

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Facebook au regard des règles européennes concernant la protection des données

Moïny, Jean-Philippe

Published in:

Revue Européenne de Droit de la Consommation

Publication date:

2010

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Moïny, J-P 2010, 'Facebook au regard des règles européennes concernant la protection des données', *Revue Européenne de Droit de la Consommation*, numéro 2, pp. 235-271.

General rights

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

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

Take down policy

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

Facebook au regard des règles européennes concernant la protection des données

JEAN-PHILIPPE MOINY¹

Introduction

Facebook² permet d'éprouver les limites d'application territoriale des règles européennes de protection des données³. Il conduit même, à certains égards, à mettre ces règles en cause, tant sa nature est spécifique. Ainsi, on s'interrogera, dans le présent article, sur le droit applicable à la société Facebook en matière de protection des données (III). Dans cette matière, c'est en principe aux responsables de traitements qu'incombe le respect des obligations. C'est aussi à l'égard de ces responsables que se pose la question de l'extraterritorialité. Pour Facebook, on devra identifier ces responsables de traitements (II). Mais avant tout, nous devons nous interroger sur le phénomène lui-même : qu'est-ce que Facebook (I)?

¹ L'auteur est aspirant du Fonds national de la recherche scientifique (F.R.S.-F.N.R.S.), Belgique. Ses recherches sont localisées au Centre de recherche informatique et droit (C.R.I.D.), Faculté universitaires Notre-Dame de la Paix, Namur, Belgique. L'auteur remercie Cécile de Terwangne, Yves Pouillet et Jean Herveg pour leurs relectures et commentaires, ainsi que Bertel De Groote pour ses judicieux conseils. Les commentaires peuvent être adressés à : jean-philippe.moiny@fundp.ac.be.

² Sauf mention contraire, d'un point de vue factuel, l'étude est à jour au 1^{er} octobre 2009. Elle a dû être rendue en version définitive le 15 novembre 2009. Relevons que la politique de confidentialité du site a été récemment modifiée, notamment en raison d'une plainte antérieurement déposée auprès du Commissariat à la protection de la vie privée du Canada, voy. E. DENHAM, «Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la loi sur la protection des renseignements personnels et les documents électroniques», 16 juillet 2009, disponible sur http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm.

³ Principalement la directive (CE) n° 95/46 du Parlement 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 («directive 95/46»), *J.O. L 281*, du 23 novembre 1995.

I. – Présentation de Facebook

A. – UN RÉSEAU SOCIAL

1. – Facebook «*can be defined as [a] website whose main purpose is to act as a connector among users*»⁴, via lequel les utilisateurs échangent tous types d'informations, à partir de profils⁵ personnalisés. Il permet à cette fin de définir des relations sociales en déterminant qui peut accéder à ces informations, communiquer avec qui et comment⁶. Il peut en outre être regardé comme un «réseau de réseaux sociaux»⁷ dès lors que de multiples contextes (le sport, l'université, le travail, la musique, la sexualité, etc.) y coexistent et s'y entrecroisent via le profil voulu unique de l'utilisateur.

2. – Le fournisseur du réseau social héberge et gère ces profils, ce que les utilisateurs y déposent. Parfois des applications peuvent y être ajoutées⁸ ou encore des liens conduisant à divers sites Web, etc. Il s'agit là de sa première activité : le stockage de diverses informations et la mise à disposition de celles-ci aux autres membres du site⁹, selon des règles définies en partie par les utilisateurs mais aussi par Facebook. Toutes ces possibilités constituent des services à distance, plus particulièrement des services de communication et de gestion des profils au-delà du simple hébergement. Ces services sont prestés à la demande des utilisateurs dont les inscriptions sont totalement volontaires, et par voie électronique, via Internet.

B. – UNE ENTREPRISE

3. – Il n'y a là rien de bien original dans le secteur d'activités des réseaux sociaux : Facebook est également une société américaine établie en Californie (Palo Alto), comme

⁴ A. LEVIN et P. SANCHEZ ABRIL, «Two Notions of Privacy Online», *Vanderbilt J. of Ent. And Tech. Law*, 2009, p. 1017.

⁵ La notion est en l'espèce duale. Il existe, d'une part, un profil que complète l'utilisateur avec les informations qu'il place volontairement sur la page du site Facebook lui étant dédiée. Et d'autre part, ce profil est aussi augmenté d'autres informations collectées par la société Facebook et enregistrées dans ses bases de données, mais auxquelles l'utilisateur n'a en principe pas accès. Il est en principe renvoyé à la première acception.

⁶ European Network and Information Security Agency, G. HOGBEN (éd.), «Position Paper N° 1 – Security Issues and Recommendations for Online Social Networks» («ENISA Position Paper»), octobre 2007, p. 5, disponible sur <http://www.enisa.europa.eu>.

⁷ Sur le concept de réseau social, voy. notamment D.M. BOYD et N.B. ELLISON, «Social Network Sites : Definition, History, and Scholarship», octobre 2007, disponible sur <http://www.danah.org/papers/>, p. 2. Voy. aussi Groupe de travail «article 29», «Opinion 5/2009 on online social networking» («W.P. 163»), 12 juin 2009, pp. 4-5.

⁸ Facebook n'héberge en principe que les applications qu'elle développe.

⁹ Quant aux caractéristiques communes des réseaux sociaux, voy. «ENISA Position Paper», *op. cit.*, p. 5.

YouTube, SecondLife, DailyMotion, Twitter, MySpace, etc.¹⁰. Cette société «possède»¹¹ aussi plusieurs *offices* (bureaux) dont des «International offices : Dublin, Ireland; London; Paris»¹². Il semble également que Facebook dispose de bureaux en Italie et en Suède¹³. Les rôles de ces «bureaux européens» peuvent utilement être évoqués (1) en raison de leurs incidences en matière de droit international privé, tant quant à la protection des données¹⁴, que quant aux contrats conclus par les consommateurs. Au sujet de ces derniers, la direction des activités de Facebook vers le territoire communautaire importe (2).

1. – Une société américaine disposant d'offices européens

4. – Les divers bureaux sont à évoquer. Celui de Londres a pour rôle – selon Facebook – de «*help support the growing advertising needs*» du marché que représente le *UK network*. Ce qui pourrait consister à servir d'intermédiaire aux partenaires commerciaux de Facebook désireux d'exploiter la fonctionnalité *ads* en achetant des *targeted ads* adressées à ce réseau géographique ou à partir du Royaume-Uni. Cet office pourrait être directement impliqué dans la vente de publicités ciblant des résidents du territoire communautaire; la fonction de conseil que Facebook offre via la page «*Integrated Solutions : Contact Us*»¹⁵, par laquelle, sur requête, celle-ci entend aider à la réalisation de la «solution idéale de publicité via Facebook»¹⁶, ne lui incomberait-elle pas?

5. – Le bureau de Paris semble se situer dans la même optique¹⁷. Il est question de «... *building a sales team in Paris in recognition of the increasing desire by companies in France and nearby countries to make advertising on Facebook a part of their growth strategy*» a affirmé B. Chandlee, le directeur commercial de Facebook pour l'Europe¹⁸. Les bureaux italien et suédois semblent également affectés à des activités similaires.

¹⁰ Facebook est toutefois «a Delaware corporation», voy. le récent jugement rendu par défaut contre le célèbre *spammer* Sanford Wallace, U.S. District Court for the Northern District of California, 29 octobre 2009, *Facebook Inc. v. Sanford Wallace et al.*, disponible sur <http://www.scribd.com/doc/21922447/Facebook-Spam-Lawsuit-Decision-Sanford-Wallace>.

¹¹ Lors de la recherche ayant conduit à la présente étude, la forme juridique de ces bureaux n'a pas été identifiée.

¹² Voy. <http://www.facebook.com/facebook?ref=pf#/press/info.php?factsheet>.

¹³ Voy. <http://www.insidefacebook.com/2009/10/20/in-depth-discussing-facebooks-advertising-future-with-vp-of-global-sales-mike-murphy/>.

¹⁴ Question analysée plus en profondeur ultérieurement, voy. *infra* n^{os} 48 et s.

¹⁵ Voy. <http://www.facebook.com/advertising/?src=pf#/business/contact.php>.

¹⁶ «*We can help you develop the ideal Facebook advertising solution. To determine the most relevant opportunities for you, please click below, and a Facebook sales representative will be in contact with you within two business days. We look forward to working with you...*», <http://www.facebook.com/business/contact.php>.

¹⁷ Voy. <http://www.paidcontent.org/entry/419-facebook-opens-paris-sales-office-as-part-of-european-expansion/>. Voy. aussi <http://www.zdnet.fr/actualites/internet/0,39020774,39383999,00.htm>.

¹⁸ Voy. <http://www.insidefacebook.com/2008/12/10/>.

6. – Enfin, le rôle de l'office de Dublin serait plus important. Selon Facebook : «Dublin will be the centre for Facebook's international operations and will provide a range of online technical, sales and operations support to Facebook's users and customers across Europe, the Middle East and Africa». ... Facebook Chief Operating Officer Sheryl Sandberg explained, '[...] Ireland was the best place to establish our new headquarters. As we grow and strive to make Facebook into a place for people around the world to connect and share information, we need local operations to better advance our efforts. The talent pool in Dublin is world-class and recruiting local talent will help us better understand the needs of local users and the regional dynamics that, in turn, can give us better insight into what features matter most'¹⁹. Ces «quartiers généraux» – «siège social international»²⁰ de l'entreprise – consolident la présence de Facebook sur le territoire européen, mais *quid* de leurs activités ?

2. – Une société américaine dirigeant ses activités vers le marché mondial

7. – Ces offices sont autant d'indices incontestables d'une stratégie commerciale dirigée, notamment, vers le territoire communautaire. Et ils ne sont pas les seules traces de cette intention : l'architecture du réseau Facebook en est – ou plus exactement, en fut – une autre de taille. En effet, le réseau social était jusqu'il y a peu notamment subdivisé en réseaux géographiques (*Region*) relatifs à des pays ou à des villes²¹, antérieurement définissables comme *primary network*, c'est-à-dire le réseau avec lequel l'utilisateur a le plus d'affinités²². Notons que cette suppression des réseaux géographiques devrait traduire une volonté de faciliter les échanges entre les utilisateurs, plutôt qu'être le signe d'un hypothétique «recul» dans la stratégie commerciale du site déjà fort bien installé sur le marché communautaire²³. Le site est d'ailleurs en outre traduit en septante langues (chinois, français, etc.). Et «*anyone can join*»; à une excep-

¹⁹ Voy. <http://www.facebook.com/press/releases.php?p=59042>.

²⁰ Commission à la protection de la vie privée du Canada, recherche effectuée par J. BARRIGAR, «La vie privée sur les sites de réseau social – Analyse comparative de six sites», février 2009, disponible sur http://www.priv.gc.ca/information/pub/sub_comp_200901_f.pdf.

²¹ Il existe aussi des réseaux relatifs à des universités, des écoles et des lieux de travail.

²² Si les réseaux géographiques n'existent désormais plus (octobre 2009), il existe toujours des réseaux relatifs à des universités, des écoles et des lieux de travail. En outre, les utilisateurs peuvent toujours préciser une situation géographique dans leurs informations de contact. Et par ailleurs, Facebook identifie la localisation des utilisateurs via leurs adresses IP dès lors que c'est par ce moyen que sont permises les publicités ciblées en fonction des pays. Par conséquent, la conscience des provenances géographiques des utilisateurs est loin d'avoir disparu.

²³ Dans le sens de l'expansion des activités du site, voy. <http://www.insidefacebook.com/2009/10/12/facebook-hiring-to-expand-european-advertising-presence/>. La suppression de ces réseaux serait notamment motivée par une amélioration de la clarté du fonctionnement des paramètres de confidentialité, voy. <http://blog.facebook.com/blog.php?post=91242982130>.

tion près²⁴ – à notre connaissance –, la société Facebook ne manifeste nulle part son souhait de restreindre sa clientèle à quelque pays que ce soit, au contraire. Enfin, *ads* permet de cibler les publicités selon les pays.

Cette volonté de diriger ses activités vers le monde²⁵ n'est pas sans incidence en droit international privé. Ainsi, en matières civile et commerciale, à l'occasion de contrats conclus par les consommateurs, quant à la compétence internationale d'une part²⁶, un tel comportement est susceptible de fonder la compétence du juge de l'État d'une personne domiciliée dans un État de la Communauté dans la mesure où cet État est ciblé²⁷. Et quant au droit applicable²⁸ d'autre part, cela pourrait entraîner l'application du droit de ce même État s'il est celui de la résidence habituelle de la personne en cause. Autrement dit, le critère de direction des activités²⁹ consacré dans les règlements Bruxelles I et Rome I pourrait être rencontré et permettre une certaine protection de l'utilisateur du réseau social. Toutefois, encore faudrait-il à cet égard que ces instruments de droit communautaire puissent s'appliquer³⁰ et que les conditions requises par leurs dispositions protectrices des consommateurs soient également rencontrées^{31 32}.

²⁴ Le Statement of Rights stipule que : «You will not use Facebook if you are located in a country embargoed by the U.S., or are on the U.S. Treasury Department's list of Specially Designated Nationals».

²⁵ «Actuellement, plus de 70% des utilisateurs de Facebook sont à l'extérieur des États-Unis», J. BARRIGAR, «La vie privée sur les sites de réseau social – Analyse comparative de six sites», recherche préparée pour le Commissariat à la protection de la vie privée du Canada, disponible sur http://www.priv.gc.ca/information/pub/sub_comp_200901_f.cfm, p. 9. Le fournisseur du réseau social pourrait limiter la clientèle vers laquelle il dirige ses activités. D'ailleurs «à l'époque, MySpace ne permettait pas aux utilisateurs situés à l'extérieur des États-Unis de s'inscrire. On les filtrait à partir de leur adresse IP », J. BARRIGAR, *op. cit.*, p. 16.

²⁶ Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *J.O. L 12*, du 16 janvier 2001, ci-après «règlement Bruxelles I».

²⁷ Voy. article 15 du règlement «Bruxelles I».

²⁸ Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008, sur la loi applicable aux obligations contractuelles («règlement Rome I»), *J.O. L 177*, du 4 juillet 2008. Il remplace la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles, *J.O. L 266*, du 9 octobre 1980. Voy. article 24, § 1^{er}, du règlement Rome I et article 6 du règlement Rome I quant aux contrats conclus par les consommateurs.

²⁹ Au sujet des règles de droit international privé évoquées, voy. J.-P. MOINY et B. DE GROOTE, «'Cyberconsommation' et droit international privé », *R.D.T.I.*, 2009, pp. 5 et s. En particulier au sujet de la direction des activités, voy. pp. 29-35.

³⁰ Quant à la compétence internationale, le cas Facebook ne satisfait en principe pas à la condition de rattachement communautaire requise par l'article 4 du règlement Bruxelles I à laquelle l'article 15 ne dérogerait qu'en ce qui concerne les *offices* de Facebook, et seulement quant aux litiges concernant leurs activités, voy. article 15, § 2, du règlement Bruxelles I. En matière de droit applicable, le règlement Rome I présente par contre, comme la Convention de Rome, un caractère universel, voy. article 2 du règlement Rome I.

³¹ Comme par exemple l'exigence d'un contrat conclu entre un consommateur et un professionnel.

³² Voy. J.-P. MOINY et B. DE GROOTE, *op. cit.*

C. – DES SERVICES DE LA SOCIÉTÉ DE L'INFORMATION

8. – Les caractéristiques des services offerts par Facebook³³ correspondent aux éléments constitutifs d'un «service de la société de l'information»³⁴. En particulier, l'activité de Facebook doit être prestée «normalement contre rémunération». Il suffit à cet égard qu'elle constitue une «activité économique», peu importe qu'elle soit ou non rémunérée directement par le destinataire du service³⁵. Or, comme le dit la doctrine : «OSNs are usually for-profit businesses»³⁶. En l'espèce, les bannières publicitaires et la fonctionnalité de publicité ciblée *ads* (ainsi que ses variantes *Social Ads* et, plus récemment, *Engagement Ads*)³⁷ – payante, offerte via Facebook et greffée sur le réseau social – permettent à la société Facebook d'obtenir une contrepartie économique. Toute entreprise peut ainsi réaliser des publicités ciblées, selon ses choix opérés à partir d'un panel de critères définis par Facebook, à diffuser aux utilisateurs du réseau³⁹. La fonctionnalité *Polls*, permettant d'effectuer des sondages au travers du réseau social, est également payante. Enfin, en utilisant Facebook, les utilisateurs concèdent à cette dernière une licence lui permettant d'exploiter commercialement

³³ Voy. *supra*, n° 2.

³⁴ «[T]out service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services», article 1^{er}, 2), a) de la directive (CE) n° 98/48 du Parlement européen et du Conseil du 20 juillet 1998, portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, *J.O. L 217*, du 5 août 1998. Voy. aussi articles 2, a) et 14, de la directive (CE) n° 2000/31 du Parlement européen et du Conseil du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive 2000/31), *J.O. L 178*, du 17 juillet 2000.

³⁵ Voy. le considérant n° 18 de la directive 2000/31.

³⁶ A. LEVIN et P. SANCHEZ ABRIL, *op. cit.*, p. 1019. «La publicité est un élément clé du modèle opérationnel de la plupart des SRS», J. BARRIGAR, *op. cit.*, p. 44.

³⁷ Voy. à ce sujet <http://www.facebook.com/advertising/?src=awgl01&v=ntl1>, <http://www.insidefacebook.com/2008/10/30/facebook-advertising-resources-the-6-types-of-ads-on-the-new-home-page/>; <http://www.insidefacebook.com/2009/01/27/facebook-relaunches-polls-as-new-home-page-engagement-ad/>, <http://www.insidefacebook.com/2009/09/23/facebook-new-sampling-engagement-ads-now-available-for-brands/>.

³⁸ Citons également *Insights*, permettant d'évaluer l'efficacité des publicités ciblées commandées, et l'application *Gifts* permettant d'envoyer des «cadeaux» (payants – 1\$ pièce) à ses «amis».

³⁹ L'âge, le pays, des mots clés, les institutions scolaires fréquentées par l'utilisateur ou les utilisateurs qui sont «fans» de certaines *Facebook Pages*, voy. <http://www.facebook.com/help.php?page=863>. Une fois sélectionnés par le commanditaire d'une publicité, ils sont ensuite identifiés par Facebook dans des champs spécifiques des profils afin de déterminer si doit y être affichée la publicité commandée.

les contenus mis à disposition sur le site et protégés par la propriété intellectuelle⁴⁰. Ce qui pourrait aussi constituer une contrepartie à son activité.

D. — DES SERVICES « À CARACTÈRE PERSONNEL »

9. — Un service de la société de l'information tel que Facebook est ce que l'on pourrait appeler un service « à caractère personnel ». Cela signifie que, d'une part, des données à caractère personnel en sont une composante; que ces données sont constamment traitées; et que ces données et leur traitement sont un élément essentiel de l'objet du service offert ainsi que, partant, du contrat conclu avec l'utilisateur⁴¹. En d'autres termes, l'économie de ce contrat se résume dans le consentement à l'exploitation commerciale – au sens large – de données à caractère personnel en échange du service offert.

1. — *Des données à caractère personnel*

10. — Dans l'environnement de Facebook, quantités d'informations « concernant une personne physique identifiée ou identifiable »⁴² sont présentes. Tout d'abord, l'utilisateur est contractuellement – si du moins un contrat existe et valablement⁴³ – obligé de fournir des informations réelles à son sujet; il doit s'identifier et n'utiliser qu'un unique compte⁴⁴.

Ensuite, quand bien même ne le devrait-il pas contractuellement, il est dans son intérêt, pour trouver ses – ou des – « amis » sur Facebook, de se présenter d'une façon permettant son identification; « *[p]osting truthful information is consistent with an intent to socialize* »⁴⁵.

⁴⁰ Ainsi, « *you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ('IP License')* », stipule notamment le *Statement of Rights and Responsibilities* – anciennement Terms of Use –, autrement dit, les conditions d'utilisation du site ou le contrat censé conclu avec Facebook, voy. *infra*, n^{os} 16 et s.

⁴¹ Voy. *infra*, n^{os} 16 et s.

⁴² C'est-à-dire de données à caractère personnel, article 2, a) de la directive 95/46.

⁴³ Voy. *infra*, n^{os} 16 et s. Faute de place, ces questions ne sont pas approfondies.

⁴⁴ À l'occasion de son inscription sur Facebook, ses nom, prénom et date de naissance sont en effet requis. Et selon le Statement of Rights : « *Facebook users provide their real names and information, and we need your help to keep it that way* », « *You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission* ». Par ailleurs, « *You will keep your contact information accurate and up-to-date* ».

⁴⁵ A. LEVIN et P. SANCHEZ ABRIL, *op. cit.*, p. 1025. Voy. aussi les statistiques évoquées par les auteurs.

Et de surcroît, même si un utilisateur désire demeurer anonyme⁴⁶, de nombreux «identifiants»⁴⁷ contribuent généralement à le rendre identifiable. Il s'agit, d'une part, de son comportement au travers du réseau social, des informations – telles que les photos – qu'il y communique et produit – enregistrées par Facebook⁴⁸ – voire encore de données provenant d'autres sites Web⁴⁹ ou des profils d'autres membres du réseau. Ces informations sont en effet susceptibles de révéler diverses facettes de son identité⁵⁰. Et d'autre part, les cookies placés sur son terminal⁵¹ ainsi que l'enregistrement systématique de son adresse IP⁵², par Facebook⁵³, contribuent aussi à son identification, soit indépendamment les uns des autres, soit par leur jeu combiné, soit encore par leur interconnexion à tout ou partie des informations précitées. Bref, ces données se croisent et permettent d'établir le «profil» de l'utilisateur, espace personnalisé et individualisé du réseau social à partir duquel il est identifiable.

11. – Notons enfin que de nombreuses données concernant des tiers au réseau social Facebook se retrouvent également dans ce dernier. Ceux-ci peuvent alors y être identifiés ou identifiables, le cas échéant, sans même en avoir connaissance.

2. – Des traitements

12. – Les informations susmentionnées sont en permanence l'objet de traitements⁵⁴. Elles sont enregistrées et organisées sur les serveurs de Facebook, diffusées

⁴⁶ Ce à quoi il peut légitimement aspirer sur l'Internet. Voy. notamment en ce sens la déclaration sur la liberté de la communication sur l'Internet, adoptée par le comité des ministres du Conseil de l'Europe, le 28 mai 2003, principe 7, disponible sur <https://wcd.coe.int/>.

⁴⁷ Ce terme est repris au groupe de travail «article 29», voy. Groupe de travail «article 29», «Avis 4/2007 sur le concept de données à caractère personnel» («W.P. 136»), 20 juin 2007, p. 15.

⁴⁸ La politique de confidentialité (*privacy policy*) du site (au 28 juillet 2009) révèle que «*When you visit Facebook you provide us with two types of information : personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site*».

⁴⁹ Selon la politique de confidentialité : «*Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags)*».

⁵⁰ Voy. article 2, a), *in fine* de la directive 95/46.

⁵¹ Au sujet des adresses IP, des *cookies* et de leurs effets combinés, voy. Groupe de travail «article 29», «Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche» («W.P. 148»), 4 avril 2008. Au sujet des *cookies* et de leurs conséquences quant au droit applicable, voy. *infra* n° 59.

⁵² L'adresse IP peut souvent être considérée comme une donnée à caractère personnel, voy. W.P. 136, p. 18.

⁵³ Selon la politique de confidentialité : «*When you enter Facebook, we collect your browser type and IP address. [...] In addition, we store certain information from your browser using 'cookies'*».

⁵⁴ Voy. article 2, b), de la directive 95/46.

aux autres utilisateurs du réseau – voire à des tiers⁵⁵ – extraites de la *Platform* par des applications et leurs développeurs, consultées à des fins de publicité ciblée, exportées vers d'autres sites Web⁵⁶, etc., dans les limites des choix réalisés par les utilisateurs au travers des paramètres de confidentialité – *privacy settings*⁵⁷ – conçus et offerts par Facebook. Et ces traitements sont automatisés, dès lors qu'ils sont toujours réalisés au moyen du site Facebook⁵⁸.

E. – QUI UTILISE FACEBOOK ?

13. – Les utilisateurs de base du réseau social – qui ne sont ni développeurs d'applications, ni commanditaires d'une publicité, ni administrateurs d'une Facebook Page⁵⁹ – peuvent *a priori* être vus de façon binaire : ils sont amis ou ne le sont pas. Or concrètement, cela ne change rien. En effet, un ami sur Facebook peut appartenir à des contextes totalement différents : il peut être membre de ma famille, collègue de travail, membre d'un même club de tennis, inconnu, etc. La notion d'«ami» est donc très relative «*nebulous at best*»⁶⁰, si elle n'est pas subvertie.

Ces réalités de «*misleading notion[s] of 'community'*» et de «*friends*»⁶¹ ont déjà été soulignées ; «*OSNs have loosened traditional notions of intimacy and friendship and their respective nomenclature*»⁶². Être un contact (un «ami» selon Facebook) a une signification ambiguë : les liens entre contacts seront ainsi tantôt forts (*strong ties*) et tantôt faibles (*weak ties*), mais nécessaires au *networking*⁶³. En synthèse, «*[a] 'friend' on Facebook is anyone who has given you permission to join their online network of 'friends', whether or not they*

⁵⁵ Tel est par exemple le cas de l'existence d'un profil qui apparaît aux yeux de tous lorsque ce dernier est indexé dans les moteurs de recherche, ce que l'utilisateur peut empêcher. La politique de confidentialité prévoit par ailleurs d'autres hypothèses de divulgation des informations à des tiers, notamment pour des raisons de défense des intérêts de Facebook.

⁵⁶ Par exemple à l'occasion du fonctionnement de Facebook Connect qui permet à un utilisateur de se connecter à un site partenaire de Facebook avec son *login* Facebook et d'y retrouver ses «amis».

⁵⁷ C'est-à-dire les paramètres d'accessibilité à l'information qu'il diffuse via son profil Facebook. Les limites des choix posés par l'utilisateur (quelles données sont accessibles à qui) sont déterminées par Facebook. Par exemple, l'utilisateur peut restreindre l'accès à son *Wall* à un groupe d'amis (liste préalablement défini, etc. Il faut encore évoquer les Application settings concernant les applications et la Facebook Platform (voy. *infra*, n° 14).

⁵⁸ Voy. en ce sens C.J.C.E., 6 novembre 2003, *Procédure pénale c. Bodil Lindqvist*, (Lindqvist), C-101/01, *Rec.*, 2003, p. I-12971, point 26.

⁵⁹ Voy. *infra*, n°s 14-15.

⁶⁰ B. KANE and B.T. DELANGE, « A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant », *Idaho L. Rev.*, 2009, p. 319.

⁶¹ Voy. International Working Group on Data Protection in Telecommunications, «Report and Guidance on Privacy in Social Network Services – Rome memorandum», Rome, 3-4 mars 2008, disponible sur <http://www.datenschutz-berlin.de/>, p. 2.

⁶² A. LEVIN et P. SANCHEZ ABRIL, *op. cit.*, p. 1018.

⁶³ J. GRIMMELMANN, « Saving Facebook », *Iowa L. Rev.*, 2009, p. 1175.

have ever met you»⁶⁴. Quitte à concéder à des étrangers l'accès à une part de notre vie privée alors qu'ils ne lui prêteront peut-être aucun égard, voire vous diffameront ou, à l'extrême, se livreront à un *identity theft* auquel peut contribuer un réseau social⁶⁵.

Par conséquent, la relation mise en place dans le cadre d'un tel réseau n'est pas nécessairement liée à un contexte d'amitié mais bien, comme cela a été évoqué, à une multitude de contextes s'entrecoupant. Ce qui est susceptible de multiplier les ruptures d'«intégrité contextuelle»⁶⁶. D'autant plus que les utilisateurs ne se limitent pas à ces «amis».

14. – Facebook rassemble en effet encore d'autres types d'utilisateurs, comme les développeurs d'applications, c'est-à-dire de programmes très divers⁶⁷ que les utilisateurs greffent à leur profil. N'importe qui ayant ouvert un compte développeur peut programmer des applications capables d'utiliser et d'extraire des données relatives aux membres du réseau social, à partir de la Facebook Platform⁶⁸, et de bénéficier des droits d'accès de ces membres dans les profils de leurs «amis», si ces derniers ne veillent pas à endiguer cette possibilité.

15. – Enfin, certains utilisateurs de Facebook sont engagés dans une activité commerciale. Il s'agit notamment des entreprises commandant des publicités ciblées via *ads*, ou encore gérant des *Page* permettant d'interagir avec les autres membres du

⁶⁴ J.D. LIPTON, «'We, the Paparazzi' : Developing a Privacy Paradigm for Digital Video», 2009 (à paraître dans la *Iowa Law Review*), disponible sur <http://www.ssrn.com>, pp. 17-18.

⁶⁵ V.R. WONG, «Social Networking : Anybody is a Data Controller!», octobre 2008, disponible sur <http://papers.ssrn.com/>, p. 3. Voy. aussi «ENISA Position Paper», pp. 12-14; «Resolution on Privacy Protection in Social Network Services», 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 17 octobre 2008, disponible sur <http://www.edps.europa.eu/>, dernièrement consulté le 3 avril 2009.

⁶⁶ V.H. NISSENBAUM, «Privacy as Contextual Integrity», *Washington L. Rev.*, vol. 79, 2004, pp. 119-157. Selon l'auteure, lorsqu'une information est produite, elle l'est dans un contexte auquel sont associées des *informational norms*, à savoir : des règles d'opportunité (*norms of appropriateness*) et de diffusion de ces informations (*norms of flow or distribution*). Si, ultérieurement, ces règles ne sont pas respectées par les parties en cause, il y a alors une violation de la *privacy*, indépendamment de la question de savoir si celle-ci est justifiée ou pas. Par exemple, dans le contexte de l'«amitié» – textuellement visé sur Facebook (*friends*) mais concrètement dénaturé – l'auteure explique que les règles d'opportunité sont assez lâches – on se dit beaucoup de choses – tandis que les règles de diffusion sont beaucoup plus strictes – mais cela doit rester entre nous. Pour une application de cette théorie dans le contexte de Facebook, voy. F. DUMORTIER, «Facebook and risks of de-contextualization of information», 2009, disponible sur http://works.bepress.com/franck_dumortier/1.

⁶⁷ Il existe actuellement plus de 350 000 applications de toutes sortes accessibles via Facebook (<http://www.facebook.com/press/info.php?statistics>). Une application peut servir de calendrier permettant d'être averti le jour de l'anniversaire de ses «amis», fournir un jeu incorporé au profil et, le cas échéant, permettre d'interagir avec les autres utilisateurs, de savoir qui visite son profil, etc.

⁶⁸ Facebook offre la possibilité de paramétrer, dans une certaine mesure, le partage d'information au travers de cette plate-forme via les Application settings et les privacy settings.

réseau, et ouvrant un *business account*. Ces utilisateurs peuvent ainsi combiner les fonctionnalités «amicales» et commerciales de Facebook.

F. — FACEBOOK ET SES UTILISATEURS : DES COCONTRACTANTS

16. — Les utilisateurs et Facebook semblent conclure un contrat⁶⁹ dont les termes sont dictés unilatéralement par Facebook : «*By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy*», lit l'internaute lorsqu'il s'inscrit. Et «*By using or accessing Facebook*», selon le Statement of Rights, vous acceptez ce dernier⁷⁰. Pour déterminer si un contrat existe, il faut se référer au droit qui serait applicable au cas où ce contrat serait formé⁷¹. C'est, en principe, le droit choisi par les parties ou l'une des parties et «imposé» à l'autre ; le droit californien dans le cas de Facebook. Bien que ce principe connaisse certaines exceptions, en particulier en matière de contrats conclus par les consommateurs – exception susceptible de s'appliquer en l'espèce⁷².

17. — En droit californien, un contrat a déjà été jugé valablement conclu avec les fournisseurs de réseaux sociaux SecondLife⁷³ et MySpace⁷⁴. Cette question conduit à la problématique des «*wrap*» *agreements*, plus précisément des «*clickwrap*» ou «*browsewrap*» *agreements*. Les «*clickwrap*» *agreements* sont des accords formés par le clic de l'internaute sur un bouton prévu à cet effet et manifestant son consentement – «j'accepte» – après, généralement, avoir eu la possibilité de consulter le contenu de l'engagement proposé. Les «*browsewrap*» *agreements*, à la différence⁷⁵, se concluraient

⁶⁹ Voy. en détail, au sujet de la formation du contrat dans le contexte des réseaux sociaux, en droit belge et en droit américain, J.-P. MOINY, «Contracter dans les réseaux sociaux : un geste adéquat pour contracter sa vie privée?», à paraître dans la *Rev. Dr. ULg*, 2010.

⁷⁰ Ce contenu peut varier. Par exemple, il y a des *terms* additionnels pour les développeurs d'applications, etc.

⁷¹ Voy. article 10, § 1^{er}, du règlement «Rome I».

⁷² Voy. *supra*, n° 7 quant aux contrats conclus par les consommateurs. Pour d'autres limites au choix de loi des parties, voy. notamment articles 9, 10, §2, et 3, §§3 et 4, du règlement Rome I.

⁷³ Voy. U.S. District Court for the Eastern District of Pennsylvania, 30 mai 2007, *Marc Bragg v. Linden Research, Inc., and Philip Rosedale*, disponible sur <http://www.paed.uscourts.gov/>.

⁷⁴ Voy. U.S. District Court for the Central District of California, 28 août 2009 (*United States of America v. Lori Drew*) («*U.S.A. v. Drew*»), disponible sur <http://volokh.com/files/LoriDrew.pdf>, où le juge Wu reconnaît de manière générale, en *obiter dictum*, la validité des «*clickwrap*» et «*browsewrap*» *agreements*.

⁷⁵ Voy. notamment les affaires suivantes : U.S. Court of Appeals for the Second Circuit, 1^{er} octobre 2002, *Christopher Specht, et al. v. Netscape Communications Corporation and America Online, Inc., (Specht v. Netscape)*; U.S. District Court for the Eastern District of Pennsylvania, 28 mars 2007, *Lawrence Feldman v. Google, Inc.* ; U.S. District Court for the Northern District of California, 30 août 2002, *Craig Comb and Roberta Toher, Jeffrey Resnick, v. Paypal, Inc.* ; et U.S. District Court for the Northern District of Ohio, 22 août 2007, *John Doe v. SexSearch.com, et al.* Ces affaires sont disponibles sur <http://www.internetlibrary.com/>. En doctrine, voy. notamment C.L. KUNZ, H. THAYER, M.F. DEL DUCA et J. DEBROW, «Click-Through agreements : Strategies for Avoiding Disputes on Validity of Assent», disponible sur <http://www.steptoe.com/assets/attachments/2353.pdf>; L.E. TRAKMAN, «Adhesion Contracts and the Twenty First Century Consumer», 2007, disponible sur <http://www.ssrn.com>, pp. 54-55.

par la simple utilisation du site Web en question, sans qu'il soit requis de cliquer sur un bouton particulier (ou de cocher une case, etc.) manifestant le consentement exprès de l'internaute, et sans que le contenu du contrat en formation ne soit exposé automatiquement à cet internaute devant cliquer sur un hyperlien pour y accéder⁷⁶.

Dans tous les cas, pour pouvoir constituer les termes d'un contrat, les conditions d'utilisation du site en cause doivent avoir fait l'objet d'une *reasonable notice*, peu importe qu'elles aient été lues. Ainsi, dès lors que l'utilisateur accepte la transaction proposée de manière générale, existe un *blanket assent* de sa part, ou consentement présumé, aux termes des conditions^{77 78}.

18. – Facebook présente un cas de «*browsewrap*» *agreement*; l'utilisateur s'enregistrant clique sur «*inscription*» et les conditions d'utilisation et politique de confidentialité ne sont consultables que via hyperliens. À ce sujet, si dans l'affaire précitée impliquant SecondLife, un «*clickwrap*» *agreement* était en cause, la validité d'un «*browsewrap*» *agreement* similaire à celui proposé par Facebook a déjà été reconnue en jurisprudence américaine comme offrant un *reasonable notice* à l'internaute⁷⁹. Un contrat pourrait donc être considéré comme formé entre l'utilisateur de Facebook et cette dernière.

19. – Or, si l'internaute contracte valablement avec le fournisseur du réseau social⁸⁰, les incidences en matière de protection des données ne sont pas négligeables : ce contrat peut fonder la légitimité d'un traitement⁸¹ et peut encore, le cas échéant,

⁷⁶ Voy. au sujet des concepts de «*clickwrap*» et «*browsewrap*» *agreements* ainsi que de leurs différences, C.L. KUNZ, H. THAYER, M.F. DEL DUCA et J. DEBROW, *op. cit.*; L.E. TRAKMAN, *op. cit.*, pp. 5 et 54-55; P.B. CUNNINGHAM et E.C. WITKOW, «Click-Wrap and Browse-Wrap Agreements, Click with Caution : Liability for Breach of Click-Wrap and Browse-Wrap Agreements», *The Computer and Internet Lawyer*, vol. 13, n° 6, juin 2006, p. 1.

⁷⁷ À ce sujet et quant à la question de la formation des contrats sur l'internet en droit américain, voy. notamment R.A. HILLMAN et J.J. RACHLINSKI, «Standard-Form Contracting in the Electronic Age», 2001, disponible sur <http://www.ssrn.com>; N.S. KIM, «Clicking and Cringing», *Oregon L. Rev.*, vol. 86, 2007, pp. 797 et s.

⁷⁸ Dans *U.S.A. v. Drew*, le juge Wu explicite la différence entre les deux types de contrats dans le contexte de MySpace (consultable sans inscription, comme certaines portions de profils Facebook depuis peu) : «[a]s a 'visitor' to the MySpace website and being initially limited to the public areas of the site, one is bound by MySpace's browsewrap agreement. If one wishes further access into the site for purposes of creating a profile and contacting MySpace members [...], one would have to affirmatively acknowledge and assent to the terms of service by checking the designated box, thereby triggering the clickwrap agreement».

⁷⁹ Voy. Court of Appeal of the State of California, 31 juillet 2007, *Michael Cohn v. Truebeginnings, LLC* et al., disponible sur <http://www.thelen.com/tlu/CohnVTruebeginnings.pdf>. Toutefois, dans deux autres hypothèses, où il n'y avait pas d'inscription sur le site en cause, le *browsewrap agreement* a été invalidé, voy. *Specht v. Netscape* et U.S. District Court for the Central District of California, 27 mars 2000, *Ticketmaster Corp.*, et al. v. *Tickets.com, Inc.*, disponible sur <http://www.internetlibrary.com/>.

⁸⁰ C'est ce que semble souhaiter ce fournisseur. Toutefois, *quid* de la validité de la convention? L'objet est-il déterminé, le consentement est-il valable? Qui sont les parties, *quid* d'éventuelles stipulations pour autrui?

⁸¹ Article 7, b), de la directive 95/46.

justifier qu'il soit dérogé à l'interdiction des flux transfrontaliers de données vers un pays tiers à l'espace économique européen n'offrant pas une protection adéquate⁸². Les solutions de droit international privé ne sont pas non plus indifférentes à l'existence de ce contrat⁸³.

II. – Des responsables de traitements

Qui sont les responsables de traitement dans le cadre de Facebook? La société Facebook ou ses utilisateurs? Le concept de responsable du traitement doit avant tout distinguer de celui de sous-traitant.

A. – LES CONCEPTS DE RESPONSABLE DE TRAITEMENT ET DE SOUS-TRAITANT

20. – Un responsable du traitement est une personne morale ou physique «qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel»⁸⁴; il est «responsable des choix qui président à la définition et à la mise en œuvre des traitements» et portent sur les finalités et moyens utilisés⁸⁵, même s'il ne dispose pas matériellement des données en cause⁸⁶. Toutefois, «il semble que la détermination de la finalité sera suffisante pour déterminer le responsable du traitement», tandis que la détermination des seuls moyens ne suffira pas⁸⁷. La doctrine se demande même s'il ne conviendrait pas d'abandonner le critère de détermination des moyens du traitement⁸⁸.

Quoi qu'il en soit, les objectifs du traitement et les moyens matériels ou humains mis en œuvre, sont, dans l'état actuel du droit, à prendre en compte et doivent être l'objet

⁸² Article 26, §1^{er}, b), de la directive 95/46. Voy. *infra*, n° 64 concernant Facebook et les Safe Harbor Principles.

⁸³ Voy. *supra*, n° 7 et *infra*, n° 71.

⁸⁴ Article 2, d), de la directive 95/46. Voy. récemment Groupe de travail «article 29», «Opinion 1/2010 on the concepts of 'controller' and 'processor'», 16 février 2010.

⁸⁵ M.-H. BOULANGER, C. DE TERWANGNE, T. LÉONARD, S. LOUVEAUX, D. MOREAUX et Y. POULLET, «La protection des données à caractère personnel en droit communautaire», *J.T.D.E.*, 1997, p. 126.

⁸⁶ M. WALRAVE, *Privacy Gescand? Direct marketing en de bescherming van de persoonlijke levenssfeer*, Leuven, Universitaire Pers Leuven, 1999, p. 224.

⁸⁷ A. BENSOUSSAN, *Informatique et libertés*, Levallois, éditions Francis Lefebvre, 2008, p. 41. Voy. aussi en ce sens A. LUCAS, J. DEVÈZE et J. FRAYSSINET, «Droit de l'informatique et de l'Internet», Paris, P.U.F., 2001, p. 91 : «le critère essentiel est celui de la détermination des finalités».

⁸⁸ T. LÉONARD et A. MENTION, «Transferts transfrontaliers de données : quelques considérations théoriques et pratiques, in *Actualités du droit de la vie privée*, B. DOCQUIR et A. PUTTEMANS (sous la dir. de), Bruxelles, Bruylant, 2008, pp. 108-109.

du pouvoir du responsable ou des coresponsables⁸⁹ de traitement ; « [l']importance est que le responsable de traitement soit la personne, l'instance administrative, la société, l'association, etc., qui dispose du pouvoir de décision sur le traitement effectué »⁹⁰ (je souligne).

21. – Le responsable du traitement est à distinguer du sous-traitant, « la personne physique ou morale, [etc.] qui traite des données à caractère personnel pour le compte du responsable de traitement »⁹¹, uniquement « sur instruction du responsable du traitement, sauf en vertu d'obligations légales »⁹². Il est soumis au pouvoir précité. Les sous-traitants seront « les sociétés en charge de la conservation des données et autres hébergeurs, les sociétés de services de maintenance, les sociétés en charge d'effectuer des opérations de traitement sur les données (tris, classements, analyses, etc.) »⁹³, etc.

22. – Ce pouvoir décisionnel vis-à-vis de ce qu'il advient des données est donc essentiel dans la distinction entre responsable de traitement et sous-traitant. T. Léonard et A. Mention soulignent par ailleurs qu'« il conviendrait peut-être de focaliser le critère de distinction du responsable sur l'identification de celui qui bénéficie de l'utilisation des données et décide ainsi réellement de leur finalité d'utilisation »... le sous-traitant « ne tir[ant] en cette qualité pas de profit de l'utilisation elle-même des données pour l'information qu'elles recèlent »⁹⁴.

23. – Notons enfin qu'« il n'est pas rare qu'une même entité puisse cumuler, dans le cadre d'une opération d'ensemble, plusieurs rôles et donc plusieurs qualités juridiques [; c]es différentes situations doivent bien entendu être distinguées les unes des autres et analysées en tant que telles »⁹⁵. Deux personnes peuvent également être coresponsables d'un même traitement⁹⁶. Ces coresponsables sont alors conjointement responsables de l'exécution des obligations vis-à-vis de la personne concernée⁹⁷, étant entendu qu'ils peuvent chacun être tenu d'appliquer des droits nationaux différents alors qu'un même traitement de données à caractère personnel est en cause⁹⁸.

⁸⁹ Le texte de la directive permet en effet de considérer que plusieurs personnes sont coresponsables d'un même traitement de données. Voy. aussi quant à la loi belge, projet de loi transposant la directive 95/46/CE du Parlement européen et du Conseil, exposé des motifs, *Doc. parl.*, Chambre, sess. ord. 1997-1998, n° 1566/1, p. 15.

⁹⁰ *Ibidem*.

⁹¹ Article 2, e), de la directive 95/46.

⁹² Article 16 de la directive 95/46.

⁹³ M.-L. LAFFAIRE, *Protection des données à caractère personnel*, Paris, éd. d'Organisation, 2005, p. 87.

⁹⁴ T. LÉONARD et A. MENTION, *op. cit.*, p. 109.

⁹⁵ M.-L. LAFFAIRE, *op. cit.*, p. 91.

⁹⁶ Voy. article 2, d), de la directive 95/46.

⁹⁷ C. KUNER, *European Data Protection Law Corporate Compliance and Regulation*, Oxford, Oxford University Press, 2007, p. 72.

⁹⁸ Voy. en ce sens L.A. BYGRAVE, « European Data Protection – Determining Applicable Law Pursuant to European Data Protection Legislation », *Computer Law & Security Review*, 2000, pp. 254-255.

B. — LA SOCIÉTÉ FACEBOOK

24. — La société Facebook détermine les finalités et les moyens de nombreux traitements de données se produisant à l'occasion du fonctionnement du réseau social⁹⁹. Il en est notamment ainsi lorsqu'elle oblige contractuellement l'utilisateur à s'identifier au travers du réseau et impose techniquement la publicité de certaines informations telles que les listes d'amis¹⁰⁰, organise l'utilisation des données personnelles de celui-ci à des fins de publicité ciblée¹⁰¹, conserve ses données dans des *back up copies* au-delà de la suppression de celles-ci par lui, enregistre son adresse IP, collecte des informations via des cookies¹⁰² ou à partir d'autres sources. Elle l'est encore lorsqu'elle transmet des données à des tiers — par exemple pour la défense ou la promotion de ses intérêts économiques ou pour toute autre finalité déclarée dans la politique de confidentialité.

De manière générale, la société Facebook définit techniquement et contractuellement les gammes de finalités et les outils informatiques de traitement de données qu'elle met en place via son service. Elle fixe et modifie les conditions d'utilisation (et en particulier la politique de confidentialité) qui peuvent limiter le comportement de l'utilisateur¹⁰³.

25. — Ceci dit, il est impossible de conclure de manière univoque quant à la qualité de Facebook vis-à-vis de tous les traitements de données réalisés via son service, sauf à élargir *a priori* le concept de traitement¹⁰⁴. Une analyse plus fine pourrait éclairer. En effet, si on considère l'utilisateur comme responsable de certains traitements¹⁰⁵, Facebook pourrait-elle être son sous-traitant, agissant au gré de ses « clics », définissant entre autres les paramètres de diffusion des données placées sur son profil? Dès que le traitement de l'information dépasserait les strictes limites de la volonté de cet utilisateur — pour peut que celle-ci puisse s'exprimer dans le cadre offert par Facebook — cette dernière redeviendrait alors seule responsable de traitement. Le pouvoir de décision de l'utilisateur quant à ces traitements, auxquels il fournit un objet — les données

⁹⁹ Quant à l'opinion du groupe de travail « article 29 », voy. W.P. 163, p. 5.

¹⁰⁰ Depuis une modification récente du site, Facebook traite comme information publiquement disponible différentes données dont les Pages dont un utilisateur est fan et son sexe, voy. E.P.I.C. et al., « Before the Federal Trade Commission », 17 décembre 2009, *In the Matter of Facebook, Inc., Complaint, Request for Investigation, Injunction, and Other Relief* (« E.P.I.C. et al. v. Facebook »), disponible sur <http://epic.org/privacy/infacebook/EPIC-FacebookComplaint.pdf>, ci-après, n° 34.

¹⁰¹ Voy. *supra*, n° 8.

¹⁰² Voy. *infra*, n° 57.

¹⁰³ Pour un aperçu des modifications opérées par la société Facebook quant au réseau (dont ses conditions d'utilisation et politique de confidentialité), voy. E.P.I.C. et al. v. Facebook, n°s 25-38.

¹⁰⁴ Voy. *infra*, n° 60.

¹⁰⁵ Voy. *infra*, n°s 27 et s.

transférées – serait alors en principe nul¹⁰⁶. Il ne serait plus qu'une source d'accès aux informations pour la société Facebook¹⁰⁷.

26. – La même question se poserait si l'entreprise commandant une publicité ciblée était considérée comme responsable de traitement, ce qui n'est pas évident¹⁰⁸. Facebook serait alors plutôt coresponsable, dès lors que son pouvoir décisionnel est déterminant dans la fonctionnalité *ads* (quant aux finalités et moyens ainsi qu'à leur évolution). Une telle coresponsabilité pourrait également, le cas échéant, être envisagée dans le cadre du fonctionnement des applications¹⁰⁹.

C. – LES UTILISATEURS

Il convient, au sujet des utilisateurs, d'établir une distinction en raison de leur nature. En effet, la soumission de l'utilisateur de base¹¹⁰ à la directive 95/46 est discutable tandis qu'il en irait en principe autrement des autres utilisateurs¹¹¹.

1. – *L'utilisateur de base*

27. – Prenons une hypothèse de départ : un utilisateur de Facebook – personne physique – se rend à une fête d'anniversaire, y photographie et filme les participants et diffuse ensuite ces informations via son profil. Il peut être soumis à la directive 95/46 (a) et, partant, peut être responsable de traitement, moyennant toutefois le respect de sa liberté d'expression (b).

a) *Soumission au champ d'application de la directive 95/46*

28. – L'article 3, § 2, de la directive 95/46, seule limitation au champ d'application de cette directive auquel l'article 13 ne permet pas de déroger¹¹², impose en l'espèce

¹⁰⁶ À moins peut-être que ces traitements ne cessent automatiquement dès que les données sont supprimées de son compte par l'utilisateur, auquel cas il aurait en outre le pouvoir d'y mettre un terme.

¹⁰⁷ La personne concernée pourrait toujours engager la responsabilité de l'utilisateur en cas de transfert illicite.

¹⁰⁸ Voy. *infra*, n° 36.

¹⁰⁹ La question gagne toutefois en complexité dans la mesure où l'utilisateur de base ajoute délibérément les applications.

¹¹⁰ Voy. *supra*, n° 13. C'est-à-dire l'utilisateur qui se limite à utiliser les fonctionnalités de base du site Facebook. Ainsi, s'il ajoute des applications, il n'en développe pas, s'il est la cible de publicités, il n'en achète pas, etc.

¹¹¹ L'utilisateur personne physique de Facebook est évidemment souvent aussi une « personne concernée ».

¹¹² C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy et Satamedia Oy* (*Satamedia*), C-73/07, *Rec.*, 2008, points 45-46.

de se demander si cette activité et les traitements subséquents ne relèvent pas de «l'exercice d'activités exclusivement personnelles ou domestiques»¹¹³.

29. – La Cour de justice interprète étroitement cette exception¹¹⁴ et a jugé – dans le cas *Lindqvist* – qu'elle visait «uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes»¹¹⁵ (je souligne). L'avocat général Tizzano avait conclu en ce sens que l'exception ne recouvrait que des «activités manifestement privées et confidentielles, destinées à ne pas sortir de la sphère personnelle ou domestique des intéressés»¹¹⁶.

Le «groupe 29»¹¹⁷ précise par ailleurs que «[i]f an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply»¹¹⁸. Dans le même sens – toujours pour exclure le jeu de l'exception – l'avocat général Tizzano avait pris en compte la «forte connotation sociale» de l'activité de catéchisme¹¹⁹.

30. – En synthèse, deux critères sont à prendre en compte : la nature de l'activité en cause et le «degré d'accessibilité de l'information»¹²⁰. Considérons – ce qui n'est pas toujours le cas – que la nature de l'activité de l'utilisateur de base n'est pas à «forte connotation sociale»¹²¹.

31. – Reste alors à déterminer si le nombre de personnes ayant accès aux données du profil de l'utilisateur précité est défini, ou – si défini – n'est pas tellement grand qu'en serait dénaturée l'exception étudiée. Inévitablement, les *privacy settings* choisis par cet utilisateur comptent. Si les données de son profil sont accessibles à au moins l'un de ses réseaux, au sens des *networks* auxquels Facebook lui permet d'appartenir,

¹¹³ Article 3, §2, deuxième tiret de la directive 95/46. Le premier tiret n'est pas pertinent en l'espèce.

¹¹⁴ Voy. en ce sens R. WONG et J. SAVIRIMUTHU, «All or nothing : this is the question? : The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet», in *John Marshall Journal of Computer & Information Law*, 2008, pp. 241-266, version électronique disponible sur <http://ssrn.com>, p. 8.

¹¹⁵ Affaire *Lindqvist*, points 46-47.

¹¹⁶ Conclusions de l'avocat général Tizzano, dans l'affaire *Bodil Lindqvist*, point 34.

¹¹⁷ Établi en vertu de l'article 29 de la directive 95/46. Il est composé d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission, et est notamment chargé de contribuer à la mise en œuvre homogène de la directive 95/46 (article 30).

¹¹⁸ W. P. 163, p. 6.

¹¹⁹ Conclusions de l'avocat général Tizzano, *op. cit.*

¹²⁰ Voy. le propos du Berlin Data Protection Commissioner reproduit par R. WONG, «Social...», *op. cit.*

¹²¹ Il peut aisément utiliser Facebook aux fins de l'organisation d'activités sportives, de sorties, etc.

l'exception ne peut jouer, un tel réseau étant par nature composé d'un nombre indéfini de personnes¹²².

Lorsque l'utilisateur limite l'accessibilité de son profil à ses « amis », autrement dit, à un cercle fermé de personnes déterminées – acceptées comme « amies » – il peut n'agir qu'à des fins strictement personnelles. Le jeu de l'exception est alors envisageable et la personne concernée par les données en cause peut toujours se reporter aux autres protections qu'offre le droit (respect de la vie privée sur la base de l'effet horizontal de l'article 8 de la Convention européenne des droits de l'homme, droit à l'image, prohibition de la calomnie et de la diffamation, etc.).

Deux difficultés subsistent toutefois. D'une part, ces « amis » sont de natures diverses. Ce qui peut conduire à la « décontextualisation »¹²³ de l'information et à sa réutilisation à des fins incompatibles avec sa diffusion originale. Et le compartimentage des « amis » a une incidence toute relative¹²⁴. En outre, des développeurs d'applications pourraient aussi accéder à des informations du profil¹²⁵.

Et d'autre part, il ne faut pas perdre de vue que les données sont transférées à Facebook établie dans un pays tiers qui, en vertu d'une politique de confidentialité relativement indéterminée et potentiellement quasi unilatéralement fluctuante¹²⁶, entend traiter les données reçues aussi selon ses propres finalités¹²⁷. Encore faudrait-il alors s'interroger sur la licéité de la pratique de Facebook qui traiterait des données relatives à un non-utilisateur du site, ou à un autre utilisateur que celui qui transfère ces données, à ces fins¹²⁸.

¹²² Certains types de réseaux (ville, université, pays) sont publiquement accessibles.

¹²³ Voy. *supra*, n° 13.

¹²⁴ Cette possibilité d'établir des listes d'amis est d'ailleurs limitée quant à la détermination des informations auxquelles elles peuvent accéder. Originellement, l'utilisateur ne pouvait qu'interdire complètement ou non l'accès de son *Wall* à une personne. Il en était de même pour les images et vidéos postées. Désormais, le site a évolué et la granularité du contrôle d'accessibilité s'est améliorée.

¹²⁵ Ce partage se faisant via la plate-forme Facebook. Il faudrait observer si l'application accède alors à des informations relatives à d'autres personnes que l'utilisateur lui-même, au sein du profil de ce dernier.

¹²⁶ L'efficacité du processus de modification de la politique de confidentialité est discutable : « *We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's new effective date. If we make material changes to this policy, we will notify you here, by email or through notice on our home page.* ».

¹²⁷ Si l'utilisateur n'est pas soumis au champ d'application de la directive 95/46, il n'est pas tenu de respecter le régime propre aux flux transfrontières de données. Il pourrait donc légalement – au regard de la protection des données – transférer des données à un responsable de traitement (fournisseur d'un réseau social, d'un site Web, etc.) établi dans un pays tiers ne garantissant pas une protection adéquate, voy. *infra*, n° 63.

¹²⁸ Dans une telle hypothèse, *quid* du respect des principes fondamentaux de la protection des données tels que celui d'information de la personne concernée? *Quid* par exemple du respect des principes de notice et de choice des Safe Harbor Principles? Voy. *infra*, n° 64 au sujet des Safe Harbor Principles.

32. – L'utilisateur de base peut donc, selon les cas, être ou pas soumis à la directive 95/46, une analyse *in concreto* de chaque cas étant nécessaire pour conclure¹²⁹.

b) *Nécessité de pondérer les droits et libertés en présence*

33. – Déterminant la finalité (communiquer à d'autres personnes) et les moyens (Facebook) d'un traitement de publication de données, l'utilisateur peut être responsable de traitement. Mais il ne l'est pas sans nuances. La protection des données ne peut notamment aboutir à restreindre indûment la liberté d'expression garantie – entre autres – par l'article 10 de la Convention européenne des droits de l'homme. C'est « au stade de la mise en œuvre sur le plan national de la réglementation transposant la directive 95/46 dans des cas d'espèce particuliers que doit être trouvé un juste équilibre des droits et intérêts visés »¹³⁰; les dispositions de la directive 95/46 ne violent pas en elles-mêmes la liberté d'expression¹³¹. Et cette réglementation doit être interprétée conformément aux droits fondamentaux et au principe de proportionnalité¹³².

34. – À cette fin, d'une part, les États membres disposent de la marge de manœuvre suffisante, dans le cadre de la directive 95/46, pour adopter des mesures spécifiques¹³³ pour « concilier » liberté d'expression et droit fondamental à la vie privée – auquel s'ajoute le droit fondamental à la protection des données¹³⁴ – et obtenir une « pondération équilibrée »¹³⁵. D'autre part, les sanctions en cas de violation de la directive doivent être proportionnées et appliquées en tenant notamment compte de la

¹²⁹ Au regard de la loi canadienne de protection des données, voy. toutefois E. DENHAM, *op. cit.*, p. 90, n° 306, selon laquelle « Lorsque les utilisateurs affichent de l'information au sujet de non-utilisateurs sur leur page de profil, leur Mur ou dans les Actualités, ces affichages sont réalisés à des fins personnelles et ne sont pas du ressort de la loi ». Voy. s. 4 (2) (b) de la loi sur la protection des renseignements personnels et les documents électroniques sanctionnée le 13 avril 2000, disponible sur http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

¹³⁰ En ce sens, affaire *Lindqvist*, point 85.

¹³¹ Affaire *Lindqvist*, point 90.

¹³² Affaire *Lindqvist*, point 87.

¹³³ Voy. articles 9, 13 et considérant n° 37 de la directive 95/46. La Cour de justice a jugé que les notions afférentes à la liberté d'expression, dont celle de journalisme, devaient être interprétées largement, et les dérogations adoptées limitées au strict nécessaire, affaire *Satamedia*, point 56. Voy. aussi point 61, où la Cour définit très largement l'activité de journalisme.

¹³⁴ Article 8 de la Charte des droits fondamentaux de l'Union européenne (*J.O. C 364*, du 18 décembre 2000); A. ROUVROY et Y. POUILLET, « The right to informational self-determination and the value of self-development, Reassessing the importance of privacy for democracy », in *Reinventing Data Protection*, S. GUTWIRTH, P. DE HERT, C. DE TERWANGNE et Y. POUILLET (éds), Springer, 2009, pp. 45 et s.; S. RODOTA, « Data Protection as a Fundamental Right », in *Reinventing Data Protection*, *op. cit.*, pp. 77 et s.

¹³⁵ Voy. l'affaire *Satamedia*, points 52-56. Pour une illustration quant à la balance à faire entre liberté d'expression et vie privée, voy. R. WONG et J. SAVIRIMUTHU, *op. cit.*, pp. 29-31. Voy. encore 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 C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, pp. 96-98.

durée de la violation et de «l'importance pour les intéressés, de la protection des données divulguées»¹³⁶.

Il appartient donc aux autorités nationales d'intervenir au nom d'autres droits et libertés fondamentaux – dont également le secret des communications électronique et de la correspondance¹³⁷ –, là où la protection des données apparaît comme réductrice d'autres libertés jugées *in casu* plus essentielles¹³⁸.

2. – Les autres utilisateurs

35. – Les développeurs d'application qui, via leurs applications, peuvent traiter et extraire des informations à caractère personnel à partir de la *Facebook Platform* pour des finalités qu'ils déterminent¹³⁹, peuvent être responsables de traitement. Facebook peut être coresponsable de traitement si elle oblige les utilisateurs à partager un minimum de données au travers de la *Facebook Platform*¹⁴⁰. Les administrateurs de *Facebook Pages* sont aussi susceptibles de collecter des données à caractère personnel et de poursuivre leurs propres finalités. Les moyens choisis sont les fonctionnalités de Facebook.

36. – *Quid* de l'entreprise qui paramètre et commande une publicité ciblée sur Facebook? Ne déterminerait-elle pas les finalités – vendre au mieux le produit ou service qu'elle offre – d'un groupe de traitements de données particulier – celui qui est nécessaire à la réalisation de sa campagne publicitaire – et le moyen utilisé à cette fin, *ads* et les bases de données de Facebook? Facebook est responsable d'un tel groupe de traitements. Toutefois, elle ne fait en principe pas de publicité ciblée pour son propre compte et de sa propre initiative via *ads*. Autrement dit, une commande est nécessaire; la volonté de l'entreprise concernée est aussi décisive quant à l'existence – leurs début et fin – des traitements de données pertinents. Par ailleurs, n'est-ce pas cette entreprise qui «bénéficie des données... pour l'information qu'elles recèlent»¹⁴¹? Ainsi, sans

¹³⁶ Affaire *Lindqvist*, points 88-89.

¹³⁷ Susceptibles de s'appliquer fréquemment dans le contexte de Facebook. Voy. notamment article 8 de la Convention européenne des droits de l'homme, article 29 de la Constitution et article 5 de la directive (CE) n° 2002/58 du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.* L 201, du 31 juillet 2002.

¹³⁸ S'il est excessif d'exiger de l'utilisateur de base de Facebook qu'il déclare son traitement auprès de l'autorité nationale de protection des données, que les juges ou législateurs nationaux écartent cette exigence en la considérant comme une atteinte injustifiée à la liberté d'expression.

¹³⁹ Facebook avertit l'utilisateur qu'il peut être amené à consentir à leur politique de confidentialité.

¹⁴⁰ Comme par exemple lorsqu'elle considère publics le nom d'un utilisateur et sa liste d'amis, permettant d'office aux applications d'y accéder dès qu'elles sont ajoutées par les utilisateurs. Ainsi, même un utilisateur qui n'aurait ajouté aucune application pourrait être impliqué dans le traitement de données résultant du fonctionnement d'une application ajoutée par un de ses amis.

¹⁴¹ Voy. *supra*, n° 22.

posséder les données à caractère personnel ¹⁴², et sans avoir quelque emprise que ce soit sur celles-ci, cette entreprise ne pourrait-elle pas quand même être considérée comme coresponsable de traitement?

III. – Droit applicable à la société Facebook

37. – La société Facebook étant, sous quelques réserves, responsable de traitement, la question du droit lui étant applicable peut désormais être étudiée ¹⁴³. Le propos se focalise sur Facebook pour deux raisons. D'une part, elle maîtrise les tenants et les aboutissants du réseau qu'elle offre dans ses moindres détails. Et d'autre part, son cas permet de tester les limites d'applicabilité territoriale de la directive 95/46. Évidemment, les développements suivants valent, *mutatis mutandis*, pour l'ensemble des responsables de traitement identifiables.

L'article 4 de la directive 95/46 détermine son champ d'application territorial. L'analyse doit être centrée sur un traitement de données ¹⁴⁴, et à partir de celui-ci, deux situations sont possibles : soit il est réalisé dans une hypothèse incluse dans cet article (A), auquel cas le régime de protection des données mis en place par celle-ci s'applique intégralement, soit tel n'est pas le cas, et le régime des flux transfrontières des données s'applique (B). Bien entendu, c'est *in fine* une disposition de droit national qui sera appliquée par une juridiction nationale et entraînera, le cas échéant, l'application extraterritoriale de la directive 95/46 (C).

¹⁴² Voy. *supra*, n° 20. Mais l'entreprise en question ne décide pas vraiment totalement ce qu'il advient des données.

¹⁴³ Si un litige est soumis à une juridiction belge, la violation de la loi belge transposant la directive 95/46 (la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, «L.V.P.») serait une faute au sens de l'article 1382 du Code civil. Or pour déterminer si une telle violation peut être invoquée en tant que telle, et si le régime de responsabilité de l'article 15bis de la L.V.P. peut jouer, il faut savoir si la L.V.P. lie Facebook. Pour les autres aspects du litige (évaluation du dommage, formation du contrat, etc.), il faudrait, me semble-t-il, se reporter aux autres règles – internationales, communautaires ou nationales – de droit international privé. Bien qu'une autre interprétation de l'article 4, comme s'étendant à tous les aspects du litige ait déjà défendue, voy. M.V. PÉREZ ASINARI, «International Aspects of Personal Data Protection *Quo Vadis EU?*», in *Défis du droit à la protection de la vie privée*, M.V. PÉREZ ASINARI et P. PALAZZI (éds), coll. Cahiers du C.R.I.D., Bruxelles, Bruylant, 2008, pp. 405-407.

¹⁴⁴ Conformément à la rédaction de l'article 4 de la directive 95/46. Voy. en ce sens D. KORFF, *Data Protection Laws in the European Union*, Richard Hagle, Federation of European Direct and Interactive Marketing and The Direct Marketing Association, 2005, p. 26. C'est d'ailleurs à l'égard d'un traitement de données que le responsable du traitement peut être identifié.

A. – ARTICLE 4 : APPLICATION INTÉGRALE DE LA DIRECTIVE 95/46

38. – Selon l'article 4 de la directive 95/46, dont la portée est d'abord discutée (1), un État membre applique sa réglementation nationale de transposition de la directive 95/46 dans deux hypothèses, en fonction du lieu d'établissement du responsable du traitement (2) et du lieu de situation de moyens de traitement (3). Sa rédaction prête toutefois à confusion quant au possible cumul de ces hypothèses vis-à-vis d'un même responsable de traitement (4).

1. – *Portée de l'article 4 de la directive 95/46*

39. – Quel rôle joue l'article 4 en droit international privé? La réflexion est similaire – si pas identique¹⁴⁵ – à celle relative à la clause dite « marché intérieur », dont la directive 2000/31 contient notamment une figure, ainsi qu'aux principes de « reconnaissance mutuelle » et du « pays d'origine »¹⁴⁶. Cet article 4 est-il une règle de conflit traditionnelle, « bilatérale », comportant une « règle de rattachement » propre à la « catégorie de rattachement » que constituerait la protection des données garantie par la directive 95/46¹⁴⁷? La rédaction des considérants 18 et 20, l'objectif de la directive d'éviter les conflits de loi¹⁴⁸, de même que les travaux préparatoires de la loi

¹⁴⁵ La directive 95/46 a d'ailleurs déjà été classée parmi les réglementations sectorielles contenant une telle clause « marché intérieur », voy. M. WILDERSPIN et X. LEWIS, « Les relations entre le droit communautaire et les règles de conflits de lois des États membres », *Rev. crit. dr. intern. privé*, 2002, p. 298.

¹⁴⁶ À propos de cette clause et de ces principes, voy. notamment M. FALLON et J. MEEUSEN, « Le commerce électronique, la directive 2000/31/CE et le droit international privé », *Rev. crit. dr. intern. privé*, 2002, pp. 480-488 et 472-476; M. WILDERSPIN et X. LEWIS, *op. cit.*, pp. 298-312 et 16-18; M.-N. JOBARD-BACHELLIER, « La portée du test de compatibilité communautaire en droit international privé contractuel », in *Le droit international privé : esprit et méthodes – Mélanges offerts en l'honneur de Paul Lagarde*, Paris, Dalloz, 2005; V. HEUZÉ, « De la compétence de la loi du pays d'origine en matière contractuelle ou l'anti-droit européen », in *Le droit international privé : esprit et méthodes*, précité; R. STEENNOT, « Internationaal privaatrechtelijke aspecten van middelen internet gesloten (consumenten) overeenkomsten », *D.A. O.R.*, 2000, pp. 199-200; D. BUREAU et H. MUIR WATT, *Droit international privé*, t. 1, Paris, P.U.F., 2007, pp. 534-538 et 542-543; F. RIGAUX et M. FALLON, *Droit international privé*, Bruxelles, De Boeck & Larcier, pp. 164-165; A. CRUQUENAIRE, avec la coll. de C. LAZARO, « La clause de marché intérieur : clef de voûte de la directive sur le commerce électronique », in *Le commerce électronique européen sur les rails? – Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, coll. Cahiers du C.R.I.D., Bruxelles, Bruylant, 2001, pp. 42-94.

¹⁴⁷ Sur les notions de « règle de rattachement » et « catégorie de rattachement », voy. F. RIGAUX et M. FALLON, *Droit international privé*, Bruxelles, De Boeck & Larcier, 2005, pp. 106 et s. Quant aux notions de règle ou méthode « multilatérales » ou « bilatérales », voy. H. BATIFFOL et P. LAGARDE, *Traité de droit international privé*, t. 1, Paris, L.G.D.J., 1993, pp. 423-425; D. BUREAU et H. MUIR WATT, *op. cit.*, pp. 332-339.

¹⁴⁸ Voy. C. KUNER, se référant à U. DAMMANN et S. SIMITIS, C. KUNER, *op. cit.*, p. 111.

belge – malgré sa rédaction¹⁴⁹ – la transposant le laisseraient entendre¹⁵⁰, en tous cas pour les cas impliquant le territoire d'un État membre selon l'un ou l'autre des critères de rattachement de l'article 4¹⁵¹.

40. – Une autre voie pourrait toutefois être suivie, en adoptant deux angles de réflexion¹⁵². Premièrement, dans une hypothèse donnée, lorsque les juridictions de l'État visé par l'article 4 sont saisies («État A»), le droit de cet État doit à tout le moins prévoir qu'il s'applique en ce qu'il transpose la directive 95/46; l'article 4 l'y oblige. La réglementation nationale transposant la directive apparaîtrait alors comme une «loi d'applicabilité immédiate» – ou «de police» –, et donc une règle de conflit «unilatérale», dont la transposition de l'article 4 est une «règle d'applicabilité directe» aux divers «facteurs d'applicabilité»¹⁵³.

41. – La loi belge – article 3bis – par exemple, colle à cette conception et stipule quand elle s'applique en reprenant presque à l'identique, *mutatis mutandis*, le texte de l'article 4 de la directive 95/46, sans préciser quel droit est applicable si ce n'est elle-même. Une application «bilatérale» de celle-ci fondée sur les principes de «reconnaissance mutuelle» et du «pays d'origine», les éléments précités¹⁵⁴ ainsi que sur les travaux préparatoires lui donnerait toutefois l'effet d'une règle de rattachement¹⁵⁵ quant à l'applicabilité du droit des États membres.

¹⁴⁹ Voy. *infra*, n° 41.

¹⁵⁰ Voy. projet de loi..., *op. cit.*, p. 26.

¹⁵¹ Voy. *infra*, n° 66 dans le cas où le responsable de traitement serait établi dans un État tiers et ne ferait pas usage sur le territoire de la Communauté de moyens aux fins de traitement. Une étape supplémentaire et fort contestable serait de considérer que la règle de conflit de lois bilatérale qu'imposerait la directive 95/46 s'étendrait, le cas échéant, à la désignation du droit d'un État tiers. Les États membres pourraient toutefois adopter une règle bilatérale de conflit de lois.

¹⁵² La réflexion de M. FALLON et J. MEEUSEN au sujet de la clause «marché intérieur» de la directive 2000/31 est transposée et adaptée au cas d'espèce, voy. M. FALLON et J. MEEUSEN, *op. cit.*, pp. 480-486.

¹⁵³ Sur les notions de «loi d'applicabilité (ou d'application) immédiate», ou «de police», et de «règle d'applicabilité directe» ainsi que de «critère d'applicabilité», voy. F. RIGAUX et M. FALLON, *op. cit.*, pp. 138-140 et 129-134. Au sujet de l'article 4 de la directive 95/46, S. FRANCOY et M. FALLON soulignent que cette disposition se présente comme une «règle d'applicabilité», voy. M. FALLON et S. FRANCOY, «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.), p. 247. Voy. également F. RIGAUX et M. FALLON, *op. cit.*, pp. 162-164. En ce sens également, selon moi, K. KREUZER, «La communautarisation du droit international privé : les acquis et les perspectives», in *Droit Global Law – Unifier le droit : le rêve impossible*, L. VOGEL (sous la dir. de), Paris, éd. Panthéon-Assas, 2001, p. 122 et note n° 117).

¹⁵⁴ Voy. *supra*, n° 39, *in fine*.

¹⁵⁵ Sur ce type d'application d'une règle unilatérale, voy. H. BATIFFOL et P. LAGARDE, *op. cit.*, p. 425.

42. – Secondement, lorsque les juridictions d'un autre État («État B») sont saisies, la règle pourrait être vue sous un autre jour. L'article 4 de la directive 95/46 n'imposerait pas, en tous cas explicitement, l'applicabilité du droit de l'«État A» ou d'un quelconque autre «État C». Dans ce contexte, l'«État B» retrouverait une certaine marge de manœuvre. Ainsi, ses règles de conflits de lois – d'applicabilité directe ou de rattachement – pourraient désigner l'application – le cas échéant partielle – du droit de cet «État B», voire d'un autre «État C»¹⁵⁶. Mais cela alors uniquement dans la stricte mesure où, dans l'hypothèse donnée, l'«application»¹⁵⁷ du droit désigné ne conduirait pas, d'une part, à «restreindre» ou «interdire» «la libre circulation des données à caractère personnel»¹⁵⁸, et, d'autre part, à violer le droit communautaire primaire¹⁵⁹. Dans le cas contraire, ce droit devrait être écarté en application d'une «exception de reconnaissance mutuelle»¹⁶⁰. Cette solution n'est pas indifférente dès lors que les États membres disposent d'une certaine marge de manœuvre dans la transposition des dispositions matérielles de la directive 95/46¹⁶¹, pouvant donner lieu à des disparités susceptibles d'influer sur la libre circulation des données à caractère personnel.

43. – En synthèse, deux interprétations sont donc possibles. Soit l'article 4 doit être transposé, *mutatis mutandis*, comme règle de rattachement désignant l'applicabilité du droit des États membres, notamment en raison du principe de reconnaissance mutuelle. Soit, pour peu que le droit d'un État membre s'applique au moins lorsque cet article le prescrit, les autorités de cet État disposent d'une marge de manœuvre résiduaire – le cas échéant, très réduite – qu'elles peuvent exploiter : en raffinant le critère d'applicabilité consacré dans l'article 4, en adoptant une règle de rattachement spécifique à la protection des données, en se référant à ses règles générales de conflits de lois – de quelque origine que ce soit – ou encore en combinant l'une et l'autre de ces possibilités. Il faut noter à ce sujet que certaines transpositions de l'article 4 de la directive 95/46 s'en écartent¹⁶² et semblent être l'expression d'un certain détachement par rapport à cet article, dont la conformité à la directive serait discutable selon

¹⁵⁶ En droit national, seule la règle de rattachement pourrait évidemment avoir cette portée.

¹⁵⁷ L'atteinte ne résulterait pas de la règle de rattachement mais bien de l'application de la règle de droit matériel désignée, voy. en ce sens M. WILDERSPIN et X. LEWIS, *op. cit.*, pp. 24 et 302.

¹⁵⁸ Voy. article 1^{er}, §2, de la directive 95/46.

¹⁵⁹ À savoir par exemple la libre prestation de service et la non-discrimination en raison de la nationalité. Voy. M. WILDERSPIN et X. LEWIS, *op. cit.*, pp. 6-37; D. BUREAU et H. MUIR WATT, *op. cit.*; M.-N. JOBARD-BACHELLIER et J.-S. BERGÉ, «La réception du droit communautaire en droit des conflits de lois», in *La réception du droit communautaire en droit privé des États membres*, session internationale d'études doctorales, Université de Paris X-Nanterre, 28 janvier-1^{er} février 2003, Bruxelles, Bruylant, 2003, p. 200 et note n° 47.

¹⁶⁰ Voy. D. BUREAU et H. MUIR WATT, *op. cit.*, p. 534, et M. FALLON et J. MEEUSEN, *op. cit.*, pp. 486-488.

¹⁶¹ Voy. à ce sujet le considérant n° 9 de la directive 95/46 et M.-H. BOULANGER *et al.*, *op. cit.*, p. 213.

¹⁶² Voy. *infra*, n° 69.

les deux interprétations. Enfin, de ces dernières, la première semble plus conforme à la logique du marché intérieur et au principe de reconnaissance mutuelle ainsi qu'à l'esprit de la directive 95/46, tandis que la seconde est plus proche de son texte et, le cas échéant, de la perception qu'ont certains États membres de l'article 4 de la directive 95/46.

2. – *Un établissement sur le territoire de la Communauté*

44. – Quelle que soit la portée de l'article 4 de la directive 95/46, il convient désormais de s'interroger sur son sens. Selon son paragraphe 1^{er}, a), un État membre applique sa réglementation nationale si le responsable du traitement y dispose d'un établissement, et que ce traitement se produit dans le cadre des activités de cet établissement. Ces éléments sont donc discutés dans un premier temps en théorie (a) pour être ensuite confrontés à l'hypothèse de Facebook (b).

a) *En théorie*

45. – La notion d'établissement nécessite, selon la jurisprudence de la Cour de justice, «la réunion permanente de moyens humains et techniques nécessaires aux prestations de service en cause»¹⁶³, et «comporte l'exercice effectif [– et réel, ajoute le considérant n° 19 de la directive 95/46 –] d'une activité économique au moyen d'une installation stable dans un autre État membre pour une durée indéterminée»¹⁶⁴, peu importe sa forme juridique¹⁶⁵, «un simple bureau, géré par le propre personnel de l'entreprise»¹⁶⁶ suffisant. L'article 4 viserait, quant aux prestataires de services de la société de l'information, «*de plaats waar het centrum (of de centra) van economische activiteit van de provider is*»¹⁶⁷.

46. – Dans ce contexte, un responsable de traitement établi dans un État tiers (la société Facebook) peut être réputé établi sur le territoire de la Communauté s'il y dispose d'un établissement au sens exposé¹⁶⁸.

¹⁶³ B. HAVELANGE et A.-C. LACOSTE, «Les flux transfrontaliers de données à caractère personnel en droit européen», *J.T.D.E.*, 2001, p. 243 et note 22, faisant référence à C.J.C.E., 7 mai 1998, *Lease Plan Luxembourg s.a. c. Belgische Staat*, C-390/96, *Rec.*, 1998, p. I-02553, points 25 à 27 en particulier.

¹⁶⁴ C.J.C.E., 25 juillet 1991, *The Queen c. Secretary of State for Transport*, ex parte *Factortame Ltd et autres*, C-221/89, *Rec.*, 1991, p. I-03905, point 20.

¹⁶⁵ Voy. considérant n° 19 de la directive 95/46.

¹⁶⁶ A précisé la Cour de justice concernant la liberté d'établissement, voy. C.J.C.E., 4 décembre 1986, *Commission c. République fédérale d'Allemagne*, 205/84, *Rec.*, 1986, p. 03755, point 21.

¹⁶⁷ P.H. BLOK, «Privacy-bescherming in alle staten – Internationaal privacy-recht en I.P.R. onder de Europese Privacy-richtlijn», *Computerr.*, 2005, p. 299. L'auteur vise «*een bedrijf dat online diensten aanbiedt*».

¹⁶⁸ V.D. KORFF, *op. cit.*, pp. 27 et 29-30.

47. – Mais pour satisfaire aux conditions de l'article 4, § 1^{er}, a), encore faudrait-il que le traitement de données en cause soit effectué «dans le cadre des activités» de cet établissement. Un indice de satisfaction à cette exigence pourrait être la «disponibilité» des données traitées à partir de l'établissement en question¹⁶⁹. C. Kuner soutient qu'il n'y serait par exemple pas satisfait si des internautes européens envoyaient leurs données directement à une société mère aux fins du traitement, via l'Internet, même si cette société dispose d'une filiale sur le territoire communautaire¹⁷⁰.

Le «groupe 29» a quant à lui développé la condition précitée dans son avis relatif aux moteurs de recherche, applicable aux réseaux sociaux¹⁷¹. Selon cet avis, l'établissement devrait jouer «un rôle significatif dans l'opération de traitement en question»¹⁷²; tel est le cas dans trois hypothèses dont une retient particulièrement notre attention : celle où «un fournisseur de [réseau social] établit un bureau [(office)] dans un État membre (EEE) qui joue un rôle dans la vente de publicités ciblées aux habitants de cet État¹⁷³»¹⁷⁴.

b) *Dans le cas de Facebook*

48. – Facebook a commencé par traduire son site dans des langues de plus en plus variées et dispose finalement de bureaux sur le territoire communautaire¹⁷⁵. Ces derniers constituent des établissements sur le territoire de la Communauté; leur implantation est durable, comme en atteste à tout le moins le rôle du bureau de Dublin, et tout porte à croire que des moyens humain et matériel sont affectés à l'exercice d'une activité effective et réelle.

49. – Cette activité, en tous cas pour l'*office* de Londres et probablement pour ceux de Suède, France et Italie, semble intégrée – d'une façon ou d'une autre – à la vente

¹⁶⁹ P.H. BLOK, *op. cit.*, p. 299.

¹⁷⁰ C. KUNER, *op. cit.*, p. 72.

¹⁷¹ Voy. W.P. 163, p. 5.

¹⁷² W.P. 148, p. 11.

¹⁷³ Et pourquoi pas aux habitants d'autres États membres?

¹⁷⁴ Pour un cas impliquant Google et les forums Usenet, voy. T.G.I. Paris, ord. réf., 14 avril 2008, disponible sur http://www.legalis.net/jurisprudence-decision.php3?id_article=2311, où le juge conclut qu'il n'est pas démontré que Google France (société à responsabilité limitée) intervient dans le processus de traitement des données personnelles impliqué par le fonctionnement du service d'archivage considéré – le service en cause relève de l'activité de Google Inc. (Californie) – malgré le fait que l'objet de la société Google France, «la fourniture de tous services et/ou conseils relatifs aux logiciels, au réseau internet, aux réseaux télématiques ou en ligne», «comporte notamment la promotion directe de produits et services et la mise en œuvre de centres de traitement de l'information».

¹⁷⁵ Voy. *supra*, n^{os} 4-7.

des publicités ciblées. Donc, eu égard à l'opinion du «groupe 29», les traitements de données engendrés par *Ads* impliquant ces bureaux pourraient être soumis à l'intégralité de la directive.

50. – Il est plus compliqué de traiter le cas de l'*office* de Dublin. Jusqu'où vont – et iront – ses activités? Celles-ci s'étendront-elles à l'administration des traitements de données réalisés dans le cadre du fonctionnement de la «branche communautaire» du réseau social Facebook? Ce qui peut être déterminant quant au droit applicable à Facebook.

51. – Resterait finalement à identifier quels traitements de données sont concrètement concernés. Ce qui n'est pas évident dès lors que l'activité même des bureaux de Facebook n'est pas aisément identifiable. Et les quelques informations dont je dispose ne me permettent pas de trancher définitivement les questions posées.

3. – *L'utilisation de moyens situés sur le territoire de la Communauté*

52. – Lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté¹⁷⁶, en vertu de l'article 4, § 1^{er}, c), un État membre applique sa réglementation nationale si ce responsable «recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté»¹⁷⁷. Après avoir explicité cette disposition en théorie (a), elle peut être appliquée en l'espèce (b).

a) *En théorie*

53. – La finalité originelle de cette disposition est d'éviter que le responsable du traitement n'évade la soumission aux obligations de la directive en s'établissant dans un pays tiers¹⁷⁸. Son application nécessite d'interpréter la notion de «moyen» («*equipment*»).

54. – T. Léonard et A. Mention ont synthétisé – en doctrine belge – les positions défendues à ce sujet¹⁷⁹. D'une part, cette notion peut être interprétée «à la lettre», et donc recevoir une portée très large. D'autre part, deux autres interprétations plus restrictives – rassemblant la doctrine belge majoritaire – peuvent être défendues : l'une

¹⁷⁶ La notion de «Communauté» vise les États membres et ceux de l'espace économique européen.

¹⁷⁷ En outre, en vertu de l'article 4, § 2, de la directive 95/46, «le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même».

¹⁷⁸ Voy. à ce sujet C. KUNER, *op. cit.*, p. 119, et P.H. BLOK, *op. cit.*, pp. 297-298.

¹⁷⁹ T. LÉONARD et A. MENTION, *op. cit.*, pp. 115-118.

est «sémantique»¹⁸⁰, l'autre «téléologique». C'est l'interprétation téléologique que les auteurs estiment «plus convaincante». Selon celle-ci, seraient visées deux hypothèses : celle du contournement délibéré par délocalisation de l'établissement du responsable de traitement, et celle où «le responsable de traitement organise activement, par des moyens propres qu'il se choisit, situés sur le territoire européen, un flux de données 'européennes' vers le pays tiers en vue du traitement ultérieure de ces données en dehors de l'EEE»¹⁸¹.

Dans tous les cas, la notion doit être concrétisée. Sont des exemples d'équipements «les PC, terminaux et serveurs [– 'servers that store, modify, or otherwise process the data other than just sending it on its way'¹⁸² –] que l'on peut utiliser pour quasiment tous types de traitement de données»¹⁸³. Un établissement du responsable de traitement devrait aussi pouvoir être considéré comme un «moyen»¹⁸⁴. Le terme «moyen» suggère un concept plus large que «any physical apparatus»¹⁸⁵. En tout cas, ces moyens ne doivent pas être de «transit»¹⁸⁶.

55. – Encore faut-il que le responsable de traitement «recoure» («makes use») à de tels moyens, «à des fins de traitement de données à caractère personnel», peu importe qu'il en soit propriétaire ou possesseur¹⁸⁷; il faut que les moyens en cause soient à sa disposition¹⁸⁸, sans pour autant que ce dernier exerce nécessairement un contrôle total sur ceux-ci. Cette maîtrise est suffisante lorsque le responsable de traitement «détermine quelles données sont collectées, stockées, transférées, modifiées, etc., de quelle manière et dans quel but»¹⁸⁹.

¹⁸⁰ Fondée sur le concept de moyen et de l'utilisation qui doit en être faite (possession, location, utilisation directe ou indirecte) par le responsable de traitement.

¹⁸¹ T. LÉONARD et A. MENTION, *op. cit.*, p. 118. En ce sens, voy. C. DE TERWANGNE et S. LOUVEAUX, «Data Protection – Data protection and online networks», *Computer Law & Security Review*, 1997, p. 238. Mais souvent, comme dans le cas de Facebook, la localisation du responsable de traitement hors Communauté «est logique et ne résulte pas d'une volonté de contourner les dispositions de la directive», B. HAVELANGE et A.-C. LACOSTE, *op. cit.*, p. 244.

¹⁸² C. KUNER, *op. cit.*, p. 122.

¹⁸³ Groupe 29, «Document de travail : Application internationale du droit de l'U.E. en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'U.E.» (ci-après : «W. P. 56»), 30 mai 2002, p. 9.

¹⁸⁴ Voy. les nuances de C. KUNER, *op. cit.*, pp. 122-123.

¹⁸⁵ D. KORFF, *op. cit.*, note 31, p. 33. L.A. BYGRAVE relèvera que le considérant n° 40 de la directive utilise tout de même le terme «means». L.A. BYGRAVE, «European Data Protection – Determining...», *op. cit.*, p. 254.

¹⁸⁶ «[L]es moyens de transit typiques [étant] les réseaux de télécommunications (dorsales, câbles, etc.) qui font partie de l'internet et par lesquels les communications internet voyagent du point d'expédition vers le point de destination», W. P. 56, p. 9.

¹⁸⁷ Voy. en ce sens, W.P. 56, p. 10. Voy. toutefois P.P. SWIRE, «Of Elephants, Mice, and Privacy : International Choice of Law and the Internet», 23 août 1998, disponible sur <http://ssrn.com>, p. 18.

¹⁸⁸ W.P. 56, pp. 9-10.

¹⁸⁹ *Ibidem*.

56. – Eu égard aux considérations précédentes, l'ordinateur d'un internaute¹⁹⁰ constituera un «moyen» si, d'une part, un logiciel – virus, *Trojan horse*, etc. – permet d'en prendre contrôle, ou permet de collecter des données à partir de celui-ci et les transfère au responsable de traitement, comme dans les hypothèses d'utilisation de *cookies*, «bannières», «JavaScripts et applications logicielles similaires»¹⁹¹. Et si d'autre part, il est impliqué dans le traitement de données à caractère personnel réalisé par le responsable de traitement.

b) *Dans le cas de Facebook*

57. – Facebook utilise à tout le moins deux types de «moyens» situés sur le territoire de la Communauté¹⁹². D'une part, elle collecte des données via *cookies*, comme le précise la politique de confidentialité¹⁹³. Les terminaux des utilisateurs sont dans ce cas des moyens situés sur le territoire de la Communauté. Et d'autre part, Facebook y dispose aussi de bureaux. Mais à nouveau, subsiste une difficulté substantielle : comment déterminer pratiquement aux fins de quels traitements, ces moyens sont utilisés par Facebook?

58. – Par ailleurs, la société Facebook pourrait utiliser d'autres moyens si, collectant des informations «à partir d'autres sources»¹⁹⁴, elle accédait directement à des bases de données situées sur le territoire communautaire¹⁹⁵, aux fins de traitement. Ce qui est toutefois fort hypothétique eu égard au manque de précisions à ce sujet.

4. – *L'application cumulée des points a) et c) de l'article 4?*

59. – Selon les termes de l'article 4, soit le responsable de traitement est établi sur le territoire de la Communauté, et s'applique alors uniquement le paragraphe 1^{er}, a), soit tel n'est pas le cas, et c'est le paragraphe 1^{er}, c) qui entre en jeu. Donc vis-à-vis d'un même responsable, il est permis de considérer que ces deux dispositions ne peuvent pas s'appliquer cumulativement¹⁹⁶.

¹⁹⁰ Voy. notamment à ce sujet W.P. 148, pp. 11-12.

¹⁹¹ Voy. W.P. 56, pp. 10-13. Quant aux *cookies*, voy. toutefois, plus nuancé, C. KUNER, *op. cit.*, pp. 123-127.

¹⁹² En élargissant le propos à d'autres intervenants que la société Facebook, le cas du développeur d'une application traitant des données à caractère personnel pourrait par exemple être visé par l'article 4, §1^{er}, c), si son application était hébergée sur des serveurs situés sur le territoire de la Communauté.

¹⁹³ Dix-sept *cookies* sont placés sur l'ordinateur de l'utilisateur par Facebook.

¹⁹⁴ «Facebook a affirmé qu'elle ne recueillait pas de renseignements personnels de sources externes, mais qu'elle avait inclus [le passage de la politique de confidentialité à ce sujet] puisqu'il n'était pas exclu qu'elle le fasse à l'avenir», E. DENHAM, *op. cit.*, p. 69, n° 225.

¹⁹⁵ Voy. M.-H. BOULANGER *et al.*, *op. cit.*, p. 175.

¹⁹⁶ À ce sujet, voy. P.H. BLOK, *op. cit.*, pp. 301-302.

60. – Mais l'analyse doit systématiquement porter sur un traitement de données à caractère personnel, et non sur un responsable de traitements en général. Ce qui peut avoir une incidence déterminante quant au droit applicable selon le «degré de découpage» (en fonction des opérations techniques et des finalités) – par le juge – d'une opération globale de traitement, en une somme de traitements distincts¹⁹⁷.

61. – Une interprétation spécifique peut être proposée. Ainsi, pour un traitement particulier – par exemple via *cookies* – réalisé par un responsable de traitement dans le cadre des activités de son établissement dans un pays tiers – et pas de celles d'un établissement communautaire – mais pour lequel des moyens sont utilisés sur le territoire de la Communauté, les points a) et c) de l'article 4 devraient pouvoir s'appliquer cumulativement. Pour ce traitement, le responsable en cause serait considéré comme n'étant pas établi sur le territoire de la Communauté¹⁹⁸, et les dispositions s'appliqueraient concomitamment à lui¹⁹⁹.

B. – ARTICLES 25 ET 26 : FLUX TRANSFRONTIÈRES DE DONNÉES

62. – L'hypothèse de départ consiste en l'inapplicabilité de l'article 4 par rapport à un traitement de données : le responsable de traitement n'est pas considéré comme établi sur le territoire de la Communauté, et il n'utilise pas des moyens localisés sur le territoire européen. Tel pourrait par exemple être le cas lorsque Facebook traite les données des utilisateurs afin de personnaliser le fonctionnement du réseau social²⁰⁰ ou lorsqu'elle les conserve au-delà de leur suppression par ces utilisateurs. Il en serait ainsi aussi si les traitements de données impliqués par la fonctionnalité Social ads ne pouvaient être inclus dans les hypothèses de l'article 4 selon l'argumentation exposée précédemment²⁰¹. Le

¹⁹⁷ En effet, une opération peut être un traitement et un ensemble d'opérations peuvent aussi être un seul traitement (article 2, b) de la directive 95/46). La Cour de justice, dans le cas *Satamedia* (point 37), semble avoir une conception «globalisante» du traitement de données, réduisant un ensemble d'opérations à un seul traitement. Ce qui paraît logique dès lors qu'une seule finalité était poursuivie à l'occasion de l'opération globale (voy. d'ailleurs article 18, §1^{er}, de la directive 95/46). Assez logiquement, le «degré de découpage» de l'opération dépendrait des finalités poursuivies. Dans ce cas, il faudrait alors déterminer quand cesse une finalité pour que commence une autre. Dans le cas de *Facebook*, les finalités commerciale et – disons – de «réseau social» doivent-elles être distinguées où sont-elles les deux versants d'une même finalité – et donc d'une même opération globale de traitement – commerciale?

¹⁹⁸ Voy. en ce sens D. KORFF, *op. cit.*, p. 33, note 30.

¹⁹⁹ Ce raisonnement serait à nuancer s'il était transposé à une hypothèse où le responsable de traitement ne serait établi que sur le territoire de la Communauté, voy. *supra*, n^{os} 39 et s.

²⁰⁰ Par exemple en proposant à un utilisateur de devenir «ami» de personnes qu'il pourrait connaître ou de devenir «fan» d'une Facebook Page, comme certains de ses «amis» (dans cette dernière hypothèse, il s'agit concrètement d'une possibilité offerte par *ads* qui permet d'ajouter des Social Actions à une publicité).

²⁰¹ Voy. *supra*, n^{os} 48 et s.

régime des flux transfrontières de données à caractère personnel²⁰² consacré dans les articles 25 et 26 de la directive s'appliquerait alors; les utilisateurs communautaires envoient des données à caractère personnel aux États-Unis à partir de la Communauté²⁰³, aux fins de traitement, ayant préalablement dû veiller à ce que le traitement que constitue ce transfert soit licite²⁰⁴.

63. – Ce régime impose aux États membres d'empêcher les flux de données vers les États tiers n'assurant pas une protection adéquate, sauf application des exceptions consacrées dans l'article 26. La Commission peut par ailleurs décider qu'un pays tiers assure ou pas une protection adéquate, auquel cas les États membres doivent se conformer à cette décision²⁰⁵.

64. – Aux États-Unis, la société Facebook a adhéré aux Safe Harbor Principles²⁰⁶ ainsi qu'au TRUSTe Privacy Seal Program²⁰⁷. Et la Commission européenne a décidé que la protection offerte par ces principes était adéquate²⁰⁸. Les États membres doivent donc se conformer à cette décision.

65. – À la lecture de l'article 25 de la directive 95/46, une décision d'adéquation de la Commission ne devrait avoir *a priori* pour effet que de lever, pour les États membres, l'obligation d'empêcher les flux de données vers le pays tiers concerné. Toutefois, la logique du système conduit à penser qu'ils ne pourraient alors plus empêcher ces flux pour le motif d'inadéquation de la protection offerte par ce pays. C'est d'ailleurs ce qui

²⁰² Selon l'article 25 de la directive 95/46, le régime du «transfert» de données à caractère personnel «faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert» vers un pays tiers.

²⁰³ La politique de confidentialité les avertit de ce transfert. Par ailleurs, d'une part, je considère que la diffusion d'informations via un site Web, par un internaute, constitue un flux transfrontière de données. Voy. en ce sens T. LÉONARD et A. MENTION, *op. cit.*, pp. 96-98, et C. DE TERWANGNE, *op. cit.*, pp. 93-96. La Cour de justice, dans l'affaire *Lindqvist*, s'est par contre positionnée dans le sens contraire, voy. points 60-71. Et d'autre part, dans le cas d'espèce, les utilisateurs envoient de toute façon les informations à la société Facebook en tant que telle.

²⁰⁴ La soumission de l'utilisateur à la directive 95/46 est d'autant plus importante que cet utilisateur peut être à l'origine d'un flux de données vers un pays tiers.

²⁰⁵ Article 25, §§4 et 6 de la directive 95/46.

²⁰⁶ Pour une présentation des Safe Harbor Principles, voy. M. V. PÉREZ ASINARI et Y. POULLET, «Privacy, personal data protection and the Safe Harbor decision – From euphoria to policy : from policy to regulation...?», in *The future of transatlantic economic relations : continuity amid discord*, Florence, European University Institute, 2005, pp. 101-134; D. KORFF, *op. cit.*, pp. 248-296; C. MOAL-NUYTS, «Le transfert de données à caractère personnel vers les États-Unis conformément au droit européen», *Rev. trim. dr. eur.*, 2002, pp. 451-470; J. KEMNER, «De Safe Harbor Principles», *Computerr.*, 2001, pp. 73-77.

²⁰⁷ Voy. <http://www.truste.org/ivalidate.php?url=www.facebook.com&sealid=101>.

²⁰⁸ Décision (CE) n° 2000/520 de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil, relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, *J.O. L 215*, du 25 août 2000.

se dégage *a contrario* de la décision de la Commission relative aux Safe Harbor Principes, précisant des cas dans lesquels les autorités compétentes d'un État membre peuvent «suspendre les flux de données vers une organisation adhérant aux principes»²⁰⁹.

66. – La logique ne voudrait-elle pas également que le droit applicable au traitement ultérieur au flux soit celui de cet État? Ce à quoi conduirait une interprétation de l'article 4, à la lumière des articles 25 et 26, comme imposant une règle de conflit de lois bilatérale également pour les cas «plus» internationaux; un caractère universel lui serait reconnu à l'instar notamment du règlement Rome I. Le texte de la directive 95/46 ne vise toutefois clairement pas l'applicabilité du droit d'un État tiers²¹⁰. En outre, l'argumentation avancée pour considérer l'article 4 comme une règle de conflit bilatérale en ce qu'elle définirait l'applicabilité du droit des États membres ne vaudrait pas en l'espèce²¹¹.

67. – Si une telle règle n'est donc pas imposée par la directive, mais que les États ne peuvent tout de même pas interdire les flux transfrontières de données en cause, ne pourraient-ils pas «encadrer» ces flux par des mesures particulières, les «freinant» le cas échéant, voire aller, dans des cas marginaux, jusqu'à exiger l'application de leur droit au responsable de traitement établi dans le pays tiers? Une mesure nationale particulière serait de prévoir l'applicabilité du droit national au droit d'accès de la personne concernée²¹², ou de soumettre le responsable de traitement à une obligation d'information renforcée. Le droit applicable pourrait-il être déterminé, le cas échéant, en application des règles de conflit de lois en matière d'atteintes à la vie privée²¹³?

²⁰⁹ Voy. article 3, § 1^{er}, de la décision (CE) n° 2000/520, *op. cit.* Cela est toutefois «Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive 95/46/CE». D'où l'utilisation de l'article «des».

²¹⁰ La directive 95/46 ne se prête pas à une telle interprétation; elle ne vise que les droits des États membres, v. au sujet de certaines règles d'applicabilité communautaires en général, M. FALLON et S. FRANCO, «Towards Internationally Mandatory Directives for Consumer Contracts», in *Private Law in the International Arena – Liber amicorum Kurt Siehr*, La Haye, T.M.C. Asser Press, 2000, pp. 166-167. Or *quid si*, dans un cas où un responsable de traitement établi dans un «État tiers A» installe ses moyens de traitement aux États-Unis et y adhère aux Safe Harbor Principles pour traiter des données communautaires et contourner la législation de l'«État tiers A», la personne concernée entend bénéficier du droit de cet «État tiers A» au motif que le responsable de traitement y est établi? La directive 95/46 n'apporte pas de solution.

²¹¹ Voy. *supra*, n°s 39 et s. Notons qu'il n'y aurait ici plus d'application du principe de reconnaissance mutuelle.

²¹² Ce que pourrait garantir le fournisseur du réseau social. Il suffit de prendre l'hypothèse de la société Dailymotion garantissant un droit d'accès sur la base du droit français, voy. <http://www.dailymotion.com/register>.

²¹³ Signalons d'emblée que le règlement Rome II ne traite pas de la question du droit applicable aux «obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité», voy. article 1^{er}, § 2, g), du règlement (CE) n° 864/2007 du Parlement européen et du Conseil, sur la loi applicable aux obligations contractuelles, *J.O. L 199*, du 31 juillet 2007. Il faudrait se reporter à l'article 99, § 2, 1^o, du C.D.I.P.

Par contraste avec les «relations intracommunautaires», la marge de manœuvre des États membres serait cette fois plus grande, mais tout de même limitée par les règles de l'O.M.C.²¹⁴.

C. — DROIT NATIONAL ET EXTRATERRITORIALITÉ
DE LA DIRECTIVE 95/46

68. — C'est le droit national des États membres, transposant les dispositions précitées de la directive 95/46, qui, interprété conformément à la directive²¹⁵, s'appliquera en cas de litige. Et les législations nationales ne sont pas uniformes²¹⁶. Si la Belgique a adopté une disposition similaire à l'article 4 de la directive 95/46, d'autres États s'en sont écartés – le cas échéant irrégulièrement – plus «originellement».

69. — Par exemple, concernant l'établissement du responsable de traitement, les droits finlandais, suédois et grec ne font pas référence au critère du «contexte des activités»²¹⁷. La loi allemande est assez vague, s'appliquant à un responsable de traitement non établi dans un État membre de l'Union (ou de l'E.E.E.) qui collecte, traite ou utilise des données à caractère personnel en Allemagne, sans définir ces notions, ni renvoyer à l'utilisation d'équipements²¹⁸. La loi danoise s'applique quant à elle notamment au responsable d'un traitement établi dans un État tiers si, aux fins du traitement en cause, la collecte des données a lieu au Danemark²¹⁹. Enfin, la réglementation grecque, antérieurement, liait les responsables de traitement non établis en Grèce dès lors

²¹⁴ À ce sujet, voy. M.V. PÉREZ ASINARI, «Is there any Room for Privacy and Data Protection within the WTO Rules?», *The Electronic Communications Law Review*, 2002, pp. 249-280; Y. POULLET, «Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données», *Comm. Com. Elec.*, 2003, pp. 11-15. Voy. par contre L. BERGKAMP, «EU Data Protection Policy, The Privacy Fallacy : Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy», *Computer Law and Security Review*, 2002, pp. 39-40.

²¹⁵ C.J.C.E., 13 novembre 1990, *Marleasing s.a. c. La Comercial Internacional de Alimentacion SA*, C-106/89, *Rec.*, 1990, p. I-04135, point 8.

²¹⁶ Voy. à ce propos 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, et l'étude qui l'accompagne, intitulée «Analysis and impact study on the implementation of Directive EC 95/46 in Member States», disponible sur http://ec.europa.eu/justice_home/, en particulier pp. 6-7 et pp. 31-35.

²¹⁷ «Analysis and impact study on the implementation of Directive EC 95/46 in Member States», *op. cit.*, p. 6.

²¹⁸ Voy. § 1^{er}, (5) Bundesdatenschutzgesetz (stand : 15 November 2006), disponible en anglais à partir de http://www.bfdi.bund.de/cln_111/EN/DataProtectionActs/DataProtectionActs_node.html.

²¹⁹ Voy. § 4, (3), 2 du Act on Processing of Personal Data (as amended), disponible en anglais à partir de <http://www.datatilsynet.dk/english/>.

que les traitements en cause se rapportaient à des personnes établies sur le territoire grec²²⁰.

Dans ces hypothèses, contrairement à ce qui se dégage de l'interprétation présentée de la directive 95/46 – la Commission affirme d'ailleurs que des «plusieurs États membres devront modifier leur législation»²²¹ – l'applicabilité intégrale de cette directive à Facebook pour de nombreux traitements de données paraît beaucoup plus vraisemblable.

70. – Dans un cas tel celui de Facebook, qu'il s'agisse de défendre une interprétation large de l'article 4, d'adopter des dispositions additionnelles aux articles 25 et 26, ou encore de suivre une interprétation «globalisante» de la notion de traitement de données, se pose la question de l'extraterritorialité de la directive 95/46 et de la tension à laquelle sont confrontés législateurs et juges dans le domaine du «cyberspace et du commerce électronique»²²².

71. – Cette extraterritorialité²²³, intégrale ou partielle²²⁴, à penser conformément aux règles de l'O.M.C., pourrait être en l'espèce justifiée pour trois raisons. Premièrement, il n'est pas question que de prestations de service mais également de droits fondamentaux – vie privée et protection des données – et de réglementation d'ordre public; l'Union européenne et les États membres ont «le droit et le devoir» «de veiller au respect de la protection des données dans le commerce mondial»²²⁵. Relevons que lorsqu'il est question de l'application de la Convention européenne des droits de l'homme, le droit désigné par la règle de conflit de lois est susceptible de devoir être écarté s'il viole les droits garantis par la Convention²²⁶.

²²⁰ C. KUNER, *op. cit.*, pp. 114 et 116. D'autres auteurs avaient souligné cette spécificité, voy. A. LUCAS, J. DEVÈZE et J. FRAYSSINET, *op. cit.*, p. 94. Désormais, la loi grecque a été modifiée et fait référence à l'utilisation d'équipements, voy. article 3, §3, b), de la Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended), disponible à partir de <http://www.dpa.gr/>.

²²¹ Premier rapport..., *op. cit.*, p. 19. Ce que les Grecs ont fait.

²²² T. SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne – Une approche critique*, coll. Cahiers du C.R.I.D., Bruxelles, Paris, Bruylant, L.G.D.J., 2005, pp. 64-65. Voy. aussi W.P. 56, p. 3.

²²³ Parfois de mise aussi outre-Atlantique, voy. le Children's Online Privacy Protection Act de 1998.

²²⁴ Mais dépassant en tous cas le régime des flux transfrontières de données tel que prévu actuellement.

²²⁵ Y. POULLET, «Pour une justification...», *op. cit.*, p. 15.

²²⁶ Rappelons que les États parties à la Convention européenne des droits de l'homme «reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de cette Convention». Ce qui peut influencer sur le droit international privé et l'éventuelle éviction du droit d'un État tiers à la Convention, voy. notamment L. GANNAGÉ, «À propos de l'absolutisme' des droits fondamentaux», in *Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*, Paris, Dalloz, 2008, pp. 265-284. Sans entrer dans la réflexion requise à ce sujet, notons que le rattachement avec l'ordre juridique communautaire évoqué en l'espèce justifierait à tout le moins que la protection des données relève – dans la mesure où elle serait fondée par la C.E.D.H. dans

Deuxièmement, il est défendable de considérer que la Commission s'est fourvoyée en proclamant adéquate – politique et économie obligent – la protection garantie par les Safe Harbor Principles²²⁷, d'autant plus que leur mise en œuvre laisse à désirer²²⁸. L'effectivité de la protection qu'offrent les articles 25 et 26 de la directive est ainsi ébranlée, même si le droit américain peut toujours évoluer et changer la donne²²⁹.

Enfin troisièmement, il faut avoir égard à la nature du service en cause et à ses destinataires : un service de la société de l'information « à caractère personnel » dirigé vers le marché communautaire²³⁰, à l'occasion de la fourniture duquel l'utilisateur contracte avec la société Facebook²³¹. En outre, cet utilisateur sera également souvent résident habituel de la Communauté, et tout porte à croire qu'il recourra audit service à partir de la Communauté.

l'article 8 de la Convention européenne des droits de l'homme – d'un certain « ordre public de proximité », voy. p. 274 : P. MAYER souligne que le contrôle de la Cour européenne des droits de l'homme à cet égard devrait se borner à vérifier que l'État concerné « respecte les droits de l'homme dans toutes les situations qui lui sont essentiellement internes », P. MAYER, « La Convention européenne des droits de l'homme et l'application des normes étrangères », *Rev. crit. dr. internat. privé*, 1991, p. 664. Voy. également l'article 1^{er} de la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg, le 28 janvier 1981.

²²⁷ Pour des commentaires au sujet de ceux-ci, voy. notamment la position du parlement européen évoquée par D. ALONSO BLAS, « Universal Effects of the European Data Protection Directive », in *A Decade of Research @ the Crossroads of Law and ICT*, J. DUMORTIER, F. ROBBEN et M. TAEYMANS (éds), Bruxelles, De Boeck & Larcier, 2001, pp. 27-28 : L. EDWARDS citant A. CHARLESWORTH, L. EDWARDS, « Privacy and Data Protection Online : The Laws Don't Work? », in *Law and the Internet*, L. EDWARDS et C. WAELDE (éds), Oxford et Portland, Hart, 2009, pp. 454-455 ; J. FRAYSSINET, « La protection des données personnelles est-elle assurée sur l'Internet? », in *Le droit international de l'Internet*, G. CHATILLON (sous la dir. de), actes du colloque organisé à Paris, les 19 et 20 novembre 2001 par le ministère de la Justice, l'Université Paris I Panthéon Sorbonne et l'Association Arpeje, Bruxelles, Bruylant, 2002, p. 439 ; Groupe 29, avis 4/2000 sur le niveau adéquat de protection assuré par les « principes de la sphère de sécurité », 16 mai 2000 ; Y. POULLET, « Les Safe Harbor Principles – Une protection adéquate? », *Juriscom.net*, 17 juin 2000 ; A. ZINSER, « International data transfers between the United States and the European Union : are the procedural provisions of the Safe Harbor solution adequate? », *Computer Law & Security Report*, 2004, pp. 182-184.

²²⁸ Voy. J. DHONT, M.V. PÉREZ ASINARI et Y. POULLET, avec l'assistance de J.R. REIDENBERG et L.A. BYGRAVE, « Safe Harbor Decision Implementation Study », 19 avril 2004, disponible sur http://ec.europa.eu/justice_home/ ; J. DHONT, « De safe harbor-beginselen – De stand van zaken één jaar na de veilighavenstudie », *Computerr.*, 2006, pp. 150-158 ; J. GRANT, « International data protection regulation, Data transfer – Safe harbor », *Computer Law & Security Review*, 2005, p. 258.

²²⁹ Voy. par exemple le Personal Data and Privacy Security Act de 2009 introduit devant le Sénat américain, disponible sur <http://thomas.loc.gov/cgi-bin/query/z?c111 :S.1490>.

²³⁰ Au sujet d'hypothèses exclues du champ d'application de la directive 95/46, voy. Groupe de travail « article 29 », « L'avenir de la protection de la vie privée », Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, 1^{er} décembre 2009, pp. 10-11.

²³¹ Voy. *supra*, n^{os} 10-11, 7 et 16-18.

72. – Ces considérations plaident en faveur d’une application extraterritoriale plus large de la directive 95/46 – moyennant la satisfaction d’un critère d’applicabilité complexe mais garantissant un «lien étroit»²³² avec la Communauté – à un responsable de traitement tel que Facebook, finalement, pour tous les traitements de données, dont elle est responsable, impliquant des résidents habituels de la Communauté recourant à son service²³³. L’application de la loi nationale de protection des données d’un État membre – ou de certaines de ses dispositions – résulterait du jeu de règles spécifiques de rattachement ou d’applicabilité, voire, le cas échéant, de la clause d’exception d’ordre public²³⁴. Et signalons que la soumission d’un fournisseur de réseau social à ce droit ne lui infligerait pas une tâche impossible à réaliser; la conformité d’un réseau social à la directive 95/46 a déjà été constatée²³⁵.

Force est toutefois de constater que l’état actuel du droit communautaire ne le permettrait que partiellement, et encore au terme de difficultés pratiques et d’interprétation, le cas échéant substantielles et rebutantes. La réflexion à cet égard doit donc se poursuivre²³⁶.

Conclusion

73. – La présentation proposée du réseau social Facebook – service de la société de l’information «à caractère personnel» – permet d’identifier une société américaine disposant d’établissements sur le territoire de la Communauté, dirigeant ses activités

²³² Voy. par exemple art. 6, §2, de la directive (CEE) n° 93/13 du Conseil du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs, *J.O. L 95*, du 21 avril 1993.

²³³ Des difficultés demeurerait toutefois quant à la détermination du droit national applicable. Une solution concrète – inenvisageable en droit positif – serait de permettre au fournisseur d’un service tel qu’envisagé dans le présent propos de n’être soumis qu’au(x) droit(s) du ou des État(s) membre(s) avec le(s)quel(s) il entretiendrait les liens les plus étroits. Voy. aussi l’éventuelle utilité d’un principe de «*home country control*» évoqué par P.H. Blok à un autre sujet, P.H. BLOK, *op. cit.*, p. 45 et les références citées par l’auteur à la note 25.

²³⁴ Le droit d’un État tiers désigné comme applicable – par quelque méthode que ce soit –, le droit d’un État membre serait appliqué par le jeu de l’exception d’ordre public international (voy. cependant T.G.I. Paris, ord. réf., *op. cit.*) via le concept d’«ordre public de proximité», voy. sur cette notion et son lien avec, notamment, la directive 93/13 précitée, P. DE VAREILLES-SOMMIÈRES, «La communautarisation du droit international privé des contrats : remarques en marge de l’uniformisation européenne du droit des contrats», in *Le droit international privé : esprit et méthodes, Mélanges offerts en l’honneur de Paul Lagarde*, Paris, Dalloz, 2005, pp. 798-800. Il faut toutefois relever que la directive 95/46 n’est pas rédigée de la même façon que les directives au sujet desquelles l’auteur écrit.

²³⁵ Voy. Groupe 29, 11^e rapport annuel sur l’état de la protection des personnes à l’égard du traitement des données à caractère personnel dans l’Union européenne et les pays tiers, portant sur l’année 2007, 24 juin 2008, p. 88.

²³⁶ La Commission européenne a d’ailleurs souligné qu’il fallait poursuivre la réflexion au sujet de l’article 4 de la directive, voy. premier rapport..., *op. cit.*, p. 20.

vers cette dernière et poursuivant une finalité commerciale. Le service offert rassemble par ailleurs une multitude d'utilisateurs de nature très variée, censés être les cocontractants de Facebook, chacun revêtant potentiellement la qualité de responsable de traitement.

74. – Les limites de l'applicabilité territoriale de la directive 95/46 ont été illustrées. Son applicabilité intégrale à des traitements de données à caractère personnel dont Facebook est responsable est discutable. De manière générale, cette société semble principalement soumise au régime des flux transfrontières de données. Alors qu'une applicabilité plus large des principes de la directive 95/46 pourrait être souhaitée.

75. – En conclusion, dans un contexte tel que celui de Facebook et des réseaux sociaux présentant ses caractéristiques, les autorités communautaires et nationales, les dernières disposant d'une certaine marge de manœuvre, sont à tout le moins confrontées à un double défi : oser l'extraterritorialité de leur réglementation quand le besoin en est ressenti, tout en veillant à ce que la mise en œuvre de celle-ci ne nuise pas illégitimement aux règles du commerce international et aux droits et libertés fondamentaux en présence.