ESPACE, POPULATIONS, SOCIETES, 2012-3 pp. 63-77

Sarah WIDMER
Francisco R. KLAUSER

Institut de géographie
Université de Neuchâtel
Espace Louis-Agassiz 1
2000 Neuchâtel
sarah.widmer@unine.ch
francisco.klauser@unine.ch

Mobilités surveillées : rôles et responsabilités des développeurs d'applications *smartphone*

INTRODUCTION

Dans nos sociétés occidentales contemporaines, les technologies de l'information et de la communication (TIC) sous-tendent une grande partie de nos activités quotidiennes. Ces technologies nous accompagnent dans nos déplacements journaliers, médiatisent certaines de nos interactions sociales et se fondent de plus en plus dans notre environnement [Dodge & Kitchin & Zook, 2009].
La perspective d'une informatisation omniprésente de nos univers quotidiens ne va, toutefois, pas sans susciter quelques réactions face aux dérives liées à ces développements. Sont fréquemment évoqués, le caractère intrusif et le potentiel surveillant de ces technologies qui « monitorent » continuellement les objets et les êtres [Graham, 2004, p. 299]. Dans ces discussions actuelles autour de la dimension surveillante des TIC, le *smartphone* – objet de cet article – n'est pas en reste. En 2011, un article du *Guardian* révélait l'existence d'un fichier caché dans les téléphones et tablettes de la société *Apple*, sauvegardant les données de localisation des utilisateurs à différents intervalles de temps. Face au retentissement occasionné par ce que certains appelaient déjà le « mouchard » de l'*iPhone*, la société *Apple* informa le public qu'elle ne traçait aucunement ses utilisateurs individuels, mais que les données anonymisées lui permettaient d'établir une base de données des relais cellulaires et des

points d'accès au Wi-Fi, afin de calculer plus rapidement et précisément la localisation de l'utilisateur lorsque celui-ci activait ce service sur son téléphone.

Certes, une grande partie de ce qui fait scandale dans l'anecdote ci-dessus, réside dans la dimension cachée de ce fichier que l'on découvre soudainement. Mais le scandale a également trait à la nature des données collectées : des données de localisation, jugées comme particulièrement personnelles par une partie du public. Face aux critiques de la presse, la réponse d'Apple est, elle aussi, intéressante. Bien sûr, la société aurait difficilement pu se justifier autrement qu'en disant : « C'est pour votre bien que nous prélevons ces données ! ». Toutefois, il paraît important de relever cette association faite entre surveillance de l'utilisateur et service rendu à ce même utilisateur : les données récoltées permettraient, en effet, de lui fournir un service plus rapide et précis lorsque celui-ci recourt à la géolocalisation.

Approche

Le présent article revient sur la dimension surveillante associée à la fonctionnalité de géolocalisation des *smartphones* et explore cette curieuse association entre « service rendu » et « surveillance ». Nous examinons cette problématique au travers du regard de six développeurs d'applications de géolocalisation avec lesquels nous avons réalisé une série d'entretiens semi-directifs[1]. Plus spécifiquement, notre étude est structurée en quatre temps. Une première partie introductive aborde la question des chances et risques d'une mobilité « assistée par logiciel ». Cette partie revient également sur les notions théoriques (« expertise », « autorité »), auxquelles nous recourons afin de saisir la position qu'occupent les acteurs étudiés. L'article se découpe ensuite en trois parties analytiques, basées sur nos données empiriques. Ces trois parties explorent les façons par lesquelles les développeurs rendent compte de leur rôle, des risques liés à leurs logiciels et de leur responsabilité face à ces risques.

CHANCES ET RISQUES LIÉS À LA GÉOLOCALISATION

Parmi les diverses fonctions qu'ils assurent, les s*martphones* peuvent notamment servir d'outils de géolocalisation. L'utilisateur d'un *smartphone* peut, en effet, connaître sa position géographique de façon relativement précise, grâce notamment à la dotation de ces appareils d'un GPS intégré. Mais l'intérêt de la géolocalisation va au-delà du simple fait d'indiquer sa position à l'utilisateur. Il réside dans le fait de localiser l'utilisateur par rapport à une information [Gordon & de Silva e Souza, 2011] : quelles sont les pizzerias situées dans son entourage ? Des radars sont-ils situés sur sa route ? Quels sont les arrêts de bus les plus proches de lui, où vont ces bus et dans combien de temps passent-ils ? Ce type d'informations peut être fourni par des logiciels téléchargeables et exécutables sur *smartphone* : des applications de géolocalisation.

Les technologies de localisation n'ont de sens que sur des interfaces mobiles (*smartphones,* tablettes) ; elles sont donc fondamentalement liées à la condition mobile de l'utilisateur. Dans cet article, nous nous concentrons précisément sur les applications géolocalisées qui permettent à l'utilisateur d'organiser ses déplacements et de gérer sa mobilité.

Du « *location-aware* » au « *user-aware* » : à la recherche de l'information pertinente

La géolocalisation et les services qui lui sont associés ont pour objectif premier de donner

[1] Ces entretiens constituent une première phase d'investigation dans le cadre d'une thèse de doctorat en cours, « Mobilités intelligentes ? *Smartphone*, géolocalisation et mobilités urbaines ».

à l'utilisateur une information pertinente correspondant à son emplacement. L'information dispensée à l'utilisateur est sélectionnée en fonction du paramètre « emplacement » que les technologies de localisation du *smartphone* captent sous la forme de coordonnées de latitude et de longitude. Parallèlement à ces applications que les sciences informatiques qualifieraient de « *location-aware* » on assiste au développement de logiciels « *context-aware* » [Garcia-Crespo *et al.,* 2009 ; Kabassi, 2010 ; Peer, 2010]. Dans ces cas, l'information dispensée n'est plus uniquement sélectionnée en fonction d'une localisation, mais tient également compte d'autres éléments du contexte tels que l'heure, la météo, etc. Dans ce cas, l'information se fait plus précise et s'adapte encore davantage à l'utilisateur et à son contexte d'utilisation.

Ce processus d'affinage se manifeste à plus forte raison encore dans certaines applications dont l'objectif est de cibler l'information en fonction des intérêts de l'utilisateur. Bien que ce terme ne soit pas utilisé par les sciences informatiques, il nous semble pertinent de qualifier ces logiciels de « *user-aware* ». Dans les applications géolocalisées existantes qui fonctionnent selon cette logique « *user-aware* », les goûts de l'utilisateur peuvent être inférés à partir de son historique d'utilisation : « *users can get recommendations of places […] based on user's current position and on user's tastes, as manifested by past movements and subsequent visits to different spots (« people that usually frequent this restaurant usually like to go to that other club* ») » [Scipioni, 2011, p. 1]. Dans ce type d'applications, l'information devient personnalisée pour l'utilisateur – ou du moins pour le profil auquel il correspondrait.

Bien que le degré de complexité de ces trois types de systèmes (*location-, context- et user-aware*) ne soit pas équivalent, la logique qui les sous-tend est globalement la même : extraire d'une masse d'informations, celles qui seront les plus pertinentes pour l'utilisateur.

Des mobilités intelligentes ?

Le fonctionnement de ces applications correspond à celui de technologies intelligentes. Cette « intelligence » repose, d'une part, sur une capacité à collecter des données, ainsi qu'à les classifier et analyser en fonction de codes préétablis ; et elle se traduit, d'autre part, en une « réponse » automatisée à une activité ou à un environnement donné (la réponse étant, dans le cas de nos applications, d'afficher une information pertinente à l'utilisateur).

L'« intelligence » de ces applications contribue-t-elle à rendre nos mobilités elles aussi plus intelligentes ? Les informations obtenues peuvent contribuer à faciliter les déplacements de l'utilisateur. L'automobiliste recevant un signal sonore lorsqu'il se trouve à 50 m d'un radar, ou pouvant situer les parkings les plus proches et voir combien de places y sont encore disponibles : n'a-t-il pas une mobilité optimisée ? Si l'on se réfère à la définition que Jacques Lévy donne du capital spatial, à savoir : l'« *ensemble des ressources, accumulées par un acteur, lui permettant de tirer avantage, en fonction de sa stratégie, de l'usage de la dimension spatiale de la société* » [Lévy & Lussault, 2003, p. 124], on peut considérer les informations fournies par ces applications comme des ressources contribuant à accroître le capital spatial de leurs utilisateurs. L'intelligence de ces logiciels génère des mobilités informées, personnalisables, mais aussi – bien souvent – plus rapides. Ces technologies offrent donc certains avantages. Elles soulèvent toutefois une série de problèmes – notamment en termes de « *privacy* » et de « tri social » – dont nous parlerons par la suite.

Une intelligence à double tranchant

L'importance que revêt l'information dans un processus de mobilité n'est pas une thématique nouvelle. Sommes-nous, ici, en train de recycler une problématique traditionnelle de la géographie en l'adaptant à un nouvel objet ? En quoi les applications *smartphone* que nous décrivons sont-elles différentes d'une carte routière ou d'un guide touristique ?

La différence fondamentale réside précisément dans l'« intelligence » de ces systèmes, dans cette capacité qu'ils ont d'accumuler, de trier et d'analyser des données pour, ensuite, fournir une réponse instantanée et automatisée. Le service dont profite l'utilisateur repose, ainsi, sur ce que David Lyon appelle la « dataveillance » [2007, p. 200] : « *surveillance based on collecting and monitoring personal data and not involving direct watching or listening […] ([term] coined by Roger Clarke [1988])* ». Cette dataveillance répond à des finalités diverses. Des finalités de direction et de protection mais aussi - et surtout - de gestion de notre quotidien ; elle s'inscrit dans une logique de commodité et de confort, destinée à seconder l'utilisateur. Or, bien que ce type de surveillance n'ait pas pour finalité première de contrôler et de réprimer le surveillé, elle n'en soulève pas moins toute une série de questions relatives à (1) la protection de la sphère privée des utilisateurs et (2) à son potentiel de « tri social ». Premièrement, la collecte et l'analyse de données (notamment de données de localisation) peuvent s'avérer problématiques du point de vue de la « *privacy* » de l'utilisateur. Les risques encourus par l'utilisateur semblent, toutefois, assez variables d'une application à l'autre. Les données de localisation sont généralement anonymisées et ne sont pas nécessairement stockées sur un serveur externe par le « *service provider* ». Toutefois, la situation devient plus délicate dans le cas d'applications *user-aware* qui analysent l'historique des déplacements de l'utilisateur afin d'en déduire ses préférences. Le fonctionnement de ce type d'applications nécessite le stockage des données de localisation de l'utilisateur, ce qui s'avère problématique lorsque ce stockage a lieu de façon externe [Scipioni, 2011, p .2]. Outre ce risque de traçage de l'utilisateur, Scipioni évoque un autre aspect problématique lié à cette forme de surveillance : le profilage des utilisateurs opéré par ces logiciels. Cette opération présente des risques pour l'utilisateur car son profil pourrait être réutilisé à des fins publicitaires, ou revendu à des tiers par le « *service provider* » [Scipioni, 2011, p. 5].

En addition à cela, l'action de profilage soulève une deuxième problématique fondamentale, évoquée par Stephen Graham au travers de la notion de « *software sorting* » [2005]. Par cette expression, Graham met en lumière le tri continuel et invisible qu'orchestre le code informatique dans nos univers quotidiens. Graham associe ce « *software sorting* » aux tendances néolibérales actuelles qui nous ont fait passer d'une conception universaliste des services à la population à une conception dans laquelle les infrastructures de base, les espaces et les services de tous les jours deviennent des commodités personnalisables et adaptables au profil du consommateur [Graham, 2005, pp. 565-566]. Les *softwares* et leurs algorithmes ont donc ce pouvoir de distinguer et de différencier ; ils ont, ainsi, la capacité de créer des géographies différenciées selon le profil de l'utilisateur. Le « *software sorting* » pose problème, car il peut potentiellement être à la base de toute une série d'inégalités socio-spatiales : en distinguant, le software peut délimiter des droits, des accessibilités, des vitesses différentes. Il peut prioriser certains, tout en discriminant d'autres individus.

Expertise technique et coalitions d'autorités en matière de mobilité intelligente

Bien souvent donc, les auteurs portant un œil critique sur la numérisation croissante de nos quotidiens font allusion à un pouvoir en partie désincarné : celui du « code » ou du « *software* » organisant de plus en plus nos existences. En prolongeant cette réflexion, cet article propose d'étudier et de questionner le rôle et la responsabilité d'un acteur particulier en matière de géolocalisation : les développeurs d'applications mobiles pour s*martphones*.

Aborder la problématique des « mobilités intelligentes » au travers de ces acteurs nous semble primordial. Les développeurs produisent des spatialités au travers de leurs logiciels et ont un impact sur la mobilité de leurs utilisateurs. Il paraît dès lors intéressant d'appréhender comment ils se représentent le « service » qu'ils fournissent, tout en examinant

leur façon de rendre compte des tensions inhérentes à leurs logiciels en termes de « *privacy* » et de « *software sorting* ». Plus spécifiquement, cette approche nous offre une perspective importante – celle des « techniciens » eux-mêmes – sur l'actuel débat relatif aux « *privacy enhancing technologies* » [Goold, 2009]. Ainsi, dans la dernière partie de notre analyse, nous abordons comment nos interlocuteurs se représentent les possibilités d'implémenter des solutions « techniques » au sein même d'applications surveillantes, afin de limiter leurs atteintes à la sphère privée des utilisateurs.

En problématisant le rôle d'acteurs privés qui font de la conception, du développement et de la diffusion de logiciels *smartphone* leur « *business* », cet article s'inspire – entre autres – de la vaste littérature en matière de gouvernance urbaine ou globale [Lipschutz, 1999 ; Roseanau, 1997 ; Cutler, Haufler & Porter, 1999]. Cette littérature démontre l'interdépendance croissante d'acteurs publics et de divers acteurs privés, dans la fabrique et la gestion de domaines traditionnellement réservés à l'État. À travers la notion « d'expertise » [Collins & Evans, 2007], notamment, sont explicitées les nouvelles coalitions d'autorités – « *autorité » définie comme « the capacity to get things done without the legal competence to command that they be done* » [Czempiel, 1992, p. 260] – qui s'appuient sur des compétences factuelles (ancrées dans des pratiques ou savoirs d'experts précis) plutôt que purement juridiques. Par conséquent, cette littérature insiste sur l'importance de réseaux d'acteurs en matière de gouvernance, combinant des connaissances, compétences et savoir-faire hétérogènes, et mobilisant des sources d'autorités variées.

Plus particulièrement, des auteurs comme Mitchell [2002] et Klauser [2009] démontrent le rôle croissant d'acteurs professionnels hautement spécialisés en IT, en matière de gouvernance urbaine de plus en plus informatisée. Cette approche « techno-politique » [Mitchell, 2002, p. 43] reprend les messages centraux de la théorie de l'acteur réseau [Akrich & Méadel, 1999 ; Latour, 1987 ; Callon, Lascoumes & Barthe, 2001], dans son attention portée aux interactions et médiations complexes façonnant des « réseaux d'acteurs thématiques », articulés autour de projets particuliers (*cf.* la notion de « *issue network* » de Heclo [1978]).

Ancrés dans une telle approche, nous proposons ici d'étudier le rôle et la responsabilité des concepteurs de logiciels de smartphones, en termes d'expertise et d'autorité, ainsi que les risques qui en découlent.

RÔLE DU DÉVELOPPEUR

Cette première partie de notre analyse s'appuie sur nos données empiriques pour examiner le rôle que jouent les développeurs dans la production d'applications *smartphone*. Notre intention est d'examiner les logiques et le savoir-faire présidant à la production de ces softwares. Il s'agit également de considérer dans quelle mesure l'expertise technico-informatique des développeurs fait de plus en plus autorité dans nos sociétés contemporaines.

Savoir-faire et autorité du développeur

La plupart des programmeurs que nous avons interrogés se sont, depuis quelques années, exclusivement spécialisés dans la création d'applications mobiles. Le développement mobile représente actuellement un business en plein essor. Il existe, d'une part, une demande des détenteurs de smartphones (toujours plus nombreux) pour ce type de logiciels ludiques ou pratiques. D'autre part, l'existence de ce marché s'explique par un effet boule de neige : les entreprises et services publics subissent une certaine pression de la part de leurs concurrents ou voisins déjà visibles sur ce type d'interfaces ; ainsi, il devient pour eux presque prescrit de fournir ce service à leurs clients ou usagers. L'un de nos interlocuteurs résume ces

mécanismes par cette simple phrase, qu'il impute à ses clients :

> « *Tous les autres le font, alors nous aussi on est obligés de le faire !* » (Stéphane Burlot, développeur *iPhone*).

À mesure que se multiplient ces développements, s'accroît l'importance du savoir-faire des programmeurs dans nos quotidiens. Dans le cas d'applications *location-, context-* ou *user-aware*, ce savoir-faire médiatise de façon croissante nos relations à l'espace et à la mobilité. Malgré l'immatérialité du logiciel et l'invisibilité du code qui le régit, ces « services informatiques » ont souvent des effets tangibles et réels. Nos interlocuteurs évoquent quelques-uns de ces effets :

> *Les matins de chutes de neige, c'est énormément utilisé. Les gens se disent « tiens est-ce que mon bus il passe ou pas »... C'est très important, ça évite aux gens de sortir, d'arriver à l'arrêt... et puis là, il ne passe pas... […] donc il reste chez lui ou il prend un autre moyen de transport... […] En fait indirectement on arrive à fluidifier les flux de personnes. […]* (Fiorenzo de Palma, développeur de l'application des transports publics lausannois).
>
> *Par exemple dans deux semaines il y a le salon de l'auto, et bien on a déployé - pour la police - une application qui permet de gérer en temps réel le trafic, si tout d'un coup il y a un bouchon, d'avoir des circuits de délestage par exemple. […]* (David Beni, ingénieur, spécialisé dans les SIG et les services géo-informatiques).

Ces deux extraits soulignent également le fait que le développeur devient un acteur participant à la gestion des mobilités et à la fluidification des flux. Comme le révèle la seconde citation, cette expertise informatique se met au service des acteurs traditionnellement responsables de l'administration des circulations. Obtenir une information sur un espace donné et sur les flux qui le traversent, voilà la plus-value que ces développeurs – capables de numériser les flux dans un logiciel mobile – sont en mesure de proposer aux acteurs responsables de la fluidité et de la sécurité du trafic.

Le rôle de plus en plus crucial que joue le code informatique dans le fonctionnement et la gouvernance de nos univers quotidiens a été abordé à plusieurs reprises en sciences sociales, et notamment en géographie [Thrift & French, 2002 ; Graham, 2005 ; Dodge & Kitchin, 2011]. Pour Thrift et French, il y a du pouvoir dans ces logiciels omniprésents, imposant leur logique de fonctionnement à l'ensemble de nos sociétés. Cette vision est partagée par nos interlocuteurs, évoquant, à leur tour, l'importance des logiciels, façonnant de multiples domaines de notre quotidienneté.

> *Le métro qui passe par ici en bas juste à côté de chez nous, il n'a pas de pilote. C'est un logiciel qui le pilote. C'est un logiciel qui décide quand s'arrêter, quand démarrer et tout ça... Et puis il n'y a pas eu un accident en quatre ans, cinq ans... […] C'est du délire ! C'est complètement fou ! Dans quel monde on habite ! Je peux demander à Siri de me faire un rendez-vous avec le docteur pour demain 10 heures... Le métro il marche tout seul, c'est un robot ! Du coup, toutes... Tout le monde dans lequel on vit est régi par des ordinateurs. […].* (Adrian Kosmaczewski, développeur *iPhone*)

Un monde « régi par des ordinateurs » est aussi un monde régi par le savoir-faire des informaticiens. Cette expertise particulière devient une forme d'autorité de plus en plus prégnante, conditionnant le fonctionnement de nos sociétés. Dans ce contexte, l'apparition des *smartphones* marque l'avènement d'une informatique réellement ubiquitaire, étendant les possibilités d'usages de logiciels à des espaces-temps jusqu'ici encore non exploités. De par les logiciels qu'il crée, le développeur intervient dans ces espaces-temps : il contribue à la gestion de nos mobilités et médiatise de façon croissante nos relations à l'espace.

La production d'une application : des associations complexes

Le savoir-faire des développeurs devient donc une source d'autorité de plus en plus répandue dans la gestion de nos espaces et

mobilités. Plusieurs auteurs évoquent également l'autorité du programmeur en avançant que le code informatique que celui-ci produit n'est pas neutre mais reflète les valeurs et choix de cet acteur : « *[…] the designers, builders and programmers of such systems […] are able to embody their prejudices and desires into the very functioning code and architecture of the systems themselves* » [Wood & Graham, 2006, p. 186].

Pourtant, d'après ce qu'il ressort de nos entretiens, l'omnipotence de cet acteur est à nuancer. Au vu des discours récoltés, il nous semble plus adapté d'emprunter à Bruno Latour sa définition de « l'acteur » : « *an actor is what is made to act by many others* » [2005, p. 46]. La production d'une application smartphone ne voit pas intervenir le seul développeur, imprimant ses désirs et sa vision du monde dans le logiciel. Au contraire, un vaste et complexe réseau d'acteurs (utilisateurs, clients, graphistes, etc.) contribue à façonner ce processus créatif.

En premier lieu, le développeur est au service de ses clients et suit, donc, en grande partie les directives provenant de ceux-ci. Le travail du développeur est, en outre, passablement dépendant du « retour » que donneront les utilisateurs finaux. Cette possibilité de feedback des utilisateurs est d'ailleurs quelque chose que nos interlocuteurs semblent parfois vivre comme une forme de tyrannie. De mauvais retours des utilisateurs peuvent, en effet, réduire le téléchargement d'une application et passablement ternir la réputation d'un développeur. Leurs logiciels étant destinés au public, nos interlocuteurs sont très soucieux de l'utilisateur final et de son opinion. Le feed-back des utilisateurs est, ainsi, parfois intégré dans le design de l'application :

> *On l'a fait ensuite… beaucoup d'utilisateurs nous disaient…. Oui… Cette option « montre-moi le quai de départ»… Parce qu'ils voulaient savoir : si j'arrive à la gare principale, sur quel quai je dois aller ? On n'avait pas… Nous-mêmes, on ne pensait pas que c'était très important mais on a quand même décidé d'intégrer une option pour les gens… S'ils veulent ça.* (Jorim Jaggi, étudiant en informatique à l'ETHZ, développeur *Android*)[2].

D'autres éléments contraignent la pratique du développeur. Les développeurs *iPhone* sont, par exemple, soumis à des directives assez strictes venant de la société Apple. Celle-ci cherche, en effet, à créer une « expérience Apple », c'est-à-dire à faire en sorte que le détenteur d'un *iPhone* retrouve une certaine unité dans les différentes applications qu'il utilise. Ainsi, toutes les puces, listes déroulantes, polices d'écriture etc. seront généralement identiques d'une application à l'autre. Ceci conditionne bien évidemment le travail des développeurs qui doivent se plier à un certain nombre de « *guidelines* » afin que leur application puisse être publiée sur l'A*ppstore*. Le développement sur la plateforme *iOS* semble donc passablement conditionné par cet acteur global, dictant les règles du jeu.

Sans remettre en cause l'importance du savoir-faire des développeurs, notre étude souligne le réseau d'acteurs au sein duquel ceux-ci évoluent. Ce réseau est à géométrie variable, différant selon les demandes du client, les habitudes du développeur, la plateforme de développement etc. Le développement d'une application mobile constitue, ainsi, un processus complexe, mêlant différents acteurs et sources d'autorités, aux intérêts parfois convergents, parfois divergents (un de nos interlocuteurs a par exemple souligné ses difficultés à travailler avec le département « *marketing* » de certains de ses clients, ces personnes se représentant l'application en termes d'image et non en termes d'utilité).

---

[2] Extrait traduit de l'anglais par les auteurs de cet article.

RENDRE COMPTE DES RISQUES LIÉS AUX APPLICATIONS

En créant une application recourant à la géolocalisation, le développeur participe à un système comportant des risques potentiels pour l'utilisateur. En employant une application *location-*, *context-* ou *user-aware*, l'utilisateur court le risque de diffuser ses données de localisation à des tiers, notamment au « *service provider* » (c'est-à-dire au client du développeur, souvent par l'intermédiaire du développeur lui-même). En outre, l'utilisateur court le risque, lorsqu'il se sert d'une application *user-aware*, d'être profilé et « trié » par le logiciel. La logique algorithmique de ces applications a, en effet, la capacité de profiler différents types d'utilisateurs, et peut potentiellement être à la base de nouvelles formes de discriminations. Dans cette partie de notre analyse nous souhaitons explorer les façons par lesquelles nos interlocuteurs se positionnent par rapport à ces deux types de risques.

Les risques d'atteinte à la sphère privée de l'utilisateur

Lors de nos entretiens, nos interlocuteurs sont souvent venus d'eux-mêmes sur les problèmes de « *privacy* ». Ceux-ci semblent particulièrement conscients de la nature privée des données en présence desquelles ils peuvent se retrouver ; ils évoquent à diverses reprises les précautions prises autour de la manipulation de ces données :

> *Nous quand on est amené à traiter ça, on anonymise. C'est-à-dire que... Même les clients font très attention. On signe des clauses déjà avec le client comme quoi on s'engage à n'utiliser les données que dans le cadre strict du projet, on s'engage à détruire les données une fois qu'on les a... Et puis encore une fois ils nous transmettent les données sans l'identifiant qui nous permet de raccrocher à une personne... Donc on est déjà sensibilisé à cela, et c'est ce que l'on essaie de faire...* (David Beni, ingénieur, spécialisé dans les SIG et les services géo-informatiques).

Toutefois, lorsqu'un utilisateur se sert d'une application *smartphone*, il n'a pas de réel moyen de contrôler que ses données ne sont pas utilisées à mauvais escient. Les développeurs que nous avons interrogés nous ont pour la plupart relaté un épisode d'abus, où des données avaient été prélevées à l'insu des utilisateurs par le *service provider* : hormis l'affaire du « *Wi-Spy* » de Google Street View (BBC News, 09.07.2010) – qui n'est pas directement en lien aux applications mobiles – deux de nos interlocuteurs ont évoqué le récent scandale autour de l'application « *Path* », qui envoyait sur l'un de ses serveurs l'ensemble du carnet d'adresses de ses utilisateurs (blog d'Arun Thampi, 08.02.2012). Comme l'illustre le cas de « *Path* », les risques que court l'utilisateur ne sont pas uniquement liés à ses données de localisation. Ces dernières constituent, toutefois, des données particulièrement sensibles, car elles permettent d'inférer énormément d'éléments sur la vie de l'utilisateur : "*Safeguarding location information is just one of the many « data point » that make up the attitude and behavior of people, yet it is a particularly powerful one, as a place is often tightly connected to an activity (e.g. a shopping mall, an office), an interest/belief (e.g. a church, a political rally), or a personal attribute (e.g. a* prison*, a clinic)*" [Scipioni & Langheinrich, 2010, p. 2]. Ainsi, malgré leur anonymisation, ces données permettent d'être relativement facilement rattachées à l'identité de l'utilisateur [*Ibid.* 2010, p. 2].

Pour nos interlocuteurs, toutefois, le risque de se faire « traquer » n'est pas spécifiquement lié à l'utilisation de la géolocalisation. En effet, comme plusieurs d'entre eux l'ont souligné, le simple fait de posséder un téléphone portable permet déjà aux opérateurs téléphoniques de savoir où vous êtes, ceci sans même que ne soient activés le GPS ou une application de géolocalisation. En soulignant que cette surveillance n'est pas spécifiquement liée à l'utilisation de la géolocalisation, certains de nos acteurs montrent une

certaine résignation face à ce risque qui, de toute façon, existe déjà du simple fait de posséder un téléphone portable. Cette résignation s'exprime*, a fortiori*, dans le discours de certains de nos interlocuteurs, évoquant le risque d'exposer ses données personnelles comme le prix à payer pour obtenir un service utile.

> *Oui, moi je suis un pragmatique, je pense que c'est inévitable, qu'il ne faut pas se battre là contre et que du moment qu'il y a un service rendu... Moi par exemple je suis prêt à ce que Google sache où je me trouve, ce que j'ai fait… […] En contrepartie, ils me fournissent Google Maps gratuitement. […] Donc c'est un système qui est... qui est équitable.* (David Beni, ingénieur, spécialisé dans les SIG et les services géo-informatiques).

> *Je peux savoir les horaires du tram, je peux savoir s'il y a un bancomat tout proche et savoir s'il y a un Coop pronto ouvert dans le coin… […] Tous ces avantages-là, si on est conscient de cela... il est évident qu'ils sont beaucoup plus grands que les désagréments qui peuvent être les... violations de la vie privée,... Après c'est à chacun de savoir où sont les limites.* (Adrian Kosmaczewski, développeur *iPhone*)

Ce qui est interprété comme une forme de résignation face à la dimension intrusive de ces technologies, peut également se lire comme une redéfinition par ces acteurs de ce qu'ils considèrent « privé ». De même que le téléphone portable a redessiné les lignes de démarcation entre espaces privés et publics en amenant dans la rue des conversations d'ordre souvent personnel [de Souza e Silva, 2006, p. 118], la définition de ce qui constitue une « donnée privée» peut varier d'une personne à l'autre et passablement se transformer au contact des NTIC. Cette renégociation de la limite du privé s'illustre notamment dans la citation suivante :

> *[…] Disons que je suis moins catégorique sur la question de la vie privée maintenant... Il y a des choses évidemment que je... Maintenant, il y a les assureurs qui proposent de mettre un GPS dans la voiture, pour connaître ta manière de conduire et tout... Ça, ça m'embêterait un peu quand même. Pour l'instant. Peut-être que mes enfants ils diront : on s'en fiche !* (Stéphane Burlot, développeur *iPhone*)

Ainsi, à l'heure où les gens exposent volontairement certains aspects de leur vie privée sur les réseaux sociaux, la question de la protection de la sphère privée des utilisateurs semble une problématique remplie d'ambiguïtés. Face à cela, Scipioni et Langheinrich [2010] définissent la « *privacy* » comme : "*the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others*". Le fait que l'utilisateur d'une application puisse difficilement contrôler l'utilisation faite de ses données, indique que ce « libre choix » n'est pas garanti. L'utilisateur n'a guère d'autres possibilités que d'espérer que ses données ne soient pas prélevées à son insu. Face à un système opaque, où il n'a pas véritablement moyen de contrôler ce qu'il advient de ses données, l'utilisateur n'a d'autre choix que de faire confiance au *service provider*. Cette confiance aveugle dont il doit faire preuve, dévoile un certain déséquilibre des pouvoirs entre l'utilisateur et le *service provider*. La capacité inégale qu'ont ces deux acteurs à maîtriser le système, révèle à nouveau l'autorité dont disposent les concepteurs et diffuseurs d'applications *smartphone*.

Les risques de profilage et de « *software-sorting* »

Outre leurs dangers en termes de « *privacy* », les applications *user-aware* (personnalisant l'information en fonction de l'utilisateur) présentent des risques liés au « *software-sorting* ». Les opérations de profilage et de tri qu'opèrent ces logiciels, peuvent potentiellement être à la base de nouvelles formes de discriminations inscrites dans le code et performées par celui-ci [Graham, 2005].

Lors de nos interviews, nos interlocuteurs se sont peu exprimés sur les risques liés à ce type d'applications. Ceci provient probablement de leur non-implication dans ce type de développements. De nos six interlocuteurs,

un seul avait collaboré à la création d'un tel logiciel et en connaissait précisément les logiques de fonctionnement. Toutefois, la possibilité de personnalisation liée au software sorting a été évoquée par l'un de nos acteurs, comme l'une des possibles caractéristiques de l'application « du futur ».

> *Le futur ça serait... Bon, là il y a des problèmes de... de vie privée... Mais ça serait une application qui me localiserait tout le temps, tout le temps, tout le temps... Et puis il faudrait qu'elle sache ce qui m'intéresse... […] Et qu'elle me dise : « ben tiens puisque tu aimes les sushis, et bien il y a un resto de sushi, là, qui est pas mal »... Avec le risque que le programme me propose toujours ce dont j'ai envie... (Stéphane Burlot, développeur iPhone*).

Derrière le « *risque que le programme me propose toujours ce dont j'ai envie* » énoncé par ce développeur, se dessine l'action de tri et de catégorisation que réalisent ces programmes, sélectionnant automatiquement une partie de la réalité à afficher à l'utilisateur et médiatisant, ainsi, de façon assez exclusive son rapport à l'espace. Toutefois le risque qu'évoque notre interlocuteur n'a pas directement trait aux mécanismes de discrimination qu'évoque Graham en parlant de *software sorting*. En quoi l'action « personnalisante » d'un logiciel *user-aware* peut-elle s'actualiser en un processus discriminatoire ? L'extrait suivant illustre, à notre sens, le potentiel discriminant de tels développements. Dans cette citation, notre interlocuteur expose comment l'application *user-aware* développée par sa société, reconnaît et exclut les « spammeurs » du système (les utilisateurs malintentionnés qui posteraient un commentaire dénigrant sur un établissement, lieu, ou monument) :

> *Si A, B, C, D jusqu'à Y disent que ce truc est bien et que Z dit que ce truc est pas bien, le système va réussir à avoir l'intelligence de dire : « bon ben si il y a 25 personnes qui adorent ce bien et qu'il y en a un dernier qui n'aime pas… ». Ce dernier va être petit à petit exclu, ne va pas faire partie du réseau de confiance... Donc il va s'éliminer, il va s'auto-éliminer. Si bien qu'à la fin pour faire très simple les tags sont classés dans l'ordre de pertinence grâce à cette confiance créée entre les utilisateurs, et donc implicitement celui qui aura mis un mauvais tag sera exclu du système et sera moins pris en compte...* (David Beni, ingénieur, spécialisé dans les SIG et les services géo-informatiques).

L'exclusion de Z est peut-être bénéfique pour A, B, C etc. qui ne seront pas importunés par son commentaire à contre-courant. Toutefois, la situation semble moins avantageuse pour Z qui n'est peut-être pas un utilisateur malintentionné mais simplement quelqu'un dont les goûts ne correspondent pas au « *mainstream* ». Bénéficiera-t-il du même service que les autres utilisateurs si personne ne rejoint son opinion ? Même s'il diverge des autres, son avis ne mérite-t-il pas être pris en compte plutôt que d'être exclu ? En rendant compte des solutions algorithmiques permettant de mettre à l'écart les spammeurs, notre interlocuteur ne thématise aucunement le danger de discrimination lié à ces systèmes. L'absence de thématisation de ce risque s'exprime à plus forte raison dans le fait que le *software sorting* est plutôt perçu comme un développement positif. Notre interlocuteur souligne, ainsi, l'intelligence de ces logiciels, capables de personnaliser leur message, et d'éviter que l'utilisateur ne se perde dans un trop plein d'informations.

> *En tant qu'usager moi je trouve ça souhaitable, c'est-à-dire que j'y vois un intérêt de... On voit aujourd'hui la tonne d'e-mail que l'on reçoit, la tonne de papier que l'on a chez nous, la tonne de publicité partout, la masse d'informations qu'on a dehors... Eh bien si demain le monde nous permet d'avoir une information qui soit ciblée et qui en plus m'apparaît comme... En plus d'être ciblée elle est absolument pertinente.* (David Beni, ingénieur, spécialisé dans les SIG et les services géo-informatiques).

Si la question de la « *privacy* » a d'emblée été évoquée par nos interlocuteurs en tant que « risque », le *software sorting* n'a, quant à lui,

pas fait l'objet de la même labellisation. Pour ces développeurs, la logique de profilage que possèdent les applications *user-aware* n'est pas perçue comme problématique. N'ayant pas conscience de ce risque, leur part de responsabilité dans la programmation de ces algorithmes – potentiellement discriminants – n'a pas été abordée lors de nos entretiens.

RESPONSABILITÉ DU DÉVELOPPEUR

De par le rôle crucial qu'il joue dans la production d'une application *smartphone,* le développeur participe à la production des risques mentionnés auparavant. Dès lors, se pose la question de sa responsabilité face à ces risques ; ceci d'autant plus que le développeur serait l'acteur-clé, capable de réfléchir aux solutions techniques garantissant la sécurité des données personnelles de l'utilisateur [Scipioni & Langheinrich, 2010 ; Goold, 2009]. Dans cette partie, nous abordons les façons par lesquelles nos acteurs rendent compte de leur responsabilité face aux dangers précédemment évoqués. Nous traitons ici de leur part de responsabilité face à ce qu'ils ont eux-mêmes qualifié de « risque », à savoir les problèmes que posent leurs logiciels du point de vue de la « *privacy* » des utilisateurs.

Transfert de responsabilité

Conscients de la dimension potentiellement intrusive des applications de géolocalisation, nos acteurs ont plusieurs fois évoqué les mesures mises en œuvre afin de réduire ce risque (anonymisation, destruction des données, etc.). L'une des régulations les plus souvent énoncées par nos interlocuteurs, est celle d'informer l'utilisateur des données qu'il va potentiellement « divulguer ». Lorsqu'une application doit accéder à des données personnelles (le carnet d'adresses de l'utilisateur, son compte *Facebook*, ses données de localisation), l'utilisateur doit en être informé et doit pouvoir accepter ou refuser cette requête en connaissance de cause. Dans le discours de nos acteurs, il semble que cette règle d'or ait valeur d'éthique implicite :

> *Alors l'autre jour (…) c'était la grande discussion sur Internet : il y a un réseau social qui s'appelle "Path" […] Il se trouve que ce logiciel, pompait tout l'Address Book de l'utilisateur, et l'envoyait dans un serveur de "Path"... […] on ne sait pas ce qu'ils en faisaient... Le problème est que l'utilisateur n'était pas averti... Ce n'est pas le problème qu'ils fassent ça. Il y a pas mal d'applications qui font ça pour te dire : « Sarah Widmer utilise Facebook, connecte-toi à Sarah Widmer » ça arrive tout le temps ! Par contre, tu dois me donner la possibilité de ne pas le faire. C'est là où « Path » a fait un faux pas... […] il n'a pas du tout informé qu'il faisait ça ! Et c'est cela, le gros problème.* (Adrian Kosmaczewski, développeur *iPhone*).

Lorsqu'il se sert d'une application, l'utilisateur doit pouvoir choisir, en accord avec la définition qu'il se fait de sa sphère privée, si oui ou non l'application peut accéder à certaines de ses données. Selon certains de nos acteurs, c'est donc à l'utilisateur d'être conscient des risques et de choisir en conséquence s'il veut ou non recourir au service proposé :

> *De dire voilà, […] on va prendre des informations, mais on ne va rien faire avec... Mais tu peux toujours dire non... Et puis, tu peux toujours désinstaller l'application si tu n'es pas content...* (Adrian Kosmaczewski, développeur *iPhone*).
>
> *Il suffit de demander. Et là il dit OK ou il dit non. On démarre une application, elle dit : « Tiens on aimerait avoir des informations géolocalisées est-ce que vous est d'accord ? »... Ça passe par ça... Alors c'est vrai qu'après il y à des applications qui sans ça ne sont plus tellement utilisables... À chacun sa liberté !* (Fiorenzo de Palma, développeur de l'application des transports publics lausannois).

Comme le révèlent ces deux extraits, l'utilisateur a le pouvoir de dire « non ». Pourtant, entre le « ok » et le « non », ne s'offrent pas énormément d'options : soit l'utilisateur accepte de prendre un risque, soit il renonce au service qu'offre l'application ; ce manque de solutions intermédiaires est quelque chose que relèvent aussi Scipioni et Langheinrich [2010, p. 2] : « *[…] it forces people to choose between « on » and « off », between « black » and « white », without considering all those « grey » levels that a dynamic privacy negociation process usually involves* ». Il semble qu'une fois l'utilisateur informé, la responsabilité du risque passe entre ses mains. Les demandes d'autorisation fonctionnent donc comme une forme de contrat : si l'utilisateur accepte ces conditions alors la responsabilité du risque lui incombe. Face aux risques que présentent les applications, plusieurs de nos acteurs préconisent de conscientiser l'utilisateur, de l'éduquer à ces nouvelles technologies afin qu'il les utilise en pleine connaissance des règles du jeu. La plupart de nos interlocuteurs tendent donc à transférer la responsabilité du risque (ou du moins sa gestion) sur les utilisateurs des applications de géolocalisation.

Régulations possibles

Il est intéressant de voir que, pour nos acteurs, la responsabilisation de l'utilisateur prime sur d'autres formes de régulations du risque. Par exemple, la recherche de solutions « *privacy-aware* » et leur intégration au sein des pratiques de développement n'ont pas été évoquées. La possibilité d'une régulation juridique de ce domaine a, quant à elle, fait l'objet d'une vive opposition de la part du seul de nos interlocuteurs à avoir mentionné cette idée.

Toutefois, un mécanisme de régulation « indirect » a plusieurs fois été abordé : il s'agit d'une sorte de « régulation par le scandale » :

> *[…] Donc je pourrais stocker les restaurants qu'il a cherché le plus souvent, je pourrais regarder quel restaurant il a mis dans les favoris […] Toutes ces informations, je pourrais les transmettre à un serveur. Si maintenant quelqu'un s'aperçoit que je fais ça, le retour de flamme est monumental ! Et c'est extrêmement, extrêmement dangereux ! (*Stéphane Burlot, développeur *iPhone*)

Ainsi, le risque d'être au cœur d'un scandale, inciterait les « *service providers* » à respecter la nature privée des données des utilisateurs et à ne pas exploiter celles-ci de façon abusive. Cette régulation par le scandale repose sur une mobilisation sociale (de la presse, des blogueurs influents, des utilisateurs *via* le *boycott*) dénonçant les abus. Toutefois, cette régulation repose également sur la maîtrise d'outils informatiques : pour révéler un abus, il faut pouvoir analyser le trafic des données « sortant » du *smartphone* lors de l'utilisation d'une application. La citation suivante évoque de quelle manière le scandale de « *Path* » a été révélé. Elle illustre les nombreuses médiations technologiques intervenant dans cette forme de régulation :

> *Et bien, en fait ça a été un développeur, qui était en train de faire... ce que l'on appelle une « analyse des paquets », des paquets de données... C'est-à-dire que tu mets un Sniffer - c'est un logiciel qui se met entre tout ce qui se passe d'un côté et de l'autre de ton câble. Et ce logiciel-là garde une trace de tout ce qui se passe... Et il a commencé à analyser tout ce qui sortait de son iPhone... Et tout d'un coup il voit que vers les réseaux de Path, il y avait un paquet de données qui contient tout son Adress Book compressé... […] Et puis ce développeur a publié un blog-post avec ses trouvailles... Dans Twitter, en moins de deux heures je crois qu'il a eu à peu près 150 000 visites, son blog a explosé ! (*Adrian Kosmaczewski, développeur *iPhone*).

Comme le précise notre interlocuteur, se trouve à l'origine de cette découverte un informaticien. Contrôler les abus nécessite donc de disposer du matériel et du savoir-faire permettant d'analyser les flux de données. Ceci atteste à nouveau de l'importance que détient actuellement l'expertise informatique dans nos sociétés. Ce résultat vient également s'ajouter aux diverses études relevant la logique « anti-démocratique » prévalant dans

la production de logiciels [Dodge, Kitchin & Zook, 2009 ; Wood & Graham, 2006]. En se basant sur des savoir-faire complexes et spécialisés, le fonctionnement et la régulation de ces systèmes deviennent de plus en plus opaques et distants des utilisateurs finaux.

CONCLUSION

Cet article rend compte du rôle et des responsabilités d'acteurs particuliers, intervenant de façon croissante dans la gestion de notre mobilité : les développeurs d'applications de géolocalisation pour *smartphone*.

Les logiciels que mettent au point ces acteurs visent à « augmenter » les mobilités en numérisant nos localisations, activités et préférences. Or, ces applications (*location-, context-* et *user-aware*) comportent, de par leur fonctionnement même, une série de risques, en termes d'atteintes à la sphère privée et de « tri social ». Les « mobilités intelligentes » issues de l'utilisation de ces logiciels ne vont donc pas sans leurs corollaires : des mobilités surveillées et gérées de façon automatique par du code informatique.

Dans cet article, nous avons abordé cette problématique au travers du regard des concepteurs d'applications. Notre étude met en avant l'autorité prégnante que détiennent ces acteurs ; une autorité ancrée dans un savoir-faire technique spécifique, leur permettant d'agir à la fois sur le fonctionnement et – par là même – sur les risques et régulations de ces logiciels.

Toutefois, notre étude tend également à relativiser le rôle central des développeurs étudiés, en démontrant leurs engagement et limitations au sein d'un vaste réseau d'acteurs. Se présentant tour à tour comme subordonnés aux demandes de leurs clients, dépendants du *feedback* des utilisateurs, et soumis aux exigences d'*Apple*, nos interlocuteurs ne se perçoivent pas comme détenteurs d'une autorité absolue ou exclusive, régissant l'élaboration de logiciels pour *smartphones*.

Pour nos interlocuteurs, la complexité de ces réseaux d'acteurs semble aussi avoir pour effet de « diluer » leur responsabilité en matière de régulation et de contrôle du bon usage des informations accumulées et codées. Ceci nous incite grandement à reposer la question des mesures et stratégies possibles pour prévenir et limiter les risques induits par l'informatisation croissante de notre quotidienneté. À qui attribuer la responsabilité de veiller aux limitations des nouvelles formes et formats de surveillance ? Comment définir les modalités et la portée de ces limitations ? Comment garantir une régulation continue de systèmes en constante évolution (du point de vue de leurs fonctionnalités, diffusion géographique, potentiel de surveillance, etc.) ?

D'un point de vue conceptuel, ces questions nous ramènent en force à la théorie de l'acteur réseaux. Elles nous poussent à compléter la présente analyse avec des études plus approfondies sur le rôle et le savoir-faire d'autres acteurs (les mandants, *Apple*, etc.) contribuant, eux aussi, aux enchevêtrements complexes des diverses sources d'autorité dans la conception, la production et la diffusion de ces logiciels. Malgré la numérisation croissante de nos vies et de nos espaces, nous ne savons guère comment – et par qui – se négocient le développement et la mise en service de nouvelles solutions visant à organiser, diriger, sécuriser, gérer, etc. nos activités quotidiennes.

Dans une même optique, le présent article mérite d'être complété par des études plus poussées, portant sur les utilisateurs de s*martphones* eux-mêmes. Il nous semble primordial de démontrer plus précisément comment ces logiciels sont en réalité vécus, appropriés et renégociés dans leurs utilisations quotidiennes. Ceci pour mieux comprendre les chances et les risques liés à l'informatisation de plus en plus généralisée et banalisée de notre monde actuel.

BIBLIOGRAPHIE

AKRICH M., MEADEL C. (1999), *Anthropologie de la télésurveillance en milieu privé*, Rapport de recherche, Pirvilles-CNRS et Institut des Hautes Études sur la Sécurité Intérieure, Centre de Sociologie de l'Innovation, Paris, École des Mines.

CALLON M., LASCOUMES P. & BARTHE Y. (2001), *Agir dans un monde incertain: essai sur la démocratie technique*, Paris, Seuil.

COLLINS H., EVANS R. (2007), *Rethinking Expertise*, Chicago, University Of Chicago Press.

CUTLER A.C., HAUFER V., PORTER T. (Eds.) (1999), *Private Authority and International Affairs*, New York, Suny Press.

CZEMPIEL E-O. (1992), « Governance and Democratization », *in* J.N. Rosenau, E.-O.Czempiel(Eds.) *Governance without Government: Order and Change in World Politics*, Cambridge: Cambridge University Press.

DE SOUZA E SILVA A. (2006), Re-Conceptualizing the Mobile Phone: From Telephone to Collective Interfaces, *Australian Journal of Emerging Technologies and Society*, vol. 4, n° 2, pp. 108-127.

DE SOUZA E SILVA A., FRITH J. (2010), Locative Mobile Social Networks: Mapping Communication and Location in Urban Spaces, *Mobilities*, vol. 5, n° 4, pp. 485-505.

DODGE M., KITCHIN R., ZOOK M. (2009), How does software make space? Exploring some geographical dimensions of pervasive computing and software studies, *Environment and Planning A*, vol. 41, n° 6, pp. 1283-1293.

GALLOWAY A., WARD M. (2005), Locative Media as Socialising and Spatializing Practice: Learning From Archaeology, *Leonardo Electronic Almanac*, vol. 14, n° 3.

GARCIA-CRESPO A., CHAMIZO J., RIVERA I., MENCKE M., COLOMO-PALACIOS R., GOMEZ-BERBIS J-M. (2009), SEPTA: Social pervasive e-Tourism advisor, *Telematics and Informatics*, n° 26, pp. 306-315.

GOOLD B. (2009), « Building it in: the role of privacy enhancing technologies (PETs) in the regulation of surveillance and data collection », *in* B. Goold, D. Neyland (Eds.), *New Directions in Surveillance and Privacy*, London, Willan Publishing.

GORDON E., DE SOUZA E SILVA A., (2011), *Net Locality: Why Location Matters in a Networked World*, Chichester, Wiley-Blackwell.

GRAHAM S. (Ed.) (2004), *The Cybercities Reade*r, New-York, Routledge.

GRAHAM S. (2005), Software-sorted geographies, *Progress in Human Geography*, vol. 29, n° 5, pp. 562-580.

HECLO H. (1978), « Issue networks and the Executive Establishment », *in* A. King (Ed.) *The New American Political System*, Washington D.C., American Enterprise Institute, pp. 87–124.

KABASSI K. (2010), Personalizing recommendations for tourists, *Telematics and Informatics*, n° 27, pp. 51-66.

KITCHIN R., DODGE M. (2011), *Code/Space: Software and Everyday life*, Cambridge MA, MIT Press.

KLAUSER F. (2009), Interacting forms of expertise in security governance: the example of CCTV surveillance at Geneva International Airport, *British Journal of Sociology*, vol. 60, n° 2, pp. 279-297.

LATOUR B. (1987), *Science in Action*, Cambridge/ Massachusetts, Harvard University Press.

LATOUR B. (2005), *Reassembling the social: an introduction to actor-network theory*, Oxford, Oxford University Press.

LÉVY J., LUSSAULT M. (sous la dir. de) (2003), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris, Belin.

LIPSCHUTZ R.D. (1999), « From Local Knowledge and Practice to Global Environmental Governance », *in* M. Hewson, T.J. Sinclair (Eds;), *Approaches to Global Governance Theory*, Albany, State University of New York Press.

LYON D. (2010), *Surveillance Studies: an overview*, Cambridge, Polity.

MITCHELL T. (2002), *Rule of experts: Egypt, technopolitics, modernity*, Berkeley, University of California Press.

PEER S. (2010), Real-Time Context-Aware Recommendations for Mobile Users, Thesis submitted for the Bachelor of Science in Applied Computer Science, Free University of Bolzano.

ROSEANAU J. (1997), *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*, Cambridge, Cambridge University Press.

SCIPIONI M. P., LANGHEINRICH M. (2010), « I'm here! Privacy Challenges in Mobile Location Sharing », in *Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU 2010)*, May 2010.

SCIPIONI M. P. (2011), « Towards Privacy-Aware Location-Based Recommender Systems ». in *IFIP Summerschool 2011*, Trento, Italy, September 2011.

THRIFT N., FRENCH S. (2002), The automatic production of space, *Transactions of the Institute of British Geographers*, vol. 27, pp. 309-335.

WOOD D., GRAHAM S. (2006), « Permeable Boundaries in the Software-sorted Society: Surveillance and Differenciation of Mobiliy », *in* M. Sheller, J. Urry, (Eds.) *Mobile Technologies of the City*, Abingdon, Routeledge, pp. 177–191.

Sources internet

BBC News, site internet, information du 09.07.2010, page consultée le 22.05.2012. http://news.bbc.co.uk/2/hi/8802741.stm

Mclov.in, blog de Arun Thampi, information publiée le 08.12.2012, site consulté le 22.05.2012. http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html