David Myles, Université du Québec à Montréal
myles.david@uqam.ca
Florence Millerand, Université du Québec à Montréal
millerand.florence@uqam.ca
Chantal Benoit-Barné, Université de Montréal
chantal.benoit-barne@umontreal.ca

Citation : Myles, D., Millerand, F. & C. Benoit-Barné. (2016). Résoudre des crimes en ligne. La contribution de citoyens au Reddit Bureau of Investigation, Réseaux, no 197, p. 173-202.

RÉSOUDRE DES CRIMES EN LIGNE : LA CONTRIBUTION DE CITOYENS AU *REDDIT BUREAU OF INVESTIGATION*

Résumé : Le développement des technologies numériques participe à l'émergence de nouveaux types d'initiatives citoyennes de sécurité. Cet article explore quatre formes de contribution en ligne de citoyens en matière de gouvernement du crime issues des sciences sociales et humaines: le travail de surveillance non institutionnalisée, le *crowdsourced policing*, les *online vigilantes* et la *civilian police*. Les enjeux soulevés par chacune de ces formes de contribution sont mobilisées pour mettre en lumière les résultats d'une démarche d'observation exploratoire au sein du *Reddit Bureau of Investigation*, un forum Internet étatsunien qui regroupe des citoyens dont l'objectif est la résolution de crimes. Les résultats témoignent du rôle clé des technologies numériques et de surveillance dans l'émergence de ces pratiques, de nouvelles conceptions du rôle du citoyen en matière de gouvernement du crime, de la construction d'une identité commune en réaction à la figure du *vigilante* et du déploiement d'une expertise profane d'investigation.

Depuis la mise en place des premières institutions policières publiques modernes au XIXe siècle (Auten, 1981), le monopole de l'État a grandement reposé sur la confiance des citoyens envers l'appareil judiciaire afin de justifier leur propre exclusion des processus assurant la sécurité des territoires (Zedner, 2006). Aujourd'hui, nous assistons à une nouvelle répartition des responsabilités en matière de sécurité entre l'État et ses citoyens, ainsi qu'à une pluralisation des agents responsables du gouvernement du crime (Bayley et Shearing, 1996). Au centre de ces changements, les professionnels de la sécurité, et les policiers en uniforme en particulier, sont appelés à redéfinir leur rôle comme l'un des (et non l'unique) groupes d'acteurs nécessaires à la création et la mise en place d'une programmation sociétale de sécurité (Shearing et Marks, 2011). Cette pluralisation d'agents en matière de gouvernement du crime s'explique

notamment par une hausse observable d'initiatives citoyennes (Zedner, 2006; Shearing et Marks, 2011).

En Amérique du Nord, cette hausse est associée à l'accroissement d'un sentiment d'autoresponsabilité chez les citoyens étant de plus en plus appelés à jouer un rôle actif dans la société (Zedner, 2006) et s'inscrit dans une trajectoire sociohistorique étatsunienne antigouvernementale marquée par un scepticisme entretenu par certains groupes de citoyens envers les agences gouvernementales de sécurité formellement mandatées par l'État (King et al., 1998). Jusqu'à présent, les initiatives citoyennes, qu'elles soient menées en collaboration avec la police publique ou non, ont entre autres pris la forme de patrouilles, de veilles de voisinage, de bulletins d'information communautaire, d'associations de prévention du crime ou de surveillance scolaire (Bayley et Shearings, 1996 : 587). Aujourd'hui, l'utilisation massive d'Internet et des technologies numériques contribuerait à la redéfinition du rôle du citoyen en matière de gouvernement du crime, passant de « consommateur passif de la protection de la police à un coproducteur actif de sécurité publique » (Bayley et Shearings, 1996 : 588). Comme le soulignent Huey et al. (2013), de nouvelles formes de collaboration spontanées entre citoyens afin de résoudre des crimes ont récemment émergé sur Internet et méritent d'être mieux documentées. En ce sens, il n'existe aucun consensus conceptuel ou axiologique dans la littérature quant à la manière d'appréhender ces pratiques émergentes. Voulant répondre à l'appel de Huey et al. (2013), cet article propose d'étudier le forum Internet *Reddit* afin d'apporter certains éléments de réponse. Neuvième site le plus visité aux États-Unis[1], *Reddit* constitue une communauté d'intérêts et d'actualités très populaire. Le site enregistre 200 millions de visiteurs uniques par mois issus de 208 pays, compte près de huit milliards de pages et contient environ 9000 sous-forums actifs[2]. La présente étude se penche spécifiquement sur le cas du sous-forum intitulé *Reddit Bureau of Investigation* (RBI). Regroupant près de 30 000 membres, l'objectif du

[1] ALEXA. (2015), « Alexa - Top Sites in United Stats », [En ligne], <www.alexa.com/topsites/countries/US>, consulté le 13 novembre 2015.

[2] REDDIT. (2015), « About Reddit », [En ligne], <www.reddit.com/about>, consulté le 13 novembre 2015.

RBI est « de résoudre des crimes et des mystères »[3]. Des usagers s'y rendent afin de solliciter l'aide d'autres membres pour résoudre des crimes dont ils sont souvent les victimes. Ainsi, cet article vise à documenter les pratiques observées au sein du RBI afin de comprendre dans quelle mesure Internet et les technologies numériques participent à la redéfinition des rôles du citoyen en matière de gouvernement du crime et, plus spécifiquement, dans la résolution de crimes.

QUATRE FORMES DE CONTRIBUTION EN LIGNE DE CITOYENS EN MATIÈRE DE GOUVERNEMENT DU CRIME

Cette section recense les différentes façons dont la contribution d'internautes en matière de gouvernement du crime a été conceptualisée dans la littérature (majoritairement anglo-saxonne) en sciences humaines et sociales. Quatre formes de contribution sont abordées : le travail de surveillance, le *crowdsourced policing*, les *online vigilantes* et la *civilian police*. Chacune de ces formes révèle d'importants enjeux contemporains qui sont ensuite décrits. Les résultats d'une phase d'observation exploratoire du RBI s'échelonnant sur une période de deux mois seront discutés à l'aune de ces enjeux. Ces résultats seront présentés dans la section subséquente.

Le travail de surveillance non institutionnalisée

La première forme de contribution citoyenne en matière de gouvernement du crime que nous relevons est le « travail de surveillance » issu des *Surveillance Studies*. Si l'intérêt scientifique pour la surveillance n'est pas nouveau (Foucault, 1975), c'est davantage sous la gouverne de David Lyon que s'est développé le courant des *Surveillance Studies*, dont l'objectif est l'étude globale et systématique des phénomènes quotidiens de surveillance humaine (Lyon et al., 2012). La surveillance évoque traditionnellement une stratégie consciemment mise en place dans une logique adversaire de collecte et d'exploitation d'information concernant un ou plusieurs individus (Marx, 2012 : xxv). Les travaux issus des *Surveillance*

[3] RBI. (2014), « RBI : Reddit Bureau of Investigation », [En ligne], <www.reddit.com/r/RBI>, consulté le 20 juillet 2014.

Studies portent entre autres sur les structures sociales encadrant la surveillance, sur les techniques de surveillance utilisées, sur la nature des données collectées, sur les objectifs visés (notamment celui de réduire la criminalité) et sur leurs conséquences (Lyon, et al., 2012). Ce courant trouve une résonance dans le champ de la communication dans la mesure où il s'intéresse particulièrement à la « nouvelle surveillance » menée par l'entremise de technologies numériques se distinguant de la surveillance humaine traditionnelle reposant essentiellement sur les sens innés, dont la vue. Sans complètement déterminer les phénomènes contemporains de surveillance observés, les technologies, dorénavant plus accessibles et relativement faciles à utiliser, en constitueraient une « prédisposition vitale » (Lyon et al., 2012 : 1).

Traditionnellement, les travaux issus des *Surveillance Studies* ont eu tendance à insister sur les processus de surveillance institutionnelle et à sous-estimer les pratiques de surveillance hors des milieux organisés. Pour Smith (2012 : 114), une définition plus inclusive du travail de surveillance (qu'il appelle *labor of watching*) serait nécessaire « afin d'incorporer les panoplies diverses de pratiques professionnelles, de technologies et d'activités comprises dans la composition contemporaine » de ce type de travail. À cet effet, l'auteur (Smith, 2012) distingue le travail de surveillance en tant qu'*activité mondaine* personnelle chez le citoyen de l'*activité organisationnelle* du travailleur répondant à des objectifs bureaucratiques. Cette distinction est intéressante, car elle permet l'inclusion de nouveaux types de travail de surveillance non institutionnalisée. Par exemple, la notion de « surveillance sociale » (Marwick, 2012) renvoie aux usagers de réseaux socionumériques tels que *Facebook* ou *Instagram* qui « épient » leurs propres amis en accédant quotidiennement aux informations personnelles que ces derniers publient sur leurs profils. Dans une perspective résolument moins « mondaine », ces mêmes informations sont ensuite utilisées par la police et les agences de sécurité à titre de renseignement (ou *social media intelligence)* (Omand et al., 2012) afin de combler des objectifs organisationnels, comme la résolution d'enquêtes criminelles ou la lutte contre le terrorisme (Trottier, 2014a).

À l'inverse, la notion de *sousveillance* (Mann et al., 2002; Ali et Mann, 2013), autre type de travail de surveillance non institutionnalisée, renvoie à l'ensemble des initiatives citoyennes menées dans le but de documenter et de critiquer les pratiques de surveillance des organisations, notamment grâce à l'usage de technologies mobiles. Les initiatives de *sousveillance* prennent souvent comme

cibles les policiers en uniforme, pratiques communément appelées *copwatching* (Meyer, 2010), et s'inscrivent fortement dans une logique de dénonciation de l'ordre social établi. Ainsi, les pratiques de *sousveillance* reposent sur une logique fortement adversaire et suppose une certaine homogénéité des objectifs (c'est-à-dire la dénonciation ou la remise en question de l'ordre social établi) et des cibles (c'est-à-dire les institutions ou leurs représentants) du travail de surveillance par les citoyens. Nous verrons que le cas du RBI pointe vers l'émergence d'un type de travail de surveillance non institutionnalisée dont l'objectif ne semble pas être de dénoncer l'ordre social établi (dans une logique qu'on voudrait émancipatrice) ni d'assurer sa simple reproduction (dans une logique qu'on voudrait aliénante), mais plutôt de répondre à des besoins ponctuels d'ordre privé. En d'autres termes, les membres de RBI semblent s'unir pour la résolution de crimes non pas pour remettre en question la légitimité des autorités, ni pour reproduire ou étendre la dominance de ces dernières, mais plutôt dans le but ponctuel d'aider les victimes qui se sont manifestées. Malgré ces distinctions conceptuelles importantes, l'émergence de divers types de travail de surveillance non institutionnalisée reposant sur l'usage d'Internet et des technologies numériques constitue une première façon de rendre compte de la complexification croissante de « l'acte contributoire » citoyen en matière de gouvernement du crime.

Le *crowdsourced policing*

La deuxième forme de contribution citoyenne en matière de gouvernement du crime évoquée dans la littérature est celle du *crowdsourced policing* (Dong et Camp, 2012)[4]. Le *crowdsourced policing* se définit comme étant « un modèle managérial reposant sur l'utilisation des contributions d'internautes par des organisations formelles de sécurité (privées ou publiques) afin de résoudre des enquêtes criminelles » (Myles, à paraître). Le *crowdsourced policin*g comporte deux principales dimensions : celle de *policing* et de *crowdsourcing*. D'un côté, la notion de *policing* renvoie à l'ensemble des processus contribuant consciemment au gouvernement du crime et à la mise en place d'une programmation sociétale de sécurité (Baley et Shearing, 1996). De l'autre, la

[4] Le terme pourrait être traduit de manière imparfaite par « approvisionnement par la foule à des fins de sécurité ».

notion de *crowdsourcing* réfère à un modèle managérial qui mélange délibérément « des processus ascendants (*bottom-up*) et créatifs avec des objectifs organisationnels descendants (*top-down*) » (Brabham, 2013 : xv). Le modèle du *crowdsourcing* sous-tend ainsi l'utilisation des savoirs théoriques et pratiques de la foule, ici comprise comme un ensemble hétérogène de citoyens, dans le but de répondre aux objectifs d'une organisation. Dans le cadre du *crowdsourced policing*, ces objectifs seront spécifiquement liés à des enjeux de sécurité. L'un des aspects-clés de ce modèle concerne le lieu de contrôle des opérations qui sera partagé entre la foule et l'organisation formelle. Si le contrôle des objectifs à atteindre est habituellement réservé à l'organisation, certaines initiatives de *crowdsourcing* attribueront une grande marge de manœuvre à la foule dans la définition des procédures et pour la sélection des stratégies de résolution de problème (Brabham, 2013). D'autres initiatives imposeront des tâches simples et répétitives à la foule, comme le suggère Haythornthwaite (2009) lorsqu'elle développe la notion de *microparticipation*.

Au Canada, Trottier et Schneider (2012) se sont intéressés aux stratégies utilisées par le corps policier de la ville de Vancouver lors d'une émeute ayant suivi un match de hockey en 2011. Les photos des responsables de dégâts lors de cette émeute ont été diffusées sur Facebook et les usagers ont été invités à identifier les individus recherchés, évoquant une logique de dénonciation publique. Le modèle du *crowdsourced policing* est également adopté par certaines firmes privées qui, par exemple, utilisent le « pouvoir de la foule » en rendant accessibles leurs nombreuses heures de vidéosurveillance (*CCTV*) archivées dans le but de déceler la présence d'activités criminelles (Trottier, 2014b). Suivant l'engouement du public pour contribuer à l'enquête criminelle des attentats de Boston de 2013, des chercheurs (Brabham, 2013b; Marx, 2013) se sont prononcés en faveur de l'utilisation du travail citoyen à des fins de gouvernement du crime advenant un meilleur contrôle de celui-ci par l'État. La mobilisation du travail citoyen suscite une série d'enjeux pragmatiques et éthiques que nous abordons plus en profondeur ailleurs (Myles, à paraître), notamment en termes de risques et de potentialités. Ici, l'intérêt du *crowdsourced policing* réside dans sa propension à reconceptualiser la relation entre les professionnels et leurs publics. En décentralisant à divers degrés le contrôle des objectifs et en mobilisant des expertises à l'extérieur des institutions de sécurité formellement mandatées, le modèle du *crowdsourced policing* oblige à revoir la frontière traditionnellement érigée entre les producteurs et les consommateurs de sécurité. Toutefois,

l'utilisation de citoyens au sein d'initiatives de *crowdsourced policing* s'est principalement limitée à l'octroi de tâches simples et répétitives, alors que les initiatives plus complexes ou nécessitant des tâches d'analyse étaient découragées (Myles, à paraître). Ceci témoigne du caractère utilitariste de la relation établie entre les professionnels de la sécurité et leurs publics, dans la mesure où les collaborations observées à ce jour reposent grandement sur une conception du citoyen en tant que ressource et non en tant que partenaire. Nous verrons que le cas du RBI soulève de nouvelles conceptions du citoyen en la matière qui rejette la conception utilitariste traditionnelle.

L'*online vigilante*

Que ce soit sous l'appellation *online vigilantes*, *Internet vigilantes* ou *digilantes* (Byrne, 2013), les recherches en sciences sociales se sont intéressées, depuis la fin des années 90, à l'usage d'Internet par certains citoyens désirant rendre, obtenir ou rétablir justice. Aux États-Unis, la figure du *vigilante* (« justicier » en français) remonterait au XVIII^{e} siècle alors que certains groupes de citoyens se réunissaient afin de restaurer ou maintenir l'ordre dans un contexte sociohistorique où les institutions policières étaient précaires et inadéquates (Byrne, 2013). Johnston (1996 : 220) décrit le *vigilantism* comme étant le contrôle de la criminalité par un groupe de citoyens pour qui cet engagement prémédité et volontaire constitue une forme d'exercice de la citoyenneté et qui utilise ou menace d'utiliser la force afin de rétablir l'ordre. Badaracco et Useem (1997) auraient été les premiers chercheurs à utiliser la notion d'*online vigilante*. Leur étude s'intéressait aux différents actes de vengeance commis en ligne par les actionnaires d'une entreprise de télécommunications tenus responsables de problèmes financiers encourus à l'époque. Depuis, la notion d'*online vigilantes* a été utilisée afin de désigner certains internautes qui décident de se faire « justice eux-mêmes » (Chua et Wareham, 2004 : 35; Vander Ende, 2014 : 1). L'*online vigilantism* sous-tendrait une logique de *shaming* (c'est-à-dire « provoquer la honte ») (Wall et Willams, 2007) et de vengeance (Sharp et al., 2008), et constituerait, pour certains auteurs, un acte criminel comparable au terrorisme (Vander Ende, 2014). En Chine, le phénomène du *Human Flesh Search Engine* (HFSE), signifiant de manière littérale « moteur de recherche pour chair humaine ») (Liu, 2008; Wang et al., 2009), renvoie aux groupes décentralisés

d'individus utilisant Internet afin de « faire honte publiquement à, surveiller et se venger de » personnes suspectées de crimes (Cheung, 2009 : 275). Parmi les exemples cités de HFSE, notons des affaires criminelles aussi variées que le meurtre d'un chat par une femme à l'aide de ses talons hauts (Cheong et Gong, 2010) ou celui d'élus gouvernementaux corrompus (Gao et Stanyer, 2014).

L'un des principaux intérêts des travaux portant sur le « justicier en ligne » est d'introduire la dimension motivationnelle des citoyens. Il a été proposé que les initiatives citoyennes en matière de gouvernement du crime ont tendance à viser des objectifs de justice plutôt que de prévention et de contrôle disciplinaire que visent plutôt les initiatives institutionnelles publiques et privées (Bayley et Shearings, 1996). Par exemple, chez Klang (2015), la figure du justicier en ligne renvoie à une « (sur)réaction sociale disproportionnée envers des actions mondaines de non-célébrités » et au fait de « patrouiller contre la transgression de normes ». Dans le cadre de cette étude (Chua et Wareham, 2004), l'appellation de justicier pourrait s'avérer problématique étant donné son caractère hautement péjoratif. Qui plus est, dans leur étude portant sur des groupes de citoyens luttant contre la fraude en ligne, Chua et Wareham (2004) ont noté qu'aucun des participants ne s'identifiait à la figure de justicier. Les auteurs (Chua et Wareham, 2014) ont alors suggéré que cette figure constituait essentiellement une construction médiatique dont l'usage était devenu populaire, mais qui ne reflétait pas la diversité et la complexité des pratiques citoyennes qu'elle désignait. Néanmoins, ce rejet de la figure du justicier par les citoyens contribuant au gouvernement du crime ne signifie pas pour autant qu'elle n'est pas pertinente pour la présente étude. Bien au contraire, nous verrons que cette figure traverse l'ensemble des activités du RBI et est fortement mobilisée par ses usagers. Ainsi, la figure du justicier apparaît intéressante non pas dans sa capacité définitoire, mais plutôt dans sa propension à fournir aux usagers un objet rhétorique contre lequel ils peuvent s'inscrire afin de définir collectivement leur identité et leur pratique.

La *civilian police*

La quatrième et dernière forme de contribution citoyenne en matière de gouvernement du crime issue de la littérature est celle de la *civilian police* (ou

« police civile » en français). Cette notion est tirée de l'étude de Huey et al. (2013) qui cherche à comprendre les motivations des citoyens qui, en collaboration plus ou moins formelle avec les autorités, mènent des enquêtes sur Internet afin d'appréhender des individus suspectés de crimes. Dans cette étude portant notamment sur des groupes citoyens luttant contre la cyberpédophilie, les auteurs (Huey et al., 2013) font la distinction entre ce qu'ils qualifient de *vigilantes* et de *civilian police*. En effet, alors que « les *vigilantes* effectuent des actes de vengeance comme le piratage informatique et le harcèlement indépendamment des institutions formelles de police », les groupes de *civilian police* « collectent et transfèrent l'information concernant des crimes ou de potentiels crimes en ligne » à ces institutions, tandis que certaines organisations hybrides utilisent les deux types de stratégies (Huey et al., 2013 : 85). Ainsi, les groupes de *civilian police* travaillent en marge du domaine policier professionnel, mais collaborent avec les autorités aux étapes d'arrestation et de poursuite judiciaire.

Dans cette même étude, Huey et al. (2013) ont identifié plusieurs raisons qui mènent les citoyens à adopter des pratiques de résolution d'enquêtes, dont la volonté de partager leur expertise technique ou professionnelle et de dévouer leur temps et leur énergie à une cause qui leur tient à cœur (Huey et al., 2013). Alors que les citoyens en question jugeaient la perception qu'ont les policiers de ce type de travail collaboratif comme étant généralement positive, les entretiens menés auprès de policiers ont dressé un portrait très différent. En effet, ces derniers ont jugé la participation des citoyens comme étant « non nécessaire » et potentiellement « problématique », soutenant que, par souci de sécurité, « la réception d'informations [de la part de citoyens] est utile, mais que l'enquête de cybercrimes devrait être réservée à la police » (Huey et al., 2013 : 93). On dénote ici une vision essentiellement utilitariste du rôle du citoyen qui est avant tout considéré dans sa potentialité à servir d'informateur (Sharp et al., 2008). Un autre policier a également utilisé les arguments de l'expertise et de la responsabilité légale afin de soutenir l'exclusion des citoyens dans la résolution d'enquêtes criminelles[5].

[5] Plus spécifiquement, le policier a dit : « Ok, I'm going to work with you, then you automatically have the same powers and duties that I do. That opens the city to way too much liability because you don't have the same training and expertise that we do » (Huey et al., 2013 : 93).

Pour Vander Ende (2014) et Winters (2008), une collaboration réussie entre citoyens et policiers professionnels passerait par la normalisation des processus de résolution d'enquêtes criminelles. Toutefois, cette normalisation devrait, selon eux, se faire exclusivement au profit des processus « professionnels », laissant présager que ceux établis par les citoyens sont *de facto* désuets. Pourtant, les pratiques des groupes de *civilian police* étudiés par Huey et al. (2013 : 94) ont permis l'arrestation de dizaines de criminels et présenteraient certains avantages, comme la détection plus rapide d'activités criminelles en ligne, l'accès à des ressources plus diversifiées de par l'hétérogénéité de la formation des membres contributeurs, ainsi qu'une rapidité accrue de collecte et d'analyse de l'information. Ainsi, la notion de *civilian police* génère des questionnements très importants liés à l'expertise mobilisée par les citoyens afin de contribuer au gouvernement du crime. Cette forme de contribution amène également à penser aux moyens utilisés par les usagers du RBI afin de définir et de légitimer leurs activités, notamment en soulignant les ressemblances ou en marquant les différences de leur propre groupe d'appartenance vis-à-vis d'autres groupes de producteurs de sécurité (policiers, détectives privés, analystes criminels, avocats criminels, justiciers, etc.). À ce titre, le nom du *Reddit Bureau of Investigation*, inspiré du *Federal Bureau of Investigation* (FBI), constitue un indice important quant à l'importance de la métaphore policière américaine comme stratégie d'identification. La notion de *civilian police* amène également à envisager la formalisation des processus collaboratifs entre citoyens sur un continuum allant de regroupements spontanés aux collectifs stabilisés et hautement organisés. Finalement, cette forme de contribution émergente nous rappelle que les pratiques citoyennes en matière de gouvernement du crime s'inscrivent dans un contexte social plus large empreint de rapports de force entre différents groupes d'acteurs luttant pour la reconnaissance de leurs intérêts et de leurs besoins (Sarfatti-Larson, 1979). À ce titre, ces pratiques citoyennes pourraient être perçues par certains groupes de travailleurs comme autant d'obstacles au processus de professionnalisation du travail policier s'opérant depuis le début du XIXe siècle.

LE *REDDIT BUREAU OF INVESTIGATION*

Le sous-forum *Reddit Bureau of Investigation* est, dans le cadre de cette étude, appréhendé comme l'un des nombreux lieux d'émergence de nouvelles pratiques citoyennes en matière de gouvernement du crime. Créé en janvier 2012, le RBI

regroupe en 2016 près de 30 000 membres[6]. L'objectif officiel du RBI a évolué au cours des années, passant de l'utilisation du « pouvoir de *Reddit*, dans le but d'élucider des crimes/mystères et d'arrêter les criminels »[7] à la mise sur pied « d'un groupe de Redditeurs intéressés à résoudre des crimes/mystères et à aider les gens dans le processus »[8]. Sur la page d'accueil figurent en gras deux principales normes éthiques de contribution, la première interdisant strictement toute chasse aux sorcières et la seconde interdisant la publication d'informations personnelles sur les suspects potentiels. De plus, la page d'accueil offre une série de normes processuelles de contribution portant sur le partage d'images à des fins d'analyse criminalistique (*forensics*), à savoir que celles-ci doivent être soumises dans leur format d'origine afin de conserver leur qualité et les métadonnées qui y sont associées. La page d'accueil propose également une liste de sites Web afin d'aider les usagers à retrouver des objets perdus ou volés (caméras, téléphones intelligents, ordinateurs, vélos, etc.), à faire face à un problème de vols d'identité ou de courrier, ou encore à identifier qui se cache derrière une adresse électronique ou IP. Jusqu'en 2015, un fil de discussion intitulé *Aidez-nous à vous aider! Lisez ce post avant de commencer le vôtre* était épinglé à la page d'accueil afin d'assurer « l'accès à de meilleures données ». En plus de proposer des normes contributives soulignant l'importance de publier des photos originales de qualité, ce *sticky post* (l'équivalent d'un *Post-it* numérique) listait les bonnes pratiques en matière de demande d'aide afin de permettre aux usagers « d'identifier un objet, un lieu, une plaque d'immatriculation et le modèle et la marque d'une voiture ». Qui plus est, les contributeurs identifiaient dans ce *sticky post* des normes processuelles de contribution, comme offrir le plus d'informations contextuelles possibles concernant l'affaire criminelle traitée dans le titre du fil de discussion créé (le lieu géographique complet, l'absence d'abréviations équivoques, etc.) et répondre rapidement aux questions posées par les autres membres.

Une phase d'observation exploratoire a été menée sur une période d'un peu plus de deux mois entre 2014 et 2015. Des 121 fils de discussion identifiés, seuls 66 portaient sur des cas criminels, dont un vol (23 cas), un délit de fuite (12 cas), un

---

[6] Étant donné le caractère anonyme du forum *Reddit*, il est difficile de dresser un portrait sociodémographique des membres du RBI. Les crimes recensés sur le RBI ont, quant à eux, été majoritairement perpétrés aux États-Unis.

[7] REDDIT (2014). Toutes les traductions de l'anglais au français ont été effectuées par les auteurs.

[8] RBI (2015).

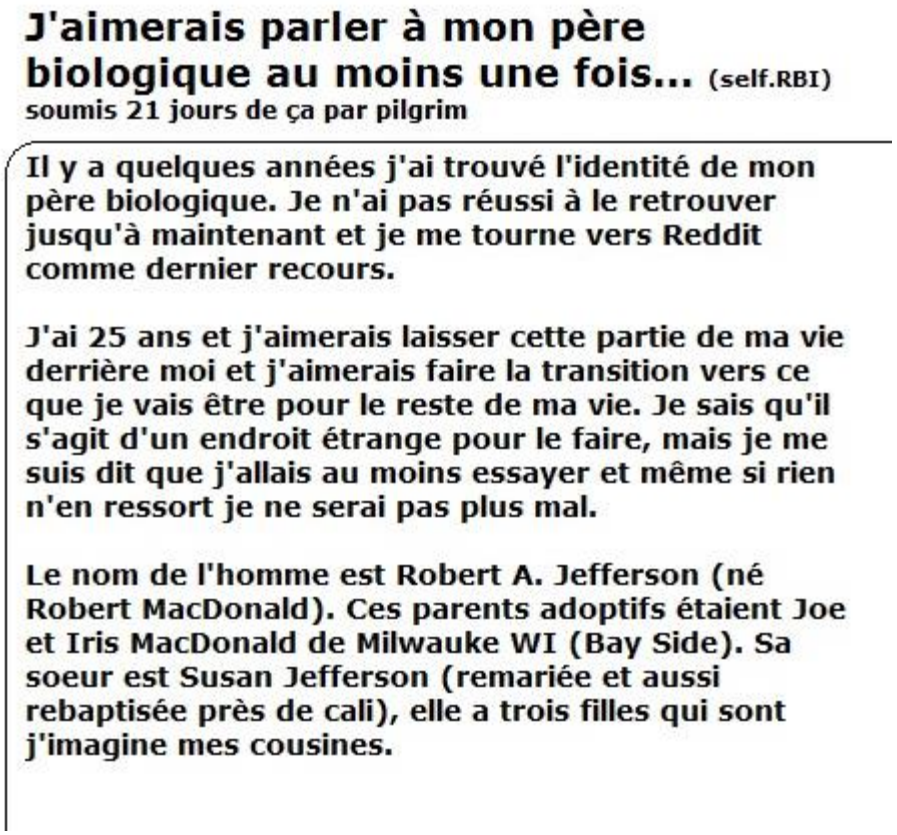
meurtre (6 cas), une agression (5 cas), une disparition (4 cas), des menaces (3 cas) et une usurpation d'identité (2 cas). Les cas non criminels étaient surtout liés à la recherche d'un membre de famille (13 cas) ou présentaient des énigmes de types très diversifiés. Les fils de discussion créés visaient différents objectifs, dont la demande générale d'aide en matière d'enquête (40 cas), la recherche d'un individu (22 cas), le décryptage d'un message ou d'un symbole (10 cas), l'identification d'une personne, notamment sur photo ou vidéo (10 cas), l'identification d'une plaque d'immatriculation captée sur photo ou vidéo (10 cas), l'identification d'un modèle ou d'une marque de voiture (8 cas), l'identification d'objets divers comme des appareils électroniques (5 cas), la recherche de l'emplacement d'objets divers (3 cas) et le travail d'image ou de son (3 cas). Seuls cinq fils de discussion n'ont pas été créés dans une logique de demande d'aide, visant plutôt un objectif de sensibilisation à un cas d'actualité ou à une problématique (3 cas), un objectif de remerciement (1 cas) ou l'offre d'un conseil (1 cas). Au sein des 121 fils, 40 faisaient spécifiquement mention de la police, c'est-à-dire qu'ils soulignaient l'existence d'une collaboration passée ou actuelle avec les autorités en lien avec la demande d'aide, ou contenaient une ou plusieurs publications conseillant de faire un signalement à la police. Quarante-six fils observés offraient un lien vers un document de travail (photo, vidéo, URL, etc.), alors que 29 cas traitaient de l'usage de bases données à accès ouvert (réseaux socionumériques, bases de données généalogiques, etc.). Dans la prochaine section, nous mobiliserons les enjeux soulevés dans la section précédente afin de mieux comprendre les pratiques observées au sein du RBI par l'entremise d'extraits issus de la phase d'observation.

Le rôle clé des technologies numériques et d'Internet

D'entrée de jeu, notre analyse a permis de constater que les pratiques observées au sein du RBI sont intimement liées au développement des technologies numériques. Les usages de trois types de dispositifs se sont dégagés : les bases de données en ligne, les dispositifs de surveillance et les technologies mobiles. D'abord, le développement et l'accessibilité en ligne de grandes bases de données permettent aux membres du RBI d'exploiter l'information disponible afin de répondre à leurs objectifs d'enquête, comme localiser ou identifier un individu. Il

faut souligner ici que ce type d'objectif est aussi fréquent au sein des cas criminels que non criminels.

Extrait 1 - À la recherche de son père biologique



J'aimerais parler à mon père biologique au moins une fois... (self.RBI)
soumis 21 jours de ça par pilgrim

Il y a quelques années j'ai trouvé l'identité de mon père biologique. Je n'ai pas réussi à le retrouver jusqu'à maintenant et je me tourne vers Reddit comme dernier recours.

J'ai 25 ans et j'aimerais laisser cette partie de ma vie derrière moi et j'aimerais faire la transition vers ce que je vais être pour le reste de ma vie. Je sais qu'il s'agit d'un endroit étrange pour le faire, mais je me suis dit que j'allais au moins essayer et même si rien n'en ressort je ne serai pas plus mal.

Le nom de l'homme est Robert A. Jefferson (né Robert MacDonald). Ces parents adoptifs étaient Joe et Iris MacDonald de Milwauke WI (Bay Side). Sa soeur est Susan Jefferson (remariée et aussi rebaptisée près de cali), elle a trois filles qui sont j'imagine mes cousines.

Dans l'extrait 1, l'usager *pilgrim* demande l'aide des membres du RBI afin de localiser son père biologique[9][10]. Ces derniers mobilisent alors diverses bases de données en accès ouvert agrégeant des informations nominatives (nom de l'individu, numéro de téléphone, adresse postale, etc.) dans le but de retrouver la personne recherchée. Dans certains cas, les usagers feront un usage hybride des bases de données en ligne qui visent volontairement un objectif de localisation ou d'identification (par exemple, les *pages blanches*, *Spokeo*, *Pipl*, etc.) et certains réseaux socionumériques dont l'aspect de localisation est secondaire à celui de mise en relation (par exemple, *Facebook*, *Twitter*, etc.). Ces pratiques rappellent le *skiptracing* qui, dans le domaine juridique, réfère au fait de « localiser des personnes, comme des débiteurs en défaut, des héritiers disparus, des témoins, des actionnaires, des investisseurs privés, etc. » (Lopez, 2012-2013 : 930). Les cas de nature familiale sont d'autant plus intéressants qu'ils permettent l'observation d'un certain paradoxe, dans la mesure où la publication d'informations personnelles d'un membre de famille recherché est tolérée, alors que celle de suspects est formellement interdite. Ensuite, les pratiques menées au sein du RBI sont également liées au développement des dispositifs de surveillance, notamment celui des caméras de vidéosurveillance (*CCTV*). Par exemple, *yessman* cherche à identifier les individus ayant commis un vol au sein de son domicile. Cet usager partage alors un hyperlien menant vers une captation vidéo du vol qu'il a générée à l'aide d'un dispositif de surveillance *Dropcam*. Ce type de dispositif enregistre automatiquement les mouvements à l'intérieur de la maison s'il constate que l'*iPhone* du propriétaire de celle-ci ne se trouve pas dans les environs. S'en suit une série d'interactions au sein de laquelle les membres tentent d'effectuer une reconstruction temporelle du crime et d'identifier les prises offrant le meilleur

[9] Les extraits cités ont été traduits de l'anglais au français et les données nominatives issues de ces extraits, incluant les noms des usagers, ont été modifiées afin de réduire les effets néfastes liés à la mise en visibilité des pratiques des personnes étudiées.

[10] Extrait original - « A few years ago I found out the Identity of my Biological father. I have been unsuccessful in tracking him down thus far and I am kind of turning to reddit as a last result. I am 25 years old and would like put the "what if" part of my life behind me and I transition into who I am going to be for the rest of my life. I know that this might be off place but I figured I would give it a shot and at least if nothing came of it then I wasnt any the worse off. The mans name is Robert A. Jefferson (born Robert MacDonald). His adoptive parents were Joe and Iris MacDonald of Milwaukee WI (Bay Side). His sister is Susan Jefferson (remarried and renamed also out of cali), she has three daughters that I guess are my cousins ».

portrait des suspects. D'autres écoutent attentivement la bande audio à la recherche d'indices, comme les prénoms des suspects.

Enfin, les pratiques d'enquêtes observées sont intrinsèquement liées au développement des technologies mobiles mondaines, c'est-à-dire celles dont l'usage premier n'est pas la surveillance, mais qui permettent néanmoins de capter sur le vif un incident, comme le téléphone intelligent. Par exemple, l'usager *colossus* témoigne avoir été victime d'un délit de fuite. Il a toutefois pu capter le véhicule du suspect et offre un lien vers une photo qu'il a prise (vraisemblablement à partir de son téléphone intelligent), permettant du coup la collaboration entre usagers. Les membres du RBI tentent alors d'identifier le modèle et la marque du véhicule du suspect, ainsi que de rendre plus clairs les caractères sur la plaque d'immatriculation (pratique qu'on appelle au sein du RBI *forensics*, soit « criminalistique » en français). Plus tard, les caractères de la plaque d'immatriculation seront entrés dans une base de données afin de voir si elle concorde avec le modèle du véhicule. Cette information sera souvent communiquée aux autorités, car les bases de données jumelant les données véhiculaires et les données nominatives des propriétaires ne sont pas accessibles au grand public. Ces pratiques collaboratives témoignent ainsi du rôle central des technologies numériques et de leur appropriation par les usagers.

Des nouvelles conceptions du rôle du citoyen

Les quatre formes de contribution émergentes que nous avons abordées plus haut soulèvent l'émergence de nouvelles conceptions du rôle du citoyen en matière de gouvernement du crime. Si l'usage d'Internet et des technologies numériques a « le potentiel d'autonomiser les individus et les communautés, ainsi que de redistribuer la balance du pouvoir » selon certains auteurs (Williamson, 2008 : xxiii), d'autres soulignent que leur usage ne ferait que renforcer les inégalités actuelles (Trottier, 2014a). Chose certaine, nous estimons que le développement des technologies numériques et d'Internet est intrinsèquement lié à une renégociation des frontières traditionnellement érigées entre les travailleurs de la sécurité formellement mandatés et leurs publics. Notre observation exploratoire a permis de soulever que, dans l'ensemble, les usagers du RBI ne semblent pas remettre en question la légitimité ou l'importance de la police publique en tant qu'institution. En effet, un signalement à la police a été mentionné ou suggéré

dans 40 des 66 crimes recensés. Qui plus est, les critiques jugées gratuites ou destructrices envers la police ne semblent pas y être tolérées :

Extrait 2 – L'importance du travail policier professionnel

[-] **Pittsjoe** 5 points 20 jours de ça

> nous avons au fond utilisé la police comme messagers pour récupérer notre matériel

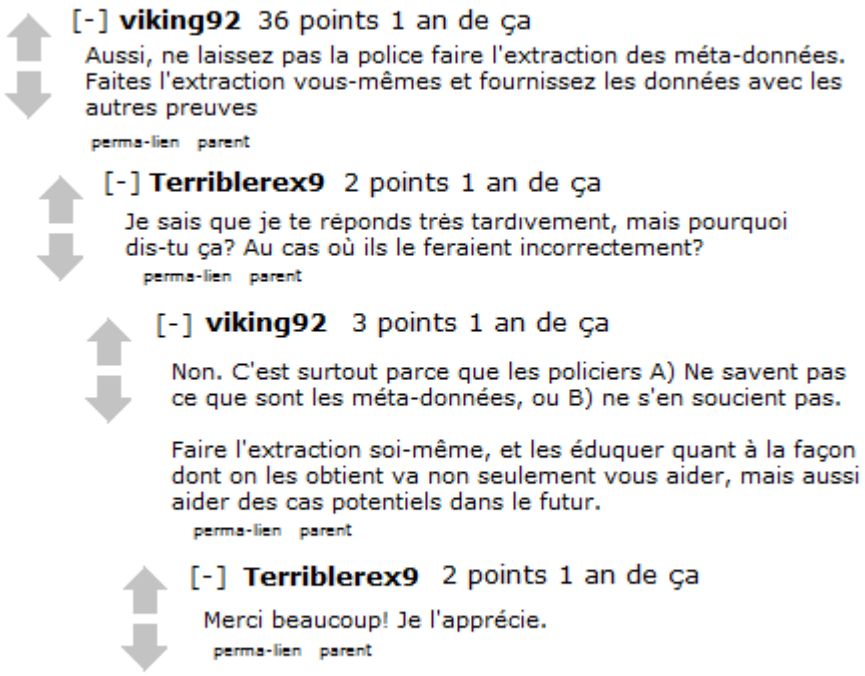
Je crois que tu sous-estimes leur implication. Ce n'est vraiment pas très difficile de localiser l'emplacement d'un ordinateur si les voleurs sont trop stupides pour effacer les données de l'équipement. Mais frapper à leur porte et leur demander de le rendre pourrait résulter par SE FAIRE POINGARDER DANS LE PUTAIN DE VISAGE ou autre saleté du genre. Ils ont été un peu plus instrumentaux que des "messagers".

perma-lien **parent**

L'extrait 2 est tiré du fil *J'ai entendu que ce forum aimerait savoir comment mon ami a retrouvé son ordinateur portable volé, certainement pas grâce à la police*[11]. Plutôt que de s'enquérir de la stratégie utilisée par l'ami du créateur du fil de discussion, les usagers du RBI ont ouvertement critiqué la manière dont l'usager avait formulé le titre de son fil. À cet effet, l'usager *Pittsjoe* souligne que si le créateur du fil et son ami avaient effectivement réussi à trouver l'emplacement des suspects, les policiers avaient été plus qu'instrumentaux, risquant leur vie en allant confronter les suspects à leur domicile. Le créateur de ce fil a même dû éditer sa demande d'aide originale afin d'inclure un *mea culpa*, avouant que la formulation « certainement pas grâce à la police » était « un peu incorrecte », dans la mesure où la victime n'avait pas contacté les policiers en premier lieu afin de recourir à leurs services. Cela dit, les demandes d'aide observées au sein du RBI, notamment celles référant à un cas criminel, reposent parfois sur des conceptions collectivement négatives ou critiques de la police. Souvent, l'usager demande l'aide du RBI parce qu'il doute de la disponibilité ou de la fiabilité des policiers. Par exemple, l'usager *CGIfree* soutient que c'est à la victime de faire le tour des prêteurs sur gages afin de retrouver des objets volés, car la police affirmera « qu'elle le fera, mais… ». Ces points de suspension laissent présager la croyance voulant que les citoyens seraient parfois laissés à eux-mêmes. Autre exemple, l'usager *goodfellow* soutient qu'il ne sait pas quoi faire afin de retrouver l'identité de la personne ayant volé ses cartes bancaires et hésite à communiquer avec les policiers, puisque ces derniers considéreraient sans doute qu'un vol de 700$ ne représente pas, pour eux, « un enjeu si important », le laissant « exaspéré ».

[11] Extrait original – Créateur du fil : « basically had to use the police as the messenger to get the property back ». Pittsjoe : « I think that you're understating their involvement. It's really not too tricky to trace the location of computer if the thieves are too dumb to wipe the equipment. However, knocking on the door and asking for it back could result in GETTING STABBED IN THE FUCKING FACE or other nastiness. They were a bit more instrumental than "messengers" ».

Extrait 3 – Nouvelle conception du rôle du citoyen



Enfin, le RBI constitue également un excellent terrain afin de relever la façon dont les citoyens conçoivent leur propre rôle dans la résolution d'enquêtes criminelles. Dans l'extrait 3, *viking92* invite les usagers du RBI à extraire eux-mêmes les métadonnées (date, heure, lieu, etc.) associées à chaque photo et à inclure explicitement ces données à l'ensemble des preuves accumulées[12]. Lorsque

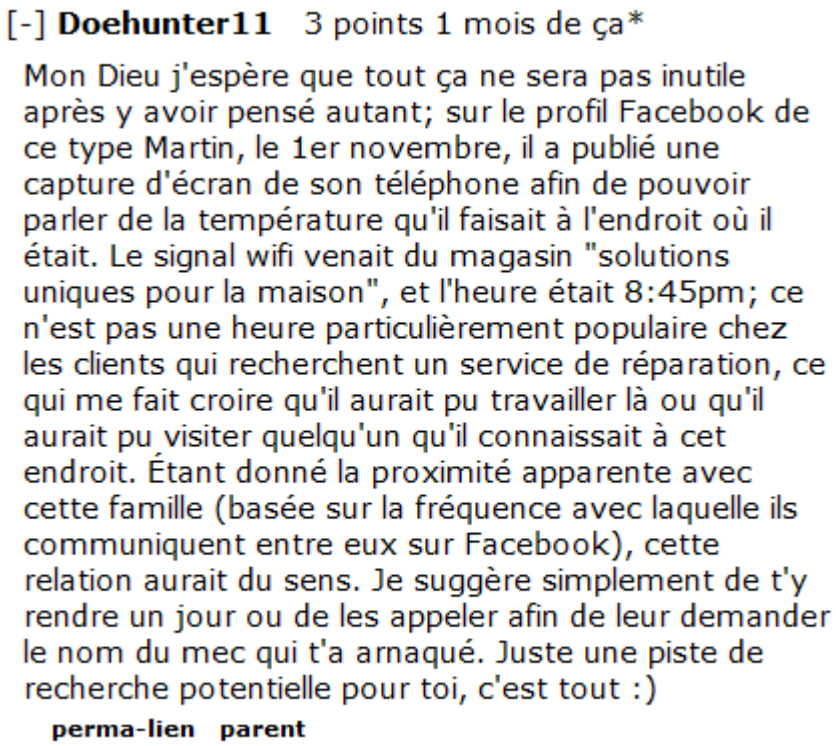
[12] Extrait original - viking92 : « Also, don't leave it to the cops to extract metadata. Extract it yourself and provide it with other evidence ». Terriblerex9 : « I know this is a really late reply but

l'usager *Terriblerex9* interroge *viking92* quant aux raisons expliquant le fait qu'il ne faille pas laisser les policiers s'acquitter de ce type de tâche, ce dernier indique que les policiers ne connaissent pas ou ne se soucient pas des métadonnées et le fait de les extraire soi-même pourrait éduquer des derniers et aider d'autres victimes. Cet extrait souligne l'existence d'une conception du policier professionnel comme étant quelqu'un qui possède des compétences informatiques inférieures à celles de certaines victimes. Il reviendrait donc aux citoyens de répondre à ce besoin de formation. Au-delà des objectifs primaires de résolution d'enquêtes criminelles, certains usagers semblent être sensibles à l'importance de « traduire » les résultats de leurs enquêtes afin qu'ils puissent être intégrés aux démarches menées par les policiers professionnels. Les propos tenus par *viking92* témoignent d'une conception s'éloignant de l'utilitarisme caractérisant la relation traditionnelle entre les policiers et les citoyens, au sein de laquelle ces derniers jouent un rôle exclusif de ressources (délateurs, témoins, etc.). Pour conclure, il importe de souligner que certaines pratiques, quoique rarement observées au sein du RBI, se rapprochent d'un travail de surveillance reposant sur un travail soutenu d'observation en ligne à proprement parlé. Le cas de *t-reader* se disant victime de la fraude d'un travailleur de la construction constitue un exemple clair de surveillance effectuée grâce aux réseaux socionumériques. Dans ce cas-ci, le travailleur en question aurait utilisé la mort de sa belle-mère afin de justifier l'arrêt des travaux en cours alors que les paiements lui avaient déjà été versés. Toutefois, en observant de plus près le profil *Facebook* du travailleur, *t-reader* apprend que la femme en question est toujours active sur le réseau socionumérique. Ce cas fera alors l'objet d'un travail plus méticuleux de surveillance en ligne par un second usager :

---

why is that? Encase they do it incorrectly? ». viking92 : « No. It's mostly because cops either A) Don't know about Metadata, or B) don't care about it. Extracting it yourself, and educating them on how to obtain it will not only help you, but potentially future cases as well ». Terriblerex9 : « Thanks very much! I appreciate it ».

Extrait 4 - La rhétorique de la surveillance



[-] **Doehunter11** 3 points 1 mois de ça*

Mon Dieu j'espère que tout ça ne sera pas inutile après y avoir pensé autant; sur le profil Facebook de ce type Martin, le 1er novembre, il a publié une capture d'écran de son téléphone afin de pouvoir parler de la température qu'il faisait à l'endroit où il était. Le signal wifi venait du magasin "solutions uniques pour la maison", et l'heure était 8:45pm; ce n'est pas une heure particulièrement populaire chez les clients qui recherchent un service de réparation, ce qui me fait croire qu'il aurait pu travailler là ou qu'il aurait pu visiter quelqu'un qu'il connaissait à cet endroit. Étant donné la proximité apparente avec cette famille (basée sur la fréquence avec laquelle ils communiquent entre eux sur Facebook), cette relation aurait du sens. Je suggère simplement de t'y rendre un jour ou de les appeler afin de leur demander le nom du mec qui t'a arnaqué. Juste une piste de recherche potentielle pour toi, c'est tout :)

perma-lien parent

Dans l'extrait 4, *Doehunter11* offre un compte-rendu détaillé des activités du suspect afin d'aider à le localiser, notamment en identifiant un commerce qu'il semble souvent fréquenter[13]. Ce type de pratique, même s'il repose sur l'usage de

[13] Extrait original - « God I hope this doesn't turn out to be meaningless after I've been thinking about it so much; on that dude Martins' FB page, on November 1st, he posted a screenshot from his phone so that he could talk about the weather where he was. The wifi signal was coming from 'unique home solutions', and the time was 8:45pm; that isn't exactly prime time for customers

données accessibles publiquement, génère certainement des enjeux liés à la vie privée, ainsi qu'à la sécurité des individus, qu'ils soient victimes ou suspects (voir Trottier, 2014b). Outre ces enjeux, et ce, face à l'importance croissante que les pratiques de surveillance occupent dans le quotidien des individus, ce cas introduit l'idée d'une *littératie* en matière de surveillance qui rendrait compte de la capacité des individus à mobiliser de manière critique les différentes informations publiquement accessibles en ligne et à les interpréter correctement (dans un contexte d'enquête criminelle ou autre). Qui plus est, la publication de *Doehunter11* amène également à réfléchir l'existence d'une certaine *rhétorique de la surveillance*, dans la mesure où le résultat de ce travail d'observation en ligne semble être mobilisé comme argument rhétorique afin de faire valoir une hypothèse ou une réflexion permettant ultimement l'acquisition d'un certain capital (social, symbolique et éventuellement financier) d'investigation. Ainsi, le cas du RBI permet d'observer l'émergence de nouveaux rôles citoyens en matière de gouvernement du crime.

La construction d'une identité commune

L'observation des pratiques menées par les membres du RBI a permis de constater que celles-ci avaient peu en commun avec les caractéristiques du *vigilante*, mettant plutôt l'accent mis sur l'usage de la force, sur une logique de vengeance et/ou de honte, ainsi que sur la volonté de se faire justice soi-même. Dans le corpus étudié, l'usage de la force est absent, voire même découragé. Par exemple, un usager demande conseil après s'être fait voler ses effets personnels par un groupe de déménageurs. L'usager *Twenty-nation* conseille à la victime de faire appel à un détective privé qui aura une meilleure connaissance des réseaux criminels de la ville de Seattle (là où a eu lieu le vol en question) et d'effectuer une veille des

looking for repair work done, making me think that he could have been working there or visiting someone he knew would be there. Given the apparent closeness of this family (based on how often they communicate with eachother on Facebook), this connection would make sense. I would simply suggest going in some day or calling them to ask about the name of the guy that ripped you off. Just a potential line of inquiry for you, that's all :) ».

sites de petites annonces *Craiglist* et *Ebay* afin de retrouver les objets volés. Dans l'éventualité où la victime retrouverait les suspects, *Twenty-nation* conseille à la victime de contacter immédiatement la police et d'éviter toute confrontation directe avec le suspect. Ce type de conseil est fréquemment observé au sein du RBI, témoignant d'une répartition des tâches entre les policiers et les citoyens où toute confrontation directe et, conséquemment, tout usage de violence ou désir de se faire justice soi-même sont explicitement proscrits. Par ailleurs, les pratiques observées au sein du RBI ne semblent pas reposer sur une logique de vengeance, bien au contraire.

Dans l'extrait 5, l'usager *Revychevy* se dit victime d'un délit de fuite. Ayant réussi à prendre en note la plaque d'immatriculation du véhicule, il demande l'aide du RBI afin de trouver l'identité du coupable[14]. Toutefois, ce dernier indique dans son appel à l'aide qu'il n'a pas l'intention de faire un signalement à la police. Ceci rend les membres du RBI suspicieux, comme en témoigne l'intervention de *razorerazor* (à gauche) qui lui demande la raison expliquant sa décision de ne pas signaler cet incident à la police. *Revychevy* répond alors que ses documents d'immatriculation ne sont pas en ordre et assure qu'il « ne veut pas se venger ou quoi que ce soit ». S'en suit une série de publications remettant en question les motivations de *Revychevy*. Le membre *entonces693* (à droite) affirme que le RBI ne tolère pas les justiciers et demande explicitement ce qu'il fera de l'information qu'on pourrait lui fournir. De son côté, *LIFEcomm* accuse le créateur du fil d'être un personnage « louche » et somme les « agents du RBI » de ne pas aider cet homme, car il est « soit un criminel ou quelqu'un qui désire se venger ». En fait, une seule mention de *shaming*, stratégie souvent employée par les justiciers en ligne dont l'objectif est de provoquer la honte pour punir une transgression normative (Wall et Willams, 2007), a été observée dans le corpus à l'étude. Dans le cas en question, le membre *tamer1234* demande l'aide du RBI, car il doute de

[14] Extrait original - razorerazor : « Why don't you want to report it to the police? ». Revychevy : « Im not going to gwt revenge or anything. Id like to talk it over. Because i havent renewed my registration yet. Overdue two months ». entonces693 : « You don't. You report it to the police. And we don't support vigilantism in this sub. What could you possibly want to do with this information? ». Lifecomm : « you sound like a shady fuck. RBI agents, do not assist this man. He's either a criminal or out to get someone ».

Extrait 5 - Une logique anti-vengeance (1)

[-] **razorerazor** 18 points 1 mois de ça

Pourquoi ne le signales-tu pas à la police?

perma-lien

[-] **Revychevy** [S] 7 points 1 mois de ça

Je ne cherche pas à me venger ou quoi que ce soit. J'aimerais pouvoir lui en parler. Parce que je n'ai pas renouvellé mes documents d'immatriculation. En retard de deux mois.

perma-lien

[-] **entonces693** 4 points 1 mois de ça

Tu ne fais pas ça. Tu le signales à la police. Et on ne tolère pas les justiciers dans ce sous forum. Que pourrais-tu possiblement faire de cette information?

perma-lien

[-] **Lifecomm** 3 points 24 jours de ça

tu as l'air louche, enfoiré. Agents du RBI, n'aidez pas cet homme. Il est soit un criminel ou quelqu'un qui veut se venger.

perma-lien

Extrait 6 - Une logique anti-vengeance (2)

[-] **hdnumbers** 1 point 1 mois de ça

Avant de faire quelque chose de dramatique, considère cette option:

> "Chère <personne-folle-qui-ment>, stp ne me contacte plus. J'en ai assez de tes mensonges inutiles. Ton dernier à propos de ta supposée fausse couche était particulièrement de mauvais goût. J'ai mené une recherche en ligne et j'ai découvert que la photo que tu m'as envoyée est en réalité une capture d'écran de cette vidéo : <lien>. Merci, tamer1234.

Ensuite, retire-la de tes amis Facebook, appelle ton avocat et va au gym.

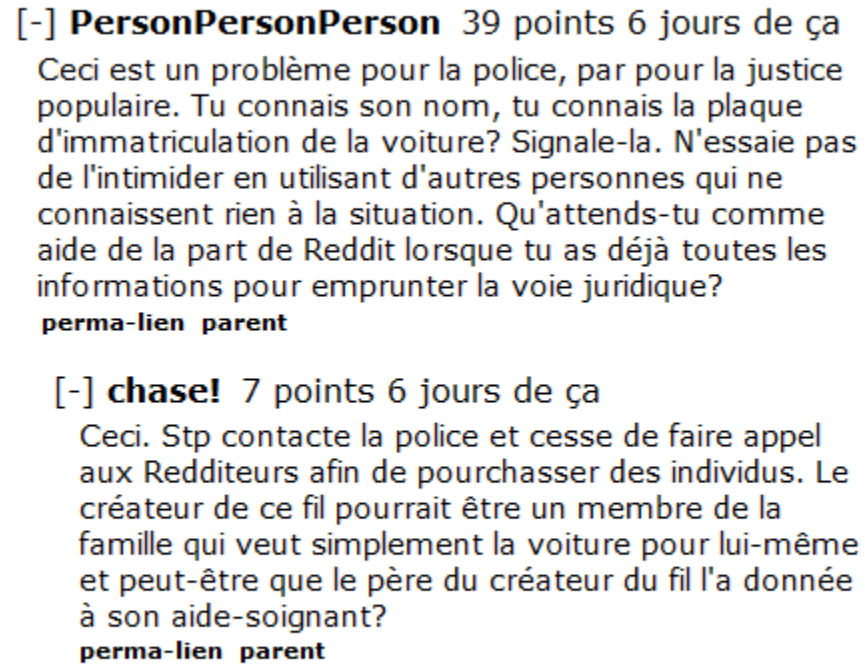
perma-lien

la véracité d'une échographie publiée par une amie sur Facebook. Les membres réussiront rapidement à trouver la vidéo originale en utilisant la fonction de recherche par image du moteur de recherche *Google*, prouvant ainsi que la vidéo n'appartenait effectivement pas à la jeune femme en question. Suite à ce constat, l'usager *TohmA* suggère au créateur du fil de publier la vidéo originale sur le profil Facebook de la jeune femme afin de lui faire perdre face publiquement.

Toutefois, comme témoigne l'extrait 6, l'usager *hdnumbers* propose une stratégie alternative moins « dramatique », soit celle d'un *mail* adressé à la jeune femme afin de mettre en lumière la supercherie et de la sommer de ne plus contacter l'auteur du fil, répondant ainsi à la stratégie initiale de *shaming* proposée par *TohmA*[15]. Si les activités menées au sein du RBI ne correspondent pas aux caractéristiques du *vigilante*, cette figure est apparue néanmoins très importante. En effet, le *vigilante* semble être fréquemment mobilisé par les membres du RBI comme argument rhétorique négatif à des fins de construction identitaire. Si la devise « pas de chasse aux sorcières » est clairement épinglée à la page d'accueil du RBI, celle-ci transcende également les activités observées. À titre d'exemple, *beatriceX* croit avoir identifié sur Facebook une photo dépeignant une scène de pédophilie. Elle demande l'aide du RBI, même si elle avoue que l'équipe de Facebook a déjà conclu n'avoir rien trouvé d'anormal à la photo. De nombreux membres remettent alors en question le bien-fondé de cette demande apparaissant comme non justifiée. *Bread.mr01* somme alors *beatriceX* d'éviter les chasses aux sorcières (*witch hunts*) et de ne pas « ruiner la réputation de quelqu'un parce que tu n'as pas suffisamment d'informations ». Outre la devise *no witch hunt*, les membres du RBI semblent aussi partager l'idée que le RBI n'est pas une armée personnelle (*not your personal army*) :

[15] Extrait original - « Before you decide to do anything dramatic, consider this option: "Dear <lyingcrazyperson>, please do not contact me anymore. I have had enough of your unnecessary lies. Your latest one about having a miscarriage was especially in poor taste. I did some research online, and I found that the picture you sent to me is actually a screen capture from this video: <link>. Thank you, tamer1234." Then defriend her from facebook, lawyer up, hit the gym ».

Extrait 7 - L'interdiction du gain personnel


[-] **PersonPersonPerson** 39 points 6 jours de ça

Ceci est un problème pour la police, par pour la justice populaire. Tu connais son nom, tu connais la plaque d'immatriculation de la voiture? Signale-la. N'essaie pas de l'intimider en utilisant d'autres personnes qui ne connaissent rien à la situation. Qu'attends-tu comme aide de la part de Reddit lorsque tu as déjà toutes les informations pour emprunter la voie juridique?

perma-lien parent

[-] **chase!** 7 points 6 jours de ça

Ceci. Stp contacte la police et cesse de faire appel aux Redditeurs afin de pourchasser des individus. Le créateur de ce fil pourrait être un membre de la famille qui veut simplement la voiture pour lui-même et peut-être que le père du créateur du fil l'a donnée à son aide-soignant?

perma-lien parent

Comme en témoigne l'extrait 7, qui concerne un cas de vol de voiture, les membres *PersonPersonPerson* et *chase!* soulignent l'importance de ne pas utiliser Reddit afin de « pourchasser des individus » ou à des fins d'intimidation[16].

[16] Extrait original - PersonPersonPerson : « This is an issue for police not mob justice. You know her name, you know the license plate of the car? Report them. Do not attempt to bully her through other people who do not know the situation. What do you expect reddit to help with when you already have enough information to follow legal avenues ». chase! : « This. Please contact the police

En ce sens, la construction identitaire du RBI et de ses membres semble se faire en réaction à la logique de justice populaire (*mob justice*) dépeinte dans cet extrait. Ainsi, si les *online vigilantes* patrouillent le Web à la recherche de transgression normative à punir (Klang, 2015), les usagers du RBI semblent beaucoup plus sensibles à la transgression normative de leurs propres membres.

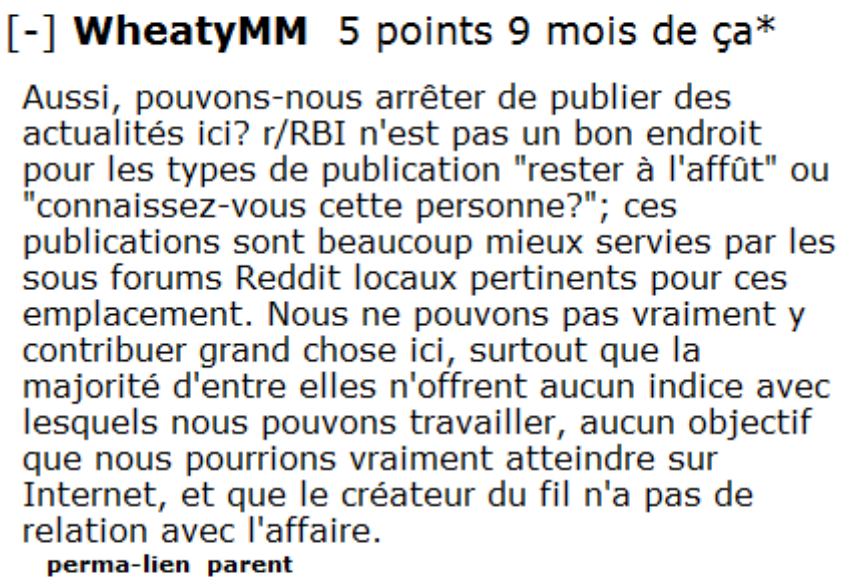
La mise en œuvre d'une expertise profane

La participation au RBI exige de ses membres le déploiement de diverses formes d'expertise profane. Dans l'un des rares fils de discussion n'empruntant pas la forme d'une demande d'aide, au sein duquel l'usager *someproblem* demande aux membres du sous-forum comment et pourquoi ces derniers mènent leurs activités, trois formes d'expertise sont dégagées : 1) *Harry01* dit avoir bénéficié d'une formation en investigation informatique dans le cadre de son travail; 2) *story_timing* soutient être un artiste graphique du domaine de la sécurité publique ayant développé une expertise dans le travail d'image (notamment avec le logiciel *Photoshop*); et 3) *Heliumite* mentionne avoir suivi des cours en recherche de bases de données ouvertes afin de se spécialiser dans la recherche d'individus. Ainsi, la possibilité de faire bénéficier de leur expertise (notamment technique ou processuelle) aux victimes de crimes ou de détenteurs d'énigmes à résoudre semble animer les membres du RBI.

---

and stop looking for redditors to hunt the person down. Op could be a greedy relative who just wants the cars for himself and maybe Op's dad gave it to the caretaker? ».

Extrait 8 - La visée du RBI


[-] **WheatyMM** 5 points 9 mois de ça*

Aussi, pouvons-nous arrêter de publier des actualités ici? r/RBI n'est pas un bon endroit pour les types de publication "rester à l'affût" ou "connaissez-vous cette personne?"; ces publications sont beaucoup mieux servies par les sous forums Reddit locaux pertinents pour ces emplacement. Nous ne pouvons pas vraiment y contribuer grand chose ici, surtout que la majorité d'entre elles n'offrent aucun indice avec lesquels nous pouvons travailler, aucun objectif que nous pourrions vraiment atteindre sur Internet, et que le créateur du fil n'a pas de relation avec l'affaire.

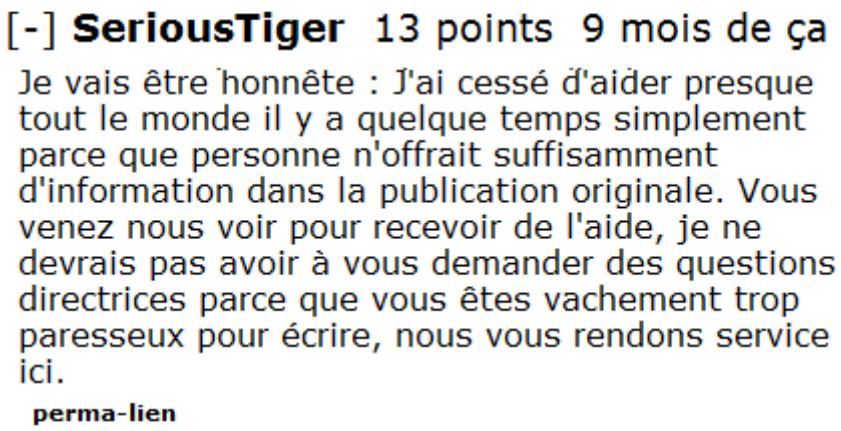
perma-lien parent

Dans l'extrait 8, tiré du fil *Aidez-nous à vous aider! Lisez ce post avant de commencer le vôtre*, l'usager *WheatyMM* somme les usagers du RBI de cesser de créer de fils concernant des cas criminels issus d'articles de journaux (par exemple, des histoires de meurtre ou d'agression dont la victime est rarement connue de celui ou celle qui a créé du fil) et de fils dont l'objectif est de « rester à l'affut » (faisant vraisemblablement référence à la recherche de suspects par la

police)[17]. *WheatyMM* semble privilégier les cas nécessitant une forme d'intervention de la part des membres du RBI et, de surcroît, qui offrent des indices avec lesquels travailler. Ainsi, dans le cadre de notre observation exploratoire, la nature des cas s'est révélée être un indicateur de moindre importance pour la contribution, confirmant l'impression que les activités menées au sein du RBI suivent une logique qui diffère de celle du *vigilante*, traditionnellement motivé par la volonté de réparer une injustice commise ou perçue. En fait, les usagers semblent avoir plus tendance à venir en aide si le créateur du fil est lui-même la victime du crime commis (ou son représentant direct) et s'il offre du matériel propice à un travail interprétatif ou analytique. Dans un fil étudié, l'usager *seabrz* remercie les autres membres pour leur aide et indique avoir « donné toutes les interprétations au Département de police de Seattle », laissant présager que les pratiques menées par les usagers du RBI sont conçues comme des pistes potentielles à fournir aux policiers (tout comme dans l'extrait 4). Il importera de suivre l'évolution des regroupements spontanés de citoyens qui collaborent en ligne afin de résoudre des crimes au cours des prochaines années, notamment afin de noter si les processus mis en place par ceux-ci réussiront à atteindre un niveau suffisamment élevé de formalisation afin d'assurer leur pérennité. Cela pourrait s'avérer difficile, car l'usage de la plateforme *Reddit* amène son lot de problèmes, notamment liés au fait que cette dernière n'a pas été créée dans le but spécifique de mener des enquêtes, mais plutôt d'échanger sur des sujets d'actualités divers. Autrement dit, il faudra voir si les usagers sauront réconcilier le mode conversationnel inscrit à même le « script » du dispositif *Reddit* et le mode de production sur lequel semble reposer une grande partie des pratiques observées. Ces tensions se font déjà sentir, comme en témoigne l'extrait 9 :

[17] Extrait original - « Also, can we stop posting news stories in here? /r/RBI is not a good place for "be on the lookout" or "do you know this person?" type posts; those are much better served by the relevant local subreddits for those locations. We really can't do anything with those here, especially when most of them have no clues for us to work with, no goal that we could actually achieve over the Internet, and the OP has no relation to the case ».

Extrait 9 - Les inconvénients de la plateformes *Reddit*



Dans cet extrait, l'usager *SeriousTiger* affirme avoir cessé de contribuer au RBI, puisque les usagers ne respectent pas les normes de contribution comme la divulgation d'informations complètes et claires[18]. Ce non-respect pourrait notamment être dû au renouvellement constant du *membership* et du grand

[18] Extrait original - « I'll be honest: I stopped helping almost everyone a while back simply because practically nobody puts enough information in the original post. You are coming to us for help, I shouldn't have to ask leading questions because you are too fucking lazy to type them out, we are doing you a favor here ».

nombre de membres. Qui plus est, une tension est aussi observable entre le règlement de *Reddit* interdisant la publication d'informations personnelles qui rend la recherche de suspects plus ardue dans le cadre d'un sous-forum dont l'objectif est la résolution d'enquêtes criminelles. Cette tension est particulièrement accentuée par le caractère visible et public des activités du sous-forum qui s'oppose au caractère secret et privé des enquêtes criminelles traditionnelles. Ce constat souligne par ailleurs le principal biais de notre démarche méthodologique qui repose exclusivement sur l'observation de traces en ligne. En effet, il est fort probable que les usagers du RBI s'adonnent à des pratiques invisibles (par exemple, des échanges par messagerie privée ou des activités menées hors ligne) n'étant accessibles que par observation participante ou par entretien. Cela dit, il sera intéressant de voir si la plateforme *Reddit* sera jugée suffisamment souple par les membres du RBI afin de continuer leurs pratiques de résolution d'enquêtes ou, plutôt, si ces derniers ne seront pas tentés de collaborer sur d'autres plateformes, voire d'abandonner simplement ce type de pratique.

CONCLUSION

Comme en témoigne le cas du *Reddit Bureau of Investigation*, le développement d'Internet et des technologies numériques offre de nouvelles potentialités au public afin de contribuer à la résolution d'enquêtes criminelles. Quoique les pratiques observées au sein de RBI en sont encore à un stade embryonnaire, elles suscitent déjà d'importantes réflexions d'ordre conceptuel et éthique, notamment pour le domaine de la sécurité publique. En effet, ces dernières s'ajoutent aux formes de contribution de citoyens en matière de gouvernement du crime déjà documentées, comme le travail de surveillance non institutionnalisée, le *crowdsourced policing*, l'*online vigilante et* la *civilian police*. Ensemble, ces formes de contribution émergentes pointent vers une transformation des conceptions qu'entretiennent les citoyens face à leur propre rôle dans la production de sécurité publique. Quoiqu'à degrés variables, ces citoyens semblent vouloir remettre en question les rôles de « ressource » ou de « contributeur passif » leur étant traditionnellement attribués par l'État et les travailleurs professionnels de la sécurité. Les chercheurs en communication et en criminologie ont tout intérêt à développer conjointement des cadres d'analyse suffisamment souples et compréhensifs afin de rendre compte de l'émergence de nouvelles pratiques citoyennes de sécurité, et ce, qu'elles découlent d'usages inédits de

nouvelles technologies numériques ou d'une transposition sur Internet de techniques d'enquête traditionnelles. Face à ces perturbations, les actions qu'entreprendront les autorités devront également faire l'objet d'études. Ainsi, verront-elles ces changements d'un bon œil ou tenteront-elles plutôt de maintenir leur emprise sur les processus de sécurité, mobilisant pour ce faire des arguments comme l'expertise des travailleurs professionnels ou, encore, les risques associés aux pratiques citoyennes? Il ne fait nul doute que les stratégies employées varieront grandement en fonction des contextes géopolitiques. De leur côté, les chercheurs devront étudier le caractère potentiellement aliénant ou émancipateur de ce type de contribution citoyenne. En effet, les futures recherches auront comme importante tâche d'identifier les contextes au sein desquels les pratiques citoyennes de sécurité participent à la reproduction d'impératifs institutionnels allant à l'encontre de leurs propres intérêts et les contextes au sein desquels les citoyens participent plutôt à un débat public légitime, voire nécessaire, portant sur le rôle contemporain de l'État en matière de gouvernement du crime.

RÉFÉRENCES

ALI, M. A. et S. MANN. (2013), « The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance », in *2013 IEEE International Symposium Technology and Society (ISTAS)*, Toronto, 27 au 29 juin.

AUTEN, J. H. (1981), « Paramilitary Model of Police and Police Professionalism », in *The Police Studies : International Review*, vol. 4, no 2, p. 67-78.

BADARACCO, J. L. et J. V. USEEM. (1997), « The Internet, Intel and the vigilante stakeholder », in *Business Ethics: A European Review*, vol. 6, no 3, p. 18-29.

BAYLEY, D. H. et C. D. SHEARING. (1996), « The future of policing », in *Law & Society Review*, vol. 30, no 3, p. 585-606.

BRABHAM, D. (2013), *Crowdsourcing*, Cambridge, Michigan Institute Press.

BRABHAM, D. (2013b), « The Boston Marathon Bombings, 4Chan's Think Tank, and a Modest Proposal for an Emergency Crowdsourced Investigation Platform », in *Culture Digitally*, 17 avril 2013, [en ligne], <www.culturedigitally.org/2013/04/boston-marathon-bombing-and-emergency-crowdsourced-investigation>, consulté le 5 octobre 2015.

BYRNE, D. N. (2013), « 419 Digilantes and the Frontier of Radical Justice Online », in *Radical History Review*, no 117, p. 70-82.

CHEONG, Pauline Hope et J. GONG. (2010), « Cyber vigilantism, transmedia collective intelligence, and civic participation », *Chinese Journal of Communication*, vol. 3, no 4, p. 471-487.

CHEUNG, A. S. (2009), « China Internet going wild: Cyber-hunting versus privacy protection », in *Computer Law & Security Review*, vol. 25, no 3, p. 275-279.

CHUA, C. E. H. et J. WAREHAM. (2004), « Fighting internet auction fraud: An assessment and proposal », in *Computer*, vol. 37, no 10, p. 31-37.

FOUCAULT, M. (1975), *Surveiller et punir*, naissance de la prison, Paris, Gallimard.

GAO, L. et J. STANYER. (2014), « Hunting corrupt officials online: the human flesh search engine and the search for justice in China », in *Information, Communication & Society*, vol. 17, no 7, p. 814-829.

HAYTHORNTHWAITE, C. (2009), « Crowds and communities: Light and heavyweight models of peer production », in *System Sciences, HICSS'09, 42nd Hawaii International Conference on, IEEE*.

HUEY, L., NHAN, J. et R. BROLL. (2013), « "Uppity civilians" and "cyber-vigilantes" : The role of the general public in policing cyber-crime », in *Criminology and Criminal Justice*, vol. 13, no 1, p. 81-97.

JOHNSTON, L. (1996), « What is vigilantism? », in *British Journal of criminology*, vol. 36, no 2,p. 220-236.

KING, C. S. et al. (1998), *Government is us: Strategies for an anti-government era*, Thousand Oaks, Sage.

KLANG, M. (2015), « On The Internet Nobody Can See Your Cape: The ethics of online vigilantism », *16e conférence annuelle de l'Association of Internet Researchers*, Phoenix, 22 octobre 2015.

LIU, D. (2008), « Human Flesh Search Engine: Is It a Next Generation Search Engine? », in *3rd Communication Policy Research South Conference*, Beijing, China.

LOPEZ, Eliberty. (2012), « Debt Collectors Disguised as Facebook Friends: Solutions to Prevent Violations of the Fair Debt Collection Practices Act on Social Media Platforms », in *Rutgers Law Rev., vol.* 65, p. 923.

LYON, D. et al. (2012), « Introducing surveillance studies », in Lyon, D., Ball, K. et K.D. Haggerty (eds), Handbook of Surveillance Studies, Londres, Routledge, p. 1.

MANN, S. et al. (2002), « Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments », in *Surveillance & Society*, vol. 1, no 3, p. 331-355.

MARX, G. T. (2012), « "Your Papers please": personal and professional encounters with surveillance », in Lyon, D., Ball, K. et K.D. Haggerty (eds), Handbook of Surveillance Studies, Londres, Routledge, p. xx-xxx.

MARX, G. T. (2013), « The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes », in *Security & Privacy, Institute of Electrical and Electronics Engineers*, vol. 11, no 5, p. 56-61.

MEYER, M. (2010), « Copwatching et perception publique de la police. L'intervention policière comme performance sous surveillance »., in *ethnographiques. org*, , no 21.

MYLES, D. (à paraître), « Utiliser les contributions d'internautes pour combattre le crime? Réflexion sur les enjeux conceptuels et éthiques du *crowdsourced policing* », in *Ethica*.

SARFATTI-LARSON, M. (1979), *The Rise of Professionalism: A Sociological Analysis*, Berkeley, University of California Press.

SHARP, D. et al. (2008), « Civilian policing, legitimacy and vigilantism: findings from three case studies in England and Wales », in *Policing & Soc.*, vol. 18, no 3, p. 245-257.

SHEARING, C. et M. MARKS. (2011), « Being a new police in the liquid 21st century », in *Policing*, vol. 5, no 3, p. 210-218.

SMITH, G. J. (2012), « Surveillance work (ers) », in Lyon, D., Ball, K. et K.D. Haggerty (eds), Handbook of Surveillance Studies, Londres, Routledge, p. 107-116.

TROTTIER, D. (2014a), « Vigilantism and Power Users : Police and User-Led Investigations on Social Media », in Trottier, D. et C. Fuchs (eds), Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube, New York, Routledge, p. 209-226.

TROTTIER, D. (2014b), « Crowdsourcing CCTV surveillance on the Internet », in *Information, Communication & Society*, vol. 17, no 5, p. 609-626.

TROTTIER, D. et C. SCHNEIDER. (2012), « The 2011 Vancouver riot and the role of Facebook in crowd-sourced policing ». in *British Columbia Studies : The British Columbian Quarterly*, no 175, p. 57-72.

VANDER ENDE, J. (2014). « Vigilantism », in *The Encyclopedia of Criminology and Criminal Justice*, p. 1-4.

WALL, D. S. et M. WILLIAMS. (2007), « Policing diversity in the digital age Maintaining order in virtual communities », in *Criminology and Criminal Justice*, vol 7, no 4, p. 391-415.

WANG, B. et al. (2009), « Human flesh search model incorporating network expansion and gossip with feedback », in *Proceedings of the 2009 13th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, IEEE Computer Society*.

WILLIAMSON, T. (2008). « Introduction to Handbook », in Williamson, T. (ed), The Handbook of Knowledge Based Policing: Current Conceptions and Future Directions, Hoboken, John Wiley & Sons.

WINTERS, C. P. (2008), « Cultivating a Relationship that Works: Cyber-Vigilantism and the Public Versus Private Inquiry of Cyber-Predator Stings », in *University of Kansas Law Review*, vol. 57, p. 427.
ZEDNER, L. (2006), « Policing Before and After the Police The Historical Antecedents of Contemporary Crime Control », in *British Journal of criminology*, vol. 46, no 1, p. 78-96.