L'établissement de la confiance dans les médias socionumériques

Coutant, Alexandre

Université de Franche-Comté, laboratoire ELLIADD, équipe OUN
alexandre.coutant@univ-fcomte.fr

1 « Ayez confiance », une injonction plus complexe qu'il n'y paraît

La question de la confiance est régulièrement convoquée lorsqu'il s'agit d'envisager le développement des services par le biais d'Internet. Ainsi de la Loi sur la Confiance dans l'Économie Numérique et de l'encadrement qu'elle propose pour qu'individus et organisations multiplient leurs activités. Ainsi aussi des différents protocoles, normes, labels ou assurances que développent les acteurs d'Internet pour s'assurer la confiance de l'internaute, sujet de préoccupation majeur pour ces derniers (Kaplan, Francou, 2012).

L'origine de cette communication se situe dans un projet de recherche accompagnant le développement d'un service d'identité numérique[1]. Il a été l'occasion d'interroger l'instauration de la confiance dans différents contextes d'interaction en ligne professionnels, amicaux ou marchands. Le service avait effectivement été envisagé initialement pour être employé par les internautes dans le cadre du e-commerce, du commerce entre particuliers, du réseautage professionnel, de la sociabilité et des jeux en ligne. Les enquêtes auprès des usagers pour comprendre comment ils menaient leurs activités dans ces différents contextes ont permis de soulever à quel point l'établissement de la confiance variait dans chaque cas. Ces découvertes ont partiellement remis en cause les représentations des supports sur lesquels faire reposer la confiance qu'avaient les innovateurs, notamment en ce qui concerne la nécessité de l'identification. Elles ont invité à s'interroger sur comment les pratiques analysées s'établissent en fonction de temporalités et de supports diversifiés, en illustrant les voies multiples et complémentaires par lesquelles un sentiment de confiance suffisant s'établit et en plaçant la question de son établissement au delà du rapport à une seule plateforme.

Nous aborderons ici en quoi le développement d'interactions médiées via Internet repose sur tout un écosystème sémiotique aboutissant à une confiance suffisante en nous focalisant sur le cas des médias socionumériques (MS). Ces derniers sont définis comme des « services Internet 1) dont le contenu est très largement produit par les internautes utilisateurs (principe UGC : user generated content), 2) qui regroupent des configurations sociotechniques très variées en termes de dynamique de participation (par intérêt, par amitié) et de visibilité (nature et finalité des données publiées en ligne) » (Stenger, Coutant, 2013 : p. 115).

Les interactions en ligne favorisées par le développement des MS soulèvent en effet des enjeux particuliers de confiance, par la médiation apportée, par le support et les formats de mise en visibilité qu'il rend possibles (Cardon, 2008 ; George, 2009). Un changement qualitatif dans les paramètres de son établissement paraît observable puisque de nombreuses interactions - sociales, informationnelles, professionnelles et même marchandes – se développent sans que les internautes ne ressentent un sentiment de confiance envers le dispositif au sein duquel ils agissent. Phishing, vols d'identité, trolls, surveillance de pair à pair, par les entreprises ou les états sont évoqués sans pour autant que les usagers renoncent à leurs activités (Casilli, 2013 ; Rallet, Rochelandet, 2011).

Ce travail n'a pas vocation à fournir un ensemble fini d'attributs permettant la confiance. Les retours de terrain ont plutôt validé l'hypothèse que les critères jouant dans son établissement diffèrent d'une situation à l'autre. Dans une optique davantage compréhensive, il tentera plutôt d'identifier les dimensions à prendre en compte lorsque l'on souhaite analyser les mécanismes permettant son émergence dans un contexte spécifique.

---

1 Ce travail est principalement issu du projet de recherche « Identic » financé par le secrétariat d'État chargé de la prospective et du développement de l'économie numérique dans le cadre du volet « Web innovant » du plan de relance. Il a réuni le Groupe La Poste, la société My.id et le laboratoire CEREGE de Poitiers dans le but de développer une offre à même de fournir aux individus une identité numérique vérifiée. La deuxième vague d'entretiens a été réalisée dans le cadre de travaux pratiques menés parallèlement à un cours sur l'innovation et sur la conception orientée par l'usager. Elle a mobilisé les étudiants de master 1 de la promotion 2011/2012 du master Produits et Services Multimédias de l'Université de Franche-Comté. Ces derniers ont participé à toutes les phases du recueil ainsi qu'aux premières analyses. Nous voulons ici remercier les différents participants de ces projets.

2 La confiance : un fondement essentiel des interactions ?

Ulrick Beck a démontré comment nos sociétés sont caractérisées par un rapport complexe à notre environnement, fondé sur le risque (Beck 1992). Les individus font effectivement reposer la gestion de leur quotidien sur l'occultation de la complexité du monde, en s'en remettant à des systèmes organisateurs qui leur garantissent une économie cognitive essentielle pour mener leurs activités ainsi qu'une certaine « sécurité ontologique » leur permettant de se représenter un monde relativement connu et stable (Giddens, 1987). Cette délégation repose cependant sur la confiance dans ces systèmes et dans les acteurs qui les composent. Les différentes crises et scandales sanitaires, économiques, politiques ayant marqué le vingtième siècle ont fortement remis en cause l'attribution de cette confiance.

Verin (Laufer, Orillard, 2007, p. 39) soulève que la confiance passe par des constructions narratives et scénographiques. Cette vision fait écho au travail de Quéré (1982), qui inclut la confiance dans la constitution de la compétence communicationnelle. Dans ce modèle, il existe des garants de ces échanges qui permettront le dialogue et qu'il s'agit de mettre en visibilité. La confiance est donc une relation mais aussi une manière de mettre en scène cette relation.

La confiance n'est pas binaire, dans le sens où elle s'établirait ou ne s'établirait pas. Il s'agit davantage d'une perception se fondant sur la prise en compte et l'interprétation d'un ensemble de facteurs humains et non humains qui vont aboutir à un certain niveau de confiance. Celui-ci n'aura pas nécessairement à être maximal pour se révéler suffisant pour que des interactions s'y déroulent, de même que tous les acteurs composant le dispositif ne devront pas nécessairement se voir accorder de la confiance. Elle est un processus collectif proche de ce que Callon, Lascoumes et Barthe (2001 : p. 85) définissent comme une intelligence distribuée.

Un second intérêt de cette vision de la confiance consiste dans le fait qu'elle ne soit pas uniquement fondée sur des éléments extérieurs, mais qu'elle relève aussi des actions des différents interactants. Peretti-Watel (2010 : p. 18) souligne que nous vivons dans une « culture du visible » qui rend complexe de faire face à l'invisibilité de la plupart des risques. Lorsqu'un danger existe, les acteurs souhaitant le faire connaître doivent le constituer en risque. Les enjeux de visibilité associés au développement de la participation sur Internet n'ont été constitué en risque que par l'action de lanceurs d'alerte ayant réussi à les faire reconnaître comme un sujet de préoccupation. De la même manière il est nécessaire, pour les acteurs souhaitant que les risques ainsi mis en exergue n'empêchent pas certaines pratiques, de témoigner de comment ils les ont désamorcés – labels, normes, engagements publics, outils de contrôle individuel de ses traces constituent autant de « gages symboliques » (Giddens, 1987) proposés par les acteurs économiques des MS pour restaurer la confiance des internautes.

2.1 La confiance sur Internet

Cette complexité se retrouve dans le cas d'Internet et des risques associés à son usage. Aux procédures techniques et juridiques cadrant les interactions comme les protocoles sécurisés, les assurances, les conditions d'utilisation, etc. doivent s'ajouter un ensemble d'éléments moins formalisés bien que compris par les internautes. Ces éléments relèvent davantage de la création de la confiance que de la maîtrise effective de l'environnement. Ainsi, on sait que le système Paypal s'est vu associer une forte confiance dès son lancement, bien que la sécurité qu'il offrait à l'époque ait été largement perfectible. Sa reconnaissance relevait davantage de l'engagement qu'il prenait à travers son positionnement en tant qu'offre commerciale que de l'évaluation experte que portaient les consommateurs à son égard.

Les approches par le risque s'avèrent particulièrement pertinentes pour comprendre les crises et scandales que soulèvent les usages d'Internet. Ewald analyse ainsi le sentiment de trahison ressenti dans les scandales sanitaires des vingt dernières années avec des termes qui s'appliqueraient tout aussi bien à l'affaire Snowden, aux failles de sécurité rendues publiques

dans des écosystèmes comme celui de la Xbox, de Snapchat ou de l'Apple Store, ou à la gestion des conditions d'utilisation de leurs services par les grands acteurs d'Internet :

> Dans tous les scandales que les années 1990 ont vu se succéder, le scandale est né d'une situation d'inégalité, d'une situation de dépendance, d'une situation où quelqu'un qui exerçait un certain pouvoir [...] l'a utilisé d'une manière qui a fait courir un risque en plaçant d'autres individus dans une situation de dépendance vis-à-vis d'un risque dont ils ne découvraient l'existence et la nature qu'après-coup (Ewald, 1998, pp. 22-23)

Ces scandales s'avèrent d'autant plus destructeurs pour la possibilité d'une confiance que Quéré (1982) souligne bien que celui qui reçoit un don de confiance contracte des obligations (il faudrait être mauvais pour la trahir) et celui qui fait ce don contracte des droits (celui de se plaindre en cas de manquement). Dans une perspective envisageant la confiance comme le résultat d'un écosystème l'amenant à un niveau suffisant ou non pour que des interactions s'y développent, ces manquements rejailliront sur l'ensemble de l'écosystème. En démontrant que des acteurs, volontairement ou non, peuvent le détourner, ces scandales abaissent le niveau général de confiance. Le baromètre de la confiance des Français dans le numérique, institué depuis 2010 par la Caisse des Dépôts et l'ACSEL, témoigne d'ailleurs de cette forte défiance des Français à l'égard des acteurs du numérique, que de nombreuses enquêtes plus spécifiques d'Internet confirment[2].

Néanmoins, le cas d'Internet possède ses spécificités par rapport aux risques usuellement analysés. L'une d'entre elles est que les mêmes études quantitatives démontrant la défiance des Français à l'égard des acteurs du numérique soulignent aussi le développement des usages de la plupart des domaines de service que propose Internet : e-commerce, mises en relation professionnelles ou amicales, recherche d'informations diverses, actualités, etc. Elles soulignent aussi que les services plus anciens, avec lesquels les usagers sont familiers, se voient accorder davantage de confiance. Le dernier baromètre de la confiance des Français dans le numérique annonce ainsi que s'ils accordent peu de confiance dans les informations diffusées sur les MS et demeurent défiants à l'égard des échanges entre pairs, ils sont en revanche 79% à avoir confiance dans le fait d'acheter des produits ou services en ligne à des enseignes et marques. Ajoutons que les usagers réguliers s'avèrent systématiquement plus confiants dans les réponses qu'ils donnent, ce qui laisse supposer le développement de compétences et habitudes pour évaluer et se sentir à l'aise dans leurs usages. Les garanties évoquées par les interrogés relèvent d'ailleurs des catégories diverses évoquées : techniques (sécurisation des paiements, labels de confiance), réputationnelles (notoriété, recommandations d'autres utilisateurs), de proximité (site français, données stockées en France), voire relevant de l'expérience individuelle (bonnes expériences).

La spécificité de cette décorrélation partielle entre confiance et activité tient sans doute au fait que la sociologie du risque s'intéresse usuellement à des risques peu visibles mais avec un potentiel de dangerosité fort et reconnu (nucléaire, OGM, etc.). Dans le cas, d'Internet, ces risques portent sur des éléments perçus comme relativement anodins (Rallet, Rochelandet, 2011). Dans tous les cas, cet apparent paradoxe justifie l'intérêt d'analyser en profondeur les conditions de l'établissement d'une confiance suffisante pour que des interactions se développent, si manifestement les acteurs du numérique n'en sont pas les garants.

2 Voir http://www.internetsanscrainte.fr/blog-actu/barometre-caisse-depots-acsel-sur-confiance-francais-sur-numerique pour la livraison 2013 du baromètre et http://www.fftelecoms.org/sites/fftelecoms.org/files/contenus_lies/barometre_tns_sofres-la_poste_confiance_numerique.pdf pour la récente édition 2014 et par exemple les résultats d'une étude portant plus spécifiquement sur les opérateurs télécoms http://www.fftelecoms.org/articles/sondage-60-millions-de-consommateurs-les-nouveaux-pieges-de-la-conso-la-confiance-numerique où 74 % des Français déclarent leur défiance à leur égard.

3 Méthodologie

Le projet Identic a nécessité la mise au point d'un recueil de matériaux pluriels associant entretiens compréhensifs individuels et collectifs, observations de forums dédiés aux problèmes d'identités numériques et de sécurité en ligne, test de script de service, suivi des initiatives des acteurs économiques et publics autour des identités numériques, association à la mise en place de la première édition du baromètre sur la confiance des Français dans le numérique, analyse juridique de l'encadrement des activités en ligne des internautes.

La question de la confiance a pu être abordée plus spécifiquement à travers les entretiens compréhensifs (n= 53), menés en 2010 et qui seront principalement employés dans cet article. Les grilles prévoyaient effectivement d'aborder trois thématiques reliées à la confiance des enquêtés : « confiance et risques perçus sur Internet » ; « identification, identité, certification en ligne » ; « méthodes et acteurs susceptibles de réduire ces risques, de garantir plus de confiance en ligne, de certifier l'identité des participants ».

Ce matériau a été complété par une deuxième phase d'entretiens compréhensifs (n= 39) réalisés dans le cadre d'un travail pédagogique sur l'innovation guidée par l'usager, mené avec des étudiants en master Produits et Services Multimédias en 2012. Les entretiens ont consisté à interroger à nouveau les différents usages d'Internet et la confiance sur ces différents espaces.

Dans les deux recueils, la variété a été recherchée en faisant varier à la fois les âges, les PCS, les lieux de résidence et la familiarité à l'égard d'Internet.

La démarche compréhensive (Kaufmann, 2006) convient particulièrement à notre sujet cherchant à comprendre un phénomène apparemment contradictoire. Elle cherche moins à valider des hypothèses qu'à laisser la chance de s'exprimer à des logiques dont la complexité ne les rend pas évidentes aux techniques de mesure habituelles. Elle offre aussi un cadre encourageant la réflexivité des enquêtés, en les aidant à prendre conscience d'usages et représentations qu'ils n'ont pas l'habitude de chercher à expliciter. En effet, les enquêtés n'étaient pas en mesure de lister des critères qui les décidaient à agir. Ceux-ci ont plutôt émergé au cours de la discussion ou par un travail de recoupement et de comparaison, notamment avec les résultats quantitatifs du baromètre sur la confiance, effectué a posteriori par les chercheurs.

4 Résultats

Nos résultats renseignent sur au moins trois types d'acteurs de la confiance dans le cadre des MS: les systèmes, les organisations et les pairs.

4.1 Système

Le rapport aux systèmes a la particularité de reposer essentiellement sur des notions et représentations profanes. Les usagers se révèlent pour la plupart très peu dotés en littératies numériques, qu'il s'agisse de la logique fondamentale de l'informatique ou du fonctionnement des logiciels qu'ils emploient pour accéder aux MS. Les gages symboliques de confiance en prennent d'autant plus d'importance. Les attentes portent sur des questions de sécurité et de garantie de service.

Ainsi, les gages de confiance évoqués passent par des traces comme le « https » ou les logos d'organismes communiquant sur leur service de garantie des échanges comme Fia.net lorsque des sites de CtoC sont employés.

> Avec FIA.net. j'ai déposé une plainte parce que quand même – c'est ce qui aussi met en confiance – le site avait le logo FiA.net #sur son serveur de vente. (…)

Ajoutons une conviction largement partagée que les banques garantissent les vols d'identité bancaires

> - Si tu te fais pirater ta carte bleue sur internet, tu es garanti par la banque
> - Et étant donné que les banques, elles assurent ça…même si ça se passe, elles te remboursent.

Parallèlement à ces garanties de sécurité, la confiance passe par l'encadrement fonctionnel des activités par le site, qui témoigne pour les enquêtés de son sérieux : mails de confirmation, services associés aux échanges permettant d'en apprendre davantage sur les interactants (localisation, avis reçus ou émis, transactions déjà effectuées, etc). Dans cet esprit, la facilité d'accès aux services d'aide en cas de problème d'utilisation fait partie des gages fondamentaux de confiance dans la fiabilité du service. Plus le service est qualitatif (simple mail, possibilité de converser via chat ou numéro de téléphone), plus ces attentes fondamentales seront comblées.

Le critère de simplicité s'avère ici fondamental : les systèmes doivent rendre intelligible et explicite leur fiabilité. L'ergonomie et l'attitude pédagogique dans la conception des interfaces ou des contenus rédactionnels sont alors essentiels. Un enquêté le spécifie clairement à propos de sites proposant aux internautes de participer à différents jeux entre pairs : « en fait, moi j'ai testé les 2, ça va plus être une question d'interface », ou encore « c'est vrai que le site est joli, ça attire ». Elles peuvent en arriver à oblitérer d'autres éléments constitutifs de la confiance. Ainsi, l'exemple de la carte Navigo pointe à quel point l'attention au respect des données personnelles, gage attendu des organisations dans l'ensemble des usages d'Internet, se trouve minimisée par l'attractivité exercée par la simplicité d'utilisation (Levallois-Barth dans Licoppe, 2009). On voit ici que cette simplicité relève des gains à l'usage qui peuvent jouer dans le niveau de confiance face à une perception de risque pourtant avérée. L'enjeu est important car beaucoup d'acteurs des MS conservent la représentation d'un utilisateur (assez) rationnel, conscient de ce qu'il fait, maître des outils qu'il emploie et des informations circulant à son propos (Battisti, 2010, p. 24). C'est ce que fait Google, lorsqu'il fait reposer sa politique à l'égard des données personnelles sur les mots-clés « transparence » (avec Google Dash Board, nouveau service qui fait apparaître sur une seule page toutes les données personnelles de ses comptes sur les services du moteur), « autodétermination » (puisqu'il appartient à l'internaute de décider ce qu'il veut que l'on oublie) et « pédagogie » (illustrée par une charte d'utilisation, traduite en une vidéo sur YouTube pour être plus explicite). Si ces principes répondent partiellement aux attentes des enquêtés à propos de la question sensible de leurs traces personnelles, ils demeurent inconnus de la plupart des internautes faute d'intelligibilité pour des usagers profanes. Ce défaut de lisibilité peut s'étendre selon Battisti à de nombreuses démarches, pourtant louables sur le fond, de privacy by design ou de privacy enhancing technologies (PETs). Ainsi, le succès d'un site de covoiturage comme Blabla Car tient à son système encadrant de manière très pointue les échanges, mais aussi à la capacité du site à traduire cet encadrement dans des mots compréhensibles pour les utilisateurs, notamment en axant directement sa communication sur la confiance avec leur personnage de marque Trustman[3].

4.2 Organisations

Ces gages sont aussi attendus des organisations. La reconnaissance de fiabilité qui peut en découler se traduit cette fois par une attention à la notoriété des organisations. Celles bénéficiant d'une notoriété précédant leurs activités en ligne peuvent ainsi jouer de leur image hors ligne (comme La Poste pour la messagerie électronique par exemple). Bien que les participants restent assez flous sur les critères de choix leur permettant de juger si les organisations sont de confiance ou non, ils se méfient de celles qui sont peu connues, mal agencées et ne disposent pas de gage de sécurité explicite.

> - Après il y a l'aspect général du site, un site qui est fait de brick et de broc il faut s'en méfier. Par exemple, des fois on cherche un matériel spécifique, on arrive sur un site et en fait on se rend compte que le marchand c'est une simple boutique qui appartient

3 http://www.betrustman.com/

> à quelqu'un qui a pas forcément bien fait son site, qui ne l'a pas forcément bien sécurisé.
> - La confiance, parce qu'on nous en a parlé.
> - On cautionne les grosses structures.

La notoriété doit être complétée par les habitudes qu'ont forgées les enquêtés pour comprendre l'élévation progressive du niveau de confiance. On retrouve ce que le baromètre souligne par les « expériences positives » des internautes, qui les sécurise sans qu'ils aient besoin pour autant de comprendre les systèmes sur lesquels reposent ces expériences. Les enquêtés expliquent qu'ils utilisent régulièrement les mêmes sites, par facilité et parce qu'il s'agit de grandes enseignes qui disposent d'une forte notoriété. Ajoutons que les systèmes de personnalisation de ces sites permettent une amélioration de l'expérience de navigation qui constitue un fort levier de captation que Boullier (2009) qualifie de « durée » dans les économies de l'attention.

On voit émerger une chronologie expliquant l'élévation du niveau de confiance et qui passe par une étape initiale où la notoriété et les avis des proches, souvent obtenus hors ligne, amènent aux premières expériences. Les expériences positives ou négatives vont ensuite remplacer ces gages et permettre à l'internaute de se forger une opinion personnelle de plus en plus fine à l'égard des organisations qu'il fréquente.

Un second axe de rapport aux organisations concerne les garanties qu'elles s'engagent à tenir vis-à-vis du cadre des interactions. Ceci est particulièrement explicite en ce qui concerne la sécurité et l'exploitation des données personnelles mais concerne aussi les efforts faits pour aider à qualifier les interactants selon les critères jugés pertinents pour les évaluer, notamment sur les sites de rencontre ou de CtoC. Nous verrons le détail de ces critères à propos de la confiance entre les pairs, mais les enquêtés associent aux organisations la responsabilité de cadrer cette mise en visibilité des interactants.

En ce qui concerne les traces personnelles, si les enquêtés comprennent, à défaut de toujours accepter, que la gratuité de certains services implique cette exploitation, ils en concluent que les organisations ne peuvent pas se voir accorder de confiance sur un usage modéré de ces traces. Le profilage par les organisations constitue moins pour eux un risque qu'un prix à payer, plus ou moins acceptable selon les cas : « Ce n'est pas un risque, c'est juste que … c'est pas un risque en soi… c'est plus une gêne qu'un risque ! ». Un profilage amènera à limiter les interactions ou à changer de plateformes uniquement s'il est excessif (newsletters, pubs, etc). Les enjeux économiques discréditent cependant les organisations sur leur moralité et les gages de confiance attendus sont donc davantage extérieurs - labels d'organismes reconnus, notamment la CNIL -, ou proximité, les organisations domiciliées en France étant soumises au respect du droit français. Les enquêtés témoignent d'une assez forte confiance à son égard. Si les risques de surveillance étatiques sont aussi évoqués, ils le sont de manière assez détachée, comme risque potentiel, uniquement si nous passions dans un régime moins démocratique. Par exemple, l'encadrement étatique du marché du jeu en ligne est perçu comme garantie de confiance par les enquêtés, à défaut d'être apprécié par les joueurs qui se retrouvent isolés d'une grande partie de leurs partenaires potentiels. Une nouvelle interrogation de ce rapport confiant à la protection de sa vie privée dans les démocraties serait intéressante aujourd'hui pour évaluer si les révélations en cascade initiées par l'affaire Snowden ont modifié cette représentation.

À la différence du rapport aux systèmes, l'évaluation se situe donc sur la moralité reconnue et non sur la compétence. Concernant les grands acteurs des MS, les enquêtés entretiennent à la fois un rapport de reconnaissance d'une maîtrise technique du système et une forte défiance à l'égard du respect des traces personnelles.

Soulignons un paradoxe « du messager » dans ce rapport aux organisations. En effet, le niveau relativement faible de perception des risques par les usagers aboutit à une situation délicate pour les organisations jouant sur des gages de confiance. Les internautes n'étant pas nécessairement conscients des enjeux portant sur le développement de leurs identités numériques, les

organisations sont effectivement très attentives à ne pas éveiller de craintes chez eux. Ce risque s'est révélé lors de la mise en place de la phase de test à grande échelle du projet Identic. Les partenaires potentiels ne souhaitaient pas s'associer à moins que tous ne le fassent en même temps. Proposer un service garantissant une identité présentait le risque pour eux de pousser les usagers à imaginer qu'il existe des problèmes d'identité et à briser la confiance dans les usages existant. Dans le cadre des réseaux socionumériques cela revenait selon eux à soulever un risque que les usagers n'évoquaient pas et dans le cadre du CtoC le risque était que les interactants ne veuillent commercer qu'avec ceux ayant effectué cette authentification. Le *statu quo*, même imparfait, leur convenait donc davantage. Cette situation délicate se trouve bien exemplifiée par le cas des comptes vérifiés de Twitter : ce service permettant de faire authentifier son compte est présenté par l'organisation comme s'adressant uniquement aux personnes célèbres et organisations, dont l'usurpation d'identité pourrait faire peser un risque sur leur image publique, mais ne revêtant pas d'intérêt pour un utilisateur courant.

Enfin, soulignons un dernier point expliquant que les interactions se développent dans un climat de relative défiance à l'égard des organisations qui les accueillent. Les garanties morales comme de cadrages ne sont effectivement pas suffisantes aux yeux des usagers, notamment en ce qui concerne les plateformes ayant fait face à des polémiques médiatisées. Cependant, les enquêtés continuent de les employer. Cet usage en situation de défiance repose sur des braconnages dans les informations transmises. Les enquêtés se rejoignent sur le fait que, par défaut, toute information jugée non essentielle n'est pas renseignée ou renseignée avec de fausses informations. Cette pratique permet de soulever une décorrélation entre ce que peuvent demander les organisations sur les internautes et l'établissement de la confiance entre pairs. Les internautes acceptent que de fausses informations circulent tant qu'elles ne se révèlent pas importantes pour le contexte d'usage particulier.

4.3 Pairs

Si les critères d'établissement de la confiance associés aux systèmes se regroupent autour de leur rôle de garants du cadre des interactions, les critères concernant les pairs vont davantage varier selon le type d'usage concerné.

Les gages de confiance attendus varient sensiblement selon le contexte et la finalité de l'usage. Par exemple, les enquêtés considèrent qu'un lien avec l'identité réelle d'un interactant est un gage de confiance pour le CtoC, mais inutile pour le jeu en ligne. De même, le CtoC renouvelle une forme de confiance par la proximité régulièrement rencontrée dans le commerce classique, où les consommateurs ont davantage confiance dans les commerçants locaux que dans les grands distributeurs. En revanche, lorsqu'il s'agit d'avis sur un produit, c'est le fait de l'avoir expérimenté dans des conditions similaires qui rentre en considération. Ces échanges à propos de la possibilité d'authentifier les interactants sur un site de CtoC illustrent comment un même gage se voit accorder une valeur différente selon le cas :

> - Là où il aurait le plus d'utilité c'est pour le commerce entre particuliers.
> - Moi, je vois un intérêt pour l'acheteur que le vendeur soit certifié.
> - Tu ne peux pas à la fois demander que le vendeur soit certifié et pas toi derrière comme acheteur. C'est moi je me cache, montre toi et moi je me cache.

Puisque le même service est envisagé différemment dès lors qu'on aborde les sites de sociabilité :

> Excusez-moi, je ne vois pas en quoi certifier que celui qui met le commentaire c'est bien moi change ma vie.

Ces critères variables peuvent aboutir à des conflits dus à des oppositions de régimes normatifs Par exemple, dans les discussions ayant lieu sur les forums, blogs ou espaces de discussion des sites informatifs, les interactants demandent aux anonymes de s'identifier s'ils veulent que leurs

propos se voient accorder une légitimité. Les normes sociales s'opposent ici aux normes de droit préservant l'anonymat.

Évoquer ces régimes normatifs permet de soulever un second point majeur de l'établissement de la confiance entre pairs. Celui-ci repose sur la mise en place très rapide de normes d'interactions sur les différentes plateformes, qui permettent aux internautes de savoir ce qu'ils peuvent dire ou ne pas dire, quels sujets, forme d'engagement, ménagement de la face, distance au rôle, invention de soi et écart par rapport à son identité hors ligne sont tolérés. Ce constat déjà effectué à propos des réseaux socionumériques (Coutant, Stenger, 2010) est régulièrement confirmé par les enquêtes ethnographiques sur différentes plateformes des MS[4]. Ainsi, le ménagement mutuel est respecté sur Facebook tandis que la violence et l'indiscrétion des échanges sur Ask sont modalisées par l'emploi de marques attestant que l'on se situe bien dans un cadre où celle-ci est acceptée, notamment par l'emploi du « Ask Me Anything » (AMA). Ces éléments actualisent pour chaque contexte d'usage ce qui a très tôt émergé autour de la nétiquette. Ils permettent de constater qu'autant les littératies numériques sont difficilement maîtrisées et peu partagées par les internautes lambda, autant ces cadres se transposent beaucoup plus aisément à partir d'autres contextes, hors ligne ou en ligne, pour encadrer les interactions sociales. Cette relative facilité avec laquelle les cadres sociaux des interactions se mettent en place explique certainement que des figures anxiogènes régulièrement évoquées dans les médias (pédophiles, violeurs, hackers) soient connues, citées, sans pour autant sembler avoir de répercussion sur les usages.

Une autre dimension évoquée avec les enquêtés concerne les avis en ligne. Ces derniers sont bien conscients des tentatives de manipulation des organisations mais continuent d'y faire appel. Le niveau suffisant de confiance s'explique cette fois par l'application de grilles d'évaluation de ces avis bricolées d'une manière qui leur semble susceptible d'écarter les faux commentaires. Ils accordent effectivement beaucoup d'importance au nombre d'avis afin de ne pas donner trop de poids à un avis isolé. Ils les complètent en multipliant les sources en ligne ou par l'avis de leurs connaissances, voire par des informations plus officielles des organisations. Ils excluent enfin automatiquement les commentaires trop élogieux qu'ils suspectent d'être un discours commercial, écrit par le commerçant lui-même.

> - Quand je trouve un produit ou un article très intéressant sur un site que je ne connais pas, j'essaie d'aller sur d'autres moteurs de recherche pour avoir des avis sur ce commerçant-là.
> - Je crois que c'est sur le nombre d'avis que ça joue.
> - Le mieux, c'est d'avoir des bons avis sur des sites différents.

Soulignons enfin un point étonnant. Le phishing, s'il est évoqué à propos du vol d'identité bancaire, n'est pas craint dans les relations entre pairs. Pourtant, les cas de vol de profil ne s'avèrent pas rares dans les entretiens. On peut rapprocher cette indifférence de l'opinion fortement partagée que leurs comptes sur les MS ne représentent pas un intérêt justifiant que quelqu'un cherche à les voler ou les usurper.

Au contraire, les enquêtés soulignent l'aspect multisupports de la plupart des pratiques menées sur les MS. En effet, l'usage d'une plateforme s'insère en général dans une pratique plus large où d'autres supports sont employés, sur des temporalités parfois élargies. Cette multiplicité est particulièrement patente dans le cadre des usages professionnels des MS, où les occasions de contacts passent aussi par des relations hors-ligne. Le multicanal protège donc de l'usurpation. Par ailleurs, les professionnels se contactent autour de leurs compétences, qui rendent difficile d'envisager un vol d'identité pérenne. Ces liens hors ligne / en ligne ressortent aussi souvent dans le CtoC. Cela permet de se rappeler à quel point les deux sont liés et les gages de confiance passent par de multiples canaux, en ligne comme hors ligne. On repère aussi cette multiplicité dans les jeux en ligne. La plupart du temps, l'identité des partenaires n'est pas importante et

4 Voir par exemple les régulières enquêtes financées par la Fédération Française des Télécom : http://www.fftelecoms.org/

lorsque les joueurs se retrouvent avec des connaissances, ils se sont échangés leur pseudonyme par d'autres voies.

En synthèse, soulignons la différence radicale des rapports de confiance selon que l'on envisage des personnes physiques ou des systèmes et organisations. Là où les seconds sont plutôt à envisager comme une absence de défiance, les premiers reposent sur de multiples voies de son établissement. Par ailleurs, son établissement n'est pas général mais granulaire : les usagers peuvent avoir confiance dans une organisation pour sa capacité à fournir un service mais pas pour leur respect des données personnelles.

5 Une confiance pluridimensionnelle, relationnelle, située et processuelle

Ces différents résultats valident l'idée que le développement d'interactions repose moins sur l'établissement d'un climat de confiance général que sur une garantie suffisante, prise en charge par un ensemble d'acteurs humains et non humains. L'évaluation de cet écosystème et du niveau suffisant de confiance (plus exactement d'absence de défiance) passe par la prise en compte de quelques critères concernant les risques mais aussi les bénéfices associés à l'usage. À ce titre, le paradigme psychométrique (Slovic, 2000) pourrait expliquer que le développement des interactions sur Internet repose davantage sur une absence de défiance forte que sur une véritable confiance Rappelons que cette explication par le paradigme psychométrique ne rend pas compte des risques effectivement encourus par les internautes mais bien de leur perception de ceux-ci. Ainsi, aux yeux de nos enquêtés, les risques encourus demeurent relativement contrôlables : il suffit de cesser d'employer un service s'il est estimé trop dangereux. Les usages analysés dans nos enquêtes sont souvent multisupports et parfois même perçus comme non essentiels. Le sentiment de ne pas pouvoir trouver d'alternative n'est donc pas rencontré. Ces usages relèvent aussi d'activités volontaires de la part des individus et n'ont de caractère subi qu'indirect (notamment par le sentiment d'être « accrocs » à certains services). En ce qui concerne le caractère connu ou mystérieux des risques, les enquêtés estiment plutôt bien appréhender leurs conséquences. Ils ne sont d'ailleurs pas ressentis comme graves. Si l'exploitation des traces personnelles constitue un sujet de préoccupation et rencontre une forte opposition, les conséquences associées ne sont pas perçues comme profondément négatives (par exemple le profilage publicitaire) et s'inscrivent dans une évolution du rapport à la visibilité des zones de l'intime qui rend moins problématique certaines formes d'exposition. Ajoutons que les normes d'interaction sociales se sont rapidement mises en place sur les différentes plateformes et ont ainsi contribué à encadrer le dicible et l'indicible, diminuant d'autant les risques d'expression d'éléments inappropriés. Les risques de vol d'identité bancaire sont estimés assurés par les banques. Enfin les risques d'être victimes d'arnaques dans les échanges de pairs à pairs ne soulèvent pas de craintes particulières car les enquêtés font appel à différents formes d'assurance : les systèmes de paiement sécurisés comme Paypal, qui permettent de limiter le risque d'un accès au compte principal et de ne laisser qu'une petite somme sur les comptes employés ; le recours à des canaux complémentaires lorsque les montants des échanges deviennent importants : rencontre en face à face, appels téléphoniques, échanges d'adresse physique, etc ; enfin, le cantonnement fréquent de ces échanges en pair à pair à des activités sans conséquences majeures : petits achats, recherche d'avis pour des domaines de consommation sans grand coût financier ou comme complément à d'autres éléments permettant un arbitrage, etc. Ces différentes dimensions tendent à minimiser l'importance des risques courus et à donner l'impression qu'ils sont évitables. Ils expliquent certainement que les autres dimensions du paradigme psychométrique, où les enquêtés se révèlent plus critiques, n'amènent pas pour autant à une forte mobilisation pour encadrer ces risques ou ne détournent pas de l'usage des MS. La difficulté à appréhender les conséquences à long terme de la multiplication des traces personnelles est ainsi minorée par le peu de conséquences négatives qu'on estime que cette pérennité pourrait provoquer. Les échanges entre pairs ou commerciaux portent quant à

eux sur des temporalités bien plus courtes. Le caractère injuste, s'il est bien reconnu puisque les enquêtés ont conscience de servir des modèles économiques imaginés par les propriétaires des plateformes qu'ils fréquentent et dont ils paieront les échecs, ne pousse pas davantage à moins employer ces plateformes. À ce titre, les figures des usagers/makers cherchant à garder un certain contrôle sur les outils numériques qu'ils emploient, s'ils existent, ne se retrouvent pas fréquemment chez les usagers lambdas. Enfin, bien que les autorités et experts ne soient pas reconnus dignes de confiance, l'inocuité supposée des éléments échangés sur ces espaces fait que la défiance envers ces acteurs majeurs de l'écosystème ne se traduit pas par une défiance générale.

Ajoutons à ce premier élément la nécessité d'être attentif à la dimension temporelle de l'établissement de la confiance. Les MS ont au moins dix ans. Ils s'inscrivent eux-même dans l'usage d'Internet se diffusant dans le grand public depuis une vingtaine d'années. Or, dès leur premier contact avec les services proposés sur internet, les internautes se sont posés ces questions d'établissement de la confiance. Ils ont donc forgé à partir de leurs expériences des habitudes et des représentations à propos des méthodes et manières de créer un lien de confiance suffisant pour interagir avec d'autres internautes ou un système. Ces habitudes et représentations typiques des savoirs profanes, issus de l'expérience, ressortent nettement des enquêtes menées. Ils ne témoignent pas d'une plus grande maîtrise de l'écosystème mais bien des bricolages pour évaluer une situation en contexte. Cet axe de la familiarité permet de comprendre l'élévation du niveau de confiance dans tous les types d'usages explorés (sociabilité, CtoC, réseautage, rehcerche d'avis, etc.). Ce constat invite à aborder sous un nouvel angle la supposée rupture générationnelle régulièrement évoquée dans les usages du numérique. Il ne s'agit pas tant de compétences ou de littératies numériques naturellement diffusées dans une génération mais plutôt de familiarité avec des dispositifs dont nous avons vu qu'elle instaure un climat de confiance propice à l'usage. Cette familiarité a donné lieu à la formation d'habitudes témoignant d'un savoir faire profane suffisant pour se sentir en confiance pour interagir, mais pas à une meilleure maîtrise de la logique des dispositifs dans lesquels ces interactions ont lieu : vérifier l'inscription https sans comprendre ce protocole, se dérober aux visibilités attendues en fournissant de fausses informations sans comprendre les voies de la traçabilité, etc.

En prenant en compte que les pratiques des individus demeurent multisupports cette analyse de la confiance ouvre des pistes pour mettre en scène les dispositifs interactionnels selon les éléments attendus par les individus. Ainsi, dans le cadre de notre projet sur les services d'identification, les modèles de visibilité mis au jour par Cardon (2008) ont pu être proposés comme guides pour la construction d'identités type dans l'outil technique qu'est un portefeuille d'identités. C'est aussi la démarche suivie par la FING lors de son projet de réflexion/innovation autour de la confiance numérique. Ses enseignements ont donné lieu à de nombreuses propositions de services permettant de la renforcer (Kaplan, Francou, 2012) qui insistent sur l'attention à porter à cet écosystème où les fonctionnalités et engagements ne seront reconnus que s'ils sont mis en scène de manière à être compris et acceptés par les usagers. La confiance peut donc bien être comprise comme une intelligence distribuée, où son établissement repose sur la complémentarité des acteurs humains et non humains impliqués.

6 Conclusion

Cette approche de la confiance s'inscrit dans un mouvement plus large de regain d'intérêt pour la matérialité sur laquelle se fondent les formes sociales. Il permet de mesurer l'intérêt de compléter l'appréhension des logiques sociales qu'elle mobilise par une analyse rigoureuse des éléments sémiotiques qui permettent de les mettre en scène. À ce titre, les travaux sur l'énonciation mobilisés récemment pour expliquer les moteurs de recherche ou de recommandations constituent des arguments supplémentaires en faveur d'une approche cumulant appréhension des logiques d'usage et contrats de communication dans lesquels se rencontrent les différents acteurs (Cardon, 2013). Cet article se veut d'ailleurs davantage une

ouverture vers des enquêtes détaillées de chaque contexte évoqué ici trop superficiellement. Il nous semble que l'intérêt de l'attention à la mise en sens de la confiance est démontré par ces retours de terrains. Ceux-ci ne s'avèrent en revanche pas assez détaillés pour expliquer chaque contexte d'usage pris en exemple. Ces premiers résultats appellent donc à des analyses plus poussées de chaque cas, que notre matériau ne permettait d'effectuer faute d'avoir été spécifiquement constitué pour ce type d'analyse.

Références bibliographiques

Battisti, Michelle (2010). Droit numérique un droit à construire, *Revue documentaliste*, vol. 47, n° 1, pp. 24-25.

Callon, Michel, Lascoumes, Pierre, Barthe, Yannick (2001). *Agir dans un monde incertain*, Paris : Seuil.

Cardon, Dominique (2008). Le design de la visibilité. Un essai de cartographie du web 2.0, *Réseaux*, n° 152/6, pp. 93-137.

Cardon, Dominique (2013). *Politique des algorithmes. Les métriques du web*, n° 177

Casilli, Antonio (2013). Contre l'hypothèse de la « fin de la vie privée », *Revue française des sciences de l'information et de la communication*, n° 3, [En ligne] http://rfsic.revues.org/630

Coutant, Alexandre, Stenger, Thomas (2010). Processus identitaire et ordre de l'interaction sur les réseaux socionumériques, *Les Enjeux de l'Information et de la Communication*, [en ligne] http://w3.u-grenoble3.fr/les_enjeux/2010/Coutant-Stenger/index.html

Georges, Fanny (2009). Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0, *Réseaux*, n° 154, pp. 165-193.

Giddens, Anthony (1987). *La constitution de la société*, Paris : PUF.

Kaplan, Dominique, Francou, Renaud (2012). *La confiance numérique*, Paris : FYP.

Laufer, Romain, Orillard, Marion (2007). *La confiance en question*, Paris : L'Harmattan.

Licoppe, Christian (2009). *L'évolution des cultures numériques*, Paris : FYP.

Peretti-Watel, Patrick (2010). *La société du risque*, Paris : La Découverte.

Quéré, Louis (1982). *Des miroirs équivoques*, Paris : Aubier Montaigne.

Rallet, Alain, Rochelandet, Fabrice (2011). Données personnelles et vie privée, *Réseaux*, Vol. 29, n° 167.

Slovic, Paul (2000). *The perception of risk*, Londres, Earthscan publications.

Stenger, Thomas, Coutant, Alexandre (2013). Médias sociaux : clarification et cartographie - Pour une approche sociotechnique, *Décisions Marketing*, n° 70, pp. 107-117.