer aux règles de droit international privé nationales du pays de la juridiction qui a été saisie, afin de déterminer le droit applicable. Il s'avère que la plupart des systèmes juridiques nationaux des États membres n'ont pas de règles particulières concernant le droit applicable en matière de responsabilité non contractuelle pour les dommages causés par les médias aux droits relatifs à la personnalité<sup>325</sup>. Le droit belge, au contraire, prévoit une disposition. Si le litige est pendant devant les juridictions belges, il faudra alors appliquer le Code de droit international privé en son article 99 §2, qui contient une règle spécifique pour ces atteintes<sup>326</sup>.

---

<sup>318</sup> L'article 6 tel que proposé par la Commission dans Proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non-contractuelles (« Rome II »), C.O.M. (2003) 427 final était rédigé comme suit :

« 1. La loi applicable à l'obligation non contractuelle résultant d'une atteinte à la vie privée ou aux droits de la personnalité est celle du for lorsque l'application de la loi désignée par l'article 3 serait contraire aux principes fondamentaux du for en matière de liberté d'expression et d'information.

2. La loi applicable au droit de réponse ou aux mesures équivalentes est celle du pays où l'organisme de radiodiffusion ou l'éditeur de journaux a sa résidence habituelle ».

<sup>319</sup> Rapport I sur la proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles ("Rome II"), article 6, P.E. Doc., A6-0211/2005, du 27 juin 2005.

<sup>320</sup> Recommandation pour la deuxième lecture relative à la position commune du Conseil en vue de l'adoption du règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles ("ROME II"), article 7bis, P.E. Doc., A6-0481/2006 du 22 décembre 2006.

<sup>321</sup> A. DICKINSON, *The Rome II Regulation : the law applicable to non-contractual obligations*, Oxford, Oxford university press, 2008, p. 240.

<sup>322</sup> G. VAN CALSTER, *European Private International Law*, Oxford, Hart, 2016, p. 248.

<sup>323</sup> M. BRKAN, « Data protection and Conflict-of-laws: (...) », *op. cit.*, p. 331; N. MICHAIL, « Le domaine d'application du GDPR: (...) », *op. cit.*, p. 75.

<sup>324</sup> *Ibid.*

<sup>325</sup> Etude de la Commission européenne, « Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality », JLS/2007/C4/028, Privacy Study, Final Report, février 2009, p. 77.

<sup>326</sup> L'article 99 §2 du Codip est rédigé comme suit : « Toutefois, l'obligation dérivant d'un acte de diffamation ou d'une atteinte à la vie privée ou aux droits de la personnalité est régie par le droit de l'Etat sur le territoire duquel le fait générateur ou le dommage est survenu ou menace de survenir, au choix du demandeur, à moins que la personne responsable n'établisse qu'elle ne pouvait pas prévoir que le dommage surviendrait dans cet Etat ».

### §3. La possibilité d'introduire une nouvelle clause dans Rome II ?

Quoique la règle prévoyant la loi applicable pour la protection des données ne se trouve finalement pas dans le règlement Rome II, ce dernier ne semble pas pour autant complètement ignorer la matière<sup>327</sup>. Il contient une clause de révision en son article 30, selon laquelle la Commission européenne est tenue de préparer une étude relative à la loi applicable aux obligations non contractuelles découlant des atteintes à la vie privée et aux droits de la personnalité, en prenant en compte notamment « [...] les questions de conflit de loi liées à la directive 95/46/CE [...] »<sup>328</sup>.

La Commission, toutefois, n'a pas pris de réelle initiative après avoir effectué l'étude<sup>329</sup>. En 2012, le Parlement européen a adopté une résolution pour faire suite aux travaux de la Commission<sup>330</sup>. Ce document avait pour but de proposer l'ajout d'un nouvel article dans le règlement Rome II, relatif à la vie privée et aux droits découlant de la personnalité. Il proposait, notamment, que la loi applicable pour les violations des droits de la personnalité résultant du traitement des données personnelles soit la loi du pays dans lequel l'éditeur, le radiodiffuseur ou le responsable du traitement a sa résidence habituelle<sup>331</sup>. L'amendement proposé par le Parlement retenait un critère différent de celui qu'avait proposé la Commission européenne, quoique non retenu *in fine*, dans les discussions qui ont précédé l'adoption du règlement Rome II. En effet, la règle de conflits de lois qu'elle énonçait était fondée sur l'application de la loi du pays du dommage direct, à savoir la loi du pays dans lequel le ou les éléments les plus significatifs du dommage surviennent ou sont susceptibles de survenir<sup>332</sup>. Cette loi tendrait à entraîner l'application de la loi du pays de résidence habituelle de la personne lésée, les services de radiodiffusion ou la publication étant principalement dirigés vers son pays<sup>333</sup>. La proposition de la Commission avait été plutôt en faveur de la personne concernée alors que celle du Parlement en faveur des médias. Cette initiative du Parlement n'a toutefois pas mené à une quelconque modification du règlement.

Le rapport de la Commission européenne prouve qu'il existe d'énormes disparités entre Etats membres sur la loi applicable aux obligations non-contractuelles, découlant de la violation de la protection des données personnelles, qui ont empêché qu'un consensus soit atteint<sup>334</sup>. Ces différences impactent bien évidemment la construction du marché intérieur. Cependant, un tel constat peut paraître contradictoire suite à l'adoption du RGPD, qui a précisément comme objectif principal d'uniformiser, de

---

<sup>327</sup> A. DICKINSON, *op. cit.*, p. 240.

<sup>328</sup> Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II), article 30 § 2, *J.O.U.E.*, 31 juillet 2007, L 199, p. 40.

<sup>329</sup> Etude de la Commission européenne, « Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality », *op. cit.* ; G. VAN CALSTER, *op. cit.*, p. 250.

<sup>330</sup> Résolution du Parlement européen du 10 mai 2012 contenant des recommandations à la Commission sur la modification du règlement (CE) n° 864/2007 sur la loi applicable aux obligations non contractuelles (Rome II), *P.E. doc.*, P7\_TA(2012)0200 du 10 mai 2012.

<sup>331</sup> *Ibid.*, art. 5bis, § 4.

<sup>332</sup> Proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non-contractuelles (« Rome II »), article 6, *C.O.M.* (2003) 427 final ; Etude de la Commission européenne, *op. cit.*, *JLS/2007/C4/028*, Privacy Study, Final Report, février 2009, p. 74.

<sup>333</sup> Etude de la Commission européenne, *op. cit.*, *JLS/2007/C4/028*, Privacy Study, Final Report, février 2009, p. 74.

<sup>334</sup> *Ibid.*, p. 7.

manière générale, la matière de protection des données et de réaliser le marché intérieur<sup>335</sup>. Or, comme le souligne la Commission européenne, l'harmonisation des règles de conflit de lois des États membres pour résoudre les litiges transfrontaliers apporterait une plus grande sécurité juridique dans l'espace judiciaire européen, puisqu'elle définirait la loi applicable à l'obligation indépendamment de la juridiction qui serait compétente<sup>336</sup>.

Se pose alors la question de savoir quel facteur de rattachement devrait être préféré, dans l'hypothèse où une règle de conflits de lois serait insérée dans le règlement Rome II. Si nous suivons une interprétation systémique de ce dernier, nous aurions tendance à plutôt proposer une règle favorable à la personne concernée (par le traitement) qui serait lésée dans ses droits. En effet, la règle générale du règlement Rome II prévue en son article 4 stipule que « *la loi applicable est celle du pays où le dommage survient, quel que soit le pays où le fait générateur du dommage se produit et quels que soient le ou les pays dans lesquels des conséquences indirectes de ce fait surviennent* »<sup>337</sup>. Le pays où le dommage survient, dans le cadre d'une violation des droits de la personnalité, correspond probablement au lieu où les effets d'une violation de ses droits en question se font le plus sentir et donc au pays de la résidence habituelle de la personne<sup>338</sup>. Cela impliquerait, en l'occurrence, que le responsable de traitement devrait prendre en considération, voire même respecter, le contenu de la loi la plus proche de la personne dont les droits sont en cause, qui est réputée être plus « faible » dans la relation. Une telle solution concorderait, par ailleurs, avec l'avis émis par la Commission européenne dans sa proposition.

#### **Chapitre 4. Bilan des questions envisagées dans le cadre de cette étude au regard du droit international privé et autres pistes de réflexion**

La résolution des conflits de lois par la méthode conflictuelle classique prévue par les règlements Rome I et Rome II a le mérite d'envisager des solutions et de combler, en partie, le silence de l'article 3 du RGPD quant au droit applicable. Toutefois, elle ne semble pas, en toute hypothèse, adaptée à l'environnement juridique des données personnelles (Section I). En effet, les incertitudes et débats sur l'application du règlement Rome II, d'une part, invitent à exclure l'application de celui-ci à l'heure actuelle, par précaution. Le droit applicable aux aspects extracontractuels d'un litige en la matière dépendra alors exclusivement du droit de l'Etat du for. En ce qui concerne les relations contractuelles, d'autre part, le règlement Rome I ne semble résoudre que certains conflits.

Toujours est-il que le recours aux règles de conflit de droit commun constitue probablement la première voie que les praticiens et juridictions vont suivre face au constat de la fragmentation du droit des données personnelles pour certaines questions. Si la résolution de notre cas pratique s'avère

---

<sup>335</sup> Considérant 2, du RGPD.

<sup>336</sup> Etude de la Commission européenne, *op. cit.*, JLS/2007/C4/028, Privacy Study, Final Report, février 2009, p. 142.

<sup>337</sup> Art. 4, §1, du règlement Rome II.

<sup>338</sup> Etude de la Commission européenne, *op. cit.*, JLS/2007/C4/028, Privacy Study, Final Report, février 2009, p.145.

effectivement source de questionnements et d'insécurité juridique dans leur pratique, comme nous le prévoyons, ils seront vite amenés à envisager d'autres pistes de réflexion (Section II).

## **Section I. L'absence de solution satisfaisante dans les règles de droit commun**

Deux constats, au moins, peuvent être établis à propos du cas pratique analysé dans le chapitre précédent. Premièrement, l'existence des lois nationales prévoyant un champ d'application spatial différent l'un de l'autre mène inévitablement à des situations de cumul et de lacune (§ 1). De ce constat en résulte un second, qui implique que le règlement Rome I désigne parfois une loi d'exécution qui n'entend pas s'appliquer à la situation, d'après la lecture seule de celle-ci. Nous nous interrogeons donc sur la nature « spéciale » de ces lois nationales par rapport aux instruments juridiques étudiés. Celle-ci peut être analysée notamment sous deux angles distincts : eu égard au phénomène de l'autolimitation, d'une part, et sur base de l'article 23 du règlement Rome I d'autre part (§ 2).

### **§1. Hypothèses de « cumul » et de « lacune » suite à l'adoption du RGPD**

Les règles, tant de droit international privé national qu'europpéen, énoncées dans le chapitre précédent, présentent clairement une structure bilatérale, en ce sens qu'elles partent d'un type de situation, de manière abstraite, pour déterminer l'ordre juridique avec lequel la situation présente les liens les plus proches<sup>339</sup>. Le bilatéralisme implique donc d'identifier un rapport de droit, afin de déterminer la loi applicable<sup>340</sup>. La règle de conflit bilatérale s'applique en fonction d'un élément de rattachement, nonobstant toute « *considération relative à l'identité ou à la localisation spatiale de ses destinataires* »<sup>341</sup>. Il s'agit donc d'une règle abstraite, en ce sens qu'elle a uniquement pour but de répartir la compétence des ordres juridiques pour régir une situation donnée<sup>342</sup>. En ce sens, elle englobe toute situation correspondant à son hypothèse d'application<sup>343</sup>. Elle est également neutre, ne s'intéressant, en principe, pas au contenu de la loi désignée suite à son application<sup>344</sup>.

Néanmoins, comme l'expliquent les auteurs, M. Attal et A. Raynouar, dans leur ouvrage portant sur les principes généraux du droit international privé, la question de la capacité au travers de la règle de conflit bilatérale est une illustration de la faiblesse du conflit bilatéral<sup>345</sup>. Ce constat est, selon nous, pertinent dans le cadre de la protection des données à caractère personnel d'un mineur dans le cadre du RGPD. En effet, si nous prenons l'exemple d'un mineur belge résidant en France, qui accepte que ses données soient traitées dans le cadre d'une relation contractuelle avec une entreprise établie sur le territoire français, le juge français saisi devra normalement appliquer sa règle de conflit. Cette dernière

<sup>339</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 145.

<sup>340</sup> M. ATTAL, A. RAYNOUAR, *Droit international privé – Tome 1 : Principes généraux*, Bruxelles, Larcier, 2013, p. 96.

<sup>341</sup> P. MAYER, « Le phénomène de la coordination des ordres juridiques étatiques en droit privé – Cours général de droit international privé », *R.C.A.D.I.*, 2007, t. 327, p. 146.

<sup>342</sup> M. ATTAL, A. RAYNOUAR, *op. cit.*, p. 98.

<sup>343</sup> S. FRANCO, « Unilateralism », in *European Encyclopedia of Private International Law*, Cheltenham, Edward Elgar Publishing, 2017, p. 1786.

<sup>344</sup> M. ATTAL, A. RAYNOUAR, *op. cit.*, p. 98.

<sup>345</sup> *Ibid.* p. 105.

soumet la capacité de la personne à un rattachement au droit du pays de la nationalité. Cela implique que les nationaux se verront appliquer les dispositions internes sur la capacité, peu importe leur lieu de résidence, et les non nationaux se verront appliquer les lois sur le sujet de leurs pays respectifs<sup>346</sup>. Par conséquent, le juge appliquerait, sans entrer dans le détail des considérations énoncées précédemment, la loi belge d'exécution du RGPD qui prévoit le seuil de l'âge de consentement valable. Fortes sont les chances qu'il s'intéresse uniquement à l'article pertinent sur l'âge du consentement, sans nécessairement avoir égard au reste du contenu de cette loi<sup>347</sup>. Or, cette loi préfère peut être appliquer ses règles en matière de capacité à consentir aux données personnelles sur base d'un critère différent, renonçant par là à l'appliquer à certaines personnes<sup>348</sup>. Une telle idée, dans notre raisonnement, aurait comme fondement le fait que la loi belge prévoit un champ d'application dans l'espace qui dépend de l'établissement en Belgique du responsable de traitement. Elle ne se réfère à aucun moment à la nationalité de la personne concernée. A supposer, toutefois, que le juge français tienne compte de la substance de la loi belge, il ne saurait alors quel droit appliquer entre le droit belge – ce qui irait hors du domaine que la loi s'assigne et méconnaîtrait ainsi sa volonté d'application – ou le droit français, dans quel cas il risquerait d'aller à l'encontre de sa propre règle de conflit bilatérale.

Le même constat peut être établi pour les autres questions de conflits de lois pour lesquelles nous serions amenés à appliquer le règlement Rome I (voy. *supra*). Les règlements européens uniformisant le droit international privé, tant en matière contractuelle qu'extracontractuelle, sont fondés sur un système bilatéral<sup>349</sup>. Nous avons montré que le règlement Rome I peut également créer des situations d'impasse, par exemple lorsque la loi nationale belge d'exécution est désignée applicable en vertu de l'article 6 du règlement Rome I, alors même que le responsable du traitement n'est pas établi sur le territoire belge. « *Est ainsi dénoncée l'insoutenable abstraction de la règle de conflit bilatérale qui fait application d'une loi dans l'hypothèse où le propre législateur de cette loi ne l'aurait pas appliquée* »<sup>350</sup>.

En réalité, les lois nationales exécutant le RGPD répondent à la logique inverse du bilatéralisme, à savoir celle de l'unilatéralisme. Au contraire d'une détermination abstraite de la loi applicable, « *la règle de droit international privé unilatérale est celle par laquelle le législateur détermine le domaine d'application de la loi qu'il édicte ou désigne les rapports tombant sous l'empire de sa propre législation* »<sup>351</sup>. Elle a, ainsi, une volonté propre d'application à certaines situations ou personnes déterminées ou déterminables<sup>352</sup>. Il s'ensuit qu'il existe forcément des cas où elle ne se veut pas applicable et il faut, par conséquent, rechercher la loi étrangère qui présente un champ d'application spatial incluant la situation<sup>353</sup>.

---

<sup>346</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 152.

<sup>347</sup> M. ATTAL, A. RAYNOUAR, *op. cit.*, p. 105.

<sup>348</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 153.

<sup>349</sup> S. FRANCO, « Unilatéralisme versus bilatéralisme : une opposition ontologique ou un débat dépassé ? Quelques considérations de droit européen sur un couple en crise perpétuelle », in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, p. 58.

<sup>350</sup> *Ibid.*

<sup>351</sup> P. GOTHOT, « Le renouveau de la tendance unilatéraliste en droit international privé », *Rev. crit. DIP.*, 1971, p. 1.

<sup>352</sup> *Ibid.*, pp. 18-19 ; S. FRANCO, « Unilatéralisme versus bilatéralisme : (...) », *op. cit.*, p. 52.

<sup>353</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 153.

La méthode unilatéraliste est, toutefois, caractérisée par des faiblesses qui sont notamment perceptibles dans la réglementation de la protection des données personnelles. L'efficacité que propose l'unilatéralisme ne se présente qu'en cas de coordination spontanée des systèmes, à savoir lorsqu'une loi en présence se veut applicable et que les autres excluent leur applicabilité<sup>354</sup>. Dans ce cas, le résultat est le même que via la règle de conflit bilatérale<sup>355</sup>. Il arrive pourtant que cette logique soit perturbée par des situations de « cumul » de compétence des ordres juridiques (conflit positif). Deux lois étrangères entendent s'appliquer à une situation concrète<sup>356</sup>. Une deuxième difficulté, à l'inverse, appelée « lacune », se présente lorsqu'aucune loi ne revendique son application (conflit négatif)<sup>357</sup>.

Nous avons montré, au départ de notre cas pratique, que ces problèmes sont plus fréquents que prévu en matière de protection des données personnelles, suite à l'entrée en vigueur du RGPD. A titre illustratif, pour tout ce qui concerne la mise en œuvre du RGPD, la loi française s'applique lorsque la personne réside en France, alors que la loi belge s'applique aux responsables de traitement ou sous-traitants établis en Belgique<sup>358</sup>. Par le fait même d'utiliser des facteurs de rattachement différents pour leur applicabilité respective, il se peut qu'une relation contractuelle ou extracontractuelle donnée rencontre les deux éléments, de telle sorte que les deux lois entrent en concurrence (un résident français et un responsable de traitement établi en Belgique) ou n'en rencontrent aucun des deux (un résident belge et un responsable de traitement établi en France). C'est précisément cette totale liberté au niveau de l'élaboration du champ d'application spatial des lois nationales qui est, à notre sens, source d'insécurité juridique dans la résolution des conflits de lois entre Etats membres.

Les auteurs unilatéralistes proposent classiquement plusieurs solutions, afin de résoudre ces conflits, tant positifs que négatifs. Pour les premiers, il a notamment été proposé d'appliquer des règles multilatérales ou encore d'appliquer la loi qui, en pratique, a les meilleures chances de s'appliquer ou que les parties avaient en vue par rapport à la situation<sup>359</sup>. Il semblerait, selon certains auteurs, qu'une option efficace pour solutionner les conflits positifs consiste également en l'application de la loi du for lorsqu'elle est en cause ou, s'il s'agit de deux lois étrangères, de la loi qui présente des critères de rattachement proches de la règle du for<sup>360</sup>. S'agissant de la lacune, des solutions similaires ont été avancées : appliquer la loi du for à titre de vocation subsidiaire, la loi en fonction de laquelle les parties se sont comportées ou celle qui présente un lien le plus logique avec la situation<sup>361</sup>. Toujours est-il que les résultats proposés ne coïncident pas avec la logique même de l'unilatéralisme, puisqu'ils « aboutissent à conférer au droit du for le soin de décider de l'applicabilité du droit étranger »<sup>362</sup>.

<sup>354</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 154.

<sup>355</sup> *Ibid.* ; M. ATTAL, A. RAYNOUAR, *op. cit.*, p. 106.

<sup>356</sup> M.-L. NIBOYET, G. DE GEOUFFRE DE LA PRADELLE, *Droit international privé*, Paris, Lextenso Editions, 4<sup>e</sup> éd., 2013, p. 167.

<sup>357</sup> O. CACHARD, *Droit international privé*, Bruxelles, Larcier, 5<sup>e</sup> éd., 2016, p. 183.

<sup>358</sup> Art. 3, II. de la loi française n° 78-17 du 6 janvier 1978 ; Art. 4, §1, de la loi belge du 30 juillet 2018.

<sup>359</sup> S. FRANCO, « Unilateralism », *op. cit.*, p. 1785. ; M.-L. NIBOYET, G. DE GEOUFFRE DE LA PRADELLE, *op. cit.*, p. 168.

<sup>360</sup> B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, pp. 154-155 ;

<sup>361</sup> S. FRANCO, « Unilateralism », *op. cit.*, p. 1785. ; B. AUDIT, L. D'AVOUT, *op.cit.*, 2013, p. 155 ; O. CACHARD, *op. cit.*, 2016, p. 183.

<sup>362</sup> M.-L. NIBOYET, G. DE GEOUFFRE DE LA PRADELLE, *op. cit.*, p. 168.

Ces considérations sur la nature unilatérale des lois d'exécution ne nous font pas spécialement progresser dans la recherche du droit applicable. Abstraction faite des incertitudes au niveau de la qualification des données à caractère personnel comme relevant de la matière civile et commerciale (voy. *supra*), nous constatons que la résolution des conflits de lois par l'intermédiaire du règlement Rome I ne semble pas apporter de solution satisfaisante dans tous les cas. Il reste donc des hypothèses où la détermination du droit applicable n'est pas claire, eu égard au champ d'application des lois nationales pertinentes.

## **§2. Argument de la « *lex specialis* »**

### 1. Le règlement Rome I peut-il forcer l'application d'une loi nationale à des situations qu'elle ne vise pas ? Raisonnement à partir du phénomène de l'autolimitation

Nous avons remarqué que le règlement Rome I mène parfois à l'application d'une loi nationale d'exécution alors même que celle-ci n'entend pas s'appliquer, le facteur de rattachement qu'elle prévoit n'étant pas rencontré dans certaines situations. Concrètement, le droit d'un pays est d'abord désigné applicable via une règle de conflit de lois, telles que celles contenues dans le règlement Rome I. Ce processus a pour but de déterminer l'ordre juridique compétent dont une situation est la plus proche sans s'intéresser, en principe, au contenu de la loi potentiellement applicable<sup>363</sup>. Ainsi, par exemple, l'article 6 du règlement Rome I soumet la loi applicable à celle du pays de la résidence habituelle du consommateur.

#### *1.1.) Contextualisation théorique*

Dans le contexte de la protection des données personnelles suite à l'entrée en vigueur du RGPD, la distinction entre la substance de la règle et les conditions pour son applicabilité pourrait s'avérer pertinente. En effet, il est possible que certaines règles présentent des facteurs d'applicabilité, sans pour autant être caractérisées de règles de conflits de lois<sup>364</sup>. Il est alors dit que la règle délimite son domaine d'application spatial de manière neutre<sup>365</sup>. Il s'agit de normes autolimitées ou du phénomène d'autolimitation<sup>366</sup>. Cela implique que, dans un premier temps, l'ordre juridique concerné doit avoir été désigné compétent d'après les règles de droit international privé<sup>367</sup>. Ce n'est que dans un second temps, après la confirmation de l'applicabilité de celui-ci aux termes des règles de conflits de lois, qu'il y a lieu d'identifier quelles règles sont pertinentes et les sélectionner<sup>368</sup>. Certaines règles, au sein d'un ordre juridique, délimitent leur champ d'application spatial et leur contenu doit être vérifié en conséquence. Cette délimitation est le résultat de critères du droit matériel et non du droit international privé<sup>369</sup>. Ces lois,

<sup>363</sup> S. FRANCO, « The Scope of Secondary Community Law in the light of the methods of Private International Law – or the other way around? », *Yearbook of Private International Law*, volume 8, 2006, p. 350.

<sup>364</sup> *Ibid.*

<sup>365</sup> *Ibid.*

<sup>366</sup> D. CHILSTEIN, *Droit pénal international et lois de police : Essai sur l'application dans l'espace du droit pénal accessoire*, Paris, Dalloz, 2003, p. 221.

<sup>367</sup> P. MAYER, « Les lois de polices étrangères », *op. cit.*, p. 282.

<sup>368</sup> S. FRANCO, « Unilateralism », *op. cit.*, p. 1788.

<sup>369</sup> P. KINSCH, « L'autolimitation implicite des normes de droit privé matériel » *Rev. crit. DIP*, 2003, p. 405.

prévoyant de s'appliquer à certaines situations géographiques, excluent forcément des situations qui « *n'entrent pas dans le domaine spatial qu'elles assignent ; l'indication de ce domaine n'aurait autrement aucun sens* »<sup>370</sup>. Par conséquent, si ces règles autolimitées ne s'appliquent pas, une autre règle du même Etat devra s'appliquer<sup>371</sup>. L'ordre juridique auquel la règle appartient ne devient donc pas incompétent pour autant<sup>372</sup>. C'est la raison pour laquelle la doctrine indique que ces règles constituent des *lex speciales*, par opposition à des *lex generales*<sup>373</sup>.

Pour déterminer le sens exact d'une autolimitation, outre une interprétation systémique, la méthode téléologique d'interprétation peut souvent être utilisée. Il revient donc au juge de se référer au but poursuivi par le législateur en édictant la norme pour conclure sur le caractère expressément ou implicitement autolimité de celle-ci<sup>374</sup>.

### 1.2.) *Qu'en est-il des lois d'exécution nationales du RGPD?*

Si le droit belge est désigné par la règle de conflit bilatérale, nous constatons qu'il faut que le traitement des données soit effectué dans le cadre des activités d'un établissement situé en Belgique<sup>375</sup>. Sans substituer le mécanisme des règles de droit international privé en matière de conflits de lois, nous nous demandons si la norme du droit qui a été désignée entend réellement être appliquée à la situation concrète qu'il s'agit de juger<sup>376</sup>. L'argument potentiellement en faveur de la qualification des lois d'exécution comme normes autolimitées serait alors de dire qu'il se peut que ces lois ne fassent pas sens au-delà de leur champ d'application, sachant qu'il y a autant de lois d'exécution que d'Etats membres. Il serait aisé de penser qu'une situation de traitement entrera « d'office » dans le champ d'application spatial d'une des 28 (bientôt 27) lois d'exécution nationales. Nous avons néanmoins prouvé qu'une telle affirmation ne peut être confirmée en l'état actuel du cadre législatif européen.

Comme argument dans le sens inverse, nous pourrions penser au fait que l'applicabilité spatiale de ces lois n'est peut-être pas de nature exclusive, mais simplement *indicative*. Il se pourrait que, même si la situation examinée ne rentre pas formellement dans le champ d'application spatial commandé par la loi, cette dernière ne refuse pas pour autant son application<sup>377</sup>. Elle s'appliquerait alors – dans tous les cas – aux critères désignés et – potentiellement – dans d'autres cas. Un raisonnement par analogie avec la matière de la protection du consommateur pourrait soutenir une telle idée, prenant acte du fait qu'en principe, « [...] *les règles relatives à la protection des consommateurs sont applicables non seulement à ceux qui sont visés par le critère spécial de rattachement, mais plus généralement à tous les*

<sup>370</sup> P. MAYER, « Les lois de polices étrangères », *op. cit.*, p. 340.

<sup>371</sup> *Ibid.*, p. 286.

<sup>372</sup> D. CHILSTEIN, *op. cit.*, p. 221.

<sup>373</sup> S. FRANCO, « The Scope of Secondary Community Law (...) », *op. cit.*, p. 350. ; B. AUDIT, L. D'AVOUT, *op. cit.*, 2013, p. 160.

<sup>374</sup> *Ibid.*, pp. 410-413.

<sup>375</sup> Article 4, §1, de la loi belge du 30 juillet 2018.

<sup>376</sup> P. KINSCH, *op. cit.*, p. 405.

<sup>377</sup> Nous insistons sur le fait qu'il s'agit ici à nouveau d'une hypothèse que nous émettons dans le cadre de notre réflexion.

*consommateurs [...] »<sup>378</sup>. Nous admettons toutefois qu'une telle considération sur un champ d'application spatial plus « ouvert » de ces lois reste fort théorique et risquerait, en outre, de créer davantage de conflits de lois<sup>379</sup>.*

Plus généralement, soutenir que la règle est autolimitée et donc exclut des situations de son champ d'application, aurait comme conséquence qu'une personne qui pensait, en théorie, être protégée par rapport à son droit fondamental à la protection des données ne le serait pas, en pratique. Reprenons l'hypothèse où l'article 6 du règlement Rome I conduit à l'application du droit belge. Suivant la logique de l'autolimitation mentionnée ci-dessus, à défaut de contracter avec un établissement situé en Belgique, par exemple, comme le prévoit la loi belge du 30 juillet 2018, il faudrait appliquer une autre loi au sein de l'ordre juridique belge, avec le risque toutefois qu'elle ne soit pas adaptée à la matière des données personnelles ou n'offre pas une protection équivalente. Pourtant, comme l'explique P. Mayer, pour un certain type de relations, il peut exister des règles homologues, non pas dans le même pays, mais « *dans un autre ordre juridique dont la compétence peut être jugée préférable* »<sup>380</sup>. Bien que nous ne puissions pas, dans la présente étude, nous étendre sur les avantages que pourrait présenter une loi nationale d'exécution par rapport à une autre qui se veut également applicable, il faut reconnaître qu'elles remplissent toutes les deux une fonction de protection des données à caractère personnel au sein de l'Union européenne. Il convient d'interpréter ces lois à la lumière du système du marché intérieur, de telle sorte que la protection voulue par le RGPD soit assurée en toute hypothèse<sup>381</sup>. L'importance serait alors de veiller à ce que dès qu'un traitement est effectué dans le cadre des activités d'un établissement d'un responsable de traitement situé « dans le territoire de l'Union », tel que le prévoit l'article 3 §1<sup>er</sup> du RGPD, une loi d'exécution puisse impérativement être considérée comme applicable, afin d'éviter les situations de lacune ou de vide juridique qui pourraient se poser.

## 2. L'article 23 du règlement Rome I

Un autre point de vue peut encore être adopté pour soutenir que la protection des données personnelles par le RGPD serait une *lex specialis*. Nous avons clarifié la relation actuelle entre le règlement Rome II et les règles de protection des données. Il reste, toutefois, à envisager un aspect du règlement Rome I, qui s'avérerait en tout cas pertinent lorsque la directive 95/46/CE était en vigueur<sup>382</sup>. Le règlement Rome I semble être la solution naturelle en matière contractuelle, afin de résoudre les conflits de lois qui se posent dans les relations intra-européennes. En effet, le droit européen a une valeur supérieure aux droits nationaux des Etats membres. Ce principe de primauté est un principe fondamental

---

<sup>378</sup> P. MAYER, « Les lois de polices étrangères », *op. cit.*, p. 341. L'auteur affirme que ces règles ne sont pas autolimitées car portant sur « la considération d'intérêts privés non liés par nature à un environnement économique ou social particulier ».

<sup>379</sup> En effet, si toutes les lois s'appliquent potentiellement à plus de situations, les conflits de lois ne seront qu'accrochés.

<sup>380</sup> P. MAYER, « Les lois de polices étrangères », *op. cit.*, p. 343.

<sup>381</sup> Voy. à cet égard, les Conclusions de l'avocat général Szpunar du 26 octobre 2016, sous l'arrêt *Agro Foreign Trade & Agency Ltd/Petersime NV*, C-507/15, EU:C:2016:809, points 22 et 55-60, qui traite du caractère autolimitatif de la législation belge transposant la directive 86/653/CE dans le cadre d'un agent commercial établi dans un Etat tiers.

<sup>382</sup> M. BRKAN, « Data Protection and Conflict-of-Laws: (...) », *op. cit.*, p. 332.

qui vaut pour tous les actes européens ayant force obligatoire et pendant toute leur durée de validité<sup>383</sup>. Cependant, les dispositions de droit national qui nous intéressent sont des dispositions qui exécutent un règlement<sup>384</sup>. Ces dispositions peuvent être considérées non pas comme soumises au règlement Rome I, mais comme devant être lues et interprétées indépendamment de celui-ci. En effet, l'article 23 de ce règlement porte sur la relation de ce dernier avec d'autres dispositions du droit européen et stipule qu'« *il n'affecte pas l'application des dispositions de droit communautaire qui, dans des domaines particuliers, règlent les conflits de lois en matière d'obligations contractuelles* »<sup>385</sup>. Nous pourrions donc soutenir que le règlement Rome I serait la *lex generalis* et le RGPD avec ses lois d'exécution seraient les *lex speciales*. C'est ainsi qu'était perçu l'article 4 de la directive 95/46/CE, comme une disposition spéciale, étant donné qu'elle réglementait un domaine particulier et, prévoyait pour celui-ci, une règle pour résoudre les conflits de lois qui se poseraient avec la transposition de la directive<sup>386</sup>. Toutefois, l'importance à accorder à cette priorité n'était pas certaine selon les auteurs et eu égard à la jurisprudence de la Cour de Justice<sup>387</sup>.

Comme évoqué précédemment, il n'existe pas d'équivalent de l'article 4 de la directive en termes de conflits de lois dans le RGPD. L'idée sous-jacente à ce raisonnement de l'article 23 du règlement Rome I serait de dire que, face aux problèmes que suscite la détermination de la loi applicable en vertu de ce même règlement, les lois nationales pourraient s'appliquer en priorité par rapport à celui-ci. Toutefois, nous avons constaté que la résolution des conflits de lois par les lois d'exécution nationales, par leur aspect unilatéral d'applicabilité, ne réduirait pas pour autant l'insécurité juridique quant au droit applicable<sup>388</sup>. En effet, même sans passer par l'intermédiaire du règlement Rome I, les problèmes de cumul ou de lacune que nous avons identifiés subsisteront (voy. *supra*). Par ailleurs, les autorités et les juges des Etats membres pourraient renforcer les conflits de lois qui risquent de se poser, s'ils interprètent plus ou moins largement le champ d'application de la loi qu'ils seront chargés d'appliquer<sup>389</sup>.

## **Section II. Quelques pistes de réflexions supplémentaires quant à la détermination du droit applicable**

Nous arrivons au constat que les règles classiques de droit international privé ne permettent pas de résoudre de manière satisfaisante l'entièreté des conflits susceptibles de se poser dans un contexte de traitement de données personnelles. Face à ce constat, il reste d'autres pistes à explorer dans le but de faire avancer la réflexion et d'espérer trouver une solution. Parmi celles-ci, l'on pourrait penser, en premier lieu, de laisser de côté les règles classiques prévues par le règlement Rome I et de se pencher sur une approche à partir de la théorie des lois de police, également appelées lois d'application immédiate<sup>390</sup>,

---

<sup>383</sup> L. VOGEL, « Chapitre 1 – Primauté du droit européen », in *Traité de droit économique – Tome 4 : Droit européen des affaires*, Bruxelles, Bruylant, 2017, p. 323.

<sup>384</sup> N. MICHAIL, « Le domaine d'application du GDPR : (...) », *op. cit.*, p.78.

<sup>385</sup> Art. 23, du règlement Rome I.

<sup>386</sup> M. BRKAN, « Data Protection and Conflict-of-Laws: (...) », *op. cit.*, p. 332.

<sup>387</sup> *Ibid.*, pp. 332-333. ; Arrêt Verein für Konsumenteninformation (...), *op. cit.*, points 72-80.

<sup>388</sup> N. MICHAIL, « Le domaine d'application du GDPR : (...) », *op. cit.*, p.78.

<sup>389</sup> *Ibid.*, p. 77.

<sup>390</sup> A. SINAY-CINTERMANN, « Présentation générale des facteurs de perturbation affectant la règle de conflit (lois de police, questions préalables, renvois) », in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, p. 84.

théorie conçue dès lors comme une dérogation aux règles précitées du règlement Rome I (§ 1). Il s'agit d'une réflexion en marge du RGPD. Toutefois, malgré son silence apparent, le règlement lui-même pourrait être source d'indices sur les critères importants qui peuvent être déterminants pour la résolution des conflits de lois dans des situations transfrontalières (§ 2).

### **§1. Les lois nationales en tant que lois de police ?**

Une analyse de la méthode conflictuelle ne pourrait être exhaustive sans prendre en considération un facteur de perturbation du raisonnement inhérent aux conflits de lois, à savoir les lois de police<sup>391</sup>. Le caractère impératif d'une norme peut, de fait, jouer un rôle crucial dans la détermination du droit applicable<sup>392</sup>. Il s'agit d'un procédé alternatif de règlement des conflits de lois par rapport aux règles bilatérales classiques<sup>393</sup>.

Ayant à l'esprit les grands principes ainsi que le double objectif du RGPD, consistant en la protection du droit fondamental des individus à la protection des données personnelles ainsi qu'en la création d'un véritable marché intérieur, afin de faciliter le transfert de ces données, il y a peu de doute quant au caractère impératif du régime qu'il entend mettre en œuvre<sup>394</sup>. La question est toutefois débattue en doctrine de savoir si tant bien le règlement que les lois d'exécutions doivent être considérées comme des lois de polices<sup>395</sup>. En toute hypothèse, le règlement étant directement applicable, il sera naturellement amené à prévaloir sur des clauses de choix de lois incluses dans les contrats liant les parties. La pertinence de la qualification de lois de police sera alors surtout déterminante pour les lois nationales, lorsqu'elles exécutent différemment le règlement ou lorsqu'elles traitent de questions non visées par celui-ci.<sup>396</sup>

#### 1. Définition et critères au départ de l'article 9 du règlement Rome I

En vertu du règlement Rome I, « *une loi de police est une disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat d'après le présent règlement* »<sup>397</sup>. Le deuxième paragraphe de l'article 9 du règlement Rome I concerne la loi de police du for, tandis que le troisième est relatif aux lois de police étrangères. Le cas qui sera probablement le plus fréquent en matière de protection des données sera lorsque le juge du for s'interrogera sur la loi de police de son propre ordre juridique. Toutefois, il faut garder à l'esprit que l'application de l'article 9 Rome I peut être constitutive d'une entrave injustifiée, qui irait donc à l'encontre de la libre circulation garantie par l'Union européenne<sup>398</sup>. En

<sup>391</sup> L. D'AVOUT, « Les lois de polices », in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, p. 91.

<sup>392</sup> N. MICHAIL, « Le domaine d'application du GDPR : (...) », *op. cit.*, p.78.

<sup>393</sup> G. LARDEUX, *Droit international privé des obligations contractuelles*, Bruxelles, Larcier, 2016, p. 164.

<sup>394</sup> C. KOHLER., « Conflict of law issues in the 2016 Data Protection Regulation of the European Union », *Rivista di diritto internazionale privato e processuale*, 2016, p. 661.

<sup>395</sup> M. BRKAN, « Data protection and Conflict-of-Laws: (...) », *op.cit.*, p. 333.

<sup>396</sup> *Ibid.*, p. 337.

<sup>397</sup> Art. 9, §1, du règlement Rome I.

<sup>398</sup> G. LARDEUX, *op. cit.*, p. 178

réalité, la définition précitée est à comprendre dans le contexte de l'arrêt *Arblade* de la Cour de justice, selon lequel les réglementations nationales susceptibles d'entraver les échanges doivent être justifiées par des raisons impérieuses liées à l'intérêt général et doivent répondre au test de proportionnalité<sup>399</sup>.

Par ailleurs, la notion de loi de police doit être interprétée de manière restrictive<sup>400</sup>. Certains auteurs se sont interrogés sur le point de savoir si la référence aux intérêts publics de l'Etat exclurait la protection de parties privées<sup>401</sup>. Malgré les désaccords sur le sujet, il existe une partie de la doctrine défavorable à cette présentation, soutenant que même si « *le bénéficiaire de la protection instaurée par la norme est une personne privée, l'auteur de la norme peut avoir un intérêt public à la voir respectée* »<sup>402</sup>. Ce point de vue est particulièrement pertinent, selon nous, pour la matière de la protection des données telle que garantie par le RGPD. Par ailleurs, la sauvegarde de l'intérêt public de ce droit peut simplement résulter des objectifs précités du règlement. Outre la réalisation du marché intérieur, qui démontre indéniablement cette nature, le fait que cet instrument juridique concrétise la protection d'un droit fondamental des personnes concernées en est une preuve supplémentaire<sup>403</sup>. Enfin, eu égard à la nature juridique de ce droit, pouvant notamment être exécuté par des organismes publics et avoir ainsi une nature administrative (voy. *supra*), il peut être considéré que sa protection poursuit un « intérêt public »<sup>404</sup>.

## 2. Remarques relatives aux lois d'exécution du RGPD

Malgré l'absence de tendance prétorienne claire allant dans ce sens, plusieurs auteurs en doctrine ont tendance à reconnaître le caractère impératif, voire dans certains cas, la qualification de lois de police, de la réglementation sur la protection des données personnelles<sup>405</sup>. Les brèves considérations ci-dessus viennent, selon nous, appuyer cette conception. Toutefois, bien qu'un tel constat puisse sembler plutôt logique pour le RGPD en lui-même, il n'est peut-être pas si évident pour les lois nationales d'exécution.

La question se pose de savoir quelle est la pertinence de qualifier de « lois de police » ces lois nationales d'exécution dans un contexte où le législateur de l'Union rapproche les droits nationaux en matière de protection des données. Il n'existe aucun doute sur le fait que les lois nationales tirent une certaine impérativité du droit de l'Union, car elles exécutent ce dernier ; mais sont-elles pour autant des lois de police ? En effet, l'adoption du règlement, directement applicable au sein des Etats membres, est constitutive d'une volonté de former un espace juridique progressivement unifié et de mener à un effacement, en tout cas pour les questions jugées essentielles, de la sphère juridique nationale au bénéfice

---

<sup>399</sup> Arrêt Procédures pénales contre Jean-Claude Arblade et Arblade & Fils SARL, C-369/96, et Bernard Leloup, Serge Leloup et Sofrage SARL, C-376/96, EU:C:1999:575, points 39 et 75. ; G. LARDEUX, *op. cit.*, p. 178 ; M. MCPARLAND, *The Rome I Regulation on the law applicable to contractual obligations*, Oxford, Oxford university press, 2015, p. 693.

<sup>400</sup> Considérant 37, du règlement Rome I.

<sup>401</sup> A. SINAY-CINTERMANN, *op. cit.*, p. 85.

<sup>402</sup> *Ibid.*

<sup>403</sup> M. BRKAN, « Data protection and Conflict-of-Laws: (...) », *op. cit.*, p. 334.

<sup>404</sup> *Ibid.*

<sup>405</sup> N. MICHAIL, « Le domaine d'application du GDPR : (...) », *op. cit.*, pp. 78-79 ; C. KOHLER, *op. cit.* p. 661 ; M. BRKAN, « Data protection and Conflict-of-Laws: (...) », *op. cit.*, pp. 333-335 et p. 337.

de l'espace communautaire intégré<sup>406</sup>. Conceptuellement, la reconnaissance des lois de police semble difficilement compatible avec le rapprochement des législations<sup>407</sup>. Bien que les législateurs nationaux aient utilisé la marge de manœuvre qui leur était accordée d'un point de vue substantiel, il faudrait sans doute considérer l'existence d'une équivalence fonctionnelle entre les législations, équivalence qui remettrait en cause l'utilité de l'application immédiate de la loi du for. De fait, comment soutenir que les lois nationales poursuivent un objectif additionnel et distinct du RGPD<sup>408</sup> qui fait que chacune pourrait être distinguée dans sa fonction ainsi que dans sa substance, et ainsi être qualifiée de loi de police ?

Pour qu'une telle qualification soit en accord avec le droit européen, l'arrêt *Unamar* peut être source d'inspiration, pour affirmer que la juridiction saisie devra constater, de façon circonstanciée que, dans le cadre de cette exécution du règlement, le législateur de l'État du for a jugé crucial, au sein de l'ordre juridique concerné, d'accorder à la personne une protection allant au-delà de celle prévue par le règlement<sup>409</sup>. Une telle analyse n'est donc pas à exclure, mais devra faire l'objet d'une appréciation par les juridictions. Il peut, en effet, être soutenu que l'âge choisi pour le consentement du mineur à ses données ou encore le type de sanctions pénales adoptées pour les infractions à la protection des données poursuit un but d'intérêt public<sup>410</sup>. La loi serait, selon un tel raisonnement, caractérisée de loi de police précisément, parce qu'elle porte sur des points hors de la sphère uniformisée par le RGPD. Ainsi, dans notre cas pratique de départ, le juge français saisi pourrait soutenir qu'il y a lieu d'appliquer la loi française d'exécution prévoyant un âge de consentement plus élevé, et non la loi belge (malgré que ce soit la loi de la nationalité du mineur), en raison du fait que cet âge est plus favorable à un mineur qui aurait consenti au traitement de ses données de manière imprudente, par exemple. En l'occurrence, il pourra également invoquer la proximité du mineur belge résidant en France avec son ordre juridique<sup>411</sup>. Il reviendra donc aux juges nationaux de montrer en quoi il s'agit de « *lois dont l'observation est nécessaire pour la sauvegarde de l'organisation politique, sociale ou économique du pays* »<sup>412</sup>.

A supposer que les lois nationales soient effectivement des lois de police, comme nous le pensons, encore faut-il que celles-ci s'appliquent au cas d'espèce par rapport à leur domaine d'application<sup>413</sup>. Ce champ d'application est déterminé soit par des critères personnels soit par des critères territoriaux, qui peuvent exclure certaines situations<sup>414</sup>. Les problèmes énoncés précédemment risquent donc de se poser au même titre, notamment si la situation concernée n'est pas visée par le champ d'application de la loi (voy. *supra*).

---

<sup>406</sup> L. PALLIER, « Les lois de police en droit de la consommation », *R.E.D.C.*, 2015, p. 40. Nous reprenons l'argument que l'auteur utilise dans un contexte du droit de la consommation pour l'appliquer, par analogie, au droit à la protection des données personnelles.

<sup>407</sup> *Ibid.*, p. 43.

<sup>408</sup> *Ibid.*, p. 52.

<sup>409</sup> United Antwerp Maritime Agencies (Unamar) NV/Navigation Maritime Bulgare, C-184/12, U:C:2013:663, point 52 et dispositif.

<sup>410</sup> Art. 8 et 84, du RGPD

<sup>411</sup> G. Lardeux, *op. cit.*, pp. 173-174.

<sup>412</sup> P. FRANCESKAKIS, « Conflit de lois », *Répertoire Dalloz Droit International*, n° 137, cité par R.-N. IONESCU, *L'abus de droit en droit de l'Union européenne*, Bruxelles, Bruylant, 2012, p. 303.

<sup>413</sup> O. CACHARD, *Droit international privé*, Bruxelles, Bruylant, 2018, p. 196.

<sup>414</sup> *Ibid.*

## §2. L'autorité chef de file et le mécanisme du « guichet unique » : un indice donné par le RGPD ?

Dans la recherche de solutions aux problèmes de conflits de lois entre Etats membres posés par le règlement 2016/679, il peut être également utile de remarquer dans quelle mesure le règlement lui-même envisage certaines situations qui impliquent un traitement transfrontalier. Tel est le cas lorsqu'il prévoit l'existence d'une autorité de contrôle « chef de file » aux termes de son article 56, déterminée en fonction de l' « établissement principal » ou unique du responsable de traitement ou du sous-traitant<sup>415</sup>. C'est dans ce contexte que les considérations évoquées précédemment sur la notion d'établissement trouvent toute leur pertinence (voy. *supra*). Concernant la désignation de l'autorité compétente lorsqu'un traitement a un impact dans plusieurs Etats membres, le règlement apporte donc une piste de solution en matière de droit applicable<sup>416</sup>. En effet, le RGPD dispose que les Etats ont l'obligation de créer, par une loi, une ou plusieurs autorités de contrôle, chargée(s) de surveiller l'application du règlement, de protéger les libertés et droits fondamentaux des personnes concernées par le traitement ainsi que de faciliter le transfert de ces données d'un Etat membre à l'autre de l'Union<sup>417</sup>. En Belgique, l'Autorité de protection des données a été créée par une loi du 3 décembre 2017<sup>418</sup>.

Outre le statut, les pouvoirs et les missions de ces autorités de contrôle, le règlement prévoit le principe selon lequel chaque autorité de contrôle est compétente pour exercer les tâches dont elle est investie sur le territoire de l'Etat membre dont elle relève<sup>419</sup>. Une telle attribution paraît évidente pour des situations purement locales. Toutefois, pour les traitements qualifiés de transfrontaliers<sup>420</sup>, typiquement dans le cadre des activités d'une entreprise multinationale active à travers plusieurs Etats membres, les compétences de plusieurs autorités de contrôle pourraient entrer en conflit et être considérées comme concurrentes<sup>421</sup>. En effet, plusieurs autorités de contrôle pourraient se prétendre compétentes<sup>422</sup>. C'est dans ce contexte que le RGPD introduit le concept de « guichet unique » (ou « *one stop shop* » *mechanism*, en anglais) pour déterminer quelle autorité de contrôle disposera de la compétence principale<sup>423</sup> et sera ainsi considérée comme autorité chef de file.

Dans les hypothèses impliquant un ou plusieurs éléments d'extranéité au sein de l'Union, Il y a lieu alors de déterminer quel est le principal établissement du responsable de traitement, afin d'identifier

---

<sup>415</sup> Art. 56, §1, du RGPD.

<sup>416</sup> R. ROBERT, « Les autorités de contrôle dans le nouveau règlement général sur la protection des données : statut, coopération et gouvernance européenne », in *Vers un droit européen de la protection des données*, Bruxelles, Larcier, 2017, p. 33.

<sup>417</sup> Art. 51, §1, du RGPD.

<sup>418</sup> Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, p. 989.

<sup>419</sup> Art. 55, §1, du RGPD.

<sup>420</sup> Le RGPD dispose aux termes de son article 4, 23° qu'il faut entendre par « traitement transfrontalier », « a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ».

<sup>421</sup> V. VERBRUGGEN, « Chapitre 18. Le rôle des autorités de contrôle de protection des données. Indépendance et polyvalence », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, p. 656.

<sup>422</sup> R. ROBERT, *op. cit.*, pp. 33-34.

<sup>423</sup> V. VERBRUGGEN, « Chapitre 18. Le rôle des autorités de contrôle de protection des données (...) », *op. cit.*, p. 656.

l'autorité chef de file<sup>424</sup>. L'établissement principal est défini comme étant « *le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal* »<sup>425</sup>. Il doit être entendu restrictivement, selon la jurisprudence antérieure de la Cour de justice (voy. *supra*).

Le mécanisme du guichet unique implique une coopération entre autorités de contrôle impliquées, avec à la tête, une autorité chef de file. La décision finale concernant un traitement transfrontalier devra être adoptée par cette autorité chef de file, après consultation des autres autorités concernées<sup>426</sup>. Elle dispose ainsi d'une quasi-exclusivité pour adopter des mesures de toute nature sur le traitement, mais a également un rôle de coordination qui l'oblige à soumettre toute décision pour avis aux autres autorités concernées et de leur partager, plus généralement, toutes les informations utiles<sup>427</sup>. Par ailleurs, l'autorité chef de file elle-même peut demander aux autres autorités de mener des enquêtes ou toute autre action qui incombe à leur compétence territoriale<sup>428</sup>. Les autres autorités gardent donc leurs pouvoirs d'investigation, mais n'ont pas de pouvoirs « correctifs » propres<sup>429</sup>.

Partant de ces considérations, nous constatons que le pays où se trouve l'établissement principal du responsable de traitement se voit accorder une importance particulière dans ces situations transfrontalières. Rappelons, à cet égard, que l'article 4 §1<sup>er</sup> de la directive 95/46/CE utilisait précisément ce critère pour les questions de conflits de lois entre Etats membres. Se pose alors la question de savoir comment interpréter cette disposition du règlement par rapport au droit applicable. En effet, le RGPD évoque la compétence d'une autorité par rapport à d'autres qui seraient concurrentes, mais n'affirme pas pour autant que l'ordre juridique instituant cette autorité devrait, pour ces situations, prévaloir sur les autres autorités concernées. Une telle déduction découlerait-elle de l'existence même d'une autorité chef de file ? De fait, il serait très naturel pour cette autorité d'appliquer le droit de son Etat membre, lorsqu'il serait nécessaire de recourir à du droit national en vertu du règlement<sup>430</sup>. Comme le soutient l'auteur J. Chen, il ne s'agit pas de dire que l'autorité chef de file devrait appliquer son propre droit national, mais seulement qu'elle aurait tendance à le faire, sachant que, comme toute autorité, elle est, en principe, chargée d'appliquer le droit de l'Etat qui l'institue et que, en outre, le RGPD la désigne directement compétente dans ces situations données<sup>431</sup>. Par conséquent, comment interpréter ce mécanisme qui départage, en quelques sortes, la compétence des Etats (via leur autorité de contrôle) ? S'agirait-il d'un indice en faveur du critère de l'établissement principal pour la résolution des conflits de lois ? La question reste ouverte.

---

<sup>424</sup> J. CHEN, *op. cit.*, p. 322.

<sup>425</sup> Article 4, 16), du RGPD.

<sup>426</sup> J. CHEN, *op. cit.*, p. 332.

<sup>427</sup> R. ROBERT, *op. cit.*, pp. 42-43.

<sup>428</sup> J.R. ROBERT, *op. cit.*, p. 42

<sup>429</sup> J. CHEN, *op. cit.*, p. 332.

<sup>430</sup> *Ibid.*

<sup>431</sup> *Ibid.*

## **Conclusion**

Des discussions à propos des conflits de lois n'étaient pas censées avoir lieu suite à l'adoption du RGPD. Ce dernier régleme la matière des données à caractère personnel de manière remarquable quant à sa substance. Pourtant, nous avons tenté de démontrer, par la présente étude, que le constat en termes d'uniformisation est mitigé. Les conflits de lois sont non seulement possibles, mais peuvent prendre une ampleur considérable dans certains cas.

Les hypothèses de conflits de lois entre Etats membres dans la matière des données à caractère personnel ont pour cause principale la conception unilatérale du champ d'application des lois nationales d'exécution, variable suivant leur teneur respective. Autant la loi belge que la loi française que nous avons abordées, déterminent leur propre champ d'application dans l'espace. Elles ont reçu une totale liberté à cet égard. Or, ce phénomène peut paraître contradictoire dans un domaine où le législateur européen se prétend uniformisateur du droit dans un but très précis. En effet, le RGPD ne semble pas avoir pris les mesures nécessaires pour encadrer les marges de manœuvre qu'il prévoit. Il fait référence au droit des Etats membres, en assortissant cette intervention de certaines conditions ou limites substantielles selon les cas, comme l'obligation d'adopter une loi ou encore l'âge du consentement du mineur qui ne peut être inférieur à 13 ans. Toutefois, aucune indication n'est donnée sur l'interaction entre ces lois nationales. Ainsi, non seulement le législateur européen n'a pas jugé utile de maintenir une règle de conflits de lois dans sa réglementation, mais en plus, il n'a pas balisé les contours précis de l'applicabilité des lois qui sont appelées à l'exécuter. Nous avons constaté que la compétence d'une loi d'exécution peut empiéter sur celle d'une autre. Dans certains cas, au contraire, aucun ordre juridique ne peut s'avérer compétent.

Plus particulièrement pour ce qui est de la question de l'âge du consentement d'un enfant au traitement de ses données, la marge de manœuvre laissée aux parlements nationaux engendre de l'incertitude pour les personnes concernées ainsi que les responsables de traitement et/ou les sous-traitants. Nous avons remarqué que le RGPD permet aux Etats membres de faire dépendre la loi applicable à un aspect concernant la capacité du mineur d'un critère autre que sa nationalité, à savoir un critère de rattachement tel que le lieu de l'établissement du responsable du traitement ou encore le lieu de la résidence de la personne concernée. Or, comme nous avons tenté de le montrer, aussi bien en Belgique qu'en France, l'état et la capacité d'une personne sont, en principe, régis par le droit de l'Etat dont celle-ci a la nationalité. Le raisonnement en droit international privé semble perturbé, si l'Etat de la nationalité ne coïncide pas avec l'Etat où se trouve l'établissement du responsable de traitement, par exemple. Ainsi, le mineur belge qui devrait se voir appliquer la loi de sa nationalité pour ce genre de question ne sera effectivement concerné par le champ d'application spatial de la loi belge d'exécution du RGPD que si l'établissement du responsable de traitement concerné se trouve sur le territoire belge. Un tel principe d'application semble, pour le moins, problématique pour la protection du mineur.

Face à ce constat, deux mesures seraient, selon nous, à envisager dans l'optique de résoudre les conflits de lois suscités par l'article 8 du RGPD.

La *première proposition* peut être déduite des remarques effectuées quant à l'articulation des différents critères de rattachement ; il s'agirait d'inviter les législateurs nationaux à modifier leurs lois d'exécution, afin de prévoir un champ d'application propre à la question de l'âge du consentement de l'article 8. Autrement dit, chaque loi préciserait que son champ d'application dans l'espace s'applique pour tout le contenu de la loi, à l'exception de la disposition prévoyant le seuil minimal pour le consentement des enfants. Celle-ci sera régie par le droit de l'Etat de la nationalité du mineur, conformément aux règles classiques de droit international privé. Cette solution paraîtrait logique car elle favoriserait une continuité dans l'interprétation des règles préexistantes sur la capacité. En outre, même si cela ajouterait une tâche aux responsables de traitement qui devraient vérifier la nationalité de tous les mineurs concernés, ces derniers bénéficieraient ainsi de l'application d'un droit dont ils sont censés connaître le contenu. Toutefois, pour un même traitement, plusieurs lois devraient être donc consultées lorsqu'un mineur serait intéressé, étant donné que la capacité serait considérée comme une question « à part » du litige.

La *deuxième proposition* a déjà été mentionnée. Il s'agirait de considérer que le consentement du mineur visé dans le RGPD renvoie à un autre type de capacité. Elle ferait, dès lors, partie d'une autre catégorie de rattachement que celle du « statut personnel », de telle sorte que la capacité en la matière ne doit pas se voir appliquer systématiquement la loi de la nationalité ou, en tout état de cause, ne doit pas être distinguée des autres articles des lois d'exécution par rapport au champ d'application. A titre illustratif, le seuil d'âge pour le consentement d'un mineur en la matière, peu importe sa nationalité, serait vérifié en fonction de la loi belge du 30 juillet 2018, à condition que le responsable du traitement soit situé sur le territoire belge. Un tel raisonnement permettrait d'assurer une cohérence dans l'interprétation et l'application de la loi d'exécution, comme l'a sans doute voulu le législateur européen, et consacrerait un type de capacité uniquement pour la protection des données à caractère personnel. Dès lors, elle serait clairement distincte de la catégorie de rattachement « état et capacité ». L'avantage d'une telle option, selon nous, est que toutes les marges de manœuvre seraient visées par un seul texte législatif au sein de chaque Etat membre. Toutefois, les conflits de lois ne seraient pas pour autant tous résolus. Comme pour les autres dispositions ouvertes du règlement, il faudrait alors probablement se référer au règlement Rome I, si les parties sont liées par un contrat, pour déterminer quelle loi d'exécution s'applique.

Quant au règlement Rome I, nous avons abordé aussi bien les règles conflictuelles classiques que les règles dérogatoires que sont les lois de police. Nous avons, tout d'abord, montré comment la disposition relative au droit de la consommation pouvait s'appliquer à notre cas pratique, impliquant un mineur. Après avoir exclu le phénomène de l'autolimitation, nous nous sommes ensuite focalisés sur la pertinence éventuelle d'autres articles du règlement Rome I, à savoir les articles 9 et 23 de ce dernier. Plus particulièrement à propos des lois de police, nous avons tenté d'identifier les doutes qui peuvent se poser quant à l'application de l'article 9 par rapport aux lois nationales, ainsi que les raisons qui nous font penser que ces lois pourraient bénéficier de ce traitement dérogatoire.

En réalité, l'article du règlement Rome I qui sera appliqué pour résoudre les conflits de lois ne semble pas être l'élément déterminant du cheminement de notre réflexion. En effet, la présente étude

révèle qu'indépendamment de l'application de l'article 9 de ce règlement, de l'article 6 sur le droit de la consommation ou encore de l'article 4, les situations d'impasse subsisteront en raison des critères de rattachement différents choisis pour l'applicabilité des lois nationales. C'est là toute la source du problème. Ainsi, la loi désignée par l'article 6 du règlement Rome I ou la loi de police du for – à supposer qu'il s'agirait effectivement d'une loi de police – désignerait un ordre juridique qui mènerait à l'application d'une loi d'exécution du RGPD, alors même que la situation de l'espèce ne rencontrerait pas le facteur de rattachement déterminant son champ d'application spatial. La loi ne devrait, par conséquent, normalement pas être appliquée. C'est dans ce contexte que nous nous demandons comment la protection voulue par le RGPD pourrait être effective et efficace si aucune loi d'exécution ne s'applique à une situation. Comment résoudre ces problèmes liés à la volonté d'application des lois ?

Ces seuls éléments nous amènent à penser que l'applicabilité des lois nationales d'exécution mériterait d'être repensée. Pourquoi ne pas utiliser le même critère de rattachement dans ces lois et pourquoi encore ne pas faire en sorte qu'elles soient rédigées en des termes similaires, afin d'assurer une cohérence de la protection de ce droit fondamental au sein de l'Union ? De telle manière, chaque situation intra-européenne tomberait nécessairement dans un des champs d'application des lois d'exécution.

Dans ce cas, quel critère choisir ? *Une première option* serait de suivre les éventuelles indications du règlement lui-même, telles que la détermination de l'autorité chef de file, et d'opter pour le critère du lieu de l'établissement principal du responsable de traitement. Ce facteur de rattachement coïnciderait, en outre, avec le prescrit de l'article 4 du règlement Rome I qui prévoit le droit applicable à défaut de choix de loi. *Un autre critère* qui pourrait être choisi serait celui de la résidence habituelle de la personne concernée par le traitement. Ce rattachement présenterait l'avantage d'être notamment utile et cohérent pour toutes les fois où cette personne est considérée comme consommateur, eu égard à la règle bilatérale prévue dans l'article 6 du règlement Rome I, qui utilise ce même critère. Le récent arrêt *Schrems II* précité est notamment pertinent en la matière pour les réseaux sociaux et, plus généralement, pour le monde numérique. Soumettre l'application des lois d'exécution au critère de la résidence de la personne concernée assurerait de la prévisibilité pour cette personne dont le droit fondamental est en cause et, plus globalement, serait gage de sécurité juridique pour toutes les parties impliquées. Par ailleurs, si une clause venait à être insérée dans le règlement Rome II par rapport aux données personnelles, le facteur de rattachement qui, à nos yeux, devrait emporter les faveurs, ainsi que nous l'avons expliqué, serait favorable à la personne concernée, renvoyant soit directement à la loi de sa résidence habituelle, soit à la loi du pays où le dommage survient ou est susceptible de survenir.

Au vu de ces observations, il n'est pas certain que le RGPD et les lois nationales, tels qu'ils existent actuellement, permettent d'assurer harmonieusement les objectifs qu'ils poursuivent. Nous invitons ainsi le législateur européen à prendre en considération les conflits de lois que suscite leur coexistence et à repenser cette dernière au départ d'un critère de rattachement unique pour l'applicabilité des lois nationales qui l'exécutent. Une modification législative serait, sans doute, la bienvenue pour faire œuvre de clarté à cet égard...

## Bibliographie

### I. LEGISLATION

#### **Législation internationale**

- Convention relative aux droits de l'enfant, signée à New York le 20 novembre 1989, approuvée par une loi du 25 novembre 1991, *M.B.*, 17 janvier 1992, p. 803.
- Convention concernant la compétence, la loi applicable, la reconnaissance, l'exécution et la coopération en matière de responsabilité parentale et de mesure de protection des enfants, signée à la Haye le 19 octobre 1996, approuvée par la loi du 25 mai 2014, *M.B.*, 22 août 2014, 63560.

#### **Législation européenne**

##### *Droit primaire*

- Traité sur l'Union européenne (version consolidée), *J.O.U.E.*, 26 octobre 2012, C 326.

##### *Règlements européens*

- Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II), *J.O.U.E.*, 31 juillet 2007, L 199, p. 40.
- Règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), *J.O.U.E.*, 4 avril 2008, L 177, p. 6.
- Règlement (UE) n°1215/2012 du Parlement européen et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *J.O.U.E.*, 20 décembre 2012, L 351, p. 1.
- Règlement (UE) n° 2016/679 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 (règlement général sur la protection des données), *J.O.U.E.*, 4 mai 2016, L 119, p. 1.

##### *Directives européennes*

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, 23 novembre 1995, L 281, p. 31.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.U.E.*, 17 juillet 2000, L 178, p. 1.
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, 4 mai 2016, L 119, p. 89.

#### *Décisions européennes*

- Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.*, 30 décembre 2008, L 350, p. 60.

#### *Conventions et Chartes*

- Convention de Bruxelles de 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, *J.O.C.E.*, L 299, 31 décembre 1972, p. 32.
- Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C 326.

#### *Travaux préparatoires européens*

- Proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non-contractuelles ("Rome II"), C.O.M. (2003) 427 final.
- Rapport I sur la proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles ("Rome II"), *P.E. Doc.*, A6-0211/2005 du 27 juin 2005.
- Recommandation pour la deuxième lecture relative à la position commune du Conseil en vue de l'adoption du règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles ("Rome II"), *P.E. Doc.*, A6-0481/2006 du 22 décembre 2006.
- Résolution du Parlement européen du 10 mai 2012 contenant des recommandations à la Commission sur la modification du règlement (CE) n° 864/2007 sur la loi applicable aux obligations non contractuelles ("Rome II"), *P.E. doc.*, P7\_TA(2012)0200 du 10 mai 2012.
- Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), C.O.M. (2012) 011, final, p. 1.

#### **Législation belge**

- Code civil, art. 909
- Code de droit international privé, art. 34 ; art. 99.
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

### *Travaux parlementaires belges*

- Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001.

### **Législation française**

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.R.F.*, 7 janvier 1978.
- Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, *J.O.R.F.*, 21 juin 2018.
- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *J.O.R.F.*, 13 décembre 2018.

### *Travaux parlementaires et autres documents français*

- Projet de loi relatif à la protection des données personnelles, n°490, Assemblée nationale, déposé le 13 décembre 2017.
- Délibération n° 2018-349 du 15 novembre 2018 portant avis sur un projet d'ordonnance prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions relatives à la protection des données personnelles (saisine n° AV 18022142).
- Rapport au Président de la République relatif à l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *J.O.R.F.*, 13 décembre 2018.

## **II. JURISPRUDENCE**

### **Jurisprudence européenne**

- Arrêt LTU Lufttransportunternehmen GmbH & Co. KG/Eurocontrol, C-29/76, EU:C:1976:137.
- Arrêt Bertrand/Paul Ott KG., C-150/77, EU:C:1978:137.
- Arrêt Athanasios Kalfelis/Banque Schröder, Münchmeyer, Hengst et Cie, et autres, C-189/87, EU:C:1988:459.

- Arrêt Jakob Handte & Co. GmbH/Traitements mécano-chimiques des surfaces SA, C-26/91, EU:C:1992:268.
- Arrêt Francesco Benincasa/Dentalkit Srl., C-269/95, EU:C:1997:337.
- Arrêt Procédures pénales contre Jean-Claude Arblade et Arblade & Fils SARL, C-369/96, et Bernard Leloup, Serge Leloup et Sofrage SARL, C-376/96, EU:C:1999:575.
- Arrêt Azienda Agricola Monte Arcosu Srl/Regione Autonoma della Sardegna, C-403/98, EU:C:2001:6.
- Arrêt Verein für Konsumenteninformation/Karl Heinz Henkel, C-167/00, EU:C:2002:555.
- Arrêt Johann Gruber/Bay Wa AG., C-464/01, EU:C:2005:32.
- Arrêt Eirini Lechouritou et Autres/Dimosio tis Omospondiakis Dimokratias tis Germanias, C-292/05, EU:C:2007:102.
- Arrêt The Bavarian Lager Co, Ltd/Commission des Communautés européennes, T-194/04, EU:T:2007:334.
- Arrêt Tietosuojavaltutettu/ Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, EU:C:2008:727.
- C Arrêt Peter Pammer/Reederei Karl Schlüter GmbH & Co. KG, C-585/08, Hotel Alpenhof GesmbH/Oliver Heller,C-144/09.
- United Antwerp Maritime Agencies (Unamar) NV/Navigation Maritime Bulgare, C-184/12, U:C:2013:663.
- Arrêt Marc Brogsitter/Fabrication de Montres Normandes EURL et Karsten Fräßdorf, C-548/12, EU:C:2014:148.
- Arrêt Digital Rights Ireland Ltd/ Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande, The Attorney General, C-293/12 et C-594/12, EU:C:2014:238.
- Arrêt Google Spain SL et Google Inc./Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, C-131/12, EU:C:2014:317.
- Arrêt Harald Kolassa/ Barclays Bank plc, C-375/13, EU:C:2015:37.
- Arrêt Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.
- l'Arrêt Patrick Breyer/Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.
- Conclusions de l'avocat général Szpunar du 26 octobre 2016, sous l'arrêt Agro Foreign Trade & Agency Ltd/Petersime NV, C-507/15, EU:C:2016:809, points 22 et 55-60.
- Arrêt Peter Nowak/Data Protection Commissioner, C-434/16, EU:C:2017:994.
- Arrêt Maximilian Schrems/Facebook Ireland Limited, C-498/16, EU:C:2018:37.
- Arrêt Flightright GmbH/Air Nostrum,Líneas Aéreas del Mediterráneo SA, C-274/16, Roland Becker/Hainan Airlines Co. Ltd, C-447/16, Mohamed Barkan et autres/ Air Nostrum, Líneas Aéreas del Mediterráneo SA (C-448/16), EU:C:2018:160.
- Arrêt Jehovan todistajat – uskonnollinen yhdyskunta, C-25/17, EU:C:2018:551

## Jurisprudence allemande

- Facebook Ireland Ltd/ Facebook Inc. c. Independent Data Protection Authority of Schleswig-Holstein, Allemagne, 13 février 2013.

## III. DOCTRINE

### Monographies

- ATTAL M., RAYNOUAR A., *Droit international privé – Tome 1 : Principes généraux*, Bruxelles, Larcier, 2013.
- AUDIT B., D'AVOUT L., *Droit international privé*, Paris, Economica, 2013.
- AUDIT B., D'AVOUT L., *Droit international privé*, Paris, Librairie générale de droit et de jurisprudence, 2018.
- BEELEN A., *Guide Pratique RGPD : fiches de guidance*, Bruxelles, Bruylant, 2018.
- BENSOUSSAN A., HENROTTE J.-F., GALLARDO M., FANTI S., *General Data Protection Regulation: texts, commentaries and practical guidelines* (sous la dir. de A. BENSOUSSAN), Mechelen, Kluwer, 2017.
- CACHARD O., *Droit du commerce international*, Paris, L.G.D.J., 2011.
- CACHARD O., *Droit international privé*, Bruxelles, Larcier, 2016.
- CACHARD O., *Droit international privé*, Bruxelles, Bruylant, 2018.
- CHILSTEIN D., *Droit pénal international et lois de police : Essai sur l'application dans l'espace du droit pénal accessoire*, Paris, Dalloz, 2003.
- CLAVEL S., *Droit international privé* (sous la dir. de D. CHAGNOLLAUD et S. GUINCHARD), Paris, Editions Dalloz, 2016.
- DICKINSON A., *The Rome II Regulation : the law applicable to non-contractual obligations*, Oxford, Oxford university press, 2008.
- DOCQUIR B., *Droit du numérique : contrats, innovation, données et sécurité*, Bruxelles, Larcier, 2018.
- IONESCU R.-N., *L'abus de droit en droit de l'Union européenne*, Bruxelles, Bruylant, 2012.
- KESSEDJIAN C., *Droit du commerce international*, Paris, PUF, 2013.
- LARDEUX G., *Droit international privé des obligations contractuelles*, Bruxelles, Larcier, 2016.
- Mc PARLAND M., *The Rome I Regulation on the law applicable to contractual obligations*, Oxford, Oxford university press, 2015.
- NIBOYET M.-L., DE GEOUFFRE DE LA PRADELLE G., *Droit international privé*, Paris, Lextenso Editions, 2013.
- PLENDER R., WILDERSPEIN M., *The European Private International Law of Obligations*, London, Sweet & Maxwell, 2009.

- REVILLARD M., *Droit International Privé et Communautaire : Pratique notariale*, Paris, Défrenois Lextenso éditions, 2010.
- SAVIN A., *EU Internet Law*, Cheltenham, Elgar, 2017.
- SCHÜTZE R., *European Constitutional Law*, Cambridge, Cambridge university press, 2016.
- VAN CALSTER G., *European Private International Law*, Oxford, Hart, 2016.
- VIGNAL T., *Droit international privé*, Paris, Sirey, 2011.

## Périodiques

- ALVAREZ AMAS E., DECHAMPS M., « Arrêt Pammer et Hotel Alpenhof : L'équilibre entre consommateurs et professionnels dans l'e-commerce », *R.E.D.C.*, 2011, pp. 447-453.
- BISPING C., « Mandatorily Protected : The Consumer in the European Conflicts of Laws », *E.R.P.L.*, 2014, pp. 513-544.
- BYGRAVE L.A., « European data protection. Determining applicable law pursuant to European data protection legislation », *Computer Law & Security Report*, 2000, pp. 252-257.
- BRKAN M., « Data Protection and European Private International Law: Observing a Bull in a China Stop », *I.D.P.L.*, 2015, pp. 257-278.
- BRKAN M., « Data Protection and Conflict-of-laws: A Challenging Relationship », *E.D.P.L.*, 2016, pp. 324-341.
- CHEN J., « How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation », *I.D.P.L.*, 2016, pp. 310-323.
- CLÉMENT-FONTAINE, M., « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Legicom*, 2017, pp. 61-68.
- COOPER D., KUNER C., « Data Protection Law and International Dispute Resolution », *Académie de Droit international 382 Recueil des Cours*, 2017, pp. 15-174.
- CUSTERS B., DECHESNE F., SEARS A. M., TANI T., VAN DER HOF S., « A comparison of data protection legislation and policies across the EU », *C.L.S.R.*, 2018, pp. 241-242.
- DE HERT P., CZERNIAWSKI M., « Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context », *I.D.P.L.*, 2016, pp. 230-243.
- DE MEYER J., « International jurisdiction and conflict of law rules for consumer claims: a survey of European legislation », *R.E.D.C.*, 2009, pp. 631-677.
- DE TERWANGNE C., ROSIER K., LOSDYCK B., C., « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, pp. 5-56.
- FRANCO S., « The Scope of Secondary Community Law in the light of the methods of Private International Law – or the other way around? », *Yearbook of Private International Law*, volume 8, 2006, pp. 333-374.
- FRANCO S., « Le règlement "Rome I" sur la loi applicable aux obligations contractuelles », *J.D.I.*, 2008, pp. 4-6.

- GAYREL C., ROBERT R., « Proposition de règlement sur la protection des données – Premiers commentaires », *J.D.E.*, 2012, pp. 173-181.
- GÖNMANN M., « The new territorial scope of EU data protection law: deconstructing a revolutionary achievement », *C.M.L. Rev.*, 2017, pp. 567-590.
- GOTHOT P., « Le renouveau de la tendance unilatéraliste en droit international privé », *Rev. crit. DIP*, 1971, pp. 1-36.
- JANSSENS K., NUYTEN M., « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk – Le Règlement général sur la protection des données : de la théorie à la pratique », *R.D.C.-T.B.H.*, 2018, pp. 401-435.
- JAULT-SESEKE F., « La portée extraterritoriale ou a-territoriale du RGPD », *R.A.E.-L.E.A.*, 2018, pp. 43-51.
- JAULT-SESEKE F., ZOLYNSKI C., « Le règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé », *D.*, 2016, pp. 1874-1880.
- JAULT-SESEKE F., ZOLYNSKI C., « Shrems II accès au juge en matière de protection des données : une solution en demi-teinte potentiellement remise en cause par le RGPD », *D.*, 2018, pp. 2000-2004.
- KINSCH P., « L'autolimitation implicite des normes de droit privé matériel », *Rev. crit. DIP*, 2003, pp. 403-435.
- KOKOTT J., SOBOTTA C., « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *I.D.P.L.*, 2013, pp. 222-228.
- KOHLER C., « Conflict of law issues in the 2016 Data Protection Regulation of the European Union », *Rivista di diritto internazionale privato e processuale*, 2016, pp. 653-675
- KRIVOKAPIĆ Đ., ADAMOVIĆ J., « Impact of General Data Protection Regulation on Children's Rights in Digital Environment », *Belgrade Law Review*, Year LXIV, 2016, pp. 205-220.
- KUNER C., « Data Protection Law and International Jurisdiction on the Internet : An International Legal Analysis (Part 1) », *I.J.L.I.T.*, 2010, pp. 176-193.
- KRAL R., « National normative implementation of EC regulations. An exceptional or rather common matter? », *E.L.R.*, 2008, pp. 243-256.
- LEONARD J., « Le droit de la concurrence entre-t-il dans l'ère du private enforcement ? La loi sur l'action en dommages et intérêts pour les infractions au droit de la concurrence », *Competitio*, 2018, pp. 4-33.
- MARQUETTE V., « Le Règlement "Rome I" sur la loi applicable aux contrats internationaux », *R.D.C.-T.B.H.*, 2009, pp. 517-537.
- MAYER P., « Les lois de polices étrangères », *J.D.I.*, 1981, pp. 277-345.
- MAYER P., « Le phénomène de la coordination des ordres juridiques étatiques en droit privé – Cours général de droit international privé (2003) », *R.C.A.D.I.*, 2007, t. 327, pp. 1-377.
- MICHAIL N., « Entre le RGPD et le Règlement Bruxelles *Ibis* : quel juge pour protéger nos données personnelles ? », *D.C.C.R.*, 2019, pp. 175-200.
- MICHAIL N., « Le domaine d'application du GDPR : de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *R.D.C.*, 2019, pp. 52-79.

- MOINY J.-P., DE GROOTE B., « “Cyberconsommation” et droit international privé », *R.D.T.I.*, 2009, pp. 5-37.
- NOLAN K, « GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law », *Berkeley Technology Law Journal*, 2018, <http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/> (consulté le 5 juillet 2019).
- NUYTS A., « Droit international privé européen », *J.D.E.*, 2018, pp. 402-410.
- PALLIER L., « Les lois de police en droit de la consommation », *R.E.D.C.*, 2015, pp. 39-69.
- PEYROU S., « Un nouveau cadre juridique général pour la protection des données au sein de l’Union européenne : une réforme législative ambitieuse », *R.A.E. – L.E.A.*, 2012, pp. 149-162.
- PEYROU S., « Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions », *R.A.E. – L.E.A.*, 2016, pp. 103-110.
- ROBERT R., PONSART C., « Le règlement européen de protection des données personnelles », *J.T.*, 2018, pp. 421-438.
- SCHLOSSER P., « Rapport sur la convention relative à l’adhésion du royaume de Danemark, de l’Irlande et du Royaume-Uni de Grande-Bretagne et de l’Irlande du Nord à la convention de Bruxelles » (Schlosser Report), *J.O.C.E.*, C 59, 5 mars 1979, pp. 71-151.
- VAN BOXTAEL J.-L., « Division du droit en catégories », *Rép. Not.*, Tome XVIII, Droit international privé, Livre 0, Code DIP – Premiers commentaires, Bruxelles, Larcier, 2018, p. 211.
- VAN RAEPENBUSCH S., « La réforme institutionnelle du traité de Lisbonne : l’émergence juridique de l’Union européenne », *C.D.E.*, 2007, pp. 573-621.
- WAUTELET P., « Le consommateur, le réseau social et l’action collective », *J.D.E.*, 2018, pp. 260-265.
- TZANOU M., « Is Data Protection the same as Privacy? An Analysis of Telecommunications’ Metadata Retention Measures », *J.I.L.*, 2013, pp. 21-34.

### **Ouvrages collectifs et contributions dans un ouvrage collectif**

- BEIL L., « Reconciling private international law with European consumer law: where to start consumer protection in the context of e-commerce? », in *Boundaries of European Private International Law. Les frontières du droit international privé européen. Las fronteras del derecho internacional privado europeo*, Bruxelles, Bruylant, 2015, pp. 537-554.
- BENABOU V.L., « Faut-il une harmonisation minimale du droit », in *Le droit international de l’internet* (sous la dir. De G. CHATILLON), Bruxelles, Bruylant, 2002, pp. 180-188.
- BERNADEAU L., « Harmonisation minimale et droit applicable », in *Garantías en la venta de bienes de consumo: Ponencias de la Conferencia Internacional. Garantías dans la vente des biens de consommation : Rapports de la conférence internationale Saint-Jacques-de-Compostelle Janvier 2004*, Santiago de Compostela, Servizio de Publicacións e Intercambio Científico da USC, 2004, pp. 149-193.

- D'AVOUT L., « Les lois de polices », in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, pp. 91-121.
- DE TERWANGNE C., « Titre 2. Définitions clés et champ d'application du RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie* (sous la dir. de C. DE TERWANGNE et K. ROSIER), Bruxelles, Larcier, 2018, pp. 59-84.
- DE TERWANGNE C., « Chapitre 9 – Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 325-368.
- DE TERWANGNE C., GAYREL C., « Titre 6. Le RGPD et les transferts internationaux de données à caractère personnel », in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie* (sous la dir. de C. DE TERWANGNE et K. ROSIER), Bruxelles, Larcier, 2018, pp. 285-335.
- DOCQUIR B., « Consentement et intérêt légitime dans le secteur privé », in *Data Protection & Privacy – Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2016, pp. 27-44.
- DOCQUIR B., « Introduction générale », in *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, pp. 7-20.
- FERRARI F., RAGNO F., « European Union », in *Consumer Protection in International Private Relationships. La protection des consommateurs dans les relations privées internationales*, Asunción, CEDEP, 2010, pp. 581-609.
- FERNANDEZ ARROYO D. P., « Consumer protection in international private relations », in *Consumer Protection in International Private Relationships. La protection des consommateurs dans les relations privées internationales*, Asunción, CEDEP, 2010, pp. 659-701.
- FRANCO S., « Unilatéralisme versus bilatéralisme : une opposition ontologique ou un débat dépassé ? Quelques considérations de droit européen sur un couple en crise perpétuelle », in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, pp. 49-81.
- FRANCO S., « Unilateralism », in *European Encyclopedia of Private International Law*, Cheltenham, Edward Elgar Publishing, 2017, pp. 1779-1791.
- HESS B., ORO MARTINES C., « Civil and commercial matters », in *Encyclopedia of Private International Law/ edited by Jurgen Basedow, Giesela Ruhl, Franco Ferrari e.a.*, Cheltenham, Edward Elgar Publishing, 2017, pp. 346-357.
- NUYTS A., « II. – Obligations contractuelles », in *Actualités en droit international privé*, Bruxelles, Bruylant, 2013, pp. 138-181.
- PEROZ H., « La gestions des biens de la personne », in *Droit International Privé Patrimonial de la famille*, Paris, LexisNexis, 2017, pp. 49-122.
- POULLET Y., « Chapitre 1 – Analyse critique du RGPD », in *La vie privée à l'ère du numérique*, Bruxelles, Larcier, 2019, pp. 97-168.
- RAGNO F., « The Law Applicable to Consumer Contracts under the Rome I Regulation », in *Rome I Regulation. The Law Applicable to Contractual Obligations in Europe*, Munich, Sellier, pp. 129-170.

- ROBERT R., « Les autorités de contrôle dans le nouveau règlement général sur la protection des données : statut, coopération et gouvernance européenne », in *Vers un droit européen de la protection des données*, Bruxelles, Larquier, 2017, pp. 21-58.
- SCOTT A., « The Scope of “Non-Contractual Obligations” », in *The Rome II Regulation on the Law Applicable to Non-Contractual Obligations : A New International Litigation Regime*, Leiden, Nijhoff, 2009, pp. 57-83.
- SINAY-CINTERMANN A., « Présentation générale des facteurs de perturbation affectant la règle de conflit (lois de police, questions préalables, renvois), in *Quel avenir pour la théorie générale des conflits de lois ?*, Bruxelles, Bruylant, 2015, pp. 83-89.
- THYSEN A., « Titre préliminaire. L’application du droit communautaire : un aspect essentiel de sa « mise en œuvre » », in *L’application et le contrôle de l’application du droit communautaire par les administrations belges*, Gent, Academia press, pp. 3-44.
- TORO J., « DIP, protection des consommateurs et contrats », in *Contrats et protection des consommateurs* (sous la dir. de C. VERDURE), Limal, Anthemis, 2016, pp. 97-108.
- VERBRUGGEN V., « Titre 1. RGPD : cœur du puzzle de l’encadrement de la protection des données à caractère personnel dans l’Union européenne, in *Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Bruxelles, Larquier, 2018, pp. 25-58.
- VERBRUGGEN V., « Chapitre 18. Le rôle des autorités de contrôle de protection des données. Indépendance et polyvalence », in *L’Europe des droits de l’homme à l’heure d’Internet*, Bruxelles, Bruylant, 2019, pp. 643-679.
- VOGEL L., « Chapitre 1 – Primauté du droit européen », in *Traité de droit économique – Tome 4: Droit européen des affaires*, Bruxelles, Bruylant, 2017, pp. 321-343.

#### **IV. DIVERS**

##### **Avis et documents du Groupe de Travail « Article 29 »**

- Document de travail du Groupe de Travail « Article 29 » sur l’application internationale du droit de l’UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l’UE (WP 56), adopté le 30 mai 2002.
- Avis 1/2010 du Groupe de Travail « Article 29 » sur les notions de « responsable du traitement » et de « sous-traitant » (WP 169), adopté le 16 février 2010.
- Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable (WP 179), adopté le 16 décembre 2010.
- Lignes directrices du Groupe de Travail « Article 29 » sur le consentement au sens du règlement 2016/679 (WP 259), adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

## Autres avis

- Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée — «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», adopté le 14 janvier 2011.
- Avis 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (CO-A-2018-026).
- Avis n°52/2018 du 22 juin 2018 de l'Autorité de protection des données relatif à l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049).

## Communications

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », adoptée le 4 novembre 2010, COM (2010) 609 final.
- Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions. Protection de la vie privée dans un monde en réseau Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle, adoptée le 25 janvier 2012, COM (2012) 9 final.

## Autres

- J. BING, « Data Protection, Jurisdiction and the Choice of Law », 21<sup>st</sup> International Conference on Privacy and Personal Data Protection, Office of the Privacy Commissioner for Personal Data, Hong Kong 1999.
- Etude de la Commission européenne, « Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality », *JLS/2007/C4/028*, Privacy Study, Final Report, février 2009.
- « Protection of privacy in private international and procedural law », *International Law Association, Sydney Conference* (2018), p.5,  
[https://www.mpi.lu/fileadmin/mpi/medien/research/ILA\\_Committee\\_Protection\\_Privacy\\_Private\\_International\\_and\\_Procedural\\_Law/ILA\\_Committee\\_Privacy\\_Interim\\_Report\\_Sydney\\_REVISÉD\\_FINAL.pdf](https://www.mpi.lu/fileadmin/mpi/medien/research/ILA_Committee_Protection_Privacy_Private_International_and_Procedural_Law/ILA_Committee_Privacy_Interim_Report_Sydney_REVISÉD_FINAL.pdf) (consulté le 8 février 2019).

- European Commission – Press release : «Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses», 25 janvier 2012, [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm](http://europa.eu/rapid/press-release_IP-12-46_en.htm) (consulté le 7 avril 2018).
- Contrôleur européen de la protection des données (CEPD), « Accès du public aux documents et protection des données », Documents de référence, Juillet 2005 [https://edps.europa.eu/sites/edp/files/publication/05-07\\_bp\\_accesstodocuments\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_fr.pdf) (consulté le 22 avril 2019).
- [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing\\_fr](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_fr) (consulté le 22 juin 2019).
- <https://edpb.europa.eu> (consulté le 28 juin 2019).
- [https://edpb.europa.eu/our-work-tools/article-29-working-party\\_fr](https://edpb.europa.eu/our-work-tools/article-29-working-party_fr) (consulté le 28 juin 2019).
- <https://www.merriam-webster.com/dictionary/shall> (consulté le 6 juillet 2019)
- FAZLIOGLU M., « What the GDPR Requires of and Leaves to the Member States », *International Association of Privacy Professionals (IAPP)*, 2018, [https://iapp.org/media/pdf/resource\\_center/GDPR-Derogations-Whitepaper-FINAL.pdf](https://iapp.org/media/pdf/resource_center/GDPR-Derogations-Whitepaper-FINAL.pdf) (consulté le 6 juillet 2019).
- *The Economist* du 6 mai 2017, « Regulating the internet giants. The world's most valuable resource is no longer oil, but data », <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (consulté le 22 août 2019).





