

Université de Montréal

L'utilisation des TIC à des fins de harcèlement criminel en  
situation de violence conjugale : la théorie des opportunités  
et des activités routinières de Cohen et Felson (1978)  
remaniée

Par Annie Bernier

École de criminologie  
Faculté des arts et sciences

Travail-dirigé présenté à la Faculté des études supérieures et postdoctorales en vue de  
l'obtention du grade de Maître ès sciences (M.Sc.) en criminologie,  
option criminalistique et information

Août 2016

© Annie Bernier, 2016

## RÉSUMÉ

Introduite en 1978, la théorie des opportunités et des activités routinières de Cohen et Felson demeure encore aujourd'hui une des plus citées pour expliquer la commission d'actes criminels qui, pour leur part, ne cessent d'évoluer au fil du temps. L'introduction des technologies de l'information et des communications, les TIC, a ainsi contribué à grandement changer le portrait de diverses formes de criminalité traditionnelle, notamment celui du harcèlement criminel. Les TIC sont, entre autres, de plus en plus utilisées dans le cas de violences conjugales pour commettre du harcèlement auprès des victimes, et ce, même lorsque celles-ci vont chercher refuge en maison d'hébergement. Cette nouvelle réalité est dénoncée par les intervenantes et les directrices de maisons d'hébergement qui y voient une véritable menace non seulement pour les femmes, mais aussi pour la maison d'hébergement et pour leurs interventions.

Avec la collaboration de policiers, d'un professeur de l'École des sciences criminelles de Lausanne et d'intervenantes en maison d'hébergement pour femmes victimes de violence conjugale, une collecte des données a été menée afin de préciser comment la théorie des opportunités et des activités routinières de Cohen et Felson peut être adaptée dans les cas de harcèlement criminel par le biais des TIC, en situation de violence conjugale post-séparation, lorsque les femmes sont accueillies en maisons d'hébergement. Le crime ciblé par cette étude, le harcèlement criminel, est d'abord explicité à partir du point de vue légal, puis à partir de la compréhension qu'en ont les policiers et les intervenantes en maison d'hébergement, afin d'en connaître les particularités.

Dans le cadre de cette étude, le délinquant motivé s'avère être le conjoint cherchant à contrôler sa victime en utilisant diverses technologies pour l'épier et la harceler même si elle a quitté le domicile familial et la situation de violence conjugale, pour se réfugier en maison d'hébergement. La cible attrayante se trouve alors être la conjointe rendue vulnérable par l'état émotionnel dans lequel elle est plongée par les agissements du conjoint. Les maisons d'hébergement pour femmes victimes de violence conjugale ainsi que l'enquête policière sont vues comme pouvant jouer un rôle de gardien efficace dans une telle situation. En effet, les femmes en maison d'hébergement se voient offrir la possibilité de se couper de toutes formes de technologies leur appartenant susceptibles de les mettre en danger. À l'inverse, bien utilisées, les TIC peuvent s'avérer une source de données riches en informations permettant de « mettre en boîte » l'agresseur, en utilisant les traces numériques que laisse l'utilisation des TIC pour constituer la preuve du délit.

Ainsi se trouve revisitée la théorie de Cohen et Felson à l'ère des TIC et se célèbre la rencontre entre criminologie et criminalistique.

Mots-clés : théorie des opportunités et des activités routinières, harcèlement criminel, violence conjugale, traces numériques, technologies de l'information et des communications (TIC)

## ABSTRACT

Introduced in 1978, the lifestyle and routine activities theory of Cohen and Felson remains one of the most cited theory to explain criminal activities. The use of information and communication technologies (ICT) has transformed traditional forms of crime, such as criminal stalking and harassment. The ICT are often used in domestic violence cases to harass and stalk the victim, even when she is seeking security in shelters. This problematic was brought to our attention by shelter workers, who consider those technologies an actual threat for women and their children, but also for the shelter and the interventions.

With the collaboration of police investigators, a professor from the École des sciences criminelles de Lausanne and shelter workers, data were collected through interviews then analyzed, in order to adapt the Cohen and Felson's lifestyle and routine activities theory in cases of ICT use for stalking, in intimate partner violence relationships. The crime targeted by this study, criminal stalking and harassment committed through ICT, is developed according to the Criminal Code but also according to the police officer and the shelter workers, to understand its particularities.

In this study, the motivated offender is the partner controlling his wife using various devices to track and harass her, even when she quit the violent situation to seek security in a shelter. In this case, her unstable emotional state and the fact that her partner knows her well make the present or former wife vulnerable and, therefore, a suitable target. Also, the emotional context surrounding the domestic violence situation can destabilize her when she receives text messages or e-mails from her partner, trying to convince her to come back. Finally, shelters and the police investigation are there seen as a capable guardian. In fact, women in shelters have the possibility to turn off their technology in a secure environment where they can get the support they need. Even if the ICT can, in one hand, impede the intervention, it can also be a rich source of information, on the other hand. Indeed, when a police investigation takes place, this digital information can be used as evidence in criminal court to prove the stalking.

Thereby, Cohen and Felson's theory of opportunities and routine activity is revisited in the ICT era and put forward the meeting of criminological and forensic science.

Keywords: lifestyle and routine activities theory, Cyberstalking, intimate partner violence, digital forensic, Information and communication technologies (ICT)

# TABLE DES MATIÈRES

RÉSUMÉ.....	ii
ABSTRACT .....	iii
TABLE DES MATIÈRES.....	iv
REMERCIEMENTS .....	vi
INTRODUCTION.....	1
CHAPITRE 1 : RECENSION D'ÉCRITS : Violence conjugale et nouvelles technologies, une rencontre explosive ! .....	3
1.1 Quelques mots sur la violence conjugale.....	3
1.2 Le harcèlement en contexte de violence conjugale.....	5
1.3 Cyberharcèlement / harcèlement via les technologies de l'information et de la communication.....	8
1.4 Les technologies de l'information et de la communication (TIC) : une évolution fulgurante .....	12
1.4.1 Les appareils téléphoniques au service du cyberharcèlement.....	13
1.4.2 Ordinateurs et Internet : des transmetteurs d'information .....	15
1.4.3 Les dispositifs de repérage par géolocalisation (GPS).....	17
1.4.4 La surveillance par caméra .....	18
1.5 La théorie des opportunités et activités routinières à l'heure des TIC .....	18
1.6 La problématique .....	22
CHAPITRE 2 : MÉTHODOLOGIE .....	24
2.1 Une approche qualitative .....	24
2.2 La collecte de données .....	25
2.3 Une analyse de contenu à visée descriptive .....	27
2.4 Considérations éthiques .....	29
2.5 Forces et limites de la démarche .....	29

CHAPITRE 3 : RÉSULTATS.....	32
3.1 Le harcèlement criminel : entre la prescription de la loi et la perception des intervenants .....	32
3.2 La difficulté de faire la preuve du harcèlement par les TIC .....	35
3.3 Les TIC au service du délinquant motivé .....	38
3.4 La conjointe « rebelle » : une cible attrayante .....	41
3.5 L'intervention d'un gardien efficace .....	43
3.5.1 Les maisons d'hébergement.....	43
3.5.2 L'enquête policière et la constitution de la preuve .....	46
3.5.3 Une preuve volatile.....	48
3.5.4 Ordinateurs et Internet : une source de données en or .....	50
3.5.5 Les données téléphoniques : un outil de surveillance et de corroboration.....	53
 CHAPITRE 4 : DISCUSSION.....	 57
4.1 Comment les suspects, en connaissant les activités routinières de la victime peuvent-ils utiliser les nouvelles technologies pour la harceler ?.....	58
4.2 Comment l'accumulation des traces numériques témoignant des activités routinières des victimes et des suspects peut-elle servir l'enquête policière.....	60
 CHAPITRE 5 : L'INTÉGRATION DES SAVOIRS CRIMINOLOGIQUE ET CRIMINALISTIQUE .....	 65
 CONCLUSION .....	 65
 BIBLIOGRAPHIE .....	 67
 ANNEXE 1 : Formulaire de consentement.....	 xiii
ANNEXE 2 : Certificat d'éthique.....	xix
ANNEXE 3 : Grilles d'entrevue .....	xx

## REMERCIEMENTS

*J'aimerais tout d'abord remercier ma directrice de recherche, Marie-Marthe Cousineau, de m'avoir soutenue dans tout ce processus de recherche. Malgré les appréhensions que tu pouvais avoir quant au mariage entre la criminalistique et la violence conjugale, je crois que nous avons réussi à faire un projet qui correspond aux besoins du milieu. Je suis très fière d'avoir pu participer à faire avancer la recherche dans ce domaine.*

*J'aimerais également remercier Trajetvi pour m'avoir permis de participer à des conférences et colloques scientifiques m'amenant à connaître une communauté scientifique et communautaire tissée serrée et qui travaille vers un but commun : aider les femmes victimes de violences conjugales.*

*Merci au Regroupement des maisons d'hébergement pour femmes victimes de violence conjugale d'avoir tout mis en place pour que la réalisation d'entrevues avec des intervenantes de vos maisons-membres soit possible. Votre collaboration est très appréciée !*

*Un énorme merci à tous les policiers qui ont pris le temps de me rencontrer, sans qui ce projet n'aurait jamais vu le jour. Merci à Claude Roy et Sylvie Montreuil de la Police de la ville de Québec ; merci à Christian Dumas de la Sûreté du Québec et merci à Normand Borduas du Service de Police de la Ville de Montréal.*

*Merci à David-Olivier Jaquet-Chiffelle, professeur à l'Université de Lausanne, d'avoir participé à mon étude.*

*J'aimerais également remercier l'Université de Montréal ainsi que l'Université de Lausanne pour la réalisation de cette maîtrise.*

*Finalement, merci à ma famille de m'avoir soutenue durant ma maîtrise. Je crois que le fait d'être dernière minute et pas très organisée vous a fait stresser plus que moi ! Une chance que vous étiez là pour me rappeler que la date limite arrivait vite et que je devrais commencer à m'y mettre sérieusement ! Au final, j'ai quand même fait à ma tête et terminé la moitié de ce travail dirigé qu'il me restait dans les deux derniers mois !*

*Merci Sab de m'avoir fait paraître à mon affaire et normale dans l'échéancier que je ne suivais pas ! Je ne sais pas encore si le fait d'essayer d'avancer nos travaux dirigés ensemble était si bénéfique, souvent parler semblait plus intéressant ! Peu importe, nous avons déposé... dans les délais!*

=

## INTRODUCTION

Grâce à l'émergence du mouvement féministe des années 1960, la violence conjugale est passée du statut de problématique privée à celui de problème social public. Autrefois, on traitait la violence conjugale au sein de la cellule familiale et intime. Les femmes victimes de violence conjugale n'avaient aucun recours ni aucun moyen de se mettre en sécurité. Les féministes ont mis en place des refuges pour accueillir les femmes victimes, dénonçant ainsi la violence subie par celles-ci.

Les maisons d'hébergement permettent désormais à un nombre important de femmes de quitter la situation de violence, d'isolement et de culpabilité. Les féministes intervenant dans les maisons d'hébergement tentent d'offrir des solutions concrètes aux femmes, leur permettant d'éviter les situations dangereuses pour elles (Lamoureux, 1992; Côté, 2017).

Par ailleurs, la violence vécue par les femmes en contexte conjugal ne cesse de se diversifier en fonction des époques, de telle sorte qu'elles peuvent désormais être harcelées et menacées via les technologies de l'information et des communications, les TIC, suivant en cela le développement de celles-ci. Or, tous les mouvements faits sur un dispositif numérique laissent des traces et celles-ci peuvent être utilisées pour la constitution de la preuve de harcèlement lorsque les TIC ont été utilisées pour perpétrer la violence à distance. Ceci étant, les TIC interviennent en violence conjugale pour le pire, comme instrument permettant le harcèlement et la géolocalisation des femmes par le conjoint violent, et pour le meilleur comme instrument de constitution de la preuve de harcèlement criminel et pour la géolocalisation du suspect.

Le harcèlement criminel fait ainsi désormais partie des crimes traditionnels auquel s'ajoute un élément technologique. En effet, différentes sources laissent entendre que, de plus en plus, les TIC sont utilisées pour réaliser la commission de cette infraction. La recension d'écrits qui constitue le premier chapitre du présent rapport en rend compte. Elle se divise en deux parties distinctes soit : 1) un aperçu du contexte de violence conjugale menant au cyberharcèlement, et 2) la part qu'y prennent maintenant les technologies de l'information et des communications (TIC). Cette recension d'écrits conduit à la précision de la problématique à la base de notre travail, qui est présentée ensuite, précisant les objectifs et sous-objectifs que nous poursuivons.

La théorie des opportunités et des activités routinières de Cohen et Felson (1978) qui soutient notre argumentaire est ensuite présentée en mettant l'accent sur ses adaptations à l'univers numérique, plus précisément au cyberharcèlement. La théorie de Cohen et Felson qui met en tension les notions de délinquant motivé, de cible attrayante et d'absence de gardien pour expliquer la commission d'un acte criminel est, en effet, l'une sinon la plus populaire encore aujourd'hui citée pour expliquer la commission d'un acte criminel. Le travail présenté ici tente de préciser comment cette théorie peut s'appliquer à un crime rarement exploré par cette théorie, soit le harcèlement criminel, alors même qu'il se transforme en pouvant être perpétré via les TIC et qu'il se précise en se produisant en contexte de violence conjugale post-séparation.

Le chapitre 2 présente la méthodologie utilisée pour la réalisation du présent travail dirigé. Il permet d'en connaître davantage sur le terrain choisi, le recrutement des participants ainsi que la méthode d'analyse des données employées, les considérations éthiques prises en compte et les limites de l'étude.

Le chapitre 3 présente les résultats s'articulant essentiellement autour des trois éléments centraux de la théorie des opportunités et des activités routinières de Cohen et Felson, soit : le délinquant motivé, la cible attrayante et l'absence ou la présence éventuel d'un gardien efficace.

La discussion tenue au chapitre 4 permet de préciser comment la théorie des opportunités et des activités routinières peut plus ou moins bien s'appliquer aux situations de harcèlement par les TIC des femmes vivant en contexte de violence conjugale.

Suivant la conclusion, qui fait un court rappel des constats énoncés dans cette étude, une section *intégration* permet de mettre en valeur la particularité de ce travail dirigé, soit l'intégration de la science forensique dans un travail criminologique



# CHAPITRE 1 : RECENSION D'ÉCRITS

## Violence conjugale et nouvelles technologies, une rencontre explosive !

Ce chapitre permet d'explorer plus en profondeur les différents aspects entourant le harcèlement criminel en contexte de violence conjugale d'après ce qui en a été dit jusqu'à maintenant dans les écrits. Une première section présente les particularités du harcèlement se produisant en contexte de violence conjugale, jusqu'à l'introduction récente du harcèlement par les technologies de l'information et de la communication (TIC) dans cet univers. La deuxième partie se fait plus technique, avec la présentation des technologies de l'information et de la communication utilisées pour harceler les femmes dans le contexte pris en compte. Cette section est divisée en quatre sous-sections qui traitent successivement des possibilités d'utilisation des appareils téléphoniques, des ordinateurs et de l'Internet pour la commission du harcèlement, et ensuite des dispositifs de repérage par géolocalisation et de la surveillance par caméra.

### 1.1 Quelques mots sur la violence conjugale

La violence conjugale est caractérisée par un rapport de force au sein d'une relation de couple dans le but d'exercer un contrôle sur la victime (Johnson, 2014; Stark, 2014; Gouvernement du Canada, 2015). Ainsi, contrairement à ce que certains pourraient soutenir, la violence conjugale ne résulte pas d'une perte de contrôle mais, bien au contraire, constitue un moyen choisi pour dominer et affirmer son pouvoir sur l'autre personne (Gouvernement du Canada, 2015). D'après cette définition, la violence conjugale est bien plus que des coups portés à une personne.

Récemment, des auteurs ont distingué trois types de violence conjugale : la violence situationnelle au sein du couple, la résistance violente et le contrôle coercitif (Johnson, 2014 ; Stark, 2014).

La violence situationnelle au sein du couple « est provoquée par la situation, alors que les tensions ou les émotions d'un affrontement particulier poussent l'un des partenaires à agir par la violence » (Johnson, 2014 : 21). Ce sont essentiellement des situations où une dispute dégénère, menant à une violence bidirectionnelle entre les partenaires. Ce type de violence entre conjoints n'est pas utilisé pour exercer un contrôle ou une domination générale sur l'autre personne, mais plutôt pour signifier, agressivement un différend dans la façon de concevoir une situation.

La résistance violente, manifestée par la victime, est plutôt caractérisée par la défense physique face à une agression de la part du conjoint. Elle réagit au contrôle coercitif. La résistance violente, le plus souvent le fait des femmes, est toutefois ordinairement inutile dans ses effets étant donné l'avantage physique des hommes qui en sont la cible. Elle peut, au contraire, contribuer à envenimer la situation (Johnson, 2014).

Finalement, le contrôle coercitif se définit par l'utilisation de diverses formes de violences afin d'exercer sur la victime, à long terme, un contrôle total et sa domination au-delà de la violence physique et psychologique (Johnson, 2014 ; Stark, 2014). Stark (2014 :39) soutient que le contrôle coercitif « constitue un moyen de s'octroyer le privilège masculin, qui permet d'établir un régime formel de domination/subordination sur la femme ». Ce modèle prend en compte l'enchaînement de plusieurs tactiques élaborées par le conjoint violent pour rendre son contrôle omniprésent, peu importe où sa conjointe se trouve. L'application du contrôle coercitif se fait de plusieurs manières, soit : par la violence physique, l'intimidation, le harcèlement, l'humiliation, l'isolement et la privation, l'exploitation et l'imposition de règles (Stark, 2014).

Au Canada, selon l'étude de Statistique Canada en matière de violence conjugale auto déclarée de 2014, environ 4% de la population, soit 760 000 personnes, ont vécu de la violence physique ou sexuelle en contexte conjugal durant l'année (Statistique Canada, 2016). Dans 80% des cas de violence conjugale répertoriés, c'est la femme qui en est victime (Gouvernement du Canada, 2015) et dans 70% des cas, elle n'est pas rapportée à la police (Statistique Canada, 2016), faisant de « ce type de violence criminelle [...] l'un des moins rapportés aux autorités » (Cousineau et Ouellet, 2014 : 118). Selon Gartner et Macmillan (1995), le chiffre noir constitué des événements de violence conjugale non déclarés aux autorités serait expliqué, en grande partie, par l'intimité partagée entre la victime et l'agresseur.

Dans la présente recherche, la définition de la violence conjugale inclut, plus spécifiquement, toutes les formes de violence survenant dans toutes les relations de couples pour lesquelles la victime se trouve en maison d'hébergement, que les protagonistes soient mariés, en union libre ou encore séparés.

Il importe d'inclure les couples en processus de séparation ou séparés, car c'est la période la plus dangereuse pour la femme (Dubé et Drouin, 2014; Stark, 2014). Dubé et Drouin (2014) soutiennent que les situations de violence conjugale continuent ou même débutent parfois à l'annonce de la séparation du couple par le biais de harcèlement criminel et de menaces de mort qui, dans certains cas, seront actualisées.

Au Canada, la violence conjugale ne constitue pas une infraction spécifique dans le Code criminel. Plusieurs comportements violents utilisés en contexte conjugal sont néanmoins punissables par la loi parce qu'ils représentent d'emblée des infractions criminelles telles que voies de fait, harcèlement criminel, menace de mort, agression sexuelle, jusqu'à l'homicide. Seul le lien entre la victime et l'agresseur permet d'identifier les cas de violence conjugale dans les jugements de la cour (ministère de la Justice, 2015). Le contexte de conjugalité lors de la commission de l'infraction constitue cependant depuis peu, aux yeux de la loi, une circonstance aggravante reconnue lors de la détermination de la peine, tel que prévu à l'article 718.2 du Code criminel. Cet aspect limite également la possibilité de recourir « aux peines d'emprisonnement avec sursis qui permettraient à l'auteur d'une infraction de purger une peine dans la communauté (article 742.1) » (ministère de la Justice, 2015).

La violence conjugale peut prendre différentes formes : physique, psychologique, économique et sexuelle. Ces catégories ne sont ni exhaustives ni mutuellement exclusives. Dans le cadre de la présente étude, c'est particulièrement la violence psychologique, prenant la forme du harcèlement, qui nous intéresse. C'est pourquoi les autres types de violence précédemment nommés ne seront pas approfondis. Le crime qui nous intéresse, le harcèlement criminel, constitue un moyen parmi tant d'autres de perpétrer la violence psychologique. Il est principalement utilisé pour surveiller, contrôler et instiller la peur chez la victime (Stark, 2014).

## 1.2 Le harcèlement en contexte de violence conjugale

Dans l'éventail des techniques mises en place pour effectuer de la violence psychologique, le harcèlement s'avère la technique prisée depuis l'avènement de l'utilisation des technologies de l'information et de la communication (TIC) en violence conjugale.

Le harcèlement se définit par la répétition d'actes, de tactiques de surveillance, pendant un certain temps, menant la victime à ressentir de la peur et à craindre pour sa sécurité et celle de son entourage (McFarlane, Campbell, Wilt, Sachs, Ulrich et Xu, 1999; NNEDV, 2005; Safety Net Canada, 2013a; Stark, 2014; Dubé et Drouin, 2015). Parmi ces actes, on peut inclure de l'abus verbal, de la dégradation, l'expression de la jalousie, du contrôle, des menaces, des abus sexuels (Logan, Shannon et Cole, 2007).

Dans environ 75% des cas de harcèlement, ce sont des femmes qui sont les victimes d'hommes qui exercent un contrôle absolu sur elles (McFarlane et coll., 1999 ; Logan, Shannon et Cole, 2007; Safety Net, 2013a,b). Les hommes peuvent également en être victimes, mais suite au harcèlement, ce sont les femmes qui sont le plus sévèrement blessées et parfois même tuées (Paludi, Wilmot et Speach, 2010).

Plusieurs études indiquent que, dans environ 55% des cas, les femmes harcelées ont été ou sont encore en couple avec l'agresseur lorsque s'instaure le harcèlement. Dans la majorité des cas, en effet, il apparaît qu'une relation de violence était déjà installée dans la relation de couple avant qu'une plainte aux autorités judiciaires ou que la séparation ne survienne (McFarlane et coll., 1999; Logan, Shannon et Cole, 2007; Norris, Huss et Palarea, 2011; Tjaden, 2014). Comme mentionné précédemment, pour les femmes victimes de violence conjugale et de harcèlement, l'annonce de la séparation et la séparation physique sont des moments dangereux : la non-acceptation de la rupture ainsi que le sentiment de perte de contrôle par le conjoint peuvent faire débiter les comportements de harcèlement ou les accentuer (Dubé et Drouin, 2014).

On observe aussi un fort lien entre le harcèlement de la conjointe et la commission d'un homicide conjugal ou de violence physique sévère (McFarlane et coll., 1999; NNEDV, 2005; Tjaden, 2014; Dubé et Drouin, 2014, 2015). Par ailleurs, les femmes victimes de violence conjugale et de harcèlement par leur conjoint signaleraient à la police plus souvent les actes de violence de celui-ci que les femmes ne vivant pas de harcèlement (Logan, Shannon et Cole, 2007). Les femmes vont dénoncer lorsqu'elles craignent sérieusement pour leur vie ou celle de leurs proches, et plus spécialement leurs enfants, lorsque des menaces de mort ont été proférées et lorsqu'elles en ont assez et qu'elles veulent que cette situation cesse (Dubé et Drouin, 2015).

Différentes conséquences psychologiques liées au harcèlement sont observables chez les victimes: la dépression, des symptômes du syndrome de stress post-traumatique, de l'anxiété et la dépendance à l'alcool ou à la drogue, pour ne nommer que celles-là (Logan, Shannon et Cole, 2007; Stark, 2014; Dubé et Drouin, 2015).

L'issue du harcèlement peut aussi s'avérer fatale se traduisant par des tentatives de meurtre ou un homicide conjugal (McFarlane et coll., 1999; NNEDV, 2005; Logan, Shannon et Cole, 2007; Safety Net Canada, 2013b; Tjaden, 2014; Dubé et Drouin, 2015). Le harcèlement est ainsi considéré parmi les formes les plus sévères de violence conjugale, étant donné la possibilité d'un dénouement souvent tragique. Selon Safety Net Canada (2013b), 76% des femmes tuées par leur conjoint actuel ou passé avaient préalablement été victimes de harcèlement par ce dernier. Dans environ 60% des cas d'homicides conjugaux, un signalement de harcèlement avait été fait à la police avant que l'harceleur commette le meurtre (McFarlane et coll., 1999; Dubé et Drouin, 2015).

Au Canada, 58% des plaintes pour violence conjugale sont liées à des voies de fait et 17% au harcèlement criminel, des propos indécents au téléphone, des appels téléphoniques harassants, ou des menaces (Statistique Canada, 2015). L'article 264 du Code criminel canadien (1985) décrit le harcèlement criminel comme suit :

**264.**(1) Il est interdit, sauf autorisation légitime, d'agir à l'égard d'une personne sachant qu'elle se sent harcelée ou sans se soucier de ce qu'elle se sente harcelée si l'acte en question a pour effet de lui faire raisonnablement craindre — compte tenu du contexte — pour sa sécurité ou celle d'une de ses connaissances.

(2) Constitue un acte interdit aux termes du paragraphe (1), le fait, selon le cas, de :

- a) suivre cette personne ou une de ses connaissances de façon répétée;
- b) communiquer de façon répétée, même indirectement, avec cette personne ou une de ses connaissances;
- c) cerner ou surveiller sa maison d'habitation ou le lieu où cette personne ou une de ses connaissances réside, travaille, exerce son activité professionnelle ou se trouve;
- d) se comporter d'une manière menaçante à l'égard de cette personne ou d'un membre de sa famille.

Selon Safety Net Canada (2013b) et Tjaden (2014), la loi contre le harcèlement est sous-utilisée principalement due à la méconnaissance de celle-ci. Cet organisme considère également qu'elle est inadaptée compte tenu de la croissance rapide des TIC.

### 1.3 Cyberharcèlement / harcèlement via les technologies de l'information et de la communication

L'accès à Internet et aux téléphones intelligents a changé considérablement la manière dont les gens communiquent entre eux (Casey, 2011). C'est également vrai dans les relations de couples. Désormais, la violence psychologique, notamment le harcèlement, peut être perpétrée via les technologies de l'information et de la communication. On le nommera alors le cyberharcèlement. Dubé et Drouin (2015 : 15) définissent le cyberharcèlement comme l'« *utilisation des technologies de l'information et de la communication (TIC) pour établir une communication virtuelle de façon répétée avec une autre personne afin de commettre des actes répétés de violence psychologique* ». Wall (2001) parle de son côté de cyberviolence qu'il définit comme étant la distribution de matériel injurieux, blessant et dangereux en ligne.

Selon les auteurs, les méthodes identifiées pour se livrer à la cyber violence, et plus spécialement au cyber harcèlement, via les TIC sont, sans s'y limiter, l'accumulation d'informations personnelles sur la victime pour la menacer ou l'intimider, l'envoi de courriels et de messages textes à répétition, des appels incessants sur son téléphone personnel ou à son emploi, la publication de photos sur les réseaux sociaux sans le consentement de la victime, l'installation de logiciel espion et la géolocalisation (Southworth, Finn, Dawson, Fraser et Tucker, 2007; Dimond, Fiesler et Bruckman, 2011; Reynolds, Henson et Fisher, 2011; Holt, 2011; Safety Net Canada, 2013c; Dubé et Drouin, 2015).

Tous ces comportements, en contexte conjugal plus spécifiquement, visent à élargir le contrôle et la domination du conjoint sur sa victime (Dimond, Fiesler et Bruckman, 2011; Marcum, 2011; Safety Net, 2013c).

Holt (2011) considère que le harcèlement par les TIC n'est pas un nouveau crime ; la nature de l'acte, soit le harcèlement, est toujours la même, c'est seulement le moyen de le commettre qui change. Ce n'est pas la technologie en elle-même qui amène ce type de comportement, mais plutôt le contraire, soutient l'auteur : ce sont les comportements violents et de contrôle qui sont transmis par les TIC. Les technologies permettent l'extension de comportements que l'agresseur aurait envers sa conjointe en face à face précisent Marganski et Melander (2015). C'est pourquoi Holt (2011) catégorise le harcèlement comme étant un « *computer-assisted crime* », ce qui signifie que les nouvelles technologies ont « *a supporting role in the commission of a crime, although the activity could be performed without computer assistance* » (Holt, 2011 : 7).

Le 8<sup>e</sup> *Rapport annuel du Domestic Violence Death Review Committee* (Office of the Chief Coroner, 2011) et Safety Net (2013a) signale que les nouvelles technologies sont souvent utilisées par les conjoints avant de commettre un homicide conjugal, constituant une préoccupation grandissante pour cet outil. En fait, selon Safety Net (2013a), 98% des intervenantes travaillant avec des femmes victimes de violence conjugale rapportent qu'elles ont aidé des femmes menacées et/ou intimidées via les nouvelles technologies (Safety Net Canada, 2013c). Les TIC permettent d'exercer un contrôle à distance sur la femme, soutiennent les auteurs. Même si la violence n'est pas physique, se savoir guettée en tout temps, ne rien pouvoir cacher de ses déplacements exerce une pression considérable et soutenue sur la femme (Association québécoise Plaidoyer-Victime, 2014; Stark, 2014). Cela signifie également que la séparation physique n'est plus un moyen de se mettre en sécurité (Stark, 2014).

Casey (2011) mentionne que la force du harceleur se trouve dans la connaissance de la victime et les informations qu'il détient sur elle. Le cyberharcèlement procure à l'agresseur des fonctions nouvelles qui n'étaient pas accessibles par le harcèlement en personne, l'avantage principal des technologies de l'information et des communications résidant dans l'anonymat qu'elles procurent. L'utilisation de pseudonymes et de diverses techniques permettent en effet l'anonymat de l'agresseur, qui n'est pas aussi possible avec le harcèlement traditionnel. Le fait de ne pas être face à la victime provoque souvent la déshumanisation de la victime faisant en sorte que l'agresseur se permet d'être beaucoup plus extrême et offensant dans ses propos (Fusco, 2014). Ceci étant, bien les menaces ne soient pas directement et oralement formulées à la victime, elles sont tout aussi blessantes et réelles pour celle-ci, soutiennent les auteurs.

Les TIC permettent aussi aux agresseurs, tout en demeurant anonymes, d'avoir plus de moyens d'espionner leur victime, ceci sans avoir à se déplacer. Ainsi, plusieurs dispositifs de localisation et logiciels espions permettent de faire savoir à la victime qu'elle est suivie sans savoir par qui ni dans elle mesure elle doit prendre les menaces au sérieux (Fusco, 2014). Dans les cas de cyberharcèlement dans une relation de couple, la victime peut fortement soupçonner l'individu à la base des menaces d'être son conjoint, mais il est possible que celui-ci ait donné ses coordonnées à quelqu'un d'autre et que cette ou ces personnes soient les auteurs des menaces.

L'agresseur peut aussi prendre une fausse identité (Marcum, 2011; Fusco 2014). Il peut, par exemple, se servir du téléphone d'une personne de sa famille pour tenter de joindre sa conjointe. La première fois, probablement qu'elle répondra, mais, par la suite, elle deviendra méfiante face à tous les appels entrants, même si le numéro qui apparaît à l'écran n'est pas celui de son conjoint.

L'auteur de cyberharcèlement joue ainsi sur la peur de la victime, créant chez elle de l'anxiété et la crainte de pouvoir être rejointe en tout lieu et à tout moment, ne sachant jamais quand l'agresseur risque d'apparaître en personne sachant où elle se trouve (Dimond, Fiesler et Bruckman, 2011; Holt, 2011; Fusco, 2014 ; Dubé et Drouin, 2015).

Autrement, mais dans le même ordre d'idée, la proximité qu'offre la relation conjugale entre les deux partenaires peut permettre au conjoint de prendre l'identité de sa conjointe pour envoyer des messages ou publier des photos d'elle sur les réseaux sociaux entraînant des conséquences très graves pour la victime. En se faisant passer pour sa conjointe, il peut, notamment, s'inscrire sur des sites auxquels elle ne souhaiterait pas être associée. Fusco (2014: 7), dans son exemple, précise que l'agresseur peut: « *create an ad on Craigslist saying that he/she fantasizes about being raped and post the victim's address. Unknowing people would then respond to the ad and show up at the victim's house. They would think it is all part of an act, while the victim would be in legitimate fear for their life* » (Fusco, 2014 : 7).

Ainsi, bien que l'harcéleur puisse se trouver loin de la victime, voire dans un autre pays, il se peut aussi qu'il soit physiquement à proximité et qu'il puisse réellement mettre à exécution ses menaces, installant un sentiment de peur diffuse, mais non moins acerbe, chez les victimes.



Le harcèlement, dans sa forme traditionnelle, nécessite beaucoup de travail et de temps tandis que le harcèlement par les TIC demande beaucoup moins d'investissement de la part de l'agresseur : il peut utiliser des outils qui garderont un œil sur sa victime où que ce soit. De plus, l'envoi de courriels et de messages est maintenant quasi instantané (Fusco, 2014; Dubé et Drouin 2015), permettant à l'agresseur d'envoyer des menaces aussitôt qu'il a « une seconde » de libre. La quantité de messages pouvant être expédiée via les TIC est ainsi immense; en quelques minutes, la victime peut recevoir des centaines de messages, contrairement à ce que permet l'expédition de lettres et de colis. Il existe en effet des dispositifs qui envoient des courriels et des messages textes automatiquement, préprogrammés pour être envoyés à un moment donné (Holt, 2011; Fusco, 2014).

L'étude de Dimond, Fiesler et Bruckman (2011) précise comment les TIC impactent les femmes victimes de violence conjugale en maison d'hébergement. Les réseaux sociaux, tels Facebook et Twitter, sont, dans ce cas, utilisés par le conjoint et son entourage pour harceler et menacer la conjointe venue y chercher refuge. Le conjoint peut également utiliser ce dispositif pour tenter de localiser sa conjointe et ses enfants en communiquant avec l'entourage de cette dernière.

Les réseaux sociaux permettent, à l'inverse, à la femme de garder contact avec son entourage : « *She states it is a risk she is willing to take to look at her sister's Facebook, to feel more connected with her family since she has had to sever all of her ties* » (Dimond, Fiesler et Bruckman, 2011 : 416). Cette citation démontre l'importance pour les femmes en maison d'hébergement de rester en contact avec leur entourage même si elles doivent être isolées (cachées) pour assurer leur sécurité. Dans l'étude de Dimond, Fiesler et Bruckman (2011) toutefois, les femmes qui étaient déjà inscrites sur les réseaux sociaux affirmaient, pour la plupart, avoir arrêté d'alimenter leur page et même avoir complètement cessé de l'utiliser par crainte d'être retrouvées ou harcelées par leur conjoint.

La voie de communication la plus utilisée par le conjoint pour tenter de joindre sa compagne est cependant le cellulaire : 7 des 10 femmes interviewées dans le cadre de l'étude de Dimond, Fiesler et Bruckman (2011) révélaient ainsi avoir reçu des menaces, des propositions sexuelles inappropriées, des messages vocaux et des messages textes harcelants, certaines affirmant même avoir été localisées via leur appareil.

Les femmes utilisent des stratégies pour éviter d'être ainsi poursuivies. Dans l'étude de Dimond, Fiesler et Bruckman (2011), certaines ont décidé de se débarrasser de leur cellulaire afin d'éviter tous risques de localisation et de harcèlement. Deux d'entre elles ont choisi de donner un faux nom au distributeur de téléphonie mobile pour éviter que leur conjoint puisse les retrouver. D'autres ont trouvé des moyens de filtrer les appels pour s'assurer de n'avoir aucun contact avec le conjoint, car ce dernier changeait de téléphone pour les rejoindre, donc elles n'étaient jamais certaines de la personne qui se trouvait au bout du fil lorsqu'elles répondaient. Étant consciente des connaissances informatiques de son conjoint, une femme indique qu'elle n'ose plus aller sur Internet ou même utiliser ses cartes de crédit, car elle sait qu'il serait capable de la retrouver.

À l'inverse, des femmes sachant que leur conjoint n'a pas accès à un ordinateur tirent avantage des postes informatiques à disposition pour parfaire leurs compétences informatiques.

Au terme de leur étude, Dimond, Fiesler et Bruckman (2011) concluent néanmoins que les conséquences négatives associées aux technologies de l'information et de la communication s'avèrent beaucoup plus grandes pour les femmes victimes de violence conjugale que les quelques avantages qu'elles pourraient en tirer (Dimond, Fiesler et Bruckman, 2011).

#### 1.4 Les technologies de l'information et de la communication (TIC) : une évolution fulgurante

À partir des années 1990, les foyers ont commencé à acheter des ordinateurs et à se brancher à l'Internet. Son faible débit décourageait alors la majorité des internautes de consulter ou encore de créer une page web. À cette époque, les forums de discussion étaient principalement ce pour quoi les gens se connectaient. À partir de 1997, des informations souvent inédites étaient publiées sur le net, qui devenait ainsi une source de renseignements de plus en plus consultée.

En 2004, le nombre d'utilisateurs connectés à Internet se chiffre à 294 millions dans le monde. Le cap du milliard d'internautes est franchi en 2009 (Ifrah, 2010). En 2010, on estime à 525 millions le nombre de téléphones intelligents commercialisés (Arpagian, 2010). En janvier 2015, 42 % de la population mondiale est connectée à Internet totalisant 3,025 milliards d'internautes (We are social, 2016).

Plus spécifiquement, on note que 29% de la population mondiale est connectée sur les réseaux sociaux et que 23% y accèdent par leur téléphone intelligent. Depuis septembre 2014, la téléphonie mobile à utilisateur unique a rejoint 50% de la population mondiale et, de celle-ci, 38% a accès à un téléphone intelligent utilisant le réseau 3G ou supérieur. En Amérique du Nord et en Europe de l'Est, c'est 85% de la population qui détient un téléphone intelligent permettant la connexion au 3G ou plus (We are social, 2016). Selon la Banque mondiale (2016), 87% des Canadiens avaient accès à Internet en 2014. Ceux-ci utilisent différents dispositifs pour consulter les pages internet, à savoir : 70% un ordinateur, 54% un téléphone cellulaire et 10% une tablette.

Ces statistiques montrent à quel point l'évolution d'Internet et du réseau mobile a été rapide et se répand à travers le monde. C'est maintenant un réseau public immense, accessible en tout temps, pour le meilleur et pour le pire, comme il est courant d'entendre.

Du côté du pire, on a pu constater que le cyberharcèlement peut aujourd'hui se faire en utilisant différents outils virtuels de mieux en mieux connus des conjoints voulant surveiller et garder le contrôle sur leur conjointe (NNEDV, 2005), comme nous le verrons maintenant.

#### *1.4.1 Les appareils téléphoniques au service du cyberharcèlement*

Un des moyens les plus populaires servant le cyberharcèlement, nous le notions plus haut, est l'appareil téléphonique. Il est, dans ce cas, principalement question d'appels téléphoniques répétés et harassants rejoignant la ligne domiciliaire et, de plus en plus, le cellulaire de la victime. À chaque numéro de téléphone est associé le nom de l'abonné et son adresse (NNEDV, 2005; Southworth et coll., 2007). À partir des appareils cellulaires, plusieurs informations supplémentaires peuvent être acquises permettant de connaître non seulement l'identité probable de l'appelant, mais aussi sa localisation. Les enquêteurs ont ainsi accès au numéro de téléphone associé à la carte SIM, l'IMEI, qui indique le numéro identifiant le boîtier de l'appareil, les numéros appelés, des informations quant aux tours cellulaires qui relaient les communications initiées à partir de l'appareil, la tour ayant reçu le premier signal, les messages textes envoyés, la date, l'heure et la durée des appels (Forte et de Donno, 2010).

Afin de mieux comprendre la valeur des informations accessibles, voyons plus en détail les notions spécifiques à l'utilisation de la téléphonie mobile.

Les téléphones cellulaires fonctionnent grâce aux tours cellulaires qui reçoivent un signal. Quand un appel d'un cellulaire est effectué, c'est la tour la plus proche de lui qui reçoit le signal, le transfère à la station de base qui, à son tour, envoie le signal à la tour la plus proche du destinataire. Les tours de cellulaire se relaient ainsi afin d'offrir le signal le plus fort possible.

Dans les données téléphoniques transmises par les distributeurs, la localisation de la tour ayant reçu le signal, nécessairement la plus proche de l'individu qui utilise le téléphone émetteur, est consignée, de même que la tour transmettant le signal au destinataire (Graves, 2014). La position d'un cellulaire peut dès lors être trouvée en utilisant la trilatération réalisée à partir des tours cellulaires, des satellites GPS ainsi que des réseaux Wi-Fi disponibles.

La carte SIM, pour sa part, enregistre des informations sur le cellulaire concernant l'utilisateur, et d'autres informations pertinentes tels les contacts, les messages textes et le numéro de téléphone associé à cette carte. Elle sert également à crypter les transmissions et s'identifie en tant que cellulaire au réseau de téléphonie mobile. Chaque carte SIM peut être protégée par un numéro d'identifiant personnel (NIP) pour s'assurer que personne, sauf le propriétaire, ne puisse l'utiliser. La carte SIM est transportable, c'est-à-dire qu'on peut la changer d'appareil et garder le même numéro de téléphone, ses contacts et les autres informations y étant emmagasinées (Graves, 2014).

L'IMEI est un numéro unique qui identifie chaque boîtier de cellulaire. C'est un numéro qui a une fonction semblable au numéro d'assurance sociale pour les habitants d'un pays. Ce numéro contient 15 chiffres : les huit premiers indiquent le modèle de l'appareil et où il a été fabriqué, les six suivants indiquent le numéro de série, et le dernier est le numéro de contrôle (Graves, 2014).

La fonction d'identification de l'appelant est un service téléphonique qui révèle le numéro de téléphone, le nom et la localisation de l'appelant (Southworth et coll. 2007; NNEDV 2005):

« *Caller ID is supported by a telephone line linked to an electronic device that captures information about incoming calls and stores it in the display unit for future use* », expliquent Southworth et coll. (2007 : 845). Leur étude révèle qu'en contexte de violence conjugale, des agresseurs ont utilisé ce dispositif pour retrouver leur conjointe qui avait quitté le domicile pour se mettre à l'abri de la violence vécue, pour plusieurs en maison d'hébergement.

De leur côté, plusieurs femmes victimes de violence conjugale ont fait retirer leurs noms des listes reliant leur nom à leur numéro de téléphone, de type bottin téléphonique. Il appert toutefois que plusieurs compagnies sur Internet vendraient ces informations (NNEDV, 2005; Southworth et coll. 2007). Les cartes d'appels prépayées apparaissent alors un moyen efficace de garder l'anonymat. Ceci est aussi vrai pour les victimes que pour les agresseurs qui peuvent ainsi harceler la victime sans que la source de l'appel puisse être retracée. Si la carte n'a pas été activée avec une carte de crédit, il est quasi impossible de remonter au détenteur de cette carte (Southworth et coll. 2007).

#### *1.4.2 Ordinateurs et Internet : des transmetteurs d'information*

Lorsqu'on parle d'Internet, une donnée primordiale à connaître est l'adresse de protocole Internet : l'adresse IP V4. Il s'agit d'un identifiant numérique de quatre nombres entre 0 et 255 séparé par des points, fourni par le fournisseur de services, pour que le client puisse naviguer sur Internet. Le fournisseur de services connaît le nom ainsi que l'adresse du client. L'adresse IP est associée à une adresse physique plus qu'à un client en particulier, car elle est signifiée au routeur qui distribue l'Internet à cette adresse physique. Or, il peut y avoir plus d'un appareil connecté auxquels le routeur distribue des adresses IP internes, non accessibles au fournisseur de service Internet ni aux sites Internet visités qui auront seulement accès à l'adresse IP du routeur, faisant qu'il est alors possible de connaître le pays, la province, et même la ville et le bâtiment où est localisé l'appareil, mais pas de localiser précisément l'utilisateur, ni qui il est. Les renseignements obtenus via l'adresse IP peuvent mener à connaître les activités associées à celle-ci, comme le partage de fichiers, la consultation des pages Web, ainsi que les adresses courriel et comptes de réseaux sociaux utilisés à partir de cet identifiant, mais encore là, la personne derrière l'adresse reste incertaine (Commissariat à la protection de la vie privée du Canada, 2013)

Les réseaux sociaux développés à partir d'Internet ont acquis, dans les dernières années, un nombre considérable d'adhérents. Ceux-ci permettent de prendre ou de rester en contact avec beaucoup de gens, amenant ainsi chaque utilisateur à être « amis » avec plusieurs personnes. Les réseaux sociaux ouvrent la possibilité d'entretenir un réseau social très large. Utilisé consciencieusement, ceci constitue le principal avantage qu'ont leur reconnaît.

A contrario, les plateformes fournies par ces réseaux sociaux se révèlent, d'un côté, un moyen efficace de harcèlement en émettant des commentaires injurieux, en publiant des photos ou de vidéos dégradants créant des préjudices majeurs à la victime. D'un autre côté, les publications émises par la victime sur ces réseaux sociaux peuvent permettre à l'agresseur de suivre ses déplacements et ses activités, en d'autres mots de la surveiller, et même la contrôler à distance. L'agresseur peut en outre avoir accès à la famille et aux amis de la victime assez facilement grâce à ces réseaux pour les menacer ou tenter d'en apprendre plus sur la localisation de la victime si elle a quitté le domicile conjugal, augmentant d'autant son rayon d'action (Dimond, Fiesler et Bruckman, 2011; Fusco, 2014).

Les réseaux sociaux offrent plus qu'une plateforme pour publier des statuts et des photos, ils offrent également des services de messageries instantanées qui donnent la localisation de la personne envoyant le message. Ceci implique que si une femme ayant quitté le domicile conjugal pour se mettre en sécurité envoie un message via la messagerie instantanée, elle donne accès à sa localisation. Les sites de courriels et de messagerie instantanée peuvent aussi être utilisés pour envoyer des menaces et harceler la victime.

La transmission d'un courriel est effectuée par un serveur gardant une copie du message à envoyer. Dépendamment du type de serveur utilisé pour la transmission du courriel, celui-ci sera gardé sur le serveur jusqu'à ce qu'il soit téléchargé ou tant que le courriel n'a pas été supprimé de la boîte de réception (Graves, 2014). Si l'agresseur connaît le mot de passe des comptes courriel de la victime, il peut envoyer des messages harcelants à sa conjointe, ou encore, il peut s'envoyer des messages menaçants à partir du courriel de la victime, et ensuite fournir ces courriels à la police pour la faire arrêter (NNEDV, 2005).

Des applications existent permettant de changer l'adresse de l'émetteur, et donc d'envoyer des courriels à des gens en se faisant passer pour la victime. Dans les courriels, l'en-tête inclus notamment les informations suivantes : *À; De; Sujet et Date*. L'adresse électronique décrite dans l'onglet *De* : ne devrait pas être considérée a priori authentique, sachant qu'il existe des techniques et des virus permettant de cacher l'identité du véritable expéditeur du courriel.

Les métadonnées enregistrées dans le courriel sont par ailleurs riches en informations. On peut y retrouver l'adresse IP, le serveur utilisé pour la transmission du courriel, l'heure et la date d'envoi, l'identifiant unique pour le courriel, ainsi que tous les dispositifs utilisés pour cacher l'identité de l'émetteur (Graves, 2014).

Les courriels peuvent par ailleurs transmettre des virus ou des logiciels espions permettant de surveiller l'appareil qui reçoit le courriel. Des *logiciels espions* en vente sur Internet pour des prix relativement bas requièrent pour leur part une accessibilité physique à l'appareil pour leur installation. Or, dans les situations de relation conjugale, l'accès physique n'est pas réellement un obstacle à leur installation étant donné que, bien souvent, les protagonistes cohabitent. Une fois installés, ces logiciels sont invisibles sur l'appareil de la victime. Ils donnent accès à toutes les actions effectuées avec l'appareil : les appels, les messages, les courriels, les photos, les éléments supprimés, les sites Internet visités et permettent la géolocalisation de l'utilisateur de l'appareil (Southworth et coll. 2007).

Le procédé d'enregistrement de frappes peut être inclus dans le logiciel espion ou acheté indépendamment. Comme en rend compte le nom, ce dispositif enregistre toutes les frappes effectuées sur le clavier donnant ainsi accès au contenu de tous les courriels envoyés, les mots de passe des différents comptes, les sites visités... (Southworth et coll. 2007).

#### *1.4.3 Les dispositifs de repérage par géolocalisation (GPS)*

Les appareils GPS utilisent les satellites pour donner la localisation avec précision d'un appareil. Maintenant, tous les téléphones sont munis de systèmes de localisation GPS installés, notamment, pour permettre aux secours de connaître la position de la personne en détresse (Southworth et coll., 2007) en plus de permettre au propriétaire du téléphone de trouver son chemin. Mais, les GPS servent également bien d'autres fonctions. Ces dispositifs de localisation sont notamment utilisés par les harceleurs pour repérer ou même suivre leurs victimes. Des appareils GPS peuvent être également cachés dans la voiture de la victime, permettant de suivre ses déplacements (NNEDV, 2005; Southworth et coll. 2007). La localisation de l'appareil se fait alors par trilatération, le même principe que pour les téléphones cellulaires, explicité plus haut (NNEDV, 2005; Southworth et coll., 2007; Graves, 2014)

Des applications ont aussi désormais comme utilité principale la géolocalisation des appareils pour différents motifs personnels ou commerciaux. Ces applications peuvent incidemment mettre en péril la sécurité des femmes victimes de violence conjugale en permettant de la repérer.

Ainsi, bien que leur but premier ne fût pas de pouvoir suivre à la trace une personne, les harceleurs se sont approprié ces technologies afin de surveiller leur victime.

#### *1.4.4 La surveillance par caméra*

Les caméras ont aussi beaucoup évolué au cours des dernières années. Certaines sont miniatures et sans-fils, pouvant être cachées facilement pratiquement partout. Elles peuvent être activées à distance et enregistrer les images qu'elles captent sur un ordinateur pour être visionnées plus tard (NNEDV, 2005; Southworth et coll. 2007). Il existe également des logiciels espions ou des virus informatiques pouvant déclencher la caméra sur le téléphone ou l'ordinateur de la victime, sans qu'elle sache que la caméra est en marche.

Encore ici, l'agresseur peut voir et surveiller tout ce que fait la victime. Et il y a tout lieu de croire qu'avec l'apparition des drones pourraient éventuellement agrandir le périmètre de surveillance.

### **1.5 La théorie des opportunités et activités routinières à l'heure des TIC**

Cohen et Felson (1979) sont à l'origine la théorie des opportunités et des activités routinières. Le but de cette théorie est de mettre en relation les différents éléments à l'origine de la commission d'un crime. Il est ainsi établi que pour qu'un crime soit commis, à un endroit et en un temps donné, il faut qu'il y ait la rencontre des trois éléments suivants : un délinquant motivé, une cible attrayante et l'absence de gardiens efficaces. Selon les auteurs de la théorie, le délinquant motivé doit être minimalement attiré vers les comportements criminels et avoir un tant soit peu de compétences pour les réaliser. La cible attrayante et l'incapacité pour un gardien de prévenir les violations criminelles sont des éléments interdépendants propices à la commission d'un crime, poursuivent les auteurs. En agissant sur l'un des deux derniers éléments, on augmente les chances qu'un délinquant motivé ne tente pas la commission d'un crime, car l'entreprise ne sera pas aussi aisée et sera plus risquée pour lui.

La théorie de Cohen et Felson (1979) est pertinente pour expliquer la commission de crimes de proximité dans une organisation spatio-temporelle des activités routinières du délinquant motivé. Il est probable que le taux de crimes diffère en fonction des époques ou des endroits, ou encore de changements de routines créant autant d'opportunités de commettre un crime.



Cohen et Felson (1979) donnent l'exemple de l'arrivée massive des biens de consommation, comme les voitures, qui crée beaucoup plus d'opportunités pour les délinquants motivés de voler le bien en question sans se faire prendre, en faisant une cible attrayante, jusqu'à ce que des mesures de protection viennent contrecarrer l'opportunité. Les auteurs constatent que plusieurs changements culturels ont pris place dans les années 1960, amenuisant le contrôle social informel auparavant plus présent, jouant le rôle de gardien. Ils concluent que ces changements dans la culture et la routine des gens ouvrent la voie à plus d'opportunités pour la commission de crimes, notamment le harcèlement.

L'étude sur le harcèlement au Canada de Reyns, Henson, Fisher, Fox et Nobles (2015), montre qu'il y a des facteurs qui augmentent les risques pour les femmes d'en être victimes. L'âge et la situation conjugale sont les facteurs qui ont le plus d'influence quant aux probabilités de harcèlement qui guettent les femmes qui présentent une différence significative par rapport aux hommes. Cette étude montre ainsi que le harcèlement est vécu en plus grande partie par les femmes et que les facteurs de risques varient entre les femmes et les hommes.

Pour Holt et Bossler (2008), la théorie des opportunités et des activités routinières peut s'appliquer dans des cas spécifiques de cybercrimes. Il importe toutefois de préciser le type de crime commis dans le monde numérique afin de permettre l'adaptation de la théorie des opportunités et des activités routinières les concernant. D'après Reyns, Henson et Fisher (2011), les activités routinières ont évolué au cours des dernières années, notamment en incorporant de plus en plus de communications et activités en ligne. Les auteurs soutiennent qu'il est impératif d'adapter les théories classiques pour qu'elles puissent s'appliquer au monde virtuel.

Holt et Bossler (2008) tout comme Reyns, Henson et Fisher (2011) tentent d'appliquer cette théorie au harcèlement commis via les technologies de l'information et de la communication. Dans leur étude, ils visent à montrer que plusieurs liens peuvent être faits entre la théorie des opportunités et des activités routinières et la victimisation associées au cybercrime. Cette étude, basée sur 788 sondages autorévélés d'étudiants universitaires, dont 57% sont des femmes, identifie la cible attrayante dans ce cas comme étant une personne qui passe beaucoup de temps sur des sites ou applications de messagerie instantanée. Ils constatent que les compétences informatiques agissent comme facteur de protection, mais seulement pour les hommes.

Les auteurs identifient deux types de gardiens qui pourraient prévenir la commission de cyber crime : un gardien physique et un gardien social. Ils précisent le gardien physique comme étant un antivirus ou tout autre logiciel visant la protection de l'ordinateur. Ce type de gardien ne réduirait toutefois pas les probabilités de victimisation dans le cas de cyberharcèlement, puisqu'il est seulement efficace contre les attaques dirigées vers l'appareil. Les gardiens sociaux auraient pour leur part une influence quant aux risques de victimisation. « *Having friends involved in computer based deviance increased the odds of being harassed, suggesting that these respondents exposed themselves to motivated offenders and minimized the number of individuals who could assist if an individual is being harassed* » (Holt et Bossler, 2008: 16).

Un élément important ressort des analyses faites par Holt et Bossler (2008) : le simple fait d'être une femme augmente de 2,75 les risques d'être harcelé en ligne. Il semble que le fait que les femmes s'adonnent à des comportements déviants en ligne, tel que le piratage ou qu'elles aient des amis qui se livrent à ce genre de comportement augmente considérablement les risques de victimisation. Holt et Bossler (2008) appuient cette différence en fonction du genre sur la culture du viol qui serait aussi véhiculée dans le monde informatique ainsi que sur la façon de communiquer en ligne particulièrement sexiste et violente qui y prévaut en vue d'asseoir sa domination d'Internaute.

La recherche de Reynolds, Henson et Fisher (2011) tente pour sa part d'établir, comme l'ont fait quelques chercheurs avant eux, comment la théorie des opportunités et des activités routinières peut s'appliquer dans les cas de cyberharcèlement. Les critères de mesure pour les trois éléments centraux de la théorie ne sont toutefois pas les mêmes que dans les autres études. Afin de calculer le degré d'exposition à un délinquant motivé en fonction de ses activités routinières, les auteurs prennent en compte le nombre d'heures passées en ligne chaque jour, le nombre de réseaux sociaux auquel l'internaute est inscrit, le nombre de fois que la personne actualise ses profils sur les différents réseaux sociaux, le nombre de photos publiées en ligne et si la personne utilise la messagerie instantanée (Reynolds, Henson et Fisher, 2011 : 1156). Leur étude montre que le nombre de photos mises en ligne, notamment, a un impact significatif lorsqu'il s'agit de prédire les risques de cyberharcèlement.

L'actualisation de statuts sur les réseaux sociaux est pour sa part associée à une augmentation modérée d'avances sexuelles indésirables transitant par voie électronique. Le nombre de comptes de réseaux sociaux ainsi que l'utilisation de la messagerie instantanée auraient aussi un impact sur les risques de victimisation de type cyberharcèlement, observent les auteurs.

Le deuxième critère évalué est la proximité en ligne de la victime avec un délinquant motivé. Cette proximité virtuelle peut être établie par le biais de la messagerie instantanée où les deux acteurs sont connectés et ont des interactions en direct. Cette proximité est aussi présente dans les forums de discussion où des interactions indirectes ont lieu.

Les trois critères qui permettent d'évaluer la proximité en ligne sont : 1) si le répondant donne accès à des étrangers à ses différents profils dans les réseaux sociaux; 2) le nombre d'amis qu'il a sur les réseaux sociaux; et 3) si le répondant utilise des services en ligne pour avoir plus d'amis sur ses comptes de réseaux sociaux (Reyns, Henson et Fisher, 2011 : 1156). Le seul critère qui semble avoir un impact sur la victimisation est d'ajouter des personnes inconnues sur ses réseaux sociaux, donnant ainsi accès à des informations personnelles permettant des contacts indésirables.

Reyns, Henson et Fisher (2011) n'utilisent pas les antivirus comme critère pour calculer l'efficacité du gardien. Pour eux, un gardien efficace pour protéger contre le cyberharcèlement se calcule en considérant les critères suivants : si l'accès est limité quant au contenu des profils sur les différents réseaux sociaux et si le répondant utilise une application qui permet de savoir qui consulte son profil, d'où il provient et quand il l'a visité. En connaissant ces informations, la victime peut être elle-même son gardien en adoptant des habitudes plus sécuritaires sur les réseaux sociaux. Comme Holt et Bossler (2008), Reyns, Henson et Fisher (2011) cherchent à savoir si la pratique de comportements déviants en ligne augmente l'exposition à des délinquants motivés, haussant ainsi les risques de victimisation. Reyns, Henson et Fisher (2011) trouvent un lien positif entre l'utilisation d'applications permettant de savoir qui visite son profil et le cyberharcèlement. Ils interprètent toutefois cette donnée comme étant la conséquence du cyberharcèlement. Ainsi, l'utilisation d'applications permettant de connaître les visiteurs sur son profil serait faite en réaction à une situation de cyberharcèlement, dans le but de prévenir ce genre de situation dans le futur. La fréquentation de pairs déviants en ligne augmenterait également les risques de cyberharcèlement, mais la commission d'actes déviants en ligne reste le critère le plus pertinent pour prédire la victimisation, concluent les auteurs.

L'attractivité de la victime potentielle, de son côté, varie d'un délinquant à l'autre. Le délinquant doit voir dans la victime une certaine valeur ou une facilité d'action pour juger qu'elle est attrayante. Dans le monde numérique, plusieurs éléments peuvent faciliter le passage à l'action : en particulier, si le délinquant détient le nom, le courriel, l'adresse ou le numéro de téléphone de la victime il sera beaucoup plus facile de la harceler, de l'infecter avec un logiciel espion ou de lui créer de faux profils sur différents réseaux sociaux.

D'autres éléments peuvent aussi rendre la cible attrayante. C'est le cas, notamment, si celle-ci publie des photos, ou des vidéos l'impliquant, ou si elle dévoile son statut conjugal et son orientation sexuelle. Il s'avère en effet que le genre et le statut conjugal ont un impact sur la probabilité de vivre du cyberharcèlement. Ainsi, le simple fait d'être une femme double le risque d'être victime de cyberharcèlement ou de contacts indésirables et triple le risque d'être l'objet d'avances sexuelles. Pour leur part, les gens en couple se révèlent susceptibles de vivre 1,5 fois plus de contacts indésirables que ceux célibataires.

## 1.6 La problématique

Jusqu'à maintenant, la majorité des études en criminologie concernant le harcèlement par les TIC cherchent à déceler les facteurs de risque pouvant permettre d'identifier les victimes potentielles utilisant les nouvelles technologies en fonction de leurs habitudes de vie. Dans la plupart des cas, ce sont des études quantitatives qui tentent d'identifier les comportements les plus utilisés pour commettre le harcèlement et les impacts du harcèlement par les TIC (Sheridan et Grant, 2007; Norris, Huss et Palarea, 2011; Cattaneo, Cho et Botuck, 2011; Borrajo, Gàmez-Guadix, Pereda et Calvete, 2015; Marganski et Melander, 2015). Les études de Reyns, Henson et Fisher (2011) comme celle de Holt et Bossler (2008) tentent de connaître les comportements de la personne susceptibles de la rendre vulnérable à une cybervictimisation.

Toutes les études traitant de harcèlement par les TIC mentionnent le sentiment de peur vécu par la victime ainsi que l'intention de l'agresseur de faire vivre ce sentiment à la victime. Safety Net Canada (2013) à l'instar de Dimond, Fiesler et Bruckman (2011) dressent un portrait plus spécifique de l'importance que prennent les TIC dans les situations de violence conjugale. Ces deux études font allusion à l'utilisation des TIC à mauvais escient et précisent comment cette utilisation impacte sur la vie des femmes qui en sont ordinairement les victimes.

NNEDV (2005) et par la suite Southworth et coll. (2007) dressent la liste des technologies de l'information et de la communication utilisées pour mener à bien le harcèlement. Pour chacune de ces technologies, des recherches en sciences forensiques (Forte et Donno, 2010; Al Mutawa, Baggili, Marrington, 2012; Graves, 2014; Horsman et Conniss, 2015; Turnbull et Randhawa, 2015) précisent quelles sont les informations qui pourraient être retirées des traces laissées par les comportements de cyberharcèlement sur l'appareil de la victime et sur celui de l'émetteur. Sans entrer dans le détail des différents processus d'extraction des données possibles, notons que des traces permettant de remonter à la source du harcèlement sont disponibles.

Holt et Bossler (2008) de même que Reyns, Henson et Fisher (2011) ont envisagé d'élargir l'utilisation de la théorie des opportunités et des activités routinières de Cohen et Felson (1978) pour expliquer les situations ou les éléments favorisant la victimisation. Ces deux études analysent le harcèlement vécu par les femmes via les TIC.

Nous proposons, dans le cadre du présent travail dirigé, une nouvelle mise à l'épreuve de la théorie de Cohen et Felson, en croisant des connaissances issues des sciences criminologique et forensique, et en les appliquant à un crime rarement exploré par cette théorie, soit le harcèlement criminel perpétré via les TIC en contexte de violence conjugale qui se perpétue au-delà de la séparation, conduisant la victime en maison d'hébergement.

Plus spécifiquement, nous cherchons à savoir comment le conjoint, « délinquant motivé », met à profit les possibilités qu'offrent les TIC pour mener à terme son harcèlement, visant la victime qui continue de constituer pour lui une « cible attrayante » malgré la séparation du couple. Finalement, nous cherchons à savoir si les maisons d'hébergement pour femmes victimes de violence conjugale et les forces policières pourraient agir à titre de « gardiens efficaces » dans ce type de crime. Ceci conduit à tracer le portrait des possibilités d'utilisation des traces numériques pour la constitution de la preuve de harcèlement criminel dans les situations de violence conjugale post séparation, étant entendu que celles-ci, aujourd'hui partie intégrante de la vie quotidienne de tout un chacun, peuvent servir à différentes fins tant pour l'agresseur : géolocaliser la victime, lui envoyer des messages hargneux, attaquer sa réputation en distribuant des images intimes; que pour la victime : rester en contact avec ses parents et amis, s'informer sur les ressources disponibles dans sa situation, etc.

## CHAPITRE 2 : MÉTHODOLOGIE

Ce chapitre présente la méthodologie utilisée pour traiter la problématique à l'étude. Il s'agit d'une étude qualitative au cours de laquelle neuf entretiens ont été effectués avec différents intervenants ayant pour les unes, les intervenantes en maison d'hébergement, une expertise sur la question de la violence conjugale, et pour les autres un avis d'expert sur les nouvelles technologies de la communication, les TIC, et leur utilisation, notamment en contexte de violence conjugale. La pertinence d'une approche qualitative, les modalités de sa réalisation pour la collecte et l'analyse des données, les considérations éthiques ainsi que les forces et limites de l'étude y sont présentées.

### 2.1 Une approche qualitative

Le devis de recherche retenu pour réaliser ce travail dirigé est résolument qualitatif. Comme Deslauriers et Kerisit (1997 : 88) le mentionnent : « une recherche qualitative de type exploratoire permet de se familiariser avec les gens et leurs préoccupations ». Étant donné la rareté des écrits (Holt et Bossler, 2008 ; Reyns, Henson et Fisher, 2011) sur la théorie des opportunités et des activités routinières appliquée aux cas de harcèlement criminel par les TIC, cette étude se démarque d'un point de vue méthodologique. La recension d'écrits a montré qu'aucune des études répertoriées ne s'intéresse à la mise à l'épreuve de la théorie de Cohen et Felson (1978) d'après un devis qualitatif. Cette étude exploratoire mènera à l'avancement des connaissances en ce qui a trait à l'utilisation des TIC permettant de commettre du harcèlement en contexte de violence conjugale, et plus précisément de violence conjugale post séparation.

L'échantillon visé par la recherche qualitative se distingue par son petit nombre compensé par la profondeur des informations recherchées (Pires, 1997). En effet, un petit échantillon permet l'exploration poussée d'expériences témoignées par les participants à l'étude. Le chercheur doit, pour ce faire, être en contact direct avec son terrain d'étude, que ce soit par le biais d'observations ou d'entretiens.

Dans le cas du présent travail dirigé, le but de la recherche est de mettre à l'épreuve la théorie des opportunités et des activités routinières de Cohen et Felson (1979) en l'appliquant à un crime rarement exploré par cette théorie, soit le harcèlement criminel perpétré via les TIC en contexte de violence conjugale qui se perpétue au-delà de la séparation conduisant la victime en maison d'hébergement.

C'est à l'aide d'entretiens qu'ont été recueillies les données permettant de dresser un portrait de la situation. Les entretiens permettent « *de rendre compte du point de vue des acteurs sociaux et d'en tenir compte pour comprendre et interpréter leurs réalités* » (Poupart, 1997 : 175). Cet instrument de collecte de données donne un accès privilégié aux expériences des individus. Ce moyen permet au chercheur de recueillir des informations auxquelles, sans la participation de l'interviewé, il n'aurait pas accès (Savoie-Zajc, 2009).

La conduite d'entretien permet à l'interviewé de donner sa conception de l'expérience vécue et d'aller en profondeur dans ses réponses (Noaks et Wincup, 2004), encouragé en cela par les relances de l'intervieweur. Étant donné le vide empirique entourant le sujet d'étude abordé dans ce travail dirigé, la conduite d'entretiens semi-dirigés permet de chercher l'information pertinente reposant sur l'expertise des interviewés, sans nécessairement connaître avec exactitude les questions à poser. L'entretien semi-directif a l'avantage, en collant à la réalité de l'interviewé et en le laissant élaborer sur un thème, largement introduit au départ de l'entrevue, pour lequel il est *expert* d'enrichir le schéma d'entretien élaboré par l'intervieweur à partir de ses connaissances théoriques du sujet (Fassin, 1990; Poupart, 1997).

## 2.2 La collecte de données

« *L'échantillon théorique vise surtout l'enracinement et le raffinement de la théorie en construction par le biais du développement et de la saturation des catégories* » (Paillé, 1994 : 178). L'échantillon de la présente étude vise trois domaines d'expertise qui sont finalement représentés par un professeur associé à l'École des sciences criminelles de Lausanne,

M. Jaquet-Chiffelle, spécialiste des traces numériques, quatre policiers experts de la constitution de la preuve en matière de harcèlement criminel, et quatre intervenantes en maison d'hébergement pour femmes victimes de violence conjugale, expertes de la question du harcèlement en contexte de violence conjugale post séparation. Parmi les quatre policiers interviewés, des organisations policières différentes sont représentées : deux d'entre eux travaillent pour le Service de police de la ville de Québec, un agit pour la Sûreté du Québec et le dernier fait partie du Service de police de la Ville de Montréal (SPVM). Leurs postes sont également différents ; il s'agit d'un sergent-spécialiste en cybercriminalité, un enquêteur criminel, une sergente détective et un lieutenant détective.

Contrairement à ce que préconisent Laperrière (1997) et Paillé (1994) concernant l'échantillonnage, la présente étude, à caractère exploratoire, ne vise pas la saturation empirique, mais une diversité de sources concernées.

Les entrevues effectuées ont été d'une durée de 60 minutes à plus de 120 minutes. L'échantillon s'est fait par tri expertisé (Anger, 1996), c'est-à-dire que les interviewés nous ont été référés compte tenu de leur expertise en traces numériques et/ou en violence conjugale. Des trois policiers recommandés, deux nous ont dirigée vers des policiers qu'ils jugeaient en mesure de répondre aux objectifs de cette recherche, l'un de ceux interviewés nous recommandant à son tour une de ses collègues plus spécialisées en violence conjugale. Les intervenantes œuvrant en maison d'hébergement, expertes en violence conjugale, ont été identifiées avec l'aide du réseau de chercheurs de Trajetvi, projet de recherche portant sur les trajectoires de violence conjugale et de recherche d'aide et de recours aux services des femmes victimes de violence conjugale en contexte de vulnérabilité (Trajetvi.ca).

Avec les deux policiers plus spécialisés en recherche de traces numériques, il a été question des possibilités d'enquête applicables en matière de harcèlement criminel, de l'utilisation des traces numériques pour la constitution de la preuve, et des limites légales de leur pouvoir. Avec la policière plus spécialisée en violence conjugale, des aspects victimologiques ont été plus spécialement abordés, à savoir : qu'est-ce qu'une femme victime doit faire pour pouvoir porter plainte et quelles sont les considérations légales à prendre en compte pour établir le harcèlement criminel.

Avec M. Jaquet-Chiffelle, professeur à l'École des sciences criminelles de l'Université de Lausanne, l'entretien a été d'une durée d'environ 75 minutes. Ce professeur a été choisi suite à notre participation à son cours *Cryptologie et Identités dans la société de l'information*. Lors de cette entrevue, la notion d'identité dans le monde virtuel a été abordée afin de connaître comment une identité retrouvée dans les traces numériques pouvait être associée à une personne. Les différentes traces permettant de relier la technologie à la personne ont été explicitées. L'utilisation des nouvelles technologies en maison d'hébergement a été discutée ainsi que les protections à mettre en place pour réduire les risques de géolocalisation des victimes de violence conjugale par le conjoint agresseur.



Finalement, quatre entrevues ont été effectuées avec des intervenantes en maison d'hébergement, membres du Regroupement des maisons d'hébergement pour femmes victimes de violence conjugale de trois villes différentes. Toutes les intervenantes interviewées avaient plus de huit ans d'expérience en intervention avec les femmes. Elles ont donc pu voir les changements qu'ont engendrés les nouvelles technologies dans la problématique de violence conjugale. Toutes les entrevues ont duré environ 90 minutes. Ces entrevues portaient sur l'impact des nouvelles technologies en maison d'hébergement pour savoir comment les TIC modifient l'expérience de victimisation des femmes et l'intervention auprès d'elles. La notion de harcèlement et la constitution de la preuve ont également été abordées afin de découvrir leurs connaissances et leurs pratiques en lien avec cet aspect de la loi.

### 2.3 Une analyse de contenu à visée descriptive

Tous les entretiens ont été transcrits intégralement par la chercheure, au fur et à mesure de leur réalisation, tel que le recommandent Rubin et Rubin (2005) et Savoie-Zajc (2009). La transcription permet, outre le fait de rendre intégralement compte des propos tenus par l'interviewé, de noter les silences, l'intonation de la voix et le non verbal apparus durant l'entretien, qui peuvent aussi être significatifs (Fontana et Frey, 2008 ; Savoie-Zajc, 2009).

Suite à la transcription, un résumé du contenu du verbatim a été fait, et une fiche d'information contenant le nom et le pseudonyme de l'interviewé, l'heure, la location, la durée de l'entretien ainsi que l'apport de cet entretien à la recherche a été remplie, tel que le recommandent Rubin et Rubin (2005).

À partir du résumé analytique de l'entretien, il convient d'identifier les concepts qui traduisent les idées importantes pour la recherche menée (Noaks et Wincup, 2004; Rubin et Rubin, 2005). Il s'agit, pour ce faire, de *fouiller* dans les données pour identifier les constances et variations dans les propos d'un interviewé et d'un interviewé à l'autre, ainsi que les thèmes pertinents à l'avancement des connaissances dans cette étude. Le chercheur doit associer un concept à chaque partie de texte analysé, en étant assez précis pour représenter exactement l'unité de sens des segments participant à définir le concept, et à la fois assez général pour pouvoir inclure plusieurs unités de sens sous un même concept (Noaks et Wincup, 2004; Baribeau, 2009 ; Rubin et Rubin, 2009 ; Packer, 2011).

Le choix des codes conceptuels associés aux mots utilisés par l'interviewé s'avère être un choix subjectif du chercheur. Certains considèrent que cette étape d'analyse constitue le passage entre des informations de tous les jours à de l'information à des fins théoriques. La rigueur est alors évidemment de mise, pour atteindre une certaine objectivité scientifique se reflétant dans les choix du chercheur, que ce soit pour les codes, ou pour les citations considérées comme importantes (Arksey et Knight, 1999; Rubin et Rubin, 2005; Baribeau, 2009; Packer, 2011).

Après avoir codifié les unités de sens précisément, on vise à regrouper ces codes sous des catégories plus larges, établissant ainsi des liens entre les différents codes. Selon Baribeau (2009 : 141) : « *il convient de définir avec le plus de rigueur possible des catégories (conceptuelles) sous lesquelles les différents codes (donc les données) seront regroupés* ».

Le va-et-vient constant entre le résumé, la codification, la catégorisation et la théorie est primordial pour établir les catégories, tant dans l'analyse verticale d'un entretien qu'à l'analyse transversale du corpus de données (Arksey et Knight, 1999; Blais et Martineau, 2006). Il s'agit de sortir du contexte des unités de sens pour les recontextualiser dans un procédé regroupant toutes les unités de sens sous la même catégorie (Arksey et Knight, 1999; Rubin et Rubin, 2005; Baribeau, 2009). À mesure que les entretiens s'accumulent, des catégories peuvent être ajoutées et d'autres éliminées pour finir avec seulement quelques grandes catégories permettant d'inclure, en l'organisant, la plus grande partie des informations relatives au sujet de recherche. Dans cette procédure, des liens sont faits à l'intérieur de chaque catégorie, mais également entre les grandes catégories, formant tranquillement la théorisation de l'entretien. L'analyse de contenu ainsi réalisée mise sur la codification et la création de catégories conceptuelles pour faire sens des données recueillies sur le terrain (Arksey et Knight, 1999 ; Rubin et Rubin, 2005 ; Baribeau, 2009; Savoie-Zajc, 2009; Packer, 2011). L'utilisation de citations pour rendre compte de l'analyse est employée pour permettre au lecteur d'avoir accès aux données permettant au chercheur de faire les liens qui lui sont présentés.

C'est essentiellement cette procédure d'analyse des données qui a été appliquée dans la réalisation de notre travail dirigé.

## 2.4 Considérations éthiques

Avant la tenue des entretiens, tous les participants ont signé un formulaire de consentement confirmant leur participation libre et éclairée à la présente étude (Annexe 1). Tous les participants sont majeurs. Leur participation à l'étude consiste à accorder une entrevue semi-dirigée d'une durée d'environ une heure sur la violence conjugale et les nouvelles technologies. Les entrevues ont été enregistrées, avec l'accord des participants afin de permettre l'écoute active durant les entrevues et faciliter la transcription des propos des interviewés en respectant intégralement leur contenu.

Les enregistrements et les verbatim ont été conservés dans un endroit auquel seules la directrice de recherche et l'étudiante réalisant l'étude avaient accès. Le nom des intervenantes, des maisons ainsi que les villes où sont situées les maisons d'hébergement ont été anonymisées. Le but de l'étude est de dresser un portrait de l'impact des nouvelles technologies sur l'événement de harcèlement en contexte de violence conjugale post séparation et sur leurs répercussions sur l'intervention en maison d'hébergement, et non d'évaluer la situation dans une maison spécifique, c'est pourquoi le nom des maisons d'hébergement ne sera pas divulgué. Les experts, pour leur part, n'ont pas expressément souhaité que leur nom soit tu.

Étant donné les fonctions des personnes interviewées, tous des professionnels dans le domaine de la violence conjugale ou des services de police et un chercheur, il a été évalué qu'il n'y avait pas de risques psychologiques ou autres à participer aux entretiens réalisés pour cette étude. Ceux-ci participent volontairement à l'étude et ne sont pas rémunérés pour le faire.

Finalement, sur ces bases, le protocole de recherche a reçu l'approbation du Comité d'éthique à la recherche de l'Université de Montréal (voir copie du certificat à l'annexe 2).

## 2.5 Forces et limites de la démarche

La force associée aux entretiens semi-directifs permet au chercheur d'aborder des sujets qui sont utiles pour l'avancement de son étude tout en laissant à l'interviewé la liberté de mettre l'accent sur les aspects qu'il juge importants. Une telle approche est particulièrement indiquée lorsque le sujet traité est méconnu et faisant que la formulation de questions précises s'en trouve compliquée, voire empêchée.

Plusieurs auteurs misent sur la saturation des données pour avoir le portrait le plus représentatif du phénomène social étudié. Or, le travail dirigé ne permet pas d'atteindre la saturation empirique, étant donné le court le délai de production qui lui est imparti. Toutefois, rigueur étant de mise, l'analyse des données visera à s'approcher le plus possible du modèle théorique prôné de manière à mettre en valeur, le mieux et le plus justement possible les données recueillies. Il ne faudra toutefois pas perdre de vue qu'il s'agit d'un travail exploratoire.

Le terrain de recherche pour cette étude a été fait en deux temps : les intervenantes et M. Jaquet-Chiffelle ont été rencontrés durant l'année 2015 et les policiers au printemps 2016. Le projet a changé partiellement entre les deux périodes de cueillette de données. Les premiers intervenants ont été consultés sur l'impact des nouvelles technologies en violence conjugale, pas seulement sur le harcèlement fait par les TIC. Le sujet avait tout de même été abordé dans les premières entrevues, mais pas aussi en profondeur qu'avec les policiers.

Il aurait été pertinent de rencontrer des femmes qui ont été victimes de harcèlement criminel par les TIC de la part de leur conjoint. Mais l'inclusion de cette catégorie d'acteurs demande des précautions éthiques et des démarches de recrutement que ne permettait pas le cadre relativement restreint du travail dirigé.

Des entretiens avec des procureurs de la Couronne auraient ajouté une valeur significative à ce travail, notamment pour préciser la notion de « gardien » en regard de la problématique à l'étude, mais étant donné encore ici le cadre restreint réservé à la production de ce travail, nous n'avons pas sollicité ces intervenants. Reste qu'il serait intéressant, dans le futur, de rencontrer des procureurs et même des juges afin de compléter le travail entrepris.

Enfin, les nouvelles technologies étant constamment en évolution, il se peut que les TIC abordées, leur usage et les traces numériques qui leur sont associées soient obsolètes dans quelques années. Malgré cette limite, cette étude permet de conscientiser à l'utilisation des nouvelles technologies dans l'action de harcèlement. Et quoi qu'il en soit de l'avenir, l'information actuelle permet de renseigner les intervenantes en maison d'hébergement et les femmes victimes de violence conjugale des possibilités d'utilisation des technologies susceptibles de les mettre en danger : géolocalisation, utilisation de logiciels espions, dénigrement via les réseaux sociaux, menaces via les outils électroniques de communication qui les mettent en danger... mais aussi des possibilités qu'offrent les TIC pour la constitution de la preuve, notamment de harcèlement, qui pourraient servir leur objectif de sortir de la situation de violence qui les affecte.

Malgré les limites qui marquent la réalisation de ce travail, celui-ci répond à un besoin des maisons d'hébergement. Suite à la production de ce travail dirigé, nous souhaitons produire des fiches d'informations pour les intervenantes et les femmes en maison d'hébergement sur les dangers des TIC, les moyens de se protéger et la possibilité de tourner la situation à l'avantage des femmes en utilisant les TIC pour recueillir la preuve des gestes posés et établir la provenance de ceux-ci.

Voyons maintenant ce qu'il en est à la lumière des données que nous avons recueillies et analysées.

## CHAPITRE 3 : RÉSULTATS

L'analyse des neuf entretiens effectués dans le cadre de ce travail dirigé a été réalisée en tenant compte des concepts centraux de la théorie des opportunités et des activités routinières de Cohen et Felson (1978), à savoir : la rencontre d'un délinquant motivé, d'une cible attrayante et de l'absence d'un gardien efficace. Globalement, il s'agit de répondre à l'objectif général qui consiste à adapter la théorie des opportunités et des activités routinières de Cohen et Felson à un crime rarement traité par cette théorie, soit le harcèlement criminel perpétré par les TIC, et ce, encore plus spécifiquement dans le contexte d'une relation de violence conjugale post séparation ayant en outre la particularité d'amener les femmes en maison d'hébergement afin d'assurer leur sécurité. Avant toute chose, il importe de préciser ce qu'est le harcèlement criminel et comment il est vécu dans une situation de violence conjugale post-séparation, afin de saisir les particularités de ce crime, pour les différents acteurs rencontrés dans le cadre de ce travail, au-delà de la définition juridique que nous avons vue dans la recension d'écrits.

### 3.1 Le harcèlement criminel : entre la prescription de la loi et la perception des intervenants

Ce sont avant tout les intervenantes des maisons d'hébergement qui se disent concernées par la question du harcèlement via les TIC. Toutes s'entendent pour dire que la préoccupation pour le harcèlement est très présente en maison d'hébergement. Selon elles, le harcèlement est vécu par la majorité des femmes hébergées, par le biais « *de textos, de messages harcelants, des menaces, des choses comme ça* » émis par le conjoint (Valérie, intervenante en maison d'hébergement).

Il ressort clairement des entrevues que le harcèlement fait maintenant partie du quotidien non seulement des femmes en maison d'hébergement, mais également des intervenantes qui en sont témoins :

*Le harcèlement, j'ai envie de te dire c'est un quotidien, c'est réellement un quotidien* (Marie, intervenante en maison d'hébergement).

D'après la Sergente détective du Service de police de la ville de Québec participant à l'étude, pour pouvoir accuser quelqu'un de harcèlement criminel, il faut d'abord que la personne sache qu'elle harcèle :

*Le harcèlement commence à partir du moment où la victime lui dit qu'elle ne veut plus entrer en contact avec lui, qu'elle ne veut plus rien savoir de lui.*

La policière précise à cet égard que le harcèlement criminel n'est pas un crime facile à identifier, car l'infraction est basée sur le sentiment de crainte produit chez la victime. Or, le sentiment de peur n'est pas un critère facile à déterminer et, surtout, varie d'une personne à l'autre, poursuit-elle. C'est exactement ce qu'avance, également, le Sergent spécialiste en cybersurveillance de la Sureté du Québec (SQ) interviewé :

*Le harcèlement c'est vraiment des propos qui sont tenus, qui sont répétés ou non, qui font craindre pour la sécurité. Qu'est-ce qui, toi, te fais craindre pour ta sécurité pis qu'est-ce que moi, ce n'est probablement pas la même chose. Donc c'est là que c'est une question de perception.*

Le défi est ainsi de prouver hors de tous doutes raisonnables que le conjoint avait l'intention coupable, le *mens rea*, de créer de la crainte chez la victime, signalent les policiers interviewés.

Le contexte est également important pour établir l'infraction de harcèlement criminel. Des menaces, qui en regard de la loi n'en sont pas, peuvent le devenir dépendamment du contexte. Par exemple, explique la sergente détective de la Police de Québec :

*Tu ne reverras pas les enfants! Ce n'est pas une menace...*

parce qu'il peut y avoir plusieurs interprétations possibles : peut-être que le conjoint signifie simplement qu'il va réclamer la garde exclusive des enfants.

*Par contre, la personne dirait : « tu ne reverras plus les enfants », mais admettons qu'il parle de suicide avant : « je m'en vais me suicider pis tu ne reverras plus les enfants », là c'est un contexte différent*

et ça pourrait devenir une menace réelle. Le lieutenant détective du SPVM renchérit en ce sens :

*tout ce qui ne constitue pas nécessairement une menace, mais qui fait en sorte que la personne sent que sa sécurité est compromise [...] va entrer dans l'infraction de harcèlement criminel.*

Le contenu et la fréquence des messages ou courriels sont également des éléments importants, mentionnés par les interviewés pour l'identification de la présence de harcèlement criminel. Des messages anodins, à la suite d'une demande explicite d'arrêter de contacter la victime, formulée à une fréquence élevée sans avoir l'effet escompté peut constituer du harcèlement, au même titre que des menaces claires répétées seulement quelques fois peuvent en constituer également, estiment les répondants.

C'est notamment dû à tous ces éléments qui, de leur point de vue, constituent l'infraction de harcèlement criminel, que tous les policiers rencontrés ne pouvaient dresser un portrait général des cas de harcèlement qui leur sont rapportés : c'est « *vraiment du cas par cas* » constate le sergent spécialiste en cybersurveillance de la SQ. Le contexte entourant l'évènement a beaucoup d'importance dans l'établissement de cette infraction, car, précise cet intervenant, le harcèlement c'est un processus qui se dessine à partir d'un ensemble d'événements. Plusieurs infractions mineures prises individuellement peuvent paraître inoffensives, indique-t-il, mais lorsqu'elles sont considérées ensemble, on voit bien l'escalade de la violence. Il l'illustre dans l'exemple suivant :

*Aujourd'hui, il est venu à mon lieu de travail, il a tourné autour du bâtiment, il m'a regardé droit dans les yeux et il est reparti... C'est anodin, mais dans un mois s'il commence à aller briser des fenêtres, ça, ce n'est pas anodin. Ça montre une gradation de la violence.*

Le manque de précision dans la définition du harcèlement, la subjectivité qui s'y rattache peut contribuer, d'une certaine façon, à l'absence de gardien efficace face à ce crime, dans la mesure où un certain arbitraire paraît présider à sa reconnaissance. Le responsable du harcèlement peut ainsi se dire qu'il est possible de faire valoir qu'il « n'avait pas l'impression » que son comportement pouvait faire naître la peur chez la victime. S'il arrive à faire valoir l'absence de *mens rea*, il pourra du même coup contester la matérialité du crime. C'est là un avis partagé par l'ensemble des intervenants rencontrés.

Les intervenantes en maison d'hébergement comme les policiers soutiennent néanmoins que le harcèlement peut être utilisé comme outil de contrôle de la part du conjoint.



*Les harceleurs vont laisser planer des doutes [...] pour terroriser les victimes, parce que c'est ça leur pouvoir, c'est ça leur emprise (Lieutenant-détective du SPVM)*

Leur emprise peut ainsi se perpétuer même lorsque la victime se trouve en maison d'hébergement, notamment par le recours aux technologies de la communication (TIC).

L'accessibilité aux femmes via leur téléphone ou leur ordinateur s'avère dès lors une préoccupation dominante pour les intervenantes qui ne savent pas comment intervenir par rapport à l'entrée de ces technologies en maison d'hébergement. La citation qui suit illustre bien les préoccupations qui marquent le quotidien des intervenantes en maison d'hébergement :

*Ce qui est inquiétant, c'est qu'elle est joignable tout le temps. [...] Tsé, avant, quand tu voulais prendre du recul face à ta situation pis que tu n'étais pas convaincue, ce n'était même pas clair si tu voulais te séparer ou pas, ben tu venais en maison d'hébergement pis tu pouvais avoir la paix. Pis si tu voulais avoir un contact avec lui, ben tu n'avais qu'à lui donner le numéro de téléphone. Parce que les femmes hébergées ont leur téléphone, asteure, justement, tout le monde a son téléphone, faque le gars il l'a le téléphone de sa blonde ou il la texte ou il lui envoie un courriel. Ça, c'est préoccupant, pis c'est achalant. C'est achalant de voir que, c'est ça, t'es tout le temps, tout le temps joignable, en pleine nuit, en plein jour, n'importe où, n'importe quand. Ça l'emprise pis le contrôle c'est l'extension de ça. (Édith, intervenante en maison d'hébergement)*

### 3.2 La difficulté de faire la preuve du harcèlement par les TIC

Si les interviewés s'entendent sur la difficulté de saisir la présence du harcèlement par les TIC, ils sont encore plus clairs quant à la difficulté de « prouver » que le conjoint utilise les TIC à la disposition de la victime à des fins de harcèlement. Ainsi, pour le sergent spécialiste en cybersurveillance de la SQ, la difficulté :

*Ce n'est pas au niveau technologique ou de compréhension, c'est vraiment la perception. De démontrer qu'il y a un acte pis après ça, il faut être convaincu qu'on peut le montrer à la cour.*

C'est en effet au procureur de la Couronne d'établir s'il y a suffisamment de contenu pour être capable de prouver hors de tous doutes qu'il y a eu harcèlement criminel. Étant donnée la subjectivité de l'article de loi définissant le harcèlement criminel, introduit par l'élément « faire craindre », les intervenants rencontrés dans le cadre de cette étude estiment que sur dix procureurs il se peut que cinq acceptent de retenir le chef d'accusation alors que les cinq autres ne pensent pas pouvoir faire la démonstration qu'il y a eu du harcèlement ; encore ici, c'est vraiment du cas par cas, concluent-ils. Ceci étant, il s'avère que les policiers doivent affiner leur enquête en vue de permettre au procureur de convaincre le juge de l'infraction commise. D'après le lieutenant détective du SPVM :

*c'est difficile d'avoir des condamnations parce que les exigences des tribunaux sont très élevées envers le travail des policiers, envers le travail de la Couronne aussi. De susciter, de soulever un doute raisonnable c'est... ce n'est pas le même fardeau ce que nous on a, de prouver hors de tous doutes.*

Les intervenantes en maison d'hébergement mentionnent que les victimes sont conscientes du fardeau de la preuve et qu'il y a une grande possibilité que la cause ne se rende même pas à la cour, ou encore qu'il n'y aura pas de condamnation à l'issue de la cause. C'est un processus éprouvant pour les victimes qui, dans bien des cas, ont peur de ne pas être crues.

La recherche de la corroboration de leurs dires paraît confirmer leur crainte et peut être vécue par les victimes comme une marque que les policiers ne les croient pas et que c'est pour ça qu'ils doivent trouver le moyen de confirmer tout ce qu'elles disent. Or, soutiennent les policiers rencontrés, en cherchant à corroborer les différents éléments de preuve qu'allègue la victime, ils ont plutôt pour but de la soutenir dans le processus et de l'accompagner à la cour pour supporter ses dires. Les policiers mentionnent à cet égard qu'ils ont souvent un travail important à faire pour rassurer la victime au sujet de sa sécurité et sur le processus judiciaire par lequel elle passera. L'un d'eux l'exprime bien :

*(la victime) peut avoir l'impression que c'est son problème, pis qu'elle n'y arrivera jamais, mais ce n'est pas vrai : il y a un paquet d'intervenants qui sont autour pour s'assurer qu'elle sorte finalement du cycle de la violence et qu'elle mette ça en arrière d'elle, et que la personne qui a commis ces gestes-là soit encadrée pis que ça se termine. Faque ça, aussi, on a un travail à faire de rassurer les gens... pis tsé, personne ne peut garantir les résultats à la cour, pas l'enquêteur, pas le procureur non plus. On peut juste garantir qu'on va faire notre travail du début à la fin pour s'assurer qu'à la fin de la journée que ça arrête. Parce que souvent c'est la seule chose que la victime veut; que ça arrête, un, pis qu'il y aille des conséquences pour le tort qu'elle a subi (Lieutenant détective, SPVM).*

À la lumière des résultats précédemment présentés, on comprend la complexité d'appliquer l'article de loi définissant le harcèlement criminel, se traduisant par la complexité de prouver hors de tout doute la culpabilité du conjoint. Par ailleurs, différents gestes à caractère criminel peuvent être commis dans un but de harcèlement. C'est notamment le cas de la diffusion de virus informatique et du piratage informatique qui s'avèrent être punissables par le Code criminel canadien sous l'article 52, traitant du sabotage. Dépendamment de l'utilisation qui en est faite, d'autres infractions concernant les données pourraient être associées au harcèlement. Si des données sont effacées ou perdues par la personne à l'origine de l'installation d'un virus ou d'un logiciel espion visant à connaître – voire à contrôler – la vie de la victime, elle peut être accusée de méfaits concernant des données (art. 430 (11)). Si le logiciel permet l'interception de communications privées, le suspect pourrait être accusé en vertu de l'article 184, qui définit cette infraction.

Le vol d'identité et la fraude à l'identité (art. 402 et 403) sont également punissables en droit criminel canadien. L'identité usurpée peut, entre autres, être utilisée dans le but de commettre du harcèlement, sous le couvert d'une identité volée.

Dans tous les cas si le harcèlement ne peut être prouvé hors de tout doute, à tout le moins les infractions mentionnées y étant associées pourront donner lieu à une poursuite pénale.

La distribution d'images intimes, qui peut se traduire comme une forme de harcèlement, est aussi désormais illégale. Le nouvel article 162.1 du Code criminel canadien donne plus de pouvoir aux policiers dans les cas de publication non consensuelle d'une image intime.

Le fait de distribuer une image intime d'une personne majeure, sans son consentement, même si celle-ci a été prise volontairement durant la relation, devient maintenant un crime passible de cinq ans de prison. Des moyens peuvent être pris en réponse à une ordonnance d'un juge pour que soient effacées ces photos. Il importe toutefois de signifier rapidement aux policiers que le conjoint a des photos intimes en sa possession pour limiter, le plus possible, les dégâts. Il y a encore là un moyen de traduire le harcèlement devant les tribunaux, lorsqu'il est ainsi produit.

La possibilité d'accuser le conjoint pour des crimes supportant le cyber harcèlement permet, au moins, d'avoir d'autres éléments d'accusation si le procureur considère que les éléments de harcèlement criminel, en tant que tel, ne sont pas assez concluants pour être portés devant la cour criminelle. Il faut se rappeler que le harcèlement se réalise à partir de différentes tactiques et que, parmi ces tactiques, certaines constituent désormais des crimes prévus au Code criminel.

Maintenant que le concept de harcèlement criminel, et plus spécialement la difficulté d'en faire la preuve en droit, est établi, les prochaines sections viseront plutôt à cerner comment peut s'appliquer la théorie des opportunités et activités routinières de Cohen et Felson au comportement de harcèlement par les TIC dans un contexte de violence conjugale post-séparation.

### 3.3 Les TIC au service du délinquant motivé

Selon la théorie des opportunités et activités routinières de Cohen et Felson (1979), le premier élément nécessaire à la commission d'une infraction est la présence d'un délinquant motivé qui doit voir un intérêt à poser le geste sanctionné – dans ce cas-ci le harcèlement criminel – et posséder un minimum de compétences pour le réaliser.

Rappelons ici la définition de contrôle coercitif caractérisant la situation de violence conjugale établie par Johnson (2014) et Stark (2014) comme étant l'utilisation de diverses formes de violences dans le but d'exercer sur la victime un contrôle total et sa domination à long terme. Dans la situation qui nous importe, le délinquant est motivé par des ambitions d'exercer un tel contrôle sur sa conjointe et les TIC lui fournissent l'opportunité d'y parvenir, moyennant un minimum de compétence, par différentes formes de harcèlement se perpétuant en contexte post-séparation.

Les victimes savent que le moment de la rupture est des plus dangereux pour elles et les enfants, car le conjoint violent « *perd alors le contrôle absolu* » (Valérie). Les conjoints actuels peuvent être très harcelants quand les femmes sont en maison d'hébergement, mais les intervenantes sont aussi confrontées à du harcèlement fait par les ex-conjoints. Pascale, intervenante en maison d'hébergement, mentionne que :

*les conjoints peuvent être très harcelants ici [...] pis des fois c'est ça : « là ça n'arrête plus, il me texte sans arrêt, il est harcelant, je reçois 20 messages par soirées de lui ». Moi je pense que c'est beaucoup plus avec des ex-conjoints.*

Les policiers ont tous mentionné que la majorité des cas de harcèlement pour lesquels ils reçoivent des plaintes sont perpétrés par des ex-conjoints. Ils sont conscientisés à l'escalade de la violence dans ces cas et vont intervenir le plus rapidement possible pour éviter que la plainte de harcèlement en devienne une de voies de faits ou d'homicide. D'après le Sergent spécialiste en cybercriminalité de la SQ :

*Les enquêteurs sont sensibilisés à ça parce qu'on en a vu tellement d'intrafamiliales que maintenant personne ne veut qu'un de ses dossiers tourne de même.*

Le lieutenant détective du SPVM s'exprime dans le même sens en précisant que :

*Ce sont des politiques qui ont évolué avec le temps et qui ont une prise en charge vraiment très rapide [...] à cause de la situation et, malheureusement, des drames qui sont arrivés dans le passé.*

La priorité des policiers est, à ce moment, avant tout de s'assurer de la sécurité de la victime, de lui trouver un endroit sécuritaire, que ce soit chez des partenaires tels les maisons d'hébergement ou chez des personnes de son entourage, le temps qu'ils localisent le suspect pour l'arrêter.

Chacune des intervenantes participant à l'étude a été mise au courant de situations où le conjoint utilisait le compte ou le cellulaire des enfants pour passer des messages à la victime. Dans un cas, le harcèlement se faisait via le cahier de communication de l'enfant en garde partagée. Bien que *le cahier* ne constitue pas une avancée technologique, cela montre bien comment le conjoint peut se servir de tous les moyens de communication à sa disposition pour entrer en contact avec sa conjointe.

La géolocalisation des femmes en maison d'hébergement par leur conjoint ou ex-conjoint est une possibilité mentionnée par deux intervenantes et deux policiers ayant eu à intervenir en situation de violence conjugale. Les deux policiers de la ville de Québec ont, en effet, témoigné qu'un homme s'était présenté à la maison d'hébergement où sa conjointe était hébergée, sachant pertinemment qu'elle s'y trouvait. Il avait réussi à la localiser grâce à une application gratuite accessible lorsque deux cellulaires sont achetés ensemble. La victime qui avait fermé son cellulaire, l'a ouvert une minute dans la maison pour vérifier ses courriels, et c'est à ce moment que sa position dans la maison a été révélée au conjoint. Il s'est alors présenté à la maison d'hébergement venant chercher sa conjointe qui avait quitté la situation conjugale violente et s'y était réfugiée.

D'après le professeur Jaquet-Chiffelle, « *quand on connaît très bien une personne c'est beaucoup plus facile de l'infecter* » avec un logiciel espion. La personne visée peut être infectée en pensant ouvrir un courriel d'une amie, par exemple, alors qu'en réalité c'est le conjoint qui a utilisé un service d'installation de logiciel espion passant par un courriel envoyé en se faisant passer pour l'amie et infectant l'appareil de la victime à l'ouverture du courriel. Par la suite, plusieurs informations peuvent être recueillies par la personne ayant utilisé le service de logiciel espion qui pourrait même permettre d'enclencher la caméra et le micro de l'appareil, enregistrer les mots de passe de tous ses comptes, rouvrir l'appareil, activer la localisation sur l'appareil; tout ça sans que la victime ne s'en rende compte.

C'est pourquoi les policiers et le professeur de l'École des sciences criminelles recommandent de non seulement fermer le cellulaire, mais même d'en enlever la batterie, lorsque celui-ci n'est pas utilisé. D'après les policiers interviewés, l'utilisation de logiciels espions a été répertoriée dans peu de cas, mais :

*on est appelé à en avoir, je pense, plus parce que c'est plus disponible, tu peux trouver ça facilement* » (Sergent spécialiste en cybersurveillance de la SQ).

Dans certains cas, la femme ne désire pas inquiéter son entourage en dévoilant la situation de violence qu'elle vit, mais la révélation peut venir du conjoint qui contacte la famille à différentes fins, comme dans le cas rapporté par Valérie, une des intervenantes rencontrées, où le conjoint a contacté la famille en prétendant :

*qu'elle a kidnappé son enfant pis que maintenant ils vont [l]'amener en prison. Donc il menace la famille pour que la famille fasse pression sur la femme pour qu'elle retourne avec lui et ramène les enfants.*

Les intervenantes mentionnent également que les réseaux sociaux permettent beaucoup plus facilement « *de faire une campagne de salissage avec un impact plus large* » (Pascale, intervenante en maison d'hébergement), que ce soit par la distribution d'images intimes ou la publication de commentaires haineux par le conjoint, par la création de faux profils dénigrant la conjointe, ou encore le piratage de ses comptes. Dans tous les cas, les conséquences peuvent être très dévastatrices : en plus de salir la réputation de la femme, les conjoints savent très bien qu'une fois que « *c'est parti sur le web, on ne peut plus l'enlever* » (lieutenant détective du SPVM) et ça devient hors de contrôle.

Les TIC serviront donc le dessein du délinquant motivé à s'assurer le contrôle de sa conjointe par le truchement du harcèlement criminel, malgré les démarches entreprises par celle-ci pour assurer sa sécurité en quittant, en premier lieu, le domicile conjugal.

### 3.4 La conjointe « rebelle » : une cible attrayante

Nous avons eu l'occasion de le mentionner, dans les situations de violence conjugale, le conjoint souhaite exercer sa domination sur sa compagne de vie de différentes façons, notamment en se livrant au harcèlement. Ainsi, la conjointe se retrouve dans la position de cible attrayante. Le conjoint ne cherche pas à atteindre n'importe qui par son harcèlement, au contraire, il connaît très bien sa victime et le fait dans un but précis : assurer un contrôle absolu sur cette personne. Les diverses tactiques utilisées telles l'imposition de règles, l'isolement, l'humiliation et autres, pour assouvir son emprise sur celle-ci, contribuent à la rendre de plus en plus vulnérable.

Toutes les intervenantes observent des conséquences liées à l'utilisation des TIC en maison d'hébergement. Selon elles, le cycle de violence continue à s'exercer via les technologies à travers lesquelles le conjoint, dans un premier temps, exprime son repentir faisant passer assez rapidement les femmes au stade de la « lune de miel » du cycle de la violence. Encouragées par les messages contrits que leur adresse leur conjoint, ces femmes gardent espoir que celui-ci a changé et qu'il ne recommencera plus. Le contexte émotif entourant la violence conjugale rend la victime très vulnérable à la réception de ces messages.

Émotivement déstabilisée suite à la sortie du milieu violent, le contrôle exercé, durant souvent des années, rend la victime facilement manipulable par le conjoint. Avant l'avènement des TIC, les femmes arrivaient en maison d'hébergement suite à la phase d'agression, elles avaient le temps de prendre du recul sur leur situation et de penser par elle-même pour elle-même. Maintenant, c'est différent, raconte Valérie, intervenante en maison d'hébergement :

*Pendant l'hébergement, il n'y a pas d'agression directe, mais il y a la lune de miel qui s'installe : « je t'aime, je m'ennuie de toi », tu as 1000 messages, même si la femme ne répond pas, elle ne peut pas s'empêcher d'aller voir les messages, donc souvent ce que ça fait, c'est qu'elle tombe en lune de miel plus vite.*

Pascale, une autre répondante en maison d'hébergement, mentionne qu'il est d'autant plus difficile d'intervenir en regard du contenu des messages suscitant et entretenant la phase de lune de miel, qu'« elles ont tellement envie d'y croire » :

Plusieurs fois, racontent les intervenantes en maison d'hébergement, elles ont vu des situations changer drastiquement après que la femme ait vu sur Internet que son conjoint fréquentait une autre femme pendant qu'elle était en maison d'hébergement. Marie témoigne :

*J'ai vu des situations virer bout pour bout où la femme voulait vraiment partir; c'était terminé pis là oups! Il est question d'une autre femme, il y a des photos avec une autre femme tous ses objectifs et tout son senti est centré complètement sur autre chose.*

Les intervenantes mentionnent toutes que l'accessibilité des femmes via les TIC vient souvent contrecarrer l'intervention faite en maison d'hébergement, les faisant reculer de quelques pas. Elles témoignent d'une situation fréquente en intervention:

*On fait quelques pas, oups! Elle reçoit des textos toute la nuit, ben là on recule un peu, au niveau de la démarche*

Certaines mentionnent que les femmes qui ne sont pas capables de se détacher de leur téléphone ou de leur ordinateur vont nécessiter plus de temps d'intervention pour avancer dans leurs démarches que les femmes qui sont capables de mettre un frein à tous contacts avec le conjoint. Par ailleurs, les femmes en maison d'hébergement vont elles-mêmes utiliser les TIC afin de garder ou établir un contact avec leur entourage.



Le fait de rebâtir des liens avec un entourage soutenant aide au cheminement de la femme soutiennent notamment Dimons, Fiesler et Bruckman (2011). En contrepartie, rester connecté à son réseau ou en utilisant les TIC à d'autres fins, notamment le magasinage en ligne, la rend vulnérable à l'infiltration de logiciels espions, à la géolocalisation, et à la réception d'appels et de messages harcelants de la part du conjoint, indiquent les policiers rencontrés dans le cadre de notre étude. De plus en plus, les maisons d'hébergement sont conscientisées aux risques que représentent les TIC dans ce contexte. C'est à ce point, avec l'éducation et la conscientisation concernant les risques engendrés par le TIC, que les maisons d'hébergement pourraient se poser en gardien efficace agissant auprès de la cible attrayante.

### 3.5 L'intervention d'un gardien efficace

Cohen et Felson (1979), on l'a vu, mentionnent que pour qu'un crime ait lieu, il faut un délinquant motivé compétent, une cible attrayante ou vulnérable ainsi que l'absence de gardien efficace. La présence d'une cible attrayante et l'absence d'un gardien efficace sont deux éléments interdépendants, prétendent les auteurs; ainsi, en agissant sur l'un ou l'autre, on réduit les risques de commission d'un acte criminel en créant une plus grande difficulté pour le délinquant motivé de mener à terme la commission du crime. Dans la situation qui nous intéresse dans ce travail dirigé, deux institutions pourraient agir à titre de gardien efficace : les maisons d'hébergement pour femmes et enfants victimes de violence conjugale et les corps policiers menant l'enquête criminelle. Voyons comment.

#### 3.5.1 *Les maisons d'hébergement*

Les maisons d'hébergement viennent en aide aux femmes victimes de violence conjugale qui, en situation d'urgence, cherchent à se mettre à l'abri en quittant le milieu violent. On l'a déjà mentionné, les femmes arrivent en maison d'hébergement avec leur attirail électronique (téléphone intelligent, tablette) et leurs différents accès aux TIC (compte de messagerie courriel, compte Facebook, Instagram...), ces éléments faisant maintenant partie des éléments de base, d'utilité courante, desquels une grande portion - sinon la plus grande - de la population ne saurait plus se passer. C'est alors l'occasion de les conscientiser aux risques des TIC, d'un côté, et à leur utilité pour la constitution de la preuve des violences subies, en particulier sous forme de harcèlement, d'un autre côté.

Toutes les maisons d'hébergement ont des *modes d'emploi* à suivre concernant les nouvelles technologies. Toutefois, les dispositions concernant les nouvelles technologies sont à la discrétion de la maison. Certaines ont un téléphone fixe qu'elles mettent à la disposition des femmes hébergées, leur permettant de communiquer avec l'extérieur sans utiliser leur propre appareil, alors que d'autres n'en ont pas. Il est de même pour les postes d'ordinateurs fixes et le Wi-Fi.

Dans tous les cas, la réglementation mise en place concernant les TIC dans les maisons d'hébergement l'est dans le meilleur intérêt des femmes et enfants hébergés, indiquent les intervenantes participant à cette étude. Les maisons mettent en place ces dispositions dans le but de les protéger étant donné la situation particulière qu'elles vivent, précisent-elles.

Plus globalement, toutes les intervenantes disent s'efforcer de conscientiser clairement les femmes sur les dangers reliés à l'utilisation des TIC, mais il semble que les femmes ne voient pas toutes ou toujours le réel danger lié à leur situation.

Dans la majorité des cas, les maisons d'hébergement demandent que la fonction donnant accès à la localisation soit désactivée à l'arrivée de la victime. Toutefois, il ne s'agit pas là d'une pratique systématiquement ni uniformément contrôlée; c'est à la discrétion de chaque intervenante qui accueille la victime d'y voir. Aussi, lors des allers et venues des femmes à l'extérieur de la maison, durant leur séjour, la localisation pourrait être réactivée sans que cette possibilité ne soit vérifiée au retour à la maison. Enfin, les appareils à l'usage des enfants sont souvent oubliés dans les procédures de contrôle.

Dans la majorité des maisons d'hébergement, la prise de photos et de vidéos ainsi que leur publication sur les réseaux sociaux est fortement découragée. Les femmes sont incitées à faire circuler uniquement les photos où l'on ne peut pas voir les autres personnes présentes dans la maison pour éviter que soient identifiés les femmes et les enfants hébergés, ou encore les membres du personnel qui pourraient être l'objet de menace. Les intervenantes demandent également aux femmes de ne pas prendre de photos près des fenêtres ou aux alentours de la maison pour ne pas qu'on puisse reconnaître et, éventuellement, localiser l'endroit.

Suite à différents incidents impliquant la géolocalisation, l'enquêteur criminel de la Police de Québec indique :

*Nous, quand on amène une victime en maison d'hébergement ou qu'elle décide d'aller chez une amie pis qu'elle décide de se sortir de la vie de cet individu-là, on lui dit : « premièrement, on ferme le téléphone et on enlève la batterie du téléphone aussi. Les deux. Pis rachètes-en un, c'est plus safe [...] Surtout pas de l'ouvrir depuis qu'on a eu l'histoire avec la maison d'hébergement.*

De même certaines maisons d'hébergement de la ville de Québec interdiraient carrément aux femmes de se servir de leurs appareils en maison d'hébergement. Ceux-ci doivent être fermés ou placés dans une enveloppe coupant les ondes, indique l'enquêteur. Ces maisons semblent toutefois être l'exception à la règle, puisque toutes les intervenantes rencontrées affirment que les femmes et les enfants arrivent avec leur cellulaire, leur ordinateur portable et leur tablette et qu'elles ont le droit de les utiliser dans la maison.

La majorité des intervenantes indiquent qu'elles n'osent pas ajouter de protocoles autour des technologies : il y a déjà suffisamment des règlements mis en place pour veiller au bon fonctionnement de la vie communautaire, estiment-elles. Quand des règlements sont ajoutés, précise Marie, intervenante en maison d'hébergement :

*C'est toujours en réaction à une situation problématique [...] et il n'y a aucune règle qui a été complètement maintenue.*

Les intervenantes rencontrées remarquent, par ailleurs, que l'environnement sécuritaire que constitue la maison d'hébergement permet à certaines femmes hébergées poursuivies par leur conjoint par voie technologique d'éteindre leurs appareils sans crainte de représailles, ce qui n'était pas le cas lorsqu'elles se trouvaient sous l'emprise du conjoint. L'une d'elles mentionne :

*Le fait que les femmes soient soutenues ici, ça les aide peut-être un peu, et peut-être aussi parce qu'elles ont la possibilité de mettre leur téléphone sur off.*

### *3.5.2 L'enquête policière et la constitution de la preuve*

L'enquête policière n'empêche pas le harcèlement de se produire, mais entre en jeu une fois que la femme entreprend de porter plainte pour harcèlement criminel. Les traces numériques laissées dans le cas où le harcèlement se réalise via les TIC constituent une preuve tangible de l'événement, alors qu'auparavant la preuve de harcèlement reposait essentiellement sur la parole des deux acteurs... qui s'opposaient.

La révélation du harcèlement criminel, commis dans son aspect original, reposait ainsi essentiellement sur des impressions mettant en présence la parole de l'une (la victime) contre l'autre (son conjoint). Lorsque le harcèlement est commis via les TIC, plusieurs traces numériques peuvent être recueillies, permettant la constitution d'une preuve qui ne reposera plus entièrement sur des paroles rapportées et des interprétations, mais bien, sur des éléments concrets, les traces, permettant un rapport d'expertise fournissant des preuves matérielles « objectives » des faits allégués. L'enquête policière peut alors jouer le rôle d'un gardien efficace qui, s'il n'a pu empêcher l'infraction, peut la faire cesser.

Lors de l'appel à la police d'une femme victime de harcèlement dénonçant le délinquant motivé qu'est devenu son conjoint ou ex-conjoint, il est recommandé de présenter tous les éléments qui pourraient prouver qu'il y a eu du harcèlement ; les courriels, les messages textes, une preuve des appels harassants, etc., dans le but d'avoir un commencement de preuve permettant d'aller chercher les mandats nécessaires pour la compléter. Lors de la première rencontre de la victime voulant porter plainte avec un patrouilleur, le but sera de dresser un portrait complet de la situation prenant place entre la victime et le suspect, et d'aider la victime à formaliser ses sentiments de crainte, afin de statuer si un crime a été commis. C'est à ce moment que le contexte entourant la situation sera exploré et que l'urgence d'agir sera établie. Il est primordial, à ce moment, que la victime relate tous les événements qui se sont produits et dresse le bilan de toutes les informations que le conjoint pourrait avoir en sa possession susceptibles de conduire au harcèlement, en précisant la manière dont ces informations ont été obtenues. Si celles-ci ont transité via les TIC, il sera alors éventuellement possible de les retracer. Les policiers s'affaireront à recueillir toute la preuve disponible dans le but d'aller en cour et obtenir une condamnation.

Lorsque le patrouilleur et l'enquêteur à sa suite auront constaté qu'il y a du harcèlement criminel et qu'il paraît y avoir assez d'éléments pour constituer une preuve solide, la rédaction du rapport de police sera faite et la plainte ira de l'avant, précise le lieutenant détective du SPVM :

*Il y a plusieurs mécanismes qui se mettent en place en même temps, donc on va tenter, selon l'urgence de la situation, de localiser l'agresseur ou le harceleur. On va transmettre le dossier à une unité d'enquête, il y a un enquêteur qui va être attiré dans habituellement les premiers jours de la réception de la plainte, parce que toutes ces situations-là, ce sont des situations potentiellement explosives pis ça peut évoluer très rapidement.*

La première préoccupation des policiers est d'assurer la sécurité de la victime, poursuit notre interlocuteur. Suite à l'évaluation du risque de la situation, les policiers vont s'assurer qu'elle a un endroit sécuritaire où rester en attendant la localisation du suspect. Parmi les options s'offrant à la victime, il y a l'accueil chez des membres de la famille, des amis ou dans une maison d'hébergement.

Une fois la victime en sécurité, toute l'attention sera dirigée à localiser le suspect pour l'arrêter. Plusieurs moyens d'enquête seront mis en place pour le retrouver et aucun moyen d'enquête ne sera négligé pour protéger la vie de la victime et de ses enfants, soutiennent les policiers rencontrés. Une fois arrêté, il se peut que le présumé harceleur soit relâché avec des conditions émises par un juge ou par les policiers, ou qu'il soit incarcéré. Dans tous les cas, tous les policiers estiment que :

*le plus tôt qu'on peut intervenir dans le processus de la violence conjugale, que ce soit à travers les intervenants, les partenaires. [Qu'il y ait] une intervention policière à faire tout de suite pour arrêter ça (Lieutenant détective du SPVM).*

Il faut en effet agir rapidement dans la situation de harcèlement pour éviter que les faits s'enveniment et donnent lieu à un délit encore plus grave. D'après le sergent spécialiste en cybercriminalité de la SQ, il convient de prioriser les plaintes de harcèlements impliquant des conjoints versus d'autres crimes contre la personne où l'évènement serait terminé et la victime en sécurité. Dans la plainte de harcèlement entre conjoints, le danger n'est généralement pas écarté, c'est pourquoi elle devrait être priorisée : « *Ce n'est pas parce que tu le priorises que tu vas le prouver* », mais ça peut désamorcer une situation potentiellement explosive. Il faut cependant faire attention, car les procédures pourraient aussi attiser le suspect s'il sait qu'il est enquêté. Une rencontre avec le suspect s'impose afin d'avoir sa version de la situation, et pour connaître ses intentions.

### 3.5.3 Une preuve volatile

La preuve de harcèlement criminel, même lorsque celui-ci est perpétré via les TIC, est malgré tout très volatile. Il importe d'intervenir rapidement pour avoir accès au plus d'information possible, et pouvoir s'en saisir. Le sergent spécialiste en cybercriminalité de la SQ estime que c'est dans la première semaine suivant l'infraction que la meilleure preuve est accessible. Par la suite, plusieurs éléments peuvent disparaître, notamment en étant supprimés.

Le temps est ainsi une variable cruciale dans le cas de crimes commis à partir des TIC. Il faut agir rapidement entre autres pour l'obtention de mandats. Les policiers doivent convaincre le juge de paix qui autorisera le mandat que l'information est probablement toujours présente dans l'appareil, qu'il s'agisse d'un téléphone ou d'un ordinateur. Si trop de temps s'est écoulé depuis l'infraction, il sera plus difficile d'obtenir le mandat, car le juge estimera qu'il y a de grands risques que l'information ne soit plus accessible :

*De façon générale, la difficulté en harcèlement ce n'est pas d'identifier le suspect [...] souvent c'est un ex-conjoint, c'est plutôt d'aller chercher tous les mandats nécessaires pour avoir une preuve solide.*

Avant l'avènement des nouvelles technologies :

*La quantité de mandats qu'on avait à faire pour résoudre une enquête, ça ne se compare pas avec la quantité d'aujourd'hui » (Lieutenant-détective du SPVM).*

Maintenant, le nombre de mandats nécessaire à la constitution de la preuve s'élèverait facilement à quatre ou cinq, si les policiers souhaitent perquisitionner tous les appareils du suspect susceptibles d'avoir été utilisés pour commettre le harcèlement, et demander les ordonnances obligeant la communication de leur contenu. *L'ordonnance de communication* est un document canadien qui ordonne à la compagnie à qui il est transmis de communiquer aux policiers des informations telles l'adresse IP, les données téléphoniques, le nom de la personne relié au compte. Le mandat de perquisition est obtenu dans le but de faire une recherche sur un appareil pour y recueillir de la preuve. Tous les appareils qui pourraient avoir servi à commettre le crime devraient y être soumis.

Dans la demande de mandat de perquisition, les éléments recherchés doivent être énumérés et seulement les éléments jugés pertinents à l'établissement de la preuve pourront être extraits. Le mandat de perquisition est utilisé principalement pour le suspect, car en général, la victime aura volontairement fourni ses appareils en vue de la constitution de la preuve. La nature de la preuve recherchée étant précisée, les techniciens iront directement là où ils pensent la trouver; ils n'iront pas fouiller dans tout le cellulaire, précise le sergent-spécialiste en cybercriminalité de la SQ :

*Des fois, les gens ont peur parce qu'ils ne veulent pas qu'on fouille dans leurs affaires personnelles, l'autorisation qu'on leur demande, c'est toujours par rapport au dossier.*

Toutefois, s'il advenait que le technicien tombe, par hasard, sur un contenu illégal, par exemple de la pornographie juvénile, le propriétaire de l'appareil pourrait également être accusé de cette infraction. Il en est de même si la victime a fait des menaces au suspect et que les policiers ont des motifs raisonnables de croire que la vie du suspect pourrait également être en danger : la victime n'a pas l'immunité. Advenant le cas de plaintes croisées, où des accusations sont formulées de part et d'autre, il est probable que celles-ci avortent avant même d'être entendues en cour, faute de preuve des deux côtés. Les policiers sont tout de même tenus de constituer la preuve dans les deux cas. Ce sont les procureurs qui décident d'autoriser les chefs d'accusation à la cour qui, par conséquent, devront trancher quant à la recevabilité et la valeur de la preuve leur étant présentée.

Les policiers vont utiliser des méthodes d'enquête conventionnelles et techniques pour constituer cette preuve. Dans la majorité des cas, les deux façons de faire vont être utilisées pour résoudre une enquête, expliquent le sergent-spécialiste en cybercriminalité de la SQ, mais la voie technique, plus nouvelle, demande encore à être maîtrisée et sa pertinence établie :

*La partie technique est nouvelle, faque il faut la rentrer dans l'âme. C'est un outil supplémentaire, ça ne remplace rien, mais ça vient bonifier l'enquête.*

La prise en compte d'éléments techniques amène un côté neutre à la constitution de la preuve qui est dès lors moins influencée par les sentiments et les impressions. La confection technique de la preuve est toutefois rarement parfaite. C'est pourquoi un témoin permettra de compléter les bribes d'histoire manquant aux enregistrements recueillis. Il faut jongler avec les deux méthodes afin d'avoir la preuve la plus complète possible, plaident les policiers rencontrés.

Dans le cas de harcèlement criminel réalisé via les TIC, des traces numériques sont disponibles dans tous les appareils utilisés. Le simple fait d'ouvrir l'ordinateur ou le cellulaire laisse des traces. Des techniciens spécialisés contribueront à retrouver une grande partie des traces par un procédé d'extraction de données qu'ils mettront en œuvre. Le technicien utilise aussi un logiciel qui permet de retrouver même ce qui a été apparemment supprimé d'un appareil. Dans les cas de harcèlement criminel, la recherche se fait souvent par mots-clés étant donné que le technicien sait exactement ce qu'il doit aller chercher. Il se charge alors d'extraire les données répondant au mot clé, les mettre sur un DVD, un support non modifiable' il s'assure ensuite que la chaîne de possession du contrôle a été ininterrompue, permettant d'établir ainsi que la preuve n'a pu être contaminée par qui que ce soit, à quel que moment que ce soit. Le rapport rédigé par le technicien devient un élément recevable en cour témoignant de l'authenticité de la preuve recueillie. Il est primordial pour la victime de ne pas tenter d'extraire elle-même les données, au risque de « corrompre » ou détruire la preuve.

#### *3.5.4 Ordinateurs et Internet : une source de données en or*

Les ordinateurs, comme les téléphones cellulaires, sont une source d'informations « en or » pour les policiers. Comme mentionné plus haut, tous les mouvements effectués sur ces machines sont enregistrés. Afin d'assurer la validité de la preuve, lors d'une perquisition, les policiers vont débrancher l'ordinateur, précise l'enquêteur-criminel de la police de la ville de Québec :

*[il va y avoir] un shut down qui se fait automatiquement faque le technicien va être capable de savoir à telle heure il y a eu un shut down donc tout ce qui s'est passé avant ce n'est pas la police qui l'a faite, c'est le suspect.*

Dépendamment des logiciels utilisés sur l'ordinateur, plusieurs éléments supprimés peuvent être retrouvés. Ainsi, si l'auteur ne fait que supprimer des éléments, sans l'intermédiaire d'un logiciel spécifiquement utilisé à cet effet, les éléments supprimés pourront être aisément retrouvés, en quasi-totalité. Mais si le contenu a été supprimé avec un logiciel spécifiquement destiné à la destruction des données, il pourra ne plus être possible d'avoir accès au contenu. Le professeur David-Olivier Jaquet-Chiffelle explique en outre que :



*Si l'ordinateur ou le cellulaire a presque toute sa mémoire d'utilisée, et puis que la personne en libère une partie [en supprimant des éléments], assez vite ça va récrire dessus parce qu'il n'y a pas de mémoire disponible (David-Olivier Jaquet-Chiffelle)*

Dans ce cas, l'information sera perdue.

La majorité des crimes commis à partir d'un ordinateur ont recours à Internet pour le commettre. Pour avoir le nom et l'adresse de la personne reliée à l'adresse IP qui identifie la source, il faut formuler une demande de communication aux fournisseurs d'accès Internet. Il faut par ailleurs bien comprendre que l'adresse IP fait le lien avec une adresse physique, pas une personne en particulier utilisant cette adresse. Dans le cas où un routeur est utilisé, l'identification de la personne derrière l'adresse IP se complique. Le routeur s'occupe en effet de distribuer l'accès Internet à tous les appareils qui lui sont connectés en redistribuant des adresses IP internes, pour lesquelles aucun registre n'est gardé. Il faut, dans ce cas, pousser l'enquête plus loin pour connaître qui utilisait Internet à cette adresse et à ce moment. Des techniques d'enquête traditionnelle, incluant l'interrogatoire, seront utilisées pour savoir qui était derrière le clavier lors de la commission de l'infraction à cette adresse. Certains sites Internet pourraient permettre d'associer l'adresse IP avec l'adresse physique, mais tous les policiers et le spécialiste en traces numériques rencontrés s'entendent pour dire que l'adresse physique donnée par ces sites web n'est généralement pas fiable.

À partir d'une recherche d'effectuée sur l'ordinateur, le technicien peut retrouver des traces si un logiciel espion ou un *malware* a été installé sur l'appareil. Il faut, de son côté, qu'il ait accès à l'appareil pour savoir si un logiciel espion y a été installé, alors que pour installer ce type de logiciel, l'accès à l'appareil n'est pas toujours nécessaire.

D'après le professeur Jaquet-Chiffelle, « *quand on connaît très bien une personne c'est beaucoup plus facile de l'infecter* » avec un logiciel espion. La personne visée peut être infectée en ouvrant un courriel qu'elle pense provenir d'une amie, alors qu'en réalité c'est le conjoint qui a utilisé un service pour envoyer le courriel en se faisant passer pour l'amie et ainsi pouvoir infecter l'appareil de la victime à l'ouverture du courriel.

Plusieurs informations peuvent être recueillies par la personne ayant utilisé le service de logiciel espion. Celui-ci pourrait même enclencher la caméra et le micro de l'appareil, enregistrer les mots de passe de tous les comptes appartenant à la victime, rouvrir l'appareil, activer la localisation, tout ça sans que la victime s'en rende compte. C'est pourquoi les policiers et le professeur de l'École des Sciences criminelles recommandent de fermer et enlever la batterie du cellulaire, lorsque celui-ci n'est pas utilisé.

D'après les policiers interviewés, l'utilisation de logiciels espions a été répertoriée dans peu de cas à ce jour, mais :

*on est appelé à en avoir, je pense, plus parce que c'est plus disponible, tu peux trouver ça facilement* » (Sergent spécialiste de la SQ).

Pour constituer la preuve de harcèlement, on cherche la preuve de propos harcelants et de menaces enregistrés sur les appareils utilisés par le délinquant motivé. Plusieurs techniques seront utilisées pour y avoir accès. Notamment, si la conversation est toujours accessible par le compte de la victime, les policiers vont faire signer une autorisation à la victime permettant d'aller chercher la preuve dans son compte. Si la victime décide de fermer son compte, Facebook offre une période de grâce de 90 jours durant laquelle toutes les informations y étant contenues seront conservées. Après cela, il est encore possible de réactiver le compte, toujours avec l'autorisation de la victime, en souhaitant que les informations y soient toujours, mais il est alors fort possible que tel ne soit pas le cas.

Les informations de contenu de Facebook se trouvent aux États-Unis, donc pour y avoir accès *un mandat d'entrée à l'international* doit être produit. C'est un processus « *plutôt exceptionnel parce que c'est très long et très coûteux* », et probablement l'ultime moyen utilisé pour un cas de harcèlement criminel entre ex-conjoints. Lors d'une demande d'ordonnance de communication d'adresse IP ou d'une demande d'entrée à l'international, le Facebook ID est primordial. C'est un numéro unique et stable dans le temps permettant d'identifier un utilisateur de Facebook.

### 3.5.5 *Les données téléphoniques : un outil de surveillance et de corroboration*

Nous l'avons déjà mentionné à quelques reprises : les données cellulaires sont une source importante d'information. Dans la grande majorité des cas, elles vont être utilisées pour corroborer les versions de la victime et du suspect. De nos jours, indique le lieutenant détective du SPVM :

*presque tout le monde a un téléphone cellulaire qui est actif à n'importe quel moment de la journée, faque c'est sûr que ça nous donne des moyens d'enquête pis des données.*

L'envoi fréquent de messages textes permet aux policiers de pouvoir suivre le téléphone à la trace. Les données cellulaires donnent la position de la tour la plus proche de l'émetteur, ainsi que le numéro du destinataire permettant de savoir si les messages ou les appels étaient destinés à la victime. La position des tours permet de connaître la position du suspect lors de l'envoi.

Dans la majorité des cas, les policiers vont aller chercher une *ordonnance de communication* pour avoir accès au registre cellulaire de la victime et du suspect et ainsi pouvoir corroborer les éléments qui ont été témoignés par l'un et par l'autre. Lors de l'interrogatoire, le registre cellulaire sera très utile pour confronter le suspect et savoir s'il ment. Avec des méthodes traditionnelles d'enquête, le policier peut faire avouer au suspect que le cellulaire repéré est le sien et qu'il l'a toujours avec lui. Ainsi, lorsque le policier, plus tard dans l'interrogatoire, fait référence aux données contenues dans le cellulaire, le suspect peut difficilement nier qu'il en est l'auteur. L'extraction des messages texte du cellulaire de la victime peut également être un élément clé pour l'interrogatoire. En montrant les deux versions des messages tirés des appareils appartenant respectivement à la victime et à l'agresseur, souvent le suspect en viendra aux aveux.

Le contenu des messages textes n'est pas accessible par la compagnie de téléphonie mobile, faisant en sorte que les enquêteurs ne peuvent pas demander le contenu des messages aux compagnies. Ils peuvent seulement avoir accès aux données cellulaires encore contenues sur le téléphone, qui sont ordinairement accessibles pour une période d'environ 60 jours après avoir été produites. Par la suite, il y a risque de perdre des informations.

Pour obtenir des données moins récentes, les policiers devront passer par une ordonnance de communication, procédure qu'on a vue plus tôt. La compagnie de téléphonie peut prendre jusqu'à 30 jours pour honorer l'ordonnance, et entre temps, des données risquent d'être détruites. Donc le plus tôt la demande est faite, le plus d'informations on peut espérer acquérir. L'enquêteur peut toujours demander une préservation des données, s'il craint que des informations précieuses pour son enquête risquent d'être détruites, mais rien ne garantit que la manœuvre sera effectuée à temps.

#### *3.4.4 Les traces numériques introuvables, jusqu'à maintenant*

L'Internet cellulaire (3G et LTE) pose problème aux enquêteurs, car il n'y a plus assez d'adresses IP V4 pour tous les appareils connectés à Internet. Les distributeurs de téléphones mobiles, pour remédier à la situation, utilisent le *Carrier Grade Network* (CGN). Le CGN agit comme un routeur à l'intérieur d'une maison sauf qu'il distribue des adresses IP Internet aux clients d'une compagnie. Les compagnies vont, avec un CGN, redistribuer Internet aux abonnés d'une région, par exemple l'Est du Canada. Dans ce cas, quand la police demande une ordonnance de communication à la compagnie pour l'adresse IP issue de l'Internet cellulaire d'un client, elle obtient le nom de la compagnie mobile et CGN, Est du Canada. Ceci signifie que le policier sait seulement que c'est un client d'une telle compagnie basée dans l'Est du Canada. Il devient donc impossible de savoir qui est à l'origine de l'infraction commise sur Internet si le client a utilisé l'Internet 3G ou LTE pour rendre actif son appareil mobile.

Les Wi-Fi d'accès gratuits posent également problème pour l'identification des suspects. Lorsqu'une demande d'ordonnance est demandée pour une adresse IP provenant d'un Wi-Fi public, parfois seulement le nom de la compagnie, par exemple McDonald Canada, qui offre le service est disponible. Dans de rares cas, on pourra identifier lequel des restaurants de la chaîne a été utilisé. Donc c'est le même principe qu'avec le 3G, l'identification vaut pour une des personnes au Canada qui était connectée à ce moment-là, dans ce restaurant, sans plus de précision. Il devient alors pratiquement impossible d'établir, hors de tout doute, qui est à l'origine de l'envoi du ou des messages. Dans les deux cas, les policiers ont une adresse courriel ou un identifiant quelconque localisant l'émetteur, mais la corroboration est plus difficile, voire impossible à faire, dans ce cas, puisque l'appareil à la base de l'infraction ne peut être singulièrement identifié.

L'utilisation de l'info nuage, de proxy et de Tor permet d'anonymiser la possession d'un appareil en brouillant l'adresse IP. Lorsque ces serveurs sont utilisés, il est encore à ce jour impossible de retracer l'adresse IP à partir de laquelle un message est envoyé, donc d'établir que c'est le suspect qui aurait commis une infraction. L'information est souvent envoyée dans ce cas à partir d'un serveur hébergé ailleurs dans le monde, dans un pays avec lequel le Canada n'a pas d'entente visant la communication des adresses IP. C'est clairement là un problème : il n'y a pas d'ententes internationales concernant ce qui se passe sur Internet. Internet n'a pas de frontière, mais le pouvoir policier oui; il peut agir seulement sur ce qui se trouve au Canada. Autrement, il faut demander l'aide d'Interpol ou un mandat d'entrée à l'international : les démarches, on l'a déjà signalé, deviennent dès lors beaucoup plus complexes, coûteuses, et extrêmement longues. Pour une enquête active, l'utilisation d'un mandat international devient impraticable. Une telle limite d'action n'avantage personne, surtout si le suspect est connu.

Quoi qu'il en soit, dans tous les cas, la collaboration de la victime favorise grandement l'enquête, lorsqu'elle donne accès à ses appareils. Le délai d'analyse pour produire l'expertise nécessaire à la mise en accusation reste long, mais tous les policiers et le professeur de l'Université de Lausanne s'entendent pour dire que la victime a tout avantage à fournir ses appareils à la police pour faciliter l'enquête qu'elle a elle-même déclenchée.

#### 3.4.5 *La corroboration des faits*

Le but de l'enquête est de corroborer les faits racontés par la victime, d'une part, et par le suspect d'autre part. C'est pourquoi les policiers recommandent de garder une trace de tout ce qui pourrait permettre de confirmer les menaces ou le harcèlement :

*La qualité de la preuve c'est la corroboration parce que n'importe qui peut alléguer n'importe quoi sur n'importe qui, mais en l'absence d'une preuve indépendante ben on dit : « c'est la parole d'un contre l'autre » (Lieutenant-détective, SPVM).*

Il est important de rappeler que la défense doit seulement créer un doute raisonnable pour que la condamnation n'ait pas lieu ; donc plus grand est le nombre d'éléments indépendants corroborant la version de la victime, moins la défense aura de jeu pour instaurer le doute raisonnable. Le lieutenant-détective du SPVM insiste sur le fait qu'il faut vraiment tout dire, car parfois :

*on dit des choses, on fait de choses qu'on est pas toujours fier, on n'est pas trop porté à le dire à la police parce qu'on a peur que ça affecte notre crédibilité. Au contraire, au contraire ce qui est important c'est de relater toutes les informations.*

Suite à la déposition complète, le but des policiers est d'étoffer la version fournie par la victime avec toutes les corroborations possibles. Une copie des courriels, des messages textes, des discussions sur les réseaux sociaux permet de corroborer la version de victime et donne une preuve indépendante. Il reste qu'une extraction de données doit quand même être faite pour prouver hors de tout doute d'où viennent ces éléments. Même si certaines données comme l'adresse IP, l'identifiant Facebook ou le numéro de téléphone d'où proviennent les messages sont des éléments permettant d'identifier une personne, la partie n'est pas terminée. Il faut que les policiers réussissent à identifier la personne derrière le clavier. Durant l'interrogatoire, la présentation des données permettant de confronter le suspect peut l'amener à avouer qu'il a bel et bien harcelé la victime. Sinon, il faut recourir à des moyens d'enquête plus traditionnels, par exemple interroger des témoins qui auraient vu le suspect harceler la victime.

Le Lieutenant-détective du SPVM mentionne également la preuve par *modus operandi*, où les policiers établiraient que c'est le suspect qui aurait harcelé la victime d'après sa technique de harcèlement, son écriture, etc. Il mentionne que :

*le suspect va harceler la victime d'une certaine façon ou il va tenir certains propos qui sont propres à cette personne, que ce soit par écrit, courriel ou textos, qui va faire en sorte que nous on va être capables de faire une preuve à la cour par une série de faits mis ensemble (Lieutenant-détective du SPVM).*

Ce n'est pas une preuve qui est facile à faire, mais cette avenue peut être utilisée.

## CHAPITRE 4 : DISCUSSION

Dans le cadre de cette recherche, nous avons cherché à voir s'il était possible d'adapter la théorie des opportunités et des activités routinières développée par Cohen et Felson (1978) au harcèlement produit via les TIC dans le contexte d'une relation conjugale, actuelle ou passée. Au terme de ce travail, nous pensons pouvoir répondre par l'affirmative.

La théorie des opportunités et des activités routinières de Cohen et Felson (1978) qui soutient notre argumentaire, rappelons-le encore une fois, met en tension les notions de délinquant motivé, de cible attrayante et d'absence de gardien pour expliquer la commission d'un acte criminel. Le délinquant motivé est, dans le cas qui nous concerne, le conjoint ou l'ex-conjoint de la victime. Ses motivations sont celles d'un conjoint cherchant à exercer un contrôle coercitif sur sa compagne, tel que décrit par Stark (2014). Le contrôle qu'il cherche à imposer à sa compagne est mis en péril lorsque celle-ci décide de le quitter ou menace de le faire ; il pourra alors chercher à la contacter par tous les moyens pour l'implorer de revenir, la guetter, ou le menacer, ou encore il pourra chercher à ternir sa réputation en utilisant les réseaux sociaux. La situation de conjugalité donne accès au délinquant motivé à une foule d'informations qu'il peut mettre à profit pour mener à bien son harcèlement : à tout prendre, il connaît très bien les activités routinières de la victime ce qui lui permet une grande facilité d'action la concernant (Reyns, Henson et Fisher, 2011). Comme l'a mentionné le professeur Jaquet-Chiffelle :

*La victime est vraiment très vulnérable quand c'est quelqu'un de proche qui veut l'attaquer.*

La cible attrayante se trouve être ici la conjointe victime de violence conjugale post-séparation qui s'exprime sous forme de harcèlement produit par le conjoint pour miner la qualité de vie de celle qui, dans son esprit, le trahit en l'abandonnant. La conjointe, lorsqu'elle entreprend de quitter le domicile familial pour aller se réfugier en maison d'hébergement, se trouve pour sa part, ordinairement, dans une situation émotionnelle vulnérable.

La majorité des femmes dans cette situation arrivent désormais en maison d'hébergement en apportant les différents appareils de communication électroniques en leur possession qu'elles comptent utiliser pour rester en contact avec leur réseau social. L'utilisation de ces appareils peut toutefois les mettre dans une situation périlleuse étant donné que par le truchement de ces appareils :

*les conjoints ont une emprise sur la femme parce qu'ils réussissent à lui envoyer un paquet de cochonneries, de menaces, d'insultes.*

La maison d'hébergement ainsi que les intervenantes qui y travaillent peuvent alors jouer un rôle important de gardien. Une intervenante mentionne :

*Le fait que les femmes soient soutenues ici, ça les aide peut-être un peu, [...] parce qu'elles ont la possibilité de mettre leur téléphone sur off.*

Les femmes victimes de violence conjugale « en fuite » accueillies en maison d'hébergement seront toutefois invitées à fermer tous leurs appareils. Le gardien le plus efficace, dans ce cas, c'est effectivement de ne plus utiliser leurs appareils ou, à tout le moins, de changer leurs mots de passe ainsi que leur numéro de téléphone. De cette façon, le contact entre le harceleur et la victime sera coupé ; mais, incidemment, la victime sera aussi plus difficilement joignable par tout le reste de son entourage.

Dans le cadre de la présente étude, l'analyse a été effectuée en cherchant à voir comment les maisons d'hébergement et l'enquête criminelle peuvent jouer le rôle de gardien efficace en contexte de violence conjugale. Ces deux éléments semblent effectivement jouer un rôle important dans la protection de la victime. A contrario, il est évident qu'en l'absence de l'intervention effectuée en maison d'hébergement et d'une plainte déposée à la police, le délinquant motivé peut commettre d'autant plus facilement son harcèlement.

Il s'avère que, dans ce contexte, les TIC peuvent intervenir de deux façons : elles peuvent, d'un côté, servir les fins du harceleur en rendant accessible à distance la victime qui refuse de couper le contact avec le monde extérieur en gardant ouvertes les voies de communication électroniques; et elles peuvent, d'un autre côté, contribuer à la constitution de la preuve du harcèlement en gardant la trace des communications harcelantes.

#### 4.1 Comment les suspects, en connaissant les activités routinières de la victime peuvent-ils utiliser les nouvelles technologies pour la harceler ?

Le harcèlement, décrit comme étant un éventail de techniques de contrôle et de surveillance mises en place dans le but de faire craindre la victime pour sa sécurité (Safety Net, 2013a), se révèle être un comportement criminel grandement utilisé par un conjoint ou un ex-conjoint.



La relation conjugale permet au conjoint harcelant de mener à terme plus facilement son harcèlement, car il connaît bien les habitudes de vie de la victime.

D'après Eoghan Casey (2011: 423):

*the crux of a stalker's power is information about and knowledge of the victim. Stalkers use information like telephone numbers, addresses, and personal preference to impinge upon their victim's lives.*

Souvent suite à une séparation, le conjoint, en perte de contrôle sur sa victime, tentera par tous les moyens de la contacter pour l'influencer dans son processus en maison d'hébergement et faire changer sa décision, et les TIC lui faciliteront la tâche, mentionne Marie, intervenante en maison d'hébergement :

*Je vois que la différence ou le recul n'est pas présent du tout parce qu'il y a toujours un contact via les technologies*

Du simple fait de savoir que la victime amène avec elle ses appareils technologiques, le conjoint comprend qu'il peut continuer, notamment via les textos, d'exercer son contrôle sur elle. Il y a désormais des applications qui suivent tous les déplacements et indique le temps passé à un certain endroit, donc le conjoint n'a même plus à se déplacer pour savoir ce que fait sa conjointe. L'enquêteur criminel de la police de la ville de Québec a fait l'expérience d'une application gratuite de localisation, avec le consentement de sa conjointe, pour montrer à quel point les technologies permettent de suivre facilement la vie d'une autre personne. Une fois séparée, si la femme ne sait pas que cette application a été installée sur ses appareils de communication, elle laisse l'ex-conjoint savoir exactement où elle se trouve, ce qui lui permet de s'y présenter et la suivre, faisant naître chez elle un sentiment de crainte.

En somme, comme l'avance Fusco (2014) plusieurs applications ont été mises sur pied pour recueillir les données de localisation souvent utilisée par les harceleurs pour suivre à la trace leur conjointe. Mais d'autres applications permettent de recueillir et garder la trace des éléments (texto, courriels, interrogations) servant à géolocaliser et harceler la victime, en un mot de poursuivre le contrôle du conjoint sur sa compagne amorcer dans la relation conjugale, au-delà de la réparation, allant jusqu'à la faire craindre pour sa vie, trop souvent avec raison.

En définitive, notre étude a montré que le comportement de harcèlement via les TIC en contexte de violence conjugale post séparation réunit bien les trois éléments nécessaires à la commission d'un crime identifié par Cohen et Felson (1978) à avoir : le délinquant motivé (le conjoint), la cible attrayant (la victime « en fuite ») et l'absence de gardien, condition amplifiée du fait qu'on connaît encore mal les différentes applications des TIC susceptibles de rendre possible le harcèlement criminel.

C'est donc en cernant mieux les possibilités reliées à l'utilisation des TIC, pour le meilleur et pour le pire, qu'il deviendra possible d'éviter le pire, la géolocalisation et le harcèlement à fins criminelles, et de favoriser la constitution de la preuve, le cas échéant.

#### 4.2 Comment l'accumulation des traces numériques témoignant des activités routinières des victimes et des suspects peut-elle servir l'enquête policière

Les appareils numériques de toutes sortes sont des sources riches de données rendant compte des activités routinières des gens. C'est notamment ce qui permet à la police de corroborer plusieurs éléments de preuve établissant la commission d'un acte criminel. Les communications téléphoniques dévoilent une panoplie d'informations tels le numéro associé à la carte SIM, l'IMEI, la date et l'heure de la communication, l'emplacement de la tour cellulaire ayant transmis le signal, le contenu de la communication ainsi que le destinataire (Forte et De Donno, 2010) :

*Aujourd'hui tu sais très bien que les textos, c'est une centaine par jour donc on peut suivre les gens à la trace (Sergent-spécialiste, Sûreté du Québec).*

À partir d'une ordonnance de communication émise par un tribunal associée à un appareil donné, la position ainsi que le destinataire de la communication enregistrés dans la mémoire de l'appareil peuvent être révélés. Or, notent Forte et de Donno (2010: 525) :

*Determining the location of a mobile device can be important for assessing alibis of suspects or the whereabouts of victims in the past, and ongoing tracking of the location can be useful in cases of abduction, missing persons, and other ongoing criminal activities.*

Les policiers vont chercher ces données, soit pour corroborer les faits ou pour confronter le suspect sur un mensonge, dans le cadre d'un interrogatoire de police.

Il est de même pour les ordinateurs ainsi que toutes les connexions faites aux différents réseaux sociaux. À partir de l'adresse IP, l'enquêteur peut demander une ordonnance de communication pour obtenir l'adresse physique ainsi que le nom du suspect, permettant par la suite la perquisition de l'appareil. Il importe, pour l'enquêteur, de chercher les traces qui auraient pu être laissées derrière, ce qui a été détruit ou même ce qui a disparu des appareils numériques de la victime :

*Therefore, investigators should thoroughly examine the point of contact avec cybertrails (e.g., the Web, Usenet, and personal computers) for digital evidence that exposes the offender's behavior” (Casey, 2011: 430).*

Toutes les traces retrouvées pourront témoigner des activités du suspect commises dans le but de harceler la victime.

Casey (2011) mentionne, comme tous les policiers interviewés dans le cadre de notre étude, qu'il faut recueillir le plus d'éléments de preuves et d'éléments corroboratifs possible pour démontrer la persistance du harcèlement ainsi que la crainte engendrée chez la victime.

## CHAPITRE 5 : L'INTÉGRATION DES SAVOIRS CRIMINOLOGIQUE ET CRIMINALISTIQUE

En partant du postulat de Locard (1920 : 139) qui stipule que « *nul ne peut agir avec l'intensité que suppose l'action criminelle sans laisser des marques multiples de son passage* », il paraît maintenant clair que ce postulat s'applique bien dans le monde virtuel : toutes activités sur Internet et même sur un cellulaire laissent des traces (Gold, 2013). « *Digital evidence is the term used to describe information of evidential value that has been stored or transmitted in digital form* » (Tilstone, Savage et Clark, 2006 : 116). Les traces numériques telles que décrites dans ce travail peuvent aider l'enquête au même titre que des documents écrits ou imprimés. Les traces numériques sont désormais une source d'information considérable dans la reconstitution des événements et dans la constitution des dossiers de preuves aux fins de poursuite judiciaire. Elles peuvent être trouvées dans des documents, des courriels produits et conservés sur des appareils mobiles, des ordinateurs, dans le « nuage », alors qu'elles transitent sur les réseaux de téléphonie et Internet (Graves, 2014). Le travail de l'enquêteur consiste alors à relier une personne aux outils technologiques permettant la commission du crime. Pour ce faire, les adresses IP, les cartes SIM et parfois les pseudonymes peuvent permettre d'identifier l'adresse réelle de la personne à la base du crime commis (Desgens-Pasanau et Freyssinet, 2009; Graves, 2014).

C'est notamment dans l'extraction des données et la mise en relation des différentes traces pouvant conduire à identifier des comportements de harcèlement et les associer à leur auteur que la science forensique pourrait se joindre à la criminologie dans l'élucidation des cas de violence conjugale se poursuivant au-delà de la séparation. La violence psychologique particulièrement complexe à prouver devient une voie exploitable grâce aux nouvelles technologies laissant des traces d'abus psychologique plutôt que physique. Au Canada, outre les accusations de voies de fait ; la plus populaire dans les cas de violence conjugale, l'accusation de harcèlement peut également être utilisée. L'article 264 du Code criminel canadien (1985) décrit le harcèlement criminel comme suit :

**264.** (1) Il est interdit, sauf autorisation légitime, d'agir à l'égard d'une personne sachant qu'elle se sent harcelée ou sans se soucier de ce qu'elle se sente harcelée si l'acte en question a pour effet de lui faire raisonnablement craindre — compte tenu du contexte — pour sa sécurité ou celle d'une de ses connaissances.

(2) Constitue un acte interdit aux termes du paragraphe (1), le fait, selon le cas, de :

- a) suivre cette personne ou une de ses connaissances de façon répétée;
- b) communiquer de façon répétée, même indirectement, avec cette personne ou une de ses connaissances;
- c) cerner ou surveiller sa maison d'habitation ou le lieu où cette personne ou une de ses connaissances réside, travaille, exerce son activité professionnelle ou se trouve;
- d) se comporter d'une manière menaçante à l'égard de cette personne ou d'un membre de sa famille.

La mise en accusation pour harcèlement n'aboutit généralement pas, due à l'absence de preuves tangibles accessibles pour la Couronne. Le harcèlement est vécu via les nouvelles technologies par l'abondance de messages textes, d'appels, de messages vocaux, de courriels, la géolocalisation et les logiciels espions installés dans les différents appareils électroniques utilisés par la victime, à son insu. Safety Net Canada (2013) rapporte que l'utilisation abusive des nouvelles technologies dans les relations de violence conjugale s'avère un thème récurrent et préoccupant dans les cas d'homicides conjugaux. Le 8<sup>e</sup> rapport annuel du *Domestic Violence Death Review Committee* (Office of the Chief Coroner, 2011) signale que les nouvelles technologies sont souvent utilisées par les conjoints avant de commettre un homicide conjugal. La copie des messages envoyés n'ayant pas assez de poids et, surtout, le fait qu'il est difficile de prouver hors de tous doutes que l'accusé a bien écrit ces messages, mettent en danger la vie des femmes, et souvent même celle de leurs enfants, du fait même que les traces laissées sont encore peu connues et peu reconnues. C'est exactement là où la science forensique viendrait jouer un rôle important dans la mise en accusation. Les traces numériques présentées par un forensicien donneraient plus de poids à la Couronne pour prouver que du harcèlement a eu lieu.

Il suffirait d'une fois où une mise en accusation de harcèlement établie sur les bases de traces numériques aboutisse à une condamnation pour créer un précédent et ainsi faire jurisprudence pour les femmes se trouvant dans des situations similaires, à l'avenir. L'analyse des procès où les traces numériques auraient été utilisées permettrait aussi d'établir un profil type des traces qui auront été utiles dans ces poursuites, permettant ainsi aux forensiciens de savoir plus précisément où chercher.

Ce profil pourrait également être exploité pour renseigner les intervenantes en maison d'hébergement pour femmes victimes de violence conjugale sur les mesures à prendre pour protéger les traces numériques sur l'appareil de la victime. Ainsi, la science forensique aurait un impact direct en contribuant à l'intervention préventive faite dans les maisons d'hébergement concernant l'impact des nouvelles technologies susceptibles d'être utilisées « pour le pire et pour le meilleur » dans la vie de ces femmes

En bout de course, les sciences forensiques pourraient permettre la condamnation d'hommes violents envers leur conjointe lors d'une plainte pour harcèlement ou voies de fait avant que la situation ne dégénère en homicide conjugale, ce qui rejoint évidemment le vœu des intervenants en maison d'hébergement.

## CONCLUSION

Plusieurs auteurs se sont intéressés au harcèlement fait par le biais des technologies de l'information et des communications dans le but de continuer d'exercer un contrôle à distance sur la victime. Safety Net Canada (2013) a montré la pertinence de se préoccuper de ce sujet, car, de plus en plus, les femmes victimes de violence conjugale, même lorsqu'elles cherchent à se mettre en sécurité en se réfugiant en maison d'hébergement, continuent d'utiliser leurs appareils électroniques. Si cela leur permet de rester en contact avec leur entourage et ainsi obtenir du soutien, cela les met, également, en danger de géolocalisation, ou d'être la proie de logiciels espions ou de plusieurs autres dispositifs répertoriés dans ce travail dirigé. Celui-ci avait pour objectif général de sonder si et de quelle façon la théorie des opportunités et des activités routinières de Cohen et Felson pourrait s'appliquer à un crime encore peu connu, soit le harcèlement criminel perpétré par les TIC en contexte de violence conjugale post-séparation.

Les résultats témoignent de la complexité de l'infraction de harcèlement criminel, et plus spécialement de la complexité de l'élément central de cette infraction, soit le sentiment de crainte vécu par la victime du fait du harcèlement. Les témoignages des intervenantes et des policiers illustrent, par le biais d'exemples, comment un conjoint violent peut être ce que l'on entend par délinquant motivé. Les TIC sont des outils qui permettent au conjoint d'étendre son contrôle au-delà de l'interaction physique; il peut désormais exercer son contrôle à distance grâce aux TIC. La victime, par le lien qui l'unit au délinquant, peut pour sa part s'avérer une cible attrayante, même si elle a quitté la situation de violence. Malgré le fait qu'elle soit en sécurité en maison d'hébergement, elle reste psychologiquement vulnérable aux messages du conjoint qui tenterait de la faire changer d'idée. Il ne faut pas oublier que la victime peut avoir des enfants avec le conjoint, ne permettant pas de couper toutes communications avec lui.

Finalement, les maisons d'hébergement peuvent jouer un rôle de gardien efficace dans le sens qu'elles donnent aux femmes hébergées l'opportunité de fermer leurs appareils en toute sécurité, et d'obtenir le support et l'intervention nécessaires dans une situation aussi complexe que la violence conjugale qu'elles cherchent à quitter. L'enquête criminelle joue également un rôle de gardien efficace, dans le sens où, suite à l'enregistrement d'une plainte, une grande partie des traces numériques laissées sur les appareils de la victime et du harceleur peuvent être retrouvées pour constituer la preuve.

Les traces numériques accessibles dans le cas de harcèlement perpétré via les TIC offrent aux policiers et à la victime la possibilité d'avoir une preuve technique plus objective que les témoignages des différentes parties impliquées dans la situation de violence conjugale. Les policiers vont tout mettre en place pour protéger la victime et étoffer le plus possible la preuve qui sera présentée au DPCP. En continuant de perfectionner la constitution de la preuve utilisant les traces numériques lors des plaintes de harcèlement criminel, il y a tout lieu de croire que le rôle de gardien efficace dévolu aux policiers pourrait s'accroître et, éventuellement, contribuer à décourager les conjoints violents de commettre du harcèlement criminel via les TIC.

Dans une étude ultérieure, il serait intéressant d'interviewer des femmes victimes de harcèlement criminel pour connaître les impacts qu'ont les nouvelles technologies dans leur vie entravée par une relation de violence conjugale. Il serait pertinent de connaître les impacts des TIC tant en maison d'hébergement que dans la vie de tous les jours, ainsi que les moyens de protection mis en place pour déjouer le contrôle et la surveillance du conjoint via ces nouveaux outils, de leur point de vue.

Afin de combler une des limites de cette étude, éventuellement, il serait également pertinent de rencontrer des procureurs pour en apprendre davantage sur ce qui justifie qu'une plainte de harcèlement criminel via les TIC sera autorisée alors qu'un autre cas semblable ne le sera pas.

Finalement, il serait pertinent de diffuser les résultats obtenus dans le cadre du présent travail dirigé afin d'informer la population des risques associés à l'utilisation des nouvelles technologies dans un objectif de contrôle et d'espionnage. En sensibilisant les femmes victimes de violence conjugale non seulement quant aux risques qu'elles présentent, mais également aux possibilités qu'offrent les TIC pour la constitution de la preuve de harcèlement criminel et l'accusation d'autres crimes reliés au TIC, on peut favoriser une reprise de pouvoir sur leur vie et la sortie de la relation violente.



## BIBLIOGRAPHIE

- Acosta, F., Pires, A.P. (1998). Constructivisme versus réalisme. Quelques réflexions sur les notions de crime, déviance et situations problématiques. Dans Cartuyvels, Y. et alia, éd(s), *Politique, Police et Justice au Bord du Futur. Mélanges pour et avec Lode Van Outrive*. (pp. 21- 44). Paris, Montréal: L'Harmattan.
- Al Mutawa, N. Baggili, I. et Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9, s24-s33.
- Arksey, H. et Knight, P.T. (1999). Meanings and Data Analysis. Dans H. Arksey, et P.T. Knight, (Ed.), *Interviewing for Social Scientists: An Introductory resource with examples*. (149-173). London : SAGE Publications, Ltd.
- Arpagian, N. (2010). La cybersécurité. Paris : Les Presses Universitaires de France.
- Association québécoise Plaidoyer Victime. (2014). 24 heures textos. Repéré à <http://www.aqpv.ca/index.php/services-et-activites/2013-03-11-20-03-38/16-services-et-activites/158-24-heures-textos>.
- Banque Mondiale. (2016). Utilisateurs Internet (pour 100 personnes). Repéré à <http://donnees.banquemondiale.org/indicateur/IT.NET.USER.P2?locations=CA>
- Barbier, M. (2010). La face cachée de la violence conjugale : la relation d'emprise, une violence dissimulée, Dans G. Francequin, *Tu me fais peur quand tu cries ! Sortir des violences conjugales* (p. 53-61). Toulouse : ERES.
- Baribeau, C. (2009). Analyse des données des entretiens de groupe. *Recherches qualitatives*, 28(1), 133-148.
- Blais, M. et Martineau, S. (2006). L'analyse inductive générale : description d'une démarche visant à donner un sens à des données brutes. *Recherches Qualitatives*, 26(2), 1-18.
- Casey, E. (2011). Cyberstalking. Dans E. Casey (dir.), *Digital Evidence and Computer Crime. Forensic Science, Computer and the Internet*. (3e ed. P.421- 434). New-York: Elsevier.
- Cattaneo, B.L. Cho, S. et Botuck, S. (2011). Describing Intimate Partner Stalking Over Time : an Effort to Inform Victim-Centered Service Provision. *Journal of Interpersonal Violence*, 26(17), 3428-3454.
- Chagnon, R. Côté, L. et Mikaelian, V. (2015). Le droit criminel, la justice transformatrice et la violence faite aux femmes : regards croisés. *Droits et libertés*, 34 (1) : 38-40.

- Code criminel, (L.R.C. (1985), c. C-46). Repéré à <http://laws-lois.justice.gc.ca/fra/lois/c-46/page-138.html#docCont>
- Cohen, E.L. et Felson, M. (1979). Social Change and Crime Rate Trends: a Routine Activity Approach. *American Sociological Review*, 44(4), 588-608.
- Commissariat à la protection de la vie privée du Canada. (mai 2013). Ce qu'une adresse IP peut révéler à votre sujet. Repéré à [https://www.priv.gc.ca/information/research-recherche/2013/ip\\_201305\\_f.pdf](https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_f.pdf)
- Côté, I. (2017). *L'évolution des pratiques en maison d'hébergement pour femmes victimes de violence conjugale au Québec*, Montréal, Université de Montréal, École de travail social, Thèse de doctorat inédite
- Cousineau, M-M. et Ouellet, F. (2014). Les femmes victimes de violence conjugale au Québec. Examen des caractéristiques de la femme, de l'homme et de la relation. Dans M. Rinfret-Raynor, É. Lesieux, M-M. Cousineau, S. Gauthier, É. Harper (dir.), *Violence envers les femmes. Réalités complexes et nouveaux enjeux dans un monde en transformation* (1<sup>ère</sup> éd., p.117-134). Québec : Presses de l'Université du Québec.
- Desgens-Pasanau, G. et Freyssinet, E. (2009). *L'identité à l'ère numérique*. Dalloz : Paris.  
IBN : 9782247080618.
- Deslauriers, J.P. et Kérisit, M. (1997). Le devis de la recherche qualitative. Dans J. Poupart, J.P. Deslauriers, L.H. Groulx, A. Laperrière, R. Mayer, et A.P. Pires, *La recherche qualitative : Enjeux épistémologiques et méthodologiques*, (p.85-111). Montréal: Gaëtan Morin Éditeur.
- Dimond, J.P. Fiesler, C. et Bruckman, A.S. (2011). Domestic violence and information communication technologies. *Interacting with computers*, 23(5), 413-421.
- Dubé, M. et Drouin, C. (2014). Démystifier le rôle de la planification dans l'homicide conjugal. Dans M. Rinfret-Raynor, É. Lesieux, M-M. Cousineau, S. Gauthier, É. Harper (dir.), *Violence envers les femmes. Réalités complexes et nouveaux enjeux dans un monde en transformation* (1<sup>ère</sup> éd., p.135-147). Québec : Presses de l'Université du Québec.
- Dubé, M. Drouin, C. (2015). Les TIC : une voie empruntée pour le harcèlement criminel dans la relation conjugale. Présentation Power Point.
- Fassin, D. (1990). Décrire. Entretien et observation. Dans D. Fassin, et Y. Jaffré, (dir.), *Sociétés, développement et santé*, (p. 87-106). Paris : Les Éditions Ellipses.
- Fleishman, G. (2011). How the Iphone knows where you are. Repéré à [http://www.macworld.com/article/1159528/how\\_iphone\\_location\\_works.html](http://www.macworld.com/article/1159528/how_iphone_location_works.html)

- Fontana, A. & Frey, J. (2008). The Interview: from neutral stance to political involvement. Dans N.K. Denzin, & S.Y. Lincoln (dir.), *Collecting and Interpreting qualitative materials* (3<sup>e</sup> ed., p. 115-160). Thousand Oaks, Californie: SAGE Publications.
- Forte, D. et de Donno, A. (2010), Mobile Network Investigations. Dans E. Casey. Handbook of Digital Forensic and Investigation. (P.517-557). Burlington, MA: Elsevier Academic Press.
- Fusco, C.A. (2014). Stalking 2.0: The era of cyberstalking (Mémoire de Maîtrise, Utica College). Accessible par ProQuest Dissertations & Theses. 1571120
- Gartner, R. et MacMillan, R. (1995). The effect of victim-offender relationship on reporting crimes of violence against women. *Canadian journal of criminology*, 37, 393-429.
- Gold, S. (2013) Understanding the Digital Fingerprint. *Network Security*, 2013(12),15-18.
- Gouvernement du Canada. (2015). Qu'est-ce que la violence conjugale?. Repéré à [http://violenceconjugale.gouv.qc.ca/comprendre\\_acte.php](http://violenceconjugale.gouv.qc.ca/comprendre_acte.php).
- Graves, W.M. (2014) Digital Archaeology: The Art and Science of Digital Forensics. Michigan : Addison-Wesley.
- Hirigoyen, M-F. (2010). Pourquoi il est important d'aider les femmes à refuser la violence psychologique, Dans G. Francequin, *Tu me fais peur quand tu cries ! Sortir des violences conjugales* (p. 53-61). Toulouse : ERES.
- Holt, T.J. et Bossler, A.M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25.
- Holt, T.J. (2011). Crime On-Line: Correlates, causes, and context. Dans Holt, T. J (Ed.), *Crime On-Line: correlates, causes, and context* (p. 3- 28). Durham : Carolina Academic Press.
- Horsman, G. et Conniss, R.L. (2015). An Investigation of Anonymous and Spoof SMS Ressources used for the purpose of Cyberstalking. *Digital Investigation*, 13, 80-93.
- Ifrah, L. (2010). L'information et le renseignement par Internet. Paris : Presses Universitaires de France.
- Johnson, M.P. (2014). Types de violence familiale. Dans M. Rinfret-Raynor, É. Lesieux, M-M. Cousineau, S. Gauthier, É. Harper (dir.), *Violence envers les femmes. Réalités complexes et nouveaux enjeux dans un monde en transformation* (1<sup>ère</sup> éd., p.15-31). Québec : Presses de l'Université du Québec.
- Lamoureux, D. (1992). Nos luttes ont changé nos vies. L'impact du mouvement féministe. Dans G. Daigle, et G. Rocher (dir.), *Le Québec en jeu. Comprendre les grands défis*. (p. 693- 711). Montréal: Les Presses de l'Université de Montréal.

- Locard, E. (1920). L'enquête criminelle et les méthodes scientifiques. Flammarion : Paris.
- Logan, T.K. Shannon, L. Cole, J. (2007). Stalking victimization in the context of intimate partner violence. *Violence and Victims*, 22(6), 669-683.
- Marcum, C. (2011). Examining Cyberstalking and Bullying : Causes, Context, and Control. Dans T.J. Holt, (Ed.), *Crime On-Line: correlates, causes, and context*, 175-191. Durham : Carolina Academic Press.
- Marganski, A. et Melander, L. (2015). Intimate partner violence victimization in the cyber and real world: examining the extend of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, 1-25. DOI: 10.1177/0886260515614283.
- McFarlane, J.M. Campbell, J.C. Wilt, S. Sachs, C.J. Ulrich, Y. Xu, X. (1999). Stalking and intimate partner femicide. *Homicide Studies* 3(4) : 300-316.
- Ministère de la Justice. (2015). Lois sur la violence familiale. Repéré à <http://www.justice.gc.ca/fra/jp-cj/vf-fv/lois-laws.html>.
- NNEDV. (2005). La haute technologie et ses méfaits : Technologies, Traque et Activités de défense. Violence against women online resources. Repéré à [http://nnedv.org/downloads/SafetyNet/NNEDV\\_HighTechTwist\\_PaperAndApxA\\_French08.pdf](http://nnedv.org/downloads/SafetyNet/NNEDV_HighTechTwist_PaperAndApxA_French08.pdf).
- Noaks, L. & Wincup, E. (2004). *Criminological Research, Understanding qualitative methods*. London : SAGE Publications.
- Norris, S.M. Huss, M.T. et Palarea, R.E. (2011). A pattern of violence: Analyzing the relationship between intimate partner violence and stalking. *Violence and Victims*, 26(1) : 103-115.
- Office of the Chief Coroner. (2011). Domestic Violence Death Review Committee – 2010, Eighth Annual Report. Toronto : Ontario
- Packer, M. (2011). *The science of qualitative research*. New-York : Cambridge University Press.
- Paillé, P. (1994). L'analyse par théorisation ancrée. *Cahiers de recherche sociologique*, 23, 147-181.
- Paludi, M.A. Wilmot, J. et Speach, L. (2010). Intimate partner violence as a workplace concern: impact on women's emotional and physical well-being and careers. Dans Paludi M.A., *Feminism and Women's rights Worldwide* (vol. 2, p.103-137). Santa Barbara, Californie : Praeger.

- Pires, A.P. (1997). Échantillonnage et recherche qualitative : essai théorique et méthodologique. Dans Poupart, J.P. Deslauriers, L.H. Groulx, A. Laperrière, R. Mayer, et A.P. Pires, *La recherche qualitative : Enjeux épistémologique et méthodologiques*, (p.173-210). Montréal: Gaëtan Morin Éditeur.
- Poupart, J. (1997). L'entretien de type qualitatif: considérations épistémologiques, théoriques et méthodologiques. Dans Poupart, J.P. Deslauriers, L.H. Groulx, A. Laperrière, R. Mayer, et A.P. Pires, *La recherche qualitative : Enjeux épistémologique et méthodologiques*, (p.173-210). Montréal: Gaëtan Morin Éditeur.
- Reyns, B.W. Henson, B. et Fisher, B. (2011) Being pursued online. Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and behavior*, 38(11): 1149-1169.
- Reyns, B.W. Henson, B. Fisher, B.S. Fox, K.A et Matt, M.R. (2015) A gendered lifestyle-routine activity approach to explaining stalking victimization in Canada. *Journal of Interpersonal violence*: 1-25.
- Rubin, H.J. & Rubin, I. (2005). *Qualitative Interviewing: The art of hearing Data* (2<sup>e</sup>). Thousand Oaks, Californie : SAGE publications.
- Safety Net Canada. (2013a). Organizational technology practices for anti-violence programs. Protecting the safety, privacy & confidentiality of women, youth & children. Repéré à [http://bcsth.ca/sites/default/files/SNC/SNC\\_OrgPracticesforAVPVAW-ES-2013.pdf](http://bcsth.ca/sites/default/files/SNC/SNC_OrgPracticesforAVPVAW-ES-2013.pdf).
- Safety Net Canada. (2013b). Canadian legal remedies for technology-enabled violence against women. Repéré à [http://bcsth.ca/sites/default/files/SNC\\_Executive%20SummaryLegalRemedies2013\\_2.pdf](http://bcsth.ca/sites/default/files/SNC_Executive%20SummaryLegalRemedies2013_2.pdf)
- Safety Net Canada. (2013c). Assessing technology in the context if violence against women & children. Examining benefits & Risks. Repéré à [http://bcsth.ca/sites/default/files/SNC/SNC\\_AssessingTechVAWC-ES-2013.pdf](http://bcsth.ca/sites/default/files/SNC/SNC_AssessingTechVAWC-ES-2013.pdf).
- Savoie-Zajc, L. (2009). L'entrevue semi-dirigée. Dans B. Gauthier (Dir.) *Recherche sociale : de la problématique à la collecte de données* (5<sup>e</sup> éd., p. 337-360). Québec : Presses de l'Université du Québec.
- Sheridan, L.P. et Grant, T. (2007). Is cyberstalking different?. *Psychology, Crime & Law*, 13(6), 627-640.
- Southworth, C. Finn, J. Dawson, S. Fraser, C. et Tucker, S. (2007). Intimate Partner Violence, Technology, and Stalking. *Violence Against Women*, 13(8), 842- 856.

- Stark, E. (2014). Une re-présentation des femmes battues. Contrôle coercitif et défense de la liberté. Dans M. Rinfret-Raynor, É. Lesieux, M-M. Cousineau, S. Gauthier, É. Harper (dir.), *Violence envers les femmes. Réalités complexes et nouveaux enjeux dans un monde en transformation* (1<sup>ère</sup> éd., p.33-51). Québec : Presses de l'Université du Québec.
- Statistiques Canada. (2011). Les refuges pour femmes violentées au Canada, 2010. (Publication N° 85-002-X). Repéré à <http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11495-fra.htm#a2>.
- Statistique Canada. (2016). La violence familiale au Canada : un profil statistique, 2014. (Publication n°11-001-X). Repéré à <http://www.statcan.gc.ca/daily-quotidien/160121/dq160121b-fra.pdf>
- Tilstone, W.J. Savage, K.A. et Clark, L.A. (2006). *Forensic Science: An Encyclopedia of History, Methods, and Techniques*. ISBN: 9781280711756.
- Tjaden, P.G. (2014) Stalking and Cyberstalking. Dans J.S. Albanese (dir.), *The encyclopedia of criminology and criminal justice* (p.1-6). Hoboken, N-J: John Wiley & Sons Inc.
- Turnbull, B. et Randhawa, S. (2015). Automated event and social network extraction from digital evidence sources with ontological mapping. *Digital Investigation*, 13, 94- 106.
- Wall, D.S. (2001). *Crime and the Internet*. New-York: Routledge.

## ANNEXE 1

### **FORMULAIRE D'INFORMATION ET DE CONSENTEMENT Pour les experts des traces numériques participant à l'étude**

#### **Les traces numériques au secours des femmes victimes de harcèlement criminel**

Étudiante chercheuse : Annie Bernier, étudiante à la Maîtrise, École de criminologie,  
Université de Montréal  
Directrice de recherche : Marie-Marthe Cousineau, professeure titulaire, École de  
criminologie, Université de Montréal

Vous êtes invité à participer à un projet de recherche. Avant d'accepter, veuillez prendre le temps de lire ce document présentant les conditions de participation au projet. N'hésitez pas à poser toutes les questions que vous jugerez utiles à la personne qui vous présente ce document.

#### **A) RENSEIGNEMENTS AUX PARTICIPANTS**

---

##### **1. Objectifs de la recherche**

Ce projet vise à dresser un portrait de l'utilisation des traces numériques pour la constitution de la preuve de harcèlement criminel dans les cas de violence conjugale. Pour ce faire, nous comptons sur la participation d'experts en traces numériques et de policiers afin de nous renseigner sur les différents avantages et désavantages que peuvent présenter les nouvelles technologies dans ce contexte.

##### **2. Participation à la recherche**

Votre participation consiste à accorder une entrevue à l'étudiante chercheuse qui vous demandera spécifiquement comment les traces numériques sont répertoriées et quels dispositifs doivent être mis en place pour assurer la sécurité des femmes et des maisons d'hébergement.

L'entrevue devrait durer environ une heure. Le lieu et le moment de l'entrevue seront déterminés avec l'étudiante chercheuse, selon vos disponibilités.

Cette entrevue sera enregistrée, avec votre autorisation, sur support audio afin de permettre à l'intervieweuse une écoute active durant l'entretien et d'en faciliter ensuite la transcription aux fins d'analyse.

##### **3. Risques et inconvénients**

Il n'y a pas de risque particulier à participer à ce projet.

##### **4. Avantages et bénéfices**

L'avantage de ce projet est de pouvoir sensibiliser les femmes en maison d'hébergement à une utilisation plus sécuritaire de la technologie dans leur contexte. Vous contribuez ainsi à la documentation d'un phénomène nouveau et préoccupant.

##### **5. Confidentialité**

Étant donnée la nature de votre participation à l'étude en tant qu'informateur clé, votre nom ainsi que votre titre seront publiés, à moins d'avis contraire de votre part. Ainsi, afin de vous donner le crédit qui

vous revient, les informations que vous nous fournirez durant l'entretien seront citées en votre nom. De plus, les informations ainsi citées seront plus crédibles si l'expert est identifiable. Les données seront conservées dans un local barré auquel seules l'étudiante et sa directrice ont accès et sur un disque dur externe protégé par un mot de passe. Les notes et enregistrements seront transcrits dans un premier temps pour les besoins d'analyse, et seront par la suite systématiquement détruits, à la fin du projet. Aucune donnée, quelle qu'elle soit, ne sera conservée au-delà de ce délai.

## 6. Droit de retrait

Votre participation à ce projet est entièrement volontaire et vous pouvez à tout moment refuser de répondre à une question ou vous retirer de la recherche sur simple avis verbal et sans devoir justifier votre décision, sans conséquence pour vous.

Si vous décidez de vous retirer de la recherche, veuillez communiquer avec la chercheuse à l'adresse courriel indiquée ci-dessous. À votre demande, tous les renseignements qui vous concernent pourront alors être détruits. Cependant, après le déclenchement du processus de publication, il sera impossible de détruire les analyses et les résultats portant sur vos données.

## B) CONSENTEMENT

### Déclaration du participant

- Je comprends que je peux prendre mon temps pour réfléchir avant de donner mon accord ou non à participer à la recherche.
- Je peux poser des questions à l'équipe de recherche et exiger des réponses satisfaisantes.
- Je comprends qu'en participant à ce projet de recherche, je ne renonce à aucun de mes droits ni ne dégage les chercheurs de leurs responsabilités.
- J'ai pris connaissance du présent formulaire d'information et de consentement et j'accepte de participer au projet de recherche.
- Je consens à ce que les données recueillies dans le cadre de cette étude soient utilisées pour des projets de recherche subséquents de même nature, conditionnellement à leur approbation par un comité d'éthique de la recherche et dans le respect des mêmes principes de confidentialité et de protection des informations. **Oui**  **Non**
- Je consens à ce que mon entrevue soit enregistrée sur support audio **Oui**  **Non**

Signature du participant : \_\_\_\_\_ Date : \_\_\_\_\_

Nom : \_\_\_\_\_ Prénom : \_\_\_\_\_

### Engagement de l'étudiante chercheuse

J'ai expliqué au participant les conditions de participation au projet de recherche. J'ai répondu au meilleur de ma connaissance aux questions posées et je me suis assurée de la compréhension du participant. Je m'engage, avec l'équipe de recherche, à respecter ce qui a été convenu au présent formulaire d'information et de consentement.

Signature de l'étudiante chercheuse : \_\_\_\_\_ Date : \_\_\_\_\_  
(ou de son représentant)

Nom : \_\_\_\_\_ Prénom : \_\_\_\_\_

**Pour toute question relative à l'étude, ou pour vous retirer de la recherche, veuillez communiquer avec Annie Bernier à l'adresse courriel [annie.bernier.4@umontreal.ca](mailto:annie.bernier.4@umontreal.ca).**



Pour toute préoccupation sur vos droits ou sur les responsabilités des chercheurs concernant votre participation à ce projet, vous pouvez contacter le Comité d'éthique de la recherche en arts et en sciences par courriel à l'adresse [ceras@umontreal.ca](mailto:ceras@umontreal.ca) ou par téléphone au 514 343-7338 ou encore consulter le site Web <http://recherche.umontreal.ca/participants>.

Toute plainte relative à votre participation à cette recherche peut être adressée à l'ombudsman de l'Université de Montréal en appelant au numéro de téléphone 514 343-2100 ou en communiquant par courriel à l'adresse [ombudsman@umontreal.ca](mailto:ombudsman@umontreal.ca) (**l'ombudsman accepte les appels à frais virés**).

**L'impact des nouvelles technologies en violence conjugale**

Étudiante chercheuse : Annie Bernier, étudiante à la Maîtrise, École de criminologie,  
Université de Montréal  
Directrice de recherche : Marie-Marthe Cousineau, professeure titulaire, École de  
criminologie, Université de Montréal

Vous êtes invité à participer à un projet de recherche. Avant d'accepter, veuillez prendre le temps de lire ce document présentant les conditions de participation au projet. N'hésitez pas à poser toutes les questions que vous jugerez utiles à la personne qui vous présente ce document.

**A) RENSEIGNEMENTS AUX PARTICIPANTS**

---

**1. Objectifs de la recherche**

Ce projet vise à dresser un portrait des conséquences que peuvent avoir les nouvelles technologies pour les femmes victimes de violence conjugale en maison d'hébergement. Pour ce faire, nous comptons sur la participation de femmes victimes de violence conjugale et d'intervenantes en maison d'hébergement.

**2. Participation à la recherche**

Votre participation consiste à accorder une entrevue à l'étudiante chercheuse qui vous demandera spécifiquement comment les nouvelles technologies ont pu avoir un impact dans l'intervention que vous menez auprès des femmes, dans les maisons d'hébergement.

L'entrevue devrait durer environ une heure trente minutes. Le lieu et le moment de l'entrevue seront déterminés avec l'étudiante chercheuse, selon vos disponibilités.

Cette entrevue sera enregistrée, avec votre autorisation, sur support audio afin de permettre à l'intervieweuse une écoute active durant l'entretien et d'en faciliter ensuite la transcription aux fins d'analyse.

**3. Risques et inconvénients**

Il n'y a pas de risque particulier à participer à ce projet.

**4. Avantages et bénéfices**

L'avantage de ce projet est de pouvoir sensibiliser les femmes en maison d'hébergement à une utilisation plus sécuritaire de la technologie dans leur contexte. Vous contribuez ainsi à la documentation d'un phénomène nouveau et préoccupant.

**5. Confidentialité**

Les renseignements personnels que vous nous donnerez demeureront confidentiels. Aucune information permettant de vous identifier d'une façon ou d'une autre ne sera publiée. Chaque participante à la recherche se verra attribuer un nom fictif (anonymisation des données). Les données seront conservées dans un local barré où seule l'étudiante et sa directrice ont accès et sur un disque dur externe protégé

par un mot de passe. Les notes et enregistrements seront transcrits dans un premier temps pour les besoins d'analyse, et seront par la suite systématiquement détruits, ainsi que toute information personnelle, à la fin du projet. Aucune donnée, quelle qu'elle soit, ne sera conservée au-delà de ce délai.

## 6. Droit de retrait

Votre participation à ce projet est entièrement volontaire et vous pouvez à tout moment refuser de répondre à une question ou vous retirer de la recherche sur simple avis verbal et sans devoir justifier votre décision, sans conséquence pour vous.

Si vous décidez de vous retirer de la recherche, veuillez communiquer avec la chercheuse à l'adresse courriel indiquée ci-dessous. À votre demande, tous les renseignements qui vous concernent pourront alors être détruits. Cependant, après le déclenchement du processus de publication, il sera impossible de détruire les analyses et les résultats portant sur vos données.

## B) CONSENTEMENT

---

### Déclaration du participant

- Je comprends que je peux prendre mon temps pour réfléchir avant de donner mon accord ou non à participer à la recherche.
- Je peux poser des questions à l'équipe de recherche et exiger des réponses satisfaisantes.
- Je comprends qu'en participant à ce projet de recherche, je ne renonce à aucun de mes droits ni ne dégage les chercheuses de leurs responsabilités.
- J'ai pris connaissance du présent formulaire d'information et de consentement et j'accepte de participer au projet de recherche.
- Je consens à ce que les données recueillies dans le cadre de cette étude soient utilisées pour des projets de recherche subséquents de même nature, conditionnellement à leur approbation par un comité d'éthique de la recherche et dans le respect des mêmes principes de confidentialité et de protection des informations. **Oui**  **Non**
- Je consens à ce que mon entrevue soit enregistrée sur support audio **Oui**  **Non**

Signature de la participante : \_\_\_\_\_ Date : \_\_\_\_\_

Nom : \_\_\_\_\_ Prénom : \_\_\_\_\_

### Engagement de l'étudiante chercheuse

J'ai expliqué à la participante les conditions de participation au projet de recherche. J'ai répondu au meilleur de ma connaissance aux questions posées et je me suis assurée de la compréhension de la participante. Je m'engage, avec l'équipe de recherche, à respecter ce qui a été convenu au présent formulaire d'information et de consentement.

Signature de l'étudiante chercheuse : \_\_\_\_\_ Date : \_\_\_\_\_  
(ou de son représentant)

Nom : \_\_\_\_\_ Prénom : \_\_\_\_\_

**Pour toute question relative à l'étude, ou pour vous retirer de la recherche, veuillez communiquer**

avec Annie Bernier à l'adresse courriel [annie.bernier.4@umontreal.ca](mailto:annie.bernier.4@umontreal.ca).

Pour toute préoccupation sur vos droits ou sur les responsabilités des chercheurs concernant votre participation à ce projet, vous pouvez contacter le Comité d'éthique de la recherche en arts et en sciences par courriel à l'adresse [ceras@umontreal.ca](mailto:ceras@umontreal.ca) ou par téléphone au 514 343-7338 ou encore consulter le site Web <http://recherche.umontreal.ca/participants>.

Toute plainte relative à votre participation à cette recherche peut être adressée à l'ombudsman de l'Université de Montréal en appelant au numéro de téléphone 514 343-2100 ou en communiquant par courriel à l'adresse [ombudsman@umontreal.ca](mailto:ombudsman@umontreal.ca) (**l'ombudsman accepte les appels à frais virés**).

Comité d'éthique de la recherche en arts et en sciences

Le 6 juillet 2015

**Objet: Approbation éthique – « L'impact des nouvelles technologies en violence conjugale »**

Mme Bernier,

Le Comité d'éthique de la recherche en arts et en sciences (CERAS) a étudié le projet de recherche susmentionné et a délivré le certificat d'éthique demandé à la suite de la satisfaction des exigences précédemment émises. Vous trouverez ci-joint une copie numérisée de votre certificat; copie également envoyée à votre directrice de recherche et à la technicienne en gestion de dossiers étudiants (TGDE) de votre département.

Notez qu'il y apparaît une mention relative à un suivi annuel et que le certificat comporte une date de fin de validité. En effet, afin de répondre aux exigences éthiques en vigueur au Canada et à l'Université de Montréal, nous devons exercer un suivi annuel auprès des chercheurs et étudiants chercheurs.

De manière à rendre ce processus le plus simple possible et afin d'en tirer pour tous le plus grand profit, nous avons élaboré un court questionnaire qui vous permettra à la fois de satisfaire aux exigences du suivi et de nous faire part de vos commentaires et de vos besoins en matière d'éthique en cours de recherche. Ce questionnaire de suivi devra être rempli annuellement jusqu'à la fin du projet et pourra nous être retourné par courriel. La validité de l'approbation éthique est conditionnelle à ce suivi. À la suite de la réception du dernier rapport de suivi en fin de projet, votre dossier sera clos.

Il est entendu que cela ne modifie en rien l'obligation pour le chercheur, comme indiqué sur le certificat d'éthique, de signaler au CERAS tout incident grave dès qu'il survient ou de lui faire part de tout changement anticipé au protocole de recherche.

Nous vous prions d'agréer, Madame, l'expression de nos sentiments les meilleurs.

Marie-Pierre Bousquet, Vice-présidente  
Comité d'éthique de la recherche en arts et en sciences (CERAS)  
Université de Montréal

c. c. Mme Marie-Marthe Cousineau, professeure titulaire, FAS-École de criminologie  
Mme Monique Lespérance, TGDE, FAS-École de criminologie

p. j. Certificat n°CERAS-2015-16-066-P

**adresse postale**  
C.P. 6128, succ. Centre-ville  
Montréal QC H3C 3J7

**adresse civique**  
Pavillon Lionel-Groulx  
3150, rue Jean-Brillant  
Local C-9104  
Montréal QC H3T 1N8

Téléphone : 514-343-7338  
ceras@umontreal.ca  
www.ceras.umontreal.ca

## Grille d'entretien pour les intervenantes en maison d'hébergement

**Thèmes explorés : Les nouvelles technologies****Les politiques et protocoles mis en place dans la maison d'hébergement****L'anonymat des maisons****Les préoccupations**

- 
- Comment qualifierez-vous vos connaissances et votre aisance face aux possibilités des nouvelles technologies ?
  - Est-ce que vous avez remarqué des problématiques en lien avec les nouvelles technologies qui se posent à la maison d'hébergement ?
    - à la maison même (en particulier anonymat - comment)
    - pour les femmes
  - Comment les nouvelles technologies ont-elles changé vos tâches de tous les jours?
  - Est-ce que votre maison d'hébergement a mis en place des mesures, politiques ou des protocoles afin de contrer les conséquences des nouvelles technologies?
    - Quelles sont-elles? (Wi-Fi, utilisation des cellulaires, gestions des données de localisation, adresse IP cryptée)
    - Est-ce qu'elles ont été mises en place en prévention ou en réaction à un évènement qui aurait mis la sécurité des femmes ou l'anonymat de la maison en péril?
 

Dans quelle mesure ces interventions bousculent-elles la philosophie d'intervention de la maison ?
  - Quelles sont les problématiques en lien avec les nouvelles technologies qui vous préoccupent le plus?
    - pour la maison
    - pour les femmes

## Grille d'entrevue pour les experts des traces numériques

### **Thèmes explorés : Renseignements privés/ publics**

#### **Les traces numériques**

#### **La constitution de la preuve judiciaire**

#### **Les logiciels espions**

#### **La géolocalisation**

- 
- Dans quelle mesure les renseignements mis sur les réseaux sociaux sont du domaine privé ou public?
  - Dans quelle mesure les règles s'appliquent-elles aux instances officielles (policiers, enquêteurs, magistrats...)
  - Comment les traces numériques laissées par Internet ou par les téléphones cellulaires peuvent-elles être retracées?
    - Comment ces traces peuvent-elles constituer une menace pour la femme victime de violence conjugale?
    - Comment, au contraire, ces traces peuvent-elles être utiles pour les femmes ?
      - Comment la preuve peut-elle être constituée à partir de ces traces?
      - Dans quelle mesure une preuve ainsi constituée peut-elle servir en cour dans l'éventualité de poursuites judiciaires – comment s'assurer qu'elles soient recevables en preuve
  - Quels sont TOUS les moyens de localiser quelqu'un?
  - Comment protéger les maisons d'hébergement et les femmes de la géolocalisation?
  - Comment savoir si un téléphone est espionné par un logiciel-espion?
  - Quels moyens recommanderiez-vous aux maisons d'hébergement afin de se protéger contre la localisation et le piratage de leur poste d'Internet?
  - Et pour les femmes, comment
    - Assurer leur sécurité
    - Garder une trace des menaces en vue d'une éventuelle poursuite devant les tribunaux



## Grille d'entrevue des policiers spécialisés en violence conjugale

### Thèmes abordés : Harcèlement criminel

Preuve judiciaire

Traces numériques

Victimes

Processus de plainte

---

- D'un point de vue légal, qu'est ce qui constitue l'infraction de harcèlement criminel?
  - Quels sont les éléments primordiaux à y retrouver?
- Voyez-vous beaucoup de plaintes de harcèlement criminel dans les cas de violence conjugale?
- Quelles sont les techniques de harcèlement les plus fréquentes?
- Comment utilisez-vous les traces numériques pour la constitution de la preuve?
- Est-ce une preuve facile à faire?
- Quels sont les défis pour la victime quand elle veut porter plainte?
- Dans les plaintes de violence conjugale, en général, quels sont les préjugés/ appréhensions des victimes?
- Quels moyens recommanderiez-vous aux maisons d'hébergement afin de se protéger contre la localisation et le piratage de leur poste d'Internet?
- Et pour les femmes, comment
  - Assurer leur sécurité
  - Garder une trace des menaces en vue d'une éventuelle poursuite devant les tribunaux