

L'applicabilité de la protection européenne des données personnelles : interrogeons Google !

Mémoire réalisé par
Nikitas MICHAÏL

Promoteur(s)
Stéphanie FRANÇOIS

Année académique 2015-2016
Master en droit

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une oeuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

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

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

Introduction

« Les inventions et méthodes commerciales récentes attirent l'attention sur la nécessité de franchir une nouvelle étape dans la protection des personnes [...] ». En effet, « les photographies instantanées et la presse, ont envahi l'enceinte sacrée de la vie privée et domestique »¹. Un tel constat s'avère singulièrement actuel, et pourtant ces phrases ont été rédigées en 1890. C'est bien la preuve que la question de la protection des données personnelles n'est pas neuve et préoccupe les personnes depuis bien longtemps, alimentant leurs craintes et leurs prédictions.

La réglementation protégeant les données personnelles répond ainsi à un besoin réel de la population et, constitue, de surcroît, un des enjeux majeurs pour le développement futur du marché intérieur². En outre, cette problématique évolue sans cesse, suivant le rythme effréné des avancées technologiques, ce qui rend la tâche du législateur particulièrement ardue. En effet, ce dernier n'est pas en mesure d'anticiper les développements technologiques à venir lorsqu'il adopte un instrument destiné à protéger les données personnelles ce qui crée un décalage permanent entre le cadre juridique et la réalité. La directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données³ en constitue un exemple flagrant puisqu'elle fut très vite dépassée par l'émergence d'internet et ce retard n'a fait qu'augmenter tant les évolutions en matière de technologie et de communication ont été nombreuses au cours des deux dernières décennies. Toutefois, cette directive demeure toujours en vigueur à l'heure actuelle malgré vingt années de (r)évolution numérique, et il faudra encore attendre deux ans avant de la voir disparaître au profit du règlement récemment adopté par les institutions européennes⁴.

Le législateur européen n'est pas le seul à avoir amorcé une réforme de la réglementation à propos des données personnelles. Il s'agit, effectivement, d'une tendance qui s'observe également sein du Conseil de l'Europe ainsi que dans de nombreux Etats tiers, qui, pour certains, ne révisent pas mais adoptent leur premier texte relatif à la protection des données personnelles, preuve encore de l'intérêt croissant que suscite cette matière⁵. Toutefois, même si la protection des données personnelles connaît un développement mondial, l'Union européenne reste un terrain privilégié pour l'étudier étant donné que les standards de protection des données personnelles y sont élevés et que cette protection fait l'objet d'une

¹ S. D. WARREN and L. D. BRANDEIS, « The Right to Privacy », *Harvard Law Review*, 1890, Volume 4, p. 193. « Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops" »

² Particulièrement s'agissant du marché digital. Voy. V. REDING, « The European data protection framework for the twenty-first century », *International Data Privacy Law*, 2012, Volume 2, p. 124.

³ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE*, 1995, L 281/31 (ci-après directive « données personnelles »).

⁴ Le règlement sera applicable à partir du 25 mai 2018. Voy. Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après règlement général sur la protection des données ou RGPD), *JOUE*, 2016, L 119/1, article 94, §1 et 99, §2.

⁵ C. GAYREL et R. ROBERT, « Proposition de règlement sur la protection des données - Premiers commentaires », *Journal de droit européen*, 2012, p. 173 ; M. TAYLOR, « The EU's human rights obligations in relation to its data protection laws with extraterritorial effect », *International Data Privacy Law*, 2015, Volume 5, pp. 246-248 ; C. KUNER, F. CATE, C. MILLARD et D. SVANTESSON, « Editorial : The extraterritoriality of data privacy laws—an explosive issue yet to detonate », *International Data Privacy Law*, 2013, Vol. 3, No. 3, p. 147.

longue tradition sur le Vieux Continent⁶. Du reste, il paraît indéniable que la législation européenne en la matière influence celle des Etats tiers⁷.

Toutefois, si la protection des données personnelles a depuis longtemps fait l'objet de l'attention de divers acteurs juridiques, ce n'est pas le cas de la question particulière concernant le domaine d'applicabilité des dispositions qui consacrent cette protection, et ce malgré la mondialisation et l'apparition d'internet⁸. Certains prédisent ainsi que la question de l'applicabilité de la réglementation des données personnelles va s'affirmer comme l'une des problématiques de premier plan en matière de droit international privé⁹. Cette « prophétie » a commencé à se réaliser, d'abord timidement et singulièrement avec l'affaire *Lindqvist*¹⁰ et, ensuite, plus largement avec l'affaire *Google Spain*¹¹.

Cette dernière affaire constitue d'ailleurs l'axe principal de cette étude. En effet, il s'agit d'une décision d'une ampleur inédite en droit européen de la protection des données personnelles, qui intervient en même temps que la réforme de la directive « données personnelles » et qui met particulièrement en lumière les lacunes de la directive en matière d'applicabilité. En outre, la configuration du cas d'espèce mérite également une attention particulière en raison de l'organisation adoptée par Google, à savoir un siège établi aux Etats-Unis et des bureaux de promotion en Europe, et de son « rôle » d'amplificateur dans la diffusion des informations, qui sont des éléments communs à d'autres opérateurs et qui pourraient aisément être le cadre d'autres litiges. C'est donc tout naturellement que nous commencerons le titre premier par un bref rappel des faits de cette affaire, ce qui nous permettra également de définir plus en avant la problématique de l'applicabilité concernant la directive « données personnelles ». Ensuite, dans la seconde partie du premier titre, nous commencerons l'analyse à proprement parler du texte de la directive « données personnelles » en examinant ses objectifs et sa base légale au regard de son domaine d'applicabilité.

Le deuxième titre sera consacré à l'étude détaillée des articles de la directive définissant son domaine d'applicabilité. Nous y étudierons l'ensemble des notions auxquelles la directive a recours pour déterminer dans quelle mesure elle entend s'appliquer et nous remarquerons que, malgré une interprétation subtile, l'articulation des dispositions de la directive n'est pas irréprochable. Ce sera aussi l'occasion de revenir de façon plus critique sur l'affaire *Google Spain* et d'analyser les conséquences de l'interprétation que la Cour fait des dispositions de la directive. Une fois le domaine d'applicabilité de la directive « données personnelles » précisé, il nous faudra observer la façon dont cette directive résout le conflit de lois de transposition, dans la mesure où le législateur européen a choisi de régler cette question et celle de l'applicabilité de la directive dans la même disposition. Par conséquent, nous ne pouvons pas sérieusement nous intéresser à l'interprétation et à l'application des dispositions relatives à l'applicabilité de la directive sans nous préoccuper des conséquences sur la solution du conflit de lois de transposition. Nous clôturerons ce deuxième titre par quelques considérations sur l'harmonisation des lois nationales résultant des transpositions respectives de la directive « données personnelles ».

⁶ M. TAYLOR, *op. cit.*, pp. 246-248.

⁷ D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *Stanford Journal of International Law's*, 2014, p. 61.

⁸ C. KUNER, F. CATE, C. MILLARD et D. SVANTESSON, *op. cit.*, p. 147.

⁹ *Ibidem*, p. 147.

¹⁰ CJCE, 6 novembre 2003, aff. C-101/01, *Procédure pénale c. Bodil Lindqvist*, *Rec.*, 2003, p. I-12971.

¹¹ CJUE, 13 mai 2014, aff. C-131/12, *Google Spain et Google*, *Rec.*, 2014, p. I-317. (ci-après arrêt *Google Spain*)

Le troisième et dernier titre de ce travail sera l'occasion de nous pencher sur le règlement adopté par le législateur européen, qui viendra remplacer la directive dans quelques mois. Il nous faut, toutefois, noter qu'ayant été adopté récemment et n'étant pas encore en vigueur, ce règlement n'est éclairé par aucune jurisprudence et les commentaires restent encore très prospectifs. Nous analyserons, du point de vue de l'applicabilité, le choix de refondre la réglementation concernant la protection des données personnelles dans un règlement et la volonté du législateur européen d'adopter un cadre légal global. Enfin, nous examinerons les différences entre les critères d'applicabilité de la directive et ceux du règlement en nous interrogeant sur la capacité de ces derniers à apporter une solution plus claire à l'égard de l'affaire *Google Spain*.

Titre 1. Le cadre de l'applicabilité et les objectifs de la directive 95/46

Dans un premier temps, nous nous intéresserons de manière générale à la problématique de l'applicabilité que nous tenterons de concrétiser au travers de l'affaire *Google Spain* (chapitre 1). Ensuite, nous d'examinerons les objectif de la directive « données personnelles » (chapitre 2)

Chapitre 1. La définition de la problématique au travers de l'arrêt *Google Spain*

Nous entamons ce premier chapitre par un bref rappel des faits et du raisonnement final de la Cour dans l'affaire *Google Spain* (Section 1) de manière à illustrer concrètement la question de l'applicabilité que nous définirons ensuite (Section 2).

Section 1. *Google Spain* : Faits et raisonnement de la Cour

L'arrêt *Google Spain* de la Cour de justice de l'Union européenne abondamment commenté par la doctrine¹² a été qualifié de décision majeure¹³ par les uns, d'audacieuse¹⁴ par les autres. Cet intérêt considérable résulte, en partie de l'impact mondial et du caractère nouveau de cette affaire dans laquelle la Cour a été amenée à se prononcer sur la protection des données personnelles dans le cadre de l'utilisation d'internet. En effet, cet arrêt met en lumière, pour la première fois dans un contexte véritablement mondial, l'applicabilité de la réglementation en matière de données personnelles et illustre les difficultés qui en résultent. C'est pour cette raison que nous avons décidé d'entamer cette étude par la présentation de cette affaire¹⁵.

Les faits qui donnent lieu à l'arrêt précité se sont produits en Espagne. Un citoyen espagnol introduit auprès de l'Agence espagnole de protection des données (AEPD) une demande visant la suppression de certains liens proposés à la suite d'une recherche sur *Google*, effectuée à partir de son nom. Ces liens menaient vers le site internet d'un journal espagnol, *La Vanguardia Ediciones*, et plus particulièrement vers un article paru en 1998 relatant des faits survenus exclusivement en Espagne. En outre, une demande est également dirigée contre le journal en question, visant à supprimer la page vers laquelle les liens contestés renvoyaient. Finalement seule la requête concernant *Google Inc.* et sa filiale espagnole, *Google Spain*, fut favorablement accueillie par l'agence espagnole. Cette décision sera contestée par *Google* et *Google Spain* devant une juridiction espagnole et c'est dans le cadre de ce litige que la Cour de justice rendra une décision préjudicielle en grande chambre, concernant l'applicabilité de la directive « données personnelles ». Précisons, au surplus, que *Google Inc.* est établi aux Etats-Unis à partir d'où il opère le traitement de données pour son service de moteur de recherche, et que *Google Spain* est localisé en

¹² C. KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *LSE Law, Society, and Economy Working Paper Series*. ed. London : London School of Economics and Political Science, n°3, 2015, p.13.

¹³ E. CRUYSMANS et A. STROWEL, « Un droit à l'oubli face aux moteurs de recherche - droit applicable et responsabilité pour le référencement de données inadéquates non pertinente ou excessives », *Journal des tribunaux*, 2014, p. 457.

¹⁴ L. MARINO « Un 'droit à l'oubli' numérique consacré par la CJUE », *La semaine juridique*, p. 1300.

¹⁵ C. KUNER, « *Google Spain* in the EU and international context », *Maastricht Journal of European and Comparative Law*, 2015, p. 163.

Espagne où il réalise la promotion et la vente des espaces publicitaires disponibles sur le site web de *Google*.

Dans le cadre de ce litige, plusieurs questions sont soumises à la Cour concernant l'interprétation des notions de la directive « données personnelles » afin de déterminer *in fine* si cette dernière est applicable au cas d'espèce soumis à la juridiction espagnole. En effet, il s'agit d'une question dont la portée pratique est primordiale car s'il s'avérait que la situations présentée sort du champ d'application de la directive, les dispositions de celle-ci devraient purement et simplement être écartées¹⁶.

A priori, à la simple lecture des faits, une intuition légitime amène à penser que la directive « données personnelles » s'applique au cas présent étant donné la proximité des faits avec l'Union européenne. Les faits se sont déroulés sur le territoire de l'Union, concernent un citoyen espagnol, sont relatés par un journal espagnol et indexés sur son site internet. D'ailleurs la Cour arrive au même résultat. En effet, après avoir jugé que les activités du moteur de recherche consistaient en un traitement de données¹⁷ au sens de la directive, la Cour de justice a considéré que le traitement est effectué dans le cadre des activités de *Google Spain*¹⁸. Ce fut également la position de la Commission européenne¹⁹.

A l'inverse, pour éviter l'application de la loi de transposition espagnole, *Google Inc* défendait l'idée que sa filiale espagnole était étrangère au traitement de données du citoyen espagnol en cause, et que, dès lors, le critère d'applicabilité de la directive n'était pas satisfait²⁰. Cette dernière position, rejetée par la Cour, a pourtant trouvé les faveurs d'une juridiction française²¹ et d'une partie de la doctrine²². Au vu de ces différentes positions et de l'intérêt pratique de la question, il paraît opportun de s'interroger sur l'applicabilité de la directive.

Pour l'heure, force est de constater que selon l'interprétation de la Cour, *Google Inc*, bien qu'établi aux Etats-Unis, est soumis au régime de la directive « données personnelles » au travers des activités de promotion et de vente de sa filiale espagnole. Si nous nous essayons à une généralisation du cas d'espèce présent, et du raisonnement de la Cour, cela revient à s'interroger sur la situation suivante : une société opère un service internet à partir d'un Etat tiers dans lequel elle est établie, mais dispose de bureaux (de promotion, de vente, etc.) dans un ou plusieurs Etats membres dont les activités sont « indissociablement

¹⁶ M. FALLON et J. BERGE, « Marché intérieur et Espace de liberté sécurité justice : la dimension spatiale des espaces », *Les petites affiches*, n°112, 2010, p.8.

¹⁷ CJUE, 13 mai 2014, aff. C-131/12, *Google Spain* et *Google*, *op. cit.*, points 27 et 28. A l'inverse de la Cour, Google contestait que ses activités puissent être qualifiées de traitement de données au sens de la directive données personnelles et, qu'au surplus, Google puisse être considéré comme le responsable du traitement de ces données. Ces notions seront détaillées par la suite, il s'agit ici de souligner la problématique de l'applicabilité avant de s'interroger sur le critère de rattachement.

¹⁸ CJUE, 13 mai 2014, C-131/12, *Google Spain* et *Google*, *op. cit.*, points 55 et 56.

¹⁹ CJUE, 13 mai 2014, C-131/12, *Google Spain* et *Google*, *op. cit.*, point 47.

²⁰ CJUE, 13 mai 2014, C-131/12, *Google Spain* et *Google*, *op. cit.*, point 51.

²¹ Dans une affaire concernant Google et les forums Usenet, le Tribunal de grande instance de Paris a considéré « que la promotion directe de produits et services et la mise en oeuvre de centres de traitement de l'information, ne démontre pas que cette société [Google France] intervient dans le processus de traitement des données personnelles qu'implique le fonctionnement du service d'archivage considéré » et « que la requérante ne démontre pas en réalité que la société Google Inc. est établie en France ou utilise pour l'archivage litigieux les moyens, matériels ou humains, de la société Google France, ou de tout autre entité située sur le territoire français, autrement qu'à des fins de transit ». Voy. T.G.I. Paris, ord. réf., 14 avril 2008, disponible sur http://www.legalis.net/jurisprudence-decision.php3?id_article=2311, (Consulté le 8 juillet 2016).

²² B. HARDY, « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *Revue trimestrielle de droit européen*, 2014, p. 887. qui estime qu'il ne s'agit pas d'un traitement de données « effectué dans le cadre des activités » de l'établissement de Google Spain.

liées »²³ avec l'établissement principal et, à ce titre, se voit imposer comme droit applicable le droit de l'Union européenne²⁴. C'est en gardant à l'esprit cette situation²⁵ que nous examinerons de manière plus générale la question de l'applicabilité de la directive « données personnelles ».

Du reste, cet arrêt revêt également une importance considérable concernant le « droit à l'oubli ». Toutefois, ce droit, pour autant qu'il existe en de tels termes, ne constitue pas le sujet de présent travail qui se limite à l'applicabilité de la directive en question.

Section 2. L'applicabilité : une question problématique mais déterminante

Il convient ici de baliser l'objet de cette étude en précisant d'abord les aspects de l'applicabilité que nous allons étudier (paragraphe 1) et de les distinguer d'autres notions qui peuvent également conditionner l'application d'une règle juridique (paragraphe 2). Enfin, dans cette section, nous débiterons l'analyse de la directive « données personnelles » en évoquant certains choix majeurs opérés par le législateur européen pour définir l'applicabilité de cette directive (paragraphe 3).

§1. L'applicabilité dans sa dimension spatiale

Une norme juridique s'applique toujours à une situation qui est définie dans le temps et dans l'espace et, partant, implique de prendre en compte un nombre considérable de situations influencées par des facteurs spatiaux et temporels. Bien que la question de la temporalité dans l'application des règles relatives à la protection des données personnelles revête une importance croissante²⁶, c'est la question du champ d'application spatial de la directive qui retient notre attention ici et nous limitons donc notre étude à ce qui peut être qualifié de dimension spatiale de l'applicabilité des règles européennes relatives aux données personnelles. En d'autres termes, c'est la manière dont la directive délimite dans l'espace les situations auxquelles elle entend s'appliquer qui va constituer l'objet de nos commentaires.

Ceci dit, cela ne signifie pas que nous allons nous concentrer uniquement sur les aspects territoriaux de l'application des règles européennes. En effet, il est traditionnellement admis qu'outre l'aspect spatial et temporel, le champ d'application d'une règle de droit dispose également d'un aspect personnel et matériel²⁷. En outre, il nous faut dès à présent souligner qu'identifier le territoire de l'Union européenne²⁸ ne suffit pas à régler la question de l'applicabilité des normes de droit communautaire²⁹, en particulier de la directive

²³ CJUE, 13 mai 2014, aff. C-131/12, *Google Spain* et *Google*, *op. cit.*, point 56.

²⁴ Nonobstant la généralisation à laquelle nous nous essayons, cette présentation des faits reste subjective et s'inscrit dans la perspective de l'opérateur. En effet, il est également possible de résumer la situation en partant de la perspective de la personne concernée et considérer ainsi que des données personnelles d'un résident européen, concernant des faits localisés en Europe, ont été traitées par un opérateur établie dans un état tiers et que ce traitement est régie par les règles européenne en matière de protection des données personnelles.

²⁵ La configuration de Google est loin d'être exceptionnelle parmi les sociétés qui opèrent un service internet et pourrait constituer le cadre de litiges européens ultérieurs en matière de protection des données. Pour ne citer qu'elle, Facebook utilise un modèle très similaire, établie aux Etats-Unis, le réseau social dispose également de bureaux de promotion en Europe. Sur l'organisation de Facebook, voy. J. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *Revue européenne de droit de la consommation*, 2010, p. 236-239.

²⁶ Notamment la problématique de la conservation des données personnelles de manière permanente pour des utilisations ultérieures.

²⁷ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, Bruylant, 2005, p.8. Comme l'auteur le précise, il s'agit d'une distinction artificielle qui n'est pas absolu et, partant, il se peut qu'un critère revêt simultanément un caractère spatial et personnel.

²⁸ En effet, les article 52 TUE et 355 TFUE précisent le territoire de l'Union mais ces articles ne suffisent pas à définir le domaine d'applicabilité des actes de droit européen.

²⁹ M. FALLON et J. BERGE, *op. cit.*, p.6.

« données personnelles ». Précisons que cette affirmation nécessite au surplus de distinguer l'applicabilité d'une norme de sa force obligatoire.

§2. L'applicabilité et la force obligatoire

Tant la force obligatoire que l'applicabilité ont une dimension spatiale et influencent l'application de la norme dans l'espace. Toutefois, afin d'appréhender correctement l'applicabilité d'une norme dans sa dimension spatiale, il convient de la distinguer de la force obligatoire, et ce principalement au niveau des destinataires et de la portée territoriale³⁰.

La force obligatoire d'une norme ne s'adresse qu'aux destinataires dits « *institutionnels* »³¹ qui ont la charge, dans un état donné, d'appliquer les normes adoptées par cet état. En outre, la force obligatoire d'une norme ne la rend obligatoire en tant que telle pour les autorités sur le territoire de l'état qui a adopté cette norme.

En revanche, l'applicabilité d'une norme concerne les destinataires dits « *finaux* »³², ce qui peut inclure les institutions³³ mais pas uniquement puisqu'il s'agit, en réalité, de toutes les personnes dont le comportement entend être régulé par la norme en question. Ainsi l'applicabilité de la norme n'est pas limitée au territoire³⁴ d'un état, où en l'occurrence au territoire de l'Union européenne, et peut donc viser des situations localisées à l'extérieur de ce territoire, sans toutefois obliger les autorités étrangères à appliquer la norme.

Par conséquent, une règle peut viser des situations localisées à l'étranger (applicabilité) mais ne sera appliquée en tant que telle que dans l'état dont elle émane (force obligatoire). Concrètement, si la force obligatoire d'une règle de droit européen ne peut franchir les frontières du territoire de l'Union européenne, cela implique que les autorités européennes ne peuvent pas ordonner ou vérifier l'application d'une telle règle au-delà des frontières de l'Union. Il faut donc constater que « *les vellétés d'application extraterritoriale véritable d' [une norme européenne] sont soumises au bon vouloir d'un législateur étranger* »³⁵ et surtout que « *rien n'assure au législateur [européen] que des opérateurs étrangers localisés sur le territoire d'un pays étranger [...] respectent les principes qu'il souhaite leur imposer* »³⁶. Toutefois, comme nous l'avons souligné, l'applicabilité peut s'étendre bien au-delà du territoire européen et cette dernière hypothèse amène parfois à parler d'extraterritorialité ou d'application extraterritoriale. C'est notamment le cas lorsqu'il est question de la directive « données personnelles » et particulièrement dans l'arrêt *Google*, qui concerne un opérateur établi aux Etats-Unis. Il convient, dès lors, de s'interroger sur cette notion d'extraterritorialité.

³⁰ Sur la distinction entre force obligatoire et applicabilité, Voy. S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 50 et s.

³¹ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 52.

³² *Ibidem*, p. 52.

³³ En effet, certaines normes visent à réguler le comportement des autorités publiques qui sont alors obligées d'appliquer la norme et d'adapter leur comportement à ce que cette dernière prescrit.

³⁴ M. FALLON et J. BERGE, *op. cit.*, p. 6.

³⁵ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 272.

³⁶ *Ibidem*, p. 6. Cela revient à observer qu'il ne semble pas exister de prétention qui permettrait justifier qu'un ordre juridique soit contraint de se plier au respect du champ d'application défini unilatéralement d'une règle émanant d'un autre ordre juridique.

§3. L'applicabilité et l'extraterritorialité

L'application « extraterritoriale » d'une norme communautaire vise la situation dans laquelle cette norme est amenée à être appliquée comme telle à des parties situées en dehors du territoire de l'Union³⁷. En d'autres mots, le phénomène ainsi visé est celui par lequel le législateur européen détermine unilatéralement que la règle qu'il édicte va s'appliquer à des personnes physiques ou morales établies dans des états tiers. Il s'agit en réalité d'un phénomène qui touche plusieurs domaines du droit européen et qui va de pair avec le développement du marché intérieur³⁸. Cette tendance est encore plus marquée lorsqu'il est question d'activités associées à l'émergence d'internet puisque la création de ce réseau international de communication a démultiplié de façon inédite, les possibilités d'interaction entre les opérateurs non-communautaires, d'une part, et, les citoyens et opérateurs européens, d'autre part³⁹. La protection des données personnelles est un domaine qui illustre donc particulièrement la nécessité d'une définition extraterritoriale de l'applicabilité des règles européennes, puisqu'à défaut l'Union ne serait pas en mesure d'assurer une protection effective des données personnelles des citoyens européens vis-à-vis des opérateurs étrangers⁴⁰.

Ce constat appelle deux observations. La première concerne l'absence, en droit international, de règle, de principe ou de coutume, qui proscrie ou limite une définition extraterritoriale de l'applicabilité d'une norme⁴¹. Du reste, la Cour de justice précisa que pareille interdiction ou limite n'existe pas non plus dans les Traités⁴². Cependant, il convient de relever qu'en matière de données personnelles certains auteurs qualifient de problématique, voire d'inacceptable, l'extraterritorialité qui caractérise la réglementation européenne, en précisant qu'une application sur le plan mondial de la législation européenne est irréaliste⁴³. Cette dernière affirmation nous amène à formuler notre deuxième observation. En effet, comme nous venons de le constater⁴⁴, l'application du droit communautaire au-delà des frontières de l'Union ne dépend pas exclusivement de la volonté unilatérale du législateur européen. Ceci nous amène à nuancer quelque peu, en tout cas en pratique, la distinction dressée ci-avant, entre l'applicabilité et la force obligatoire, et, à relativiser le caractère extraterritorial qui peut qualifier l'application des normes européennes. De fait, les pouvoirs des institutions européennes, tout particulièrement celui de contrainte, ne pouvant s'exercer au-delà des frontières européennes, les conséquences d'une application, ou plutôt d'une définition d'un domaine d'application extraterritoriale, doivent être relativisées⁴⁵.

³⁷ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 172-173.

³⁸ H. DE VERDELHAN, « Chronique de jurisprudence : Introduction générale », *Revue internationale de droit économique*, 2016, p.35.

Comme le remarque l'auteur, les entreprises étrangères sont de plus en plus présentes sur le marché intérieur ce qui pose la question de l'application du droit européens à leur égard dans de nombreux domaines tels que le droit de la consommation, le droit du travail, le droit du transport, le droit de la concurrence, le droit bancaire et financier, la protection des données personnelles, etc.

³⁹ *Ibidem*, p. 35.

⁴⁰ D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », op. cit., p. 55.

⁴¹ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 80, pp. 160-162, p. 167 et p. 173.

⁴² CJCE, 15 novembre 1994, Avis 1/94, Rec., 1994, p. I-5267, point 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 à l'égard des pays tiers ni de prescrire les attitudes à prendre par les États membres vis-à-vis de l'extérieur ».

⁴³ 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, Volume 1, p. 29 ; D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », op. cit., p. 59.

⁴⁴ Voy. *supra*, p. 8.

⁴⁵ D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », op. cit., pp. 94 et s. ; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 237-238, à propos de règlement en matière de transport.

De plus, il s'avère que l'application des normes européennes demeure liée à un élément localisé dans l'Union européenne. Par conséquent, l'application extraterritoriale dont il est question nécessite l'existence d'un certain degré de proximité entre la situation en question et l'Union européenne. Il convient donc également de constater que si l'applicabilité de la norme européenne n'est pas limitée par les frontières communautaires, un lien étroit existe entre l'applicabilité extraterritoriale et le territoire de l'Union ce qui le qualifie d'extraterritorial⁴⁶.

Des considérations qui précèdent, la conclusion suivante s'impose : « *l'affirmation d'un domaine véritablement extraterritorial est parfaitement valide mais n'est pas pour autant efficace* »⁴⁷ au-delà du territoire communautaire. C'est ce qui explique que dans une certaine mesure, le législateur s'est essayé à pallier l'absence de force obligatoire au-delà des frontières communautaires au travers la mise en place de régimes spécifiques, souvent basés sur la négociation internationale. Ces régimes viennent compléter l'extraterritorialité des règles communautaires en tentant d'exporter des règles ou des standards européens⁴⁸. Toutefois, selon nous, ces régimes spécifiques doivent être distingués de l'application extraterritoriale *stricto sensu* dans le sens où ce n'est pas la règle adoptée unilatéralement par le législateur européen qui est appelée à s'appliquer en tant que telle.

§4. L'applicabilité et les choix du législateur européen

Nous venons de distinguer la dimension spatiale de l'applicabilité d'une norme, de sa force obligatoire en soulignant le caractère extraterritorial qui peut affecter l'applicabilité de cette norme. Il nous faut maintenant observer comment le législateur a délimité l'applicabilité de la directive « données personnelles ». Ceci nécessite, avant d'analyser les objectifs précis de cette directive et les critères d'applicabilité qu'elle comporte, de nous attarder sur certaines questions qui s'imposent au législateur européen lorsqu'il délimite l'applicabilité d'un instrument.

1. Une délimitation explicite ?

Adresser explicitement la question de l'applicabilité ou rester silencieux à ce propos est le premier choix que le législateur européen est amené à poser lorsqu'il s'agit d'applicabilité. En effet, tous les instruments communautaires n'envisagent pas explicitement leur domaine d'application. Loin s'en faut⁴⁹. Notons également qu'aucune disposition générale dans les traités n'est dédiée à la question. Il revient donc à la Cour de déterminer l'applicabilité des actes de droit dérivé lorsque le texte adopté reste muet sur cet aspect⁵⁰.

Concernant la directive « données personnelles », le champ d'application est déterminé explicitement au travers d'une disposition qui en mentionne les critères d'applicabilité. Néanmoins, la lecture de cette seule disposition n'est pas suffisante pour définir le domaine sur lequel la directive entend s'appliquer. En effet, l'interprétation de cette disposition doit se faire, d'une part, conformément aux objectifs de la directive,

⁴⁶ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 247-248.

⁴⁷ *Ibidem*, p. 272.

⁴⁸ *Ibidem*, p. 247.

⁴⁹ H. DE VERDELHAN, op. cit., p. 36. L'auteur observe que « la plupart [des instruments communautaires] ne s'attardent pas sur cette question ».

⁵⁰ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 334 et s., p. 384 et s. ; H. DE VERDELHAN, op. cit., pp. 36 et s.

et, d'autre part, à lumière des autres dispositions et tout particulièrement des celles qui définissent les concepts utilisés par les critères d'applicabilité⁵¹.

Le choix de déterminer le champ d'application d'une directive au sein de cette directive semble, *de facto*, impliquer un autre choix du législateur. En effet, s'il choisit de définir les critères d'applicabilité dans de l'acte lui-même, le législateur écarte la théorie bilatéraliste et, partant, l'application d'une règle de rattachement bilatérale, pour lui préférer une délimitation unilatérale.

2. Une délimitation unilatérale ?

Comme nous venons de l'énoncer « *l'autodétermination du domaine d'applicabilité exclut apparemment le jeu concurrent d'une règle de rattachement qui viendrait déterminer ses hypothèses d'application* »⁵².

Il nous faut rappeler qu'il est traditionnellement fait référence à deux méthodes de délimitation de l'applicabilité des normes en droit international privé. La première, l'unilatéralisme, qui paraît être privilégié dans le cas de la directive « données personnelles », consiste à déterminer le domaine d'applicabilité d'un acte par des dispositions présentes au sein même de cet acte. Elle s'oppose à la seconde, le bilatéralisme. Cette deuxième méthode amène le législateur à régler la question de l'applicabilité au moyen d'une règle de rattachement qui va désigner l'ordre juridique dont les règles vont régir la situation visée⁵³. Ces deux méthodes visent donc à déterminer le domaine d'applicabilité d'une norme mais elles diffèrent dans la manière d'envisager la norme. Ainsi, l'unilatéralisme envisage dès le départ la norme avec une portée limitée et, de ce fait, ne nécessite l'intervention d'aucune autre norme, alors que le bilatéralisme pense la norme avec une portée spatiale illimitée et, par conséquent appelle à l'adoption de règles distinctes indiquant les situations qui se rattachent à la norme⁵⁴.

S'il semble indiscutable que la directive détermine elle-même son applicabilité selon la méthode unilatéraliste⁵⁵, le choix de la méthode, lui, peut être discuté. En effet, *a priori*, rien n'empêche de concevoir que l'applicabilité de la réglementation européenne en matière de protection de données personnelles puisse être définie selon la méthode bilatéraliste. Toutefois, il convient de souligner que la méthode unilatéraliste permet de sécuriser l'application des dispositions européennes en dehors de l'Union, ou à tout le moins de sécuriser⁵⁶ une telle application de manière plus directe que la méthode bilatéraliste. C'est probablement une des raisons qui explique que le législateur européen opte pour une délimitation

⁵¹ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 381 -382. L'auteur observe notamment qu'une technique utilisée à plusieurs reprises « consiste à intégrer les éléments déterminants du domaine d'application spatiale dans la définition des termes clefs de l'acte législatif ».

⁵² *Ibidem*, p. 363.

⁵³ *Ibidem*, pp. 15 et s.

⁵⁴ *Ibidem*, pp. 16 et 17.

⁵⁵ M. FALLON et S. FRANCO, « La coopération judiciaire civile et le droit international privé : Vers un droit proprement communautaire des conflits de loi ou de juridiction » in *Une Constitution pour l'Europe : Réflexions sur les transformations du droit de l'Union européenne*, O. DE SCHUTTER et P. NIHOUL (coord.), Bruxelles, Larcier, 2004, p. 247.

⁵⁶ S. FRANCO, « The external dimension of Rome I and Rome II : neutrality or schizophrenia » in *Private law in the external relation of the EU*, M. CREMONA and H. MICKLITZ (dir.), Oxford, Oxford University Press, 2016, p 91. Rappelons, toutefois, le constat que nous faisons ci-avant, l'application du droit européen en dehors de l'Union reste dans une certaine mesure tributaire de la volonté des autorités des états tiers ce qui conduit à modérer la signification de « la sécurisation de l'application » du droit communautaire.

unilatéraliste de l'applicabilité de ses actes et que la Cour, lorsqu'elle y est appelée, interprète selon cette même théorie l'applicabilité des actes européens⁵⁷.

Quoi qu'il en soit, au vu de ces considérations, il s'avère que les questions de l'extraterritorialité et de l'unilatéralité des directives semblent liées dans la mesure où toutes deux participent à la volonté d'exporter, au sens large, l'application des standards européens en dehors des frontières communautaires. Cette volonté témoigne, en outre, d'une absence de confiance dans les législations des pays tiers, et notamment en ce qui nous concerne, d'une absence de confiance dans les législations relatives à la protection des données personnelles⁵⁸.

Si l'adoption de la méthode unilatérale procède d'une volonté dans le chef du législateur européen de sécuriser l'application du droit communautaire, il faut souligner que cette méthode n'écarte pas toutes les difficultés et notamment les conflits de lois, en particulier les conflits « positifs »⁵⁹. Remarquons, toutefois, que dans l'arrêt *Google*, la Cour de justice ne s'embarrasse pas de savoir si un autre droit, le droit américain par exemple, est applicable. La haute juridiction de l'Union se borne à conclure à l'application du droit européen et à justifier cette application⁶⁰.

La question de l'application du droit d'un état tiers ainsi que l'absence de confiance dans un ordre juridique non-communautaire nous amène au dernier choix que nous examinons dans cette section, à savoir le caractère impératif de l'applicabilité.

3. Une délimitation impérative ?

Avant tout autre propos, il nous faut préciser que la délimitation, quant bien même explicite, d'un domaine d'applicabilité ne lui confère pas, *ipso facto*, un caractère impératif⁶¹. Ainsi, constater que la directive « données personnelles » définit son domaine d'applicabilité, ne permet pas de faire l'économie d'une analyse de son éventuel caractère impératif. Toutefois, il semble que la délimitation de l'applicabilité de la directive apparaisse comme une condition nécessaire, mais non suffisante, pour conclure au caractère impératif de cette dernière⁶².

La question de l'impérativité recouvre traditionnellement une double nature : l'impérativité interne et l'impérativité externe⁶³. En effet, l'impérativité externe « s'oppose à la désignation par les parties d'une législation qui contourne les objectifs de la directive », alors que l'impérativité interne, prohibe toute clause entre parties qui serait dérogatoire au contenu de la directive⁶⁴. Cependant, dans le cas de la directive

⁵⁷ De telles considérations sur la délimitation générale du droit dérivé dépassent le cadre de cette étude. Pour analyse détaillée sur la question voy. S. FRANCCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit. L'auteur y analyse les méthodes utilisées par le législateur européen pour déterminer le champ d'application des instruments de droit dérivés dans les divers domaines de la politique communautaire.

⁵⁸ S. FRANCCQ, « The external dimension of Rome I and Rome II : neutrality or schizophrenia », op. cit., p. 105.

⁵⁹ S. FRANCCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 121. L'auteur observe que les règlements européens en matière de concurrence « adopte la méthode propre à la théorie unilatéraliste » et « que l'on y retrouve certaines des difficultés classiques de l'unilatéralisme ». Cette remarque nous semble transposable s'agissant de la directive « données personnelles ».

⁶⁰ Prédominance du droit du for, voir cours DIPE.

⁶¹ S. FRANCCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 423.

⁶² *Ibidem*, p. 423. L'auteur observe, toutefois, que si la délimitation semble être nécessaire pour conclure à l'impérativité cette délimitation peut être implicite.

⁶³ Également appelé impérativité internationale.

⁶⁴ S. FRANCCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 336 et pp. 433 et s.

« données personnelles », il serait possible de limiter la question à l'examen de l'impérativité interne puisque la directive détermine elle-même son applicabilité. Ainsi, désigner contractuellement une autre législation que la directive dans le cas où elle est applicable reviendrait à déroger à son contenu. En d'autres termes, si la directive revêt un caractère impératif interne, il ne serait pas possible pour les parties d'insérer une clause désignant une loi applicable qui contourne les dispositions de la directive « données personnelles ». Un raisonnement inverse n'est cependant pas envisageable ; l'absence d'impérativité interne n'implique pas nécessairement l'absence d'impérativité externe⁶⁵.

Ces précisions établies, il nous faut constater qu'à sa lecture, la directive ne donne aucune précision explicite sur un éventuel caractère impératif. Ainsi, elle délimite son domaine d'applicabilité mais reste muette sur son impérativité. Ce silence peut conduire à deux conclusions radicalement opposées⁶⁶ : soit cette absence de précision signifie que la directive est dénuée d'impérativité, soit le caractère impératif se déduit de l'interprétation de la directive et de ses objectifs.

La Cour ne se prononce pas sur le caractère impératif de la directive « données personnelles » dans l'affaire *Google Spain*. En effet, rien ne l'incitait à aborder la question. Les parties n'ont pas soulevé ce point⁶⁷ et pour cause même si les conditions générales d'utilisation de *Google* s'accompagnaient d'une clause de choix de loi, il eut été difficile de prétendre que la requête du citoyen espagnol à l'AEPD, à savoir l'effacement de son nom, impliquait l'utilisation dans un cadre contractuel des services de *Google* par ledit citoyen⁶⁸. Cependant, dans une autre affaire⁶⁹, la Cour est amenée à trancher la question de l'impérativité de certaines dispositions d'une directive concernant les agents commerciaux⁷⁰. La Cour a considéré que ces dispositions étaient impératives sans distinguer l'impérativité externe de l'impérativité interne. Cette décision se fonde essentiellement sur les objectifs⁷¹ de la directive mais également sur deux dispositions de la directive⁷² ; la première⁷³ prévoyant que « *les parties ne peuvent pas y [s'agissant de la directive] déroger au détriment de l'agent commercial avant l'échéance du contrat* », et la deuxième⁷⁴ prescrivant l'application immédiate de la directive aux contrats en cours.

Une interprétation analogue basée sur les objectifs de la directives « données personnelles », principalement sur la protection des données personnelle, est possible, d'autant plus qu'il ressort de la directive une volonté à la fois d'éviter le contournement de ses dispositions et de s'assurer que le traitement des données personnelles ne soit pas soumis à une loi qui n'offrirait pas un niveau de protection adéquat⁷⁵. En outre, au vu du raisonnement clairement orienté vers la protection des données personnelles dans l'affaire *Google*, une interprétation de la directive « données personnelles » similaire à celle de la directive

⁶⁵ *Ibidem*, pp. 424 - 425.

⁶⁶ *Ibidem*, pp. 326 - 327.

⁶⁷ Si Google conteste l'application de la directive ce n'est pas sur base d'une clause de droit applicable mais parce que, selon lui, le critère d'applicabilité de la directive n'est pas satisfait.

⁶⁸ Le traitement des informations de la personne concernée n'est pas lié à l'utilisation par cette personne de Google. De les données en question ont été référencées indépendamment de l'utilisation de Google par la personne concernée.

⁶⁹ CJCE, 9 novembre 2000, aff. C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, Rec., 2000, p. I-9305. Voy. S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 406 et s.

⁷⁰ Directive 86/653/CEE du Conseil, du 18 décembre 1986, relative à la coordination des droits des Etats membres concernant les agents commerciaux indépendants, JOCE, 1986, L 383/17.

⁷¹ CJCE, 9 novembre 2000, C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, op. cit., pts 21, 23 et 24.

⁷² CJCE, 9 novembre 2000, C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, op. cit., p. I-9305, pts 21 et 22.

⁷³ Article 19 de la directive 86/653/CEE relative aux agents commerciaux.

⁷⁴ Article 22 de la directive 86/653/CEE relative aux agents commerciaux.

⁷⁵ Directive « données personnelles », Considérant 18, 19 et 57.

sur les agents commerciaux consacrée par la Cour dans l'affaire *Ingmar* ne serait guère surprenante, même s'il n'existe pas dans la directive « données personnelles » de disposition analogue à celle que la Cour a employée dans la directive sur les agents commerciaux pour justifier son raisonnement.

Toutefois, en l'absence d'une disposition explicite quant à son impérativité, il nous semble impossible d'affirmer avec certitude que la directive « données personnelles » dispose d'un caractère impératif⁷⁶ et ce en raison de la place laissée au consentement dans le texte de cette dernière. Effectivement, à deux reprises, le législateur permet de déroger aux règles de la directive sur base du consentement de la personne concernée par le traitement de données. Si la première dérogation⁷⁷ permet le traitement, normalement interdit, de certaines données considérées comme sensibles, la deuxième⁷⁸, quant à elle, autorise le transfert de données personnelles vers un pays tiers n'assurant pas un niveau de protection adéquat et à ce titre nous intéresse plus directement. En effet, cette deuxième dérogation ne permet pas *stricto sensu* d'écarter, sur base du consentement, la directive là où elle serait applicable⁷⁹ ; en revanche en autorisant le transfert consenti de données vers un pays tiers sur lequel la directive ne s'applique pas, la dérogation permet à la personne concernée d'accepter que le traitement de ses données soit soumis à la législation de ce pays tiers⁸⁰. Ainsi, l'existence de cette dérogation constitue, à notre sens, un contre-argument important à l'impérativité de la directive.

Enfin, nous constatons que si la question de l'impérativité peut sembler théorique, elle est susceptible d'avoir des implications concrètes considérables. En effet, bon nombre de données sont susceptibles d'être recueillies et traitées dans le cadre d'un contrat ou, à tout le moins d'une relation qui peut être qualifiée de contractuelle, telle que l'utilisation de services fournis par des exploitants de réseaux sociaux⁸¹. Or il n'est pas rare qu'un tel exploitant insère dans ses conditions d'utilisation une clause de choix de loi⁸². La question de l'impérativité revient concrètement à se demander si une telle clause peut véritablement déployer ses effets en écartant la directive et, partant, la protection qu'elle assure aux personnes concernées.

Chapitre 2. Les objectifs de la réglementation sur les données personnelles

Après avoir illustré et précisé la question de l'applicabilité, il nous faut nous intéresser aux objectifs visés par la réglementation en matière de données personnelles. En effet, ainsi que nous allons l'observer les objectifs revêtent une importance prépondérante dans l'analyse de l'applicabilité d'un instrument (Section 1). Ensuite, dans la mesure où d'autres instruments relatifs aux données personnelles ont précédé

⁷⁶ Une telle absence est donc regrettable si le législateur conçoit cette directive comme un instrument d'application impérative.

⁷⁷ Article 7, point (a), directive « données personnelles ».

⁷⁸ Article 26, paragraphe 1^{er}, point (a), directive « données personnelles ».

⁷⁹ Sur cette question, le législateur européen ne se prononce pas explicitement dans la directive puisqu'il reste silencieux sur le caractère impératif de la directive.

⁸⁰ En quelque sorte, par cet Article 26, paragraphe 1^{er}, point (a) de la directive « données personnelles », le législateur permet aux parties de contourner la directive même si le niveau de protection de la personne concernée est moindre pour autant que cette dernière y consente.

⁸¹ J. MOINY, *op. cit.*, pp. 245-247.

⁸² A titre d'exemple, Facebook prévoit dans ses conditions « de service » que « *Le droit de l'État de Californie régit cette Déclaration, de même que toute action entre vous et nous, sans égard aux dispositions en matière de conflits de lois* ». Les conditions de service de Facebook consultable à l'adresse suivante https://m.facebook.com/terms/?locale2=fr_FR (consulté le 16 juillet 2016).

et influencé⁸³ l'œuvre du législateur européen, il convient de les évoquer (Section 2) avant d'examiner les objectifs de la directive « *données personnelles* » (Section 3).

Section 1. Les objectifs et l'applicabilité

Comme nous l'avons souligné précédemment, le domaine d'applicabilité d'un instrument s'interprète à la lumière de ses objectifs, *a fortiori* lorsqu'il est question d'un instrument de droit européen, étant donné l'interprétation téléologique traditionnellement adoptée par la Cour. L'arrêt *Ingmar*, déjà évoqué⁸⁴, est un exemple incontestable dans lequel la Cour juge la directive relative aux agents commerciaux, applicable à la situation en cause sur base des objectifs de ladite directive⁸⁵. Cela vaut aussi lorsque l'acte juridique détermine lui-même son domaine d'applicabilité. Ainsi dans l'arrêt *Google*, il est indéniable que la Cour a interprété la disposition déterminant l'applicabilité de la directive à la lumière de la protection des données personnelles⁸⁶. Ces deux arrêts démontrent une interaction manifeste entre les objectifs d'un instrument et son domaine d'applicabilité⁸⁷.

D'un point de vue plus institutionnel, les objectifs sont également essentiels parce qu'ils permettent de vérifier si l'acte adopté relève effectivement de la compétence de l'Union européenne⁸⁸ et, partant, d'identifier la base légale qui sous-tend l'acte. Enfin, notons que la disposition du droit primaire qui sert de base légale à l'instrument de droit dérivé peut avoir une influence directe sur le domaine d'applicabilité de cet acte dérivé⁸⁹.

Section 2. Les objectifs des autres instruments de protections des données personnelles

Il est intéressant de noter que la directive n'est pas le premier instrument à protéger les données personnelles. En effet, dans les années septante apparaissent les premières lois nationales relatives à la protection des données personnelles, qui sont surtout une réaction aux méthodes utilisées durant la deuxième Guerre mondiale⁹⁰. Il fallut attendre dix ans de plus pour voir apparaître les premières initiatives internationales protégeant spécifiquement les données personnelles⁹¹, notamment sous l'égide de l'OCDE et du Conseil de l'Europe. Si la Convention européenne de sauvegarde des droits fondamentaux protégeait

⁸³ Le législateur européen fait ainsi référence aux principes généraux du droit communautaire, à l'article 8 de la CEDH et à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n°108), faite à Strasbourg le 28 janvier 1981, dans le considérant 10.

⁸⁴ Voy. *supra*, p. 13.

⁸⁵ S. FRANCO, « The external dimension of Rome I and Rome II : neutrality or schizophrenia », *op. cit.*, pp. 94-95.

⁸⁶ L. MARINO « Un 'droit à l'oubli' numérique consacré par la CJUE », *La semaine juridique*, p. 1302.

⁸⁷ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p. 375 et pp. 410 et s.

⁸⁸ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p. 512.

⁸⁹ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, pp. 512-514. En effet, le principe d'attribution s'applique selon toute vraisemblance tant à l'aspect matérielle des règles qu'au sujet de leur applicabilité. Il nous faudra ainsi nous interroger sur l'influence que l'article 114 TFUE peut avoir sur l'applicabilité de la directive « données personnelles ».

⁹⁰ D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, p. 57.

⁹¹ : C. KUNER, *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013, pp. 9-10 ; C. BERNARD-GLANZ, « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », *Cahiers de droit européen*, 2014, pp. 686-687.

déjà dans une certaine mesure⁹² les données personnelles, cette dernière a été complétée par la « Convention 108 ».

En ce qui concerne le droit communautaire, la protection des données personnelles est jusqu'à l'adoption de la directive « données personnelles », l'apanage du droit primaire qui la consacre au travers du principe général de droit garantissant la protection de la vie privée. Par la suite, la Charte des droits fondamentaux définit la protection des données personnelles comme un droit fondamental dans une disposition, à savoir l'article 8, spécifique et distincte de l'article 7, qui consacre le droit à la vie privée⁹³.

Deux observations s'imposent. Premièrement, nous constatons qu'antérieurement à la directive, les instruments s'intéressant aux données personnelles sont orientés sur le droit, désormais fondamental, des personnes à la protection des données personnelles. Deuxièmement, depuis les années quatre-vingt, et notamment depuis la Convention « 108 » du Conseil de l'Europe, la protection des données personnelles fait l'objet d'une protection à part entière, indépendante du droit au respect de la vie privée. Certains⁹⁴ justifient cette différence en soutenant que le droit à la vie privée est invocable par les personnes morales tandis que la protection des données personnelles ne s'applique qu'aux personnes physiques⁹⁵ ou encore que la protection de la vie privée ne couvre pas nécessairement l'ensemble des données personnelles protégées⁹⁶ par le droit à la protection des données personnelles. A notre sens, c'est l'évolution technologique et l'émergence d'une marchandisation des données personnelles qui fait de la protection de ces données un droit quelque peu à part, sans pour autant le détacher complètement du droit au respect à la vie privée.

Section 3. Les objectifs de la directives 95/46

Si, comme nous l'avons observé ci-dessus, l'objectif des instruments antérieurs relatifs aux données personnelles est la protection de ces données, il n'en va pas exactement de même pour la directive « données personnelles ». En effet, la directive s'inscrit avant tout dans le cadre du marché intérieur et vise à y faciliter la circulation des données⁹⁷ (paragraphe 1). Toutefois, il est certain que le législateur européen ne pouvait pas faire fi du droit à la protection des données (paragraphe 2).

§1. La libre circulation des données dans le marché intérieur

L'article 1^{er}, §2 de la directive énonce que « *les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etat membres pour des raisons relatives à la*

⁹² La Cour européenne des droits de l'homme a interprété largement le droit à la protection de la vie privée étendant dans une certaine mesure au droit à la protection des données personnelles. Voy. CEDH, Aff. *Amann v. Switzerland* [GC], no. 27798/95, CEDH 2000-II, § 65, dont la jurisprudence est confirmée dans CEDH, Aff. *Rotaru v Romania* [GC], no. 28341/95, CEDH 2000-V, § 43.

⁹³ J. KOKOTT & C. SOBOTTA, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *International Data Privacy Law*, 2013, Volume 3, p. 223.

⁹⁴ J. KOKOTT & C. SOBOTTA, *op. cit.*, p. 225. Ces auteurs ajoutent encore que les conditions pour pouvoir déroger à ces deux droits fondamentaux seraient différentes.

⁹⁵ Dans le même sens, l'article 1 de la directive « données personnelles » précise que la protection s'applique aux données personnelles des personnes physiques. Toutefois, tant la Charte des droits que le Traité sur le fonctionnement de l'Union européenne énoncent que « *Toute personne a droit à la protection des données à caractère personnel* » (nous soulignons) et donc n'exclut pas les personnes morales.

⁹⁶ La directive « données personnelles » vise les données personnelles qui permettent directement ou indirectement d'identifier la personne concernée. Dans l'absolu, il ne peut être exclu que certaines données ne soit pas considérées comme couverte par le droit à la vie privée mais permettent d'identifier la personne concernée.

⁹⁷ C'est, de fait, le premier objectif de la directive « données personnelles » qui, adoptée sur base de l'article 114 TFUE, vise avant tout l'achèvement et le fonctionnement du marché intérieur. Ce n'est, toutefois, pas le seul objectif de la directive.

protection [des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel] assurée en vertu du paragraphe 1 » (nous soulignons).

La directive « données personnelles » illustre parfaitement le rôle du droit dérivé dans l'achèvement du marché intérieur, à savoir compléter le droit primaire. Ce dernier impose aux Etats membres des règles qui ouvrent les marchés nationaux mais n'éliminent, toutefois, pas tous les obstacles à l'établissement d'un marché unique. En effet, des règles d'origine nationale, entravant la libre circulation que le droit primaire entend instaurer, subsistent au motif qu'elles protègent certains objectifs d'intérêt général. S'agissant de la libre circulation des données, des obstacles persistaient au nom de la protection des libertés et droits fondamentaux des personnes. C'est là qu'intervient le droit dérivé en harmonisant au niveau européen la gestion de ces objectifs pour mettre fin à la disparité des réglementations nationales et aux exigences cumulatives qu'elles peuvent impliquer⁹⁸. Concrètement, la directive « données personnelles » vient harmoniser les règles nationales des Etats membres concernant la protection des données personnelles lors de leur traitement, et supprime ainsi les règles nationales qui entravaient la libre circulation des données, au motif de la protection de la vie privée et des données personnelles des personnes⁹⁹.

Une telle action de l'Union européenne est possible sur base de l'article 114 du Traité sur le fonctionnement de l'Union européenne. Cette disposition constitue la base légale permettant cette harmonisation qui complète le droit primaire et supprime les entraves subsistantes. Cependant l'usage de l'article 114 doit être justifié par le législateur européen. Il ne s'agit pas simplement de prétendre prendre des mesures au nom de l'établissement et du fonctionnement du marché intérieur, il faut encore identifier concrètement les disparités entravant la libre circulation, visées par l'harmonisation¹⁰⁰. C'est ce que le législateur européen s'efforce de faire en précisant que « *les différences entre Etats membres quant au niveau de protection [...] à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un Etat membre à celui d'un autre Etat membre* » et ajoutant que « *ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire et fausser la concurrence* »¹⁰¹. Notons que le choix de la base légale est susceptible d'être soumis au contrôle¹⁰² de la Cour qui le, cas échéant, pourrait invalider l'acte¹⁰³.

En l'occurrence, le choix de la base légale n'a pas été contesté en annulation et, partant, la directive « données personnelles » n'a pas été invalidée. Cependant, cela ne signifie pas que l'objectif

⁹⁸ M. FALLON, *Droit matériel général de l'Union européenne*, Louvain-la-Neuve, Bruylant, 2002, p. 144 et p. 222-225 ; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 512 et pp. 540-543.

⁹⁹ Ce rôle du droit dérivé est énoncé dans l'article 1^{er} de la directive « données personnelles » par la partie de phrase que nous mettons en évidence ci-dessus.

¹⁰⁰ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 341-342 et p. 481.

¹⁰¹ Directive « données personnelles », Considérant 7.

¹⁰² S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 525-526. L'auteur souligne que la Cour ne peut opérer un contrôle politique sur les mesures que nécessite l'établissement et le fonctionnement du marché intérieur ce qui constitue bémol dans sa compétence de contrôle par rapport au choix de l'article 114 TFUE comme base légale d'un instrument de droit dérivé.

¹⁰³ A titre d'exemple, voy. CJCE, 5 octobre 2000, aff. 376/98, *République Fédérale d'Allemagne c. Parlement et Conseil*, Rec., 2000, p. I-8419.

d'harmonisation des réglementations des Etats membres en matière de données personnelles ait effectivement été atteint par la directive¹⁰⁴.

Ainsi que nous venons de l'évoquer, l'acte du législateur européen doit matériellement être conforme à la base légale, et il en va de même s'agissant de l'applicabilité. Il convient donc d'examiner si le domaine d'applicabilité de la directive « données personnelles » excède les limites qui lui sont imposées par le droit primaire, et plus précisément par l'article 114 du traité sur le fonctionnement de l'Union européenne. Concrètement, dans la mesure où l'article 114, TFUE, vise l'établissement et le fonctionnement du marché intérieur, la question se pose de savoir si, sur cette base, le législateur peut légitimement régir des situations concernant les relations avec les états tiers, d'une part, et, des situations internes, d'autre part. Il est vrai que l'article 114 du Traité vise exclusivement le marché intérieur et donc qu'*a priori* n'est pas censé permettre au législateur européen de prendre des mesures qui s'étendent au-delà de ce marché ou visent des situations exclusivement nationales¹⁰⁵.

1. La situation purement nationale

Concernant les situations internes, dans une affaire où tous les éléments sont localisés en Autriche, la Cour a jugé que « *toute donnée à caractère personnel est susceptible de circuler* »¹⁰⁶. Même si l'application du droit européen à une situation interne n'est pas contestée par les parties, cette affirmation de la Cour nous amène à penser que la directive « données personnelles » est applicable tant aux situations internes qu'aux situations intracommunautaires¹⁰⁷. En d'autres termes, il ne semble pas nécessaire que la situation comporte effectivement un élément d'extranéité localisé dans un autre Etat membre pour que la directive soit applicable et ce, même si la base légale de l'acte en cause se trouve être l'article 114 du TFUE¹⁰⁸.

A notre sens, la solution adoptée ici par la Cour n'est pas nécessairement transposable en tant que telle à d'autres domaines que les données personnelles, même si elle confirme une tendance dans la jurisprudence de la Cour¹⁰⁹. En effet, s'agissant des données personnelles, pour justifier de l'application du droit communautaire à la situation interne en question, la Cour se base sur le caractère extrêmement mobile des données et considère, de ce fait, qu'il n'y a pas lieu de distinguer les situations domestiques des situations européennes. En outre, il nous faut reconnaître qu'une telle distinction risquerait d'impliquer certaines difficultés pratiques¹¹⁰ s'il s'avérait que des règles différentes dussent être appliquées aux données dites domestiques et aux données destinées à « sortir » de l'Etat membre¹¹¹.

¹⁰⁴ Voy. *infra*, p. 53 et s. sur le niveau d'harmonisation atteint par la directive. Précisons déjà que certains auteurs remettent fortement en cause le caractère « marché intérieur » de cette mesure car elle n'atteint pas son but en matière d'harmonisation. Voy. L. MOEREL, « Back to basics: when does EU data protection law apply », *International Data Privacy Law*, 2011, Vol. 1, No. 2, pp. 92-93.

¹⁰⁵ M. FALLON, *Droit matériel général de l'Union européenne*, op. cit., 2002, p. 144; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 284-285 et pp. 481 et s.

¹⁰⁶ CJCE, 20 mai 2003, aff. jointes C-465/00, C-138/01, C-139/01, *Rechnungshof*, Rec., 2003, p. I-4989, pt. 40. Autrement dit, dès lors qu'il s'agit de données personnelles, l'élément d'extranéité nécessaire pour considérer la situation comme intra-européenne existe en germe.

¹⁰⁷ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 515-518.

¹⁰⁸ Précisément s'agissant de l'article 114, TFUE, la Cour considère que l'usage de cette disposition « ne présuppose pas l'existence d'un lien effectif avec la libre circulation entre EM dans chacune des situations envisagées par l'acte ». Voy. CJCE, 20 mai 2003, aff. jointes C-465/00, C-138/01, C-139/01, *Rechnungshof*, op. cit., pt. 41.

¹⁰⁹ M. FALLON et J. BERGE, op. cit., p.3. Les auteurs observent « une nette tendance de la jurisprudence de la Cour de Justice à étendre le champ d'application de ce droit (le droit européen de la libre circulation) à des situations nationales ».

¹¹⁰ En effet, il est de plus en plus difficile de distinguer les données sur base de leur origines et rien ne garantit que celles-ci ne circuleront pas par la suite.

¹¹¹ V. REDING, « The European data protection framework for the twenty-first century », op. cit., p. 123.

Enfin, il convient de préciser que ni la directive « données personnelles », ni l'article 8 de la Charte fondamentale ne distinguent les situations purement domestiques des situations européennes¹¹².

2. La situation impliquant des Etats tiers

A propos de l'application aux relations avec les Etat tiers, d'un acte dit « marché intérieur », la Cour a répondu à une question préjudicielle¹¹³ concernant la directive tabac¹¹⁴ dont la réponse est à notre sens, tout à fait transposable à la directive « données personnelles ». Dans son arrêt concernant la directive tabac, la Cour a considéré que *« s'agissant des objectifs poursuivis par la directive, il convient de rappeler que son objectif principal est d'améliorer le fonctionnement du marché intérieur dans le domaine des produits du tabac en garantissant un niveau élevé de protection de la santé »*¹¹⁵, et d'ajouter que *« dès lors, il y a lieu de considérer que les dispositions de la directive concernent en principe uniquement les produits du tabac destinés à être commercialisés dans le marché intérieur »*¹¹⁶. Certes, la directive « données personnelles » ne concerne pas les produits du tabac mais les données personnelles et vise à garantir un niveau élevé de protection de ces données et non pas de la santé. Cependant ces constatations valent également pour la directive « données personnelles ».

A propos de la directive tabac, la Cour continue en estimant que *« le risque d'affectation du marché intérieur peut justifier l'adoption, sur le fondement de l'article 95 CE (actuellement 114 TFUE), d'une disposition qui concerne des produits exportés vers des pays tiers, en tant que mesure destinée à éviter le contournement des dispositions édictées pour le marché intérieur »*¹¹⁷. Il nous semble qu'un risque d'affectation du marché intérieur existe également à l'égard du traitement des données personnelles et peut donc justifier l'adoption, sur le fondement de l'article 114, TFUE, de dispositions concernant des opérateurs non-établis sur le territoire de l'Union, pour éviter que ces derniers puissent contourner les dispositions en matière de données personnelles édictées pour le marché intérieur¹¹⁸. En d'autres termes, il nous paraît que le critère d'affectation du marché intérieur est également applicable pour justifier l'adoption de dispositions qui, en vertu de l'article 114, TFUE, entendent s'appliquer au-delà des limites territoriales du marché intérieur.

Dans les considérations ci-avant, nous précisons que l'Union peut agir pour harmoniser les législations nationales qui entraveraient le marché intérieur sur base de l'article 114, TFUE, mais doit, dans ce cadre, justifier son action. Toutefois, l'article 114, TFUE, n'exclut pas que le législateur européen poursuive d'autres objectifs dans son action d'harmonisation. La Cour l'a d'ailleurs confirmé s'agissant de la protection de la santé humaine¹¹⁹. Le droit européen de la consommation regorge également d'exemples d'actes

¹¹² V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 123. L'auteur remarque que cette distinction n'est pas non plus présente dans la Convention « 108 » du Conseil de l'Europe.

¹¹³ CJCE, 10 décembre 2002, aff. C-491/01, *British American Tobacco, Rec.*, 2002, p. I-11453.

¹¹⁴ Directive 2001/37/CE du Parlement européen et du Conseil, du 5 juin 2001, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de fabrication, de présentation et de vente des produits du tabac, *JOCE*, 2001, L 194/26.

¹¹⁵ CJCE, 10 décembre 2002, C-491/01, *British American Tobacco, op. cit.*, pt. 211.

¹¹⁶ CJCE, 10 décembre 2002, C-491/01, *British American Tobacco, op. cit.*, pt. 212.

¹¹⁷ CJCE, 10 décembre 2002, C-491/01, *British American Tobacco, op. cit.*, pt. 213.

¹¹⁸ volonté d'éviter le contournement tant pour protéger les droits des citoyens que pour protéger les entreprise EU S'il y a la volonté de faciliter la libre circulation des données dans le cadre du Marché intérieur, il y a également la volonté de soumettre l'ensemble des opérateurs qui traitent des données personnelles dans le cadre du Marché intérieur aux mêmes règles afin de ne pas fausser la concurrence au détriment des opérateurs européen.

¹¹⁹ CJCE, 10 décembre 2002, C-491/01, *British American Tobacco, op. cit.*, pt. 62. Dans ce même point, la Cour va même plus loin puisqu'elle précise que *« l'article 152, paragraphe 1, premier alinéa, CE prévoit qu'un niveau élevé de protection de la santé humaine »*

adoptés sur la base de l'article 114 TFUE qui en plus d'harmoniser les législations nationales organisent un régime de protection du consommateur¹²⁰. Le législateur européen ne s'est donc pas privé dans la directive « données personnelles », de poursuivre un objectif de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, parallèlement à l'objectif de libre circulation des données.

§2. Le droit à la protection des données personnelles

Pour atteindre son objectif de libre circulation de manière satisfaisante, le législateur européen ne pouvait pas ignorer la question de la protection des données. En effet, si des mesures pour faciliter la circulation des données personnelles au sein du marché intérieur devenaient nécessaires¹²¹, elles ne pouvaient être prises au détriment de la protection des personnes¹²². En outre, un niveau élevé de protection des données personnelles participe également au fonctionnement du marché intérieur dans la mesure où il constitue un facteur qui favorise le commerce, particulièrement le commerce électronique¹²³. Enfin, c'est surtout parce que le droit à la protection des données personnelles est considéré comme un droit fondamental et que la protection des données fait l'objet d'une tradition ancrée au sein des Etats membre que l'Union ne pouvait ignorer cet aspect dans la directive¹²⁴.

1. Un droit fondamental

Ce statut de droit fondamental n'est pas sans conséquence. Il en découle des obligations pour les Etats membres qui doivent s'abstenir de toute violation de ce droit mais aussi en assurer le respect. C'est également le cas pour l'Union européenne dans la mesure où la protection des données personnelles revêt, désormais, aussi un caractère fondamental dans l'ordre juridique communautaire au travers de la Charte de droits fondamentaux et du Traité sur le fonctionnement de l'Union européenne. L'Union est donc tenue de respecter et de faire respecter la protection des données personnelles¹²⁵. Si l'application de l'obligation négative concerne tous les actes de l'Union et ne suscite pas de difficulté particulière, l'applicabilité de l'obligation positive est plus incertaine. Faut-il considérer qu'elle s'étende au-delà du territoire européen ? Cette question est intéressante puisque l'Union européenne, appuyée par une partie de la doctrine, utilise le caractère de droit fondamental de la protection des données personnelles pour en justifier l'application

est assuré dans la définition et la mise en oeuvre de toutes les politiques et actions de la Communauté ». En d'autres termes, le législateur européen est obligé de veiller à ce qu'un niveau élevé de protection soit assuré.

¹²⁰ Parmi d'autres, Directive 2011/83/UE du Parlement européen et du Conseil, du 25 octobre 2011, relative aux droits des consommateurs, modifiant la Directive 93/13/CEE du Conseil et la Directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la Directive 85/577/CEE du Conseil et la Directive 97/7/CE du Parlement européen et du Conseil, *JOUE*, 2011, L 304/64 ; Directive 1999/44/CE du Parlement européen et du Conseil, du 25 mai 1999, sur certains aspects de la vente et des garanties des biens de consommation, *JOCE*, 1999, L-171/12.

¹²¹ Directive « données personnelles », Considérants 3 à 5.

¹²² En réalité, à l'époque où la directive est adoptée il semble que rien n'obligeait l'Union à assurer la protection des données personnelles dans la mesure où, formellement, aucune disposition du droit primaire ne prévoyait une telle obligation. Toutefois, politiquement il aurait été délicat d'assurer la libre circulation des données personnelles en baissant la protection dont elle bénéficiait sous les régimes nationaux. En outre, les Etats membres avaient déjà souscrit à une obligation d'assurer la protection des données personnelles.

¹²³ V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 124. L'auteur point l'inquiétude des consommateurs comme l'une des principales raisons qui les réfrène de consommer ou d'acheter en ligne et identifie ainsi la protection des données comme crucial pour renforcer la confiance de ces consommateurs dans les services en ligne.

¹²⁴ M. TAYLOR, *op. cit.*, pp. 246-248.

¹²⁵ *Ibidem*, pp. 246-248. Remarquons que pour satisfaire la face négative de son obligation, le législateur européen a adopté le Règlement (CE) 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *JOCE*, 2001, L 8/1.

extraterritoriale¹²⁶. Mais l'Union est-elle tenue de définir la portée des dispositions protégeant ce droit au-delà du territoire communautaire ?

Le droit primaire n'apporte pas de réponse claire à cette question. Le Traité sur l'Union européenne prévoit que l'Union « *promeut ses valeurs et intérêts dans ses relations avec le reste du monde* »¹²⁷. La Charte des droits fondamentaux n'apporte de réponse plus éclairante. Toutefois, si la portée d'une telle obligation dans le chef de l'Union reste discutable, le constat n'est pas tout à fait identique pour les Etats membres. En effet, en tant que parties à la Convention Européenne des droits de l'homme et à la Convention sur les droits civils et politiques, les Etats membres risqueraient de manquer à leur obligation d'assurer une protection effective des données personnelles s'ils limitent la protection en question aux frontières de leur territoire¹²⁸.

Enfin, il convient d'observer que ce statut de droit fondamental n'est pas reconnu avec la même intensité dans tous les ordres juridiques¹²⁹. Précisons également que même en Europe, il n'est pas absolu et ce droit peut faire l'objet de limitation¹³⁰, notamment lorsqu'il entre en conflit avec d'autres droits fondamentaux. Ces deux aspects sont très importants dans l'interprétation de la directive puisque le juge qui interprète *in concreto* les dispositions de la directive « données personnelles », ou de l'acte qui la transpose, sera très souvent confronté à des situations où la protection des données personnelles s'opposera à d'autres droits fondamentaux.

2. La protection des données et les autres droits fondamentaux

Comme nous venons de le souligner, lorsqu'il est question de la protection des données personnelles, à l'instar de l'affaire *Google Spain*, cela risque inévitablement d'impliquer une articulation entre différents droits fondamentaux selon les parties en présence. En effet, l'application des droits au respect de la vie privée et à la protection des données personnelles de la personne concernée, risque d'empiéter sur le droit d'expression de l'opérateur, voire sur sa liberté d'entreprendre, et sur le droit à l'information du public¹³¹.

En théorie, aucun de ces droits n'est absolu et aucune hiérarchie n'est formellement établie entre eux. Par conséquent, ils peuvent tous faire l'objet de limitations et, en cas de conflit entre ces droits, la tâche revient au juge d'effectuer une analyse au cas par cas. Toutefois, s'il semble que la Cour de justice charge le juge national d'opérer la balance des intérêts en cas de conflit opposant des droits fondamentaux, la jurisprudence en matière de données personnelles de la haute juridiction communautaire, nous conduit à penser qu'une primauté s'est établie en faveur de la protection des données personnelles et du droit à la vie privée¹³². L'arrêt *Google Spain* ne fait que confirmer cette tendance, notamment lorsque la Cour y déclare

¹²⁶ M. TAYLOR, *op. cit.*, p. 246-248 ; C. KUNER, F. CATE, C. MILLARD et D. SVANTESSON, *op. cit.*, p. 147 ; J. MOINY, *op. cit.*, p. 268 ; D. SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, p. 55.

¹²⁷ TUE, Article 3, paragraphe 5.

¹²⁸ Cela pourrait conduire à permettre le traitement des données personnelles par des opérateurs étrangers sans que ceux-ci ne soit soumis à la législation de l'Etat partie aux conventions mentionnées et donc contrevenir à la protection effective commandée par la convention européenne des droits de l'homme et la conventions des droits civils et politiques.

¹²⁹ M. TAYLOR, *op. cit.*, p. 247.

¹³⁰ BERNARD-GLANZ C., *op. cit.*, p. 707 ; M. TAYLOR, *op. cit.*, p. 253.

¹³¹ À cet égard l'avocat général observe qu'un "équilibre doit être trouvé entre plusieurs droits fondamentaux, tels que la liberté d'expression, la liberté d'information et la liberté d'entreprise, d'une part, et la protection des données à caractère personnel et de la vie privée des individus, d'autre part."

¹³² BERNARD-GLANZ C., *op. cit.*, p. 711-717 ; C. KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *op. cit.*, p.13.

que les droits de la personne concernée « *prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne* »¹³³. Une telle jurisprudence a pour conséquence de faire prévaloir l'applicabilité des dispositions de la directive « donnée personnelle » lorsqu'elles entrent en conflit avec d'autres droits fondamentaux¹³⁴. D'aucuns critiquent cette jurisprudence, estimant qu'elle conduirait dans certains cas à compromettre le droit à l'information du public ou la liberté d'expression qui constituent des valeurs fondamentales dans un système démocratique tel que celui de l'Union européenne¹³⁵. D'autres critiquent l'absence de justification de la Cour pour faire prévaloir la protection des données personnelles¹³⁶.

Du reste, ces critiques ne proviennent pas exclusivement de la doctrine puisque certains Etats tiers se montrent également opposés à la jurisprudence de la Cour. Comme nous l'avons relevé, la protection des données personnelles n'est pas protégée selon la même intensité dans tous les ordres juridique et l'articulation qui résulte de la jurisprudence de la Cour est loin de faire l'unanimité au sein de la communauté internationale. Les Etats-Unis, par exemple, se montrent très critiques par rapport à la balance des droits fondamentaux qui se dégage de la jurisprudence de la Cour et cela constitue de toute évidence une difficulté importante pour l'application de la directive aux opérateurs établis aux Etats-Unis¹³⁷. En effet, ces derniers voient leur liberté d'expression et d'entreprendre limitée au profit de la protection des données personnelles et une telle articulation entre ces droits fondamentaux ne correspond manifestement pas à la celle qui prévaut aux Etats-Unis.

Pour conclure ce commentaire sur les objectifs de la directive « données personnelles », nous observons que si l'objectif premier de cette directive était d'harmoniser les règles concernant la protection des données afin d'optimiser le marché intérieur, l'attention se déplace progressivement vers la protection des données personnelles. La volonté de protéger les données personnelles a toujours été présente dans le chef du législateur européen mais semble s'autonomiser de plus en plus par rapport au marché intérieur, sans pouvoir, toutefois, s'en détacher complètement. Une telle évolution serait conforme aux préoccupations exprimées par les citoyens européens¹³⁸. Elle est en tout cas visible dans la jurisprudence de la Cour, notamment au travers de l'interprétation orientée vers la protection du citoyen espagnol, que la Cour adopte à l'occasion de l'affaire *Google Spain*. Enfin, la protection des données est également inscrite, depuis le traité de Lisbonne, dans le droit primaire avec l'adoption d'une nouvelle disposition qui prévoit que « *toute personne a droit à la protection des données à caractère personnel la concernant* » ce qui traduit indubitablement l'intérêt croissant de l'Union dans cette matière.

CJUE, 13 mai 2014, *Google et Google Spain*, *op. cit.*, pt. 97.

¹³⁴ BERNARD-GLANZ C., *op. cit.*, p. 716 ; p.13. Soulignons que l'avocat général appelait à « dégager un équilibre correct, raisonnable et proportionné entre la protection des données à caractère personnel, l'interprétation cohérente des objectifs de la société de l'information, et les intérêts légitimes des opérateurs économiques et des internautes au sens large » (conclusions présentées le 25 juin 2013, aff.131/12, pt. 31).

¹³⁵ BERNARD-GLANZ C., *op. cit.*, p. 716 qui cite les conclusions de l'AG, (pt121 et pt 125).

¹³⁶ C.KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *op. cit.*, pp. 20-22.

¹³⁷ KUNER C., « *Google Spain* in the EU and international context », *op. cit.*, pp. 159-162 ; M. TAYLOR, *op. cit.*, p. 246-247 ; M. FAZLIOGLU, « Forget me not : the clash of the right to be forgotten and freedom of expression on the internet », *International Data Privacy Law*, 2013, Volume 3, p. 155 - 156.

¹³⁸ V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 124. L'auteur cite un sondage récent selon lequel plus de 70% des européens se disent concernés à propos de la façon dont les entreprises utilisent leurs données personnelles.

Titre 2. L'applicabilité de la directive 95/46/CE

Dans le premier titre, nous avons précisé la question de l'applicabilité et analysé les objectifs de la directive « données personnelles », ce qui nous a déjà permis d'approcher son domaine d'applicabilité. Ce deuxième titre est consacré à une analyse plus détaillée de l'applicabilité de la directive en elle-même, et plus particulièrement de ses critères d'applicabilité. Notre volonté est d'opérer une analyse générale de ces critères tout gardant à l'esprit la situation de l'affaire *Google Spain* telle que nous l'avons objectivée¹³⁹.

Cette analyse nous conduira à commenter essentiellement deux articles de la directive, à savoir les articles 3 et 4 qui déterminent l'applicabilité que nous avons qualifiée de *stricto sensu* dans le premier titre de cette étude puisqu'elle vise l'application des dispositions de la directive en tant que telle. Néanmoins, nous ne pouvons nous limiter à l'étude exclusive de ces deux dispositions dès lors qu'elles font elles-mêmes appel à des notions définies par d'autres dispositions de la directive. En revanche, nous ne nous pencherons pas directement sur les articles 25 et 26 qui mettent en place le régime spécifique concernant le transfert de données vers un état tiers.

Au cours de l'étude de ces deux dispositions, nous nous rendrons compte qu'en réalité, elles remplissent une double fonction, en particulier s'agissant de l'article 4¹⁴⁰. En effet, cet article délimite non seulement le domaine applicable de la directive à l'aide de critères d'applicabilité mais encore, il détermine la loi de transposition applicable. C'est surtout la première fonction de l'article 4 qui nous intéresse et qui fera l'objet d'une analyse détaillée (Chapitre 1).

Toutefois, il nous faudra consacrer la fin de ce titre au conflit de transposition (Chapitre 2) qui mettra en lumière certaines difficultés rencontrées lors de l'application de l'article 4 de la directive tel qu'il est formulé et interprété actuellement. Ce deuxième chapitre sera plus succinct, d'une part parce qu'il implique des notions qui auront déjà été définies dans le premier chapitre et, d'autre part, parce que le conflit de lois de transposition constitue une difficulté qui, à terme, est vouée à disparaître dès l'entrée en vigueur du règlement qui succèdera à la directive « données personnelles ».

Chapitre 3. Les articles 3 et 4 de la directive 95/46/CE : Les critères d'applicabilité

Dans ce chapitre, nous allons examiner les critères d'applicabilité utilisés par la directive pour déterminer les cas dans lesquels ces dispositions entendent s'appliquer. Comme nous l'avons mentionné ci-avant, ces critères sont localisés dans l'article 4 de la directive. Ils sont au nombre de trois et ne s'appliquent pas cumulativement mais concernent des situations différentes. En d'autres termes, l'application d'un critère exclut l'application des autres¹⁴¹.

¹³⁹ Voy. *infra*, pp. 8-9.

¹⁴⁰ B. HARDY, *op. cit.*, p. 884.

¹⁴¹ J. MOINY, *op. cit.*, p. 263 ; P. BLOK, « Privacy-bescherming in alle staten – Internationaal privacy-recht en I.P.R. onder de Europese Privacy-richtlijn », *Computerr.*, 2005, pp. 301-302. D'ailleurs dans le point 59 à 61 son arrêt *Google Spain*, la Cour n'examinera pas l'application du point (c) du paragraphe 1^{er}, article 4 de la directive car elle jugera applicable le point (a) de la même disposition

Nonobstant leurs différences, ces critères partagent des conditions communes regroupées au sein de l'article 3 (Section 1) qu'il nous faut envisager en premier lieu. Ensuite, il convient d'opérer une analyse individualisée de chaque critère. Toutefois, précisons d'ores et déjà que l'article 4, (1), (b), qui est le siège du deuxième critère, ne sera pas examiné, compte tenu de son faible intérêt pratique¹⁴². En revanche, le critère d'applicabilité contenu à l'article 4, §1^{er}, point (a), retiendra particulièrement notre attention (Section 2) car il s'agit du critère utilisé dans l'affaire *Google Spain* et, plus généralement, du critère le plus souvent appliqué. En outre, le législateur a décidé de le conserver dans le nouveau règlement relatif aux données personnelles. Enfin, il nous restera à examiner le point (c) de l'article 4 qui établit le troisième et dernier critère d'applicabilité et à évoquer son articulation avec le critère du point (a) (section 3).

Section 1. Article 3 : Les conditions générales d'applicabilité de la directive 95/46

La directive « données personnelles » ne peut s'appliquer qu'en présence de *données personnelles* (§1) qui feraient l'objet d'un *traitement* (§2) opéré par un *responsable* (§3) pour l'exercice d'activités qui relèvent du *champ d'application du droit communautaire* (§4) et qui ne constituent pas des *activités exclusivement personnelles ou domestiques* (§5)¹⁴³.

§1. Les données personnelles

Au risque d'une tautologie, la directive relative à la protection des données personnelles protège les données personnelles. Encore faut-il pouvoir déterminer que les données en cause soient effectivement des données personnelles. La directive définit ces données comme « *toute information concernant une personne physique identifiée ou identifiable* »¹⁴⁴ et cite comme exemple un numéro d'identification ou des éléments spécifiques, propres à l'identité physique, physiologique, psychique, économique, culturelle ou sociale de la personne concernée. Ainsi définie, la notion de donnée personnelle ne limite pas l'applicabilité de la directive et permet de couvrir un large éventail de données¹⁴⁵ qui peut dépasser le champ des données protégées par le droit au respect de la vie privée. Cette définition des données personnelles est donc nécessaire pour définir l'applicabilité de la directive « données personnelles » mais en outre, elle permet, de distinguer, théoriquement du moins, le domaine d'applicabilité du droit à la vie privée, de celui de la protection des données personnelles¹⁴⁶.

Comme nous l'avons souligné, la protection des données personnelles est également consacrée au travers de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Dans ce cadre, la Cour européenne des droits de l'homme a défini ce qu'elle entendait par données

¹⁴² Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable (WP 179), adopté le 16 décembre 2010, p. 20. Le point (b), paragraphe 1^{er}, article 4 vise les cas où le droit d'un Etat membre s'applique à un bateau, un avion, une ambassade.

¹⁴³ E. CRUYSMANS et A. STROWEL, *op. cit.*, p. 457.

¹⁴⁴ Directive « données personnelles », Article 2, point (a).

¹⁴⁵ BERNARD-GLANZ C., *op. cit.*, p. 702 ; B. KOOPS, « The trouble with European data protection law », *International Data Privacy Law*, 2014, Volume 4, pp. 256-257. L'auteur critique cette large définition données aux données personnelles estimant que les limites de cette notion ne sont pas clairement identifiées ce qui rend son application très délicate. Il nous faut, toutefois, souligner que la notion de données personnelles ne pose pas de réel problème en pratique et n'a d'ailleurs fait l'objet d'aucun débat dans l'affaire Google ce qui confirme l'avis de l'avocat général qui considéra au point 71 de ses conclusions qu'« il n'est pas nécessaire de se lancer dans une longue discussion pour apporter une réponse positive à cette question. La directive a conféré à la notion de données à caractère personnel une définition large, qu'a appliquée le groupe de travail « Article 29 » et qu'a confirmée la Cour ».

¹⁴⁶ Voy., *supra*, p. 16.

personnelles comme « *toute information relative à un individu identifié ou identifiable* »¹⁴⁷, se rapprochant ainsi de la définition de la directive. En outre, la Cour de Strasbourg, observe que ces données ont été « *collectées et stockées systématiquement* »¹⁴⁸ sans préciser explicitement s'il s'agissait d'une condition supplémentaire nécessaire à la qualification de données personnelles¹⁴⁹. Si la question paraît encore ouverte dans le cadre de la CEDH, il n'en va pas de même s'agissant de la directive « données personnelles ». Cette dernière précision qui restreindrait le domaine d'application de la directive n'a, en effet, jamais été évoquée par la Cour de Luxembourg.

Notons également, que, si la définition des données protégées par la directive « données personnelles » est très large, celle-ci n'a *a priori* pas vocation à protéger des informations techniques ou commerciales. Les premières sont essentiellement protégées par des brevets et les secondes font l'objet d'une proposition de directive sur les secrets d'affaires. Au surplus, les données des personnes morales, particulièrement concernées par la protection des informations techniques et commerciales, sont exclues de la directive « données personnelles », qui vise exclusivement les personnes physiques¹⁵⁰. Toutefois, il n'est pas exclu que des informations commerciales concernant des personnes physiques, rentrent dans la définition des données personnelles, créant ainsi un chevauchement potentiel entre le champ d'application de la future directive « secrets des affaires » et celui de la directive « données personnelles »¹⁵¹.

Enfin, précisons que si la directive « données personnelles » protège toutes les données personnelles, elle en distingue, parmi ces dernières, certaines qu'elle qualifie de plus sensibles en raison de leur contenu. Il en résulte une interdiction de principe¹⁵² concernant leur traitement mais le domaine d'application de ces dispositions relatives aux données plus sensibles demeure inchangé.

§2. Le traitement

« *Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel* »¹⁵³ constitue un traitement de données personnelles au sens de la directive « données personnelles ». La directive vise ainsi une très grande variété d'opérations, en atteste la liste d'exemples qui vient illustrer cette définition¹⁵⁴. La latitude de cette notion est confirmée, voire amplifiée, par l'interprétation qu'en fait la Cour, pour qui la simple « *opération consistant à faire figurer, sur une page internet, des données à caractère personnel* »¹⁵⁵ constitue un traitement de données. La définition est à ce point large qu'à notre sens, dès qu'il est question de données personnelles, il y a

¹⁴⁷ CEDH, Aff. *Amann v. Switzerland* [GC], *op. cit.*, § 65 ; CEDH, Aff. *Rotaru v Romania* [GC], *op. cit.*, § 43.

¹⁴⁸ CEDH, Aff. *Rotaru v Romania* [GC], *op. cit.*, § 44.

¹⁴⁹ J. KOKOTT & C. SOBOTTA, *op. cit.*, p. 225. Les auteurs, semblent suggérer que la Cour européenne ajoute cette condition à la définition de données personnelles.

¹⁵⁰ Directive « données personnelles », article 1^{er}, paragraphe 1^{er}.

¹⁵¹ Voy. Proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, COM(2013)813 final, les Considérants 23 et 24 et Article 8, point (4).

¹⁵² Directive « données personnelles », Article 8, § 1^{er}, prévoit l'interdiction du traitement de données à caractère personnelles qui relèvent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Notons, que le paragraphe 2 de cette disposition prévoit certaines exceptions.

¹⁵³ Directive « données personnelles », Article 2, point (b).

¹⁵⁴ L'article 2, (b), de la directive « données personnelles » cite la collecte, l'enregistrement, l'organisation, 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 ainsi que le verrouillage, l'effacement ou la destruction

¹⁵⁵ CJUE, 13 mai 2014, *Google et Google Spain*, *op. cit.*, pt 26. La Cour rappelle ainsi sa jurisprudence issue de l'arrêt *Lindqvist*.

nécessairement un traitement au sens de la directive. En d'autres termes, il n'y a pas un seuil minimum de manipulations ou d'opérations à effectuer pour que la directive s'applique. Une simple consultation, conservation ou collecte des données suffit pour que la directive soit applicable.

A la lumière de ces considérations, il semble très difficile pour un opérateur de contester que ses activités constituent un traitement de données. *Google* s'y est pourtant essayé en soutenant que dans son activité, il ne distinguait pas les données personnelles des autres informations et que les données en cause sont accessibles sur internet, indépendamment de son action¹⁵⁶. La Cour, conformément aux conclusions de l'avocat général, a rejeté ces deux arguments¹⁵⁷. Elle considère qu'il est sans importance que les données en question aient déjà fait l'objet d'une publication, ajoutant même qu'une telle exception risquerait de vider la directive de sa substance, et que les données personnelles soient traitées indistinctement des autres informations¹⁵⁸.

S'agissant des moteurs de recherche, la Cour ajoute, que leur activité « *joue un rôle décisif dans la diffusion globale des données* »¹⁵⁹ en favorisant l'accessibilité de ces données auprès des internautes. En effet, il est indéniable que les moteurs de recherche ont un effet multiplicateur sur la visibilité et l'accessibilité des données personnelles ainsi que sur l'information en général. Par conséquent, leurs activités sont susceptibles « *d'affecter significativement les droits fondamentaux de la vie privée et de la protection des données à caractère personnel* »¹⁶⁰. Pour l'avocat général, les moteurs recherche conditionneraient même « *l'accessibilité universelle* »¹⁶¹ des informations sur internet. C'est donc un raisonnement très pragmatique de la Cour, qui pouvait difficilement faire autrement sous peine de rendre la directive inapplicable aux activités d'un acteur majeur dans la diffusion des données personnelles sur internet. En outre, l'interprétation de la Cour est tout à fait conforme aux exemples d'opération constituant un traitement, cités par la directive¹⁶².

Nous observons, enfin, que si certaines données sont considérées comme sensibles et font l'objet d'un régime de protection plus strict, le législateur européen ne fait pas de distinction entre les différents traitements alors qu'il se peut que certains traitements, soient susceptibles d'avoir un impact plus important que d'autres, sur la protection des données personnelles, notamment en fonction du média utilisé.

§3. Le responsable du traitement

Au vu des deux paragraphes précédents, il n'est pas contestable, à l'instar de ce que la Cour a décidé, que *Google* réalise un traitement de données personnelles au travers de ses activités de moteur de

¹⁵⁶ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt 22. L'argument nous paraît ici inopérant. En effet, dans ce point de l'arrêt, la Cour explique que le moteur de recherche traite « *les informations accessibles sur internet [...] sans faire le tri entre les données à caractère personnel et les autres informations* ». Cet argument ne paraît pas de nature à exclure la qualification de traitement aux activités de *Google* mais éventuellement d'éviter que le moteur de recherche soit considéré comme le responsable du traitement. Nous le verrons cet argument relatif à la notion de responsable du traitement, quand bien même il serait exact, s'avèrera être également inopérant.

¹⁵⁷ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pts 27 et 28.

¹⁵⁸ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pts 29 et 30..

¹⁵⁹ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt 36.

¹⁶⁰ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt 38. Cette phrase souligne et illustre l'importance accordée aux droits fondamentaux dans l'interprétation de la Cour, ici à propos du traitement et des activités du moteur de recherche.

¹⁶¹ Conclusions présentées le 25 juin 2013, aff.131/12, pts. 45-46 ; BERNARD-GLANZ C., op. cit., pp. 703-704.

¹⁶² CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt 28, la Cour vise notamment les opérations de collecte, d'organisation et de mise à disposition.

recherche. Toutefois, il reste à déterminer si *Google* est bien responsable de ce traitement de données personnelles.

Si la notion de responsable du traitement n'apparaît pas dans l'article 3 de la directive, elle est néanmoins centrale dans l'article 4 quel que soit le critère d'applicabilité employé. En outre, il nous semble impossible d'évoquer la notion de traitement sans celle de responsable du traitement¹⁶³. De fait, tout traitement de données nécessite qu'une ou plusieurs personnes mettent des moyens en place et vise souvent un objectif défini. Ce sont précisément ces deux éléments utilisés que la directive utilise pour définir un responsable du traitement. En l'occurrence, il s'agit de la « *personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* »¹⁶⁴. Le critère essentiel est donc bien la détermination de la finalité et des moyens et aucune importance n'est véritablement accordée à la détention matérielle des données personnelles traitées¹⁶⁵.

Par conséquent, dès lors qu'un opérateur traite des données en déterminant la finalité et les moyens de ce traitement, il doit être qualifié de responsable du traitement. A cet égard, la Cour a considéré que *Google* répondait à ces critères et qu'il était donc le responsable du traitement. Nous ne pouvons qu'acquiescer la décision de la Cour puisque *Google* détermine à la fois la finalité du traitement des données, à savoir être en mesure de fournir une liste de résultats classés et indexés lorsqu'une recherche lui est soumise, et les moyens, à l'exemple de l'algorithme utilisé pour établir le classement.

Toutefois, *Google* a contesté être le responsable du traitement en réitérant les deux arguments utilisés pour contester le fait que ses activités constituaient un traitement. En effet, selon *Google*, il ne pourrait pas être tenu comme responsable du traitement des données, car les données en question sont déjà accessibles sur des sites internet dont le contenu relève de la responsabilité de leur éditeur¹⁶⁶. Dans le cas contraire, *Google* soutient que cela reviendrait à déplacer la responsabilité de ces éditeurs sur les moteurs de recherche qui ne font que classer et indexer ces sites internet. En d'autres termes, *Google* tente d'affirmer qu'il ne pourrait être considéré comme responsable puisqu'il n'a pas de contrôle sur les données personnelles que traitent les sites internet qu'il référence.

Cependant, en déterminant lui-même les moyens avec lesquels il réalise son référencement, *Google* dispose en réalité d'un certain contrôle sur le classement qu'il établit et, par conséquent, sur les données dont il facilite la diffusion¹⁶⁷. En outre, comme la Cour l'a constaté, le traitement des données réalisé par les moteurs de recherche est susceptible d'avoir un effet distinct et additionnel à celui du traitement

¹⁶³ Dans l'affaire *Google Spain*, la Cour examine d'ailleurs ces deux questions simultanément aux points 21 et s.

¹⁶⁴ Directive « données personnelles », Article 2, (d).

¹⁶⁵ M. WALRAVE, *Privacy Gescand? Direct marketing en de bescherming van de persoonlijke levenssfeer*, Leuven, Universitaire Pers Leuven, 1999, p. 224 ; J. MOINY, *op. cit.*, p. 247.

¹⁶⁶ A notre sens, cela rejoint dans une certaine mesure l'Avis 1/2008 du Groupe de Travail « Article 29 » sur les aspects de la protection des données liés aux moteurs de recherche (WP 148), adopté le 4 avril 2008, pp. 14-15 et p. 27. Le groupe de travail « article 29 » y distingue « les deux principaux rôles des fournisseurs de moteurs de recherche [...], celui de responsables du traitement des données d'utilisateur (qu'ils collectent auprès des utilisateurs et leur historique de recherche propre), [pour lequel] ils doivent être tenus pour entièrement responsables » et « celui de fournisseurs de données de contenu, [pour lequel] en général ils ne doivent pas être considérés comme les principaux responsables » ; BERNARD-GLANZ C., *op. cit.*, pp. 687-688 ; B. HARDY, *op. cit.*, pp. 882-883.

¹⁶⁷ E. CRUYSMANS et A. STROWEL, *op. cit.*, p. 457.

exécuté par l'éditeur du site internet¹⁶⁸. Ceci explique que le traitement opéré par *Google* peut être mis en cause en tant que tel, c'est-à-dire, alors même que les données en question demeureraient présentes sur un site internet¹⁶⁹. L'inverse reviendrait à nier l'effet décisif du référencement de *Google* et, plus généralement, à permettre aux moteurs de recherche d'éviter l'application des dispositions de la directive puisque ces derniers renvoient nécessairement à des données déjà publiées lorsqu'ils classent et référencent des sites internet.

De plus, *Google* ajoute qu'il n'est pas responsable du traitement des données personnelles dans la mesure où il traite indistinctement ces données et toute autre information¹⁷⁰. Pour reprendre les termes de l'avocat général, les activités du moteur de recherche consistent simplement en « *la localisation d'informations publiées ou placées sur internet par des tiers, leur indexation automatique, leur stockage temporaire, et, enfin, leur mise à disposition aux internautes selon un ordre de préférence donné* »¹⁷¹. Dans la suite de son raisonnement, l'avocat général considère, à l'instar de *Google*, que le responsable du traitement ne peut être qualifié comme tel que s'il « *est conscient de l'existence d'une certaine catégorie définie d'information correspondant à des données personnelles, et qu'il les traite en étant animé de quelque intention* »¹⁷². L'avocat général conclura ainsi que *Google* n'est pas responsable du traitement de données¹⁷³. *A priori*, il nous semble qu'une telle interprétation rajoute un élément moral dans la définition du responsable, qui pourrait avoir des conséquences pratiques considérables, notamment en ce qui concerne la charge de la preuve ; sur qui repose la charge de prouver l'existence de cette intention et peut-elle se présumer ?

Au vu de la définition de responsable du traitement de la directive « données personnelles », il nous faut reconnaître qu'il n'est, toutefois, pas dépourvu de sens de considérer que déterminer les moyens et les finalités du traitement impliquent que le responsable ait conscience du caractère personnel des données qu'il traite. Reste néanmoins, comme le concède l'avocat général, que considérer *Google* comme responsable du traitement peut « *aisément être défendu en tant que conclusion logique d'une interprétation littérale, voire téléologique, de la directive, étant donné que les définitions de base de la directive ont été formulées de manière exhaustive afin de couvrir les nouvelles évolutions* »¹⁷⁴.

Enfin, le rôle toujours plus actif que toute personne peut occuper sur internet, implique nécessairement de s'interroger sur le statut des utilisateurs privés. En d'autres termes, il convient de se demander si un particulier peut être qualifié de responsable du traitement de données personnelles, et

¹⁶⁸ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt 38.

¹⁶⁹ En l'occurrence c'est le cas dans l'affaire *Google* s'agissant des articles du quotidien espagnol contre lesquels la requête de la personne concernée a été rejeté par l'agence espagnole. De manière très concrète, il est probable que ce qui gêne le plus la personne concernée n'est pas que les articles demeurent présents sur le site du quotidien espagnole mais que des liens vers ces articles apparaissent lorsqu'une recherche est lancé à partir de son nom, ce qui démontre bien l'importance et l'impact du référencement de *Google* sur les données personnelles, particulièrement sur le diffusion, et illustre l'effet additionnel dont parle la Cour.

¹⁷⁰ CJUE 13 mai 2014, *Google et Google Spain*, op. cit., pts 22-24.

¹⁷¹ Conclusions présentées le 25 juin 2013, aff.131/12, pt. 70 ; BERNARD-GLANZ C., op. cit., pp. 705-706.

¹⁷² Conclusions présentées le 25 juin 2013, aff.131/12, pt. 82.

¹⁷³ Pour atteindre cette conclusion, l'avocat général fera également référence à l'argument développé ci-avant selon lequel *Google* « *n'exerce pas de contrôle sur les données à caractère personnelle figurant sur les pages web des tiers* » (conclusions présentées le 25 juin 2013, aff.131/12, pt. 84).

¹⁷⁴ Conclusions présentées le 25 juin 2013, aff.131/12, pt. 82. Comme nous l'avons précisé, l'avocat général défendra toutefois le point de vue contraire dans ses conclusions.

donc se voir appliquer les dispositions de la directive ? Nous examinerons cette question dans le dernier paragraphe de cette section.

§4. Le champ d'application du droit communautaire

L'article 3, §2, premier tiret, de la directive « données personnelles » prévoit que cette dernière « *ne s'applique pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relève pas du champ d'application du droit communautaire* ». Cette disposition peut paraître étonnante, voire inutile, puisqu'il semble logique que cette directive ne puisse pas s'appliquer au-delà des matières dont l'Union a la compétence¹⁷⁵. Néanmoins, nous l'avons souligné antérieurement, cette obligation de demeurer dans le champ d'application du droit communautaire n'empêche pas la directive de trouver à s'appliquer aux situations purement internes ainsi que, dans une certaine mesure, aux situations qui impliquent un état tiers¹⁷⁶.

Relevons qu'en pratique, l'article 3, §2, premier tiret, a été soulevé dans deux affaires afin d'éviter l'application de la directive au traitement en cause. En l'occurrence, il fut contesté que l'activité, pour laquelle le traitement des données était mis en œuvre, relevait du champ d'application du droit communautaire car, d'une part, cette activité ne se rapportait pas à l'exercice des libertés garanties par le droit primaire et, d'autre part, elle ne présentait pas de lien avec le fonctionnement et l'établissement du marché intérieur pourtant nécessaire au vu de l'article 114, TFUE, constituant la base légale de la directive¹⁷⁷.

La Cour a répondu dans la première affaire « *que le recours à la base juridique de l'article 100 A du traité [actuelle l'article 114 TFUE] ne présuppose pas l'existence d'un lien effectif avec la libre circulation entre États membres dans chacune des situations visées par l'acte fondé sur une telle base* »¹⁷⁸ et la Cour d'ajouter que « *ce qui importe [...] c'est que l'acte adopté sur ce fondement ait effectivement pour objet l'amélioration des conditions de l'établissement et du fonctionnement du marché intérieur* »¹⁷⁹. La Cour considéra, en outre, que la manière dont les exceptions étaient rédigées dans la directive « données personnelles » confirmait une telle interprétation, à savoir que ladite directive n'était pas « *exclusivement applicable à des situations comportant un lien suffisant avec l'exercice des libertés de circulation* »¹⁸⁰.

Dans la seconde affaire, la Cour a rappelé sa jurisprudence en ce que la base juridique en question « *ne présuppose pas l'existence d'un lien effectif avec la libre circulation [...] dans chacune des situations visées* »¹⁸¹ avant de préciser que « *dans ces conditions, il ne serait pas approprié d'interpréter l'expression « activités qui ne relèvent pas du champ d'application du droit communautaire » comme ayant une portée telle qu'il serait nécessaire de vérifier, au cas par cas, si l'activité spécifique en cause affecte directement la*

¹⁷⁵ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 515-517. Prévoir l'inverse reviendrait à violer les Traités et le principe de spécialisation.

¹⁷⁶ Voy. *supra.*, pp. 18-19.

¹⁷⁷ V. REDING, « The European data protection framework for the twenty-first century », op. cit., p. 123.

¹⁷⁸ CJCE, 20 mai 2003, C-465/00, C-138/01, C-139/01, *Rechnungshof*, op. cit., pt. 41 ; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., pp. 516-518.

¹⁷⁹ CJCE, 20 mai 2003, C-465/00, C-138/01, C-139/01, *Rechnungshof*, op. cit., pt. 41.

¹⁸⁰ CJCE, 20 mai 2003, C-465/00, C-138/01, C-139/01, *Rechnungshof*, op. cit., pt. 43 ; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 517.

¹⁸¹ CJCE, 6 novembre 2003, aff. C-101/01, *Procédure pénale c. Bodil Lindqvist*, op. cit., point 40 ; C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », obs. sous CJCE, arrêt du 6 novembre 2003, Bodil Lindqvist, affaire C-101/01, *Revue du droit des technologies de l'information*, 2004, pp. 67-99.

libre circulation entre États membres »¹⁸². Dans la même affaire, la Cour a estimé que les exemples mentionnés dans l'article 3, §2, premier tiret « *sont destinées à définir la portée de l'exception* »¹⁸³. En outre, les exceptions prévues par ladite disposition ne s'appliquent qu'aux seuls exemples qu'elle mentionne et aux activités « *qui peuvent être rangées dans la même catégorie* »¹⁸⁴.

Au surplus, il nous faut constater que cette jurisprudence tire ses racines de l'arrêt *British American Tobacco*. Toutefois, si dans cet arrêt concernant les produits du tabac, la Cour a admis la possibilité pour une disposition adoptée sur base de l'article 114, TFUE, de poursuivre un autre objectif parallèlement à l'établissement et au fonctionnement du marché intérieur, dans les deux affaires susmentionnées, la Cour va plus loin en permettant l'application d'un texte adopté sur base de l'article 114, TFUE, à une situation qui ne présente aucun lien, à tout le moins aucun lien direct, avec les libertés de circulation¹⁸⁵.

Il semble, cependant, que s'agissant du nouveau règlement, un tel raisonnement ne sera plus nécessaire pour justifier de l'application de la directive à des situations étrangères aux libertés de circulation, telles que celles en cause dans les arrêts précités. En effet, le règlement qui est destiné à succéder à la directive « données personnelles », a été adopté sur autre base juridique, à savoir l'article 16, TFUE, qui consacre la protection des données personnelles en tant que telle¹⁸⁶. Dès lors, il nous semble qu'il n'est plus indispensable de justifier expressément l'application de la réglementation au travers des libertés de circulation.

Enfin, remarquons que dans son nouveau règlement, le législateur européen maintient la disposition qui nous avait déjà étonné dans la directive, et qui précise que le « *règlement ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union* »¹⁸⁷.

§5. Les activités exclusivement personnelles ou domestiques

Outre la limitation relative au champ d'application du droit communautaire, l'article 3, §2, de la directive « données personnelles » prescrit une seconde limitation. Celle-ci prévoit que la directive ne s'applique pas au traitement de données personnelles « *effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques* ». Le considérant 12 de la directive cite comme exemple d'activités exclusivement personnelles ou domestiques « *la correspondance et la tenue de répertoires d'adresses* ». C'est sur cette base que la Cour a interprété cette limitation comme « *visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers* »¹⁸⁸.

¹⁸² CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, point 42. La Cour considère l'exception de l'article 3, §2, premier tiret, de la directive « données personnelles » ne s'applique pas contrairement aux conclusions de l'avocat général, voy. pt 44. Ce dernier a considéré que « *ne relève pas du champ d'application de la directive un traitement de données à caractère personnel consistant en la création, sans aucun but lucratif, d'une page d'accueil du type de celle en cause, qui est exclusivement destinée à servir de support à une activité de catéchiste exercée, à titre bénévole et en dehors de toute relation de travail* ».

¹⁸³ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, p. I-12971, point 44.

¹⁸⁴ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, p. I-12971, point 44.

¹⁸⁵ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, pp. 517-518..

¹⁸⁶ V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 124.

¹⁸⁷ Règlement général sur la protection des données, Article 2, §2, point (a).

¹⁸⁸ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, point 47. L'interprétation de cette exception par la Cour est très proche de celle proposée par l'avocat général qui parle « *d'activités manifestement privé et confidentielles destinées à ne pas sortir de la sphère personnelle ou domestique* ».

La question à laquelle la Cour a été confrontée dans l'arrêt *Lindqvist* consistait à déterminer si « le traitement de données à caractère personnel tel que celui visé [à savoir, faire référence, sur une page Internet, à diverses personnes et les identifier soit par leur nom, soit par d'autres moyens¹⁸⁹] relève de l'une des exceptions figurant à l'article 3, paragraphe 2, de la directive 95/46 »¹⁹⁰. Assez logiquement, la Cour a jugé qu'un tel traitement ne pouvait se soustraire à l'application de la directive. En effet, par essence, la diffusion de données sur internet rend ces dernières « accessibles à un nombre indéfini de personnes »¹⁹¹ et, partant, le seul constat possible est que le « traitement effectué échappe clairement à la sphère personnelle et domestique »¹⁹².

Il nous faut ainsi observer qu'à la lumière de cet arrêt, les cas d'application de cette seconde exception apparaissent relativement limités. Ceci étant dit, une conséquence plus remarquable se manifeste à la suite du raisonnement de la Cour : toute personne physique ou morale, en ce compris les particuliers, est susceptible de glisser dans le domaine d'applicabilité de la directive données personnelles, dès lors qu'elle opère un traitement de données personnelles sur internet, en particulier si ce traitement consiste en une diffusion des dites données. A cet égard, étant donné qu'un site internet est en principe également accessible à partir d'un pays tiers, tel que c'est le cas dans l'affaire *Lindqvist*, il faudrait considérer ce traitement comme « un transfert de données vers des pays tiers » au sens de la directive, ce qui implique l'application d'un régime spécifique plus restrictif. Si cette interprétation devait se confirmer, le régime spécifique mis au point par le législateur européen trouverait en réalité à s'appliquer de manière bien plus fréquente que ce dernier ne l'avait imaginé¹⁹³.

A notre sens, l'affaire en cause illustre ainsi un double phénomène que le législateur européen n'a pu anticiper au moment de l'adoption de la directive « données personnelles ». Le premier phénomène dont le législateur n'a pu tenir compte, notamment lorsqu'il a réglementé le transfert de données vers des pays tiers, est l'émergence d'internet. Ce constat est d'ailleurs confirmé par la Cour, « *Eu égard, d'une part, à l'état du développement d'Internet à l'époque de l'élaboration de la directive 95/46 et, d'autre part, à l'absence, dans son chapitre IV, de critères applicables à l'utilisation d'Internet, on ne saurait présumer que le législateur communautaire avait l'intention d'inclure prospectivement dans la notion de «transfert vers un pays tiers de données» l'inscription [...] de données sur une page Internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder* ».

A fortiori, le deuxième phénomène, lié à l'émergence du Web dit « 2.0 »¹⁹⁴, n'a pu être anticipé par le législateur européen. Il s'agit du rôle plus « actif » que peut désormais adopter tout particulier sur internet. En effet, à l'heure actuelle, tout internaute est susceptible de diffuser, communiquer, transmettre mais aussi modifier ou adapter des données présentes sur internet. Ce qui tranche avec l'attitude passive à

¹⁸⁹ Préablement, au point 27 de l'arrêt *Lindqvist*, la Cour avait qualifié de traitement de données personnelles « l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens ». Ce qui ne nous étonnera pas au vu de la définition large de la notion de traitement.

¹⁹⁰ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, point 29.

¹⁹¹ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, point 47.

¹⁹² Conclusions présentées le 19 septembre 2002, aff. 101/02, pt. 34.

¹⁹³ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, *op. cit.*, point 69.

¹⁹⁴ W. ROUSH, « 'Web 2.0' has arrived », *MIT Technology Review*, 2005, <https://www.technologyreview.com/s/404799/web-20-has-arrived/> (consulté le 29 juin 2016).

laquelle il était bien souvent contraint par le passé, à savoir la consultation des informations mises en ligne¹⁹⁵.

Ainsi, dans l'affaire *Lindqvist*, la Cour a donc considéré que faire référence à diverses personnes et les identifier sur une page Internet, constituait un traitement de données personnelles qui ne relevait d'aucune des deux exceptions prévues par l'article 3, §2, de directive « données personnelles »¹⁹⁶. La question qui s'est encore posée à la Cour était de savoir si le traitement en cause devait être qualifié de « transfert de données vers des pays tiers »¹⁹⁷. Nous l'avons souligné, *a priori*, une réponse positive ne serait pas étonnante puisqu'en principe un site internet est accessible mondialement. Toutefois, comme la Cour l'a constaté, cela impliquerait que « le régime spécial [...] de ladite directive deviendrait donc nécessairement, en ce qui concerne les opérations sur Internet, un régime d'application générale »¹⁹⁸. Ceci, alors qu'il ne saurait être présumé « que le législateur communautaire avait l'intention d'inclure prospectivement dans la notion de «transfert vers un pays tiers de données» l'inscription [...] de données sur une page Internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers »¹⁹⁹ et, qu'en outre, « dès que la Commission constaterait, en application de l'article 25, paragraphe 4, de la directive 95/46, qu'un seul pays tiers n'assure pas un niveau de protection adéquat, les États membres seraient obligés d'empêcher toute mise sur Internet de données à caractère personnel »²⁰⁰. En d'autres termes, considérer qu'un transfert de données vers des pays tiers a lieu à chaque fois que des données sont téléchargées sur internet, ne paraît pas conforme à la volonté du législateur et soulèverait également des problèmes d'application considérables²⁰¹.

Ces différentes considérations ont amené la Cour à juger qu'il n'y avait pas en l'espèce de « transfert vers un pays tiers de données » au sens de la directive « données personnelles », à tout le moins à la suite des opérations effectuées par Mme *Lindqvist*²⁰². Si les motivations de la Cour pour éviter l'application de la directive s'avèrent évidentes et pragmatiques, la justification apportée par la Cour dans l'affaire *Lindqvist* apparaît, à tout le moins, étonnante²⁰³. En effet, la Cour considère que les opérations effectuées par Mme *Lindqvist* ne constituent pas un «transfert vers un pays tiers de données» car « les données à caractère personnel qui arrivent sur l'ordinateur d'une personne située dans un pays tiers, en provenance d'une personne qui les a chargés sur un site Internet, n'ont pas été transférées directement entre ces deux personnes mais au travers de l'infrastructure informatique du fournisseur de services d'hébergement où la page est stockée »²⁰⁴ et la Cour d'ajouter que la « question posée par la juridiction de renvoi ne concerne que ces opérations [à savoir celles de Mme *Lindqvist*], à l'exclusion de celles effectuées par les fournisseurs de services d'hébergement »²⁰⁵.

¹⁹⁵ C. KUNER, *Transborder data flows and data privacy law*, op. cit., p. 14.

¹⁹⁶ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 48.

¹⁹⁷ C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », op. cit., pp. 89 et s.

¹⁹⁸ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 69.

¹⁹⁹ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 68.

²⁰⁰ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 69.

²⁰¹ C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », op. cit., pp. 89-91.

²⁰² CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 70.

²⁰³ C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », op. cit., pp. 92-93.

²⁰⁴ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 61.

²⁰⁵ CJCE, 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, C-101/01, op. cit., point 62.

En réalité, nous pouvons considérer que la Cour n'exclut pas totalement que le téléchargement des données sur une page internet résulte en un «transfert vers un pays tiers de données», mais elle convient qu'en tout cas, si transfert il y a, ce transfert ne serait pas opéré par la personne qui télécharge les données. Du reste, elle ne se prononce pas sur la possibilité qu'il y ait un transfert du *fournisseur de services d'hébergement* et, partant, n'exclut pas cette éventualité qui comporte les mêmes inconvénients que ceux décrits ci-dessus, à savoir l'application générale du régime spécifique.

Par ailleurs, cette justification n'est pas exempte de critique par rapport à la notion de responsable du traitement ; il est évident que la responsable du traitement est la personne qui télécharge les données sur internet puisqu'elle détermine elle-même la finalité et les moyens du traitement. Selon nous, il serait donc contraire à la directive de désigner le fournisseur de service d'hébergement comme responsable du transfert de données vers un pays tiers.

De manière très subjective, il nous semble que cet arrêt pourrait aussi se lire à la lumière d'une distinction entre particulier et professionnel, même si rien dans la directive ne permet d'appuyer cette distinction et que la Cour n'en parle absolument pas, à tout le moins explicitement. En effet, elle considère que les activités de Mme *Lindqvist*, particulier, ne constituent pas un transfert de données vers un pays tiers, mais n'exclut, toutefois, pas que les activités du fournisseur de service d'hébergement, professionnel, en soient un. Quelle aurait été la réponse de la Cour si le téléchargement n'avait pas été effectué par Mme *Lindqvist* mais par un opérateur comme *Google* ou *Facebook* ?

À notre sens, certains arguments pourraient justifier une telle distinction. Imposer le même régime aux opérateurs professionnels et aux particuliers peut être attentatoire à la liberté d'expression de ces derniers, qui pourraient ne pas être en mesure d'assumer les mêmes obligations que les opérateurs professionnels. De plus, vérifier la bonne application d'un régime complexe à toutes les opérations effectuées par des particuliers sur internet semble illusoire. Dès lors, ne vaut-il pas mieux leur appliquer un régime assoupli ? La question pourrait s'avérer intéressante d'autant plus qu'une telle distinction entre professionnel et particulier existe déjà dans d'autres réglementations européennes, s'agissant par exemple du droit à la consommation²⁰⁶. Reste, toutefois, qu'une protection des données personnelles est nécessaire, peu importe que le traitement soit réalisé par un opérateur professionnel ou un particulier.

Quoi qu'il en soit, ce qui ressort manifestement de l'affaire *Lindqvist*, c'est la nécessité de prendre en compte l'émergence et l'utilisation d'internet dans la réglementation des données personnelles²⁰⁷.

²⁰⁶ Directive 2011/83/UE du Parlement européen et du Conseil, du 25 octobre 2011, relative aux droits des consommateurs, modifiant la Directive 93/13/CEE du Conseil et la Directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la Directive 85/577/CEE du Conseil et la Directive 97/7/CE du Parlement européen et du Conseil, JOUE, 2011, L 304/64.

²⁰⁷ C. DE TERWANGNE, « Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *op. cit.*, p. 95. L'auteur considère discute la question de soumettre internet à un régime spécifique et considère qu'« *internet est un média qui présente des risques particuliers tenant notamment à son accessibilité mondiale et à la perte de contrôle qu'il engendre sur les données mises à disposition. Il est donc normal que l'utilisation de ce média soit soumise à un régime (légèrement) plus strict que le régime général* ».

Section 2. Article 4 : Les critères d'applicabilité alternatifs et exclusifs

§1. Article 4, §1^{er}, (a) : « Le cadre des activités d'un établissement »

Nous venons d'examiner les conditions nécessaires à l'application de la directive. A cet égard, l'article 3 précise que les seules situations visées sont celles qui impliquent un traitement de données personnelles lié à l'exercice d'activités relevant du champ d'application du droit communautaire. Il faut encore déterminer quel est le lien de connexion entre ces situations que la directive entend régir, et l'Union européenne, afin de justifier l'application du droit de l'Union. C'est l'objet de cette section et de la suivante.

Le premier critère d'applicabilité énoncé par la directive prévoit que la loi de transposition des Etats membres, et à travers elle la directive, s'applique lorsque « *le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre* »²⁰⁸ (nous soulignons). Nous avons déjà examiné les notions de traitement et de responsable, il nous faut maintenant compléter l'analyse en s'intéressant à celles d'*établissement* (paragraphe 1) et de *cadre des activités* (paragraphe 2).

1. Un établissement

Contrairement aux notions étudiées ci-avant, la directive « données personnelles » ne définit pas ce qu'elle entend par « *un établissement* ». Toutefois, comme la Cour l'indique²⁰⁹, le considérant 19 précise que la notion d'établissement implique « *l'exercice effectif et réel d'une activité au moyen d'une installation stable* » et ajoute que « *la forme juridique retenue pour un tel établissement [...] n'est pas déterminante* ». En d'autres termes, il importe peu que l'établissement dispose ou non de la personnalité juridique.

A défaut d'une définition donnée par la directive, il est possible de se référer à la jurisprudence de la Cour qui, dans le cadre de la liberté d'établissement²¹⁰, définit un établissement stable comme « *la réunion permanente de moyens humains et techniques nécessaire aux prestations de service en cause* »²¹¹. Toujours sur base de la jurisprudence en matière de liberté d'établissement, certains auteurs se sont penchés sur la question du lien entre l'opérateur et son établissement au sens de la directive²¹². A cet égard, lorsqu'il est question d'une filiale ou d'une succursale, la relation entre les deux entités ne pose pas de problème. La filiale ou la succursale qui opère le traitement de données sera, selon toute vraisemblance, qualifiée d'établissement du responsable²¹³. Néanmoins, la solution ne semble pas aussi limpide lorsqu'un opérateur tiers opère un traitement de données pour le compte d'une autre société. Cet opérateur tiers, pourrait-il être considéré comme un établissement de la société en question ou est-il

²⁰⁸ Directive « données personnelles », Article 4, § 1^{er}, point (a).

²⁰⁹ CJUE, 13 mai 2014, *Google et Google Spain*, *op. cit.*, pt. 48 ; B. HAVELANGE et A. LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *Journal des tribunaux*, 2012, p. 243 ; J. MOINY, *op. cit.*, pp. 259-260.

²¹⁰ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 20 ; J. MOINY, *op. cit.*, pp. 259-260.

²¹¹ CJCE, 4 juillet 1985, aff. 168/84, *Gunter Berkholz c. Finanzamt Hamburg-Mitte-Altstadt*, *Rec.*, 1985, p. 2251, pt 18. et CJCE, du 7 mai 1998, aff. C-390/96, *Lease Plan Luxembourg SA contre Belgische Staat*, *Rec.* 1998, p. I-2553, 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 services publicitaires avec Google Inc.

²¹² 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? », *op. cit.*, pp. 34-35 ; L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, pp. 98-100.

²¹³ 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? », *op. cit.*, p. 35

nécessairement le responsable du traitement ? Au vu de la jurisprudence de la Cour en matière de liberté d'établissement, la réponse dépend du degré d'indépendance de l'opérateur tiers. Ce degré d'indépendance est généralement fonction, entre autres, de la possibilité pour l'opérateur tiers d'agir pour le compte de sociétés concurrentes ou d'organiser lui-même son travail²¹⁴. A notre sens, si la question venait à se poser en pratique dans le cadre de la protection données personnelles, nul doute que la possibilité de déterminer les moyens du traitement serait fondamentale²¹⁵ en vue de qualifier l'opérateur tiers d'établissement. Ajoutons, en outre, qu'un opérateur tiers ne serait considéré comme un établissement d'une autre société que dans des circonstances très particulières²¹⁶.

Au demeurant, comme le rappelle le Groupe de travail « article 29 » sur la protection des données, il n'est « *pas certain que cette interprétation et celles données ultérieurement par la CJUE concernant la liberté d'établissement prévue par l'article 50 du traité UE puissent s'appliquer intégralement aux situations visées à l'article 4 de la directive sur la protection des données* »²¹⁷. En outre, précisons que dans l'affaire *Google Spain*, la qualification d'établissement de *Google Spain*, n'a pas été contestée par *Google Inc*²¹⁸. De manière générale, la question de la qualification d'établissement ne suscite que peu de débats en jurisprudence dans le cadre de la directive « données personnelles », mais elle n'en est pas moins porteuse d'enseignement sur la directive en question.

En effet, le choix de l'établissement du responsable comme élément de localisation pour l'application de la directive n'est pas anodin. Cela implique que le législateur européen articule l'application de la directive autour de l'opérateur qui ambitionne de traiter les données personnelles et non pas autour de la personne concernée²¹⁹. Ainsi, dans une certaine mesure, ce choix opéré par le législateur européen permet au responsable du traitement de se soustraire au régime de la directive en localisant son établissement hors du territoire de l'Union²²⁰. Mais, par ailleurs, il résulte également de ce choix qu'aucun lien de connexion entre la personne concernée et l'Union n'est requis pour l'application de la directive. En d'autres termes, dès lors que l'établissement d'un opérateur est localisé sur le territoire de l'Union européenne, il semble que toute personne dont les données personnelles sont traitées par cet opérateur, peut potentiellement²²¹ obtenir la protection de la directive, quelle que soit sa nationalité ou son domicile²²². Ainsi, en théorie, un Australien établi au Japon, qui se connecte sur un site internet, basé aux Etats-Unis et disposant d'une filiale en Europe, pourrait s'adresser à l'autorité de protection des données dans l'Etat

²¹⁴ *Ibidem*.

²¹⁵ Le critère de la finalité du traitement serait moins déterminante puisqu'en toute logique c'est la société qui commande le traitement de donnée à l'opérateur tiers qui en déterminerait la finalité.

²¹⁶ 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? », *op. cit.*, p. 35.

²¹⁷ Avis 8/2010 du Groupe de Travail « Article 29 », *op. cit.*, p. 13.

²¹⁸ CJUE, 13 mai 2014, *Google et Google Spain*, *op. cit.*, pt. 49.

²¹⁹ B. HARDY, *op. cit.*, p. 885.

²²⁰ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p. 306. A propos de la Convention de Rome, l'auteur observe très justement que localiser les liens les plus étroits d'un contrat de vente au lieu de résidence du vendeur « *représente bien sûr un avantage substantiel pour ce dernier, puisqu'en choisissant son lieu d'établissement, il choisit la loi applicable* ». Si nous transposons ce raisonnement à la directive « données personnelles », nous remarquons que les liens les plus étroits du traitement de données ne sont pas exactement localisés au lieu d'établissement du vendeur puisque le texte de la directive a été amendé *in extremis* pour viser non plus simplement le lieu où est établi l'opérateur mais plus largement le cadre des activités de l'établissement du responsable du traitement qui est situé sur le territoire de l'Union, et ce de manière à éviter que l'opérateur puisse simplement échapper à la directive en choisissant un lieu d'établissement en dehors de l'Union européenne.

²²¹ Pour autant que la personne concernée puisse démontrer que le traitement a lieu « dans le cadre des activités ».

²²² Directive « données personnelles », Considérant 2 ; S. FRANCO, « The external dimension of Rome I and Rome II : neutrality or schizophrenia », *op. cit.*, p.96 ; B. HARDY, *op. cit.*, p. 885 ; C.KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *op. cit.*, pp.11-12.

membre où est basée ladite filiale pour obtenir la protection de ses données sur base de la directive²²³. Ceci offre une voie royale au *law shopping* pour les personnes souhaitant voir le traitement de leurs données personnelles soumis à la directive « données personnelles »²²⁴. Cependant, si une telle situation devait être soumise à la Cour, il ne fait aucun doute, pour notre part, que l'application de la directive se verrait critiquée à la lumière de sa base juridique puisqu'il n'est pas certain que le bon fonctionnement du marché intérieur suppose la protection des données personnelles d'un Australien résidant au Japon²²⁵.

Du reste, remarquons que la nouvelle disposition concernant la protection des données personnelles introduite dans le traité de Lisbonne, consacre le droit à la protection des données à caractère personnel pour « toute personne » et ne fait aucune distinction qu'il s'agisse d'un citoyen européen ou d'une personne qui réside sur le territoire de l'Union²²⁶.

2. Le cadre des activités

Dans le cadre de l'article 4, §1^{er}, point (a), il ne suffit pas que l'opérateur ait un établissement sur le territoire de l'Union européenne pour que la directive « données personnelles » soit applicable. Encore faut-il que le traitement en cause soit effectué dans le cadre des activités de cet établissement pour qu'il puisse être rattaché à l'Union européenne et que le droit de l'Union s'applique.

Toutefois, la directive ne donne aucune définition et très peu d'indications sur la manière dont il faut interpréter cette condition qui reste donc très vague. Dans son avis sur le droit applicable, le groupe de travail « article 29 » tente de rendre plus concrète cette condition en soulignant trois éléments qui sont à « considérer » lors d'une analyse de l'applicabilité de la directive basée de ce critère²²⁷. Ainsi, le groupe de travail « article 29 » pointe en premier lieu l'importance du « degré de participation du ou des établissements aux activités dans le cadre desquelles des données à caractère personnel sont traitées »²²⁸. Deuxièmement, le groupe de travail « article 29 » estime qu'il faut également considérer « la nature des activités des établissements »²²⁹ et, enfin, il rappelle la nécessité de « tenir compte de l'objectif général de la directive, puisque celle-ci vise à assurer une protection efficace aux personnes physiques ». Si cet avis nous éclaire sur la façon dont il faut interpréter la notion du cadre des activités d'un établissement, il ne lève pas toutes les interrogations quant à la manière de satisfaire cette condition, pas plus que ne le fit un avis antérieur où le Groupe de Travail « article 29 » considéra que l'établissement doit « jouer un rôle significatif dans l'opération de traitement en question »²³⁰.

²²³ De nombreux auteurs critiquent cette possibilité qui ne semble pas écarté à la lumière de l'affaire Google Spain.

²²⁴ C.KUNER, « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *op. cit.*, pp.11-12.

²²⁵ A notre sens, ni la volonté de décloisonner les marchés nationaux ni celle d'éviter une distorsion de concurrence ne justifie l'application de la directive dans la situation en cause.

²²⁶ TFUE, article 16, paragraphe 1^{er} ; V. REDING, « The upcoming data protection reform for the European Union », *International Data Privacy Law*, 2011, Volume 1, p. 3.

²²⁷ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 16.

²²⁸ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 16.

²²⁹ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 16.

²³⁰ l'Avis 1/2008 du Groupe de Travail « Article 29 » *op. cit.*, p. 11. Avis sur les moteurs de recherches. Toutefois, il faut reconnaître que cet avis étant accompagné d'exemples qui peuvent parfois être éclairant s'agissant d'une situation particulière. Ainsi le Groupe de Travail a considéré que lorsqu'un moteur de recherche « établit un bureau dans un État membre (EEE) qui joue un rôle dans la vente de publicités ciblées aux habitants de cet État » (nous soulignons) ce bureau joue « manifestement » un « rôle significatif dans l'opération de traitement » et constitue dès lors un établissement.

La Cour de justice n'apporte pas beaucoup plus de précisions sur la question, mais ajoute néanmoins que le traitement doit être fait « *dans le cadre des activités de l'établissement* » mais pas nécessairement « *par* » l'établissement²³¹. En conséquence, ni le lieu où les opérations de traitement sont effectuées, ni même le lieu où les données sont détenues est déterminant. Comme le souligne la Cour, une telle interprétation a pour but d'éviter tout contournement de la directive « données personnelles » et, partant, se justifie afin d'« *assurer une protection efficace et complète* »²³².

Cependant, cette condition relative au cadre des activités de l'établissement, reste encore discutée notamment en doctrine, où certains auteurs proposent de considérer que les données sont traitées dans le cadre des activités de l'établissement si ces dernières sont « *disponibles* » à partir de l'établissement²³³. Ils jugent par exemple que les données ne seraient pas disponibles à partir de l'établissement si la personne concernée envoie directement ses données à l'établissement principal situé en dehors du territoire de l'Union²³⁴. Cette interprétation nous semble plus restrictive que celle de la Cour puisqu'elle nécessite, à tout le moins, que les données transitent par l'établissement situé sur le territoire de l'Union pour que la directive s'applique sur base de l'article 4, §1^{er}, (a)²³⁵.

Dans l'affaire *Google Spain*, la question du cadre des activités de l'établissement fit l'objet d'un débat nourri et fut déterminante²³⁶. A la question est-ce que le traitement des données du citoyen espagnol fut effectué dans le cadre des activités de l'établissement du responsable du traitement, à savoir *Google Spain*, *Google Inc.* répondait par la négative. En effet, pour sa part, le moteur de recherche considérait que le traitement des données personnelles avait été effectué « *exclusivement* » par lui-même et « *sans aucune intervention de la part de Google Spain* », ajoutant que l'activité de sa filiale espagnole « *se limite à la fourniture d'un soutien à l'activité publicitaire du groupe Google* »²³⁷. Face à cet argument, il convient de rappeler que la Cour ne considère pas qu'une intervention de l'établissement dans le traitement des données soit nécessaire pour considérer que le traitement a eu lieu dans le cadre de ses activités.

D'ailleurs, il ne fut pas établi que « *Google Spain réalise en Espagne une activité directement liée à l'indexation ou au stockage d'information de données contenues dans les sites web de tiers* »²³⁸. De plus, ainsi que l'affirme *Google Inc.*, l'activité de sa filiale ne vise pas les habitants de l'Etat membre dans lequel elle est localisée²³⁹. De fait, *Google Spain* déploie ses activités à l'égard d'entreprises, il est vrai, « *essentiellement* » établies en Espagne mais ne dirige donc pas ses activités vers les citoyens espagnols, en tout cas, pas plus qu'il ne les dirige vers les citoyens français, américains ou japonais²⁴⁰. Le constat paraît relativement clair : si *Google Spain* est bien un établissement de *Google*, il semble manquer le lien entre *Google Spain* et le citoyen espagnol, ou plus précisément entre les activités de la filiale espagnole et le traitement des données du citoyen.

²³¹ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 52; L. MARINO, op. cit., p. 1301.

²³² CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pts. 52-53.

²³³ J. MOINY, op. cit., p. 260 ; C. KUNER, *European Data Protection Law Corporate Compliance and Regulation*, Oxford University Press, Oxford, 2007, p.72

²³⁴ J. MOINY, op. cit., p. 260.

²³⁵ Il nous paraît clair qu'une telle condition n'est pas exigée, notamment à la lumière de l'affaire *Google Spain*, puisque nulle part la Cour exige que les données de la personne concernée aient transitées par la filiale espagnole.

²³⁶ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pts. 44 et s.

²³⁷ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 51.

²³⁸ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 46.

²³⁹ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 47.

²⁴⁰ S. FRANCO, « The external dimension of Rome I and Rome II : neutrality or schizophrenia », op. cit., p.96.

Ce n'est évidemment pas l'avis du citoyen dont les données ont été traitées et qui entend bien obtenir l'application de la directive. Ce dernier estime que les activités de *Google Inc* et *Google Spain* sont unies par un lien indissociable et qu'il faut donc considérer que le traitement de ses données personnelles a été effectué dans le cadre des activités de *Google Spain*²⁴¹. Il est rejoint dans son raisonnement par la Commission²⁴². La Cour de justice leur donnera raison. En effet, la Cour considère que « *les activités du moteur de recherche et celles de son établissement [...] sont indissociablement liées* » et elle justifie ce lien en estimant que les activités publicitaires de l'établissement « *constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités* »²⁴³. En d'autres termes, la Cour souligne un lien de dépendance économique entre *Google Spain* et *Google Inc* : les activités du premier étant indispensables au deuxième et *vice versa*. Si l'analyse du modèle économique de *Google* dressée par la Cour est sans doute exacte²⁴⁴, le raisonnement de la Cour du point de vue de l'applicabilité ne convainc pas. De fait, il nous semble que ce lien de dépendance économique n'explique pas en quoi le traitement des données est effectué dans le cadre des activités de *Google Spain*, sauf si un tel lien permet en soi de considérer que les activités du responsable sont *ipso facto* effectuées dans le cadre des activités de son établissement. Si cela devait être le cas, le même raisonnement devrait pouvoir être tenu pour chacun des bureaux de *Google* localisé sur le territoire de l'Union²⁴⁵ et pas seulement pour son bureau espagnol²⁴⁶.

Les considérations ci-avant peuvent remettre en cause le bien fondé du jugement de la Cour, mais cette dernière ne s'embarrasse pas de telles questions. La haute juridiction de l'Union européenne utilise de manière appuyée la protection des libertés et des droits fondamentaux pour justifier sa décision. En effet, dans les deux paragraphes qui précèdent son raisonnement sur le « *lien indissociable* » entre le moteur de recherche et son établissement, la Cour rappelle que l'objectif de la directive est « *d'assurer une protection efficace et complète* »²⁴⁷ des données personnelles et que « *le législateur de l'Union a entendu éviter qu'une personne soit exclue de la protection garantie* » par la directive, notamment « *en prévoyant un champ d'application territorial particulièrement large* »²⁴⁸. Par la suite, la Cour conclut à l'applicabilité de la directive à cette affaire en ajoutant qu'il « *ne saurait être accepté que le traitement de données à caractère personnel effectué pour les besoins du fonctionnement dudit moteur de recherche soit soustrait aux obligations et aux garanties prévues par la directive 95/46, ce qui porterait atteinte à l'effet utile de celle-ci et à la protection efficace et complète des libertés et des droits fondamentaux des personnes physiques qu'elle vise à assurer* »²⁴⁹.

²⁴¹ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 47.

²⁴² CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 47.

²⁴³ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 56.

²⁴⁴ Il est indéniable que les services publicitaires n'auraient aucun intérêt si le service de moteur de recherche n'était pas proposé. Toutefois, *Google* souligne que les services publicitaires de la filiale espagnole sont liés, au sens propre, non pas à l'indexation effectuée par l'exploitant du moteur de recherche mais aux recherches des utilisateurs. Le moteur de recherche américain prétend ainsi que *Google Spain* peut exercer ses activités indépendamment du traitement effectué par *Google Inc.* mais, en réalité, l'argument semble falacieux. Si des internautes effectuent des recherches sur le moteur de recherche c'est précisément parce que celui-ci a indexé les données présentes sur internet.

²⁴⁵ Il y en a plus de 20, Voy. <https://www.google.fr/about/company/facts/locations/> (consulté le 3 juillet 2016).

²⁴⁶ S. FRANCO, « The external dimension of Rome I and Rome II : neutrality or schizophrenia », op. cit., p.96. L'auteur fait observer qu'il n'y a pas plus de lien entre *Google Spain* et la personne concernée qu'entre *Google France* et cette même personne.

²⁴⁷ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 53.

²⁴⁸ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 54.

²⁴⁹ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 58.

S'il paraît difficile de justifier le jugement de la Cour sur base des termes de la directive « données personnelles », c'est probablement parce que le critère qui a guidé la juridiction dans son interprétation n'est pas tant le « *cadre des activités de l'établissement du responsable du traitement* », que le lien étroit existant entre la situation en cause et l'Union européenne²⁵⁰. Dans les premières pages de ce travail, nous faisons référence à une « intuition logique » qui conduisait à considérer que le droit de l'Union serait applicable à la situation tant les éléments de cette affaire entretenaient une proximité avec le territoire européen. Ainsi, il semble qu'au vu de ce degré de proximité, la Cour ait pu juger légitime l'application de la directive et, partant, la protection des données personnelles qui en découle, au traitement de données en question.

Ce raisonnement apparaît d'autant plus crédible à la lumière de la jurisprudence *Ingmar*²⁵¹. Dans cette affaire, la Cour conclut que le droit de communautaire s'applique en se basant sur l'existence d'un « *lien étroit avec la Communauté* »²⁵². Il ne nous semble pas impossible de considérer que la Cour ait eu le même raisonnement dans l'affaire concernant *Google Spain* même si elle ne le dit pas expressément. De fait, dans ces deux affaires, les directives en cause poursuivent un objectif de protection d'une partie qui peut être considérée comme la partie faible dans le cadre d'un rapport juridique. En outre, cet objectif de protection revêt une importance encore plus particulière dès lors qu'il s'agit d'une situation internationale où la partie faible, établie sur le territoire de l'Union européenne, se trouve confrontée à une partie localisée en dehors de l'Union²⁵³. En d'autres termes, il nous est possible de considérer que tant dans l'affaire *Ingmar* que dans celle concernant *Google Spain*, « *c'est dans les relations avec un opérateur d'Etat tiers que la protection de l'agent* (ou de la personne concernée s'agissant des données personnelles) *se révélera le plus nécessaire* »²⁵⁴. Par conséquent, l'application du droit européen aux deux situations est rendue nécessaire, non seulement pour l'accomplissement des objectifs du traité, à savoir la réalisation du marché intérieur, mais également par un souci de protection des parties faibles dans ces situations qui présentent un lien étroit avec le territoire de l'Union.

Notons, toutefois, que les deux affaires comportent certaines différences qui empêchent une application inconditionnelle du raisonnement de l'arrêt *Ingmar* à l'affaire *Google Spain*. En effet, la directive concernant les agents commerciaux ne définit pas elle-même son domaine d'applicabilité, ce qui a permis à la Cour de concrétiser assez librement le lien étroit observé entre la situation et le territoire de l'Union au travers de la localisation de l'établissement de l'agent²⁵⁵. Une telle concrétisation du lien étroit à partir de la directive « données personnelles » semble plus difficile. Ainsi, par exemple la Cour n'aurait pas pu désigner la résidence de la personne concernée comme critère d'applicabilité et ainsi concrétiser le lien étroit existant entre la situation et l'Union européenne.

²⁵⁰ B. HARDY, *op. cit.*, p. 890.

²⁵¹ CJCE, 9 novembre 2000, C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, *op. cit.*

²⁵² CJCE, 9 novembre 2000, C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, *op. cit.*, pt 25.

²⁵³ Sur les considérations à propos de l'arrêt *Ingmar*, Voy. S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, pp. 405 et s.

²⁵⁴ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p. 414. C'est à propos de l'arrêt *Ingmar* que l'auteur énonce ces considérations.

²⁵⁵ De fait, la présence d'un critère d'applicabilité explicite tel que c'est le cas dans la directive « données personnelles » peut engendrer un « défaut de souplesse » en comparaison d'un critère implicite. S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p. 384.

§2. **Article 4, §1^{er}, (c) : « Le recours à des moyens situés sur le territoire Communautaire »**

L'article 4 de la directive « données personnelles » contient un deuxième critère d'applicabilité. Celui-ci s'applique « *lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté* » et que ce responsable a recours à des « *moyens* » situés sur le territoire de l'Union européenne. La directive prévoit, néanmoins, que ce critère d'applicabilité ne s'appliquera pas si les moyens en question « *ne sont utilisés qu'à des fins de transit* ». Nous examinons dans la présente section la notion de « moyens » (paragraphe 1) avant de nous intéresser à l'interaction de ce critère d'applicabilité avec celui examiné ci-avant (paragraphe 2). Toutefois, comme nous l'avons souligné dans l'introduction à ce chapitre, les développements consacrés à l'article 4, §1^{er}, point (c), seront plus brefs que l'analyse du point (a) de la même disposition. Ceci se justifie, d'une part, parce que ce critère est très peu utilisé en pratique, et, d'autre part, parce qu'il n'a pas été retenu dans le nouveau règlement concernant les données personnelles, et est donc voué disparaître.

1. **Les « moyens » utilisés à des fins de traitement de données personnelles**

Concernant ce deuxième critère d'applicabilité, l'interprétation de la notion de moyens est cruciale puisque l'applicabilité de la directive dépend de l'utilisation et de la localisation de ces moyens²⁵⁶. Toutefois, la directive ne définit pas ce qu'il faut entendre par « moyens » dont l'utilisation peut entraîner l'application de la directive.

A l'instar des autres notions de la directive « données personnelles », il convient de réserver une interprétation large à cette notion de « moyens » et ce pour plusieurs raisons²⁵⁷. Premièrement, dans le langage commun²⁵⁸, un moyen désigne « *ce qui sert pour arriver à un résultat, à une fin* »²⁵⁹. Une telle définition semble logiquement appeler une interprétation large. Cependant, il nous faut signaler que la version anglaise de la directive utilise non pas le terme « *means* » mais « *equipment* »²⁶⁰ et que les différentes versions linguistiques ont la même valeur²⁶¹. Selon certains auteurs, le terme « *equipment* » pourrait impliquer une interprétation plus restrictive et suggérer que la disposition ne s'applique qu'en présence d'un dispositif « physique » destiné à traiter les données personnelles en cause²⁶². A cet égard, le Groupe de Travail « article 29 » qui s'est penché sur la question estime que l'interprétation basée sur le terme de « *moyens* » doit prévaloir dans la mesure où cette terminologie est celle qui semble être la plus conforme à « *la formulation de l'article 2, point d), qui définit le responsable du traitement comme la personne qui détermine les finalités et les moyens* »²⁶³, et à la volonté du législateur.

²⁵⁶ 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? », *op. cit.*, pp. 32-33.

²⁵⁷ *Ibidem*, pp. 33-34 ; Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 23.

²⁵⁸ 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? », *op. cit.*, pp. 33.

²⁵⁹ *Le Robert de poche 2008*.

²⁶⁰ C'est également le cas s'agissant de la version suédoise et italienne de la directive « données personnelles » ; 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? », *op. cit.*, p. 33.

²⁶¹ CJCE, 6 octobre 1982, aff. 283/81, *CILFIT c. Ministry of Health*, *Rec.*, 1982, p. 3415, pts 18 et s. ; 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? », *op. cit.*, p. 33..

²⁶² 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? », *op. cit.*, p. 33, note 24.

²⁶³ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 23.

En outre, une interprétation large et indépendante d'un critère physique, permet de couvrir l'évolution des instruments utilisés pour le traitement des données. En effet, la pratique des opérateurs a beaucoup évolué. D'un traitement de données qui se faisait au travers d'un réseau de télécommunications câblé, au développement actuel de logiciels dits « *espions* » aussi appelés « *cookies* », qui sont installés sur l'appareil des personnes concernées, les moyens utilisés pour le traitement des données se sont largement diversifiés. Ceci appelle, de fait, une interprétation large de la notion de « *moyens* »²⁶⁴. Une question qui a accompagné cette évolution des moyens de traitement, concerne la relation juridique du responsable du traitement avec les moyens utilisés. Là encore, les réponses apportées en doctrine se gardent de restreindre la notion de « *moyens* » puisqu'il est généralement considéré que la propriété ou la possession du moyen importe peu²⁶⁵. Il n'est pas non plus nécessaire que le responsable du traitement exerce un contrôle total sur les moyens. Il suffirait que l'opérateur ait une « maîtrise » qui lui permette de déterminer « *quelles données sont collectées, stockées, transférées, modifiées, etc., de quelle manière et dans quel but* »²⁶⁶.

Enfin, il nous semble que cette disposition ne pourrait s'accommoder d'une interprétation restrictive au vu de l'objectif de protection des données personnelles poursuivi par la directive et souligné à plusieurs reprises par la Cour. *A fortiori*, dans la mesure où cette disposition participe à la volonté du législateur européen d'éviter qu'une personne soit exclue de la protection qui lui est garantie par la directive « données personnelles » et, partant, qu'elle a pour but de compléter et couvrir les situations qui échapperaient à l'article 4, §1, point (a), une interprétation large nous paraît devoir s'imposer²⁶⁷. A l'inverse, pour ces mêmes raisons, l'exception relative à l'utilisation des moyens à des fins de transit, dont « *l'application effective [...] devient rare* »²⁶⁸, devrait s'interpréter restrictivement.

2. L'articulation entre les critères d'applicabilité de la directive 95/46/CE

Nous évoquons l'articulation entre les deux critères d'applicabilité de la directive « données personnelles » dans cette section consacrée à l'article 4, §1^{er}, point (c), car la finalité de cette disposition, est comme nous venons de le souligner, d'éviter que le responsable du traitement ne contourne le critère du point (a) et ainsi puisse échapper aux obligations de la directive²⁶⁹. Il faut donc y voir un complément à l'article 4, §1^{er}, point (a) et l'interpréter en conséquence, en évitant toute application cumulative.

Si l'application du point (a) de l'article 4 de la directive « données personnelles » nécessite la présence d'un établissement sur le territoire de l'Union européenne, le point (c) du même article n'a vocation à s'appliquer qu'en l'absence d'un tel établissement sur le territoire européen. C'est le sens de la première phrase du point (c), qui prévoit ainsi son application lorsque « *le responsable du traitement n'est pas établi sur le territoire de la Communauté* ». Prise à la lettre cette première phrase, dans sa formulation actuelle, pourrait signifier que le point (c) s'applique dès lors que l'établissement *principal* du responsable

²⁶⁴ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, pp. 23-24.

²⁶⁵ J. MOINY, *op. cit.*, p. 262 ; Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 23.

²⁶⁶ J. MOINY, *op. cit.*, p. 262, notes 189 et 186.

²⁶⁷ Directive « données personnelles », Considérant 20 ; Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 21 ; HAVELANGE B. et LACOSTE A., *op. cit.*, p. 244 ; J. MOINY, *op. cit.*, pp. 261- 262.

²⁶⁸ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 23. Le Groupe de Travail justifie cette affirmation en estimant que « *dans la pratique, les services de télécommunication sont de plus en plus nombreux à fusionner les services de transit et les services à valeur ajoutée, comme le filtrage anti-spam ou autres services de manipulation des données à l'occasion de leur transmission* » et que par conséquent « *la simple transmission par câble de point à point disparaît peu à peu* » ; C. KUNER, *Transborder data flows and data privacy law*, *op. cit.*, p. 16.

²⁶⁹ Directive « données personnelles », Considérant 20.

du traitement n'est pas situé sur le territoire de l'Union européenne²⁷⁰. Néanmoins, une telle interprétation risquerait de conduire fréquemment à une application simultanée du point (c) et du point (a), contrairement à la volonté du législateur européen²⁷¹.

En vérité, il semble donc qu'il faille comprendre cette première phrase comme disposant que le point (c) s'applique lorsque le responsable du traitement n'a pas d'établissement, au sens du point (a), sur le territoire de la Communauté²⁷². Toutefois, il faut encore affiner cette interprétation, car si la simple présence d'un établissement sur le territoire de l'Union européenne faisait *ipso facto* obstacle à toute application du point (c) de l'article 4 de la directive « données personnelles », alors la personne concernée pourrait vite se retrouver exclue de la protection de ladite directive. En effet, le point (a) de l'article 4 nécessite, non seulement la présence d'un établissement sur le territoire communautaire mais également, que les données personnelles soient traitées dans le cadre des activités de cet établissement. Si les données personnelles ne sont donc pas traitées dans le cadre des activités de l'établissement et que la présence dudit établissement empêche l'application du point (c), conformément à l'interprétation proposée ci-dessus, la personne concernée serait privée de la protection de la directive. Afin d'éviter une telle situation, le Groupe de Travail « article 29 » préconise donc 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 »²⁷³. Cette recommandation du groupe de travail permettrait une articulation plus complète des dispositions en cause²⁷⁴.

Nous le constatons, sur base des termes de la directive actuelle, une interprétation permettant l'application complémentaire et efficace des points (a) et (c) de l'article 4, tel que le souhaite le législateur européen, ne va pas sans difficulté.

Par ailleurs, à notre sens, malgré toutes ces précautions dans l'interprétation de l'article 4, un hiatus dans l'applicabilité de la directive et, par conséquent, dans la protection des données personnelles ne peut être évité. En effet, si nous envisageons la situation dans laquelle les données personnelles seraient traitées en dehors du cadre des activités de l'établissement, nous observons que la seule possibilité pour que la directive s'applique est que le responsable du traitement ait eu recours à des moyens situés sur le territoire de l'Union européenne²⁷⁵. En l'absence de tels moyens sur le territoire de l'Union ou de recours à ceux-ci par l'opérateur, le traitement des données ne sera pas soumis au régime de la directive. Selon nous, ce risque aurait pu se matérialiser dans l'affaire *Google Spain* sans l'interprétation de la Cour,

²⁷⁰ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 22..

²⁷¹ Il pourrait s'agir d'un oubli de la part du législateur européen. Dans une version déjà amendée par rapport à la version originelle, l'article 4, (1), (a), prévoyait son application si le responsable du traitement était établi sur le territoire communautaire. Par la suite, cette disposition a été modifiée pour prendre la formulation que nous avons examiné mais le (c) du même article a conservé la formulation être établie. Sur l'historique législative de l'article 4, paragraphe 1^{er}, directive « données personnelles », 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? », *op. cit.*, p. 32 et s.

²⁷² C'est l'interprétation que préconise le Groupe de Travail « article 29 ». Voy. Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, pp. 22-23.

²⁷³ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 22.

²⁷⁴ Une telle interprétation permet de répondre partiellement au « gap » mis en évidence en doctrine. Voy. à propos de « gap », 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? », *op. cit.*, p. 35 et B. HARDY, *op. cit.*, p. 884.

²⁷⁵ Pour autant que ces moyens ne soient pas utilisés exclusivement à des fins de transit.

particulièrement large, voire extensive, et orientée sur la protection des données. Nous l'avons souligné, il n'est pas si évident d'admettre que le traitement de *Google Inc.* s'inscrive dans le cadre des activités de *Google Spain*. Par ailleurs, si la Cour avait opté pour la solution contraire, elle aurait dû envisager l'application de l'article 4, §1^{er}, (c). L'analyse aurait alors nécessité de s'interroger sur le recours par *Google Inc.* à d'éventuels moyens situés sur le territoire de l'Union afin de déclarer la directive applicable²⁷⁶. La Cour fit l'économie d'un tel examen puisqu'elle a considéré que le critère d'applicabilité du point (a) de l'article 4 était satisfait²⁷⁷, ce qui exclut l'application du (c). Il est évident que le constat que nous tirons ci-dessus ainsi que la faille qu'il met en lumière, contrarie la volonté du législateur qui veut « éviter tout contournement »²⁷⁸ ou « qu'une personne soit exclue de la protection »²⁷⁹ de la directive, mais il semble difficile de colmater la brèche constatée sans une réforme de l'article 4, sauf au prix d'une lecture créative de la directive qui, pour le moins, est susceptible de laisser perplexes les observateurs.

Toutefois, cette lacune dans l'applicabilité de la directive n'est pas insurmontable. D'ailleurs, une solution nous semble assez élémentaire puisqu'elle consiste à aligner les deux critères. En effet, cette faille nous paraît liée à l'amendement du point (a), qui a remplacé le critère de « l'établissement principal » par celui du « cadre des activités d'un établissement », mais qui n'a donné lieu à aucune modification du point (c). Or, une complémentarité absolue des deux dispositions aurait sans doute nécessité que le législateur européen alignât le critère du point (c) sur celui du point (a) lorsqu'il amenda ce dernier²⁸⁰. Quoi qu'il en soit, la situation méritait bien une réflexion d'autant plus que cette faille dans le domaine d'applicabilité de la directive, qui s'est révélée dans l'affaire *Google Spain*, risque de ressurgir dans d'autres litiges, dès lors qu'utiliser des bureaux assurant des services publicitaires dans l'Union est devenu une pratique courante chez les opérateurs.

Enfin, il est intéressant de remarquer, que si le point (c) de l'article 4 ne s'accorde pas parfaitement avec le point (a) du même article, et laisse ainsi sans protection une situation qui en appellerait une, il rend potentiellement applicable la directive à une situation qui pourrait semble-t-il ne pas nécessiter de protection, à tout le moins de protection du législateur européen. Ainsi, si nous imaginons une société qui installe ses moyens de traitement sur le territoire de l'Union et, grâce à ces moyens, traite des données personnelles concernant des citoyens d'un pays tiers, ce traitement sera soumis à la directive « données personnelles » qui établit un niveau élevé de protection, probablement plus élevé que celui de la législation du pays tiers²⁸¹. Ceci pourrait avoir des répercussions sur la décision des opérateurs d'effectivement s'installer sur le territoire de l'Union²⁸². Nous pourrions donc penser que le législateur, en adoptant le point (c) de l'article 4, a en partie manqué sa cible et en a touché une autre et qu'il conviendrait donc de rectifier le tir. Toutefois, dans une certaine mesure, résonner de cette façon comporte le risque d'ignorer le

²⁷⁶ J. 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 *Enjeux européens et mondiaux de la protection des données personnelles*, A. GROSJEAN (dir.), Bruxelles, Bruylant, 2015, pp. 186-187. L'auteur estime que l'analyse du point (c), paragraphe 1^{er}, directive « données personnelles » aurait en l'espèce abouti à l'application de la directive.

²⁷⁷ CJUE, 13 mai 2014, *Google et Google Spain*, op. cit., pt. 59.

²⁷⁸ Directive « données personnelles », Considérant 19.

²⁷⁹ Directive « données personnelles », Considérant 18.

²⁸⁰ Il faudrait revoir le « rapport de subsidiarité », voy. B. HARDY, op. cit., p. 884.

²⁸¹ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », op. cit., p. 74 ; Avis 8/2010 du Groupe de Travail « Article 29 » op. cit., p. 24.

²⁸² Peut-être contestable au vu de la base juridique qu'est l'article 114, TFUE.

caractère fondamental du droit à la protection des données personnelles²⁸³ et du rôle que l'Union européenne s'est donnée²⁸⁴ s'agissant de la promotion des droits fondamentaux au niveau international.

Chapitre 4. La transposition de la directive 95/46 dans les droits nationaux

C'est un aspect que nous n'avons pas encore abordé mais qui est inhérent à toute directive : la transposition. En effet, la directive « données personnelles », comme toutes les directives, ne peut déployer ses effets qu'au travers d'une loi nationale. Toutefois, étant donné que la directive doit être transposée par tous les États membres, elle est censée, à ce jour, déployer ses effets au travers de 28 lois nationales. À la suite de ces considérations, une question émerge nécessairement en pratique, à savoir, celle du conflit de la loi de transposition (section 1). Nous le verrons, cette question est d'autant plus importante que l'harmonisation opérée par la directive ne peut être qualifiée d'optimale (section 2).

Il nous faut, ici, avertir le lecteur que les développements que nous consacrons à la transposition de la directive « données personnelles » seront limités dans la mesure où les critères utilisés pour régler le conflit de lois sont les mêmes que ceux qui déterminent le domaine d'application. En outre, un règlement viendra très prochainement remplacer cette directive et, partant, supprimera les questions liées à sa transposition. Néanmoins, il nous a semblé que des considérations sur la transposition restaient nécessaires, notamment pour évaluer le choix du législateur européen de refondre la réglementation en matière de données personnelles au sein d'un règlement.

Section 1. Le conflit de lois de transposition

Lorsqu'il est concrètement question d'appliquer la directive « données personnelles » à une situation, il faut déterminer la ou les loi(s) nationale(s) applicable(s) et, le cas échéant, régler le conflit de lois qui peut survenir²⁸⁵. À l'instar de la détermination du domaine d'application, notre première constatation est qu'il faut appliquer l'article 4 de la directive « données personnelles ». Cette disposition intitulée « *droit national applicable* », règle logiquement le conflit de lois de transposition. La même disposition sert donc à définir l'application de la directive et la loi de transposition applicable. C'est ce qui a été appelé en doctrine « *la nature hybride* » de l'article 4²⁸⁶.

En outre, il est remarquable que l'article 4 détermine unilatéralement le domaine d'application de la directive alors qu'il agit à la manière d'une règle de rattachement multilatérale concernant la désignation de la loi de transposition. En d'autres termes, l'article 4 remplit non seulement une double fonction mais, en outre, il exerce chacune de ces fonctions selon une méthode différente. Une telle configuration n'est vraisemblablement pas de nature à faciliter l'interprétation de cet article, ni sa transposition en droit national.

²⁸³ En 2009, au travers de l'article 16 du Traité, l'Union a confirmé son souhait de consacrer et protéger un droit à la protection des données personnelles pour « toute personne ». V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 120 ; V. REDING, « The upcoming data protection reform for the European Union », *op. cit.*, p. 3.

²⁸⁴ TUE, article 3, paragraphe 5.

²⁸⁵ S. FRANCO, *L'application du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, pp. 279-280.

²⁸⁶ B. HARDY, *op. cit.*, p. 884.

Tout comme pour le domaine d'applicabilité, il nous faut analyser l'application du point (a) de l'article 4 (paragraphe 1) ainsi que le point (c) du même article (paragraphe 2). Nous faisons une nouvelle fois l'économie d'une analyse du point (b) de l'article 4 pour les mêmes raisons que précédemment.

§1. **« Le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre »**

L'article 4, §1^{er},(a), prévoit que « *chaque état membre applique les dispositions nationales [...] lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre* ». La situation est claire lorsque le cas d'espèce concerne un traitement de données exclusivement effectué dans le cadre des activités du seul établissement de l'opérateur sur le territoire de l'Union. De fait, dans un tel cas il n'y a pas de conflit de lois de transposition.

Toutefois, la question se complique lorsque cet opérateur dispose de plusieurs établissements sur le territoire de l'Union. A cet égard, la deuxième phrase du point (a) dispose que « *si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable* ». En d'autres termes, chaque établissement doit se conformer aux obligations prescrites par le droit national du lieu où il est situé. C'est, en tout cas, l'interprétation majoritaire en doctrine²⁸⁷. Ceci implique qu'un même responsable du traitement, s'il dispose de plusieurs établissements au sein de l'Union, devrait s'accommoder de la législation de chaque état membre dans lequel il dispose d'un établissement. En outre, nous le verrons, le risque d'une application cumulative des lois de transposition n'est pas à écarter alors même que la volonté du législateur européen est d'éviter « *l'application double/multiple des lois nationales* »²⁸⁸ afin de parfaire le marché intérieur.

Pour examiner plus en avant le risque d'application cumulative, il nous faut revenir sur la chronologie²⁸⁹ de l'adoption et de l'interprétation de la directive « données personnelles » jusqu'à l'arrêt *Google Spain*.

L'idée première du législateur européen était d'introduire le principe du pays d'origine qui permet de déterminer et d'appliquer une seule législation et, partant, d'éviter tout cumul, en excluant l'application des autres législations nationales²⁹⁰. Ainsi, dans la proposition originale de la Commission, ce principe se traduisait par la détermination de la loi de transposition de l'état où était localisé le fichier²⁹¹.

²⁸⁷ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, p. 96, note 28 ; V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, pp. 120 - 121.

²⁸⁸ Avis du Groupe de Travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE (WP 56), adopté le 30 mai 2002, p. 6.

²⁸⁹ Pour une synthèse sur la chronologie de l'adoption du point (a), paragraphe 1^{er}, Directive « données personnelles », voy. L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, p. 94 et s.

²⁹⁰ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, pp. 95 et s. L'auteur prône avec insistance l'adoption d'un critère d'applicabilité qui permette le retour au principe d'origine.

²⁹¹ Proposition modifiée de directive du Conseil 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, COM(92)122 final, JOCE, 1992, C 311/04, pp 40-41. Cette volonté d'éviter l'application d'une autre législation nationale était notamment manifeste dans le paragraphe 3 de cette version originale qui a ensuite été abandonnée et qui prévoyait que « *lorsqu'un fichier est déplacé temporairement d'un Etat membre vers un autre Etat membre ce dernier n'oppose aucun obstacle et n'exige aucune formalité additionnelle aux règles applicables dans l'Etat membre de localisation permanent du fichier* ».

Par la suite, la Commission a modifié sa proposition et, dès lors, la législation nationale appelée à s'appliquer était celle de l'état sur le territoire duquel le responsable du traitement était établi²⁹². La modification opérée doit se comprendre à la lumière du domaine d'applicabilité et non pas de la question du conflit de lois. En effet, si choisir la localisation du fichier comme critère pour déterminer la loi de transposition applicable ne pose pas de problème et évite une application cumulative des législations nationales, un tel critère ne paraît pas satisfaisant s'agissant du domaine d'applicabilité, puisqu'il est aisé pour l'opérateur de délocaliser le fichier, et, de ce fait, d'éluder la directive. Ceci dit, dans sa version modifiée, le principe du pays d'origine demeurerait la règle puisque la seule loi nationale applicable au responsable du traitement était celle du lieu de son établissement principal, ce qui constitue une expression du principe du pays d'origine²⁹³.

Cependant, ce ne fut pas non plus cette version modifiée que le législateur adopta puisqu'une deuxième modification intervint. Le législateur européen, animé par la même volonté d'éviter tout contournement de la directive a, en définitive, adopté l'article 4, §1^{er}, point (a), tel que nous l'avons reproduit au début de ce paragraphe. Par cette seconde modification, les institutions législatives communautaires voulaient éviter qu'un opérateur échappe aux obligations de la directive en déplaçant son établissement principal en dehors de l'Union. Elles ont donc décidé que la présence d'un simple établissement suffirait à rendre la directive applicable, pour autant que le traitement de données s'inscrive dans le cadre des activités de cet établissement²⁹⁴. Il convient, néanmoins de constater, que cette dernière formulation implique l'abandon du principe du pays d'origine. Cette idée est confirmée par l'ajout dans cette version finale du point (a), de la deuxième phrase qui prévoit que l'opérateur disposant d'établissements « *sur le territoire de plusieurs Etats membres doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable* ». En effet, si l'opérateur responsable du traitement doit vérifier que chacun de ses établissements se conforme aux règles de l'Etat membre dans lequel ils sont localisés, l'opérateur n'est, de fait, plus soumis à une seule législation nationale comme cela aurait été le cas si la version originale ou la première version modifiée avait été adoptée²⁹⁵. Du reste, dans la version finale de la directive « données personnelles », le considérant 19 résume à la fois l'objectif qui a motivé cette modification et l'obligation de conformité avec la législation de chaque état au sein duquel l'opérateur dispose d'un établissement. Ce même considérant précise ainsi « *que lorsqu'un même responsable est établi sur le territoire de plusieurs Etats membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux* » (Nous soulignons).

A la suite de ces considérations sur les amendements du point (a), §1^{er}, de l'article 4, il nous semble que le législateur européen a porté une attention toute particulière lors de l'adoption de cet article afin

²⁹² Proposition modifiée de directive du Conseil 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, COM(92)122 final, JOCE, 1992, C 311/04, pp 40-41.

²⁹³ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, p. 95.

²⁹⁴ *Ibidem*, pp. 96-98. La version finalement adoptée vise le « *cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre* » (souligné par nous) à la différence de la version modifiée qui envisageait l'Etat sur lequel « *le responsable est établi* ». L'auteur souligne que cette terminologie différente témoigne du changement entre la version finale et la version modifiée. Dans la version finalement adoptée, il suffit que l'opérateur dispose d'un établissement sur le territoire communautaire sans pour autant être lui-même établi au sein de l'Union. C'est ainsi que cet auteur souligne la différence entre "have an establishment" et "being established".

²⁹⁵ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, pp. 96-97, note 28 ; V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, pp. 120 - 121.

d'éviter tout contournement de la directive ; mais, ce faisant, il n'a peut-être pas mesuré toutes les implications des amendements, sur le conflit de lois de transposition.

Néanmoins, il faut reconnaître que certains ont mis en doute le raisonnement exposé ci-dessus, estimant que l'article 4, §1^{er}, point (a), tel que rédigé dans sa version finale continuait d'appliquer le principe d'origine²⁹⁶. Cela est notamment dû à un avis du Groupe de Travail « article 29 » qui affirmait que la directive « données personnelles », « *utilise comme critère ou « facteur de lien » le « lieu d'établissement du responsable du traitement » ou en d'autres termes, le principe du pays d'origine habituellement appliqué sur le marché intérieur* ». De surcroît, le Groupe de Travail « article 29 » considérait qu'il s'agissait en réalité de « *l'application la plus stricte* » de ce principe puisque « *lorsque le responsable choisit d'avoir non un mais plusieurs établissements, il ne bénéficie pas de l'avantage selon lequel respecter une seule loi suffit pour toutes les activités exercées sur l'ensemble du marché intérieur* »²⁹⁷. Il concluait, dès lors, que « *ce responsable doit donc appliquer en parallèle les lois nationales correspondant à chacun des établissements* »²⁹⁸. Le Groupe de Travail « article 29 » a notamment été suivi dans son avis par l'autorité de contrôle des Pays-Bas et par certains auteurs. Il nous faut également souligner que la formulation du considérant 18, à l'inverse de celle du considérant 19, semble être de nature à alimenter cette thèse.

Cependant, dans ses avis postérieurs, le Groupe de Travail est revenu sur sa position et a admis que le principe du pays d'origine ne s'appliquait pas dans la version finalement adoptée de l'article 4, §1^{er}, point (a). Toutefois, il a précisé que ce principe aiderait à « *simplifier les règles de détermination du droit applicable* » dans la mesure où il implique que « *tous les établissements d'un même responsable du traitement dans l'UE appliqueraient la même législation, indépendamment du territoire sur lequel ils seraient situés* »²⁹⁹.

En fin de compte, il nous semble effectivement qu'un opérateur qui dispose d'établissements sur le territoire de plusieurs Etats membres, devra se conformer aux législations de chaque Etat membre sur lequel il est présent, et non pas à une seule législation tel que ce serait le cas dans un marché analogue à celui existant sur un territoire national. Par conséquent, ce constat constitue, à notre sens, un échec quant à l'établissement et au fonctionnement du marché intérieur.

Toutefois, postérieurement à ces discussions, il fut considéré en doctrine que « *l'application de la loi de plusieurs Etats membres à un même établissement n'est pas considéré comme problématique ; seule l'application de plusieurs lois à un même traitement de données doit être empêchée* »³⁰⁰. La question prépondérante serait donc de savoir si la directive préviendrait l'application de plusieurs législations de transposition à un même traitement de données. A cet égard, il nous faut constater que rien dans la

²⁹⁶ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, p. 103 ; L. A. BYGRAVE, *op. cit.*, pp. 255–256.

²⁹⁷ Avis du Groupe de Travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE (WP 56), *op. cit.*, p. 7.

²⁹⁸ Avis du Groupe de Travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE (WP 56), *op. cit.*, p. 7.

²⁹⁹ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 35.

³⁰⁰ B. HARDY, *op. cit.*, p. 888, note 60. Notons toutefois que l'application de la loi de plusieurs Etats membres à un même établissement est, à notre sens, problématique dans le cadre du marché intérieur.

directive empêche formellement qu'un traitement de données ne soit soumis à l'application cumulative des législations de transposition.

En outre, l'interprétation de l'article 4, §1^{er}, point (a), donnée par la Cour dans l'affaire *Google Spain* est particulièrement délicate concernant la détermination de la loi de transposition applicable. En effet, dans son arrêt, la Cour considère que le critère d'applicabilité de cette disposition est satisfait mais, nous l'avions souligné, le lien établi par les juges entre les activités de la filiale espagnole et le traitement de données effectué par *Google Inc*, nous avait semblé peu convaincant, tant il était possible de considérer que le traitement de données avait été effectué dans le cadre des activités d'autres filiales européennes du moteur de recherche. Si l'absence d'un lien qui permet de rattacher exclusivement le traitement de données à la filiale espagnole, n'a pas empêché la Cour de juger la directive applicable à la situation en cause, une telle absence rend, toutefois, bien malaisée la détermination exclusive d'une loi de transposition applicable³⁰¹. D'ailleurs, la Cour ne se penche pas sur la question de la loi applicable, qu'elle aurait bien été en peine de résoudre au vu de ses considérations sur l'article 4, §1^{er}, (a), et elle se limite à la question de l'applicabilité.

Il nous semble ainsi, qu'à l'instar du législateur européen lors de l'adoption de l'article 4, §1^{er}, (a), la Cour ait, dans une certaine mesure, perdu de vue la question du conflit de lois de transposition, et a focalisé son interprétation sur le domaine d'applicabilité pour assurer une large protection de la personne concernée. Par conséquent, notre constat est que ni la formulation, ni l'interprétation de l'article 4, §1^{er}, (a), de la directive ne permet de régler un éventuel conflit de lois.

§2. « **Le responsable de traitement qui n'est pas établi sur le territoire et qui a recours à des moyens sur le territoire communautaire** »

Le conflit de lois de transposition dans le cadre de l'article 4, §1^{er}, point (c), a fait l'objet de très peu de développements en doctrine. Il semble, en effet, que le point (c) nécessite moins de développement que le point (a), non seulement parce qu'en pratique cette disposition est beaucoup moins utilisée que le point (a), mais surtout parce que la configuration des situations auxquelles s'applique le point (c) de l'article 4, diffère singulièrement des situations visées par le point (a) et apparait moins problématique.

En effet, le point (c) n'a vocation à s'appliquer que dans la mesure où le « *responsable du traitement n'est pas établi sur le territoire* » d'un Etat membre. Nous nous souvenons qu'il fallait comprendre que le point (c) s'applique lorsque l'opérateur ne dispose ni de son établissement principal, ni d'aucun autre établissement pertinent sur le territoire de l'Union européenne³⁰². Dans une telle situation, la question du principe d'origine ne se pose pas puisque si tous les établissements de l'opérateur, et notamment le principal, ne sont pas localisés dans un Etat membre, cet opérateur ne serait *a priori* pas soumis à la loi d'un Etat membre, et donc échapperait au régime harmonisé de la directive.

En réalité, dans l'hypothèse où l'opérateur n'est pas établi sur le territoire communautaire au sens de la directive et, partant, qu'il n'est pas soumis à la loi d'un Etat membre mais à celle d'un Etat tiers, si le

³⁰¹ B. HARDY, *op. cit.*, pp. 888-889.

³⁰² Voy, *infra*, p. 44 et s.

point (c) devait s'appliquer, ce n'est pas un problème de conflit de lois de transpositions qui se poserait mais une question d'application extraterritoriale des règles européennes à un opérateur qui est, éventuellement, déjà soumis à une autre réglementation³⁰³.

Enfin, le seul cas dans lequel l'application du point (c) conduirait à un véritable conflit de lois de transposition, serait l'hypothèse dans laquelle l'opérateur a eu recours à des moyens situés sur le territoire de plusieurs États membres. Si une telle situation devrait survenir en pratique, il nous semble que la directive ne donne aucune indication sur la façon dont l'application multiple des lois de transposition devrait se régler. Force est donc de constater « *qu'en application du critère des « moyens » de l'article 4, §1^{er}, (c), plusieurs lois nationales peuvent déjà s'appliquer simultanément à un même traitement de données lorsque des moyens sont situés dans plusieurs Etats membre* »³⁰⁴.

Nous ne pouvons conclure cette section sur le conflit de lois de transpositions qu'en constatant l'échec de la directive « données personnelles » à offrir une solution claire aux conflits de loi de transposition, et donc à éviter « *l'application double/multiple des lois nationales* », ce qui était pourtant l'un des objectifs du législateur européen. Toutefois, l'ampleur de cet échec pourrait être nuancée, en pratique à tout le moins, si l'harmonisation opérée par la directive s'avérait complète. De fait, si plusieurs lois de transposition sont appelées à s'appliquer mais qu'elles se révèlent être identiques ou extrêmement similaires, la question du conflit de lois de transposition continue à se poser en théorie, mais constitue un enjeu de moindre intérêt en pratique.

Section 2. L'harmonisation

Comme nous venons de le souligner, une harmonisation complète des législations nationales permettrait d'atténuer les difficultés pratiques dues au conflit de lois de transposition que la directive ne parvient pas à régler intelligiblement. La question est donc de savoir quel degré d'harmonisation a pu être établi sous le régime de la directive « données personnelles ».

En termes d'harmonisation, il semble que l'objectif de la directive soit d'atteindre une harmonisation complète des législations des États membres en matière de données personnelles. La cohérence même de son double objectif implique une telle harmonisation³⁰⁵. En effet, permettre aux Etats membres d'instaurer un niveau de protection plus élevé que celui établi par la directive risquerait de contrarier l'objectif de libre circulation des données. Pareillement, accepter que le droit national fixe un niveau de protection plus bas que celui de la directive ne serait pas compatible avec l'objectif de cette dernière qui est d'assurer un niveau de protection élevé des droits et libertés fondamentaux des personnes.

Toutefois, il faut bien reconnaître que certaines dispositions de la directive se caractérisent par une certaine flexibilité qui laisse une marge de manœuvre aux Etats membres lors de la transposition³⁰⁶. Ceci implique, par conséquent, que nous pouvons nous attendre à ce que l'harmonisation des législations

³⁰³ L. A. BYGRAVE, « Determining Applicable Law pursuant to European Data Protection Legislation », *Computer Law & Security Report*, 2000, volume 16, pp. 255–256.

³⁰⁴ B. HARDY, *op. cit.*, p. 888, note 62.

³⁰⁵ V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 120.

³⁰⁶ HAVELANGE B. et LACOSTE A., *op. cit.*, p. 243, note 15 ; V. REDING, « The European data protection framework for the twenty-first century », *op. cit.*, p. 120-121.

nationales ne soit pas en tout point absolue. De fait, comme souligné à de multiples reprises en doctrine, les disparités entre les législations des Etats membres sont nombreuses. C'est précisément le constat tiré par la Commission dans son « *premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)* »³⁰⁷. En outre, l'interprétation de la directive par les différentes autorités nationales de contrôle ne semble qu'amplifier le défaut d'harmonisation. Nous soulignerons tout particulièrement que l'absence d'harmonisation est apparente non seulement au niveau des règles matérielles, mais également s'agissant des critères d'applicabilité de la directive et de l'interprétation qui en est faite par les autorités nationales. Ce constat ne peut, toutefois, nous surprendre au vu de la complexité que suscite la formulation de l'article 4³⁰⁸.

Pour conclure ce chapitre consacré à l'harmonisation, le constat d'un échec relatif s'impose. Il est vrai que la directive a entraîné un certain rapprochement des législations nationales concernant la protection des données personnelles, qui pouvaient parfois être fort divergentes. Cependant, ce rapprochement est loin de constituer une véritable harmonisation maximale telle que semblent l'exiger les objectifs du législateur européen. De surcroît, les opérateurs actifs dans le marché intérieur demeurent confrontés au risque de devoir appliquer simultanément ces différentes législations. L'absence d'une harmonisation maximale et d'une solution claire concernant le conflit de lois de transposition crée donc une incertitude sur les règles applicables, tant dans le chef de l'opérateur, que dans celui de la personne concernée, et engendre des coûts évitables qui ne devraient pas exister dans un marché intérieur.

³⁰⁷ Commission, «Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)», 15 mai 2003, COM. (265) final, p. 9 et s.

³⁰⁸ L. MOEREL, « Back to basics: when does EU data protection law apply », *op. cit.*, p. 93 ; SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, pp. 65-66.

Titre 3. Une réforme inévitable

Nous avons pu le constater, les 20 années passées sous le régime de la directive 95/46 ont démontré qu'elle n'était pas exempte de tous défauts, notamment concernant son application. Nous avons essentiellement observé qu'il existait une brèche dans son domaine d'applicabilité, ce qui risquait de laisser une personne sans protection. Il nous est également apparu que l'harmonisation des législations nationales restait incomplète. Cette dernière observation, couplée à l'absence d'une solution claire au conflit de lois de transposition, crée une incertitude sur les règles applicables lorsqu'un traitement de données implique plus d'un Etat membre. Ces considérations nous amènent à conclure que ni l'objectif d'achèvement et de fonctionnement du marché intérieur, ni celui de protection des libertés et droits fondamentaux des personnes physiques n'est pleinement atteint.

En outre, l'analyse de la directive « données personnelles » a mis en évidence à quel point son domaine d'applicabilité était complexe. Ceci est d'autant plus regrettable dans la mesure où il s'agit d'une réglementation qui a vocation à toucher intimement le citoyen. Une simplification des dispositions qui régissent l'applicabilité de la directive « données personnelles », serait donc bienvenue même s'il faut concéder que c'est une matière qui conservera toujours un certain degré de complexité, notamment parce qu'elle est directement liée au développement technologique.

Ce dernier point mérite d'être souligné. En effet, depuis longtemps³⁰⁹, il existe un lien étroit entre la protection des données personnelles et les développements technologiques. C'est ce qui explique l'évolution constante de la réglementation, puisque non seulement cette dernière doit s'adapter aux avancées de la technologie, mais également aux mutations économiques et sociales que génèrent de telles avancées. Ainsi, il convient d'observer que postérieurement à l'adoption de la directive données personnelles, le développement technologique a été considérable avec l'émergence d'internet et la mise au point de technologies de plus en plus interactives et mobiles³¹⁰.

Ces changements ne sont évidemment pas sans incidence sur la réglementation relative aux données personnelles. Ils rendent l'échange de données mondial plus aisé et permettent, voire oblige, les internautes à partager et divulguer leurs données personnelles³¹¹. L'affaire *Lindqvist* a ainsi illustré certaines questions juridiques qu'une diffusion mondiale plus aisée et un rôle actif de l'internaute peuvent impliquer. Ces nouvelles technologies ont également pour conséquence de profondément transformer l'activité commerciale et économique liée aux données personnelles³¹². A l'heure actuelle, ces dernières constituent ainsi une préoccupation majeure pour bon nombre de professionnels, de plus en plus enclins à offrir des services ou du contenu sans contrepartie pécuniaire mais en échange des données de l'utilisateur³¹³. Ce n'est donc pas uniquement les comportements des particuliers qui viennent à se modifier, mais également le modèle économique et le mode d'organisation des sociétés commerciales.

³⁰⁹ O. TENE, « Privacy : The new generations », *International Data Privacy Law*, 2011, Volume 1, p. 15 ; S. D. WARREN and L. D. BRANDEIS, *op. cit.*, p. 193.

³¹⁰ Règlement général sur la protection des données, Considérant 6 et 7 ; BERNARD-GLANZ C., *op. cit.*, pp. 702-703 ; 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? », *op. cit.*, p. 28.

³¹¹ M. FAZLIOGLU, *op. cit.*, p. 149 ; B. HAVELANGE et A. LACOSTE, *op. cit.*, p. 241. p. 147

³¹² Voy. *supra*, p. 31 et s.

³¹³ M. FAZLIOGLU, *op. cit.*, p. 149 ; C. KUNER, F. CATE, C. MILLARD et D. SVANTESSON, *op. cit.*, p. 147.

L'affaire *Google Spain* en est un parfait exemple; elle concerne une activité basée sur les technologies développées postérieurement à la directive, qui participent et amplifient largement la diffusion de données personnelles et qui impliquent un nouveau modèle économique et d'organisation qui se répand rapidement. S'agissant de l'applicabilité des règles relatives à la protection des données personnelles, il paraît également évident que toutes ces mutations ne sont pas neutres, notamment parce que les activités de traitement sont de plus en plus mobiles et internationales rendant leur localisation et celle des opérateurs plus difficiles³¹⁴.

D'une part, les enseignements que nous avons pu tirer de l'analyse des articles 3 et 4 de la directive « données personnelles », et, d'autre part, ces dernières considérations sur les développements technologiques nous amènent à adopter le constat, très largement partagé en doctrine, que cette directive est dépassée et, partant, qu'une réforme était nécessaire.

C'est dans ce contexte qu'en premier lieu, nous allons analyser de manière générale l'instrument (Chapitre 1) résultant de cette réforme. Ensuite, à l'instar de ce que nous avons fait pour la directive, nous allons examiner les critères d'applicabilité du règlement (Chapitre 2).

Chapitre 1. Le règlement général sur la protection des données : Quel(s) instrument(s)

Ce chapitre est consacré à l'étude du choix d'un règlement (Section 1) et de la question d'un texte unique qui réglerait l'ensemble de la matière (Section 2).

Section 1. Un règlement ?

A priori, il s'agit probablement du changement le plus important et, en tout cas, le plus visible. La refonte de la réglementation liée à la protection des données personnelles dans un règlement, nous semble être une excellente initiative et, de manière générale, celle-ci reçoit un accueil favorable en doctrine³¹⁵.

Cet enthousiasme est dû au caractère directement applicable du règlement dans les ordres juridiques nationaux. En effet, à l'inverse de la directive, le règlement ne nécessite ni transposition, ni aucune autre mesure de réception en droit national³¹⁶. A cet égard, nous avons souligné que les législations nationales de transposition n'offraient pas un degré d'harmonisation satisfaisant, en particulier à propos des critères d'applicabilité dont la transcription dans les législations nationales a posé certaines difficultés.

Le règlement ne se contente pas d'apporter une solution au manque d'harmonisation, il répond également à la problématique du conflit de lois entre les législations nationales. En effet, il suffit de vérifier que la situation entre dans le champ d'application du règlement pour conclure à l'application directe de ce

³¹⁴ C. KUNER, *Transborder data flows and data privacy law*, op. cit., pp. 3-4.

³¹⁵ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », op. cit., pp. 68-69 ; V. REDING, « The European data protection framework for the twenty-first century », op. cit., pp. 120-121.

³¹⁶ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 440 et pp. 474-475 ; W. KOTSCHY, « The proposals for a new General Data Protection Regulation problem solved », *International Data Privacy Law*, 2014, Volume 4, p. 274.

dernier. Ceci facilite grandement la tâche du juge qui ne devra plus s'interroger sur la loi applicable et, partant, apporte de la sécurité juridique aux parties³¹⁷. En outre, le risque d'application cumulative des législations nationales auquel est confronté l'opérateur sous le régime de la directive disparaît.

Les avantages découlant de l'harmonisation opérée par règlement sont donc nombreux. Toutefois, il nous faut mentionner que l'article 85 du règlement dispose que « *les États membres prévoient des exemptions ou des dérogations [...] si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information* » mais uniquement « *dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire* ». Cette disposition ne met évidemment pas en péril l'harmonisation des règles en matière de protection de données personnelles entre les États membres. En réalité, la seule critique que nous avons pu constater réside en ce que le choix d'un règlement n'a permis l'adoption d'un texte unique réglant tous les aspects de la protection des données personnelles en droit communautaire³¹⁸. A notre sens, ceci s'explique par l'absence de compromis politique concernant la protection des données personnelles dans des domaines particulièrement sensibles³¹⁹.

Section 2. Un texte unique ?

Lorsque le législateur européen amorça le processus qui devait aboutir à une réforme de la réglementation européenne en matière de données personnelles, l'ambition était d'élaborer « *une approche globale et cohérente, qui garantisse le plein respect du droit fondamental des personnes à la protection des données à caractère personnel* »³²⁰. Dans ce contexte, l'idée « *d'un instrument global, applicable aux opérations de traitement des données dans tous les secteurs et tous les domaines d'action de l'Union* » avait été émise³²¹. Ceci rejoignait la position du Groupe de Travail « article 29 » qui, dans son avis sur la proposition de réforme³²², rappelle qu'il a, à plusieurs reprises, souligné l'importance d'un cadre légal global.

Toutefois, il convient de constater, qu'au terme de la réforme, la réglementation européenne sur les données personnelles se composera non pas d'un mais de trois instruments; ce qui peut contraster avec la volonté affichée du législateur européen d'adopter un cadre légal global³²³. En outre, il nous faut rappeler que certains domaines restent en dehors de la réglementation européenne en la matière, notamment le traitement des données qui serait réalisé dans le cadre de la sécurité nationale³²⁴ ou de la politique étrangère et de sécurité commune. Il y a donc potentiellement des règles de trois natures différentes qui sont susceptible de s'appliquer : les dispositions du règlement général et celles du règlement visant les institutions européennes, les règles nationales qui découlent de la transposition de la directive et le droit

³¹⁷ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, op. cit., p. 440 et pp. 474-475.

³¹⁸ GAYREL C. et ROBERT R., op. cit., p. 173-174, note 12.

³¹⁹ *Ibidem*, p. 173-174, note 12.

³²⁰ Communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions concernant – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM(2010) 609 final, p. 4.

³²¹ Communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions concernant – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM(2010) 609 final, p. 4.

³²² Opinion 01/2012 of the « Article 29 » Data Protection Working Party on the data protection reform proposals (WP 191), adopted on 23 March 2012, p. 5.

³²³ GAYREL C. et ROBERT R., op. cit., p. 174.

³²⁴ V. REDING, « The European data protection framework for the twenty-first century », op. cit., pp. 121-122. Reding 22, p. 3 note 2 ; GAYREL C. et ROBERT R., op. cit., p. 174.

national lorsqu'il s'applique dans les domaines non couverts par la réglementation européenne. Par conséquent, une telle configuration comporte sans aucun doute des risques concernant l'articulation des différents instruments qui réglementent la protection des données personnelles dans les Etats membres. Ainsi, certains regrettent que la réforme n'ait pas accouché d'un texte unique, quitte à prendre la forme d'une directive.

A notre sens, il faut d'abord rappeler que le règlement, même s'il ne couvre pas l'ensemble des domaines de la réglementation européenne en matière de données personnelles, devrait apporter une solution au cadre légal fragmenté qui résulte de la transposition de la directive « données personnelles ». Toutefois, il n'est pas absurde d'envisager une réglementation qui apporterait une protection sectorielle à propos des données personnelles, au lieu de chercher à tout prix un régime central et globalisé. En effet, régler l'ensemble des questions liées à la protection des données personnelles avec un seul instrument, s'avère être un exercice particulièrement périlleux³²⁵. Effectivement il nécessite de couvrir, au travers d'un seul texte, des traitements de données dont la configuration est extrêmement variable. Ces traitements peuvent, de fait, survenir dans le cadre d'une relation contractuelle ou extracontractuelle, dans des rapports entre consommateurs et professionnels ou entre employeurs et employés, ou encore entre administrations et administrés. Il nous semble donc que la thèse d'un texte unique est utopique et ne constitue pas la panacée en terme de protection des données personnelles.

Chapitre 2. Les critères d'applicabilité du règlement : du nouveau ?

A l'instar de la directive « données personnelles », le règlement adopte la méthode unilatérale puisque comme l'énonce très sobrement la Commission dans son mémorandum, l'article 3 du règlement, intitulé « *champ d'application territoriale* », « *détermine le champ d'application territorial du règlement* »³²⁶. Cette disposition reprend la logique de l'article 4 de la directive « données personnelles ». En effet, le §1^{er} de l'article 3 du règlement, prévoit que celui-ci s'applique si le traitement a eu lieu « *dans le cadre des activités d'un établissement d'un responsable du traitement* » ; le §2, quant à lui, vient étendre l'application du règlement lorsque l'opérateur n'est pas « *établi* » dans l'Union. Il s'agit donc à nouveau d'un système dont les dispositions sont appelées à « s'emboîter » pour « *garantir qu'une personne physique ne soit pas exclue de la protection* »³²⁷. Notons, toutefois, que dans le règlement, le législateur européen abandonne le critère du « *moyen* » situé sur le territoire communautaire pour lui préférer un nouveau critère que nous examinerons plus loin³²⁸.

En outre, nous observons qu'à l'inverse de l'article 4 de la directive « données personnelles », l'article 3 du règlement « n'a plus qu'une » fonction. En effet, cette disposition du règlement n'a plus à déterminer quelle(s) législation(s) nationale(s) serai(en)t applicable(s).

³²⁵ B. KOOPS, *op. cit.*, pp. 256 et s. L'auteur considère que c'est une erreur d'essayer de « tout » régler dans un seul texte.

³²⁶ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, p. 71. L'auteur regrette ce manque d'explication à propos d'une disposition si importante et si discutée dans le cadre de la directive « données personnelles ».

³²⁷ Règlement général sur la protection des données, Considérant 23.

³²⁸ M. GALLARDO MESEGUER, « Aperçu de la dimension internationale du règlement général sur la protection des données à caractère personnel » in *Enjeux européens et mondiaux de la protection des données personnelles*, A. GROSJEAN (dir.), Bruxelles, Bruylant, 2015, p. 120.

Dans la suite de cette section, nous procéderons comme pour l'article 4 de la directive « donnée personnelles » en analysant, dans un premier temps, l'application lorsque le traitement est effectué « *dans le cadre des activités d'un établissement d'un responsable du traitement* » (Section 1^{er}) avant d'analyser la situation dans laquelle l'opérateur « *n'est pas établi dans l'Union* » (Section 2). Toutefois, dans la mesure où le §1^{er} de l'article 3 du règlement reprend le même critère que l'article 4, §1^{er}, point (a), de la directive, nous nous limiterons à un commentaire soulignant brièvement les quelques changements apportés à ce critère. Par ailleurs, nous nous concentrerons sur le §2 de la même disposition puisqu'elle diffère considérablement des critères d'applicabilité de la directive. Notons, enfin, que nous ferons l'économie de l'examen du §3 de l'article 3 du règlement qui reprend les termes de l'article 4, §1^{er}, point (b) et, comme son prédécesseur, ne présente qu'un intérêt pratique très limité.

Section 1. *Etabli dans l'Union : toujours le cadre des activités d'un établissement sur le territoire de l'Union*

Le §1^{er} du règlement, reprenant le même critère d'applicabilité que celui de l'article 4, §1^{er}, (a), de la directive ne nécessite pas de commentaire supplémentaire à ce que nous avons observé précédemment. Toutefois, nous avons repéré quelques modifications par rapport à la disposition de la directive qu'il nous semble intéressant de commenter.

Tout d'abord, le législateur européen vise non plus « *un établissement du responsable du traitement* » mais parle « *d'un établissement d'un responsable du traitement* ». Ce changement terminologique est davantage en phase avec la possibilité qu'un traitement ait plusieurs responsables.

Ensuite, le législateur européen intègre dans ce critère, l'éventualité d'une intervention d'un sous-traitant et prévoit à cet égard que le traitement effectué « *dans le cadre des activités d'un établissement [...] d'un sous-traitant sur le territoire de l'Union* » entraîne également l'applicabilité de la directive. En d'autres termes, le domaine d'applicabilité s'étend désormais non seulement aux établissements de l'opérateur mais également à ceux de son éventuel sous-traitant³²⁹.

En outre, c'est en ajoutant « *que le traitement ait lieu ou non dans l'Union* » que le législateur européen conclut ce §1^{er} de l'article 3. Par cette dernière précision, il affirme que l'application du règlement ne nécessite pas que le traitement de données soit effectué sur le territoire de l'Union³³⁰, ce qui était déjà bien établi dans la jurisprudence de la Cour.

Enfin, il nous faut préciser que la seconde phrase du point (a), §1^{er}, de l'article 4 de la directive est supprimée puisqu'elle visait l'hypothèse d'un opérateur disposant d'établissement sur le territoire de plusieurs Etats membres et, partant, confronté à l'application de plusieurs législations nationales. Cette seconde phrase perd son utilité dans le cadre du règlement.

Du reste, nous constatons que le §1^{er} de l'article 3 du règlement ne serait applicable à une situation semblable à l'affaire *Google Spain*, qu'au prix d'une interprétation extensive, similaire à celle adoptée par

³²⁹ M. GALLARDO MESEGUER, *op. cit.*, p. 120.

³³⁰ *Ibidem*, pp. 119-120.

la Cour pour déclarer la directive données personnelles applicable au moteur de recherche et à sa filiale espagnole.

Section 2. Etabli hors de l'Union : enfin la prise en compte de la localisation de la personne concernée

A l'inverse du §1^{er} de l'article 3 du règlement qui reprend un critère d'applicabilité de la directive « données personnelles », le §2 de la même disposition se différencie des critères existants dans ladite directive. En effet, même si ce §2 a vocation à compléter le §1^{er}, et, partant, le domaine d'applicabilité du règlement lorsque le responsable du traitement n'est pas établi dans l'Union, il n'a pas recours au critère du moyen situé sur le territoire communautaire, contrairement au point (c), §1^{er}, de l'article 4 de la directive « données personnelles ». Ainsi, le législateur européen a préféré conditionner l'applicabilité du règlement à la localisation de la personne concernée puisque lorsque l'opérateur n'est pas établi dans l'Union européenne, le règlement s'applique au traitement des données personnelles des personnes concernées, pour autant que cette dernière « se [trouve] sur le territoire de l'Union ».

Toutefois, se trouver sur le territoire de l'Union européenne ne suffit pas pour qu'une personne bénéficie de la protection du règlement. Encore faut-il que les activités du traitement en cause, soient liées soit « à l'offre de biens ou de services à [cette personne concernée] dans l'Union, qu'un paiement soit exigé ou non de [ladite personne] », soit « au suivi du comportement de [cette personne], dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

En résumé, le §2 de l'article 3 du règlement s'applique si les conditions suivantes sont réunies, à savoir, l'opérateur n'est pas établi dans l'Union (paragraphe 1), la personne concernée, se trouve effectivement sur le territoire de l'Union (paragraphe 2) et le traitement des données est lié à une offre de biens ou de services dans l'Union proposés à cette personne (paragraphe 3) ou au suivi de son comportement dans l'Union (paragraphe 4).

§1. Etre établi hors de l'Union

Nous avons déjà examiné cette condition lors de l'examen de la directive et avons alors considéré que l'opérateur n'était pas établi dans l'Union s'il n'avait pas d'établissement « pertinent » sur le territoire de l'Union. Nous avons, en outre, souligné qu'il ne suffisait pas que l'établissement principal soit situé en dehors de l'Union pour conclure que le responsable du traitement n'était pas établi dans l'Union³³¹. La même interprétation s'applique-t-elle dans le cadre du règlement ? A notre sens, cela ne va pas de soi.

Tout d'abord, la terminologie « être établi », nous amène à préférer une interprétation basée sur l'établissement principal. Ensuite, s'agissant de la directive, le Groupe de Travail « article 29 »³³² avait déjà alerté les institutions européennes sur la formulation potentiellement problématique de cette disposition. C'est donc en connaissance de cause, que le législateur conserve les termes « être établi ». Nous remarquons également que l'interprétation se rapportant à l'absence d'établissement pertinent sur le

³³¹ Voy., *supra*, p. 42 et s.

³³² Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 22.

territoire communautaire, se justifiait pour éviter une application simultanée des législations nationales. Cette justification a disparu avec la refonte de la directive en un règlement. Enfin, le législateur introduit et définit la notion d'établissement principal dans le règlement³³³.

Nous l'observons, les arguments en faveur d'une interprétation fondée sur l'établissement principal apparaissent plus nombreux dans le règlement que dans la directive « données personnelles ». Toutefois, à l'instar de la directive « donnée personnelles », le règlement a pour objectif « *d'éviter qu'une personne soit exclue de la protection* »³³⁴. Or, le choix d'une interprétation basée sur l'établissement principal risque de provoquer une brèche dans la protection offerte par le §1 et le §2 de l'article 3 du règlement qui se veut hermétique. En effet, il se pourrait que le traitement de données ne soit pas réalisé dans le cadre des activités d'un établissement d'un responsable du traitement sur le territoire de l'Union, échappant ainsi au §1^{er} du règlement, et qu'en outre, l'établissement principal du responsable se situe sur le territoire d'un Etat membre, ce qui écarterait le §2 du règlement et laisserait la personne concernée sans protection. A l'inverse, cette brèche est évitée si les termes « *n'est pas établi dans l'Union* » sont interprétés comme signifiant que le responsable du traitement ne dispose pas d'établissement pertinent, c'est-à-dire, d'établissement dans le cadre duquel le traitement des données a été effectué, sur le territoire de l'Union. Il semble donc regrettable que le législateur européen n'ait pas profité de la refonte de la directive pour clarifier le critère qu'il énonce simplement par « être établi »³³⁵.

Toutefois, en pratique, l'interprétation large que la Cour fit des termes « *dans le cadre des activités d'un établissement du responsable du traitement* » dans l'affaire *Google Spain*, nous conduit à penser qu'il serait assez étonnant que l'établissement principal du responsable soit établi dans l'Union et que le traitement de données ne soit pas rattaché au cadre des activités de cet établissement.

§2. Des personnes concernées qui se « trouvent » sur le territoire de l'Union

Le §2 de l'article 3 du règlement apporte une innovation majeure dans le droit européen de la protection des données en adoptant un critère centré sur la personne concernée. Pour la première fois, l'applicabilité de la réglementation relative aux données personnelles est donc envisagée dans la perspective de la personne concernée et du droit fondamental à la protection des données. Ce changement de perspective constitue très certainement une amélioration dans la consécration et la protection de ce droit, et il s'inscrit dans la continuité de la tendance qui a présidé à l'adoption de l'article 8 de la Charte des droits fondamentaux et à celle de l'article 16 du TFUE. C'est d'ailleurs l'article 16 du TFUE qui, en tant que base juridique, permet au règlement d'adopter une telle orientation, sans que l'acte ne soit remis en cause pour une éventuelle absence de lien avec le marché intérieur. Ceci dit, les deux hypothèses de la troisième exigence, démontrent bien que ce §2 reste proche des considérations du marché intérieur.

³³³ Règlement général sur la protection des données, Article 4, 1, (16) et Considérant 36. Voy. également l'article 56 du règlement général sur la protection qui détermine l'autorité de contrôle « chef de file » comme celle de l'état membre sur le territoire duquel est localisé l'établissement principal. C'est le principe du guichet unique, à ce sujet voir Communication de la Commission au Parlement européen concernant la position du Conseil sur l'adoption d'un 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) et abrogeant la directive 95/46/CE, COM(2016)214 final.

³³⁴ Règlement général sur la protection des données, Considérant 23.

³³⁵ HENROTTE et F. COTON, *op. cit.*, p. 192.

Pour notre part, nous sommes particulièrement favorables à l'utilisation de la localisation de la personne concernée comme critère d'applicabilité. En effet, ce critère nous paraît particulièrement pertinent pour assurer la protection des données des personnes localisées dans l'Union; ceci n'est pas nécessairement le cas d'un critère utilisant la localisation de l'opérateur ou du fichier. Nous l'avons souligné dans l'analyse du point (a), §1^{er} de l'article 4 de la directive « données personnelles », le critère « *du cadre des activités du responsable* » est susceptible de protéger des personnes qui ne présentent aucun lien avec l'Union comme un internaute australien résidant au Japon, mais pourrait ne pas assurer la protection de tous les traitements de données concernant des personnes localisées au sein de l'Union. Le résultat serait le même si le critère d'applicabilité était *stricto sensu* la localisation de l'opérateur ou celle du fichier.

Toutefois, si nous adhérons au choix de la localisation de la personne concernée comme critère d'applicabilité, nous ne pouvons pas en dire autant de la façon dont ce critère est concrétisé dans la version finale du §2, de l'article 3 du règlement. Ainsi, cette disposition s'applique pour autant que la personne concernée « *se trouve sur le territoire de l'Union* » (nous soulignons). 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. Par cette formulation, faut-il comprendre que le législateur européen fait référence à la résidence de la personne concernée ? Nous pensons que la réponse est négative, sinon pourquoi le législateur a-t-il amendé la proposition de la Commission qui prévoyait précisément l'application du règlement si la personne résidait sur le territoire de l'Union³³⁶.

A notre sens, cet amendement permet surtout au règlement d'être en phase avec l'article 16 du TFUE et l'article 8 de la Charte fondamentale, qui consacrent un droit à la protection des données personnelles à l'égard de « *toute personne* ». C'est, en outre, cette même intention qui ressort très clairement des considérants 2 et 14 du règlement. Ce dernier explique ainsi que « *la protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence* ». L'Union affirme donc, 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. Du reste, cette volonté était déjà présente au sein de la directive « données personnelles », ce qui n'avait d'ailleurs pas manqué d'être observé par plusieurs auteurs à la suite de l'arrêt *Google Spain*. La différence étant, toutefois, que la directive trouvant sa base légale dans l'article 114, TFUE, il était contestable que l'établissement et le fonctionnement du marché intérieur nécessitât la protection de personnes sans lien avec l'Union. Ce n'est plus le cas avec le règlement puisqu'il a été adopté en vertu de l'article 16, TFUE. Néanmoins, la question demeure: l'Union européenne a-t-elle vraiment vocation à protéger de manière globale le droit fondamental à la protection des données personnelles au travers de ce règlement, quitte à rendre le critère d'applicabilité incertain?³³⁷ En effet, à notre sens la formulation du §2, de l'article 3 du règlement s'avère incertaine. Par exemple, le §2 s'applique-t-il à un résident européen qui voyagerait en dehors de l'Union pour un court séjour, ou à un résident d'un Etat tiers qui voyagerait en Europe pour ses vacances ? De fait, dans pareils cas, le résident

³³⁶ Cette amendement n'est arrivé qu'au stade de la première lecture au Parlement, les différentes discussions en commissions parlementaires n'avaient pas abouti à une modification du texte sur ce point, tout au plus un amendement proposait de substituer au critère de résidence celui de domicile.

³³⁷ En d'autres termes, il semble certain que l'Union doit protéger et promouvoir ce droit comme tous les droits fondamentaux, mais 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 ?

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.

En outre, il convient également de déterminer le moment de référence pour évaluer si la personne concernée se trouve sur le territoire européen. Est-ce au moment où les données sont collectées, enregistrées, diffusées, ou au cours d'une autre opération de leur traitement, ou encore à un tout autre moment ? Cette disposition pose également question s'agissant de la loi applicable en cas de conservation des données. Ainsi, il nous semble que les questions entourant l'interprétation du §2, de l'article 3 du règlement sont nombreuses et à n'en pas douter, nécessiteront les lumières de la Cour de justice.

Toutefois, selon nous, malgré à une volonté affichée de la part du législateur européen de protéger les données personnelles indépendamment de la nationalité ou de la résidence de la personne concernée, le critère d'applicabilité du §2 de l'article 3, exige un double rattachement de la situation avec l'Union. D'une part, nous venons de le souligner, il faut que la personne concernée se trouve sur le territoire de l'Union, et, d'autre part, il faut que le traitement soit lié à l'offre de biens ou de services à cette personne concernée dans l'Union ou au suivi du comportement de cette personne qui a lieu au sein de l'Union. En d'autres termes, tant l'activité pour laquelle les données sont traitées, que la personne dont les données sont traitées, doivent avoir un lien avec l'Union. Il nous semble, par conséquent, que s'agissant du degré de proximité entre la situation en cause et l'Union, le critère d'applicabilité contenu dans ce paragraphe est plus exigeant que les autres critères que nous avons analysés dans la directive « données personnelles ».

§3. **L'offre de biens ou de services à la personne concernée**

Ainsi qu'il vient d'être précisé, il ne suffit pas que le responsable du traitement ne soit pas établi dans l'Union et que la personne concernée se trouve sur le territoire de l'Union pour que le critère de l'article 3, §2 soit satisfait. Encore faut-il que le traitement soit lié à une offre de biens ou de services à la personne concernée dans l'Union, ou au suivi de son comportement au sein de l'Union.

La première hypothèse vise clairement les consommateurs. Par son point (a), §2 de l'article 3 du règlement offre aux consommateurs une protection harmonisée de leurs données personnelles au sein du marché intérieur. Cela participe à la volonté des institutions européennes d'encourager les consommateurs à entrer en contact avec des opérateurs localisés dans d'autres Etats membres et, partant, à établir un marché intérieur, et notamment un marché intérieur digital dans lequel la protection des données est un facteur primordial.

La protection de ce point (a) s'applique dès lors qu'il existe une offre de biens ou de services et ne nécessite donc pas la conclusion d'un contrat³³⁸. Toutefois, il convient de circonscrire la notion d'« *offres ou de services dans l'Union* », notamment en vue d'éviter une application mondiale du règlement à l'ensemble des sites internet. En effet, il ne pourrait être considéré qu'une offre de biens ou de services existe au sens du règlement, simplement parce que le site de l'opérateur qui propose le bien ou le service

³³⁸ HENROTTE et F. COTON, *op. cit.*, p. 190.

est accessible par le consommateur se trouvant sur le territoire de l'Union³³⁹. C'est d'ailleurs le sens du considérant 23 qui précise que pour « *déterminer si un tel responsable du traitement [...] offre des biens ou des services à des personnes concernées [...] la simple accessibilité du site internet du responsable du traitement [...], 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* ». En d'autres termes, le point (a), §2 de l'article 3 du règlement, combiné au considérant 23 renvoie à un certain « *degré de ciblage* » qui avait déjà été évoqué par le groupe de travail « article 29 » à propos du point c, §1^{er}, article 4 de la directive « données personnelles ». Dans son avis, le groupe de travail avait alors considéré qu'« *un critère similaire pour la législation de l'UE en matière de protection des données pourrait faire l'objet d'une réflexion lors des futures discussions sur la révision du cadre juridique* »³⁴⁰.

Au-delà du domaine des données personnelles, le critère de « l'activité dirigée » ou de la « dirigeabilité des activités » ne constitue nullement un critère inédit en droit européen³⁴¹. En effet, il est déjà présent dans le règlement Bruxelles Ibis³⁴² ainsi que dans le règlement Rome I³⁴³. Ce dernier l'a adopté afin de régler les conflits de lois à propos des contrats de consommation³⁴⁴, et contient dans ses considérants, à l'instar du considérant 23 dans le règlement « données personnelles », l'idée que « *le simple fait qu'un site internet soit accessible ne suffit pas pour rendre applicable* » les dispositions qui protègent les consommateurs. Toutefois, notons que dans les règlements Rome I et Bruxelles Ibis, l'application des dispositions spécifiquement relatives aux contrats de consommation nécessitent la conclusion du contrat et non la simple existence d'une offre.

Il convient de ne pas oublier qu'en définitive il reviendra à la Cour d'interpréter le critère de l'article 3, §2, point (a), du règlement. A cet égard, la jurisprudence de la Cour à propos du règlement Bruxelles Ibis, mérite d'être mentionnée puisque la juridiction de l'Union y a déjà interprété la notion « *d'activité dirigée vers* » dans le cadre d'internet. La Cour considère tout d'abord que cette notion implique « *la volonté du commerçant de se tourner vers un ou plusieurs autres États membres* »³⁴⁵, en précisant par la suite qu'une telle volonté n'est pas « *toujours présente dans le cas de la publicité au moyen d'Internet* » même si « *une publicité faite sur un site Internet par un commerçant est en principe accessible dans tous les États et, par conséquent, dans l'ensemble de l'Union européenne* »³⁴⁶. Par conséquent, la Cour affirma que « *le commerçant doit avoir manifesté sa volonté d'établir des relations commerciales avec les consommateurs d'un ou de plusieurs [...] États membres, au nombre desquels figure celui sur le territoire duquel le consommateur a son domicile* »³⁴⁷, et que cette volonté se manifeste au travers d'« *indices démontrant que le commerçant envisageait de commercer avec des consommateurs domiciliés dans d'autres États*

³³⁹ M. GALLARDO MESEGUER, *op. cit.*, p. 120., *op. cit.*, pp. 120-121

³⁴⁰ Avis 8/2010 du Groupe de Travail « Article 29 » *op. cit.*, p. 28 ; HENROTTE et F. COTON, *op. cit.*, p. 190.

³⁴¹ M. GALLARDO MESEGUER, *op. cit.*, pp. 120-121 ; HENROTTE et F. COTON, *op. cit.*, pp. 190-191.

³⁴² 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, JOUE, L 351, 20 décembre 2012, p. 1. (Bruxelles I bis).

³⁴³ Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, JOUE, L 177, 4 juillet 2008, p. 6. (Rome I).

³⁴⁴ Ce critère apparaît également dans le règlement Bruxelles Ibis.

³⁴⁵ CJUE, 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, Rec., 2010, p. I-12527, pt 63 ; M. GALLARDO MESEGUER, *op. cit.*, p. 120-121.

³⁴⁶ CJUE, 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, *op. cit.*, pt 68.

³⁴⁷ CJUE, 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, *op. cit.*, pt 75

membres, dont celui sur le territoire duquel ce consommateur a son domicile »³⁴⁸. Par la suite, la Cour a réitéré sa jurisprudence *Pammer et Alpenhof* dans des affaires étrangères à l'application du règlement Bruxelles Ibis. Ainsi dans un arrêt *L'Oréal*³⁴⁹ contre E-bay, elle a précisé, en faisant explicitement référence à l'arrêt *Pammer et Alpenhof*, « que la simple accessibilité d'un site Internet sur le territoire couvert par la marque ne suffit pas pour conclure que les offres à la vente y affichées sont destinées à des consommateurs situés sur ce territoire ». Il y a fort à parier qu'elle fera de même lorsqu'elle sera amenée à interpréter le point (a), §2, article 3 du règlement.

§4. Le suivi du comportement de ces personnes

A défaut d'être lié à une offre de biens ou de services à la personne concernée dans l'Union, le traitement ne sera soumis au règlement que s'il est lié au suivi du comportement de la personne concernée et pour autant qu'il s'agisse d'un comportement qui a lieu au sein de l'Union. C'est la deuxième hypothèse dans laquelle le législateur entend protéger les données personnelles de la personne concernée qui se trouverait sur le territoire de l'Union.

Le « suivi du comportement » n'est pas défini en tant que tel par la directive. Néanmoins, 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 apparaît que le point (b) vise en particulier la pratique du profilage que le règlement définit comme un traitement de données consistant à « évaluer certains aspects personnels³⁵⁰ relatifs à une personne physique ». Il convient de souligner l'effort du législateur européen d'appréhender ce nouveau phénomène du profilage auquel l'application de la directive « données personnelles » était malaisée au travers du critère « des moyens » situés sur le territoire communautaire. Le règlement apporte ainsi une réponse en termes d'applicabilité aux activités de certains opérateurs, consistant à recueillir des informations à propos des personnes concernées, en vue de constituer leur profil, parfois aussi considéré comme le double virtuel de la personne. En outre, dans la mesure où le profilage a souvent recours, entre autres, à l'utilisation de « cookies » ou de bannières *JavaScript*, le point (b) du §2 permet également de prendre en compte ces logiciels qualifiés parfois « d'espions »³⁵¹.

³⁴⁸ CJUE, 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, op. cit., pts 77-78, 81 et 83-84. La Cour donne certains exemples de ce qui peut constituer des indices et de ce qui n'en est pas. Elle considère par exemple que la mention d'une adresse électronique ou géographique ne constitue pas de tels indices dans la mesure où il s'agit de mentions obligatoires. A l'inverse, « la mention selon laquelle ce dernier offre ses services ou ses biens dans un ou plusieurs États membres nommément désignés » démontre l'existence d'une volonté du commerçant de se tourner vers les consommateurs des États membres nommément désignés. Une combinaison d'indices est également susceptible de démontrer l'existence d'une telle volonté, la Cour relève ainsi le nom de domaine utilisé. Voy. aussi le point 93 pour une liste non-exhaustive de indices permettant de considérer que l'activité du commerçant est dirigée vers l'État membre du domicile du consommateur.

³⁴⁹ CJUE, 12 juillet 2011, aff. C-324/09, *L'Oréal SA et autres contre eBay International AG et autres*, Rec., 2011, p. I-6011, pt 64.

³⁵⁰ Règlement général sur la protection des données, Article 4, (4). Ce traitement vise notamment à « analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

³⁵¹ HENROTTE et F. COTON, op. cit., pp. 191-192. Il nous semble opportun de rajouter que même si le législateur avait en tête le suivi du comportement sur internet de la personne concernée au travers des « cookies » ou de bannière *JavaScript*, le paragraphe 2, point (b) de l'article 3 vise simplement le suivi du comportement de la personne concernée. Ceci laisse donc la possibilité d'inclure également dans l'interprétation de cette disposition toutes les données qui peuvent être recueillies avec les objets « connectés », comme par exemple les données qui sont mesurées et enregistrées par les bracelets ou montres connectés.

Notons encore, 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 européen³⁵². Cette dernière précision n'était ni présente dans la proposition originale de la Commission, ni dans le texte qui a été adopté par le Parlement en première lecture, mais a été ajoutée à la fin du processus d'adoption. Son absence avait d'ailleurs été critiquée³⁵³ alors que le point (a) du même paragraphe précisait lui, dès la proposition originale, que l'offre de biens ou de services devait être dirigée vers l'Union. La critique portait sur fait que le point (b), §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 critère général du §2 n'exigeait plus que la personne concernée réside dans l'Union, mais simplement qu'elle se trouve sur son territoire. Par conséquent, la critique constatée ci-dessus n'était plus fondée.

En outre, la dernière phrase du point (b) l'inscrit dans la même tendance que le point (a). En effet, au critère général du §2 exigeant que la personne concernée se trouve sur le territoire de l'Union européenne vient s'ajouter un critère alternatif qui lie explicitement la protection du règlement au marché intérieur. Ce faisant, le législateur se rapproche de ce que certains, en doctrine, ont appelé la doctrine du « *market sovereignty* »³⁵⁴. L'idée sous-jacente à cette doctrine consiste pour l'opérateur à accepter les règles du marché intérieur, s'il veut y être actif et y proposer des biens ou des services. La doctrine du « *market sovereignty* » permettrait ainsi de justifier que le domaine d'applicabilité de la réglementation européenne sur les données personnelles s'étende à des opérateurs qui ne sont pas établis sur le territoire de l'Union, puisqu'il paraît normal pour ces opérateurs d'accepter les règles du marché sur lequel ils veulent se déployer³⁵⁵.

La question qui s'impose naturellement après l'analyse de ce § 2 du règlement, est de savoir si ce critère peut s'appliquer de manière plus convaincante dans le cadre de l'affaire *Google Spain* que le critère du « cadre des activités d'un établissement du responsable » ? Le préalable pour que le §2 s'applique consiste à considérer que le traitement de données en cause n'est pas effectué dans le cadre des activités de *Google Spain*, mais uniquement dans le cadre des activités de *Google Inc*, ce qui nous l'avons vu, aurait pu être retenu par la Cour.

Ensuite, il nous semble que le premier critère est effectivement rempli en ce que le citoyen espagnol se trouvait bien sur le territoire de l'Union, à tout le moins il n'y a pas d'élément qui peut nous laisser penser le contraire. Enfin, il faut encore que l'une des deux hypothèses du dernier critère soit avérée. A cet égard, le traitement en cause, à savoir la diffusion dans les résultats proposés par *Google*, de la page internet du journal espagnol, n'est pas lié, à notre sens, à un « suivi du comportement » du citoyen

³⁵² *Ibidem*, p. 191.

³⁵³ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, pp. 71-72.

³⁵⁴ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, pp. 98-102. En outre, l'auteur estime qu'il s'agit également d'une théorie qui permettrait de rendre l'application de la réglementation européenne sur les données personnelles plus effective.

³⁵⁵ SVANTESSON, « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *op. cit.*, pp. 98-102 ; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, *op. cit.*, p 272.

espagnol par *Google* au sens du règlement. Reste donc à déterminer si ce traitement est lié à une « offre de biens ou de services » au citoyen espagnol dans l'Union ? Nous pensons que la réponse peut être positive. En effet, il semble qu'il soit peu contestable qu'une offre³⁵⁶ de services de la part de *Google Inc.* soit dirigée vers l'Espagne permettant aux personnes se trouvant en Espagne d'effectuer des recherches sur le moteur proposé par *Google*. En outre, à notre sens, la présence de la page internet du journal espagnol dans les résultats proposés par *Google*, est liée au service qu'il offre en Espagne et notamment à la personne concernée.

Toutefois, la position inverse peut également être défendue. Ainsi, contrairement à ce qui a été écrit en doctrine³⁵⁷, l'application du point (a), du §2 à *Google Inc* ne nous paraît pas si évidente. A notre sens, l'article 3, §2, point (a) vise explicitement la situation dans laquelle un consommateur communique ses données personnelles dans le cadre d'une offre de biens ou de services, par exemple lorsqu'il commande un article sur internet ou s'abonne à un service de musique en streaming. Dans ces deux derniers cas, le consommateur communique une série de données personnelles dont le traitement est indéniablement mais également exclusivement lié à l'offre de biens ou de services faite à la personne concernée. Dans l'application de l'article 3, §2, point (a), à l'affaire *Google Spain* que nous avons proposée ci-dessus, le lien entre le traitement et l'offre de service est d'une autre nature puisque ce traitement fait partie du contenu du service qui est proposé mondialement et n'est pas lié spécifiquement à l'offre du service faite à la personne concernée. En d'autres termes, le traitement de données est lié au service offert par *Google* parce que ce traitement est nécessaire à l'existence du service, peu importe à qui l'offre de service est adressée mais il n'est pas directement lié au fait que *Google* offre ce service à la personne concernée.

Enfin de compte, à notre avis, le §2, article 3 du règlement ne semble pas apporter une réponse plus convaincante à la question du domaine d'application qui se pose dans le cadre de l'affaire *Google Spain* que le critère du « cadre des activités d'un établissement du responsable ».

³⁵⁶ L'article 3, paragraphe 2, point (a) du règlement général sur la protection des données, précise qu'il importe peu qu'un paiement soit exigé ou non à la personne concernée en contre partie du bien ou du service.

³⁵⁷ HENROTTE et F. COTON, *op. cit.*, p. 191. Les auteurs considèrent que « le cas soumis à la Cour de Justice de l'Union européenne par la Cour d'appel nationale espagnole serait clairement rentré dans son [article 3, paragraphe 2, point (a), règlement général sur la protection des données] champ d'application »

Conclusion

Ce travail avait pour but d'étudier le domaine d'applicabilité de la directive et, partant, d'examiner les critères qui le déterminent. A cet égard, il est très vite apparu que les objectifs de la directive occupaient une place prépondérante dans cet examen et que les critères d'applicabilité contenus dans la directive devaient nécessairement s'analyser à la lumière de ces objectifs. L'affaire *Google Spain* l'a d'ailleurs parfaitement illustré. En effet, dans cette affaire, la Cour a manifestement opté pour une interprétation privilégiant la protection des données personnelles et, par conséquent, a garanti que la protection de ce droit fondamental ne soit pas affaiblie par la mise en place de la libre circulation des données, souhaitée par le législateur dans le cadre du développement du marché intérieur.

Le législateur lui-même avait reconnu lors de l'adoption de la directive, que la libre circulation des données, qui est l'objectif premier de ladite directive, ne pouvait se faire au détriment de la protection des données personnelles. A cette fin, le législateur s'est efforcé de concevoir un domaine d'applicabilité qui visait à éviter tout contournement de la directive, et partant, d'assurer à chacun une protection efficace et complète. C'est dans cet esprit qu'il a adopté l'article 4 de la directive, en établissant un premier critère d'applicabilité qui vise l'hypothèse où l'opérateur est établi sur le territoire communautaire et un deuxième critère, complétant le premier, qui régit les cas où l'opérateur est établi en dehors du territoire communautaire. De surcroît, le législateur européen n'exige pas que l'opérateur soit établi sur le territoire de l'Union. En effet, la version finale du premier critère ne requiert pas que l'établissement principal de l'opérateur soit localisé dans un Etat membre, mais se satisfait de la présence d'un simple établissement de l'opérateur sur le territoire de l'Union, pour autant que le traitement de données s'inscrive dans le cadre des activités dudit établissement. C'est d'ailleurs sur base de ce critère que la Cour a jugé la directive applicable au traitement de données en cause dans l'affaire *Google Spain*.

Toutefois, nous nous sommes montrés critiques par rapport à ce raisonnement de la Cour. En effet, le traitement des données fut exclusivement réalisé par *Google Inc* et surtout rien ne permettait de rattacher ce traitement de données aux activités de *Google Spain*. Cependant, la Cour a profité de l'existence d'un lien économique entre *Google Spain* et *Google Inc* pour considérer que le traitement de données était, en quelque sorte, indirectement indispensable à l'activité de *Google Spain*. Ceci constitue à notre sens une interprétation extensive des termes de la directive qui, en outre, emporte des conséquences à propos du conflit de lois de transposition, que la Cour semble ignorer. Ainsi, si une telle interprétation de l'article 4, qui règle à la fois l'applicabilité de la directive et le conflit de lois, rend cette disposition applicable à la situation en cause, elle ne permet pas de déterminer une loi applicable, puisque l'ensemble des filiales européennes du moteur de recherche présentent le même lien économique que *Google Spain* avec *Google Inc*. Dans cette optique, l'ensemble des lois de transposition devrait s'appliquer au traitement de données en cause, ce qui est en contradiction absolue avec le principe du marché intérieur et force à constater l'échec de la directive à satisfaire son objectif d'achèvement du marché intérieur. Nous pouvons donc en conclure que la Cour, en jugeant que le traitement de données s'inscrit dans le cadre des activités de *Google Spain*, s'est focalisée sur l'applicabilité de la directive en vue de garantir la protection des données de la personne concernée, mais a, de ce fait, ignoré la question du conflit de lois et, *in fine*, mis à mal l'idée de libre circulation des données.

Dans cette affaire, l'alternative pour la Cour aurait été de considérer que le traitement de données en cause n'avait pas été effectué dans le cadre des activités de *Google Spain* et de préserver ainsi l'article 4 d'une interprétation préjudiciable au marché intérieur. La Cour aurait alors dû appliquer le deuxième critère qui nécessite que l'opérateur ne soit pas établi sur le territoire communautaire, mais utilise pour son traitement de données des moyens qui, eux, sont situés le territoire d'un Etat membre. Dans cette perspective, ce n'est plus l'échec de la directive à satisfaire son objectif d'achèvement du marché intérieur qui se dévoile, mais celui à garantir la protection des données personnelles. En effet, la seule possibilité d'aboutir à l'application de la directive sur base de ce deuxième critère, en préservant à la fois l'objectif de libre circulation des données et celui de la protection des personnes concernées, est de considérer que les termes de la directive « *ne pas être établi sur le territoire de la Communauté* » signifient en réalité ne pas disposer sur le territoire communautaire d'un établissement dans le cadre des activités duquel le traitement en cause serait effectué et, que dans ces circonstances, l'opérateur responsable du traitement ait recours à des moyens localisés sur le territoire communautaire. C'est, enfin, ici que la faille du champ d'application se révèle.

La configuration des faits dans l'affaire *Google Spain* illustre donc la circonspection dont il faut faire preuve dans l'interprétation des termes de l'article 4 pour préserver les objectifs de la directive. Au surplus, en poussant le raisonnement à son terme, cette affaire permet de découvrir la faille du champ d'applicabilité de la directive que même les précautions d'interprétation ne semblent pas pouvoir combler.

Ces seuls éléments nous amèneraient à penser que l'applicabilité de la directive « données personnelle » mérite d'être repensée. Si d'aventure, la présence d'une faille dans l'emboîtement des critères d'applicabilité et l'inévitable complexité de l'interprétation qui en résulte ne suffisaient pas à convaincre de la nécessité d'une réforme, le défaut d'harmonisation des régimes nationaux et l'obsolescence de la directive par rapport aux évolutions technologiques vingt ans après son adoption, ne laissent plus subsister aucun doute à ce sujet.

Sans surprise, ces considérations nous amènent à saluer l'adoption d'un nouveau cadre législatif, à savoir, un règlement, à propos consacrant la protection des données personnelles. La refonte de la directive en un règlement apparaît particulièrement positive à l'égard de l'harmonisation des règles nationales et, partant, du fonctionnement du marché intérieur. Néanmoins, il semble que le choix du règlement n'ait pas permis l'adoption d'un texte unique et, par conséquent, le cadre légal régissant la matière des données personnelles en droit européen, demeure fragmenté. Cependant, s'agissant de l'hypothèse d'un texte unique, nous conservons une certaine réserve, tant il nous paraît illusoire de pouvoir régler au travers d'un seul texte l'ensemble des situations où intervient la protection des données personnelles.

Concernant les critères d'applicabilité, le règlement général sur les données personnelles a conservé la logique de la directive « données personnelles » en adoptant deux critères ; l'un étant appelé à s'appliquer lorsque l'opérateur est établi sur le territoire de l'Union et l'autre visant les situations où l'opérateur n'est pas établi sur ce territoire. En reprenant la notion du cadre des activités de l'établissement d'un responsable, le premier critère est très similaire à celui de la directive « données personnelles ». En

revanche, le deuxième critère d'applicabilité du règlement, diffère considérablement de celui de la directive puisqu'il s'articule autour de la localisation de la personne concernée, ce à quoi nous sommes très favorables.

En outre, le deuxième critère, tout en étant centré sur la localisation de la personne concernée, conserve l'exigence d'une proximité avec le territoire de l'Union européenne et surtout du marché intérieur, dans la mesure où il ne permet l'application du règlement que pour autant que le traitement des données soit lié à une offre de biens ou de services dans l'Union proposés à la personne concernée, ou, à défaut, soit lié au suivi du comportement de cette personne dans l'Union. Cette proximité avec le marché intérieur nous apparaît comme positive dans la mesure où elle justifie et, partant, renforce la légitimité de la directive à s'appliquer à des opérateurs établis en dehors du territoire de l'Union. En effet, l'opérateur étranger qui veut déployer ses activités sur un marché doit s'attendre à être soumis aux règles de ce marché. A cet égard plus le marché est grand, plus le rapport de force incitera l'opérateur à en respecter les règles ; l'avantage de gérer cette politique au niveau européen apparaît dès lors renforcé

Toutefois, en ce qui concerne le deuxième critère, nous regrettons que le législateur européen ait conservé les termes « *n'est pas établi* » puisque, interprété littéralement, ils aboutissent à considérer que ce critère exige que l'établissement principal ne soit pas situé sur le territoire de l'Union pour s'appliquer, ce qui laisse apparaître de nouveau une faille dans le domaine d'applicabilité du règlement. Il est également regrettable, à notre sens, que ce deuxième critère du règlement ait été amendé pour protéger les personnes qui se « *trouvent* » sur le territoire européen et non celles qui y résident. En effet, si cet amendement s'accorde davantage avec le souhait du législateur européen de garantir une protection des données personnelles pour toute personne, la concrétisation de ce critère s'avère autrement plus incertaine que celle du critère de la résidence.

Enfin, le règlement traduit l'inversion progressive dans la priorité des objectifs. En effet, ce dernier trouve sa base légale non pas dans l'article 114, TFUE, qui permet l'adoption de mesures en vue d'achever le marché intérieur, mais dans l'article 16, TFUE, qui prévoit, pour toute personne, le droit à la protection des données personnelles. En d'autres termes, si l'harmonisation des régimes nationaux de protection des données pouvait être vue comme l'objectif premier lors de l'adoption de la directive, il est manifeste, qu'à l'heure actuelle, l'objectif premier du règlement vise la protection des données personnelles. Il semble donc que le législateur européen ait suivi la tendance qui, d'une part se dégageait depuis un certain temps du droit primaire et, d'autre part, prévalait également dans la jurisprudence de la Cour. Ainsi, le législateur européen protège désormais les données personnelles non plus au travers d'une mesure « marché intérieur » mais bien dans le cadre d'une politique à part. Si cette réforme nous semble salubre pour la protection des données personnelles, nous en sommes désormais convaincus, elle ne sera pas la dernière évolution législative en la matière.

Tables des matières

Introduction	4
Titre 1. Le cadre de l'applicabilité et les objectifs de la directive 95/46.....	7
Chapitre 1. La définition de la problématique au travers de l'arrêt <i>Google Spain</i>.....	7
Section 1. Google Spain : Faits et raisonnement de la Cour	7
Section 2. L'applicabilité : une question problématique mais déterminante.....	9
§1. L'applicabilité dans sa dimension spatiale	9
§2. L'applicabilité et la force obligatoire	10
§3. L'applicabilité et l'extraterritorialité.....	11
§4. L'applicabilité et les choix du législateur européen.....	12
Chapitre 2. Les objectifs de la réglementation sur les données personnelles	16
Section 1. Les objectifs et l'applicabilité	17
Section 2. Les objectifs des autres instruments de protections des données personnelles ..	17
Section 3. Les objectifs de la directives 95/46	18
§1. La libre circulation des données dans le marché intérieur	18
§2. Le droit à la protection des données personnelles.....	22
Titre 2. L'applicabilité de la directive 95/46/CE	25
Chapitre 3. Les articles 3 et 4 de la directive 95/46/CE : Les critères d'applicabilité	25
Section 1. Article 3 : Les conditions générales d'applicabilité de la directive 95/46	26
§1. Les données personnelles	26
§2. Le traitement	27
§3. Le responsable du traitement.....	28
§4. Le champ d'application du droit communautaire	31
§5. Les activités exclusivement personnelles ou domestiques	32
Section 2. Article 4 : Les critères d'applicabilité alternatifs et exclusifs.....	36
§1. Article 4, §1 ^{er} , (a) : « Le cadre des activités d'un établissement ».....	36
§2. Article 4, §1 ^{er} , (c) : « Le recours à des moyens situés sur le territoire Communautaire »	42
Chapitre 4. La transposition de la directive 95/46 dans les droits nationaux.....	46
Section 1. Le conflit de lois de transposition	46
§1. « Le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre »	47
§2. « Le responsable de traitement qui n'est pas établi sur le territoire et qui a recours à des moyens sur le territoire communautaire »	50
Section 2. L'harmonisation.....	51
Titre 3. Une réforme inévitable	53
Chapitre 1. Le règlement général sur la protection des données : Quel(s) instrument(s)	

Section 1. Un règlement ?	54
Section 2. Un texte unique ?	55
Chapitre 2. Les critères d'applicabilité du règlement : du nouveau ?	56
Section 1. Etabli dans l'Union : toujours le cadre des activités d'un établissement sur le territoire de l'Union	57
Section 2. Etabli hors de l'Union : enfin la prise en compte de la localisation de la personne concernée	58
§1. Etre établi hors de l'Union	58
§2. Des personnes concernées qui se « trouvent » sur le territoire de l'Union.....	59
§3. L'offre de biens ou de services à la personne concernée.....	61
§4. Le suivi du comportement de ces personnes.....	63
Conclusion	66
Tables des matières	69
Bibliographie.....	71

Bibliographie

Législations

Conventions internationales

- Traité sur le fonctionnement de l'Union européenne.
- Traité sur l'Union européen.
- Charte des droits fondamentaux de l'Union européenne.
- Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n°108), faite à Strasbourg le 28 janvier 1981.
- La Convention de sauvegarde des droits de l'homme et libertés fondamentales.

Règlements

- Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *JOUE*, 2016, L 119/1.
- 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, *JOUE*, 2012, L 351/1 (Bruxelles I bis).
- Règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, *JOUE*, 2008, L 177/6 (Rome I).
- Règlement (CE) 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *JOCE*, 2001, L 8/1.

Directives

- Directive 2011/83/UE du Parlement européen et du Conseil, du 25 octobre 2011, relative aux droits des consommateurs, modifiant la Directive 93/13/CEE du Conseil et la Directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la Directive 85/577/CEE du Conseil et la Directive 97/7/CE du Parlement européen et du Conseil, *JOUE*, 2011, L 304/64.
- Directive 2001/37/CE du Parlement européen et du Conseil, du 5 juin 2001, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de fabrication, de présentation et de vente des produits du tabac, *JOCE*, 2001, L 194/26.
- Directive 1999/44/CE du Parlement européen et du Conseil, du 25 mai 1999, sur certains aspects de la vente et des garanties des biens de consommation, *JOCE*, 1999, L-171/12.
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE*, 1995, L 281/31.

- Directive 86/653/CEE du Conseil, du 18 décembre 1986, relative à la coordination des droits des Etats membres concernant les agents commerciaux indépendants, *JOCE*, 1986, L 383/17.

Propositions

- Proposition modifiée de directive du Conseil 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, COM(92)122 final, *JOCE*, 1992, C 311/04.
- Proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, COM(2013)813 final.

Jurisprudences

- CJUE, 13 mai 2014, aff. C-131/12, *Google Spain et Google*, *Rec.*, 2014, p. I-317.
- CJUE, 12 juillet 2011, aff. C-324/09, *L'Oréal SA et autres contre eBay International AG et autres*, *Rec.*, 2011, p. I-6011.
- CJUE, 7 décembre 2010, aff. jointes C-585/08 et C-144/09, *Pammer et Alpenhof*, *Rec.*, 2010, p. I-12527.
- CJCE, 6 novembre 2003, aff. C-101/01, *Procédure pénale c. Bodil Lindqvist*, *Rec.*, 2003, p. I-12971.
- CJCE, 20 mai 2003, aff. jointes C-465/00, C-138/01, C-139/01, *Rechnungshof*, *Rec.*, 2003, p. I-4989.
- CJCE, 10 décembre 2002, aff. C-491/01, *British American Tobacco*, *Rec.*, 2002, p. I-11453.
- CJCE, 9 novembre 2000, aff. C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, *Rec.*, 2000, p. I-9305.
- CJCE, 5 octobre 2000, aff. 376/98, *République Fédérale d'Allemagne c. Parlement et Conseil*, *Rec.*, 2000, p. I-8419.
- CJCE, du 7 mai 1998, aff. C-390/96, *Lease Plan Luxembourg SA contre Belgische Staat*, *Rec.* 1998, p. I-2553.
- CJCE, 15 novembre 1994, Avis 1/94, *Rec.*, 1994, p. I-5267, point 79, p. 5411.
- CJCE, 4 juillet 1985, aff. 168/84, *Gunter Berkholz c. Finanzamt Hamburg-Mitte-Altstadt*, *Rec.*, 1985, p. 2251.
- CEDH, Aff. *Amann v. Switzerland* [GC], no. 27798/95, CEDH 2000-II
- CEDH, Aff. *Rotaru v Romania* [GC], no. 28341/95, CEDH 2000-V
- T.G.I. Paris, ord. réf., 14 avril 2008, disponible sur http://www.legalis.net/jurisprudence-decision.php3?id_article=2311, (Consulté le 8 juillet 2016).

Doctrines

Monographie

- FRANCQ S., *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, Bruylant, 2005.

- KUNER C., *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013.
- KUNER C., *European Data Protection Law Corporate Compliance and Regulation*, Oxford University Press, Oxford, 2007.
- WALRAVE M., *Privacy Gescand? Direct marketing en de bescherming van de persoonlijke levenssfeer*, Leuven, Universitaire Pers Leuven, 1999.

Contribution dans une monographie

- FALLON M. et FRANCO S., « La coopération judiciaire civile et le droit international privé : Vers un droit proprement communautaire des conflits de loi ou de juridiction » in *Une Constitution pour l'Europe : Réflexions sur les transformations du droit de l'Union européenne*, O. DE SCHUTTER et P. NIHOUL (coord.), Bruxelles, Larcier, 2004 p. 239-301.
- FRANCO S., « The external dimension of Rome I and Rome II : neutrality or schizophrenia » in *Private law in the external relation of the EU*, M. CREMONA and H. MICKLITZ (dir.), Oxford, Oxford University Press, 2016, pp. 71-106.
- GALLARDO MESEGUER M., « Aperçu de la dimension internationale du règlement général sur la protection des données à caractère personnel » in *Enjeux européens et mondiaux de la protection des données personnelles*, A. GROSJEAN (dir.), Bruxelles, Bruylant, 2015, pp. 117-159.
- HENROTTE J. et COTON F., « 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 *Enjeux européens et mondiaux de la protection des données personnelles*, A. GROSJEAN (dir.), Bruxelles, Larcier, 2015, pp. 171-188.

Articles

- BERNARD-GLANZ C., « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », *Cahiers de droit européen*, 2014, pp. 685 et s.
- BLOK P., « Privacy-bescherming in alle staten – Internationaal privacy-recht en I.P.R. onder de Europese Privacy-richtlijn », *Computerr.*, 2005, pp. 301 et s.
- BYGRAVE L. A., « Determining Applicable Law pursuant to European Data Protection Legislation », *Computer Law & Security Report*, 2000, volume 16, pp. 252 et s.
- CRUYSMANS E. et STROWEL A., « Un droit à l'oubli face aux moteurs de recherche - droit applicable et responsabilité pour le référencement de données inadéquates non pertinente ou excessives », *Journal des tribunaux*, 2014, pp. 457 et s.
- DE TERWANGNE C., « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », obs. sous CJCE, arrêt du 6 novembre 2003, Bodil Lindqvist, affaire C-101/01, *Revue du droit des technologies de l'information*, 2004, pp. 67 et s.
- DE VERDELHAN H., « Chronique de jurisprudence : Introduction générale », *Revue internationale de droit économique*, 2016, pp. 5 et s.
- FALLON M. et BERGE J., « Marché intérieur et Espace de liberté sécurité justice : la dimension spatiale des espaces », *Les petites affiches*, n°112, 2010, pp.5 et s.

- FAZLIOGLU M., « Forget me not : the clash of the right to be forgotten and freedom of expression on the internet », *International Data Privacy Law*, 2013, Volume 3, pp. 149 et s.
- FRANCO S., « The external dimension of Rome I and Rome II : neutrality or schizophrenia » in *Private law in the external relations of the EU*, M. CREMONA and H. MICKLITZ (dir.), pp. 71 et s.
- GAYREL C. et ROBERT R., « Proposition de règlement sur la protection des données - Premiers commentaires », *Journal de droit européen*, 2012, pp. 173 et s.
- HARDY B., « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *Revue trimestrielle de droit européen*, 2014, pp. 879 et s.
- HAVELANGE B. et LACOSTE A., « Les flux transfrontaliers de données à caractère personnel en droit européen », *Journal des tribunaux*, 2012, pp. 241 et s.
- KOKOTT J. & SOBOTTA C., « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *International Data Privacy Law*, 2013, Volume 3, pp. 222 et s.
- KOOPS B., « The trouble with European data protection law », *International Data Privacy Law*, 2014, Volume 4, pp. 250 et s.
- KOTSCHY W., « The proposals for a new General Data Protection Regulation problem solved », *International Data Privacy Law*, 2014, Volume 4, pp. 274 et s.
- KUNER C., « Google Spain in the EU and international context », *Maastricht Journal of European and Comparative Law*, 2015, pp. 158 et s.
- KUNER C., « The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges », *LSE Law, Society, and Economy Working Paper Series. ed. London : London School of Economics and Political Science*, n°3, 2015, pp. 1 et s.
- KUNER C., CATE F., MILLARD C. et SVANTESSON D., « Editorial : The extraterritoriality of data privacy laws—an explosive issue yet to detonate », *International Data Privacy Law*, 2013, Vol. 3, No. 3, pp. 147 et s.
- MARINO L., « Un 'droit à l'oubli' numérique consacré par la CJUE », *La semaine juridique*, pp. 1300 et s.
- MOEREL L., « 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, Volume 1, pp. 28 et s.
- MOEREL L., « Back to basics: when does EU data protection law apply », *International Data Privacy Law*, 2011, Vol. 1, No. 2, pp. 92 et s.
- MOINY J., « Facebook au regard des règles européennes concernant la protection des données », *Revue européenne de droit de la consommation*, 2010, pp. 235 et s.
- REDING V., « The European data protection framework for the twenty-first century », *International Data Privacy Law*, 2012, Volume 2, pp. 119 et s.
- REDING V., « The upcoming data protection reform for the European Union », *International Data Privacy Law*, 2011, Volume 1, pp. 3 et s.
- SVANTESSON D., « The extraterritoriality of EU data privacy law : Its theoretical justification and its practical effect on U.S. businesses », *Stanford Journal of International Law's*, 2014, pp. 53 et s.
- TAYLOR M., « The EU's human rights obligations in relation to its data protection laws with extraterritorial effect », *International Data Privacy Law*, 2015, Volume 5, pp. 246 et s.
- TENE O., « Privacy : The new generations », *International Data Privacy Law*, 2011, Volume 1, p. 15 et s.
- WARREN S. D. and LBRANDEIS L. D., « The Right to Privacy », *Harvard Law Review*, 1890, Volume 4, pp. 193 et s.

Divers

Avis du Groupe de Travail « Article 29 »

- Opinion 01/2012 of the « Article 29 » Data Protection Working Party on the data protection reform proposals (WP 191), adopted on 23 March 2012, p. 5.- Avis 8/2010 du Groupe de Travail « Article 29 » sur le droit applicable (WP 179), adopté le 16 décembre 2010.
- Avis 1/2008 du Groupe de Travail « Article 29 » sur les aspects de la protection des données liés aux moteurs de recherche (WP 148), adopté le 4 avril 2008.
- Avis du Groupe de Travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE (WP 56), adopté le 30 mai 2002.

Communications

- Communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions concernant – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM(2010) 609 final, p. 4.

Autres

- Commission, «Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)», 15 mai 2003, COM. (265) final, p. 9 et s.
- Les conditions de service de Facebook consultable à l'adresse suivante https://m.facebook.com/terms/?locale2=fr_FR (consulté le 16 juillet 2016).
- W. Roush, « 'Web 2.0' has arrived », *MIT Technology Review*, 2005, <https://www.technologyreview.com/s/404799/web-20-has-arrived/> (consulté le 29 juin 2016).
- La liste des bureaux de Google en Europe, <https://www.google.fr/about/company/facts/locations/> (consulté le 3 juillet 2016).

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique www.uclouvain.be/drt

