Du consommateur et de sa protection face à de nouvelles applications des technologies de l'information

Colin, Caroline; Poullet, Yves

Published in:
Droit de la consommation

Publication date:
2010

Document Version
le PDF de l'éditeur

Du consommateur et de sa protection face à de nouvelles applications des technologies de l'information : risques et opportunités[1] [2]

Caroline COLIN[3] et Yves POULLET[4]

1. La réflexion proposée entend souligner les risques qu'encourt le consommateur du fait de nouvelles applications des technologies de l'information et de la communication.

Ces applications sont celles développées par des laboratoires de recherche et sont déjà, pour certaines, implémentées de façon expérimentale par des grandes surfaces ou des sociétés prestataires de services de la société de l'information dans le cadre de la télévision interactive. Elles se fondent sur des technologies de collecte de données à distance – comme la RFID et la vidéosurveillance –, sur des logiciels permettant la reconnaissance automatique des émotions et des déplacements des consommateurs et, enfin, sur des méthodes de profilage. Leur but est d'acquérir une connaissance de la clientèle la plus individualisée possible, et ce afin de pouvoir lui proposer le service et/ou la publicité la plus appropriée.

La première partie (chapitre 1) présente certaines de ces applications nouvelles sur la base de deux scénarios à géométrie variable.

À partir de ces deux scénarios, deux types de questions juridiques seront posées. Le premier (chapitre 2) étudie les implications que le développement de ces deux scénarios peut avoir en matière de protection des données à caractère personnel et, plus largement, en

[1] Cet article s'inscrit dans le cadre des recherches entreprises par le CRID (Centre de Recherche Informatique et Droit des FUNDP, Namur) dans le cadre du projet MIAUCE, projet du 6e programme-cadre de l'Union européenne analysant certaines technologies multimodales de surveillance («Multi modal Analysis and Exploration of Users within a controlled Environment», IST Call 5, FP6-2005-IST-5). Les auteurs remercient les chercheurs du CRID travaillant sur ce projet pour leur apport, en particulier Antoinette Rouvroy, docteur en droit et chercheur qualifié F.N.R.S. et Denis Darquennes, informaticien et physicien. Ce projet regroupe un vaste consortium à la fois, d'une part, de centres de recherche universitaires développant des technologies d'observation multimodales du comportement humain (en particulier la reconnaissance des émotions et des déplacements) et des équipes de recherche en matière éthique, juridique et sociologique et, d'autre part, des entreprises intéressées par le développement d'applications nées de ces technologies. Sur ce programme, voy. le site du projet MIAUCE (http://www.miauce.org).

[2] Les auteurs remercient Mme C. Delforge pour sa relecture de l'article et ses conseils précieux.

[3] Docteur en droit et chercheur au CRID.

[4] Professeur aux facultés de droit de Namur et de Liège, directeur du CRID.

matière de protection des libertés et de la dignité humaine. Notre propos soulignera alors la difficulté pour les législations actuelles de répondre totalement et adéquatement aux risques encourus par le consommateur et plaidera, dès lors, en faveur d'un approfondissement de certains concepts et principes des législations de protection des données, voire en faveur de l'adoption de nouvelles réglementations.

Le second type de questions (chapitre 3) s'adressera aux législations de protection des consommateurs. Il s'agira alors d'apprécier dans quelle mesure ces applications nouvelles constituent, dans certains cas, des pratiques déloyales, voire des pratiques discriminatoires, condamnées par la législation européenne en matière de protection des consommateurs.

Au terme de cette double réflexion, et en conclusion, l'article préconisera le croisement ou le cumul des deux types de protection, celle des consommateurs d'une part, et celle de la protection des données, d'autre part. Cette proposition rejoint ce qu'il est convenu d'appeler la «*Consumer Privacy Approach*» mise en évidence aux États-Unis, et dont nous tenterons de démontrer l'intérêt. L'article soulignera, enfin, l'urgence de débats sociétaires sur ces nouvelles technologies qui augurent d'une «société de l'observation»[5] et, en particulier, sur le besoin d'une réflexion fondamentale sur les droits de l'homme dans une telle société.

Chapitre 1. Présentation de deux scénarios

2. Avant d'aborder l'étude des deux scénarios (B), il importe de dire quelques mots sur les méthodes de profilage (A) qui les caractérisent et, de manière plus générale, sur les applications nouvelles fondées sur l'utilisation de données collectées massivement à distance et ayant pour objectif de cibler l'utilisateur afin de lui offrir un service personnalisé (comme, par exemple, l'aide offerte, en temps réel, au porteur d'un GSM lors de ses déplacements ou l'envoi de bannières publicitaires personnalisées, comme le propose désormais Google). Nous terminerons ce chapitre en relevant les risques qu'encourent, à notre sens, les utilisateurs qui font usage de telles applications (C).

[5] Définition donnée dans le rapport MIAUCE (précité), du «*multimodal observation paradigm*» : «this paradigm combines multimodal capture of data 'extracted' from human bodies (facial expressions, eye gaze, postures and motions) with an implicit understanding or interpretation of these data as valid and privileged sources of 'truth' about the persons, their preferences, intentions etc. following the preconception according to which the 'body does not lie' whereas, *a contrario* anything transiting through the prism of individuals' consciousness is a priori suspect and unreliable».

A. Le profilage[6]

3. La société de l'information est entrée dans une nouvelle phase de développement. Celle-ci se caractérise par le déploiement progressif, dans les espaces tant privés que publics, de nouvelles technologies souvent convergentes. Ces technologies sont dotées de capacités inédites de capture, de communication et de traitement de toutes les informations qui naissent des interactions des individus avec leur environnement, que cet environnement soit physique (déplacement, direction du regard) ou digital (*surfing* sur les sites web).

4. Les entreprises opèrent tantôt la rétention et le traitement des données de trafic ou de localisation, tantôt enregistrent les requêtes des utilisateurs d'Internet, leurs habitudes d'achat et leurs mouvements sur le net. Elles traitent les données de géolocalisation générées par les utilisateurs de téléphones mobiles.

On note, en outre, d'une part, le déploiement progressif de caméras de vidéosurveillance dites «intelligentes», équipées de logiciels qui permettent l'enregistrement et facilitent l'interprétation des trajectoires, des attitudes et des comportements des personnes, et d'autre part, le placement de systèmes RFID[7]. La RFID, *Radio Frequency IDentification*, est une puce fonctionnant comme un terminal et qui, grâce à un dispositif technologique, permet le marquage et la lecture sans contact des marchandises ou du corps des individus, auxquels cette puce est intégrée. La structure technique de ces dispositifs est la suivante :

– une mémoire qui peut atteindre une grande capacité, organisée autour d'un microprocesseur;

– un dispositif de communication sans contact, grâce à une antenne d'émission à distance reliée au microprocesseur; au plus l'antenne est grande au plus loin pourra s'effectuer la lecture;

– un mécanisme de production d'énergie, assuré soit par une pile interne, soit par les réactions du bobinage de l'antenne à la traversée d'un champ électromagnétique, ce qui dispense de piles et assure un usage illimité.

Ces éléments sont regroupés pour constituer des puces miniatures, appelées de façon synonyme RFID, *smart tag*, *radio-tag* ou «*transponder*» (*transmitter/responder*). Ces

---

[6] Sur les décisions prises sur la base du profilage des individus, profilage issu d'opérations de «*data mining*» (forage de données) et leur importance dans la prise de décisions des administrations et des entreprises, voy. J.-M. DINANT, C. LAZARO, Y. POULLET et A. ROUVROY, «Rapport au Comité consultatif 'Convention n° 108' du Conseil de l'Europe», septembre 2008, disponible sur le site du Conseil de l'Europe. Voy. également l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. HILDEBRANDT et S. GUTWIRTH, *Profiling the European citizen, Cross disciplinary Perspectives,* Springer Science, Dordrecht, Pays-Bas, 2008.

[7] Sur les RFID, le lecteur consultera le site très complet : http://www.rfida.com/nb/identity.htm.

puces peuvent être lues à distance par un dispositif de lecture (mobile ou stationnaire), qui est également appelé «*transceiver*» (*transmitter/receiver*). Tous ces éléments n'ont de sens qu'à l'intérieur d'un système RFID, qui combine les RFID tags, les lecteurs, les bases de données et les réseaux. Tous ces éléments, en intercation, permettent la collecte, la transmission, le traitement et le stockage des données générées par le RFID ou liées à la possession de celui-ci. Ce système doit être considéré comme un tout. De cette miniaturisation extrême et du fait que les RFIDs sont des dispositifs de communication «sans contact» naît la possibilité d'interactions largement invisibles entre les «choses».

L'ensemble de ces applications par lesquelles les personnes seront entourées par des interfaces intelligentes et interactives gravées (*embedded*) dans des objets de tous les jours et un environnement reconnaissant et répondant à la présence d'individus de manière invisible, constitue ce qu'il est convenu d'appeler l'«internet des objets». Cet internet des objets ouvre des perspectives nouvelles notamment en termes de facilitation des tâches quotidiennes et de surveillance des personnes. Ces systèmes de collecte et de traitement des données «ubiquitaires», dans la mesure où les puces peuvent être placées en tous lieux, préfigurent ce que la Commission européenne[8] appelle les «systèmes d'intelligence ambiante».

Une fois réalisé, le stockage de ces données venant d'une source unique ou de sources multiples s'opère dans de vastes entrepôts de données. Au sein de ces entrepôts, les données sont exploitées de manière de plus en plus performante et ciblée, grâce à des logiciels de corrélation statistique de données (forage de données). Il s'agit, par l'utilisation et l'appariement à une vaste échelle de données individuelles, de mettre en évidence des «profils» qui pourront être utilisés à des fins de prédiction des préférences, comportements et attitudes individuelles, ou de décisions à l'égard de clients, existants ou futurs.

L'expression «profilage» s'entend ainsi d'une technique de traitement des données au service d'une ou de diverses finalités qui tend, à partir de corrélations statistiques opérées sur de nombreuses observations individuelles – anonymisées ou non – d'inférer, quoiqu'avec une part d'incertitude, des informations relatives à une personne (identifiée ou identifiable) à partir des données relatives à un groupe de personnes auquel cette dernière appartient ou est supposée appartenir[9].

---

[8] Le terme est utilisé pour la première fois en 1999 par le Group consultatif du programme IST de l'Union européenne (L'ISTAG) dans son rapport sur le futur des technologies. Sur tout cela, J. AHOLA, «Ambient Intelligence», *ERCIM News*, 2001, n° 47, disponible sur le site : www.ercim.org/publications/Ercim_News/enw47. *Cfr*. également l'expression «d'*Ubiquitous Computing*» lancée dès 1991 par M. WEISER, «The computer for the 21st Century», *Scientific American*, 265 (3), pp. 66 à 75. Sur les défis nouveaux de l'intelligence ambiante, voy. A. ROUVROY, «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence», *Studies in Ethics, Law, and Technology,* Berkeley Electronic Press, 2008.

[9] Sur les décisions prises sur la base de profilage des individus, profilages issus d'opérations de «*data mining*» (forage de données) et leur importance dans la prise de décisions des administrations et des entreprises, voy.

5. Une première caractéristique du profilage – sur laquelle nous reviendrons[10] – peut ainsi être soulignée : le profilage se distingue des traitements classiques de données à caractère personnel dans la mesure où un individu identifiable ou identifié se voit *in fine* attribuer certaines données qui ne sont pas les siennes, mais celles d'un groupe auquel il appartient plus ou moins probablement.

Une deuxième caractéristique mérite d'être énoncée, qui distingue le profilage de la statistique classique. Le traitement statistique a pour but de générer des résultats qui soit décrivent et permettent de comprendre une situation, soit aident à une prise de décisions privées ou publiques abstraites (ainsi, le coût moyen d'une journée d'hospitalisation étant statistiquement d'autant, le gouvernement décide de fixer le remboursement à autant). Ces décisions, une fois prises, auront des effets sur les ou certaines personnes. En d'autres termes, ce qui caractérise le traitement statistique, c'est l'aide à la prise de décision non individuelle, mais globale. Le profilage inclut certes des opérations statistiques, mais il poursuit une finalité distincte de la statistique traditionnelle qui s'intéresse aux seuls résultats agrégés. En matière de profilage, l'application du résultat des opérations statistiques n'a pas pour but de nourrir une décision globale ou de modifier une ligne d'action, mais est directe et individuelle. Ainsi, lorsque Google définit les profils appropriés en fonction des caractéristiques propres à tel produit ou tel service, dont il souhaite assurer une publicité *one-to-one*, il ne s'agit pas, pour lui, de mieux connaître l'état du marché ni, le cas échéant, de prendre une décision stratégique quant à l'évolution de ses propres services. L'intérêt réside ailleurs : le profilage se situe, en effet, en aval de décisions déjà prises par Google et permet simplement d'assurer à celles-ci une effectivité maximale lors d'un envoi publicitaire individualisé, par l'application des critères les plus appropriés et des corrélations les plus riches.

En ce sens, le profilage permet une application immédiate de son résultat. Ainsi, lorsque la personne réagit de telle manière devant son poste de télévision interactive ou lorsqu'elle pose tel ou tel choix de programmes comme nous le verrons dans le scénario 1, la correspondance constatée en temps réel de tels choix au profil X va permettre l'envoi immédiat de l'un(e) ou l'autre bannière ou spot publicitaire.

J.-M. Dinant, C. Lazaro, Y. Poullet et A. Rouvroy, «Rapport au Comité consultatif 'Convention n° 108' du Conseil de l'Europe», septembre 2008, disponible sur le site du Conseil de l'Europe http://www.coe.int/. Voy. également, l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. Hildebrandt et S. Gutwirth, *Profiling the European citizen, Crossdisciplinary Perspectives*, Springer Science, Dordrecht, Pays-Bas et N. Lefever et Y. Poullet, «Entrepôts de données et vie privée», *R.D.T.I.*, 2008/30, pp. 7-20, http://www.stradalex.be.

[10] *Cfr. infra,* n° 21.

B. Les deux scénarios

1. Le scénario : TV interactive

6. Ce scénario consiste à développer des services liés à l'utilisation de la télévision interactive via l'internet et qui sont adaptés aux besoins supposés du client[11]. Il se fonde sur les choix opérés par les spectateurs en ce qui concerne tant les programmes télévisuels offerts dans ce contexte que les autres contenus vidéo qui sont accessibles de cette manière. L'enjeu est d'analyser le comportement de l'utilisateur dans son environnement, chez lui, et de lui fournir des services et informations personnalisés. Il s'agira de publicités répondant aux goûts supposés du spectateur ou de conseils dans la suggestion des programmes à suivre. Ainsi, lorsque le spectateur étiqueté «amateur de voyages exotiques», sportif, passionné par les animaux, mais n'aimant pas les scènes cruelles et disposant de moyens financiers élevés, allumera son poste de télévision, il sera automatiquement invité à rejoindre la dernière émission relative à un reportage sur la Polynésie et les îles du Pacifique en même temps qu'il se verra proposer des publicités sur des safaris photo lointains.

Les concepteurs partent du principe qu'il existe un besoin grandissant de développer un système qui aide les utilisateurs à accéder à des vidéos répondant aux goûts qui correspondent à leurs profils.

La première étape du projet consistera à tester un tel système dans un contexte expérimental, avant de l'intégrer dans un contexte réel. Des volontaires placent ainsi leurs visages devant un ordinateur muni de web caméras afin que leurs réactions face à des scènes puissent être analysées par des logiciels de reconnaissance faciale des émotions, et ce en vue de leur proposer ensuite des vidéos adaptées à leurs désirs ou besoins, exprimés ou non. Ainsi, l'analyse des émotions exprimées tout au long de la visualisation des images et séquences interviendra dans la confection des profils (p. ex. le sourire esquissé en voyant telle actrice, l'expression de dégoût ou de terreur face à une scène dramatique d'un thriller), à côté de l'analyse de la sélection des programmes et de l'utilisation des possibilités de *surfing* que permet un tel type de technologie. Cette technologie multimodale, dans la mesure où elle combine différentes sources d'observation, permet l'élaboration de profils. De plus, le risque de transfert des profils à des tiers est élevé.

[11] La question de la surveillance des consommateurs et de leur comportement en ligne a fait l'objet de nombreux rapports et discussions au sein de la FTC (*Federal Trade Commission*) américaine; voy. notamment le rapport et les discussions relatives à l'«Online Behavioral Advertising Moving the Discussion Forward to Possible Selfregulatory Princples», disponible sur le site : http://www.ftc.gov.bcp/ avec le débat tenu les 1er et 2 novembre 2007 sur le thème : «Behavioral Advertising : Tracking, Targeting and Technology». Voy. également World Privacy Forum, *The Network Advertising Initiative : Falling at Consumer Protection and Selfregulation,* publié le 2 novembre 2007 sur le site : http://www.worldprivacyforum.org.

2. Le scénario : cartes de fidélité munies d'une puce RFID et l'essayage en ligne

7. L'amélioration de la connaissance du client et de ses habitudes de consommation est réalisée grâce à son profilage à partir de données stockées sur la carte de fidélité grâce à des puces RFID[12].

Avec un tel système, les commerçants collectent, tout d'abord, les informations concernant les achats des clients titulaires des cartes de fidélité. La présence d'une puce RFID sur la carte permet, par ailleurs, grâce à des lecteurs de carte placés dans le supermarché, de suivre la personne dans ses déplacements dans les rayons. Le scénario peut même être encore complété. La présence conjointe de puces RFID sur la carte de fidélité, d'une part, et sur les produits en rayon, d'autre part, permet de connaître les produits achetés, les produits approchés voire les produits qui ont été choisis, puis remis dans le rayon. La présence d'un produit dans le caddie couplée à la localisation de la personne dans le magasin permet, via une vidéo placée sur le caddie, d'attirer l'attention du consommateur sur l'intérêt d'acheter un produit qui se marie parfaitement avec celui qu'il a déjà choisi : tel vin pour tel fromage, par exemple. Toutes ces données sont analysées pour élaborer des profils de consommation. Le client qui entre dans un magasin de la chaîne peut automatiquement voir afficher, via la vidéo placée sur le caddie, la liste des courses qui sont habituellement les siennes, se voir rappeler tel oubli ou suggérer tel achat en promotion ou correspondant à ses goûts.

L'intérêt de la carte devient évident si, outre les réductions qui sont déjà proposées et les conseils et services que le client peut recevoir tout au long de sa visite du supermarché, d'autres avantages sont liés à l'enregistrement automatique sur la carte ou via la carte. Ainsi, des magasins proposent, dès maintenant, le système de paiement sans caissière. Le client dont le caddie est rempli d'articles dotés de puces RFID ne doit plus faire la file aux caisses : les achats sont automatiquement comptabilisés et le paiement se fait via le couplage de la carte avec une carte de crédit. On ajoute que la détention d'un certificat de garantie n'est plus nécessaire lorsque, via la carte, la personne peut s'identifier et faire la preuve de l'achat d'un produit dont elle souhaite l'application de la garantie. Des chaînes

[12] Sur les RFID et leurs multiples applications, D. DARQUENNES et Y. POULLET, «RFID : Quelques réflexions introductives à un débat de société», *R.D.T.I.*, 26/2006, pp. 255 à 285. Les RFID se fondent sur une technologie de l'infiniment petit. L'équipement terminal, c'est-à-dire le microprocesseur qui, tantôt, collectera, traitera, émettra ou recevra les informations ou les communications externes, tantôt, se limitera à l'une ou l'autre de ces opérations, peut voir sa taille réduite à la grosseur d'une tête d'épingle ou d'un grain de sable, à tel point que l'on peut parler de «*Smart Dust*». Ces développements technologiques induisent la possibilité d'interactions largement invisibles entre les «choses» (la souris de l'ordinateur, les marchandises, les vêtements, etc.) ou les personnes sur lesquelles seront implantés ces microprocesseurs et des systèmes d'information. Cette interaction permettra aux individus porteurs de ces choses d'être aidés dans leur vie de tous les jours à accomplir leurs tâches ou à des tiers de surveiller leurs activités.

de grands magasins, comme Wal-Mart en Amérique du Nord et Metro en Allemagne, proposent déjà de tels avantages.

8. Deux variantes du scénario sont utiles à notre analyse.

Premièrement, on pourrait imaginer que les clients du supermarché aient la possibilité, grâce aux sites internet de ces boutiques et à la carte de fidélité qui permet de les identifier et de veiller au paiement en ligne, d'essayer virtuellement les vêtements, coiffures… en numérisant une de leurs photos, voire en précisant simplement leurs mensurations sur le site. Les données ainsi récoltées sur le site internet pourraient être couplées avec celles stockées sur la carte de fidélité de manière à améliorer le profil, en particulier, par l'analyse automatisée des réactions psychologiques et des goûts du consommateur.

Une seconde variante peut être proposée. Si la carte permet l'identification de son porteur et de le «tracer» d'une visite à l'autre en gardant en mémoire les opérations qu'il a effectuées, on peut imaginer le fonctionnement de systèmes moins sophistiqués pour les clients ou consommateurs ayant refusé de voir insérer une puce RFID dans leur carte *shopping* : une puce RFID pourrait être placée sur le caddie du client entrant, le caddie étant, par ailleurs, comme dans le scénario complet, doté d'un écran vidéo. Cette puce permettra alors de localiser le client X et d'enregistrer le panier de produits qu'il se constitue comme dans le scénario de base; certes, le supermarché disposera de peu d'informations mais on peut cependant imaginer un profilage limité qui permettra d'adresser tel ou tel conseil publicitaire.

3. Conclusions des deux scénarios

9. Les scénarios des nouvelles applications liées aux technologies ICT que nous venons d'exposer révèlent toute la complexité des systèmes d'information qui permettent leurs mises en œuvre. De tels systèmes autorisent la compilation de toutes les données recueillies et offrent la possibilité, à partir de leur entreposage, de les croiser de façon aléatoire afin de statistiquement dégager des profils très précis des personnes à propos desquelles les données sont collectées, voire de futurs clients. Ainsi, à partir de tel parcours à l'intérieur du magasin, que l'on combine à la présence de tels produits dans le «panier de la ménagère», on peut déduire l'intérêt statistiquement confirmé de l'achat de tel produit. De même, à partir de la séquence des choix d'un spectateur devant une télévision interactive et de la manifestation de telle et telle émotion devant tel et tel passage d'une séquence, on peut déduire telle ou telle tendance en matière de goût artistique, de sexualité ou de voyage.

Ces opérations de profilage, rendues possibles grâce à la collecte d'informations obtenues dans le cadre de l'utilisation d'une télévision interactive ou de cartes de fidélité, mêlent à la fois des données «objectives» (comme la fréquence de visites au magasin, le nombre

et le type d'articles achetés…) et des données «subjectives» (comme la préférence pour telle ou telle couleur de vêtement, le ressenti de telle émotion en regardant tel programme, etc.).

C. Les risques de la société de l'observation et du profilage

10. Ces deux scénarios illustrent cependant aussi les risques encourus du fait de ce qu'il est convenu d'appeler la société de l'observation[13]. Citons les dangers nés :

– du déséquilibre des pouvoirs respectifs[14] des responsables des traitements, qui disposent d'une information de plus en plus précise des habitudes de consommation et de vie de ceux dont ils «traitent» les profils, et du citoyen consommateur concerné.

  Ce déséquilibre peut conduire à toutes sortes de discriminations. Ainsi, on connaît la technique de l'«*adaptative pricing*» développée par Amazon[15], le plus puissant libraire en ligne, qui, en fonction du profil du candidat acheteur, décide du prix affiché sur le site web. Au-delà, on peut aussi songer à l'exclusion automatique de l'accès à certains services ou produits de personnes jugées «peu intéressantes» à partir de leur profil;

– de la «décontextualisation»[16] : les données qui circulent sur la toile sont «émises» par les personnes concernées dans une finalité précise ou dans un contexte particulier. Les croisements de données de toutes sortes, provenant de sources diverses, engendrent la crainte que nous soyons jugés «hors contexte»;

– de l'opacité[17] du fonctionnement tant des *terminaux* (les *cookies*, les RFID) que des *infrastructures* (voir les «agents distribués» localisés tout au long de systèmes d'infor-

---

[13] Voy. définition *supra,* note n° 5.

[14] D.J. Solove, «Privacy and Power : Computer Data Bases and Metaphors for Information Privacy», 53 *Stanford Law Review,* 2001, 6, pp. 1393 et s.

[15] Dans le scénario marketing, le supermarché peut «taguer» les cartes de fidélité qui identifient les clients par leur nom dans l'objectif de connaître et d'enregistrer leurs préférences et habitudes de consommation. Par exemple, des informations comme le temps passé dans le magasin, le nombre de visites en un mois ou le temps passé sans se rendre au magasin… sont autant de données susceptibles d'être collectées puis analysées. Le commerçant bénéficie alors d'une stratégie marketing d'autant plus efficace. L'un des effets pervers de ces actions marketing personnalisées à l'extrême pourrait consister à adopter lors d'achat sur l'internet des prix différents selon les consommateurs. Par exemple, plus vous aimez le chocolat, plus vous le payez cher. Cette technique dite aussi du «*dynamic pricing*» peut être considérée comme une dérive du *profiling*.

[16] L'importance du respect des «contextes», c'est-à-dire des zones de confiance dans lesquelles une donnée à caractère personnel est transmise par la personne concernée a été remarquablement mise en évidence par H. Nissenbaum («Privacy as contextual Integrity», 79 *George.Washington Law Rev.,* 2004, pp. 150 et s.). L'auteur affirme : «*the freedom from scrutiny and zones of 'relative insularity' are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution*».

[17] Les dangers de l'opacité de nos sociétés de l'information comme menace pour nos sociétés de l'information, où les citoyens ne peuvent connaître de manière exacte le fonctionnement des systèmes d'information, les

mation comme ceux dits d'intelligence ambiante). Cette opacité entraîne la crainte de traitements non sollicités, non voulus et la volonté, dès lors, de se conformer à un comportement qui est celui que nous pensons être attendu en ces nouveaux lieux invisibles de surveillance ;

– du *réductionnisme*[18] : de plus en plus, les données collectées à propos des événements même les plus insignifiants de notre vie (comme notre arrêt devant tel rayon d'un supermarché, notre hésitation à acheter tel produit ou notre réaction face à telle émission) se multiplient et les systèmes d'information nous analysent à travers ces données et réduisent notre personnalité, notre identité à des «profils» créés à partir de données personnelles, mais surtout de données relatives à autrui, et ce en fonction de conceptions et en vue de finalités définies par ceux qui utilisent ces données, voire directement par le dispositif technologique[19]. Ainsi, par exemple, l'expression faciale est décodée suivant des algo-

---

données collectées, les lieux de traitement, les finalités poursuivies par ceux qui traitent ces données, sont mis en évidence dès 1983 par le fameux jugement constitutionnel dans l'affaire du recensement (Bundesverfassungsgerichtshof, 15 décembre 1983, *EuGRZ,* 1983, pp. 171 et s.). Les citoyens sont alors tentés d'adopter le comportement qu'ils croient attendu par la société et de ne point oser s'exprimer librement, ce qui est dommageable pour nos démocraties : «*The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights.* ***This would not only impact his chances of development but would have also impact the common good ('Gemeinwohl'), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate*****»**.

[18] Ce danger de «réductionnisme» est déjà dénoncé en 1966 par Karst («'The files' : Legal Control Over the Accuracy and Accessibility of Stored Personal Data», 31 *Law and Contemporary problems,* 1966, p. 361) qui souligne le danger d'«a centralized, standardized data processing» qui ne retient comme signifiants, à propos du sujet de la recherche, que les faits repris et traités par l'ordinateur. Dans le même sens, l'ouvrage de J. Rosen, *The unwanted Gaze : the Destruction of Privacy in America*, 2000, cité par D.J. Solove, *ibidem*, p. 424 : «*Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge*».

[19] C'est précisément la raison de l'article 15 de la directive européenne 95/46 en matière de protection des données qui prévoit des dispositions en matière de systèmes automatisés de décision. La préoccupation majeure a trait à l'automatisation croissante des processus décisionnels à l'égard des individus. Comme le révèlent les travaux préparatoires, le législateur européen en est venu à s'inquiéter d'une telle automatisation tant elle diminue le rôle joué par les personnes dans les processus de décision : «*This provision is designed to protect interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institution deprives the individual*

rithmes savants et, quelle que soit notre culture (un japonais sourit-il comme un belge ?), est traduite unilatéralement comme significative de tel ou tel sentiment[20]. Dans les systèmes d'intelligence ambiante où l'homme est mis en réseau avec un ensemble d'objets qui l'entourent, il devient, au sein de ce réseau, un objet communiquant parmi d'autres et c'est le rapprochement de ces «objets» (ma présence au rayon des fromages) qui va déclencher une action fondée sur mon profil (le rappel de mon achat antérieur et la parfaite combinaison de tel fromage ave le vin que je viens d'acheter);

– de l'abolition de la distinction entre *sphère publique* et *sphère privée*[21]. L'homme perdu dans la foule d'un grand magasin peut être suivi, tracé; l'homme placé devant son poste de télévision révèle ses émotions et son «*surfing*» révèle ses choix et ses préoccupations. Même chez lui, enfermé à double tour, son utilisation de la TV interactive ou de son ordinateur relié à Internet, permettent qu'il soit espionné, «poursuivi» et que ses secrets d'alcôve soient percés. Nous reviendrons sur ce point. La protection du domicile physique, lieu inviolable, apparaissait traditionnellement et aux yeux du droit comme quelque chose de fondamental pour la construction de la personnalité de l'individu. Cette protection-là se trouve, elle aussi, nécessairement bousculée à l'heure actuelle par les nouveaux développements technologiques.

En conclusion, on relèvera surtout le risque, déjà identifié en 1983 par le Tribunal constitutionnel allemand[22] dans l'affaire du recensement statistique, d'une normalisation des

the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'». Une autre préoccupation concerne le fait que l'automatisation galopante des processus de décision engendre une acceptation quasi automatique de la validité et de la pertinence de ces décisions et, corrélativement, un désinvestissement et une déresponsabilisation de décideurs «humains». À cet égard, la Commission relève que «*the results produced by the machine, using more and more sophisticated software, and even expert system, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities*».

[20] Dans le cadre du projet MIAUCE *(*«Multi modal Analysis and Exploration of Users within a controlled Environment», IST Call 5, FP6-2005-IST-5), l'une des technologies concerne l'analyse automatique du regard et des expressions de la physionomie du visage pour en déduire les réactions émotives des personnes vis-à-vis soit de produits de consommation, soit de programmes de télévision.

[21] Sur cette distinction classique et sa radicale remise en cause, J.A. FICHBAUM, «Towards an autonomy-based theory of constitutional Privacy : Beyond the ideology of familial privacy», *Harvard Civil Rights – Civil Liberties Review,* 1979, 14, pp. 361-384. Sur ce point, voy. également, D.J. SOLOVE, «Conceptualizing Privacy», 90 *California Law Review,* 2002, spécialement pp. 1138 et 1139.

[22] Bundesverfassungsgericht, 15 décembre 1983, *EuGRZ,* 1983, pp. 171 et s. Sur cette décision, voy. E.H. RIEDL, «New bearings in German Data Protection», *Human Rights Law Journal*, 1984, vol. 5, n° 1, pp. 67 et s.; H. BURKERT, «Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences», *Dr. Inf.*, 1985, pp. 8 et s.

comportements et des pensées des citoyens[23] dictée par la tyrannie d'un pouvoir informationnel diffus, insaisissable et dont la puissance est sans limites[24].

Chapitre 2. Les législations de protection des données à l'épreuve des développements technologiques

11. Le droit résiste-t-il au progrès technologique ? Peut-il s'adapter aux évolutions techniques de manière à toujours garantir la protection adéquate de nos libertés ?

La législation de protection des données à caractère personnel n'échappe pas à l'interrogation. Confrontées aux nouvelles technologies intelligentes, les règles en la matière doivent, le cas échéant, s'adapter. Il ne s'agit pas de remettre en cause l'essence de la loi mais, au contraire, de faire en sorte qu'elle puisse être applicable à des nouveaux contextes.

Il conviendra, dans un premier temps, de préciser les difficultés rencontrées à propos de l'application de quelques définitions clés de la législation de protection des données à caractère personnel dans ces contextes nouveaux (A). Nous nous concentrerons, ensuite, sur les incertitudes liées à l'application des principes essentiels de nos législations de protection des données : la légitimité, la transparence et la sécurité des traitements de données (B).

A. Les définitions à l'épreuve des applications nouvelles de la société de l'observation

12. Cette partie de l'étude s'attarde sur quelques définitions dont les applications nouvelles obligent à repenser la compréhension. Ainsi, la définition des «données à caractère

---

[23] Voy. D. LYON, «An electronic *Panopticon*? A sociological critique of the surveillance society», *Sociological Review,* 1993, 41(4), 653-678. Pour une analyse de ces enjeux, voy. A. ROUVROY, «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence» (September 11, 2007). Disponible sur SSRN : http://ssrn.com/abstract=1013984.

[24] À cet égard, l'attendu très explicite du tribunal constitutionnel allemand : «*The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights.* ***This would not only impact his chances of development but would have also impact the common good ('Gemeinwohl'), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate***».

personnel» est au centre de controverses récentes qu'il convient d'exposer. L'extension de la notion de données «sensibles» mérite, également, quelques réflexions, de même que la distinction entre «responsable de traitement» et «sous-traitant», qui n'est guère aisée en ces applications nouvelles. Enfin, l'utilisation des méthodes de *profiling* interroge le concept de traitement. Tels sont les points sur lesquels nous proposons de nous arrêter à présent.

1. La notion de «donnée à caractère personnel»

13. La directive 1995/46 définit la notion de «*donnée à caractère personnel*» à l'article 2, *a*) comme «toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui 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».

Si les personnes donnent leur nom pour obtenir une carte de fidélité ou pour avoir la possibilité d'essayer virtuellement tel ou tel vêtement, elles sont assurément identifiables et les règles relatives à la protection des données personnelles s'appliquent. Mais si les nouvelles technologies permettent de profiler les individus ou de faire d'autres traitements en ne recueillant pas les données directement ou indirectement nominatives (numéro de client lié à la facturation par exemple), est-ce à dire que la législation de protection relative à ces données soit inapplicable? Cette interrogation est suscitée par l'analyse du scénario minimaliste que nous avons décrit à propos du traçage des clients dans le supermarché.

14. L'approche de la notion de donnée à caractère personnel évolue avec les nouvelles technologies et, notamment, avec les systèmes RFID qui permettent d'identifier un objet, mais non une personne – et ce même s'il va de soi que, derrière le repérage de l'objet, c'est en définitive son détenteur, personne physique, qui est visé et auquel s'adressera la décision[25] –. Étant donné que ces techniques peuvent fonctionner sans avoir besoin d'identifier les individus, on peut, si du moins on estime que l'utilisation de telles données

[25] Prenons le cas de la puce RFID mise sur le caddie du grand magasin plutôt que sur la carte de fidélité. Le repérage des mouvements du caddie permet de connaître les déplacements du consommateur (non identifiable certes) et grâce au croisement des RFID placés sur les produits du grand magasin et du RFID du caddie, les produits achetés. En d'autres termes, nonobstant la conservation du caractère anonyme des données collectées, le système d'information pourra sélectionner des publicités appropriées («Vous venez d'acheter tel vin, vous êtes au rayon des fromages, nous vous conseillons ….») et les envoyer sur la vidéo placée sur le caddie. Bref, même sans chercher le moins du monde à identifier la personne, le système permet cependant une individualisation de la décision à prendre vis-à-vis d'une personne et ce en fonction d'un profil créé à partir de données qui restent anonymes. Le même raisonnement peut être tenu à propos de cookies qui permettent d'identifier non un individu mais une session sur un ordinateur. On sait que la qualification des cookies comme données à caractère personnel est défendue par le Groupe de l'article 29. Elle est cependant contestable.

présente des risques pour les libertés des individus, suggérer deux pistes. La première serait d'étendre le concept de donnée personnelle dans un sens tout à la fois plus large et plus flexible. La seconde serait de réglementer comme telles ces données qui, sans identifier la personne, permettent néanmoins de l'individualiser afin de prendre des décisions à son égard. La question mérite d'être posée à propos d'autres données, comme celles collectées via les *cookies* qui ne réfèrent pas à un individu, mais à une session ouverte sur un ordinateur et donc, en d'autres termes, également à un objet.

En 2007, le Groupe de l'article 29 a adopté une opinion sur le concept de donnée à caractère personnel[26] dans le sens de la première option. En se fondant sur la *ratio legis* du législateur européen, il adopte une définition large de la donnée à caractère personnel qui doit couvrir toutes les informations qui peuvent être reliées à un individu[27].

Si, selon la définition rappelée, l'information, pour constituer une donnée à caractère personnel, doit concerner une personne physique identifiée ou identifiable[28], cette notion doit s'entendre, selon le Groupe de travail de l'article 29 – qui se réfère à un précédent document de travail consacré précisément aux RFID –, non seulement comme le fait que les données concernent une personne physique «si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne»[29], mais également si «cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée»[30]. En d'autres

[26] Groupe de travail «article 29» sur la protection des données, «Avis 4/2007 sur le concept de données à caractère personnel», 20 juin 2007, WP 136, disponible en ligne.

[27] Voy. les références données par le Groupe de l'article 29, précité, spéc. p. 4.

[28] Selon le considérant n° 26, «pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne». Ainsi, l'adresse IP, même dans le cas où l'attribution de cette adresse est purement temporaire comme c'est le cas dans le cadre de l'IP v.4, serait une donnée à caractère personnel puisque celui qui la traite peut, le cas échéant, retrouver le fournisseur d'accès et lui demander à quel client il a fourni une telle adresse. La Cour de cassation française remet en cause ce raisonnement en soulignant à juste titre selon nous que précisément selon la loi il est interdit aux fournisseurs de délivrer une telle information sauf aux autorités de police et estime donc qu'hormis pour la police, la donnée IP n'est pas une donnée à caractère personnel (Cass., 1er mai 2007 et 27 avril 2007) : «Cette série de chiffres (ne constituent) en rien une donnée indirectement nominative à la personne dans la mesure où elle ne se rapporte qu'à une machine et non à l'individu qui utilise cette machine» et «l'adresse IP ne (permettait pas d'identifier le ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur d'accès l'identité de l'utilisateur». Voy. également la décision de la même instance du 13 janvier 2009 plus prudente certes mais aboutissant aux mêmes conclusions. À propos de ces décisions, voy. Y. Defraigne et A.M. Escoffier, «La vie privée à l'heure des mémoires numériques», Rapport d'information, Commission des lois, n° 441, 2008-2009, disponible sur le site du sénat français : www.senat.fr.

[29] Le Groupe de l'article 29 met en exergue le «caractère dynamique» du critère en ce sens que la technologie pourra permettre l'identification des personnes à un instant t+1 alors qu'elle ne pouvait pas le faire à l'instant t.

[30] Groupe de travail «article 29» sur la protection des données, «Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)», 19 janvier 2005, WP 105, disponible en ligne sur le site : http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.

termes, la donnée est à caractère personnel soit par sa nature ou son contexte qui renverrait à la possibilité d'identification, soit par sa «finalité» ou par son «résultat» recherché, à savoir pouvoir prendre une décision vis-à-vis d'une personne même non identifiée ou non identifiable[31].

L'élément de finalité consiste dans le fait que les données sont susceptibles de permettre à une entreprise ou une administration de traiter une personne différemment.

L'élément de résultat peut être défini, selon le Groupe de l'article 29, comme l'impact provoqué par l'utilisation des données afin d'influer sur le statut ou le comportement d'une personne. L'impact n'a pas besoin d'être important. Il suffit que le procédé aboutisse à traiter un individu d'une manière différente. C'est le cas dans le scénario minimaliste que nous venons d'évoquer; c'est le cas lorsqu'à partir de *cookies*, des sociétés de *cybermarketing* (comme *Double click*), voire des entreprises comme Amazon semble-t-il, peuvent cibler la publicité à envoyer, voire différencier les pages web et les prix affichés sur ces pages à partir du profil généré par l'utilisation des données collectées via les *cookies*.

15. Faut-il suivre l'opinion du Groupe de l'article 29? Nous ne le pensons pas. Cette opinion poursuit, certes, le but louable d'étendre le régime de protection des données à caractère personnel, mais cette extension, outre qu'elle ne respecte pas la définition de la directive, pose des problèmes délicats lorsqu'il s'agit d'appliquer le droit d'accès prévu pour la personne concernée. La personne X à laquelle se réfère un *cookie* ou un tag RFID devra, pour accéder aux données générées par ce *cookie* ou cet RFID, commencer par s'identifier et, en d'autres termes, révéler à celui qui, jusqu'à présent, pouvait la tracer, voire l'individualiser sans l'identifier, les données d'identification qui jusque là lui manquaient[32]. N'est-il, dès lors, pas préférable, comme le suggère la directive 2002/58 dite *e-privacy*, de réglementer le traçage même sans identification des personnes en appliquant les principes de transparence et de proportionnalité[33]?

[31] Groupe de travail «article 29» sur la protection des données, «Avis 4/2007 sur le concept de données à caractère personnel», *op. cit*., spéc. p. 11.

[32] … sauf à autoriser le droit d'accès via le même «identifiant» que celui utilisé par le responsable du système, c'est-à-dire le «cookie» ou le numéro du tag.

[33] Sur cette idée d'une législation de troisième génération, voy. Y. POULLET, «Pour une troisième génération de réglementation de protection des données», in *Défis du droit à la protection à la vie privée*, coll. Cahiers du CRID, tome 31, Bruxelles, Bruylant, 2008, pp. 25-70. Et plus récemment, du même auteur, «About the E-Privacy Directive : Towards a third generation of data protection legislation?», in S. GUTWIRTH, Y. POULLET et P. DE HERT (eds.), *Citizens in a profiled World*, Proceedings of the second CPDP Conference, janvier 2009, Springer Verlag, Dordrecht, en voie de publication.

2. La notion de «donnée sensible»

16. L'article 8 de la directive dispose que : «1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle». Cette catégorie particulière de données ne doit pas être traitée excepté si «*a*) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée».

Le consentement de la personne concernée est souvent présenté comme le critère déterminant pour légitimer les traitements de données sensibles. On note, cependant, que les lois internes des États membres peuvent affirmer que le traitement des données sensibles est interdit même en présence d'un tel consentement. Les législations ne sont pas toutes égales à ce sujet[34] et cette disparité témoigne des craintes ressenties vis-à-vis du principe selon lequel le consentement permettrait de légitimer n'importe quel traitement.

17. Qu'est-ce qu'une «donnée sensible»?

Dans notre hypothèse, si un client achète un livre qui aborde des thèmes religieux ou sexuels et que ce produit est enregistré sur sa carte de fidélité et est utilisé pour construire son profil, il pourrait être soutenu que des données sensibles ont été traitées.

D'un autre côté, il serait tout à fait possible de dire que le lien entre le produit et la personne qui l'a acheté n'est pas si évident. Tout d'abord, les gens peuvent acheter tel ou tel article dans le seul objectif de s'informer sur un sujet sans que cet achat reflète réellement leurs goûts personnels. Ensuite, les clients peuvent acheter un produit pour quelqu'un d'autre. L'appréciation de ce qu'est une donnée sensible dépend de la nature du produit et de la nature de la transaction[35]. Par exemple, un auteur relève, en ce qui concerne la nature du produit, que «*an academic treatise on Satanism will tend to say less about the purchaser's personal religious inclinations than, say, a video-clip depicting satanistic rituals for the purpose of viewer entertainment*»; de même concernant la nature de la transaction : «*a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products on a similar theme*»[36].

---

[34] Voy. A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, Travaux du CERIC, Bruylant, 2007, p. 63.

[35] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, Information Law Series, Kluwer Law International, 2002, n° 18.4.3, pp. 344-345.

[36] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit*., n° 18.4.3, pp. 344-345.

De surcroît, des données qui, à l'origine, ne sont pas considérées comme sensibles, pourraient le devenir si elles sont collectées et organisées dans de grandes bases de données et acquièrent alors une forte valeur économique. Les données en elles-mêmes ne sont pas sensibles, mais leur volume, et donc le fait qu'elles peuvent donner lieu à une opération lucrative, a un impact sur leur caractéristique[37]. Ce ne serait donc pas tant la nature de la donnée elle-même qu'il faudrait prendre en compte pour attester de son caractère sensible ou pas, mais plutôt la nature de sa communication.

18. Les applications des TIC amènent à s'interroger sur la nécessité de consacrer une nouvelle catégorie de données sensibles : les identifiants numériques, les RFID placés dans les cartes de fidélité, les *cookies* ou l'adresse IP dans le cadre de la télévision interactive de demain. Une évolution remarquable des systèmes d'information, qu'ils soient locaux ou globaux, résulte en effet de la disponibilité et de l'utilisation de méthodes d'identification et d'authentification des acteurs/utilisateurs des systèmes d'information. Ces méthodes permettent à ces derniers de se faire connaître ou reconnaître lorsque cette «identification» conditionne l'accès à une ressource (*cfr*. les systèmes dits d'*Identity Management)*, à un service ou à une information. Elles autorisent également d'identifier ces utilisateurs de manière sûre lorsqu'il s'agit d'additionner, de croiser ou de déduire des données nouvelles à leur propos et ce à partir d'éléments d'information dispersés dans des bases de données distribuées dans le réseau. On note par ailleurs que ces réseaux peuvent être sans limites de frontières[38]. Ces «*digital identities*» constituent alors des métadonnées qui permettent de croiser les informations relatives à une personne dans des bases de données diverses[39]. On souligne le danger lié à l'utilisation de *digital identities* communes à plusieurs secteurs de notre existence. Il est évident que plus une méthode d'identification est commune à de nombreuses bases de données, plus le croisement de ces bases de données est facile. Ainsi, si l'accès à tous les fichiers administratifs est conditionné par l'utilisation du code d'accès lié à la carte d'identité, il est possible de tracer toutes les

---

[37] J. Bing, «Introduction – Notions of sensitive personal data», in *Challenges of privacy and data protection law, Perspectives of european and north american law*, Bruylant, Cahiers du CRID, tome 31, 2008, pp. 191-208, spéc. p. 195.

[38] C'est ce que nous avons appelé les données d'ancrage, données à caractère personnel qui permettent de faire le lien entre des données relatives à un même individu mais localisées dans des bases de données diverses. Cette notion s'oppose aux données biographiques qui décrivent un élément de la vie de l'individu ou le caractérisent. Notre propos était de souligner l'insuffisante attention portée par les législations de protection des données à cette catégorie de données : Y. Poullet et J.-M. Dinant, «L'autodétermination informationnelle à l'ère de l'Internet», Rapport pour le Conseil de l'Europe, novembre 2004, disponible en ligne sur le site du Conseil de l'Europe.

[39] Sur ces dangers, M.C. Rundle et P. Trevithick, «Interoperability in the new Digital Identity Infrastructure», (Feb. 13, 2007) papier publié sur Social Science Research Network, disponible sur le site : http://papers.ssrn.com/sol3/papers.cfm?abstract._id=962701 ; M.C. Rundle, «International Personal Data and Digital Identity Management Tools», Research Publication Paper, The Berckman Center for Internet and Society, n° 2006, juin 2006, disponible sur le site : http://cyberlaw.law.harcvard.edu/publications.

requêtes d'un citoyen par rapport à l'ensemble des sites et bases de données de l'administration. De manière générale, c'est toute la question de l'intégrité contextuelle qui est posée par ce partage d'identifiants entre les responsables de traitements.

3. La distinction entre responsable de traitement (art. 2, b) de la directive), sous-traitant (art. 2, d)) et de quelques nouveaux venus

19. Si, pour ce qui concerne la gestion des cartes de fidélité, le responsable de traitement sera le commerçant, en règle générale, les opérations de profilage sont «sous-traitées» à une société qui agit alors sous le contrôle du responsable. En effet, étant donné que le profilage est une activité très spécifique et nécessite de vastes entrepôts de données et des logiciels permettant de découvrir des inférences statistiques, les magasins sont obligés de déléguer l'analyse des données collectées à des sociétés spécialisées. Ces sociétés sont-elles de simples sous-traitants au sens de la directive et, dès lors, soumises au régime de son article 17.3[40]? Ces sociétés peuvent, en effet, être intéressées par les plus-values que peut offrir le croisement avec des données venant d'autres sources (p. ex. des données statistiques sur les revenus de la population visée, les préférences exprimées vis-à-vis d'autres services, etc.) ou la vente des profils à d'autres. Dans de tels cas, nous aurons affaire à deux responsables de traitement, qui pourraient être tenus solidairement selon l'article 2, *b*).

20. À ce duo, il faut ajouter l'intervention de l'opérateur ou concepteur du système d'information, de même que du fabricant des terminaux. La notion de «terminal» est définie par la directive européenne sur les équipements terminaux[41] de la façon suivante : «un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications (à savoir des réseaux de télécommunications servant entièrement ou en partie à la fourniture de services de télécommunications accessibles au public)». Cette définition, très large, permet d'englober non seulement les ordinateurs personnels, les terminaux classiques comme le téléphone (mobile ou non), le fax ou autres,

[40] L'article 17-3 de la directive, qui appréhende la sécurité du processus de traitement, dispose que «la réalisation de traitements en sous-traitance doit être régie par un contrat». Celui-ci doit mentionner que le sous-traitant n'agit que sur la seule instruction du responsable de traitement. L'article 17-2 indique qu'il incombe au responsable de traitement de choisir un sous-traitant «qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer». Il a le devoir d'attester de la qualité du sous-traitant. De plus, il doit vérifier que le sous-traitant respecte ses obligations contractuelles sans les outrepasser. À titre d'exemple, ce dernier ne peut traiter les données collectées pour d'autres finalités que celles inscrites au contrat. Sinon il devient à son tour un responsable de traitement et encourt alors des sanctions pour non-respect des règles légales en la matière.

[41] Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.,* n° L 091 du 7 avril 1999, pp. 0010-0028.

mais également la télévision interactive, les RFID (*Radio Frequency Identifiers*)[42], les cartes à puces[43] et, demain, les molécules «intelligentes» implantées au sein même du corps des individus.

Le récent débat européen sur les RFID a amené la Commission européenne à émettre la Recommandation du 12 mai 2009[44] qui affirme la responsabilité des constructeurs d'équipements terminaux et des fournisseurs des systèmes RFID, c'est-à-dire des infrastructures qui englobent tant les systèmes de collecte et de transmission des données générées par les terminaux RFID que les bases de données dans lesquelles ces données seront analysées et grâces auxquelles les décisions *ad hoc* seront prises. Cet élargissement de la protection des données à une réglementation des infrastructures et des terminaux est indispensable. Comment assurer la protection des données de manière effective si des solutions techniques ne prennent pas en compte ces exigences et ne les traduisent pas efficacement? Ainsi, pour reprendre l'exemple des RFID, souhaite-t-on, avec le Groupe de l'article 29[45], permettre que le porteur de la puce puisse aisément la désactiver, que le système de transmission utilise les solutions de la cryptographie? Cette approche dite «*privacy by design*»[46], affirmée par la récente Recommandation européenne[47], se fonde sur une réflexion fondamentale, qui fut traduite pour la première fois par les rédacteurs de la loi française de 1978 : «L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit

[42] Pour rappel (voy. *supra*, n° 4), les terminaux que sont les RFID possèdent les éléments suivants :
– un processeur;
– une mémoire morte;
– une antenne qui permet tout à la fois de communiquer avec un terminal et de recevoir l'énergie requise pour faire fonctionner l'ordinateur;
– absence de périphériques d'entrée/sortie accessibles à un être humain;
– très haut degré de miniaturisation (de l'ordre de quelques millimètres, antenne incluse).
Sur les RFID, le lecteur consultera le site très complet : http://www.rfida.com/nb/identity.htm.

[43] Certaines cartes à puces sont équipées de processeurs aussi puissants que les célèbres Apple du début des années 80.

[44] Recommandation sur l'application des principes de vie privée et de protection des données à caractère personnel, C (2009) 3200 Final. À propos de cette recommandation, voy. nos réflexions in «About the E-Privacy Directive : Towards a third generation of data protection legislation?», in S. Gutwirth, Y. Poullet et P. de Hert (eds.), *Citizens in a profiled World*, Proceedings of the second CPDP Conference, janvier 2009, Springer Verlag, Dordrecht.

[45] «Working paper on the questions of data protection posed by RFID technology», 19 janvier 2005, WP No. 105 disponible sur le site de la Commission européenne : http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.

[46] Comme affirmé par A. Cavioukan, Commissioner of Data Protection for the Province of Ontario, Canada, dans l'introduction aux «Privacy Guidelines for RFID Information Systems», disponible sur le site : http://www.ipc.on.ca : «Privacy and Security must be built in from the Outset – at the design Stage».

[47] La recommandation européenne invite l'opérateur RFID (tant le fabricant des terminaux que le designer du système d'information) à rédiger et publier un rapport sur l'impact de son système ou de son terminal sur la protection des données et la vie privée des personnes concernées par le développement du système RFID.

porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques». À partir de ce texte, les autorités de protection des données ont, à plusieurs reprises, affirmé le principe de la responsabilité des fournisseurs d'équipements terminaux et des concepteurs d'infrastructures quant aux risques que l'utilisation de leurs infrastructures ou terminaux peuvent engendrer vis-à-vis de la protection des données de leurs utilisateurs.

En conclusion, il nous semble que le rôle de chacun des intervenants que nous venons de décrire, celui qui assure la collecte des données et les traitent selon la méthode de profilage, le fabricant des terminaux qui permet cette collecte, le concepteur du système d'information, celui ou ceux qui utilisent *in fine* le profil vis-à-vis des utilisateurs de son service, doit être clairement déterminé et qualifié à des fins d'imputation des éventuelles responsabilités. Les contrats entre les parties devraient, de même, être très précis sur l'imputation des risques nés du recours à de tels systèmes. Ainsi, que se passe-t-il si le profil de «mauvais» client conduit à bloquer l'accès à certains services ou certains produits ou entraîne des discriminations vis-à-vis de ce dernier? Qui en supporte la responsabilité? Que se passe-t-il en cas de mauvais fonctionnement du système qui aboutit à réclamer une somme inexacte à un client voire à le suspecter de vol d'un produit? Enfin la mauvaise sécurité des bases de données créées pour déterminer les profils peut aboutir à l'utilisation par un tiers non autorisé des profils des consommateurs. Faudra-t-il en imputer la responsabilité partielle au concepteur du système ou à l'entreprise qui l'utilise?

4. La notion de «traitement» au regard de l'utilisation des techniques de profilage

21. Le *profiling* est-il un traitement ou une méthode d'exploitation des données au service d'un traitement? Dans les scénarios proposés, le profilage réalisé tantôt à partir des cartes de fidélité des clients des magasins et des puces RFID, tantôt à partir des données de *surfing* couplées avec les données émotionnelles du spectateur poursuivent la même finalité : établir une dynamique de marketing *one-to-one*. En d'autres termes, il ne paraît pas que le profilage soit en soi une finalité, mais il permet simplement de poursuivre plus aisément la finalité du traitement marketing. La finalité pourrait être multiple. Outre celle du marketing, il s'agirait, par exemple, dans le scénario «supermarché», de contrôler les déplacements des clients, d'éviter les vols dans les grands magasins, de déterminer l'offre à faire à la clientèle, voire de vendre les profils à d'autres sociétés. Le profilage peut alors être défini comme : «*the interference of a set of characteristics (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics. The set of characteristics will typically relate to the behaviour (actual or expected) of a person/entity. (…) What is new (…) is the increasingly extensive, systematic use by organisations of relatively formalised and*

sophisticated profiling practices ***for a variety of control purposes*** »[48]. En d'autres termes, le *profiling* n'est pas un objectif en lui-même, mais bien un moyen technique d'obtenir un résultat particulier au sein d'un ou de plusieurs traitements[49].

22. Il n'empêche que le profilage, comme d'ailleurs les systèmes automatisés de décisions visés à l'article 15 de la directive[50], constitue une technique qui requiert une protection spécifique tant il est vrai que, grâce à elle, les traitements de données deviennent de plus en plus puissants. Il suffit, à cet égard, de songer au nombre croissant de données traitées ou à la sophistication grandissante de tous ces procédés[51].

23. Ainsi, l'agrégation de données en provenance de diverses bases de données permettra de déduire avec un taux de 89% de certitude que la composition de tel panier d'achat par un consommateur se présentant dans une grande surface à telle heure de la journée induit le fait que cette personne est vraisemblablement célibataire, amateur de voyages lointains et fraudeur potentiel. Le profil du terroriste se déduit du croisement de données aussi diverses que le registre de la population, les utilisations de cartes de crédit, les déplacements recensés grâce aux mobilophones, les cartes de fidélité, la consommation de médicaments, etc.[52] La diminution drastique des coûts de stockage, la sophistication des outils d'analyse de données et les puissances de calcul de nos ordinateurs autorisent ces croisements aléatoires d'où sort la vérité, au moins statistique, des profils qu'il reste à confronter aux données relatives à des personnes particulières. En d'autres termes, le citoyen se voit ici appliquer le résultat d'une connaissance déduite de ce profil construit à partir de

---

[48] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit*., n° 17.2, p. 301. *Cfr*. également l'excellent ouvrage collectif : *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. Hildebrandt et S. Gutwirth (éd.), *op. cit.*; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», Council of Europe, 13/14 mars 2008; S. Ranse, «Le *profiling* des internautes au regard du droit au respect de la vie privée : le coût de l'efficacité!», *R.D.T.I.,* 20/2004. Et récemment, «Data collection, targeting and profiling of consumers for commercial purposes in online environments», European Commission, Health and Consumers Directorate-General, Bruxelles, 5 mars 2009.

[49] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», *op. cit*., spéc. p. 32.

[50] *Cfr. infra,* n° 30.

[51] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», *op. cit*., spéc. p. 33. Et les auteurs de poursuivre : «*Without such protective arrangements, there is a significant risk that commercial undertakings will make increasing and systematic use of rapid and inexpensive profiling of their customers. Such profiling will inevitably result in certain individuals being excluded from particular goods or services or having to pay a higher price for them*». Voy. également l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. Hildebrandt et S. Gutwirth, *Profiling the European citizen, Cross disciplinary Perspectives, op. cit.*

[52] À propos des applications du «*data mining*», en matière de sécurité publique, voy. D.J. Solove, «Data Mining and The Security – Liberty Debate», 75 *University Chicago Law Review*, 2008, pp. 343 et s. L'auteur évoque en particulier le programme américain Matrix (*Multistate Anti-Terrorism Information Exchange*).

données qui ne le concernent pas, qui ont souvent peu de lien logique avec l'opération pour laquelle ce profil est utilisé et qui lui sont largement inconnues. Pire, ce profil induit pour le responsable du traitement une meilleure connaissance de la personne concernée que celle qu'elle a d'elle-même et si cette personne conteste que ce profil lui convient ou que la décision prise à son égard est erronée, il lui appartiendra de faire la preuve de cette erreur[53] .

B. Les principes

24. La suite détaille les questions soulevées à propos de quelques principes : légitimité, proportionnalité, loyauté, transparence et sécurité.

1. Le principe de loyauté et de transparence

25. L'article 6.1 de la directive 95/46/EC exige la loyauté de la collecte des données et du traitement. Ce prescrit d'une collecte loyale implique que la personne soit informée chaque fois que des données sont collectées. Le fonctionnement, d'une part, des systèmes RFID, vu la dimension du terminal voire son fonctionnement invisible et, d'autre part, des modes de collecte liés à la télévision interactive et de manière générale à l'internet, justifie l'attention particulière donnée à ce premier principe. Une première obligation est dégagée par les opinions du Groupe de l'article 29 en matière de RFID et consacrée par la Recommandation évoquée *supra*[54] : il s'agit de l'obligation de rendre transparente, en ce compris par l'affichage d'un label, la présence des RFID. De surcroît, comme il a été souligné, ces modes de collecte vont bien au-delà des «attentes raisonnables» de la personne. Ainsi, même si cette dernière connaît l'existence de la puce RFID, peut-elle imaginer que cette puce permettra d'enregistrer ses déplacements, ses hésitations devant tel ou tel produit, que la collecte ne s'arrête pas à une seule visite mais couvre l'ensemble des visites opérées dans les magasins de la chaîne et que cette mémoire autorise un profilage serré ?

L'article 10 de la directive fait écho à cette exigence de loyauté en obligeant le responsable de traitement à fournir l'information nécessaire sur le nom du responsable, les finalités, les tiers auxquels les données seront communiquées et l'existence du droit d'accès. L'article ajoute que ce devoir d'information doit s'étendre à toute information qui apparaîtrait nécessaire pour garantir le caractère loyal du traitement au vu des circonstances particulières de celui-ci. Cet ajout trouve tout son sens dans le cas de l'utilisation de ces technologies nouvelles au fonctionnement opaque. Il est important que la personne dont

[53] Sur ce renversement de la preuve induit par le profilage, voy. D.J. STEINBOCK, «Data Matching, Data Mining and Due Process», 40 *GA Law Rev,* (2005), 1, pp. 82 et s.

[54] *Cfr. supra,* n° 20.

le maniement de la télévision interactive, voire ses émotions, sont suivis, soit au courant non seulement de la collecte de toutes ces données mais de l'application à toutes ces données voire à d'autres, des techniques de profilage. Le même raisonnement vaut dans le cadre du scénario RFID.

26. Le droit d'accès, de correction ou de complément affirmé par l'article 12 de la directive prolonge ce devoir de transparence du responsable du traitement. L'article 12 prévoit que ce droit couvre l'accès non seulement aux données collectées mais également aux informations résultant du traitement et, en cas de décision automatisée, à la logique du système[55]. Dans la mesure où les profilages auxquels les scénarios font allusion constituent des systèmes automatisés de décision, même si *in casu* leur portée (envoi de publicité ou ajustement de prix) est insuffisante pour que joue l'article 15 de la directive relatif à ces systèmes automatisés de décision[56], nous estimons au vu de la généralisation de l'utilisation des techniques de profilage et des risques de manipulation des individus qu'elles entraînent, que la disposition prévoyant l'accès à la logique devrait s'appliquer. En d'autres termes, la personne à laquelle un profil est opposé devrait pouvoir connaître la «logique» certes toute aléatoire mais bien présente qui a permis d'établir le profil. Savoir que l'on me recommande tel ou tel programme de télévision sur la base du fait que mon *surfing* et mes émotions me rangent dans telle catégorie est, à notre avis, une exigence si on désire – ce qui est le but du droit d'accès – permettre à la personne de retrouver un certain équilibre informationnel dans sa relation avec les responsables de traitement. C'est sur la base de cette connaissance que la personne concernée pourra le cas échéant rectifier le jugement d'autrui fondé sur l'application automatisée du profil voire s'opposer à la poursuite de son profilage.

Ce droit d'accès n'est cependant pas absolu. Il suppose que le responsable connaisse cette logique… Ensuite, celle-ci devrait être disponible, documentée, prête à être consultée. La documentation doit contenir des informations sur les catégories de données traitées et sur leur rôle dans le processus de décision[57]. Par ailleurs, il est tout à fait probable que la méthode de *profiling* constitue un savoir-faire[58], que le responsable du traitement ou son sous-traitant opposera à la demande d'accès de la personne concernée. La société qui est en charge de cette activité développe en effet certainement ses propres moyens techniques

[55] Le droit d'accès inclut «la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15, § 1er» (article 12, *a*) de la directive).

[56] *Cfr. infra,* n° 30.

[57] Lee A. Bygrave, «Data Protection Law, Approaching Its Rationale, Logic and Limits», *op. cit.*, n° 18.3.1, p. 325.

[58] Sur le sujet, voy. notamment *Le know-how*, 5e rencontre de Propriété industrielle, Travaux de la Faculté de droit et des sciences économiques de Montpellier, Librairies techniques, Actualités de droit de l'entreprise, tome 7, 1976.

ou algorithmes pour réaliser des profils de haute qualité. Son succès dépend de ses compétences particulières. Le savoir-faire a une valeur économique importante et est donc gardé secret. L'entreprise ne détient pas de droit privatif sur le savoir-faire. Toutefois, celui-ci est protégé par deux moyens. La concurrence déloyale est l'un d'eux, au cas où un individu aurait l'intention de révéler le savoir-faire à d'autres sociétés sans permission, ou si un concurrent le volait en s'adonnant à l'espionnage industriel. La révélation d'un secret d'affaires est également réprimée pénalement. Il existe une situation similaire en droit de la concurrence quand l'individu impliqué dans une procédure en la matière se voit accordé un droit d'accès aux dossiers de la Commission pour garantir le principe d'égalité des armes[59]. En fait, bien que ce droit d'accès soit consacré dans différents textes de la Communauté européenne, il ne peut être exercé qu'en respectant la protection conférée au secret d'affaires[60]. Le droit d'accès devrait être, selon nous, limité par ce qui est strictement nécessaire au maintien du secret d'affaires[61], qui ne peut être un argument pour rejeter en bloc toute demande d'un individu d'accéder à ses données à caractère personnel.

2. Le principe de légitimité des finalités poursuivies par la collecte des données

a. Le *profiling* et la question de la finalité légitime et/ou compatible

27. En vertu de l'article 6 de la directive de 1995, «Les États membres prévoient que les données à caractère personnel doivent être : *b*) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées».

Ce qui nous intéresse est le traitement ultérieur des données qui pourrait être fait. Seul un traitement visant les mêmes finalités que le traitement originel est accepté; si les finalités sont incompatibles, le traitement est interdit ou plutôt doit faire l'objet d'une base de légitimité propre, ne pouvant s'appuyer sur la légitimité du traitement de base. Pour savoir si

[59] Voy. A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, *op. cit.*, p. 43.

[60] Article 27 (1) et (2) de la recommandation du Conseil (EC) n° 1/2003 du 16 décembre 2002 sur la mise en œuvre des règles de concurrence des articles 81 et 82 du Traité de l'UE. Voy. A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, *op. cit*., pp. 43-44.

[61] Article 15 (1) et (2) de la Recommandation du Conseil (EC) n° 773/2004 du 7 avril 2004 concernant les procédures menées par la Commission conformément aux articles 81 et 82 du Traité de l'UE. Voy. A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, *op. cit*., pp. 43-44.

une finalité est compatible ou non avec celle d'origine, il faut se référer au critère de la «*reasonable expectation*» des personnes concernées : les individus sont-ils en mesure de supposer, au début du procédé de traitement des données, que celles-ci pourront être traitées d'une autre manière ? Plus spécifiquement, l'objectif initial du traitement de données – les cartes de fidélité par exemple – inclut-il le *profiling* ? En cas de réponse positive, le nouveau procédé est compatible avec le premier, et donc aucune formalité supplémentaire n'est à accomplir. Mais en cas de réponse négative, le procédé doit satisfaire toutes les règles requises par la loi pour être légitime.

28. L'exigence de compatibilité ne s'applique qu'aux finalités des traitements de données. Et dans la mesure où le *profiling* ne constitue pas une finalité mais une méthode de traitement, la question de la «*reasonable expectation*» ne doit pas être soulevée en termes de légitimité mais le cas échéant comme déjà affirmé en matière de loyauté ou de transparence[62] et de proportionnalité[63]. En effet, la technique du *profiling* est mise au service de la finalité «*marketing*» qui peut trouver sa légitimité soit dans l'article 7, *f*) de la directive[64], soit dans le consentement des personnes concernées[65]. Ce deuxième fondement fait l'objet des réflexions qui suivent; disons un mot à propos du premier fondement. L'article 7, *h*) exige que l'on mette en balance les intérêts du responsable du traitement, ceux de tiers auxquels les données seraient communiquées, d'une part, et ceux de la personne concernée, d'autre part. Il est clair que l'utilisation des méthodes de *profiling* va influer sur cette balance dans la mesure où, comme nous l'avons dit, le *profiling* entraîne des risques supplémentaires pour la personne concernée. Ainsi si l'utilisation des techniques sophistiquées de profilage qui permet un *marketing one-to-one* ne soulève pas de problème de compatibilité, il nous apparaît cependant qu'elle soulève une question délicate de légitimité du traitement au regard de l'article 7, *h*)[66].

---

[62] *Cfr. supra,* n° 25.

[63] *Cfr. infra,* n° 31.

[64] Article 7, *f*); «(Le traitement est légitime s'…) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, paragraphe 1».

[65] À première vue, il semble difficile d'affirmer que l'une des hypothèses visées puisse se rencontrer dans un scénario marketing. Collecter des données pour des cartes de fidélité ou un profilage n'est pas nécessaire à l'exécution d'un contrat, ni au respect d'une obligation légale ni à la sauvegarde de l'intérêt vital de la personne concernée, ni à l'exécution d'une mission d'intérêt public.

[66] Comme l'indique le rapport sur les aspects juridiques et éthiques et sociaux rédigé dans le cadre du projet MIAUCE : «*it's true that this possibility [public interest] is often advanced by marketers to justify their processing : 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject...'. They argue that their interest as marketers is legitimate and that the prejudice they cause to the data subject is minor in comparison with the benefits the data subjects will get from the publicity and with their own legitimate interests. As the value behind data protection is the fundamental right to privacy, including the right not to undergo excessive pres*

Les intérêts du responsable de traitement et ceux des personnes concernées doivent être mis en balance. Telle est également l'opinion du Groupe de l'article 29 : «dans la plupart des scénarios où est utilisée la technologie RFID, le consentement des personnes sera le seul motif légal que pourront invoquer les responsables du traitement des données pour légitimer la collecte d'informations par radio-identification. Par exemple, un supermarché qui marque des cartes de fidélité devra, soit expliciter les règles contractuelles, soit obtenir le consentement de la personne pour lier l'information personnelle obtenue dans le contexte de la délivrance de la carte de fidélité avec l'information collectée au moyen de la technologie RFID»[67].

Pour conclure, la seule hypothèse qui peut légitimer le traitement de données dans le contexte de cartes de fidélité ou de *profiling* reste donc l'indubitable consentement donné par les clients.

b. La présomption de légitimité des traitements de données par le consentement

29. L'article 7 de la directive prévoit que «le traitement de données à caractère personnel peut être effectué si *a*) la personne concernée a indubitablement donné son consentement». Le texte ne précise pas si le consentement doit être écrit, ni s'il doit être explicite ou s'il suffit qu'il soit implicite. Néanmoins, le fait que le consentement doive être indubitable suggère qu'il ne peut être simplement implicite. Ainsi, les systèmes *opt-in* doivent être préférés à ceux de type *opt-out*. De plus, le consentement n'est valable que s'il est libre, c'est-à-dire donné sans contrainte qu'elle soit physique ou psychologique, spécifique à un certain traitement et éclairé, ce qui suppose que la personne ait été informée du traitement de données. Comment ce consentement peut-il être considéré comme indubitable dans le cadre de nos scénarios ?

Un consentement est valide si trois conditions sont satisfaites. D'abord il doit être libre. Il s'avère inconcevable que le professionnel exerce une quelconque pression sur les clients. Par exemple, les priver des conseils d'un vendeur s'ils refusent de prendre une carte de fidélité est une contrainte qui empêche le consentement d'être libre. Refuser une carte de fidélité ou le fait

sures and constrains in the autonomous development of one's personality, and that individualized marketing and advertising may come to be so effective that it may indeed exercise such an excessive pressure, the marketers' argument does not appear sufficient to justify in all cases such data processing. The legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed may legitimize the processing as long as these interests are not overridden by interests for fundamental rights and freedoms of the data subject. A balance must therefore be made between the data controller's and the data subject's interests. The more the processing infringes upon the data subject's fundamental liberties and freedoms, the less probable it is that the processing will appear legitimate».

[67] Groupe de travail «article 29» sur la protection des données, «Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)», 19 janvier 2005, WP 105, disponible en ligne.

d'être profilé ne devrait pas mener à un désavantage pour le client, ce qui nous l'avons vu[68], est loin d'être évident. Ensuite, le consentement doit être spécifique. Cela signifie que chaque traitement de données nécessite l'accord des personnes. Certes, nous avons vu que le *profiling*, en tant que méthode de traitement et non finalité de traitement, n'exigeait pas de consentement de la part des clients. Toutefois, le développement exponentiel de cette pratique combiné aux risques sous-jacents qu'elle engendre ont conduit à prôner la nécessité d'une réglementation spécifique. Dès lors, pour la cohérence de notre propos, bien que le consentement des individus ne soit pas (encore) requis par la loi pour le *profiling*, il semble qu'il soit opportun que le consentement ne soit donné qu'après diligente information sur son existence et les méthodes utilisées. Cette démarche volontaire de la part des responsables de traitements est à encourager. Enfin, le consentement doit être éclairé. Les commerçants doivent donner aux clients, sous une forme compréhensible, toute information sur le traitement des données afin qu'ils puissent donner leur consentement en toute connaissance de cause. De plus, le consentement doit être révocable. Les clients doivent être en possession des moyens techniques leur permettant d'effacer les données collectées sur les cartes de fidélité servant à établir leur profil. À cette première réflexion s'en ajoute une autre : le profilage permet des décisions automatisées comme nous l'avons dit. Dès lors, l'article 15 de la directive 95/46 a-t-il vocation à s'appliquer?

c. L'application de l'article 15 relatif aux décisions individuelles automatisées et le profilage

30. En vertu de l'article 15, tout individu a «le droit de ne pas être soumis à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.».

Cette disposition «*restricts a particular application of a particular type of profiling process. It does not directly restrict the creation of profiles*»[69]. Quatre conditions doivent en effet être satisfaites pour que le système de décision automatisée tombe sous l'application de l'article 15. Tout d'abord une décision doit être prise. Ensuite, celle-ci doit produire des effets juridiques significatifs sur l'individu. La décision doit résulter d'un traitement

[68] *Cfr. supra,* n° 6, le cas du scénario n° 2 qui relate les facilités obtenues grâce à la carte de fidélité comme la possibilité du passage rapide aux caisses et surtout les facilités en matière de garantie.

[69] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, n° 18.3.1, p. 319.

automatisé des données. Enfin, il faut que les données soient traitées dans le but d'évaluer certains aspects de l'individu comme son comportement, ses préférences ou besoins[70].

Qu'est-ce qu'un «effet juridique affectant de manière significative» un individu? Doit-on l'appréhender dans un sens objectif, sans prendre en compte les perceptions propres des personnes concernées? Les effets peuvent-ils être économiques? Ou alors ne sont-ils qu'économiques? *A priori*, l'envoi de publicités ciblées, les propositions de programmation qui résultent des applications de nos deux scenarios ne rentrent pas dans cette catégorie. Toutefois, les considérants 9, 10 et 23 invitent à prendre en considération les effets matériels et immatériels de ce genre de décisions. De plus, si nous considérons que l'article 15 vise la protection de l'intégrité et de la dignité des individus face à un monde de plus en plus automatisé, les perceptions propres des personnes devraient être prises en compte. Ce qui n'empêche pas de se préoccuper également d'un nombre considérable d'autres individus pour fonder la réflexion sur une base raisonnable[71]. En outre, les effets engendrés doivent être contraires aux intérêts de la personne. Il est vrai que la disposition ne mentionne pas cette restriction; mais il serait quand même étrange que l'article 15 puisse s'appliquer à une décision qui produit des effets positifs sur l'individu. Dès lors, un «effet significatif» ne peut s'entendre que d'un «effet contraire significatif»[72].

Par exemple, l'envoi d'une brochure à une liste de personnes sélectionnées sur la base d'un procédé automatisé ne peut pas être considéré comme les affectant significativement et en tout cas certainement pas de manière négative. En revanche, certains types de publicité ont la faculté de provoquer des effets contraires significatifs sur les individus, lorsque le ciblage est tel qu'il permet une manipulation de ces derniers. Par ailleurs, quand le procédé tend à opérer une discrimination déloyale entre les clients, l'effet produit peut être significatif[73]. Par exemple, si certains produits sont offerts à la vente à un prix supérieur à certains consommateurs, ou si certains d'entre eux sont empêchés d'acquérir tel type de produit contrairement à la majorité, ces pratiques sont susceptibles de provoquer des effets négatifs significatifs sur les clients. Il n'est pas incongru d'imaginer que le prix d'un produit puisse être directement proportionnel aux

---

[70] Sur tous ces points, voy. Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.,* n° 18.3.1, p. 319.

[71] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.,* n° 18.3.1, p. 322 : «the legal weight of the perception will depend on the extent to which it is regarded by a considerable number of other persons as having a reasonable basis».

[72] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.,* n° 18.3.1, p. 323.

[73] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits, op. cit.,* n° 18.3.1, p. 323. Voy. aussi J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», *op. cit*., spéc. p. 14.

habitudes et préférences du consommateur. Dans la mesure où le *profiling* ou marketing *one-to-one* permet de connaître et donc d'offrir des services personnalisés aux clients, pourquoi se priver d'une adaptation personnalisée des prix ? Avec la technique dite du *dynamic pricing*, les responsables de traitement «*can judge with greater accuracy than the consumer may know, the latter's willingness to pay for a particular product, based on past behaviour*»[74].

En définitive, la compréhension de l'article 15 doit-elle être large ? Il pourrait être possible, dans certains cas, d'arguer que le simple fait d'être jugé par une machine peut être appréhendé comme une insulte à la dignité de l'individu, ce qui conduirait à reconnaître, dans tous les cas, à une telle décision un effet significatif[75]. Ne faut-il pas dès lors considérer que «*the simple fact of individual's being subjected to automated profiling to assess certain aspects of their personality should be sufficient by itself to entitle them to be informed of this profiling and of its underlying logic, and to challenge it, at least in certain cases of automated processing deemed to be capable of making such assessments*»[76] et soumettre à une réglementation spécifique les activités de profilage même en dehors de l'article 15 de la directive ?

3. La proportionnalité des données traitées et conservées

31. L'article 6, *c*) de la directive affirme que les données collectées et utilisées doivent être «adéquates, relevantes et non excessives» au regard des finalités poursuivies. Ce principe de proportionnalité des données au regard des finalités interdit également la conservation des données au-delà de la durée nécessaire à la réalisation de la finalité. Ainsi, collecter l'adresse de la personne lors de la remise de la carte de fidélité est certes nécessaire si à cette carte est liée la possibilité de garanties sur les produits achetés ou de livraison à domicile. Elle pourrait l'être moins dans les autres cas. Réclamer des données sur la situation familiale (nombre et âge des enfants) ne semble pas indispensable par exemple. Au-delà, peut-on considérer comme proportionnée à des fins de marketing personnalisé, la collecte systématique des parcours d'un client à l'intérieur de la grande surface ? De manière plus fondamentale, le respect de la proportionnalité dans le cadre de l'utilisation de telles techniques de marketing peut-il s'accommoder de la collecte et du traitement de n'importe quelle donnée au motif que la caractéristique même de cette tech-

---

[74] «Data collection, targeting and profiling of consumers for commercial purposes in online environments», European Commission, Health and Consumers Directorate-General, Bruxelles, 5 mars 2009, spécialement p. 12.

[75] Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit*., n° 18.3.1, p. 322.

[76] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», *op. cit*., spéc. p. 34.

nique publicitaire l'exige ? Même réflexion à propos de la durée lorsque la collecte des données est justifiée par l'octroi d'une garantie donnée à l'acheteur d'un produit : peut-on considérer que la conservation de cette donnée pendant toute la durée de la garantie est nécessaire, soit le cas échéant pendant plusieurs années ?

L'application de ce principe pose plus de difficultés encore dans le cadre des opérations de profilage. Ces opérations se caractérisent en effet par la découverte de corrélations statistiques non nécessairement prédictibles. La présence et la combinaison de tels produits dans le panier de la ménagère qui, par ailleurs, fait ses courses à six heures du soir et présente des mensurations d'autant, révèle une personne sensible aux produits de pays lointains et encline à des dépenses irréfléchies. Au contraire des autres traitements où le caractère nécessaire de telle ou telle donnée peut s'analyser *a priori* par l'examen de la finalité et le lien logique qui existe entre le traitement de telle ou telle donnée et la poursuite de cette finalité, dans le cas du profilage, un tel lien de nécessité se découvre *a posteriori* par la découverte d'inférences statistiques insoupçonnées au départ. Certes, on peut exiger que les données soient codées : «tel consommateur devient M. X» mais il n'empêche que ce codage, même s'il assure une certaine sécurité du processus, en particulier s'il est opéré par une entreprise tierce, n'empêche pas que la donnée reste bien une donnée à caractère personnel.

4. Le principe de sécurité

32. La directive, en son article 17, § 1er, oblige le responsable du traitement à prendre des mesures de sécurité appropriées eu égard en particulier aux risques que pourraient présenter les défauts d'intégrité, de disponibilité et de confidentialité des données traitées et en tenant compte des risques que présente le système d'information de collecte et de traitement.

Les scénarios analysés attirent l'attention sur les particularités des systèmes d'information envisagés. Ils se basent en effet sur des terminaux qui permettent la collecte mais également constituent des bases de données ; ainsi la carte de fidélité munie d'une puce RFID émet des informations sur la situation des consommateurs mais peut également enregistrer les données nées des achats successifs des produits, le moment, le nom de la caissière, le lieu, etc.[77] On note également que les deux scénarios utilisent des infrastructures de communication, un intranet qui relie l'ensemble des puces RFID dispersées dans le magasin et l'infrastructure câblée utilisée par l'opérateur de TV interactive. La présence de ces terminaux et le transport par ces réseaux de communication multiplient les risques. Ainsi,

[77] Pour une analyse notamment en matière de sécurité, se reporter à l'article : «Les cartes sans contact : d'une comparaison de trois utilisations en billettique à la recommandation européenne en matière de RFID», par Denis Darquennes, sous la supervision de Yves Poullet, *R.D.T.I.*, n° 37, 2009.

on peut imaginer la lecture à distance du contenu de la puce RFID du consommateur, l'interception des messages en provenance de la TV interactive du spectateur. La sécurité des données prend donc dans ces scénarios une nouvelle dimension et oblige à étendre à de nouveaux acteurs. Ainsi, celui qui conçoit ou produit le terminal se doit de sécuriser l'accès à la puce RFID, de crypter automatiquement les communications en provenance de celles-ci, etc. Celui qui conçoit le système d'informations qui permet la collecte et la transmission des données doit également veiller à ce que des interceptions de communication ne soient pas possibles et que des logiciels espions ne puissent être introduits dans le terminal de la personne concernée. Ces obligations nouvelles apparaissent clairement dans la recommandation européenne et l'opinion du Groupe de l'article 29[78].

Chapitre 3. Les technologies intelligentes à travers le prisme de la législation relative aux pratiques commerciales déloyales

33. Le *marketing*, que révèle l'étude des deux scénarios, n'est plus un marketing de masse, mais un *marketing* personnalisé, autrement dit un marketing *one-to-one*[79]. La tendance a évolué dans le sens d'une «prise de conscience de la valeur individuelle d'un client»[80]. Le *leitmotiv* n'est plus de suivre les besoins du consommateur mais de les devancer. De plus, ce dernier a besoin de connivence pour être fidèle. La collecte de données se rapportant à sa consommation s'avère alors indispensable pour «reconstituer le plus fidèlement possible la relation individuelle née chez le commerçant de proximité»[81]. L'heure n'est plus à l'établissement d'«artéfacts» statistiques qui ne correspondent à aucun individu en particulier, mais à la volonté de retrouver l'homme derrière ces artefacts[82]. En effet, «le pari du *One-to-one* est de passer de l'abstraction du consommateur à la réalité de la personne»[83]. Et c'est bien là que réside le problème. La connaissance de l'individu que peuvent acquérir les professionnels du *marketing* apparaît désormais sans limite puisqu'ils réussissent même à déceler et analyser les émotions au moment du visionnage d'un film. C'est ce que montre le scénario de télévision interactive. L'objectif consiste à approcher au plus près le ressenti de l'humain pour pouvoir lui proposer ensuite des produits ou des services adaptés. La manipulation n'est peut-être plus très loin.

---

[78] Déjà citées et commentées, *supra,* n° 20.

[79] L'expression a été trouvée par M. ROGERS et D. PEPPERS, *Le One-to-One – Valorisez votre capital-client*, éd. d'Organisation, 1998.

[80] J.-L. GIROT, «Pourquoi l'entreprise doit-elle développer sa connaissance des clients?», in *Le harcèlement numérique*, Institut Présage, Dalloz, 2005, spéc. pp. 51-73, spéc. p. 55.

[81] *Ibidem.*

[82] Ph. LEMOINE, «Commerce électronique, marketing et liberté», in *La protection de la vie privée dans la société de l'information*, Pierre Tabatoni (sous la dir.), tome 2, PUF, 2002, pp. 9-23, spéc. pp. 15 et s.

[83] Pensée de PEPPER et ROGGERS résumée par E. BARCHECHATH, «Une lecture critique du *One-to-One*», in *Commerce électronique, marketing et libertés*, Cahier Laser, n° 2, Laser, 1999, pp. 87 à 104, spéc. p. 98.

L'approche de ces technologies intelligentes sous l'angle des règles qui régissent les pratiques *marketing* mérite quelques considérations.

34. Le texte de référence en la matière est la directive 2005/29/CE du Parlement et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur[84]. Il s'agit d'une «directive-cadre qui couvre l'ensemble des pratiques déloyales visant les consommateurs»[85]. La directive 2005/29 opère une harmonisation totale – contrairement aux directives précédentes qui n'exigeaient qu'une harmonisation minimale – en ce sens que la protection des consommateurs à l'échelle nationale ne pourra être ni inférieure ni supérieure à celle proposée par la directive[86]. La publicité et le *marketing* ne font pas l'objet d'un traitement spécifique par la directive. Celle-ci situe sur le même plan ce type d'actes et toute autre démarche en lien direct avec la promotion ou la vente de produits aux consommateurs[87]. Les actions *marketing* à destination des consommateurs entrent donc dans le champ d'application de la directive. La pratique commerciale bénéficie d'une approche généreuse en ce qu'elle est définie comme «toute action, omission, conduite, démarche ou communication commerciale, y compris la publicité et le *marketing*, de la part d'un professionnel, en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs[88]»[89]. Une telle pratique sera déloyale si «*it deemed to be unacceptable with regards to the con-*

[84] Cette directive modifie la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil.

[85] J. Calais-Auloy et F. Steinmetz, *Droit de la consommation*, Dalloz, Précis Droit privé, 7e éd., 2006, n° 80-2, pp. 89-90.

[86] J. Calais-Auloy et F. Steinmetz, *Droit de la consommation*, *op. cit*., n° 80-2, p. 90.

[87] Le considérant n° 7 précise que «la présente directive porte sur les pratiques commerciales qui visent directement à influencer les décisions commerciales des consommateurs à l'égard des produits».

[88] *Cfr*. considérant n° 7 : «La présente directive porte sur les pratiques commerciales qui visent directement à influencer les décisions commerciales des consommateurs à l'égard de produits. Elle ne s'applique pas aux pratiques commerciales mises en œuvre principalement à d'autres fins, parmi lesquelles figurent par exemple les communications commerciales destinées aux investisseurs, telles que les rapports annuels et la documentation promotionnelle des entreprises. Elle ne s'applique pas aux prescriptions légales concernant le bon goût et la bienséance, qui sont très variables d'un État membre à l'autre. Des pratiques commerciales telles que, par exemple, la sollicitation commerciale dans la rue peuvent être malvenues dans certains États membres pour des raisons culturelles».

[89] Article 2, *d*) de la directive 2005/29. Comparer avec l'article 2, *f*) de la directive 2000/31 du 8 juin 2000 sur le commerce électronique, qui définit la «communication commerciale» comme «toute forme de communication destinée à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation ou d'une personne ayant une activité commerciale, industrielle, artisanale ou exerçant une profession réglementée. Ne constituent pas en tant que telles des communications commerciales : – les informations permettant l'accès direct à l'activité de l'entreprise, de l'organisation ou de la personne, notamment un nom de domaine ou une adresse de courrier électronique; – les communications relatives aux biens, aux services ou à l'image de l'entreprise, de l'organisation ou de la personne élaborées d'une manière indépendante, en particulier lorsqu'elles sont fournies sans contrepartie financière».

sumer, according to specified criteria»[90]. Le considérant n° 8 met l'accent sur la protection des intérêts économiques des consommateurs contre les pratiques commerciales déloyales des entreprises à leur égard, à l'exclusion d'autres intérêts comme la santé ou la sécurité[91].

35. Les scénarios *marketing* envisagés seront étudiés sous l'angle de la législation protectrice des consommateurs (A). Cette démarche, centrée sur la législation protectrice des consommateurs, ne sera pas exclusive d'une approche sous l'angle des dispositions relatives à la protection des données personnelles. Les deux législations peuvent, certes, être étudiées en parallèle mais il semble qu'il soit possible de proposer une réflexion davantage «intégrative», dans le sens où une infraction à la législation relative aux données personnelles pourrait constituer une pratique commerciale déloyale au sens de la directive 2005/29. La violation de la législation sur les données personnelles par des entreprises pourrait en elle-même s'apparenter à une pratique commerciale déloyale envers les consommateurs (B). L'approche semble intéressante, d'autant plus que de tels arguments ont déjà été avancés par des entreprises à l'encontre d'autres entreprises concurrentes. Finalement, il conviendra d'appréhender les moyens d'action dont disposent les consommateurs lorsqu'ils sont victimes de pratiques commerciales déloyales de la part des entreprises, et d'envisager ce qu'il en advient lorsque de telles pratiques consistent en une violation de la législation sur les données personnelles (C).

A. Les pratiques commerciales déloyales au sens de la directive 2005/29

36. Pour savoir si une pratique commerciale tombe sous le coup de la directive 2005/29, il convient de vérifier tout d'abord si elle fait partie de la liste noire édictée par la directive (1). Si tel n'est pas le cas, il faut alors s'interroger sur le fait de savoir si elle rentre dans la définition d'une pratique commerciale agressive (2) ou d'une pratique commerciale trompeuse[92]. Si la pratique commerciale ne correspond pas à l'une ou l'autre de ces définitions, la réflexion s'orientera vers l'article 5 qui proscrit les pratiques commerciales déloyales qui ne seraient ni agressives ni trompeuses (3).

[90] «The Unfair Commercial Practices Directive, Questions and Answers», European Commission, Press release, 12 décembre, 2007, disponible en ligne.

[91] «La directive relative aux pratiques commerciales déloyales», Direction générale Santé et protection des consommateurs, Commission européenne, 2006, spéc. p. 18.

[92] Nous n'aborderons pas ici les pratiques commerciales trompeuses (articles 6 et s. de la directive 2005/29).

1. Liste noire des pratiques commerciales déloyales en toutes circonstances

37. La directive 2005/29 a établi une liste noire des pratiques déloyales en toutes circonstances[93] (annexe 1)[94] sans se référer au test du consommateur moyen[95]. Une évaluation au cas par cas n'est pas requise. Sont incluses par exemple dans cette liste, parmi les pratiques commerciales agressives, le fait de :

«24) Donner au consommateur l'impression qu'il ne pourra quitter les lieux avant qu'un contrat n'ait été conclu.

25) Effectuer des visites personnelles au domicile du consommateur, en ignorant sa demande de voir le professionnel quitter les lieux ou de ne pas y revenir, sauf si et dans la mesure où la législation nationale l'autorise pour assurer l'exécution d'une obligation contractuelle[96].

26) Se livrer à des sollicitations répétées et non souhaitées par téléphone, télécopieur, courrier électronique ou tout autre outil de communication à distance, sauf si et dans la mesure où la législation nationale l'autorise pour assurer l'exécution d'une obligation contractuelle. Cette disposition s'entend sans préjudice de l'article 10 de la directive 97/7/CE, et des directives 95/46/CE (1) et 2002/58/CE».

On pourrait prendre l'exemple de *Doubleclick* (rachetée par Google) dont l'activité est de gérer les espaces publicitaires de nombre d'entreprises actives sur l'Internet. Si *Doubleclick* envoie de manière répétée des bannières publicitaires à des internautes, elle pourrait être concernée par l'annexe 1 de la directive. En effet, cette pratique pourrait faire partie de la liste noire édictée par la directive et être interdite en toutes circonstances.

---

[93] En Belgique, la directive 2005/29 a été transposée par la loi du 5 juin 2007 qui a modifié la loi du 14 juillet 1991 sur les pratiques du commerce et l'information et la protection du consommateur. Cette loi a été abrogée et remplacée par la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur (*M.B.*, 12 avril 2010, p. 20803) (voy. à cet égard la contribution de E. BALATE et M. GOUVERNEUR dans ce numéro). Les pratiques commerciales déloyales en toutes circonstances sont listées aux articles 91 et 94 de la loi du 6 avril 2010. Le contexte européen de la recherche nous a amené à privilégier la référence aux textes européens et non à la législation nationale qui les transpose.

[94] Se reporter au considérant n° 17 de la directive 2005/29.

[95] *Cfr. infra.*

[96] On pourrait imaginer que l'ordinateur personnel puisse être considéré comme le domicile virtuel du consommateur…

2. *Interdiction des pratiques commerciales agressives*

38. L'article 8 de la directive[97] dispose qu'«Une pratique commerciale est réputée agressive si, dans son contexte factuel, compte tenu de toutes ses caractéristiques et des circonstances, *elle altère ou est susceptible d'altérer de manière significative, du fait du harcèlement, de la contrainte, y compris le recours à la force physique, ou d'une influence injustifiée, la liberté de choix ou de conduite du consommateur*[98] *moyen*[99] à l'égard d'un produit, et, par conséquent, l'amène ou est susceptible de l'amener à prendre une décision commerciale qu'il n'aurait pas prise autrement».

Comme la Commission européenne l'explique, «*a practice is considered aggressive if the average consumer's freedom of choice or conduct is significantly impaired*»[100]. La question est la suivante : est-ce qu'une pratique commerciale influence à ce point un consommateur qu'il est empêché de prendre une décision en toute connaissance de cause?

39. En vue de déterminer le caractère loyal d'une telle pratique, la directive donne quelques indices. L'article 9[101] appréhende l'utilisation du harcèlement, de la contrainte ou d'une influence injustifiée en disposant que : «Afin de déterminer si une pratique commerciale recourt au harcèlement, à la contrainte, y compris la force physique, ou à une influence injustifiée, les éléments suivants sont pris en considération :

'a) le moment et l'endroit où la pratique est mise en œuvre, sa nature et sa persistance;

b) le recours à la menace physique ou verbale;

---

[97] *Cfr.* article 91 de la loi du 6 avril 2010.

[98] La définition du consommateur est donnée par l'article 2, *a*) de la directive : «toute personne physique qui, pour les pratiques commerciales relevant de la présente directive, agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale». Un consommateur ne peut donc pas être une personne morale.

[99] Le critère d'évaluation pris par la directive est le *consommateur moyen*, «qui est normalement informé et raisonnablement attentif et avisé, compte tenu des facteurs sociaux, culturels et linguistiques, selon l'interprétation donnée par la Cour de justice» (considérant n° 18 de la directive). Ce considérant précise que «La notion de consommateur moyen n'est pas une notion statistique. Les juridictions et les autorités nationales devront s'en remettre à leur propre faculté de jugement, en tenant compte de la jurisprudence de la Cour de justice, pour déterminer la réaction typique du consommateur moyen dans un cas donné». La directive prévoit aussi «des dispositions visant à empêcher l'exploitation de consommateurs dont les caractéristiques les rendent particulièrement vulnérables aux pratiques commerciales déloyales», comme les enfants par exemple. Dans cette hypothèse, «il est souhaitable que son incidence soit évaluée du point de vue du membre moyen de ce groupe» (considérant n° 18). «Par conséquent, il convient d'inscrire sur la liste des pratiques réputées déloyales en toutes circonstances une disposition qui, sans édicter une interdiction totale de la publicité à destination des enfants, protège ces derniers d'incitations directes à acheter». C'est chose faite au point n° 28 de la liste noire.

[100] «The unfair commercial practices Directive, Questions and Answers», précit., spéc. p. 2.

[101] *Cfr.* article 93 de la loi belge du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur.

c) l'exploitation en connaissance de cause par le professionnel de tout malheur ou circonstance particulière d'une gravité propre à altérer le jugement du consommateur, dans le but d'influencer la décision du consommateur à l'égard du produit;

d) tout obstacle non contractuel important ou disproportionné imposé par le professionnel lorsque le consommateur souhaite faire valoir ses droits contractuels, et notamment celui de mettre fin au contrat ou de changer de produit ou de fournisseur;

e) toute menace d'action alors que cette action n'est pas légalement possible'».

Le considérant n° 16 insiste sur le fait que «Les dispositions sur les pratiques commerciales agressives devraient couvrir les pratiques qui altèrent de manière significative la liberté de choix du consommateur. Il s'agit de pratiques incluant le harcèlement, la contrainte, y compris le recours à la force physique, ou une influence injustifiée».

Dans les scénarios présentés, on relève certaines pratiques commerciales dont la nature et la persistance pourraient permettre de les faire rentrer dans le cadre de l'hypothèse *a*) de l'article 9 et donc dans la catégorie des pratiques agressives. Par exemple, si les commerçants rappellent à leurs clients, chaque fois qu'ils se rendent dans les magasins, que ce serait une bonne idée d'acheter telle ou telle chemise car ils ont acheté tel ou tel pantalon, et ce, tant qu'ils ne l'ont pas achetée, cette attitude ne pourrait-elle pas être constitutive d'une pratique commerciale agressive déloyale? De même, il s'avère légitime de se demander si le fait que les professionnels utilisent la passion dévorante d'un consommateur pour les jeux vidéo pour influencer ses décisions d'achat dans ce domaine pourrait correspondre à l'hypothèse *c*) de l'article 9. On pourrait également ajouter que l'activité menée par *Doubleclick*[102], si elle s'avérait ne pas faire partie de la liste noire des pratiques commerciales déloyales en toute circonstance édictée par la directive, pourrait peut-être s'apparenter à du harcèlement au sens de l'article 9.

40. En outre, la directive définit «l'influence injustifiée» (art. 6, *j*)) comme «l'utilisation d'une position de force vis-à-vis du consommateur de manière à faire pression sur celui-ci, même sans avoir recours à la force physique ou menacer de le faire, de telle manière que son aptitude à prendre une décision en connaissance de cause soit limitée de manière significative».

Dans les scénarios *marketing*, le commerçant risque d'exploiter sa position dominante vis-à-vis des consommateurs en leur offrant tel type de produits et pas les autres. S'ils sont significativement affectés, la pratique commerciale tombera dans le champ d'application de l'article. L'enjeu est de savoir si le comportement du commerçant limite significativement l'aptitude du consommateur à prendre une décision éclairée. La frontière

[102] *Cfr. supra,* n° 37.

n'est pas si évidente car les actions marketing ont justement pour objectif d'emmener les consommateurs vers ce type de produits et non cet autre type.

3. Interdiction générale des pratiques commerciales déloyales

41. L'article 5[103] interdit de manière générale les pratiques commerciales déloyales. En effet, de nouvelles pratiques peuvent émerger, qui ne seraient ni trompeuses ni agressives, mais qui seraient malgré tout déloyales. Il dispose que : «1. Les pratiques commerciales déloyales sont interdites. 2. Une pratique commerciale est déloyale si :

'a) elle est contraire aux exigences de la diligence professionnelle,

et

b) elle altère ou est susceptible d'altérer de manière substantielle le comportement économique, par rapport au produit, du consommateur moyen qu'elle touche ou auquel elle s'adresse, ou du membre moyen du groupe lorsqu'une pratique commerciale est ciblée vers un groupe particulier de consommateurs'».

L'article définit un «standard de comportement»[104]. Les deux conditions exigées sont cumulatives. La première condition est «objective»[105]. L'article 2, *h*) définit la «diligence professionnelle» comme «le niveau de compétence spécialisée et de soins dont le professionnel est raisonnablement censé faire preuve vis-à-vis du consommateur, conformément aux pratiques de marché honnêtes et/ou au principe général de bonne foi dans son domaine d'activité». Le professionnel[106] doit non seulement adopter un comportement respectueux des usages honnêtes, mais il doit également être compétent et consciencieux. Le juge devra rechercher si «une norme équivalant à un comportement de référence, tel celui du bon père de famille, existe»[107]. Alors la notion de «diligence professionnelle» s'approcherait de la notion de faute[108]. Pour être sanctionné, le commerçant devra commettre une faute provoquant un dommage pour le consommateur, avec un

[103] *Cfr.* article 84 de la loi belge du 6 avril 2010.

[104] Y. De Cordt, C. Delforge, Th. Leonard et Y. Poullet, *Manuel de droit commercial*, Anthemis, Académie Universitaire Louvain, 2009, n° 890, p. 499.

[105] Y. De Cordt, C. Delforge, Th. Leonard et Y. Poullet, *Manuel de droit commercial*, *op. cit*., n° 890, p. 499.

[106] La définition du professionnel est donnée par l'article 2, *b*) de la directive : «toute personne physique ou morale qui, pour les pratiques commerciales relevant de la présente directive, agit à des fins qui entrent dans le cadre de son activité, commerciale, industrielle, artisanale ou libérale, et toute personne agissant au nom ou pour le compte d'un professionnel».

[107] I. Ferrant, *Les pratiques du commerce (depuis les modifications législatives de 2007)*, Kluwer, Pratique du droit, tome 34, 2008, n° 103, p. 51.

[108] L. De Brouwer, «La directive 2005/29/CE du 11 mai 2005 relative aux pratiques commerciales déloyales», *R.D.C.,* 2005/7, septembre 2005, pp. 793 et s., spéc. p. 795.

lien de causalité entre ces deux éléments. Le dommage peut être effectif ou simplement potentiel. Seul l'intérêt économique est pris en compte.

Concernant la seconde condition, «subjective»[109], posée par l'article 5.2, il faut tout d'abord préciser qu'est simplement requise la possibilité d'une altération substantielle du comportement économique. Cette altération n'a pas à être effective mais juste potentielle pour que l'article 5 soit applicable. Ensuite, l'«altération substantielle du comportement économique des consommateurs» doit être comprise, selon l'article 2, *e*), comme «l'utilisation d'une pratique commerciale compromettant sensiblement l'aptitude du consommateur à prendre une décision en connaissance de cause et l'amenant par conséquent à prendre une décision commerciale qu'il n'aurait pas prise autrement». L'altération substantielle du comportement économique est donc en jeu quand une pratique commerciale menace considérablement l'aptitude du consommateur à prendre une décision en connaissance de cause. Le consommateur est donc amené à prendre une décision qu'il n'aurait pas prise autrement. L'influence de la pratique commerciale sur le comportement du consommateur doit être déterminante.

À cet égard, les possibilités qu'offre le *marketing one-to-one* sont tellement infinies qu'elles en deviennent inquiétantes. Les risques de dérive ne sont pas négligeables. L'exploitation abusive des caractéristiques psychologiques d'un individu pourrait tomber sous le coup de l'article 5. Si le professionnel utilise à outrance la sensibilité d'un consommateur sur un sujet particulier, par exemple la défense des animaux sauvages, afin de l'inciter à prendre une décision qu'il n'aurait pas prise autrement, comme verser des sommes d'argent colossales pour un service en relation avec ce sujet, il pourrait être attaquable sur le fondement de l'article 5[110].

42. Les articles 5 et 2, *e*) sont formulés en des termes généraux afin de pouvoir s'appliquer à toute pratique commerciale déloyale, même non trompeuse ou non agressive. Néanmoins, il semble que certaines pratiques marketing ne tombent pas sous le coup de la directive. Le considérant n° 6 *in fine* estime que : «La présente directive n'affecte pas (…) les pratiques publicitaires et commerciales admises, comme le placement légitime de produits, la différenciation des marques ou les incitations à l'achat, qui peuvent légitimement influencer la perception d'un produit par le consommateur ainsi que son comportement, sans altérer son aptitude à prendre une décision en connaissance de cause». Les exemples fournis par la directive ne sont pas limitatifs. D'autres pratiques commerciales qui se contenteraient d'influencer le comportement d'achat du consommateur mais sans lui retirer son aptitude à prendre une décision éclairée pourraient être admises.

---

[109] Y. De Cordt, C. Delforge, Th. Leonard et Y. Poullet, *Manuel de droit commercial*, *op. cit.*, n° 890, p. 499.

[110] Et peut-être aussi sur le fondement de l'article 8 relatif aux pratiques commerciales agressives. *Cfr. supra,* n^os^ 38 et s.

43. L'enjeu est de réussir à distinguer les pratiques commerciales qui *affectent légitimement* les perceptions des produits par les consommateurs et les influencent sans menacer leur aptitude à prendre des décisions informées, et les pratiques commerciales qui *affectent considérablement* leur aptitude à prendre de telles décisions. La frontière n'est pas si claire. Et qui plus est, elle ne semble pas immuable. En effet, le curseur risque de se déplacer au profit du second type de pratiques si elles finissent par devenir la norme en matière de *marketing*, c'est-à-dire le jour où les consommateurs trouveront cela tout à fait légitime. En somme, des pratiques *marketing* qui, à l'heure actuelle, sont considérées comme affectant considérablement l'aptitude des consommateurs à prendre des décisions éclairées, pourraient, dans un futur plus ou moins proche, devenir légitimes car acceptées comme étant la nouvelle norme. Il est alors permis d'espérer que les consommateurs auront appris, de leur côté, à se départir de leur influence…

B. La violation de la législation de protection des données personnelles comme pratique commerciale déloyale

44. Se pourrait-il que, dans le cadre des scénarios marketing, une infraction à la législation de protection des données personnelles constitue une pratique commerciale déloyale au sens de la directive 2005/29 ? En somme, le fait de ne pas respecter les règles relatives à la protection des données personnelles pourrait-il être une pratique commerciale agressive ou déloyale dans un sens plus large ? En d'autres termes, la violation de la législation vie privée pourrait-elle être utilisée dans des procédures intentées par les consommateurs contre les commerçants ? Il se trouve que la législation sur les données personnelles a déjà été invoquée dans des procédures opposant des entreprises en situation de concurrence pour dénoncer des pratiques contraires aux usages honnêtes du commerce (1). À notre connaissance, le recours à cette législation dans le cadre de litiges entre consommateurs et entreprises pour faire constater une pratique commerciale déloyale n'est, pour l'instant, pas fréquent mais pourrait se révéler efficace (2).

1. Dans des litiges entre entreprises

45. La législation sur les données personnelles a souvent été invoquée par des entreprises en situation de concurrence pour demander au juge de constater un acte contraire aux usages honnêtes du commerce. La violation d'une telle disposition – par exemple, la cession des données à caractère personnel sans le consentement des personnes concernées, un traitement de données incompatible avec les objectifs originels… – entraînerait une concurrence illégitime dans le monde des affaires. C'est ce qu'ont décidé plusieurs juridictions. Dans le cadre d'une action en cessation, les juges de la cour d'appel d'Anvers[111] ont condamné une

[111] Anvers, 3 mai 1999, *A.J.T.,* 1999/2000, p. 437, note C. De Vos ; Y. Poullet, «Chronique de jurisprudence 'Vie privée'», in *Les dossiers du Journal des tribunaux*, Larcier, 2003, spéc. n° 151. Voy. également l'affaire

banque pour avoir utilisé à des fins publicitaires pour l'offre de produits d'assurance des données relatives à sa clientèle obtenues à partir de l'analyse d'ordres de paiement. La cour a mis en cause la légitimité du traitement opéré par la banque en ce que l'utilisation «*marketing*» par le banquier de données transmises par le client aux fins de virement, excédait les prévisions raisonnables du client de la banque. Seul le consentement de la personne concernée semble dès lors pouvoir être une cause légitime d'une utilisation marketing par le banquier des données relatives à la réalisation d'un virement. Récemment, la cour d'appel de Bruxelles a estimé que le fait que la banque utilise des données à caractère personnel collectées lors d'ordres de paiement donnés par les clients constitue une violation des usages honnêtes en matière commerciale vis-à-vis de ses concurrents[112]. Un manquement à une disposition légale – en l'occurrence à la législation de protection des données à caractère personnel – à l'occasion de l'exercice d'un commerce peut caractériser une violation aux usages honnêtes en matière commerciale. Il est même arrivé que le juge vérifie incidemment, lors d'une action en cessation, que le responsable a bien rempli son obligation de déclaration des traitements automatisés[113].

2. Dans des litiges entre consommateurs et entreprises

46. La démarche opérée par les sociétés entre elles pourrait être entreprise par les consommateurs à leur égard. Dans la mesure où une infraction à la législation de protection des données à caractère personnel répondrait à la définition d'une pratique commerciale déloyale au sens de la directive 2005/29, il n'existe, *a priori*, aucun obstacle à ce que le consommateur invoque, à l'encontre du commerçant, cette infraction dans le cadre d'une action en cessation[114]. C'est d'ailleurs ce qui s'est passé dans une affaire opposant l'association de consommateurs Test-Achats à la banque Fortis. L'association de consommateurs a reproché à la société de conclure avec les clients des contrats d'hospitalisation individuels en se servant de documents contractuels dans lesquels se trouvent plusieurs

FEBIAC, Comm. Bruxelles (prés.), 12 juillet 1996, *D.A. O.R.,* 39/1996, p. 73, note G. Ballon; *D.C.C.R.,* 1996, p. 351, note F. Domont-Naert; *R.W.*, 1996-1997, p. 855, note J. Meeusen; Y. Poullet, «Chronique de jurisprudence 'Vie privée'», in *Les dossiers du Journal des tribunaux*, Larcier, 2003, spéc. n° 153. Et l'affaire *KBC*, Comm. Gand, 23 avril 1997, *T.G.R.,* 1997, p. 174; Y. Poullet, «Chronique de jurisprudence 'Vie privée'», in *Les dossiers du Journal des tribunaux*, Larcier, 2003, spéc. n° 152.

[112] Bruxelles, 15 février 2005, *Prat. comm. & conc . – Annuaire 2005*, H. De Bauw (éd.), Kluwer, 2006, pp. 495 et s.

[113] Aff. *Belgacom,* Comm. Bruxelles (prés.), 19 juillet 1995, *J.T.,* 1995, p. 188; Y. Poullet, «Chronique de jurisprudence 'Vie privée'», in *Les dossiers du Journal des tribunaux*, Larcier, 2003, spéc. n° 165.

[114] Comp. aux États-Unis, la Federal Trade Commission (FTC) qui fait appliquer la loi sur les pratiques commerciales déloyales et trompeuses et qui a le pouvoir de déclencher des actions contre les entreprises qui se livrent à de telles pratiques (y compris celles qui ne respectent pas leur *privacy policy*). Sur le sujet, voy. N.J. King, «When mobile phones are RFID-equiped – Finding EU-US solutions to protect consumer privacy and facilitate mobile commerce», *Michigan Telecommunications and Technology Law Review*, vol. 15, Issue 1, Fall 2008, spéc. pp. 157, 166, 191 et 195.

infractions à la loi vie privée. D'une part, le responsable de traitement doit prendre toutes les mesures techniques et organisationnelles pour garantir la confidentialité des données traitées. Dès lors, le fait de fusionner le questionnaire médical avec la proposition d'assurance sans mettre en place aucune mesure de protection de la confidentialité des données médicales enfreint la loi. D'autre part, le fait que le questionnaire médical se soit retrouvé entre les mains de l'assureur viole la règle selon laquelle les données à caractère personnel médicales doivent être traitées sous la responsabilité d'un professionnel de santé. Ces infractions à la législation de protection des données personnelles constituent des pratiques contraires aux usages honnêtes en matière commerciale. C'est en ces termes que la cour d'appel de Bruxelles, le 16 juin 2003, s'est prononcée : «est contraire aux usages honnêtes en matière commerciale la pratique qui consiste à fusionner en un seul document la proposition d'assurance et le questionnaire médical»[115].

47. Dès lors, on peut envisager qu'une association de consommateurs intente d'autres actions en cessation contre des entreprises sur le fondement d'une pratique commerciale déloyale constituée par une infraction à la législation sur les données personnelles, dans bien d'autres domaines et notamment le marketing *one-to-one*. La violation de ces dispositions devra soit rentrer dans le champ d'application de l'article 8 de la directive 2005/29 consacré aux pratiques commerciales agressives[116], soit correspondre à la définition de l'article 5 dédié aux pratiques commerciales déloyales qui ne seraient ni trompeuses ni agressives.

C. Les moyens d'action

48. Dans l'hypothèse où une infraction à la législation protectrice des données personnelles pourrait s'analyser en une pratique commerciale déloyale, le consommateur ne pourrait-il pas exercer une action en cessation contre l'entreprise sur ce motif (3.)? Avant de répondre, il convient d'appréhender les actions envisageables pour faire sanctionner une entreprise qui se serait livrée à une pratique commerciale déloyale (1.), avant d'examiner celles qui ont pour objectif de faire constater une violation des dispositions protectrices des données personnelles (2.).

1. Dans l'hypothèse d'une pratique commerciale déloyale

49. La directive 2005/29 indique simplement que les législations nationales doivent prévoir des voies de recours pour engager une action en justice contre les pratiques commerciales déloyales[117], étant précisé que les sanctions doivent être effectives, proportionnées et dis-

[115] Comm. Bruxelles (cess.), 16 juin 2003, *D.C.C.R.,* n° 163, 2004, p. 104.
[116] …ou trompeuses.
[117] *Cfr.* le considérant n° 21.

suasives[118]. En la matière, nous nous concentrerons sur la législation belge. En Belgique, la directive a été transposée par la loi de 2007, qui a donc modifié celle du 14 juillet 1991. Cette loi du 14 juillet 1991 fut abrogée et remplacée par la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur. Le chapitre 4 est intitulé «Pratiques interdites»; la section 1 «Pratiques commerciales déloyales à l'égard des consommateurs» reprend l'essentiel de la directive et de la loi du 14 juillet 1991. Les consommateurs belges disposent de l'action en cessation qui est visée au chapitre 6 de la nouvelle loi. L'article 2 de la loi du 6 avril 2010 concernant le règlement de certaines procédures prévoit qu'une action en cessation peut être déclenchée pour les infractions visées par la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur[119]. Toute pratique commerciale déloyale exercée à l'égard des consommateurs peut donc constituer le fondement d'une telle action. L'action en cessation est introduite contre l'auteur de l'acte litigieux. C'est le professionnel au sens de la directive; l'entreprise au sens de la loi belge. Conformément à l'article 113 de la loi belge du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, l'action en cessation est ouverte notamment aux «intéressés», et à «une association ayant pour objet la défense des intérêts des consommateurs et jouissant de la personnalité civile, pour autant qu'elle soit représentée au Conseil de la consommation ou qu'elle soit agréée par le ministre, suivant des critères déterminés par arrêté royal délibéré en Conseil des ministres, sauf lorsque la demande porte sur un acte visé à l'article 95. (…) Par dérogation aux dispositions des articles 17 et 18 du Code judiciaire, les associations et groupements [professionnel ou interprofessionnel ayant la personnalité civile] visés à l'alinéa premier, 3° et 4°, peuvent agir en justice pour la défense de leurs intérêts collectifs statutairement définis». L'avantage de cette action en cessation est qu'elle peut être déclenchée non seulement par les consommateurs, mais également par les associations qui les représentent et les défendent. Dans la pratique, il semble que l'action en cessation soit rarement exercée par les individus eux-mêmes[120]. Les associations de consommateurs peuvent agir sous réserve de satisfaire trois conditions[121] : avoir la personnalité civile, avoir pour objet la défense des intérêts des consommateurs, être représentées au Conseil de la consommation ou à, défaut, être agréées par le ministre des Affaires économiques en fonction des critères déterminés par arrêté royal délibéré en Conseil des ministres. Cette possibilité d'action pour la défense d'intérêts

[118] *Cfr*. le considérant n° 22 et l'article 13.

[119] Le consommateur dispose également de l'action en responsabilité civile. Il convient également de préciser que, dans le cadre d'une action en cessation, lorsque le juge émet un ordre de cessation d'un acte illicite, il est alors possible de demander réparation du préjudice subi devant le juge du fond qui sera tenu par l'autorité de la chose jugée.

[120] A. Tallon (sur la base du texte initial d'A. De Caluwé), «La procédure», sous la dir. de A. De Caluwé, Larcier, *Les pratiques du commerce*, 2008, n° 64, p. 75.

[121] I. Ferrant, *Les pratiques du commerce (depuis les modifications législatives de 2007)*, *op. cit*., n° 428, p. 175.

collectifs «facilite l'action en cessation dont l'unique objectif sera de rétablir un ordre social et un équilibre concurrentiel approximativement général»[122].

Cette action collective n'a rien à voir avec la *class action* du système américain. Il s'agit d'une action en indemnisation à grande échelle par laquelle un certain nombre de consommateurs attaque un producteur déterminé. La transaction globale permet alors l'indemnisation des acteurs à l'action mais aussi celle de ceux qui n'ont pas agi. La demande unique a donc un effet collectif. Une telle procédure n'exige pas l'identification préalable des consommateurs lésés. En Belgique, la Commission créée par le ministre des Affaires économiques appelait de ses vœux la création d'une procédure de type *class action* en faveur des consommateurs, sous réserve toutefois que l'exercice soit réservé aux associations de consommateurs[123]. Sans doute, un effet pervers lié à la création d'une telle action serait d'enrichir les intermédiaires, qu'ils soient avocats ou associations. Certains auteurs se demandent s'il faut abandonner pour autant toute idée de *class action* et suggèrent de réfléchir à une forme spécifique «tant il est vrai que la production de masse de plus en plus importante dans notre monde qu'on se plaît à appeler globalisé peut entraîner dans le chef des consommateurs des préjudices, peut-être minimes, mais dont la multiplication nuit à l'intérêt général, au seul profit de quelques-uns»[124].

50. De surcroît, une action au pénal serait également envisageable[125]. Conformément à l'article 124 de la loi belge du 6 avril 2010, sont punis d'une amende de 250 à 10 000 euros, «ceux qui commettent une infraction aux dispositions des articles 86, 91 et 94, relatifs aux pratiques commerciales déloyales à l'égard des consommateurs, à l'exception des articles 91, 12°, 14°, 16° et 17°, et 94, 1°, 2° et 8°». Sont donc condamnables pénalement les pratiques commerciales déloyales qui ne seraient ni trompeuses ni agressives, les pratiques commerciales déloyales trompeuses ou agressives et les pratiques commerciales agressives et trompeuses édictées dans la liste noire excepté certaines hypothèses visées spécifiquement par l'article 124. Mais la procédure pénale s'arrête généralement au stade de la procédure administrative qui donne lieu au versement d'amendes transactionnelles fixées par l'A.R. du 27 avril 1993, entre 20 et 25 000 euros[126].

---

[122] A. Tallon (sur la base du texte initial d'A. De Caluwé), «La procédure», *op. cit.*, n° 78, p. 95.

[123] Th. Bourgoignie, «Propositions pour une loi générale sur la protection des consommateurs en Belgique. En marge de la publication du rapport de la Commission d'étude pour la Réforme du Droit de la Consommation (CERDC)», in *Le droit des affaires en évolution, L'entreprise et son client : un partenariat constructif*, 8e Journée du juriste d'entreprise, Bruylant, Bruxelles, 1997, pp. 3-29, spéc. p. 25.

[124] A. Tallon (sur la base du texte initial d'A. De Caluwé), «La procédure», *op. cit.*, n° 78, pp. 95-96. Sur la *class action*, voy. J. Simon, «L'action de groupe : l'illusion tragique, Le point de vue des entreprises», in *Le droit des affaires en évolution – La sanction dans la vie des affaires*, tome 18, Bruylant, Kluwer, 2007, pp. 89 et s.

[125] En vertu de l'article 128, «Lorsque les faits soumis au tribunal font l'objet d'une action en cessation, il ne peut être statué sur l'action pénale qu'après qu'une décision coulée en force de chose jugée a été rendue relativement à l'action en cessation».

[126] A. Tallon (sur la base du texte initial d'A. De Caluwé), «La procédure», *op. cit.*, n° 153, p. 175.

51. Il convient également de mentionner la procédure d'avertissement[127] qui est une procédure administrative préventive (et facultative) dont dispose le ministre des Affaires économiques et plus particulièrement la Direction générale Contrôle et Médiation (DGCM) pour informer les auteurs de leurs pratiques illicites et les inciter à respecter la loi[128]. La procédure semble efficace. Il se pourrait alors que ce ministère s'adresse aux professionnels et les incite à respecter la législation protectrice des consommateurs via les règles relatives à la protection des données personnelles.

2. Dans l'hypothèse d'une infraction à la législation relative aux données personnelles

52. L'individu peut tout d'abord s'adresser à la Commission de la protection de la vie privée. En vertu de l'article 31 de la loi belge du 8 décembre 1992 (ci-après loi vie privée), la Commission examine les plaintes que lui adressent les intéressés, sans préjudice de toute action devant les tribunaux et sauf si la loi en dispose autrement. Si la Commission estime que la plainte est recevable, elle accomplit une mission de médiation. Si son action débouche sur une conciliation des parties, elle dresse un procès-verbal avec exposé de la solution. En cas d'échec, la Commission émet un avis sur le caractère fondé de la plainte et peut l'accompagner de recommandations à l'intention du responsable de traitement. Les décisions, avis et recommandations de la Commission doivent être motivés[129]. L'article 32, §2 de ladite loi prévoit que la Commission, sauf si la loi en dispose autrement, dénonce au procureur du Roi les infractions dont elle a connaissance. Le §3 de ce même article donne au président de la Commission le pouvoir de soumettre au tribunal de première instance «tout litige concernant l'application de la présente loi et de ses mesures d'exécution».

53. L'individu peut également agir sur le fondement de l'article 14 de la loi vie privée qui permet au président du tribunal de première instance, siégeant comme en référé, de connaître «de toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou,

[127] *Cfr*. article 123 de la loi du 6 avril 2010.

[128] Pour des développements, se reporter à A. TALLON (sur la base du texte initial d'A. DE CALUWÉ), «La procédure», *op. cit*., n^{os} 201 et s., pp. 217 et s.

[129] Comp. avec la CNIL (l'équivalent français de la Commission vie privée) qui peut prononcer des sanctions à l'égard d'un responsable de traitement (art. 11, 2°, *g* de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004) : avertissement, mise en demeure avec sommation de cesser un comportement illicite dans un délai qu'elle fixe, sanction pécuniaire ne pouvant excéder 150 000 euros et/ou injonction de cesser le traitement de données ou un retrait de l'autorisation. Les décisions de la CNIL sont motivées et notifiées au responsable de traitement. Elles sont susceptibles de recours devant le Conseil d'État. Voy. M.-L. LAFFAIRE, *Protection des données à caractère personnel*, éd. d'Organisation, Guide pratique, 2005.

compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits (au traitement de laquelle la personne concernée s'est opposée) ou encore qui a été conservée au-delà de la période autorisée». La grande différence dans le cadre de tels recours est qu'elle s'entend d'une action individuelle et non collective comme l'est l'action en cessation.

3. Dans l'hypothèse d'une infraction à la législation relative aux données personnelles constitutive d'une pratique commerciale déloyale

54. Si l'infraction à une disposition de la loi vie privée constitue une pratique commerciale déloyale, l'individu victime d'un tel comportement devrait pouvoir exercer plusieurs types d'actions : une action en cessation – de préférence par le biais d'une association de défense des consommateurs – sur le fondement d'une pratique commerciale déloyale, le dépôt d'une plainte devant la Commission vie privée, le déclenchement d'une action en référé devant le président du tribunal de première instance sur le fondement d'une infraction à la loi vie privée.

55. De surcroît, les actions ne sont pas exclusives les unes des autres. Le consommateur pourrait choisir de s'adresser tout d'abord à la Commission vie privée pour ensuite, éventuellement, continuer une procédure sur le fondement d'une pratique commerciale déloyale ou sur celui d'une infraction à la législation vie privée. En effet, l'avantage de s'adresser à la Commission vie privée réside dans le fait qu'elle est spécialiste des questions relatives à la protection des données personnelles. Sa mission de médiation peut déboucher sur une conciliation des parties, ce qui n'est pas négligeable au lieu de s'engager dans la voie d'une action en justice. En cas d'échec de conciliation, si la Commission émet un avis favorable à la plainte déposée par l'individu et que le responsable refuse de s'y conformer, l'individu pourra alors décider soit de ne pas poursuivre en justice, soit d'agir sur le fondement de la législation vie privée ou sur celui des pratiques commerciales déloyales – si l'infraction en question constitue une telle pratique – dans le cadre d'une action en cessation. Le grand intérêt d'une association de consommateurs est qu'elle peut agir pour défendre des intérêts collectifs du moment que les statuts le mentionnent. Elle peut également agir seule au nom de l'intérêt collectif de ces membres. Dès lors, on peut s'interroger sur le fait de savoir s'il ne serait pas judicieux que la Commission vie privée puisse un jour avoir la possibilité de traiter des actions collectives et prendre des décisions à propos de ceux qui enfreignent la législation de protection des données.

Conclusions

56. Les conclusions de notre réflexion à propos des utilisations des TIC dans les relations avec les consommateurs seraient multiples. Nous les limiterons à deux points essentiels. Le premier porte sur l'intérêt, que révèlent les réflexions du chapitre 3, d'une approche qualifiée par les auteurs américains de «*Consumer Privacy*», c'est-à-dire d'une approche qui combine protection de la vie privée et protection des consommateurs. La seconde est plus fondamentale. Elle montre que les enjeux que dévoile l'utilisation de techniques de profilage, l'intelligence ambiante – ce qu'il est convenu d'appeler l'«*Internet of Things*»[130] – oblige à réouvrir les débats fondamentaux qui sous-tendent la consécration de la «vie privée» et donnent à ce concept une portée bien au-delà des législations de protection des données.

A. L'intérêt de l'approche «Consumer Privacy»

57. Notre propos plaide pour cette approche. Au-delà des questions de droits de l'homme, le développement des technologies de l'information et de leurs applications présente des enjeux économiques importants pour la défense des consommateurs. L'économie de l'Internet repose largement sur les ressources publicitaires et les technologies qui l'animent permettent de donner à ceux qui désirent maximiser l'intérêt de la publicité, les moyens appropriés pour le faire. Le marketing *one-to-one* est en pleine expansion et l'apparition de sociétés spécialisées dans cette technique de prospection et d'entreprises – comme les plateformes du web 2.0 ou comme Google – en relation directe avec les individus qui «consomment» leurs services hautement personnalisés font craindre une exploitation de plus en plus pointue de l'expression des choix des consommateurs ou des données à caractère hautement personnel que ces derniers confient à la toile (liste d'amis, *hobbies,* photos de vacances, etc.). Bref, protection des consommateurs et protection de la vie privée trouvent une occasion de cause commune que les dispositions légales permettent d'encourager : utilisation des dispositions en matière de pratiques commerciales déloyales ou agressives, possibilité d'actions collectives et au-delà intérêt d'un rapprochement des autorités de protection des données, des associations de libertés civiles et des associations de protection des consommateurs. L'intérêt de cette approche commune est attesté par l'analyse de l'action remarquable de la *Federal Trade Commission* américaine[131] en matière de *privacy*. Cette juridiction administrative spécialisée en matière de

[130] Sur cette question, voy. A. Rouvroy, «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence», *Studies in Ethics, Law, and Technology,* Berkeley Electronic Press, 2008.

[131] Voy. le site de la FTC http://www.ftc.gov/. Le 22 juillet de cette année, la FTC témoignait devant la Commission sénatoriale américaine «*Commerce, Science and transportation*», en matière d'«*Advertising trends and Consumer Protection*».

protection des consommateurs a pu, nonobstant l'absence de législation en matière de protection des données, développer une réflexion et des actions importantes dans les domaines qui nous concernent, qu'il s'agisse des utilisations à des fins commerciales des RFID[132] ou des techniques de profilage[133]. Cette action a pu être menée sur la base de la loi américaine relative aux pratiques déloyales, en particulier du «*False and Deceiptive Statement Act*» et devrait inspirer nos propres autorités publiques de protection des consommateurs.

B. Au-delà de la protection des données à caractère personnel, un débat fondamental pour nos libertés

58. La *privacy* en tant que protection de l'«autodétermination informationnelle» est plus large que la protection des données. Elle renvoie à des débats fondamentaux sur l'ensemble de nos libertés dans la mesure où elle les conditionne toutes[134]. Les problèmes liés au développement de ces nouvelles technologies intelligentes montrent que la *privacy* n'est pas qu'une lutte de protection de l'intimité ou de perte de contrôle de nos données à caractère personnel. Cela va plus loin désormais. Les technologies touchent à ce qui nous est le plus propre, nos émotions[135], notre liberté de mouvement, d'expression … Le débat

[132] Sur cette action en matière de RFID et l'importance dans ce contexte de l'association CASPIAN de protection des consommateurs, association spécialisée dans la matière des RFID, voy. N. KING, «Direct Marketing, Mobile Phones and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices», *Federal Communications Law Journal,* mars 2008, 2, vol. 60, pp. 229 et s.

[133] La question du suivi des consommateurs et de l'analyse de leur comportement en ligne a été l'objet de rapports et de discussions menées par la FTC, voy. en particulier le rapport sur l'«*Online Behavioral Advertising Moving the Discussion Forward to Possible Selfregulatory Principles*», disponible sur le site de la FTC : http://www.ftc.gov.bcp/ et les débats tenus sur ce thème les 1er et 2 novembre 2007 : «*Behavioral Advertising : Tracking, Targeting and Technology*». Voy. également World Privacy Forum, «The Network Advertising Initiative : Falling at Consumer Protection and Selfregulation», publié le 2 novembre 2007 sur le site : http://www.worldprivacyforum.org. Très récemment (13 janvier, 2009) le *Center for Digital Democracy*, centre spécialisé en matière de droits de l'homme, a adressé une plainte devant le FTC, plainte dont le contenu est disponible sur le site de la FTC. Cette plainte contient un rapport qui détaille la stratégie de différentes sociétés américaines en la matière et l'ampleur des risques liés à ces pratiques, en particulier par l'utilisation de données liées à la détention de téléphones portables.

[134] Sur la *privacy*, comme liberté «fondamentale», c'est-à-dire en tant que liberté, condition de possibilité de toutes les autres libertés, voy. H. BURKERT, «Dualities of Privacy – An Introduction to 'Personal Data Protection and Fundamental Rights'», in *Défis du droit à la protection de la vie privée,* M.V. PEREZ, A. PALAZZI (eds.), Cahier du CRID, 2008, pp. 13 et s. Voy. également nos réflexions, in 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,* colloque tenu à Bruxelles, novembre 2007, Springer Verlag, Dordrecht, 2009, pp. 50 et 51.

[135] Les scénarios marketing affectent notre vie privée. Les entreprises qui recourent à des services personnalisés et à des techniques de profilage mettent en danger ce droit : «*This kind of personalized services may be a threat to privacy because they provide companies and organisations using such techniques with a powerful instrument to know in detail what an individual wants, who he is, whether his behaviour shows certain pat-*

privacy change de nature. Au-delà de la protection offerte par la législation sur les données à caractère personnel – et qu'elle soit applicable ou non[136] – il convient de s'intéresser aux différentes atteintes que peuvent engendrer ces nouvelles techniques du point de vue des droits fondamentaux. Plusieurs d'entre eux semblent en effet menacés. Rappelons, avant de les énumérer, le sacro saint principe affirmé par l'article 1er de la Charte des droits fondamentaux de l'Union européenne selon lequel la dignité humaine est inviolable et doit être respectée et protégée. La dignité humaine doit guider toutes nos réflexions en la matière. Cette ligne directrice est fondamentale dans nos traditions et cultures juridiques occidentales : elle répond à l'impératif éthique kantien selon lequel la façon dont nous concevons et vivons nos rapports avec autrui doit être inspirée par le fait qu'autrui n'est jamais un moyen pour atteindre une fin mais toujours une fin en soi. Ce principe exclut une vision purement utilitariste de nos rapports avec autrui qu'ils soient, dans le cadre de nos scénarios, consommateurs de produits ou services de grande surface ou simples spectateurs de télévision.

1. Le droit au respect de l'intégrité physique et mentale

59. L'article 3 de la Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000 dispose que «Toute personne a droit à son intégrité physique et mentale». Cette prérogative rend illégales toute intervention sur le corps d'un individu ainsi que toute manipulation forcée de son mental. Si les actions *marketing* personnalisées exercent une influence trop importante sur les choix des consommateurs – que ce soit dans le contexte du *profiling* et/ou de l'essayage virtuel – il pourrait être soutenu que leur intégrité mentale est menacée. Cet impact serait effectif dans l'hypothèse d'une manipulation psychologique qui serait excessive au point d'affecter le comportement des consommateurs. L'enjeu consiste à déterminer les effets normaux, légitimes du *marketing*, et ceux qui sont anormaux, disproportionnés, dans le sens où la stratégie commerciale aurait pour objectif la manipulation des émotions à un degré élevé. Par exemple, si le système met en place des procédés subliminaux, l'influence alors exercée sur le consommateur serait déloyale et donc anormale. Ainsi l'atteinte au droit à l'intégrité de l'individu ne sera pas dramatique, à condition que le marketing s'en tienne à des stratégies raisonnables.

---

terns, et cetera» (S. VAN DER HOF et C. PRINS, «Personalisation and its influence in identities, behaviour and social values», in *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. HILDEBRANDT et S. GUTWIRTH (ed.), *op. cit.*, spéc. p. 116).

[136] *Cfr.* nos réflexions *supra,* nos 5 et s., à propos des données non personnelles dans certains cas d'utilisation de données liées à des objets mais ayant un impact sur les porteurs ou détenteurs de ceux-ci.

2. *Liberté de pensée, de conscience et de religion*

60. La liberté de conscience et de religion est consacrée par plusieurs textes : la Déclaration universelle des droits de l'homme à l'article 18[137], la Convention européenne des droits de l'homme à l'article 9[138], et la Charte des droits fondamentaux de l'Union européenne à l'article 10[139]. Cette liberté vise à assurer une diversité culturelle, religieuse et philosophique indispensable à nos sociétés démocratiques[140] et en ce sens, doit être considérée comme «*one of the most vital elements that constitute the identity of believers and their conception of life*»[141]. Comme le tribunal constitutionnel allemand le notait déjà, les applications des technologies de l'information peuvent conduire à une normalisation des comportements, voire des pensées. Sans vouloir être pessimiste, relevons la conclusion d'une étude récente sur le profilage : les services personnalisés, offerts dans notre société de l'information, «*could put cultural and social diversity at risk : one political or religious message is to dominate the whole discourse*». Et les mêmes auteurs, d'ajouter : «*it [personalisation] could imply that behaviour is manipulated, freedom of self-determination and personal autonomy are limited and societal freedom is eroded. With personalised services, many individuals differences are reduced to one or some of them taking into account preferences, characters… of human beings… Because of its tendency to generalise, personalisation may lead to diminishing preferences, differences and values*»[142].

[137] Article 18 de la Déclaration (10 décembre 1948) : «Toute personne a droit à la liberté de pensée, de conscience et de religion; ce droit implique la liberté de changer de religion ou de conviction ainsi que la liberté de manifester sa religion ou sa conviction seule ou en commun, tant en public qu'en privé, par l'enseignement, les pratiques, le culte et l'accomplissement des rites».

[138] Article 9 de la Convention (1950) : «1. Toute personne a droit à la liberté de pensée, de conscience et de religion; ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites. 2. La liberté de manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui».

[139] Article 10 de la Charte européenne des droits fondamentaux (2000) : «Toute personne a droit à la liberté de pensée, de conscience et de religion. Ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites».

[140] A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, *op. cit*., spéc. p. 102 : «The pluralism indivisible from a democratic society depends on it».

[141] A. Cammilleri-Subrenat et C. Levallois-Barth, *Sensitive Data Protection in the European Union*, *op. cit*., p. 102.

[142] S. Van Der Hof et C. Prins, «Personalisation and its influence in identities, behaviour and social values», in *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. Hildebrandt et S. Gutwirth (eds.), *op. cit*., spéc. p. 121.

3. Le droit de jouir de ces libertés sans discrimination

61. L'article 2 de la Déclaration universelle des droits de l'homme[143] et l'article 21 de la Charte européenne[144] consacrent le droit de l'individu à jouir de ces libertés sans discrimination comme le fait l'article 14 de la Convention européenne des droits de l'homme : «La jouissance des droits et libertés reconnus dans la présente Convention doit être assurée, sans distinction aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation».

L'utilisation de services marketing personnalisés peut engendrer la discrimination de certaines catégories de personnes. Le recours à la technique du *dynamic pricing*, qui fait que le prix demandé aux consommateurs pour tel produit n'est pas le même suivant des critères déraisonnables[145], risque fort d'aboutir à des discriminations[146]. Sans doute, les risques de discrimination seront d'autant plus présents qu'il s'agit d'un bien ou service jugé «essentiel» dans notre société de l'information. Ainsi, dans la récente controverse sur la loi française Hadopi, le Parlement européen[147] et le Conseil constitutionnel français[148] ont-ils pu juger que l'accès à internet constituait en tout cas un de ces biens essentiels à l'heure actuelle; mais on peut également songer à des services de transactions en ligne comme certaines assurances obligatoires ou des services d'enseignement en ligne.

---

[143] Article 2 de la Déclaration : «1.Chacun peut se prévaloir de tous les droits et de toutes les libertés proclamés dans la présente Déclaration, sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation. 2. De plus, il ne sera fait aucune distinction fondée sur le statut politique, juridique ou international du pays ou du territoire dont une personne est ressortissante, que ce pays ou territoire soit indépendant, sous tutelle, non autonome ou soumis à une limitation quelconque de souveraineté».

[144] Article 21 de la Charte européenne : «Est interdite, toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. 2. Dans le domaine d'application du traité instituant la Communauté européenne et du traité sur l'Union européenne, et sans préjudice des dispositions particulières desdits traités, toute discrimination fondée sur la nationalité est interdite».

[145] Voy. *supra,* n° 10.

[146] S. Van Der Hof et C. Prins, «Personalisation and its influence in identities, behaviour and social values», in *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. Hildebrandt et S. Gutwirth (eds.), *op. cit*., spéc. p. 121. Les mêmes auteurs nuancent cependant avec raison leur propos : «*Personalisation is an effective tool to achieve an efficient market*». Il est vrai que les responsables marketing pourront arguer que l'inclusion ou l'exclusion de certaines catégories d'individus peut être considérée comme économiquement profitable en ce sens que les services personnalisés évitent des investissements inutiles et satisfont efficacement les différentes préférences des consommateurs.

[147] Voy. le communiqué de presse du Parlement européen : http://www.europarl.europa.eu/news/expert/infopress_page/058-54125-111-04-17-909-20090421IPR54124-21-04-2009-2009-false/default_fr.htm.

[148] Décision du Conseil constitutionnel n° 2009-580 du 10 juin 2009.

4. Liberté de mouvement

62. La liberté de mouvement, consacrée par l'article 2 du Protocole additionnel n° 4 de la Convention du Conseil de l'Europe et par l'article 45 de la Charte des droits fondamentaux de l'Union européenne, implique que nous puissions nous déplacer sans être constamment suivis ou «tracés». Comme le relève l'Opinion 4/2004 du Groupe de l'article 29, la liberté de mouvement doit s'entendre de manière large : «*Freedom of movement does not only mean that one must be free to move in the physical space, but also that one must be free to move withouth inevitably leaving continuous and/or frequent traces of one's movements for the benefit of systems enabling permanent optical observation and grassing out. Being seen without seeing may indeed constrain the person in her movements and trajectories*».

Sans doute, certains scénarios de publicité personnalisée liée à la géolocalisation via nos GSM de nouvelle génération[149] permettant de détecter adéquatement notre position en rapport avec tel ou tel produit ou commerce pourraient-ils être visés par cette réflexion.

63. Concluons. Que les technologies de l'information apportent à chacun une occasion de se libérer, de découvrir des mondes nouveaux, de s'affranchir des contraintes que tissent son lieu et son cadre d'existence, de s'exprimer et d'entrer en communication avec qui il souhaite, est évident. Qu'elles apportent à chacun des avantages tant sur le plan économique (achat à distance, économie de déplacements) que sur le plan de la sécurité (système de vidéosurveillance) est indéniable.

Mais ces mêmes technologies représentent une menace d'autant plus grande pour nos libertés que leurs avantages mis en avant par leurs protagonistes nous amènent à multiplier les risques : non seulement à accepter d'être suivis, à nous voir réduits à un numéro, à subir les messages qui nous arrivent à tout moment sur nos boîtes aux lettres, sur nos écrans voire dans nos corps, mais au-delà à jouer le jeu de la marchandisation de l'information personnelle en nous exhibant sur le net à travers les réseaux sociaux et autres. En cela, un enjeu essentiel du droit à la protection de la vie privée est la défense de l'humain, de son développement et de sa dignité comme valeurs absolues ; et cela passe par le renvoi des logiques absolues de sécurité et d'efficacité économique à leur dimension toute relative.

Notre réflexion s'achève ou plutôt ouvre de nouveaux chantiers : elle réclame un débat large, si possible européen, permettant à toutes les catégories d'intérêts, les entreprises présentes sur le web, les fournisseurs d'équipements terminaux, les «*designers*» des sys-

[149] Sur ces nouvelles applications, voy. N. KING, «Direct Marketing, Mobile Phones and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices», art. précité.

tèmes d'information, les consommateurs, les associations de libertés, les autorités de protection des données, les organismes officiels de protection des consommateurs, de pouvoir s'exprimer sur ces applications nouvelles des technologies, leurs impacts en matière tant de protection des consommateurs que de protection des libertés. Il ne s'agit pas de négliger l'apport de telles technologies au profit des citoyens mais de veiller à une meilleure éducation du public, à rappeler les impératifs réglementaires en la matière voire à les évaluer et surtout à chercher ensemble, en ce compris par la technologie elle-même, les solutions qui s'imposent.