



HAL
open science

Entreprise et Respect de la vie privée du consommateur

Régis Dumoulin, Caroline Lancelot Miltgen

► **To cite this version:**

Régis Dumoulin, Caroline Lancelot Miltgen. Entreprise et Respect de la vie privée du consommateur : De l'usage autorisé à l'utilisation souhaitable des données personnelles. *Revue Française de Gestion*, 2012, 38 (224), pp.95-109. hal-01115987

HAL Id: hal-01115987

<https://audencia.hal.science/hal-01115987>

Submitted on 12 Feb 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Entreprise et Respect de la vie privée du consommateur :

De l'usage autorisé à l'utilisation souhaitable des données personnelles ¹

REGIS DUMOULIN
PROFESSEUR DES UNIVERSITES, UNIVERSITE D'ANGERS

Coordonnées professionnelles :
LUNAM Université
Université d'Angers
GRANEM (Groupe de Recherche ANgevin en Economie et Management)
UFR de Droit, d'Economie et de Gestion
13, Allée François Mitterrand
BP 13633
49036 Angers Cedex 01
TEL : 02 41 96 21 55
Email : regis.dumoulin@univ-angers.fr

CAROLINE LANCELOT MILTGEN
MAITRE DE CONFERENCES, UNIVERSITE D'ANGERS

Coordonnées professionnelles :
LUNAM Université
Université d'Angers
GRANEM (Groupe de Recherche ANgevin en Economie et Management)
UFR de Droit, d'Economie et de Gestion
13, Allée François Mitterrand
BP 13633
TEL : 02 41 22 66 00
Email : caroline.miltgen@univ-angers.fr

¹ Les auteurs sont cités dans l'ordre alphabétique. Ils remercient le rédacteur en chef pour la confiance qu'il leur a accordée et les relecteurs pour leurs commentaires.

Entreprise et Respect de la vie privée du consommateur :
De l'usage autorisé à l'utilisation souhaitable des données personnelles

Résumé

Les préoccupations croissantes des consommateurs pour le respect de leur vie privée et, à l'opposé, la volonté grandissante des entreprises de connaître chaque jour davantage leurs clients rendent nécessaire une meilleure définition des conditions d'équilibre. Dans cet article, nous analysons la manière dont l'entreprise doit appréhender les enjeux de la collecte et ses marges de manœuvre. Nous montrons aussi l'intérêt de définir une réelle stratégie relationnelle dans un contexte institutionnel ambigu.

Abstract

A better definition of equilibrium is required when, on the one hand, consumer's privacy concerns are growing and, on the other hand, the desire for companies to find out more about their customers is increasing daily. In this article we analyse the way in which companies must tackle the issues and limits concerning data collection. We also show why it is important to define a real relational strategy, in an ambiguous institutional context.

Entreprise et Respect de la vie privée du consommateur :

De l'usage autorisé à l'utilisation souhaitable des données personnelles

Introduction

Nous avons tous l'idée intuitive que certains aspects de notre vie sont privés. On sépare d'ailleurs le côté privé du côté public depuis longtemps, sans que le terme de protection ou de respect de la vie privée (RVP) ne soit pour autant systématiquement utilisé. L'idée de protéger les aspects privés de notre vie est donc largement répandue même si la césure traditionnelle entre vie publique et vie privée est aujourd'hui remise en cause. Par ailleurs, la conception de la vie privée est différente selon les cultures (Milberg et al. 2000) et les générations (Lenhart et Madden 2007). Dans de nombreux pays, notamment ceux de l'Union Européenne, la protection de la vie privée se manifeste par la reconnaissance d'un droit fondamental et inaliénable. Pour Sykes (1999), l'existence d'un tel droit est le fondement même de la démocratie car, sans vie privée, l'homme serait constamment surveillé et perdrait donc sa liberté. Warren et Brandeis (1890) considèrent ainsi le droit au respect de la vie privée comme un besoin humain majeur et le droit le plus valorisé par les hommes civilisés.

Il est admis que le premier article sur le thème de la vie privée a été publié dans une revue juridique américaine en 1890. Ecrit par Warren et Brandeis, il définissait alors le droit à la vie privée comme le droit d'être laissé seul (« *the right to be let alone* »). Depuis, d'autres définitions sont venues compléter celle-ci, sans qu'il y ait pour autant de réel consensus sur la signification de ce terme. Certaines définitions se focalisent ainsi sur la notion de secret tandis que d'autres soulignent plutôt son opposition avec la vie publique et/ou professionnelle. Pour Terré (2000), la délimitation de ce qui constitue la vie privée est d'autant plus délicate que certaines données fort personnelles servent aussi à identifier la personne dans la société, à

permettre de l'individualiser. Pour cet auteur, 'au cœur de la vie privée, il y a la vie personnelle. Peuvent être rattachées à ce premier cercle les données tenant à l'identité, à l'origine raciale, à la santé physique ou mentale, au caractère ou aux mœurs de l'individu auxquelles s'ajoutent, dans un cercle plus large, les éléments intéressant sa vie sentimentale, conjugale, extra-conjugale, familiale, ses relations amicales et sa participation à des réunions à caractère privé' (Terre, 2000, p 141).

Outre les problèmes de définition, les atteintes à la vie privée n'ont pas les mêmes implications juridiques selon les continents voire même selon les pays. Ainsi, aux Etats-Unis, la vie privée n'est pas un droit garanti par la Constitution mais un privilège légal. En Europe par contre, elle fait partie des droits de l'homme, au même titre que la liberté.

Un des enjeux majeurs autour de la question du respect de la vie privée concerne la capacité des individus à contrôler la collecte et la diffusion d'informations les concernant. Les craintes en matière de respect de la vie privée (au sens large) ainsi que celles portant plus particulièrement sur la protection des données à caractère personnel¹, se sont historiquement cristallisées face à l'État pour peu à peu se déplacer vers les opérateurs privés (Belen, 2005). En effet, la priorité stratégique des entreprises s'oriente aujourd'hui de plus en plus vers la maîtrise du maximum de données sur les individus (prospects, clients, consommateurs, salariés, futurs collaborateurs, ...) (Terre, 2000). Les outils technologiques actuels permettent ainsi l'identification de ces individus (notamment des clients et des salariés), le suivi voire le traçage de l'ensemble de leurs activités et l'exploitation des données à des fins de meilleur rendement. La disparition de l'anonymat ne concerne pas seulement les relations salariales mais aussi les relations marchandes (Isaac et Kalika, 2001). De nombreux consommateurs s'inquiètent alors des risques de dérive auxquels pourrait conduire un espionnage de leur vie quotidienne dans ses moindres détails (où ils sont allés, ce qu'ils consomment, ce qu'ils lisent,

¹ Nous entendons ce terme au sens de la définition donnée par la Loi Informatique et Liberté (1978). Il s'agit de « données relatives à un individu identifié ou identifiable par un ou plusieurs éléments qui lui sont propres (nom, numéro de sécurité sociale ...) ». Les données obtenues sont alors clairement liées à cet individu.

écoutent, font) (Lemoine, 2000) sans pour autant réellement mettre en œuvre des stratégies visant à cloisonner davantage ce qui relève du domaine public et ce qui devrait rester dans une sphère familiale, amicale ou professionnelle. L'exemple de Facebook illustre parfaitement ce phénomène de *privacy paradox* qui amène des individus pourtant hostiles à toute utilisation de leurs données à fournir parfois un portrait extrêmement détaillé de leur profil et à le laisser libre d'accès à tout individu circulant sur la toile.

Le traitement et, plus spécifiquement, la collecte et l'utilisation de données personnelles est donc un sujet, si ce n'est de préoccupation, au moins d'attention, dans un grand nombre de communautés, incluant les groupes d'activistes qui cherchent à protéger les droits de l'individu, et les médias qui veulent informer l'opinion publique des dérives potentielles. L'importance du phénomène se voit aussi dans la volonté des gouvernements (notamment européens) de promouvoir des lois protégeant les consommateurs en particulier et les citoyens en général. Le sujet concerne également les entreprises (et leurs responsables) dont les besoins en informations sont confrontés à la nécessité de respecter la vie privée de leurs clients et prospects et de se conformer à la législation en vigueur. La question intéresse, enfin, la communauté académique qui souhaite comprendre comment on peut aboutir à un tel équilibre.

L'objectif de cet article est de proposer un cadre d'analyse de la collecte de données personnelles. La relation entreprise-client n'est pas dyadique mais s'inscrit dans un contexte social et sociétal plus large, que la théorie des parties prenantes aide à circonscrire. Au sein de ce cadre, nous analysons la manière dont l'entreprise doit appréhender les enjeux de la collecte et ses marges de manœuvre. Nous montrons l'intérêt – pour elle et ses clients – de définir une réelle stratégie relationnelle dans un contexte institutionnel ambigu.

L'importance de cette problématique est justifiée tant par le contexte économique, technologique et réglementaire dans lequel évoluent actuellement les entreprises que par le

manque de connaissance établies sur le sujet. Ainsi, nous ne savons toujours pas vraiment ce que les individus considèrent comme une information personnelle ni dans quel cas ils estiment qu'un traitement de données constitue une invasion de leur vie privée. De même, nous avons très peu d'informations sur le processus amenant à la décision de diffuser ou non des données personnelles ou d'accepter que celles-ci soient collectées, utilisées et/ou transférées à d'autres. Les préoccupations croissantes des consommateurs pour le respect de leur vie privée, rapportées à travers de nombreux sondages récents² et, à l'opposé, la volonté grandissante des entreprises de connaître chaque jour davantage leurs clients rendent nécessaire une meilleure définition des conditions d'équilibre. De telles interrogations sont prégnantes en France compte tenu du nombre restreint de travaux qui traitent de ce sujet.

Dans une première partie, nous dressons un état des lieux du respect de la vie privée dans notre société en discutant l'aspect culturel de la question. Nous nous intéressons plus particulièrement aux conséquences de l'intrusion accrue de technologies et de démarches toujours plus utilisatrices d'informations personnelles. Dans une seconde partie, nous présentons les enjeux - stratégiques, réglementaires ou éthiques - liés à la question du respect de la vie privée en nous attachant à les relier à la théorie des parties prenantes. Nous montrons dans quelle mesure la protection réglementaire de la vie privée est perçue comme insuffisante ou inefficace, au moins en France, et en déduisons l'intérêt pour les entreprises de passer d'un système d'usage autorisé à une utilisation raisonnable des données clients.

1. Etat des lieux du respect de la vie privée

1.1. Europe / USA : une conception différente de la vie privée

En Europe, la volonté de protéger la vie privée des citoyens est affirmée dans des instruments juridiques (déclarations, directives, lois, décrets, etc.) relativement contraignants. La Directive 95/46/CE s'efforce ainsi de respecter une présentation équilibrée

² Sondage réalisé par IPSOS pour la CNIL en 2008, Sondage EPITECH sur la vie privée et la sécurité sur Internet réalisé en 2009, Sondage réalisé par TNS Sofres pour Microsoft en 2010 sur la vie privée des français.

de deux objectifs plutôt difficiles à concilier: « respecter les libertés et droits fondamentaux des personnes, notamment la vie privée », et « contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus » (Considérants 2 et 3 à 11). L'enjeu de la législation européenne est donc d'impliquer davantage les individus et d'assurer les conditions de maîtrise de leurs informations personnelles, en leur reconnaissant un véritable droit à déterminer l'usage qui doit être fait de ces données. Cette implication passe par une information en amont et une éducation sur les différents processus de collecte et de traitement des données. En France, cela s'est traduit surtout par la fameuse loi dite 'Informatique et Libertés' publiée dès 1978. Plus récemment, la Loi pour la Confiance dans l'Economie Numérique (LCEN) publiée en 2004 est venue renforcer ce dispositif législatif en exigeant un accord explicite de la part du consommateur pour recevoir des courriels publicitaires. Cette position réglementaire s'est révélée plutôt efficace, pendant un certain temps au moins, la conjonction de la législation et des règles déontologiques des professions (FEVAD, ACSEL, Code de déontologie des professionnels du marketing direct) aboutissant à des politiques de RVP mises en place sur les sites marchands de manière assez satisfaisante (Gauzente, 2003).

Les Etats-Unis offrent au contraire l'exemple d'une approche décentralisée et « fragmentée » majoritairement fondée sur l'autorégulation. Que ce soit au niveau des Etats ou au niveau fédéral, les mesures réglementaires se focalisent sur des pratiques ou des cibles particulières parfois spécifiques à certaines industries. Ces dernières ont alors créé des droits légaux défendables devant les cours à défaut d'être assurés par une administration centrale comme c'est le cas en Europe. La protection repose toutefois davantage sur les codes de conduite mis en place par les entreprises et les associations professionnelles pour rassurer les citoyens quant à la manipulation de leurs données personnelles. Aujourd'hui, on peut ainsi difficilement fréquenter un site élaboré du commerce électronique américain sans

rencontrer une rubrique *privacy*³ (Lemoine, 2000). Les gestionnaires de sites n'ignorent plus qu'il faut répondre à une préoccupation croissante et légitime des consommateurs.

Plusieurs 'affaires' ont pourtant montré que l'on pouvait difficilement accorder une confiance absolue et aveugle aux seules promesses de l'autorégulation (Lemoine, 2000). Ces dernières années, les géants de l'internet comme Google⁴ et Facebook⁵ ont été critiqués à plusieurs reprises concernant leur gestion plutôt laxiste des données et du respect de la vie privée numérique en général. Si l'autorégulation peine ainsi à s'imposer sur le marché des données à caractère personnel en Europe, c'est notamment dû à l'asymétrie d'information existant entre le responsable de fichier d'une part et l'individu dont on collecte et/ou utilise les données d'autre part, l'ignorance de ce dernier induisant souvent une certaine méfiance et une faible volonté d'échange d'informations.

L'étude de Gurau et alii (2003) sur un échantillon de sites commerciaux américains, anglais et français montre que les pays européens, probablement parce qu'ils sont plus réglementés, mettent généralement davantage en avant leur charte et se montrent moins exigeants en demande d'informations personnelles. Une rubrique souffre cependant souvent de laisser-aller, celle du choix laissé à l'internaute quant à l'usage et à la divulgation des informations qu'il confie. Les sites commerçants disposant de labels ou de chartes communiquent également davantage sur leur politique de respect de la vie privée (Gauzente, 2003). Le cadre législatif mis en place en France et en Europe semble ainsi peser fortement sur les pratiques, engendrant des effets bénéfiques pour les citoyens.

En dépit de systèmes de régulation différents, Américains et Européens sont chacun attentifs à l'utilisation qui peut être faite de leurs données personnelles. Les atteintes à la vie

³ Terme utilisé par les anglo-saxons pour faire référence à la vie privée.

⁴ Au lancement de Google Buzz (réseau social associé à la messagerie Gmail) le 9 février 2010, les utilisateurs ont eu la surprise de voir leur liste de contact Google Buzz automatiquement accessible par les autres utilisateurs du service (http://www.lemonde.fr/technologies/article/2010/09/06/vie-privée-reglement-a-l-amiable-d-une-plainte-contre-google-buzz_1407171_651865.html#xtor=RSS-3208).

⁵ Selon une révélation du Wall Street Journal en mai 2010, le nom et l'identifiant de certains utilisateurs de Facebook et de MySpace auraient été transmis à des annonceurs afin de cibler leurs publicités (http://www.lexpress.fr/actualite/societe/vie-privée-facebook-pris-la-main-dans-le-sac_894040.html).

privée peuvent donc engendrer des réactions si ce n'est similaires ou tout le moins comparables dans des communautés pourtant éloignées, géographiquement et culturellement. Ceci est d'autant plus vrai aujourd'hui avec l'arrivée d'outils technologiques dont l'impact sur la vie privée se fait ressentir des deux côtés de l'Atlantique.

1.2. L'impact des technologies sur le respect de la vie privée

1.2.1. Les TIC et Internet

Depuis les années 90, les menaces pesant sur la vie privée des individus ont fortement évolué. Ce qui a tout d'abord changé, c'est la manière avec laquelle les données personnelles des consommateurs sont collectées puis utilisées. Alors que les entreprises se sont longtemps contentées de récolter des informations liées au marché (i.e. caractéristiques de la cible, audience média, parts de marché, ...), elles focalisent aujourd'hui leur attention sur des données spécifiques à chaque individu (i.e. de nature personnelle) comme ses caractéristiques sociodémographiques, ses goûts et préférences et ses habitudes en matière de consommation. Ensuite, alors que la collecte se faisait traditionnellement en face à face, par téléphone ou par courrier, l'arrivée des Technologies de l'Information et de la Communication (TIC) est venue bouleverser le paysage. L'essor de ces technologies a permis une augmentation de la vitesse avec laquelle les données sont collectées, stockées et transmises, mais également du montant d'informations susceptibles d'être récoltées et utilisées. On parle ainsi de « *cyber panopticon* » pour évoquer la facilité avec laquelle les renseignements peuvent aujourd'hui être collectés et partagés d'une part et les consommateurs surveillés d'autre part, depuis l'arrivée d'Internet (Helms, 2001).

1.2.2 Les réseaux sociaux numériques

L'arrivée des réseaux sociaux numériques (RSN) a changé les frontières entre ce qui entre dans le domaine public et ce qui concerne la vie privée, à la fois en mettant aux yeux de

tous des éléments autrefois considérés comme privés ou personnels et en supprimant de fait la distinction entre les deux. Avec ces réseaux, les individus deviennent non seulement des consommateurs mais aussi des producteurs de contenus (Squicciarini et al. 2009). Or, cette capacité à produire et à partager de l'information introduit de fait une incertitude quant à savoir quelle information peut être partagée, sous quelle forme et avec qui ? De plus, en permettant à chacun de développer des relations interpersonnelles à distance, les RSN transforment chaque conversation en un ensemble de données numériques faciles à collecter et à utiliser. Dès lors, alors que les utilisateurs considèrent ces interactions comme des conversations personnelles et éphémères, elles sont de fait difficiles à effacer et deviennent même des éléments archivés pouvant faire l'objet d'utilisations ultérieures (Pekarek et Leenes 2009) y compris par les professionnels du marketing voire même par les organismes publics.

Dans la littérature sur les réseaux sociaux, la question du respect de la vie privée est de loin la plus étudiée. On y trouve notamment des travaux sur le paradoxe de la vie privée, fait que les individus révèlent de nombreuses informations sur eux à travers ces réseaux parce qu'ils pensent qu'il s'agit d'espaces privés alors qu'ils sont en réalité publics ou quasi publics (e.g. Hoadley et al. 2009). De l'ensemble de ces travaux, il ressort très nettement que les internautes révèlent plus d'informations sur eux qu'ils veulent bien l'avouer et qu'il serait raisonnable de le faire. Comprendre jusqu'à quel point les individus peuvent et doivent se dévoiler et pourquoi ils ont tendance à sous-évaluer leur exposition de soi demeure un aspect sous-étudié et donc largement irrésolu (Tufekci 2008).

1.2.3 Un environnement de plus en plus collecteur d'informations privées

Internet est loin d'être la seule technologie concernée. D'autres technologies ont fait leur apparition avec des incidences tout aussi importantes sur le respect de la vie privée. Deux exemples parmi tant d'autres : mise en place de caméras tant dans des lieux publics (gares, aéroports, centres-villes, ...) que dans des lieux plus privés et recours aux scanners dans les

aéroports. Prévus pour remplacer les anciens compteurs électriques d'ici 2017, les futurs compteurs électriques intelligents sèment aussi le trouble en France et en Europe. Cette nouvelle technologie, censée faciliter les économies d'énergie et donc lutter contre le réchauffement climatique, suscite déjà des interrogations en matière de respect de la vie privée. Capables de transmettre en temps réel au fournisseur d'énergie des informations sur la consommation de chaque client, le risque d'une tentation de la part des compagnies électriques de vendre les données ainsi récupérées est réel et a été dénoncé dès novembre 2009 au sein de la conférence internationale de protection des données et de la vie privée.

Globalement, de plus en plus de démarches amènent à collecter et/ou utiliser les données personnelles des citoyens, et ce, de manière plus ou moins légale. L'utilisation d'une carte bancaire ou la possession d'un téléphone mobile permettent ainsi d'être géo-localisés. Google a, pour sa part, enregistré de nombreuses données personnelles émanant de wifi non sécurisés lors des prises de photos « streetview » alimentant le site googlemaps. Il est également techniquement possible de pirater un téléphone mobile et d'en détourner les SMS. Le recensement permanent de la population est aussi l'occasion d'une saisie importante de données sur les modes de vie. Enfin, pour se prémunir contre les risques liés à la fraude ou au non remboursement, les organismes de prêts exigent désormais copie des relevés de compte bancaire sur plusieurs mois. La collecte d'informations sur les revenus, les habitudes de consommation et le mode de vie en général est en soi un problème. Mais le principal souci c'est que l'individu ne peut pas toujours compter sur les institutions pour le protéger de ces intrusions, les organismes publics abusant parfois eux-mêmes du système. Depuis avril 2011, l'Etat français s'arroge ainsi le droit de revendre les données figurant sur les cartes grises à des organismes commerciaux, à un tarif variant de 0,20 à 0,089 € selon le volume acheté⁶.

⁶ Challenges, n° 263, 30 juin 2011, p. 71.

Cet essor des pratiques de collecte et d'utilisation des données personnelles ne s'opère toutefois pas sans que les citoyens y trouvent à redire. Les enquêtes d'opinion réalisées sur le sujet révèlent ainsi qu'ils sont de plus en plus sensibles aux risques que font peser ces pratiques, qu'ils sont souvent réticents à fournir des données personnelles et qu'ils se méfient de l'utilisation qui peut être faite des données divulguées. Un sondage d'Octobre 2008 réalisé pour la CNIL⁷ montre que les Français témoignent d'une défiance accrue à l'égard du niveau de protection de leur vie privée sur Internet, 71 % le jugeant « insuffisant » et 37% « pas du tout satisfaisant ». Par ailleurs, selon un sondage réalisé par Microsoft en 2010, les Français sont inquiets à l'idée que des informations qu'ils ont laissées sur Internet puissent être vues et utilisées par des pirates (75%), des entreprises (61%) voire des collègues de travail (35%). Ces sondages indiquent également que les individus sont autant préoccupés par ce que les entreprises peuvent connaître d'eux que par la manière dont elles ont obtenu et utilisent ces informations. En général, les personnes interrogées estiment ainsi qu'on leur soutire trop de données personnelles et qu'elles ont peu de contrôle sur ce qu'il en advient. Se dessine alors un conflit majeur qui oppose le droit du consommateur/citoyen de protéger son intimité et le droit de l'organisation à s'approprier les informations recueillies. On se trouve en effet à la croisée de plusieurs libertés qui se trouvent être en contradiction : la liberté du commerce et des échanges d'un côté et la liberté individuelle de l'autre. De plus, on touche ici un point particulièrement sensible dans la mesure où, de tous les droits de l'individu, celui lié au respect de la vie privée est l'un des plus fondamentaux.

Si l'arrivée de technologies a eu un impact favorable sur l'économie et des avantages pour les consommateurs (notamment un meilleur ciblage des propositions commerciales reçues), des effets pervers dus à une intrusion accrue dans leur intimité ont également été mis à jour. Car, si le traitement d'informations personnelles améliore la capacité des firmes et de

⁷ <http://www.cnil.fr/la-cnil/actu-cnil/article/article//71-des-francais-jugent-la-protection-de-la-vie-privée-sur-internet-insuffisante/>

l'administration à fournir des services adaptés aux besoins des individus, ces derniers sont aujourd'hui nombreux à considérer ces pratiques comme une atteinte à leur vie privée. Six pratiques sont plus particulièrement décriées (Wang et Wang, 1998) :

- la collecte : fait que trop de données ou des données trop sensibles soient récoltées
- le stockage non autorisé : lié à la confidentialité et à l'intégrité des données fournies
- les erreurs : altération accidentelle ou délibérée des données fournies
- l'accès impropre : fait que des personnes non autorisées puissent accéder aux données
- l'utilisation interne : réception d'offres commerciales non désirées et non sollicitées
- l'utilisation externe : fait que les données soient cédées à d'autres sans autorisation

Ces pratiques engendrent des réactions variées chez les individus : d'un dégoût résigné pour certains, à un boycott absolu pour d'autres, en passant par un bouche-à-oreilles négatif pouvant être rapidement relayé par des tiers ou par les médias (Culnan et Armstrong 1999). Or, ce type de buzz peut s'avérer d'autant plus dommageable aujourd'hui avec la puissance du web 2.0 dont la capacité de diffusion semble sans limite (Le Deuff, 2006).

2. L'entreprise, la collecte et l'utilisation de données clients

2.1. Le cadre d'analyse des parties prenantes

La théorie des parties prenantes peut offrir un cadre d'analyse des enjeux liés à la collecte et à l'utilisation des données clients. Pour Freeman (1984), tout groupe ou individu qui peut affecter ou être affecté par la réalisation des objectifs d'une organisation constitue une partie prenante à cette organisation. Martinet et Reynaud (2004) proposent une définition plus générale, qui englobe la réciproque de celle de Freeman. Les parties prenantes sont des individus ou des groupes sociaux qui dépendent de l'entreprise pour atteindre leur propre objectif et dont l'entreprise dépend en retour. La responsabilité sociétale de chaque acteur est ainsi engagée : l'idée de partie prenante a émergé lorsque la société civile a demandé aux entreprises internationales des comptes sur les conséquences sociales de leurs activités.

La théorie des parties prenantes interroge directement les pratiques de l'entreprise au sein de la société. L'entreprise doit alors gérer les relations qu'elle entretient avec ses parties prenantes de manière à minimiser les conflits coûteux en ressources, qui pourraient à terme la conduire à disparaître. Pelle-Culpin (1998) distingue trois catégories de parties prenantes (PP). Les PP institutionnelles ont en charge la réglementation et l'organisation de la profession. Dans notre schéma (cf. figure 1, ci-après) il s'agit essentiellement des organismes de régulation chargés de faire appliquer la loi et des tiers certificateurs. Les parties prenantes économiques concernent les agents économiques évoluant sur les marchés de l'entreprise. Elles sont nombreuses et concernent au premier chef les entreprises et les consommateurs, mais également les fournisseurs de solution de protection et les fournisseurs de bases de données et de solutions techniques. Les PP éthiques représentent les groupes de pression éthiques et politiques de l'environnement (par exemple, les associations de défense des consommateurs) Nous pouvons ainsi réaliser la cartographie des parties prenantes concernées par la collecte, l'utilisation et/ou la protection de données privées.

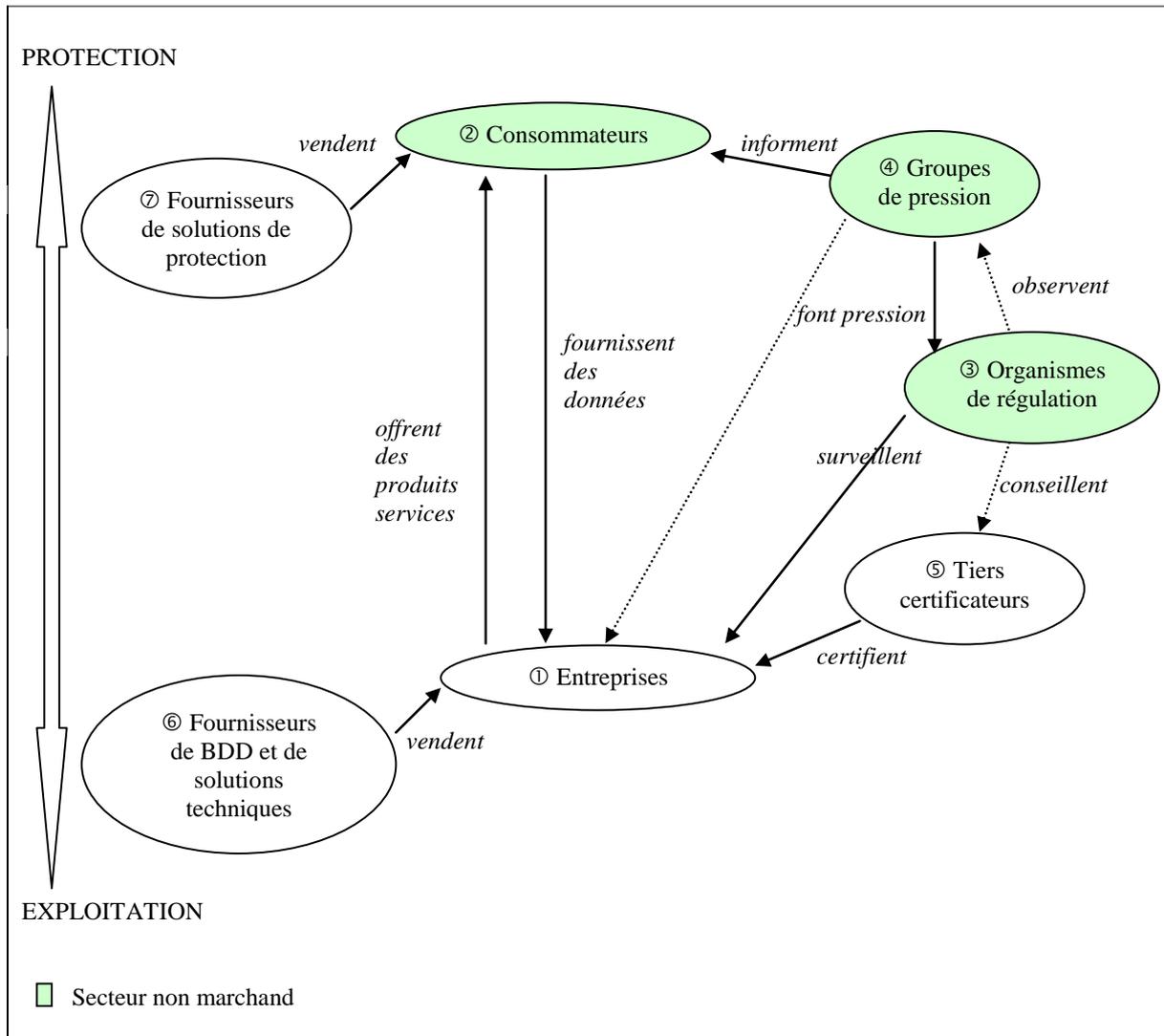


Figure 1. Cartographie des parties prenantes concernées par la collecte, l'utilisation et/ou la protection de données privées

2.2. Les enjeux stratégiques, réglementaires et éthiques de la collecte de données

Les firmes collectent de plus en plus d'informations sur leurs clients. Elles doivent cependant faire face au dilemme d'utiliser les données qu'elles auront obtenu avec profit, sans créer de préjudice majeur aux PP économiques, et tout en respectant la réglementation en vigueur et en évitant la vindicte des groupes de pression. La collecte de données auprès de clients représente ainsi un triple enjeu pour les entreprises : stratégique, réglementaire et éthique.

C'est un enjeu stratégique dans la mesure où l'information est devenue une source de valeur majeure pour les entreprises. La connaissance (entendue comme le prolongement de la détention d'informations) a remplacé l'énergie comme ressource première de la société post-industrielle. L'autre source de valeur résulte de la commercialisation possible des données ainsi collectées. La collecte et l'utilisation efficaces des données représentent donc aujourd'hui l'un des plus grands défis du management puisque c'est l'un des principaux moyens d'obtenir des avantages en termes de compétitivité. Ainsi, comme le résumait Pierre Tabatoni dès 2000 : *« dans la nouvelle économie fondée sur l'innovation technologique et le rôle central accordé aux consommateurs par le marché, les données personnelles représentent une ressource compétitive essentielle »*.

C'est aussi un enjeu réglementaire puisque, bien que délicate, la prise en compte de l'aspect juridique du respect de la vie privée demeure indispensable. Le modèle de régulation adopté dans chaque pays aurait une influence notable sur le niveau de préoccupation des citoyens. Or, malgré l'encadrement des pratiques, censé être assuré par la réglementation en Europe et l'autorégulation aux USA, les menaces à l'égard du respect de la vie privée des citoyens en général et des consommateurs en particulier sont toujours aussi présentes, et ce, dès deux côtés de l'Atlantique. Par ailleurs, l'Europe appuie également son mécanisme de protection sur les parties prenantes institutionnelles que sont les organismes indépendants créés pour informer les citoyens et s'assurer de la bonne mise en œuvre des lois dans ce domaine. Ce rôle est joué en France par la CNIL, organisme créé en 1978 par la Loi dite 'Informatique et Libertés'.

C'est, enfin, un enjeu éthique dans la mesure où les consommateurs sont de plus en plus conscients des bénéfices que les entreprises retirent de l'utilisation de leurs données. Les cris émanant de l'opinion publique à propos de l'utilisation non autorisée de ces informations sont ainsi, chaque jour davantage, le résultat d'une connaissance accrue de la valeur de

données divulguées naguère gratuitement. La valeur marchande acquise aujourd'hui par les informations personnelles – les fichiers se vendent d'autant plus cher qu'ils sont enrichis et permettent d'établir des profils – conduit aujourd'hui les consommateurs à une vigilance accrue quant au respect de leur vie privée par les entreprises.

Cette prudence ne les empêche cependant pas de délivrer du contenu privé, sur les réseaux sociaux par exemple, par manque de conscience de l'exploitation commerciale qui en est faite. En cela, la protection des données personnelles est un enjeu important qui dépasse la relation entreprise - client : l'émergence de PP éthiques en est la traduction la plus visible.

Devant cette prise de conscience, les entreprises sont ainsi encouragées –même si c'est encore loin d'être une réalité- à respecter encore davantage la vie privée des consommateurs, notamment sur Internet, et ce, pour deux raisons majeures. Tout d'abord, la protection de la vie privée est instrumentalement utile car elle est nécessaire pour développer la confiance. Les internautes ont besoin de cette confiance pour accepter de commercer avec une entité commerciale, a fortiori lorsqu'il n'existe pas de contact direct avec un vendeur. Ensuite, pour Mason (1986), respecter la vie privée de ses clients/prospects est « moralement nécessaire », quand les données sont amenées à circuler sur la toile et a fortiori quand la réglementation s'avère insuffisante pour vraiment rassurer les individus.

2.3 Une protection réglementaire peu efficace

Il existe tout d'abord une différence notable entre la définition légale de certains termes et l'image que les individus s'en font. Les travaux de Lancelot Miltgen (2006) montrent que les perceptions des internautes relatives au phénomène de vie privée sont dans l'ensemble plus larges que les définitions proposées par le législateur. Ainsi, pour le terme de donnée personnelle, au-delà de la distinction du caractère public ou privé de l'information tel qu'il est souligné dans la réglementation, les consommateurs veulent surtout indiquer le lien

affectif qui les unit à ces données : « c'est une information relative à la personne, qui implique l'individu en tant que tel ».

Ensuite, les français ont une faible connaissance des pratiques utilisées par les entreprises pour collecter et exploiter leurs données personnelles (Lancelot Miltgen 2003). Ceci se vérifie d'autant plus sur Internet, signe de l'impact significatif de la technologie. Les français paraissent également peu informés de leurs droits en matière de respect de la vie privée. Ainsi, dans une étude menée auprès de 2014 jeunes français âgés de 15 à 25 ans (Lusoli et Miltgen 2009), 16% déclarent n'avoir jamais entendu parler de lois dans ce domaine, 39% en ont entendu parler mais estiment ne pas vraiment les connaître et 38% les connaissent seulement 'un peu'. Parallèlement, les consommateurs considèrent que les pratiques de collecte de données sont dans l'ensemble insuffisamment réglementées et ont peu confiance dans les pouvoirs publics pour réguler la démarche. Le même sondage (Lusoli et Miltgen 2009) confirme que 32% seulement des 15-25 ans interrogés font confiance au gouvernement français pour réglementer l'accès aux données personnelles, un chiffre équivalent au niveau de confiance accordé aux entreprises. Cette méfiance n'est cependant pas partagée par tous dans la mesure où certains font la différence entre l'existence d'une loi et son application, tandis que d'autres évoquent leurs craintes quant au manque d'efficacité de la loi ou aux difficultés à la faire appliquer. Il est à craindre que les dérives de l'Etat quant à la commercialisation de données personnelles renforcent l'idée d'un manque de vigilance de la part des parties prenantes institutionnelles, voire décrédibilise le système législatif en place.

Enfin, concernant les réactions aux sollicitations de données personnelles, bien que certains consommateurs s'avouent excédés par de telles pratiques, aucun ne déclare vouloir porter plainte. Il est cependant difficile de distinguer, parmi les raisons expliquant ce renoncement à se défendre, celles liées au manque d'information concernant leurs droits, celles dues au scepticisme quant à l'efficacité de telles solutions et celles liés à la faiblesse du

préjudice subi. Le coût de l'action en justice et la difficulté de l'action collective constituent d'autres obstacles à la judiciarisation de l'atteinte à la vie privée.

Tout ceci laisse apparaître des différences notables entre les droits que la réglementation confère aux citoyens et la manière dont ces derniers les appréhendent. Les acteurs institutionnels et économiques sont donc vivement encouragés à mettre en place des démarches plus protectrices afin que les individus se sentent davantage en confiance.

2.4 De l'usage autorisé à l'utilisation souhaitable des données

La compréhension des préoccupations et des comportements des consommateurs en matière de vie privée doit aider les entreprises à distinguer les usages autorisés des utilisations souhaitables des données à caractère personnel. Devant l'absence de règles clairement définies, le retard du législateur en la matière et le comportement ambigu des PP institutionnelles, c'est au manager d'arbitrer entre ce qu'il peut, d'un point de vue légal, collecter auprès de ses clients et ce qu'il est raisonnable qu'il demande, dans une optique de marketing relationnel.

Quatre critères permettent d'identifier les pratiques susceptibles d'entraîner des réactions négatives de la part des consommateurs (Lancelot Miltgen 2006). Ces critères concernent : (1) l'absence ou le manque de garantie en matière de confidentialité des données, (2) la sollicitation de données trop personnelles ou (3) non pertinentes par rapport à la transaction en cours. Enfin, le fait pour un individu d'entrevoir plus de risque à répondre que de bénéfices à en retirer (4) peut également l'encourager à s'abstenir de fournir des renseignements privés voire le conduire à une réaction plus radicale comme le boycott de la marque incriminée.

Plusieurs solutions visant à rassurer les individus et à accroître leur confiance dans la capacité des entreprises à respecter leurs engagements en matière de vie privée peuvent être

mises en œuvre. La première consiste à adopter une politique de respect de la vie privée claire et cohérente, à la fois respectueuse des lois en vigueur et empreinte d'une certaine éthique. Le deuxième impératif réside dans l'élaboration d'une collecte limitée aux données strictement nécessaires à la transaction en vigueur et qui ne soient pas considérées comme sensibles. Enfin, une autre solution susceptible de rassurer le consommateur consiste à accroître son intérêt à fournir des informations (par exemple en octroyant des avantages en échange des données fournies, tels que des offres privilégiées, des bons de réduction, des cadeaux, des échantillons, etc ...) et/ou à réduire les coûts liés à la fourniture des renseignements (champs pré-remplis par exemple). Une vision gagnant-gagnant de l'échange de données personnelles où le consommateur est récompensé de la fourniture de renseignements de nature privée est clairement à privilégier aujourd'hui.

Les entreprises doivent aussi être attentives aux conséquences possibles d'une sollicitation de données qui serait jugée abusive et/ou trop intrusive. Plusieurs éléments sont susceptibles d'influencer la réaction de l'individu voire de l'inciter à rompre la relation avec l'organisme l'ayant sollicité. Parmi ces éléments, on trouve notamment : le contexte dans lequel les informations ont été recueillies (par exemple, l'offre de participer à un jeu-concours peut être mal vécue par certains clients) et, dans une moindre mesure, l'ancienneté de la relation avec l'organisme à l'origine du traitement.

La fourniture de données personnelles est nécessaire au développement de relations entre les parties prenantes. D'un côté, elle peut participer d'un phénomène d'engagement – le fait pour le consommateur de devoir fournir ces mêmes données à une autre entreprise constituant alors une barrière au changement – elle a, d'un autre côté, le pouvoir de détruire ces relations. La complexité de la livraison d'informations privées doit inciter l'entreprise à définir en amont une stratégie de recueil et à anticiper ses conséquences sur la perception, les attitudes et les comportements des clients et des usagers.

Conclusion

Alors que les données personnelles représentent aujourd'hui un facteur clé de succès dans l'économie, la question du respect de la vie privée reste d'une importance stratégique. Comprendre comment le consommateur perçoit une collecte d'informations personnelles et de quelle manière il y répond présente un intérêt majeur. Cela permet de mieux comprendre comment il fait le choix de fournir ou non les données demandées. Connaître ces critères de décision donne alors la possibilité de prendre des décisions informées et de mettre ainsi en place des procédures de collecte plus respectueuses, et de la législation en vigueur, et des préoccupations grandissantes des citoyens pour le respect de leur vie privée. Se faisant moins pressantes et moins intrusives, les demandes de renseignements auront alors plus de chance d'aboutir à une meilleure qualité des informations recueillies et donc potentiellement à une audience plus forte.

Les enjeux autour de la question du respect de la vie privée ne se limitent pas au seul secteur privé. Ils intéressent également l'ensemble des organismes publics concernés soit par la collecte et l'utilisation des données personnelles des citoyens (exemple des administrations au niveau central, régional ou local), soit par la protection de ces mêmes données. La CNIL, commission chargée de réglementer le traitement de données à caractère personnel sur le territoire français, consciente de l'importance des enjeux autour de ces questions, vient d'ailleurs de se doter d'une direction de l'innovation et de la perspective pour mieux anticiper l'impact de l'usage des outils numériques sur la protection de la vie privée. Par ailleurs, la Directive Européenne 95/46/CE sur la protection des données à caractère personnel devrait être révisée prochainement, en raison de l'évolution du contexte technologique dans lequel nous vivons aujourd'hui (cloud computing, techniques de marketing comportemental, explosion des réseaux sociaux notamment) avec pour but principal de simplifier et d'uniformiser les formalités de déclaration et de renforcer les droits de la personne.

Toutefois, même si la législation dans ce domaine a été renforcée et doit être révisée à nouveau, force est de constater que les choses sont encore loin d'être réglées. Les perceptions des citoyens à ce sujet sont d'ailleurs très hétéroclites, certains se plaignant d'un manque de réglementation quand d'autres évoquent son manque d'efficacité. Par ailleurs, malgré certains progrès, de nouvelles pratiques et technologies toujours plus intrusives apparaissent chaque jour. Le conflit entre besoin des entreprises en informations et droits des consommateurs à préserver leur intimité n'est donc pas prêt de se résoudre. Gageons que cet article permettra néanmoins d'y voir plus clair et d'identifier des pistes prometteuses en la matière.

Références

- Belen V. (2005), Les tentatives de protection des données personnelles des individus : difficultés de définition et risques nouveaux, *Market Management*, 2005/2 (5), 65-80
- Culnan M. et Armstrong P.K. (1999), Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Sciences*, 10 (1), 104-115
- Dwyer et al. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and Myspace. *Proceedings of AMCIS*
- Freeman R.E. (1984), *Strategic Management: A Stakeholder Approach*, Massachusetts, Pitman Publishing Inc.
- Gauzente C. (2003), Vie privée et internet : la pratique des sites français, *Décisions Marketing*, 30, 7-16.
- Gurau C., Ranchhod A. et Gauzente C. (2003), To legislate or not to legislate : a comparative exploratory study of privacy-personalisation factors affecting French, UK and US web sites, *Journal of Consumer Marketing*, 20, 7, 652-654
- Helms, Shawn C. (2001), Translating Privacy Values with Technology, Boston University *Journal of Science and Technology Law*, 288-325

Hoadley, C. M., Heng X., Joey J.L., and Rosson M.B. (2009), Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry, *Electronic Commerce Research and Applications*, 9 (1), 50-60.

Isaac H. et Kalika M. (2001), Organisation, technologies de l'information et vie privée, *Revue Française de Gestion*, 134, 101-105

Lancelot Miltgen C. (2003), Vie privée et Internet : influence des caractéristiques individuelles et situationnelles sur les attitudes et les comportements face à la collecte de données personnelles, Congrès de l'Association Française du Marketing, Tunis, Mai

Lancelot Miltgen C. (2006). Dévoilement de soi et réponses du consommateur face à une sollicitation de ses données personnelles : une application aux formulaires sur Internet. Thèse de Doctorat en Sciences de Gestion, U. Paris Dauphine.

Le Deuff O. (2006), Le succès du web 2.0 : histoire, techniques et controverse, <http://halshs.archives-ouvertes.fr/docs/00/13/35/71/HTML/>

Lemoine P. (2000), Commerce électronique, marketing et liberté, Travaux du groupe d'études société de l'information et vie privée, Académie des Sciences Morales et Politiques, Rapport final (2), Chapitre 7.

Lenhart A. et Madden M. (2007), Teens, Privacy and Online Social Networks, Washington, DC: Pew Internet & American Life Project.

<http://www.pewInternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx>

Lusoli W., Miltgen C. (2009), Young People And Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks, JRC Scientific and Technical Reports EUR 23765 EN. Lusoli, W., Compañó, R. & Maghiros, I. (Eds.) Sevilla: EC JRC IPTS, <http://ftp.jrc.es/EURdoc/JRC50089.pdf>

Martinet A.C. et Reynaud E. (2004), Entreprise durable, finance et stratégie, *Revue Française de Gestion*, 152, Septembre-Octobre, 121-136

- Mason R. (1986), Four ethical issues of the information age, *MIS Quarterly*, 10, 1, 5-12
- Milberg SJ., Smith HJ. et Burke SJ. (2000), Information privacy: Corporate management and national regulation, *Organization Science*, 11(1), 35-57.
- O'Reilly, T., (2007), What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1008839.
- Pekárek M. et Leenes R. (2009), Privacy and social networking sites: follow the money!, W3C Workshop on the Future of Social Networking Barcelona, January 15-16 2009, <http://www.w3.org/2008/09/msnws/papers/tilt.pdf>
- Pelle-Culpin I. (1998), Du paradoxe de la diffusion d'informations environnementales par les entreprises européennes, Thèse de Doctorat en Sciences de Gestion, U. Paris Dauphine
- Squicciarini, AC., Shehab M., et Paci F. (2009), Collective privacy management in social networks. *Proceedings of the 18th international conference on World wide web*. <http://portal.acm.org/citation.cfm?doid=1526709.1526780>.
- Sykes C. (1999), *The End of Privacy*, New York: St. Martin's Press
- Tabatoni P. (2000), Vie privée et management de l'information, *Revue Française de Gestion*, Juin-Juillet-Août, 108-116
- Terré F. (2000), Vie privée, Travaux du groupe d'études société de l'information et vie privée, Académie des Sciences Morales et Politiques, Rapport final, Chapitre 7.
- Tufekci Z. (2008). Can You See Me Now? Audience and Disclosure Management in Online Social Network Sites, *Bulletin of Science and Technology Studies*, 11(4), 544-564.
- Warren S. et Brandeis L. (1890), The right to privacy, *Harvard Law Review*, 4, 5, 193-220