L'insécurité numérique au quotidien : de la régulation quotidienne aux logiques d'alertes

REY Bénédicte

France Telecom R&D
Laboratoire SENSE
38-40 rue du General Leclerc
92130 Issy les Moulineaux

Résumé : Avec le développement de « l'informatique ambiante », les technologies de l'information et de la communication sont de plus en présentes dans notre quotidien. Nos actes, même les plus banals, laissent alors de multiples traces de notre passage, de notre identité, de nos préférences, de nos habitudes, et cette diffusion du numérique exacerbe les préoccupations relatives à la préservation de la vie privée et de l'intimité des usagers. La question se pose alors de savoir si une forme d'insécurité numérique accompagne les individus dans leurs usages quotidiens. Au travers de l'analyse d'un matériau composé d'entretiens et d'un corpus documentaire, il s'agira d'explorer cette question, en s'interrogeant sur les représentations qui peuvent affecter les individus, et en analysant les stratégies de régulations des risques qui se mettent en place, tant au niveau des usages quotidiens, qu'à un niveau plus large, autour de logiques d'alerte.

Mots clés : insécurité numérique – vie privée – régulation des risques

Résumé : The development of ubiquitous computing gives information and communication technologies more and more significance in our everyday lives. Even ordinary acts leave lots of tracks of one's presence, of one's identity, of one's preferences and habits, and the spreading of digital services sharpens privacy concerns. Thus, do users feel that they are living within a kind of digital insecurity? This question is explored through the analysis of a material composed of interviews and of a documentary corpus. Representations that affect individuals, but also strategies of risks' regulation are analysed, starting with observing everyday uses, and then questioning how alerts are given, and what consequences may occur.

Mots clés : digital insecurity – privacy – risk's regulation

« La société de l'information est devenue une société de l'informatique, ce qui a bouleversé l'antique relation entre l'individu et les renseignements auxquels il a accès ou qui le concernent », constate Rigaux [2002]. C'est cette relation des individus aux informations qui les concernent que nous nous proposons d'interroger ici, sous l'angle de la question plus particulière de l'insécurité numérique, et des risques pour la vie privée à l'heure du numérique. Il s'agira ainsi de s'intéresser aux grandes représentations qui habitent les usagers, aux formes de tensions perçues, mais aussi aux tensions vécues, à différentes échelles micro-sociale, méso-sociale et macro-sociale [Desjeux 2006 ; 2004]. Nous nous efforcerons ce faisant d'appréhender les formes de régulation des risques, et de normalisation, qui peuvent prendre place, depuis les usages quotidiens, jusqu'à l'étude de controverses et de logiques d'alerte.

Nous nous appuierons pour ce faire sur un matériau composite. Deux enquêtes de terrain sont ici mobilisées : d'une part, une enquête qualitative par entretiens semi-directifs, menée par France Telecom R&D auprès de 36 personnes dans le cadre de leurs usages domestiques des TIC[1] ; d'autre part, un terrain qualitatif exploratoire mené par entretiens qualitatifs semi-directifs, auprès de 19 personnes (usagers dans leur cadre professionnel ; professionnels ; experts). Par ailleurs, l'étude d'un certain nombre d'affaires, ainsi que l'analyse de forums de discussion font partie du matériau exploité.

1. Les traces numériques, une forme d'insécurité ?

1.1. Les traces numériques : des données anodines ou une source d'insécurité ?

A l'ère numérique, à l'heure de l'usage courant des TIC et du développement de l'informatique ambiante, de multiples traces numériques liées à nos usages sont générées. Ces traces qui peuvent être invisibles, qui sont souvent mal identifiées par les usagers, peuvent être à l'origine de certaines craintes, parfois fantasmées, et parfois plus concrètes et liées aux risques de dévoilement de données privées par exemple, ce que notent P. Monot et M. Simon [2002] : « 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 finalement anodines, ou portent-elles le risque, comme bien des textes le soulignent de façon parfois alarmiste, de menacer notre vie privée et nos libertés individuelles ? Ces traces sont-elles source d'une forme d'insécurité numérique, rendent-elles les individus plus vulnérables ? 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'usager laisse derrière lui : « le premier sens de la trace est donc bien l'empreinte, qu'elle soit matérielle ou morale » [Serres 2002]. Cet auteur estime que la trace fait sens au regard de son contexte d'existence et d'utilisation.

[1] Technologies de l'information et de la communication.

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 de fait 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'ampleur. Aujourd'hui, les traces sont multiples, les fichiers de données sont nombreux, et les capacités de traitement de telles informations sont accrues. Elles peuvent être conscientes ou inconscientes, volontaires ou involontaires, lointaines (dans le réseau) ou rapprochées (sur l'ordinateur domestique par exemple) [Boyer 2000]. Dans un tel contexte, la question de la vulnérabilité des individus, et de l'insécurité qu'ils peuvent ressentir ou expérimenter en lien avec les traces numériques que leurs usages des TIC génèrent apparaît être un enjeu crucial, que nous nous proposons d'explorer ici.

1.2. Une insécurité perçue

1.2.1. De quelques grandes représentations autour de l'insécurité numérique…

La question se pose en effet de savoir ce que signifie, dans la vie quotidienne des usagers, les notions de sécurité ou d'insécurité numérique. La notion de sécurité est définie par le dictionnaire[2] comme la « confiance, [la] tranquillité d'esprit résultant de la pensée qu'il n'y a pas de péril à redouter ». Les résultats issus des deux terrains d'enquêtes exploités témoignent de ce que la confiance des usagers quant à l'usage qui peut être fait de leurs traces est toute relative, tout comme leur « tranquillité d'esprit ».

L'une des grandes représentations, partagée par une large part des usagers rencontrés, fait apparaître la figure de « big brother ». Traiter des questions d'informatique et de vie privée fait en effet émerger une grande inquiétude, mêlée de certitude, quant à la surveillance possible des outils de communication. Elle peut être vécue sur le mode d'un malaise et d'un risque latents, comme en témoigne cet extrait d'entretien au sujet de la vidéosurveillance : « Dans l'absolu c'est toujours gênant de se sentir filmée, je veux dire dans le métro c'est pareil, tu as des caméras partout […] c'est le truc de Big Brother, je veux dire, j'ai rien inventé… Le problème c'est qu'il faut y penser, après je pense que tu peux l'oublier assez facilement, mais dès que t'y penses un peu oui, c'est gênant. […] Ça me dérangerait s'il y avait des caméras à la fois dans le métro, dehors, dans mon immeuble, plus dans mon bureau… Oui, ça m'embêterait. J'aurais pas envie qu'on puisse me tracer… parce que c'est atteinte à ma liberté, à mon autonomie[3] ! » [Aline, 29 ans, en couple, chargée de mission en urbanisme]. Parmi les personnes rencontrées, nombreuses sont celles qui ne disposent, somme toute, que d'une connaissance limitée des types de traces laissées par leurs usages, et de ce qui peut en advenir. Pourtant, la conviction d'être surveillé, ou de pouvoir être surveillé, est omniprésente, et s'accompagne d'une crainte de contrôle généralisé opéré par la puissance publique.

Mais si une telle représentation reste très présente, se constituant en grande peur gênante mais somme toute vivable, on constate cependant que la crainte des utilisateurs de nouvelles technologies se porte aussi vers un autre type d'acteur que sont les entreprises. La crainte de voir les données générées tant par le commerce électronique que par l'utilisation de la messagerie exploitées à des fins marketings et commerciales est en effet marquée. Au premier rang des entreprises mises en cause, les personnes rencontrées citent ainsi les FAI[4], mais

---

2 *Dictionnaire des noms communs*. Larousse, Paris, 1972.

3 Terrain qualitatif, B. Rey.

4 Fournisseurs d'Accès à Internet

également les fournisseurs de messagerie, et en particulier les grands groupes tels que Google, Yahoo ou Microsoft. Les pratiques des entreprises à l'égard des fichiers de donnée sont mises en cause dans les entretiens exploités. Si telles pratiques existent, il est intéressant de noter que celles-ci restent difficiles à observer, étant donné que les entreprises gardent pour elles le trésor de leurs fichiers et de leurs méthodes. Les utilisateurs n'en ont pas moins la certitude d'être observés, tracés, et cela est vécu comme une gêne et comme une menace pour leur vie privée.

Cette grande représentation vient se juxtaposer à la première, sans la faire disparaître. Si un certain déplacement s'est opéré [Castells 1998 ; Armatte 2001], ces deux grandes peurs de voir des risques de manipulation et d'invasion de la vie privée se concrétiser restent présentes, accompagnant de manière diffuse les usagers au quotidien. Une autre grande peur vient également se surajouter à cela, qui est liée à la technologie et à ses potentialités réelles ou fantasmées [Duclos 1989]. Face à des progrès techniques rapides, et au développement de l'informatique omniprésente, les usagers ressentent comme un risque cette diffusion de moins en moins visible des outils de communication. Le sentiment de ne pas avoir de contrôle sur la multiplication des échanges de données, ainsi que sur le devenir de toutes les informations générées, tend ainsi à renforcer une forme d'insécurité, de méfiance globale à l'égard de la technologie, et des possibilités de surveillance et de nuisance qui lui sont prêtée.

1.2.2. ...Renforcées par des affaires médiatisées

Si ces grandes représentations sont parfois taxées de n'être que des formes de fantasmes exagérés, il apparaît que certaines affaires viennent renforcer le sentiment de vulnérabilité lié à la dissémination des traces d'usage. Ces affaires sont parfois médiatisées, devenant des histoires collectives qui ont force d'argument pour ceux, individus ou groupes plus actifs, qui en appellent à une vigilance accrue.

L'affaire AOL en est un exemple. En août 2006, une équipe d'AOL Research a mis en ligne par erreur, avant de le retirer très vite, « un document contenant des millions de données sur les recherches effectuées par ses utilisateurs américains (concernant quelques 685 000 internautes ayant effectué quelques 20 millions de requête sur les mois de mars, avril et mai 2006)[5] ». Mais ce fichier mis en ligne par erreur a été téléchargé de nombreuses fois, et a fait l'objet d'exploitations de la part tant de chercheurs, qui n'ont pas si souvent accès à de telles données, que par des internautes. Le site www.aolsearchdatabase.com permet ainsi à tout visiteur de faire des recherches dans ces données d'utilisateurs. Si certains internautes réagissent, suite aux articles publiés sur cette affaire, en estimant que le rapprochement de données de recherche ne permet pas de caractériser une personne, et ne constitue pas un risque, une majorité de réactions s'inquiète de ce qu'une telle erreur dévoile. « L'utilisatrice 11110859 à New York, le 7 mars, a recherché des "fringues hip-hop". Le 26, elle a cherché "perdre sa virginité" avant de s'interroger pendants plusieurs semaines pour savoir si on "pouvait tomber enceinte même après avoir eu ses règles". Quelques temps plus tard, elle s'interroge à nouveau "pourquoi les gens font-ils du mal aux autres ?". Le 19 mai, elle demande : « comment aimer quelqu'un qui vous maltraite ?", "que dit Jésus à propos d'aimer ses ennemis ?". Ensuite, elle demandera encore "la direction de la prison de New York" avant de demander au moteur "quels objets a-t-on le droit d'y apporter ?[6]" ».

Cette reconstitution d'un profil témoigne du degré important d'exposition des usagers, et du risque, pour leur intimité, lorsque de telles données sont collectées. Si AOL a présenté des excuses pour cette erreur, et si plusieurs personnes ont été remerciées par l'entreprise en signe

---

[5] GUILLAUD, H. : *A qui appartiennent mes logs ?*. 07/09/2006. Source : http://www.internetactu.net/?p=6549 (visité le 09/09/2006).

[6] GUILLAUD, H. : op cit.

de repentance, certains des usagers concernés ont choisi d'engager une action à son encontre. L'affaire AOL s'est ainsi constituée en histoire collective témoignant de ce que les traces d'usage peuvent menacer l'intimité des individus, en révélant des informations précises. Les usagers peuvent être caractérisés par l'analyse de leurs recherches, quand bien même leur nom resterait inconnu.

Une telle affaire contribue à faire exister un sentiment d'insécurité pour les usagers, qui tendent à livrer en toute confiance, depuis leur poste, leurs interrogations relatives tant à des sujets anodins qu'à des questions très personnelles. Qu'il s'agisse d'erreurs ou d'une supposée malveillance des entreprises, il apparaît ainsi que les individus utilisent les TIC dans un environnement latent de méfiance et d'insécurité, nourri tant par de grandes représentations que par les affaires médiatisées.

1.3. Insécurité numérique et régulation des risques perçus : la « confiance assurée »

Les traces d'usage, qui touchent à la vie privée, ont une valeur certaine pour les entreprises, mais aussi pour les pouvoirs publics. Mais elles ont aussi une grande valeur pour les usagers, dans la mesure où elles parlent d'eux, de leur identité, mais aussi de leurs préférences commerciales, de leurs centres d'intérêts, de leurs habitudes… C'est en ce sens que les données générées par l'usage d'outils numériques peuvent devenir une source de risque pour les individus, du point de vue notamment de la préservation de leur vie privée.

Alors comment expliquer que les usagers, malgré les risques qu'ils perçoivent, utilisent les TIC ? D'une part, si ces grandes peurs sont largement partagées, tous les usagers ne les appréhendent pas de la même manière. Deux positions se distinguent nettement, lors de l'analyse des entretiens réalisés et des contributions consultables sur les forums de discussion. L'un des types de réactions rencontré fait état d'une préoccupation latente mais manifeste connectée à ces grandes représentations. Mais un autre type de réaction, qui s'oppose souvent à la première en la taxant d'être rétrograde ou conservatrice, tend à privilégier le fait de vivre avec la modernité, et à ne pas se sentir menacé par les formes de surveillance politique ou commerciale qui accompagneraient les usages. Une forme de tyrannie de la transparence, pour imiter la formule de Sennet, semble alors émerger, autour de l'idée que celui qui n'a rien à se reprocher n'a rien à craindre, quand bien même il serait en effet surveillé. Une telle approche est bien connue des défenseurs de la vie privée et des libertés publiques, qui estiment qu'il faut s'entendre sur les normes sociales et juridiques au regard desquelles on évaluera ce qu'il y a ou non à se reprocher, comme l'illustre bien le débat autour du peer to peer.

D'autre part, les grandes représentations évoquées, ainsi que certaines des affaires qui font grand bruit, interviennent à un niveau difficilement palpable pour les usagers, mobilisant des périodes de l'histoire passée, se déroulant dans une autre ère géographique… Le risque pour la vie privée est perçu, mais de façon latente, diffuse. Et si l'individu contemporain souhaite éviter ce risque, quelle alternative s'offre à lui, sinon éviter l'usage des TIC, ce qui n'est pas chose aisée aujourd'hui. L'usager peut refuser de se rendre en certains lieux s'il ne souhaite pas que des caméras de surveillance le filment ; il peut, aussi, choisir un autre moyen de transport s'il ne veut pas souscrire à une application télébilletique ; il peut, encore, éviter l'usage de l'Internet. Mais l'on s'aperçoit bien vite qu'une telle alternative est contraignante, voire impossible à mettre en place, notamment dans le cadre de travail. L'usager doit, d'une certaine façon, accorder une forme de confiance, proche de la « confiance assurée » de Luhmann [2001], pour mener nombre de ses activités quotidiennes à l'ère numérique. Pour Luhmann en effet, on ne peut vivre sans former des attentes par rapport aux événements contingents, et on doit, dans une certaine mesure, s'abstenir de tenir compte de la possibilité

que ces attentes soient déçues. La « confiance assurée », pour Luhmann, prend place notamment lorsqu'aucune alternative n'est aisément envisageable, auquel cas l'individu tend à placer une forme de confiance dans le fonctionnement global du système en place.

Mais cette forme de confiance, et l'esprit de fatalisme qui peut sembler l'accompagner, ne doivent cependant pas occulter le fait que peuvent se mettre en place des stratégies de régulation des risques perçus, à différents niveaux.

2. Des stratégies de régulation des risques au niveau des usages quotidiens

2.1. La régulation des risques par des stratégies d'arbitrage : la « confiance décidée »

Si les usagers peuvent difficilement, aujourd'hui, se passer totalement des TIC, et ainsi éviter totalement les risques qu'ils y associent, il apparaît qu'ils conservent une marge de manœuvre et de choix, ce dont témoignent les terrains d'enquêtent analysés. Ainsi, dans le cas de formulaires à remplir, des stratégies d'arbitrage se mettent en place, qui visent à limiter les risques. A l'exception des cas de démarches officielles, ou professionnelles, la plupart des usagers adoptent une stratégie de remplissage minimaliste des formulaires lorsqu'ils souhaitent accéder à un service. Cette stratégie est justifiée par le fait de limiter ainsi les données personnelles diffusées. Mais lorsqu'il s'agit d'accéder à un service par simple curiosité, en retour duquel rien de suffisamment important n'est attendu, nombre d'usagers remplissent alors les formulaires de fausses informations : « Je sais que quand on met son nom sur la toile, après, ça reste gravé en fait, avec tout ce que tu as écrit et tout donc… je mets mon nom juste pour quelque chose de pertinent qui m'intéresse et qui… et qui peut me rapporter[7]. » [Alain, 25 ans, en couple, Etudiant]. Une autre stratégie a également pu être observée, qui consiste pour certains usagers à se priver d'un service, plutôt que de remplir un formulaire et de donner des informations personnelles. L'objectif pour l'usager est d'annuler le risque de recevoir des sollicitations commerciales non désirées, ou de savoir certaines traces et informations personnelles hors de sa portée et de son contrôle, ce qui est vécu comme autant de risques d'intrusions dans la vie privée.

C'est également le cas des usagers qui effacent les traces d'usage qui sont à leur portée. Dans le cadre professionnel en particulier, l'effacement de l'historique de navigation vise à protéger du regard d'autrui l'aspect privé des certaines visites sur internet. Si les administrateurs réseau peuvent accéder à de telles informations, l'usager limite-t-il au moins le risque que d'autres collègues accèdent à son historique de navigation, même si pour cela il doit se priver d'y recourir lui-même comme à un outil facilitant sa navigation. De la même façon, la gestion des cookies témoigne d'une préoccupation concrète liée à la protection de la vie privée. Les cookies, qui s'installent sur l'ordinateur de l'usager lors de sa navigation, sont une source d'informations pour les entreprises (qui parfois les imposent aux usagers en ne permettant pas l'ouverture d'une page lorsque les cookies sont refusés par le paramétrage de l'ordinateur). Mais nombre d'usagers n'apprécient pas ce système : « Même si ça ne me gêne pas qu'on nous piste, je supprime quand même tout. […] On sait que l'on peut te suivre à la trace mais tu limites les possibilités. Donc je supprime les historiques et les cookies régulièrement. C'est une question de principe aussi en même temps. […]J'ai aussi le pare-feu qui limite les cookies en plus. Ca bloque les sites commerciaux, la CAMIF par exemple. Je reçois un petit message accompagnant la page HTLM ou alors je débloque, je regarde si ça m'intéresse mais en

[7] Terrain qualitatif, France Telecom R&D.

général, je n'ouvre pas. Ca va directement à la poubelle[8]. » [Fred, 41 ans, en couple avec 3 enfants, Stagiaire IUFM].

Ces exemples concrets rejoignent la notion de « confiance décidée » développée par Luhmann. Pour lui, nous l'avons abordé, il est une forme de « confiance assurée » qui prend place dans certaines conditions. Mais d'autres formes de confiance existent, qui peuvent lui être complémentaires. La « confiance décidée » requiert un engagement préalable de la personne : celle-ci peut éviter de prendre le risque, mais elle doit alors accepter de renoncer aux avantages y sont associés. Les extraits d'entretiens précédents montrent qu'en effet des stratégies sont mises en place, les usagers évaluant d'une part les coûts, en termes de risque d'intrusion dans la vie privée notamment, et d'autre part les bénéfices attendus. Ainsi, si les usagers ne peuvent limiter les risques en se passant totalement des TIC, ils parviennent, dans leurs usages quotidiens, à opérer certains choix face aux risques concrets qu'ils rencontrent, afin de limiter la crainte de se rendre vulnérables, ou tout au moins de choisir à quelles nuisances ils s'exposent.

2.2. Le manque de contrôle comme source d'insécurité

Parmi les éléments qui participent d'une forme d'insécurité numérique, le manque de contrôle expérimenté par les usagers quand à la dissémination des traces et informations les concernant est très présent. Le cas de Laetitia, rencontrée en entretien, en est une illustration. Fonctionnaire rattachée à un ministère, elle envisage de changer de poste pour partir travailler outre-mer. Dans cette optique, Laetitia a eu l'idée de vérifier quelles informations un recruteur pouvait trouver sur elle en tapant son nom dans un moteur de recherche. Elle découvre alors que deux sites internet mentionnent une information relative à son récent investissement politique. Elle estime que cette information peut être gênante, dans la mesure où les postes qu'elle vise pourraient s'inscrire dans une autre approche que celle portée par le parti auquel elle est associée : « D'un côté ça me dérange de réagir comme ça, je n'ai qu'à assumer. Que ça soit paru dans le gratuit, bon, c'est une chose. […] Mais par contre… le fait que ce soit relayé comme ça sur internet, déjà t'es pas au courant, j'ai trouvé ça par hasard… Et puis du coup ça devient accessible si tu tapes mon nom. Et bon, je me suis trouvée sur cette liste électorale parce qu'il leur fallait quelqu'un, histoire de parité et tout ça […] Et du coup, pour ce genre de raisons, qui ne sont pas purement professionnelles en fait, ça peut me passer sous le nez. […] J'ai écris aux deux sites, il y en a un qui a enlevé le truc, mais l'autre ils ne répondent pas […] Du coup, on m'a conseillé de faire en sorte que ça n'apparaisse pas si haut, sur la première page. Alors je me suis inscrite sur copains d'avant, j'ai créé de faux blogs, des trucs comme ça. Et du coup le truc est passé en deuxième page des résultats. Mais bon j'ai l'impression que ça fluctue, donc il va falloir que je vérifie ». Cet extrait d'entretien, volontairement conséquent, illustre bien la difficulté pour les usagers à maîtriser les informations qui circulent sur eux. La stratégie adoptée ici vise à brouiller les pistes, de sorte pour l'usager à reprendre une part de contrôle sur le profil numérique qui lui correspond.

D'autres cas, plus médiatisés, illustrent les risques liés au déplacement et à la médiatisation d'informations personnelles, non très intimes mais traditionnellement localisées, ce qui en limitait la portée. L'affaire Petite Anglaise, par exemple, montre comment des informations privées peuvent venir perturber la vie professionnelle. Dans cette affaire, Catherine Sanderson, qui tenait un blog personnel de façon anonyme depuis 2004, a été renvoyée par son employeur en 2006, après que celui-ci ait découvert son blog, et estimé qu'il pouvait nuire à l'image de l'entreprise. Catherine Sanderson a porté l'affaire devant les Prud'hommes, qui en mars 2007 lui ont donné raison en décidant que son licenciement était abusif. Petite Anglaise

[8] Terrain qualitatif, France Telecom R&D.

livrait certes volontairement des bribes de sa vie privée, mais sans envisager que cela pouvait la rendre vulnérable sur un plan professionnel. En devenant un cas traité par les Prud'hommes, la tension vécue par Catherine Sanderson dans ses usages quotidiens s'inscrit ainsi dans un contexte plus large, s'ajoutant aux décisions qui peuvent finalement donner un cadre réglementaire et un sens à la régulation des risques.

Afin de se protéger de ce qui peut les mettre en insécurité, les usagers tendent aussi à recourir à des outils techniques. La technologie, qui constitue ainsi une source d'inquiétudes et qui tend à être perçue comme une menace pour la vie privée, pourrait-elle finalement en devenir une solution ? Dans le cas des e-mails par exemple, le logiciel PGP[9], accessible gratuitement, permet aux usagers de procéder au cryptage de leurs e-mails et fichiers. Ces solutions techniques, globalement nommées « PETs » ou « Privacy Enhancing Technologies », ne rencontrent cependant pas encore un large public. Bien qu'elles visent à permettre aux usagers de disposer eux-mêmes d'outils pour protéger leurs données, et leur vie privée, les PETs ne sont pas encore très largement diffusées, notamment en raison de leur trop grande complexité pour nombre d'usagers [Bohn et al. 2004]. Mais d'autres services ne nécessitent pas de compétences trop avancées, et permettent de pallier à des risques comme ceux expérimentés par les usagers victimes de l'affaire AOL. Ainsi, le moteur de recherche Ixquick Meta Search, se positionne-t-il comme l'outil qui « élimine Big Brother[10] », en proposant à l'usager d'effectuer par son intermédiaire des requêtes sur douze moteurs de recherche, sans que ces derniers n'aient accès à ses informations personnelles. Les sites proposant des e-mails jetables, aussi, permettent-ils aux usagers de limiter les sollicitations commerciales. L'installation comme navigateur par défaut de Mozilla Firefox, encore, permet-elle d'effacer aisément les traces visibles de navigation. D'autres outils, parfois payants, se positionnent ainsi sur une forme de marché de protection de la vie privée, lequel pourrait bien se développer dans les années à venir, tant les cas de tension vécus par les usagers, portés devant la justice, ou mis en exergue par les médias exacerbent le sentiment qu'il est nécessaire de se protéger[11].

De tels cas montrent combien des informations qui peuvent sembler anodines, et qui sont déjà pour partie rendues publiques, peuvent cependant affecter l'usager concerné lorsqu'elles sont rapportées à d'autres contextes. Des éléments de vie privée, qui sans être cachés restaient localisés, circonscrits, peuvent ainsi devenir accessibles aisément. L'individu peut ainsi se sentir vulnérable, être mis en danger, d'une certaine façon, sans possibilité de contrôler vraiment ce qui paraît. Afin de réguler de tels risques, les usagers semblent de plus en plus prompts à suivre leur propre existence numérique, et à intervenir, de diverses manières et y compris en s'en remettant à des instances supérieures de décision, pour limiter et réguler les nuisances possibles et la vulnérabilité ressentie.

Ainsi, les usages quotidiens s'inscrivent régulièrement dans des formes de tension, et ces micro-affaires sont une entrée analytique intéressante pour mieux comprendre ce qui fait insécurité relativement à la vie privée à l'ère numérique. Mais afin de mieux appréhender ce qui fait insécurité, et la manière dont des formes de régulation des risques prennent place, l'analyse devient intéressante en articulant ce qui se joue au niveau micro-social, dans les usages quotidiens, avec ce qui se joue à un niveau plus méso-social, et au niveau macro-social de la normalisation. Les modalités d'action au niveau des usages, mais aussi au niveau des

---

9 Pretty Good Privacy.

10 *Ixquick élimine Big Brother*, Communiqué de presse du 13 juin 2006. Source : http://us.ixquick.com/fra/press/pr_big_brother.html (visité le 17/10/2006).

11 On notera cependant que pour certains acteurs, il n'est pas souhaitable que de tels outils soient mis en avant comme seule solution, car les usagers deviendraient alors les seuls responsables de la protection de leur vie privée, à l'exclusion d'autres acteurs comme les entreprises ou les autorités publiques.

logiques d'alerte, visent en effet à réguler, de différentes manières, les risques relatifs à la vie privée, mais aussi aux libertés individuelles et publiques.

3. De l'alerte à la normalisation

3.1. De l'alerte à la controverse : Les affaires Benetton et Gilette

Au-delà des formes de régulation des risques opérées par les individus, ainsi, d'autres formes d'action prennent place. Les risques perçus comme étant liés aux TIC font en effet l'objet d'un travail de mise en visibilité, sur la base notamment d'un travail de veille et de vigilance porté par des acteurs défenseurs de la vie privée et des libertés individuelles et publiques. Ces acteurs, souvent associatifs, se placent ce faisant dans une logique d'alerte au sens de Chateauraynaud [2005, 1999] : « Lancer une alerte, c'est avant tout manifester une perte de prise, l'impossibilité de réduire un danger ou de contrôler une source de risques. […] Une alerte interpelle des instances supposées avoir prise sur le futur. […] Pour être fondée, une alerte, mais aussi une critique ou une protestation, suppose une présence éveillée au monde ». Par un travail de suivi de l'actualité tant commerciale, qu'expérimentale, juridique ou politique, les porteurs d'alerte s'efforcent de fait d'alerter les individus, mais également les instances jugées aptes à intervenir pour réguler les risques et menaces dénoncés.

Une telle situation correspond par exemple au cas de la structure américaine CASPIAN[12]. Fondée en 1999, cette ONG autofinancée a pour objectif de lutter contre les intrusions commerciales dans la vie privée, au travers notamment des cartes de crédits, et a progressivement élargi son champ de vigilance à d'autres technologies jugées intrusives comme les puces RFID. Le site internet de l'ONG propose différentes entrées qui visent d'une part à faire prendre conscience aux consommateurs que les programmes de fidélité sont intrusifs, et d'autre part à les alerter sur certains « combats » menés, contre telle chaine de supermarché ou tel système de carte de crédit à la consommation. Le mode d'action de CASPIAN consiste ainsi essentiellement en un travail de dénonciation via son site.

Mais ce travail de veille et d'alerte a cependant connu un tournant en 2003, avec les affaires Benetton et Gilette. En mars 2003, un communiqué de presse annonce que le distributeur Benetton vendra des vêtements équipés de puces RFID. La même année, en Juillet 2003, Gillette et un supermarché de la chaîne Tesco ont mis en place, à Cambridge, une expérimentation sur des lames de rasoir. Associant puce RFID et caméras vidéo, ce test avait pour objectif officiel d'expérimenter un nouvel outil pour lutter contre le vol. Suite à chacune de ces annonces, le mode d'action choisit par CASPIAN est un appel au boycott de ces entreprises. L'ONG établit à cet effet deux sites internet spécifiques : www.boycottbenetton.com et www.boycottgillette.com, qui souhaitent frapper l'opinion[13]. Cette action semble avoir trouvé un écho assez large, du fait d'une diffusion mondiale via Internet, et d'une appellation dangereuse pour l'image des deux groupes. Sur ces sites, et dans ses interventions dans la presse, CASPIAN reproche aux groupes des procédés intrusifs (en particulier dans le cas de Gillette), et une absence d'information préalable des consommateurs. L'ONG exige un renoncement public, de la part des deux groupes, quant au fait d'implanter des puces RFID au plus près du consommateur, et ce sans consultation préalable. La réaction des deux groupes ne se fait pas attendre très longtemps, chacun craignant pour son image de marque. Moins d'un mois après l'intervention de CASPIAN, le groupe Benetton déclare

[12] Consumers Against Supermarket Privacy Invasion And Numbering. Site internet: www.nocards.org.

[13] Pour exemple, sur le site boycottbenetton.com, le slogan, appuyé de photos, est « rather go naked » : plutôt être nu (que porter des puces RFID).

renoncer à implanter des puces RFID, se préservant toutefois une marge de manœuvre à moyen terme, en précisant que le groupe travaille sur cette technologie mais n'envisage pas d'applications concrètes avant plusieurs années. De même, un mois après l'intervention de CASPIAN, c'est au tour de Gillette de faire profil bas, par l'intermédiaire d'un article du Financial Times qui annonce que Gillette renonce pour au moins 10 ans à tout procédé permettant de tracer individuellement chacun de ses produits. Si CASPIAN se félicite de ces reculs annoncés publiquement, l'ONG attend toujours un renoncement plus affirmatif. Les sites de boycott existent toujours, et restent consultables.

En s'attaquant à deux groupes mondialement connus, CASPIAN a vu sa notoriété et sa présence dans les médias s'accroître. D'une posture de « lanceur d'alerte » [Chateauraynaud 2005], l'ONG a pu émerger comme acteur stratégique de défense de la vie privée en mobilisant l'attention autour de ces affaires. Au-delà de l'appel au boycott, et de la seule préoccupation pour ces affaires, CASPIAN a en effet souhaité faire du bruit autour de ces affaires, pour que les messages de vigilance et de mise en alerte, qu'elle porte depuis sa création en 1999, soient finalement relayés à cette occasion. Car avant ces deux affaires, les actions de CASPIAN (dont un premier appel au boycott en 2002, concernant une autre entreprise) n'avaient pas eu le même écho. Mais si l'ONG a tiré un certain profit, notamment en termes de notoriété et d'audience, de ces deux affaires, il n'en reste pas moins que son combat est plus large, s'inscrivant dans une logique d'alerte et de mobilisation autour de risques identifiés. En France, un certain nombre d'acteurs tels que le CREIS, IRIS, les BBA[14], Souriez vous êtes filmé, etc. s'efforcent d'agir dans une telle logique également, avec chacun leurs modalités d'action et de prise de parole, afin d'alerter l'opinion, mais aussi les instances de décision, sur les risques associés à la mise en place de technologies comme la biométrie, le vote électronique, ou sur les dangers perçus comme inhérents à des projets de loi touchant aux données numériques par exemple.

Chateauraynaud [2005] estime que « de nos jours, les relais institutionnels sont plus nombreux et les lanceurs d'alerte jouissent d'une légitimité plus grande ». Mais, si les lanceurs d'alerte s'efforcent de toucher un large public, il semble cependant difficile de sortir des réseaux déjà concernés par ces problématiques pour aller sensibiliser au-delà. C'est en ce sens que le passage de l'alerte à la controverse est une étape utile, sinon incontournable, pour la prise en charge publique et politique de certains dossiers : « La figure la plus frayée de basculement de l'alerte dans une arène publique est celle de l'ouverture d'un débat ou d'une controverse. […] En rendant tangibles des atteintes, réelles ou potentielles, pour d'autres acteurs, les porteurs d'alertes ou de dénonciation parviennent à déconfiner leur cause » [Chateauraynaud 2005]. Pour autant, contribuer à faire émerger une controverse n'apparaît pas être l'objectif en soi. La controverse prend sens en ce qu'elle permet d'élargir la prise de conscience, et partant la visibilité des acteurs, mais également en ce qu'elle permet souvent la mise en place des conditions de prise en charge d'un dossier.

3.2. De la controverse à un processus de normalisation

De fait, dans le cas rapporté, la mobilisation de CASPIAN ne s'est pas limitée à la dénonciation. L'ONG a en effet développé des propositions, qui vont dans le sens de la participation à un processus de régularisation des risques dénoncés, et de normalisation. CASPIAN a en effet proposé des solutions de régulation permettant de protéger les consommateurs de certaines atteintes à la vie privée, en militant par exemple en faveur de la création d'un label prévenant de la présence d'une puce RFID dans les produits, ce qui ne pourrait se mettre en place qu'avec la participation des entreprises, ou en faveur du

[14] Big Brother Awards, en lien avec la structure Privacy International.

développement de solutions techniques qui permettraient au consommateur de désactiver les puces. L'ONG a également agi en faveur de solutions réglementaires pour protéger les consommateurs, en travaillant à un projet de loi fédérale, le « RFID Right to Know Act of 2003[15] ». Ce projet de loi, écrit avec l'aide de juristes et d'universitaires, 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. Ce projet de loi n'a pas encore abouti. En effet, si CASPIAN a pu accroitre sa visibilité au travers de ces affaires, l'ONG ne semble pas être parvenue à se hisser en position de trouver les appuis parlementaires pour relayer son projet. Pourtant, suite à l'éclatement de la controverse, il apparaît que c'est bien une recherche de normalisation qui s'opère, même si CASPIAN n'a pas encore pu imposer, face au secteur commercial puissant, une mobilisation suffisante pour une mise sur agenda et une prise en charge de la question de la régulation.

En France, l'affaire SAFARI illustre également ce cheminement de l'alerte, à la controverse, puis à la normalisation. Sans revenir en détail sur cette affaire, on peut rappeler que la loi n°78-17 du 06 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi née sur fond de scandale populaire [Vitalis 1981]. La révélation, par le quotidien Le Monde et par quelques parlementaires, du projet SAFARI, lequel visait à permettre l'interconnexion des grands fichiers publics via l'usage du numéro de sécurité sociale, donnée identifiante s'il en est [Gentot 2002]. C'est ce scandale qui a permis, ou tout au moins accéléré, la mise sur agenda d'une réflexion globale sur la question des données de fichiers. La loi de 1978, réactualisée depuis[16], a posé, en France, les principes de régulation liés au traitement de données à caractère personnel, et a porté création de la CNIL, instance dont les missions de veille et de contrôle sont régulièrement critiquées, en raison notamment d'un manque de moyens.

Pour Chateauraynaud [2005], « lorsque le *déconfinement*[17] des alertes est réussi, il a pour effet d'accroitre le *concernement* d'acteurs éloignés, ce qui créé les conditions d'une "explosion médiatique" et d'une "mise sur l'agenda politique", pour utiliser ici des expressions courantes en matière de "gestion de crises" ». Les affaires évoquées ici témoignent de ce qu'un tel processus n'est pas sûr d'aboutir. Mais le travail de vigilance que réalisent les lanceurs d'alerte, et le déploiement régulier de controverses, sont autant de jalons qui construisent le temps de l'alerte, et qui, finalement, peuvent conduire à un moment de balancement lors duquel une ultime controverse pourra déclencher la prise en charge publique et politique des risques dénoncés.

Entre les grandes représentations partagées, qui véhiculent un imaginaire de risques et de craintes, et les affaires médiatisées qui viennent nourrir une histoire collective parlant de vulnérabilité des individus face aux technologies et aux acteurs qui les exploitent, il apparaît qu'une forme d'insécurité numérique accompagne les pratiques quotidiennes des usagers, relativement à leurs données et à leur vie privée. L'observation des tensions au niveau des usages, mais également l'analyse et le déploiement d'un certain nombre d'affaires, et de leurs connexions possibles avec les évolutions réglementaires et un processus de normalisation, permettent d'appréhender les formes de régulation qui se mettent en place face à des risques perçus et vécus.

[15] http://www.nocards.org/rfid/rfidbill.shtml

[16] Réactualisée par la loi n° 2004-801 du 06 Août 2004 sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui transpose la Directive européenne de 1995.

[17] En italique dans le texte cité.

Bibliographie

Armatte, E. : *Informatique et libertés : de Big Brother à Little Sisters*. In Terminal « Fichiers et libertés : le cybercontrôle 25 ans après », n°88, 2001.

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., Rohs, M. : *Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing*. Institute for Pervasive Computing, ETH Zurich, 2004.

Boyer, J. : *L'internet et la protection des données personnelles et de la vie privée*. In Cahiers français « L'Internet » (Capul, J.-Y.), La Documentation Française, 74-79, n° 295, Paris, mars-avril, 2000. ,

Castells, M. : *La société en réseaux. L'ère de l'information*. Arthème Fayard, Paris, 1998.

Chateauraynaud, F., Torny, D. : *Mobiliser autour d'un risque. Des lanceurs aux porteurs d'alerte*. In Risques et crises alimentaires (Lahellec, C., coord.), Paris, Tec & Doc Lavoisier, 2005.

Chateauraynaud, F., Torny, D. : *Les sombres précurseurs. Une sociologie pragmatique de l'alerte et du risque*. Paris, EHESS, 1999.

Desjeux, D. : *La consommation*. Coll. « Que sais-je ? », Paris, PUF, 2006.

Desjeux, D. : *Les sciences sociales*, Coll. « Que sais-je ? », Paris, PUF, 2004.

Gentot, M. : *La protection des données personnelles à la croisée des chemins*. In La protection de la vie privée dans la société d'information (Tabatoni, P., dir.), Tome 3, Chap. 1, 24-46, coll. « Cahier des sciences morales et politiques », PUF, Paris, 2002. Source : http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf (visité le 29/08/2005).

Luhmann, N. : *Confiance et Familiarité. Problèmes et alternatives*. In Réseaux « La confiance » (Quere, L.), 15-35, vol.19 n°108, 2001.

Monot, P., Simon, M. : *Habiter le cybermonde*. Editions de l'Atelier/Editions Ouvrières, Paris, 1998

Rigaux, F. : *L'individu, sujet ou objet de la société de l'information.* In La protection de la vie privée dans la société d'information (Tabatoni, P., dir.), Tome 3, Chap. 6, 122-137, coll. « Cahier des sciences morales et politiques », PUF, Paris, 2002. Source : http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitre6.pdf (visité le 29/08/2005).

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

Vitalis, A. : *Informatique et libertés : Une problématique toujours pertinente*. In Actes du colloque « Que ne peut l'informatique », CNAM, Paris, 1999.

Vitalis, A. : *Informatique, Pouvoir et Libertés*. Coll. « Politique Comparée », Economisa, Paris, 1981.