“ Publiquement privé ” et le contexte La vie privée des jeunes sur les médias sociaux

Mary Jane Kwok Choon

Communication

Information médias théories pratiques

vol. 35/1 | 2018 :
Vol. 35/1
Hors thème

« Publiquement privé » et le contexte

La vie privée des jeunes sur les médias sociaux

Mary Jane Kwok Choon

Résumés

Français English Español
L'auteure analyse les attitudes et les perceptions de la vie privée des jeunes adultes au cours de leurs usages des réseaux socionumériques. Son étude montre qu'il existe des tensions entre les formes de visibilité en tant que reconnaissance et celles qui sont déployées par les surveillants pour exercer le contrôle social. Ces jeunes adultes expérimentent la collision et la collusion de contexte. Il importe de prendre en compte la dimension sociale et contextuelle de la vie privée dans la constitution des politiques de confidentialité.

The author analyzes young adults' attitudes and perceptions of privacy with regard to their use of digital social networks. Her study shows that there are tensions between visibility as a form of recognition and visibility as a way for people of authority to exercise social control. These young adults are experiencing a collision and collusion of context. It is important to take into account the social and contextual dimension of privacy in the development of privacy policies.

La autora analiza las actitudes y percepciones de la vida privada de los jóvenes adultos durante sus usos en las redes sociodigitales. Su estudio demuestra que existen tensiones entre las formas de visibilidad, como reconocimiento y las que son desplegadas por los vigilantes para ejercer el control social. Estos jóvenes adultos experimentan el choque y colusión del contexto. Sin embargo, hay que tener en cuenta el aspecto social y contextual de la vida privada en la creación de las políticas sobre la confidencialidad.

Entrées d'index

Mots-clés : vie privée, réseaux socionumériques, surveillance, contrôle social, confidentialité
Keywords : privacy, digital social networks, surveillance, social control, confidentiality

Palabras claves : vida privada, redes sociodigitales, vigilancia, control social, confidencialidad

Texte intégral

1 Depuis les années 1990, les débats liés à la vie privée se sont multipliés en raison de l'infiltration des technologies de l'information et de la communication, telles qu'Internet, dans chaque sphère de la société. Pour des raisons relatives à la sécurité nationale et à l'économie, différentes techniques de surveillance se déploient pour recueillir et analyser les données personnelles des usagers d'Internet (Bennett, 2011).

2 Avec le développement des médias sociaux, la protection de la vie privée est de plus en plus au cœur des débats. Les révélations d'Edward Snowden ont mis en évidence que la *National Security Agency* (NSA) intercepte les communications privées des citoyens sur les sites de réseaux sociaux (Bennett *et al.*, 2014). Plusieurs problèmes relatifs à la protection de la vie privée ont émergé au sein des réseaux socionumériques[1] (RSN), tels que Facebook et Twitter. À titre d'exemple, l'intégration du News Feed sur Facebook a suscité de vives réactions chez les usagers, car l'information publiée sur le RSN n'était pas restreinte aux amis Facebook, mais visible par un public élargi. De plus, des développeurs d'applications ont eu accès aux informations d'identification des usagers, violant ainsi l'une des politiques de confidentialité de Facebook et la loi canadienne sur la vie privée (Steel et Fowler, 2010). En 2011, un pirate informatique a réussi à obtenir les mots de passe des utilisateurs de Twitter et les a publiés ensuite sur des blogues (France Info, 2011).

3 Les RSN contribuent au problème de la protection de la vie privée en public. Les problèmes relatifs à la vie privée qui ont émergé au sein de ces sites montrent que, bien que des informations aient été dévoilées dans un contexte précis, les usagers ne veulent pas qu'elles glissent vers d'autres contextes. De ce fait, il est important de comprendre comment les usagers protègent leur vie privée sur les RSN, et les normes de la vie privée qu'ils appliquent à ces contextes en ligne. En l'occurrence, la prise en compte des attentes en matière de protection de vie privée s'avère nécessaire lors de la constitution des politiques de confidentialité (Nissenbaum, 2011). Comment l'analyse des attitudes et des perceptions de la vie privée des usagers des médias sociaux nous permet-elle de comprendre la vie privée à l'ère des développements technologiques et quels en sont les enjeux pour les débats liés à la protection de la vie privée ?

4 Le présent texte propose une analyse des attitudes et des perceptions de la vie privée des jeunes adultes liées aux usages de Facebook et de Twitter. Les résultats de cette recherche ethnographique de dix mois montrent que ces jeunes adultes négocient la vie privée au cours des interactions sociales, mais que la faible visibilité des pratiques de surveillance institutionnelle court-circuite les moyens qu'ils mobilisent pour protéger leur vie privée. Il existe des tensions entre les formes de visibilité en tant que reconnaissance et celles qui sont déployées par les surveillants pour exercer le contrôle social. Ces jeunes adultes ont ainsi expérimenté la collision et la collusion de contexte. Il est de ce fait important de prendre en compte la dimension sociale et contextuelle de la vie privée dans la constitution des politiques de confidentialité.

Entre l'inconscience des risques et l'impudeur corporelle

5 Les études antérieures sur les pratiques de la vie privée dans le contexte des RSN ont montré que l'exposition de soi est façonnée par plusieurs facteurs tels que l'inconscience des risques, la fréquence d'usage, la connaissance de la surveillance, une quête de reconnaissance et le fait de mimer des pratiques de microcélébrité. Dans le contexte de

l'Amérique du Nord, l'une des premières études à ce sujet a montré que les usagers qui s'exposent le plus sur Facebook sont inconscients des risques associés à la vie privée (Gross et Acquisiti, 2005). Au fil des années, les recherches tendent à montrer que les usagers des RSN ont ainsi développé une attitude bien plus critique envers la vie privée. Danah Boyd et Ezster Hargittai (2010) ont découvert que plus les jeunes utilisent Facebook, plus ils sont enclins à changer leurs paramètres de confidentialité et à moins s'exposer. L'hypothèse d'une forme d'intériorisation des normes institutionnelles de la vie privée a été posée par Alison L. Young et Anabel Quan Hasse (2013) pour expliquer pourquoi les usagers canadiens de Facebook attachent moins d'importance aux moyens que proposent les institutions pour protéger la vie privée (*institutional privacy*). Cependant, ces mêmes utilisateurs ont développé plusieurs stratégies et négocient ainsi leur vie privée au cours des interactions sociales. En ce qui concerne les participants de la recherche d'Alice E. Marwick et Danah Boyd (2011), ils s'exposent sur Twitter en ayant pour objectif de mimer des pratiques de microcélébrité. Les jeunes font usage des stratégies communicationnelles pour accroître leur popularité en ligne comme les célébrités. Dans le processus, ils se censurent.

6 De l'autre côté de l'Atlantique, les chercheurs français arguent que l'exhibitionnisme des utilisateurs des RSN leur permet d'accumuler du capital social (Aguiton *et al.*, 2009). Par ailleurs, l'étude de Fabien Granjon et Julie Denouël (2010) met en évidence le lien entre l'exposition de soi et la reconnaissance. Les étudiants ont tendance à être plus impudiques sur Facebook, car ils sont dans une quête de reconnaissance. De son côté, Christian Fuchs (2009) souligne le lien entre le dévoilement de soi et la connaissance que les usagers de Salzburg ont des pratiques de surveillance contemporaines et des RSN. Les étudiants interviewés ayant une plus grande connaissance de certains RSN, ont développé une attitude bien plus critique envers la protection de la vie privée.

7 La vie privée est ainsi négociée par les usagers des RSN. Toutefois, relativement peu d'études proposent une analyse des attitudes et des perceptions de la vie privée des usagers des RSN par rapport à différents contextes technologiques. Ce type d'analyse est pertinent pour les débats, car il fait ressortir les attentes que les utilisateurs ont en matière de protection de la vie privée. À partir de l'expérience vécue des usagers, nous pouvons proposer des recommandations qui serviraient à protéger davantage leur vie privée. Par ailleurs, les problèmes relatifs à la vie privée qui ont émergé au sein des RSN montrent que la surveillance remet en cause par moments l'efficacité des modèles de la vie privée que les sites Web proposent. L'information personnelle se retrouve ainsi exposée sans le consentement des usagers. À partir de ces constats, notre recherche analyse les pratiques de la vie privée des jeunes sur les RSN et les normes de la vie privée qu'ils appliquent à différents contextes technologiques. Nous discutons ensuite de leurs implications pour les débats. Notre étude met en évidence les rapports complexes entre la surveillance, la visibilité et la vie privée à travers les pratiques des usagers.

Une approche contextuelle et sociale de la vie privée

8 La vie privée est une construction sociale. En abordant la vie privée en ligne, il est important de reconnaître qu'il existe un lien étroit entre les pratiques de surveillance et leurs répercussions sur la protection de la vie privée. Ainsi Bennett a-t-il affirmé à ce sujet que « [the] effects of surveillance on individuals do not just reduce their privacy. They also can affect their opportunities, life chances and lifestyle. Excessive surveillance also impacts on the very nature of society[2] » (2011 : 488). Dans le cas des sites Web, il est important de considérer les pratiques de surveillance en « arrière-plan » et en « avant-plan » (Stalder, 2011). Dans le premier cas, il s'agit des serveurs et des bases de données qui soutiennent les activités des usagers et qui sont accessibles uniquement aux

propriétaires des sites. Ces données sont utilisées pour servir des buts spécifiques et modeler des interfaces plus ou moins faciles d'utilisation. Dans le deuxième cas, des contenus (données et métadonnées[3]) sont générés à travers ces interfaces par le biais des algorithmes et les formes de surveillance sont visibles, peu visibles ou invisibles au cours des interactions. Il est nécessaire pour les surveillants de mettre en place des architectures de visibilité[4], c'est-à-dire des interfaces qui rendent visibles et accessibles les attitudes des usagers et leurs informations personnelles. Julie E. Cohen avait souligné à quel point les architectures de visibilité favorisent le prolongement et l'articulation de différentes pratiques de surveillance institutionnelle, ce qui peut mettre en danger la vie privée :

> Visibility is an important determinant of accessibility, but threats to privacy from visual surveillance becomes more acute when visual surveillance and databased surveillance are integrated, enabling both real-time identification of visual surveillance subjects and subsequent searchers of stored visual and databased surveillance records[5] (2008 : 183).

9 Pour Andrea Mubi Brighenti (2010), différentes règles de visibilité sont imposées et négociées à travers des architectures qui favorisent l'exercice de la surveillance. Dans le cadre des technologies, des règles de visibilité sont déployées par les surveillants pour exercer le contrôle social (*visibility as control*). Ces règles qui sont appliquées à l'information personnelle vont être différentes selon les architectures des sites Web, leurs conditions de service et leurs politiques de confidentialité. Les sites Web proposent, la plupart du temps, un contrat où l'on offre la possibilité à l'usager d'accepter les conditions de service et les politiques de confidentialité (*opt in*) et de se retirer de certaines conditions (*opt out*) (Nissenbaum, 2011). Certaines règles de visibilité au cours des interactions sociales peuvent être modifiées, et ce, au détriment des usagers (Trottier et Lyon, 2012). Par exemple, les propriétaires des sites ajoutent des paramètres par défaut aux interfaces sans le consentement des utilisateurs, ce qui circonscrit l'accès et la visibilité de l'information personnelle par défaut à une audience élargie.

10 Alors que les pratiques de surveillance institutionnelle sont de plus en plus décentralisées et que les règles de visibilité de l'information personnelle peuvent changer soudainement, la conception selon laquelle la vie privée est une sphère qui est sous le contrôle de l'individu domine les débats (Cohen, *op. cit.* ; Bennett, 2011). La vie privée peut renvoyer à la définition suivante :

> Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations[6] (Solove, 2008 : 1).

11 L'approche du contrôle sur l'information personnelle qui a été développée par Alan Westin (2003) a souvent été utilisée pour aborder la vie privée par rapport aux contextes technologiques et communicationnels. L'auteur définit la vie privée comme le droit des individus de déterminer dans quelle mesure leurs informations personnelles peuvent être communiquées aux autres. Bien qu'au fil des années Westin reconnaisse la dimension sociale de la vie privée, l'approche du contrôle tend à définir la vie privée comme un processus unilatéral, sans pour autant reconnaître sa dimension contextuelle. Plusieurs chercheurs ont ainsi souligné que la vie privée existe en contexte. Par exemple, Ferdinand D. Schoeman (1984 : 406) a mentionné le fait que le dévoilement de soi à l'extérieur d'un contexte spécifique peut s'avérer indésirable et préjudiciable pour un individu. Gary T. Marx a affirmé que le « public » et le « privé »[7] ne sont pas des entités fixes, mais plutôt fluides, situationnelles ou contextuelles, et correspondent à des significations différentes dépendamment de la manière dont ces notions sont abordées (2001 : 160).

12 Le cadre théorique proposé par Nissenbaum (1997, 2004, 2011) permet d'aborder la protection de la vie privée en reconnaissant sa dimension contextuelle. Ces apports théoriques s'avèrent pertinents, car les technologies de l'information et de la communication telles qu'Internet pratiquent par défaut la surveillance. L'auteure a

développé l'approche de l'intégrité contextuelle et défend l'idée selon laquelle le contexte est important et que l'exposition de soi en dehors d'un contexte non souhaité par les individus peut contribuer à une violation de la vie privée. Nissenbaum a identifié deux types de normes : les normes communément admises et les normes de circulation de l'information. Dans le premier cas, ces normes définissent les informations qui sont « appropriées » pour être partagées, dévoilées ou diffusées dans un certain contexte plutôt que dans un autre. Par exemple, dans un contexte médical, il semble « approprié » que le patient dévoile des informations liées à sa santé à son médecin. Dans le deuxième cas, Nissenbaum (2004) offre l'exemple de la circulation de l'information dans le contexte d'une amitié, la confidentialité étant la norme par défaut. Dans une relation, une personne peut se sentir trahie si son ami a révélé un secret à quelqu'un d'autre. Ces deux normes illustrent que des principes de transmission régissent la circulation de l'information et déterminent si une information peut être partagée ou non de manière consensuelle (Nissenbaum, 2004 et 2011). La violation des normes communément admises et celle de la circulation de l'information contribuent à la mise en danger de l'intégrité de l'information personnelle.

13 Jenny L. Davis et Nathan Jurgenson (2014) utilisent le cadre théorique de Nissenbaum afin d'expliquer qu'au sein des RSN, les usagers peuvent expérimenter la collision et la collusion de contexte. Le premier type de collision est favorisé par les architectures des RSN. L'information personnelle glisse d'un contexte à un autre. Par exemple, l'ajout des paramètres de confidentialité par défaut « public » se fait sans avoir eu au préalable le consentement des usagers. Un autre exemple est que des applications Facebook ont exposé les informations d'identification des usagers (Steel et Fowler, *op. cit.*). Les propriétaires des RSN concluent des partenariats avec des tiers tels que les annonceurs et les propriétaires d'applications avec pour objectif de vendre les données personnelles des usagers. Ces tiers se positionnent comme un parti qui a accès à l'information personnelle. Les propriétaires des sites et les usagers sont les deux autres partis, qui sont liés par ce « contrat ». Parfois, ces tiers peuvent contribuer à la collision de contexte et violer la vie privée des usagers. Ce type de collision contribue à la violation de la vie privée par triangulation (*privacy violation triangulation*) (Etzioni, 2015). Le deuxième type d'enchevêtrement des contextes peut être causé par une personne qui copie, rapporte et sauvegarde une information provenant de la page de profil d'un usager. L'information personnelle est ensuite interprétée dans un autre contexte et s'avère préjudiciable pour l'utilisateur. Par exemple, des individus ont perdu leur emploi en raison de billets qu'ils ont partagés sur Facebook. Leurs amis Facebook ont communiqué ces billets à leur employeur (Randall et Richards, 2008 ; Daily Mail Reporter, 2011). La collusion de contexte est ainsi l'une des conséquences de la surveillance interpersonnelle / sociale qui se pratique entre les individus au cours des interactions sociales médiatisées par les architectures des RSN (Marwick, 2012 ; Kwok Choon et Caron, 2012 ; Kwok Choon, 2016a, 2016b). Les travaux de Nissenbaum (2011) peuvent également être utilisés pour aborder les normes de la vie privée qu'appliquent les usagers aux contextes d'usage. Les perceptions de la vie privée des usagers reflètent ces normes contextuelles. Nous concevons que les perceptions de la vie privée par rapport aux RSN sont liées aux expériences quotidiennes (Viseu et Clément, 2003) et relèvent à la fois de la vision et de ce que les individus pensent par rapport à la protection de la vie privée (Merleau-Ponty, 1964).

14 Étant donné que ces perceptions sont liées à ce qu'ils font en ligne, il faut reconnaître que la vie privée est aussi négociée par les individus au cours des interactions sociales. Pour conceptualiser cette forme de vie privée (*social privacy*), les apports d'Erving Goffman (1973) s'avèrent utiles (Tufecki, 2008 ; Marwick et Boyd, *op. cit.* ; Young et Quan-Hasse, *op. cit.*). Goffman a offert une brillante approche de la performativité de la vie privée (Nippert-Eng, 2010). Il est ainsi judicieux de concevoir que, lors des interactions sociales, les individus vont se créer des portions d'accessibilité et d'inaccessibilité au moi pour négocier les frontières entre le « privé » et le « public » (*ibid.*). Dans ce même ordre

d'idées, Antonio Casilli conçoit que la vie privée doit être abordée à travers la notion de *privacy as negotiation*. Ainsi, « les acteurs optimisent le dévoilement d'informations personnelles en se positionnant le long d'un continuum dont "ouverture" et "fermeture" sont les extrêmes » (2013 : 7). Ils vont mobiliser des stratégies pour protéger leur vie privée. Selon les audiences, les stratégies de la protection de la vie privée et les informations dévoilées seront différentes. Ils procèdent ainsi à la séparation des audiences. En effet, les exemples de ces stratégies sont nombreux, comme la suppression de commentaires du mur Facebook et de connaissances de la liste d'amis, ou encore le partage des informations « privées » sur la messagerie Facebook, la stéganographie sociale, qui est l'art de crypter le sens inhérent aux messages partagés sur les RSN et, finalement, l'autocensure (Raynes-Goldie, 2010 ; Boyd, 2010 ; Marwick et Boyd, *op. cit.*). Non seulement l'individu va essayer de négocier les frontières entre le « public » et le « privé », mais il va également tenter d'avoir un contrôle sur ce processus. Cette négociation est aussi un processus dialectique, c'est-à-dire que les individus vont essayer de maîtriser l'information qu'ils partagent, tout comme celle qui provient également des autres, afin d'atteindre un niveau souhaité de vie privée (Altman, 1975).

15 Nous devons aussi prendre en considération que le fait de dévoiler, voire d'exposer certaines informations sur les RSN est façonné par plusieurs facteurs, dont la reconnaissance. Les formes de visibilité qui sont déployées par les surveillants pour exercer le contrôle social sont toujours en tension avec les formes de visibilité négociées par les individus pour obtenir de la reconnaissance. Brighenti (*op. cit.*) offre des outils conceptuels pour comprendre les formes de visibilité en tant que reconnaissance au cours des interactions quotidiennes. Le chercheur a identifié quatre formes de reconnaissance. Premièrement, elle est catégorielle, se reposant ainsi sur la catégorisation routinière des individus au cours des interactions. Au cours de ce processus, les individus se rendent visibles à travers des catégories (apparence physique, comportements verbaux et non verbaux) et des caractéristiques sociales. Deuxièmement, elle peut être individuelle. À ce stade, des moyens de surveillance sont mobilisés pour identifier, catégoriser, évaluer et contrôler les individus en vue de les rendre visibles. L'identification et la reconnaissance des individus s'effectuent selon les critères qui ont été définis par les institutions. Troisièmement, la reconnaissance peut être singulière. Elle prend forme entre des individus quand ils sont en train d'entamer et d'entretenir des relations au cours des interactions. Cette reconnaissance peut revêtir différents aspects étant donné que la présentation de soi au cours des interactions sociales est un processus singulier. La quatrième forme de reconnaissance est liée au spectacle. C'est la reconnaissance que les célébrités obtiennent de leurs *fans*. Les *fans* peuvent concevoir que ces célébrités sont des connaissances alors qu'il n'existe pas de relation entre eux et ces personnes.

16 La mise en visibilité de l'information personnelle sur les RSN est un processus stratégique pendant lequel un individu négocie également sa vie privée. En même temps que les utilisateurs rendront l'information personnelle visible à une audience, certaines informations seront moins visibles au cours des interactions sociales, voire dissimulées pour diverses raisons. Toutefois, comme l'a souligné Dominique Cardon, les usagers des RSN « sont en revanche impliqués pratiquement dans la gestion de leur visibilité face à la "surveillance interpersonnelle". Or, de ce point de vue avant d'être un risque, la visibilité est perçue par certains comme une opportunité » (2009 : 61-62). La mise en visibilité de l'information personnelle se positionne comme un moyen qui permet d'obtenir des bénéfices.

Privilégier la démarche de l'ethnographie virtuelle

17 Pour comprendre les attitudes et les perceptions de la vie privée des usagers des RSN, nous avons privilégié une démarche qui relève de l'ethnographie virtuelle[8]. Nos méthodes ont été l'observation participante et les entrevues qualitatives en face à face. Pour les besoins de notre article, nous présentons les données recueillies au cours des entrevues. Les jeunes adultes sont ceux qui sont les plus présents sur les RSN dans le contexte du Québec (CEFRIO, 2010 et 2014). Un appel à participation a été envoyé par courriel à des étudiants inscrits à un programme de baccalauréat dans une université à Montréal. La majorité des jeunes adultes qui utilisent les RSN sont d'ailleurs des étudiants (*ibid.*). Le courriel est un mode de communication qui est fréquemment utilisé pour se tenir au courant des actualités en lien avec leur programme d'étude. Le critère de recrutement s'est basé sur l'âge (18-34 ans) et sur le simple fait d'utiliser à la fois Facebook et Twitter. Après avoir eu le consentement des usagers, nous sommes devenue leur amie Facebook et nous avons commencé à suivre leurs comptes Twitter. En prenant en compte le critère de saturation des données, nous avons constitué un échantillon de 20 usagers. Notre objectif n'était pas d'avoir une représentativité des pratiques des jeunes adultes, mais d'avoir un profond aperçu de leurs attitudes et perceptions de la vie privée en lien avec les RSN dans le contexte du Québec. Des entretiens non dirigés et semi-dirigés d'une durée de 90 minutes ont été réalisés en face à face. Le premier entretien était en fait une discussion ouverte devant l'ordinateur. Nous avons posé la question suivante à chaque utilisateur : peux-tu me montrer ce que tu fais sur Facebook et Twitter ? Ce type d'entretien se positionne comme un moyen de comprendre les phénomènes du point de vue des usagers plutôt que de les expliquer (Spradley, 1979). Les thèmes qui ont émergé lors du premier entretien ont servi à construire la grille pour le deuxième entretien semi-dirigé. Il s'agissait d'inciter les usagers à réfléchir sur leurs propres pratiques et à donner leurs points de vue sur certains aspects d'un phénomène. Parmi les thèmes de notre grille d'entretien, nous comptons les perceptions par rapport aux politiques de confidentialité, aux conditions de service ainsi qu'à la réputation de ces sites en matière de protection de la vie privée, et ce que les jeunes adultes considèrent comme relevant du « public » et du « privé ». Donc, nous avons pu comprendre les normes de la vie privée que ces jeunes adultes appliquent à ces contextes. Nous n'avons pas évoqué le lien intrinsèque entre les pratiques de surveillance et leurs répercussions sur la protection de la vie privée. Nous avons voulu que les usagers abordent eux-mêmes ce lien. Le codage manuel a permis de mettre en évidence les thèmes qui ont émergé lors de l'étude de terrain et de les mettre en relation (*ibid.*). Afin de protéger l'anonymat des usagers, nous utilisons des pseudonymes dans le présent texte. Les prochaines sections décrivent les principaux thèmes de notre recherche.

Résultats

Les pratiques de l'ordre du *show off* et la quête de reconnaissance

18 Ces jeunes adultes exposent différentes informations au cours des interactions sur les profils, notamment les *selfies*, les photos témoignant de la participation des usagers à des activités sociales, les endroits où ces photos ont été prises, les *inside jokes* et des liens vers différents faits d'actualité ainsi que des informations d'identification, comme une photo de profil, le nom réel de l'usager, son université d'attache, son employeur, sa ville de résidence ou de naissance. De plus, au sein des groupes, ils dévoilent des informations liées à l'organisation des rencontres avec leurs amis et leurs collègues, des documents et des hyperliens en relation avec leurs travaux universitaires. Les sujets d'actualité et le fait de se localiser à un endroit public précis sont des informations considérées comme de l'ordre du « public ». Les *selfies*[9], les photos les montrant dans des activités sociales et les

inside jokes relèvent du « privé ». Ces utilisateurs ne souhaitent pas que ce type d'information glisse vers d'autres contextes.

Tableau 1. Nombre d'amis Facebook, d'abonnés et d'abonnements Twitter

Participants	Nombre d'abonnements Twitter	Nombre d'abonnés Twitter	Nombre d'amis Facebook
Tara	502	28	556
Karine	11	9	445
Lana	135	30	328
Molly	226	41	326
Lily	270	33	550
Sheila	220	33	536
Lovna	223	98	545
Mira	644	70	448
Élissa	212	28	350
Ludovic	190	29	438
Illona	816	1 616	580
Sébastien	600	150	330
Maurice	80	8	566
Corinne	121	28	338
Joey	14	27	600
Roméo	94	27	122
Giliane	139	41	116
Léa	120	59	588
Liloo	16	3	476
Noémie	339	53	431

19 L'exposition de soi est effectuée pour que leurs audiences voient qu'ils ont une vie sociale riche et de ce fait, ils peuvent obtenir de la reconnaissance de celles-ci. Par exemple :

> Molly : C'est tellement du fun de dire, regarder j'ai une vie sociale je suis là ! Mais en même temps, je me rends compte que les gens savent où tu es.
>
> Ilona : Je géolocalise juste quand c'est quelque chose de fun, mettons un spectacle. J'étais allée à New York, j'ai marqué ça, je prends un verre, j'ai mis ça. Je ne localise pas pour rien. Tu veux montrer aux gens quelque chose de ta vie. Quand tu t'en vas à Cancún. Tu veux que tout le monde sache que tu es à Cancún, pour que le monde sache que tu as une vie.

20 Cette forme de reconnaissance est catégorisée comme étant singulière (Brighenti, *op. cit.*). Ils sont jugés entre autres sur la singularité de leurs contributions. Les formes d'appréciation de leurs publications, telles que le nombre de « *Like* » et l'identification sur des photos, sont des signes de cette reconnaissance. Ils adhèrent ainsi à la norme du paraître qui est liée à l'exposition de soi. À ce stade, nous constatons un lien entre l'engagement des utilisateurs dans les pratiques de l'ordre du *show off* et leur volonté de plaire à leurs réseaux sociaux et d'accumuler plus de contacts (Aguiton *et al.*, *op. cit.*). En effet, nos participants pensent que le nombre de retours reçus sur l'information publiée en ligne pourrait réduire et que leurs amis Facebook cesseraient peut-être de s'intéresser à leur personne s'ils ne s'engagent pas dans de telles pratiques.

La crainte de la surveillance sociale

21 Toutefois, ces jeunes adultes essaient d'alterner entre l'exposition de soi et le fait de dissimuler des informations (Altman, *op. cit.*). Ils attachent de l'importance à la protection de la vie privée et à leur réputation. Ils craignent les conséquences de la surveillance sociale. L'idée que quelqu'un quelque part puisse accéder à leurs informations personnelles est omniprésente chez ces jeunes. Ils sont conscients de la propension des

architectures des sites Web à favoriser la présence d'une audience invisible (Marwick et Boyd, *op. cit.*) :

> Mira : Quand je publie les photos, je me dis, j'ai beaucoup de photos, quelqu'un pourrait m'écœurer, quelqu'un qui me suit. On se dit que ça n'arrive pas à moi, le jour que ça arrive à toi c'est trop tard. Tu publies tes affaires, ta petite page à toi, c'est toi qui choisis ta photo de couverture, tes amis, tu as l'impression que c'est « privé », quand moi j'y vais, je n'ai pas l'impression que tout le monde me voit et peut accéder à mon profil. Des affaires peuvent revenir contre moi. Le « privé » c'est mou sur Facebook. Ça existe, mais ça n'existe pas.

> Noémie : On a vu plein de fois, ces temps-ci, souvent, soit sur Facebook ou sur Twitter, quelqu'un qui photographie les commentaires qu'il a reçus par rapport à des trucs. À partir du moment que tu publies et qu'il y a un autre qui a accès ça ne t'appartient plus vraiment. Il faut que tu fasses attention. Faire des captures d'écran, le partager dans un autre contexte, le bouger, le changer avec Photoshop c'est facile là.

22 Cette perception est aussi façonnée par leurs propres expériences et par ce qu'ils ont entendu dans les médias, en salle de classe et de la part de leurs amis au sujet de la propension du site de réseau social à favoriser la présence d'une audience invisible.

De la stéganographie sociale à un compte restreint aux amis seulement

23 De ce fait, ces usagers mobilisent plusieurs stratégies[10] sur Facebook. Nous pouvons compter la stéganographie sociale, la suppression des amis Facebook de leurs listes, le partage des informations relevant de l'ordre du « privé » par le biais de la messagerie privée et l'autocensure, qui se traduit par le fait de ne pas dévoiler des informations, telles que les photos *trash* ou d'impudeur corporelle. Ces utilisateurs ont aussi un compte restreint aux amis Facebook seulement. L'activation de la fonction de géolocalisation lorsqu'ils sont à leur domicile, chez leurs amis ou chez le médecin, est inappropriée. S'ils sont identifiés sur certaines photographies de ce type, ils retireront ces « identifications » en faisant usage des paramètres adéquats. Les propos de ces usagers traduisent certaines stratégies mobilisées :

> Ludovic : Ça c'est une *inside joke* avec mes amis. C'est assez niaiseux, c'est une *joke* de bord. C'est un peu vulgaire, c'est ça (rire). Personne ne comprend, à part Mika qui était là au bar. Elle étudie en sexologie, puis au bar elle a dit « as-tu déjà fait ça Ludovic ? » Et puis, elle dit, la prochaine fois que tu me verras, tu me diras si tu l'as fait. Puis, à chaque fois que tu vas me voir, il faudra que tu me le dises. C'est pour ça qu'elle dit : « Puis là, tu l'as-tu faite ? » Et je dis non. Ça ressemble pas mal à ça (rire).

> Mira : Sur Facebook, c'est difficile de savoir dans quels contextes que tu es, tu sais quand tu as 430 amis. J'en ai beaucoup, tu sais, des fois, je vais voir ma liste d'amis, je vais faire le ménage. Je me dis : « toi je ne te veux plus, je ne te vois plus et je ne veux plus que tu vois mes affaires ». Je fais un peu le ménage.

> Roméo : Je trouve cela inquiétant ces lieux la. Pour un événement à un bar, tu peux dire que tu es là. Je me suis assuré qu'il est désactivé sur mon téléphone parce que je ne veux pas que quand je poste quelque chose, ça dise où j'étais quand je l'ai posté. Je trouve que cela est un peu envahissant au niveau de la vie privée. Si c'est un endroit public, cela ne me dérange pas.

> Molly : Des photos de moi, en party vraiment saoule comme je suis à terre. Ça ne me dérange pas d'être dans un bar. On ne prend pas des photos de nous quand on a l'air folle là, des photos irrespectueuses je ne mets pas. Parce que je me dis si jamais j'ai un employeur qui voit mes photos, ou je sors souvent, il ne va pas dire que je suis *hangover*, je suis capable d'avoir une vie sociale et de balancer les deux.

24 Comme Goffman l'a affirmé, « bien que, dans certaines représentations déterminées, et même dans certains rôles particuliers, l'acteur soit en situation de ne rien devoir cacher, il y a en général, quelque part dans l'ensemble de ses activités, quelque chose qu'il ne peut aborder ouvertement » (*op. cit.* : 66). Ces stratégies liées à la protection de la vie privée montrent que les usagers procèdent à la séparation des audiences. Elles traduisent la volonté des utilisateurs de dissimuler des informations à une audience spécifique.

La collision de contexte

25 Force est de constater que ces jeunes adultes ont expérimenté la collision de contexte (Davis et Jurgenson, *op. cit.*). La majorité d'entre eux n'ont pas lu la section des politiques de confidentialité depuis que Facebook y a intégré des changements. Ils n'avaient pas vu l'annonce de ces changements. L'information personnelle qu'ils pensaient avoir restreinte à leurs amis seulement s'est retrouvée, par défaut, visible et accessible au plus grand nombre d'usagers. Les changements constants effectués dans les politiques de confidentialité peuvent contribuer à l'émergence des formes de visibilité non anticipées par les usagers (Trottier et Lyon, *op. cit.*) et à un accès non consenti à l'information personnelle (Cohen, *op. cit.*). À titre d'exemple, les profils des jeunes adultes étaient répertoriés par les moteurs de recherche externes, les photos de profil étaient visibles par tout le monde et les applications avaient accès à leurs informations personnelles sans leur consentement. Par exemple :

> Roméo : Euh, non. Quelqu'un peut me chercher sur Google et voir mon profil Facebook ? J'ai l'impression que quand Facebook change ses politiques, cela arrive énormément ces derniers temps avec la pression pour essayer d'être rentable au niveau des actions. Il rajoute différentes clauses qui sont mises en *nuage* automatiquement ou moins confidentielles. Google c'est un espace plus public, et je ne suis pas intéressé que quelqu'un puisse *googler* mon nom et trouver mon information.

26 Ces usagers se sont empressés d'activer les paramètres adéquats au cours de notre entretien. De leurs points de vue, les propriétaires du site les laissent dans le flou quant à l'étendue d'accès et de visibilité de l'information personnelle. Ces jeunes adultes ont avoué qu'ils trouvent que les politiques de confidentialité et les conditions de service sont rédigées dans un langage juridique (Etzioni, *op. cit.*) qu'il est difficile de comprendre. Toutefois, ils se sont avoués satisfaits de l'état de protection de leurs profils après avoir activé les paramètres de confidentialité.

La collusion de contexte et le sentiment de perte de contrôle sur la vie privée

27 Les attitudes sont différentes quand ils sont confrontés à une collusion de contexte. Ceux qui se sont sentis traqués par des amis Facebook ou des étrangers à un moment ou à un autre sur le RSN ont mentionné avoir ressenti un sentiment de perte de contrôle sur la vie privée. Joey et Sheila ont eu le sentiment d'avoir été victimes de la surveillance sociale :

> Joey : Il y avait une fille que je fréquentais à l'époque qui a cherché des informations sur mon Facebook, mais des informations que je ne savais même pas qui étaient là, des informations par rapport à ma vie privée. Elle s'est rendu compte de ces trucs-là, elle est revenue vers moi avec ça. Ça a comme brisé un lien de confiance. Je me suis rendu compte que je ne pouvais pas vraiment lui en vouloir parce que c'est l'information que j'affichais publiquement. Je me suis rendu compte que Facebook pouvait être un outil à double tranchant.

> Sheila : Mon ancien copain avait eu un différend avec un autre gars et on pensait qu'il m'avait retrouvé et qu'il voulait me causer des problèmes puisque j'avais reçu des demandes d'amis de personnes ayant de faux profils (seulement deux amis, pas d'historique sur le Timeline). J'avais peur qu'on puisse me retracer puisque je m'indique à des lieux parfois, je publie beaucoup de photos.

28 Étant donné qu'ils pratiquent eux-mêmes cette forme de surveillance et que certains d'entre eux ont vécu une intrusion dans leur vie privée à cause de celle-ci, les risques qui y sont liés apparaissent concrets. Selon les propos d'Ana Viseu et Andrew Clément (*op. cit.* : 14), pour certains usagers d'Internet, la mise en danger de la vie privée revêt un caractère abstrait et lointain au quotidien. La vie privée devient une valeur privilégiée quand elle est mise en péril.

Les pratiques de microcélébrité et la quête de reconnaissance sur Twitter

29 Les perceptions de la vie privée que les jeunes adultes ont par rapport à Twitter sont différentes de celles qui sont liées à Facebook. D'abord, l'objectif d'avoir un compte Twitter est de partager de l'information à un plus grand nombre d'usagers et de se construire une réputation dans la twittosphère. Donc, ils choisissent d'avoir un compte public. Leurs cercles sociaux sont constitués principalement des étrangers[11]. Parmi leurs abonnements, il y a des célébrités du *show-business*, des animateurs de télévision et de radio, des journalistes, des journaux en ligne, des magazines, des chaînes de télévision et des organismes culturels. Ils comptent entre cinq et dix amis Facebook parmi leurs abonnés. Ils n'ont jamais rencontré la majorité des gens qui les suivent et auxquels ils se sont abonnés.

30 Les usages de Twitter s'apparentent à des pratiques de microcélébrité (Marwick et Boyd, *op. cit.*). L'idée est de mimer le comportement des célébrités en *tweetant* lors des événements culturels et de faire part des émotions positives et négatives.

Capture écran 1. *Tweet* de Sébastien

31 L'exposition de soi sur Twitter permet aussi d'attirer l'attention des audiences et d'obtenir de la reconnaissance. Selon Marwick et Boyd, « [the] ability to attract and command attention becomes a status symbol[12] » (*op. cit.* : 127) dans la twittosphère. La reconnaissance sur Twitter est obtenue des étrangers. Le fait que leurs *tweets* soient *retweetés* et mis en favoris ainsi que les éventuels « retours » en lien avec le contenu généré et l'augmentation de leurs abonnés sont autant de signes de l'attention et de la reconnaissance que des étrangers leur accordent. Par exemple :

> Mira : Je *retweet* beaucoup leurs affaires, et je trouve ça cool. Je leur fais de la pub un peu. Les gens vont voir que Place des arts s'est abonné à moi. C'est un peu le prestige quand même. C'est le fun quand ils te répondent aussi. Par exemple, Rihanna est avec Chris Brown à nouveau. C'est quoi cette histoire-là ? Ils répondent : « Oui, Mira tu peux aller voir sur notre site web ». C'est le fun ! Tu te sens un peu importante. Même Dany Turcotte il fait beaucoup de jokes. Des fois j'ai des jeux de mots en tête et il va me *retweeter*.

32 La mise en visibilité de l'information personnelle est perçue comme une chance (Cardon, *op. cit.* : 62) de devenir encore « plus visible » dans la twittosphère. C'est la

reconnaissance de la part des étrangers qui permettrait ainsi à ces jeunes adultes d'avoir un statut dans cette sphère.

Ce que nous faisons sur Twitter est impersonnel

33 De leurs points de vue, ce qu'ils font au sein du site relève majoritairement de l'ordre de l'impersonnel. Premièrement, le partage de l'information n'est pas lié à la sphère de l'amitié. Deuxièmement, l'information se noie dans le flux de *tweets* de la twittosphère. Il est très difficile de déterminer qui sont ceux qui vont réagir à leurs *tweets*. Par exemple, Sébastien explique que Twitter peut être une sphère à la fois impersonnelle et personnelle, dans le sens qu'il peut publier une information plus ou moins « privée ». Toutefois, celle-ci va devenir impersonnelle dans le flot général et parce que personne ne va réagir à l'information. Troisièmement, les *tweets* sont abordés comme des fragments d'information de 140 caractères, qui ne reflètent pas des aspects de leur individualité. Ils considèrent qu'ils ne dévoilent rien de vraiment « privé » sur le site, car celui-ci n'offre pas de paramètres de confidentialité pour séparer les audiences.

34 Cependant, il y a une catégorie de *tweet* qui est considéré comme « privé » et que nos participants veulent protéger du regard de leurs amis Facebook. Par exemple, Élissa raconte qu'elle a publié un *tweet* dans lequel elle fait part de ses émotions par rapport à un concours sur le lait et qu'elle ne veut pas que ses amis Facebook le voient. Mira avoue qu'elle « chiale » beaucoup sur Twitter et critique des célébrités lors des événements et que « son comportement est acceptable » sur le site. Ce type de *tweets* n'est pas exposé sur Facebook. Les usagers considèrent que leurs amis Facebook auraient pu porter un jugement négatif sur ce genre d'information.

L'autocensure comme seule stratégie liée à la vie privée

35 L'autocensure est une stratégie qui a souvent été mobilisée par des usagers de Twitter, car le site ne propose pas des paramètres adéquats pour séparer les audiences (Marwick et Boyd, *op. cit.*). De ce fait, certaines informations ne sont pas dévoilées sur Twitter. Les photos prises lors des fêtes ou d'autres événements sociaux n'intéressent pas les membres de leurs communautés. La négociation de la vie privée s'effectue à ce niveau. En raison du caractère public du site, ils ne peuvent pas contrôler la diffusion de ces photos, notamment parce que celles-ci seront exposées devant des inconnus. De plus, la fonction de géolocalisation n'a pas été activée sur le RSN, car leurs réseaux sont constitués d'étrangers. Certains ne savaient pas que le RSN offre cette fonction, alors que d'autres ont veillé à ne pas l'activer par inadvertance sur l'application mobile[13]. La crainte d'être traqué[14] par des inconnus sur Twitter est présente :

> Illona : Ce n'est pas intéressant. Il y a plus de monde que je ne connais pas et ça fait un peu *creep*. Mettons je mets je suis chez moi, et quelqu'un sait où j'habite, et je ne le connais pas. Si je ne l'ai jamais vu dans ma vie, je ne le connais pas. Sur Facebook, j'ai eu au moins une interaction avec eux. Même si c'est quelqu'un de passage, je sais c'est qui. Sur Twitter, du monde partout me follow.

36 Pour expliquer de quelle manière l'autocensure est mobilisée devant des individus que l'on connaît peu, Goffman a offert l'exemple d'un mari et de sa femme qui se chamaillent et qui sont mis en présence de quelqu'un qu'ils connaissent peu. Ils redeviennent alors courtois. L'auteur l'explique en ces termes :

> Ainsi un mari et sa femme en train de se chamailler et soudainement mis en présence d'un invité qu'ils ne connaissent pas depuis longtemps mettent de côté leurs querelles intimes et rétablissent entre eux des rapports presque aussi courtois et aussi bienveillants que les sentiments affichés à l'intention du nouveau venu (*op. cit.* : 174).

37 Par ailleurs, le site Twitter est considéré comme ayant plus ou moins une bonne réputation en matière de protection de la vie privée. Les utilisateurs n'ont pas entendu, dans les médias, en salle de classe ou venant de leurs amis, que le site a contribué à l'émergence de problèmes relatifs à la protection de la vie privée :

> Giliane : Les gens n'en parlent pas vraiment pas. Le discours que j'entends s'est plus associé à Facebook qu'à Twitter.
>
> Illona : Je n'ai rien entendu à ce sujet. Mais, pour vrai, je pense que c'est plus protégé que Facebook parce que ton *tweet* tu peux le bloquer et tu peux même les effacer. Peut-être que Facebook a déjà une réputation bien ancrée que ce n'est pas protégé.
>
> Tara : On en parle moins, parce que les gens publient moins de leur vie privée dessus.

38 Nos participants n'ont jamais lu la section des politiques de confidentialité sur Twitter. Force est de constater que ces jeunes adultes n'étaient pas au courant que les profils publics sont visibles et accessibles par le biais des moteurs de recherche Google et Bing. Cette exposition non souhaitée de l'information personnelle n'est pas considérée comme une violation de la vie privée en raison de la nature impersonnelle de leurs usages sur le RSN.

L'inconscience des risques liés à l'usage de l'information personnelle par les institutions

39 À aucun moment les participants à la recherche n'ont émis le désir d'avoir un contrôle sur l'usage de l'information personnelle par les institutions et des tiers. Ces jeunes adultes attachent peu d'importance aux moyens que proposent ces sites Web pour protéger leur vie privée. Ils sont inconscients des risques possibles de violation de la vie privée par triangulation (*privacy violation triangulation*) (Etzioni, *op. cit.*). D'ailleurs, les publicités sont perçues comme une forme d'exploitation de données personnelles, mais elles ne constituent pas des risques d'atteinte à la protection de la vie privée. Par exemple :

> Lily : C'est la publicité ciblée, ils retiennent tes intérêts comme consommateur et en fonction de ça ils te mettent de la pub. Si jamais tu réactives ton Facebook, tout revient. Ils n'ont pas fait tout ce travail-là à refaire, c'est quoi tes goûts, tes profils, les types de consommateurs, pour mieux t'avoir, il y a des compagnies qui paient cher pour que Facebook fasse ça. Ça va directement au public et ils ont plus de chance de vendre.
>
> Noémie : Ce n'est pas correct. Ce que j'ai compris, selon mes recherches, selon mes commentaires, selon les pages que j'ai aimées, ils font des profils de consommateurs, et ils vendent ça à des compagnies. Mark Zuckerberg, ce n'est pas un messie non plus, ce n'est pas un bon samaritain qui a créé quelque chose pour rendre les gens heureux là. Il fait de l'argent avec ça, il a trouvé un moyen.

40 Notons qu'ils n'avaient jamais vu les publicités commanditées sur Twitter. Ce désintérêt par rapport aux pratiques institutionnelles de la vie privée a été également observé lors des études antérieures (Boyd, 2008 ; Young et Quan Hasse, *op. cit.*). Cette attitude peut être expliquée par le fait que les risques d'atteinte à la vie privée liés à la surveillance institutionnelle semblent abstraits pour ces utilisateurs en raison de leur connaissance limitée en la matière.

Le « publiquement privé » et le contexte

41 La norme de la vie privée qui est associée aux usages de Facebook est l'intégrité contextuelle (Nissenbaum, 2004 ; 2011). Ces jeunes adultes souhaitent que l'information

personnelle circule uniquement dans des contextes préalablement choisis, bien qu'ils sachent que l'intégrité de l'information personnelle peut être mise en danger sur ce site de réseau social. Par exemple, Mira est un peu offusquée, car elle ne comprend pas pourquoi Facebook ne peut pas être « privé » et « limité comme un site du gouvernement ». Elle qualifie les barrières de protection de la vie privée de « molles » et elle aimerait bien que ce soit plus « privé ». Giliane souhaite que, lorsqu'elle partage une photo sur Facebook, les personnes qui ne la connaissent pas ne puissent pas voir cette photo, puisqu'il y a toujours la possibilité d'être « stalkée » sur le RSN. Illona veut que ce qui est partagé sur Facebook reste « vraiment entre elle et ses amis et que cela devienne une règle générale ». Ludovic souhaite que l'information personnelle sur son profil ne soit pas accessible et visible aux employeurs potentiels, car cette information peut faire l'objet d'une interprétation et ce serait préjudiciable pour sa carrière. À ce stade, la pensée de Schoeman permet de comprendre les perceptions des usagers : « Disclosure of information to groups, even potentially large groups, might still be considered private provided still larger groups were excluded[15] (Schoeman, 1984) » (Nissenbaum, 1997 : 215). Rappelons que des informations à la fois de l'ordre du « privé » et du « public » sont partagées au sein de ces deux sites. En comparaison, la « transparence négociée » est la norme qui s'applique aux pratiques de Twitter. Ils négocient la vie privée à travers l'autocensure. En ayant un compte public, ils adhèrent à l'une des normes institutionnelles de la vie privée prônées par le site de réseau social, qui est la mise en transparence de l'information personnelle à un plus grand nombre d'usagers. D'un contexte technologique à un autre, les normes de la vie privée qui y sont appliquées varient. De ce fait, les perceptions de la vie privée des jeunes adultes se construisent autour des notions du « publiquement privé » et du contexte.

L'intériorisation de la surveillance

42 Ces pratiques montrent les tensions entre les formes de visibilité négociées par les usagers pour obtenir de la reconnaissance et celles qui sont déployées sur les architectures des RSN pour exercer le contrôle social (Brighenti, *op. cit.* ; Proulx et Kwok Choon, 2011 ; Kwok Choon et Proulx, 2012). En effet, les frontières entre le « public » et le « privé » sont floues au cours des interactions sociales sur les RSN et il est difficile d'avoir un contrôle sur l'information publiée en contexte d'usage. L'information personnelle glisse vers d'autres contextes par moments. La vie privée se retrouve en l'occurrence menacée.

43 La visibilité est ainsi perçue comme une opportunité au sein des sites où s'exerce le contrôle social (Cardon, *op. cit.*). Selon les propos de Brighenti, dans le cadre d'un tel régime de visibilité, les individus tendent à percevoir davantage les bénéfices liés à leurs mises en visibilité que des désavantages et le contrôle social qui s'y exerce : « There is a systematic distortion in favor of the perception of the advantages of becoming part of new media visibility, to the detriment of the perception of its disadvantages and specifically the dimension of social control that is implied by them[16] » (Brighenti, *op. cit.* : 158).

44 Ces jeunes adultes aperçoivent le caractère néfaste de la visibilité uniquement en présence d'une intrusion dans la vie privée, causée par les pairs. En ayant conscience que les interfaces des RSN soumettent l'information personnelle à des risques de collusion et collision de contexte, ils continuent pourtant à s'engager dans des pratiques d'exposition de soi. Nous arrivons à la conclusion que ces utilisateurs intériorisent de manière volontaire et involontaire la surveillance. Ce processus est involontaire dans le sens qu'ils sont inconscients des risques d'atteinte à la protection de la vie privée liés à l'usage des données personnelles par les propriétaires des RSN, par les développeurs d'applications ainsi que par les autres tiers comme des annonceurs. Ces jeunes adultes n'ont pas une connaissance approfondie des modes opératoires de la technologie contrairement aux représentations qui sont généralement associées aux usagers faisant partie de la catégorie des « natifs numériques ». Ils ne sont pas en train de s'exhiber sur les RSN comme l'évoquent certains discours à leur sujet dans les médias. La faible visibilité des annonces

des changements architecturaux en contexte d'usage contribue aussi à ce que les risques potentiels pour la vie privée apparaissent lointains, voire abstraits.

Les enjeux pour les débats liés à la vie privée

45 Ces résultats montrent qu'il y a aussi un manque de transparence en lien avec les changements architecturaux, les conditions de service et les politiques de confidentialité. Les conditions de service et les politiques de confidentialité ont été également traduites littéralement de l'anglais au français. Cela a d'ailleurs des répercussions sur la syntaxe des phrases et rend leur compréhension difficile pour les usagers francophones. En vue de fortifier un consentement éclairé, il est à la fois nécessaire de développer de la transparence autour des politiques de confidentialité et des conditions de service et de rendre explicites les règles contextuelles. Comme l'a précisé Nissenbaum :

> If pursued conscientiously, the process of articulating context-based rules and expectations and embedding some of them in law and other specialized codes will yield the safety nets that buttress consent in fields such as health care and research. With these precautions in place, plenty of room would still remain to express personal preferences and to maintain a robust role for informed consent[17] (2011 : 45).

46 Il est aussi nécessaire de rendre plus visibles les annonces liées aux changements architecturaux, tels que les paramètres par défaut « public ». En novembre 2014, les responsables du site ont affirmé que ceux qui s'inscrivent à Facebook pour la première fois verront leurs paramètres être circonscrits au mode « privé »[18]. Toutefois, il n'est pas précisé si cette condition s'applique aux usagers qui sont déjà inscrits au site. De nombreux participants souhaitent ainsi que les paramètres soient prédéfinis en mode « privé ». Nos interviewés n'ont également pas vu l'annonce qui est liée à la possibilité de se retirer de la liste des annonceurs. Le site de réseau social Facebook offre la possibilité aux usagers de contrôler l'usage de leurs données personnelles par les annonceurs et autres tiers à travers l'intégration d'un onglet dans la section Publicité vers le site Digital Advertising Alliance. Il faut approximativement 10 minutes pour y accéder et être retiré de cette liste. Ici, nous tenons compte du temps qu'il faut à l'usager pour aller vers la section Confidentialité de la page Facebook, à la section Publicité, pour ensuite lire le paramètre, cliquer sur le lien Digital Advertising Alliance of Canada[19], chercher l'onglet « Opt out » sur la page de Digital Advertising Alliance et, finalement, lire ce qui est expliqué sur cette page. L'usager a alors deux choix : cliquer sur l'onglet « Opt out » ou faire défiler la première page et cliquer sur le lien « Consumer opt out page ». Ensuite, il peut « choisir » de se retirer de la liste des différentes compagnies qui s'affichent sur la page. Cela requiert un effort considérable de la part des usagers. De plus, il est important de souligner que Facebook utilise toujours les données personnelles de tous les usagers à des fins commerciales même si des utilisateurs se sont retirés de cette liste. Sur Twitter, l'onglet « Protéger mes *tweets* » est accessible après avoir cliqué sur les onglets « La section des politiques de confidentialité » et « En savoir plus ». De ce fait, il est nécessaire de réduire le parcours que doit entreprendre un usager pour accéder à certaines politiques de confidentialité. Cela favoriserait le consentement éclairé.

47 Cependant, nos participants ne sont pas conscients des risques de violation de la vie privée par triangulation et ne prennent pas le temps de lire et de rechercher les conditions de service et les politiques de confidentialité. Il est de ce fait judicieux d'offrir une éducation critique aux médias qui comprend un volet qui sert à enseigner des moyens techniques visant à obscurcir les procédés de surveillance et de collecte de données (*obfuscation*) aux usagers, afin qu'ils puissent se protéger contre les répercussions de ces pratiques en contexte d'usage. Finn Brunton et Helen Nissenbaum ont expliqué que ces

moyens peuvent permettre aux usagers de détourner dans une certaine mesure les moyens de surveillance qui ont été instaurés par des surveillants (2015 : 40). Entre autres, Facecloak est un logiciel qui permet aux usagers de dissimuler les informations personnelles qu'ils partagent sur Facebook d'une audience spécifique, en les cryptant et en les sauvegardant sur un autre serveur que sur celui de Facebook. Il faudrait reconnaître l'importance d'avoir un public avisé par rapport aux risques relatifs à la protection de la vie privée associés aux usages des technologies de l'information et de la communication, tout en veillant à développer des compétences techniques de différentes générations d'internautes.

Conclusion

48 Notre recherche a mis en évidence les pratiques liées à la vie privée et les perceptions des jeunes adultes en la matière lorsqu'ils utilisent les médias sociaux. Il existe des rapports complexes entre la visibilité, la surveillance et la vie privée. La protection de la vie privée ne dépend pas seulement des choix que font les usagers quand ils utilisent les RSN. Plusieurs partis façonnent la vie privée par rapport à ces contextes technologiques, que ce soit les propriétaires de sites Web, les annonceurs, les développeurs d'applications ou les cercles sociaux en ligne des usagers. Des lois canadiennes de la vie privée assurent le respect des droits des utilisateurs. Toutefois, en contexte d'usage, des problèmes liés à la vie privée peuvent survenir. De ce fait, nous avons souligné la nécessité que les propriétaires des RSN renforcent leurs pratiques de responsabilisation par rapport à la vie privée. Il est également judicieux de favoriser la réflexion critique sur les pratiques de surveillance institutionnelle et les technologies relatives à la protection des renseignements personnels, puisque c'est un élément nécessaire à une société responsable (Marx, 2015 : 126). Cela est d'autant plus important que les technologies sont de plus en plus mobiles et qu'il est maintenant difficile d'évaluer les nombreux risques, étant donné que la collecte de données se fait d'un appareil à un autre (Commissariat à la protection de la vie privée, 2016). Par ailleurs, les gens continuent à s'exposer bien qu'ils aient perdu le contrôle sur leur vie privée à cause de la surveillance sociale. Par conséquent, nous devons nous demander dans quelle mesure la confiance que placent les usagers des RSN en leurs contacts en ligne façonne leurs rapports avec la vie privée.

Bibliographie

AGUITON, Christophe *et al.* (2009), « Does showing off help to make friends? Experimenting a sociological game on self-exhibition and social networks », *Actes de colloques Third International ICWSM conférence*. [En ligne]. https://aaai.org/ocs/index.php/ICWSM/09/paper/view/178. Page consultée le 18 juin 2017.

ALTMAN, Irwin (1975), *The Environment and Social Behavior*, Pacific Grove (CA), Brooks/Cole Publishing Company.

BENNETT, Colin (2011), « In defence of privacy: The concept and the regime », *Surveillance & Society*, 8(4) : 485-496.

BENNETT, Colin J. *et al.* (2014), *Vivre à nu. La surveillance au Canada*, Edmonton, Athabasca Press.

BOYD, Danah (2008), « Facebook's privacy trainwreck: Exposure, invasion, and social convergence », *Convergence: The International Journal of Research into New Media Technologies*, 14(1) : 13-20.

BOYD, Danah (2010), « Social steganography learning to hide in plain sight ». [En ligne]. http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html. Page consultée le 25 février 2017.

BOYD, Danah et Ezster HARGITTAI (2010), « Facebook privacy settings: Who cares? », *First Monday*, 15(8). [En ligne]. http://firstmonday.org/article/view/3086/2589. Page consultée le 25 février 2017.

BRIGHENTI, Andrea Mubi (2010), *Visibility in Social Theory and Social Research*, Houndmills, Palgrave Macmillan.

BRUNTON, Finn et Helen NISSENBAUM (2015), *Obfuscation a User's Guide for Privacy and Protest*, Massachusetts, MIT Press.

CARDON, Dominique (2009), « L'identité comme stratégie rationnelle », *Hermès*, 1(5) : 61-66.

CASILLI, Antonio (2013), « Contre l'hypothèse de la "fin de la vie privée" », *Revue française des sciences de l'information et de la communication*, 3 : 1-14.

CEFRIO (2010), « L'explosion des médias sociaux au Québec », *NETendances*, 1 : 1-18.

CEFRIO (2011), « L'engouement pour les médias sociaux au Québec », *NETendances*, 2 : 1-20.

CEFRIO (2012), « Les médias sociaux ancrés dans les habitudes des Québécois », *NETendances*, 3 : 1-16.

CEFRIO (2014), « Actualité et nouvelles au Québec : l'ère de la mobilité et de l'information en temps reel », *NETendances*, 5 : 1-14.

COHEN, Julie E. (2008), « Privacy, visibility, transparency, and exposure », *University of Chicago Law Review*, 75(1) : 181-201.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE (2016), *Rapport annuel au Parlement 2015-2016 concernant la Loi sur la protection des renseignements personnels et les documents électroniques. Le temps est venu de moderniser les outils du 20e siècle.* [En ligne]. https://www.priv.gc.ca/media/4161/ar_201516_fra.pdf. Page consultée le 25 février 2017.

DAILY MAIL REPORTER (2011), « Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook », *Mail Online*, 7 février. [En ligne]. http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html. Page consultée le 25 février 2017.

DAVIS, Jenny L. et Nathan JURGENSON (2014), « Context collapse: Theorizing context collusions and collisions », *Information, Communication & Society,* 17(4) : 476-485.

DIGITAL ADVERSTISING ALLIANCE OF CANADA (2017), [En ligne]. http://youradchoices.ca/fr/. Page consultée le 25 février 2017.

ETZIONI, Amitai (2015), *Privacy in a Cyber Age*, Houndmills, Palgrave Macmillan.

FRANCE INFO (2011), « Le compte Twitter de Barack Obama piraté depuis la France », 1er novembre. [En ligne]. http://www.franceinfo.fr/actu/faits-divers/article/le-compte-twitter-de-barack-obama-pirate-depuis-la-france-154013. Page consultée le 25 février 2017.

FRIED, Charles (1984), « Privacy. A moral analysis » dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy*, Cambridge, Cambridge University Press, p. 203-222.

FUCHS, Christian (2009), « Social networking sites and the surveillance society. A critical case study of the usage of STUDIVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance », Salzburg, Vienne, Research Group UT. [En ligne]. http://fuchs.uti.at/wp-content/uploads/SNS_Surveillance_Fuchs.pdf. Page consultée le 25 février 2017.

GOFFMAN, Erving (1973), *La mise en scène de la vie quotidienne*, Paris, Minuit.

GRANJON, Fabien et Julie DENOUËL (2010), « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, 1(1) : 25-43.

GROSS, Ralph et Alessandro ACQUISITI (2005), « Information revelation and privacy in online social networks (the Facebook case) », *Actes du colloque Workshop on privacy in the electronic society (WPES)*. [En ligne]. https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf. Page consultée le 25 février 2017.

HINE, Christine (2009), « Virtual ethnography: Modes, verities, affordances » dans Nigel G. FIELDING, Raymond M. LEE et Grant BLANK (dir.), *The SAGE Handbook of Online Research Methods*, Los Angeles, Sage Publications, p. 257-270.

KWOK CHOON, Mary Jane (2016a), « La déconnexion temporaire à Facebook : entre le FOMO et l'intériorisation douce du contrôle social », *TIC & Société*, 10(1) : 1-19.

KWOK CHOON, Mary Jane (2016b), Les perceptions de la vie privée des jeunes adultes liées à leurs pratiques et usages des réseaux socionumériques : le paradoxe de la vie privée revisité. Thèse de doctorat en communication, sous la direction d'Éric GEORGE, Université du Québec à Montréal. [En ligne]. http://www.archipel.uqam.ca/8933/. Page consultée le 25 février 2017.

KWOK CHOON, Mary Jane et Isabelle CARON (2012), « Artveillance practices: From graffiti to social network sites », *Actes de colloque Technology & emerging media track, Canadian Communication Association*. [En ligne]. www.tem.fl.ulaval.ca/www/wp-content/PDF/Waterloo_2012/KWOK-CARON-TEM2012.pdf. Page consultée le 25 février 2017.

KWOK CHOON, Mary Jane et Serge PROULX (2012), « Luttes pour la reconnaissance de groupes associatifs : l'usage de Facebook par deux ONG de l'île Maurice » dans Serge PROULX, Serge, Mélanie MILLETTE et Lorna HEATON (dir.), *Médias sociaux. Enjeux pour la communication*, Québec, Presses de l'Université du Québec, p. 82-100.

LYON, David (2002), « Editorial. Surveillance studies: Understanding visibility, mobility and the phenetic fix », *Surveillance & Society*, 1(1) : 1-7.

MARWICK, Alice E. (2012), « The public domain: Social surveillance in everyday life (draft version) », *Surveillance & Society*, 9(4) : 378-393.

MARWICK, Alice E. et Danah BOYD (2011), « I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience », *New Media & Society*, 13(1) : 114-133.

MARX, Gary T. (2015), « Coming to terms and avoiding information techno-fallacies » dans Marc ROTENBERG, Julia HORWITZ et Jeramie SCOTT (dir.), *Privacy in the Modern Age. The Search for Solutions*, New York, The New Press, p. 118-126.

MARX, Gary T. (2001), « Murky conceptual waters: The public and the private », *Ethics and Information Technology*, 3 : 157-169.

MERLEAU-PONTY, Maurice (1964), *L'œil et l'esprit*, Saint-Amand, Gallimard.

NIPPERT-ENG, Christina (2010), *Islands of Privacy*, Chicago/London, University of Chicago Press.

NISSENBAUM, Helen (1997), « Toward an approach to privacy in public: Challenges of information technology », *Ethics & Behavior*, 7(3) : 207-219.

NISSENBAUM, Helen (2004), « Privacy as contextual integrity », *Washington Law Review*, 79 : 101-139.

NISSENBAUM, Helen (2010), *Privacy in Context. Technology Policy and Integrity of Social Life*, California, Stanford University Press.

NISSENBAUM, Helen (2011), « A contextual approach to privacy online », *Daedalus*, 140(4) : 32-48.

PROULX, Serge et Mary Jane KWOK CHOON (2011), « L'usage des réseaux sociaux numériques : une intériorisation douce et progressive du contrôle social », *Hermès*, 59 : 105-111.

RANDALL, David et Victoria RICHARDS (2008), « Facebook can ruin your life. And so can myspace, bebo... », *The Independent*, 1er mars 2008. [En ligne]. http://www.informationliberation.com/?id=24911. Page consultée le 18 juin 2017.

RAYNES-GOLDIE, Kate (2010), « Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook », *First Monday*, 15(1). [En ligne]. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432. Page consultée le 18 juin 2017.

SCHOEMAN, Ferdinand (1984), « Privacy and intimate information » dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy*, Cambridge, Cambridge University Press, p. 403-424.

SOLOVE, Daniel J. (2008), *Understanding Privacy*, Cambridge, Harvard University Press.

SPRADLEY, P. James (1979), *The Ethnographic Interview*, New York, Rinehart and Winston.

STALDER, Félix (2011), « Autonomy beyond privacy? A rejoinder to Bennett », *Surveillance & Society*, 8(4) : 508-512.

STEEL, Emily et Geoffrey G. FOWLER (2010), « Facebook in privacy breach », *Wall Street Journal*, 18 octobre 2010. [En ligne]. http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html. Page consultée le 25 février 2017.

TADDICKEN, Monika (2012), « Exploring the user's perspective via focus groups » dans Christian FUCHS *et al.* (dir.), *Internet Surveillance. The Challenges of Web 2.0 and Social Media*, New York, Routledge, p. 255-272.

THOMPSON, John B. (2005), « La nouvelle visibilité », *Réseaux*, 1(129-130) : 59-87.

TROTTIER, Daniel et David LYON (2012), « Key Features of Social Media Surveillance » dans Christian FUCHS, et *al.* (dir.), *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*, New York, Routledge, p. 255-272.

TUFEKCI, Zeynep (2008), « Grooming, gossip, Facebook and Myspace », *Information, Communication & Society*, 11(4) : 544-564.

VISEU, Ana et Andrew CLEMENT (2003), « Situating privacy online complex perceptions and everyday practices » (draft version). [En ligne]. https://www.oii.ox.ac.uk/archive/downloads/collaboration/seminars/20040317_Situating_Privacy_Online.pdf. Page consultée le 25 février 2017.

WESTIN, Alan (2003), « Social and political dimensions of privacy », *Journal of Social Issues*, 59(2) : 431-453.

YOUNG, Alison L. et Anabel QUAN-HAASE (2013), « Privacy protection strategies on Facebook », *Information, Communication & Society*, 16(4) : 479-500.

Notes

1 D'après Kaplan et Haenlein (2010), les médias sociaux sont une famille de sites. Les réseaux socionumériques font partie de cette famille et permettent aux usagers de se créer des listes d'amis et de contribuer au partage du contenu.

2 « Les impacts de la surveillance sur les individus ne menacent pas seulement la protection de la vie privée. Ils peuvent affecter leurs chances dans la vie et leur mode de vie. La surveillance excessive a aussi des impacts sur la nature même de la société » (traduction de l'auteure).

3 Ce sont des données en lien avec celles qui ont été produites par les utilisateurs.

4 John B. Thompson conçoit que « le visible est qui peut être vu, ce qui est perceptible par le sens de la vue ; l'invisible est ce qui ne peut être vu, ce qui est imperceptible ou caché à la vue » (2005 : 66).

5 « La visibilité est un important déterminant de l'accessibilité, mais les menaces pour la vie privée liées à la surveillance visuelle deviennent plus grandes quand elle s'articule à la dataveillance, permettant ainsi une identification en temps réel des surveillés "visibles" et les fouilles des archives visuelles et des bases de données » (traduction de l'auteure).

6 « À la liberté de pensée, au contrôle sur son identité, à la solitude dans son domicile, au contrôle sur l'information personnelle, au fait d'être libéré de la surveillance, à la protection de sa réputation et au fait de se protéger des recherches et des interrogations » (traduction de l'auteure).

7 Dans le présent texte, nous mettons entre guillemets « public » et « privé », car ces notions peuvent être définies de différentes manières.

8 C'est une ethnographie par et à travers Internet (Hine, 2009). Cette recherche fait partie d'une recherche doctorale que nous avons mené de 2009 à 2016. Nous remercions le Ministère de L'Éducation, du Loisir et du Sport (MELS), ainsi que la Faculté de Communication et l'École des Médias de l'Université du Québec à Montréal pour leur appui financier. Nous sommes aussi reconnaissante envers notre directeur de thèse et les participants de cette recherche.

9 D'après le dictionnaire Oxford en ligne, le *selfie* désigne « une photographie de soi prise par soi-même, qui a généralement été prise par un téléphone intelligent ou une webcam et qui a été partagée sur un média social ».

10 Le terme *stratégie* est ici utilisé au sens de stratégie communicationnelle que mobilise l'acteur au cours des interactions sociales (Goffman, *op. cit.*).

11 Voir tableau 1 pour le nombre d'abonnés et d'abonnements sur Twitter. Notons que nous n'avons pas étudié le lien entre le nombre de personnes dans des cercles sociaux en ligne et la propension des usagers à s'exposer davantage. Dans le cadre de notre étude, les utilisateurs s'engagent dans les mêmes pratiques, bien que leur nombre d'abonnés et d'abonnements varie.

12 « La capacité d'attirer et celle de retenir l'attention sont des marques de son statut » (traduction de l'auteure).

13 Souvent, l'application mobile génère une fenêtre *pop-up* pour demander à l'usager de donner accès à son emplacement.

14 Il s'agit ici d'être sujet à la surveillance sociale, voire ensuite d'être harcelé.

15 « Le dévoilement de l'information à des groupes plus ou moins grands peut être reconnu comme relevant du "privé" étant donné que des groupes plus importants sont exclus » (traduction de l'auteure).

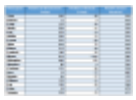
16 « Il existe une déformation systématique des perceptions. On perçoit des avantages de participer aux nouvelles formes de visibilité médiatique au détriment des perceptions des formes de contrôle social qui y sont rattachées » (traduction de l'auteure).

17 « Si le processus de mettre en relation les règles contextuelles et les attentes des individus et d'intégrer quelques-unes d'entre elles dans le code se fait de manière consciencieuse, nous pourrons créer des filets de sécurité qui appuient le consentement dans le domaine de la santé et de la recherche par exemple. Avec ces précautions mises en place, il y aura beaucoup de place pour exprimer des préférences personnelles et pour maintenir le rôle important qui doit être attribué au consentement éclairé » (traduction de l'auteure).

18 « Facebook changes new user default setting to friends only-Add privacy check-up ». [En ligne]. http://www.forbes.com/sites/larrymagid/2014/05/22/facebook-changes-default-privacy-setting-for-new-users/. Page consultée le 22 septembre 2017.

19 Digital Advertising Alliance of Canada. [En ligne]. http://youradchoices.ca/fr/. Page consultée le 22 septembre 2017.

Table des illustrations



Titre	Tableau 1. Nombre d'amis Facebook, d'abonnés et d'abonnements Twitter
URL	http://journals.openedition.org/communication/docannexe/image/7571/img-1.png
Fichier	image/png, 73k
Titre	Capture écran 1. *Tweet* de Sébastien
URL	http://journals.openedition.org/communication/docannexe/image/7571/img-2.png
Fichier	image/png, 20k

Pour citer cet article

Référence électronique
Mary Jane Kwok Choon, « « Publiquement privé » et le contexte », *Communication* [En ligne], vol. 35/1 | 2018, mis en ligne le 27 février 2018, consulté le 02 mars 2018. URL : http://journals.openedition.org/communication/7571

Auteur

Mary Jane Kwok Choon
Mary Jane Kwok Choon est membre du Centre de recherche interuniversitaire sur la communication, l'information et la société (CRICIS), Université du Québec à Montréal. Courriel : kwok_choon.mary_jane@courrier.uqam.ca

Droits d'auteur