Enjeux juridiques liés à l'analyse des comportements de consommation par la géolocalisation

Vanreck, Odile

Published in:
Vie privée et données à caractère personnel

Publication date:
2014

Document Version
le PDF de l'éditeur

9. LA GÉOLOCALISATION

CHAPITRE 9.1.
ENJEUX JURIDIQUES LIÉS À L'ANALYSE DES COMPORTEMENTS DE CONSOMMATION PAR LA GÉOLOCALISATION

Odile VANRECK

Introduction

« Considérant qu'[…] il est fait de plus en plus fréquemment appel au traitement de données à caractère personnel dans les divers domaines de l'activité économique et sociale ; que les progrès des technologies de l'information facilitent considérablement le traitement et l'échange de ces données ; [...] » Le considérant 4 de la directive (CE) n° 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1] (ci-après, « la directive ») dresse un constat qui est plus que jamais d'actualité aujourd'hui : des traitements de données à caractère personnel sont couramment mis en œuvre par des acteurs privés dans un objectif économique.

Il se produit, à l'heure actuelle, un développement exponentiel des technologies de l'information et de la communication, ce qui engendre la création de services nouveaux, notamment basés sur le traitement de données à caractère personnel. L'ensemble des acteurs impliqués dans la conception, la fabrication ou l'utilisation de ces technologies doit être attentif au respect du cadre juridique, en particulier aux règles relatives à la protection des données et au droit au respect de la vie privée[2].

Cette contribution s'attache à un traitement spécifique réalisé par les commerçants afin de connaître au mieux les habitudes de consommation de leur clientèle. Les commerçants présents sur Internet utilisent le système des *cookies*, ce qui leur permet d'obtenir des informations utiles pour connaître les internautes de manière approfondie et, *in fine*, leur proposer une expérience personnalisée. Ils sont ainsi au

1. Directive (CE) n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.*, n° L 281, 23 novembre 1995, pp. 0031 à 0050.
2. C. DE TERWANGNE et J.-N. COLIN, « Protection de la vie privée et des données personnelles dans l'environnement numérique », in C. DE TERWANGNE (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pp. 21 et s.

courant de chaque action de l'internaute et, notamment, des pages visitées, du temps passé sur chacune, des recherches effectuées, de sa localisation et, le cas échéant, des achats réalisés[1]. De la même manière, les propriétaires de magasins physiques aimeraient également disposer de connaissances précises au sujet des personnes fréquentant leur établissement. Par conséquent, des services se sont développés afin que les commerçants puissent suivre les consommateurs durant leur trajet dans les magasins, et ce, par le biais de leur téléphone portable. C'est la technologie de la géolocalisation qui est utilisée, technique qui permet de définir la localisation d'une personne ou d'un objet de manière relativement précise en s'appuyant généralement sur « les interfaces de communication d'un téléphone »[2] portable. Ce dernier rend, dès lors, possible le « *tracking* comportemental »[3] dans le monde réel[4]. Ce mécanisme est appelé le *retail analytics*, le *shopper tracking* ou, encore, l'*analyse des comportements de consommation par la géolocalisation*[5].

La présente contribution s'attachera, dans un premier temps, à poser les bases de la réflexion par l'explicitation du phénomène, ce qui délimitera l'objet même de l'analyse, et reprendra une réaction intuitive des individus face au *retail analytics* (1). Ensuite, une partie sera consacrée aux défis juridiques liés à cette technologie (2). Finalement, des mesures pouvant être mises en œuvre par divers acteurs afin d'assurer un meilleur respect de la législation dans le cadre de l'analyse des comportements de consommation par la géolocalisation seront développées (3). Dans un objectif de compréhension, il sera réalisé, dès que possible, des liens avec les pratiques de sociétés présentes en Europe et proposant des services de *retail analytics* comme Walkbase, WiFiProfs ou Amoobi.

1. Explications du mécanisme de l'analyse des comportements de consommation par la géolocalisation

Avant de présenter la technologie du *shopper tracking* ainsi que ses implications, notamment juridiques, il convient d'exposer son fonctionnement (1.1) et d'indiquer les avantages de cette technologie (1.2). Subséquemment, il sera intéressant de for-

1. B. Doucet, *Amoobi : vous bougez, je décrypte*, août 2012, http://www.regional-it.be/2012/08/23/amoobi-geolocalisation-indoor-retail ; A. Malone, *On the Third Day of Privacy, My Smartphone Followed Me*, December 2013, http://www.privacyandsecuritymatters.com/2013/12/on-the-third-day-of-privacy-my-smartphone-followed-me ; X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, février 2013, http://www.panoptinet.com/cybersecurite-decryptee/grandes-surfaces-notre-profil-de-consommation-devoile-par-le-wi-fi/.
2. CNIL, *La géolocalisation*, http://www.cnil.fr/les-themes/ deplacements-transports/geolocalisation.
3. B. Fung, *How Stores Use Your Phone's WiFi to Track Your Shopping Habits*, October 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits.
4. X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.* ; A. Malone, *op. cit.*
5. Ces trois dénominations recouvrent, dans le cadre de cette contribution, la même réalité : la technologie dont le fonctionnement est explicité dans le point 1.1.

muler de manière concise les inquiétudes eu égard à ce phénomène et de présenter le cadre juridique applicable aux hypothèses de traitement de données à caractère personnel (1.3).

1.1. Fonctionnement du *retail analytics*

Le fonctionnement de l'analyse des comportements de consommation par la géolocalisation est relativement aisé. Généralement, deux acteurs interviennent : la société proposant comme service l'analyse des comportements de consommation par la géolocalisation et le commerçant qui désire obtenir des informations sur les personnes présentes dans son magasin.

Tout d'abord, des capteurs sont installés, par la société proposant le service, dans le magasin faisant l'objet de l'examen. Ceux-ci détectent les téléphones portables dont les fonctions Wi-Fi ou Bluetooth sont activées[1]. Ces fonctions envoient de manière régulière des signaux afin de trouver des réseaux disponibles. Or ces signaux communiquent l'adresse MAC de l'appareil, qui est en réalité le numéro de série du module de la radio qui se trouve dans l'appareil et qui est, dès lors, « un identifiant unique attribué »[2] à un équipement[3]. De fait, toute carte Wi-Fi ou Bluetooth est identifiable grâce à l'adresse MAC[4]. Les détecteurs collectent également la force du signal, ce qui rend possible la définition de la position du téléphone à l'intérieur du bâtiment[5]. C'est ce qu'on appelle l'« indoor positioning »[6]. Ensuite, après avoir été collectées, les données sont enregistrées et conservées dans des bases de données stockées dans des serveurs[7]. Afin d'assurer une certaine sécurité et confidentialité, les données sont hachées avant d'être enregistrées[8]. Généralement, plusieurs cryptages successifs de l'adresse MAC ont lieu. Une fois sur les serveurs, les données sont analysées et agrégées afin qu'en ressortent les éléments demandés par le client de la société proposant les services de *retail analytics*, c'est-à-dire par le commerçant. Ces statistiques, rapports et schémas sont alors mis à la disposition du client

1. Voy. B. Doucet, *Amoobi : petits cailloux blancs virtuels*, avril 2012, http://datanews.levif.be/ict/centre-de-connaissance/jeunes-entreprises/amoobi-petits-cailloux-blancs-virtuels/article-4000079904631.htm ; S. Godart, « Amoobi, un outil d'analyse intelligent », *L'Écho*, mai 2012, p. 72 ; J. L., *Les mobiles bientôt traqués par des grandes surfaces pour tout connaître des clients*, octobre 2011, http://www.numerama.com/magazine/20191-les-mobiles-bientot-traques-par-des-grandes-surfaces-pour-tout-connaitre-des-clients.html ; C. Van Rompaey, « Amoobi analyse le flux de clients chez Makro », *Storecheck*, mai 2012, p. 20 ; X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.*
2. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, mai 2011, 881/11/FR, *WP* 185, p. 5.
3. *Ibid.*, p. 10 ; Amoobi, *How We Handle Privacy*, http://www.amoobi.com/company/page19/page19.html.
4. B. Fung, *op. cit.*
5. X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.*
6. F. Giannotti et D. Pedreschi, « Mobility, data mining and privacy : a vision of convergence », *in Geographic Knowledge Discovery*, Berlin, Springer, 2008, p. 12.
7. J. L., *Les mobiles bientôt traqués par des grandes surfaces pour tout connaître des clients*, *op. cit.*
8. X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.*

en vue de leur utilisation pour optimiser l'organisation quotidienne et l'agencement de la surface commerciale[1].

Via cette technologie, le commerçant peut connaître diverses informations concernant les habitudes de consommation des clients, informations qui s'avèrent essentielles du point de vue marketing : définition des zones de passage, attractivité d'un espace ou d'un point précis, placement stratégique de produits, connaissance des effets d'une promotion localisée à un endroit déterminé, mais également fréquence[2] et durée des visites d'un client[3]. Ainsi, le commerçant peut adapter la disposition et l'organisation de sa surface commerciale en vertu des modèles de comportements des consommateurs, qui sont déterminés à partir de l'analyse de la localisation des téléphones portables de ces derniers et, dès lors, de leur position[4]. L'objectif final est de rentabiliser l'espace et de pousser les personnes présentes dans l'établissement à la consommation grâce à une meilleure connaissance de leurs habitudes, sans que celles-ci n'aient, de leur propre chef, communiqué les informations[5].

1.2. Avantages du *retail analytics*

La technologie de l'analyse des comportements de consommation par la géolocalisation présente divers avantages par rapport à d'autres techniques qui peuvent être mises en place par les commerçants pour connaître les habitudes des personnes fréquentant leur magasin.

Parmi ces autres moyens, il y a l'installation de caméras de surveillance. Ces dernières ont plusieurs inconvénients, d'une part, liés à la protection des données à caractère personnel, puisque les consommateurs se montrent assez réticents à l'idée d'être filmés[6], et, d'autre part, en raison du fait que, lorsque la personne filmée sort du champ d'une caméra, son parcours est inconnu jusqu'au moment où elle entre dans le champ de vision d'une autre caméra. Par conséquent, le trajet suivi par le client n'est pas connu de son entrée à sa sortie du magasin[7]. En outre, des caméras de surveillance intelligentes sont également développées et installées dans les

1. Le magasin ne reçoit donc que des données agrégées, des tendances, et non pas des données individuelles sur les consommateurs. Voy J. L., *Les mobiles bientôt traqués par des grandes surfaces pour tout connaître des clients*, *op. cit.* ; X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.*
2. En effet, un commerçant est capable de reconnaître les clients grâce à leur adresse MAC ou grâce à un numéro d'identification unique qui est, en réalité, l'adresse MAC cryptée. Voy. S. CLIFFORD et Q. HARDY, *Attention, Shopper : Store Is Tracking Your Cell*, July 2013, http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0 ; S. GODART, *op. cit.*, p. 72.
3. S. CLIFFORD et Q. HARDY, *op. cit.* ; B. DOUCET, *Amoobi : vous bougez, je décrypte*, *op. cit.* ; S. GODART, *op. cit.*, p. 72 ; J. L., *Les mobiles bientôt traqués par des grandes surfaces pour tout connaître des clients*, *op. cit.* ; B. DOUCET, *Amoobi : petits cailloux blancs virtuels*, *op. cit.*
4. FUTURE OF PRIVACY FORUM, *Mobile Location Analytics. Code of Conduct of the 22nd of October 2013,* http://www.futureofprivacy.org/issues/smart-stores, p. 1.
5. J. L., *Les mobiles bientôt traqués par des grandes surfaces pour tout connaître des clients*, *op. cit.*
6. C. VAN ROMPAEY, *op. cit.*, p. 20.
7. C. CHARLOT, « Caméras et géolocalisation pour analyser le comportement. Vos mouvements en magasin sous la loupe », *Trends*, novembre 2012, p. 76.

magasins. Celles-ci sont « équipées de logiciels qui permettent l'enregistrement et facilitent l'interprétation des trajectoires, des attitudes et des comportements des personnes »[1]. Ces caméras peuvent avoir comme fonctionnalité de déterminer le sexe et la tranche d'âge de l'individu filmé. Il est aussi possible, par une analyse de l'*eye tracking*, qui se focalise sur l'étude des yeux des personnes, de définir les parcours réalisés, le temps passé dans les différentes zones et « la facilité avec laquelle [les clients] trouv[…]ent certains produits »[2]. Ces caméras intelligentes présentent néanmoins les mêmes faiblesses que les caméras de surveillance traditionnelles.

Par ailleurs, la technologie RFID constitue une technique utilisée dans de nombreux secteurs et notamment par les commerçants[3]. Par exemple, des puces RFID sont installées sur les chariots de supermarché pour mesurer les trajectoires des personnes et le temps passé dans les différentes parties de l'établissement. Dans ce cas, les informations ne sont pas d'une précision optimale puisqu'il n'est pas rare que les clients laissent leur caddie à l'entrée des rayons. La technologie RFID permet également de proposer au client de la publicité personnalisée, notamment, sur un écran placé sur le chariot[4]. De plus, une puce RFID peut être insérée dans les cartes de fidélité, afin de connaître énormément d'informations sur le client, puisque, non seulement il y a une collecte des données liées aux achats de l'individu, mais il est aussi possible de localiser la personne et de définir sa trajectoire par le biais de lecteurs de puces placés dans l'établissement.

Des méthodes supplémentaires peuvent être mises en place en vue d'obtenir une connaissance approfondie des clients. Elles présentent également des points négatifs par rapport à l'analyse des comportements par la géolocalisation des téléphones portables. En effet, au contraire de ce que permet l'examen des tickets de caisse et des cartes de fidélité traditionnelles, le *retail analytics* rend possible une connaissance des personnes présentes dans l'enceinte, même si elles ne procèdent à aucun achat, ainsi que de leur comportement dans le magasin et non pas uniquement du résultat de leurs courses[5]. En outre, la localisation par le biais des fonctions Wi-Fi et Bluetooth du téléphone portable de la personne présente dans le magasin est plus efficace que celle réalisée par le biais des signaux émis par la fonction GPS de l'équipement, étant donné que tels signaux sont bloqués par les éléments situés à l'intérieur du bâtiment, comme les cloisons, les murs ou d'autres obstacles, ce qui rend impossible une localisation exacte des personnes[6].

1. C. Colin et Y. Poullet, « Du consommateur et de sa protection face à de nouvelles applications des technologies de l'information : risques et opportunités », *D.D.C.R.*, n° 88, 2010, p. 96.
2. C. Charlot, *op. cit.,* p. 75.
3. C. Colin et Y. Poullet, *op. cit.,* p. 96.
4. W. Schreurs, M. Hildebrandt *et al.*, « Cogitas, Ergo Sum. The role of data protection law and non-discrimination law in group profiling in the private sector », *in Profiling the European Citizen, Cross-Disciplinary Perspectives*, Berlin, Springer, 2008, pp. 246 et 247.
5. C. Charlot, *op. cit.,* p. 76 ; C. Van Rompaey, *op. cit.*, p. 20
6. B. Doucet, *Amoobi : vous bougez, je décrypte, op. cit.*

Finalement, il ressort de cette partie de la contribution que le *shopper tracking* constitue une solution efficace pour obtenir des informations sur les personnes fréquentant un établissement. Un avantage supplémentaire de cette technique de collecte d'informations par les signaux émis par les téléphones portables réside dans la facilité de son implémentation. En effet, nul équipement ne doit être placé sur les clients ou sur un chariot et il n'est pas nécessaire « d'adapter spécifiquement la solution à l'IT du magasin »[1], ni d'installer des câbles[2].

1.3. Réaction intuitive des individus

Face à la géolocalisation par les téléphones portables, la réaction de la plupart des individus est l'étonnement ainsi que le sentiment d'être traqué. Il existe différents types de collecte de données de géolocalisation réalisés à l'insu des personnes concernées[3]. Cet exposé se focalise uniquement sur la collecte qui est effectuée par certaines sociétés dans les supermarchés afin de connaître les comportements d'achat des individus, ces derniers étant suivis par le biais de leur équipement mobile.

Comme souvent, lorsque l'on parle de vie privée et de collecte des données, deux catégories de personnes peuvent être rencontrées. Il y a celles qui considèrent qu'une telle collecte est anodine. Ces personnes ne sont pas alarmées à l'idée que des données les concernant soient disponibles et utilisées par des sociétés privées et elles peuvent même y être favorables, étant donné que les informations marketing qui en ressortent sont employées pour optimiser la disposition des rayons dans les magasins concernés. À l'opposé, il y a les personnes qui ressentent ces pratiques comme une intrusion dans leur vie privée, comme une violation de leurs droits et libertés fondamentaux. Plusieurs éléments peuvent les déranger. Tout d'abord, il y a le fait même que les sociétés privées collectent des données venant de leur téléphone portable, outil qui est généralement considéré comme personnel et intime. Ensuite, ces pratiques peuvent être réalisées sans que les personnes soient conscientes de l'existence du phénomène ou n'en soient informées, d'autant plus que leur fonctionnement est invisible[4]. Il y a donc une perte de contrôle du citoyen sur les informations qui le concernent[5]. Au surplus, ce mécanisme a un objectif uniquement commercial[6]. Enfin se posent les questions de l'utilisation, de la conservation et de la destruction des données. Pour conclure, il ressort d'une étude que

1. S. Godart, *op. cit.*, p. 72.
2. B. Doucet, *Amoobi : petits cailloux blancs virtuels*, *op. cit.*
3. J.-M. Dinant, *op. cit.*, p. 4.
4. C. de Terwangne et J.-P. Moiny, « Partie 2 », *in Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques*, Strasbourg, Conseil de l'Europe, novembre 2010, disponible à http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf.
5. J.-M. Dinant, *op. cit.*, pp. 4 et 5.
6. X., *Grandes surfaces : notre profil de consommation dévoilé par le Wi-Fi ?*, *op. cit.*

presque la moitié des Européens interviewés sont inquiets du fait d'être traqués par leur téléphone portable, notamment par le mécanisme de la géolocalisation[1].

Cependant, au-delà des réactions individuelles, le phénomène du *retail analytics* doit également interpeller la société dans son ensemble puisqu'il entraîne des questions dépassant l'individu appréhendé isolément. Il semble, dès lors, indispensable qu'un débat sociétal soit envisagé.

Ces inquiétudes ont amené les juristes à s'interroger sur les outils dont dispose le client afin de protéger sa vie privée, afin que ses données à caractère personnel ne soient pas utilisées de manière incontrôlée. Plusieurs instruments juridiques existants apparaissent comme pouvant s'appliquer dans le cadre du *shopper tracking*. Cette contribution s'attachera à l'analyse 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 (ci-après, la « loi vie privée » (LVP) ou « la loi »)[2], qui constitue, dans sa version révisée en 1998, la transposition en droit belge, de la directive (CE) n° 95/46 précitée. Il semble également pertinent d'évoquer le droit à l'autodétermination informationnelle[3], dont le principe est d'offrir aux individus une maîtrise de leur environnement informationnel, notamment en encadrant les traitements de données réalisés par des responsables du traitement. Ces derniers peuvent être des organismes publics ou privés agissant en vertu de leur liberté d'entreprendre et d'association[4]. Ainsi, il existe un « droit de contrôler ses propres données »[5], qui découle du droit au respect de la vie privée.

1. Cette inquiétude est plus importante dans le groupe des 25-39 ans, puisque, dans ce cas, 55 % des personnes interviewées se disent inquiètes. Uniquement 41 % des plus de 55 ans partagent les mêmes inquiétudes. Cette différence peut s'expliquer par le fait que 14 % des plus de 55 ans ont également répondu que cette question ne s'appliquait pas à eux. Les auteurs en déduisent que ces personnes ne possèdent pas de téléphone portable permettant la géolocalisation. Voy. TNS OPINION & SOCIAL, « Attitudes on data protection and electronic identity in the European Union », *Special Eurobarometer 359*, at the request of Directorate general Justice, Information, Society & Media and Joint Research Centre, June 2011, http://ec.europa.eu/public_opinion/archives/eb_special_359_340_fr.htm, pp. 71 et 72.
2. 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, pp. 5801 et s.
3. C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 14.
4. Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain*, Bruxelles, Bruylant, 2008, p. 42.
5. Résolution 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin 1998, *in* C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 14.

2. Défis juridiques liés à l'analyse des comportements de consommation par la géolocalisation

Malgré l'apparition de technologies innovantes et l'inhérent développement de mécanismes et services nouveaux, la législation liée à la protection des données reste d'application et s'adapte à ces nouveautés[1].

Pour que la loi vie privée s'applique[2], il faut démontrer que l'analyse des comportements de consommation par la géolocalisation des téléphones portables implique des traitements (2.2) de données à caractère personnel (2.1). Par la suite, il convient de définir quel rôle jouent les acteurs présents, c'est-à-dire le magasin et la société proposant le service de *shopper tracking* (2.3). Enfin, la dernière section est consacrée à l'explicitation des obligations devant être respectées par les acteurs (2.4).

2.1. Données à caractère personnel

À ce stade du raisonnement, il convient d'établir que le mécanisme du *retail analytics* implique un traitement de *données à caractère personnel*, concept en permanente mouvance[3]. Il ressort de l'explication du fonctionnement du mécanisme que les données captées par les détecteurs sont les adresses MAC des téléphones portables et que, de ces informations, est déduite la localisation des possesseurs de ces équipements.

Ce point sera subdivisé en trois parties. Dans la première sera réalisée une analyse de la définition de la *donnée à caractère personnel* (2.1.1). La seconde partie reprendra des arguments jouant en faveur de la qualification des données impliquées dans le *shopper tracking* en *données à caractère personnel* (2.1.2), alors que la troisième partie s'attachera à développer les notions de *données pseudonymisées* et *anonymisées* (2.1.3).

2.1.1. Définition et commentaires

La loi, en son article 1er, § 1er, définit la donnée à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable ». De cette

1. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », « 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 », décembre 2009, 02356/09/FR, *WP* 168, p. 2.
2. L'hypothèse prise dans cette contribution est celle d'un traitement de données à caractère personnel effectué par un responsable du traitement sur le territoire belge. Les exigences de l'article 3*bis* de la loi, liées à la compétence territoriale, sont donc rencontrées.
3. D. Djokic, *Protection de la vie privée sur Internet et Conseil de l'Europe. Évolution du concept et adaptation réglementaire,* Saarbrücken, Éditions universitaires européennes, 2011, p. 35.

définition peut se déduire une volonté d'appréhender de manière extensive la notion, dans l'objectif de couvrir l'ensemble des informations qui peuvent être rattachées à une personne physique[1].

Cependant, certaines limites sont apportées à ce concept, comme cela ressort de la lecture même de l'article 3 de la LVP. En effet, pour que l'instrument législatif trouve à s'appliquer, le traitement doit être automatisé ou, dans le cas contraire, les données doivent être contenues dans un fichier structuré[2]. Cette condition est remplie dans le cadre du *retail analytics*. En outre, la disposition contient, en son paragraphe 2, une exception pour les traitements effectués « pour l'exercice d'activités exclusivement personnelles ou domestiques »[3] et, dans les paragraphes suivants, des exceptions pour les traitements « effectués aux seules fins de journalisme ou d'expression artistique ou littéraire » ou réalisés à des fins de sécurité publique de manière large. Étant donné que cette contribution se concentre sur les traitements réalisés par des acteurs privés dans un objectif économique, ces exceptions ne sont pas rencontrées dans le cas d'espèce[4].

Bien qu'il n'ait pas expressément consacré d'avis au phénomène du *shopper tracking*, le Groupe de travail « Article 29 » (ci-après, le « Groupe 29 ») en a émis un au sujet de la définition des données à caractère personnel. Son analyse se base sur une découpe de la notion en quatre éléments constitutifs qui sont interdépendants et étroitement liés[5] : *toute information* (a.), *concernant* (b.), *une personne physique* (c.), *identifiée ou identifiable* (d.). Il convient, dès lors, d'exposer ces composants et, simultanément, de vérifier si les données traitées lors de l'analyse des comportements de consommation par la géolocalisation, c'est-à-dire la localisation des personnes par le biais de leur adresse MAC, rencontrent ces éléments[6].

a. Toute information

L'élément *toute information* participe de manière incontestable au caractère large du concept de *données à caractère personnel*, puisqu'il est satisfait quel que soit le type d'informations traitées, indépendamment du contenu, de la nature, du format ou du support de présentation[7]. Au sujet du contenu des informations, il peut s'agir d'informations qui concernent des personnes physiques, quelles que soient leur qualité ou

1. C. Colin et Y. Poullet, *op. cit.,* p. 107 ; Groupe de travail « Article 29 », Avis 4/2007 sur le concept de données à caractère personnel, juin 2007, 01248/07/FR, *WP* 136, p. 4 ; D. Korff, *WP 2 – Data Protection Laws in the EU : The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments*, European Commission- Directorate general Justice, Freedom and Security, January 2012, p. 41.
2. Considérant 15 de la directive (CE) n° 95/46 ; article 3 LVP.
3. Article 3, §§ 3 à 7, LVP.
4. W. Schreurs, M. Hildebrandt *et al*., *op. cit.*, p. 242.
5. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 6.
6. J. Eynard, *Les données personnelles : quelle définition pour un régime de protection efficace ?*, Paris, Michalon, 2013, p. 46.
7. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 6. Voy. aussi Y. Poullet, « About the E-Privacy directive : towards a third generation of data protection legislation », *in Data Protection in a Profiled World,* Dordecht, Springler, 2010, pp. 3 à 30 ; V. Verbruggen, *Protection des données à caractère personnel : loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Loi Vie privée*, 2e éd., Bruxelles, Larcier, 2011, p. 12.

leur situation[1]. Comme la nature des informations importe peu, tout type de renseignements donnés au sujet d'une personne entre dans la définition de données à caractère personnel, que ces renseignements soient vrais ou faux, objectifs ou subjectifs[2]. Finalement, le format et le support sur lequel est présentée l'information sont indifférents. En effet, les informations peuvent être numériques, photographiques, alphabétiques, graphiques ou acoustiques[3].

Dans le cas d'espèce, cet élément est aisément satisfait en raison de l'extensive compréhension de la définition. La combinaison de l'adresse MAC et de la localisation de la personne est incluse dans les termes « toute information », et les informations, qui concernent les personnes présentes dans le magasin, sont objectives et sous format numérique.

b. Concernant

Les informations doivent *concerner* une personne, c'est-à-dire avoir trait à cette personne de manière générale[4]. Cette vision semble simpliste, mais l'exercice qui consiste à établir que des données *concernent* une personne n'est pas toujours aisé, en particulier lorsque les informations sont liées de manière directe, non pas à une personne, mais à un objet. C'est d'ailleurs le cas dans l'hypothèse du *shopper tracking*. Le Groupe 29 a pointé l'importance de cet élément et a déterminé trois facteurs distincts qui permettent de conclure qu'une information *concerne* un individu : un élément, soit de contenu, soit de finalité, soit de résultat, doit être présent[5].

Premièrement, l'élément de contenu est présent si les informations en question ont trait à la personne, la *concernent*, ce dernier terme devant être compris dans son acceptation commune. Par exemple, un dossier médical concerne le patient[6]. Ensuite, il est possible de se baser sur l'élément de finalité afin d'apprécier si une personne est concernée par les informations. Le Groupe 29 considère que cet élément est rencontré si les données sont, ou sont susceptibles d'être, utilisées pour traiter d'une manière spécifique ou pour influencer le comportement ou le statut d'une personne, en prenant en considération les circonstances de l'espèce. Ainsi, même si les données peuvent être liées à différentes personnes, il peut s'agir de données à caractère personnel en raison des finalités attachées au traitement[7]. Enfin, même si une information ne remplit pas les éléments de contenu ou de finalité, elle concerne une personne dans les cas où l'utilisation de cette information est susceptible d'avoir une conséquence sur les droits ou intérêts de la personne en question. Il s'agit de l'élément de résultat, qui n'exige pas que « le résultat potentiel ait un impact

1. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 7.
2. *Ibid.*
3. *Ibid*., p. 8.
4. *Ibid*., p. 10.
5. *Ibid.,* pp. 11 et 12 ; V. VERBRUGGEN, *op. cit.,* p. 12.
6. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 11.
7. *Ibid.,* pp. 11 et 12 ; C. COLIN et Y. POULLET, *op. cit.,* p. 108.

majeur »[1], mais que la personne « puisse être traitée différemment par rapport à d'autres »[2] à la suite de ce traitement de données. Il faut qu'il y ait un impact provoqué du fait de l'utilisation des données[3].

Lors de la mise en œuvre du *retail analytics*, il apparaît que la géolocalisation de la personne par le biais de son adresse MAC *concerne* une personne physique, puisque ces éléments ont trait à cet individu. L'élément de contenu est rencontré.

c. Personne physique

La protection de la loi vie privée ne s'applique qu'aux personnes physiques[4]. Même si la combinaison de l'adresse MAC et de la position est, en fait, liée à un téléphone portable, il va de soi que c'est le comportement de la personne physique détentrice de l'objet qui est visé par l'analyse[5]. De fait, le téléphone portable est un objet intimement lié à son propriétaire. La majorité des personnes le gardent en permanence sur elles[6].

d. Identifiée ou identifiable

Pour qu'il y ait une donnée à caractère personnel, il faut que la personne physique soit *identifiée ou identifiable*. Une personne est identifiée si elle se distingue, si elle peut être différenciée des autres membres au sein d'un groupe. En effet, dans le contexte technologique, l'accent est mis sur l'individualisation plutôt que sur l'identification, ce qui implique qu'il n'est pas nécessaire de connaître l'identité de la personne concernée[7]. De surcroît, une personne est identifiable si elle « peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[8]. En d'autres termes, s'il est possible d'identifier un individu même si cette identification n'a pas (encore) été entreprise, il est identifiable[9].

Afin de déterminer si, dans un cas précis, une personne est identifiable, il faut prendre en compte « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre [à cette fin], soit par le responsable du traitement, soit par une autre personne »[10]. Ce prescrit induit qu'une simple possibilité négligeable ou hypothé-

1. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 12.
2. *Ibid*.
3. C. Colin et Y. Poullet, *op. cit.,* p. 108.
4. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 24.
5. C. Colin et Y. Poullet, *op. cit.,* pp. 106 à 108.
6. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, *op. cit.*, pp. 7 et 19.
7. *Ibid*., p. 14 ; C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 21 ; J. Eynard, *op. cit.,* p. 44 ; D. Korff, *op. cit.,* p. 45.
8. Article 1er, § 1er, LVP.
9. J. Eynard, *op. cit.,* p. 46.
10. Considérant 26 de la directive (CE) n° 95/46.

tique de différencier un individu parmi un groupe n'est pas suffisante pour estimer cet individu identifiable. Ainsi, n'est pas comprise l'identification des personnes qui exigerait un recours à des méthodes extrêmement complexes[1]. Par ailleurs, dans l'analyse des moyens pouvant raisonnablement être mis en place, il faut appréhender des facteurs tels que le coût de cette identification, les défaillances techniques et organisationnelles, les intérêts des parties et la structure du traitement[2], en tenant compte de « l'état d'avancement technologique au moment du traitement et des changements éventuels »[3] pendant la durée de conservation[4]. De plus, il ressort du considérant 26 de la directive que les moyens pour identifier la personne concernée doivent pouvoir être mis en œuvre soit par le responsable du traitement, soit par un autre individu[5]. Finalement, une personne est identifiable si elle peut être, *directement ou indirectement*, identifiée. Le terme *indirectement* permet d'appréhender « le phénomène des combinaisons uniques »[6]. Il s'agit des situations où il n'est pas possible, en raison des éléments disponibles, de directement identifier la personne, mais cette dernière peut être distinguée des autres par la combinaison de ces éléments et d'autres informations qui sont dans les mains du responsable du traitement ou d'un tiers[7]. Cette précision entraîne une compréhension large du caractère d'identifiabilité[8]. Il faut en déduire que toute information en lien avec l'individu peut potentiellement être qualifiée de donnée à caractère personnel en fonction des circonstances de l'espèce[9].

En conclusion, l'analyse des quatre composants de la définition de la *donnée à caractère personnel* amène à considérer que les données traitées dans le cadre de l'analyse des comportements de consommation par la géolocalisation, c'est-à-dire l'adresse MAC d'un téléphone portable et sa localisation, remplissent les conditions susmentionnées et sont, dès lors, des données à caractère personnel. Notons que les exigences pour qu'une telle qualification soit opérée sont aisément aisément atteintes en raison de la compréhension large des divers critères et du fait que la connaissance précise de l'identité de l'individu n'est pas nécessaire pour conclure à la présence d'une donnée à caractère personnel. En l'espèce, la personne est directement identifiable par le responsable du traitement ou par un tiers qui aurait accès aux données, puisqu'elle peut être distinguée des autres individus d'un groupe de par sa localisation, qui est connue grâce à l'adresse MAC de son téléphone.

1. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 16.
2. J. EYNARD, *op. cit.,* p. 46.
3. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 16.
4. En effet, bien que l'identification ne soit pas réalisable au jour de la collecte, l'évolution des moyens étant tellement rapide, le responsable du traitement est contraint de prendre en compte le fait qu'une identification pourrait intervenir durant le délai de conservation. Voy. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 17.
5. C. DE TERWANGNE, « La nouvelle loi belge de protection des données à caractère personnel », *in La protection de la vie privée dans la société d'information*, Paris, Faculté de droit, Centre de recherche Information, Droit et Société, 2002, pp. 92 et 93 ; D. KORFF, *op. cit.,* p. 45.
6. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 14.
7. *Ibid*.
8. J. EYNARD, *op. cit.,* p. 45.
9. *Ibid.*

2.1.2. Arguments complémentaires en faveur de la qualification de *données à caractère personnel*

Pour appuyer la position selon laquelle les données traitées dans le cadre du *retail analytics* sont des données à caractère personnel, il est pertinent de reprendre une opinion du Groupe 29 au sujet des services de géolocalisation sur les smartphones. Dans celle-ci, le Groupe a précisé que « l'adresse MAC d'un point d'accès Wi-Fi, combinée à sa position calculée, devrait être considérée de la même manière que des données à caractère personnel »[1]. Un parallèle pourrait être réalisé avec la situation étudiée dans laquelle la position d'une personne est connue par le biais de l'adresse MAC de son téléphone.

En outre, le Groupe 29, l'autorité française de protection des données (la Commission nationale de l'informatique et des libertés, ci-après, la « CNIL ») et la doctrine sont d'avis que les données de localisation, qui permettent de « connaître la situation géographique d'une personne à un instant T »[2] ou de retracer son itinéraire via son téléphone portable connecté, doivent recevoir la qualification de *données à caractère personnel* du fait de la facilité avec laquelle une personne peut être retrouvée à partir de sa position géographique[3]. Précisons que la géolocalisation consiste en l'établissement de la position d'un objet ou d'une personne. Dans le cadre du *shopper tracking*, il s'agit de la position de l'adresse MAC du téléphone portable, connue grâce aux signaux émis par ledit dispositif mobile et, conséquemment, la position de la personne.

Finalement, le Secrétariat de la Commission de la protection de la vie privée a indiqué, lors d'un échange de courriers, que « l'adresse MAC constitu[ait] bel et bien une donnée à caractère personnel »[4].

2.1.3. Données pseudonymisées et données anonymisées

Dans l'exposé du fonctionnement de la technologie, il a été souligné qu'après avoir été collectées, les données étaient hachées pour obtenir un numéro d'identification. En effet, de tels numéros sont suffisants pour analyser les trajectoires des clients, la durée de leur visite et les autres informations intéressant les commerçants[5]. Liée à cette idée, une précision peut être apportée au sujet de deux types de données : les données anonymisées et les données pseudonymisées.

---

1. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, *op. cit.*, p. 12.
2. G. Haas et F. Picard, *Guide juridique de l'e-marketing : noms de domaine, marque, publicité, prospection, e-mail, collecte de données, ciblage, e-réputation*, Saint-Herblain, ENI, 2013, p. 209.
3. *Ibid*.
4. Il convient de noter que cette information est issue d'un échange de courriers entre l'auteur et la Commission de la protection de la vie privée et que la réponse de la Commission contenait cette indication : « La présente analyse vous est communiquée sur la base des informations dont dispose le Secrétariat de la Commission » et « elle ne préjuge pas de la position qui pourrait être prise, le cas échéant, par la Commission en tant qu'organe collégial ».
5. F. Giannotti et D. Pedreschi, *op. cit.*, p. 12.

Diverses méthodes de cryptage peuvent être employées afin d'obtenir des numéros d'identification, certaines permettant la réidentification ultérieure (comme le cryptage à double sens) et d'autres non (par un cryptage à sens unique)[1]. Dans ce second cas, les données deviennent alors des données anonymes.

Dans la première situation, il s'agit de données pseudonymisées, c'est-à-dire des données ayant subi un traitement dissimulant l'identité de la personne concernée en vue de la réalisation de collectes additionnelles au sujet de la même personne, mais sans qu'il faille connaître son identité. Les données pseudonymisées sont retraçables et doivent être appréciées comme des données à caractère personnel vu qu'il s'agit d'« informations sur des personnes physiques indirectement identifiables »[2]. Les règles prévues dans la loi s'appliquent, mais de manière plus souple, puisque le traitement de ces données présente des risques plus minimes pour les personnes concernées[3]. Les données codées constituent une illustration de données pseudonymisées, puisqu'elles peuvent être retracées grâce à l'utilisation d'une clé permettant d'établir la « correspondance entre ce code »[4] et la personne physique. À l'inverse, la notion de *données anonymisées* renvoie à des données, qui, auparavant, concernaient une personne identifiée ou identifiable, mais qui désormais ne permettent plus l'identification. Les données sont devenues anonymes et la protection offerte par l'instrument européen ne s'applique pas. L'anonymisation, au contraire de la pseudonymisation, « doit être totalement irréversible »[5]. Il ressort de l'avis du Groupe 29 sur les moteurs de recherche que toute possibilité d'identification des individus, même par la combinaison avec des informations détenues par d'autres responsables de traitements, doit être exclue pour que ces données soient considérées comme des données anonymes[6].

L'établissement d'une distinction entre les données anonymes et les données à caractère personnel peut apparaître comme un processus aisé. Toutefois, dans la pratique, il n'est pas simple, notamment compte tenu du poids apporté à l'analyse de l'existence éventuelle de moyens pouvant être raisonnablement implémentés pour parvenir à l'identification et en raison des possibilités techniques d'irréversibilité. Pour déterminer si les numéros d'identification obtenus par les sociétés proposant des services de *shopper tracking* sont des données anonymes, il faut donc analyser les méthodes utilisées pour rendre ces documents méconnaissables et le degré de sécurité employé. Il convient cependant de garder à l'esprit que les hackers peuvent être très doués et que la garantie d'offrir un anonymat est extrêmement difficile[7].

1. Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, *op. cit.,* p. 19.
2. *Ibid.,* p. 20.
3. *Ibid.*
4. *Ibid.*
5. V. Verbruggen, *op. cit.,* p. 70.
6. *Ibid*., p. 71.
7. F. Giannotti et D. Pedreschi, *op. cit.,* p. 18.

Certaines sociétés offrant des services de *retail analytics* considèrent que les données qu'elles traitent sont des données anonymes. Ainsi, la société Walkbase affirme, sur son site Internet, que « all data that we gather is anonymous and we do not store any personal information »[1] et la société WiFiProfs indique également sur son site que les données qu'elle collecte sont anonymes[2]. Pourtant, le mécanisme proposé par ces sociétés se base également sur les adresses MAC des téléphones portables et sur la localisation des personnes. Il s'agit donc bien de données à caractère personnel.

Afin de clôturer cette partie consacrée aux données à caractère personnel, il est pertinent d'insister sur le fait qu'en raison de la vision extensive qui est accordée à la notion et à la suite de l'examen réalisé dans cette partie de la contribution, les données qui sont récoltées afin de réaliser l'analyse des comportements de consommation par la géolocalisation sont assurément des données à caractère personnel, et ce, même si la finalité du traitement des données de localisation n'est pas l'identification des utilisateurs[3].

2.2. Traitement

Après avoir déterminé que des données à caractère personnel étaient en jeu à l'occasion du *retail analytics*, il est nécessaire de vérifier si cette technologie implique la réalisation de *traitements* sur ces données. Le traitement de données à caractère personnel est défini à l'article 2, § 2, de la LVP. Il s'agit de « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ». S'ensuit une énumération d'opérations qui constituent des traitements[4].

Cette définition est très large et recouvre en fait toute opération qui peut être effectuée sur des données à caractère personnel. De plus, il suffit qu'une seule opération soit réalisée pour qu'il y ait un traitement[5].

Dans le cadre de l'analyse des comportements de consommation par la géolocalisation, plusieurs traitements peuvent être pointés. D'abord, il y a la collecte des adresses MAC des téléphones portables, ce qui permet la localisation de la personne. Ensuite, le processus par lequel la société transforme les adresses MAC en un numéro d'identification constitue aussi un traitement[6]. Au surplus, la distinction

1. WALKBASE, *Privacy*, http://www.walkbase.com/privacy.
2. WIFIPROFS, *Privacy*, http://www.wifiprofs.com/in-store-retail-analytics/privacy.
3. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, *op. cit.*, p. 11.
4. « La collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou destruction de données à caractère personnel ».
5. TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.,* 1999, p. 378.
6. W. SCHREURS, M. HILDEBRANDT *et al*., *op. cit.*, p. 249.

opérée entre les données anonymisées et les données pseudonymisées réapparaît. En effet, dans ce second cas, la conservation des données, les différentes opérations effectuées sur celles-ci et leur suppression constituent également des traitements de données. Par contre, une fois les données anonymisées, les traitements réalisés sur celles-ci ne sont plus soumis à la loi vie privée.

2.3. Acteurs

La loi contient, en son article 1er, les définitions des différents acteurs pouvant jouer un rôle lors du traitement de données à caractère personnel. Ainsi sont délimités les concepts du *responsable du traitement*, du *sous-traitant*, du *tiers* ou, encore, du *destinataire*[1]. L'objectif de l'attribution de ces titres aux acteurs présents dans une situation spécifique est de déterminer qui doit assurer le respect des obligations prévues dans les instruments juridiques[2]. La lecture des définitions donne l'impression qu'il est facile d'attribuer un titre à un acteur. Une fois encore, la réalité est plus complexe. En effet, le développement des technologies a engendré la création de modèles originaux et, dès lors, d'acteurs nouveaux pour lesquels la catégorisation est malaisée.

En vue de déterminer le rôle des divers acteurs présents, il convient d'expliciter les concepts de *responsable du traitement* (2.3.1) et de *sous-traitant* (2.3.2). Ensuite, la pratique sera confrontée à la théorie (2.3.3).

2.3.1. Responsable du traitement

L'article 2, § 4, de la LVP contient la définition du responsable du traitement. Il s'agit de « la personne physique ou morale, [de] l'association de fait ou [de] l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel […] ». Cette notion est fonctionnelle en ce qu'elle a comme objectif d'« attribuer les responsabilités aux personnes qui exercent une influence de fait »[3] en s'appuyant sur une analyse concrète de la situation.

1. La notion de tiers inclut les acteurs qui n'ont aucune autorisation ni légitimité pour réaliser un traitement de données à caractère personnel. Un tiers est tout acteur, autre que le sous-traitant, le responsable du traitement et les personnes sous leur autorité. Dans l'hypothèse où un tiers recevrait, licitement ou non, des données à caractère personnel, il deviendrait le responsable du traitement si les conditions requises pour opérer cette qualification étaient réunies. Enfin, la loi précise également le concept du *destinataire*, concept proche de celui de tiers, puisque, comme ce dernier, il comprend les organismes recevant communication des données à caractère personnel. Cependant, à la différence du tiers, le destinataire peut « faire partie de l'entité du responsable du traitement ou du sous-traitant ». Voy. article 1er, §§ 6 et 7, LVP ; Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, février 2010, 00264/10/FR, *WP* 169, p. 33 ; Th. Léonard et Y. Poullet, *op. cit.,* p. 379 ; V. Verbruggen, *op. cit.,* p. 29.
2. Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, *op. cit.*, p. 2.
3. *Ibid.*, p. 1.

Cette définition peut être décomposée en trois éléments qui sont étroitement liés[1]. Premièrement, les termes *la personne physique ou morale, l'association de fait ou l'administration publique* renvoient à l'idée d'une entité. Généralement, il est souhaitable de désigner comme responsable du traitement « la société ou l'organisme en tant que tel, plutôt qu'une personne en son sein »[2]. Deuxièmement, la possibilité d'une responsabilité plurielle est comprise dans la définition (*seul ou conjointement avec d'autres*). En effet, il est possible que plusieurs acteurs soient coresponsables d'un traitement, cette coresponsabilité pouvant se présenter sous diverses formes et ne devant pas nécessairement être attribuée à la suite d'un partage égal[3]. Troisièmement, l'article 2, § 4, de l'instrument législatif donne les critères permettant de différencier le rôle du responsable du traitement de celui des autres acteurs, puisque le responsable est celui qui détermine les finalités et les moyens du traitement[4]. Ce troisième volet de la définition mérite de retenir l'attention.

Pour fixer quel organisme détermine les finalités et les moyens, il faut prendre en compte à la fois les circonstances factuelles de l'espèce et des éléments de droit[5]. Le Groupe 29, dans un avis de 2010, a précisé que trois catégories de situations peuvent se présenter.

Premièrement, la responsabilité peut découler « d'une compétence explicitement donnée par la loi »[6], ce qui n'est pas la situation dans le modèle du *retail analytics*. Deuxièmement, la responsabilité peut être déduite d'une règle de droit générale ou d'une « pratique juridique établie relevant de différentes matières »[7], bien que cette responsabilité ne soit pas expressément prévue juridiquement et qu'elle ne constitue pas la conséquence immédiate d'une disposition explicite. Il s'agit de la responsabilité issue d'une compétence implicite, ce qui ne correspond pas non plus à la situation analysée. Troisièmement, la responsabilité peut découler d'une influence de fait. Dans cette hypothèse, le responsable du traitement est désigné à la suite d'une évaluation sérieuse et approfondie des éléments factuels de l'espèce. Ainsi, pour déterminer quel organisme exerce une influence de fait, peuvent être effectués un examen du « degré de contrôle réel exercé par une partie, [de] l'image donnée aux personnes concernées et [des] attentes raisonnables que cette visibilité peut susciter chez ces dernières »[8] ou, encore, une analyse des relations contractuelles existant entre les acteurs présents, bien que cet élément ne soit pas nécessairement déterminant[9].

Dans cette troisième situation, correspondant au *shopper tracking*, le responsable du traitement sera l'acteur qui prend les décisions concernant non seulement les

1. *Ibid.*, pp. 1 et 8.
2. V. Verbruggen, *op. cit.*, p. 27.
3. *Ibid.*
4. Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, *op. cit.*, p. 1.
5. V. Verbruggen, *op. cit.*, p. 27.
6. Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, *op. cit.*, p. 10.
7. Comme le droit commercial ou le droit civil. Voy. *ibid.*, p. 11.
8. *Ibid.*, p. 12.
9. *Ibid.*, pp. 12 et 13.

moyens à mettre en place mais aussi la finalité de ce traitement. D'abord, le responsable est celui qui détermine la ou les finalité(s) poursuivie(s) par un traitement et, par conséquent, qui fixe également les données qui feront l'objet de ce traitement. Le fait qu'une entité pose le choix de traiter certaines données précises dans un but déterminé implique automatiquement la qualification de cet organisme en *responsable du traitement*[1]. Ensuite, le responsable du traitement fixe les moyens par lesquels l'objectif défini pourra être réalisé, ce qui inclut les moyens techniques nécessaires pour le traitement et le « comment du traitement »[2], tels que les catégories de données traitées, les personnes ayant accès à ces données ou, encore, la durée de conservation de celles-ci. Il est accepté que le responsable délègue au sous-traitant la détermination des moyens, en ce qui concerne des éléments organisationnels ou techniques[3]. D'autres moyens, considérés comme intrinsèquement liés au responsable, doivent être déterminés par ce dernier, comme le choix des données à traiter, des personnes pouvant y avoir accès ou encore de la durée de leur conservation[4].

En conclusion, la qualification de responsable du traitement nécessite la mise en œuvre d'une approche pragmatique mettant l'accent sur le pouvoir dont dispose l'acteur pour fixer les finalités et les moyens[5].

2.3.2. Sous-traitant

Le sous-traitant est « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données », comme le définit l'article 2, § 5, de la loi. En d'autres termes, le sous-traitant est une entité « juridiquement distincte du responsable mais agissant pour son compte »[6], qui réalise une activité consistant soit en une tâche précise, soit en un ensemble de fonctions[7]. Pour qu'un sous-traitant soit présent dans un modèle de traitement de données à caractère personnel, il est indispensable qu'un responsable ait décidé « de déléguer tout ou partie des activités de traitement à une organisation extérieure »[8] plutôt que de réaliser ces traitements au sein de sa propre organisation. Divers critères peuvent être pris en considération pour qualifier correctement un acteur de sous-traitant : la présence d'instruction ou la surveillance du responsable du traitement, le pouvoir discrétionnaire accordé aux diverses parties[9], etc.

1. *Ibid.*, p. 15.
2. *Ibid.*
3. P. ex., la question du logiciel à utiliser. Voy. V. VERBRUGGEN, *op. cit.*, p. 26.
4. V. VERBRUGGEN, *op. cit.*, p. 15.
5. Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, *op. cit.*, p. 14.
6. *Ibid*., p. 26.
7. *Ibid*., p. 27.
8. *Ibid*., p. 26.
9. V. VERBRUGGEN, *op. cit.*, p. 29.

L'article 16, § 1er, 1° et 4°, de la LVP précise que le sous-traitant ne peut être choisi par le responsable du traitement qu'à condition qu'il apporte des garanties suffisantes par rapport aux mesures de sécurité organisationnelle et technique et qu'il « n'agi[sse] que sur la seule instruction du responsable du traitement ».

2.3.3. Application au cas d'espèce

Il est certain que l'évolution des technologies et, de manière concomitante, le développement des services pouvant être offerts viennent compliquer une qualification correcte des acteurs. Ainsi, dans le cas du *shopper tracking*, trois hypothèses sont envisageables. Une illustration de cette difficulté peut apparaître à la suite de l'analyse des déclarations réalisées par la société Amoobi auprès de la Commission de la protection de la vie privée. Ainsi, sur les trois déclarations examinées, une désignait le magasin comme responsable[1], alors que les deux autres indiquaient deux responsables de traitement[2] : le magasin concerné et Amoobi.

La première hypothèse consiste à considérer que le responsable du traitement est la société offrant les services d'analyse des comportements de consommation. En effet, cette dernière propose un service, décide des données qui seront récoltées, mais aussi de la manière dont les données seront collectées en fonction des besoins du commerçant. Dans cette hypothèse, le magasin dans lequel les informations sont concrètement récoltées ne joue aucun des rôles définis dans la loi. En effet, il ne traite pas de données à caractère personnel, puisque la société ne lui transfère, généralement, que des données agrégées, des données anonymes.

Selon la seconde supposition, le responsable du traitement est le commerçant, qui désire connaître de manière approfondie les personnes fréquentant son établissement et qui, pour ce faire, s'appuie sur un outil existant et proposé par une société réalisant l'analyse des habitudes de consommation. Il détermine les moyens afin d'atteindre l'objectif qu'il a lui-même défini en fonction des informations qu'il désire obtenir. Dans ce cas, la société offrant le service d'analyse des comportements de consommation est un sous-traitant.

Une troisième hypothèse est envisageable, celle de la coresponsabilité. En effet, la définition du responsable précisait que plusieurs acteurs peuvent être en même temps responsables d'un traitement[3]. Ainsi, lorsque plusieurs acteurs fixent conjoin-

1. CPVP, « Déclaration du 23 juillet 2012 », *Registre public*, https://eloket.privacycommission.be/elg/publicRegister.htm ?decArchiveId=80957.
2. CPVP, « Déclaration du 27 septembre 2012 », *Registre public*, https://eloket.privacycommission.be/elg/publicRegister.htm ?decArchiveId=81874 ; CPVP, « Déclaration du 18 février 2014 », *Registre public*, https://eloket.privacycommission.be/elg/publicRegister.htm?decArchiveId=93790.
3. Voy. les termes « seul ou conjointement avec d'autres » de l'article 2, § 4, LVP.

tement « soit la finalité, soit les éléments essentiels des moyens »[1] mis en œuvre pour un traitement, il y a coresponsabilité.

Prenant en compte le principe central selon lequel il convient de fixer où se situe le centre de gravité des décisions prises concernant la finalité et les moyens, la théorie suivie dans cette contribution sera la seconde hypothèse : le commerçant est le responsable du traitement et la société proposant le service de *retail analytics* est le sous-traitant. De fait, il s'agit d'une entité distincte du responsable du traitement qui agit pour le compte de ce dernier, puisqu'elle suit les instructions données par le commerçant et adapte l'analyse en fonction des requêtes du client. Les deux conditions prévues dans la définition du sous-traitant sont remplies. Le responsable du traitement délègue une partie de la détermination des moyens au sous-traitant (p. ex., le choix entre l'utilisation de la fonction Wi-Fi ou Bluetooth ou le nombre et la localisation des capteurs), tout en conservant le pouvoir de décision concernant les finalités. Le fait que le responsable du traitement n'ait pas les données à caractère personnel en main n'empêche pas que cette vision soit pertinente. En effet, il existe d'autres situations où un tel phénomène se produit, par exemple avec les radiographies qui sont directement envoyées en Inde afin qu'un avis médical soit donné. Dans ce cas, les sociétés qui proposent ce service en Inde sont les sous-traitants, et l'hôpital européen, le responsable du traitement, ne connaît que les résultats de ces analyses. En outre, il est, dans la pratique, accepté que le responsable du traitement puisse déléguer ses obligations liées au droit d'accès. Dès lors, le fait que, dans les déclarations, Amoobi se présente comme l'entité à l'encontre de laquelle doit être exercé le droit d'accès ne constitue pas un argument en faveur de l'hypothèse selon laquelle la société proposant les services de *shopper tracking* devrait être qualifiée de responsable du traitement.

En vue de conforter la théorie présentée, un parallèle peut être dressé avec un mécanisme plus connu : la carte de fidélité dans laquelle une puce RFID est insérée. Dans cette situation, le commerçant est le responsable du traitement qui consiste en la gestion des cartes de fidélité. Le commerçant sous-traite alors les activités de profilage à une société indépendante, mais qui agit sous son contrôle. Dans l'hypothèse où cette société autonome mettrait en place des mécanismes de « croisement avec des données venant d'autres sources »[2] ou vendrait les profils réalisés dans un magasin à d'autres acteurs, cette société perdrait son statut de sous-traitant pour devenir également responsable des deux traitements précités. Il y aurait alors « deux responsables de traitement, qui pourraient être tenus solidairement responsables »[3] selon l'article 2, § 4, de la LVP. Par contre, si la société ne traite les données que pour le compte du magasin et selon ses instructions, elle conserve la qualification de sous-traitant. De la même façon, les activités d'analyse des comportements voulues

1. Groupe de travail « Article 29 », avis 1/2010 sur les notions de responsable de traitement et de sous-traitant, *op. cit.*, p. 20.
2. C. Colin et Y. Poullet, *op. cit.*, p. 111.
3. *Ibid.*

par un commerçant sont déléguées à une société. Si les données récoltées dans un magasin ne sont pas utilisées pour d'autres projets que celui dans le cadre duquel elles ont été collectées et qu'il n'y a pas d'utilisation croisée des données, la société collectant les données est bel et bien un sous-traitant.

2.4. Obligations des acteurs

Une lecture attentive de la loi, de la directive et de la doctrine permet de constater l'étendue des obligations devant être respectées par les différents acteurs impliqués dans le traitement des données à caractère personnel et, particulièrement, par le responsable du traitement[1]. Dans cette section seront explicitées les exigences spécifiquement pertinentes dans la mise en œuvre du *retail analytics.* Il y a notamment l'article 4 de la LVP qui impose un traitement loyal et licite (2.4.1) et qui comprend des obligations liées à la finalité du traitement (2.4.2), ainsi qu'à la qualité des données (2.4.3). De plus, des exigences relatives au droit d'opposition (2.4.4) et à la confidentialité et sécurité (2.4.5) sont reprises dans la loi vie privée. Finalement, d'autres exigences doivent être respectées par les acteurs jouant un rôle dans la technologie du *shopper tracking* (2.4.6).

2.4.1. Traitement loyal et licite

En premier lieu, l'article 4, § 1er, 1°, de la loi impose que les données à caractère personnel soient traitées de manière loyale et licite. Alors que la loyauté renvoie à l'obligation de transparence dans la réalisation d'opérations sur les données, la licéité induit le respect des autres normes juridiques s'appliquant en raison du traitement[2].

Le principe de la transparence doit être respecté dès le premier traitement effectué sur des données, c'est-à-dire la collecte. Cela implique qu'à ce moment, une information complète et effective doit être fournie à la personne concernée. De fait, un traitement est loyal si la personne est avertie non seulement de l'existence du traitement, mais aussi des autres informations devant être obligatoirement fournies en vertu de l'article 9 de l'instrument législatif[3]. Cette disposition couvre deux hypothèses distinctes : celle où la collecte est réalisée directement auprès de la personne concernée et celle où les données n'ont pas été collectées auprès de la personne concernée. Dans la situation du *shopper tracking*, il s'agit d'une collecte directe, et l'article 9, § 1er, de la LVP trouve à s'appliquer. Le responsable du traitement doit, dès lors, mettre les personnes concernées au courant de son identité, des finalités poursuivies par le traitement, de l'existence d'un droit de s'opposer, ainsi que

1. Certaines de ces exigences sont assorties d'exceptions, mais ces dernières ne sont pas d'application dans le cadre de cette analyse.
2. Th. Léonard et Y. Poullet, *op. cit.,* p. 385 ; Th. Léonard, « E-marketing et protection des données à caractère personnel », *ASBL Droit & Nouvelles Technologies*, 2000, http://www.droit-technologie.org/dossier-17/e-marketing-et-protection-des-donnees-a-caractere-personnel.html, p. 12.
3. C. Colin et Y. Poullet, *op. cit.,* p. 115 ; Th. Léonard et Y. Poullet, *op. cit.,* p. 385.

d'autres informations complémentaires, qui, en vertu des circonstances spécifiques de l'espèce, sont nécessaires afin d'assurer la loyauté du traitement[1]. Ainsi, outre l'information concernant les données traitées, la personne doit également être informée des applications pour lesquelles les données en question seront utilisées[2]. De plus, l'information doit revêtir une certaine qualité, puisqu'elle doit être claire, compréhensible par un public non initié, visible et accessible de manière aisée et permanente[3]. Cela signifie que l'information doit être directement communiquée à la personne concernée et qu'il n'est pas suffisant que les renseignements « soient disponibles quelque part »[4].

La transparence constitue non seulement une condition préalable et indispensable à un consentement valable, mais également un prérequis à l'application d'autres droits reconnus à la personne concernée, comme le droit d'accès ou d'opposition[5]. En effet, « la personne concernée ne peut s'intéresser à et s'informer sur un traitement dont elle ne soupçonne pas l'existence »[6]. En outre, le principe de la loyauté du traitement et son corollaire, la transparence, jouent un rôle central dans le respect du droit à l'autodétermination informationnelle dont bénéficie chaque individu. Ce droit, qui trouve son fondement dans les principes fondamentaux du droit au développement personnel et de la dignité humaine, accorde à chaque individu le pouvoir de poser lui-même un choix au sujet des traitements effectués sur ses données à caractère personnel[7]. Étant donné que les développements technologiques impliquent un affaiblissement de la maîtrise de chaque individu sur son environnement informationnel, ce phénomène doit être compensé par une application effective de ses droits et, notamment, de ceux qui ne peuvent être mis en œuvre qu'à la suite d'une information[8].

Le respect de cette exigence n'impliquerait pas de grands investissements, ni en temps ni en argent, et pourrait prendre plusieurs formes, en fonction de ce qui semble le plus adapté aux circonstances concrètes. Par exemple, le Groupe 29, au sujet des puces RFID, a considéré que l'obligation de rendre le traitement transparent pouvait être respectée par l'affichage de panneaux précisant que de telles puces sont utilisées[9]. Ces affiches doivent, en outre, comprendre les autres éléments devant être transmis aux personnes concernées, comme le nom du responsable du

1. L'article 9, § 1er, de la loi pointe, comme illustration d'informations supplémentaires : « les destinataires ou les catégories de destinataires des données, le caractère obligatoire ou non de la réponse, ainsi que les conséquences éventuelles d'un défaut de réponse, l'existence d'un droit d'accès et de rectification des données ».
2. C. Colin et Y. Poullet, *op. cit.,* p. 116.
3. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, *op. cit.*, p. 18.
4. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, juillet 2011, 01197/11/FR, *WP* 187, p. 22.
5. J. Eynard, *op. cit.,* p. 196 ; Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 9 ; D. Le Métayer, « Privacy by design : a matter of choice », *in Data Protection in a Profiled World,* Dordecht, Springler, 2010, p. 330.
6. C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 39.
7. A. Rouvroy et Y. Poullet, « The right to informational self-determination and the value of self-development : reassessing the importance of privacy for democracy », *in Reinventing Data Protection*, Dordrecht, Springer, 2009, p. 56.
8. C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 40.
9. C. Colin et Y. Poullet, *op. cit.,* p. 116.

traitement, la personne chez qui exercer le droit d'accès ou, encore, la possibilité d'exprimer son refus de participer au traitement. Dans une opinion au sujet de la vidéosurveillance, le Groupe 29 a précisé que l'endroit surveillé devait être indiqué de manière non ambiguë et que les affiches devaient être synthétiques, visibles, efficaces et d'une taille proportionnée par rapport aux lieux[1]. Il est pertinent de transposer ces enseignements relatifs à l'affichage dans l'hypothèse du *retail analytics*. D'autres canaux de communication peuvent être envisagés afin que toute personne entrant dans un établissement où est mise en œuvre la technologie du *shopper tracking* soit au courant de celle-ci, telles une inscription dans les journaux publicitaires ou sur le site Web du magasin ou une annotation sur les tickets de caisse. Le fait de placer cette information sous divers formats permettrait de toucher plus largement les personnes concernées, puisque chaque individu peut être plus sensible à l'un ou l'autre canal d'information.

2.4.2. Exigences liées à la finalité du traitement

Des exigences sont également imposées en ce qui concerne les finalités poursuivies par le responsable du traitement. En effet, les finalités doivent être « déterminées, explicites et légitimes et [les données collectées ne peuvent] pas être traitées ultérieurement de manière incompatible avec ces finalités »[2]. Alors que deux exigences ne nécessitent pas de commentaires supplémentaires (*déterminées* et *explicites*), les deux autres peuvent être succinctement précisées.

Avant tout, un traitement ultérieur de données qui ont été collectées pour la réalisation d'un premier traitement ne pourra être acceptable que s'il vise des finalités identiques ou compatibles à celles de ce traitement originel, à moins qu'il ne fasse l'objet d'une nouvelle base de légitimation[3]. Afin d'apprécier la compatibilité d'une finalité avec celle d'origine, le critère des prévisions raisonnables de la personne concernée doit être pris en considération : est-ce que celle-ci est « en mesure de supposer, au début du procédé de traitement des données, que […] [les données collectées] pourront être traitées d'une autre manière »[4] ? Une réponse négative à cette question induit que le traitement ultérieur est incompatible et qu'il constitue un traitement à part entière devant respecter le prescrit légal[5].

Ensuite, il est admis qu'afin qu'une finalité soit légitime, cette dernière « ne peut causer un préjudice plus grand que l'intérêt que représente le traitement »[6]. Ainsi, le responsable du traitement doit « procéder à un examen de proportionnalité entre »[7],

1. Groupe de travail « Article 29 », avis 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, février 2004, 11750/02/FR, *WP* 89, p. 19.
2. Article 4, § 1er, 2°, LVP.
3. C. Colin et Y. Poullet, *op. cit.,* p. 117.
4. *Ibid*., p. 118.
5. *Ibid.* ; C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 31.
6. C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 28.
7. Y. Poullet, « Pour une troisième génération de réglementation de protection des données », *op. cit.,* p. 45.

d'une part, ses propres intérêts et, d'autre part, ceux de la personne concernée. L'article 5 de la LVP reprend une liste de présomptions, d'hypothèses qui peuvent, abstraitement et *a priori*, rendre un traitement légitime, tels le consentement de la personne concernée ou la réalisation d'une balance des intérêts entre les parties. Si un traitement rentre dans une de ces hypothèses, il convient de réaliser une vérification ultérieure et concrète du respect de la légitimé du traitement, c'est-à-dire de sa compatibilité avec l'exigence de l'article 4, § 1er, 2°, de l'instrument législatif[1]. En d'autres termes, le fait qu'une des conditions de l'article 5 soit remplie n'entraîne pas automatiquement que l'exigence de légitimité inscrite à l'article 4 soit *de facto* rencontrée, ces deux dispositions s'appliquant de manière cumulative[2].

Dans le cadre du *retail analytics*, deux bases prévues à l'article 5 de la loi pourraient être invoquées par le responsable du traitement pour légitimer les opérations sur les données : le consentement (a) et la mise en balance des intérêts des parties (b).

a. Consentement

L'article 5, a), de la LVP indique que le consentement, c'est-à-dire « toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée […] accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »[3], peut constituer une base de légitimité du traitement. De cette définition ressortent divers éléments qu'il convient d'analyser individuellement.

En premier lieu, le fait qu'un consentement soit constitué par *toute manifestation de volonté* pointe vers une interprétation large de la notion. Au minimum, l'expression peut revêtir la forme de « tout type de signe, suffisamment clair pour permettre d'exprimer la volonté d'une personne concernée et être compris par le responsable du traitement »[4]. Les éléments *manifestation de volonté* et *accepte* induisent cependant la nécessité d'une action, qu'il s'agisse d'une signature, d'une déclaration orale ou d'un « comportement dont on peut raisonnablement déduire un accord »[5]. Dans son opinion relative au consentement, le Groupe 29 propose une illustration pouvant éclairer le raisonnement dans le cadre du *retail analytics*. Il s'agit des panneaux publicitaires Bluetooth, qui envoient, aux personnes passant à proximité, des messages sollicitant l'établissement d'une connexion Bluetooth, afin de leur adresser par la suite des publicités. Les messages publicitaires ne sont envoyés qu'aux personnes qui ont activé la fonction Bluetooth de leur téléphone. Néanmoins, le fait d'avoir activé cette fonction n'équivaut pas, à lui seul, à un consentement valable, cette activation pouvant avoir eu lieu à d'autres fins. La manifestation de la volonté est établie lorsque la personne, après avoir été informée du service, décide de s'approcher, à

1. C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 30 ; TH. LÉONARD, *op. cit.*, p. 11.
2. C. DE TERWANGNE, *op. cit.*, p. 98 ; TH. LÉONARD et Y. POULLET, *op. cit.,* p. 384.
3. Article 2, § 8, LVP.
4. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, *op. cit.,* p. 12.
5. *Ibid.*

quelques centimètres, du panneau publicitaire. Généralement, dans la pratique, il reste malaisé pour le responsable du traitement de déduire un consentement « en l'absence de comportement actif de la personne concernée »[1].

En second lieu, le consentement doit être libre, ce qui signifie qu'il doit être donné sans pression ni contrainte physique ou psychologique et sans risque de discrimination en cas de refus[2]. Il a été précisé qu'un consentement n'était pas libre si les répercussions de l'absence de consentement restreignaient la liberté de choix des personnes[3]. De surcroît, le consentement doit être spécifique pour chaque finalité précise annoncée par le responsable pour le traitement de données. Cela signifie qu'il ne peut pas être donné pour un objet général[4] ou par « l'intermédiaire de l'acceptation des conditions générales »[5]. Aussi, si le responsable du traitement modifie significativement les finalités du traitement ou en ajoute, une nouvelle acceptation de la personne concernée doit être obtenue[6]. Cette exigence implique également que le consentement doit revêtir certaines qualités : il doit être intelligible, mentionner clairement et précisément l'étendue du traitement et ses effets, et doit porter sur les divers aspects du traitement en question. Les attentes raisonnables de la personne concernée doivent être prises en considération pour déterminer si le consentement est suffisamment spécifique. Le caractère *spécifique* d'un traitement est « intrinsèquement lié au fait que le consentement doit être informé »[7]. D'ailleurs, suivant la disposition susmentionnée, le consentement doit également être éclairé, ce qui implique une obligation pour le responsable du traitement de communiquer à la personne concernée toutes les informations nécessaires « à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés »[8]. L'information, qui doit être fournie sous une forme compréhensible, doit survenir préalablement au consentement de la personne concernée. Cette dernière doit être en mesure de pleinement comprendre les répercussions de son acceptation[9]. L'information doit être de qualité, comme cela a été exposé dans le point 2.4.1.

Outre ces éléments repris de la définition, le consentement doit respecter d'autres exigences, notamment le fait de pouvoir être retiré, par la personne concernée, à tout moment[10]. De plus, l'article 5, a), de la loi précise que le consentement doit être indubitable, ce qui signifie que la procédure suivie pour l'obtention du consentement « ne doit laisser aucun doute quant à l'intention de la personne concernée de donner son consentement »[11]. Aucune ambiguïté relative à l'acceptation de la personne,

1. *Ibid.*, p. 13.
2. C. Colin et Y. Poullet, *op. cit.,* p. 120 ; Th. Léonard, *op. cit.*, p. 17.
3. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, *op. cit.,* p. 14.
4. Th. Léonard, *op. cit.*, p. 17.
5. Groupe de travail « Article 29 », avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, *op. cit.*, p. 20.
6. *Ibid.*, pp. 15 et 16.
7. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, *op. cit.,* p. 19.
8. Th. Léonard et Y. Poullet, *op. cit.,* p. 380.
9. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 19 ; Th. Léonard, *op. cit.*, p. 18.
10. C. Colin et Y. Poullet, *op. cit.,* p. 120.
11. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, *op. cit.,* p. 23.

aucun doute sur son intention ne peuvent subsister. Selon certains, cette qualité insinue que le consentement devrait être explicite et que doivent être préférés des systèmes de type *opt-in* à ceux d'*opt-out*. D'après eux, un consentement implicite ne remplirait pas l'exigence du consentement non ambigu[1].

Une fois que tous les composants du consentement ont été appréhendés, il convient de s'interroger au sujet de deux arguments qui pourraient être avancés par le responsable du traitement. Ce dernier peut, premièrement, estimer que le consentement de la personne concernée est, dans le cas du *retail analytics*, implicite, puisqu'il découle du fait que la personne a décidé, de sa propre initiative, de rentrer dans un magasin où des mécanismes de *shopper tracking* sont mis en œuvre et qu'elle a choisi de laisser ses fonctions Wi-Fi et/ou Bluetooth allumées. Pour que cet argument puisse tenir, il faut qu'il soit incontestable que la personne a été informée du traitement, mais aussi des finalités, des moyens de s'opposer, des conséquences de son acceptation et des autres éléments précités et qu'en connaissance de cause, elle ait décidé de maintenir les fonctions de son téléphone portable activées. De plus, il convient de prendre en considération l'enseignement concernant la manifestation de la volonté tiré de l'illustration du Groupe 29 sur les panneaux publicitaires Bluetooth et le fait qu'une action doit intervenir, tout en gardant à l'esprit que, généralement, ces fonctions sont continuellement activées. Enfin, le responsable du traitement devra également démontrer que le consentement de la personne concernée est dénué d'ambiguïté, ce qui pourrait poser problème. Deuxièmement, le responsable du traitement pourrait également mettre en avant la possibilité d'*opt-out* qu'il met à disposition des individus, par exemple sur son site Web. De nouveau, il convient d'analyser l'ensemble des exigences susmentionnées pour déterminer si le consentement est valable.

En guise de conclusion, trois remarques supplémentaires peuvent être ajoutées. Tout d'abord, il appartient au responsable de démontrer qu'un consentement a été valablement donné, notamment en cas de litige entre les parties. Il est donc dans son intérêt de conserver des preuves attestant « que le consentement a effectivement été donné »[2]. Ensuite, il ressort d'une étude de 2011 que 74 % des personnes interrogées considèrent que leur consentement spécifique devrait être exigé avant tout traitement de données à caractère personnel[3]. Finalement, le futur règlement général sur la protection des données[4], en son considérant 25, contiendra l'exigence expresse d'un consentement explicite.

1. *Ibid*. ; C. Colin et Y. Poullet, *op. cit.,* p. 120 ; Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 19.
2. Groupe de travail « Article 29 », avis 15/2011 sur la définition du consentement, *op. cit.,* p. 24.
3. TNS Opinion & Social, *op. cit.,* p. 153.
4. Considérant 25 de la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), *COM*(2012) 11.

b. Mise en balance des intérêts

L'article 5, f), de la LVP propose une autre base de légitimité qui peut s'appliquer dans le cadre du *shopper tracking*. Un traitement peut être réalisé s'il « est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement […] à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ». Un équilibre doit être trouvé par le responsable du traitement entre son intérêt légitime et les droits et libertés de la personne concernée. Les commerçants ont effectivement un intérêt légitime à la collecte et au traitement des adresses MAC et des données de localisation, puisqu'il est important pour eux de connaître les habitudes de consommation de leurs clients dans l'objectif d'optimiser l'organisation et l'agencement de leur surface commerciale.

Cependant, cette base de légitimité entraîne des difficultés. De fait, certains estiment qu'il est étonnant que le seul intérêt du responsable du traitement puisse constituer une base suffisante pour justifier d'un traitement sans le consentement de la personne concernée et les garanties qui y sont inhérentes, d'autant plus que la prévalence des droits et intérêts des personnes concernées apparaît être faible pour constituer une protection véritablement effective[1]. De plus, cette hypothèse de légitimité ne va pas dans le sens de la protection du citoyen qui est prônée dans le cadre législatif.

En conclusion, l'article 5 de la LVP prévoit deux bases de légitimité pouvant être avancées dans le cadre du *retail analytics.* Cependant, chacune présente des fragilités. D'une part, le responsable du traitement peut se baser sur le consentement de la personne concernée, base de légitimité qui offre des garanties à la personne concernée, notamment en raison des exigences liées à l'information ou la nécessité d'une action dans son chef. Concrètement, pour obtenir le consentement, le responsable pourrait mettre en place, lors d'un passage obligatoire pour entrer dans le magasin, des affiches visibles indiquant non seulement qu'un traitement aura lieu passé cet endroit, mais aussi les mentions obligatoires exposées ci-dessus et expliquant qu'il est possible de désactiver les fonctions Wi-Fi et Bluetooth de son téléphone portable. Toutefois, il pourra être extrêmement malaisé et lourd pour le responsable du traitement de prouver, par exemple devant la Commission de la protection de la vie privée ou devant un juge, qu'il a obtenu un consentement qui répond à toutes les exigences précitées, particulièrement les caractères non ambigu, libre et manifeste. De plus, obtenir un tel consentement diminuerait pour les responsables l'intérêt de l'analyse des comportements de consommation. Par ailleurs, le responsable du traitement peut invoquer avoir réalisé une mise en balance des intérêts réciproques des parties, et que celle-ci a penché, à la suite d'une analyse, en sa faveur. Le traitement pourrait alors être mis en œuvre sans que la personne concernée n'y ait consenti. Cette base est néanmoins fragile en raison de la grande difficulté pour le

1. J. EYNARD, *op. cit.,* p. 199.

responsable du traitement de démontrer, devant les autorités susmentionnées, que son intérêt est plus élevé que les droits de la personne concernée, notamment le droit au respect de sa vie privée. Finalement, en outre de la base de légitimité de l'article 5, qu'il s'agisse du consentement ou de la mise en balance des intérêts, le responsable du traitement doit prouver *in concreto* que le traitement qu'il entreprend est bel et bien légitime, comme le prescrit l'article 4 de la LVP.

2.4.3. Exigences de qualité des données

L'article 6, § 1er, 3° et 4°, prévoit que les données doivent être « adéquates, pertinentes et non excessives au regard des finalités », mais aussi « exactes et, si nécessaire, mises à jour ». De plus, le point 5 de la même disposition prescrit que les données ne peuvent pas être « conservées sous une forme permettant l'identification des personnes concernées » pour une durée qui excède « celle nécessaire à la réalisation des finalités ». À ce sujet, le Groupe 29 précise que le délai de conservation des données doit être réduit au minimum nécessaire et que le responsable du traitement « doit être en mesure de justifier la nécessité »[1] d'un tel délai par des arguments pertinents et concrets. Les objectifs poursuivis par cette obligation sont le respect du principe de proportionnalité et la garantie de la transparence et de la légitimité du traitement[2].

Avec cette question de la qualité des données, la distinction entre les données pseudonymisées et les données anonymisées survient de nouveau. En effet, si le responsable ou le sous-traitant conserve des données codées, il est tenu par ce principe de proportionnalité et par les exigences précitées, puisqu'il s'agit de données à caractère personnel.

2.4.4. Droit d'opposition

Le responsable du traitement est tenu d'assurer, en vertu de l'article 12, § 1er, alinéas 2 et suivants, de la LVP, un droit d'opposition aux personnes concernées. Deux situations différentes peuvent être dégagées. Premièrement, la personne concernée peut s'opposer, sans justification, au traitement réalisé à des fins de marketing direct. Cette hypothèse ne s'applique pas ici. Deuxièmement, la personne concernée peut s'opposer à tout traitement de ses données « pour des raisons sérieuses et légitimes tenant à une situation particulière ». Ce droit joue un rôle central dans l'hypothèse où la base de légitimation du traitement est celle inscrite à l'article 5, f), de la loi, c'est-à-dire qu'à la suite de la réalisation d'une balance des intérêts en présence, le responsable du traitement a considéré « qu'il pouvait légitimement traiter les données »[3]. L'article 12 prévoit donc la possibilité pour la personne concernée d'exprimer son opposition face à un traitement qui a été réalisé

1. V. Verbruggen, *op. cit.,* p. 71.
2. *Ibid.,* p. 72.
3. C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 41.

sans son consentement, sur la base d'une balance opérée par le responsable et, *in fine,* à l'avantage de ce dernier[1].

2.4.5. Confidentialité et sécurité

La confidentialité et la sécurité des traitements sont prévues par l'article 16 de la LVP. Le responsable de traitement ainsi que l'éventuel sous-traitant sont tenus de mettre en œuvre « les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel »[2] contre toute destruction, accès non autorisé, perte ou modification et contre toute autre forme de traitement illicite. En outre, la personne concernée doit pouvoir « contrôler les accès […] qui ont eu lieu »[3], afin d'être capable de vérifier si des mesures de sécurité liées à l'accès ont été mises en place[4]. Le niveau de sécurité à assurer doit être approprié en prenant en compte le coût de la mise en place, l'état de l'art, les risques du traitement et la nature des données. L'article 16 de l'instrument législatif comporte également des obligations relatives au sous-traitant qui doit également apporter des garanties de sécurité technique et organisationnelle par rapport aux traitements en cause.

Par exemple, la cryptologie ou l'anonymisation des données, en ce qu'elles permettent de garantir que les données conservées par le responsable du traitement ne soient pas directement compréhensibles en cas d'accès non autorisé ou de perte de données, assurent la sécurité du système d'information. Une protection doit également être mise en place au niveau du système lui-même. De manière concrète, la réalisation de hachages unidirectionnels successifs des adresses MAC avant que celles-ci ne soient conservées ou la sécurisation des serveurs sur lesquels les numéros d'identification sont stockés participent à garantir le respect de l'exigence de sécurité.

2.4.6. Autres obligations

D'autres obligations sont inscrites dans la loi ou ont été déduites par la doctrine. Cette partie reprendra celles apparaissant comme pertinentes à l'occasion de la présente analyse.

Primo, l'article 10, § 1er, de la loi porte sur le droit de la personne concernée à l'accès, sous une forme intelligible, à toutes les données la concernant et détenues par le responsable du traitement ou le sous-traitant. Il garantit également à chaque individu le droit de recevoir « la confirmation que des données [le] concernant sont ou ne sont pas traitées » et d'obtenir des renseignements au sujet des finalités, des catégories de données traitées, des destinataires éventuels des données et de leur

1. *Ibid.*
2. Article 16, § 4, LVP.
3. C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 35.
4. *Ibid.*

origine. Dès lors, les individus concernés par le traitement opéré dans le cadre du *shopper tracking* peuvent obtenir plus d'informations sur ce mécanisme. Comme il a été exposé, la demande d'accès peut être adressée au responsable du traitement ou au sous-traitant, si cette fonction lui a été déléguée. Lié à ce droit d'accès, l'article 12, § 1er, alinéa 1er, précise que la personne concernée peut bénéficier de la rectification de données inexactes la concernant.

Secundo, en vertu de l'article 17, § 1er, de la LVP, les responsables de traitement ont l'obligation de notifier à l'autorité nationale de contrôle visée à l'article 23 de l'instrument (en Belgique, à la Commission de la protection de la vie privée) tout traitement de données à caractère personnel qui sera réalisé, sous réserve d'exceptions prévues dans les textes législatifs ou réglementaires. Ces déclarations étant conservées dans un registre public et géré par l'autorité nationale, tout individu peut avoir accès à celles-ci. C'est ainsi qu'ont été obtenues certaines des informations au sujet de la société Amoobi qui servent de base à la présente analyse.

Tertio, il est inscrit, à l'article 15*bis* de la loi, que le responsable du traitement qui cause dommage à autrui en raison d'« un acte contraire aux dispositions déterminées par ou en vertu de la […] loi » est tenu de réparer ledit préjudice. En outre, le Groupe 29 suggère que la responsabilité soit accompagnée d'un corollaire[1] : l'obligation d'apporter la preuve qu'ont effectivement été mises « en œuvre des mesures appropriées et efficaces en vue de garantir le respect des principes et obligations prévus »[2] par les normes juridiques applicables en la matière.

Quarto, la doctrine a déduit, d'une série de dispositions, un droit de la personne concernée à ne pas être pistée. Ce droit est apparu en raison du développement de l'Internet des choses et particulièrement de l'usage des puces RFID. L'idée derrière ce droit de ne pas être suivi à la trace est que les individus doivent disposer de la possibilité de « se déconnecter de leur environnement réseau à tout moment »[3]. Les autorités européennes ont également réagi face à ce phénomène et, notamment, la Commission européenne qui a émis des lignes de conduite pour que l'exploitation des applications RFID soit réalisée de manière éthique, licite, politiquement et socialement acceptable et dans le respect du droit à la vie privée et de la protection des données à caractère personnel[4]. Une extension de ce droit en ce qui concerne la géolocalisation par le téléphone portable pourrait être envisagée.

1. Groupe de travail « Article 29 », avis 3/2010 sur le principe de la responsabilité, juillet 2010, 00062/10/FR, *WP* 173, p. 10.
2. C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 378.
3. *Ibid.,* p. 45.
4. *Ibid.*

3. Mesures envisageables

Comme cela a été précédemment exposé, les règles juridiques s'adaptent à la création de nouveaux modèles et services qui est inhérente aux développements des technologies. Mais il convient de s'interroger : est-ce que le droit est, à l'heure actuelle, suffisant pour assurer la protection des citoyens face aux traitements de leurs données à caractère personnel ? Certains répondent par la négative à cette question et affirment que d'autres mesures doivent être prises en complément du cadre juridique[1].

Diverses solutions, qui seraient mises en œuvre soit par les acteurs privés (3.1), soit par les autorités compétentes en matière de protection des données (3.2), peuvent être appréhendées.

3.1. Acteurs privés

Des acteurs privés peuvent intervenir dans le sens du respect du droit de la protection des données et, principalement, le responsable du traitement et le sous-traitant. Ceux-ci, en plus de se conformer à la législation, peuvent prendre des mesures proactives qui démontrent leur volonté de respecter les objectifs de la loi du 8 décembre 1992[2].

Trois mesures principales seront présentées : le principe de la *privacy by design* (3.1.1), l'autorégulation (3.1.2) et un mécanisme de désinscription globale (3.1.3). D'autres dispositifs plus ponctuels seront ensuite exposés (3.1.4).

3.1.1. *Privacy by design*

La technologie elle-même peut apporter une solution dans l'objectif d'assurer le respect de la protection des données. Dans le schéma qui semble le plus commun pour l'analyse des comportements de consommation par la géolocalisation, il apparaît que le sous-traitant est celui qui conçoit et fabrique le mécanisme. Dès lors, il est celui concerné par le concept de la *privacy by design*. En effet, il est de plus en plus considéré qu'en outre de la responsabilité portée par le responsable du traitement, les organismes créant les applications, mécanismes ou systèmes d'exploitation, c'est-à-dire les technologies, partagent également une fraction de la responsabilité du respect de la protection des données[3]. Cette idée est appréhendée sous le terme de *privacy by design* ou, en français, *protection intégrée de la vie privée,* qui peut

1. Y. Poullet, « About the E-Privacy directive : towards a third generation of data protection legislation », *op. cit.*, p. 29.
2. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 22.
3. Commission européenne, *Technologies renforçant la protection de la vie privée*, Bruxelles, mai 2007, Mémo/07/159, p. 1 ; J. Eynard, *op. cit.,* p. 311.

être définie comme un ensemble de principes qui assurent le respect de la vie privée et de la protection des données dès la conception des technologies[1].

Diverses évocations de ce mécanisme se trouvent dans la loi vie privée et dans la directive (CE) n° 95/46, par exemple à l'article 4 de la loi qui concerne la qualité des données et à l'article 16 du même instrument relativement à la sécurité et à la confidentialité. En outre, au considérant 46 de la directive, il est précisé que, « tant au moment de la conception qu'à celui de la mise en œuvre du traitement », des mesures techniques et organisationnelles adéquates doivent être prises[2].

D'après le Bureau du commissaire à l'Information et à la Protection de la vie privée de l'Ontario, les grands principes qui fondent la *privacy by design* sont au nombre de sept. Tout d'abord, la *privacy by design* soutient la prise de décisions proactives afin de prévenir les atteintes à la vie privée[3]. Ainsi, les concepteurs doivent, de manière autonome et anticipée, mettre en place des mesures de sécurité[4]. Le second principe implique que la protection de la vie privée et des données doit être systématique, intégrée dans le système[5]. Dès lors, le mode par défaut de la technologie doit être un mode en faveur de la protection des données[6]. Troisièmement, la protection des droits est intégrée dans la conception des pratiques et de l'architecture des systèmes. Ce mécanisme est appelé la *Privacy Enhancing Technology* (ci-après, « PET »)[7]. Le but poursuivi par les outils et systèmes participant à ce mécanisme est d'assurer au mieux le respect du droit au respect de la vie privée et de la protection des données. Ainsi, la protection de ces droits doit être envisagée comme une « partie intégrante des fonctions du système d'information »[8], et non pas comme une fonctionnalité annexe. De nombreuses techniques participent à la PET, comme la limitation de la collecte des données à ce qui est strictement nécessaire ou la présentation conviviale et simple des dispositifs liés au respect des droits[9]. De manière plus concrète, parmi les mécanismes de PET, on peut citer le cryptage[10] ou « l'anonymisation automatique après un certain laps de temps »[11]. Le quatrième principe promeut la fin des fausses dichotomies qui impliquent des compromis réciproques inutiles, comme « celle qui oppose la protection de la vie privée à la

1. C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36.
2. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 14.
3. PRIVACY BY DESIGN, *7 principes fondamentaux,* http://www.viepriveeintegree.ca/index.php/a-propos-de-la-pivp/sept-principes-fondamentaux.
4. C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36.
5. PRIVACY BY DESIGN, *7 principes fondamentaux, op. cit.*
6. C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36 ; C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 50 ; Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 14 ; Y. POULLET et J.-M. DINANT, *Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunication : l'autodétermination informationnelle à l'ère de l'Internet : éléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif*, Strasbourg, Conseil de l'Europe, Faculté de droit, Centre de recherche Information, Droit et Société, 2004, p. 55.
7. PRIVACY BY DESIGN, *7 principes fondamentaux, op. cit.*
8. C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36 ; Y. POULLET et J.-M. DINANT, *op. cit.*, p. 56.
9. COMMISSION EUROPÉENNE, *Technologies renforçant la protection de la vie privée*, *op. cit*., p. 2 ; C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36 ; Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 16 ; D. LE MÉTAYER, *op. cit.,* p. 330.
10. D. LE MÉTAYER, *op. cit.,* p. 323.
11. COMMISSION EUROPÉENNE, *Technologies renforçant la protection de la vie privée*, *op. cit*., p. 2.

sécurité »[1] par la démonstration de la réalisation de ces objectifs de manière concomitante. Ensuite, les principes de la *privacy by design* doivent être respectés durant l'entièreté de la période de conservation des données à caractère personnel traitées[2]. Sixièmement, le fonctionnement et les éléments composant le système doivent être transparents et visibles. Finalement, le respect de la vie privée des utilisateurs doit, en tout temps, être placé au centre des préoccupations des concepteurs[3].

À l'heure actuelle, bien que certains affirment que de l'art en matière de technologie permette que soient mis en place les principes de la *privacy by design*, il a été observé que la plupart des systèmes sur le marché ne les respectent pas, voire vont à leur encontre[4]. Pour assurer à ces principes plus d'effectivité, l'État pourrait jouer un rôle, par exemple, en octroyant des subsides aux centres de recherche développant des technologies se basant sur les principes susmentionnés ou en mettant en place des « systèmes volontaires de certification ou d'accréditation des solutions élaborées »[5] et en assurant la publicité de ces systèmes.

En conclusion, par le biais de ce principe qui s'ajoute au cadre juridique, la solution viendrait des technologies elles-mêmes et repose principalement sur le secteur privé[6]. Respecter la *privacy by design* n'apparaît pas inaccessible, mais il est essentiel que les principes applicables en droit au respect de la vie privée et en droit de la protection des données soient connus des concepteurs et des fabricants[7].

3.1.2. Autorégulation

En outre du cadre juridique, l'autorégulation pourrait jouer un rôle en apportant une plus-value aux règles législatives tant au niveau de leur effectivité qu'au niveau de leur contenu. Ainsi, l'article 27 de la directive prévoit que « l'élaboration des codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises en application de la présente directive » doit être encouragée par les États membres et la Commission. Comme le suggèrent les paragraphes 2 et 3 de la disposition précitée, il conviendrait d'accompagner les projets de code d'un contrôle ou d'un encadrement pour s'assurer de leur conformité avec la législation. Ce contrôle pourrait être réalisé par les autorités nationales de protection des données[8].

1. PRIVACY BY DESIGN, *7 principes fondamentaux, op. cit.*
2. *Ibid.* ; C. DE TERWANGNE et J.-N. COLIN, *op. cit.*, p. 36.
3. PRIVACY BY DESIGN, *7 principes fondamentaux, op. cit.*
4. D. LE MÉTAYER, *op. cit.,* p. 326.
5. Y. POULLET et J.-M. DINANT, *op. cit.*, p. 56.
6. C. DE TERWANGNE et J.-N. COLIN, *Défis pour la vie privée et la protection des données posés par la technologie*, Namur, FUNDP, 2011, p. 14 ; COMMISSION EUROPÉENNE, *Technologies renforçant la protection de la vie privée*, *op. cit.*, p. 2.
7. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 17 ; D. LE MÉTAYER, *op. cit.,* p. 330.
8. Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *op. cit.,* p. 47.

L'autorégulation représente une opportunité pour les sociétés privées d'un secteur spécifique de s'auto-imposer des règles allant dans le sens, voire au-delà du cadre réglementaire et de présenter aux citoyens une image positive. Une pression joue sur les participants, ce qui les incite à respecter les règles établies. Cependant, des faiblesses de ce mécanisme peuvent être pointées. Ainsi, la mise en place du code, son adhésion et le respect de ses règles ne reposent que sur la bonne volonté des acteurs. Ensuite, les règles ne sont établies que par les acteurs privés, ce qui peut entraîner un déséquilibre, même inconscient, entre les intérêts des parties[1].

Un code de conduite, mettant l'accent sur la transparence et la sécurité des données et se positionnant dans le sens de la protection des consommateurs, a été réalisé aux États-Unis par un groupe de sociétés offrant des services de *retail analytics*[2]. Le code contient sept articles et une liste de définitions. Parmi les dispositions, plusieurs s'avèrent intéressantes pour la présente analyse[3]. Tout d'abord, l'article 1er concerne l'information, qui doit être fournie aux clients et respecter certaines caractéristiques telles que la clarté, la concision et un format standard. Ces sociétés doivent également disposer des affiches dans des endroits qui attirent l'attention afin d'informer de la collecte et des traitements subséquents. Le code évoque également la création d'une icône type qui contiendrait les informations essentielles devant être communiquées ainsi qu'un renvoi vers un lieu où des informations complémentaires sur les mécanismes peuvent être obtenues[4]. Toutefois, il est précisé que, si les données sont agrégées ou non uniques à un individu, il n'est pas requis d'informer les consommateurs de la collecte[5]. Le second principe exige que la collecte soit limitée aux données nécessaires pour réaliser les services d'analyse. Si des informations personnelles ou des informations concernant un équipement unique, telles que les adresses MAC, sont collectées, elles doivent immédiatement être anonymisées, sauf si le consommateur a donné son consentement[6]. D'ailleurs, le troisième principe est lié au consentement. Il affirme que les sociétés proposant ces services doivent offrir aux consommateurs la possibilité de refuser que leurs téléphones portables soient utilisés dans le cadre de ces services d'analyse. Doivent alors être fournies les informations nécessaires pour exercer ce choix, soit auprès de la société en question, soit auprès d'une base de données commune où il est possible de réaliser une

1. C. de Terwangne et J.-N. Colin, *Défis pour la vie privée et la protection des données posés par la technologie*, pp. 14 et 15 ; J. Eynard, *op. cit.*, p. 315.
2. A. Grande, *Shopper Tracking Code Overreaches, Retail Group Exec Says*, February 2014, http://www.law360.com/articles/511165/shopper-tracking-code-overreaches-retail-group-exec-says ; J. Romero, *Big Brother Is Watching You (Shop for Pants) : Mobile Analytics Firms Implement Code of Conduct for Tracking Customers While They Shop*, November 2013, http://www.privacyandsecuritymatters.com/2013/11/big-brother-is-watching-you-shop-for-pants-mobile-analytics-firms-implement-code-of-conduct-for-tracking-customers-while-they-shop ; A. Scuria, « Shopper tracking companies adopt new privacy framework », *Law 360*, October 2013, http://www.law360.com/articles/482206/shopper-tracking-companies-adopt-new-privacy-framework.
3. Les autres sont les articles 4 à 7. Alors que l'article 4 concerne la limitation de la collecte et de l'utilisation des données, l'article 5 évoque des transferts consécutifs à des tiers. La sixième disposition est au sujet de la conservation limitée et le septième article se rapporte à l'éducation des consommateurs. Voy. Future of Privacy Forum, *Mobile Location Analytics. Code of Conduct of the 22nd of October 2013, op. cit.*, p. 4.
4. Future of Privacy Forum, *Mobile Location Analytics. Code of Conduct of the 22nd of October 2013, op. cit.*, p. 1.
5. J. Romero, *op. cit.*
6. Future of Privacy Forum, *Mobile Location Analytics. Code of Conduct of the 22nd of October 2013, op. cit.,* p. 3.

désinscription globale. Il existe des exceptions à la règle. Le code précise également dans quelles hypothèses un consentement dit affirmatif du consommateur, un *opt-in*, est requis[1]. Par contre, ce dernier n'est pas nécessaire si l'analyse se limite aux trajectoires des personnes[2].

Un code de bonne conduite qui vient, d'une part, compléter et soutenir le cadre juridique existant et, d'autre part, renforcer son effectivité devrait être encouragé en Europe[3]. En effet, si beaucoup de sociétés y participent, les magasins désirant profiter de ce service devront faire appel à celles-ci, ce qui est finalement bénéfique pour les individus. Les autorités nationales de protection des données, voire le Groupe 29, pourraient guider les acteurs privés dans la rédaction de ce code.

3.1.3. Désinscription commune

Actuellement, certaines sociétés offrant les services d'analyse des comportements de consommation par la géolocalisation intègrent, sur leur site Web, la possibilité pour les possesseurs de téléphone portable de désinscrire leur adresse MAC afin que celle-ci ne puisse être enregistrée par les capteurs disposés dans les magasins dans lesquels une analyse est réalisée. Ainsi, les sociétés Amoobi et WiFiProfs offrent la possibilité d'effacement de l'adresse MAC de leur base de données[4].

Cependant, il est très contraignant de se désinscrire de la sorte auprès de chaque société et il faut encore qu'un tel mécanisme existe et que les consommateurs en soient informés. Une solution peut prendre en compte ces difficultés : la possibilité de se désinscrire de manière commune pour tous les magasins ou du moins auprès de toutes les sociétés de *shopper tracking* qui acceptent de participer à l'initiative. Ce mécanisme est évoqué dans le code de bonne conduite des sociétés de *retail analytics* et mis en place aux États-Unis[5]. De nouveau, une initiative semblable pourrait être prise en Europe, soit par le secteur privé seul, soit avec l'aide des autorités nationales de protection des données ou du Groupe 29.

3.1.4. Autres mesures

D'autres mesures, faciles à mettre en œuvre, pourraient être prises par les responsables du traitement et/ou les sous-traitants impliqués dans les analyses des comportements de consommation par la géolocalisation.

En premier lieu, il peut être envisagé qu'au sein de chaque organisme, soi(en)t désignée(s) une ou plusieurs personnes en charge du respect du cadre législatif en

1. Il s'agit des hypothèses où des informations personnelles sont liées au téléphone portable de la personne ou quand un consommateur sera contacté sur la base des informations collectées dans le cadre du service. Voy. *ibid*.
2. A. Scuria, *op. cit.*
3. C. de Terwangne et J.-N. Colin, *op. cit.*, p. 15.
4. Amoobi, *Opt-out*, http://www.amoobi.com/company/page19/page23/page23.php ; WiFiProfs, *Privacy*, http://www.wifiprofs.com/in-store-retail-analytics/privacy.
5. B. Fung, *op. cit.*

matière de protection des données. Ces personnes seraient sensibilisées à l'importance du respect de la vie privée et de la protection des données et interviendraient dans les décisions touchant à ces concepts[1]. En second lieu, les sociétés proposant les services de *shopper tracking* aux commerçants devraient faire appel à l'autorité nationale de protection des données afin de s'assurer que leur pratique est en conformité avec la législation et afin d'obtenir des conseils. En troisième lieu, des audits ou des rapports de conformité pourraient être mis en œuvre soit par une autorité indépendante, soit par les autorités nationales de protection des données. L'objectif est de vérifier si des mesures sont prises par les sociétés afin d'assurer le respect du cadre juridique. Ainsi, l'autorité désignée pourrait attribuer des labels de qualité à l'occasion d'un système de certification[2]. Enfin, pourrait être prévue, à la suite de la création d'un nouveau service entraînant le traitement de données à caractère personnel, une « mesure de précaution préalable à la mise en œuvre de tels traitements »[3]. Une telle mesure pourrait consister en l'obligation pour le concepteur d'effectuer une « étude d'impact sur la vie privée »[4] de son service.

3.2. Autorités de protection des données

Les autorités nationales de protection des données jouent un rôle primordial en vue de la compréhension et du respect de l'application des règles inscrites dans la directive (CE) n° 95/46 et transposées en droit interne, tout comme le Groupe 29, au niveau européen. Ces organismes émettent des opinions ou décisions au sujet de mécanismes existants ou explicitent des points théoriques par des exemples concrets. Ces documents s'avèrent très utiles dans la pratique.

Il pourrait donc être envisageable qu'avec le développement du phénomène du *retail analytics* en Europe, le Groupe 29 ou les autorités nationales de protection des données, comme la Commission de la protection de la vie privée, rédigent un document afin de clarifier certains points posant problème.

En outre, les autorités nationales de protection des données ont été évoquées plusieurs fois dans le point 3.1. Elles pourraient, en effet, être impliquées dans la rédaction d'un code de bonne conduite, dans l'attribution de labels, dans la réalisation de rapports de conformité ou d'étude d'impact, dans l'apport d'une aide et de conseils ponctuels aux sociétés privées ou, encore, dans la mise en œuvre d'un système de désinscription commune.

1. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* p. 22.
2. Groupe de travail « Article 29 » et Groupe de travail « Police et Justice », *op. cit.,* pp. 17 et 22 ; S. RODOTÀ, « Data protection as a fundamental right », *in Reinventing Data Protection*, Dordrecht, Springer, 2009, p. 82.
3. C. DE TERWANGNE et J.-P. MOINY, *op. cit.,* p. 53.
4. *Ibid.*

Conclusion

L'objectif de cette contribution est double. Tout d'abord, dans une vision théorique, il est intéressant de présenter le phénomène de l'analyse des comportements de consommation par la géolocalisation et de le confronter à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cela a permis de mettre en avant les difficultés se posant lors de l'application de l'instrument législatif à une situation concrète, en l'espèce au service de *retail analytics*. Lors de la présente étude, presque chaque confrontation entre un point de droit et la pratique a nécessité un raisonnement poussé, tel que lors de la qualification des informations collectées en *données à caractère personnel*, lors de l'attribution des rôles de chaque acteur ou, encore, au sujet de la base de légitimité du traitement. La présente analyse a tenté de proposer des réponses claires à ces différentes questions en se basant sur les connaissances actuelles, à la fois techniques et juridiques. Ensuite, différentes mesures qui pourraient, en outre du cadre juridique, assurer le respect des droits des citoyens ont été avancées. En second lieu, cette contribution participe à un mouvement d'éducation des individus au sujet du cadre juridique en matière de protection des données et à un mouvement de sensibilisation face à l'existence des techniques de *shopper analytics*[1]. Ces deux éléments constituent des prérequis indispensables à un comportement réfléchi des consommateurs et à une application effective de leurs droits[2]. Ainsi, ils permettent notamment que les individus soient plus attentifs à la présence éventuelle d'affiches informant de la collecte lors de leur arrivée dans un magasin afin qu'ils puissent désactiver les fonctions Wi-Fi et Bluetooth de leur téléphone portable s'ils ne souhaitent pas y participer. De manière générale, l'analyse a pointé à quel point il est crucial que les personnes soient conscientes et informées du traitement.

La technologie du *retail analytics* s'inscrit dans ce qui est appelé la *société de l'observation*, qui aurait remplacé la *société de l'information*. En raison de ce passage, un débat sociétal doit être tenu afin que les droits et libertés des citoyens, et en particulier ceux liés à la vie privée et à la protection des données, ne soient pas mis au second plan[3]. Dans cette nouvelle perception de la société, des technologies sont développées et des mécanismes et services créés afin d'obtenir une connaissance toujours plus approfondie des personnes. Ainsi, les innovations technologiques ont apporté d'importants avantages tant du point de vue économique que du point de vue sécuritaire[4], mais elles ont également progressivement engendré le développe-

1. Il ressort d'un sondage, réalisé en France, que, « sur un échantillon de jeunes gens âgés de 15 à 24 ans », seuls 33 % de ceux-ci « ont conscience de leurs droits en matière de données à caractère personnel ». Voy. Y. Détraigne et A.-M. Escoffier, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », *Les rapports du Sénat*, n° 441, 2008-2009, p. 67.
2. *Ibid.* ; C. de Terwangne et J.-N. Colin, *op. cit.*, p. 15.
3. C. Colin et Y. Poullet, *Défis pour la vie privée et la protection des données posés par la technologie*, p. 95.
4. *Ibid.,* p. 144.

ment d'une société où « il n'y a virtuellement pas de limites »[1] à l'ingéniosité des hommes pour créer des services impliquant de nouvelles formes de traitement, à la quantité de données qui peut être conservée et à la durée de cette conservation.

Certains peuvent encore être incertains de l'intérêt de cette contribution. En effet, il n'est pas rare, dans le cadre de discussions touchant à la vie privée, d'entendre des réflexions telles que « Ça ne me dérange pas qu'une société privée connaisse le chemin que j'emprunte dans son magasin » ou « C'est également bénéfique pour les consommateurs si le magasin est mieux agencé ». Répondre à ces commentaires revient à démontrer l'importance que revêtent la protection de la vie privée et la protection des données dans la *société de l'observation*. Tout d'abord, le respect de ces droits constitue une condition nécessaire à l'application de plusieurs droits et libertés et au respect du principe de dignité[2]. En vertu de ce principe, l'individu ne peut être appréhendé selon « une vision purement utilitariste »[3] ni considéré comme un « simple objet de la surveillance et du contrôle d'autrui »[4], que cette surveillance soit réalisée par des acteurs publics ou privés. Il implique que ne peut être tolérée une utilisation des données d'une manière qui transforme l'être humain en un objet sous surveillance continuelle[5]. D'ailleurs, face à des traitements de données à caractère personnel ou des atteintes à la vie privée, toute réflexion doit être guidée par ce principe de la dignité humaine[6]. Ensuite, en vertu de la liberté de mouvement, qui doit s'interpréter de manière extensive, les individus doivent pouvoir se déplacer « sans être constamment suivis ou tracés »[7]. Cette liberté inclut celle de se mouvoir sans laisser de traces des mouvements effectués[8]. Enfin, du droit au respect de la vie privée découle un droit à l'autodétermination informationnelle ou à l'autonomie personnelle des individus. Ce droit peut être bafoué en raison de l'émergence de divers phénomènes. Ainsi, le droit à l'autodétermination est nié lorsque le comportement des personnes est manipulé ou lorsque « les applications des technologies de l'information […] [conduisent] à une normalisation des comportements, voire des pensées »[9]. De fait, les services et publicités personnalisés réduisent les différences individuelles et la liberté de choix des personnes. De plus, le droit à l'autodétermination implique que l'individu doit disposer d'une maîtrise sur son environnement et sur les données le concernant. Cependant, cette maîtrise est mise à mal par une série de risques présents dans la société actuelle. D'abord, il existe un déséquilibre entre les pouvoirs respectifs de la personne concernée et du responsable du traitement, ce dernier détenant une masse immense d'informations au sujet des habitudes de

1. A. Rouvroy et Y. Poullet, *op. cit.*, p. 68.
2. C. de Terwangne et J.-P. Moiny, *op. cit.,* p. 17 ; Y. Détraigne et A.-M. Escoffier, *op. cit.*, p. 12 ; A. Rouvroy et Y. Poullet, *op. cit.*, p. 61.
3. C. Colin et Y. Poullet, *op. cit.,* p. 141.
4. C. de Terwangne et J.-P. Moiny, *op. cit.,* pp. 15 et 16.
5. S. Rodotà, *op. cit.*, p. 81.
6. C. Colin et Y. Poullet, *op. cit.,* p. 141.
7. *Ibid.,* p. 144.
8. *Ibid.*
9. *Ibid.,* p. 142.

consommation de ces personnes[1]. Ensuite, un problème se pose au niveau de l'opacité et de la complexité du fonctionnement des technologies, pouvant entraîner une méfiance de la part de la personne concernée et une tendance à agir de manière conformiste[2]. Est également pointé le souci du réductionnisme, qui découle de la collecte et du traitement de données liées à des événements insignifiants de la vie quotidienne, tels que le temps passé dans un rayon spécifique, afin d'en déduire des tendances et de créer des profils à partir de données personnelles à l'individu, mais aussi relatives à autrui[3]. Finalement, il y a une mise en cause de la distinction entre la sphère privée et la sphère publique, puisque même quand il effectue une activité anodine de la vie quotidienne, l'individu peut être suivi[4].

Pour conclure, il ressort de cette contribution la nécessité d'encadrer, juridiquement, mais également par d'autres mesures, les mécanismes d'analyse des comportements de consommation par la géolocalisation, puisqu'ils impliquent des traitements de données à caractère personnel. Néanmoins, si les règles sont respectées par les acteurs concernés par l'analyse, cette technologie semble moins intrusive et attentatoire à la vie privée et à la protection des données que d'autres méthodes pouvant être mises en place par les commerçants comme les caméras de surveillance intelligentes et les cartes de fidélité contenant une puce RFID pour ceux établis dans un magasin réel ou les *cookies* pour ceux présents sur Internet.

1. *Ibid.,* p. 102 ; Y. Poullet, « Pour une troisième génération de réglementation de protection des données », *op. cit.,* p. 39 ; A. Rouvroy et Y. Poullet, *op. cit.*, p. 68.
2. Y. Détraigne et A.-M. Escoffier, *op. cit.*, p. 67.
3. C. Colin et Y. Poullet, *op. cit.,* p. 103.
4. *Ibid.,* pp. 102 à 104.