L'économie collaborative et la protection des données

Van Gyseghem, Jean-Marc

Published in:
Aspects juridiques de l'économie collaborative

Publication date:
2017

Document Version
le PDF de l'éditeur

L'économie collaborative et la protection des données : quel partage de données ?

Jean-Marc Van Gyseghem
Directeur de recherches au CRIDS[1]
Avocat au barreau de Bruxelles

Introduction

1. L'économie collaborative ou, dans sa version anglaise, la *sharing economy*, est un phénomène grandissant prenant dans la plupart des cas appui sur l'explosion de l'internet et des outils de communication tels que les smartphones.

L'objectif visé par ce type d'économie est le partage de l'usage d'un produit, d'un service entre différents acteurs[2].

Dans sa note du 2 juin 2016, la Commission européenne a défini le terme d'économie collaborative comme désignant :

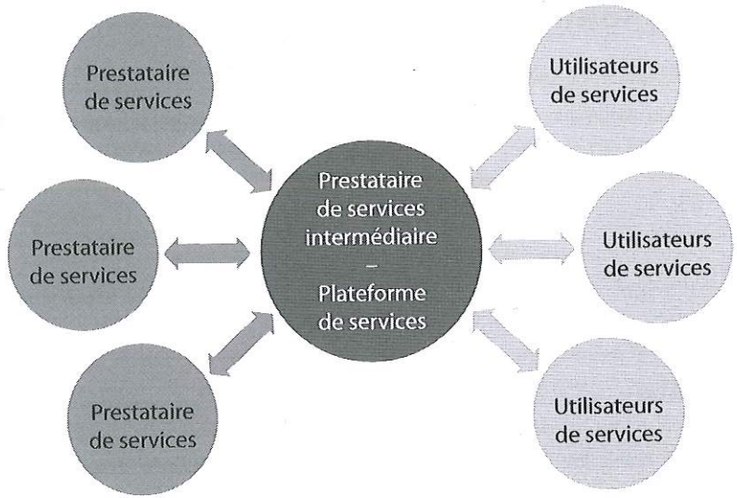
> « Aux fins de la présente communication, le terme "économie collaborative" désigne des modèles économiques où des plateformes collaboratives qui créent un marché ouvert pour l'utilisation temporaire de biens et de services souvent produits ou fournis par des personnes privées facilitent des activités. L'économie collaborative fait intervenir trois catégories d'acteurs : i) des prestataires de services, qui partagent des actifs, des ressources, du temps et/ou des compétences – il peut s'agir de personnes privées qui proposent des services sur une base occasionnelle ("pairs") ou des prestataires de services qui interviennent à titre professionnel ("prestataires de services professionnels") ; ii) des utilisateurs de ces services ; et iii) les intermédiaires qui mettent en relation – via une plateforme en ligne – les prestataires et les utilisateurs et qui facilitent les transactions entre eux ("plateformes collaboratives"). Les transactions réalisées dans le cadre de l'économie collaborative n'entraînent généralement pas de transfert de propriété et peuvent avoir un caractère lucratif ou non lucratif. »[3]

---

1 www.crids.eu.

2 Pour une analyse juridique, voy., entre autres, S. BRADBURN, *Les systèmes d'échange locaux. Contribution à l'étude juridique de l'économie collaborative*, Paris, Dalloz, 2017.

3 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions proposant un agenda européen pour l'économie collaborative, 2 juin 2016.



Trois acteurs interagissent donc :

- un prestataire de services ;
- un intermédiaire de services / une plateforme de services ;
- les usagers du service.

L'économie collaborative peut prendre place dans le cadre tant d'une volonté de lucre que de pure collaboration entre des individus dans une optique de « troc ».

Les précurseurs de ce type d'économie ont été, sans conteste, Uber, qui offre à ses clients une plateforme via laquelle ils peuvent solliciter un service lié aux transports, ou encore Airbnb, qui offre des biens immeubles à la location via sa plateforme de location.

L'utilisation d'une plateforme pour gérer un tel système de partage génère nécessairement un traitement de données à caractère personnel au sens du Règlement général sur la protection des données (RGPD ou règlement, ci-après) qui entrera, de façon définitive, dans notre paysage législatif le 25 mai 2018[4].

2. Par données à caractère personnel, l'on entend « toute information se rapportant à une personne physique identifiée ou identifiable ("personne concernée") » et qu'« est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son

4 Voy. également le commentaire article par article réalisé par Thierry Léonard et Didier Chaumont et disponible sur le site www.gdpr-expert.eu.

identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[5].

La personne concernée sera donc cette personne physique à laquelle se rapportent les informations. Il est utile de relever que le RGPD précise, en son considérant 14, que « la protection conférée par le [RGPD] devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel ». Le RGPD se veut donc indépendant de la notion de nationalité ou de résidence. En d'autres mots, le simple fait de se trouver sur le territoire de l'Union européenne suffirait à se trouver sous la protection du RGPD.

Nous attirons l'attention sur le fait que cette notion de personne concernée ne vise qu'une personne *physique* à l'exclusion des personnes morales. Cette limitation peut s'expliquer par le fait que le RGPD traite d'un droit fondamental qui, par définition, ne serait l'attribut que desdites personnes physiques[6]. Nous devons cependant préciser que, quand les données relatives à une personne morale se rapportent à leur tour à une personne physique, le règlement pourra s'appliquer[7].

Par ailleurs, la définition est extrêmement large dès lors qu'elle vise toute information sans aucune limitation. L'information peut donc être liée à la sphère privée comme publique. L'on doit relever que « le fait que les données soient relatives à un commerçant, un indépendant, une profession libérale ou l'administrateur d'une société » n'exclut pas l'application du règlement dès lors qu'il « ne fait pas de distinction entre le caractère public ou privé de la donnée. Le fait qu'elles se trouvent dans des registres publics accessibles au public n'exclut pas non plus son application. »[8]

Ces données à caractère personnel peuvent être le nom, le prénom, les adresses IP, un *log* ainsi que l'a considéré la Cour d'appel de Liège dans un arrêt du 22 octobre 2009[9], mais également la Cour de justice de l'Union européenne[10]. Des images vidéo

5 Art. 4, 1, du RGPD.

6 Pour une analyse de l'évolution de cette limite entre personne physique et personne morale, voy. M. Isgour, « Examen de la jurisprudence européenne récente en matière de droit à l'image des personnes physiques et d'image de marque des personnes morales », *in Droits de la personnalité*, Limal, Anthemis, 2013, pp. 47-97.

7 J.-Ph. Moiny et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 83 ; voy. également Comm. Courtrai (1re ch.), 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 100, confirmé par Gand, 6 janvier 2005, *T.G.R.-T.W.V.R.*, liv. 2, 2007, pp. 92-93. La Cour d'appel de Bruxelles a considéré que « le droit au respect de la vie privée bénéficie aussi, dans une certaine mesure, aux personnes morales. Dès lors, il peut être admis que le droit au respect de la vie privée des personnes morales englobe la protection de leurs secrets d'affaires. » (Bruxelles, 30 juin 2010, *J.L.M.B.*, 2011/25, p. 1184) Il semble cependant que la cour se soit limitée à l'article 8 de la Convention européenne des droits de l'homme et ne soit pas allée jusqu'à la loi « vie privée ».

8 J.-Ph. Moiny et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *op. cit.*, p. 83.

9 Liège (7e ch.), 22 octobre 2009, *R.D.T.I.*, n° 38/2010, pp. 95 et s.

10 CJUE, 24 novembre 2011, *Scarlet Extended c. SABAM*, C-70/10, ECLI:EU:C:2011:771, § 51.

peuvent également l'être[11]. Le Conseil d'État a également estimé, dans un arrêt du 27 octobre 2005, qu'« un test d'haleine entraîne la collecte d'une donnée à caractère personnel »[12].

3. Il faut, mais il suffit, par ailleurs que la personne physique soit identifiée ou identifiable. Si le premier terme est assez évident à comprendre, tel n'est pas le cas du second qui donne lieu à beaucoup de discussions.

Pour en comprendre la portée, nous devons nous reporter au considérant 26 du RGPD qui précise que :

> « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens *raisonnablement* susceptibles d'être utilisés par le *responsable du traitement* ou par *toute autre personne* pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. »[13]

Pour considérer qu'une personne physique est identifiable, le responsable du traitement devra donc vérifier si lui-même ou toute autre personne peut identifier ladite personne.

Dans une affaire *Patrick Breyer c. Bundesrepublik Deutschland*[14], la Cour a eu l'occasion de rappeler que le considérant 26 « fait référence aux moyens susceptibles d'être raisonnablement mis en œuvre tant par le responsable du traitement que par une "autre personne" »[15], ce qui implique donc qu'« il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'une seule personne »[16]. Elle a également reproduit un argument de l'avocat général qui avait précisé que les moyens mis en œuvre ne pouvaient pas être considérés comme raisonnables, « si l'identification de la personne concernée était interdite par la loi ou irréalisable en pratique, par exemple en raison du fait qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre, de sorte que le risque d'une identification paraît en réalité insignifiant »[17]. La Cour s'est ainsi interrogée sur la possibilité de combiner les adresses IP et des informations complémentaires permettant d'identifier la personne concernée et a conclu que « le fournisseur de

11 Voy. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A. & M.*, 2002, p. 198 ; voy. aussi Liège (6e ch.), 27 juin 2003, *R.D.T.I.*, 2004, n° 18, p. 105 et Mons (1re ch.), 2 mai 2005, *J.L.M.B.*, 2005/24, p. 1057.

12 C.E., 27 octobre 2005, arrêt n° 150.861, http://www.raadvst-consetat.be.

13 Nous soulignons.

14 CJUE, 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

15 *Ibid.*, § 43.

16 *Ibid.*

17 *Ibid.*, § 46.

services de médias en ligne dispose de moyens susceptibles d'être raisonnablement mis en œuvre afin de faire identifier, à l'aide d'autres personnes, à savoir l'autorité compétente et le fournisseur d'accès à Internet, la personne concernée sur la base des adresses IP conservées »[18].

La définition donnée par le RGPD est donc extrêmement large dès lors que, dès l'instant où quelqu'un, quel qu'il soit, pourra identifier la personne concernée, il s'agira d'une donnée à caractère personnel, sous réserve des limites fixées par la Cour de justice de l'Union européenne ci-dessus.

Imaginons, par exemple, qu'une société de statistique soit chargée par plusieurs chaînes de supermarchés de réaliser une enquête de taux de fréquentation de divers établissements afin de voir si les clients sont fidèles à une seule chaîne ou en fréquentent plusieurs. Pour ce faire, la société de statistique enregistre les plaques d'immatriculation des véhicules entrant dans les parkings des supermarchés pour ensuite analyser leur fréquentation. Au regard du RGPD, il s'agit de données à caractère personnel dès lors qu'un tiers peut identifier les propriétaires des véhicules, à savoir la DIV. Or, la société de statistique n'a pas accès aux registres de la DIV de telle manière que cela rend les moyens à mettre en œuvre déraisonnables pour identifier la personne physique se trouvant derrière le numéro d'immatriculation.

Il est donc utile d'analyser cette définition de manière contextuelle et en rapport avec la finalité du traitement. Cela permettrait de considérer que la société de statistique ne traite pas de données à caractère personnel et ne tomberait donc pas dans le champ d'application matériel du règlement.

4. La présente contribution va donc porter sur l'analyse de ces traitements de données à caractère personnel au regard des notions de finalité, de responsable de traitement, de sous-traitant et de transparence. Ces diverses questions sont d'autant plus prégnantes que les usages de données à caractère personnel sont variés.

I. Quelle utilisation des données au regard des finalités ?

5. Il est important, à ce stade-ci de la contribution, de préciser que tout traitement de données ne pourra se faire que dans le cadre d'une ou plusieurs finalités qui doivent, en vertu de l'article 5 du RGPD, être déterminées, explicites et légitimes. De cette finalité vont dépendre les données à caractère personnel qui vont être traitées par le responsable de traitement ou toute autre personne travaillant sous ses instructions et/ou pour son compte.

Nous devons noter que le principe de finalité est fondamental dans le RGPD, comme il l'a été dans la directive 95/46/CE relative à la protection des personnes physiques

18 *Ibid.*, § 48.

à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (directive 95/46, ci-après)[19].

D'emblée, nous constatons que l'article 5, 1, b, du RGPD donne les conditions, ou plutôt les caractéristiques de cette finalité sans pour autant les expliciter dans les considérants.

6. Le Groupe de travail de l'article 29 (Groupe 29, ci-après) a cependant publié un avis en 2013[20] dans lequel il reprend le principe de finalité en le décortiquant et en donnant, pour autant que faire se peut, des lignes directrices.

À titre de préambule, le Groupe 29 précise que la détermination de la finalité est une étape essentielle dans l'application de la réglementation sur la protection des données et la mise en œuvre de garde-fous en termes de protection pour tout traitement. En effet, la finalité va permettre de déterminer la raison d'être du traitement et l'objectif que le responsable de traitement veut atteindre. Cet objectif peut être précisé d'emblée, dès la collecte, mais peut également l'être ultérieurement, dans le cadre de ce qu'on appellera « le traitement ultérieur ».

Ainsi que l'ont précisé les professeurs Léonard et Poullet[21], la finalité est l'élément unificateur du traitement. En d'autres termes, c'est la finalité attachée à un ensemble d'opérations appliquées à des données à caractère personnel qui donnera à ces différentes opérations leur cohérence et permettra de conclure que l'ensemble forme un traitement de données.

À noter que répondre à la question de la finalité, c'est en réalité répondre à la question : « pourquoi » les données à caractère personnel sont-elles traitées ?

L'on doit cependant distinguer le traitement initial du traitement ultérieur ; traitements qui devront remplir les conditions fixées par l'article 5, 1, b, du RGPD qui précise que les finalités doivent être déterminées, explicites et légitimes.

A. Traitement initial

7. Le traitement initial, opposé donc à celui qui est ultérieur, se caractérise par le fait qu'il ne pourra se prévaloir, dans la majorité des cas, d'aucune exception en termes d'informations, de consentements ou d'autres droits liés à la personne concernée.

8. Le Groupe 29 a précisé que, par finalité déterminée, le règlement (et la directive 95/46/CE avant lui) implique que la finalité doit être définie avec suffisamment de précision pour permettre la mise en place de toutes mesures nécessaires à la protection des données mais également de délimiter le champ du traitement. La détermination

19 À ce sujet, voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, pp. 5 et s.

20 Groupe de travail « Article 29 », *Opinion 03/2013 on purpose limitation*, 2 avril 2013.

21 Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, pp. 377 et s.

des finalités requiert un travail très précis dès lors que, dans les hypothèses où un consentement est requis, ce consentement devra être donné pour l'ensemble des finalités déterminées préalablement[22].

Le seul allègement de ce principe de précision dans la détermination des finalités concerne la recherche. Dans cette dernière hypothèse, le considérant 33 du RGPD précise en effet que « les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet ».

La détermination de la finalité requiert un travail en interne du responsable du traitement, et ce, avant le démarrage du traitement lui-même qui souvent coïncide avec la collecte des données à caractère personnel. Le Groupe 29 précise cependant que la communication de cette finalité à la personne concernée ne doit pas être contre-productive par une longueur exagérée de description légale ou autre[23]. Il faut permettre à la personne concernée de se rendre compte de façon aisée de la raison pour laquelle ces données sont traitées.

Ce travail de précision est requis pour toutes les finalités du traitement qui n'ont pas de lien entre elles. Si, par contre, les différentes finalités pour lesquelles le responsable de traitement traite les données sont liées entre elles, il est utile de trouver une finalité globale mais néanmoins précise qui les reprend toutes. Cela doit toujours se faire dans une optique de simplicité dans la compréhension par la personne concernée ainsi que le suggère, de manière très adéquate et pragmatique le Groupe 29[24].

9. Une deuxième caractéristique de la finalité est le caractère explicite de cette dernière qui implique donc que la finalité doit être clairement expliquée à la personne concernée. Cela requiert un travail particulier dans le chef du responsable de traitement qui ne pourra en effet le rencontrer qu'à condition d'avoir procédé à une détermination précise de la finalité. Nous constatons donc que ces deux caractères – déterminé et explicite – de la finalité se nourrissent l'un l'autre dans un travail pédagogique dans le chef du responsable de traitement à l'égard de la personne concernée.

10. La finalité doit également être légitime, ce qui signifie que :

> « la finalité ne peut induire une atteinte disproportionnée aux intérêts de la personne concernée par les données, au nom des intérêts poursuivis par le responsable de traitement. La notion de légitimité invite donc à un examen de

22 Voy. art. 6, 1, a, du RGPD et le considérant 32.

23 Groupe de travail « Article 29 », *Opinion 03/2013 on purpose limitation*, *op. cit.*

24 *Ibid.*, p. 16.

proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées »[25].

Le législateur européen a retenu, dans le RGPD, des bases de légitimité qui sont reprises aux articles 6, 9 et 10 du RGPD. Il est utile de relever que ce renvoi d'article en article impose une méthodologie de lecture du règlement qui peut être résumée comme suit :

- vérifier que les données sont traitées de manière licite, loyale et transparente au regard de la personne concernée (art. 5, 1, a, RGPD) ;
- vérifier que les finalités sont déterminées, explicites et légitimes (art. 5, 1, b, RGPD) ;
- pour ce dernier point, appliquer les articles 6, 9 et 10 du RGPD selon le type de données à caractère personnel afin de pouvoir vérifier les bases de légitimé présumées ;
- dès cette dernière étape accomplie, revenir à l'article 5.

Ainsi, il s'agit d'« un jeu de piste » qui doit être « joué » dans cet ordre pour pouvoir arriver, autant que faire se peut, à une lecture correcte et aisée du RGPD.

Cette notion de légitimité renvoie également à la notion de compatibilité avec le droit existant dans sa large acceptation. En d'autres termes, la finalité qui sera fixée ne pourra être contraire à la législation existante, tant nationale qu'européenne.

11. En l'espèce, la finalité du traitement effectué par un opérateur d'économie collaborative sera la gestion, d'une part, des clients, mais également, d'autre part, des collaborateurs.

En ce qui concerne la gestion des collaborateurs, cela entre, en général, dans un traitement « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie » tandis que, pour ce qui est des clients, le traitement trouve sa base légale dans soit l'exécution d'un contrat de service entre l'opérateur et ce client, soit le consentement donné par le client dans le traitement de ses données dans une finalité d'offre de service. Il nous semble, en effet, que seules ces deux bases légales trouvent à s'appliquer dans les situations d'économie collaborative. Nous verrons, ci-après, qu'il peut en être autrement dans le cadre de traitement ultérieur.

Par ailleurs, ce type d'économie fait rarement intervenir des données particulières au sens de l'article 9 du RGPD dans la finalité initiale. Si, par contre, le traitement s'applique à des données particulières au sens de l'article 9 du RGPD, seul le consentement pourra servir de base dans le cadre d'une économie collaborative. En effet, la base contractuelle ne pourra être utilisée, dans cette hypothèse, qu'aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de :

- droit du travail ;
- sécurité sociale ;
- protection sociale.

[25] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, Bruxelles, Academia-Bruylant, 2005, p. 157 avec notes infrapaginales.

Or, il ne peut être considéré que les prestataires de services dans l'économie collaborative entrent dans une de ces catégories, de sorte que de telles données ne pourront être traitées sur cette base de licéité.

B. Traitement ultérieur

12. Après avoir précisé les caractéristiques de la finalité, l'article 5, 1, b, précise que les données collectées pour des finalités déterminées, explicites et légitimes ne peuvent pas être traités ultérieurement d'une manière incompatible avec lesdites finalités. Toute la question repose cependant sur la notion d'incompatibilité entre le traitement ultérieur et les finalités initialement fixées.

Il est habituellement considéré que le premier critère à prendre en compte est celui de la prévisibilité raisonnable dans le chef de la personne concernée. Cela revient à dire que si le traitement ultérieur présente un lien logique avec la ou les finalités initiales, la personne concernée peut raisonnablement s'attendre à ce traitement ultérieur. En conséquence de cette prévisibilité, l'on considérera compatible ce traitement ultérieur et donc légal.

Le règlement prévoit cependant une présomption de compatibilité avec les finalités initiales lorsqu'il s'agit d'un traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherches scientifiques ou historiques ou, encore, à des fins statistiques, tout en renvoyant à l'article 89, 1, dudit règlement.

Sous l'empire de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et transposant la directive 95/46, l'arrêté royal du 13 février 2001 exécutant cette loi prévoyait des dispositions particulières pour ce qui concernait le traitement ultérieur des données à caractère personnel à des fins historiques, statistiques ou scientifiques. Cependant, cet arrêté royal perdra de sa pertinence et même de sa force par l'entrée en vigueur du RGPD le 25 mai 2018.

Nous devons donc attendre que le législateur belge légifère par rapport à ce traitement ultérieur spécifique qui est effectué à des fins de recherches scientifiques ou historiques ou à des fins statistiques.

13. Dans le cadre des économies collaboratives, le prestataire de service pourra être tenté d'utiliser les données collectées dans le cadre de la finalité initiale de gestion des clients pour offrir des services à valeur ajoutée à des tiers tels que le profilage des clients ou le déplacement de ces mêmes clients dans une ville pour leur offrir des publicités ciblées et personnalisées en fonction de leur localisation.

14. Si le traitement ultérieur ne concerne pas de données particulières au sens des articles 9 et 10 du RGPD, il devra cependant respecter l'article 6.4 du règlement qui indique des conditions dans lesquelles un traitement ultérieur est possible à « une

fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ».

Pour rappel, le prestataire de service, que ce soit le prestataire lui-même ou l'intermédiaire, traite des données dans le cadre d'un service déterminé. Si la finalité ultérieure n'est pas du tout liée à cette finalité du traitement initial, il sera difficile de considérer qu'il y a compatibilité entre les deux finalités au moyen des critères mentionnés par cet article 6.4, à savoir :

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ;
d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

15. Le traitement ultérieur pourrait également concerner des données telles que l'analyse des déplacements des clients révélant des appartenances religieuses, politiques ou encore des informations relatives à la santé, et ce, uniquement à travers l'analyse de ces déplacements ou des services demandés. Le traitement ultérieur concernerait alors des données particulières au sens de l'article 9 du RGPD et serait soumis à des règles de légitimité particulières dès lors que le règlement, et la directive 95/46 avant lui, assure une protection accrue à ces données qui sont considérées comme sensibles *in se*.

Ainsi, un arrêt a été rendu par la Cour constitutionnelle dans le cadre d'une requête en annulation déposée contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru.

La Cour constitutionnelle a considéré que :

> « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions soient posées qui ne sont pas pertinentes ou qui sont excessives et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité »[26].

Elle a ainsi clairement rappelé que la proportionnalité devait être analysée au niveau des données afin d'éviter que des données non nécessaires à la finalité ne soient traitées.

La Cour européenne des droits de l'homme a également précisé que :

> « Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R(87)15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police). »[27]

Au niveau du droit interne, l'article 6.1 de la loi du 4 avril 2014 relative aux assurances stipule que :

> « Le médecin choisi par l'assuré peut remettre à l'assuré qui en fait la demande, les certificats médicaux nécessaires à la conclusion ou à l'exécution du contrat. Ces certificats se limitent à une description de l'état de santé actuel.
>
> Ces certificats ne peuvent être remis qu'au médecin-conseil de l'assureur. Ce dernier ne peut communiquer aucune information non pertinente eu égard au risque pour lequel les certificats ont été établis ou relative à d'autres personnes que l'assuré.
>
> L'examen médical, nécessaire à la conclusion et à l'exécution du contrat, ne peut être fondé que sur les antécédents déterminant l'état de santé actuel du candidat-assuré et non sur des techniques d'analyse génétique propres à déterminer son état de santé futur.
>
> [...]. »

L'on constate que la collecte de données médicales est particulièrement réglementée pour éviter que des tiers désireux de recueillir ce type d'information n'exercent des

[26] C.C., 10 novembre 2011, n° 166/2011, B.16.7, www.const-court.be.
[27] Cour eur. D.H., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, req. n°s 30562/04 et 30566/04, § 103, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052.

pressions sur les personnes concernées afin d'obtenir des informations qui, certes, leur seront bien utiles, mais peuvent se révéler disproportionnées aux yeux du législateur. Nous pouvons, à notre sens, y intégrer toutes les données particulières précisées aux articles 9 et 10 du RGPD.

Il est également utile de relever que la Cour européenne des droits de l'homme de Strasbourg a considéré que « les informations personnelles relatives à un patient appartiennent à sa vie privée »[28] et qu'« il est primordial d'avoir des règles claires et détaillées en matière de divulgation d'informations médicales confidentielles et qui offrent des garanties suffisantes contre le risque d'abus et d'arbitraire »[29]. « La Cour répète à cet égard que la protection des données à caractère personnel, en ce compris les informations médicales, est d'une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale. »[30]

De plus, le traitement ultérieur de telles données particulières pourrait être considéré comme incompatible avec le traitement initial qui, pour rappel, est lié à une finalité de service. Cette incompatibilité imposera au responsable du traitement de considérer celui-ci comme initial avec, comme corollaire, le respect de toutes les obligations liées à ce statut.

16. Par ailleurs, la personne concernée – le client en l'espèce – devrait recevoir une information préalable afin de pouvoir exercer, le cas échéant, ses droits tels que fixés par le RGPD. Le considérant 39 du règlement ne dit rien d'autre en précisant que « le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées »[31].

La Professeure de Terwangne précise également que :

> « on ne peut communiquer les données à caractère personnel que l'on traite à n'importe qui ni pour n'importe quel motif. Toute communication de données doit respecter le principe de finalité. Cela implique que l'on ne peut communiquer les données qu'aux personnes et que dans les cas qui découlent des finalités de collecte des données ou qui sont compatibles avec ces finalités.
>
> C'est donc en tenant compte de la finalité initiale du traitement de données que l'on saura à qui on peut transmettre les données. Toute opération de mise à disposition des données devra se faire de manière compatible avec cette finalité initiale »[32].

28 J. Herveg, « Chronique de jurisprudence », *R.D.T.I.*, 2015, n^os^ 59-60, p. 94.
29 *Ibid.*
30 *Ibid.*
31 Considérant 39 du RGPD.
32 C. de Terwangne et J.-M. Van Gyseghem, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *in Vie privée et données à caractère personnel*, Bruxelles, Politea, 2013, feuillets mobiles.

Nous constatons donc que le prestataire de service sera, dans la majorité des cas, limité dans le traitement des données à caractère personnel des clients sans une information claire et précise de ce dernier et surtout son consentement ou, à tout le moins, un droit d'opposition selon les cas.

17. Certains lecteurs peuvent légitimement se poser la question du type de traitement ultérieur pouvant être effectué en matière d'économie collaborative. Comme exemple, nous pouvons prendre celui d'établissement d'un profil des utilisateurs du service afin de pouvoir évaluer les éventuels risques (santé, violence, quartier défavorisé, etc.) dans leur prise en charge et pouvoir adopter une attitude spécifique à leur égard en majorant les tarifs par exemple.

Il s'avère qu'un tel profilage se révélera possible s'il est, par exemple, nécessaire à la conclusion ou à l'exécution du contrat de transport ou qu'il a obtenu le consentement de la personne concernée. En contrepartie, le responsable de traitement devra mettre en « œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes [de l'assuré], au moins du droit de la personne concernée d'obtenir une intervention humaine de [sa] part, d'exprimer son point de vue et de contester la décision »[33] qui serait prise sur la base de ce profilage.

Ce profilage, ou à tout le moins les décisions qui en découleront, ne pourra s'effectuer sur les données particulières telles que celles relatives à la santé ou aux infractions, à moins qu'il y ait eu consentement de la personne concernée[34]. Dans cette hypothèse, le prestataire du service ou le prestataire intermédiaire devra mettre en place « des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes »[35] de la personne concernée.

II. Quels sont les acteurs et quels sont leurs statuts au regard du RGPD ?

18. Dans le contexte de l'économie collaborative, la difficulté sera d'établir le rôle que chaque acteur devra jouer avec, d'une part, un responsable de traitement qui nous reste à déterminer et, d'autre part, la personne concernée et l'éventuel sous-traitant.

La difficulté réside dans le fait que l'économie collaborative fait intervenir, selon la Commission européenne[36], divers acteurs allant du prestataire de service collaboratif au prestataire mettant en place la plateforme d'échange, en passant par le client.

33 Art. 22.3 du RGPD.
34 Les autres exceptions ne peuvent, à notre estime, s'appliquer dans le cadre de l'économie collaborative.
35 Art. 22.4 du RGPD.
36 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions proposant un agenda européen pour l'économie collaborative, 2 juin 2016.

La personne concernée sera, ainsi que cela a déjà été explicité en termes d'introduction, tant les éventuels collaborateurs que les clients eux-mêmes. Dans le cadre de la présente contribution, nous n'avons pris en considération que la situation du client en tant que personne concernée, statut qui a déjà été analysé.

Ainsi, dans cette partie-ci de la contribution, nous allons, dans un premier temps, analyser les aspects concernant le responsable de traitement, pour, dans un second temps, examiner ceux du sous-traitant.

A. Responsable de traitement

19. Un responsable de traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »[37]. Le RGPD précise également que « lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre »[38].

Dans le cadre de la présente contribution, seul le premier alinéa nous intéresse dès lors qu'il donne les trois critères permettant de déterminer le responsable de traitement, à savoir la détermination (1) des finalités (2) et des moyens (3).

Le Groupe 29 a considéré qu'« être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres »[39]. Il s'agira bien souvent d'une analyse factuelle, qui obligera le juge, par exemple, à vérifier si le responsable du traitement peut être considéré comme tel au regard de sa capacité de détermination qui « se déduira généralement d'une analyse des éléments factuels ou des circonstances de l'espèce : il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions "pourquoi ce traitement a-t-il lieu ?" et "qui l'a entrepris ?" »[40].

Outre cette capacité de déterminer, il faut encore qu'il y ait détermination des finalités et des moyens.

Selon le Groupe 29 :

> « On peut en outre affirmer que la détermination des finalités et des moyens revient à établir respectivement le "pourquoi" et le "comment" de certaines activités de traitement. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le "pourquoi" et le "comment" pour être qualifiée de responsable du traitement.
>
> [...]
>
> Lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable du traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant. Ces définitions prennent tout leur sens lorsque divers acteurs interviennent dans le traitement de données à caractère personnel et qu'il est nécessaire de déterminer lesquels d'entre eux sont responsables du traitement (seuls ou conjointement avec d'autres) et lesquels sont à considérer comme des sous-traitants, le cas échéant. »[41]

Par finalité telle que nous l'avons précédemment analysée, l'on entend l'objectif poursuivi par le responsable de traitement, le « pourquoi » évoqué par le Groupe 29.

Les moyens qui, pour leur part, expriment la façon par laquelle on atteindra l'objectif/la finalité pourront être techniques mais aussi organisationnels.

L'on doit également noter que, pour recevoir cette qualification de responsable du traitement, « il n'est pas nécessaire que cette personne dispose d'un pouvoir de contrôle complet sur tous les aspects du traitement »[42].

Au terme d'une telle analyse, la Cour d'appel de Mons a considéré qu'un détective privé devait être qualifié de responsable du traitement au motif qu'il a établi un rapport contenant des données à caractère personnel en utilisant un logiciel de traitement de texte[43]. Cette analyse est cependant contestable dès lors qu'un détective pourrait être considéré comme agissant pour le compte d'un tiers et sous ses instructions, ce qui est les attributs d'un sous-traitant ainsi que nous verrons ci-dessous.

À noter que cette qualité de responsable de traitement peut être partagée.

20. Dans le cadre de l'économie collaborative, le rôle de responsable du traitement peut être rempli par différents acteurs, à savoir tant le prestataire de service que le prestataire intermédiaire mettant à disposition une plateforme, ou encore le client qui pourra également être fournisseur de service ainsi que nous le verrons ci-après.

Nous devons ainsi procéder à l'analyse de chacun des intervenants afin de pouvoir identifier le responsable du traitement au regard des critères de détermination repris et expliqués ci-dessus.

37 Art. 4, 7, du RGPD.

38 *Ibid.*

39 Groupe de travail « Article 29 », *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.

40 *Ibid.*

41 *Ibid.*, p. 14.

42 CJUE, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, conclusions de l'avocat général du 24 octobre 2017, point 62, http://curia.europa.eu.

43 Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, pp. 80 et s.

21. Dans un premier temps, il convient de poser la question du « pourquoi », c'est-à-dire de la personne qui va déterminer la finalité du traitement.

La question va s'avérer, ainsi que nous l'avons déjà relevé, extrêmement factuelle et devra prendre en compte l'influence réelle tel que cela l'a été dans le cadre de l'affaire *SWIFT* qui se présentait comme étant un service de messagerie électronique pour la transmission de messages confidentiels entre institutions financières.

À ce titre, il était soutenu que SWIFT remplissait une fonction de sous-traitance[44] dès lors qu'elle ne posait des actions qu'au nom et pour le compte de ses clients. Il s'est cependant avéré que SWIFT décidait, de manière autonome, du niveau d'informations fournies aux institutions financières en relation avec le traitement[45].

Par ailleurs, et outre d'autres éléments propres à la qualité du responsable de traitement, le Groupe 29 a considéré que SWIFT négociait et rompait « en toute autonomie ses accords de services » et rédigeait et modifiait « ses divers documents contractuels et ses diverses politiques qui forment les moyens pratiques et juridiques de ses opérations »[46].

22. Au niveau de l'analyse du système d'économie collaborative, il est intéressant de rapprocher cette analyse concernant SWIFT avec l'avis rendu par l'avocat général près la Cour de justice de l'Union européenne dans l'affaire *Asociacioñ Profesional Elite Taxi contre Uber Systems Spain*[47].

Dans cette affaire, pendante à l'heure actuelle devant la Cour, l'avocat général, au terme d'une analyse de l'activité de la société Uber, a considéré que :

> « Uber exerce un contrôle sur tous les aspects pertinents d'un service de transport urbain : sur le prix, bien évidemment, mais également sur les conditions minimales de sécurité par des exigences préalables concernant les chauffeurs et les véhicules, sur l'accessibilité de l'offre de transport par l'incitation des chauffeurs à exercer aux moments et aux endroits de grande demande, sur le comportement des chauffeurs au moyen du système d'évaluation et, enfin, sur la possibilité d'éviction de la plateforme. [...] Uber contrôle donc les facteurs économiquement pertinents du service de transport offert dans le cadre de sa plateforme. »[48]

Il a conclu son raisonnement en excluant que « Uber soit considéré comme un simple intermédiaire entre les chauffeurs et les passagers » en estimant que « les chauffeurs qui roulent dans le cadre de la plateforme Uber n'exercent pas une activité propre qui existerait indépendamment de cette plateforme. Au contraire, cette activité peut exister uniquement grâce à la plateforme, sans laquelle elle n'aurait aucun sens »[49].

44 Voy. ci-dessous pour ce concept.

45 Groupe de travail « Article 29 », *Avis 10/2006 sur le traitement des données à caractère personnel par la société de télécommunication inter bancaire mondiale (SWIFT)*, 22 novembre 2006, p. 12.

46 *Ibid.*, pp. 12 et 13.

47 CJUE, *Asociacioñ Profesional Elite Taxi c. Uber Systems Spain*, C-434/15, conclusions de l'avocat général Maciej Szpunar du 11 mai 2017, ECLI:EU:C:2017:364.

48 *Ibid.*

49 *Ibid.*

L'on constate donc que, dans le cadre d'une économie collaborative, ce type de prestataire intermédiaire de service a une maîtrise totale sur le système et, partant, sur la finalité du traitement des données à caractère personnel effectué qui est intrinsèquement lié à son activité économique. Cette maîtrise nous semble devoir donc être considérée comme une réelle détermination des finalités par cet intermédiaire ; finalité qui est une prestation de service et même de transport dans le cas d'Uber selon l'avocat général avec, en corollaire, un traitement des données sans lequel le service ne pourrait être fourni.

23. Il s'agit à présent de vérifier si cet intermédiaire détermine également les moyens pour atteindre la finalité fixée. Pour ce faire, il nous paraît logique que l'on adopte une analyse similaire à celle développée dans le cadre de la détermination de la finalité.

Il ne peut être contesté que ce prestataire de service intermédiaire qui détermine déjà les finalités du traitement – qui pour rappel est l'offre de service, à tout le moins pour ce qui concerne la finalité initiale – détermine également les moyens mis en œuvre pour atteindre ladite finalité. Ces moyens sont aussi divers que la mise en place de la plateforme elle-même, mais également des « conditions minimales de sécurité par des exigences préalables concernant les chauffeurs et les véhicules, sur l'accessibilité de l'offre de transport par l'incitation des chauffeurs à exercer aux moments et aux endroits de grande demande, sur le comportement des chauffeurs au moyen de système d'évaluation et, enfin, sur la possibilité d'éviction de la plateforme »[50].

L'on ne peut donc nier que le prestataire intermédiaire est en réalité le pivot de tout le service offert, mais également du traitement des données à caractère personnel nécessaire à ce service en déterminant, de la même manière, les moyens nécessaires pour atteindre la finalité.

À noter que, pour mettre en œuvre ces moyens, le prestataire de service intermédiaire utilise des sous-traitants, ainsi que nous le verrons ci-dessous.

En conclusion et dans les conditions reprises ci-dessus, nous pourrons considérer cet intermédiaire de service comme le responsable de traitement au sens du RGPD[51]. Ce sera le cas dans la majorité des cas d'économie collaborative.

24. Nous pourrions cependant avoir, dans certaines situations, un intermédiaire qui n'offre qu'un service de fourniture de plateforme sans exercer un quelconque contrôle sur le traitement de données outre qu'une gestion classique d'intermédiaire[52] et sans déterminer les finalité et moyen. N'étant plus responsable du traitement alors que des traitements de données sont cependant effectués, il faudra déterminer l'acteur du système qui remplit cette fonction.

50 *Ibid.*

51 À noter que, dans leurs *privacy policies*, tant Uber qu'Airbnb se considèrent comme responsable de traitement.

52 Droits d'accès, portefeuille virtuel, etc.

Dans ce cas de figure-ci, cette fonction sera, en réalité, exercée par le prestataire de service lui-même « qui partagent des actifs, des ressources, du temps et/ou des compétences »[53], c'est-à-dire la personne privée ou professionnelle qui offre le service final. Nous pouvons penser au Système d'Échange Local (SEL, en abrégé)[54] qui met en place une plateforme pour permettre à des particuliers d'échanger des services, des objets ou même des savoirs via une monnaie d'échange[55]. En effet, ce fournisseur de service utilisera l'intermédiaire de service (la plateforme) dans la mise en œuvre des moyens qu'il aura, lui-même, déterminés préalablement tout comme les finalités. Il sera donc responsable du traitement.

Cette situation n'est cependant pas anodine en termes de protection des données à caractère personnel. En effet, si le responsable du traitement est une personne physique et que le traitement n'est effectué que « dans le cadre d'une activité strictement personnelle ou domestique », il ne sera pas soumis au RGPD.

Pour comprendre ces notions d'« activité strictement personnelle ou domestique »[56], l'on doit se reporter au considérant 18 qui précise que le règlement :

> « ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités »[57].

Dans l'affaire *Lindqvist*, l'avocat général avait encore précisé que « cette catégorie recouvre uniquement des activités [...] manifestement privées et confidentielles, destinées à ne pas sortir de la sphère personnelle ou domestique des intéressés »[58].

Il est intéressant de se référer à ce qu'écrit la Professeure de Terwangne à ce propos :

> « La sphère personnelle peut être définie en faisant intervenir différents critères. Parmi ces critères, on trouve celui retenu par la Cour de justice de l'Union européenne dans son arrêt *Lindqvist*[59] et repris par la Cour à plusieurs reprises par la suite. La Cour de justice de l'Union européenne a commencé par dire

53 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions proposant un agenda européen pour l'économie collaborative, 2 juin 2016.

54 www.sel-lets.be/.

55 Système d'Échange Local de Temps. X unités SEL = 1 heure de service.

56 À noter que la version anglaise du règlement parle de « in the course of a purely personal or household activity ».

57 Considérant 18 du RGPD.

58 CJCE, 6 novembre 2003, *Lindqvist*, C-101/01, conclusions de l'avocat général Antonio Tizzano du 19 septembre 2002, ECLI:EU:C:2002:513.

59 CJCE, 6 novembre 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

> que l'exception doit être interprétée comme "visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers"[60]. »[61]

25. Dans le cadre de l'économie collaborative, peut-on considérer que le particulier traitera les données à caractère personnel dans le cadre d'une activité strictement personnellle ou domestique ? Il nous semble que la prestation de service s'inscrivant dans un système d'échange ne peut être considérée comme s'inscrivant en dehors d'une visée économique, d'autant plus que le système utilise une monnaie d'échange, le SELT. S'il est vrai qu'il n'y a pas de payement au sens littéral du terme, l'on ne peut pas nier qu'il y a un payement sous forme de service réciproque ou de monnaie virtuelle d'échange organisé via une plateforme servant à permettre l'offre et la demande de se rencontrer. Eu égard à cet élément, l'on ne peut que considérer que l'activité s'inscrit dans une activité économique au sens large du terme et surtout au sens du RGPD.

Comme conséquence de cette qualification, le traitement de données à caractère personnel lié à cette activité entre dans le champ d'application matériel du RGPD. En corollaire, le particulier sera considéré comme responsable du traitement avec toutes obligations qui en découlent, dont, entre autres, le respect des droits de la personne concernée. Ce qui sera évidemment original dans le cadre de ce type d'économie collaborative est le fait que chaque participant cumulera la qualité de personne concernée avec celle de responsable du traitement éventuellement conjoint.

B. Sous-traitant

26. Un second acteur important dans un traitement de données à caractère personnel sera le sous-traitant qui intervient souvent dans la mise en œuvre des moyens préalablement déterminés par le responsable de traitement.

Le RGPD le définit comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[62]. Ce sous-traitant n'est pas placé sous l'autorité directe du responsable de traitement[63] tel que cela ressort de l'analyse de la définition du « tiers » qui distingue le sous-traitant de cette personne placée sous l'autorité directe du responsable de traitement[64]. En d'autres termes, un sous-traitant ne pourra se trouver, pour les tâches liées à la sous-traitance concernée, dans un contrat de travail ou dans une relation hiérarchique avec le responsable de traitement. Bien souvent, le

60 *Ibid.*, point 47.

61 C. DE TERWANGNE, « L'exception concernant les traitements de données à des fins personnelles et domestiques de la directive 95/46 relative à la protection des données : note d'observations sous Cour de justice de l'Union européenne (4e ch.), 11 décembre 2014 », *R.D.T.I.*, 2015, n° 58, pp. 39 à 51.

62 Art. 4, 8, du RGPD.

63 La directive 95/46 était plus précise à ce niveau-là.

64 Art. 4, 10, du RGPD.

sous-traitant interviendra au niveau de la mise en œuvre des moyens déterminés par le responsable du traitement pour atteindre les finalités dès lors qu'il sera fait appel à lui pour ses compétences particulières. Ce sera le cas de fournisseurs de services internet tels que les fournisseurs de *cloud computing*[65].

27. Dans le cadre de l'économie partagée, il faudra distinguer deux hypothèses déjà analysées ci-dessus, à savoir celle dans laquelle le prestataire de service intermédiaire est le responsable du traitement et celle dans laquelle le prestataire de service revêt ce rôle de sous-traitant.

Si le prestataire intermédiaire est considéré comme responsable de traitement tel que c'est le cas dans le système Uber, y a-t-il un sous-traitant travaillant sous ses instructions au niveau du traitement de données à caractère personnel ? Il nous semble, à l'analyse du système développé par Uber, que les sous-traitants travaillant pour son compte seront les chauffeurs. En effet, ces derniers produisent des données pour le compte d'Uber étant, par exemple, les points de départ et d'arrivée de la course, le payement, etc. Par ailleurs, ces chauffeurs ne traiteront pas les données pour leur propre compte mais exclusivement pour celui d'Uber.

Par contre, si le prestataire de service est considéré comme responsable de traitement tel que c'est le cas des SEL, le sous-traitant sera alors le prestataire de service intermédiaire qui met à disposition une plateforme d'échange et, éventuellement, d'autres services annexes tels que le portefeuille virtuel.

28. Si la sous-traitance était peu traitée par la directive 95/46, il n'en est pas de même pour le RGPD qui lui consacre plusieurs articles en augmentant également les obligations du sous-traitant.

La première obligation, qui est essentielle, est l'existence d'un contrat[66] entre le responsable de traitement et le sous-traitant à défaut de tout autre acte juridique ; contrat qui doit prévoir un certain nombre de points tels que la mise en place de mesures de sécurité adéquates ou le fait que le sous-traitant ne peut traiter les données que sur instruction du responsable du traitement.

Par ailleurs, le sous-traitant est tenu d'informer « immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »[67]. Qu'en est-il du chauffeur d'Uber qui communique des données sensibles à Uber telles que des destinations révélant des informations particulières liées à la religion ou à la santé alors que ces informations ne sont pas

65 Voy. à ce propos, J.-M. Van Gyseghem, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, n° 42, pp. 35-50. Voy. également Groupe de travail « Article 29 », *Avis 05/2012 sur l'informatique en nuage*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

66 Art. 28, 3, du RGPD.

67 *Ibid.*

nécessaires à la finalité initiale mais bien à une finalité ultérieure ? Doit-il signaler que cette instruction est contraire au RGPD ? À notre sens, la réponse est affirmative même si le RGPD ne détermine pas l'attitude que le responsable du traitement doit adopter par rapport à la suite à apporter à un tel signalement.

De plus, le sous-traitant devra notifier au responsable du traitement toute faille de sécurité afin que ce dernier puisse remplir sa propre obligation de notification à l'égard de l'autorité de contrôle et, le cas échéant, de la personne concernée.

Nous avons quelques doutes quant au respect de ces diverses obligations, parmi d'autres que la présente contribution ne nous permet d'analyser, tant par le responsable de traitement que par le(s) sous-traitant(s) dans l'univers de l'économie collaborative.

III. Quelle transparence au regard du (des) traitement(s) ?

29. L'un des principes fondamentaux du RGPD est la notion de transparence de tout traitement à l'égard de la personne concernée. Cette transparence est, évidemment, tempérée par le devoir de confidentialité à l'égard des tiers.

Ce principe se retrouve à divers niveaux, à commencer par l'obligation d'informer la personne concernée. Ainsi, le considérant 39 rappelle que :

> « le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples ».

Cette notion est transcrite dans l'article 4, 1, a, du RGPD et, au niveau de l'information, dans les articles 12 et suivants du RGPD. Ainsi, le responsable de traitement doit prendre « des mesures appropriées pour fournir toute [l']information [prévue par le RGPD] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant »[68].

30. L'obligation de transparence donne également naissance aux droits accordés à la personne concernée avec, en premier lieu, celui d'accès qui est fondamental pour cette dernière afin qu'elle puisse procéder à diverses vérifications dont bien évidemment celle de savoir si des données à caractère personnel la concernant sont traitées. Si la réponse est positive, elle pourra alors en prendre connaissance et s'assurer que le traitement est conforme aux finalités annoncées ainsi qu'au RGPD.

68 Art. 12, 1, du RGPD.

De ce premier droit qui est, en quelque sorte, une porte d'entrée au traitement pour la personne concernée, découle l'exercice d'autres droits tels que celui de rectification, d'opposition, etc.

Il est intéressant de relever que la Cour de justice de l'Union européenne a considéré, dans un arrêt du 7 mai 2009 que :

> « 49. Ce droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés. Ainsi qu'il est énoncé au quarante et unième considérant de la directive, afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement.
>
> 50. À cet égard, l'article 12, sous a), de la directive prévoit un droit d'accès aux données de base ainsi qu'à l'information sur les destinataires ou les catégories de destinataires auxquels ces données sont communiquées.
>
> 51. Ce droit d'accès est nécessaire pour permettre à la personne concernée d'exercer les droits visés à l'article 12, sous b) et c), de la directive, à savoir, dans le cas où le traitement de ses données ne serait pas conforme à cette directive, celui d'obtenir que le responsable du traitement rectifie, efface ou verrouille ses données [sous b)] ou qu'il notifie aux tiers auxquels les données ont été communiquées ces rectification, effacement ou verrouillage, si cela ne s'avère pas impossible ou ne présuppose pas un effort disproportionné [sous c)].
>
> 52. Ce droit d'accès est également nécessaire pour permettre à la personne concernée d'exercer le droit d'opposition au traitement de ses données à caractère personnel visé à l'article 14 de la directive ou le droit de recours en cas de dommage subi prévu aux articles 22 et 23 de celle-ci.
>
> 53. S'agissant du droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données de base ainsi que sur le contenu des données communiquées, la directive ne précise pas si ce droit concerne le passé ni, le cas échéant, la période visée dans le passé.
>
> 54. À cet égard, il convient de constater que, pour assurer l'effet utile des dispositions visées aux points 51 et 52 du présent arrêt, ce droit doit nécessairement concerner le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi.
>
> [...]

> 70. Il y a lieu, dès lors, de répondre à la question posée de la manière suivante :
>
> - L'article 12, sous a), de la directive impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.
> - Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires. »[69]

Si, bien entendu, la Cour a fondé son raisonnement sur la directive 95/46, il est transposable pour le RGPD.

L'on doit noter que le règlement prévoit des exceptions dans l'exercice des droits par la personne concernée et, plus particulièrement, au niveau des traitements ultérieurs.

31. Dans le cas de l'économie collaborative, l'information à l'égard de la personne concernée, c'est-à-dire de l'utilisateur du service, est primordiale et doit porter sur toutes les finalités des traitements de données à caractère personnel, en ce compris et surtout les traitements ultérieurs qui, ainsi que nous l'avons vu par ailleurs, peuvent concerner des données particulières. Cette information doit être fournie dans un langage compris par l'utilisateur.

Or, la lecture des *privacy policies* telles que celles d'Uber montre que la langue utilisée est l'anglais[70] alors que le site est destiné aux clients francophones. Les clients ne lisant pas l'anglais manqueront donc certaines informations qui sont pourtant essentielles pour donner un consentement éclairé.

---

69 CJCE, 7 mai 2009, *Rijkeboer c. Pays-Bas*, C-553/07, ECLI:EU:C:2009:293.

70 https://privacy.uber.com/policy.

Ainsi, on lit que :

> « We also use the information we collect :
> - To enhance the safety and security of our users and services
> - For customer support
> - For research and development
> - To enable communications to or between users
> - To provide promotions or contests
> - In connection with legal proceedings
>
> Uber does not sell or share your personal information to third parties for third party direct marketing purposes. »

L'on constate qu'Uber utilisera les données pour des finalités autres que celles liées directement au service de transport, à savoir la fourniture de services ajoutés. Mais ce qui est encore plus étonnant est le fait qu'Uber précise que les données ne seront pas vendues ou partagées avec des tiers pour des finalités de marketing direct. Cela semble indiquer que, pour ce qui ne concerne pas cette finalité précise, le partage de données avec de tels tiers est possible. L'on peut penser au profilage, à du *benchmarking*, etc., c'est-à-dire des traitements ultérieurs non précisés par ailleurs.

L'on constate donc que l'information parcellaire fournie, de surcroit en anglais et non en français, langue choisie sur le site internet, ne répond pas au prescrit du RGPD et cette infraction invalide le consentement requis des clients, à tout le moins pour les traitements ultérieurs. Cela ouvre donc la voie à d'éventuelles « amendes administratives pouvant s'élever jusqu'à 20.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »[71].

La même question de transparence peut se poser au niveau des prestataires de service dans un SEL.

Conclusion

32. L'on constate que l'économie collaborative est multiple, ce qui rend son analyse difficile en termes de traitement de données à caractère personnel entre autres.

Cette difficulté ne pourra cependant pas autoriser les fournisseurs de services à fuir leurs obligations imposées par le RGPD qui protègent les utilisateurs des services de l'économie collaborative contre les abus en termes de traitement que les prestataires de service, intermédiaires ou non, pourraient être tentés de commettre. En effet, ces

[71] Art. 83, 5, du RGPD.

prestataires ont en leur possession des données qui ont une valeur économique non négligeable. La revente de ces données ou leur réutilisation à d'autres fins que celles d'offrir un service demandé par l'usager a déjà cours dans les environnements « *cloud* » et le sont également dans l'économie collaborative. Certains modèles financiers sont principalement basés sur cette revente ou réutilisation.

33. La présente contribution a voulu identifier les différents acteurs mais également les obligations qui leur incombait à l'égard des usagers sans pouvoir, cependant, être exhaustive tant ces obligations sont importantes. Nous avons cependant tenté d'en dégager certaines qui pourront ouvrir la voie à d'autres réflexions mais dont l'analyse peut surtout servir à la défense des droits de l'usager souvent considéré comme une mine d'information consentante alors qu'il ne l'est pas.

L'usager doit être protégé et le RGPD lui en donne l'occasion. Qu'il la saisisse !