# Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union

*Nikitas Michail*[1]



**RÉSUMÉ**

*Le règlement général sur la protection des données (GDPR), entré en vigueur le 25 mai 2016 et applicable depuis le 25 mai 2018, constitue une véritable évolution en matière de protection des données à caractère personnel. Par rapport à son prédécesseur – la directive n° 95/46 –, le GDPR apparaît plus à même de protéger les personnes physiques contre les dangers que présente le traitement des données personnelles. Toutefois, malgré l'harmonisation matérielle qu'il concrétise, le GDPR ne parvient pas à éviter les difficultés liées à la détermination de son domaine d'application. En effet, cette opération continue d'impliquer la délicate tâche d'interpréter les notions de données personnelles, de traitement, de responsables ou de sous-traitants et de susciter le débat sur l'extraterritorialité. En outre, le GDPR ne signe pas la fin des législations nationales en matière de protection des données. Au contraire, il laisse à plusieurs reprises une marge de manœuvre aux législateurs nationaux pour adapter le règlement aux spécificités de chaque Etat membre sans, toutefois, anticiper le conflit de lois qui pourrait survenir.*

1. Assistant en droit international et européen, Université catholique de Louvain. L'auteur peut être contacté à l'adresse suivante nikitas.michail@uclouvain.be. Nous tenons à remercier le professeur Stéphanie FRANCQ pour son soutien et ses précieux conseils dans la rédaction de cette contribution. Toutes erreurs ou omissions sont les nôtres.

**SAMENVATTING**

*De algemene verordening gegevensbescherming (GDPR), die op 25 mei 2016 in werking is getreden, is van toepassing sinds 25 mei 2018. In vergelijking met richtlijn nr. 95/46 – die de verordening vooraf gaat – lijkt de GDPR beter in staat om natuurlijke personen te beschermen tegen de risico's die gepaard gaan met de verwerking van persoonsgegevens. Ondanks de materiële harmonisatie die de GDPR bereikt, kan deze verordening echter niet voorbij de moeilijkheden omtrent het bepalen van haar toepassingsgebied. Het bepalen van het toepassingsgebied van de GDPR blijft immers een gevoelige zaak, aangezien deze de interpretatie vereist van begrippen als persoonsgegevens, verwerking, verwerkingsverantwoordelijke en verwerker, alsmede het debat uitlokt over de extraterritorialiteit. Bovendien betekent de inwerkingtreding van de GDPR niet het einde van de nationale wetgeving inzake gegevensbescherming. Integendeel, de verordening laat voldoende speelruimte aan nationale wetgevers om het Europees wetgevend kader aan te passen aan de kenmerken eigen aan elke lidstaat. De EU-wetgever heeft hierbij het risico op mogelijke wetsconflicten echter niet in overweging genomen.*

**1.** Le 25 mai dernier, le règlement général sur la protection des données personnelles[2] (ci-après le GDPR ou le règlement) entrait en application[3]. Les lignes de force de ce règlement ont, avant même toute application, bénéficié d'une attention rarement observée pour un règlement européen, tant dans la presse généraliste[4] que dans la doctrine[5]. Les principes relatifs au traitement des données à caractère personnel (art. 5-11), les droits de la personne concernée (art. 12-23), les obligations du responsable du traitement et du sous-traitant (art. 24-43) et le statut et les missions des autorités de contrôle et du Comité européen de la protection des données (art. 51-76) ont ainsi déjà été exposés ailleurs et appelleront, sans aucun doute, encore de nouveaux commentaires au fur et à mesure de la mise en œuvre du GDPR.

**2.** En revanche, la question du domaine d'application du GDPR, objet de cette contribution, a suscité moins de développements. Nous abordons, en premier lieu, cette question par l'analyse des termes de l'article 3 du GDPR[6] (Section 1.). L'ambition de cette première section consiste à souligner la latitude des notions définissant le domaine d'application du règlement afin de mettre en exergue l'éventail des hypothèses auxquelles le GDPR peut s'appliquer. Après avoir démontré que ce règlement ne concerne pas exclusivement des situations européennes, nous nous concentrerons sur la dimension internationale externe du GDPR (Section 2.)[7] et, plus précisément, sur le débat concernant son extraterritorialité. Au vu de l'intérêt grandissant de l'Union européenne pour des opérateurs étrangers comme Facebook, dont le fondateur a été auditionné par le Parlement européen le 22 mai 2018, le débat autour de l'extraterritorialité du GDPR ne cesse de croître. En tant qu'entreprise américaine, il est vrai que Facebook pourrait, à l'instar de Google[8], contester l'application des règles européennes à leurs activités de traitement de données personnelles.

**3.** Le cas de Facebook, tout comme celui de Google, illustre à quel point la question de l'internationalité externe du GDPR s'impose avec acuité dans le monde contemporain. L'importance de cette dimension externe de l'internationalité du règlement ne doit pas pour autant occulter celle de son pendant interne. En effet, une fois le règlement jugé applicable, il est encore nécessaire de déterminer la loi nationale d'exécution devant concrètement s'appliquer. C'est la question de l'internationalité non plus externe, mais interne

2. Le règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données), *J.O.*, L. 119, 4 mai 2016. Contrairement à ce qui est parfois écrit, le GDPR est entré en vigueur le 25 mai 2016, le 25 mai 2018 étant la date d'entrée en application du règlement. Voy. l'art. 99 du GDPR.

3. Le règlement remplace la directive n° 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.C.E.*, L. 281, 23 novembre 1995 (ci-après directive n° 95/46).

4. Parmi beaucoup d'autres, P. LALOUX, « Le RGPD, un nouveau cadre européen », *in Le Soir*, 25 mai 2018, disponible sur www.lesoir.be (consulté le 2 août 2018). Sur base d'une simple recherche à partir de l'acronyme « GDPR », le site du *Soir* propose plus de 100 articles.

5. Parmi d'autres, R. ROBERT et C. PONSART, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, pp. 421-438; C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, pp. 5-56.

6. Pour ce faire, nous examinons les plus récentes décisions de la Cour de justice de l'Union européenne. Celles-ci portent formellement sur la directive n° 95/46. Néanmoins, au vu de la similitude entre les textes des deux instruments, ces décisions restent pertinentes s'agissant du règlement. Sur la pertinence de la jurisprudence concernant l'art. 4 de la directive n° 95/46 dans l'analyse de l'art. 3 du GDRP, voy. not. M. GÖMANN, « The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement », *Common Market Law Review*, 2017, vol. 54, n° 2, pp. 574 et 583.

7. Sur la distinction entre l'internationalité externe et l'internationalité interne, voy. J.-S. BERGÉ, « La double internationalité interne et externe du droit communautaire et le droit international privé », *in Droit international privé: travaux du Comité français de droit international privé*, 17e année, 2004-2006, 2008, pp. 29-62.

8. C.J.U.E., 13 mai 2014, *Google Spain* et *Google*, C-131/12, EU:C:2014:317. Voy. également l'affaire pendante C-507/17, *Google (Portée territoriale du déréférencement)* et les conclusions de l'avocat général SZPUNAR présentées le 10 janvier 2019.

du GDPR (Section 3.). Bien qu'il s'agisse d'un règlement, nous verrons que cette dimension interne revêt une importance considérable; le texte du GDPR faisant lui-même référence à plusieurs reprises au droit national des Etats membres et renonçant ainsi à uniformiser complètement la protection des données personnelles au niveau européen.

## SECTION 1. L'ARTICLE 3 DU GDPR OU COMMENT LE GDPR NE DÉCRIT QUE SON INTERNATIONALITÉ EXTERNE

**4.** Dans son article 3, point 1., le GDPR dispose qu'il « s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ». Il est complété par un point 2. selon lequel « le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

(a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
(b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Un point 3. prévoit encore que le GDPR « s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où le droit d'un Etat membre s'applique en vertu du droit international public ». Malgré une formulation particulièrement large, ce point ne sera pas examiné dans la présente contribution compte tenu de son faible intérêt pratique[9].

**5.** Après avoir constaté que le législateur européen a opté pour une délimitation unilatérale et explicite du domaine d'application du GDPR (Sous-section 1.), nous examinons les aspects matériels, personnels et spatiaux de ce domaine (Sous-section 2.).

### Sous-section 1. Une délimitation unilatérale et explicite, un choix délibéré du législateur européen

**6.** Nombreux sont les actes législatifs européens qui ne délimitent pas explicitement leur domaine d'application[10]. En revanche, le GDPR, à l'instar de la directive n° 95/46[11], détermine explicitement son propre domaine d'application dans son article 3. Cette disposition exprime un choix délibéré du législateur européen qui impose l'application du règlement à toute situation correspondant aux hypothèses visées à l'article 3. Ce faisant, le règlement écarte l'hypothèse d'une règle de conflits de lois bilatérale et opte plutôt pour une délimitation unilatérale. Ce choix n'est, toutefois, pas évident et, théoriquement, rien n'empêche d'imaginer que la détermination de la loi applicable puisse se faire, en matière de protection des données personnelles, par l'application de la méthode bilatérale.

### Sous-section 2. Le champ d'application matériel, personnel et spatial du GDPR

**7.** L'analyse du domaine d'application du GDPR, nécessite de passer en revue son champ d'application matériel[12] (§ 1.), personnel (§ 2.) et spatial (§ 3.). Ces trois aspects, bien que généralement distingués dans un souci de clarté, sont, pour reprendre un terme cher à la Cour de justice de l'Union européenne (ci-après C.J.U.E. ou Cour de justice) en matière de protection des données, *inextricablement* liés et doivent donc être envisagés ensemble[13].

#### *§ 1. Le champ d'application matériel du GDPR*

**8.** L'article 3 du GDPR prévoit que le règlement général sur la protection des données s'applique à un traitement de données à caractère personnel. Au-delà de cette tautologie, il

9. Ce point vise notamment les hypothèses où le droit d'un Etat membre s'applique, en vertu du droit international, à un bateau, un avion, une ambassade. Voy. le considérant 25 du GDPR et l'avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable (WP 179), adopté le 16 décembre 2010, p. 20.
10. Voy. S. FRANCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, Bruylant, 2005, not. pp. 106 et s.; H. DE VERDELHAN, « Chronique de jurisprudence: Introduction générale », *R.I.D.E.*, 2016, p. 36.
11. Art. 4 de la directive n° 95/46.
12. Concernant le champ d'application matériel, nous nous concentrons sur les notions présentes dans l'art. 3 du GDPR et nous n'examinons donc pas l'ensemble des notions de l'art. 2.
13. S. FRANCQ, *o.c.*, p. 8. Il se peut qu'un critère revête simultanément un caractère matériel, personnel et/ou spatial et il est certain que notre classification des critères entre ces trois catégories emporte sa part de subjectivité.

reste à déterminer ce que recouvre la notion de traitement (1.) et de données personnelles (2.). Cette tâche n'est, toutefois, pas aisée comme a pu l'expérimenter récemment la cour d'appel de Liège et, dans la foulée, la Cour de cassation[14].

### *1) Un « traitement »*

**9.** Selon le GDPR, un traitement correspond à « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel »[15]. L'article 4, litera b), du GDPR vise une très grande variété d'opérations comme en atteste la liste d'exemples qui l'accompagne[16]. La Cour de justice l'a d'ailleurs confirmé en considérant que la simple opération « consistant à faire figurer, sur une page Internet, des données à caractère personnel »[17] constitue un traitement de données.

S'agissant du champ d'application matériel du GDPR[18], la définition de l'article 4 doit néanmoins être complétée par la distinction, basée sur les moyens utilisés lors du traitement, entre les traitements partiellement ou complètement automatisés, les traitements manuels structurés et les traitements manuels non structurés[19]. En effet, alors que tout traitement utilisant un moyen automatisé[20] tombe dans le champ d'application matériel du GDPR, ce n'est pas forcément le cas des traitements manuels. Parmi ces derniers, ne sont concernés par le GDPR que les traitements manuels structurés, c'est-à-dire ceux aux termes desquels les données personnelles sont contenues dans un fichier ou sont appelées à y figurer[21]. En d'autres termes, il suffit pour que le GDPR s'applique qu'un moyen automatisé soit utilisé ou que les données figurent, ou soient destinées à figurer, dans un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés »[22]. Nonobstant la jurisprudence de la Cour de cassation[23], ces deux hypothèses sont belles et bien alternatives; si l'une d'elles est rencontrée, le traitement en cause entre dans le champ d'application du GDPR.

**10.** En pratique, mise à part l'hypothèse exceptionnelle du traitement manuel non structuré, la définition du traitement est à ce point large que, dès qu'il est question de données personnelles, il est très probablement également question de traitement au sens du GDPR[24].

### *2) De « données à caractère personnel »*

**11.** Une donnée personnelle est définie comme « toute information se rapportant à une personne physique identifiée ou identifiable »[25]. Déjà à l'époque de la directive n° 95/46, la volonté du législateur européen était d'adopter une définition « la plus globale possible de la notion de donnée à caractère personnel afin de couvrir toutes les informations qui peuvent être reliées à une personne »[26]. Le Groupe de Travail « Article 29 » (ci-après GT29), remplacé désormais par le Comité européen de la protection des données (ci-après CEPD)[27], ainsi que la Cour de justice[28] ont confirmé la nature extrêmement large de cette définition[29].

14. C. DE TERWANGNE, « La difficile application de la législation de protection des données à caractère personnel » (note sous Cass., 22 février 2017), *J.T.*, 2017, p. 752; O. VANRECK, « Quand la Cour de cassation s'emmêle: du champ d'application de la loi du 8 décembre 1992 au droit d'accès » (note sous Cass., 22 février 2017), *R.D.T.I.*, 2017, p. 169.
15. Art. 4, b), du GDPR.
16. L'art. 4, b), du GDPR cite 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
17. C.J.U.E., 13 mai 2014, C-131/12, *Google Spain* et *Google*, *o.c.*, pt. 26. La Cour rappelle ainsi sa jurisprudence issue de l'arrêt *Lindqvist* (voy. C.J.C.E., 6 novembre 2003, C-101/01, *Procédure pénale / Bodil Lindqvist*, EU:C:2003:596).
18. Art. 2, 1., du GDPR. Voy. égal. L. COUDRAY, *La protection des données personnelles dans l'Union européenne: naissance et consécration d'un droit fondamental*, Sarrebruck, Editions Universitaires Européennes, 2010, pp. 121-123.
19. Avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, Doc. 01248/07/FR. La loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, traduit bien cette distinction lorsqu'elle décrit son champ d'application et précise, en son art. 2, al. 1er, que « la présente loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers ».
20. Les procédés automatisés « englobent toutes les technologies de l'information et de la communication ». Voy. C. DE TERWANGNE, « La difficile application … », *o.c.*, p. 752.
21. Art. 2, 1., du GDPR.
22. Art. 4, 6), du GDPR; L. COUDRAY, *o.c.*, pp. 122-123.
23. C. DE TERWANGNE, « La difficile application … », *o.c.*, p. 752; O. VANRECK, *o.c.*, p. 173.
24. F. BORGESIUS, « Singling out people without knowing their names: Behavioural targeting, pseudonymous data, and the new Data Protection Regulation », *Computer Law & Security Review*, 2016, p. 259.
25. Art. 4, 1), du GDPR.
26. Voy. la Proposition amendée de directive du Conseil et du Parlement européen sur la protection des individus au regard du traitement de leurs données à caractère personnel, 15 octobre 1992, COM (92)422 final, p. 10.
27. Art. 68 et s. du GDPR.
28. C.J.U.E., 6 novembre 2003, C-101/01, *Lindqvist*, *o.c.*, pts. 24-27; C.J.U.E., 20 mai 2003, C-465/00, *Österreichischer Rundfunk*, EU:C:2003:294, pt. 64; C.J.U.E., 16 décembre 2008, C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy et Satamedia*, EU:C:2008:727, pts. 35-37; C.J.U.E., 16 décembre 2008, C-524/06, *Huber*, EU:C:2008:724, pt. 43; C.J.U.E., 7 mai 2009, C-553/07, *Rijkeboer*, EU:C:2009:293, pt. 62; C.J.U.E., 19 avril 2012, C-461/10, *Bonnier Audio*, EU:C:2009:293, pt. 93; C.J.U.E., 20 décembre 2017, *Peter Nowak*, *o.c.*, pt. 34.
29. Avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136.

**i) « Toute information »**

**12.** Le GDPR entend s'appliquer à toute information, quel que soit son format, son origine ou son support[30]. Du point de vue de son champ d'application matériel, il est sans importance que l'information soit exacte ou inexacte[31], objective ou subjective[32]. Par ailleurs, le règlement ne limite pas son champ d'application matériel aux seules informations touchant à la vie privée et familiale[33]. Au contraire, le GDPR vise, de manière très large, l'ensemble des informations se rapportant à la personne concernée, en ce compris les informations qui sont publiques. Nous ne nous attardons pas sur la différence conceptuelle entre le droit à la vie privée et le droit à la protection des données personnelles[34]. Cependant, cette différence n'est pas sans conséquence en droit international privé. En effet, les règles de conflit de juridictions et de conflits de lois sont susceptibles de différer selon que la violation invoquée est une violation de la vie privée ou de la protection des données personnelles. Or, il n'est pas rare qu'un cas de violation du droit à la vie privée constitue également une violation de la protection des données personnelles, et *vice versa*. Par conséquent, adopter pour ces matières des règles de conflits de juridictions et de conflits de lois distinctes, multiplie les juridictions compétentes ainsi que les lois potentiellement applicables.

**ii) « Se rapportant à »**

**13.** Si le GDPR est susceptible de s'appliquer à tout type d'information, il entend *uniquement* s'appliquer aux informations se rapportant à une personne identifiée ou identifiable. *A priori*, cette condition limite le champ d'application matériel du règlement. Toutefois, l'interprétation qui en est faite par la Cour de justice ne le restreint en réalité que très peu.

Dans un arrêt récent[35], la C.J.U.E. confirme le test mis en avant par le GT29[36] pour déterminer si des données se rapportent effectivement à une personne et, partant, si elles sont soumises au GDPR. Selon la Cour, il faut, ou plutôt il suffit, que l'information soit liée à une personne déterminée en raison de son contenu, de sa finalité *ou* de son effet. Le premier critère, à savoir le contenu, nous paraît le plus évident. Il semble logique qu'une information dont une personne est le sujet, soit considérée comme se rapportant à cette personne. Le deuxième critère, la finalité, est lui relatif au but poursuivi, ou susceptible d'être poursuivi, par le responsable au terme du traitement. Ce critère sera satisfait dès lors que « les données sont utilisées ou susceptibles d'être utilisées, compte tenu de l'ensemble des circonstances du cas d'espèce, afin d'évaluer, de traiter d'une certaine manière ou d'influer sur le statut ou le comportement d'une personne physique »[37]. C'est notamment le cas des données permettant d'évaluer les capacités professionnelles d'un candidat[38]. Enfin, le troisième critère, celui de l'effet ou du résultat[39], est lié non pas au but du traitement des données, mais à ses conséquences. Une information qui est susceptible d'avoir un effet sur les droits et les intérêts d'une personne identifiée ou identifiable est donc une donnée personnelle se rapportant à cette personne. En ajoutant au critère du contenu, celui de la finalité et de l'effet et en les considérant tous les trois comme alternatifs[40], la C.J.U.E., à l'instar du GT29 confère au GDPR un champ d'application matérielle extrêmement vaste, à tel point que citer une information qui serait, sans aucun doute, une donnée non personnelle devient un exercice particulièrement complexe. Aussi, compte tenu du caractère alternatif de ces critères, il est probable qu'une information soit, simultanément, une donnée personnelle vis-à-vis de plusieurs personnes.

**iii) « Une personne physique identifiée ou identifiable »**

**14.** Le dernier élément de la définition d'une donnée personnelle consiste à vérifier que l'information se rapporte bien à une personne identifiée ou identifiable. La personne concernée ne peut être identifiée ou identifiable que si des identifiants existent, à savoir « des informations spécifiques qui présentent une relation particulièrement privilégiée et étroite avec la personne physique concernée »[41]. La per-

30. *Ibid*., pp. 6-9. Voy. égal. L. COUDRAY, *o.c.*, pp. 118-121.
31. Dans cette dernière hypothèse, la personne concernée disposera d'un droit de rectification selon l'art. 16 du GDPR.
32. C.J.U.E., 20 décembre 2017, *Peter Nowak*, *o.c.*, pt. 34; avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, pp. 6-9; L. COUDRAY, *o.c.*, pp. 118-121.
33. *Ibid*.
34. Voy. à cet égard parmi d'autres, J. KOKOTT et C. SOBOTTA, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *International Data Privacy Law*, 2013, vol. 3, pp. 222-228; C. DOCKSEY, « Articles 7 and 8 of the EU charter: two distinct fundamental rights », *in* A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Bruylant, 2015, pp. 71-99; R. TINIÈRE, « Article 8: Protection des données à caractère personnel », *in* F. PICOD et S. VAN DROOGHENBROECK (dirs.), *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article, B* ruxelles, Bruylant, 2018, pp. 185-204.
35. C.J.U.E., 20 décembre 2017, *Peter Nowak*, *o.c.*
36. Avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, pp. 10 et s.
37. *Ibid.*, p. 11.
38. C.J.U.E., 20 décembre 2017, *Peter Nowak*, *o.c.*, pt. 38.
39. S'agissant du troisième critère, le Groupe 29 ne parle pas d'effet mais de résultat; avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, p. 12. Nous préférons la terminologie de la Cour qui semble mieux décrire l'enjeu de ce troisième critère et, surtout, induit moins de confusion entre le deuxième critère et le troisième critère.
40. Avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, pp. 11-13.
41. *Ibid*., p. 13.

sonne en cause sera *identifiée* dans la mesure où les informations dont il est question constituent ou sont accompagnées par un identifiant qui révèle directement l'identité de cette personne[42]. En pratique un tel identifiant sera le plus souvent le nom de la personne[43].

**15.** Toutefois, la définition de données personnelles vise également des informations se rapportant à des personnes *identifiables* qui ne sont donc pas identifiées, mais peuvent l'être. Si une information constitue ou est accompagnée d'un identifiant qui ne révèle pas directement l'identité de la personne concernée, mais qui combiné à d'autres informations permet, *in fine*, d'identifier cette personne, il se *peut* que cette information soit également une donnée personnelle au sens du règlement. Dans l'affaire *Breyer*, la question se posait de savoir s'il fallait qualifier une adresse IP dynamique[44] de donnée personnelle lorsqu'elle était collectée par un fournisseur de service de média en ligne, étant entendu qu'une telle adresse IP n'est pas en soi suffisante pour permettre l'identification de l'utilisateur par le fournisseur de service de média[45]. La Cour de justice a précisé que pour « qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule, d'identifier la personne concernée »[46] et la Cour d'ajouter, qu'il n'est pas, non plus, nécessaire que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne[47].

**16.** A la suite de ces précisions, la Cour de justice, en se référant au considérant 26 de la directive n° 95/46, repris dans le GDPR, a retenu comme critère décisif, pour déterminer si une donnée se rapporte à une personne identifiable, l'existence de « moyens susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne »[48]. Le responsable du traitement doit donc vérifier s'il est susceptible que les informations en cause soient combinées avec des informations complémentaires afin d'identifier la personne concernée. La C.J.U.E. indique que ce ne sera pas le cas « si l'identification de la personne concernée était interdite par la loi ou irréalisable en pratique, par exemple en raison du fait qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre »[49]. Outre le temps et le coût nécessaires à l'identification de la personne, le considérant 26 du GDPR tient aussi compte des technologies disponibles au moment du traitement et de leur évolution[50]. Le GT29 ajoute qu'il faut, en plus de ces éléments, avoir égard à la finalité et à la structuration du traitement, à l'intérêt escompté du responsable du traitement, aux intérêts en jeu pour les personnes ainsi qu'aux risques de dysfonctionnement organisationnel et aux défaillances techniques[51]. Par ailleurs, les représentants des autorités nationales insistent particulièrement sur la prise en compte de la finalité du traitement jusqu'à l'utiliser pour présumer « l'identificabilité » de la personne concernée. « Lorsque la finalité du traitement implique l'identification de personne physique, il est permis de penser que le responsable du traitement ou toute autre personne concernée dispose ou disposera de moyens 'susceptibles d'être raisonnablement mis en œuvre' pour identifier la personne concernée. »[52]. Une pareille présomption semble faire sens. Dès lors que la finalité d'un responsable de traitement est de traiter des données de personnes qu'il lui est possible d'identifier, il est normal d'attendre de ce responsable qu'il mette en œuvre le GDPR sans avoir à vérifier qu'il traite effectivement des données personnelles.

### iv) L'examen de l'identificabilité[53]

**17.** Après l'affaire *Breyer*, il est certain que pour déterminer si une donnée se rapporte à une personne identifiable, il faut tenir compte du contexte de l'espèce. En revanche, l'approche générale qu'il convient d'adopter pour juger si une donnée revêt un caractère personnel est moins claire. Selon une première approche dite objective ou absolue[54], une donnée devrait nécessairement être considérée comme revêtant un caractère personnel dès lors qu'une personne, peu importe laquelle, est en mesure de déterminer l'identité

42. C.J.U.E., 19 octobre 2016, C-582/14, *Patrick Breyer*, EU:C:2016:779.
43. Avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, p. 14.
44. Ce sont des adresses IP attribuées de manière provisoire par les fournisseurs d'accès au réseau lors de chaque connexion à Internet de leurs clients; ces adresses sont modifiées à chaque connexion ultérieure.
45. Voy. les conclusions présentées le 12 mai 2016 par l'avocat général M. CAMPOS SÁNCHEZ-BORDONA dans l'affaire *Breyer*, pt. 4; M. MERIANI, « A relative notion of personal data and a flexible balance test on online platforms: are dynamic IP addresses too new for the old rules? Beyer v Bundesrepublik Deutschland », *Computer and Telecommunication Law Review*, 2017, p. 3. Est exclue l'hypothèse dans laquelle l'internaute a lui-même divulgué son identité lors de la connexion, auquel cas on est en présence de données personnelles relatives à ne personne identifiée.
46. C.J.U.E., 19 octobre 2016, *Patrick Breyer*, *o.c.*, pt. 41.
47. *Ibid.*, pt. 43.
48. *Ibid.*, pt. 42.
49. *Ibid.*, pt. 46.
50. Sur l'évaluation dynamique de la notion de donnée personnelle voy. avis 4/2007 du Groupe 29 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, pp. 16-17.
51. *Ibid.*, p. 16.
52. *Ibid.*, p. 16. Voy. égal. F. BORGESIUS, « Singling out people … », *o.c.*, p. 260.
53. Nous empruntons ce terme aux conclusions présentées le 12 mai 2016 par l'avocat général M. Campos Sánchez-bordona dans l'affaire *Breyer*, pt. 33.
54. Voy. les conclusions présentées le 12 mai 2016 par l'avocat général M. CAMPOS SÁNCHEZ-BORDONA dans l'affaire *Breyer*, pt. 52.

de la personne à laquelle cette donnée se rapporte en la combinant avec d'autres données. Selon une seconde approche, qualifiée de relative[55], il faudrait considérer le caractère personnel d'une donnée que de manière relative par rapport à un opérateur déterminé et aux informations dont il dispose. La Cour évoque ces deux approches, mais, au regret de certains[56], elle n'en consacre explicitement aucune et les observateurs sont divisés lorsqu'il s'agit de qualifier l'approche à privilégier[57]. A notre sens, la Cour penche plutôt vers une approche subjective. Lorsqu'elle détermine si une adresse IP est bien une donnée personnelle, la Cour prend soin de distinguer l'hypothèse dans laquelle l'adresse IP est collectée par le fournisseur d'accès Internet de celle dans laquelle l'adresse IP est enregistrée par le fournisseur de services de médias en ligne. S'agissant du fournisseur d'accès Internet, la Cour, a par le passé[58], considéré qu'une adresse IP constituait une donnée personnelle. Par conséquent, si la Cour avait résolument opté pour une approche objective elle aurait pu simplement répondre qu'une adresse IP collectée par le fournisseur de services de médias en ligne est une donnée personnelle, dès lors qu'un tiers – le fournisseur d'accès Internet – était en mesure de déterminer l'identité de la personne concernée en combinant l'adresse IP avec d'autres données. Toutefois, ce n'est pas ce qu'a fait la Cour. En effet, la Haute Juridiction a évalué si le fournisseur de services de médias en ligne disposait de moyens raisonnablement susceptibles d'être mis en œuvre pour lui permettre de combiner l'adresse IP en question avec d'autres informations complémentaires afin d'identifier la personne[59]. Cette démarche confirme qu'une adresse IP peut, en fonction du contexte, être ou non une donnée personnelle[60]. En l'espèce, selon la Cour, sous réserve de vérifications devant être effectuées par la juridiction nationale, le fournisseur de services de médias en ligne dispose de moyens susceptibles d'être raisonnablement mis en œuvre afin d'identifier la personne concernée[61] dès lors, qu'en contactant le fournisseur d'accès Internet, il lui est possible d'obtenir les informations nécessaires à l'identification de la personne utilisant l'adresse IP.

**18.** En outre, l'approche subjective nous paraît plus en phase avec la formulation particulièrement prudente du considérant 26, tant celui de la directive que celui du règlement, qui ne vise pas tous les moyens possibles pour identifier la personne concernée, mais uniquement les moyens *raisonnablement*[62] *susceptibles* d'être mis en œuvre. Selon nous, le texte de ce considérant implique qu'il ne suffit pas de démontrer que le responsable ou toute autre personne peut, *in abstracto*, déterminer l'identité de la personne concernée mais, encore faut-il que cette hypothèse soit susceptible de se réaliser *in concreto*.

**19.** Au terme de l'analyse de la définition de donnée personnelle, un constat s'impose. A l'instar de la notion de traitement, celle de donnée à caractère personnel est interprétée de manière extrêmement large. Par conséquent, nombreuses sont les hypothèses, localisées exclusivement en Europe ou non, entrant dans le champ d'application matériel du règlement.

## *§ 2. Champ d'application personnel du GDPR*

**20.** Pour déterminer si une hypothèse entre dans le domaine d'application de l'article 3 du GDPR, il faut identifier le ou les responsables du traitement (1)) et, le cas échéant, le ou les sous-traitants (2)) qui participent au traitement des données personnelles.

### *1) Le responsable du traitement*

**21.** Le règlement définit le responsable du traitement comme « 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 »[63].

Selon cette définition, le responsable du traitement peut être tant une personne physique qu'une personne morale, qu'elle soit de droit public ou de droit privé. En revanche, bien que cela ait pu être envisagé, la qualification de responsable ne pourrait s'appliquer à une entité qui ne disposerait pas de la

55. *Ibid*., pt. 53.
56. F. NIEMANN et L. SCHLUSSLER, « CJEU decision on dynamic IP adresses touches fundamental DP law question », *Bird & Bird*, 21 octobre 2016, disponible sur www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions (consulté le 7 août 2018).
57. Considérant que la Cour privilégie une approche objective, voy. F. BORGESIUS, « Singling out people … », *o.c.*, p. 135. *Contra* voy. P. DE HERT, « Data Protection's Future without Democratic Bright Line Rules. Coexisting with Technologies in Europe after Breyer », *E.D.P.L.*, 2017, pp. 27-28 et F. NIEMANN et L. SCHLUSSLER, « CJEU decision on dynamic IP addresses … », *o.c.*
58. C.J.U.E., 24 novembre 2011, C-70/10, *Scarlet extended*, EU:C:2011:771, pt. 51.
59. C.J.U.E., 19 octobre 2016, *Patrick Breyer*, *o.c.*, pt. 44.
60. P. DE HERT, *o.c.*, 2017, p. 27; M. MERIANI, *o.c.*, p. 4.
61. C.J.U.E., 19 octobre 2016, *Patrick Breyer*, *o.c.*, pts. 47-48.
62. Si cette précaution de langage (« susceptible ») apparaissait également dans la version anglaise du considérant 26 de la directive n° 95/46 (« likely »), elle était, en revanche, absente de la version néerlandaise ou n'apparaissait, à l'instar de la version allemande, que le terme raisonnablement (« redelijk »). Voy. T. HICKMAN, M. GOETZ, D. GABEL et C. EWING, « IP addresses and personal data: Did CJEU ask the right question? », *Privacy Laws & Business*, février 2017, p. 32. Désormais, tant dans la version anglaise, française que néerlandaise du GDPR, le législateur européen vise les moyens raisonnablement susceptibles d'être utilisés (en anglais, « likely reasonably to be used » et, en néerlandais, « alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt »).
63. Art. 4, 7), du GDPR.

personnalité juridique[64]. L'existence de pareille entité n'est, toutefois, pas sans importance au niveau du champ d'application spatial du règlement, car si elle ne peut être qualifiée de responsable en tant que telle, une entité sans personnalité juridique peut, en revanche, être qualifiée d'établissement du responsable et, dans certaines circonstances, déclencher l'application du règlement.

**22.** La personnalité juridique est donc un préalable nécessaire, mais, à l'évidence, pas suffisant, pour qu'un opérateur soit qualifié de responsable du traitement. Selon le GDPR, pour être qualifié de responsable, un opérateur doit déterminer les finalités et les moyens du traitement. Ceux-ci peuvent, respectivement, être résumés au « pourquoi » et au « comment » du traitement[65]. En d'autres termes, l'élément décisif pour la qualification de responsable est l'influence que l'opérateur exerce sur une série de décisions ayant trait aux moyens ou aux finalités du traitement (i)), et non pas le fait que l'opérateur qui traite les données, puisse y accéder ou en disposer. Nous verrons, en outre, que cette influence peut être exercée par plusieurs personnes à la fois (ii)).

### i) Déterminer les moyens et les finalités: une question d'influence

**23.** Pour qu'une partie puisse déterminer les finalités et les moyens du traitement, elle doit être en mesure d'exercer une influence sur ces aspects du traitement. Cette influence peut découler directement ou indirectement de la loi, mais, généralement, il s'agira d'une influence de fait et impliquera une appréciation factuelle. A cet égard, le GT29 note que « la désignation d'une entité en tant que responsable du traitement […] des données dans un contrat ne permet […] pas de déterminer avec certitude son véritable statut »[66]. Au demeurant, même si les clauses contractuelles ne lient ni l'autorité ni, le cas échéant, le juge, l'existence d'un contrat entre les différents acteurs impliqués dans le traitement constitue un élément central dans la détermination du responsable, quand bien même ce contrat ne désigne aucun responsable du traitement.

**24.** Dans un récent arrêt de la C.J.U.E. rendu en la matière, un passage soulève certaines questions quant à l'interprétation de la notion de responsable. La Cour indique que *peut* être qualifiée de responsable « 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 »[67]. Dans ce passage, la Cour précise que l'influence exercée par le responsable sur le traitement l'a été à des fins qui lui sont propres, sans préciser s'il s'agit d'une condition supplémentaire. Il serait, toutefois, peu probable qu'il s'agisse réellement d'une condition supplémentaire puisque le règlement n'exige pas que l'influence exercée par le responsable, le soit à des fins qui lui sont propres? En outre, cela réduirait le champ d'application de la notion de responsable, pourtant centrale dans le système mis en place par le GDPR.

Par ailleurs, la C.J.U.E. laisse entendre qu'une personne qui exerce une influence, à des fins qui lui sont propres, sur le traitement de données participe *de ce fait* à la détermination des finalités et des moyens de ce traitement alors que la définition du règlement exige non pas une influence sur le traitement, mais une influence sur la finalité et les moyens du traitement. La définition a déjà été interprétée largement par le GT29 considérant qu'une personne est responsable dès lors qu'elle influence soit les finalités soit les moyens essentiels du traitement, mais, ici, la Cour semble aller plus loin. Elle englobe dans l'exercice d'une influence sur la finalité et les moyens du traitement toute influence sur le traitement. Cette interprétation extensive serait-elle justifiée par le fait que l'influence est exercée à des fins propres au responsable du traitement? Aucune indication n'est donnée en ce sens.

**25.** Notons également que la Cour utilise le verbe pouvoir ce qui suppose que dans certains cas, bien qu'une personne influe à des fins qui lui sont propres sur un traitement de données et participe *de ce fait* à la détermination des finalités et des moyens, elle *pourrait* ne pas être considérée comme le responsable du traitement en question. Il faut probablement y voir une référence à l'avis du GT29 qui requiert un degré d'influence minimum pour qualifier une partie de responsable[68]. En d'autres termes, il y aurait un seuil d'influence en dessous duquel une entité, qui influencerait le pourquoi et le comment du traitement, ne devrait pas être considérée comme un responsable du traitement.

En réalité, ce degré minimal d'influence paraît atteint dès que l'entité en cause dispose d'un pouvoir de décision s'étendant au-delà des seules « questions techniques et d'organisation » que sont, par exemple, le choix du matériel informatique ou celui du logiciel à utiliser pour collecter, stocker ou transférer les données[69]. S'agissant des décisions

64. L. MOEREL, « Back to Basics: when does EU data protection law apply », *International Data Privacy Law*, 2011, vol. 1, No. 2, p. 99. Voy. égal. la thèse doctorale de B. VAN ALSENOY, *Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing*, KUleuven, Leuven, 2016, pp. 81-82, disponible sur www.limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1711667&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1 (consulté le 5 août 2018).
65. Avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, 16 février 2010, WP 169, p. 13.
66. *Ibid*., pp. 9-10.
67. C.J.U.E., 10 juillet 2018, C-25/17, *Jehovan todistajat*, EU:2018:551, pt. 68 (nous soulignons).
68. Avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, *o.c.*, p. 14.
69. Ces décisions ne relèvent pas des aspects essentiels. *Ibid*., p. 15. Voy. aussi Information Commissioner's Office's Guindance on Data Protection Act 1998 concerning « data controllers and data processors: what the differenc is and what the governance implications are », p. 7, publiée le 30 mars 2015, disponible sur ewww.ico.org.uk/for-organisations/guidance-index/data-protection-act-1998/ (consulté le 18 juillet 2018).

relatives aux aspects essentiels des moyens du traitement, elles sont « traditionnellement et intrinsèquement réservées à l'appréciation du responsable du traitement »[70]. Quant à la détermination des finalités, aucun degré minimum ne semble requis. En effet, le GT29 accorde une importance primordiale à la détermination de la finalité à tel point que selon lui, « la détermination de la finalité du traitement emporterait systématiquement la qualification de responsable du traitement »[71]. Le responsable du traitement se définirait donc plutôt comme la personne qui détermine les finalités *et/ou les aspects essentiels* des moyens du traitement que comme celle qui détermine les finalités *et* les moyens du traitement. Cet avis n'est, toutefois, pas partagé unanimement au sein de la doctrine[72].

Pour sa part, la C.J.U.E. maintient l'exigence du cumul de la détermination des finalités et des moyens, du moins formellement. Dans l'affaire *Fanpage*[73], la Cour considère que l'administrateur d'une page Facebook est, au même titre que Facebook et conjointement avec ce dernier, un responsable du traitement des données opéré par Facebook, car cet administrateur participe, selon la C.J.U.E., à la détermination des finalités et des moyens. A cet égard, la Cour remarque que l'administrateur peut définir, au travers des filtres mis à sa disposition par Facebook, les critères à partir desquels les statistiques des visites de sa page doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données à caractère personnel par Facebook. L'administrateur peut donc avoir une influence sur la détermination des moyens, mais cette possibilité n'est pas nécessairement réalisée et, la Cour n'exige d'ailleurs pas qu'elle le soit[74].

**26.** Concernant la participation de l'administrateur d'une page Facebook à la détermination des finalités du traitement opéré par Facebook, nous sommes, pour le moins, dubitatifs par rapport au raisonnement de la Cour. L'administrateur ne reçoit que des statistiques anonymes qui sont, en plus, exclusivement liées à son activité sur Facebook. Ainsi même si l'administrateur le souhaitait, il lui serait difficile d'utiliser ces données pour une autre finalité que celle de développer son activité de promotion sur Facebook, par exemple pour démarcher directement les personnes ayant visité sa page. C'est donc Facebook qui détermine la finalité et la manière dont l'administrateur tire profit de ce traitement, sans réellement permettre à l'administrateur de déterminer lui-même, en ajoutant ou en modifiant, les finalités du traitement en cause[75].

Pour justifier la qualification de l'administrateur d'une page Facebook comme responsable, la Cour a souligné, de manière originale, que l'administrateur, par la création de sa page, « offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan »[76]. La Cour semble considérer l'administrateur comme un responsable parce qu'il offre la possibilité à Facebook de traiter des données personnelles. Or, il ne ressort pas du règlement qu'un opérateur qui « offre » une possibilité à un autre opérateur de traiter des données serait de ce fait un responsable du traitement. Une telle interprétation étendrait très largement la notion de responsable[77]. En l'espèce, la Cour fait, toutefois, référence à la possibilité de placer des *cookies* grâce à la création de la page et, partant, il peut être considéré que l'administrateur influence les moyens du traitement des données opérées par

70. Avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, *o.c.*, p. 15. Sont considérés comme des décisions influençant les moyens essentiels du traitement les décisions déterminant notamment les données à traiter, le temps durant lequel les données seront traitées et stockées ou encore les personnes ayant accès aux données.

71. *Ibid*.

72. Pour une vision critique de la question, voy. B. VAN ALSENOY, *Regulating data protection …*, *o.c.* pp. 52-54 et 471-473. L'auteur admet qu'il existe une ambiguïté à la suite de l'avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, mais il considère qu'il s'agit d'une exigence cumulative et maintient que le responsable est celui qui détermine à la fois la finalité et les moyens.

73. C.J.U.E., 5 juin 2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig-Holstein GmbH* (ci-après l'affaire *Fanpage*), EU:C:2018:388.

74. C.J.U.E., 5 juin 2018, *Fanpage*, *o.c.*, pts. 36-37. La Cour constate qu'un « administrateur peut, à l'aide de filtres mis à sa disposition par Facebook, définir les critères à partir desquels ces statistiques [les statistiques sur les visites de la page de l'administrateur] doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données ». Cependant, la Cour n'indique à aucun moment qu'il doit être vérifié, par les juridictions nationales, que l'administrateur a bien utilisé cette possibilité. Remarquons, en outre, que selon cette large interprétation, toutes personnes s'inscrivant sur les sites permettant d'utiliser des critères ou des filtres de recherches, par exemple les sites de rencontres, pourraient, voire devraient, être considérées comme des responsables du traitement.

75. Ce constat est confirmé par l'« accord », au sens de l'art. 26 du GDPR, que Facebook propose désormais aux administrateurs de page. Cet accord stipule notamment que « Facebook Ireland accepte de prendre la responsabilité principale en vertu du RGPD pour le traitement des données statistiques » et « que *seul Facebook Ireland puisse prendre et mettre en œuvre des décisions concernant le traitement* des données statistiques ». En considérant cet accord comme reflétant la réalité, il est contestable de considérer l'administrateur de page comme étant un responsable du traitement puisqu'il ne peut ni prendre ni mettre en œuvre une décision concernant le traitement des informations. Voy. www.facebook.com/legal/terms/page_controller_addendum (consulté le 23 septembre 2018).

76. C.J.U.E., 5 juin 2018, *Fanpage*, *o.c.*, pt. 35.

77. Par exemple, une plateforme comme l'App Store d'Apple pourrait-elle être considérée comme un responsable, voire un responsable conjoint, du traitement des données effectué par les opérateurs proposant des applications mobiles sur la plateforme? En effet, la plateforme App Store offre également la possibilité à des opérateurs de placer des logiciels sur un appareil de la personne concernée. Au demeurant, il est certain que Apple est responsable du traitement des données qu'il collecte directement sur les utilisateurs au travers de leurs achats et de leur utilisation de l'App Store.

Facebook en créant sa page[78]. Rappelons, néanmoins, que selon le GT29, le choix du matériel ou du logiciel, tel que les *cookies*, à utiliser pour collecter les données relève des aspects accessoires du traitement et n'est donc pas exclusivement réservé au responsable du traitement.

**27.** De manière plus pragmatique, nous nous interrogeons sur l'opportunité de considérer les administrateurs de page Facebook comme des responsables du traitement pour les traitements opérés par Facebook. La réponse de la Cour ne paraissait pas évidente au vu des décisions, en première instance et en appel, des juridictions allemandes qui ont précédé la question préjudicielle à l'origine de cet arrêt[79]. En effet, le degré d'influence d'un administrateur de page Facebook dans le traitement de données est loin d'être évident. Toutefois, voir la Cour de justice interpréter largement une disposition de la directive n° 95/46 n'a rien de surprenant. C'est l'effet utile de la directive, et avec elle, la protection des libertés et des droits fondamentaux des personnes physiques qui est en jeu. Néanmoins, il n'est pas certain que considérer les administrateurs comme responsables du traitement opéré par Facebook favorise la protection des données personnelles[80]. En imposant ce statut et les obligations qui y sont liées aux administrateurs, la Cour risque d'aiguiser leur appétit à l'égard des données des personnes qui visitent leur page. Ces administrateurs devant assumer la responsabilité et les coûts des obligations prévues par le GDPR, ils voudront probablement pouvoir exploiter pleinement les données dont il est question; par exemple prendre connaissance de l'identité précise des personnes visitant leur page, et non plus seulement se contenter des données statistiques anonymes que leur fournit Facebook.

**28.** En outre, cette décision risque d'inciter les plus petits opérateurs à quitter les réseaux sociaux. En effet, à défaut d'assumer les obligations de responsable du traitement, les commerces de proximité qui trouvent en Facebook un médium leur permettant d'informer facilement leurs clients, notamment de leurs heures d'ouverture ou de leur adresse, sont contraints de clôturer leur page Facebook et, ce même s'ils n'influencent pas concrètement le traitement des données et n'utilisent pas les outils mis à leur disposition par Facebook. Comme le souligne l'autorité allemande[81] de protection des données, à la suite de l'arrêt *Fanpage*, si un opérateur, quel qui soit, est un administrateur d'une page Facebook et veut maintenir sa page, il doit, d'une part, conclure un accord avec Facebook conformément à l'article 26 du GDPR[82], et, d'autre part, il doit être en mesure de démontrer que le traitement des données dont il est conjointement responsable, à savoir celui opéré par Facebook, est licite et respecte le GDPR.

**29.** En d'autres termes, seuls les opérateurs pouvant se permettre d'assumer le statut de responsable du traitement conserveront une page Fan et, en contrepartie de cette responsabilité, ces opérateurs risquent d'exiger de Facebook plus d'information sur les utilisateurs qui fréquentent leur page. A la lumière de ces considérations, nous pensons qu'il aurait été préférable de considérer l'administrateur d'une page Facebook comme responsable du traitement seulement s'il désignait *in concreto* les catégories des personnes faisant l'objet d'un traitement de données personnelles, à charge pour le juge national de vérifier que cette condition soit satisfaite. En réalité, même avec cette modification, la solution de l'arrêt *Fanpage* resterait critiquable parce que si la détermination des catégories des personnes concernées est un aspect essentiel des moyens du traitement, il faut encore démontrer que l'administrateur participe aux finalités du traitement. Du reste, si l'administrateur de la page Facebook n'avait pas été qualifié de responsable, Facebook Ireland et Facebook Inc. restaient responsables tant pour mettre fin aux traitements illicites que pour indemniser les personnes concernées. Dans le cas d'espèce, il nous faut donc conclure que l'interprétation extensive ne profite pas de manière certaine à l'effet utile des règles protégeant les données personnelles.

78. Ce passage de l'arrêt permet d'anticiper la réponse de la Cour dans l'affaire pendante C-40/17, *Fashion ID*. Cette affaire concerne non pas les administrateurs de page Facebook mais les gestionnaires de site web qui insèrent dans leur site un module social (p. ex. un bouton « j'aime » de Facebook) entraînant une transmission de données à caractère personnel de l'ordinateur de la personne qui visite le site web à Facebook. Dans cette situation, le gestionnaire du site web offre, comme l'administrateur d'une page Facebook, la possibilité à Facebook de placer des cookies sur l'ordinateur de la personne qui visite le site web. Le lien entre les deux affaires a été mis en évidence par l'avocat général dans l'affaire *Fanpage*. Voy. les conclusions présentées le 24 octobre 2017 par l'avocat général Y. BOT dans l'affaire *Fanpage*, pts. 66-67.

79. Les juridictions allemandes tant en première instance qu'en appel ont rejeté la qualification de responsable concernant l'administrateur de la page Facebook à propos des données collectées par Facebook. Voy. C.J.U.E., 5 juin 2018, *Fanpage*, *o.c.*, pts. 19-21.

80. Nous entendons l'argument de l'avocat général considérant qu'en faisant porter, partiellement, la responsabilité du traitement des données opéré par Facebook sur l'administrateur de la page, cela incitera Facebook à se conformer au GDPR. Une telle solution suppose que les responsables disposent d'alternatives à Facebook. Or, actuellement, cela ne semble pas être le cas. Voy. les conclusions présentées le 24 octobre 2017 par l'avocat général Y. BOT dans l'affaire *Fanpage*, pt. 74 et N. BLANC, « Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsability of Facebook Fan Page Administrators for Infringement to European Data Protection Law? », *European Data Protection Law Review*, 2011, p. 124, 2018. Par ailleurs, il nous semble que, même sans faire porter cette responsabilité à l'administrateur de la page, les incitants pour faire respecter le GDPR par Facebook sont déjà importants.

81. Voy. la décision du 5 septembre 2018 par la Conférence des autorités indépendantes de protection des données du gouvernement fédéral et des Länder, disponible sur www.datenschutzzentrum.de/artikel/1253-Beschluss-der-DSK-zu-Facebook-Fanpages.html (consulté le 12 septembre 2018).

82. Facebook propose désormais un modèle type d'accord, au sens de l'art. 26 du GDPR, aux administrateurs de page Facebook, voy. www.facebook.com/legal/terms/page_controller_addendum (consulté le 23 septembre 2018).

**ii) Le cas des responsables conjoints**

**30.** Le règlement précise qu'une personne physique ou morale peut être responsable d'un traitement de données personnelles « seul ou conjointement ». Toutefois, toutes les situations dans lesquelles deux ou plusieurs responsables interagissent dans le cadre d'un traitement de données ne sont pas nécessairement des cas de responsabilité conjointe. Ainsi, dans la mesure où les différents responsables ne déterminent pas conjointement les finalités et les moyens, leur responsabilité sera distincte. C'est par exemple le cas dans l'hypothèse d'un simple transfert de données[83].

**31.** Le règlement est assez succinct sur cette hypothèse de coresponsabilité, et ce malgré les conséquences qu'elle implique. L'article 26 du GDPR définit les responsables conjoints comme « deux responsables du traitement ou plus qui déterminent conjointement les finalités et les moyens du traitement ». Dans pareille situation, les responsables conjoints doivent « par voie d'accord entre eux »[84] définir de manière transparente et claire leurs obligations respectives[85]. Le GDPR commande que cet accord reflète les rôles respectifs des responsables conjoints et qu'il soit mis à la disposition de la personne concernée, à tout le moins dans ses grandes lignes[86]. Par ailleurs, le règlement dispose également qu'indépendamment des termes de l'accord, la personne concernée doit pouvoir exercer les droits que lui confère le présent règlement contre chacun des responsables du traitement. Ce dernier paragraphe de l'article 26 crée une responsabilité solidaire entre responsables conjoints[87]. A cet égard, dans son arrêt *Fanpage*, la Cour souligne que « la reconnaissance d'une responsabilité conjointe […] contribue à assurer une protection plus complète des droits des personnes »[88]. Dès lors qu'il existe une obligation solidaire entre responsables conjoints, la personne concernée sera mieux protégée dans la mesure où elle pourra s'adresser à chacun des responsables pour le tout.

**32.** Cette affirmation de la Cour pourrait aussi se justifier du point de vue du droit international privé: une hypothèse de responsabilité conjointe produisant également des conséquences sur la loi applicable. L'article 3, point 1., du GDPR définit, en premier lieu, son domaine d'application par rapport à l'établissement « d'*un* responsable du traitement ». Selon cette disposition, l'ensemble des établissements de chacun des responsables conjoints doit être pris en compte. Par conséquent, pour autant que le traitement soit effectué dans le cadre d'un seul établissement d'un seul des responsables, l'ensemble du traitement et, donc, l'ensemble des coresponsables sont soumis au régime du règlement. En d'autres termes, la présence d'un établissement d'un des coresponsables conjoints sur le territoire de l'Union « contamine » l'ensemble du traitement. Le responsable doit ainsi se demander non seulement si lui-même entre dans le champ d'application du GDPR, mais également si les autres responsables conjoints du traitement entrent dans le champ d'application dudit règlement.

**33.** Cependant, face à cette interprétation très large de l'article 3 du GDPR, une autre interprétation plus restrictive peut être envisagée. Elle consisterait à distinguer les opérations de traitement réalisées par les différents responsables et à n'appliquer le GDPR que vis-à-vis de chaque responsable individuellement pour autant que ce responsable dispose, sur le territoire de l'Union, d'un établissement dans le cadre duquel le traitement a été effectué. L'avis du GT29 laisse entendre que cela n'est possible que « si, d'un point vu glo-

83. B. VAN ALSENOY, *Regulating data protection …*, *o.c.*, p. 57. Pour reprendre brièvement un exemple du Groupe 29, si « une agence de voyages envoie les données à caractère personnel de ses clients aux compagnies aériennes et à une chaîne d'hôtels, en vue de faire des réservations pour un voyage à forfait […], l'agence de voyages, la compagnie aérienne et l'hôtel seront trois responsables du traitement différents ». Dans ce dernier cas, il ne s'agit donc pas de responsable conjoint au sens du règlement et donc l'art. 26 ne devrait pas s'appliquer. Voy. avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, *o.c.*, p. 21.

84. Selon l'art. 26, 1., du GDPR, la seule exception dans laquelle un tel accord n'est pas obligatoire est l'hypothèse où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'Etat membre auquel les responsables du traitement sont soumis.

85. Voy. égal. le considérant 79 du GDPR.

86. Ce qui implique, en pratique, que l'accord existe sous une forme écrite même si le GDPR ne le prévoit pas explicitement.

87. Cette idée est renforcée par le point 4. de l'art. 82 et le considérant 146 du GDPR selon lequel, « lorsque des responsables du traitement ou des sous-traitants participent à un même traitement, chaque responsable du traitement ou chaque sous-traitant devrait être tenu responsable pour la totalité du dommage ». Le *solvens* pouvant par la suite réclamer à chacun de ses codébiteurs sa contribution à la dette du dommage comme l'indique l'art. 82, 5. et le considérant 146, *in fine*, du GDPR. Voy. égal. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *o.c.*, p. 37.

88. La Cour a, toutefois, rajouté que « l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différends opérateurs […]. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes circonstances pertinentes du cas d'espèce ». Cette dernière déclaration de la Cour peut être lue comme remettant en cause le principe de solidarité entre responsables conjoints. D'autant plus que le GT 29 écrit également que les situations des responsables conjoints peuvent « parfois se traduire par une responsabilité solidaire, mais pas systématiquement: bien souvent, les différents responsables du traitement peuvent être chargés, et donc responsables, du traitement de données à caractère personnel à différents stades et à différents degrés ». Dans son avis, le GT 29 semble considérer que les responsables pourraient opposer aux personnes concernées de respecter la répartition des responsabilités entre responsables et donc qu'il n'y aurait pas de solidarité entre responsables. Outre les critiques émises en doctrine (voy. B. VAN ALSENOY, « Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation », *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2016, pp. 281-282), cette solution ne semble pas, ou à tout le moins plus, tenable sous le régime du règlement. Selon nous, par ces termes, la Cour ne fait que confirmer l'existence d'une action récursoire au profit du *solvens*, telle que désormais prévue dans le règlement, mais elle ne remet pas en cause l'existence d'une solidarité entre les responsables.

bal, les opérations de traitement ne doivent pas être considérées comme 'un ensemble d'opérations' poursuivant une finalité commune *ou* utilisant des moyens déterminés conjointement »[89]. Dans un avis plus récent, s'agissant d'une situation non pas entre des responsables conjoints, mais entre un responsable du traitement et son sous-traitant[90], le CEPD considère que le traitement effectué par chaque entité doit être considéré séparément[91].

La première interprétation – la plus large – semble, dans le cas de responsables conjoints à tout le moins, plus fidèle au texte de l'article 3 du règlement. De surcroît, cette interprétation a l'avantage de contribuer à assurer une protection plus complète des droits des personnes, objectif auquel la Cour de justice est sensible en matière de protection des données à caractère personnel.

**34.** Par ailleurs, une situation de responsabilité conjointe crée un rapport juridique entre les responsables conjoints pour lequel la loi applicable n'est pas déterminée par le règlement[92]. Cette question est susceptible de se poser non pas au stade de l'obligation à la dette, mais à celui de la contribution à la dette, autrement dit uniquement entre les responsables conjoints. Par conséquent, il faudrait régler la situation sur base des règles de conflits de lois de droit commun et, plus précisément, selon nous, sur base des règles de conflits de lois régissant la matière contractuelle puisqu'aux termes de l'article 26 un « accord » devrait gouverner les activités conjointes des responsables vis-à-vis de la personne concernée. En effet, même si le GDPR n'impose pas formellement que les relations entre responsables conjoints soient réglées contractuellement, dès lors que l'action récursoire d'un responsable vise la réparation du dommage d'une personne concernée, survenu dans le cadre du traitement conjoint censé être encadré par un accord entre les deux responsables, nous pouvons en déduire que cette action aura bien une nature contractuelle[93]. Cependant, pour éviter toute incertitude, il est préférable que les responsables conjoints déterminent dans leur « accord » la loi applicable entre eux[94].

**35.** Ainsi s'abstenir de conclure l'accord visé à l'article 26, en plus de constituer une violation intrinsèque du règlement, représente une occasion manquée de clarifier la relation entre responsables conjoints.

### *2) Le sous-traitant et sa relation avec le responsable*

**36.** Le règlement définit le sous-traitant 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 »[95]. En intégrant le concept de sous-traitant dans la directive n° 95/46, la volonté de la Commission européenne était « d'éviter qu'un traitement par un tiers pour le compte du responsable […] ait pour conséquence d'affaiblir la protection de la personne concernée »[96]. La Commission voulait, de cette manière, anticiper et encadrer les conséquences d'une externalisation, par les responsables, de leurs activités de traitement des données.

La définition du sous-traitant, comme celle du responsable, est susceptible de s'appliquer à toute personne physique ou morale. Néanmoins, cette personne ne pourra être reconnue comme sous-traitant, au sens du règlement, que si elle est distincte du responsable du traitement[97]. En outre, l'élément décisif dans la qualification de sous-traitant est le traitement de données personnelles pour le compte du responsable.

**37.** Lorsqu'un sous-traitant prend part au traitement des données, le règlement prévoit que ce sous-traitant et le responsable doivent conclure, non pas un « accord » comme dans l'hypothèse de la responsabilité conjointe, mais un « contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un Etat membre »[98]. Ce contrat ou cet autre acte juridique « lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement »[99]. Le règlement impose encore que ce contrat ou cet acte juridique contienne d'autres clauses, notamment l'obligation de ne traiter les données à caractère personnel

89. Avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, *o.c.*, p. 22 (nous soulignons).
90. Voy. *infra*, n° 38.
91. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 9.
92. Le seul texte du GDPR est loin de régler tous les aspects du rapport entre responsables conjoints.
93. Par analogie, voy. C.J.U.E., 15 juin 2017, C-249/16, *Kareda*, EU:C:2017:472 au sujet du caractère contractuel d'une action récursoire entre codébiteurs solidaires d'un contrat de crédit.
94. A titre d'exemple, à la suite de l'arrêt *Fanpage*, Facebook a introduit une telle clause au profit du droit irlandais dans les conditions appelées « Addenda sur les Statistiques de Pages » qui constitue l'accord devant être conclu entre les responsables conjoints, c'est-à-dire entre les administrateurs de page Facebook et Facebook, au titre de l'art. 26 du GDPR. Ces conditions sont disponibles à l'adresse suivante www.facebook.com/legal/terms/page_controller_addendum (consultée le 23 septembre 2018).
95. Art. 4, 8), du GDPR.
96. Avis 1/2010 du Groupe 29 sur les notions de responsable du traitement et de sous-traitant, *o.c.*, p. 26.
97. *Ibid.*, p. 25; B. VAN ALSENOY, *Regulating data protection …*, *o.c.* p. 46.
98. Art. 28, 3., du GDPR.
99. *Ibid*.

« que sur instruction documentée du responsable du traitement »[100].

**38.** A l'instar de l'hypothèse de la responsabilité conjointe, il n'est pas à exclure que la présence d'un sous-traitant dans le cadre d'un traitement de données produit des effets au niveau du droit applicable. Ainsi, selon la même interprétation de l'article 3 du GDPR que celle exposée ci-avant, il pourrait suffire qu'un établissement d'un sous-traitant se trouve sur le territoire européen et que le traitement entre dans le cadre des activités de cet établissement pour que le règlement soit applicable à l'ensemble du traitement et, donc, à l'ensemble des autres entités qui prennent part à ce traitement. Toutefois, dans son dernier avis en date sur la question[101], le CEPD exclut cette hypothèse. Selon le successeur du GT29, un responsable de traitement ne disposant pas d'établissement en Europe n'est pas soumis au GDPR, en vertu du point 1. de son article 3, par le simple fait qu'il s'adresse à un sous-traitant européen. En effet, dans pareille situation, si le point 2. n'étant pas applicable au responsable, ce dernier ne sera pas soumis au GDPR. En revanche, le CEPD précise que le traitement sera effectué dans le cadre des activités du sous-traitant qui, lui, sera soumis au GDPR. Dans la configuration inverse, si le responsable effectue un traitement dans le cadre des activités d'un de ces établissements européens en ayant recours à un sous-traitant qui n'est pas établi sur le territoire de l'Union, au titre de l'article 3, point 1., du GDPR, seul le responsable sera soumis audit règlement. Néanmoins, pour éviter au responsable d'enfreindre le GDPR, le sous-traitant devra conclure avec le responsable un contrat, ou garantir par un autre acte juridique, qu'il effectue le traitement en cause conformément au GDPR. En d'autres termes, c'est par une extension contractuelle que le GDPR s'appliquera au sous-traitant[102].

**39.** Enfin, pas plus que pour les responsables conjoints, le règlement ne fournit d'indication quant aux aspects de droit international privé de la relation entre le responsable et le sous-traitant. Le responsable et le sous-traitant devront dès lors se rabattre sur les règles générales de droit international privé régissant la matière contractuelle en vertu du contrat qui les lie. A cet égard, rien ne les empêche d'ajouter aux clauses contractuelles imposées par le règlement, une clause de loi applicable afin de régler la question en amont.

**40.** Cette analyse du champ d'application personnel du GDPR renforce notre constat sur l'ampleur du domaine d'application de ce règlement. En effet, la définition de responsable reçoit une interprétation de la C.J.U.E. et du GT29 telle qu'une personne exerçant une influence même minime sur un traitement de données encourt le risque d'être qualifié de responsable et de devoir en assumer les obligations. De surcroît, comme l'illustre l'affaire *Fanpage*, cette personne pourrait se retrouver non seulement responsable, mais responsable conjointe d'un traitement et donc devoir être en mesure de garantir que l'ensemble des opérations des responsables conjoints respecte les prescriptions du GDPR. Une telle interprétation des notions de responsable et de traitement conjoint aurait d'autant plus d'impact sur le domaine d'application du GDPR, si ce dernier s'étend à toutes hypothèses dans laquelle un établissement du responsable ou, le cas échéant, un établissement des coresponsables ou des sous-traitants, est localisé sur le territoire de l'Union.

## *§ 3. Le champ d'application spatial*

**41.** Après avoir identifié le responsable du traitement ainsi que les éventuels responsables conjoints ou sous-traitants, il faut s'interroger sur la localisation de leurs établissements (1)). Cette première étape est essentielle puisque le GDPR détermine son application différemment dans le cas où le responsable ou son sous-traitant dispose d'un établissement sur le territoire de l'Union (2)) du cas où, ni le responsable, ni le sous-traitant ne sont établis sur le territoire de l'Union (3)).

### *1) Disposer d'un établissement et/ou[103] ne pas être établi sur le territoire de l'Union*

**42.** L'article 3 du GDPR s'articule entre deux paragraphes. Le premier s'appliquant si le responsable ou le sous-traitant dispose d'un établissement sur le territoire de l'Union (i)). Le deuxième visant les situations dans lesquelles le responsable du traitement ou le sous-traitant n'est pas établi dans l'Union (ii)).

#### i) Disposer d'un établissement sur le territoire de l'Union

**43.** Le règlement ne définit pas ce qu'il entend par « un établissement »[104] ni par « être établi ». Néanmoins, la notion d'établissement est précisée dans les considérants du règlement et a été interprétée par la Cour de justice. Dans

100. Art. 28, 3., a), du GDPR.
101. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 10.
102. *Ibid*., pp. 9-10.
103. Disposer d'un établissement sur le territoire de l'Union et ne pas être établi dans l'Union ne sont pas deux situations parfaitement opposées. Voy. L. MOEREL, « The long arm of EU data protection law: does the data protection directive apply to processing of personal data of EU citizens by websites worldwide? », *o.c.*, pp. 35-36 et B. HARDY, « Application dans l'espace de la directive 95/46/CE: la géographie du droit à l'oubli », *Rev. trim. dr. eur.*, 2014, p. 884.
104. Le GDPR définit la notion d' « établissement principal », voy. art. 4, 16), GDPR, mais pas celle d'établissement. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), 16 novembre 2018, p. 5, disponible sur www.edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3¬_en (consulté le 22 novembre 2018).

l'affaire *Weltimmo*, la C.J.U.E. rappelle qu'aux termes du considérant 19 de la directive n° 95/46, devenu le considérant 22 du GDPR[105], l'existence d'un établissement d'un responsable dans un Etat membre « suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable et que la forme juridique retenue […], qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante »[106]. Elle précise, en outre, que la notion d'établissement reçoit, en matière de protection des données, une interprétation « souple » qui « écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée »[107]. Afin de déterminer si un établissement existe, il faut donc évaluer le degré de stabilité de l'installation et la réalité de l'exercice des activités de cet établissement, sans nécessairement avoir égard au lieu d'enregistrement ni à la forme juridique.

**44.** Pour décrire la notion d'installation stable, le CEPD se réfère à la définition de l'établissement stable de la C.J.U.E. en matière de liberté d'établissement[108]. Ainsi, une installation stable nécessite « la réunion permanente de moyens humains et techniques nécessaires aux prestations de service en cause »[109], ce qui exclut de la qualification d'établissement la simple existence de serveur ou d'ordinateur sur un territoire. Cette définition, pour autant qu'elle soit interprétée largement, semble bien s'accorder avec les indications de la Cour qui précise « que la présence d'un seul représentant (moyen humain) peut, dans certaines circonstances, suffire pour constituer une installation stable si celui-ci agit avec un degré de stabilité suffisant à l'aide de moyens (techniques) nécessaires à la fourniture des services concrets concernés »[110]. Le critère d'installation stable est ainsi très largement défini et susceptible d'être aisément rencontré. Dans le même arrêt, la Cour a, d'ailleurs, estimé qu'un représentant, un compte bancaire destiné au recouvrement de créance, et une boîte aux lettres étaient susceptibles de constituer un établissement[111]. Dans un arrêt ultérieur, la Cour a confirmé cette interprétation en considérant qu'il n'est pas exclu qu'une entreprise, ne possédant ni filiale, ni succursale dans un Etat membre, y possède, néanmoins, un établissement[112]. En phase avec la jurisprudence de la Cour, le considérant 22 du règlement, qui remplace le considérant 19 de la directive n° 95/46, n'utilise plus le terme d'installation pour lui préférer celui de dispositif, ce qui confirme l'idée qu'un faible degré de stabilité suffit.

**45.** En ce qui concerne le critère de l'exercice effectif et réel d'une activité, la Cour adopte également une interprétation très large puisqu'elle estime que ce critère est satisfait dès lors qu'une « activité réelle et effective, *même minime* »[113] est exercée au travers d'un dispositif stable. En l'espèce, l'exploitation de plusieurs sites Internet d'annonces immobilières par la société Weltimmo est une activité effective et réelle. La Cour a localisé l'exercice effectif et réel de l'activité non pas en Slovaquie, état d'immatriculation de Weltimmo, mais en Hongrie, en justifiant notamment que les annonces immobilières concernaient des biens situés en Hongrie et qu'elles étaient rédigées en langue hongroise[114]. La direction des activités a donc une influence pour déterminer la localisation de l'exercice effectif et réel de ces activités[115]. Dans cet arrêt, la Cour a, d'ailleurs, précisé que pour évaluer le degré de stabilité de l'installation et la réalité de l'exercice des activités, il convient de tenir « compte de la nature spécifique des activités économiques et des prestations de services en question », ajoutant que « cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet »[116]. Notons, toutefois, que la simple accessibilité d'un site Internet du responsable d'un traitement, depuis un Etat membre, ne permet pas de fonder l'existence d'un établissement de ce responsable dans cet Etat membre[117].

---

105. Le considérant 22 du GDPR évoque non pas un établissement stable, mais un dispositif stable. A cette exception près, il utilise les mêmes termes que le considérant 19 de la directive n° 95/46. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 5.
106. C.J.U.E., 1er octobre 2015, C-230/14, *Weltimmo*, EU:C:2015:426, pt. 28.
107. *Ibid*., pt. 29.
108. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 4; Avis 8/2010 du Groupe de Travail « Article 29 » *o.c.*, p. 20; J. MOINY, « Facebook au regard des règles européennes concernant la protection des donnees », *R.E.C.O.*, 2010, pp. 259-260.
109. C.J.C.E., 4 juillet 1985, 168/84, *Gunter Berkholz / Finanzamt Hamburg-Mitte-Altstadt*, EU:C:1985:299, pt. 18 et C.J.C.E., 7 mai 1998, C-390/96, *Lease Plan Luxembourg SA / Belgische Staat*, EU:C:1998:206, pts. 25-27. Dans l'affaire *Google Spain*, il n'est pas contesté que *Google Spain* avait les moyens d'effectuer un traitement de données puisque, comme le rappelle la Cour au point 43 de son arrêt, cet établissement a été désigné par Google Inc comme responsable du traitement à l'égard de données personnelles de clients ayant conclu des contrats de service publicitaire avec Google Inc.
110. C.J.U.E., 1er octobre 2015, *Weltimmo*, *o.c.*, pt. 30.
111. *Ibid*., pt. 33.
112. C.J.U.E., 28 juillet 2016, C-191/15, *Verein für Konsumenteninformation*, EU:C:2016:612, pt. 76.
113. C.J.U.E., 1er octobre 2015, *Weltimmo*, *o.c.*, pt. 31 (nous soulignons).
114. *Ibid*., pts. 16 et 32. Dans l'affaire en question, il était évident que l'activité réelle de la société était dirigée vers la Hongrie et ne correspondait pas au lieu d'enregistrement. Il ressort également des éléments de la procédure que la société Weltimmo n'exerçait aucune activité effective en Slovaquie et avait, à plusieurs reprises, transféré son siège d'un Etat membre à un autre.
115. *Ibid*., pt. 41.
116. *Ibid*., pt. 29.
117. C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation*, *o.c.*, pt. 76.

**46.** Sur un plan plus général, il n'est pas anodin que le point 1. de l'article 3 du GDPR s'articule autour de l'établissement du responsable et non pas autour de la personne concernée[118]. Ce choix du législateur européen implique qu'aucun lien de connexion entre la personne concernée et l'Union n'est requis pour l'application de ce point 1. En d'autres termes, dès lors que l'établissement d'un opérateur est localisé sur le territoire de l'Union européenne, toutes les personnes, quel que soit leur nationalité ou leur domicile, dont les données sont traitées par cet opérateur peuvent potentiellement[119] obtenir la protection du règlement[120]. En théorie, un Australien établi au Japon, dont les données sont traitées par un opérateur basé aux Etats-Unis, mais disposant d'une filiale en Europe, pourrait revendiquer l'application du règlement. Cette approche correspond tant au texte de l'article 16 du traité sur le fonctionnement de l'Union européenne qu'à celui de l'article 8 de la Charte des droits fondamentaux de l'Union. Ces deux dispositions consacrant le droit à la protection des données à caractère personnel pour « *toute* personne », peuvent, effectivement, être lues comme impliquant le respect de ce droit par tout opérateur disposant d'un établissement sur le territoire de l'Union, peu importe la nationalité ou la résidence des personnes dont il traite les données[121].

**47.** Enfin, il convient d'ajouter que, dans son avis récent, le CEPD précise que le représentant, désigné au sens de l'article 27 du GDPR par un responsable de traitement non établi sur le territoire de l'Union, ne serait constituer un établissement de ce responsable[122]. La solution inverse reviendrait à priver le point 2. de l'article 3 du GDPR de toute application[123].

### ii) Ne pas être établi dans l'Union

**48.** Le point 2. de l'article 3 a été rédigé en vue d'éviter que le responsable du traitement puisse échapper à l'application du GDPR en contournant le point 1. Le législateur européen a ainsi prévu l'application du point 2. que dans la mesure où ni le responsable du traitement ni son sous-traitant n'est *établi dans l'Union*.

**49.** Sous le régime de la directive n° 95/46[124], les termes « lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté » devaient être compris, selon le GT29, comme renvoyant aux responsables ne disposant d'aucun établissement sur le territoire de l'Union dans le cadre duquel était effectué le traitement de données personnelles en cause[125]. Toute autre interprétation risquait d'être problématique[126].

**50.** A cet égard, une autre interprétation possible aurait été de considérer un responsable ou un sous-traitant établi dans la Communauté par la simple présence d'un de ses établissements sur le territoire de la Communauté. Sous la directive n° 95/46, une telle interprétation aurait créé une lacune dans la mesure où, l'article 4, point 1., litera a), de cette directive prévoyait son application en présence d'un établissement sur le territoire de la Communauté *uniquement* si les données personnelles étaient traitées *dans le cadre des activités de cet établissement*. En d'autres termes, en interprétant les termes « établi sur le territoire de la Communauté » comme synonymes de disposé d'un établissement sur le territoire de la Communauté, le risque était d'exclure l'application de la directive n° 95/46 aux données personnelles qui n'étaient pas traitées dans le cadre des activités de l'établissement d'un responsable, lorsque ce dernier disposait, néanmoins, d'un établissement sur le territoire de la Communauté. En effet, puisque les données personnelles n'étaient pas traitées dans le cadre des activités de l'établissement du responsable, le litera a) du point 1. de l'article 4 de la directive n° 95/46 ne pouvait pas s'appliquer et le litera c) de cette même dis-

118. B. HARDY, *o.c.*, p. 885.

119. Pour autant que la personne concernée puisse démontrer que le traitement a lieu dans le cadre des activités d'un établissement sur le territoire de l'Union.

120. S. FRANCQ, « The external dimension of Rome I and Rome II: neutrality or schizophrenia », *in* M. CREMONA et H. MICKLITZ (dirs.), *Private law in the external relation of the EU*, Oxford, Oxford University Press, 2016, p. 96; B. HARDY, *o.c.*, p. 885; C.KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *o.c.*, pp. 11-12.

121. Art. 16, 1., TFUE et considérant 2 GDPR. Voy. égal. le considérant 2 du GDRP ainsi que V. REDING, « The upcoming data protection reform for the European Union », *International Data Privacy Law*, 2011, vol. 1, p. 3.

122. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 20.

123. M. GÖMANN, « The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement », *CML Rev.*, 2017, vol. 54, n° 2, p. 576.

124. Pour rappel, le litera a) du point 1. de l'art. 4 de la directive n° 95/46 énonçait que : « Chaque Etat 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'Etat membre* … » et le litera c) disposait que « Chaque Etat membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque 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 Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté. » (nous soulignons).

125. Dans son avis, le Groupe de Travail « Article 29 » indiquait ainsi que « l'article 4, paragraphe 1, point c), s'applique lorsque le responsable du traitement possède un établissement 'non pertinent' dans l'UE, c'est-à-dire lorsqu'il dispose d'établissements dans l'UE mais que leurs activités sont sans rapport avec le traitement de données à caractère personnel »; voy. avis 8/2010 du Groupe de Travail « Article 29 » *o.c.*, p. 22.

126. Voy. L. MOEREL, « The long arm of EU data protection law: does the data protection directive apply to processing of personal data of EU citizens by websites worldwide? », *o.c.*, p. 35 et B. HARDY, *o.c.*, p. 884.

position n'aurait pas non plus été applicable étant donné que ce responsable, par la présence de son établissement sur le territoire de la Communauté, aurait été considéré comme établi dans la Communauté[127]. Ce problème subsiste dans le cadre du GDPR et il serait, par conséquent, également problématique de considérer que sous le GDPR disposer d'un établissement sur le territoire de l'Union signifierait être établi dans l'Union.

**51.** Une deuxième possibilité aurait été de considérer que, sous le régime de la directive n° 95/46, le responsable du traitement était établi dans la Communauté, dès lors que son siège statutaire, son administration centrale ou son établissement principal se trouvait sur le territoire de la Communauté[128]. Cette interprétation était également problématique parce qu'elle risquait d'impliquer une application simultanée de l'article 4, point 1., litera a) et c), de la directive n° 95/46[129]. Or, l'application simultanée des litera a) et c) de la directive n° 95/46 devait être évitée car ces deux dispositions, en outre de déterminer le domaine d'application de la directive n° 95/46, désignaient la loi nationale de transposition applicable. Par conséquent, si le litera a) et le litera c) étaient d'application simultanément, ils risquaient de ne pas désigner les mêmes lois de transposition. C'est pour éviter un conflit de lois de transpositions qu'il a été considéré que l'application du litera a) de la directive n° 95/46 excluait l'application du litera c) de la même directive et *vice versa*.

**52.** Contrairement à la directive n° 95/46, le GDPR ne détermine plus la loi nationale de transposition applicable. Dans ces circonstances, sous le régime du règlement, il n'est plus nécessaire d'exclure l'application du point 2. de l'article 3, du GDPR lorsque le point 1. de ce même article s'applique[130]. Dit autrement, la volonté d'éviter l'application simultanée des critères d'applicabilité de la directive n° 95/46, ne trouve plus de justification sous le GDPR et, partant, il serait tout à fait possible de considérer, désormais, qu'un responsable est établi dans l'Union lorsqu'il dispose de son siège statutaire, de son administration centrale ou de son établissement principal sur le territoire de l'Union. Les facteurs d'applicabilité du GDPR ne seraient donc plus des facteurs exclusifs, comme ils l'étaient dans la directive n° 95/46 selon l'interprétation du GT29, mais ils seraient des facteurs alternatifs[131].

Etant donné l'interprétation large du domaine d'application du règlement que nous avons observé dans les sections précédentes, il serait, en théorie, cohérent de considérer les facteurs d'applicabilité du GDPR comme alternatifs plutôt que comme exclusifs, les facteurs alternatifs favorisant une détermination extensive du domaine d'application.

### *2) Lorsque le responsable dispose d'un établissement sur le territoire de l'Union: l'application du point 1. de l'article 3*

**53.** Si un responsable ou un sous-traitant dispose d'un établissement sur le territoire de l'Union, le traitement de données personnelles sera soumis au règlement pour autant qu'il soit « effectué dans le cadre des activités » de cet établissement.

**54.** Cette dernière condition est particulièrement large et abstraite. Pour qu'un traitement soit effectué dans le cadre des activités d'un établissement, il n'est pas nécessaire que le traitement soit effectué par l'établissement en question ou même que les données y soient accessibles. Le lieu du traitement et l'identité de la personne qui effectue le traitement ne sont pas décisifs pour déterminer si un traitement a été effectué dans le cadre d'un établissement[132]. De même, la localisation des données, le lieu où elles sont accessibles ou le lieu vers lequel elles sont transférées est sans importance[133].

**55.** Le traitement sera effectué dans le cadre d'un établissement, si cet établissement participe, non pas au traitement, mais, à des activités indissociablement liées à ce traite-

127. Voy. les conclusions de l'avocat général N. JÄÄSKINEN dans l'affaire *Google Spain*, pt. 63. Il indique que, selon une interprétation littérale, l'existence d'un établissement de *Google* sur le territoire de l'Union exclurait l'applicabilité de l'article 4, 1., sous c), de la directive.

128. En droit international privé européen, ce sont des critères communément utilisés, en présence de personnes morales. A titre d'exemples, voy. l'art. 63, 1., du 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.*, L. 351, 20 décembre 2012, p. 1. (Bruxelles I*bis*) et l'art. 19, 1., du règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, *J.O.*, L. 177, 4 juillet 2008, p. 6. (Rome I). Voy. égal., F. RIGAUX et M. FALLON, *Droit international privé*, Précis de la Faculté de Droit de l'Université catholique de Louvain, Bruxelles, Larcier, 2005, p. 984.

129. Sur la base de cette interprétation, une telle application simultanée des litera a) et c) 1., de l'art. 4 de la directive n° 95/46 aurait effectivement eu lieu dans la mesure où le traitement des données avait été effectué dans le cadre des activités d'un établissement du responsable situé sur le territoire de la Communauté mais que le siège statutaire ou l'établissement principal du responsable n'était pas situé sur le territoire de la Communauté.

130. Dans le GDPR, l'art. 3, 1. et 2., succèdent respectivement à l'article 4, 1., litera a) et litera c).

131. Sur les notions de facteur d'applicabilité alternatif et exclusif, voy. F. RIGAUX et M. FALLON, *Droit international privé*, *o.c.*, not. les pp. 123 et 132.

132. Dans l'affaire *Google spain*, la Cour indiquait déjà que la directive n'exigeait « pas que le traitement de données à caractère personnel en question soit effectué 'par' l'établissement concerné lui-même, mais uniquement qu'il le soit 'dans le cadre des activités' de celui-ci ». Le GDPR, en son article 3, 1., a confirmé la décision de la Cour, en précisant qu'il était applicable dès lors que le traitement avait eu lieu dans le cadre des activités d'un établissement sur le territoire de l'Union, « que le traitement ait lieu ou non dans l'Union ».

133. Avis 8/2010 du Groupe de Travail « Article 29 », *o.c.*, p. 18. La proposition avait été émise en doctrine de considérer que des données sont traitées dans le cadre des activités d'un établissement à partir du moment où elles sont disponibles à partir de l'établissement. Voy. à cet égard, C. KUNER, *European Data Protection Law Corporate Compliance and Regulation*, Oxford, Oxford University Press, 2007, p. 72 et J. MOINY, *o.c.*, p. 260.

ment[134]. Deux éléments caractérisent une telle participation: la nature des activités de l'établissement et le lien entre les activités de l'établissement et le traitement des données[135]. Dans l'arrêt *Google Spain*, la Cour a considéré qu'un lien indissociable existait bien entre le traitement de données personnelles opéré par Google et les activités de promotion de Google Spain. Selon la Cour, ces activités de promotion « constituent le moyen pour rendre le moteur de recherche […] économiquement rentable et […] ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités »[136]. Le point 1. de l'article 3 serait ainsi applicable à tous les opérateurs dont le modèle commercial consiste à fournir un service qu'ils rentabilisent, partiellement à tout le moins, en collectant des données pour autant qu'ils aient un établissement chargé de la promotion de ce service sur le territoire de l'Union.

Aux termes de l'arrêt *Google Spain*, un lien indissociable est nécessaire entre les activités de l'établissement et le traitement de données pour rendre le règlement applicable sur la base du point 1. de l'article 3. Selon le GT29, ce lien indissociable peut même être indirect[137]. En l'espèce, ledit Groupe de Travail considère que ne sont pas des obstacles à l'existence d'un lien indissociable entre les activités de Google Spain et le traitement de données de Google Inc., le fait que l'argent généré par les activités de Google Spain ne soit pas utilisé pour financer le moteur de recherche www.google.es ou encore le fait que les contrats liés à la publicité sur le moteur de recherche soient conclus non pas par Google Spain, mais par Google Ireland[138].

**56.** Dans l'affaire *Google Spain*, la Cour souligne un autre élément qui n'apparaissait pas dans l'article 4 de la directive et qui ne se retrouve pas non plus dans le point 1. de l'article 3 du règlement. Elle juge que le traitement de données opéré par Google est effectué dans le cadre des activités de son établissement espagnol « dont l'activité vise les habitants »[139] de l'Etat sur le territoire duquel cet établissement se situe. Cette précision supplémentaire laisse penser que la direction des activités de l'établissement joue un rôle pour déterminer si le traitement en cause a bel et bien été effectué dans le cadre de son activité.

### *3) Lorsque le responsable n'est pas établi sur le territoire de l'Union: l'application du point 2. de l'article 3*

**57.** Un traitement de données personnelles n'échappe pas au champ d'application du GDPR par le seul fait que le responsable, ou le sous-traitant, l'ayant effectué n'est pas établi sur le territoire de l'Union. Dans cette hypothèse, le point 2., de l'article 3 du règlement prévoit spécifiquement que le règlement s'applique au traitement de données personnelles si les personnes concernées « se trouvent sur le territoire de l'Union » (i)) et que les activités de traitement sont liées soit à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes (ii)), soit au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union (iii)).

#### i) Les personnes concernées qui se trouvent sur le territoire de l'Union

**58.** Le point 2. de l'article 3 du règlement apporte une innovation majeure dans le droit européen de la protection des données en ajoutant un critère d'applicabilité centré sur la localisation de la personne concernée. Ceci dit, les deux hypothèses dans lesquels le point 2. de l'article 3 s'applique, à savoir l'offre de biens ou de services et le suivi du comportement, révèlent bien la dimension consumériste du règlement[140] et démontre qu'il reste étroitement lié au marché intérieur.

**59.** Ce nouveau critère d'applicabilité a pour conséquence de recentrer le point 2. sur la protection des personnes localisées dans l'Union. Cependant, la manière dont ce critère a été concrétisé pose question. Le point 2. s'applique pour autant que la personne concernée « *se trouve* sur le territoire de l'Union ». Comment comprendre cette condition? Le règlement ne donne pas de précision sur ce qu'il entend par « se trouver » sur le territoire de l'Union. Faut-il comprendre que le législateur européen fait référence à la résidence ou au domicile de la personne concernée? Si oui, pourquoi le législateur a-t-il amendé la proposition de la Commission qui prévoyait précisément l'application du règlement à la personne résidant sur le territoire de l'Union[141]?

A notre sens, cet amendement permet surtout au règlement

134. Update of Opinion 8/2010 of the « Working Party 29 » on applicable law in light of the CJEU judgement in Google Spain, 16 décembre 2015, WP 179, pp. 4 et 7. Voy. égal. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 6.
135. Avis 8/2010 du Groupe de Travail « Article 29 », *o.c.*, pp. 15-16; Update of Opinion 8/2010 of the « Working Party 29 », *o.c.*, p. 4.
136. C.J.U.E., 13 mai 2014, C-131/12, *Google Spain* et *Google*, *o.c.*, pt. 56.
137. Update of Opinion 8/2010 of the « Working Party 29 », *o.c.*, p. 5.
138. *Ibid*.
139. C.J.U.E., 13 mai 2014, C-131/12, *Google Spain* et *Google*, *o.c.*, pts. 55 et 60; Update of Opinion 8/2010 of the « Working Party 29 », *o.c.*, p. 4.
140. F. JAULT-SESEKE et C. ZOLYNSKI, « Le règlement 2016/679/UE relatif aux données personnelles: aspects de droit international privé », *Recueil Dalloz*, 2016, p. 1875.
141. Cet amendement est arrivé au stade de la première lecture au Parlement, avant cela les différentes discussions en commissions parlementaires avaient abouti à un amendement proposant de substituer au critère de résidence celui de domicile.

d'être en phase avec l'article 16 du TFUE et l'article 8 de la Charte des droits fondamentaux, qui consacrent un droit à la protection des données personnelles à l'égard de « toute personne ». L'Union semble affirmer, au travers de ce règlement, sa volonté de protéger le droit à la protection des données à caractère personnel, indépendamment de la nationalité ou de la résidence de la personne concernée[142], quitte à rendre le critère d'applicabilité incertain[143]. En effet, il paraît actuellement difficile de déterminer avec précision qui est visé par le point 2. de l'article 3 du règlement et, partant, à qui s'applique le GDPR. Par exemple, le point 2. s'appliquerait-il à un résident européen qui voyageant en dehors de l'Union pour un court séjour ou à un résident d'un Etat tiers qui se rendrait en Europe pour ses vacances? Dans pareils cas, le résident européen ne se trouve plus, au sens commun du terme, sur le territoire de l'Union contrairement au résident de l'Etat tiers. Ceci voudrait donc dire que le résident européen serait dépourvu de la protection du règlement alors que le résident de l'Etat tiers en bénéficierait. Par ailleurs, cela risque de soulever d'épineuses questions de preuve.

**60.** De surcroît, le point 2. de l'article 3 du GDPR ne donne aucune indication sur la solution du conflit mobile, c'est-à-dire, sur la détermination du moment de référence pour évaluer si la personne concernée se trouve sur le territoire européen. Or, il n'est pas exclu que la personne concernée voyage durant une période pendant laquelle ses données sont traitées. Le moment décisif pour déterminer la loi applicable pourrait être celui de la collecte des données, de l'enregistrement des données, voire de leur diffusion ou d'une autre opération? Il est aussi imaginable de se référer au moment de la formulation de l'offre ou du suivi du comportement. Cette dernière hypothèse est d'ailleurs privilégiée par le CEPD[144]. Ces questions entourant l'interprétation des termes « se trouve » risquent de nécessiter les lumières de la Cour de justice.

**61.** Enfin, et ce n'est probablement pas un détail s'agissant du règlement général sur la protection des données, le point 2. de l'article 3 exige du responsable qu'il détermine où se trouve la personne afin d'établir si le GDPR est d'application. Par conséquent, avant même de savoir si le GDPR s'applique, le responsable va devoir traiter au moins une donnée personnelle de la personne concernée ou, dit autrement, la personne concernée, si elle se trouve sur le territoire de l'Union, va devoir divulguer une donnée personnelle pour obtenir la protection du règlement. Ce « *visibility paradox* »[145] est inhérent au choix d'un facteur d'applicabilité centré sur la personne, qu'il s'agisse de l'endroit où elle se trouve ou de la localisation de son domicile ou de sa résidence.

**ii) L'offre de biens ou de services à la personne concernée**

**62.** Dans l'hypothèse où la personne concernée se trouve sur le territoire de l'Union, au sens de l'article 3, point 2., un autre facteur d'applicabilité doit encore être satisfait.

**63.** La première hypothèse posée par le litera a) du point 2. de l'article 3 du GDPR vise clairement les consommateurs. Elle tente d'offrir une protection harmonisée de leurs données personnelles au sein du marché intérieur. Cela participe à la volonté de l'Union de développer la confiance des Européens dans le marché unique numérique.

**64.** Le règlement prévoit ainsi son application dès lors que le traitement est lié à une offre de biens ou de services faite à la personne concernée, sans toutefois nécessiter la conclusion d'un contrat[146]. Comme le souligne le considérant 23, l'intention d'offrir des biens ou des services à des personnes dans l'Union suffit pour que le traitement des données relatif à cette offre de bien ou de service soit soumis au GDPR[147]. Par ailleurs, pour établir l'existence d'une intention d'offrir des biens ou des services, ce même considérant adopte un raisonnement très proche de celui développé par la C.J.U.E. dans son arrêt *Pammer et Alpenhof*[148]. En effet, le considé-

142. Considérants 2 et 14 du GDPR. A cet égard, le CEPD note également que le point 2. de l'art. 3 du GDPR ne se limite pas aux seuls résidents ou citoyens européens. Voy. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 13.

143. En d'autres termes, il semble certain que l'Union doit protéger et promouvoir ce droit comme tous les droits fondamentaux ; voy. à cet égard M. TAYLOR, « The EU's human rights obligations in relation to its data protection laws with extraterritorial effect », *International Data Privacy Law*, 2015, vol. 5, n° 4, pp. 246 et s. Toutefois, cela implique-t-il que le règlement doit, en tant que tel, être rendu applicable à toute personne sans considération de sa résidence ou de sa nationalité?

144. Guidelines 3/2018 of the European Data Protection Board on the territorial scope of the GDPR (art. 3), *o.c.*, p. 13.

145. Paradoxalement, pour obtenir une protection plus étendue de ses données, la personne concernée doit d'abord divulguer des données personnelles. J. AUSLOOS et P. DEWITTE, « Shattering One-Way Mirrors: Data Subject Access Rights in Practice », *International Data Privacy Law*, 2018, vol. 8, n° 1, p. 13.

146. J.-F. HENROTTE et F. COTON, « Application territoriale de la législation européenne en matière de protection des données et transfert de données vers des pays tiers: vaincre la peur de l'autre », *in* A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Bruylant, 2015, p. 190.

147. Selon le considérant 23 du GDPR, c'est l'intention d'offrir des services à des personnes concernées dans un ou plusieurs Etats membres qui est déterminante. Pour une discussion entre une approche du critère de direction des activités basée sur l'intention et une approche basée sur le résultat concret; voir not. D.J.B. SVANTESSON, « Extraterritoriality and targueting in EU data privacy law: the weak spot undermining the regulation », *International Data Privacy Law*, 2015, vol. 5, n° 4, pp. 231-232.

148. C.J.U.E., 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, EU:C:2010:740, pt. 63. Cette affaire concerne les art. 15 et 16 du Règlement Bruxelles I*bis*. Ces dispositions obligent le professionnel agissant contre un consommateur d'agir au lieu du domicile du consommateur et permettent au consommateur d'agir contre un professionnel au lieu de son propre domicile pour autant que le professionnel dirige ses activités vers l'Etat sur le territoire duquel le consommateur a son domicile.

rant 23 précise que « la simple accessibilité du site Internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention ». Il ajoute, en revanche, que « l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs Etats membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union »[149].

**65.** Toutefois, si le point 2. de l'article 3 du GDPR se rapproche, sous certains aspects, des articles 17 et 18 du Règlement Bruxelles I*bis* et de l'article 6 du Règlement Rome I dans l'utilisation de la direction des activités comme facteur de rattachement, il s'en écarte sous d'autres aspects. Ainsi, contrairement au GDPR, les Règlements Bruxelles I*bis* et Rome I limitent l'application de la direction des activités comme facteur de rattachement aux seuls cas où un contrat de consommation a été conclu[150]. Par ailleurs, les Règlements Bruxelles I*bis* et Rome I sont plus larges dans leur formulation puisqu'ils prennent en compte « tous les moyens » par lesquels le professionnel peut diriger son activité alors que le GDPR fait référence à une liste d'indices, très probablement non exhaustive, dans ses considérants. Il est, néanmoins, très probable que la Cour de justice étende cette liste aux indices qu'elle cite dans l'affaire *Pammer et Alpenhof*. Notons également que s'agissant des indices pertinents pour déterminer la direction des activités, dans le GDPR, le législateur européen accorde une pertinence aux langues utilisées et aux devises affichées pour déterminer la direction des activités d'un opérateur, ce qu'il a refusé dans le Règlement Rome I[151], même si ce refus a été nuancé par la Cour[152].

**66.** Enfin, le litera a), *in fine*, n'exige pas que le bien ou le service soit offert contre paiement. Le GDPR entend offrir aux consommateurs le même niveau de protection de ses données personnelles, que les biens et services lui soient proposés à titre onéreux ou gracieux.

**iii) Le suivi du comportement des personnes concernées**

**67.** Le litera b) du point 2. de l'article 3 du GDPR vise de manière alternative une seconde hypothèse dans laquelle le législateur entend protéger les données personnelles d'une personne se trouvant sur le territoire de l'Union. A défaut d'être lié à une offre de biens ou de services, un traitement effectué par un responsable ou un sous-traitant qui n'est pas établi dans l'Union sera, néanmoins, soumis au règlement si ce traitement est lié au suivi du comportement de la personne concernée, et ce pour autant que le comportement en question ait lieu au sein de l'Union.

**68.** Le « *suivi du comportement* » n'est pas défini en tant que tel par le GDPR. Toutefois, le considérant 24 précise que pour qualifier une activité de traitement comme un suivi du comportement de la personne concernée, « *il y a lieu d'établir si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* ». Aux termes de ce considérant, il est évident que le litera b) du point 2. de l'article 3 vise notamment, mais pas exclusivement, la pratique du profilage que le règlement définit comme un traitement de données consistant à « *évaluer certains aspects personnels relatifs à une personne physique* »[153] et que le législateur souhaitait explicitement encadrer en faisant évoluer le domaine d'application de la directive n° 95/46. Grâce à cette disposition, le règlement s'applique aux traitements des données personnelles effectués au travers de logiciels, comme les *cookies* ou les bannières *JavaScript*[154], ou à l'aide d'objets connectés, à l'image des montres connectées ou des voitures connectées.

**69.** Le texte du litera b) dispose, en outre, que le règlement ne s'appliquera au traitement de données en cause que « *dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* », ce qui exclut les hypothèses où le comportement de la personne concernée est suivi lorsqu'elle voyage hors du territoire européen[155], quand bien même il s'agirait d'un citoyen ou d'un résident européen.

149. Pour une critique du critère de direction des activités à cause des difficultés de sa mise en œuvre et du manque de prévisibilité et de sécurité juridique, voy. D.J.B. SVANTESSON, « Extraterritoriality and targeting in EU data privacy law ... » *o.c.*, pp. 231-232 et D.J.B. SVANTESSON, « Digital Contracts in Global Surroundings », *in* S. GRUNDMANN (dir.), *European Contract Law in the Digital Age*, Cambridge, Intersentia, 2018, p. 75 et M. GÖMANN, « The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement », *o.c.*, pp. 584-586.
150. C.J.C.E., 20 janvier 2005, C-27/02, *Engler*, EU:C:2005:33.
151. Considérant 24, *in fine,* Règlement Rome I.
152. C.J.U.E., 7 décembre 2010, *Pammer et Alpenhof*, *o.c.*, pt. 84.
153. Art. 4, 4), GDPR.
154. J.-F. HENROTTE et F. COTON, *o.c.*, pp. 191-192.
155. *Ibid.*, p. 191.

**70.** Cette condition – la localisation du comportement au sein de l'Union – n'était pas présente dans la proposition de la Commission. Son absence avait d'ailleurs été critiquée[156] alors que le litera a) du même point précisait que l'offre de biens ou de services devait être dirigée vers l'Union. La critique portait sur fait que le litera b) du point 2. de l'article 3 semblait offrir une protection à la personne concernée à l'égard du suivi de son comportement, peu importe où elle se trouvait, simplement parce qu'elle résidait sur le territoire de l'Union. Toutefois, entretemps, le point 2. n'exigeait plus que la personne concernée réside dans l'Union, mais qu'elle se trouve sur le territoire de l'Union. Il demeure que le législateur européen a préféré préciser que l'application du litera b) du point 2. de l'article 3 du GDPR nécessite que la personne concernée doit non seulement se trouver sur le territoire de l'Union, mais, qu'en outre, son comportement ait lieu au sein de l'Union.

## SECTION 2. L'INTERNATIONALITÉ EXTERNE DU GDRP: UNE EXTRATERRITORIALITÉ NÉCESSAIRE ET PROPORTIONNÉE?

**71.** L'examen ci-avant de l'article 3 du GDPR révèle la très large ampleur de son domaine d'application. Les dispositions du règlement visent non seulement des opérateurs européens, mais également des opérateurs non européens. Ce constat confirmé, nous nous interrogeons sur le caractère extraterritorial du règlement et sur sa nécessité (Sous-section 1.). Par la suite, nous postulons que d'autres solutions, que celles adoptées par le GDPR pour déterminer son domaine d'applicabilité, méritaient d'être explorées au vu du principe d'effectivité et de proportionnalité (Sous-section 2.).

### Sous-section 1. L'extraterritorialité du GDPR: une nécessité justifiée

**72.** En adoptant le GDPR, l'Union tente de réguler des comportements et des actes posés tant par des opérateurs européens qu'étrangers. Cette situation a été critiquée au motif que le GDPR serait un acte extraterritorial. Certains allant même jusqu'à en déduire que ce règlement serait contraire au droit international[157]. Sans épuiser le propos, ni étudier l'extraterritorialité de manière approfondie, nous pouvons, néanmoins, noter que ces critiques sont, dans une large mesure, exagérées pour diverses raisons explicitées ci-après.

**73.** A supposer que le droit international limite réellement les titres d'exercice législatif d'une activité normative extraterritoriale, l'application du GDPR à des situations partiellement localisées à l'étranger serait légitime sur le fondement de trois théories. Premièrement, les hypothèses dans lesquelles le responsable ou le sous-traitant dispose d'un établissement dans le cadre duquel le traitement a été effectué peuvent s'apparenter à une application du principe de personnalité active, qui permet à un Etat d'exercer ses compétences sur ses nationaux. En effet, le comportement du responsable ou du sous-traitant peut être assimilé au comportement d'une entreprise européenne, si ce dernier dispose d'un établissement sur le territoire de l'Union. La C.J.U.E. a déjà eu recours à ce raisonnement en droit de la concurrence[158]. Deuxièmement, s'agissant des situations où les personnes concernées se trouvent sur le territoire européen, la compétence de l'Union pourrait se justifier sur base du principe de personnalité passive[159]. Dans sa conception classique, ce principe autorise un état à exercer ses compétences vis-à-vis de l'auteur d'une infraction lorsque la victime de cette infraction est un national[160]. Troisièmement, le principe de territorialité, en ce compris la doctrine des effets, pourrait également venir justifier la compétence de l'Union.

**74.** En soulignant la possibilité, bien connue en droit international privé, d'appliquer une règle à des situations partiellement localisées hors du territoire du législateur, J. SCOTT[161] apporte, par ses récents travaux sur l'extraterritorialité du droit européen, un éclairage intéressant à propos du principe de territorialité concernant les actes législatifs européens comme le GDPR. En effet, J. SCOTT ne qualifie pas d'extraterritoriale, mais d'extension territoriale, la règle dont l'application est déclenchée par un acte localisé en dehors du territoire de l'Etat auteur, pour autant que l'application de cette règle dépende de l'existence d'un lien territorial perti-

156. D.J.B. SVANTESSON, « The extraterritoriality of EU data privacy law: Its theoretical justification and its practical effect on U.S. businesses », *o.c.*, pp. 71-72.

157. L. MOEREL, « The long arm of EU data protection law: does the data protection directive apply to processing of personal data of EU citizens by websites worldwide? », *International Data Privacy Law*, 2011, vol. 1, p. 29. Voy. égal. les auteurs cités par D.J.B. SVANTESSON, « The extraterritoriality of EU data privacy law … », *o.c.*, p. 59 et les officiels américains par C. KUNER, « Extraterritoriality and regulation of international data transfers in EU data protection law », *International Data Privacy Law*, 2015, vol. 5, p. 235.

158. C.J.C.E., 14 juillet 1972, 48/69, *Imperial Chemical Industries*, EU:C:1972:70, pts. 125 et s. Voy. à cet égard G. VAN CALSTER, *Regulating the internet. Prescriptive and Jurisdictional Boundaries to the EU's 'right to be forgotten'*, p. 12, disponible sur www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2686111 (consulté le 11 août 2018).

159. D.J.B. SVANTESSON, « A 'layered approach' to the extraterritoriality of data privacy laws », *International Data Privacy Law*, 2013, vol. 3, p. 279.

160. J . KLABBERS, *International Law*, *o.c.*, p. 93; M.N. SHAW, *International Law*, 8e éd., *o.c.*, pp. 497-499.

161. J. SCOTT, « Extraterritoriality and Territorial Extension in EU Law », *American Journal of Comparative Law*, vol. 62, 2014, p. 90. Voy. égal. J. SCOTT, « The New EU 'Extraterritoriality' », *Common Market Law Review*, 2014, p. 1366.

nent avec l'Etat auteur. En d'autres termes, J. SCOTT considère qu'une règle ne peut être qualifiée d'extraterritoriale s'il existe un lien territorial entre la personne désignée comme le destinataire de la règle et l'Etat dont émane cette règle. Selon cette vision, le GDPR devrait être qualifié non pas d'extraterritorial, mais d'extension territoriale[162] et, partant, la compétence de l'Union pourrait se justifier sur la base du principe de territorialité.

**75.** Par ailleurs, même si le GDPR devrait être qualifié d'extraterritorial, rien n'assure qu'un acte extraterritorial soit contraire au droit international. En effet, en droit international, aucune règle, principe ou coutume ne proscrit ou ne limite une définition extraterritoriale de l'applicabilité d'une norme[163]. De même, en droit européen, selon la C.J.U.E., une telle interdiction ou limite est absente des traités[164].

**76.** Il convient, également, de rappeler que l'application du droit de l'Union au-delà des frontières des Etats membres ne dépend pas exclusivement de la volonté unilatérale du législateur européen. La distinction entre le domaine d'application et la force obligatoire amène ainsi à relativiser les conséquences d'une application, ou plutôt d'une définition d'un domaine d'application extraterritoriale, puisque les pouvoirs de contrainte des institutions européennes ne peuvent s'exercer au-delà des frontières européennes[165]. Pour résumer la situation, nous ne pouvons que nous rallier au constat suivant: « *l'affirmation d'un domaine véritablement extraterritorial est parfaitement valide, mais n'est pas pour autant efficace* »[166].

**77.** S'interroger sur l'extraterritorialité du GDPR, doit se faire en gardant à l'esprit que son caractère extraterritorial est un élément fondamental. Quelle serait l'utilité de ce règlement s'il ne produisait aucun effet extraterritorial? Actuellement, les législations protégeant les données qui existent au niveau mondial ne permettent pas d'assurer, hors du territoire européen, le niveau de protection recherché par l'Union[167]. Dans ce contexte, si le règlement visait exclusivement les traitements de données effectués sur le territoire européen, les opérateurs pourraient facilement et rapidement relocaliser leurs activités pour éviter l'application du GDPR. En outre, en ne visant que les opérateurs européens, l'Union créerait un avantage concurrentiel au détriment de ces derniers. Par conséquent, si l'Union souhaite assurer une protection effective des données personnelles, pour l'heure, elle n'a pas d'autres choix que d'accompagner ses règles en la matière d'un large champ d'application.

**78.** Précisons, toutefois, que la nécessité d'une portée extraterritoriale ne signifie pas que l'Union puisse se dispenser de respecter le droit international. Au contraire, le traité sur l'Union européenne impose à l'Union le strict respect du droit international dans ses relations avec le reste du monde[168]. Cela ne signifie pas non plus, selon nous, que l'Union devrait se dispenser de rechercher la solution qui atteint au mieux son objectif tout en limitant ses effets extraterritoriaux. A cet égard, dans la prochaine sous-section, nous postulons que l'application du principe de proportionnalité – principe bien connu en droit européen[169] – à la détermination du domaine d'application du GDPR permettrait, tout à la fois, d'atteindre un niveau de protection des données personnelles plus élevé, d'atténuer l'intensité des discussions sur l'extraterritorialité et d'améliorer la coopération entre l'Union et les Etats tiers[170].

## Sous-section 2. Plus de proportionnalité pour plus d'efficacité

**79.** A notre sens, la recherche de proportionnalité dans le domaine d'application du règlement aurait pu recevoir davantage d'attention au moment de l'adoption du GDRP. En effet, d'autres modèles, dont certains évoqués par la doctrine, mériteraient d'être examinés plus en détail.

**80.** A titre d'exemple, Svantesson propose une solution alternative sur base de ce qu'il appelle une « layered approach »[171], consistant à classer les règles du GDPR en

162. M. TAYLOR, « The EU's human rights obligations … », *o.c.*, p. 247.
163. S. FRANCQ, *L'applicabilité du droit communautaire dérivé*, *o.c.*, voy. not. pp. 80 et 173.
164. C.J.C.E., 15 novembre 1994, avis 1/94, EU:C:194:384, pt. 79. A l'occasion de cet avis, la Cour a jugé « que rien dans le traité n'empêche les institutions d'organiser, dans les règles communes qu'elles arrêtent, des actions concertées a l'égard des pays tiers ni de prescrire les attitudes a prendre par les Etats membres vis-a-vis de l'extérieur ». S. FRANCQ, *L'applicabilité du droit communautaire dérivé*, *o.c.*; voy. not. pp. 80 et 173. Cette question limite est au cœur de l'affaire pendante C-507/17, *Google (Portée territoriale du déréférencement)*.
165. D.J.B. SVANTESSON, « The extraterritoriality of EU data privacy law … », *o.c.*, pp. 94 et s.; S. FRANCQ, *L'applicabilité du droit communautaire dérivé …*, *o.c.*, pp. 237-238, à propos de règlement en matière de transport.
166. S. FRANCQ, *L'applicabilité du droit communautaire dérivé …*, *o.c.*, p. 272.
167. D.J.B. SVANTESSON, « A 'layered approach'… », *o.c.*, p. 279. Voy. égal. du même auteur, « Extraterritoriality in the context of data privacy regulation », *Masaryk University Journal of Law and Technology*, 2012, p. 95.
168. Art. 3, 5., TUE.
169. Art. 5 TUE. Selon l'art. 5 du TUE, et surtout selon le deuxième protocole sur l'application des principes de subsidiarité et de proportionnalité annexé aux traités européens, le principe de proportionnalité entend s'appliquer essentiellement au bénéfice des Etats membres et des citoyens européens. C'est donc bien une application plus générale de ce principe de proportionnalité que nous proposons ici.
170. Atténuer l'intensité des discussions sur l'extraterritorialité et améliorer la coopération entre l'Union et les Etats tiers contribuerait, selon nous, au respect mutuel entre les peuples ce qui est, aux termes, de l'art. 5 TUE un des objectifs de l'Union dans ses relations avec le reste du monde.
171. D.J.B. SVANTESSON, « A 'layered approach' … », *o.c.*, pp. 278-286. L'auteur estime qu'une solution plus juste peut être trouvée concernant l'application extraterritoriale de la protection des données personnelles; voy. p. 279.

différentes catégories. Pour sa part, il distingue trois catégories de règles, à savoir, les règles qui visent à interdire et sanctionner une utilisation abusive de données personnelles, celles qui confèrent des droits à la personne concernée et, enfin, celles qu'il qualifie d'administratives, à l'image de l'obligation de désigner un délégué à la protection des données personnelles. L'idée étant que chacune des trois catégories soit assortie d'un domaine d'application spécifique. L'auteur reconnaît lui-même que la création des catégories est un exercice impliquant une part importante de subjectivité et que plusieurs catégorisations sont possibles. Il admet également qu'il s'agit d'un exercice compliqué, car il n'est pas évident de classer toutes les règles dans une catégorie bien définie et que certains articles du GDPR contiennent plusieurs règles susceptibles d'appartenir à plusieurs catégories, ce qui peut nécessiter une réorganisation du règlement. En outre, il semble que la principale difficulté soit ailleurs. En effet, la protection des données personnelles est un droit fondamental et cette méthode revient à différencier des règles que la Charte des droits fondamentaux de l'Union consacre explicitement[172].

**81.** Une autre possibilité serait de s'inspirer du concept de « contingency » mis en avant par J. SCOTT. Le principe sous-jacent consiste à renoncer d'appliquer le droit de l'Union aux activités d'un opérateur étranger lorsque ces activités sont déjà réglementées de manière satisfaisante par un Etat tiers[173]. L'idée est d'appliquer ce concept à la protection des données. Concrètement, cela nécessiterait de revoir le régime des transferts internationaux de données personnelles et surtout de l'articuler avec le domaine d'application tel qu'il est décrit à l'article 3 du GDPR.

Rappelons que le GDPR n'autorise les transferts internationaux de données personnelles que sous certaines conditions, et ce afin d'éviter que les données personnelles soumises au règlement ne soient, par l'effet d'un transfert, dépourvues de toute protection[174]. Les transferts internationaux de données sont autorisés par le règlement si l'Etat tiers vers lequel ces transferts ont lieu fait l'objet d'une décision d'adéquation de la Commission, reconnaissant que cet Etat tiers assure un niveau de protection adéquat. Un tel transfert sera également autorisé si des garanties appropriées existent. Pareilles garanties sont constituées par les clauses contractuelles types adoptées par la Commission, les clauses contractuelles types adoptées par une autorité nationale de contrôle et approuvées par la Commission ou les clauses contractuelles *ad hoc*. Dans le cas d'un groupe d'entreprises, les règles d'entreprise contraignantes peuvent également, pour ce groupe d'entreprises, jouer le rôle de garanties appropriées. L'adhésion à un code de conduite ou à un mécanisme de certification est également reconnue, par le GDPR, en tant que garanties appropriées. Enfin, les transferts internationaux peuvent encore être fondés sur une des dérogations prévues à l'article 49 du GDPR.

Parmi ces différentes hypothèses, nous remarquerons que la décision d'adéquation a une portée très large puisqu'elle autorise tous les transferts à destination d'un état tiers déterminé. Les autres hypothèses, notamment les clauses contractuelles ou les règles d'entreprise contraignantes ne s'appliquent qu'à des transferts au sein d'un groupe d'entreprises ou, encore plus restrictif, qu'à une seule opération déterminée et nécessite d'être renouvelées pour toute autre opération.

Au regard des nombreux transferts de données personnelles et de l'importance de ce régime, il est étonnant que la notion de transfert international ne soit définie ni par le GDPR, ni par la Cour de justice. En pratique, cette notion a été interprétée de manière très large et recouvre, notamment, l'envoi ou la transmission de données personnelles vers un pays tiers[175]. Il y a donc manifestement une absence d'articulation entre l'article 3 et les articles 45 et suivants du GDPR qui mettent en place le régime du transfert international de données[176]. Comme nous l'avons décrit, le domaine d'application du GDPR est extrêmement large et, partant, est susceptible de s'appliquer à des opérateurs étrangers, qu'ils disposent ou non d'un établissement sur le territoire de l'Union. En outre, l'article 3 ne tient pas compte de la localisation des données. Or, selon l'interprétation extensive de la notion de transfert international de données, il est tout à fait probable qu'une situation soit directement visée par le règlement, à travers son article 3, mais également par le régime de transfert international créant donc un chevauchement des dispositions. Par exemple, si Google Spain communique des données personnelles à Google Inc., malgré que ce dernier soit directement soumis au GDPR en vertu de l'article 3, la communication en cause sera considérée comme un transfert

172. L'art. 8 de la Charte consacre sur un même pied des règles relevant de la première et de la deuxième catégorie proposé par Svantesson.
173. J. SCOTT, « The New EU 'Extraterritoriality' », *o.c.*, p. 1366.
174. Sur le régime des transferts internationaux de données, voy. parmi d'autres, C. BURTON et S. CADIOT, « Règlement général sur la protection des données: les transferts internationaux de données », *in* de B. DOCQUIR (coord.), *Vers un droit européen de la protection des données?*, Bruxelles, Larcier, 2017, pp. 59-88.
175. C. BURTON et S. CADIOT, *o.c.*, p. 62.
176. C. KUNER, « Extraterritoriality and regulation of international data transfers in EU data protection law », *International Data Privacy Law*, 2015, vol. 5, p. 244.

international de données[177]. Afin d'éviter ce chevauchement de règles, il serait plus logique de considérer que le régime du transfert international de données personnelles ne s'applique que dans l'hypothèse où l'opérateur en question n'est pas déjà visé par l'article 3.

Pour appliquer le concept de « contingency », plus encore que la possibilité d'établir une articulation entre l'article 3 et le système des décisions d'adéquation, ce qui nous intéresse est la possibilité d'approfondir cette articulation et la rendre dynamique. Concrètement, l'idée serait de cesser l'application du GDPR aux opérateurs étrangers dès lors que ces opérateurs sont soumis à la législation d'un Etat tiers pour lequel la Commission a émis une décision d'adéquation. Les bénéfices pourraient être substantiels puisque l'incitant des Etats tiers à faire l'objet d'une décision d'adéquation et, donc, à développer leur législation en matière de protection des données serait plus important[178]. Cela créerait également des opportunités de dialogue sur le renforcement de la protection des données entre les Etats tiers et l'Union puisque même si, formellement, la décision d'adéquation est un acte unilatéral, substantiellement, elle est le fruit de discussions entre l'Etat tiers et la Commission. En d'autres termes, cela pourrait permettre d'encourager le développement de la protection des données à l'échelle mondiale tout en atténuant le caractère extraterritorial du GDPR. Notons également que l'avantage de cette solution est qu'il existe déjà, pour ces décisions d'adéquation, des garanties tant *a priori* qu'a *posteriori* impliquant différents acteurs[179].

**82.** Enfin, une troisième possibilité serait d'opter pour la méthode de droit international privé dite bilatérale et d'intégrer une règle de conflit de lois dans les règlements généraux de droit international privé. Il est, pour l'instant, peu probable que cette hypothèse se réalise au vu des difficultés éprouvées par les Etats membres au sujet des conflits de lois en matière de vie privée et des droits de la personnalité, qui ont conduit à exclure cette matière du Règlement Rome II. Une harmonisation des règles de conflit de lois pour les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité ne serait, toutefois, pas sans intérêt[180]. Dans le cadre d'une telle harmonisation, il pourrait être intéressant de penser la règle de conflit de lois concernant les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité pour s'assurer qu'elle soit également applicable aux obligations non contractuelles découlant d'une atteinte à la protection des données personnelles. Cette solution mérite d'être explorée dès lors qu'elle présente le double avantage d'aligner la détermination de la loi applicable en matière d'atteinte à la vie privée et en matière de donnée personnelle ainsi que d'offrir une solution claire s'agissant des conflits entre les lois nationales d'exécution du GDPR en matière extracontractuelle.

177. Pour prendre un second exemple, à la suite de l'arrêt *Scherms* de la C.J.U.E. (C.J.U.E., 6 octobre 2015, C-362/14, *Schrems*, EU:C:2015:650.), il ne fait pas de doute que les données personnelles des utilisateurs de Facebook résidant sur le territoire de l'Union sont transférées vers des serveurs appartenant à Facebook Inc, situés sur le territoire des Etats-Unis, où elles font l'objet d'un traitement, et que ces transferts sont soumis aux règles du régime de transfert international. Or, dans son jugement du 16 février 2018, le tribunal de première instance de Bruxelles a, en suivant la jurisprudence de la C.J.U.E. sur le domaine d'application de la directive n° 95/46, condamné Facebook Inc. pour violation de la loi de transposition de la directive n° 95/46 (Civ. Bruxelles, 16 février 2018, disponible sur le site de l'autorité de la protection des données, www.gegevensbeschermingsautoriteit.be/nieuws/overwinning-voor-de-privacycommissie-facebook-procedure (consulté le 7 juillet 2018)). En d'autres termes, lorsque des données d'utilisateurs ou de non-utilisateurs belges de Facebook sont transférées à Facebook Inc, elles sont soumises au régime de transfert international alors qu'il s'agit d'un traitement qui entre, en vertu de son art. 3, dans le champ d'application du GDPR, désormais et plus de la directive n° 95/46. Par conséquent, sont appliquées à la fois les règles imposées directement par le règlement et les règles decoulant du régime de transfert international. C'est ce que C. KUNER décrit comme une « 'belt and suspenders' approach »; voy. C. KUNER, « Extraterritoriality and regulation of international data transfers in EU data protection law », *o.c.*, p. 244.

178. C. BURTON et S. CADIOT, *o.c.*, p. 88. Ces auteurs constatent que ce régime est, somme toute, peu efficace.

179. La décision d'adéquation ne peut être prise que par la Commission et doit nécessairement prendre en compte les critères détaillés par le règlement. En outre, avant que la décision soit définitivement adoptée, elle doit être soumise sous la forme d'un projet de décision à un comité composé de représentants des Etats membres de l'UE. Une fois la décision adoptée, la Commission a l'obligation d'évaluer de manière régulière le niveau de protection dans le pays tiers qui a fait l'objet de la décision, et ce en tenant compte des éventuelles observations du Parlement européen, du Conseil de l'Union, du Contrôleur européen de la protection des données ou encore du Comité européen de la protection des données. Une surveillance peut également être exercée par les autorités nationales, qui peuvent examiner les transferts de données effectués vers un pays tiers, ainsi que par les particuliers et peut aboutir à examen de validité de la décision d'adéquation devant la Cour de justice, seule autorisée à invalider une décision de la Commission. Voy. C. BURTON et S. CADIOT, *o.c.*, pp. 65-71.

180. 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), *J.O.*, 2013, C. 261, E/17. Dans sa résolution, le Parlement européen demande à la Commission de soumettre une proposition visant à ajouter au Règlement Rome II une disposition régissant la loi applicable aux obligations non contractuelles résultant d'atteintes à la vie privée et aux droits de la personnalité.

## SECTION 3. L'INTERNATIONALITÉ INTERNE DU GDPR IGNORÉE: COMMENT RÉGLER LE CONFLIT DE LOIS AU SEIN DE L'UNION?

**83.** Déterminer qu'une situation entre dans le domaine d'application du GDPR ne suffit pas pour connaître précisément l'ensemble des règles relatives à la protection des données personnelles qui s'appliquent à cette situation. En effet, dans chaque état membre, en sus du GDPR, des lois nationales ont été adoptées pour exécuter le règlement (Sous-section 1.). Dès lors, la question qui se pose naturellement est de savoir comment déterminer la loi nationale applicable (Sous-section 2.). Enfin, nous concluons cette section en nous interrogeant sur le caractère impératif du GDPR et des lois nationales qui l'exécutent (Sous-section 3.).

### Sous-section 1. L'exécution normative du GDPR[181]

**84.** Le GDPR n'assure pas une harmonisation complète de la protection des données personnelles au sein de l'Union. Au contraire, différentes dispositions de ce règlement appellent à l'adoption de mesures d'exécution de la part des Etats membres. La situation n'est pas exceptionnelle bien qu'il s'agisse d'un règlement, possédant, en principe, un effet direct[182].

**85.** En premier lieu, comme tout autre acte communautaire, les règles du GDPR s'insèrent dans des ordres juridiques nationaux. Ces derniers sont censés être complets et présenter une cohérence interne, ce qui implique, qu'en ajoutant de nouvelles règles dans ces ordres juridiques nationaux, le règlement risque d'entraîner la modification[183] des règles existantes[184]. Ensuite, dans certains cas, le GDPR impose explicitement aux Etats membres d'adopter des mesures. A titre d'exemple, le règlement prévoit que les Etats membres « concilient, par la loi, le droit à la protection des données à caractère personnel […] et le droit à la liberté d'expression et d'information »[185] ou encore, il impose, à chaque Etat membre, la création d'une autorité nationale[186]. Dans d'autres cas, il s'agit d'une simple faculté des Etats membres de modifier, dans des limites déterminées, la règle prescrite par le règlement. Un Etat *peut*, par exemple, prévoir des dérogations aux droits de la personne concernée lorsque les données personnelles sont traitées à « des fins de recherches scientifiques ou historiques ou à des fins statistiques »[187]. De même, un Etat membre *peut*, par la loi, prévoir qu'un traitement de données, relatif à un enfant et effectué dans le cadre d'une offre directe d'un service de la société de l'information, est licite par le seul consentement de l'enfant, si ce dernier est âgé d'au moins 13 ans[188].

**86.** A plusieurs reprises, le règlement requiert que l'exécution normative passe par un acte législatif. Cette exigence peut également découler de sources distinctes[189] du règlement. Cela signifie donc que les Etats membres doivent adopter des dispositions législatives pour exécuter le GDPR mais, pour ce faire, ils disposent d'une certaine marge de

181. L'expression d'exécution normative d'un règlement a notamment été empruntée à A. THYSEN, « 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, 2003, p. 11.

182. R. KRÁL, « National normative implementation of EC regulations. An exceptional or rather common matter », *European Law Review*, 2008, pp. 243-256; R. SCHÜTZE, *European Constitutional Law*, Cambridge, Cambridge University Press, 2016, p. 92.

183. Ainsi le législateur belge a adopté la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (*M.B.*, 10 septembre 2018, p. 69.589).

184. De telles modifications sont d'autant plus souvent nécessaires que le maintien de règles contraires aux dispositions d'un règlement est constitutif d'un manquement au droit européen par l'Etat membre. Voy. C.J.C.E., 13 juillet 2000, C-160/99, *Commission / France*, EU:C:2000:410. Dans le cas du GDPR, la modification de la législation nationale apparaît incontournable puisque le GDPR reprend des dispositions de la directive n° 95/46. Par conséquent, les lois de transposition de la directive n° 95/46 contiennent des dispositions similaires au GDPR; or si le texte de la directive doit être transposé dans la législation nationale, le texte d'un règlement ne peut être reproduit dans une législation nationale sous peine du compromettre le caractère communautaire du règlement. Les dispositions législatives qui ont transposé la directive devront donc, sauf exception, être abrogées. Voy. à propos de l'interdiction de reproduire le texte d'un règlement dans une loi nationale et son exception, R. KRÁL, *o.c.*, pp. 243-256.

185. Art. 85 du GDPR.

186. Art. 54, 1), du GDPR. Le législateur belge a créé cette autorité par la loi du 3 décembre 2017 portant de l'Autorité de protection des données (*M.B.*, 10 janvier 2018, p. 989).

187. Art. 89 du GDPR.

188. Art. 8, 1., du GDPR. En l'absence d'indication, le GDPR requiert que l'enfant soit âgé d'au moins 16 ans.

189. L'article 84 du GDPR dispose que « les Etats membres déterminent le régime des autres sanctions [que les amendes prévues à l'article 83] applicables en cas de violation du présent règlement ». Les Etats membres sont ainsi libres d'assortir la violation des règles de protection des données personnelles de sanctions pénales, ce qu'a notamment prévu le législateur belge. Dans cette hypothèse, même si, formellement, le règlement n'impose pas que les sanctions pénales soient prévues par une loi, les Etats membres sont tenus de respecter le principe de la légalité des incriminations et des peines, consacré par l'article 15 du pacte international relatif aux droits civils et politiques ainsi qu'à l'article 7 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950.

manœuvre[190]. Par conséquent, les législations d'exécution du GDPR adoptées par les Etats membres diffèrent les unes des autres laissant apparaître un risque de conflits de lois[191].

## Sous-section 2. Le conflit des lois d'exécution

**87.** Les conflits qui pourraient survenir entre les lois nationales d'exécution du GDPR ne trouvent pas de réponse dans le règlement. En effet, à la différence de l'article 4 de la directive n° 95/46, qui avait un statut hybride en ce qu'elle déterminait à la fois le domaine d'application de la directive et la loi de transposition applicable, l'article 3 du GDPR n'indique pas la loi nationale applicable[192]. Le législateur européen, qui s'est focalisé sur l'internationalité externe du GDPR, a ainsi ignoré la dimension interne de l'internationalité du règlement. Désormais, il faut donc se tourner vers d'autres textes pour trouver une réponse au conflit de lois. Nous examinons ci-dessous, en premier lieu, une solution consistant à déterminer la loi nationale de transposition en vertu des textes généraux de droit international privé (§ 1.). En second lieu, nous cherchons une solution par l'application des lois nationales d'exécution (§ 2.). Enfin, nous constatons qu'aucune de ces deux solutions n'offre un résultat pleinement satisfaisant (§ 3.).

### *§ 1. L'application des règles de droit commun*

**88.** Une première solution, pour autant que le litige relève bien de la matière civile et commerciale, serait de déterminer la loi applicable en vertu des règles de conflits de lois de droit commun[193], à savoir le Règlement Rome I en matière contractuelle, et les règles nationales de droit international privé[194] en matière extracontractuelle. Le Règlement Rome II n'est, en effet, pas applicable, puisque son article 1er, point 2., litera g), exclut les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité[195].

### *§ 2. L'application des lois nationales d'exécution*

**89.** Une seconde solution serait de préférer, à ces règles de conflits de lois de droit commun, les règles de conflit de lois contenues dans les lois nationales d'exécution du GDPR, dans la mesure où de telles règles sont adoptées. A cet égard, nous constatons que le législateur néerlandais[196] (1.) et le législateur français[197] (2.) ont inséré une disposition réglant le champ d'application de la loi qu'ils ont adoptée en exécution du GDPR. Le législateur belge a suivi la même démarche (3.).

#### *1) La loi néerlandaise d'exécution du GDPR*

**90.** La loi néerlandaise est très proche de l'article 3 du règlement. Cette loi dispose en son article 5, paragraphe 1er, qu'elle s'applique aux traitements des données personnelles effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant aux Pays-Bas. Dans un second paragraphe, cet article 5, paragraphe 1er, ajoute que la loi néerlandaise s'applique aux traitements de données effectués par un responsable ou un sous-traitant qui n'est pas établi dans l'Union, à condition que la personne concernée se trouve aux Pays-Bas et, que le traitement concerne soit l'offre de bien ou de service faite à cette personne aux Pays-Bas, soit le suivi du comportement de cette personne pour autant qu'il ait lieu aux Pays-Bas.

#### *2) La loi française d'exécution du GDPR*

**91.** En revanche, on ne retrouve pas la même similitude avec l'article 3 du GDPR dans la disposition qui définit le champ d'application de la loi française. Selon son article 5, la loi du 6 janvier 1978 s'applique aux traitements de données personnelles effectués par un responsable établi sur le territoire français, étant entendu qu'un responsable est considéré comme établi sur le territoire français si ce dernier

190. Plusieurs auteurs ont recensé les dispositions du GDPR laissant une marge de manœuvre aux Etats membres, voy. parmi d'autres, J. CHENG, « How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation », *International Data Privacy Law*, 2016, vol. 6, pp. 313-314 et A. BENSOUSSAN (dir.), GENERAL DATA PROTECTION REGULATION: TEXTS, COMMENTARIES AND PRACTICAL GUIDELINES, Mechelen, Wolters Kluwer, 2017, pp. 521-522.

191. A titre d'exemple, en vertu du droit belge, un traitement de données relatif à un enfant et effectué dans le cadre d'une offre directe d'un service de la société de l'information est licite lorsque l'enfant y a consenti s'il est âgé d'au moins 13 ans alors qu'il devrait être âgé d'au moins 15 ans selon le droit français. Voy. pour le droit belge l'art. 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.*, 5 septembre 2018, p. 68.617) et, pour le droit français, art. 7-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.R.F.*, 7 janvier 1978, telle que modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *J.O.R.F.*, 21 juin 2018.

192. F. JAULT-SESEKE et C. ZOLYNSKI, *o.c.*, p. 1875; J. CHENG, « How the best-laid plans go awry … » *o.c.*, p. 311.

193. *Ibid*.

194. Loi du 16 juillet 2004 portant le Code de droit international privé (*M.B.*, 27 juillet 2004, p. 57.344).

195. Règlement (CE) n° 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (*J.O.*, L. 199, 31 juillet 2007, p. 40) (Rome II). Voy. F. JAULT-SESEKE et C. ZOLYNSKI, *o.c.*, p. 1875.

196. Wet van 16 mei 2018, houdende regels ter uitvoering van verordening (EU) n° 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (*PbEU* 2016, L. 119) (uitvoeringswet algemene verordening gegevensbescherming), *Staatsblad van het koninkrijk der Nederlanden*, n° 144, 22 mei 2018.

197. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.R.F.*, 7 janvier 1978, telle que modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *J.O.R.F.*, 21 juin 2018.

exerce sur ledit territoire une activité « dans le cadre d'une installation, quelle que soit sa forme juridique ». Cette disposition fait référence à l'activité du responsable et à l'existence d'une installation sur le territoire français, mais contrairement au GDPR qui exige que le traitement soit effectué dans le cadre des activités de l'établissement localisé sur le territoire de l'Union, il n'y a, ici, aucune exigence de lien entre l'activité de cette installation et le traitement de données. En outre, le législateur français ne fait référence qu'au responsable du traitement et ne vise, dans aucune situation, le sous-traitant.

Dans le paragraphe 2 du même article, le législateur français soumet au droit français le traitement de données, effectué par un responsable qui n'est pas établi sur le territoire de l'Union, mais qui a recours « à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne ». Ce critère d'applicabilité rappelle celui utilisé par la directive n° 95/46 qui a été supprimé dans le GDPR.

Enfin, à la suite de l'entrée en vigueur du GDPR, un nouvel article 5-1 a été inséré dans la loi du 6 janvier 1978[198], complétant son champ d'application. Cette dernière disposition prévoit que « les règles nationales [françaises] prises sur le fondement des dispositions du règlement (UE) n° 2016/679 […] s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France ». L'article 5-1 de la loi française du 6 janvier 1978 fait écho au point 2. de l'article 3 du GDPR. Toutefois, la loi française ne protège pas la personne concernée qui *se trouve* sur le territoire français, mais bien la personne concernée qui *réside* en France et, en outre, elle ne conditionne pas son application à l'existence d'une offre de bien ou de service ou au suivi du comportement de la personne concernée. Le législateur français a également pris soin d'insérer, dans l'article 5-1 de la loi française, une exception lorsqu'il s'agit d'un traitement de données visé à l'article 85, point 2., du GDPR, autrement dit, lorsqu'il s'agit d'un traitement « réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire ». Dans pareil cas, même si la personne concernée réside en France, le traitement de données sera soumis aux « règles nationales […] dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne ».

### *3) La loi belge d'exécution du GDPR*

**92.** Concernant la législation belge, la principale loi d'exécution du GDPR est finalement entrée en vigueur le 5 septembre 2018[199]. A l'instar des lois française et néerlandaise, ce texte contient également une disposition prévoyant son propre champ d'application. L'article 4 de la loi belge adopte une structure similaire à l'article 5 de la loi néerlandaise. Son paragraphe 1er dispose que la loi belge s'applique aux traitements des données personnelles effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire belge. Le paragraphe 2 vise les traitements de données effectués par un responsable ou un sous-traitant qui n'est pas établi sur le territoire de l'Union alors que la personne concernée se trouve sur le territoire belge et que le traitement concerne, soit l'offre de bien ou de service faite à la personne concernée sur le territoire belge, soit le suivi du comportement de cette personne pour autant qu'il a lieu sur le territoire belge. Cet article 4 contient, enfin, un paragraphe 3 selon lequel « par dérogation au paragraphe 1er, lorsque le responsable du traitement est établi dans un Etat membre de l'Union européenne et fait appel à un sous-traitant établi sur le territoire belge, le droit de l'Etat membre en question s'applique au sous-traitant pour autant que le traitement a lieu sur le territoire de cet Etat membre ». Si cette disposition permet d'éviter qu'un même traitement soit soumis simultanément à la loi de l'Etat membre sur le territoire duquel est établi le responsable et à la loi belge, ce qui devrait normalement être le cas du fait de la présence du sous-traitant sur le territoire belge, elle risque d'être difficile à appliquer puisqu'elle nécessite de localiser sur un territoire précis l'acte de traitement qui, par nature, est un acte dématérialisé et donc difficile à localiser.

**93.** La seule lecture de ces trois dispositions nationales permet de supposer que les conflits de lois risquent d'être nombreux dans tous les domaines où le GDPR laisse une marge de manœuvre aux Etats membres. Ce risque sera renforcé si les autorités et les juges des Etats membres adoptent, à l'instar de la C.J.U.E., une interprétation très large du champ d'application de la loi qu'ils sont chargés d'appliquer. En vertu de l'interprétation de la Cour de justice des termes « d'établissement » et de « cadre des activités », un même traitement de données est susceptible d'entrer dans le cadre des activités d'un établissement du responsable situé sur le territoire belge ainsi que dans le cadre des activités d'un établissement du responsable situé aux Pays-Bas et, de surcroît, il se peut que le responsable soit établi, au sens de

198. L'art. 5-1 a été inséré par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *J.O.R.F.*, 21 juin *2018*.

199. 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. 68.617). Le législateur belge a assuré l'exécution normative du règlement par deux autres lois, elles aussi désormais entrées en vigueur, à savoir la loi du 3 décembre 2017 portant de l'Autorité de protection des données (*M.B.*, 10 janvier 2018, p. 989) et la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (*M.B.*, 10 septembre 2018, p. 69.589).

la loi française, sur le territoire français ou que la personne concernée réside en France. *A priori*, une telle situation entre dans le champ d'application de chacune des trois lois nationales examinées ci-dessus et, force est de constater que, en l'état actuel, aucune règle n'est expressément prévue pour régler les conflits pouvant survenir entre ces lois nationales.

### *§ 3. L'absence d'une solution satisfaisante*

**94.** La question demeure de savoir laquelle des deux solutions – entre l'application du droit commun ou des lois d'exécution – il faut retenir. En matière extracontractuelle, la seconde solution nous paraît s'imposer puisqu'à défaut d'harmonisation européenne en la matière, ce sont les règles nationales qui s'appliquent. Dans le cas de la Belgique, en attendant l'adoption de la loi d'exécution du GDPR, la seule disposition qui semblait pouvoir offrir une solution était l'article 99 du Code de droit international privé. Cette dernière disposition laisse désormais place à la règle d'applicabilité contenue dans la loi d'exécution belge du GDPR.

**95.** En matière contractuelle, la réponse est moins évidente. Le choix du Règlement Rome I pour trancher le conflit de lois pourrait se justifier au regard du principe de primauté du droit européen sur le droit national des Etats membres. Cependant, les dispositions de droit national dont il est question sont des dispositions d'exécution d'un règlement et l'article 23 du Règlement Rome I prévoit que ledit règlement « 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 ». La question revient donc à se demander si, au titre de loi d'exécution d'un règlement, la loi nationale pourrait s'appliquer par priorité au règlement sur base de l'article 23 du Règlement Rome I.

**96.** Dans tous les cas, il nous faut remarquer que le règlement du conflit de lois par application des lois nationales d'exécution du GDPR serait pour le moins insatisfaisant. Pour reprendre un exemple déjà cité, le GDPR prévoit qu'un traitement de données, relatif à un enfant et effectué dans le cadre d'une offre directe d'un service de la société de l'information, est licite lorsque l'enfant est âgé d'au moins 16 ans. Le règlement précise, toutefois, que les Etats membres peuvent abaisser cette limite à 13 ans. Ainsi la France a fixé cet âge à 15 ans et la Belgique à 13 ans[200]. Par conséquent, un opérateur dont le seul établissement se situe en Belgique et qui collecte, dans le cadre d'une offre de services de la société de l'information, des données sur des enfants âgés de moins 15 ans résidant en France, est placé dans une situation particulièrement mal aisée. En effet, en vertu du droit français, applicable dès lors que la personne concernée réside en France, ce traitement est illicite. En revanche, en vertu du droit belge, dont l'application se justifie par la localisation de l'établissement, ce traitement est licite.

**97.** La détermination de la loi applicable en vertu du Règlement Rome I n'est pas non plus entièrement satisfaisante. S'il est vrai que les règles de rattachement dudit règlement permettent d'identifier une loi applicable et, partant, d'éviter les conflits de lois, l'application du Règlement Rome I aux litiges en matière de données personnelles risque de soulever certaines questions de qualification particulièrement délicate: un litige en matière de protection des données relève-t-il de la matière civile et commerciale? Est-il relatif à une obligation contractuelle? De surcroît, le Règlement Rome I favorise, au travers de dispositions spécifiques, certaines catégories de personne. Or, le GDPR entend être un règlement général offrant un même niveau de protection à la personne concernée, peu importe son statut.

**98.** En bref, la situation actuelle est problématique: non seulement il n'est pas possible d'identifier une solution claire, mais surtout, aucune des solutions possibles ne paraît être entièrement satisfaisante.

## Sous-section 3. La loi de police comme solution?

**99.** Le caractère impératif des normes en cause peut, en pratique, s'avérer crucial au moment de déterminer la loi applicable. Bien que la question ne soit pas définitivement tranchée[201] ni à l'égard du règlement ni concernant les lois d'exécution, plusieurs arguments permettent de considérer ces dernières comme des lois de police au sens de l'article 9 du Règlement Rome I. Ainsi, nous pouvons notamment relever que tant le GDPR que les trois lois nationales examinées déterminent leur propre champ d'application, qu'elles concrétisent la protection d'un droit fondamental et que leur application est assurée par une autorité publique indépendante, ce qui laisse penser que ces règles poursuivent bien la sauvegarde d'un intérêt public. En revanche, la place laissée dans le GDPR au consentement de la personne concernée pourrait indiquer que les articles de ce règlement ne sont pas des dispositions impératives. En effet, le consentement de la personne concernée est présenté comme la première base juridique autorisant un responsable à traiter des données personnelles[202]. Il est également cité comme le premier motif permettant de déroger à la fois à l'interdiction de traiter des données personnelles appartenant aux catégories particulières mentionnées par l'article 9[203] ainsi qu'à l'interdiction de

200. Voy. pour la Belgique, art. 7 loi du 30 juillet 2018, *o.c.* et pour la France, art. 7-1 loi du 6 janvier 1978, *o.c.*
201. M. BRKAN, « Data Protection and Conflict-of-laws: A Challenging Relationship », *E.D.P.L.*, 2016, p. 333.
202. Art. 6, 1., a), du GDPR.
203. Art. 9, 2., a), du GDPR.

transférer des données personnelles vers un pays tiers sans décision d'adéquation ou garanties appropriées[204].

**100.** En l'absence d'une disposition ou d'une tendance prétorienne claire consacrant le caractère impératif des règles relatives à la protection des données, il semble impossible d'affirmer avec certitude que le GDPR ou les lois nationales d'exécution revêtent bien un caractère impératif, même si cette conclusion est, selon nous, la plus logique. Notons, toutefois, que l'absence d'une disposition explicite en ce sens n'implique pas que les règles relatives à la protection des données soient dépourvues du caractère impératif[205].

**101.** Ceci étant, si la loi d'exécution du GDPR d'un Etat membre devait effectivement être qualifiée de loi de police, le juge relevant de cet Etat membre serait en mesure d'appliquer cette loi, sans avoir égard aux règles de conflit de lois de droit commun. En quelque sorte, la notion de loi de police apparaît comme une troisième solution pour déterminer la loi applicable, mais cette dernière rend la détermination du juge compétent particulièrement décisive[206].

## CONCLUSION

**102.** Sous le régime de la directive n° 95/46, l'article 4, qui déterminait son domaine d'application, était déjà considéré comme l'une des dispositions les plus compliquées et controversées de cette directive[207]. Devenue l'article 3 dans le GDPR, cette disposition ne s'appréhende pas plus facilement et soulève, à son tour, son lot d'interrogations.

**103.** En premier lieu, à l'instar de la directive n° 95/46, l'article 3 du GDPR mobilise des notions, comme le traitement ou les données à caractère personnel, nécessitant les lumières de la Cour de justice. Cette dernière a interprété systématiquement le domaine d'application de la protection des données personnelles de manière large. Une telle interprétation a engendré des critiques, en particulier d'opérateurs et de politiciens américains qui qualifient le GDPR d'acte extraterritorial. En réalité, à défaut de trouver une base juridique solide, ces critiques appartiennent plutôt à la sphère politique. Cependant, elles manifestent l'existence d'un malaise qui devrait, à notre sens, pousser l'Union européenne à examiner d'autres pistes, d'autant plus qu'une solution plus efficace et consensuelle pourrait en découler.

**104.** En second lieu, contrairement à l'article 4 de la directive cette fois, le GDPR n'établit aucune règle permettant de déterminer la loi applicable. En effet, le législateur européen a, dans le cas de ce règlement, ignoré l'internationalité interne du droit de l'Union. Ce faisant, il permet, ou plutôt oblige, chaque Etat membre à déterminer le champ d'application des règles nationales qu'ils adoptent ce qui augmente le risque de conflit de lois et complique la tâche des responsables et sous-traitants. Ceux-ci, en l'absence d'une solution claire au conflit de lois, sont, de fait, contraints d'examiner chaque loi nationale et d'évaluer si leurs activités tombent dans leur domaine d'application.

**105.** Au vu de cette dernière observation, le constat est nécessairement mitigé au moment d'apprécier l'harmonisation opérée par l'adoption du GDPR du point de vue du conflit de lois. S'il est indéniable que ce règlement apporte une harmonisation matérielle bien venue, il est, en revanche, manifeste que l'absence d'harmonisation au niveau du conflit de lois nationales constitue un sérieux obstacle à la libre circulation des données personnelles dans l'espace économique européen. En conclusion, il n'est pas certain que le GDPR tel qu'il existe actuellement, sans règle de conflit de lois, permette « de réduire la fragmentation juridique et d'apporter une plus grande sécurité juridique »[208].

---

204. Art. 49, 1., a), du GDPR.
205. C.J.C.E., 9 novembre 2000, C-381/98, *Ingmar*, EU:C:2000:605. Dans cette affaire, bien que la directive en cause ne donnait aucune indication explicite sur son éventuel caractère impératif, la Cour de justice a déduit, des objectifs et du texte de cette directive, son caractère impératif.
206. Voy. à ce sujet les articles 78 et 79 du GDPR qui énoncent des règles de conflits de juridictions.
207. L.A. BYGRAVE, *Data Privacy Law: An International Perspective*, Oxford, Oxford University Press, 2014, p. 99 cité par D.J.B. SVANTESSON, « The CJEU'S Weltimmo data privacy ruling – Lost in the Data Privacy Turmoil, Yet So Very Important », *Maastricht Journal of European and Comparative Law*, 2016, vol. 2, p. 334; J. CHENG, « How the best-laid plans go awry … » *o.c.*, p. 311.
208. 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), COM(2012) 11 final, Bruxelles, 25 janvier 2012, p. 6.