

LA NOTION DE « PRIVACY » A L'HEURE NUMERIQUE

La « privacy » comme analyseur des formes de régulation

Bénédicte SY-REY (SUSI, France Telecom R&D, CERLIS, U. Paris V,
benedicte.syrey@orange-ftgroup.com)

RESUME

La vie privée serait menacée, plus que jamais, par les technologies. L'un des grands enjeux relatif à la « privacy » semble s'axer autour de l'information, et du contrôle de celle-ci. Car la valeur accordée à l'information, c'est-à-dire aux données de connexion, de navigation, d'achat, de déplacement, auxquelles on peut travailler pour donner un sens (les profils de consommateurs, par exemple), mais aussi les risques que l'information peut comporter, sont significatifs.

Selon nombre de rapports professionnels, et de recherches en sciences humaines et sociales, la vie privée, en tant que droit fondamental, ne devrait pas avoir à être défendue : elle devrait être reconnue comme une valeur immuable. Mais au-delà de valeurs et de standards d'ordre moral, la « privacy », si elle n'est pas respectée, peut avoir des conséquences concrètes sur la vie des individus. C'est en ce sens que la nécessité de régulation peut être comprise.

Entre droit fondamental de l'être humain, pilier sans lequel l'essence de l'humain, son épanouissement personnel ne saurait être possible, et enjeu majeur en termes de contrôle de l'information sur soi, c'est-à-dire aussi de contrôle de soi, la « privacy » apparaissait déjà hier comme un enjeu majeur. Aujourd'hui, avec la diffusion massive d'Internet, et le développement des technologies communicantes, il s'agit d'un défi qui appelle des réponses tant juridiques, que sociales et techniques.

Mots-clé : Vie privée – Privacy – Régulation – RFID – Traces

introduction

S'intéresser aux formes de régulation à l'œuvre autour des technologies de l'information et de la communication, c'est s'intéresser à la manière dont nous intégrons, dans nos vies quotidiennes, des systèmes techniques en changement. En ce sens, c'est s'intéresser à notre société, et à son devenir. L'une des entrées qui apparaît pertinente, et dont l'actualité ne devrait que se renforcer, consiste à s'interroger sur la notion de « privacy », à l'heure où l'environnement numérique est de plus en plus omniprésent.

De fait, l'ensemble des recherches et articles de presse annonce l'avènement de « l'informatique ambiante ». Mais sans attendre un demain souvent fantasmé, où l'interactivité, et même le « machine to machine » seraient à leur apogée, la question de la « privacy » se pose dès aujourd'hui. Plus encore, se la poser dès aujourd'hui apparaît fondateur d'un demain moins incertain, dans lequel les grandes inquiétudes, plus ou moins réalistes pourraient trouver certaines réponses. De telles réponses passent par différentes formes de régulation, régulation sociale, mais aussi régulation juridique, et technique.

C'est pourquoi, afin de mieux saisir ce qu'est aujourd'hui le « privé », à l'heure du numérique et des traces multiples que laissent nos usages, le travail mené dans le cadre de cette thèse vise à analyser les usages, tout en intégrant la dimension réglementaire. De fait, il s'agira d'étudier de manière systématique un certain nombre de cas, dans lesquels la tension qui s'est fait jour permet de mieux comprendre quelles sont les frontières du « privé ». L'étude de telles affaires, par ailleurs, se complètera d'une analyse des usages. A ce jour, deux corpus d'entretiens sont en cours d'exploitation : d'une part, un corpus d'entretiens semi-directifs, menés auprès d'utilisateurs dans leur cadre domestique ; d'autre part, un corpus d'entretiens réalisés avec des utilisateurs dans leur cadre professionnel.

Le présent article s'attachera à montrer en quoi la notion de « privacy » est un analyseur pertinent pour montrer les formes de régulation qui opèrent autour de la diffusion sociale des technologies de l'information et de la communication. Après avoir précisé la définition de la notion de « privacy », nous nous intéresserons à un certain nombre de formes de régulation.

1. LA NOTION DE PRIVACY DANS UN UNIVERS NUMERIQUE

1.1. La « privacy » : un concept à part entière ?

La notion de « privacy » n'est pas d'usage récent, pas plus que ne l'est l'expression française de « vie privée ». Mais si la sphère du privé est globalement considérée comme étant une sphère à préserver, il apparaît que ses contours sont flous. Il semble difficile de s'en tenir à une définition qui fasse l'unanimité, à moins d'en rester à une interprétation globalisante dont l'intérêt pourrait s'en trouver limité. Par ailleurs, les sources visitées, tant françaises qu'anglo-saxonnes, font état de la « privacy » comme d'une valeur certes fondamentale, et, malgré quelques nuances, universellement reconnue, mais dont la portée varie selon les époques, et selon les environnements tant culturels, sociaux, qu'économiques ou techniques.

Pourtant le travail de recherche mené autour de la notion de « privacy » indique que la sphère du privé est reconnue dans nombre de textes fondateurs, et dans nombre de textes de loi, comme une forme de limite au-delà de laquelle il y aurait ingérence dans des affaires tenues pour privées, et au-delà de laquelle il est reconnu à l'individu une forme de droit à vivre

librement son intimité, ses opinions, son image, ou encore ses actes ou propos, sans que ceux-ci puissent lui être enlevés, voire être simplement portés à la connaissance d'autrui.

Littéralement, le terme de « privacy » peut se traduire par le fait d'être seul, par l'expression « vie privée », ainsi que par les termes de secret, d'intimité¹. Le terme anglais de « privacy » n'a donc pas de traduction simple en français, même si l'expression de « vie privée » lui vaut traduction dans nombre de textes. Dans le cas plus précis des sites Internet, les sites anglo-saxons affichent une rubrique « privacy policy ». Les sites français proposent alternativement une rubrique intitulée le plus souvent « politique de confidentialité », ou « protection des données personnelles² ». Plusieurs termes français, donc, pour une même notion de « privacy ». Nous faisons le choix de conserver l'usage de l'expression anglo-saxonne aux côtés des expressions françaises, afin de ne pas se limiter *a priori* à une dualité privé/public trop nette. Nous faisons en effet l'hypothèse que comprendre les formes de régulation à l'œuvre autour des enjeux de privacy s'opère en différentes nuances, différents degrés du « privé ».

Sans établir ici tout l'historique de la notion de « privacy », il apparaît important de retenir quelques points clés. La première définition formalisée de la notion de « privacy » est le plus souvent attribuée à S. Warren et L. D. Brandeis (1890). Leur texte en appelle à un fondement légal de la « privacy » comme droit fondamental, et souligne en particulier le « droit à être laissé tranquille », ou « droit à être laissé seul ». Ils écrivent notamment que les photographies instantanées, ainsi que les journaux, ont envahi les principes sacrés de la vie privée et domestique, faisant porter sur ces principes certaines menaces. Car ils distinguent le fait d'exprimer délibérément ses pensées et émotions dans une œuvre artistique ou littéraire, de leur simple expression dans la vie quotidienne. Ils estiment en ce sens que la nécessité d'une protection adaptée ne fait aucun doute, afin de défendre le droit de chacun à s'exprimer, à ressentir, à penser, et de protéger un principe de « personnalité inviolable » qu'ils tiennent pour constructif du droit à l'immunité.

Avec S. Warren et L. D. Brandeis, ce sont aussi deux autres notions clé qui sont mises en avant, notions centrales aujourd'hui dans les débats sur le développement de l'informatique ambiante. En particulier, nous retiendrons d'une part la notion d'équilibre entre l'intérêt individuel à se protéger, et l'intérêt général à prendre connaissance de quelque chose, et d'autre part la notion de consentement³. De fait, pour ces auteurs, dès 1890, la « privacy » s'articule largement autour du contrôle par l'individu de l'information le concernant, thème qui reste central dans la problématique « privacy » actuelle, comme nous le verrons plus loin. S. Warren et L. D. Brandeis en appellent à une définition globale de la « privacy », qui puisse devenir un droit à part entière.

¹ D'après le dictionnaire Harrap's Unabridged Pro (édition électronique).

² La définition des « données personnelles » est précisée par la loi n° 2004-801 du 06 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (modifiant la loi n°78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et transposant la directive européenne du 12/07/2002 « vie privée et communications électroniques »). Article 1^{er}: « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». La loi précise que, « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

³ La question du consentement reste d'actualité, et illustre les différences d'approche en matière de protection de la vie privée. Aux Etats-Unis par exemple, le principe dit de « l'opt-out » est privilégié. Dans cette logique, l'utilisateur consent « par défaut » à ce que ses données soient utilisées, voire partagées avec des tiers ; il doit cependant en être informé, et dispose du droit de s'y opposer. En France, et en Europe, c'est le principe de « l'opt-in » qui est soutenu, par lequel l'utilisateur doit donner un accord explicite.

Ils s'inscrivent, avec cette position, dans une distinction entre l'approche des tenants d'un « concept privacy », et ceux qui estiment d'autre part qu'un tel droit n'a pas lieu d'être (J. DeCew, 2006). D'après cet auteur en effet, on peut distinguer deux courants qui approchent différemment cette notion. D'une part, les « réductionnistes », pour lesquelles, explique l'auteur, ce que l'on appelle « privacy » est moins un ensemble à part entière que différents enjeux ayant trait à d'autres droits et d'autres valeurs. Il leur semble plus approprié de balayer en termes de « standard moral et de catégories légales » tout enjeu où la question du privé peut se poser. D'autre part, les « cohérentistes » (auxquels s'apparentent Warren et Brandeis) : pour ces derniers, « privacy » est un concept, dont les enjeux sont cohérents les uns par rapport aux autres. En ce sens, ils estiment que le concept de « privacy » a une valeur intrinsèque, et qu'il fait partie des concepts fondamentaux, bien qu'il n'y ait pas nécessairement unanimité quant aux éléments définissant la « privacy ».

1.2. Le défi numérique

Si la « privacy » est essentielle à l'homme, et si l'on a compris que de longue date, les penseurs se sont interrogés sur cette question, le changement technologique des dernières décennies semble bien exacerber, et renouveler parfois le débat. En effet, la diffusion d'Internet, de la téléphonie mobile, de techniques d'identification, ou d'autres objets communicants multiplient les traces, conscientes ou inconscientes, volontaires ou involontaires, que laissent nos activités quotidiennes, et qui peuvent sembler anodines.

Anticipant une diffusion large de l'informatique ambiante et des nanotechnologies, Y. Pouillet (2005) écrit que « l'Homme ainsi est saisi par les TICS non seulement dans son action ou ses attributs externes mais au plus profond de lui ». Mais sans attendre les nanotechnologies corporelles, les applications biométriques, comme c'est le cas dans certains lieux de travail, ou dans certaines cantines scolaires (Dubey G., Guchet X., Craipeau S., 2004), témoignent de ce que les traces laissées par les usages sont implicantes pour l'utilisateur. Et c'est en ce sens qu'elles sont sensibles, et peuvent faire tension. Elles sont une forme d'empreinte de lui, et peuvent permettre de le connaître, dans ses préférences, ses opinions, ou ses habitudes de transport par exemple. C'est aussi ce que notent P. Monot et M. Simon : « nos déplacements en voiture ne constituent qu'une infime partie des traces électroniques que nous laissons partout autour de nous. Lorsque nous payons par carte de crédit ou lorsque nous retirons de l'argent, lorsque nous utilisons un téléphone cellulaire, ou que notre voiture passe au télépéage des autoroutes, lorsque nous pointons sur notre lieu de travail ou que nous prenons l'avion, lorsque nous passons devant une caméra l'une de ces multiples caméras vidéo ou que nous achetons quelque chose par correspondance, lorsque nous payons un film sur une chaîne de télévision à péage, ou que nous téléphonons du lieu de travail, chaque opération est inscrite quelque part dans un fichier informatique. Tous nos mouvements, tous nos choix peuvent ainsi être épiés, stockés, analysés. Ces traces électroniques sont innombrables, prêtes à être utilisées dans un but malveillant par n'importe quel individu, société commerciale ou Etat. Toute notre vie privée semble menacée ».

Ces traces sont-elles anodines, ou portent-elles le risque, comme bien des textes le soulignent, de menacer notre vie privée et nos libertés individuelles ? Si l'on en revient à la notion même de trace, on constate que ce sont bien des formes de marqueurs de soi que l'utilisateur laisse derrière lui. A. Serres (2002) estime que la trace « n'existe que par rapport à autre chose (un événement, un être, un phénomène quelconque), elle est de l'ordre du double, voire de la représentation et ne prend son sens que sous le regard qui la déchiffre ». Il écrit que « le premier sens de la trace est donc bien l'empreinte, qu'elle soit matérielle ou morale ». L'une

de ses conclusions fait état du fait que « penser les traces revient à penser les processus d'extériorisation de l'homme à travers ses artefacts et notamment le processus d'extension de la mémoire collective, depuis les premiers silex jusqu'aux mémoires numériques actuelles ».

La trace n'a pas attendu les nouvelles technologies pour exister, et pour parler de l'individu. Mais les applications numériques, et la diffusion d'objets communicants, initient un changement d'échelle. Dans un tel contexte, les traces sont multiples, les fichiers de données sont nombreux, et les capacités de traitement de telles informations sont accrues.

2. LES ELEMENTS STRUCTURANTS DE LA « PRIVACY »

2.1. La « privacy » comme valeur humaine fondamentale, garante de la liberté individuelle

Pour les défenseurs d'un concept de « privacy », il s'agit avant tout d'une valeur force directement reliée à la notion de dignité humaine. Cela rejoint la notion de « personnalité inviolable » évoquée précédemment, la dignité reposant notamment sur les obligations réciproques de respect, de confidentialité, de divulgation maîtrisée d'information dans l'échange entre deux parties (G.A. Gow, 2005). La notion de « privacy » définirait ce qui fait qu'on peut se dire être humain, incluant des valeurs fondatrices de ce concept, dont la dignité et l'intégrité, l'autonomie personnelle et l'indépendance (DeCew, 2006).

Avec un tel concept fondateur, c'est la liberté humaine qui serait également fondée de plein droit : la liberté de ne pas être dérangé lorsqu'on n'y a pas consenti, ainsi que la liberté de ne pas être contraint dans ce que l'on fait, ni dans la manière dont on le fait (C. Potts, G. Tech, 2001). La « Privacy » serait ainsi également la liberté et le droit à l'autodétermination de chacun concernant ses opinions, ses relations sociales. D'après J. DeCew (2006), la notion de « privacy » apparaît indispensable pour le développement de la personnalité de chacun, et l'établissement de relations intimes où la confiance, et le respect d'autrui autant que de soi-même ont leur place.

Le droit à être laissé tranquille prend ici tout son sens. Il s'agit de ne pas être gêné par des sollicitations non souhaitées émanant de tiers, comme la publicité non désirée. Mais sauf à vivre reclus, nos relations avec les autres sont porteuses d'une part de notre « privacy », plus ou moins grande et plus ou moins intime selon les relations. La « privacy », selon ces auteurs, apparaît comme une garantie, une valeur de protection contre les indiscretions ou malveillance dont l'individu pourrait être victime du fait de ce partage avec autrui d'éléments de la vie privée, partage souvent involontaire, mais qui est partie prenante de notre vie quotidienne.

2.2. L'information : l'axe majeur de la privacy

2.2.1. Le contrôle de l'information

Depuis plusieurs années, c'est l'information qui semble dominer le débat. Selon la logique déroulée jusqu'ici, l'on comprend combien le fait, pour un individu, d'avoir le contrôle des informations le concernant est crucial. Ce point n'a pas attendu les TIC pour s'inscrire dans une problématique en termes de vie privée. En effet, la diffamation, ou le fait de rendre public des informations embarrassantes au sujet d'une personne peuvent être réprimés depuis

longtemps. Aujourd'hui, les multiples données que laissent nombre d'actes de la vie quotidienne sont le plus souvent collectées sans que l'utilisateur s'en rende compte. Cela ne se fait pas nécessairement « à son insu », comme on le lit dans nombre d'articles de presse, car l'utilisateur peut être informé ou conscient de cet état de fait. La Loi Informatique et Liberté de 1978⁴, stipule bien l'obligation d'informer l'utilisateur de son droit d'accès et de rectification aux données le concernant. Il n'en reste pas moins que l'utilisateur ne sait pas nécessairement que des données sont collectées⁵, ni quelles sont ces données, ce qu'elles peuvent dire de lui, ou encore quel(s) tiers y auront accès.

Permettre à l'utilisateur de savoir ce qui se passe avec ses données, c'est lui permettre de mesurer l'ampleur et les circonstances de circulation de ses données, et c'est lui permettre de choisir. G. Vincent (1987), pour un contexte plus grave, écrivait que la liberté ultime, dans une société totalitaire, peut devenir le choix de se donner la mort. Se voler au système totalitaire, c'est faire le choix d'une dernière forme d'autonomie. Pour l'utilisateur des nouvelles technologies, savoir ce qu'il advient de ses données peut lui permettre de choisir s'il souhaite refuser, quitte à devoir réaliser un choix alternatif, même moins confortable. L'utilisateur peut refuser de se rendre en certains lieux s'il ne souhaite pas que des caméras de surveillance le filment, il peut choisir un autre moyen de transport s'il ne veut pas souscrire à une application télébilletique.

Dès les années soixante, on voit apparaître ce déterminant essentiel de la privacy, qui consiste en l'aptitude à déterminer pour soi-même dans quelles circonstances (quand, comment, etc.) le partage d'informations nous concernant est envisageable (Westin A., 1967⁶). Concevoir la « privacy » comme un enjeu informationnel, cela permettrait ainsi de donner le « pouvoir » à l'individu de contrôler la publication et la distribution d'informations le concernant (Bohn et al., 2004). Il manque certes un maillon, car l'utilisateur n'accèdera pas aux bases de données réellement conservées par l'entreprise. Pour cela il pourra se reposer sur un organisme comme la CNIL⁷, dont la mission de contrôle doit mettre assez de « pression » aux acteurs pour qu'ils respectent les droits des usagers. Par ailleurs, pour contrôler la diffusion de ses données, et trouver des solutions qui puissent lui assurer un certain niveau de « privacy », certaines solutions techniques peuvent être envisagées, comme nous le verrons plus loin.

2.2.1. La valeur de l'information : régulation informelle autour d'une forme de marché des données personnelles

Le contrôle de l'information serait donc essentiel à la « privacy ». Mais si ces informations peuvent menacer la vie privée, elles sont aussi une source de valeur économique. Aussi le débat se pose-t-il en termes du bénéfice de cette valeur : puisque les données génèrent de la valeur, pourquoi celui qui, de par ses usages, permet cette valeur ne pourrait-il pas en bénéficier ? Un point de vue consiste à considérer que la valeur appartient à ceux qui collectent et travaillent ces données. Mais d'autres constatent le développement d'une forme de propriété de l'information au profit de l'utilisateur : « La référence à un hypothétique droit à l'intimité s'efface. Il est désormais question de faire respecter un droit de propriété. [...] Certains défenseurs de la vie privée, désireux de s'opposer aux formes les plus agressives du marketing relationnel, se rallient à cette idée de rémunérer les individus. [...] Le droit de

⁴ Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, du 06/01/1978.

⁵ Le terrain réalisé par entretiens individuels auprès d'utilisateurs, en cours d'analyse, montre ainsi que, même parmi des utilisateurs se disant sensibles aux questions d'intrusion dans leur vie privée, certains disposaient d'un « Pass Navigo » sans savoir qu'il contient une puce RFID, ni ce que cela implique.

⁶ In ROY (2006).

⁷ Commission Nationale Informatique et Liberté : <http://www.cnil.fr>

propriété sur les données donne une réponse très imparfaite à la question de la protection de la vie privée » (Belleil A., 2001).

Pourtant, comment parler de marché, quand, malgré les imprécisions de définition, le droit au respect de la vie privée, à l'intimité, est assimilé à un droit humain fondamental, et est à ce titre incessible. Le débat autour de la propriété de la valeur pose cependant la question de savoir si l'on parle de propriété privée, ou de propriété intellectuelle (Bohn et al., 2004). Mais derrière les principes et les débats, des formes d'échanges marchands se développent, dans lesquelles les données sont échangées contre des services. Certains sites, par exemple, exigent le remplissage d'un formulaire pour accéder à une prestation... gratuite, à condition d'y laisser des données personnelles. D'autres mécanismes « récompensent » celui par qui l'entreprise apprend à mieux connaître ses clients. Les systèmes de points de fidélité, ainsi, permettent-ils de « payer » le consommateur pour sa fidélité, mais aussi pour son attention. Les pratiques sont cependant fréquentes, de la part des usagers, qui consistent à répondre avec de fausses informations afin de limiter le retour publicitaire lié à leur souhait d'accéder à un service, ce dont les entreprises sont conscientes⁸. D'autres encore choisissent de se priver du service plutôt que de donner des informations les concernant⁹.

D'une certaine façon, l'utilisateur arbitre, et décide si le service qu'il souhaite « vaut » ses données. Nombreux sont en effet les usagers qui ne remplissent les formulaires de façon scrupuleuse que dans les cas où ils achètent quelque chose. On constate ainsi que la propriété de l'information, même s'il ne s'agit pas de se transmettre des titres de propriété, reste un enjeu dont la régulation s'opère davantage par les pratiques que par une intervention du droit. Car si les lois françaises par exemple encadrent la collecte et le traitement des données personnelles, les moyens limités de la CNIL notamment ne permettent qu'un contrôle imparfait, relativement impuissant face aux bénéfices attendus des fichiers de données. Il semble qu'alors ce sont les usagers qui, de par leurs pratiques, opèrent un arbitrage, une forme de régulation face aux entreprises si friandes de leurs informations.

3. QUELLES FORMES DE REGULATION POUR LA « PRIVACY » ?

3.1. Pourquoi protéger la privacy ?

Nombre d'auteurs, nous l'avons vu, se soucient de la protection de la vie privée, et cherchent à en fonder une définition qui l'impose comme un droit humain fondamental, garant de nos libertés individuelles. Mais pourquoi une telle sensibilité à cette question ? Sans discuter du bien-fondé de la nécessité de protéger la vie privée, ou d'en contester l'importance au regard de la personnalité individuelle, il convient de resituer certains risques.

Les usagers semblent se partager entre une crainte associant la technologie à la surveillance, avec l'expression « big brother » récurrente, et un rejet de toute crainte. C'est ce que nous montre l'analyse des réactions recueillies autour de certaines applications de la technologie RFID¹⁰, comme le titre de transport Navigo, mis en place par le Stif¹¹. Les réactions émises

⁸ Corpus d'entretiens menés auprès de professionnels.

⁹ Entretiens individuels menés dans le cadre d'une enquête France Telecom R&D.

¹⁰ Radio Frequency Identification. La technologie RFID fait appel à des micro-puces insérées le plus souvent dans des étiquettes qui elles-mêmes sont apposées sur des produits de consommation (X. Lamarteleur, 2004). Elles permettent une lecture à distance par le biais d'ondes radio, et à une distance variable, des données nécessaires au fonctionnement d'une machine ou d'un service (T. Kyndt, 2006).

¹¹ Syndicat des Transports d'Ile de France.

par des internautes à la suite de certains articles de presse sur ce sujet¹² témoignent d'une part de craintes, liées au risque perçu d'intrusion dans la vie privée, mais aussi liées aux erreurs possibles de la technologie, qui viendraient contraindre l'utilisateur dans sa liberté de déplacement, voire dans sa dignité. Mais on note également des réactions d'internautes qui ne s'inquiètent pas de leurs traces, et qui estiment finalement que la sécurité (dans les transports par exemple) vaut bien quelques identifications. Ils estiment, en particulier, que lorsque l'on n'a rien à se reprocher, on n'a pas à craindre d'être identifié, ou filmé. Selon cette logique, le fait de ne pas vouloir être « traçable » tend à rendre l'utilisateur suspect, comme s'il voulait cacher quelque chose de nécessairement répréhensible : si l'on est en accord avec la loi, pas de crainte à avoir, ni de réticence, avec le fait d'être « traçable ». Cette forme d'exigence normative ne laisse pas de place à une quelconque réticence, qui semblerait alors suspecte. Le fait de vouloir garder certaines choses pour soi, même un simple sentiment de liberté, tend ici à être remis en cause, ce qui remet également en cause la notion de « privacy », entendue comme le droit être laissé tranquille, à se soustraire du regard d'autrui, à se déconnecter.

Mais au-delà de la représentation fantasmée, ou au contraire de l'adhésion sans retenue à une technologie comme la RFID, certains risques d'exploitation à mauvais escient des données existent néanmoins, qui peuvent porter atteinte, de diverses manières, à la vie privée des individus, et à leur liberté. Pour P. Monot et M. Simon (1998), de tels traitements informatiques peuvent avoir des conséquences réelles et importantes pour la vie des individus. Ils estiment que le problème de la protection de la vie privée, même si chacun y est sensible, n'est pas le problème principal. Pour eux, le « danger » réside plutôt dans la « discrimination qu'entraînent la collecte ; le traitement, et l'utilisation des données liées à la vie privée. [...] A terme, quelques bits d'information traités automatiquement créent des catégories entières de gagnants et de perdants dans la population, d'abord au niveau économique, mais également à d'autres niveaux, lorsque ces informations sont utilisées par un éventuel employeur, assureur ou avocat, ou pour déterminer le risque qu'encourt un propriétaire à louer un logement ». Si, pour un fournisseur de service, le fait de réduire les risques répond à une logique de rentabilité, les auteurs estiment que pour les individus, cela peut conduire à de la discrimination.

Concernant les traitements automatisés de données, P. Monot et M. Simon (1998) estiment que les individus ne peuvent pas vraiment comprendre ni maîtriser ce qui les assigne à telle ou telle catégorie. Dans d'autres cas, ce ne sont pas tant les données collectées, que des informations émises parfois volontairement qui peuvent en retour menacer la vie privée des individus, mais aussi avoir des conséquences au-delà de l'intrusion. L'exemple du contrôle parental à cet égard est éclairant. Les récentes campagnes, ainsi que la décision dernièrement prise d'obliger les fournisseurs à proposer un logiciel de contrôle pour la navigation sur Internet pour inciter à la vigilance, témoignent du risque qu'il y a, pour des enfants en particulier, à diffuser, sans en mesurer les implications possibles, des informations relatives à leur vie privée.

Pour l'ensemble de ces cas, la sphère du privé est très sensible aux intrusions, et c'est en ce sens que la nécessité de réguler peut être comprise.

3.2. Les grands types d'encadrement réglementaire

Sans régulation, de fait, les abus décrits précédemment seraient et deviendraient sans doute courants. Différentes formes de régulation sont à l'œuvre, parmi lesquelles un encadrement

¹² Voir bibliographie.

réglementaire s'efforce de suivre les débats à mesure de la diffusion de technologies. Il existe plusieurs types de modèles réglementaires. Nous retiendrons d'une part, les systèmes proposant des lois sectorielles, et d'autre part les systèmes proposant une loi globale.

Le modèle des lois sectorielles est par exemple celui des Etats-Unis. Les lois s'appliquent alors à un secteur particulier. Par exemple, le « Privacy Act » de 1974 s'appliquent aux administrations américaines, mais ne régulent pas le secteur privé. Selon Privacy International (2006), ce modèle tend à présenter des failles en termes de protection des données personnelles des individus, notamment aux Etats-Unis. Dans le modèle de loi globale, des lois visent à régir la collecte et le traitement des informations personnelles, dans les secteurs tant public que privé. Un organisme, ou un commissaire à la protection des données, se consacre à coordonner les actions de veille et de contrôle en ce sens, afin d'assurer l'application, et parfois la modernisation des lois. Globalement, ces organismes de contrôle manqueraient de moyens pour mener au mieux leur tâche (Privacy International, 2006). Ce modèle est celui de la France par exemple, dans laquelle la CNIL assure un travail d'information, d'analyse des enjeux, mais aussi de contrôle des fichiers et d'instruction des plaintes notamment. C'est aussi le modèle de l'Union Européenne.

Ces deux grands modèles, s'ils permettent de comprendre dans les grandes lignes les types de cadre réglementaires, sont cependant modulables. Ainsi, par exemple, certains pays recourent à des lois sectorielles en complément d'une réglementation générale, afin de préciser les formes de protection pour certaines catégories d'information, comme les télécommunications, ou les fichiers de police (Privacy International, 2006). D'autres différences se font jour dans la conception de comment protéger les individus. Mais au-delà de l'encadrement réglementaire, d'autres formes de régulation existent, en remplacement ou en complément de celui-ci.

3.3. L'auto-régulation

Si l'encadrement réglementaire apparaît incontournable, certaines formes d'auto-régulation existent. C'est par exemple le cas lorsque les entreprises du secteur privé décident de travailler ensemble à la définition de règles de respect de la vie privée. Dans le cas des données personnelles, le développement de telles formes de régulation semble assez récent, si bien qu'il est un peu tôt pour en évaluer les effets (M. Rotenberg¹³, 2001). Comparant l'approche américaine à l'approche européenne, M. Rotenberg estime ainsi les Etats-Unis ont laissé de côté le secteur privé. Il note cependant que les entreprises ont amorcé le débat, au travers de quelques efforts d'auto-régulation. Mais malgré les quelques efforts qu'il constate, M. Rotenberg se montre sceptique quant aux effets positifs à moyen et long terme de l'auto-régulation comme unique mode de régulation du secteur privé. Il s'inquiète en particulier du risque de redéfinition de la notion de « privacy », et de la capacité de la FTC à agir comme une agence fédérale pour la « privacy ».

Si l'auto-régulation seule, comme le suggère M. Rotenberg, semble à la fois insuffisante et imparfaitement crédible, parfois cette approche se développe en complément d'un cadre légal : on parle alors de co-régulation. De tels modèles mixtes ont ainsi été adoptés au Canada, ou en Australie. Dans ce cas, le secteur privé développe certaines règles, qu'elle applique en accord avec l'agence nationale pour la protection de la vie privée (Privacy International, 2006). Cette solution apparaît ainsi plus riche que la seule auto-régulation. Elle a l'avantage d'impliquer le secteur entrepreneurial dans le respect des données personnelles,

¹³ Juriste et Directeur exécutif de l'EPIC – Electronic Privacy Information Center

tout en permettant aux individus d'accorder une certaine crédibilité à des règles validées par une agence nationale.

3.3. De la mobilisation sociale à la responsabilité individuelle

3.3.1. La mobilisation des acteurs sociaux comme facteur de régulation

Si l'on conçoit difficilement de se passer d'un encadrement légal, celui-ci n'existe pas hors du contexte social. En France, la loi Informatique et Libertés de 1978 doit son existence au scandale SAFARI. Sans revenir en détails sur SAFARI, déjà largement traité (A. Vitalis, 1981), rappelons que c'est un article du quotidien *Le Monde* qui a déclenché l'affaire, des suites de laquelle une réflexion a été mise en place, aboutissant à la loi de 1978. Il serait présomptueux d'affirmer que sans l'affaire SAFARI, la France ne se serait pas dotée d'une loi Informatique et Libertés. Mais ce cas a permis de comprendre l'importance d'une mobilisation, ici des médias, et l'impact effectif que cela peut avoir.

Des formes de mobilisation sociale, aussi, s'efforcent de se faire entendre. Aux Etats-Unis, l'Organisation Non Gouvernementale CASPIAN¹⁴ en est une illustration. Structure auto-financée, elle a été créée en 1999 pour lutter en particulier contre les intrusions commerciales dans la vie privée. Nous retiendrons ici les affaires Benetton et Gilette, qui ont conduit CASPIAN à proposer un projet de loi fédérale.

L'affaire Benetton déclenche la réaction de CASPIAN en 2003. Le 11 mars 2003, un communiqué émanant de Philips Electronics met le feu aux poudres, en annonçant que des puces RFID ont été vendues à Benetton : « La ligne de vêtements Sisley, de Benetton, contiendra des identifiants par radio ondes de Philips Electronics, qui remplaceront les codes barres que l'on doit scanner manuellement¹⁵ ». Suite à cette annonce, CASPIAN lance un appel au boycott de Benetton, et établit à cet effet un site Internet spécifique : www.boycottbenetton.com¹⁶. CASPIAN exige un renoncement public, de la part de Benetton. Par ailleurs, la structure milite en faveur de la création d'un label, afin que les consommateurs soient systématiquement prévenus de la présence d'une puce RFID dans les produits qu'ils achètent. La désactivation, aussi, fait partie des attentes de CASPIAN : « pour que la traçabilité des produits ne soit pas synonyme de flicage des consommateurs, il faut absolument que les puces radio soient désactivées à la sortie des magasins ou que les clients aient un moyen de les détruire définitivement » (A. Piquard, 17/09/2003). Le 04 avril, le groupe Benetton publie un communiqué de presse par lequel il affirme que, contrairement à ce que différents articles de presse ont rapporté, il n'y a pas d'étiquettes intelligentes dans les vêtements produits et vendus par le groupe, y compris dans la ligne Sisley (qui était incriminée). Ce communiqué indique prudemment que Benetton travaille sur la technologie RFID pour en évaluer les caractéristiques techniques, mais que « aucune étude de faisabilité n'a été entreprise en vue d'une possible introduction industrielle de cette technologie ». Mais

¹⁴ Consumers Against Supermarket Privacy Invasion and Numbering: <http://www.nocards.org>

¹⁵ Source : 11/03/2003, « Benetton clothing to carry tracking transmitters ».

<http://archives.tcm.ie/breakingnews/2003/03/11/story91318.asp> (visité le 07/12/2006).

¹⁶ On pourra noter que les RFID sont un cas intéressant, car elles peuvent créer des tensions diversifiées. Si la réaction est moins importante dans le cas du transport, la sensibilité dans le cas présent est vive, au point que les individus se sentiraient moins exposés dans leur vie privée en vivant nus (« rather go naked »), qu'en vivant avec des objets dotés de puces RFID...

Benetton se réserve aussi « de prendre la décision la plus appropriée pour générer le maximum de valeur pour ses actionnaires et ses clients¹⁷ ».

Le résumé de ces faits témoigne de la réaction relativement rapide de Benetton, laquelle est assez mal vécue dans le secteur industriel, la réaction du groupe étant perçue comme un pas en arrière : « au lieu de donner des réponses, ils se sont dérobés de leur engagement. C'est un pas en arrière pour l'industrie des RFID » (E. Batista, 08/04/2003). Cette réaction de Benetton, même si elle ne donne aucune garantie pour l'avenir, vise cependant à faire lever le boycott. Et CASPIAN se dit satisfait de ce recul annoncé publiquement.

La même année, CASPIAN dénonce Gillette, qui aurait testé « dans un supermarché anglais un nouveau procédé permettant de photographier chaque client prenant dans un rayon un paquet de lames de rasoir Gillette Mach3 » (T. Dupont, 21/08/2003). Outre l'aspect intrusif du procédé, l'ONG reproche à Gillette de n'en avoir rien dit. La réaction ne se fait pas attendre, et, comme pour Benetton, CASPIAN lance un appel au boycott, et ouvre le site www.boycottgillette.com. Gillette ne réagit pas aussi clairement et promptement que Benetton, aussi CASPIAN ne lève pas son appel au boycott. Le 14 août 2003, pourtant Gillette se montre plus conciliant, annonçant dans un article du Financial Times que l'entreprise renonce « pour au moins 10 ans à tout procédé permettant de tracer individuellement chacun de ses produits. Jusqu'en 2013, Gillette dit vouloir se contenter d'implanter des puces électroniques dans ses palettes et ses cartons de lames de rasoir pour en suivre l'acheminement, depuis l'usine jusqu'au magasin » (T. Dupont, 21/08/2003).

Suite à ces deux affaires, CASPIAN travaille à un projet de loi, le « RFID Right to Know Act of 2003¹⁸ », rendu public le 17/06/2003. Pourtant, aux Etats-Unis, d'après A. Piquard (24/06/2003) : « il est assez rare que des membres de la société civile écrivent des projets de loi. D'habitude, les ONG réagissent a posteriori aux textes écrits par les parlementaires ». Ce projet place CASPIAN en situation de faire du lobbying, afin de faire discuter sa loi (E. Grossman, 2005). Ce projet de loi vise à combler l'absence de régulation juridique pour le secteur privé américain, et demande, en plus du "droit de savoir", des garanties sur les conditions de collecte d'informations par les entreprises (A. Piquard, 24/06/2003). Katherine Albrecht¹⁹ explique que CASPIAN demande « un moratoire mondial sur cette technologie, parce qu'elle a été développée dans le secret le plus total, sans aucun avis des consommateurs et des citoyens. Aux Etats-Unis, nous préparons un projet de loi sur la question, qui propose le moratoire et prévoit au minimum une labellisation obligatoire signalant qu'un produit contient une étiquette intelligente. Nous le rédigeons avec l'aide d'une université et comptons le transmettre au Congrès américain d'ici un mois. [...] Nous prenons le problème en amont pour arrêter les étiquettes intelligentes avant qu'elles ne deviennent ce que sont maintenant les OGM : un état de fait » (A. Piquard, 27/03/2003).

La mobilisation de CASPIAN, si elle n'a pas encore produit tous les effets escomptés, témoigne de l'importance de la mobilisation sociale comme facteur de régulation. Car si l'ONG a du mal à imposer sa loi, elle a cependant réussi à toucher deux importants acteurs industriels. Les actions d'appel au boycott mené, avec les sites Internet, étaient accessibles dans le monde entier, ce qui pouvait nuire grandement aux deux marques concernées. Ces dernières se sont rétractées... au moins pour l'instant. Face à toute la mobilisation que s'est efforcée de lancer CASPIAN, les résultats peuvent sembler minces, étant donné que malgré ce recul, Benetton et Gillette se sont tous deux prononcés sur le futur proche, ne s'engageant pas sur un terme plus long. Mais la mobilisation sociale exposée ici a abouti à faire exister, au

¹⁷ Archives du site Internet de Benetton.

¹⁸ <http://www.nocards.org/rfid/rfidbill.shtml>

¹⁹ Directrice de CASPIAN.

moins un petit peu, une position que ni les industriels ni les politiques ne tenaient en considération. Elle a aussi permis à CASPIAN, en tant qu'acteur social, de se positionner comme acteur de régulation.

3.3.2. Des formes de régulation à la portée des usagers

Au-delà de l'encadrement juridique, et de la mobilisation sociale, il apparaît important que les individus se saisissent aussi, à leur niveau, de certaines formes de régulation. Nous l'avons compris avec l'enjeu de contrôle de l'information. La technologie, largement présentée comme une menace pour la vie privée, fait désormais partie de notre quotidien, et nous apporte un confort certain. Aussi est-il important d'apprendre à composer avec elle. Car des solutions peuvent être mises en place, qui permettraient de donner davantage de contrôle aux usagers : « l'apparition des services de regroupement d'identifiant est un des indices qui tendent à montrer que l'on est passé d'une logique de protection/interdiction à une logique de maîtrise de la diffusion de "ses" données personnelles » (D. Kaplan, A. Belleil, 2004).

La technologie elle-même peut donner aux usagers les moyens d'exercer leur droit à la « privacy », par le contrôle de l'information, exposé précédemment. Ainsi dans le cas des puces RFID, par exemple, des solutions pourraient être trouvées pour que l'utilisateur puisse d'une part savoir dans quelles circonstances les puces RFID disséminées sur les objets qu'il porte sont lues (par quel lecteur, pourquoi, quand), et d'autre part qu'il puisse se déconnecter lorsqu'il le souhaite, ce qui répond au droit à être laissé tranquille. « Dataprivatizer », par exemple, permettrait à l'utilisateur de repérer les puces RFID : cet appareil « jouerait le rôle d'un lecteur de puces RFID, dans une version simplifiée et accessible » (A. Piquard, 18/11/2003). De la même façon, le logiciel PGP²⁰, accessible gratuitement, permet aux utilisateurs de procéder au cryptage de leurs e-mails et fichiers (EFF²¹, 2002).

Ces solutions techniques sont globalement nommées « PETs » ou « Privacy Enhancing Technologies ». Elles visent à permettre aux utilisateurs de disposer eux-mêmes d'outils pour protéger leurs données, leur vie privée. Ainsi des logiciels de cryptographie, d'anonymisation peuvent-ils être téléchargés gratuitement, ou achetés. Cependant, les PETs ne sont pas encore très largement diffusées, notamment en raison de leur trop grande complexité pour nombre d'utilisateurs (Bohn et al., 2004).

De telles solutions, on le comprend, n'enlèvent rien aux entreprises, dont l'argumentaire repose sur la réduction des coûts, la traçabilité logistique, mais aussi la lutte contre le vol, et les nouvelles possibilités de fidélisation que la technologie RFID permet d'envisager. Cependant, il convient d'être prudent quant à leur diffusion, car elles tendent à mettre entre les mains des seuls utilisateurs, face aux entreprises, la charge de la protection de la « privacy » (Bohn et al., 2004). En prenant certaines précautions, il semble que la « privacy » puisse devenir une forme « d'utilité » par laquelle les utilisateurs pourraient se protéger eux-mêmes de sollicitations non désirées, et pourraient se prévaloir concrètement du droit à être laissé tranquille (A. Gow, 2005).

CONCLUSION

²⁰ Pretty Good Privacy.

²¹ Electronic Frontier Foundation

Ainsi, la « privacy » constitue un analyseur intéressant pour comprendre les formes de régulation s'opérant autour des TICs. Régulation juridique, régulation sociale ou technique, il apparaît cependant qu'aucune de ces formes n'est suffisante en elle-même. Cela s'explique pour partie du fait de la diffusion constante d'innovations, qui peut faire émerger de nouveaux enjeux, ou mettre l'accent sur certaines failles. Ainsi, par exemple, la question de la temporalité se posera de plus en plus vivement : que deviennent les traces de connexions, mais aussi les traces volontaires comme un blog par exemple, après le décès d'une personne ? Que deviennent les fichiers d'une entreprise lorsque celle-ci fait faillite ? Et comment gérer le fait que ce qu'un usager peut avoir écrit sur un forum cinq ans auparavant peut toujours être lu et associé à lui, alors que cet usager a pu changer, qu'il peut ne pas vouloir se définir ainsi, ni se souvenir de tout ? Qu'en est-il, alors, du droit à l'oubli ? L'ensemble de ces interrogations, et bien d'autres encore, devront trouver des réponses, des formes de régulation, car elles défient une « privacy » à la définition encore vaste.

Au regard de l'analyse portée sur la notion de « privacy », et sur son axe majeur qu'est le contrôle de l'information, l'on constate que se mêlent bien souvent diverses formes de régulation. Leur complémentarité tient à la nécessité de combler certaines lacunes, comme on l'a vu dans le cas de CASPIAN, qui par sa capacité de mobilisation en tant qu'acteur social s'efforce de construire une réglementation complémentaire. Mais cette complémentarité semble tenir aussi au fait que ces diverses formes de régulation agissent à différentes échelles (D. Desjeux, 2004), chaque niveau d'action étant nécessaire à la protection du « privé ».

BIBLIOGRAPHIE

BELLEIL A. (2001), « E-Privacy. Le marché des données personnelles : protection de la vie privée à l'âge d'Internet », Paris, Dunod.

BOHN J., COROAMA V., LANGHEINRICH M., MATTERN F., ROHS M. (2004), *Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing*, Institute for Pervasive Computing, ETH Zurich.

DECEW J. W. (2006 –1^{ère} publication 2002), *Privacy*. Source : <http://www.plato.stanford.edu/entries/privacy/> (visité le 17/10/2006).

« Déclaration universelle des droits de l'homme, adoptée le 10/12/1948 à Paris par l'assemblée générale des nations unies », in Journaux Officiels (2002), *Le respect de la vie privée*, Paris, Edition des journaux officiels, coll. « La loi au quotidien ».

DESJEUX D. (2004), *La consommation*, Paris, PUF, coll. « Que sais-je ? ».

DUBEY G., GUCHET X., CRAIPEAU S. (2004), *La Biométrie. Usages et représentations*, Rapport INT – Cetcopra, Projet incitatif GET 2003.

EFF (2002), *Les 12 conseils de l'EFF pour protéger votre vie privée en ligne*. Source : http://www.bugbrother.com/eff/eff_privacy_top_12.html (visité le 11/07/2006)

GOW G. A. (2005), *Privacy and Ubiquitous Network Societies*, International Telecommunication Union Workshop, 6-8 April 2005. Source : <http://www.itu.int/ubiquitous> (visité le 17/05/2006).

GROSSMAN E. (dir. – 2005), « Lobbying et vie politique », in *Problèmes politiques et sociaux*, n° 918 de novembre 2005, Paris, La Documentation Française.

KAPLAND., BELLEIL A. (2004), *Confiance et sécurité dans les réseaux*, FING.

KYNDT T. (15/05/2006), « De la FRID à un "Internet d'objets". Et notre vie privée ? », in *Du côté des consommateurs*, n° 201. Source : <http://www.oivo-crioc.org/textes/1687.shtml> (visité le 12/10/2006).

LANCELOT MILTGEN C. (2002), *Vie privée et Internet*, Mémoire de DEA (Dir. P. VOLLE), Université Paris Dauphine.

LEMARTELEUR X. (2004), *Traçabilité contre vie privée : les RFIDs ou l'immixtion des technologies dans la sphère personnelle*, Mémoire de DESS « Droit du multimédia et de l'informatique », Université Paris II – Panthéon Assas.

MONOT P., SIMON M. (1998), *Habiter le cybermonde*, Paris, Editions de l'Atelier/Editions Ouvrières.

POTTS C., TECH G. (2001), *What is Privacy?*, NCSU Presentation. Source : http://www.theprivacyplace.org/presentations/ncsu01_slides.pdf (visité le 21/05/2006).

POULLET Y., (2005), « Pour une troisième génération de réglementations de protection des données », in *Jusletter* du 03 Octobre 2005. Source : <http://www.privacyconference2005.org/fileadmin/PDF/poullet.fr> (visité le 09/10/2006).

Privacy International (29/10/2006), « Overview of Privacy », in *Privacy and Human Rights 2005*, Rapport 2005. Source : [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-543673](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673) (visité le 08/11/2006)

ROTENBERG M. (01/03/2001), *Privacy in the Commercial World*, U.S. House of Representatives. Source : http://www.epic.org/privacy/testimony_0301.html (visité le 13/12/2006).

ROY (2006), *Privacy Law*, Reading for the Faculty of Piercelaw. Source : <http://www.faculty.piercelaw.edu/roy/06PrivacyLaw/Reading%208-22.doc> (visité le 11/07/2006).

SERRES A. (2002), *Quelle(s) Problématique(s) de la trace ?*, Communication, Séminaire du CERCOR du 13/12/2002.

VINCENT G. (1987), « Secrets de l'histoire et histoire du secret », in ARIES P., DUBY G. (dir.), *Histoire de la vie privée. De la Première Guerre mondiale à nos jours*, Paris, Seuil, coll. « L'Univers Historique », p. 157-1999.

VITALIS A. (1981), *Informatique, Pouvoir et Libertés*, Paris, Economisa, Coll. « Politique Comparée ».

WARREN S., BRANDEIS L. D. (1890), « The Right to Privacy », in *Harvard Law Review*, n°4, p. 193-220. Source <http://www.louisville.edu/library/law/brandeis/privacy.html> (visité le 13/11/2006).

Articles de presse Internet

BATISTA E. (08/04/2003), « Step Back for Wireless ID Tech? », in *Wired.com*. Source: www.wired.com/news/wireless/0,1382,58385,00.html (visité le 07/12/2006)

BATISTA E. (12/03/2003), « What Your Clothes Say About You », in *Wired.com*, Source : <http://www.wired.com/news/wireless/0,1382,58006,00.html> (visité le 07/12/2006)

DEVILLARD A. (09 mars 2005), « Le billet électronique Navigo prend la Carte Orange », in *01net*

DUMOUT E. (28/12/2004), « Cartes Navigo: cinq euros pour ne pas figurer dans un fichier commercial », in *ZDNet France*. Source : <http://zdnet.fr/actualites/telecoms/0,39040748,39195591,00.htm> (visité le 20/03/2006)

DUPONT T. (07/10/2003), « La Cnil s'inquiète du fichage dans les transports en commun », in *ZDNet France*. Source : <http://zdnet.fr/actualites/internet/0,39020774,39125887,00.htm> (visité le 18/05/2006).

DUPONT T. (21/08/2003), « Gillette renonce à fliquer les acheteurs de rasoirs. Les défenseurs de la vie privée en ont encore le poil hérissé », in *Transfert.net*. Source : <http://www.transfert.net/Gillette-renonce-a-fliquer-les> (visité le 07/12/2006)

GUILLAUD H. (07/09/2006), « A qui appartient mes logs ? », in *Internetactu.net*, Source : <http://www.internetactu.net/?p=6549> (visité le 09/09/2006).

PIQUARD A. (18/11/2003), « Des solutions pour protéger la vie privée du consommateur face aux "étiquettes intelligentes" », in *Transfert.net*. Source : <http://www.transfert.net/i9593> (visité le 10/08/2006)

PIQUARD A. (24/06/2003), « Une ONG américaine propose une loi pour encadrer les codes-barres du futur. Pour défendre la vie privée, il faut de l'étiquette dans l'étiquette », in *Transfert.net*. Source : <http://www.transfert.net/a9022> (visité le 07/12/2006)

PIQUARD A. (27/03/2003), « Benetton est socialement irresponsable », in *Transfert.net*.
Source : <http://www.transfert.net/Benetton-est-socialement> (visité le 07/12/2006)

TREGUIER C. (12/11/2002), « Moneo, Navigo, Calypso: cartes à puces en quête de respectabilité », in *ZDNet France*. Source : <http://zdnet.fr/actualites/telecoms/0,39040748,2125770,00.htm> (visité le 17/11/2006)

ZDNet (10/05/2006), « La carte orange passe à l'ère électronique avec Navigo », in *ZDNet France*. Source : <http://zdnet.fr/actualites/informatique/0,39040745,39347738,00.htm> (visité le 17/11/2006)