Rapport de recherche sur l'avenir du travail policier

Soumis à la Fraternité des policiers et policières de Montréal

Benoît Dupont, Anthony Amicelle, Rémi Boivin,
Francis Fortin et Samuel Tanner

Table des matières

Introduction 4
Chapitre 1. Radicalisation, police et extrémisme violent 8
1. Radicalisation, extrémisme violent et société : un état des connaissances 9
1.1. Définir et appréhender la radicalisation 9
1.2. La dimension macro : les structures d'opportunités et leurs impacts cognitifs . 11
1.3. La dimension méso : socialisations violentes, entourages, réseaux, allégeances et sociabilités 12
1.4. La dimension micro : logiques psychosociales de l'engagement 15
1.5. Un cadre intégratif d'appréhension de la radicalisation 17
2. Les pratiques et expertises policières : besoins et défis anticipés 19
2.1. Défis structurels et opérationnels en matière de lutte contre la radicalisation . 20
2.2. Pratiques policières en matière de lutte contre la radicalisation 23
2.3. Impacts des technologies : la lutte contre la radicalisation en ligne 26
2.4. Lutte contre la radicalisation, formation et police 28
3. Les limites de la prévention et de la lutte contre la radicalisation 30
Références 34
Chapitre 2. Police et prévention de la cybercriminalité 38
1. La disponibilité et la fiabilité des instruments de mesure de la cybercriminalité 40
1.1. Les tendances récentes de la cybercriminalité 41
1.2. La sous-déclaration chronique des cybercrimes à la police 43
2. Les expertises policières disponibles et les besoins anticipés 45
2.1. Les perceptions qu'ont les patrouilleurs, les enquêteurs et les gestionnaires policiers de la cybercriminalité 45
2.2. Le rôle et les capacités des unités d'enquête spécialisées 48
2.3. Besoins en formations spécialisées et générales 51
2.4. Pertinence de faire appel à l'expertise complémentaire d'employés civils ou de bénévoles 54
2.5. Recueillir, accéder à et analyser la preuve numérique dans un environnement où la cryptographie est omniprésente et où les volumes de données augmentent exponentiellement 56
3. Les limites des stratégies mono-institutionnelles et le potentiel de l'intervention en partenariat 58

3.1. Trois stratégies d'intervention contre la cybercriminalité : répression, perturbation et réduction des méfaits 59
3.2. Efficacité et limites des modèles d'intervention en partenariat 61
Conclusion 63
Références 63
Chapitre 3. Les nouvelles contraintes procédurales et la productivité policière 70
1. La quantification du travail policier 70
2. Les risques associés à la quantification du travail policier 73
2.1. Augmenter la pression de rendement 73
2.2. L'effet de la surveillance du travail policier sur la sécurité 74
2.3 Profilage social, racial, ou criminel ? 77
Conclusion 78
Références 79
Chapitre 4. Les plateformes de médias sociaux et l'intervention policière 82
1. L'utilisation des médias sociaux 82
2. L'utilisation des médias sociaux dans un contexte de renseignement 85
3. Les manifestations virtuelles et le doxing 87
3.1. Les manifestations virtuelles 87
3.2. Médias sociaux et impacts du doxing (dénoncer et condamner 2.0) 88
4. La demande accrue en formation 91
Références 93
Chapitre 5. *Policing*, nouvelles technologies et algorithmes 97
1. Penser le rôle et la force d'action des nouvelles technologies 99
2. Le *policing* financier et l'exemple des algorithmes de détection 101
2.1. Trouver (technologiquement) l'aiguille dans la botte de foin 102
2.2. Surveiller et détecter des individus et des comportements suspects à l'ère du big data 102
2.3. Les formes de détection algorithmiques 103
2.4. Les algorithmes de détection à l'épreuve des faux-positifs 104
3. PredPol et l'exemple des algorithmes de prédiction 106
3.1. Les spécificités (à nuancer) du « predictive policing » 106
3.2. Retour sur le lancement commercial et les promesses du logiciel PredPol 107
3.3. Entre critiques d'efficacité prédictive et de justice sociale 109

3.4. Une finalité gestionnaire ? 111
4. Propos conclusifs sur les processus crucial d'appropriation des technologies 112
Références 114

Introduction

Dans un article publié il y a presque 15 ans et consacré aux vagues de réformes ayant déferlé sur le SPVM entre 1987 et 2005, l'éminent criminologue Jean-Paul Brodeur (2005) mettait en parallèle le souci des organisations policières d'adapter leurs fonctions et leurs pratiques à un environnement politique et social en constante évolution avec l'approche trotskyste de la révolution, qui refuse de se contenter d'avancées insignifiantes et énonce le besoin de poursuivre la révolution une fois le pouvoir conquis. Loin de se réjouir aveuglément de cette propension des services de police à adopter à marche forcée des réformes importées parfois hâtivement de pays jugés à l'avant-garde, mais refusant par ailleurs de sombrer dans la critique systématique de toute tentative d'améliorer la qualité des services offerts à la population, Jean-Paul Brodeur procède dans son article à l'analyse rigoureuse des tensions qui rythment inévitablement les ajustements de l'institution policière aux soubresauts de son environnement externe. Son souci majeur est d'identifier les pratiques permettant d'éviter un divorce désastreux entre les principes de sécurité et de justice qui sous-tendent le travail policier dans les démocraties libérales.

Force est de constater qu'une telle démarche analytique reste d'une grande actualité face aux rapides et profondes transformations technologiques et sociales associées depuis un quart de siècle à l'avènement de l'internet et à la mondialisation des échanges. Ce rapport réalisé à l'instigation de la Fraternité des policiers et policières de Montréal (FPPM) tente ainsi de mieux comprendre quelles sont les principales tendances sociotechniques venant modifier le travail policier. À l'exception du rapport publié en 2014 par le Conseil des académies canadiennes sur les défis organisationnels que devront relever les services de police au cours de la prochaine décennie (CAC 2014), aucun document ne dresse malheureusement à l'heure actuelle un portrait détaillé de ces tendances, qu'elles soient sociales, technologiques ou économiques. Pourtant, elles influencent et façonnent irrémédiablement les pratiques professionnelles au sein des institutions chargées de faire appliquer la loi et de garantir la sécurité des citoyens, et il est essentiel de documenter la nature de ces changements, ainsi que leur impact anticipé sur les institutions policières au cours des prochaines années.

Les auteurs de ce rapport proviennent tous du Centre international de criminologie comparée de l'Université de Montréal, l'un des principaux regroupements de chercheurs spécialisés sur les phénomènes criminels, leur contrôle et la sécurité. Ils y ont développé depuis quelques années des programmes de recherche ambitieux et novateurs sur la police, la sécurité, les stratégies de régulation et les nouvelles formes de déviance. La collaboration avec la FPPM que ce rapport incarne vient consolider les apports de ces recherches en proposant des recensions thématiques et critiques de la littérature scientifique disponible sur cinq tendances émergentes qui nous ont communément semblé prioritaires : la radicalisation, l'avènement d'une cybercriminalité de masse, les nouvelles contraintes procédurales du travail policier, l'explosion des médias sociaux et la nouvelle visibilité policière qu'elle induit, et l'automatisation du travail policier par les

algorithmes. Pour chacun de ces thèmes, une recension exhaustive de la littérature scientifique et professionnelle a été menée, ce qui permet de présenter les données quantitatives et qualitatives les plus significatives, d'examiner leur impact existant et attendu sur les politiques et les pratiques policières, avant de discuter des modalités d'adaptation envisageables pour les organismes d'application de la loi. Ce rapport est par conséquent divisé en cinq chapitres.

Le premier chapitre a pour objectif de dresser un portrait des enjeux entourant le phénomène de radicalisation appréhendé aussi bien sous l'angle cognitif que dans sa dimension de passage à l'acte. Loin de se limiter à une analyse de l'extrémisme violent centrée exclusivement sur le djihadisme, ce chapitre prend également en considération d'autres déclinaisons comme les mouvements identitaires et d'extrême-droite. Le cadre de réflexion présenté dans ce chapitre s'applique tout autant aux études sur les groupes anticapitalistes et d'extrême-gauche, ou encore les mouvements antiféministes ou anti-spécistes. Il explore le rôle que les organisations policières jouent dans sa compréhension, sa prévention et sa régulation. Tous les mouvements étudiés possèdent des dynamiques propres, qui sont bien distinguées les unes des autres, mais un certain nombre de défis sont néanmoins communs, notamment en matière d'anticipation des comportements radicaux et de leur prévention.

Le deuxième chapitre examine l'explosion de la cybercriminalité associée à la révolution numérique qui modifie en profondeur les relations économiques et sociales depuis un quart de siècle. Si les cybercrimes représentent maintenant près de la moitié de l'ensemble des crimes subis par les victimes dans les pays développés, les ressources et l'expertise policière disponibles n'ont pas suivi la même croissance exponentielle. Les statistiques de la cybercriminalité restent encore fragmentaires et manquent de fiabilité, ce qui ne favorise pas la redistribution des ressources policières requise par une transformation aussi profonde de la délinquance. On peut toutefois discerner certaines tendances qui démontrent la nécessité de considérablement renforcer l'expertise policière, aussi bien dans les unités d'enquête spécialisées que parmi les patrouilleurs en uniforme. Le rôle des partenaires issus du secteur privé et des ONG dans la lutte contre la cybercriminalité est également un sujet susceptible de reconfigurer les paramètres de l'intervention policière.

Le troisième chapitre se penche sur les nouvelles contraintes procédurales venant encadrer le travail policier. Aucun métier ne suscite autant d'intérêt parmi la population que celui de policier, dont les représentations foisonnent dans la presse d'information et les œuvres de fiction. Pourtant, aucun n'est aussi encadré, que ce soit par le biais des dispositions procédurales contenues dans le Code criminel canadien et la jurisprudence qui l'accompagne, le Code de déontologie policière québécois, ou encore les règlements internes afférents aux procédures et à la discipline. La complexité de cet encadrement est accentuée par la forte pression exercée par les organisations policières depuis quelques années afin d'augmenter la productivité de leurs agents, parfois au détriment de leur autonomie. La tendance à la quantification de chaque facette du travail policier est examinée, ainsi que les quatre risques organisationnels qui en découlent : minimiser la

complexité du travail policier, se focaliser sur le rendement plutôt que sur l'efficacité, dissuader les activités proactives, et encourager involontairement le profilage pour accélérer l'intervention policière.

Le quatrième chapitre analyse l'impact des plateformes de médias sociaux (Facebook, Twitter, LinkedIn), omniprésentes dans la vie quotidienne de la population, sur l'intervention policière. Cet effet est ambigu : d'une part, ces plateformes ont contribué à façonner un nouveau rapport à la visibilité et à la vie privée qui s'est traduit par l'accessibilité publique de vastes quantités d'informations personnelles continuellement mises à jour par les usagers. Les enquêteurs policiers peuvent librement consulter ces données dont l'obtention aurait probablement été plus difficile il y a quelques années seulement. Mais si les médias sociaux permettent une collecte automatisée et à grande échelle du renseignement criminel, ils exposent aussi les policiers qui en sont des utilisateurs tout aussi assidus que le reste de la population à une visibilité accrue de leurs décisions professionnelles (qui sont systématiquement filmées et diffusées en ligne lorsqu'elles se déroulent en public), ainsi que de leur vie privée, ce qui peut culminer en des actes d'intimidation.

Finalement, le cinquième chapitre étudie les modalités par lesquelles les algorithmes font leur apparition dans le travail policier. De manière simplificatrice, les algorithmes sont définis comme des séries d'instructions permettant de traiter de gigantesques quantités de données afin d'obtenir un résultat. Ils permettent aux organisations d'augmenter considérablement le volume, la variété et la vélocité des données qu'elles collectent et qu'elles utilisent dans leurs différents processus de prise de décision. Après avoir présenté les implications générales de la diffusion des algorithmes dans les pratiques de surveillance et de renseignement, ce chapitre montre comment ils sont utilisés concrètement pour contrôler les flux de biens, de personnes ou financiers, et quelles promesses ils font miroiter en termes de police prédictive. Il se termine par une réflexion sur les points de friction qui se manifestent entre les attentes démesurées qui accompagnent généralement le déploiement des nouvelles technologies et la réalité de leur appropriation sur le terrain.

Comme le soulignaient avec le même sens de l'absurde et à quelques décennies d'intervalle Paul Valéry et Yogi Berra, « l'avenir est comme le reste : il n'est plus ce qu'il était ». Le rythme effréné du développement et de l'obsolescence subséquente des nouvelles technologies bouscule l'ensemble des organisations, leurs structures, leurs stratégies et leurs pratiques. Les services de police, dont le mandat est d'assurer la sécurité de la population quel que soit le contexte économique et social ne sont pas épargnés par cette lame de fond. Ils se trouvent même en première ligne face à l'exploitation criminelle que des délinquants tout aussi innovants que les entreprises les plus créatives de la Silicon Valley font des technologies numériques. Toutefois, l'adaptation des institutions policières à ce nouvel environnement de travail ne peut se faire sur la seule considération d'une efficacité accrue qui viendrait oblitérer les principes démocratiques qu'elles ont le devoir d'incarner. Comme les auteurs de ce rapport le soulignent unanimement, c'est uniquement dans la quête perpétuelle d'un fragile équilibre entre innovation,

performance, sécurité et justice qu'elles conserveront la confiance des citoyens au nom desquels elles agissent.

Références

Brodeur, J.-P. (2005), Trotsky in blue : Permanent policing reform, *The Australian and New Zealand Journal of Criminology*, 38 (2) : 254-267.

CAC (2014), *Le maintien de l'ordre au Canada au XXIe siècle : Une nouvelle police pour de nouveaux défis*, Conseil des académies canadiennes, Ottawa.

Chapitre 1. Radicalisation, police et extrémisme violent
Samuel Tanner

Les attaques récentes qui se sont produites à Paris, Londres, Berlin, Québec, Toronto ou Pittsburg, pour n'en mentionner que quelques-unes, sont autant de déclinaisons de l'extrémisme violent responsable de bouleversements majeurs dans les sociétés qu'il frappe, tant sur le plan social, politique que de santé publique. On observe des transformations de politiques publiques de sécurité, de prévention et de lutte contre le terrorisme, par la mise sur pied de nouveaux instruments et acteurs de sa régulation dont les implications demeurent encore à évaluer. Ces évènements ont forcé les organisations policières à y faire face dans un contexte où les connaissances sur ce phénomène sont encore embryonnaires, mais aussi où les ressources – humaines, matérielles, technologiques – demeurent limitées.

Ces attaques sont envisagées comme le produit d'une *radicalisation*, concept désormais incontournable de lecture et de compréhension de l'extrémisme violent. Or la notion de radicalisation, si elle exerce un fort impact politique, nécessite une attention particulière pour saisir la réalité complexe – les dynamiques et logiques par lesquelles cette violence se développe et opère – que ce terme recouvre. Laissant entendre une double dimension, à la fois cognitive et de passage à l'acte, une appréhension du sens commun de la notion de radicalisation présume un passage automatique de l'une à l'autre, ce qui est problématique.

Par ailleurs, la réflexion sur la radicalisation, ainsi que l'extrémisme violent, est largement demeurée centrée sur le djihadisme. Pourtant, d'autres déclinaisons et répertoires d'action s'observent dans nos sociétés, parmi lesquelles les mouvements identitaires et d'extrême-droite, ou encore anticapitalistes et d'extrême-gauche, antiféministes, les groupes aux préoccupations environnementales, ou encore anti-spécistes. Tous ces mouvements, jusqu'ici peu étudiés, si ce n'est pour l'extrême-gauche, présentent un potentiel important de perturbation de la société et de l'ordre public.

Ce chapitre a pour objectif de dresser un portrait généraliste mais précis des enjeux entourant le phénomène de radicalisation et, en particulier, la question du rôle ou de la place des organisations policières dans sa compréhension, sa prévention et sa régulation. Chacun des mouvements répertoriés ci-dessus se caractérise par ses dynamiques propres. Or, tous n'ont pas été traités par la recherche avec autant d'attention que l'extrémisme islamique. Ceci vaut autant en matière de politiques publiques que de stratégies de régulation développées par les organisations policières.

Une première section dressera une compréhension fine de la notion de radicalisation (qu'il faut distinguer de l'extrémisme violent). Elle reposera sur les résultats de recherche développés à partir de travaux sur l'Islam radical ainsi que l'extrême-droite, qui ont à ce jour concentré les efforts des chercheurs. Deuxièmement, nous dresserons un état des

connaissances et des défis qu'il reste à mener sur la prévention, l'anticipation et la réponse policière face à la radicalisation et l'extrémisme violent. Enfin, nous proposerons une réflexion sur les limites des pratiques/politiques de lutte contre la radicalisation et l'extrémisme violent, tout en offrant des propositions pour y palier.

1. Radicalisation, extrémisme violent et société : un état des connaissances

Au cours des dernières années, et suite aux nombreux attentats liés à l'extrémisme violent qui ont bouleversé des sociétés occidentales, parmi lesquelles la France, le Canada, la Belgique, les États-Unis, la Grande Bretagne, ou encore l'Allemagne, pour ne citer que quelques exemples, la notion de radicalisation, servant de cadre d'appréhension et de compréhension à ces phénomènes, a gagné une très haute visibilité. Or cette notion, à laquelle un impact émotionnel et politique fort est associé, offre une basse résolution dans la compréhension des phénomènes qu'elle tend pourtant à décrire. En effet, elle présuppose une double dimension, à la fois cognitive et de passage à l'acte qui présume une transition automatique de l'un à l'autre, ce qui est problématique comme nous allons le voir. Cette section vise à définir, décortiquer et expliciter davantage la notion de radicalisation.

1.1. Définir et appréhender la radicalisation

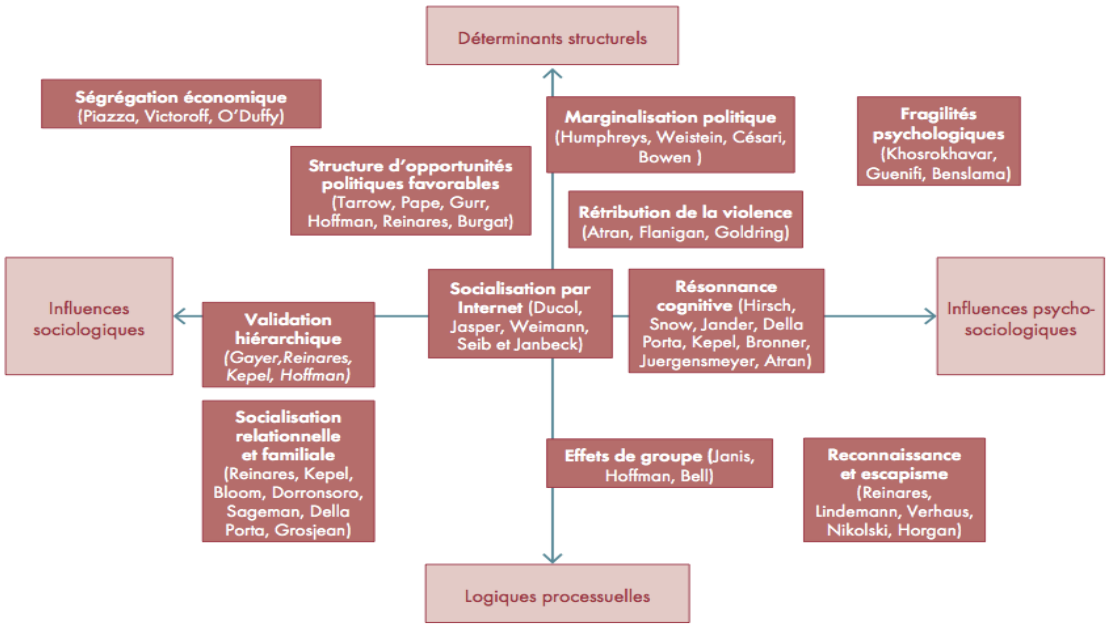
L'extrémisme violent est-il systématiquement le résultat d'une radicalisation ? La radicalisation, quant à elle, mène-t-elle automatiquement à l'extrémisme violent ? Ces questions soulèvent des problèmes complexes et pour y répondre il est nécessaire dans en premier lieu de distinguer ces deux notions. Si l'extrémisme violent renvoie à une pensée dogmatique qui préconise des modes d'actions violents (ex. extrême-droite, djihadisme), la radicalisation, quant à elle, est plus complexe. Selon Crettiez et Sèze (2017), celle-ci s'envisage comme :

> *« L'adoption progressive et évolutive d'une pensée rigide, vérité absolue et non négociable, dont la logique structure la vision du monde des acteurs, qui usent pour la faire entendre de répertoires d'action violents, le plus souvent au sein de structures clandestines, formalisées ou virtuelles, qui les isolent des référents sociaux ordinaires et leur renvoient une projection grandiose d'eux-mêmes. Trois éléments fondent donc l'approche de la radicalisation : sa dimension évolutive, l'adoption d'une pensée sectaire, l'usage de la violence armée » (Crettiez et Sèze 2017 : 10).*

Ainsi, saisir la radicalisation – et ultimement l'extrémisme violent – pose une double énigme. La première vise à comprendre ce que les personnes pensent mais aussi le processus par lequel elles en viennent à penser ce qu'elles pensent. Puis, une seconde énigme vise à comprendre comment ces personnes progressent – ou pas – de la pensée à l'action. Ces questions ont fait l'objet d'une littérature abondante et la présente section

vise à présenter les faits saillants de la recherche (Borum 2012a, 2012b, Crettiez et Sèze 2017, Ducol 2015, Kudnani 2012, Neuman 2013, Alimi, Demetriou, Bosi, 2015, Sommier 2012). La notion de radicalisation évacue une réflexion qui porte strictement sur les causes du terrorisme, ou de l'extrémisme violent (pourquoi ?) en mettant davantage l'accent sur les **processus** et les dynamiques (comment ?) qui sous-tendent l'engagement des individus dans des parcours pouvant mener à l'extrémisme violent. À cet effet, Il apparaît pertinent d'adopter un cadre d'appréhension de ce phénomène qui tienne compte d'une triple approche à la fois centrée sur les individus (niveau micro), leurs affiliations et leurs sociabilités (niveau méso), ainsi que, ultimement, les dimensions structurelles de l'environnement dans lequel ils évoluent (niveau macro).

Figure 1 : Modèle intégratif de compréhension de la radicalisation (Crettiez et Sèze 2017 : 11)



Dans un objectif intégratif de la littérature traitant du processus de radicalisation, Crettiez et Sèze (2017) regroupent les connaissances développées autour de **deux axes principaux de réflexion** (cf. figure 1). Dans un **axe horizontal**, les théories se répartissent sur un continuum qui s'étend des approches dites sociologiques et organisationnelles aux approches psychologiques. Les premières renvoient aux influences de l'environnement (famille, milieu professionnel, amis, etc.), alors que les secondes évoquent des dimensions dispositionnelles (personnalité, vulnérabilité psychologique, etc.). L'**axe vertical** classe les théories sur un continuum qui envisage à une extrémité les dimensions structurelles qui auraient un impact direct sur la radicalisation (la marginalisation politique, la frustration causée par des rétributions attendues, mais refusées, etc.) puis, à l'autre extrémité, des logiques processuelles (l'influence que les individus vivent au sein des groupes auxquels ils sont affiliés et ce, non pas tant en termes déterministes, mais bien plutôt processuels et de construction de cadres de références). Tel qu'indiqué, ce cadre d'appréhension

nécessite de s'envisager à travers une lecture qui opère une distinction entre approche macro-, méso- et microsociologique de la radicalisation et qui envisage le phénomène de radicalisation, y compris celle menant à la violence, comme avant tout un processus. Passons en revue chacune de ces dimensions.

1.2. La dimension macro : les structures d'opportunités et leurs impacts cognitifs

La dimension macro évoque les raisons structurelles d'un engagement radical. La littérature renvoie alors au concept de structure des opportunités politiques, soit *« la manière dont l'État facilite ou réprime l'action collective, affectant ainsi directement son coût tout comme les gains anticipés par les acteurs »* (Ancelovici et Rousseau 2009 : 6). Parmi ces dimensions, évoquons à titre d'exemples la ségrégation économique ou la marginalisation politique qui peuvent servir de déclencheurs pour certains de s'engager violemment pour contester une situation vécue comme étant injuste. Cette ségrégation peut d'autant plus mener à une radicalisation si elle est perçue comme le résultat d'une politique intentionnelle du pouvoir en place, ou d'une majorité (Gurr 1970, Pape 2005, McAdam, Tarrow et Tilly 2001). Ce n'est pas tant un état absolu (pauvreté, par exemple) plutôt que subi qui est susceptible de mener à des actions violentes. La marginalisation politique d'un groupe, soit sa mise à l'écart intentionnelle des décisions politiques au profit d'un autre groupe dominant, rival ou hostile, peut également être source de violence pour le groupe qui cherche alors à entrer dans le champ politique et s'imposer comme un interlocuteur crédible.

Par ailleurs, le contexte international et/ou national peut également conduire certains acteurs à se radicaliser, confrontés à des situations qu'ils jugent inacceptables ou injustes. Un exemple de contexte national s'illustre par le cas où un gouvernement soutient un allié dans un conflit armé (ex. le soutien apporté aux États-Unis dans leur guerre contre le djihadisme en Syrie). Quant au contexte international, on peut relever le traumatisme vécu par certaines communautés dans un contexte « d'occupation » du territoire par une force armée étrangère, facilitant par exemple le soutien d'une partie de la population musulmane au djihadisme (dans le cadre national ou à l'étranger). Dans ce cadre, Robert Pape a montré l'effet traumatisant de l'occupation de troupes occidentales dans des lieux saints pour la communauté musulmane comme source importante de motivation des attentats suicides (Pape 2005).

Aussi éloignées puissent sembler les dimensions dont il est question ici, il ne faut pas pour autant négliger leurs incidences sur la perception que s'en font les acteurs. Une réflexion sur la radicalisation, nécessite de tenir compte des dimensions cognitives et idéologiques qui accompagnent les perceptions et l'éventuelle trajectoire des individus vers l'extrémisme violent. En particulier, la littérature a identifié une série de facteurs.

Il faut tout d'abord tenir compte de ce que nous pourrions qualifier de « cadre d'injustice ». Par exemple, et en lien aux attaques djihadistes, la lecture religieuse diffusée par certains prédicateurs salafistes, via les outils numériques, mais aussi les chaînes satellites, a permis

d'ancrer le sentiment d'injustice fondé sur des explications victimaires relative à ce qui est perçu à travers le durcissement des politiques de sécurité mis en place par les pays occidentaux, se superposant à la lutte globale contre le djihadisme, comme une attaque généralisée de la communauté occidentale contre la communauté musulmane. Ici, l'idéologie agit comme un ressort victimaire.

En second lieu, relevons la prise en considération de l'influence des doctrines et idéologies professées par les militants : valorise-t-elle la violence ? C'est notamment le cas de l'idéologie religieuse et millénariste de Daesh, à laquelle se superpose une valorisation de l'expérience militaire. Si dans le cas précédent nous avons décrit une doctrine à ressort victimaire, il est ici question de doctrine violente.

Enfin, et loin d'épuiser une recension exhaustive des dimensions cognitives et idéologiques liées à la radicalisation, il ne faut pas non plus négliger le lien entre idéologie et émotions, où l'intensité de ces dernières est susceptible d'encourager l'action violente et radicale. Ainsi, le rôle des affects et émotions dans l'intentionnalité de l'action radicale s'avère important (Aminzade et McAdam 2002). À titre d'exemple, mentionnons le cas de l'idéologie islamiste dans le contexte de la Tchétchénie et de la valorisation de la guerre sacrée (djihad) contre l'ennemi infidèle, encouragée par la façon brutale avec laquelle les Russes administrent le pays et encouragent une réaction hostile (Crettiez et Sèze 2017).

Rappelons qu'en accord avec la figure 1, l'ensemble de ces dimensions doit être envisagé comme un processus cognitif : les individus s'engagent pas à pas sur ces chemins idéologiques qui, en d'autres contextes, auraient pu leur sembler déraisonnables (Sommier 2012; Tanner 2011, 2012).

1.3. La dimension méso : socialisations violentes, entourages, réseaux, allégeances et sociabilités

Si les structures macrosociologiques exercent une influence dans l'engagement d'un individu sur la voie de la radicalisation, elles ne suffisent pas à elles-seules à précipiter un individu sur la voie de la radicalisation. Bien souvent cette influence s'opère à travers les groupes, ou affiliations, auxquels s'identifient les personnes, ainsi que l'importance des effets de socialisation et d'influence qui existent en leur sein. Tel que l'affirment Crettiez et Sèze :

> *« C'est tout d'abord la validation hiérarchique de l'entrée dans la violence qui doit être soulignée : la radicalisation sera d'autant plus forte et rapide qu'elle bénéficie du soutien moral et plus encore opérationnel d'acteurs politiques ayant une posture hiérarchique dominante sur le personnel radicalisé » (Crettiez et Sèze 2017 : 16).*

Ceci s'observe particulièrement dans le contexte où des acteurs étatiques ont fourni des ressources (humaines, matérielles, financières) à des groupes armés étrangers dans le cadre de conflits. On peut citer le cas du gouvernement pakistanais et son soutien et

influence dans la radicalisation du mouvement séparatiste sikh en Inde (Gayer 2009). On retrouve dans ce contexte les groupes où l'entourage offre à la fois une validation opérationnelle, en fournissant par exemple des instructions sur la manière d'opérer, mais aussi morale, en offrant un cadre cognitif ou idéologique justifiant les actions violentes. Il ne faut pas non plus négliger le rôle des réseaux virtuels, sur lesquels nous allons revenir, comme par exemple le site de droite radicale/alt right thedailystormer.org et les ressources morales qu'il fournit pour les activistes de droite (Hawley 2017; Wendling 2018). Aussi, en matière de radicalisation islamiste, il ne faut pas non plus négliger le rôle que peuvent jouer certains imams dans l'endoctrinement radical d'individus, à la fois dans les pays arabes, mais aussi dans les sociétés occidentales (Kepel 2015). Crettiez et Sèze rappellent enfin toute l'importance de la géographie de la socialisation au djihad et la radicalisation de jeunes Occidentaux ayant réalisé un séjour dans des zones où la violence est encouragée, valorisée et apprise, ce qui facilite ainsi le passage à l'acte (Crettiez et Sèze 2017)[1].

La radicalisation peut aussi s'opérer par le biais d'une socialisation familiale et relationnelle. L'appartenance à une lignée de combattants, l'encouragement familial à entrer dans la lutte armée, ou encore le respect imposé d'une culture clanique violente sont tout autant de dimensions qui peuvent influencer un individu et faciliter son cheminement vers l'extrémisme violent.

Tout aussi importants sont les réseaux amicaux, sportifs, associatifs (Atran 2003) et relationnels dans le processus de radicalisation. Mark Sageman (2004) affirme que dans le cadre du terrorisme islamiste, ce type de réseau est particulièrement significatif, peut-être même davantage que la question idéologique, où il estime que 70% des personnes s'étant affiliées à Al-Qaïda l'ont fait en vertu de liens amicaux (Sageman 2004). Ces conclusions valent pour d'autres contextes documentés, dont notamment les cas de radicalisation observés dans les quartiers populaires dans de nombreux pays occidentaux, dont la France, où l'on observe une influence importante de réseaux religieux clandestins (Crettiez et Sèze 2017).

Enfin, il faut également relever l'importance de l'expérience d'incarcération et son influence documentée en lien à la radicalisation (Khosrokhavar 2004; Trujilo et al. 2009) de par les affinités des personnes détenues, l'influence d'imams parfois improvisés, mais aussi le traumatisme provoqué par les mauvais traitements (Crettiez et Sèze 2017, Sommier 2012). De manière générale : « on mettra en avant l'importance de 'personnes ressources' qui peuvent servir de guides spirituels et de modèles opérationnels pour favoriser le passage à l'acte » (Crettiez et Sèze 2017 : 17).

[1] Ces auteurs indiquent que : *« sur les 19 membres identifiés du réseau djihadiste responsable des attentats du 13 novembre 2015 à Paris, 11 avaient séjourné en Syrie ou sur des zones de conflit au sein de camps djihadistes »* (Crettiez et Sèze 2017 : 16).

Enfin, il faut relever encore l'impact des technologies et en particulier le rôle d'Internet comme élément facilitateur de radicalisation. D'emblée, il est crucial de rappeler de ne pas surdéterminer le rôle des technologies, mais il est démontré qu'elles jouent un rôle important dans l'influence des individus dans l'évolution de leurs cognitions et leur cheminement vers la radicalisation (Ducol 2015). Une compréhension exhaustive du phénomène de radicalisation doit prendre en considération le rôle des environnement virtuels et leur impact – et la nature de cet impact – sur la socialisation et les pratiques des individus dans leur cheminement vers un système de croyances et des cadres cognitifs, ou des représentations, par lesquels la violence politique devient à leurs yeux une avenue légitime d'action.

Il est important, dès lors que l'on cherche à comprendre le phénomène de radicalisation, d'intégrer le rôle des outils numériques et de l'environnement en ligne du fait qu'ils sont susceptibles d'exposer les individus à une palette relativement large d'influences (locales et étrangères). Il faut cependant tenir compte de l'environnement physique dans lequel évoluent les individus, puisque ces deux sphères contribuent tout autant à l'émergence et au développement de configurations cognitives qui peuvent soutenir la violence politique.

Les outils numériques, dont Internet et le web 2.0 – ici défini comme un ensemble d'applications numériques à travers lesquelles les individus organisent leur vie par la création et l'échange de contenu généré par les utilisateurs (Van Dijk 2013) - ont altéré la manière dont l'extrémisme violent est compris à l'époque contemporaine. En particulier, il constitue un espace de prolifération de masse de contenus extrémistes et de points de vue soutenant le terrorisme, ou la violence. Au même titre, Internet offre un espace ou un lieu additionnel d'extrémisme politique, quelle que soit l'idéologie défendue et la géographie de sa provenance. Il permet d'exprimer et faire valoir ses idées et ce, à un coût faible. Internet s'est alors très rapidement répandu au sein des porteurs d'un discours extrémiste, qu'il s'agisse d'individus convaincus ou « d'extrémistes de salon », voyant dans la facilité d'utilisation de l'outil une manière de canaliser toutes sortes de frustrations de la vie quotidienne. Internet offre également la possibilité d'augmenter la visibilité d'un discours, d'un contenu (Wolfson 2014) et, par ce fait, le bassin de recrutement et de mobilisation de nouveaux adhérents (Ellinas 2018). Ces outils s'accompagnent également d'une capacité de produire des identités collectives (Garret 2006), tout en facilitant des échanges d'information et de ressources entre les personnes qui ne se connaissent pas toujours. Internet facilite la propagation de buts communs tout en créant de nouvelles solidarités (della Porta et Mosca 2006), mais aussi offre du contenu validant et légitimant des idées radicales. Ceci a pour conséquence de façonner des contenus circulant au sein de ces communautés. Par ailleurs, l'ensemble de ces dimensions ont été potentialisées avec la transformation de l'architecture du web, la démocratisation du web mobile et du Web 2.0 qui ont mené à des environnements en ligne plus centrés sur les utilisateurs. De fait, l'extrémisme politique s'étend bien au-delà des canaux ou sites « officiels » des groupes terroristes, qui eux-mêmes disposent de réseaux de sympathisants qui relaient et diffusent l'information via leurs propres pages dans l'espace numérique. Ainsi, les outils numériques et Internet doivent être désormais considérés comme des « agents »

importants d'organisation et de chorégraphie de l'action collective ainsi que de la radicalisation (Gerbaudo 2012).

Malgré tout, cette littérature ne permet pas d'identifier avec certitude la manière dont Internet et le Web 2.0 interviennent précisément en lien au processus de radicalisation. Pourtant, la quasi-totalité des individus arrêtés reconnaissent avoir interagit avec Internet à un moment ou à un autre de leur trajectoire. En dépit de la production scientifique sur le rôle d'Internet en matière de radicalisation, un fossé de connaissances fines demeure qui nous permettrait de développer une meilleure appréhension des liens entre les deux phénomènes. Un écueil important, qui jusqu'ici a limité la compréhension que nous avons du rôle des outils numériques en lien à la radicalisation tient au fait que la grande majorité des travaux se sont limités à ce que nous pourrions qualifier de la dimension « *offre* » que proposent ces outils, sans pour autant appréhender la manière dont leurs utilisateurs – la « *demande* » – se les approprient, ni sur leur expérience concrète en lien avec ces outils. Quelles significations leurs donnent-ils ? Comment les comprennent-ils ? Quels objectifs leur prévoient-ils ? Pourquoi utiliser une plateforme plutôt qu'une autre ? Comment les pérégrinations et les usages des acteurs en lien à ces outils influencent-ils leurs trajectoires vers la radicalisation et/ou possiblement l'extrémisme violent dans le monde physique, et vice-versa ? Si les difficultés méthodologiques s'avèrent importantes pour répondre à ces questions, ne serait-ce que pour collecter le point de vue des principaux intéressés, cette démarche offrirait pourtant une approche intégrative qui permettrait d'une part de ne plus considérer les médias d'un point de vue strictement fonctionnaliste – ou l'approche dite de la seringue hypodermique qui injecterait des contenus susceptibles de radicaliser les personnes – mais aussi elle permettrait, d'autre part, de réduire la distinction encore trop prégnante entre milieux en-ligne / hors-ligne. Aussi immergés soient-ils dans le monde virtuel, les usagers des plateformes numériques évoluent dans la dimension physique et leurs comportements ne peuvent pas être appréhendés en dehors de leur milieu de socialisation, qui exerce une contrainte sur leurs croyances et informe leur comportement et leur vie quotidienne. Également, Internet n'est pas un objet tout puissant et ne peut être envisagé que comme une dimension parmi d'autres du puzzle de la radicalisation. D'importants défis se dessinent pour la recherche dans l'objectif d'affiner davantage la compréhension que nous avons de ce lien.

1.4. La dimension micro : logiques psychosociales de l'engagement

Enfin, et pour compléter le cadre analytique et une approche globale à la compréhension de la radicalisation, il est besoin de tenir compte de la dimension individuelle, ou micro de l'analyse du phénomène. La recherche insiste ici principalement sur deux éléments complémentaires, soit les dimensions rétributive et psychologique de l'action violente. Par exemple, des entrevues menées auprès de personnes incarcérées en lien à des violences djihadistes permettent de déceler une vulnérabilité mentale de certains individus radicalisés (Kosrokhavar, 2014). L'auteur reconnaît cependant que, de manière générale, la proportion de personnes présentant une telle vulnérabilité en milieu carcéral est relativement élevée, ce qui s'explique en particulier par la privation de liberté. Si

l'approche psychologisante peut rendre compte des raisons pour lesquelles la violence peut être choisie par certains profils sociopathes, elle ne permet cependant pas de comprendre l'ensemble des engagements belliqueux, ou violents, au sein des collectifs structurés et caractérisés par une idéologie forte (Crettiez et Sèze 2017). Pourtant, plusieurs caractéristiques psychosociologiques ont été mises de l'avant par la recherche qui tendent à éclairer le processus de radicalisation.

En premier lieu, on note une valorisation de l'estime de soi, qui peut faciliter l'engagement radical, où devenir un djihadiste semble accroître l'estime de soi au-delà de son identité sociale véritable (Wilhelmsen 2005). Xavier Crettiez et Romain Sèze mettent cependant en garde sur la nécessité de coupler cette estime de soi : « avec une analyse prenant en compte l'environnement social et économique des acteurs violents, mais aussi le contexte politique dans lequel ils évoluent » (2017 : 19).

Certaines recherches considèrent la radicalisation sous l'angle de la reconnaissance sociale, où l'engagement dans la violence serait lié à leur besoin de reconnaissance (Crenshaw 2011, Braud 2004). À cet égard, le sentiment de reconnaissance est lié à un déséquilibre entre, d'une part, une image revendiquée de la part des individus et, d'autre part, renvoyée par la société et où les individus estiment qu'ils ne sont pas appréciés à leur juste valeur (Lindeman 2010). Dans cette optique, le respect ou l'honneur constituent des clés de lecture plus pertinentes qu'une volonté de maximiser des ressources matérielles ou de pouvoir (Lindeman 2013). Soulignons ici la nature relative et subjective de la reconnaissance. Dans un contexte social et médiatique où la radicalisation constitue un phénomène de haute visibilité, s'engager sur un tel chemin permet d'acquérir un statut.

À ces questions d'estime de soi et d'un engagement violent qui permettrait de les combler, on peut ajouter des phénomènes traumatisants pour une large communauté, comme l'occupation d'un territoire ou de lieux saints par des troupes étrangères. Ainsi, des groupes comme Al-Qaeda ou Daesh peuvent être envisagés comme des solutions de protection (Luizard 2015).

Les enjeux d'intégration au sein d'une société occidentale se posent également comme piste de lecture de l'engagement radical. Des situations qui placent des individus issus de l'immigration et vivant une tension entre, d'une part, une société d'accueil qui les garde à la marge et, d'autre part, une attirance pour des discours radicaux leur faisant miroiter des perspectives d'accomplissement et de valorisation mettent alors en exergue de réelles fragilités identitaires facilement exploitables par la consommation de contenus médiques présentant le groupe d'appartenance comme une victime de «l'agression occidentale » mais aussi par des entrepreneurs de morale (Benslama 2016). Ces dynamiques indiquent alors toute l'importance qu'il faut accorder à l'identité.

Pour Crettiez et Sèze, la radicalisation s'explique sur le plan de l'individu, par ce qu'ils qualifient d'escapisme, soit : « le plaisir intense que peuvent retirer des militants politiques à s'engager dans des actions radicales totalement éloignées d'une forme de quotidienneté

et assurant à ceux qui s'en prévalent une image de soi grandiose et mythifiée » (Crettiez et Sèze 2017 : 21). Cet escapisme, nous disent les auteurs, peut offrir un réel sens à la vie d'individus et s'accompagner de sa propre mise en scène par ceux-ci, qui peuvent aller jusqu'à pratiquer des sports de combats, se former à la manipulation d'armes pour ainsi littéralement incarner ce qu'ils pensent être le rôle du combattant.

Certains auteurs relèvent aussi ce qu'ils appellent un phénomène d'anticipation de la réussite d'un mouvement (White 2002) qui exercerait une séduction sur les individus. Ainsi, la capacité d'un mouvement, ou d'un groupe armé, à aboutir à la mise en place de ses objectifs politiques ou sociaux, et ce par l'usage de la violence, tendrait à exercer une séduction sur de potentiels adeptes. On comprend ici alors l'importance de s'intéresser aux messages diffusés par les groupes et leur intérêt à projeter une victoire dans leur mise en scène, offrant une meilleure opportunité de recruter des membres.

Pour terminer cette recension des travaux portant sur la dimension individuelle et macro, il est important de tenir compte des bénéfices immédiats de l'utilisation de la violence. Ceux-ci peuvent être symboliques, comme nous l'avons vu ci-dessus, mais tout autant matériels (par l'accès à des ressources matérielles), statutaires ou financiers (Bloom 2008).

Ainsi, à travers une compréhension processuelle du phénomène de radicalisation et en dépassant une approche centrée sur les causes, on constate que l'approche décrite ci-dessus offre la possibilité de dépasser de simples (simplistes ?) explications à causalité unique – telle que l'idéologie, par exemple – encore trop diffusées et partagées dans les médias de masse ainsi que le sens commun.

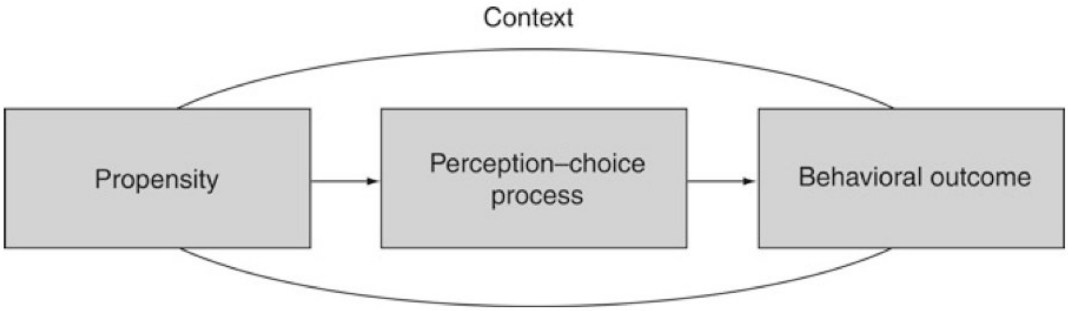
1.5. Un cadre intégratif d'appréhension de la radicalisation

Pour conclure cette section, il apparaît nécessaire d'offrir un cadre conceptuel intégratif qui résume l'ensemble des dimensions présentées, tout en tenant compte de la distinction – bien souvent artificielle mais utile du point de vue de la compréhension – entre espace physique et virtuel de la radicalisation. Les travaux de Benjamin Ducol sont à cet égard très pertinents.

À la base de la réflexion de ce cadre théorique gît l'idée selon laquelle toute action – incluant l'extrémisme violent et la radicalisation – constitue une convergence dans le temps et dans l'espace entre la propension et l'exposition d'une personne à un cadre signifiant, initiant alors de fait un processus de « perception-choix » qui lui, ultimement, résulte en une action ou inaction. Les actions sont alors envisagées comme le résultat d'une perception et d'une évaluation que se font les individus de leurs options, ou alternatives, telles qu'elles se présentent à eux, ainsi que le choix qu'ils opèrent parmi un répertoire d'actions dont ils disposent et ce, dès lors qu'ils sont confrontés à une situation. Par exemple, un individu tombe en panne d'essence sur un chemin de campagne alors qu'il vient de croiser une station-service cinq kilomètres plus tôt. S'il fait beau temps, il sera peut-être enclin à marcher, alors que s'il pleut, il appellera peut-être une assistance

routière. Le principe est résumé par la figure 2 : 1) lorsque confrontés à une situation, les individus peuvent décider d'agir ou pas (propension) ; 2) ce choix s'opère dans un environnement qui offre – ou pas – diverses options et qui vont être prises en compte par l'individu dans son choix suite à l'évaluation desquelles ; 3) il va agir ou pas. L'ensemble de cette proposition s'appelle la théorie de l'action situationnelle.

Figure 2 : théorie de l'action situationnelle (Ducol 2015 : 95)



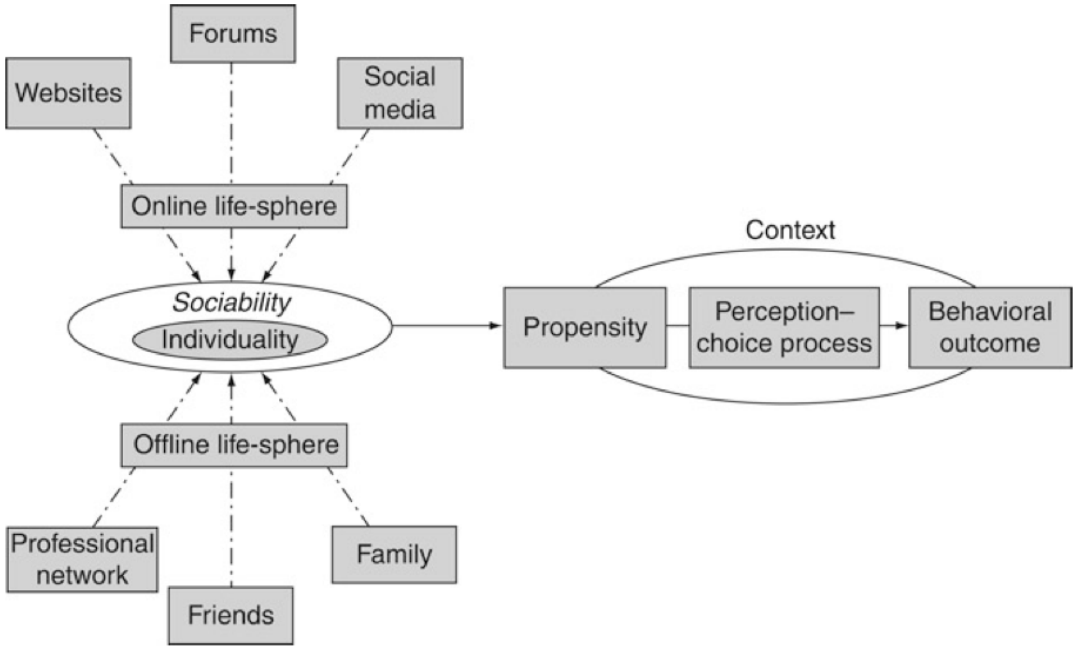
Ainsi, selon ce schéma, la radicalisation peut être définie comme un processus situationnel par lequel un individu développe une propension, et dans certains cas une intention, de s'engager dans des activités d'extrémisme violent. Selon ce qui a été décrit ci-dessus, cette propension peut être influencée par différentes sources (macro, meso ou micro). Rappelons que la transition de la radicalisation à l'extrémisme violent – l'action – peut être envisagée comme une étape finale, mais non systématique, ou automatique, du processus de radicalisation.

Pour expliquer l'extrémisme violent, ce modèle implique qu'il faut en premier lieu comprendre comment les individus en arrivent à croire à, et percevoir le terrorisme comme une avenue légitime d'action. Ici, le processus de perception-choix résulte d'une exposition durable à un cadre radicalisant dans lequel les individus sont exposés graduellement à des contenus et des apprentissages moraux qui valident l'implication dans la violence politique clandestine et la rendent légitime à leurs yeux.

Dès lors, se pose la question de la manière dont ces schèmes cognitifs en viennent à être incorporés par les individus et comment ils sont mis en forme par l'environnement social plus large et le champ des activités dans lequel les acteurs sont impliqués. Également, la manière dont ces cadres et situations sociales peuvent évoluer à travers le temps vers des formes plus radicales de cognitions constitue un enjeu important de compréhension de la radicalisation. Comment un individu entretient-il une conversation, ou interagit-il, avec des contenus extrémistes ? Pour ce faire, et comme nous l'avons décrit ci-dessus, il est nécessaire de tenir compte des réseaux de sociabilité en lien à la radicalisation – à la fois hors-ligne, mais également en-ligne – que l'on peut qualifier de structures de significations et de sociabilités, tel que l'indique la figure 3. Ces deux modes de sociabilité exercent un

rôle clé dans l'exposition sélective des individus à de nouveaux cadres socialisant et à l'acquisition de nouvelles croyances, motivations et d'incitation pour les individus.

Figure 3 : sphères de socialisation et action situationnelle (Ducol 2015 : 98).



Ce modèle théorique, en prolongement avec l'analyse présentée ci-dessus, avance donc que les changements de croyances, ainsi que l'identité sociale, sont hautement corrélés à la transformation de la sociabilité de l'individu, c'est-à-dire le ré-ordonnancement de la hiérarchie des valeurs dans sa vie. Si la sociabilité constitue une dimension centrale de radicalisation, ce modèle rappelle que l'Internet à lui seul, et de manière générale les médias, ne suffisent pas au processus de radicalisation.

2. Les pratiques et expertises policières : besoins et défis anticipés

La littérature traitant de lutte et de la prévention contre la radicalisation est abondante, tout comme les modèles suggérés par la multiplicité des acteurs de la sécurité, qu'ils soient privés, publics ou encore non-gouvernementaux (RAN 2016, Neuman 2017, Gouvernement du Canada 2013). Cela étant, ces politiques sont en grande partie élaborées à partir de modèles théoriques qui ne tiennent pas systématiquement compte des réalités de terrain, et en particulier de la réalité policière. Sur la base d'une revue de la littérature, tant académique que de rapports provenant de diverses organismes (police, gouvernement, ONG), nous nous intéresserons dans cette section aux besoins et défis identifiés par les organisations policières en matière de prévention et de lutte contre la radicalisation. Forte des contraintes – politiques, légales et de ressources – qui caractérisent le travail policier, nous relèverons dans un premier temps les défis structurels

et opérationnels rencontrés par la police dans sa mission de prévenir et, surtout, de lutter contre la radicalisation. Dans un second temps, nous dresserons un portrait des pratiques en cours sur la base de travaux de recherche encore balbutiants en ce domaine. Cette partie portera notamment sur l'impact des technologies en lien à la radicalisation et sa lutte. Ensuite, une troisième section traitera de l'impact des technologies en matière de lutte contre la radicalisation en ligne. Enfin, nous dresserons un répertoire de programmes existants de formation policière en lien à la lutte et la prévention de la radicalisation.

2.1. Défis structurels et opérationnels en matière de lutte contre la radicalisation

L'avènement des nouvelles technologies d'information a indiscutablement favorisé la mise en réseau des sociétés, de collectivités ainsi que de mouvements sociaux et activistes politiques (Wolfson 2014, Mattoni 2012). Ceci vaut tout autant pour les mouvements terroristes et les acteurs de l'extrémisme violent. On assiste à une globalisation et une mise en réseau de l'extrémisme violent qui, depuis les attentats du 11 septembre 2001, provoque une rupture majeure d'appréhension et de compréhension de ce phénomène. D'un extrémisme violent jusqu'ici organisé de façon hiérarchique, suivant un programme politique clair et prompt à revendiquer la responsabilité de ses actions, on observe désormais un terrorisme aux motivations mystico-religieuses, prêt à utiliser des armes toujours plus diversifiées – et agitant parfois le spectre des armes de destruction massive, même si celles-ci sont très rares dans le répertoire d'action des groupuscules radicaux – et opérant surtout selon un structure décentralisée (Sageman 2004, Dupont 2015).

L'architecture de type militaire, pyramidale, qui caractérisait le terrorisme jusqu'à récemment se transforme alors en une structure distribuée capable de résister à des attaques répétées et opérant même lors que son commandement est affaibli ou neutralisé. La mort d'Oussama Ben Laden n'a pas pour autant éliminé le terrorisme d'Al Qaida. Le fonctionnement distribué, ou en réseau, du terrorisme n'est pourtant pas récent. Ce qui a changé, par contre, se résume en deux dimensions importantes. D'une part, on note le progrès de l'évolution des réseaux d'information, avec la transformation majeure de la relation des réseaux sociaux avec le temps et l'espace. Notamment, les potentialités d'Internet et du Web 2.0, telles que décrites ci-dessus, en matière de communication, d'échange d'informations, la diffusion de la propagande, le recrutement de membres et la formation à distance ont indiscutablement facilité la connexion des réseaux qui jusqu'alors était compliquée, voire impossible, pour des questions géographiques. On assiste alors à une convergence de réseaux techniques et sociaux. D'autre part, l'évolution des outils de visualisation utilisés pour observer les relations sociales complexes et leur influence sur les organisations de sécurité dans leur compréhension des phénomènes contre lesquels ils luttent, y compris le terrorisme, sont majeures. Ces outils ont exercé un impact important sur la manière dont les organisations d'application de la loi lisent leur environnement. À titre d'illustration, l'analyse de réseau, et notamment la possibilité d'identifier des nœuds clés de type « courtier » dans la structure du terrorisme, a permis alors aux organisations policières de redistribuer leurs ressources en matière de lutte contre la radicalisation (Sageman 2004).

Ainsi, cette nouvelle morphologie et les moyens qui la sous-tendent ont provoqué une transformation majeure de la réponse des autorités en matière de lutte contre l'extrémisme violent et la radicalisation qui, elles aussi, ont opté pour une réponse en réseau. Cette approche a été qualifiée d'isomorphique (Dupont 2015). Cependant, un certain nombre de défis demeurent. Pour s'en rendre compte, commençons par la présentation de trois grandes familles de réponses développées par les organisations d'application de la loi en Occident. Nous envisagerons ensuite leurs conséquences.

Une première approche vise à identifier et exploiter les faiblesses d'un réseau terroriste ou de radicalisation en vue de perturber ses structures. Parmi les stratégies employées, mentionnons la suppression d'acteurs qui exercent le plus grand impact dans le réseau, en le coupant ainsi de ressources stratégiques, ou d'un relais crucial dans la transmission d'une ressource (information, financement, formation). Une seconde stratégie consiste à faire circuler et inonder le réseau de fausses informations pour saturer ses capacités puisque chaque communication doit alors être vérifiée, ce qui augmente le coût de transaction (Dupont 2015, Deibert et Stein 2002). Dupont indique trois moyens d'évaluer ces stratégies (Dupont 2015). En premier lieu, leur efficacité devrait provoquer une baisse d'échange d'informations entre les membres du réseau. Deuxièmement, et d'un point de vue qualitatif, ces stratégies devraient s'accompagner d'une difficulté accrue pour les membres du réseau de parvenir à un consensus (par exemple sur l'objectif, le répertoire d'action à adopter, les cibles de leur action). Enfin, ces stratégies devraient s'accompagner de difficultés accrues pour le réseau d'accomplir ses tâches et pour les membres du réseau, de les interpréter (Dupont 2015, Carley et. al. 2002).

Une seconde approche vise le déploiement d'une stratégie de réseau au sein même des acteurs d'application de la loi et de renseignement dans la lutte contre le terrorisme, plutôt que de frapper le réseau terroriste en tant que tel. Partant du constat que des structures verticales d'application de la loi n'étaient pas assez efficaces pour lutter contre des « menaces non-étatiques asymétriques » (Dupont 2015 : 154), les acteurs de la lutte contre l'extrémisme violent – incluant la sphère militaire, policière et de renseignement – se sont développé en réseau, perçu plus apte à surmonter les lourdeurs propres à la bureaucratie (Sheptycki 2014), tel qu'on a pu le constater après le 11 septembre et qui n'ont pas permis de prévenir l'attaque. L'objectif visant avant tout le développement d'une approche permettant de partager plus facilement les ressources entre acteurs de la lutte contre cette forme de criminalité, de créer des interdépendances entre les acteurs dans un objectif de consolider la confiance entre eux et ainsi favoriser le compromis et la réciprocité, principales caractéristiques de ce type de structures (Dupont 2015 : 154-155).

Cette seconde approche a favorisé un processus d'hybridation entre le secteur public et le secteur privé, troisième famille de réponses en lien à la lutte et la prévention contre l'extrémisme violent. Ce processus se caractérise par plusieurs éléments qui, à leur tour, se résument en trois grandes dimensions. En premier lieu, on observe une diminution importante du monopole de l'État avec un accroissement de la participation du secteur

privé qui s'observe à la fois dans la protection, l'application de la loi, le renseignement et la participation des agences militaires. En matière de lutte et prévention de la radicalisation, et puisque celle-ci est susceptible d'affecter plusieurs sphères de la société (santé, éduction, transport), des institutions comme l'école ou les hôpitaux intègrent progressivement les acteurs de sécurité, apportant tous leurs propres ressources, mais aussi leur manière d'envisager le phénomène, créant alors d'autres types de tensions entre les acteurs. Par ailleurs, cette hybridation s'accompagne d'un flou problématique entre sécurité intérieure et sécurité nationale et qui s'observe par une fragilisation des droits de la personne. Enfin, cette hybridation se caractérise également par une redistribution et un brouillage des responsabilités entre les partenaires domestiques et internationaux et mène à des initiatives de sécurité dont la mise en application transcende les catégories et responsabilités traditionnelles en matière de sécurité intérieure et nationale. Par exemple, les organisations municipales de police, qui se trouvent occuper la ligne de front lors qu'une attaque liée à l'extrémisme violent se produit, ont considérablement augmenté leurs activités anti-terroristes, tant par leur collaboration avec les acteurs nationaux que sur une base autonome (Dupont 2015). Ce dernier élément risque d'exercer un fort impact sur la confiance qu'un service de police développe auprès des citoyens. Si les polices municipales sont demeurées ancrée dans un rôle de basse police – où le principal bénéficiaire est le public – son évolution, ou hybridation, vers une rôle de haute police – dont le bénéficiaire est l'État – implique un ensemble de pratiques, parmi lesquelles la surveillance, la collecte de renseignement, l'interception des communications, la manipulation d'informateurs, alors nécessaires dans la prévention et la lutte contre la radicalisation, qui ont cependant pour conséquence l'affaiblissement de la confiance du public (Mawby 2002).

Les défis rencontrés par les organisations policières impliquées dans ces transformations majeures de la structure de lutte et de prévention contre l'extrémisme violent et la radicalisation sont nombreux. Mentionnons par exemple, le chevauchement entre sécurité intérieure et nationale, comme indiqué ci-dessus. Il constitue une menace contre la protection des droits des citoyens où, à travers la mise sur pied d'instruments juridiques tels que la Loi antiterroriste C-36 adoptée au Canada en 2001, ou encore une modification du mandat du Centre de la sécurité des télécommunications et des règles entourant l'interception des communication provenant de l'étranger ainsi que la facilitation d'échanges d'informations avec les organisations étrangères de lutte contre le terrorisme, provoque une érosion des barrières légales de protection des informations personnelles. Paradoxalement, ces instruments juridiques s'avèrent pourtant peu utilisés dès lors qu'il s'agit de juger un suspect d'une attaque liée à l'extrémisme violent. Prouver l'Intention terroriste d'une personne hors de tout doute raisonnable est difficile, comme a pu le révéler le cas d'Alexandre Bissonnette, auteur de la tuerie du Centre islamique de Québec, en janvier 2017. Mais surtout, et en second lieu, si l'idée qui prévaut au développement de réseaux isomorphiques de manière à adapter la réponse policière à la structure de l'extrémisme violent s'avère pertinente, elle s'accompagne d'une croyance illusoire en une symétrie parfaite entre les réseaux illicites (criminels ou terroristes) et les réseaux institutionnels de la lutte contre le terrorisme. Or trois paradoxes précisent les limites à un

tel bon fonctionnement (Dupont 2015). Le premier, le paradoxe de la confiance, met en exergue le fait que, contrairement aux réseaux illicites où la confiance repose sur des intérêts convergents et des croyances partagées, les réseaux institutionnels fonctionnent de manière plus situationnelle. Ceci implique que la confiance doit être réévaluée sur une base constante pour prévenir tout comportement opportuniste de la part d'un « partenaire ». Cette confiance nécessite alors le déploiement de ressources coûteuses pour être maintenue et demeurer fonctionnelle, offrant une limite importante au bon fonctionnement du réseau. Le second est qualifié de paradoxe de l'information, qui renvoie à une information circulant beaucoup plus difficilement dans les réseaux institutionnels, puisque tous les acteurs n'ont pas les mêmes privilèges d'accès à l'information. Par ailleurs, l'analyse du flot constant d'informations demeure un défi de taille qui entraîne une difficulté supplémentaire dans la production d'analyses de qualité. Les capacités d'analyse de l'information ne se sont pas développées aussi rapidement que les technologies de sa collecte, compliquant alors son tri et sa métabolisation pour les agences de sécurité. Enfin, un dernier paradoxe, dit de la légalité, exprime la nécessité pour les réseaux anti-terroristes de se contraindre à une série d'obligations de moyens (notamment en lien à la préservation des libertés individuelles) tels que définis dans le droit constitutionnel national et appliqués par les plus hautes cours de justice. Cette obligation est la plupart du temps mise en tension avec le principe d'efficience de la lutte contre le terrorisme et l'emploi de techniques peu ou pas encore sanctionnées par le droit.

2.2. Pratiques policières en matière de lutte contre la radicalisation

La lutte contre la radicalisation, et par conséquent les pratiques policières qui la sous-tendent, ont suivi une évolution rapide et différentielle dépendamment des pays dans lesquels elles se sont développées. En préambule, et comme le souligne Silva Derek (2019), il est important de rappeler que cette lutte est hautement tributaire de la perspective théorique et des discours académiques qui ont prévalu dans la compréhension du phénomène (Young et al. 2015, Kundnani 2012). En retracer l'évolution détaillée dépasse l'objectif du présent chapitre. Relevons toutefois que trois perspectives ont dominé et sont à l'origine de deux rapports importants qui ont largement inspiré les pratiques policières en matière de lutte contre l'extrémisme violent (FBI 2006, Silber et Bath 2017).

La première perspective renvoie à un modèle théorique essentiellement centré sur la dimension psychosociale. Aussi, le processus de radicalisation serait le résultat d'une disposition culturelle et psychosociale qui peut être observée et sur laquelle ceux en charge de la lutte contre la radicalisation peuvent intervenir. Les recherches portent alors sur les causes profondes (root-causes) d'une disposition psychologique à la radicalisation (Laqueur 2004). Le terroriste se distinguerait de la personne « normale » par des caractéristiques spécifiques qu'il ne reste plus qu'à identifier. La principale critique que des courants de pensée plus récents ont formulée sur cette perspective tient au fait qu'un processus aussi complexe que la radicalisation ne peut être résumé à des facteurs uniformes de risque, telle qu'une disposition psychologique (Kundnani 2015). Ce courant a pourtant été le plus influent en matière d'élaborations de politiques publiques de lutte

contre la radicalisation, ainsi que de pratiques policières. Bien que fondées sur une empirie toujours plus solide (Borum 2011, Corner et al. 2016), ces études continuent à être influentes sur le processus gouvernemental de prise de décision, mais elles ne tiennent pas compte d'une dimension pourtant centrale du contrôle social de la radicalisation. Pour ces approches, la clé de la lutte contre la radicalisation menant à la violence et la mise en place de stratégies demeure la compréhension de la manière dont des individus et des groupes deviennent radicaux. Or, pour certains, il s'agit davantage de porter attention à la manière dont des individus considérés à risque de radicalisation sont sujets aux pratiques de contrôle social (Derek 2019).

Par ailleurs, et en second lieu, une perspective visant à comprendre la radicalisation au travers d'aspects théologiques a également constitué la base de stratégies de lutte contre ce phénomène (Derek 2019). Ces approches considèrent la radicalisation comme un processus théologique, ou idéologique, par lequel l'identité qu'un individu s'attribue est envisagée comme un mécanisme causal d'un passage vers la violence politique et, ainsi, à la base du changement du comportement chez les terroristes issus du contexte domestique (*homegrown terrorists*) dans leur parcours de radicalisation. Sans surprise, ces travaux se sont avant tout concentrés sur l'Islam comme étant la source de changement du comportement des candidats à la violence politique (Jenkins 2011, Sageman 2004, 2008, Wiktorowicsz 2005). Ces recherches traitent de la manière dont les individus s'endoctrinent dans des idéologies djihadistes. Ce courant a également influencé les stratégies légales et policières de lutte contre la radicalisation dont les pratiques se sont alors concentrées sur l'évaluation des risques que des individus – de par leur appartenance à une communauté et non pas sur une base individuelle – présentent et susceptibles de les mener sur la voie de la radicalisation et de l'extrémisme violent. Cette approche, plutôt que lutter efficacement contre la radicalisation, offre une liste de recette pour la surveillance de masse de la population musulmane en associant la radicalisation à un groupe – par ailleurs perçu comme uniforme – et qui partagerait les mêmes croyances religieuses. Cette littérature semble davantage justifier des pratiques d'interventions ciblées de la part de la police sur des communautés déjà largement marginalisées (Derek 2019).

Au début des années 2000, et peu après les attentats du 11 septembre 2001, on observe un changement majeur dans les approches de lutte contre la radicalisation et le terrorisme. D'une approche essentiellement, voire strictement militarisée (comme par exemple l'intervention militaire en Afghanistan), se développe une doctrine, ou des approches, dites préemptives et qui reposent sur la doctrine de prévention du risque et du terrorisme et, par extension, de la radicalisation. Il s'agit de combattre le risque d'attaques *futures*, plutôt que des interventions rétroactives militaires ou légales. La contre-radicalisation devient dans ce contexte une stratégie prioritaire pour les agences d'application de la loi.

Cette approche est née en Grande Bretagne, à travers le programme *Prevent* (Home Office 2011) et a été adoptée au Canada sous le même nom dans la stratégie nationale de lutte contre la radicalisation. Concrètement, l'objectif de ce programme est de réunir sous une

même entité des agences gouvernementales disparates, ainsi que des acteurs privés et civils, dans l'objectif de contrer les activités d'extrémisme violent et ce, par l'identification de ceux considérés à risque de se radicaliser et ainsi d'intervenir dans leur trajectoire afin que celle-ci ne mène pas à la violence. Plus spécifiquement, et en termes de pratiques, les objectifs poursuivis par cette stratégie prévoient une communication accrue parmi les différents représentants de la communauté, qu'il s'agisse des agences d'application de la loi, des milieux d'affaires locaux, ou encore de leaders religieux, de manière à offrir une alternative et un contre-discours aux idéologies qui soutiennent le terrorisme et la radicalisation et ceux qui en font la promotion. Ainsi, et tout comme dans le cadre de la police communautaire, la stratégie *Prevent* place les agences d'application de la loi au centre de l'assemblage dans l'interaction entre les acteurs étatiques et gouvernementaux et les communautés qui, à ce titre, deviennent des acteurs stratégiques de la prévention de la radicalisation. Par exemple, en Grande Bretagne, un programme nommé *Prevent Engagement Officers* vise à former les policiers d'organisations locales à développer des liens avec les communautés, les milieux d'éducation (Association of Chiefs Police Officers, 2012) ou encore les communautés culturelles et religieuses, pour identifier les risques et partager l'information avec les partenaires. Il est attendu des organisations policières qu'elles alignent leurs pratiques avec les objectifs du programme *Prevent*. Elles ont alors pour mandat de bâtir des interactions entre communautés ciblées et police, de les conscientiser aux risques liés à la radicalisation et au passage à l'extrémisme violent, créant en cela des nouveaux partenariats entre les agences tout en fournissant du soutien social en complément à des techniques traditionnelles de police (surveillance, cartographie du crime, enquête, saisie et les arrestations). En conséquence, la diffusion de ces techniques a provoqué un élargissement de l'appareil policier en lien à la lutte contre, et la prévention de, la radicalisation.

Tel qu'indiqué plus haut, le Canada a également adopté la stratégie *Prevent*, du moins dans ses principes fondamentaux, en mobilisant davantage les partenaires sociaux dans la prévention et la lutte contre la radicalisation. Aussi, et plutôt que de s'intéresser à ses causes, la stratégie de lutte contre la radicalisation vise à prévenir non seulement des individus présentant des risques mais aussi, pour ceux-ci, d'évoluer vers l'extrémisme violent. Bien que quelques différences s'observent par rapport au contexte britannique, qui s'expliquent avant tout par les structures nationales et le nombre accru de paliers de décisions (fédéral, provincial et municipal) relatifs à l'application de la loi, la philosophie demeure identique. On observe un couplage entre une approche fédérale « par le haut » et de multiples initiatives provinciales ou municipales « par le bas », impliquant une pluralité d'acteurs (Derek 2019).

Parmi les initiatives locales les plus reconnues, citons le *Centre pour la Prévention de la Radicalisation Menant à la Violence* (CPRMV) mis sur pied par la ville de Montréal[2]. En matière policière, une autre initiative locale, municipale, de lutte contre la radicalisation inspirée par la stratégie *Prevent* est le programme *ReDirect* du service de police de la ville

[2] https://info-radical.org/fr/

de Calgary. Son objectif consiste à fournir des interventions au niveau micro élaborées et mises en place en partenariat avec la police, les services à la communauté et au voisinage de la ville de Calgary (City of Calgary Community and Neighbourhood) et d'autres organisations privées ou communautaire à but non-lucratif pour identifier et fournir du soutien et prévenir les individus à risque de radicalisation de s'engager vers la violence.

En conclusion, et tel qu'exprimé par Derek (2019), l'objectif de ces pratiques vise essentiellement à intégrer les questions de préemption et de sécurité dans la vie quotidienne de la population et ce, à travers un triple objectif. En premier lieu, elle rend la population consciente de l'omniprésence de la menace liée à la violence extrémiste. Deuxièmement, en transférant la responsabilité de rapporter de possibles menaces à la sécurité, les agences d'application de la loi sont en mesure d'engager les communautés comme partenaires essentiels dans le processus de préemption (Murray et al. 2015). Finalement, par la diffusion de la stratégie préemptive à travers les structures sociales – écoles, universités, milieux de la santé, institutions religieuses, dans les médias et plus généralement dans l'espace public – les agences d'application de la loi, avec la police en figure de proue, participent au développement d'une population capable de s'auto-gouverner en matière de menace terroriste (Derek 2019). Les citoyens deviennent agents de contre-radicalisation et l'esprit préemptif pénètre progressivement des espaces du domaine public qui n'avaient jusqu'ici aucune responsabilité en matière de lutte contre la radicalisation ou l'extrémisme violent (école, institutions religieuses, hôpitaux, etc.). Dans certaines situations, comme c'est le cas à Londres, de solides réseaux de coopération unissent police et services sociaux, mais aussi des professeurs, enseignants, docteurs et infirmiers qui ont désormais tous l'obligation légale de coopérer dans le cadre de la stratégie *Prevent*. Cette stratégie présente certains risques, dont en matière de protection des droits de la personne, comme certains l'ont révélé (Dudenhoefer 2018).

2.3. Impacts des technologies : la lutte contre la radicalisation en ligne

Les stratégies de lutte contre la radicalisation en ligne reposent sur un nombre encore restreint de certitudes quant à la manière dont les groupes extrémistes opèrent sur Internet, ainsi que l'impact de ces technologies sur de potentielles recrues et la manière dont elles répondent à ces contenus.

À ce jour, deux grandes familles de stratégies peuvent être observées. La première, que nous pourrions qualifier de « stratégie de bannissement » repose sur l'observation, ou le truisme pourrions-nous dire, qui reconnaît Internet et les différentes plateformes qui peuvent le composer – soit le Web 2.0 dont les forums de discussion de type *IRC*, ou *message boards* de type 4chan – comme un espace nourrissant la radicalisation et potentiellement facilitant un passage vers l'extrémisme violent. Rappelons que le Web 2.0 peut être définit comme un groupe d'applications numériques qui permettent de coordonner et d'organiser la vie de ses utilisateurs à travers les contenus qu'ils produisent et s'échangent (Van Dijk 2013, Kaplan et Haenlein 2010). La stratégie de bannissement part du constat que de nombreux auteurs d'attaques, tant en Europe qu'en Amérique du Nord,

ont été endoctrinés, ou du moins ont été actifs sur des forums extrémistes. L'objectif vise à réguler ces plateformes, principalement en bannissant ces acteurs et leurs comptes des hébergeurs. C'est notamment une démarche poursuivie par Facebook, Twitter ou YouTube, pour ne nommer que les plus représentatives (Cox, 2018). Nous reviendrons sur ce principe plus en détail dans la troisième section de ce rapport, en abordant les dilemmes éthiques, mais aussi les effets parfois contre-productifs qu'elle pose. Notons que la prise de conscience de la nature problématique du discours de haine par les géants du Web – GAFA[3] – est relativement récente. En effet, ce n'est qu'à la suite des événements de Charlottesville, en août 2017, où la manifestation du mouvement *Unite the Right* aux États-Unis a dégénéré et où un individu Alexander Field s'est lancé avec sa voiture dans la foule, tuant une manifestante, que ces compagnies, pressées par l'opinion publique, ont décidé d'agir. Rappelons que l'un des sites extrémistes les plus influents – stormfront.org – est présent et actif sur le web depuis les années 90 sans pour autant qu'il n'ait jamais été la cible d'un bannissement.

Une seconde famille de stratégies consiste à s'engager directement avec des potentielles recrues et intervenir dans le processus de radicalisation. C'est notamment le cas d'une méthode – the *ReDirect Method*[4] – fondée par *Jigsaw*, think tank lui-même issu de Google. Cette méthode repose sur l'observation de traits de personnalité récurrents chez les individus radicalisés – qu'il s'agisse de candidats à la radicalisation d'extrême-droite ou islamique. Parmi ces traits de personnalité, et pour n'en citer qu'un, on observe un grand scepticisme envers les médias traditionnels – *mainstream* – et une quête d'informations et des médias alternatifs, principalement en ligne. Fort de ces constats, le temps de l'action – *timing* – devient central dans la mesure où l'intervention par les acteurs de la prévention – que nous allons décrire sous peu – dispose d'une fenêtre d'opportunité restreinte puisqu'il faut opérer entre, d'une part, l'intérêt initial de l'individu pour une idéologie extrémiste et, d'autre part, la décision de joindre la cause et, éventuellement, de glisser vers l'extrémisme violent. Une fois la cause rejointe, les individus semblent par la suite hors de portée de la prévention et semblent s'écarter de toute information alternative à leur mode de pensée et leur engagement.

Concrètement, la méthode *ReDirect* consiste en la production de vidéos dont le propos est d'offrir une contre-réalité à celle qui leur est présentée dans les images de propagande diffusées sur les sites extrémistes et dépeignant la vie sous le califat et l'état islamique en Syrie, par exemple. En particulier, les vidéos produites par *ReDirect* exposent les mauvais traitements ainsi que, de manière plus générale, les conditions de vie difficiles que les populations subissent sous le règne islamique. De manière particulièrement intéressante, la diffusion de ces vidéos repose sur le même principe algorithmique que le ciblage publicitaire déployé par Google, par exemple. Ces vidéos sont alors « poussées » vers de potentielles recrues identifiées par leur usage du web et les sites qu'ils fréquentent. À ce stade, l'effet concret de ces vidéos doit encore faire l'objet d'une évaluation scientifique

[3] Google, Amazon, Facebook, Apple.
[4] https://redirectmethod.org/

mais Jigsaw affirme qu'elles sont amplement visionnées et ce, en entier. Ainsi, présume la compagnie, et sur le nombre, on peut émettre l'hypothèse que certains de ces contenus ont prévenu des parcours de radicalisation menant à la violence. D'autres organismes de lutte et de prévention contre la radicalisation, comme *MoonshotCVE*[5], en Grande Bretagne, affirment également engager des travailleurs sociaux spécialisés dans la radicalisation et les enjeux numériques, pour diffuser discrètement des vidéos de cette nature sur les forums extrémistes les plus fréquentés, qu'ils soient en lien à l'extrême droite ou à l'islam radical (Manjoo 2017).

En dépit de ces stratégies, il est important de ne pas verser vers le fétichisme de la technologie et préserver malgré tout une attitude pondérée. À cet égard, le portrait que dresse le magazine *GQ* de l'auteur suprémaciste blanc d'une attaque extrémiste récente des plus marquantes, Dylan Roof, et qui a perpétré le 17 juin 2015 une fusillade dans une église de Charleston, en Caroline du Sud, tuant 9 personnes afro-américaines est éloquent. Si l'on peut présumer que l'Internet et les forums extrémistes qu'il fréquentait ont exercé une influence dans sa trajectoire et son geste, le portrait du jeune homme révèle tout autant sa vulnérabilité psychique, son isolement social, ses problèmes personnels, bref une grande vulnérabilité personnelle qui doit tout autant être considérée (Kaadzi Ghansah 2017). On peut pourtant et raisonnablement formuler que les stratégies de perturbation de tels forums permettront certainement de dissuader quelques candidats à de tels gestes.

2.4. Lutte contre la radicalisation, formation et police

En matière de formation policière axée sur la lutte contre la radicalisation, une très vaste palette de programmes sont offerts à travers le monde, et un rapport détaillé du RAN (*Radicalization Awareness Network*) publié en 2016 en répertorie une liste complète (RAN, 2016). Dresser une liste exhaustive de l'ensemble de ces programmes dépasse l'objectif du présent rapport, mais relevons cependant les grands axes qu'ils couvrent. Parmi ces axes de formation figurent :

1) Les intervenants de première ligne, dont les éducateurs, les policiers directement liés aux communautés, les enseignants ou encore les travailleurs de la santé, travaillant avec des individus ou groupes vulnérables et présentant le risque de radicalisation. L'objectif de ces programmes, dont une liste exhaustive est disponible dans le document du RAN, ont pour objectif la sensibilisation de ces intervenants aux dynamiques de la radicalisation, leur fournir des outils pour repérer des individus à risque de se radicaliser, leur offrir des outils pour y répondre en conséquence et stimuler les partenariats multi-agences afin de dissuader ces individus de verser vers la radicalisation. Cette stratégie inclut les organisations policières, tel que le révèle le programme *«Training at police academy».* De façon plus détaillée, les policiers suivent une formation sur les rudiments de la radicalisation et du terrorisme; la manière dont les terroristes opèrent ainsi que les responsabilités des diverses agences en lien à la lutte contre le terrorisme; une formation

[5] http://moonshotcve.com/

sur les assauts contre le terrorisme, notamment pour les unités de police spécialisés (Groupe d'intervention Tactique); une formation sur les potentiels loups solitaires et notamment sur les règles en matière d'administration et de gestion des clubs de tir; la manière d'identifier des comportements précurseurs susceptibles d'être liés à des individus terroristes (détection de comportements dits «typiques»).

2) Les programmes dits de « sortie » et de désengagement de la radicalisation, principalement axés sur les dimensions cognitives et l'offre de contenus alternatifs aux individus radicalisés avec l'objectif de les réintégrer dans la société.

3) Les programmes d'engagement de la communauté qui visent essentiellement à la sensibiliser au phénomène de radicalisation et en repérer les signes avant-coureurs. Ces programmes visent aussi à soutenir les communautés dans ces efforts et faciliter l'échange de ressources et d'information avec les agences gouvernementales locales. Enfin, ces programmes visent également à bâtir de la résilience au sein des communautés dès lors qu'elles sont touchées par le phénomène de radicalisation ou d'extrémisme violent.

4) Les programmes d'éducation de la jeunesse qui portent essentiellement sur des enjeux de citoyenneté, de stéréotypes, de discrimination, d'extrémisme, de valeurs démocratiques, de compréhension des médias, pensée critique et de diversité culturelle et qui visent à renforcer leur résistance face à la radicalisation, ainsi que leur résilience.

5) Le soutien aux familles qui, là aussi, vise à offrir des ressources à un milieu considéré comme crucial en matière de prévention de la radicalisation. Ces programmes visent avant tout à sensibiliser les familles aux questions de radicalisation, y bâtir de la résilience contre l'extrémisme violent et leur fournir des ressources afin qu'elles puissent identifier les services et les organisations capables de leur venir en aide dès lors qu'elles sont aux prises avec le phénomène de radicalisation.

6) L'offre de contenus alternatifs visant à briser les effets de l'exposition des individus aux contenus extrémistes dans les médias, sur Internet ou dans leur communauté. Ces programmes fonctionnent sur le même principe que la méthode *ReDirect* décrite plus haut.

7) Les approches multi-agence qui ont pour objectif le développement d'infrastructures de Lutte Contre l'Extrémisme Violent (*Countering Violent Extremism*) qui permettent aux personnes à risque d'avoir accès, dès les premiers stades, au soutien de diverses infrastructures et organismes critiques, publics ou privés, nationaux ou internationaux, en matière de ressources sans pour autant que ceux-ci ne soient systématiquement liés aux agences d'application de la loi.

3. Les limites de la prévention et de la lutte contre la radicalisation

La lutte contre la radicalisation et la prévention présentent certaines limites. Nous nous concentrerons dans cette section exclusivement aux stratégies décrites et développées ci-dessus et relatives à la dimension en ligne, plus particulièrement à la stratégie de bannissement du fait qu'elle est la cible des critiques les plus importantes. Rappelons que les stratégies de luttes contre la radicalisation et l'extrémisme violent sont avant tout distribuées, c'est-à-dire qu'elles reposent sur une pluralité d'acteurs publics, privés, communautaires, religieux, de l'éducation, ou encore de la santé, pour n'en mentionner que quelques-uns. Dans leur dimension en ligne, ces stratégies sont donc aussi de la responsabilité des géants de l'Internet – GAFA – et des hébergeurs de contenus. Une première critique à ce modèle distribué vient des organisations de protection de la vie privée et de défense des utilisateurs de l'Internet, avec notamment la *Electronic Frontier Foundation* en tête de ligne, pour qui ces méthodes de régulation ont « force de loi » dans les faits mais sont mises en place par des acteurs qui n'ont pas les mêmes responsabilités que des organismes publics en matière d'imputabilité et de reddition de comptes. Les récents scandales impliquant Facebook et le partage de données à un tiers (Cambridge Analytica) ont révélé à quel point les décisions prises par le géant des médias sociaux manquent de transparence et d'imputabilité (New York Times 2018). Par ailleurs, certaines enquêtes journalistiques ont révélé les conditions difficiles dans lesquelles les modérateurs de contenus, alors responsables d'identifier les comptes à bannir, réalisent leur travail. On relève des salaires très bas, une surcharge importante de la tâche, qu'ils doivent exécuter dans un laps de temps très court pour que les contenus problématiques ne risquent pas de se diffuser trop largement. Cette situation nécessite une réponse rapide, mais présente aussi le risque de bannir des contenus qui n'étaient pourtant pas problématiques, ouvrant le débat alors sur les enjeux éthiques de régulation des contenus et discours sur le web (Tusikov 2017).

La régulation des contenus par les géants du web offre indiscutablement des pistes de solutions pertinentes, mais ces stratégies manquent encore cruellement de régulation et de cadres légaux et éthiques pourtant nécessaires pour le respect des droits des utilisateurs de l'Internet et se conformer aux principes démocratiques qui constituent le fondement de nos sociétés. Tel qu'observé par le passé, les règles que l'on met en place pour lutter contre des comportements répréhensibles (terrorisme, abus sexuels sur les enfants, discours de haine) sont souvent élargies par la suite pour cibler d'autres formes de discours. Que ferons-nous quand ces censeurs sans surveillance s'attaqueront à des contenus qu'ils trouveront offensant alors que ce ne sera pas notre cas, se demande pertinemment Natasha Tusikov (Tusikov 2017) ?

Une autre critique à l'encontre de la stratégie de bannissement évoque les risques qui accompagnent le blocage de certains contenus. En effet, cette méthode ne viendrait que temporairement déstabiliser ces espaces de radicalisation, les acteurs pourraient éventuellement se dissimuler davantage dans le web et pénétrer des espaces d'autant plus difficiles à atteindre dès lors que l'on vise à déployer d'autres stratégies de prévention,

dont les méthodes de type *ReDirect*. Ainsi, déléguer la responsabilité de la régulation aux acteurs privés, comme Facebook ou Google – eux-mêmes agissant sur la pression parfois très forte de leurs utilisateurs et abonnés – est problématique dans la mesure où ils opèrent en absence de règles transparentes et équitables.

En guise de réflexion finale, et sous forme de recommandations, il semble intéressant de s'inspirer de méthodes de régulation du web telles qu'elles ont été imaginées pour la cybercriminalité. Par extension, nous verrons qu'elles peuvent s'avérer utiles en matière de régulation de contenus. Le modèle développé par David Wall est prometteur (Wall 2007) et qui ouvre une porte centrale aux acteurs publics de la régulation, y compris la police.

La régulation et la lutte contre la cybercriminalité s'est, depuis déjà quelques années, exercée sur une mode nodal, ou en réseau. Ainsi, et tout comme pour la régulation de la radicalisation, décrite ci-dessus, elle repose sur des partenariats entre acteurs publics, privés et civils destinés à renforcer la résilience du cyberespace et aider les victimes, dès lors qu'elles sont touchées par cette forme de criminalité, à restaurer l'intégrité de leur équipement et développer des moyens efficaces pour s'en prévenir. Qui plus est, et en matière d'infractions et de violation des valeurs ou principes démocratiques, la production de contenus problématiques susceptibles de mener à la radicalisation offre une similarité avec la cybercriminalité comme la fraude, par exemple. En effet, elle constitue une forme « d'infraction de masse » dont les caractéristiques – fort volume mais impact faible ou difficilement mesurable de chaque infraction – sont incompatibles avec un système de justice pénale davantage pensé pour traiter un faible volume de crimes ou d'infractions, mais qui ont un fort impact à l'intégrité physique des personnes.

De prime abord, la régulation du web pose un certain nombre de défis et ce, qu'il s'agisse de la cybercriminalité ou de la production de contenus susceptibles d'exercer un impact en lien à la radicalisation et l'extrémisme violent. David Wall, traitant de la cybercriminalité, en soulève au moins six.

1) *De Minimism* – les cybercrimes, tout comme le contenu susceptible de radicalisation, ont un faible impact relativement au volume de personnes touchées *localement* – par comparaison à d'autres types de criminalités ou de dommages sociaux – mais provoquent des pertes, ou offrent un potentiel important en matière de radicalisation, dès lors qu'ils sont appréhendés de manière agrégée et en fonction de leur distribution globale et à travers une série de juridictions. Cette caractéristique, en particulier ce faible impact local, ou du moins la difficulté de le mesurer, rend difficile la justification l'augmentation de ressources policières.

2) *Nullum Crimen Disparities* – selon ce principe, et pour susciter une réaction de contrôle social, il faut que l'offense, même transfrontalière, provoque le même intérêt, ou priorité (politique, sociale, économique) en matière de régulation et ce, à travers les diverses juridictions. Si ce n'est pas le cas, alors la probabilité que le comportement incriminé fasse

l'objet d'une régulation uniforme globale est moindre et le risque d'observer une grande disparité dans les ressources attribuées à sa lutte – et son succès – est grand. À cet égard, il ne faut pas négliger la disparité de réactions sociales que peut susciter un même comportement ou la production de contenus problématiques qui risquent de ne pas toujours être régulés par les mêmes instruments juridiques (code criminel vs. civil). En matière de production de contenus susceptibles de mener à la radicalisation, cela signifie que des sites hébergeurs de ce type de discours peuvent être situés dans des juridictions beaucoup plus laxistes et tolérantes.

3) *Les disparités juridictionnelles* – Pour ce qui est des affaires criminelles transfrontalières – caractérisant la base même les enjeux de cybercriminalité et de production de contenu en lien à la radicalisation – les acteurs de la justice, y compris les acteurs policiers, « magasinent » leur forum de juridiction, de manière à s'assurer la condamnation d'une personne responsable d'un usage frauduleux de l'Internet. Ceci vaut notamment dans des cas qui génèrent un grand consensus transnational, comme les affaires de pornographie juvénile. Or ce principe peut mettre sous pression des institutions judiciaires dans des zones qui se sont dotées d'outils juridiques performants de lutte contre ces formes de criminalité et provoquer un étouffement du système et des tensions diplomatiques.

4) *Activités non-routinières et culture policière* – la régulation de ces formes de criminalités, ou d'usage problématique du web, doivent également s'envisager en lien à la capacité policière de répondre à des activités criminelles non-routinières, ou extraordinaires. Par exemple, et dans un contexte où la lutte contre l'extrémisme violent au Canada est largement demeurée centrée sur l'Islam, on peut présumer que la lutte contre l'extrême droite nécessite encore un processus important de sensibilisation de sa nature, son déploiement et ses dynamiques au sein des organisations d'application de la loi pour qu'elles soient capables de saisir ses structures – y compris sur le web – et établir des stratégies de contre-radicalisation. Dès lors, et si la lutte contre l'extrémisme violent est depuis longtemps intégrée dans la culture policière, toutes ses formes n'ont pas été investies au même titre – souvent pour des questions de ressources – affectant alors sa régulation.

5) *Un sous-signalement* – on observe généralement un sous-signalement de la criminalité qui se produit dans le cyberespace (Wall 2007). Ce phénomène est en grande partie lié à des attentes basses de la part du public envers la police locale et sa capacité à résoudre cette forme de criminalité. En matière de radicalisation, et au vu parfois d'un contrôle social nettement plus intense vis-à-vis de certains groupes sociaux, ou minorités visibles, on présume également une réticence de certains à rapporter des activités qui semblent suspectes afin de ne pas précipiter une réaction parfois jugée abusive ou inéquitable à l'encontre de groupes ou minorités visibles. Les conséquences d'un tel signalement peuvent être perçues comme étant beaucoup plus importantes sur le sort d'une personne et ainsi dissuader des signalements.

6) *Faire la police en utilisant des méthodes non-traditionnelles* – ce dernier point évoque la capacité dormais accrue pour les organisations policières, du moins présumée par David Wall, à faire appel à des technologies toujours plus performantes par la police pour lutter contre la cybercriminalité et la radicalisation en ligne. Dans de nombreux cas, Internet facilite l'enquête ou la collecte de preuves (Schneider et Trottier 2012) et ainsi permettent de sécuriser une poursuite et une condamnation. Or, en matière de radicalisation et de lutte contre des contenus à caractère haineux et faisant la promotion de l'extrémisme violent, la situation est plus complexe. Premièrement, tout contenu ne s'inscrit pas automatiquement dans la promotion de la haine. Par exemple, les stratégies actuelles employées par la droite radicale, ou l'alt-right, se basent largement sur la diffusion de fausses nouvelles qui, si elles ne semblent à priori pas criminelles en elles-mêmes, provoquent pourtant un bouleversement important dans la manipulation de l'information accessible au public et la capacité, dans certains cas, d'alimenter son indignation (Marwick et Lewis 2017, Lewis 2018, Hawley 2017). Ainsi, les outils développés pour lutter contre les contenus problématiques tels que basés sur l'identification de mots-clés (insultes, termes dégradant identifiants certains groupes, etc.) ne suffisent pas à identifier ces contenus problématiques, où le risque d'une radicalisation vers l'extrémisme violent est désormais lié à des dynamiques nettement plus complexes pour susciter l'indignation et le ressentiment, autant de sources d'engagement radical.

En conclusion, et forts de ces remarques, on comprend que la police et les acteurs publics de la régulation de la cybercriminalité et, par extension, de la prévention et de la lutte contre la radicalisation sont confrontés à de nombreux défis. Par analogie à la dimension physique, cette lutte, telle qu'elle s'opère dans l'espace numérique, nécessite tout autant de s'envisager en réseau. Or, quel que soit l'espace dans lequel on se situe – numérique ou physique – ces partenariats multi-niveaux et multi-secteurs de régulation présentent un défi majeur, ne serait-ce qu'à se coordonner et s'entendre. Pour qu'ils soient opérationnels et efficaces, ces réseaux doivent bâtir et consolider des relations de confiance afin de réduire la compétition entre les acteurs et, ainsi, développer une appétence au partage crucial d'informations entre eux. Or, et on l'aura compris tout au long de ce rapport, en dépit de la diversité des acteurs impliqués dans ce réseau, tant par leur intérêt, ressources, cadres cognitifs d'appréhension de la radicalisation et des risques de transition vers la violence, tous et sans exception ont comme point de mire la régulation – qu'il s'agisse de la lutte ou de la prévention – de la radicalisation menant à la violence. En ce sens, et si leur coordination est parfois difficile, une culture et un ensemble de valeurs communes animent ces acteurs. C'est là, nous semble-t-il, que la proposition de David Wall (2007) semble particulièrement pertinente. Reprenant l'argument historique de la naissance de la police de Peel au XIXè siècle et la nécessité d'identifier un acteur capable de coordonner l'ensemble des participants à l'offre de sécurité, Wall entrevoit un rôle central de la police dans la lutte contre la cybercriminalité – et par extension contre la radicalisation, affirmons-nous – puisque si elle manque de ressources (matérielles, humaines, de temps) pour lutter à elle-seule contre ce phénomène, elle dispose cependant d'un avantage crucial par rapport aux autres acteurs : son autorité légale qui la place en

position stratégique dans la coordination du réseau. En ce sens, elle peut persuader et contraindre les autres acteurs et leur astreindre des responsabilités spécifiques.

En conséquence, la police aurait pour objectif non plus tant de procéder à elle seule aux interventions et en faisant valoir son monopole de coercition, mais plutôt de mandater les autres acteurs – et ainsi chorégraphier – leurs ressources et leur rôle dans un réseau de lutte et de prévention de la radicalisation menant à la violence.

Références

Alimi, E. Y., Demetriou, C. et Bosi, L., (2015), The Dymanics of Radicalization : A Relational and Comparative Perspective. New York : Oxford University Press.

Aminzade, R., et McAdam, D., (2002) Emotions and contentious politics, Mobilization : an International Quarterly, 7(2) : 107-109.

Ancelovici, M., et Rousseau, S., (2009), Présentation : les mouvements sociaux et la complexité institutionnelle / Content, Sociologie et Société, 41(2) : 5-14.

Association of Chief Police Officers, (2012), *Prevent*,Police and colleagues : Guidance for police officers & polcie staff to help colleges contribute to the prevention of terrorism

Atran, S. (2003), Genesis of Sucide Terrorism, Science, 299 : 1534-1539.

Benslama, F., (2016), Un furieux désir de sacrifice. Le surmusulman, Paris : Seuil.

Borum, R. (2012a), Radicalizartion Into Violent Etremism I : A Review of Conceptual Models and Empirical Research, Journal of Stretagis Studies, 4(4) : 7-36.

Borum, R. (2012b), Radicalization Into Violent Extremism II : A Review of Conceptual Models and Empirical Research, Journal of Strategic Studies, 4(4) : 37-62.

Braud, P., (2004), Violences politiques, Paris : Seuil.

Carley, K., Lee, J.-S. et Krackhard, D., (2002), Destabilizing networks, Connections, 24(3) : 79-92.

Corner, E., Gill, P. et Mason, O. (2016), Mental health disorders and the terrorist : A research note probing selection effects and disorder prevalence, Studies in Conflict and Terrorism, 39(6) : 560-568.

Cox, J. (2018), These are Facebook's policies for moderating white supremacy and hate, Motherboad, 29 mai. Accessible à : https://motherboard.vice.com/en_us/article/mbk7ky/leaked-facebook-neo-nazi-policies-white-supremacy-nationalism-separatism?wpisrc=nl_cybersecurity202&wpmm=1

Crenshaw, M., (2007), Explaining Terrorism : Causes, Processes and Consequences, New York : Routledge.

Crettiez, X. et Sèze, R., (2017), Saisir les mécanismes de la radicalisation violente : pour une analyse processuelle et biographique des engagements violents, Rapport de recherche pour la Mission Droit et Justice, avril 2017.

Deibert, R., et Stein, J., C., (2002), Hacking networks of terror, Dialogue IO 1(1) : 1-14.

Della Porta, D., & Mosca, L. (2006). "Ricercando nella rete: stili democratici dei siti web del movimento per una giustizia globale". *Rassegna italiana di sociologia*, *47*(4), 529-556.

Derek, S., (2019), Police and Radicalization, in Deflem, M. (Ed.) The Handbook of Social Control, Malden, MA: Wiley Blackwell: 249-262.

Ducol, B., (2015), A Radical Sociability : In defense of an off-line/on-line multidimensional approach to radicalisation, in Bouchard, M. (dir.), *Social Networks, Terrorism and Counter-Terrorism : Radical and Connected Account*. Londres : Routledge : 87-107.

Dudenhoefer, A.-L., (2018), Resisting radicalization: A critical analysis of the UK Prevent duty, Journal for Deradicalization, 14: 153-191.

Dupont, B. (2015), Security networks and counter-terrorism : a reflection on the limits of adversarial isomorphism, in Bouchard, M. (dir.), *Social Networks, Terrorism and Counter-Terrorism : Radical and Connected Account*. Londres : Routledge : 151-168.

Ellinas, A. A. (2018), "Media and the Radical Right", in Rydgren, J. (Ed.), *The Oxford Handbook of the Radical Right*. New York: Oxford University Press. DOI: 10.1093/oxfordhb/978019274559.013.14.

Federal Bureau of Investigation, (2006), The Radicalization process: from conversion to jihad.

Garret, R. K. (2006), "Protest in an Information Society: A Review of Literature on Social Movements and New ICT's", *Information, Communication and Society*, 9(2), pp. 202-224.

Gayer, L., (2009), Le parcours du combattanrt: une approche biographique des militants Sikhs du Khalistan, CERI/IEP, 28: 1-63.

Gerbaudo, P. (2012), *Tweets and the Streets. Social Media and Contemporary Activism*. London: Pluto Press.

Gouvernement du Canada, (2013), Renforcer la resilience face au terrorisme: stratégie antiterroriste au Canada, deuxième edition.

Gurr, T. R., (1970), Why Men Rebel, Princeton: Princeton University Press.

Hawley, G. (2017). *Making Sense of the Alt-Right*. New York: Colombia University Press.

Home Office, (2011), Prevent Strategy, Londres: HM Government.

Jenkins, M., (2011), Stray dogs and virtual armies: Radicalization and recruitment jihadist terrorism in the United States since 9/11, Santa Monica, CA: RAND Corporation.

Kaadzi Ghansah, R., (2017), A most American terrorist: the making of Dylan Roof, GQ, 21 août, accessible à: https://www.gq.com/story/dylann-roof-making-of-an-american-terrorist

Kaplan, A.M. & Haenlein, M. (2010), "Users of the World, Unite! The Challenges and Opportunities of Social Media". *Business Horizons* 53(1): 59-68.

Kepel, G., (2015), *Terreur dans l'Hexagone*. Genèse du djihad français. Paris: Gallimard.

Khosrokhvar, F., (2014), Radicalisation, Paris: MSH éditions.

Khosrokhvar, F., (2004), L'Islam dans les prisons, Paris, Balland.

Kudnani, A., (2012), Radicalisation : The Journey of a Concept, Race & Classe, 54(2) : 3-25.

Lacqueur, W., (2004), The terrorist to come, Policy Review, 126 : 46-64.

Lewis, R., (2018), Alternative influence : Broadcasting the reactionary right on YouTube, Data & Society, 18 septembre.

Lindeman, T. (2013), The case for an empirical and social-psychological study of recognition in international relation, International Theory, 5(1) : 150-156.
Lindeman, T., (2010), La guerre, Paris : Armand Colin.
Luizard, P.-J., (2015), Le piège Daech, Paris : La Découverte.
McAdam, D., Tilly, C., et Tarrow, S., (2001), Dynamics of Contentious Dynamics, Cambridge : Cambridge University Press.
Manjoo, F., (2017), A hunt for ways to combat online radicalization, New York Times, 23 août. Accessible à : https://www.nytimes.com/2017/08/23/technology/a-hunt-for-ways-to-disrupt-the-work-of-online-radicalization.html?smid=tw-share
Marwick, A. & Lewis, R. (2017), *Media Manipulation and Disinformation Online*. *Data & Society*. 15 May.
Mawby, R., C., (2002), Policing images : policing, communication and legtimacy, Londres : Willan Publisher.
Murray, A., Mueller-Johnson, K., et Sherman, L., W. (2015), Evidence-Based Policing of U.K. Muslim communities : Linking confidence in the police with are vulnerability to violent extremis, International Criminal Justice Review, 25(1) : 64-79.
Neuman, P., (2017), Countering violent extremism and radicalisation that lead to terrorism : ideas, recommandations, and good practices from the OSCE region, 28 septembre.
Neuman, P., (2013), The Trouble with Radicalization, International Affairs, 89(4) : 873-893.
New York Times (2018), « Did Facebook Learn Anything From the Cambridge Analytica Debacle? », *New York Times*, 6 octobre, Editorial Board.
Pape, R., (2005), Dying to Win : The Strategic Logic of Suicide Terrorism, New York : Random House.
Radicalisation Awareness Network/RAN, (2016), Preventing radicalisation to terrorism and violent extremism : approaches and practices.
Young, H. F.; Rooze, M. et Hoslappel, J. (2015), Translating conceptualizations into practical suggestions : what the literature on radicalization may offer to practitioners, *Peace & Conflict*, 21(2) : 212-225.
Sageman, M., (2008), Leaderless Jihad: Terror networks in the twenty-first century, Philadelphia: University of Pennsylvania Press.
Sageman, M., (2004), Understanding Terror Networks, Philadelphia: University of Pennsylvania Press.
Schneider, C. & D. Trottier, (2012) «The Vancouver Riot and the Role of Facebook in Crowd Policing», *BC Studies*, vol. 175, automne : 57-72.
Sheptycki, J. W. E., (2014), Réflexions critique sur le crime transnational et les services de police transnationaux, Criminologie, 47(2): 13-34.
Silber, M., D. et Bhatt, A. (2007), Radicalization in the West: The Homegrown threat. New York: New York Police Department Intelligence Division.
Sommier, I. (2012), Engagement radical, désengagement et déradicalisation. Continuum et ligne de fracture. *Lien social et Politiques*, 68 : 15-35.

Tanner, S. (2012), Réflexion autour de la banalité du mal : inspirée d'une conversation avec Jean-Paul Brodeur, Champ Pénal / Penal Field [En ligne], Vol. IX mis en ligne le 23 mai 2012. URL : http://champenal.revues.org/8336.

Tanner, S. (2011), Towards a pettern in mass violence participation? An Analysis of Rwandan perpetrators' accounts from the 1994 genocide, Global Crime 12(4) : 266-289.

Trujillo, H., Jordán, J., Gutiérrez, J. A., González-Cabrea, J., (2009), Radicalization in prison? Field research in 25 Spanish Prisons, Terrorism and Political Violence, 21(4) : 558-579.

Tusikov, N. (2017), «Who Sould be Policing Hate Speech Online?,» *The Star*, 19 août.

Van Dijk, J. (2013), *The Culture of Connectivity. A Critical History of Social Media*. New York: Oxford University Press.

Wall, David (2007), «Policing Cybercrimes : Situating the Public Police in Networks of Security within Cyberspace», *Police Practice and Research : An International Journal*, 8(2) : 183-205.

Wendling, M. (2018), *Alt Right. From 4Chan to the White House.* Halifax & Winnipeg: Fernwood Publishing.

Wilhelmsen, J., (2005), Between a rock and a hard place: the islamization of the Chechen Separatist Movement, Europe-Asia Studies, 57(1): 35-59.

White, R., (2002), Structural identity theory and the post recruitment activism of Irish, republicans: persistance, disengagement, splits and dissidents in social movement organizations, Social Problems, 57: 341-370.

Wiktorowicz, Q., (2005), Radical Islam rising: Muslim extremists in the West, Oxford, UK: Rowmann & Littlefield.

Wolfson, T. (2014), *Digital Rebellion. The Birth of the Cyber Left*. Chicago: University of Illinois Press.

Chapitre 2. Police et prévention de la cybercriminalité
Benoît Dupont

Aucune activité humaine n'échappe désormais à la transformation numérique qui a déferlé sur nos sociétés au cours des deux dernières décennies, et qui s'exprime notamment par l'omniprésence dans nos vies de technologies telles que la téléphonie mobile, l'internet, et de manière croissante les objets connectés. Au Québec, plus de 85% de la population utilise internet à des fins personnelles sur une base quotidienne, que ce soit pour socialiser, magasiner, effectuer des transactions bancaires, se distraire ou accéder à des services publics (Bernier 2017). Par ailleurs, 62% de la population adulte possède un téléphone intelligent et 52% une tablette électronique qui leur permet aussi d'accéder à internet (CEFRIO 2017). L'internet est devenu tellement indispensable à notre bien-être que dans un récent sondage, 46% des canadiens se disaient prêt à renoncer à des repas de restauration rapide pendant un an afin de conserver l'accès à cette technologie, et qu'une proportion presque aussi importante de la population était disposée à ne pas consommer d'alcool (34%), de chocolat (31%), de café (26%), ou même à se priver de relations sexuelles (9%) pendant la même durée pour continuer à aller sur le web (ACEI 2017). Si les avantages sociaux et les bénéfices économiques que procurent l'internet et la téléphonie mobile sont indéniables, l'avènement rapide de ces technologies s'est aussi accompagné de nouveaux risques criminels exploitant de nombreuses failles de sécurité et tirant profit d'une complexité rendant très difficile le contrôle des comportements illégaux. Qu'il s'agisse de fraudes bancaires dont ils sont les victimes, de la protection défaillante de leurs données personnelles par les organisations avec lesquelles ils transigent en ligne, de l'exposition de leurs enfants à la cyberintimidation, de la banalisation des images de pornographie juvénile, des contenus propices à la radicalisation déployés par des groupes extrémistes de tous bords, ou encore de la prolifération des « fausses nouvelles » sur les plateformes de médias sociaux, les internautes sont exposés à de nombreux risques criminels qui ont historiquement relevé de la sphère de responsabilité des institutions policières. Toutefois, ces dernières semblent éprouver de la difficulté à opérer une transition stratégique vers ce nouvel environnement criminel et à adapter leurs structures et leurs pratiques.

Les causes à l'origine de ces difficultés d'adaptation relèvent de deux logiques complémentaires : complexité excessive et manque de capacité (Klap et de Groot 2013 : 91-92). D'abord, la nature technique des systèmes informatiques qui rendent les cybercrimes possibles induit une complexité technologique qui entrave les enquêtes criminelles. Cette complexité technologique des enquêtes sur les cybercrimes les plus sophistiqués comme les actes de piratage informatique ou les cyberattaques contre les infrastructures critiques requiert la mobilisation par les organisations policières d'expertises nouvelles et de ressources financières et techniques disponibles en quantité limitée. Cependant, tous les cybercrimes ne dépendent pas de la technologie pour exister. Certains d'entre eux constituent plutôt l'évolution inévitable de formes traditionnelles de crimes comme la fraude, l'exploitation sexuelle des enfants ou encore le vol. On utilise

pour distinguer les deux catégories les termes respectifs de crimes cyber-dépendants (*cyber-dependent*) et de crimes cyber-facilités (*cyber-enabled*) (McGuire et Dowling 2013). Le principal problème auquel fait face la police dans le cas des crimes cyber-facilités n'est pas celui de la complexité technique, car celle-ci demeure généralement faible, mais plutôt de la capacité de traitement de milliers de nouveaux dossiers générés par l'automatisation et l'industrialisation de la délinquance numérique.

La cybercriminalité est devenue la principale forme de crime contre la propriété et représente dorénavant la moitié des incidents criminels répertoriés par les enquêtes de victimisation. Cette forme de délinquance s'articule en un mode d'organisation par projets impliquant des participants disséminés sur l'ensemble de la planète, ce qui rend les enquêtes policières particulièrement difficiles à mener. La tension entre le mode d'organisation local du travail policier et la structure mondialisée de la cybercriminalité explique de surcroît pourquoi les organisations policières éprouvent de la difficulté à adapter leurs modes d'intervention et laissent jusqu'à présent le secteur privé occuper le terrain de la prévention et de l'enquête. Au-delà des problèmes de complexité et de capacité, les services de police se posent désormais la question des transformations structurelles, professionnelles, et culturelles requises afin de relever avec succès le défi de la transition numérique. Ces transformations concernent les quatre grandes fonctions policières liées à la délinquance économique, réunies dans le modèle des quatre P : 'Poursuivre' pénalement les groupes criminels et perturber leurs activités, 'Prévenir' l'entrée dans la carrière criminelle des individus à risques, 'Protéger' les organisations et les particuliers contre les risques de victimisation, et 'Préparer' les organisations et les particuliers à faire face aux risques criminels et à en atténuer les effets négatifs[6] (Levi et al. 2015 : 5).

Afin d'examiner quelles transformations sont déjà engagées, et quels efforts supplémentaires sont requis, ce chapitre est organisé en trois parties. Dans une première section, le problème de la quantification de la cybercriminalité est étudié. Un déficit chronique de statistiques fiables empêche en effet les organisations policières de prendre la pleine mesure du phénomène de la cybercriminalité et de planifier les stratégies d'intervention susceptibles de produire les résultats les plus efficaces en matière de prévention et de répression. Dans une seconde section, nous nous penchons sur les expertises policières disponibles et les besoins anticipés, aussi bien en termes de connaissances générales des patrouilleurs que d'expertise technique spécialisée de la part des enquêteurs et de leurs équipes de soutien technique. Cela implique notamment de se questionner sur la formation des divers intervenants, la pertinence de confier les enquêtes sur les cybercrimes à des unités spécialisées ou au contraire de diffuser l'expertise plus largement au sein de l'organisation, le rôle que pourraient être amenés à jouer les employés civils dans ce type d'enquête et les obstacles posés aux méthodes d'enquête par l'évolution constante des technologies. Finalement, la troisième et dernière partie se

[6] Ce modèle a été formulé pour la première fois afin de conceptualiser les diverses dimensions de la lutte anti-terroriste au Royaume-Uni, mais il a été étendu depuis à d'autres domaines d'intervention policière.

tourne vers les stratégies d'intervention en partenariat qui pourraient être envisagées par les organisations policières afin de compenser leurs manques de ressources et d'expertise, même si se pose l'épineuse question du contrôle et de l'efficacité de ce type d'interventions.

1. La disponibilité et la fiabilité des instruments de mesure de la cybercriminalité

Le discours public sur la cybercriminalité et les politiques de prévention et de répression qui en découlent reposent sur un recours intensif à des statistiques dont la nature, la provenance et la qualité s'avèrent problématiques (Flôrencio et Herley 2013, Côté et *al.* 2016, Levi et al. 2015, Dupont 2018). La recension et l'utilisation des statistiques sur la cybercriminalité doivent alors s'accompagner d'un examen critique de leur origine et de leur validité. Parmi les principales objections soulevées aux chiffres disponibles, citons l'importance prise par les acteurs privés de la cybersécurité dans la production et la diffusion de rapports de référence basés sur des méthodologies opaques et destinés à susciter un sentiment d'insécurité propice à la commercialisation de leurs services (Dupont 2016a, Levi at al. 2015), le recours à des sondages d'opinion reposant sur des échantillons réduits de répondants pour quantifier la prévalence d'un phénomène inégalement distribué dans l'espace, le temps et au sein de la population (Furnell et al. 2015), la difficulté de comparer des statistiques collectées par des acteurs qui mobilisent des méthodologies d'analyse très variées, la fréquence irrégulière de collecte des données qui limite l'analyse temporelle de l'évolution des phénomènes étudiés (Reep-van den Bergh et Junger 2018), la difficulté méthodologique de comptabiliser les comportements criminels qui comprennent à la fois des composantes en ligne et hors-ligne (Levi 2017), ainsi que l'épineux problème de la sous-déclaration des cybercrimes aux services de police (Caneppele et Aebi 2017).

La critique des statistiques de la cybercriminalité s'est aussi questionnée sur l'impact de l'émergence d'une délinquance en ligne endémique sur la quantification du volume global de la criminalité. Certains auteurs estiment en effet que la baisse spectaculaire de la criminalité traditionnelle enregistrée depuis la moitié des années 1990 dans les pays occidentaux (le *crime drop*) correspond en réalité à l'apparition de nouvelles formes de crimes dans lesquelles les délinquants se sont reconvertis (Tcherni et al. 2016). Sans apporter de preuve définitive du déplacement de la délinquance de ses sphères d'activités traditionnelles vers les cybercrimes, il est indéniable que le volume actuel de ces derniers, qui représente selon les pays du tiers à la moitié de l'ensemble des crimes, remet sérieusement en question le mythe de la chute drastique de la criminalité depuis une vingtaine d'années (Caneppele et Aebi 2017). Autrement dit, le déficit de statistiques fiables sur la cybercriminalité aurait biaisé notre interprétation de l'évolution réelle de la délinquance globale depuis deux décennies.

1.1. Les tendances récentes de la cybercriminalité

En dépit des limites mentionnées précédemment, il ne fait aucun doute que la cybercriminalité représente la forme de délinquance connaissant la plus forte augmentation depuis un quart de siècle et qu'elle constitue l'un des défis les plus complexes auxquels sont confrontées les organisations policières. Les chiffres les plus récents provenant d'enquêtes rigoureuses sont à cet égard éloquents. Une étude européenne faisant la synthèse de neuf enquêtes de victimisation conduites en Allemagne, en France, en Hollande, au Luxembourg, au Royaume-Uni et en Suède de 2010 à 2016 auprès d'un échantillon cumulatif de 187 000 répondants sélectionnés au hasard indique ainsi les taux de prévalence suivants pour six grandes catégories de cybercrimes :

Type de cybercrime	Pourcentage de la population victimisée au cours des douze mois précédents
Fraude au commerce en ligne	0,6 à 3,5%
Fraude bancaire en ligne	0,4 à 2,2%
Autres cyber-fraudes	0,2 à 0,4%
Cyberintimidation	3%
Logiciels malveillants	2 à 15%
Piratage informatique	1,2 à 5,8%

Source : Reep-van den Bergh et al. 2018.

Ces chiffres qui représentent en valeur absolue des millions de victimes sont probablement sous-estimés, car une part non négligeable de ces dernières n'a pas l'expertise technique requise pour identifier les attaques dont elles font l'objet et n'ont ainsi pas toujours conscience d'être exposées à des actes criminels (Leukfeldt et al. 2013 : 12). Par ailleurs, certaines formes de cybercriminalité recensées plus haut connaissent une croissance annuelle soutenue du fait de l'augmentation des opportunités criminelles provoquée par les transformations de notre système économique : la fraude en ligne connaît ainsi en Angleterre une progression de 3% par an (Hitchcock et al. 2017 : 12).

Les statistiques disponibles pour le Canada sont moins récentes mais tout aussi préoccupantes. La dernière enquête de cyber-victimisation menée en 2009 par Statistique Canada auprès d'un échantillon de 19 500 ménages indiquait ainsi que 7% de la population âgée de plus de 15 ans avait été victime de cyberintimidation, avec un pic à 17% pour les 15 à 24 ans. Les cas de fraude bancaire en ligne touchaient quant à eux 4% de la population des plus de 15 ans, mais faisaient seulement 2,6% de victimes au Québec. Les problèmes causés par des achats en ligne—incluant les fraudes et les erreurs attribuables aux marchands— concernaient 14% des internautes, alors que la victimisation liée à des infections par logiciels malveillants culminait à plus de 65% de l'échantillon. Le piratage informatique de comptes de courriel ou de fichiers d'ordinateurs était finalement signalé par 9% des répondants. Il semble donc que les taux de victimisation sont plus élevés au Canada qu'en Europe, même s'il est difficile de tirer des conclusions définitives en l'absence de données plus récentes. On peut également noter que les taux de déclaration

à la police restent extrêmement faibles au Canada, où seulement 7% des cas de cyberintimidation ont fait l'objet d'un signalement aux autorités (Perreault 2011). Par comparaison, 31% des incidents de victimisation avec violence et des ménages avaient été déclarés à la police la même année (Perreault 2015). Bien qu'il soit difficile de dresser un parallèle exact entre les chiffres tirés de l'étude de Statistique Canada et les plaintes reçues par le Centre antifraude du Canada, la seule plateforme nationale de collecte des plaintes en matière de fraude par marketing de masse et de vol d'identité, on peut noter que seulement 13 600 victimes s'étaient manifestées auprès du CAFC en 2009, dont 5900 au Québec (Tison 2011), ce qui confirme des taux de déclaration à la police qui restent très en-deçà de la réalité. Cette constatation est généralisable aux autres pays ayant mené des enquêtes de victimisation au cours des dernières années (Leukfeldt et al. 2013 : 12, Bangs 2018).

Type de cybercrime	Pourcentage de la population de plus de 15 ans victimisée	Nombre de victimes de plus de 15 ans
Problème concernant les achats en ligne	14%	3,8 millions
Fraude bancaire en ligne	4%	1,1 millions
Cyberintimidation	7%	1,9 millions
Logiciel malveillant	65%	18,3 millions
Piratage informatique	9%	2,5 millions

Source : Perreault 2011.

Les entreprises, bien qu'en apparence mieux protégées contre la cybercriminalité, sont aussi lourdement exposées aux préjudices financiers qui y sont associés. Dans une étude menée par Statistique Canada en 2018 auprès de 12 597 entreprises de toutes tailles, les dépenses de ces dernières en cybersécurité étaient évaluées à 14 milliards de dollars en 2017, ce qui incluait les dépenses liées à la formation du personnel, à la mise en œuvre de mesures techniques et organisationnelles de prévention, et à la réponse aux incidents. Bien que 21% des entreprises déclaraient avoir été victimes d'une attaque cette année-là, seulement 10% d'entre elles le signalèrent à un service de police bien que la majorité de ces incidents aient été de nature criminelle. Les principales raisons invoquées par les entreprises victimes pour ne pas communiquer avec la police étaient que l'incident avait été résolu à l'interne (53%), avec le soutien d'entreprises spécialisées en cybersécurité (35%), ou encore parce que les impacts n'étaient pas jugés suffisamment importants (29%) (Statistique Canada 2018). Les préjudices découlant d'une cyber-attaque, souvent causée par un comportement criminel, sont pourtant loin d'être négligeables, puisqu'on estimait en 2017 le coût d'une brèche de donnée à 5,78 millions de dollars par incident pour les entreprises canadiennes affectées (Ponemon Institute 2017 : 8). Une étude adoptant une méthodologie différente évalue le coût annuel moyen des activités de prévention, de réponse et des mesures d'atténuation liées aux brèches de données à 3,7 millions de dollars par entreprise (Scalar 2018).

Les statistiques fragmentaires et souvent relativement anciennes sur la cybercriminalité reflètent un déficit de connaissances problématique pour la planification et la mise en œuvre de programmes de prévention et d'application de la loi efficaces pour contrôler une délinquance caractérisée par sa très rapide évolution. Les enquêtes de cyber-victimisation devraient ainsi être menées selon un rythme beaucoup plus fréquent, à l'instar du *Crime Survey for England & Wales* dont les résultats sont disponibles sur une base annuelle. Cette mise à jour constante des statistiques s'avère particulièrement utile pour les formes de crime qui font l'objet d'une sous-déclaration marquée à la police, comme c'est le cas pour la cybercriminalité, même si les résultats remettent en question le mythe d'une diminution de la délinquance. La disponibilité de statistiques fiables et récentes capables de mesurer aussi bien la prévalence du phénomène que son impact sur les victimes (préjudices directs et indirects et coûts induits) permettrait de mieux cibler les besoins en termes de priorité des interventions policières, ainsi que de mettre en place des démarches évaluatives probantes facilitant l'identification des stratégies efficaces et de celles qui ne produisent pas les résultats espérés (Anderson et al.2013, McGuire et Dowling 2013).

1.2. La sous-déclaration chronique des cybercrimes à la police

L'importance des statistiques publiques colligées régulièrement auprès de vastes échantillons de la population est d'autant plus grande que les mécanismes de déclaration à la police restent sous-utilisés par le public, même lorsque des efforts considérables sont mis en œuvre afin de simplifier les procédures. Plusieurs pays ont créé dès le début des années 2000 des plateformes en ligne permettant aux victimes de signaler les cybercrimes auxquels elles ont été exposées. Certains pays comme le Canada (Centre antifraude du Canada[7]), les États-Unis (Internet Crime Complaint Centre[8]), ou encore le Royaume Uni (Action Fraud[9]) ont concentré leurs efforts sur les fraudes en ligne, alors que la Nouvelle-Zélande (Online Reporting Button[10]) et l'Australie (ACORN[11]) adoptaient une approche beaucoup plus large incluant les cas de piratage informatique, mais aussi de harcèlement, d'intimidation et de sexting. Toutefois, seule l'Australie a procédé à une évaluation rigoureuse de l'impact de la plateforme ACORN (Australian Cybercrime Online Reporting Network). Les résultats s'avèrent mitigés.

Bien que les usagers ayant signalé un cybercrime sur la plateforme semblent généralement satisfaits de la qualité de l'interface et de la facilité avec laquelle il est possible de transmettre l'information demandée, moins du tiers d'entre eux se sont déclarés satisfaits de l'issue de la procédure, notamment en raison du manque d'enquêtes policières initiées suite à la déclaration (seulement le sixième des déclarations donnent lieu à une enquête criminelle). La plateforme ne semble pas non plus avoir contribué à augmenter les

[7] http://www.antifraudcentre-centreantifraude.ca/index-fra.htm
[8] https://www.ic3.gov/default.aspx
[9] https://www.actionfraud.police.uk/
[10] http://www.theorb.org.nz/
[11] https://www.acorn.gov.au/

connaissances du public en termes de procédures de déclaration des cybercrimes, et seulement 14% de la population australienne avait conscience de l'existence de ce nouveau mode de déclaration plus d'un an après son lancement. On peut toutefois noter que les personnes informées de l'existence d'ACORN se déclaraient plus positives envers les mesures mises en place par le gouvernement australien pour lutter contre la cybercriminalité que le reste de la population. La plateforme a également permis aux usagers d'accéder à des conseils plus ciblés en matière de prévention de la cybercriminalité, en fonction des incidents auxquels ils ont été exposés, et ces conseils sont mis en œuvre par les victimes tel que suggéré, mais rien n'indique par contre que cela ait permis de réduire les risques de victimisation à répétition. Pour les victimes ayant choisi de ne pas soumettre de déclaration, malgré l'accessibilité de la plateforme, les trois principales raisons invoquées sont le sentiment que l'incident n'était pas suffisamment grave pour justifier l'effort d'un signalement (40%), l'incertitude quant à l'organisme gouvernemental à qui un tel incident doit être signalé (39%), et l'impression que leur déclaration ne donnerait lieu à aucune suite (35,5%) (Morgan et al. 2016).

L'une des fonctions d'ACORN est de faciliter l'agrégation des données afin de consolider les renseignements criminels sur les phénomènes de cybercriminalité à l'échelle nationale et locale, afin de permettre une meilleure utilisation des ressources policières. Cet objectif a été partiellement atteint, ce qui a provoqué une augmentation significative du nombre d'enquêtes policière ouvertes pour des affaires de cybercriminalité, qui ont été multipliées par trois dans certaines juridictions. Les ressources disponibles pour mener ces enquêtes n'augmentent cependant pas toujours au même rythme, notamment en raison de l'expertise technique requise et des délais nécessaires pour recruter et former des enquêteurs compétents, ce qui explique que certains services spécialisés accumulent les affaires ouvertes mais inactives. Ces retards importants sont susceptibles de nuire aux chances d'identifier et d'arrêter les auteurs de cybercrimes, ainsi qu'à la satisfaction des victimes (Morgan et al. 2016).

Les conclusions de cette évaluation, la seule portant sur un dispositif policier visant à améliorer les taux de déclaration de cybercrimes rendue publique à ce jour, laisse penser que bien des efforts restent encore à accomplir afin de convaincre les victimes de la nécessité d'informer la police et de lui communiquer les informations nécessaires afin d'améliorer la qualité du renseignement criminel disponible et d'initier un nombre croissant d'enquêtes. Toutefois, même une faible augmentation du nombre de signalements permet d'augmenter la pression sur les organisations policières et pousse ces dernières à libérer des ressources additionnelles afin de s'adapter à leur nouvel environnement criminel. La police conserve d'ailleurs sa légitimité aux yeux du public comme institution de première ligne en cas de cyber-victimisation, si l'on en croit une étude de grande ampleur menée en Europe en 2017. Conduit auprès de 28 000 personnes provenant de 28 pays, ce sondage fait de la police l'institution la plus fréquemment mentionnée par les répondants comme premier contact en cas de vol d'identité (85%), de fraude en ligne (76%), ou encore de détection de contenus pédopornographiques en ligne (76%). C'est seulement dans le cas d'une infection par un logiciel malveillant que les

usagers européens feraient majoritairement appel à une autre organisation, en l'occurrence leur fournisseur d'accès à internet (29%). Cette légitimité reste cependant fragile, puisque seulement la moitié des citoyens européens estiment que la police fait suffisamment d'efforts pour combattre la cybercriminalité (TNS opinion & social 2017). On estime d'ailleurs que seulement 2% des cybercrimes faisaient l'objet de poursuites criminelles au milieu des années 2000, une statistique qui a probablement peu évolué depuis (Jewkes 2013: 526). Aucune statistique comparable n'est disponible au Québec, mais on peut émettre l'hypothèse que l'attitude du public y est probablement comparable, l'ampleur du problème et la nature de la réponse policière étant similaires des deux côtés de l'Atlantique. Dans un tel contexte, le défi des expertises policières disponibles et des besoins requis afin de répondre aux attentes du public s'avère un enjeu crucial dans le processus d'adaptation des organisations policières à la prolifération de la cybercriminalité.

2. Les expertises policières disponibles et les besoins anticipés

Comme l'a fait remarquer Theresa May lorsqu'elle était Ministre de l'Intérieur du Royaume Uni, « les policiers utilisent trop souvent des technologies qui accusent un retard considérable sur celles qu'ils utilisent en tant que consommateur » (Hitchcock et al. 2017 : 19). Ce décalage entre les technologies grand-public et les systèmes informatiques parfois désuets déployés par les organisations policières illustre de manière cruelle les obstacles que ces dernières doivent surmonter afin d'adapter l'expertise et les moyens d'enquête traditionnels aux mutations imposées par la cybercriminalité. Parmi les principaux défis associés à cette transition numérique des institutions policières, cinq doivent attirer tout particulièrement notre attention : la perception qu'ont les policiers de la gravité que représente le phénomène de la cybercriminalité et du rôle que la police doit jouer dans sa prévention et son contrôle; les capacités et le rôle des unités d'enquête spécialisées dans l'architecture de la réponse policière; les difficultés spécifiques rencontrées dans le domaine de la collecte et de l'analyse de la preuve numérique face à l'augmentation exponentielle des données numériques générées et au cryptage croissant de ces données; les besoins en formations générales et spécialisées découlant des décisions prises quant aux stratégies d'intervention face aux cybercrimes; et enfin la pertinence de faire appel à des employés civils ou à des sous-traitants privés pour certaines tâches d'enquête spécialisées.

2.1. Les perceptions qu'ont les patrouilleurs, les enquêteurs et les gestionnaires policiers de la cybercriminalité

La perception qu'ont les policiers du phénomène de la cybercriminalité, de la place que cette dernière occupe dans la hiérarchie informelle des crimes, et de la performance actuelle de la réponse policière constitue un élément important de toute stratégie de transformation des agences d'application de la loi. En effet, ces attitudes influencent les comportements et les pratiques des policiers face aux incidents qui leurs sont signalés par

le public, ainsi que leurs capacités d'adaptation à de nouvelles stratégies et les compétences nouvelles requises pour implanter ces dernières. Par exemple, plusieurs rapports de recherche préconisent que les policiers en uniforme (ou premiers intervenants) soient formés afin de jouer le même rôle dans les enquêtes sur les cybercrimes que celui assumé depuis quelques décennies dans les crimes traditionnels (Goodman 1997, Stambaugh et al. 2001, NIJ 2008, Leukfeldt et al. 2013), en étant par exemple sensibilisés au dépôt de plaintes de membres du public, à la préservation des scènes de crime, des indices matériels et numériques, et à leur documentation initiale avant que les enquêteurs spécialisés et les experts forensiques n'arrivent sur les lieux et prennent le contrôle de l'affaire tout en maintenant la continuité de la preuve (UNODC 2009). Pourtant, une telle approche ne peut être adoptée et généralisée que si elle s'appuie sur la conviction des policiers que les cybercrimes relèvent pleinement de leur domaine d'intervention et qu'ils souscrivent à un modèle de réponse local (Holt et al. 2018 : 3).

Historiquement, les études menées sur la perception qu'ont les policiers en uniforme de la cybercriminalité postulent un désintérêt de la part des intervenants de première ligne, qui sous-estimeraient la gravité de cette forme de délinquance en raison de l'absence de contact physique entre les auteurs et leurs victimes et ne se sentiraient pas suffisamment formés et équipés techniquement pour y répondre (Huey 2002, Powell et Henry 2018). Le fait que les enquêtes en matière de cybercriminalité ressemblent aux méthodes déployées pour combattre la criminalité en col blanc, c'est à dire qu'elles se mènent derrière un bureau plutôt que sur le terrain, contribuerait aussi à cette supposée indifférence en raison de la nature plus administrative qu'opérationnelle des enquêtes sur les crimes en ligne (Goodman 1997, Holt et al. 2018).

Les données empiriques restent cependant très limitées, à l'exception de quelques sondages menés aux États-Unis et au Royaume-Uni par la même équipe de chercheurs et qui viennent nuancer cette vision pessimiste (Bossler et Holt 2012, Bossler et Holt 2013, Holt et al. 2018). Les premiers sondages conduits aux États-Unis à la fin des années 2000, dans des services de police régionaux de quelques centaines de patrouilleurs, laissent entrevoir des organisations où la majorité des agents (61,5%) n'avait jamais été confrontée à des cybercrimes et où seulement 11,6% des répondants avaient reçu une quelconque formation dans le domaine (Bossler et Holt 2012, Bossler et Holt 2013). L'immense majorité (72,8%) estimait que la réponse aux cybercrimes relevait exclusivement des unités d'enquête spécialisées. Alors que la cybercriminalité pouvait encore être considérée comme une forme de délinquance émergente, plus de la moitié des policiers interrogés semblaient dénués d'opinion sur le degré de gravité de la cybercriminalité et la priorité qu'elle représentait pour la hiérarchie policière. Toutefois, dès la fin des années 2000, les intervenants de première ligne pressentaient que la délinquance numérique transformerait le travail policier en profondeur et semblaient soutenir les adaptations requises pour mener des enquêtes plus efficaces. Par contre, les solutions privilégiées favorisaient une plus grande responsabilisation des usagers, l'intensification des poursuites pénales et l'imposition de peines plus sévères, ainsi que l'amélioration des

capacités techniques d'enquête et de la formation des enquêteurs. A contrario, les approches de sensibilisation du public ou de partenariat avec le secteur privé, inspirées du modèle de police communautaire, semblaient moins favorisées par les répondants, alors que la démarche préventive relève justement naturellement de la sphère de responsabilité des policiers en uniforme, qui entretiennent un contact plus régulier avec la population (Dupont 2007).

Les résultats d'un sondage mené dix ans plus tard au Royaume-Uni auprès de près de 1500 policiers et reposant sur des questions similaires ne permettent malheureusement en aucune façon de comparer les résultats pour en déduire une évolution des attitudes, puisque les systèmes d'organisation du travail policier s'avèrent extrêmement différents d'un pays à l'autre. On peut néanmoins clairement observer comment en une dizaine d'années, la cybercriminalité est devenue omniprésente dans le quotidien des patrouilleurs (Holt et al. 2018). Plus du tiers (35,3%) des répondants a reçu une formation les préparant à répondre à des incidents de cybercriminalité, qui a été mise en application de façon concrète lors d'interventions par près de 95% d'entre eux au cours des douze derniers mois. La très grande majorité (86,2%) des policiers sondés estiment que les cybercrimes représentaient un sérieux problème de société et que leur impact sur les victimes constitue bien plus qu'un simple inconvénient, reconnaissant la gravité de situations de harcèlement en ligne ou de cyberfraude. Près de 80% des policiers anglais dressent également un constat alarmant du manque de connaissances du public à l'égard des cybercrimes et des risques associés à certaines activités en ligne. Une mesure du temps consacré au cours des derniers mois aux divers types de cybercrime fait ressortir une nette prévalence des affaires de harcèlement et d'abus en ligne, alors que les cyberfraudes et les cas de piratage ou d'infection par des logiciels malveillants arrivaient en dernière position. Ces formes particulièrement fréquentes de cybercrimes semblent donc moins prioritaires pour les services de police britanniques, à l'instar de la situation observée aux États-Unis (Holt et al. 2013), probablement en raison de leur volume industriel, de la dimension technique des enquêtes qui y sont associées et aussi des faibles chances de mener à bien des poursuites criminelles dans ce type de cas.

Ces résultats contredisent la perception que les policiers de première ligne sont indifférents ou sous-estiment la gravité de la cybercriminalité et de ses impacts sur les victimes, ou encore qu'ils sont réfractaires à toute forme d'intervention dans le domaine. Toutefois, ils restent insuffisamment formés à cette forme particulière de crime et doivent interagir avec des victimes qui semblent elles-mêmes assez mal équipées pour se protéger efficacement contre les risques criminels auxquels elles se trouvent confrontées en ligne. Ces résultats restent issus de modèles policiers qui divergent fortement du contexte canadien, et aucune donnée locale n'est malheureusement disponible afin de vérifier que ces conclusions peuvent être généralisées au-delà des deux pays concernés.

2.2. Le rôle et les capacités des unités d'enquête spécialisées

L'une des conséquences majeures des changements provoqués par la démocratisation des outils numériques et la prolifération des cybercrimes est l'explosion du nombre d'enquêtes policières dans lesquelles des traces numériques résidant sur un nombre sans cesse croissant d'équipements électroniques doivent être collectées, exploitées et analysées. En réponse, les organisations policières se sont dotées de quatre grandes catégories d'unités d'enquête spécialisées (CyberCrime@IPA 2011, Jewkes 2013 : 540). Le premier type d'unité se caractérise par son haut degré d'expertise technique afin d'exploiter les traces numériques extraites de divers équipements électroniques saisis. Ces unités d'analyse judiciaire informatique répondent aux besoins techniques d'autres groupes d'enquête spécialisés. Le second type d'unité se spécialise dans la collecte du renseignement sur des personnes d'intérêt ou des délinquants persistants et déploie à ce titre des méthodes d'acquisition sur les plateformes en ligne et des techniques d'interception des communications électroniques. Le troisième type d'unité est constitué des groupes qui initient eux-mêmes des enquêtes sur les cybercrimes comme le piratage informatique ou la cyberfraude à grande échelle, selon une perspective où la technologie constitue une fin ou un outil facilitant plutôt qu'un moyen d'assistance (Levi et al. 2015 : 3). Finalement, les organisations policières ont aussi établi des unités d'enquête spécialisées dans la pédopornographie en ligne, qui se focalisent sur les délinquants produisant et distribuant des contenus illicites ainsi que sur ceux cherchant à établir un contact sexuel avec des mineurs via des plateformes numériques fréquentées par ces derniers. Toutes les organisations policières ne disposent pas systématiquement de ces quatre types d'unités mais cette typologie des fonctions représente maintenant le modèle le plus répandu de distribution et d'organisation des expertises.

Dans les pays où les organisations policières fonctionnent selon une structure décentralisée, des unités de coordination ont également vu le jour afin de faciliter la mise en commun du travail des unités d'enquête locales et d'éviter une duplication des efforts. Dans certains cas, ces unités de coordination sont également responsables de l'établissement et de la gestion des partenariats avec les collaborateurs privés et académiques afin de mettre en place des mécanismes de partage du renseignement et d'accélérer les projets de recherche et développement pouvant améliorer l'efficacité des enquêteurs. Au Royaume-Uni, la *National Cyber Crime Unit* est ainsi responsable au niveau national de la coordination des unités d'enquête régionales (les *Regional Cyber Crime Units*), elles-mêmes constituées de spécialistes provenant des divers services de police locaux (HMIC 2015, Schreuders et al 2018 : 6)[12]. En France, un pays beaucoup plus centralisé mais disposant néanmoins de deux organisations policières nationales, c'est l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (l'OCLCTIC) qui assume ce mandat de coordination et de lien avec les partenaires non-policiers. Il a ainsi signé une convention avec une école d'ingénieurs afin de développer des outils sur mesure dédiés à la lutte contre la cybercriminalité

[12] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

(Robert 2014 : 37). La police hollandaise a quant à elle créé au sein de son unité spécialisée (*Team High Tech Crime*) un sous-groupe de travail (l'*Electronic Crimes Task Force*) composé d'experts provenant du secteur bancaire et de procureurs expérimentés (Levi et al. 2015 : 64). Un dernier exemple concerne la création en 2002 par le FBI américain d'une plateforme nationale (la *National Cyber-Forensics and Training Alliance*[13]) où les organisations policières, les entreprises et les chercheurs universitaires peuvent travailler ensemble et partager des renseignements criminels conduisant à des arrestations ou à la perturbation de réseaux délinquants dans un environnement de confiance (Plesco et Schneck 2011).

L'un des principaux enjeux du fonctionnement des unités spécialisées d'enquête est leur intégration dans la chaîne pénale du traitement des affaires de cybercriminalité, et notamment les liens qu'elles entretiennent en amont avec les policiers de première ligne et en aval avec les procureurs chargés de mener les poursuites pénales. Une étude hollandaise ayant analysé 454 dossiers d'enquête initiés entre 2002 et 2007 (140 en matière de piratage informatique et 314 pour des cas de cyberfraude) fit apparaître un déficit chronique de communication et de coordination entre les enquêteurs spécialisés et leurs collègues en uniforme, ce qui conduisit à des taux de poursuite pénale relativement faibles de la part des procureurs (Leukfeldt et al. 2013). Dans le processus de filtrage des enquêtes destiné à prioriser et à sélectionner celles ayant les meilleures chances d'aboutir à l'arrestation des auteurs et à leur condamnation, les enquêteurs disposent rarement d'indices clés permettant d'augmenter les chances d'une conclusion favorable, souvent par manque de connaissances des agents ayant procédé à l'enregistrement initial de la plainte et à la collecte des informations, qui ont omis de recueillir des renseignements essentiels. Par ailleurs, les cas de cybercrimes sont souvent considérés comme secondaires par rapport aux dossiers plus classiques par les enquêteurs non spécialisés qui assurent l'interface entre les policiers en uniforme et les experts techniques pour trois raisons principales : ils jugent leur impact social moindre, ils manquent d'expérience dans ce type d'enquête et ne disposent pas toujours des connaissances requises pour enquêter efficacement. Il en résulte que dans l'échantillon analysé, 80% des cas de piratage informatique et 46,4% des cas de cyberfraude ont été classés sans suite par les équipes d'enquête par manque de preuves, et que seulement 5,9% des cas de piratage et 18% des cas de cyberfraude ont été transmis aux procureurs (Leukfeldt et al. 2013 : 13).

Dans l'une des rares études empiriques menées sur ce sujet, Barril (2014) a mis en lumière les trois principaux défis opérationnels qui limitent l'efficacité des unités spécialisées, et particulièrement celles qui procèdent à des analyses judiciaires (ou forensiques). Le premier défi est celui de l'étirement des délais de traitement entraîné par des ressources insuffisantes (GRC 2012, UNODC 2013), des demandes d'assistance technique en croissance exponentielle et l'augmentation constante des quantités d'équipements et de données saisis par les enquêteurs. Cet étirement varie selon la nature des affaires traitées et les priorités organisationnelles : les demandes liées à la sécurité nationale (terrorisme)

[13] https://www.ncfta.net/

ou à la lutte contre le crime organisé sont traités plus de quatre fois plus rapidement que les cas de fraude (respectivement dans des délais de 8 et 38,5 jours). Les retards procéduraux qui peuvent découler de l'allongement des délais de traitement deviennent problématiques lorsqu'ils menacent l'intégrité des poursuites pénales, en faisant basculer ces dernières dans des délais jugés déraisonnables au sens de l'arrêt Jordan[14]. Le deuxième défi est celui de la diffusion des connaissances et des compétences au sein de l'organisation policière, afin que les autres unités spécialisées d'enquête comprennent bien les limites des résultats qu'elles peuvent espérer des cyber-forensiciens et qu'elles se débarrassent des attentes irréalistes et des perceptions erronées qui teintent parfois leurs demandes—le fameux effet *CSI* (Goodison et al. 2015 : 17, Podlas 2017), ou encore qu'elles développent en interne des capacités d'analyse judiciaire rudimentaires leur permettant de procéder sans délais aux premières extractions de preuves numériques. Par ailleurs, on peut aussi intégrer dans cette catégorie de défis la complexité associée à la formation à l'interne de spécialistes en analyse judiciaire, à la fois en raison du manque de candidats, de la durée de la formation et de l'apprentissage requis (Goodison et al. 2015 : 16), de l'instabilité des équipes en raison des promotions régulières des policiers qui les composent, et enfin des salaires attrayants offerts par d'autres services publics ou le secteur privé qui érodent la rétention des spécialistes (Harkin et al. 2018). Le troisième défi opérationnel est hors de contrôle des organisations policières, mais affecte inévitablement leurs capacités à enquêter sur les cybercrimes : il s'agit de l'évolution rapide des technologies, moteur de l'innovation criminelle (Décary-Hétu et Bérubé 2018) qui nécessite une adaptation constante des techniques d'enquête, et l'évolution concomitante de la jurisprudence qui vient fréquemment imposer de nouvelles contraintes procédurales protectrices des droits individuels (Emond et Ellyson 2014).

Aux défis opérationnels se greffent des défis organisationnels qui exacerbent les difficultés d'adaptation éprouvées par la police dans sa lutte contre la cybercriminalité. Ces défis relèvent de la visibilité réduite dont bénéficient les unités d'enquête spécialisées, aussi bien au sein de l'organisation qu'à l'extérieur de cette dernière. Ce constat n'est pas nouveau, puisque qu'il découle de la stratégie habituelle d'adaptation des organisations policières aux nouvelles formes de délinquance, qui est de créer des unités spécialisées. Si cette démarche permet de concentrer l'expertise lorsque celle-ci est rare, elle ne favorise pas sa diffusion à l'échelle de toute l'organisation et produit même parfois l'effet opposé à celui qui est recherché. En effet, le maintien de certains types d'enquêtes sous la responsabilité exclusive d'unités spécialisées participe à la marginalisation des formes de délinquance qui y sont associées plutôt qu'à leur intégration au répertoire des tâches prioritaires incombant à l'ensemble des membres de l'organisation (Wall 2007 : 191).

Dans une étude empirique portant sur trois unités spécialisées australiennes, Harkin et Whelan (sous presse) mettent en exergue trois déficits de visibilité qui compliquent considérablement leur travail et limite leur impact. Le déficit de visibilité verticale fait référence au désintérêt de la hiérarchie policière pour la cybercriminalité, encore trop

[14] R. *v.* Jordan, 2016 SCC 27, [2016] 1 S.C.R. 631

souvent perçue comme un problème marginal ou en émergence, alimenté par une 'techno-phobie' qui l'empêche de prendre toute la mesure des transformations sociales induites par la Révolution Numérique. Ce manque d'appétit des plus hauts échelons de l'organisation se traduit en un soutien limité qui fragilise le fonctionnement des unités spécialisées. Le déficit de visibilité horizontale repose sur une logique identique de désintérêt, mais de la part des pairs enquêteurs et patrouilleurs plutôt que de la hiérarchie. Les membres des unités spécialisées étudiées ont exprimé leur frustration quant au faible statut que leurs emplois occupent dans la hiérarchie informelle des fonctions policières, et de la méconnaissance généralisée de la nature de leur expertise ainsi que de ses limites (Goodison et al. 2015 : 15). La nature énigmatique du travail accompli par ces unités nuit à l'établissement de relations de collaboration basées sur des attentes réalistes et freine leur pleine intégration à l'écosystème des services d'enquête. Finalement, le déficit de visibilité externe exprime la compréhension limitée qu'ont les acteurs institutionnels tels que les médias, le personnel politique, les procureurs et les juges, mais aussi l'opinion publique, du travail des services spécialisés. En dépit de la prise de conscience collective du fléau que représente dorénavant la cybercriminalité, l'intelligibilité du travail policier et des ressources que ce dernier mobilise demeure insuffisante aux yeux des spécialistes interrogés. Ces trois déficits de visibilité s'alimentent mutuellement et expliquent certainement en grande partie pourquoi la lutte contre la cybercriminalité reste rarement priorisée par les organisations policières, malgré l'accumulation de statistiques de plus en plus préoccupantes quant à sa prévalence et son impact sur les victimes.

2.3. Besoins en formations spécialisées et générales

Les besoins exprimés par les organisations policières afin de se doter d'une expertise d'enquête numérique adéquate relèvent de deux ordres. En premier lieu, elles doivent développer une expertise technique spécialisée en lien avec l'identification, l'extraction et l'analyse d'éléments de preuve numérique saisis sur des supports aussi variés que des ordinateurs, des sites internet, des téléphones intelligents, ou encore des objets connectés. En second lieu, elles doivent diffuser auprès de l'ensemble de leurs effectifs des connaissances générales sur les caractéristiques de la délinquance numérique, les dispositions que les intervenants de première ligne doivent prendre afin de préserver la preuve numérique, et les stratégies de prévention pouvant être communiquées aux citoyens.

Comme le soulignent les sondages et études qualitatives menées sur le terrain auprès des praticiens, la formation des spécialistes en analyse judiciaire et cyber-enquêtes constitue le besoin prioritaire des organisations policières à l'heure actuelle (Hinduja 2004, Goodison et al. 2015, Harichandran et al. 2016, Schreuders et al. 2018). Mais outre les considérations de coûts induites par la formation de spécialistes en enquêtes numériques, la difficulté à identifier des programmes de formation adaptés ou de recruter en interne des formateurs suffisamment qualifiés, et les délais jugés parfois excessivement longs avant que les experts formés deviennent opérationnels, les nouvelles compétences techniques requises par les cyber-enquêtes se heurtent à un manque de standardisation des formations et

certifications offertes par les établissements de formation policière et les institutions collégiales, universitaires et privées (Goodison et al. 2015 : 16). Cette situation découle notamment du fait que les cyber-enquêteurs sont confrontés à des cas extrêmement variés (terrorisme, crimes majeurs, trafic de stupéfiant, cybercriminalité, harcèlement et intimidation, etc.) faisant appel à des méthodes et à des outils d'analyse tout aussi diversifiés qui compliquent tout effort de standardisation. L'effort de création d'une Organisation internationale sur la preuve informatique (IOCE) au milieu des années 1990, ainsi que les efforts de standardisation pilotés par le G8 lors du Sommet d'Okinawa n'ont jamais produit les résultats espérés (Srinivasan 2013). Cette question de la standardisation est loin d'être anodine, car elle détermine indirectement la qualité et la fiabilité des techniques d'enquête et de traitement de la preuve qui sont mises en œuvre, venant donc indirectement garantir (ou au contraire éroder) la validité scientifique et l'intégrité de l'ensemble des procédures criminelles (National Research Council 2009). Dans un environnement où les enquêtes se ramifient à l'échelle internationale et où les éléments de preuve numérique sont recueillis dans des pays aux usages et aux contraintes juridiques très variés, une standardisation internationale facilite également la coopération policière (Grobler 2010).

De manière plus concrète, les forensiciens numériques accumulent ainsi des certifications spécifiques aux outils qu'ils utilisent, fréquemment dispensées par les entreprises qui commercialisent ces outils. Cela s'avère problématique puisqu'en l'absence de normes standardisées de présentation des résultats produits par ces derniers, chaque logiciel est libre d'adopter un format qui lui est propre (Bariki et al. 2010, Harichandran et al. 2016). Cela donne ensuite lieu à des utilisations et des interprétations plus ou moins assurées de la part des autres acteurs de la chaîne pénales (enquêteurs, procureurs, juges, jurés, avocats). Seule l'Organisation internationale de normalisation (ISO) publie depuis 2012 la norme ISO/IEC 27037, spécifiquement dédiée à la preuve numérique[15]. Cette norme a fait l'objet d'un effort de transplantation au Canada par le Comité e-Crime de l'Association canadienne des chefs de police afin de favoriser l'adoption des meilleures pratiques internationales.

Au-delà des formations de pointe réservées aux enquêteurs spécialisés et aux forensiciens numériques, on trouve dans la littérature scientifique de nombreux appels à la généralisation de formations rudimentaires qui devraient être également dispensées aux policiers en uniforme, afin d'améliorer la prise en charge des affaires routinières et de tenir compte de la multiplication des liens entre les crimes hors-ligne et les crimes en ligne (Leukfeldt et al. 2013 : 14). La stratégie suggérée pour faciliter l'adoption de ces nouvelles compétences est de mettre en lumière leur utilité pour mener des enquêtes criminelles classiques dont l'intensité technique va en s'accroissant, plutôt que de prétendre transformer les intervenants de première ligne en spécialistes de la cybercriminalité. Dans cette perspective, l'approche de la formation en ligne semble idéalement adaptée pour atteindre un large public de patrouilleurs en un laps de temps réduit.

[15] https://www.iso.org/fr/standard/44381.html

L'Union Européenne a ainsi financé le développement, via le *European Cybercrime Training and Education Group*, d'un module de formation en ligne destiné aux premiers répondants et leur conférant des connaissances de base en matière de crimes technologiques et des méthodes d'analyse judiciaire numérique[16]. Disponible en 9 langues, le module *e-First* sera gratuitement accessible à plus d'un million d'intervenants de première ligne. Au Royaume-Uni, le *National Centre for Applied Learning Technologies* a dispensé entre 2014 et 2015 un programme de quatre cours en ligne portant sur les principes de la cybercriminalité, les enquêtes en ligne, la place des médias sociaux dans les enquêtes et le rôle de la police à l'ère numérique qui a été suivi par 43 190 policiers en uniforme. Par comparaison, un cours introductif en salle de classe dispensé à travers tout le pays par le *College of Policing* n'a rejoint pendant la même période que 4394 patrouilleurs. On voit donc bien le potentiel des nouvelles technologies pour faciliter la sensibilisation et les apprentissages à grande échelle, par comparaison avec des approches plus traditionnelles. Généralement, les policiers ont apprécié le contenu des cours suivis en ligne, mais ont signalé de nombreux cas où l'équipement informatique mis à leur disposition pour y accéder s'est avéré inadéquat ou obsolète (HMIC 2015 : 31). Par ailleurs, la rapidité avec laquelle la cybercriminalité évolue et la difficulté qu'éprouvent les organismes de formation policière à mettre à jour les contenus des formations offertes a conduit l'autorité d'inspection des services de police britanniques à suggérer une collaboration plus systématique avec des institutions universitaires et des prestataires privés (HMIC 2015 : 35).

La Nouvelle-Zélande s'est également tournée vers la formation en ligne, la moitié de ses 14 000 patrouilleurs ayant suivi des modules sur la cybercriminalité pour l'année 2017-2018 (Pullar-Strecker 2018). En Suisse, l'Institut Suisse de Police (ISP) a reçu le mandat de former tous les policiers du pays à la lutte contre la cybercriminalité, et a aussi fait le choix de la formation en ligne afin de rattraper rapidement le retard accumulé et de mettre à niveau près de 20 000 policiers. La plateforme d'apprentissage E-CC (E-Learning Cybercrime) est accessible aux policiers, mais aussi à des collaborateurs civils, et offre à la fois des segments théoriques et des mises en situation concrètes destinées à assurer le transfert des concepts techniques aux pratiques d'enquête (Brugnoni 2018). Au Canada, six cours en ligne sont disponibles via le Réseau canadien du savoir policier (Les enquêtes de la cybercriminalité Niveau 1, *Basic online investigations*, *Digital evidence : Front line investigations*, *Social media investigations*, *Cyberbullying awareness*, *Police guide to online child exploitation*)[17], mais les inscriptions restent à la discrétion des policiers ou de leur employeur et aucune approche nationale ne semble prédominer.

Nous avons fait état dans cette section des défis que les organisations policières doivent surmonter en matière de formation, et nous verrons dans la suivante que l'une des solutions possibles est de faire appel de manière complémentaire à des compétences externes. Toutefois, il est également important de signaler que la mise à niveau des

[16] https://www.ecteg.eu/running/first-responders/
[17] https://www.cpkn.ca/fr/course_catalogue

compétences doit être envisagé à l'échelle de l'ensemble du système pénal, et qu'une meilleure formation des procureurs et des juges est aussi indispensable afin d'assurer un meilleur traitement des affaires de cybercriminalité (Robert 2014 : 113).

2.4. Pertinence de faire appel à l'expertise complémentaire d'employés civils ou de bénévoles

Il est difficile d'évaluer le nombre d'experts spécialisés dans le recueil et l'analyse de la preuve numérique, que nous avons désignés plus haut sous le terme de « forensicien numérique ». Les rapports annuels des organismes policiers ou de Statistique Canada ne fournissent pas ce type de données de manière harmonisée. Cependant, des données secondaires fragmentaires laissent penser qu'une proportion importante de forensiciens numériques travaillent pour le compte d'organismes publics non-policiers ou d'entreprises privées offrant leurs services sur une base commerciale. Un sondage administré en 2015 à des forensiciens du monde entier faisait ainsi apparaître que les répondants déclarant une affiliation professionnelle policière ne représentaient que 23% de l'échantillon, 37% appartenant au secteur privé et 28% au secteur de l'enseignement et de la recherche (Harichandran et al. 2016 : 5). Même si ce sondage ne peut en aucune façon être jugé comme représentatif, il démontre néanmoins qu'il existe donc en dehors des organisations policières un important réservoir d'expertise en analyse judiciaire numérique.

Le recrutement direct d'employés civils apparaît comme une alternative possible au manque de personnel qualifié dont souffrent les organisations policières, sur le même modèle que celui adopté dans certaines juridictions pour le recrutement d'employés de soutien remplissant des fonctions administratives, de patrouille ou d'enquête (Cope 2004, Kiedrowski et al. 2017). Dans l'une des rares études ayant abordé le sujet de manière empirique, les policiers consultés ont cependant exprimé leur ambivalence vis-à-vis de cette approche (Goodison et al. 2015). Le recrutement d'employés civils permet sans nul doute de bâtir une expertise stable qui n'est pas constamment menacée par les promotions régulières des policiers assermentés et dont les coûts salariaux sont également inférieurs. Par ailleurs, les besoins de formation initiale peuvent dans ce modèle être assumés par les établissements d'enseignement supérieur qui trouveront aussi des débouchés pour leurs étudiants dans les entreprises et les organismes parapublics. Ainsi au Canada, des universités comme Ryerson, BCIT, ou l'Université du Nouveau Brunswick forment des étudiants à l'analyse judiciaire. Toutefois, si l'expertise purement technique des experts civils est souvent supérieure à celle des experts policiers, les premiers ne disposent que d'une expérience limitée sur les types de preuve pouvant être utiles dans le cadre d'une enquête policière et doivent être formés dans ce domaine. De plus, les opportunités réduites de promotion des employés civils peuvent également décourager ces derniers et les inciter à quitter l'organisation policière après quelques années, ce qui vient quelque peu oblitérer les gains réalisés par leur recrutement (Goodison et al. 2015 : 16).

Une solution intermédiaire proposée par un groupe de réflexion anglais consiste à utiliser les dispositifs existant de manière plus fréquente afin d'accélérer les transferts de connaissances entre le secteur privé et les organisations policières. Il pourrait s'agir par exemple de détacher des policiers spécialisés auprès d'organisations du secteur privé pendant quelques mois, afin d'accélérer l'acquisition de compétences de pointe souvent plus répandues dans les entreprises. Cela contribuerait également à développer des relations partenariales avec les entreprises du secteur numérique (Hitchcock et al. 2017 : 32).

Une troisième approche, faisant appel à l'assistance de bénévoles, pourrait contribuer à combler partiellement le déficit de capacité des organisations policières, particulièrement en matière de prévention et de sensibilisation du public. Les sites internet restent le mécanisme privilégié utilisé par ces organisations pour communiquer aux usagers les risques liés à la cybercriminalité et les meilleurs moyens pour s'en prémunir, bien que leur efficacité pour modifier les comportements de la population à grande échelle reste encore à démontrer. Les travaux les plus récents sur l'économie comportementale et la prévention de la cybercriminalité suggèrent en effet que les réseaux sociaux des victimes potentielles jouent un rôle important dans l'apprentissage des usages sécuritaires de l'internet et qu'ils contribuent à faire émerger des normes sociales d'hygiène numérique auxquelles ils se conformeront plus naturellement (Coventry et al. 2014 : 11). Autrement dit, les individus trouvent les conseils qu'on leur donne plus crédibles et sont plus enclins à les mettre en pratique lorsqu'ils proviennent de leurs pairs ou de personnes avec qui ils peuvent établir un lien social de confiance, et que ces conseils sont présentés de manière simple et nécessitent peu d'efforts de mise en oeuvre (Levi et al 2015 : 59). Dans ce contexte, le recours à des bénévoles issus des groupes vulnérables que l'on souhaite rejoindre ou capables d'interagir en confiance avec ces derniers pourrait s'avérer une solution permettant de dispenser des séances de sensibilisation auprès de certains groupes démographiques particulièrement touchés par la cybercriminalité, comme les jeunes usagers ou les personnes âgées. Le recours à des civils bénévoles n'est pas une approche nouvelle pour les organisations policières, en particulier dans le cadre du modèle de police communautaire (King 2007 : 1341, Gravelle et Rogers 2010, van Steden et Mehlbaum 2018).

Certains pays ont déjà instauré des programmes de bénévoles ou de réservistes afin de renforcer l'expertise policière en matière de cybercriminalité. Au Royaume-Uni, une quarantaine des 13 500 bénévoles actifs parmi les forces de police britanniques étaient affectés à la lutte contre les cybercrimes en 2007 (Hitchcock et al. 2017 : 6), la Ministre de l'intérieur Theresa May ayant annoncé au début de l'année 2016 un renforcement de cette capacité et des pouvoirs accrus pour les bénévoles, ce qui suscita une forte résistance de la part des syndicats policiers (BBC 2016). D'autres pays comme l'Estonie et la France ont choisi de créer des forces de plusieurs milliers de réservistes associés aux unités militaires spécialisées dans la cyberdéfense, mais certains de ces civils issus des écoles de génie informatique ou des entreprises spécialisées remplissent aussi des missions d'enquête et de sensibilisation du public (Blair 2015, Levi et al. 2015, Eschapasse 2016). Dans le cas de

la France, certains de ces réservistes sont placés sous l'autorité de la Gendarmerie Nationale, une force de police dépendant du Ministère des Armées.

2.5. Recueillir, accéder à et analyser la preuve numérique dans un environnement où la cryptographie est omniprésente et où les volumes de données augmentent exponentiellement

Tous les défis d'adaptation de la police ne sont pas d'ordre interne. Des facteurs exogènes découlant de la rapide évolution de certaines technologies viennent en permanence reconfigurer les paramètres du travail policier. La popularité croissante des produits et des services grand public mettant à la disposition des usagers des solutions de cryptographie extrêmement performantes qui deviennent de véritables arguments commerciaux complique considérablement le travail des unités spécialisées d'enquête lors de saisies judiciaires ou lorsqu'elles exécutent des interceptions de communications. On peut citer à titre d'exemple le protocole Tor qui permet de naviguer sur internet de manière relativement anonyme, les services de réseaux privés virtuels (VPN) qui proposent des fonctions équivalentes moyennant abonnement, des applications pour téléphone intelligent comme Signal, Telegram ou Viber qui offrent un niveau élevé de sécurité pour les conversations par messages texte, ou encore les équipements de l'entreprise Apple qui intègrent des fonctions avancées de cryptographie dans leur architecture physique et logique. De surcroît, les organisations qui conçoivent les moteurs de recherche, les navigateurs internet et opèrent l'infrastructure technique sous-jacente de l'internet (comme Google ou Mozilla) ont répondu aux révélations faites par Edward Snowden sur l'ampleur de la surveillance de masse des agences de renseignement occidentales en encourageant l'adoption par l'ensemble des sites internet du protocole de chiffrement https (Berkman Centre 2016). Depuis 2014, Google classe ainsi en tête de ses résultats de recherche les sites qui ont adopté cette technologie par défaut, et signale depuis février 2018 sur son navigateur Chrome (qui détient plus de 67% de part de marché) les sites qui n'ont pas effectué cette transition comme présentant un risque de sécurité pour les usagers (Gallagher 2018). Le protocole https, qui était auparavant essentiellement utilisé pour sécuriser les transactions financières en ligne, protège dorénavant la majorité des sites internet. D'après les statistiques de Google, plus de 80% du trafic internet était encrypté en novembre 2018[18]. Que les technologies de cryptage soient utilisées pour sécuriser les données en transit (communications en ligne) ou au repos (stockage sur des équipements électroniques), la robustesse des algorithmes employés par l'industrie rend les efforts d'interception et de déchiffrement légaux extrêmement difficiles, notamment en raison des ressources de calcul énormes que ces derniers nécessitent.

Dans ce contexte, les organisations policières éprouvent une inquiétude croissante face au phénomène d'inaccessibilité technique aux données pour lesquelles elles ont néanmoins obtenu des autorisations légales d'accès, craignant de plonger dans l'obscurité (« going dark ») (Finklea 2016, Homeland Security Committee 2016). L'exemple symptomatique

[18] https://transparencyreport.google.com/https/overview?hl=fr

d'une situation de déni d'accès technique malgré une autorisation légale créée par une technologie de cryptage est celui du téléphone intelligent ayant appartenu à l'auteur de la tuerie de San Bernardino[19], Syed Rizwan Farook, que le FBI échoua à déverrouiller par ses propres moyens. Le fabriquant (Apple) ayant fermement et publiquement refusé son assistance sur la base de considérations liées à la sécurité de l'ensemble de ses clients, le FBI dut alors faire appel à des spécialistes en sécurité informatique (des hackers éthiques) qui facturèrent leurs services environ 900 000$ US pour ce seul équipement (Nakashima 2016). Ce type de dépense n'est envisageable que dans les cas les plus sérieux ou médiatisés en lien avec la sécurité nationale ou le crime organisé, et demeure inaccessible à la majorité des services de police municipaux. Au Canada, on constate une utilisation plus fréquente des technologies par les groupes criminels organisés, le Québec se classant en tête des provinces où le plus grand nombre de groupes criminalisés utilisent des technologies de chiffrement.

Deux considérations principales informent ce débat. La première relève des nouveaux arbitrages technologiques et légaux requis afin d'assurer la sécurité en ligne des usagers. La raison principale de l'adoption généralisée de technologies de cryptographie plus robustes s'explique par le besoin de sécuriser les transactions en ligne des usagers, ces derniers étant ciblés de manière routinière par les cybercriminels. La cybersécurité collective accrue que procure la démocratisation de la cryptographie vient cependant parfois nuire à la capacité de la police de conduire certaines enquêtes. Il ne s'agit donc pas ici du dilemme classique qui consiste à opposer la sécurité des uns à la liberté des autres, mais plutôt d'un arbitrage inextricable entre la sécurité de l'ensemble des usagers d'internet, d'une part, et la sécurité individuelle de victimes impliquées dans des affaires de prédation sexuelle, de cyber-harcèlement ou de terrorisme, d'autre part. Alors que les experts scientifiques et les principaux représentants de l'industrie privilégient la nécessité de maintenir une infrastructure technique aussi robuste que possible (Abelson et al. 2015), les représentants des services de police et de renseignement des principaux pays occidentaux examinent la possibilité de forcer les entreprises du secteur numérique à introduire des portes dérobées dans leurs logiciels afin de pouvoir exceptionnellement accéder aux contenus chiffrés (Noisette 2018). Ainsi, dans un précédent assez peu médiatisé, le site *Motherboard* révéla en avril 2016 que la GRC avait obtenu en 2010 de l'entreprise Blackberry la clé universelle de cryptage des messages expédiés à l'aide des appareils vendus par la société, ce qui lui permit de déchiffrer plus d'un million de communications échangées par les membres d'un groupe mafieux (Pearson et Ling 2016). Face à de telles éventualités, les chercheurs estiment cependant que les risques d'exploitation de portes dérobées par des acteurs malveillants sont inévitables et devraient dissuader les gouvernements d'en considérer l'adoption. Par ailleurs, un certain nombre de rapports soulignent l'existence de stratégies d'enquête alternatives qui

[19] Le 2 décembre 2015, Syed Rizwan Farook et son épouse Tashfeen Malik ouvrirent le feu à l'aide d'armes automatiques sur les employés d'un organisme de santé publique réuni pour des célébrations de Noël. Le bilan de la fusillade s'éleva à 16 morts (dont les deux assaillants) et 23 blessés.

demeurent accessibles à la police dans ce type d'affaires. Cela les incite à penser que les technologies de cryptographie représentent plus une source de frustration qu'un changement radical de paradigme (UNODC 2013, Lewis et al. 2017, Kerr et Schneier 2018).

Même lorsque les données peuvent être déchiffrées, la quantité massive de fichiers à analyser constitue un obstacle majeur pour la conduite efficace des enquêtes. Dans une affaire qui représente probablement l'une des investigations les plus complexes menées par une organisation policière canadienne, la Police provinciale de l'Ontario (OPP) démantela un réseau de distribution de pornographie juvénile en ligne qui comprenait plus de 60 000 membres enregistrés provenant d'une centaine de pays. La particularité de cette enquête réside dans le fait que l'OPP identifia une entreprise d'hébergement légitime située au Canada comme le point de distribution de ce réseau, ce qui lui permit de saisir plus de 1,2 pétabits de données illégales, soit quatre fois la quantité de l'information stockée par la Bibliothèque du Congrès américaine (Ling et Braga 2015). Afin d'analyser plus d'un milliard de téléchargements portant sur 1,4 millions d'images, les enquêteurs durent faire l'acquisition auprès de l'entreprise HP d'un centre de données modulaire livré dans un container, au coût de plusieurs centaines de milliers de dollars (Murphy 2015). Si cette solution innovante a permis de répondre à un besoin exceptionnel, elle ne peut constituer le nouveau modèle d'intervention policière devant les coûts prohibitifs qui l'accompagnent et l'incapacité des institutions du système pénal de juger un tel nombre de suspects.

3. Les limites des stratégies mono-institutionnelles et le potentiel de l'intervention en partenariat

Nous nous sommes focalisés dans les pages précédentes sur les modalités répressives traditionnelles de l'intervention policière, et nous avons vu les nombreux défis à relever pour les adapter aux propriétés d'une cybercriminalité qui ne cesse d'innover. Le mythe de Sisyphe, condamné par le dieu grec Zeus à pousser éternellement un lourd rocher vers le haut d'une montagne dont le poids l'écrasait avant d'atteindre le sommet, l'obligeant ainsi à reprendre sans fin ses efforts, offre une analogie cruelle mais assez explicite des difficultés que la police éprouve à résoudre le problème de la cybercriminalité avec les outils classiques de la répression (Dupont 2014 : 186). Deux autres stratégies d'intervention en partenariat avec les acteurs du secteur privé ont été considérées ces dernières années : la perturbation des réseaux criminels à l'aide d'instruments juridiques issus du droit civil et la réduction des méfaits à l'aide de stratégies régulatoires. Nous examinerons dans cette section le rôle que la police peut jouer dans ces approches que l'on qualifie parfois de polycentriques, ainsi que leur efficacité et leurs limites.

3.1. Trois stratégies d'intervention contre la cybercriminalité : répression, perturbation et réduction des méfaits

La neutralisation des auteurs de cybercrimes et des réseaux criminels qu'ils composent par leur arrestation constitue le mode traditionnel d'intervention de la police. Elle se heurte toutefois à un certain nombre d'obstacles dont certains ont déjà été exposés plus haut. L'un des plus importants est la tension qui existe en matière de recueil de la preuve numérique : en effet, les victimes qui sont en majorité des acteurs privés accordent souvent une plus grande importance au fait de retrouver un accès immédiat aux systèmes informatiques et aux données qui ont été la cible d'un cybercrime ou en ont facilité la réalisation qu'à l'enquête criminelle qui doit permettre d'identifier les auteurs. Cela implique donc que ces systèmes ou ces données sont souvent restaurés ou réinitialisés par ceux qui les administrent afin que les usagers puissent redevenir opérationnels rapidement, ce qui s'avère incompatible avec l'exigence de préservation de la preuve numérique, qui exige au contraire que les équipements informatiques affectés soient conservés dans un état rigoureusement identique à celui en vigueur lors de l'attaque ou du piratage (Endicott-Popovsky et al. 2005). Par ailleurs, la complexité des systèmes informatiques concernés et les volumes de données à analyser, qui augmentent exponentiellement depuis quelques années avec la démocratisation de l'internet mobile, de l'infonuagique et de l'internet des objets, signifient également que les analyses forensiques sur lesquelles reposent les enquêtes policières atteignent des coûts dissuasifs pour les organisations policières et les entreprises victimes au regard du faible nombre d'arrestations et de condamnations, même si un certain nombre de tâches sont automatisables (Harichandran et al. 2016).

Mais même dans les cas d'arrestations médiatisées, les réseaux cybercriminels font preuve d'une résilience surprenante face aux interventions policières. Cela découle en partie du fait que les arrestations ne sont pas toujours accompagnées d'un démantèlement complet des infrastructures techniques contrôlées par les cyberdélinquants (souvent hébergées dans une multiplicité de pays) et que ces dernières peuvent rapidement être réactivées par des complices ou des concurrents. Ainsi, l'arrestation en octobre 2010 par la police arménienne d'un citoyen russe ayant réussi à infecter et à prendre le contrôle de plus de 30 millions d'ordinateurs conduisit à la condamnation de ce pirate informatique à quatre ans de prison après deux années de procédure judiciaire (Cluley 2012). Pourtant, deux jours seulement après l'arrestation, un autre hacker prenait le contrôle des machines infectées et reprenait ses activités de distribution de contenus malveillants. Cette résilience criminelle face à la répression policière est rendue possible par la distribution géographique mondialisée de l'infrastructure technique, mais aussi par la disponibilité des outils de cryptographie et de camouflage qui renforcent l'anonymat des délinquants (Décary-Hétu et Giommoni 2017). Certains estiment d'ailleurs, qu'à de rares exceptions près, les cybercriminels qui se retrouvent devant les tribunaux disposent probablement de compétences techniques limitées ou intermédiaires (Maurushat 2012, Dupont 2013). De plus, les peines prononcées par les tribunaux restent relativement clémentes (sauf aux États-Unis où elles se caractérisent au contraire par leur sévérité excessive), ce qui

s'explique par la jeunesse des accusés, le fait qu'il s'agit souvent de leur première infraction, qu'ils n'ont pas recours à la violence, et que leur potentiel de réinsertion sociale et professionnelle est élevé (Smith et al. 2004).

Devant l'impuissance du système pénal à protéger les victimes de cybercrimes, qui à l'exception des cas de pornographie juvénile et de cyberintimidation se caractérisent par un fort volume mais un faible impact individuel, une seconde approche permettant de déstabiliser les infrastructures criminelles en ligne a été initiée par le secteur privé. Cette stratégie de perturbation repose sur l'utilisation des outils du contentieux civil et le partenariat entre acteurs publics et privés. L'une des entreprises ayant investi le plus de ressources dans cette approche est Microsoft, qui créa en 2008 une unité spécialisée dans la lutte contre les cybercrimes (la *Digital Crimes Unit*) et se lança dans une stratégie de démantèlement des réseaux d'ordinateurs infectés (les *botnets*) en s'appuyant sur les pouvoirs d'injonction des tribunaux civils (Dupont 2017). De 2010 à 2014, Microsoft obtint des ordonnances judiciaires qui lui permirent de prendre le contrôle et de démanteler l'infrastructure technique de neuf botnets ayant fait plus de 44 millions de victimes. Quatre de ces opérations furent menées en étroite collaboration avec des services de police américains et européens. Les stratégies de perturbation ne sont pas réservées à des initiatives unilatérales pilotées par des multinationales ayant accès à des ressources techniques et juridiques considérables. Des groupes de travail *ad hoc* comprenant des entreprises mais aussi des ONG, des institutions chargées de la gouvernance d'internet et des chercheurs universitaires se forment également ponctuellement afin de bloquer des menaces criminelles pouvant menacer la stabilité du web. En 2008, le *Conficker Working Group* empêcha ainsi la mise en service d'un botnet ayant infecté plus de cinq millions de machines en bloquant l'accès de son concepteur aux serveurs permettant de l'exploiter (The Rendon Group 2010). Ce groupe de travail comprenait plus de trente organisations qui collaborèrent de manière innovante avec l'ICANN (l'organisme mondial coordonnant l'enregistrement des noms de domaine) afin de perturber durablement l'un des plus importants réseaux de cybercriminels de la fin des années 2000.

En parallèle aux actions de perturbation qui ciblent les délinquants, des actions de réduction des méfaits se focalisent sur les victimes. Ce type d'approche a initialement été utilisé par six pays (Australie, Corée du Sud, Japon, Allemagne, Hollande et Finlande) pour combattre les botnets (Dupont 2014, E. Silva 2017). Les fournisseurs d'accès à internet et les entreprises d'anti-virus collaborent avec une autorité régulatrice (généralement spécialisée dans le domaine des télécommunications) ou un centre national de réponse aux incidents informatique (les CERTs) afin d'alerter les usagers de manière proactive lorsque leurs machines sont infectées et les aider à se débarrasser des logiciels malveillants. Des mesures plus contraignantes comme une restriction temporaire de l'accès à internet sont parfois mises en œuvre avec les usagers récalcitrants. En fédérant des partenaires privés habituellement en compétition et qui sont en contact régulier avec la majorité des usagers d'internet, cette approche permet d'intervenir à l'échelle de toute une population et de produire des effets significatifs de réduction de la proportion des ordinateurs infectés par un logiciel malveillant.

Cette stratégie de réduction des méfaits a été depuis étendue à d'autres formes de cybercrimes comme les rançongiciels ou les fraudes nigérianes. Les rançongiciels sont des logiciels malveillants qui une fois installés à l'insu de leurs victimes sur leur machine chiffre l'ensemble des données qui y sont stockées, et n'en restaure l'accès que sur paiement d'une rançon de quelques centaines de dollars (Paquet-Clouston et al. 2018). En juillet 2016, la police néerlandaise, l'organisation internationale Europol et l'entreprise McAfee créèrent le site *nomoreransom.org*, qui met à la disposition des victimes les clés de déchiffrement gratuite pour plus de 80 rançongiciels, ce qui permet de leur éviter le paiement d'une rançon[20]. Depuis sa création, 39 autres services de police et plus de 70 entreprises et ONG ont rejoint cette initiative. Il s'agit là de l'application à grande échelle du principe de prévention situationnelle de déni des bénéfices que peuvent espérer les délinquants. Un dernier exemple de réduction des méfaits concerne les initiatives menées en Australie par certains services de police en collaboration avec les institutions financières pour combattre la fraude par avance de fonds (la fraude nigériane) et la fraude amoureuse (Cross 2016). Les virements suspects vers des pays réputés héberger de fortes concentrations de fraudeurs en ligne font ainsi l'objet d'une analyse criminelle plus approfondie afin d'identifier les victimes potentielles et les mettre en garde sur les risques encourus par l'envoi d'une lettre. Parmi les trois initiatives étudiées, les taux moyens de réduction du nombre de personnes envoyant de l'argent à l'étranger à des fraudeurs oscillèrent entre 62 et 77%, ce qui représente une diminution spectaculaire de la victimisation à répétition qui caractérise ce genre de fraude (Cross 2016 : 133-134).

3.2. Efficacité et limites des modèles d'intervention en partenariat

Les statistiques mentionnées plus haut illustrent l'énorme potentiel des stratégies de perturbation et de réduction des méfaits pour produire des résultats à grande échelle contre la cybercriminalité. Dans le cas des botnets démantelés par Microsoft et ses partenaires, les résultats obtenus permirent des réductions temporaires du nombre des machines infectées par des logiciels malveillants de 50% et des taux de déconnection des botnets de 32% à 38%, ce qui se traduisit en des réductions considérables du nombre de victimes de fraude financière (Dupont 2017). De la même façon, les efforts nationaux de désinfection coordonnée des machines enrôlées dans des botnets produisirent également des résultats extrêmement encourageant, faisant passer le taux d'infection du parc informatique coréen de 25% à 0,5% entre 2005 et 2011, alors qu'au Japon, il chutait de 2,5% à 0,6% pendant la même période (Dupont 2014). La simple mise en œuvre de partenariats ne suffit toutefois pas à générer les résultats attendus. Les résultats les plus robustes sont atteints dans les pays où les autorités régulatrices n'hésitent pas à s'impliquer de manière plus affirmée et où les fournisseurs d'accès à internet sentent une pression plus marquée sur la qualité de leur réponse (Asghari et al. 2015).

[20] https://www.nomoreransom.org/en/index.html

Le manque d'études évaluatives sur les approches partenariales de lutte contre la cybercriminalité montre à quel point le défi de la quantification du phénomène, mis en lumière dans la première section, s'étend aussi aux interventions visant à en réduire la prévalence et l'impact. Il est en effet complexe de mesurer l'efficacité de mesures préventives et répressives lorsque l'on ne dispose pas de statistiques de qualité permettant de mesurer l'ampleur du problème que l'on cherche à résoudre, ou son évolution dans le temps. Par ailleurs, les stratégies d'intervention en partenariat nécessitent aussi d'attribuer à chaque participant institutionnel une part de responsabilité dans les résultats obtenus, ce qui s'avère extrêmement difficile d'un point de vue méthodologique.

Adopter cette stratégie d'intervention pose également pour la police la question de la défense du bien commun face aux intérêts privés. Les entreprises du secteur numérique qui s'impliquent dans ces approches disposent en effet de capacités techniques et financières souvent démesurées par rapport à leurs partenaires policiers. Microsoft, Symantec et des associations professionnelles comme le *Forum of Incident Response and Security Teams* ou l'*Anti Phishing Working Group* jouent ainsi un rôle bien plus central dans le réseau mondial de coopération policière contre la cybercriminalité que la majorité des organismes gouvernementaux nationaux et des organisations internationales (Dupont 2016b). Certaines de ces interventions partenariales sont initiées par le secteur privé, qui détermine les priorités d'intervention et constitue des dossiers d'enquête détaillés transmis aux organisations policières qui prennent ensuite le relais afin d'initier des poursuites pénales. On peut légitimement se poser la question du contrôle effectif de ces assemblages institutionnels et de la 'capture' potentielle des services de police par leurs partenaires privés. Il est donc indispensable que toute réflexion sur l'implication du secteur privé dans la lutte contre la cybercriminalité conforte la position de la police comme acteur central représentant l'intérêt collectif des usagers de l'internet. À cet égard, le modèle de 'policing par les tierces parties' (*Third Party Policing*) est un modèle d'intervention compatible avec les principes d'intérêt public énoncés plus haut. Ce modèle, utilisé depuis quelques années pour lutter contre le trafic de drogue ou les nuisances de voisinage repose sur la mobilisation et la coordination d'acteurs institutionnels disposant des capacités de réguler directement ou indirectement certains types de crimes (Mazerolle et Ransley 2005). La police utilise alors ses pouvoirs de persuasion et de coercition afin de convaincre les partenaires concernés de passer à l'action sous son impulsion.

Dans les rares études ayant examiné de manière empirique le fonctionnement de partenariats anti-cybercriminalité, la confiance joue également un rôle central qui détermine en grande partie leur réussite ou au contraire leur échec (Nhan et Huey 2008, Levi et Williams 2012, Veenstra et al. 2013). C'est en effet cette confiance réciproque qui facilite la détermination consensuelle des objectifs communs, la répartition claire des rôles et des responsabilités, la rapidité dans les échanges de renseignements, ainsi que la qualité des informations mises en commun et des décisions prises lors des interventions.

Conclusion

Face à l'augmentation exponentielle d'une cybercriminalité transnationale qui innove constamment afin d'automatiser ses activités, les organisations policières subissent une pression de plus en plus forte afin d'adapter leur modèle d'intervention. Conçu pendant la seconde moitié du 19ème siècle en réaction aux désordres urbains provoqués par la révolution industrielle, le modèle de police professionnelle qui s'est développé afin de répondre à un nombre limité de crimes à fort impact ne semble plus adapté à une délinquance caractérisée par une prolifération de crimes à faible impact individuel. La dimension locale du travail policier est remise en question par une délinquance déployant ses réseaux à l'échelle mondiale et impliquant des assemblages complexes d'individus et de machines autonomes. Ces nouvelles configurations criminelles rendent urgentes une réflexion approfondie sur la place de la police dans la prévention et la répression de la cybercriminalité, aussi bien en termes de structures organisationnelles à adopter, de compétences à développer, que de réseaux partenariaux à faire éclore et à animer. Les quelques sondages ayant posé au public la question de la responsabilité dans la lutte contre la cybercriminalité indiquent bien la préférence générale pour le maintien par la police d'un rôle central. En l'absence d'une adaptation rapide et d'une profonde transformation de leurs pratiques, le risque pour les organisations policières est de voir leur légitimité érodée et d'encourager l'apparition de 'justiciers numériques' (*digital vigilantes*) essayant de se substituer à des mécanismes de régulation étatique jugés défaillants (Huey et al. 2013, e Silva 2018), mais ne contribuant finalement qu'à renforcer l'instabilité et l'insécurité du web.

Références

Abelson, H, Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M., et Weitzner, D. 2015), Keys under doormats : Mandating insecurity by requiring governments access to all data and communications, *Journal of Cybersecurity*, 1 (1) : 69-79.

ACEI (2017), *Dossier documentaire 2017 de l'ACEI*, Autorité canadienne pour les enregistrements internet, Ottawa.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore T., et Savage, S. (2013), Measuring the cost of cybercrime, *The economics of information security and privacy*, Springer, Berlin, 265-300.

Asghari, H., van Eeeten, M., et Bauer, J. (2015), Economics of fighting botnets : Lessons from a decade of mitigation, *IEEE Security & Privacy*, 13 (5) : 16-23.

Bangs, M. (2018), *Overview of fraud and computer misuse statistics for England and Wales*, Office of National Statistics, Londres.

Bariki, H., Hashmi, M., et Baggili, I. (2010), Defining a standard for reporting digital evidence items in computer forensics tools, in I. Baggili (dir.), *International Conference on Digital Forensics and Cyber Crime*, Springer, Berlin, pp. 78-95.

Baril, D.-E. (2014), *La transformation des enquêtes policières due à l'influence des technologies : perspective d'une unité policière spécialisée en analyse judiciaire informatique*, Rapport de stage en vue de l'obtention du grade de M.SC. en criminologie, Université de Montréal, Montréal.

BBC (2016), Civilians to help police investigate cybercrimes, says Theresa May, *BBC News*, 20 janvier, accessible en ligne à https://www.bbc.com/news/uk-35354139.

Berkman Centre (2016), *Don't panic : Making progress on the « going dark » debate*, The Berkman Centre for Internet & Society, Cambridge.

Bernier, M. (2017), *L'utilisation d'Internet chez les Québécois*, Institut de la statistique du Québec, Québec.

Blair, D. (2015), Estonia recruits volunteer army of 'cyber warriors', *The Telegraph*, 26 avril, accessible en ligne à https://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html.

Bossler, A., et Holt, T. (2012), Patrol officers' perceived role in responding to cybercrime, *Policing : An International Journal of Police Strategies & Management*, 35 (1) : 165-181.

Bossler, A., et Holt, T. (2013), Assessing officer perceptions and support for online community policing, *Security Journal*, 26 (4) : 349-366.

Brugnoni, M. (2018), Le e-learning cybercrime : Une formation harmonisée, *POLCANT info*, (109) : 12-13.

Caneppele, S., et Aebi, M. (2017), Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes, *Policing: A Journal of Policy and Practice*, DOI : 10.1093/police/pax055.

CEFRIO (2017), *Portrait numérique des foyers québécois*, CEFRIO, Québec.

Cluley, G. (2012), Bredolab: Jail for man who masterminded botnet of 30 million computers, *Naked Security Sophos Blog*, 23 mai, accessible en ligne à http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/.

Cope, N. (2004), 'Intelligence led policing or policing led intelligence ?' : Integrating volume crime analysis into policing, *British Journal of Criminology*, 44 (2) : 188-203.

Côté, A.M., Bérubé, M. et Dupont, B. (2016), Statistiques et menaces numériques : comment les organisations quantifient la cybercriminalité, *Réseaux*, 197-198 : 205-224.

Cross, C. (2016), Using financial intelligence to targetonline fraud victimisation : applying a tertiary prevention perspective, *Criminal Justice Studies : A Critical Journal of Crime, Law and Society*, 29 (2) : 125-142.

CyberCrime@IPA (2011), *Specialised cybercrime units – Good practice study*, Union Européenne et Conseil de l'Europe, Strasbourg.

Décary-Hétu, D., et Giommoni, L. (2017), Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous, *Crime, Law and Social Change*, 67 (1) : 55-75.

Décary-Hétu, D., et Bérubé, M. (dirs.) (2018), *Délinquance et innovation*, Les Presses de l'Université de Montréal, Montréal.

Dupont, B. (2007), Police communautaire et de résolution des problèmes, in M. Cusson, B. Dupont et F. Lemieux (dirs.), *Traité de sécurité intérieure*, HMH Hurtubise, Montréal, pp. 98-114.

Dupont, B. (2013), Skills and trust: A tour inside the hard drives of computer hackers, in C. Morselli (dir.), *Illicit networks*, Routledge, Oxford, pp. 195-217.

Dupont, B. (2014), La régulation du cybercrime comme alternative à la judiciarisation : le cas des botnets, *Criminologie*, 47 (2) : 179-201.

Dupont, B. (2016a), Des effets perturbateurs de la technologie sur la criminologie, *Revue Internationale de Criminologie et de Police Technique et Scientifique*, 69 (3) : 305-322.

Dupont, B. (2016b), La gouvernance polycentrique du cybercrime: Les réseaux fragmentés de la coopération internationale, *Cultures et Conflits*, (102) : 95-120.

Dupont, B. (2017), Bots, cops and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime, *Crime, Law and Social Change*, 67 (1) : 97-116.

Dupont, B. (2018), Les statistiques tronquées de la cybercriminalité, *6ème Rapport international sur la prévention de la criminalité et la sécurité quotidienne*, CIPC, Montréal.

Emond, A., et Ellyson, L. (2014), Cybercriminalité: développements jurisprudentiels et perquisitions informatiques, *La Référence*, accessible en ligne à https://www.lccjti.ca/files/sites/105/2014/11/Emond-Ellyson-cybercriminalit%C3%A9-EYB2014REP1575.pdf.

Endicott-Popovsky, B., Ryan, D., et Frincke, D. (2005), The New Zealand hacker case : A post mortem, *Oxford Internet Institute Cybersafety Conference*, Oxford University, Oxford.

Eschapasse, B. (2016), Des cyber-réservistes pour protéger les intérêts français sur le net, *Le Point*, 2 mai, accessible en ligne à https://www.lepoint.fr/high-tech-internet/des-cyber-reservistes-pour-proteger-les-interets-francais-sur-le-net-02-05-2016-2036304_47.php.

e Silva, Karine K. (2017), How industry can help us fight against botnets : notes on regulating private-sector intervention, *International Review of Law, Computers & Technology*, 31 (1) : 105-130.

e Silva, Karine K (2018), Vigilantism and cooperative criminal justice: Is there a place for cybersecurity vigilantes in cybercrime fighting?, *International Review of Law, Computers & Technology*, 32 (1): 21-36.

Finklea, K. (2016), *Encryption and the "going dark" debate*, Congressional Research Service, Washington D.C.

Florêncio D., et Herley C. (2013), Sex, lies and cyber-crime surveys, *Economics of Information Security and Privacy III*, Springer, New York, pp. 35-53.

Furnell S., Emm D., et Papadaki M. (2015), The challenge of measuring cyber-dependent crimes, *Computer Fraud & Security*, 2015(10): 5-12.

Gallagher, S. (2018), Despite Chrome's pending "mark of shame," 3 major news sites aren't HTTPS, *Ars Technica*, 6 juillet, accessible en ligne à https://arstechnica.com/information-technology/2018/07/despite-chromes-pending-mark-of-shame-3-major-news-sites-arent-https/.

Goodison, S., Davis, R., et Jackson, B. (2015), *Digital evidence and the U.S. criminal justice system : Identifying technology and other needs to more effectively acquire and utilize digital evidence*, RAND Corporation, Santa Monica.

Goodman, M. (1997), Why the police don't care about computer crime, *Harvard Journal of Law & Technology*, 10 (3) : 465-494.

Gravelle J., et Rogers C. (2010), The economy of policing – The impact of the volunteer, *Policing*, 4 (1) : 56-63.

GRC (2012), *Vérification du Programme de la criminalité technologique*, Gendarmerie royale du Canada, Ottawa.

Grobler, M. (2010), Digital forensic standards : International progress, *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, 17-18 mai, Port Elizabeth.

Harichandran, V., Breitinger, F., Baggili, I., et Marrington, A. (2016), A cyber forensics needs analysis survey : Revisiting the domain's needs a decade later, *Computers & Security*, 57, 1-13.

Harkin, D., Whelan, C., et Chang, L. (2018), The challenges facing specialist police cybercrime units: An empirical analysis, *Police Practice and Research*, 19 (6): 519-536.

Hinduja, S. (2004), Perceptions of local and state law enforcement concerning the role of computer crime investigative teams, *Policing : An International Journal of Police Strategies & Management*, 27 (3) : 341-357.

Hitchcock, A., Holmes, R., et Sundorph, E. (2017), *Bobbies on the net : a police workforce for the digital age*, Reform, Londres.

HMIC (2015), *Real lives, real crimes : A study of digital crime and policing*, Her Majesty's Inspectorate of Constabulary, Londres.

Homeland Security Committee (2016), *Going dark, going forward : A primer on the encryption debate*, House Homeland Security Committee Majority Staff, Washington D.C.

Holt, T., Bossler, A., et Fitzgerald, S. (2013), Examining state and local law enforcement perceptions of computer crime, in T. Holt (dir.), *Crime on-line : Correlates, causes and context – second edition*, Carolina Academic Press, Durham, pp. 219-244.

Holt, T., Burruss, G., et Bossler, A. (2018), An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents, *Policing and Society : An International Journal of Research and Policy*, DOI : 10.1080/10439463.2018.1450409.

Huey, L. (2002), Policing the abstract : Some observations on policing cyberspace, *Canadian Journal of Criminology*, 44 (3) : 243-254.

Huey, L., Nhan, J., et Broll, R. (2013), 'Uppity civilians' and 'cyber-vigilantes' : The role of the general public in policing cyber-crime, *Criminology & Criminal Justice*, 13 (1) : 81-97.

Jewkes, Y. (2013), Public policing and Internet crime, in Y. Jewkes et M. Yar (dirs.), *Handbook of Internet crime*, Routledge, Londres, pp. 525-545.

Kerr, O., et Schneier, B. (2018), Encryption workarounds, *Georgetown Law Journal*, 106 (4) : 989-1019.

Kiedrowski, J., Ruddell, R., et Petrunik, M. (2017), Police civilianisation in Canada : A mixed methods investigation, *Policing and Society : An International Journal of Research and Policy*, DOI : 10.1080/10439463.2017.1281925

King, W. (2007), Volunteers in policing, in J. Greene (dir.), *The encyclopedia of police science – Third edition*, Routledge, New York, pp. 1340-1342.

Klap, H., et de Groot, D. (2013), Strategy for future action in relation tothe use of digital technologies and crime, in W. Stol et J. Jansen (dirs.), *Cybercrime and the police*, Eleven International Publishing, La Haye, pp. 89-96.

Leukfeldt, R., Veenstra, S., et Stol, W. (2013), High volume cyber crime and the organization of the police : The results of two empirical studies in the Netherlands, *International Journal of Cyber Criminology*, 7 (1) : 1-17.

Levi, M. (2017), Assessing the trends, scale and nature of economic cybercrimes: overview and Issues, *Crime, Law and Social Change*, 67 (1) : 3-20.

Levi, M., Doig, A., Gundur, R., Wall, D., et Williams, M. (2015), *The implications of economic cybercrime for policing*, City of London Police, Londres.

Levi, M., et Williams, M. (2012), *eCrime reduction partnership mapping study*, Cardiff Centre for Crime, Law and Justice, Cardiff.

Lewis, J., Zheng, D., et Carter, W. (2017), *The effect of encryption on lawful access to communications and data*, Center for Strategic & International Studies, Washington D.C.

Ling, J., et Braga, M. (2015), Police could charge a data center in the largest child porn bust ever, *Motherboard*, 2 mars, accessible en ligne à https://motherboard.vice.com/en_us/article/3dk498/police-could-charge-a-data-center-in-the-largest-child-porn-bust-ever.

Maurushat, A. (2012), The role of internet service providers in combatting botnets: An examination of recent Australian initiatives and legislative reform, *Telecommunications Journal of Australia*, 62 (4): 61.1-61.18.

Mazerolle, L., et Ransley, J. (2005), *Third party policing*, Cambridge University Press, Cambridge.

McGuire, M., et Dowling, S. (2013), *Cyber crime : A review of the evidence*, Home Office, Londres.

Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I., et Smith, M. (2016), *Evaluation of the Australian Cybercrime Online Reporting Network*, Australian Institute of Criminology, Canberra.

Murphy, B. (2015), Policing challenges in the digital age, *3ème Atelier du Réseau intégré sur la cybersécurité*, 22-23 avril, Ottawa.

Nakashima, E. (2016), FBI paid professional hackers one-time fee to crack San Bernardino iPhone, *The Washinton Post*, 12 avril, disponible en ligne à https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

National Research Council (2009), *Strengthening forensic science in the United States : A path forward*, The National Academies Press, Washington D.C.

Nhan, J., et Huey, L. (2008), Policing through nodes, clusters and bandwith, in S. Leman-Langlois (dir.), *Technocrime : Technology, crime and social control*, Willan Publishing, Cullompton, 66-86.

NIJ (2008), *Electronic crime scene investigation : A guide for first responders, second edition*, Office of Justice Programs, Washington DC.

Noisette, T. (2018), « Le droit à la vie privée n'est pas absolu » : 5 Etats veulent un accès aux messages chiffrés, *L'obs*, 4 septembre, accessible en ligne à https://www.nouvelobs.com/les-internets/20180904.OBS1775/le-droit-a-la-vie-privee-n-est-pas-absolu-5-etats-veulent-un-acces-aux-messages-chiffres.html.

Paquet-Clouston, M., Haslhofer, B., et Dupont, B. (2018), Ransomware payments in the bitcoin ecosystem, *17th Annual Workshop on the Economics of Information Security (WEIS)*, arXiv:1804.04080.

Pearson, J., et Ling, J. (2016), Exclusive : How Canadian police intercept and read encrypted Blackberry messages, *Motherboard*, 14 avril, accessible en ligne à https://motherboard.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada.

Perreault, S. (2011), Les incidents autodéclarés de victimisation sur Internet au Canada, 2009, *Juristat*, Statistique Canada, Ottawa.

Perreault, S. (2015), La victimisation criminelle au Canada, 2014, *Juristat*, Statistique Canada, Ottawa.

Plesco, R., et Schneck, P. (2011), Criminal public-private partnerships : Why can't we do that?, *Georgetown Journal of International Affairs*, 11 (3) : 151-154.

Podlas, K. (2017), The « *CSI* effect », in H. Pontell (dir.), *Oxford Research Encyclopedia of Criminology*, DOI: 10.1093/acrefore/9780190264079.013.40.

Ponemon Institute (2017), *2017 Cost of a data breach study*, Ponemon Institute, Traverse City.

Powell, A., et Henry, N. (2018), Policing technology-facilitated sexual violence against adult victims : police and service sector perspectives, *Policing and Society : An International Journal of Research and Policy*, 28 (3) : 291-307.

Pullar-Strecker, T. (2018), Police to get more training on online harassment options in wake of criticism, *Stuff*, 29 août, accessible en ligne à https://www.stuff.co.nz/business/industries/106619973/lani-wendt-case-may-have-exposed-gap-in-polices-cyber-training.

Reep-van den Bergh, C., et Junger, M. (2018), Victims of cybercrime in Europe : a review of victim surveys, *Crime Science*, 7 (5) : 1-15.

Robert, M. (2014), *Protéger les internautes : Rapport sur la cybercriminalité*, Ministère de la Justice, Paris.

Scalar (2018), *The cyber security readiness of canadian organizations*, Scalar, Toronto.

Schreuders, Z. C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A. R., et Shan-A-Khuda, M. (2018), *Needs assessment of cybercrime and digital evidence in a UK police force*, Leeds Beckett University, Leeds.

Sinclair,G., Zilber, J., et Hargrave, E. (2008), *Regulating content on the internet : A new technological perspective*, Industrie Canada, Ottawa.

Smith, R., Grabosky, P., et Urbas, G. (2004), *Cyber criminals on trial*, Cambridge University Press, Cambridge.

Srinivasan, S. (2013), Digital forensics curriculum in security education, *Journal of Information Technology Education : Innovations in Practice*, 12, 147-157.

Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W., Williams, W. (2001), *Electronic crime needs assessment for state and local law enforcement*, Office of Justice Programs, Washington DC.

Statistique Canada (2018), *L'incidence du cybercrime sur les entreprises canadiennes, 2017*, Statistique Canada, Ottawa.

Tcherni, M., Davies, A., Lopes, G., et Lizotte, A. (2016), The dark figure of online property crime: is cyberspace hiding a crime wave?, *Justice Quarterly*, 33 (5) : 890-911.

The Rendon Group (2010), *Conficker Working Group : Lessons learned*, The Rendon Group, Washington D.C.

Tison, M. (2011), Fraude et escroqueries, *La Presse Affaires*, 19 mars, p. 3.

TNS opinion & social (2017), *Europeans' attitudes towards cyber security*, Commission Européenne, Bruxelles.

UNODC (2009), *Scène de crime et indices matériels : Sensibilisation du personnel non spécialisé*, Office des Nations Unies contre la Drogue et le Crime, Vienne.

UNODC (2013), *Comprehensive study on cybercrime*, UNODC, Vienne.

Van Steden, R., et Mehlbaum, S. (2018), Police volunteers in the Netherlands : A study on policy and practice, *Policing and Society : An International Journal of Research and Policy*, DOI : 10.1080/10439463.2018.1523165.

Veenstra, S., Leukfeldt, R., et Boes, S. (2013), Fighting crime in a digitized society : The criminal justice system and public-private partnerships in the Netherlands, in W. Ph. Stol et J. Jansen (dirs.), *Cybercrime and the police*, Eleven International Publishing, La Haye, pp. 75-87.

Wall, D. (2007), Policing cybercrimes : Situating the public police in networks of security within cyberspace, *Police Practice and Research : An International Journal*, 8 (2) : 183-205.

Harkin, D., et Whelan, C. (sous presse), Exploring the implications of 'low visibility' specialist cyber-crime units, *Policing and Society : An International Journal of Research and Policy*.

Chapitre 3. Les nouvelles contraintes procédurales et la productivité policière

Rémi Boivin

Aucun métier ne suscite autant d'intérêt que celui de policier. Des films et des séries télé lui sont consacrés, les affaires policières occupent une bonne part des nouvelles médiatiques ; ainsi, une bonne partie de la population a des attentes parfois irréalistes envers la police (Surette 2011). Cet intérêt reflète un autre fait : le travail policier est aussi un des plus encadrés. Au Québec, presque tous les aspects du travail policier réfèrent au Code criminel canadien, à la Loi sur la police, au Code de déontologie policière ou à plusieurs règlements entourant les procédures et la discipline. La conséquence la plus évidente est que le métier de policier est contrôlé par de multiples organismes, comme le Commissaire à la déontologie policière et le Bureau des enquêtes indépendantes, qui compilent tous des données sur certains aspects du travail policier. Cet intérêt envers le métier policier est toutefois dirigé vers la partie la plus visible du travail, même si, dans les faits, la police accomplit une grande diversité de tâches. Par exemple, Jobard et de Maillard (2015) résument le travail policier en quatre grandes fonctions : la police de tranquillité publique (qui inclut la patrouille et la réponse aux appels d'urgence), la police d'investigation, la police d'information (le renseignement) et la police des foules. Plusieurs efforts ont été initiés afin de simplifier cette complexité.

Les enjeux traités dans ce chapitre se basent sur la distinction entre les deux grands types d'activités menées par des policiers : les interventions réactives, où les policiers répondent à une demande de service (ex : appel d'urgence) et les interventions proactives, où les policiers prennent la décision d'intervenir en se basant de moins en moins sur le fameux « flair policier » mais de plus en plus sur une analyse systématique de données. Les efforts récents pour améliorer la productivité policière sont louables, mais sont associées à des risques dont il faut avoir connaissance. Dans ce chapitre, nous présenterons les tentatives de quantification du travail policier qui ont été faites au Canada et ailleurs avant d'examiner quatre risques associés à cet exercice.

1. La quantification du travail policier

Plusieurs critiques de la police partent d'un constat-choc : entre 1991 et 2016, la criminalité au Canada a baissé de plus de 40%, pendant que les dépenses en matière policière ont augmenté de plus de 70%, en dollars constants[21]. Il s'agit là d'une sursimplification de la situation qui néglige la complexité grandissante du travail policier. Il s'agit aussi de constats allant à l'encontre de l'impression assez large du manque d'effectifs policiers sur le terrain. Des chercheurs des universités Simon-Fraser et de la vallée Fraser

[21] Sources de Statistique Canada : 1) Juristat « Statistiques sur les crimes déclarés par la police au Canada, 2017 »; 2) Juristat, « Les ressources policières au Canada, 2017 », Tableau 6 : « Dépenses au chapitre des services de police, en dollars courants et en dollars constants (2002), Canada, 1986-1987 à 2016-2017 ».

se sont intéressés à cette contradiction apparente. Ils ont offert une analyse très poussée du travail des policiers de la Gendarmerie Royale du Canada en Colombie-Britannique, basée sur plusieurs sources de données complémentaires incluant une analyse documentaire de dossiers, des entrevues de groupe avec d'anciens policiers et une analyse des données d'appels reçus sur une période de 30 années (Malm et al. 2005). Ils ont démontré que depuis les années 1970 la police a connu plusieurs changements technologiques nécessitant à chaque fois une période d'ajustements et d'apprentissage, ainsi qu'une augmentation de la charge administrative. Selon leurs estimations, les policiers des années 1970 passaient environ 1h30 par quart de travail à ces tâches, tandis que le policier moyen des années 2000 passait environ 40% de son temps (environ quatre heures par quart) à rédiger des rapports et à compléter des formulaires. Les auteurs soulignent aussi que l'environnement légal dans lequel évoluent les policiers s'est grandement complexifié, entre autres en raison de la décision R. v. Stinchcombe [1991] 3 S.C.R 326 qui a exigé que les policiers transmettent à la défense des copies de tous les documents pertinents. À noter que leur analyse n'inclut pas l'arrêt Jordan, qui est susceptible d'avoir des effets importants sur le travail policier, même si la décision est trop récente (8 juillet 2016) pour avoir fait l'objet d'analyses d'impact approfondies. Malm et ses collègues reconnaissent qu'une partie de l'augmentation des effectifs policiers s'explique simplement par l'augmentation de la population de Colombie-Britannique, mais suggèrent que les changements légaux et technologiques ont eu un impact considérable sur la charge de travail des policiers, un impact qui aurait été supérieur à l'augmentation des budgets alloués à la GRC pour la même période. Toutefois, l'analyse porte essentiellement sur une seule des fonctions policières, la police de tranquillité publique.

De façon générale, les tentatives de quantifier le travail d'investigation se sont révélées encore moins satisfaisantes et moins nombreuses que celles portant sur la police de tranquillité publique. L'étude de Malm et ses collègues aborde bien la complexité grandissante du travail d'enquête en soulignant que le nombre d'étapes procédurales pour mener à bien des dossiers d'homicide, d'introduction par effraction, de violences conjugales, de conduite avec facultés affaiblies et de trafic avait considérablement augmenté au cours des dernières décennies, mais il s'agit d'une exception plutôt que de la règle. L'indicateur le plus courant est le taux de résolution, malgré le fait que sa définition même fait l'objet de débats et varie d'une étude à l'autre. Ainsi, un crime est parfois considéré résolu si un suspect a été arrêté (Mas 2006) ou seulement si un suspect plausible a été identifié sans nécessairement avoir été arrêté (Paré et al. 2007). Au Canada, la Déclaration uniforme de la criminalité distingue le taux de résolution (ou « taux de classement ») avec et sans mise en accusation, ce qui offre des portraits très différents. Puisqu'il s'agit d'un ratio (ex : nombre de crimes résolus / nombre de crimes enregistrés), il y a là une double opportunité pour augmenter la pression de rendement. Le but visé étant généralement d'augmenter le taux de résolution, des stratagèmes peuvent être développés pour augmenter le nombre de crimes résolus mais aussi pour diminuer le nombre de crimes enregistrés. Le NYPD a récemment offert un exemple qui sera développé dans la prochaine section.

L'autre débat émerge de la constatation que plusieurs crimes sont solutionnés sans le moindre travail d'enquête. Par exemple, Brodeur & Ouellet (2005) ont trouvé que les auteurs de 71% des homicides commis à Montréal étaient identifiés en moins de 24 heures et que 49% des auteurs étaient localisés dans le même délai. Enfin, différents travaux suggèrent que le taux de résolution varie en fonction de plusieurs facteurs n'ayant pas grand-chose à voir avec le travail policier ; Mancik & Parker (2018) ont ainsi trouvé que des facteurs démographiques avaient influencé le taux de résolution des homicides aux États-Unis entre 1976 et 2015, et que cet effet demeurait significatif même lorsqu'étaient pris en compte les changements dans la nature des crimes commis ainsi que la charge de travail des policiers. Autrement dit, le taux de résolution est-il vraiment un indicateur de l'efficacité de la police d'investigation ?

La police d'information (le renseignement) et la police des foules ont toutes les deux assez largement échappé à la volonté de quantifier les activités dans le but d'évaluer la productivité. Les deux aspects ont pourtant fait l'objet d'une très vaste littérature qui vise à améliorer l'intervention dans ces contextes. Par exemple, plusieurs travaux portent sur la psychologie des foules et sur les meilleures méthodes de gestion (Reicher et al. 2004), mais les travaux visent rarement la généralisation observée dans les exemples précédents. L'étude de Stott et al. (2008) illustre bien notre propos : il s'agit d'un article basé sur le cas d'un championnat de soccer européen lors duquel, selon les auteurs, l'approche non-paramilitaire privilégiée par la police explique l'absence relative d'incidents violents. Les auteurs concluent avec une discussion des implications pratiques de leurs résultats en matière de contrôle des foules, mais le but de leur analyse n'est pas d'évaluer l'ensemble des stratégies policières ni de dresser les meilleures pratiques, simplement de souligner que la stratégie adoptée dans ce cas a été bénéfique. Publiée dix ans plus tard, l'étude de Davies & Dawson (2018) se base sur les émeutes liées à la coupe Stanley et analyse l'échec perçu de la stratégie adoptée ; surtout, elle illustre l'état des connaissances en matière de contrôle de foules. Dans les deux cas, les auteurs ne font pas le pas supplémentaire qui a été fait dans les cas de la police de tranquillité publique et de la police d'investigation, c'est-à-dire de travailler au développement d'indicateurs généraux de productivité.

À noter toutefois que le modèle d'*Evidence-based policing*, actuellement favorisé par plusieurs organismes, prône l'utilisation d'analyses statistiques et défend l'idée que l'intervention devrait être guidée par l'analyse –ce qui implique une certaine généralisation des résultats. Il n'est donc pas impensable que la police des foules soit éventuellement intégrée aux évaluations de productivité, d'autant plus qu'elle est un aspect très visible du travail policier. Ce n'est pas le cas de la police d'information. Il s'agit d'un aspect méconnu du travail policier, et difficile à évaluer puisqu'il dépend plus de la subjectivité des policiers, par exemple dans la décision de compiler ou non des informations. L'*Intelligence-led policing* (la police basée sur le renseignement) est souvent définie comme le modèle en 3 i : interprétation, influence et impact (Ratcliffe 2016). Nous n'avons pas recensé d'étude impliquant cet aspect du travail policier comme indicateur de la productivité.

2. Les risques associés à la quantification du travail policier

2.1. Augmenter la pression de rendement

En 1994, la police de New York, le NYPD, a adopté un outil et une philosophie de gestion visant à améliorer la reddition de comptes, le CompStat (pour *Compare Statistics*). Le modèle est, d'une certaine façon, précurseur de l'*Evidence-based policing* puisqu'il impliquait un grand recours aux statistiques, qui étaient perçues comme plus objectives que d'autres indicateurs. CompStat incluait entre autres des rencontres hebdomadaires lors desquelles les statistiques de la semaine précédente étaient utilisées pour mesurer la productivité de la police des 77 secteurs (*precincts*) de la ville et pour définir les cibles prioritaires de la semaine à venir. L'idée était d'améliorer la transmission de l'information et la responsabilité des dirigeants locaux. CompStat est, encore aujourd'hui, présenté comme une des raisons principales ayant accéléré la baisse de la criminalité des années 1990, même si cette affirmation a souvent été nuancée. L'économiste Steven Levitt a par exemple démontré que la contribution de CompStat était minime en comparaison à d'autres facteurs, comme l'explosion du taux d'incarcération (Levitt 2004).

L'expérience new-yorkaise de CompStat a aussi démontré qu'il était possible que l'adoption d'une technologie visant à augmenter l'efficacité du travail policier s'accompagne d'une forte pression de rendement. Les travaux de John Eterno (Eterno & Silverman 2012, Eterno et al. 2016) suggèrent que le NYPD, par le biais de ses officiers, a mis en place un système managérial forçant parfois les policiers à manipuler les statistiques et à intimider les citoyens. Ainsi, des 1962 policiers retraités sondés, 58% croient que la baisse de la criminalité observée à New York depuis les années 1990 est en partie due à la manipulation des statistiques. En particulier, plusieurs policiers rapportent avoir eu personnellement connaissance de situations où un rapport d'événement aurait dû être complété mais ne l'a pas été ou qu'un code d'événement a été changé pour que les statistiques paraissent plus favorables. Les policiers sondés attribuent ces manipulations à la pression managériale.

Il s'agit évidemment d'un cas extrême pouvant être attribué au développement rapide des technologies de compilation et d'analyse des données dans des années 1990. CompStat n'a pourtant pas eu que des effets négatifs : en plus de la promotion des importants principes d'imputabilité et de transparence, la stratégie a inspiré les premiers modèles de données ouvertes sur la criminalité qui ont permis de démocratiser la connaissance sur la criminalité. Par exemple, la ville de Montréal offre depuis 2016 certaines données sur les actes criminels enregistrés sur l'île, mais surtout, le portail des données ouvertes inclut un outil de visualisation des données, ce qui permet à la population de mieux comprendre le phénomène criminel à l'aide de cartes. Il s'agit là d'un héritage évident de la stratégie CompStat, qui faisait un grand usage des outils de visualisation.

2.2. L'effet de la surveillance du travail policier sur la sécurité

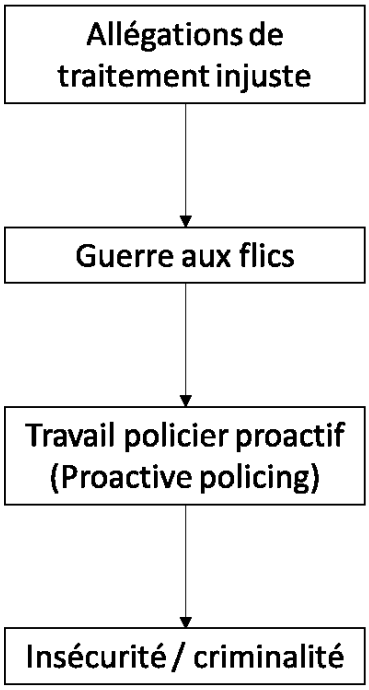
La pression de rendement peut venir plus généralement de l'opinion publique, une notion difficile à cerner qui désigne les croyances plus ou moins partagées d'un ensemble de personnes. Différents travaux ont décrit le sentiment du « nous contre eux » comme étant une composante de la culture policière (Brough et al. 2016, Reiner 2010). Les policiers auraient tendance à croire que l'ensemble des non-policiers partagent les mêmes opinions et caractéristiques, ce qui les mènerait à agir conformément. Cette tendance a été renforcée au cours des dernières années avec la montée des réseaux sociaux, principalement en raison de deux processus. Le premier processus vient du fait que les médias sociaux et les chaînes de nouvelles en continu permettent la large diffusion d'images d'interventions policières. Qu'elles soient légitimes ou non, ces images génèrent souvent de vives réactions, surtout lorsqu'elles impliquent l'emploi de la force par la police. Pour paraphraser un ancien chef de police québécois, l'emploi de la force, ce n'est jamais esthétique, même quand c'est bien exécuté. La conséquence est que la police est de plus en plus souvent appelée à commenter ou défendre ses interventions. Le deuxième processus est relié au premier : les opinions sont maintenant partagées à grande vitesse et à un public très large, ce que plusieurs désignent comme la « viralité ». En plus, les vidéos suscitant de fortes réactions affectives ou de nature à produire de la colère, comme celles qui impliquent l'emploi de force, sont plus susceptibles d'être partagées et commentées (Guadagno et al. 2013).

Ces changements sociaux récents peuvent être interprétés comme des contraintes potentielles au travail policier. Ainsi, une théorie a gagné en popularité au cours des dernières années, particulièrement aux États-Unis, celle de la « guerre aux flics » (*war on cops*) (Mac Donald 2016). Plusieurs désignent le processus qu'elle implique comme « l'effet Ferguson », du nom de la ville où ont eu lieu plusieurs manifestations suite au décès d'un jeune noir lors d'une intervention policière. La séquence d'effets serait la suivante (voir Figure 1) : la surveillance accrue (*increased scrutiny*) du travail policier mènerait à des allégations de traitement injuste, ce qui se traduirait par une crise de légitimité de la police et une remise en question générale du bien-fondé du travail policier. Un des effets de cette crise de légitimité serait de pousser certains individus à remettre en question l'intervention policière dont ils font l'objet, quitte à confronter ouvertement les policiers, par exemple en résistant à une arrestation. En réponse à cette résistance, les policiers anticiperaient des problèmes lors de certaines interventions et préfèreraient éviter ces situations ; la conséquence serait donc une diminution du travail policier proactif, ce qui engendrerait éventuellement une augmentation de la criminalité[22]. Si plusieurs observateurs simplifient la théorie en affirmant que la remise en question du

[22] Desmond, Papachristos et Kirk (2016) ont démontré empiriquement un autre effet. Le décès très médiatisé d'un jeune noir lors d'une intervention policière a été accompagné d'allégations de traitement injuste envers la communauté noire, ce qui a eu un impact significatif sur le taux de signalement dans certains quartiers de Milwaukee. Selon ce processus, l'impact de la surveillance accrue sur le travail policier est indirect, puisque les policiers auraient à répondre à moins de demandes d'aide et donc, la surveillance accrue serait associée à une diminution du travail réactif des policiers.

travail policier augmente la criminalité, la théorie de la guerre aux flics mérite qu'on s'attarde à chacun de ses éléments afin de voir s'il est plausible que ses effets soient également observés à l'extérieur des États-Unis.

Figure 1. L'effet Ferguson



Les média sociaux et traditionnels omniprésents contribuent à la diffusion des allégations d'inconduite ; sans nécessairement avoir initié les allégations, il est indéniable que l'exposition aux actualités a fondamentalement changé au cours des dernières années. Autrement dit, il est aujourd'hui presque impossible de ne pas avoir entendu parler des mouvements *Black lives matter* ou *#metoo* et donc, d'allégations d'inconduite. Ce qui est moins certain, c'est l'existence même de la guerre aux flics. Les policiers américains sondés par Nix et al. (2018) croyaient que cette remise en question existait depuis quelques années, c'est-à-dire que le travail policier serait plus souvent qu'avant soumis à un examen minutieux, par exemple via l'analyse détaillée des enregistrements vidéo d'interventions policières, dans le but de détecter la moindre faute policière (Mac Donald 2016). Il s'agit donc d'une croyance répandue, mais dont la véracité est difficile à vérifier : les citoyens auraient tendance, plus qu'avant, à résister à l'intervention policière. En d'autres termes, nous assisterions présentement à une remise en question de la légitimité de la police par certains, puisque la légalité d'action (*lawfulness*) est essentielle à l'efficacité de la police (Tankebe 2013). La légitimité de la police est un concept qui a fait l'objet d'une très vaste littérature depuis le début des années 2000 (voir Hamm et al. (2017) pour une revue), mais l'évolution temporelle a été clairement négligée, ce qui fait que l'hypothèse de la guerre aux flics n'a pas d'appui empirique ; autrement dit, les rares études existantes sur le sujet indiquent que le phénomène n'existe pas (Maguire et al. 2017) ou que la hausse des

agressions envers les policiers américains est observable depuis 2003 (Tiesman et al. 2018).

Néanmoins, la simple idée d'une guerre aux flics semble avoir un impact sur le travail des policiers. Dans leur étude sur des services de police du Missouri, Shjarback et ses collègues (2017) ont trouvé que moins d'arrestations proactives pour des infractions de circulation avaient eu lieu suite aux événements de Ferguson, particulièrement dans les territoires dont la population était constituée d'une plus grande proportion de Noirs américains. Aussi, les caméras corporelles pourraient être un outil susceptible d'accélérer le mouvement de *depolicing*, selon certains auteurs. Un article récent publié dans la prestigieuse revue *Criminology* avance l'hypothèse qu'en plus des effets souhaités par les organisations policières, comme la baisse de l'emploi de la force ou des plaintes envers les policiers, les caméras corporelles pourraient augmenter la surveillance du travail policier, surtout si les enregistrements sont présentés publiquement (Wallace et al. 2018). Bien que la situation soit différente au Canada et aux États-Unis –au Canada, les enregistrements ne peuvent pas, pour l'instant, être diffusés avant la fin des procédures judiciaires-, il s'agit d'un inconvénient potentiel majeur pour les organisations policières, surtout que le SPVM, ainsi que d'autres corps policiers canadiens, vient de mener un projet-pilote dans le but d'évaluer la possibilité d'équiper tous ses policiers de caméras corporelles. Wallace et al. (2018) ont observé le niveau d'activité et le temps de travail des policiers de Spokane équipés de caméras corporelles. Loin de confirmer l'hypothèse du *depolicing*, ils ont même trouvé que les policiers équipés de caméras étaient devenus plus proactifs que les autres. Ce « *depolicing* », c'est-à-dire le fait de délaisser des stratégies d'intervention proactive, s'ajoute à l'« *underpolicing* », c'est-à-dire au contrôle inadéquat de certaines populations ou territoires. L'*underpolicing* est une crainte souvent formulée, parfois comme une source importante d'insécurité pour les populations marginalisées, qu'elles soient autochtones, noires, sans-abri ou autres. Ces populations auraient besoin d'autant sinon plus de protection de la part de la police, mais ne l'obtiendraient pas, pour différentes raisons. La notion d'*underpolicing* est présente depuis longtemps, mais elle a eu un regain de popularité au cours des dernières décennies comme étant l'inverse du profilage (Engel et al. 2002) : le problème serait non pas que le niveau de contrôle de certaines populations serait trop élevé, mais au contraire pas assez élevé par rapport à leurs besoins. Tout comme la guerre aux flics, la notion d'*underpolicing* reste toutefois une hypothèse assez mal documentée par des études solides.

Le lien entre travail proactif et criminalité est beaucoup mieux documenté. Il s'agit même d'un argument fondateur d'une théorie adaptée sous forme d'importante stratégie policière au cours des années 1980, la théorie de la vitre brisée (*Broken windows theory*). L'idée était que le fait d'intervenir activement et rapidement face à des infractions relativement mineures comme le vandalisme avait un impact sur d'autres formes de criminalité plus graves (Wilson et Kelling 1982). Cette théorie a été adaptée sous la forme de politiques de tolérance zéro et a mené à une réforme importante de la police de New York. La stratégie est encore aujourd'hui citée comme la principale raison expliquant la baisse de la criminalité observée dans les années 1990 et a valu à William Bratton, le chef

du NYPD à l'époque, le statut de héros national. Bien qu'elle soit remise en question par plusieurs (dont Bernard Harcourt, qui a publié un livre particulièrement dévastateur sur le sujet : Harcourt 2005), la théorie de la vitre brisée a éventuellement inspiré des stratégies d'interventions ciblées, comme le *hotspot policing*. L'efficacité de ces stratégies d'interventions ciblées et proactives est bien établie : une méta-analyse (Braga et al. 2014) a par exemple trouvé que le *hotspot policing* diminuait significativement le nombre de crimes à un endroit et que ses effets bénéfiques se diffusaient souvent aux territoires environnants.

Bref, le dernier maillon de l'effet Ferguson, le lien entre travail policier proactif et criminalité est le seul qui soit établi empiriquement ; les autres éléments de cet effet, soit l'existence d'une guerre aux flics et l'impact de cette résistance accrue sur le travail proactif, sont pour l'instant anecdotiques. Reste que la perception d'une crise de la légitimité de la police peut en soi avoir des impacts importants.

2.3 Profilage social, racial, ou criminel ?

La quantification du travail policier a permis de mettre à jour des situations problématiques de profilage social ou racial, ce qui est évidemment une bonne chose. Le profilage, c'est-à-dire l'emploi de généralisations fondées sur des caractéristiques des individus, des situations ou des contextes, est courant puisqu'il permet d'accélérer le traitement de l'information et donc, l'intervention policière. En utilisant des techniques de profilage, les policiers peuvent mieux se préparer à faire face à certaines situations, ce qui peut, ultimement, mener à des prises de décisions plus rapides permettant, par exemple, d'assurer la sécurité des personnes impliquées (Brodeur 2003). Le problème, c'est quand le profilage est essentiellement basé sur des caractéristiques individuelles comme l'ethnie, la religion, les convictions politiques et le statut social, et qu'il mène à des conséquences tangibles pour la personne faisant l'objet, par exemple, de contrôles d'identité à répétition, de poursuites judiciaires ou d'emploi de la force injustifié. La Commission des droits de la personne et des droits de la jeunesse, parmi plusieurs autres organismes, dénonce alors des pratiques discriminatoires contraires aux principes de la Charte des droits et libertés de la personne, une loi fondamentale pour la société canadienne. La tension qui en résulte vient de la nécessité de tracer la ligne entre pratiques discriminatoires et pratiques souhaitables, et se traduit par la compilation de données diverses. Ainsi, le SPVM a publié en 2010 un rapport sur les contrôles d'identité, à partir de données internes analysées rigoureusement afin d'indiquer si certaines populations étaient surreprésentées, sans volonté de vérifier si ces différences étaient dues à des pratiques discriminatoires (Charest 2010). À l'opposé, des journalistes du Toronto Star ont affirmé en 2002 que les policiers de la ville avaient des pratiques discriminatoires, en se basant sur leur propre compilation de données policières. De tels exercices d'analyse et/ou de compilation de données découlent parfois d'une volonté de transparence de la part des organisations policières, parfois d'une initiative externe (comme celle du Toronto Star), mais il est aussi possible que des tribunaux exigent la compilation ou la diffusion de certaines données. Ce fut le cas au début des années 2000 à New York ; durant cette période, la pratique du « *stop-and-*

frisk » a été remise en question par des citoyens et des médias, mais surtout par des juges, qui ont demandé que les données sur les événements de « *stop-and-frisk* » soient analysées afin de vérifier les allégations de profilage racial. Dans tous les cas, le message envoyé était que le travail policier était maintenant scruté à la loupe.

La quantification force les organisations policières à rendre des comptes, ce qui risque de s'accentuer avec l'adoption croissante de stratégies liées au *Big Data* (Ferguson 2017). Le fait de lever au moins partiellement le voile sur des organisations traditionnellement discrètes est, de nouveau, une bonne chose. Par contre, le risque est que la surveillance du travail policier se traduise par l'utilisation exclusive de méthodes actuarielles dans la détermination des cibles d'intervention, afin de minimiser les risques associés aux décisions humaines. Par exemple, un policier décidant d'interpeller un citoyen noir pourra être blâmé si ce contrôle se révèle discriminatoire ; par contre, si un algorithme exige qu'une telle intervention ait lieu, qui est à blâmer ? Plusieurs notent que l'éloignement du modèle traditionnel de « profilage criminel » pourrait se faire au profit de profilages basés sur des données, mais resteraient ultimement discriminatoires envers certaines populations.

Un principe associé à l'analyse systématique de données est la dissuasion ciblée (*focused deterrence*). Ferguson (2017 : 35-36) décrit le processus : 1) un groupe de délinquants probables (mais pas nécessairement confirmés) est identifié ; 2) ce groupe fait l'objet d'une surveillance policière étroite ; 3) ces interventions, tout à fait légitimes, sont documentées et mènent potentiellement à des arrestations ; 4) les individus associés au groupe, qui est maintenant un groupe délinquant confirmé, font eux-mêmes l'objet d'une surveillance étroite, etc. Au-delà du côté auto-confirmatoire du processus, le risque est que certaines populations deviennent systématiquement des cibles, et que ces cibles soient considérées comme valides selon le système. Imaginons que les délinquants probables identifiés à l'étape 1 soient noirs (ou pauvres, ou étudiants, ou autres) ; la suite du processus vient confirmer que ces individus méritent une surveillance plus étroite, mais aussi le fait qu'en ciblant des individus noirs, la probabilité de succès d'une intervention proactive soit plus élevée. De plus, si les autres populations, par exemple, les hispaniques, en viennent à comprendre que leurs risques sont moins élevés, ils pourraient ainsi être encouragés à commettre des infractions (Harcourt 2007). L'utilisation de méthodes actuarielles, dont les algorithmes décisionnels, est fondée sur la volonté d'offrir un service plus juste envers tous, mais pourrait résulter en des conséquences contraires inattendues.

Conclusion

La plupart du temps, les grands changements et nouvelles contraintes procédurales associés au travail policier sont justifiés par une volonté d'offrir un traitement adéquat à la population et d'améliorer l'efficacité des interventions policières. Une police efficace est une police qui réagit rapidement et qui initie des interventions productives, en matière de prévention de la criminalité, de résolution des incidents, de satisfaction du public et de sentiment global de sécurité. La police fait l'objet d'une attention particulière, puisqu'elle

occupe une place particulière dans la société ; aucun autre corps de métier n'a autant de pouvoirs, ni autant de responsabilités. La question aujourd'hui est de savoir si le poids des responsabilités est en voie de devenir trop lourd pour les individus qui pratiquent ce métier.

Les trois risques associés au suivi de la productivité policière abordés dans ce chapitre partent de la prémisse que le travail policier peut influencer la sécurité des citoyens. En augmentant la pression de rendement au-delà d'un certain niveau, le NYPD a possiblement influencé la perception qu'on avait de la criminalité à New York ; la guerre aux flics a possiblement poussé les policiers américains à moins s'investir dans le travail proactif, même s'il a été démontré que ces stratégies avaient un effet significatif sur la criminalité ; enfin, la volonté d'éviter le traitement injuste de certains citoyens a mené à l'utilisation d'algorithmes qui eux-mêmes sont maintenant accusés d'encourager l'injustice. Ces trois situations partent de bonnes intentions qui ont mal tourné. Il ne faut toutefois pas tomber dans le piège de la recherche du risque zéro en matière de travail policier. Il est possible que des erreurs soient faites, et tout devrait être mis en place pour éviter ces erreurs (par exemple, en améliorant la formation offerte aux policiers), mais il faut se rappeler que le travail policier en est un de probabilités plutôt que de certitudes.

Références

Braga, A.A., Papachristos, A.V. & Hureau, D.M. (2014). The effects of hot spots policing on crime: An updated systematic review and meta-analysis. *Justice Quarterly*, 31(4), 633-663.

Brodeur, J.P. (2003). *Les visages de la police*. Montréal : Les Presses de l'Université de Montréal.

Brodeur, J.P. & Ouellet, G. (2005). L'enquête criminelle. *Criminologie*, 38(2), 39-64.

Brough, P., Chataway, S. and Biggs, A. (2016). 'You don't want people knowing you're a copper!' A contemporary assessment of police organisational culture. *International Journal of Police Science & Management*, 18(1), 28-36.

Charest, M. (2010). *Mécontentement populaire et pratiques d'interpellation du SPVM depuis 2005 : doit-on garder le cap après la tempête? Mise à jour des données (2001-2008)*. Document de travail disponible au www.spvm.qc.ca.

Davies, G. & Dawson, S.E. (2018). Spoonful of sugar or strong medicine: 'Meet and greet' as a strategy for policing large-scale public events. *Policing and Society: An International Journal of Research and Policy*, 28(6), 697-711.

Desmond, M., Papachristos, A.V. & Kirk, D.S. (2016). Police violence and citizen crime reporting in the black community, *American Sociological Review*, 81(5), 857-876.

Engel, R.S., Calnon, J.M. & Bernard, T.J. (2002). Theory and racial profiling: Shortcomings and future directions in research. *Justice Quarterly*, 19(2), 249-273.

Eterno, J.A. & Silverman, E.B. (2012). *The crime numbers game: Management by manipulation*. New York : CRC Press.

Eterno, J.A., Verma, A. & Silverman, E.B. (2016). Police manipulations of crime reporting: Insiders' revelations. *Justice Quarterly*, 33(5), 811-835.

Ferguson, A.G. (2017). *The rise of Big Data policing: Surveillance, race, and the future of law enforcement*. New York, New York University Press.

Guadagno, R. E., Rempala, D. M., Murphy, S., & Okdie, B. M. (2013). What makes a video go viral? An analysis of emotional contagion and Internet memes. *Computers in Human Behavior*, 29, 2312-2319.

Hamm, J.A., Trinkner, R. & Carr, J.D. (2017). Fair process, trust, and cooperation: Moving toward an integrated framework of police legitimacy. *Criminal Justice and Behavior*, 44(9), 1183-1212.

Harcourt, B.E. (2005). *Illusion of order: The false promise of broken windows policing*. Chicago: Harvard University Press.

Harcourt, B.E. (2007). *Against prediction: Profiling, policing, and punishing in an actuarial age*. Chicago : The University of Chicago Press.

Jobard, F. & de Maillard, J. (2015). *Sociologie de la police : Politiques, organisations et réformes*. Paris : Armand Colin.

Lamb, H.R., Weinberger, L.E. & DeCuir, W.J. (2014). The Police and mental health. *Psychiatric Services*, 53(10), 1266-1271.

Levitt, S.D. (2004). Understanding why crime fell in the 1990s: Four factors that explain the decline and six that do not. *Journal of Economic Perspectives*, 18(1), 163-190.

Mac Donald, H. (2016). *The War on cops: How the new attack on law and order makes everyone less safe*. New York : Encounter Books.

Maguire, E.R., Nix, J. & Campbell, B.A. (2017). A war on cops? The effects of Ferguson on the number of US police officers murdered in the line of duty. *Justice Quarterly*, 34(5), 739-758.

Malm, A., Pollard, N., Brantingham, P. Tinsley, P. Plecas, D., Brantingham, P., Cohen, I. & Kinney, B. (2005). *A 30 year analysis of police service delivery and costing*. Rapport présenté à la division E de la Gendarmerie Royale du Canada. Abbotsford, B.C. : International Centre for Urban Research Studies (ICURS).

Mancik, A.S. & Parket, K.F. (2018). Homicide clearances during pre- and post-UD crime drop eras: The role of structural predictors and demographic shifts, 1976-2015. *Journal of Crime and Justice*. Published online October 8 2018.

Mas, A. (2006). Pay, reference points, and police performance. *Journal of Economics*, 121(3), 783-821.

Nix, J., Wolfe, S.E. & Campbell, B.A. (2018). Command-level police officers' perceptions of the "War on cops" and de-policing. *Justice Quarterly*, 35(1), 33-54.

Paré, P.-P., Felson, R.B. & Ouimet, M. (2007). Community variation in crime clearance: A multilevel analysis with comments on assessing police performance. *Journal of Quantitative Criminology*, 23, 243-258.

Ratcliffe, J.H. (2016) Intelligence-Led Policing (2nd edition). Londres : Routledge.

Reicher, S., Stott, C., Cronin, P. & Adang, O. (2004). An integrated approach to crowd psychology and public order policing. *Policing: An International Journal*, 27(4), 558-572.

Reiner, R. (2010). *The politics of the police*. Oxford, UK: Oxford University Press.

Shjarback, J.A., Pyrooz, D.C., Wolfe, S.E. & Decker, S.H. (2017). De-policing and crime in the wake of Ferguson: Racialized changes in the quantity and quality of policing among Missouri police departments. *Journal of Criminal Justice*, 50(1), 42-52.

Steadman, H.J., Deane, M.W., Borum, R. & Morrissey, J.P. (2000). Comparing outcomes of major models of police responses to mental health emergencies. *Psychiatric Services*, 51(5), 645-649.

Stott, C., Adang, O., Livingstone, A., & Schreiber, M. (2008). Tackling football hooliganism: A quantitative study of public order, policing and crowd psychology. *Psychology, Public Policy, and Law*, 14(2), 115-141.

Surette, R. (2011). *Media, crime, and criminal justice: images, realities, and policies* 4th edition. Belmont, CA: Wadsworth Publishing Co.

Tankebe, J. (2013). Viewing things differently: The dimensions of public perceptions of police legitimacy. *Criminology*, 51(1), 103-135.

Tiesman, H.M., Gwilliam, M., Konda, S., Rojek, J. & Marsh, S. (2018). Nonfatal injuries to law enforcement officers: A rise in assaults. *American Journal of Preventive Medicine*, 54(4), 503-509.

Wallace, D., White, M.D., Gaub, J.E. & Todak, N. (2018). Body-worn cameras as a potential source of depolicing: Testing for camera-induced passivity. *Criminology*, Early view, DOI: 10.1111/1745-9125.12179.

Wilson, J.Q. & Kelling, G.L. (1982). Broken Windows. *Atlantic Monthly*, 249(3), 29-38.

Chapitre 4. Les plateformes de médias sociaux et l'intervention policière

Francis Fortin

Dans les sociétés développées comme le Québec et le Canada, le taux de pénétration des médias sociaux est de plus de 60 % dans la population, avec une moyenne d'usage quotidien de 1 h 47 (et plus du double pour les jeunes utilisateurs) (DynamicMarketing 2017). Les plateformes technologiques que sont devenues Facebook, Twitter, LinkedIn, ou encore Instagram représentent maintenant l'un des principaux outils de socialisation personnelle et professionnelle de la population. Cela implique un nouveau rapport à la vie privée et à la visibilité, dans la mesure où une grande quantité d'informations personnelles devient publiquement accessible. Pour les organisations policières, cela représente une façon de se rapprocher de la population et de rejoindre un grand nombre de personnes. Les enquêteurs peuvent aussi accéder à des données personnelles que les utilisateurs choisissent de partager, ce qui inclut les interventions policières qui sont filmées de manière routinière et immédiatement diffusées lorsqu'elles impliquent des décisions ou des comportements portant à controverse. Cela signifie qu'il est possible d'avoir accès à une multitude d'informations personnelles par l'entremise des médias sociaux, qu'elles soient partagées par des extrémistes ou des policiers. Ainsi, cette nouvelle réalité a entraîné de profonds changements dans l'intervention policière. Cette section vise à rendre compte de l'état de la situation quant à l'utilisation des plateformes de médias sociaux par les organisations policières. Plus spécifiquement, nous aborderons la question de l'adoption de ces outils dans la communauté policière. Nous développerons ensuite le sujet de l'utilisation des médias sociaux dans un contexte de renseignement. Nous décrirons ensuite deux nouvelles pratiques : les manifestations virtuelles et le *doxing*. Nous conclurons cette section en présentant des enjeux de formation et les implications générales sur ces transformations.

1. L'utilisation des médias sociaux

Comme Brodeur (2010) l'a souligné, la police est une agence multidimensionnelle impliquant plusieurs groupes d'acteurs engagés dans une vaste gamme d'activités. La recherche sur l'innovation dans le maintien de l'ordre s'est donc parfois concentrée sur la manière dont les agents de patrouille, les enquêteurs ou les unités en question adoptent de nouveaux outils, et sur la façon dont les médias sociaux ont modifié les pratiques de maintien de l'ordre et d'enquête. Un sondage mené par l'IACP (2013) auprès de 500 organisations de police américaines a révélé que la police utilise les médias sociaux (MS) à plusieurs fins, notamment pour communiquer avec les citoyens et mener ses enquêtes. L'enquête a révélé que 95 % des organisations impliquées ont confirmé qu'elles recouraient aux MS dans leurs activités. La plupart des organisations avaient intégré cette technologie à leurs opérations entre 2010 et 2012 alors que les principales plateformes de médias sociaux adoptées étaient Facebook, Twitter et YouTube (IACP 2013). Les médias sociaux étaient le plus souvent utilisés dans les enquêtes (86,1 % des agences), mais aussi

pour informer le public sur les questions pénales (74,3 % des agences), promouvoir l'engagement de la communauté (70,4 % des agences) et fournir des informations en cas de situation d'urgence (69 % des agences).

En Europe, le projet COMPOSITE, mis en place pour identifier les changements survenus dans les forces de police de 10 pays européens, a publié une étude consacrée exclusivement à la détermination des meilleures pratiques en matière d'activités liées aux MS (Denef et al. 2012). Les auteurs ont rassemblé leurs données lors de discussions avec divers membres des forces de police, ainsi qu'à partir d'informations sur l'utilisation de médias sociaux par des membres des forces de l'ordre britanniques lors des émeutes d'août 2011 à Londres. Les données ont montré que les MS pouvaient être utilisés à des fins telles que l'établissement de meilleures relations avec la collectivité, l'information que peut fournir cette dernière sur les nouvelles menaces et la demande d'assistance dans les enquêtes.

Au Canada, on observe aussi l'adoption des MS par des membres d'organisations policières. Les études canadiennes les plus remarquables sont celles de Frank et al. (2011), qui ont interrogé 11 personnes appartenant à des organismes chargés de l'application de la loi et du secteur de la sécurité privée, et Carpentier-Laberge (2015), qui a examiné les activités de diverses organisations policières en matière de médias sociaux. Les conclusions des deux études, semblables à celles observées aux États-Unis et en Europe, étaient que les MS avaient été utilisés pour communiquer avec la collectivité et en tant que nouvel outil d'enquête.

Au Québec, dans l'étude de Delle Donne et Fortin (2018), on a sondé 177 personnes travaillant dans le milieu policier pour en apprendre davantage sur leur utilisation des médias sociaux. Les répondants issus de quatre sphères d'activité (patrouilleurs, enquêteurs, analystes et gestionnaires) provenaient de six corps de police importants au Québec. Les réponses des participants quant à la perception des médias sociaux étaient très positives : ils ont estimé que la technologie pouvait être bénéfique dans le cadre de leur travail (moyenne = 3,86 sur une échelle de 5), qu'elle était compatible avec leurs pratiques, car elle répondait à un besoin (moyenne = 4,44 sur une échelle de 5). Bien que la quasi-totalité des répondants (92 %) ait affirmé que l'outil n'était pas d'une utilisation complexe, la plupart ont signalé un faible niveau de connaissance des règles d'utilisation au sein de l'organisation (moyenne = 2,90 sur une échelle de 5). Cela est cohérent quand on considère les données d'autres études et confirme l'idée que certains membres estiment ne pas savoir comment utiliser l'outil dans le contexte de leur travail. Cette étude a même permis de valider que 96 % de tous les répondants avaient utilisé les médias sociaux au moins une fois au cours de la dernière année et qu'on y avait notamment recouru dans un contexte d'enquête (trouver des éléments de preuve – 65 %, localiser un suspect – 79 %), un contexte de renseignement (explorer l'environnement d'un suspect – 84 %, produire une analyse – 46 %), un contexte de prévention (communiquer avec des citoyens – 18 %) et dans un contexte d'urgence (situation de crise – 6 %, évaluation de risque – 10 %) (Delle Donne et Fortin 2016).

Plusieurs études ont mis l'accent sur l'utilisation des médias sociaux dans un contexte de rapprochement avec la population. De nombreux corps de police au Québec et au Canada ont un compte Twitter ou Facebook afin de communiquer avec la population. Ainsi, on considère qu'une communication efficace entre la police et le public à travers les médias sociaux est un aspect fondamental de la police de proximité pour quatre raisons (Lieberman et al. 2013). Premièrement, la communication permet la mobilisation des citoyens, ce qui leur donne l'occasion de devenir des membres actifs dans la réduction du crime et du désordre et de participer à leur propre défense. Deuxièmement, il favorise des relations positives entre la police et le public. Troisièmement, il offre aux citoyens la possibilité de suggérer des solutions potentielles aux problèmes de la collectivité. Quatrièmement, une communication efficace conduit à un plus grand engagement de la population.

Une étude américaine a tenté d'établir une typologie des organisations policières en fonction de leur recours aux médias sociaux (Edlins et Brainard 2016). En analysant l'utilisation de Facebook de 15 organisations policières américaines, on a pu distinguer les types suivants :

1- Le combattant du crime. Bien que seul le service de police de Philadelphie fasse partie de ce type, il se distingue par la publication de messages sur les crimes et les criminels (86,8 %), laissant les autres types de messages de côté. L'objectif des interventions semble être de montrer au public à quel point le service de police est engagé dans la lutte contre le crime et qu'il en fait une tâche principale et primordiale.

2- Le policier traditionnel. Bien que ces organisations policières aient aussi diffusé une grande quantité de messages sur les crimes et les criminels (48,9 %), elles ont également publié des messages impliquant l'entretien des relations entre la police et le public (25,0 %) ainsi que des conseils de prévention (12,3 %). L'impression qu'on voulait laisser est que ces services de police veulent aller au-delà du rôle traditionnel de force et d'ordre et essayent également d'établir et de maintenir de bonnes relations avec la population.

3- L'agent de relations publiques. La majorité des messages de ce type montrait des contenus abordant et relatant les relations entre la police et le public (56,1 %), mais accordait aussi une certaine place à la publication d'autres contenus tels que le personnel (par exemple, la présentation d'un nouveau policier au département) (20,0 %) et les crimes et les criminels (16,3 %). Ces organisations menaient manifestement une action de relations publiques sur les médias sociaux.

4- L'agent mixte équilibré. D'autres organisations réussissent à trouver un équilibre entre les différents types de contenus, renforçant ainsi l'image

professionnelle d'un service de police moderne et doté de compétences diverses. Pour ce type, tous les genres de messages sont diffusés dans des proportions comparables.

De nombreuses études ont reproché aux organisations policières le manque d'interactivité dans leur utilisation des médias sociaux (voir van del Velde et al. 2014), mais un certain nombre de facteurs expliquent cet état de fait. La plupart des études comparent l'utilisation des médias sociaux par les policiers avec les principes régissant son utilisation par les organismes privés. Ainsi, on émet l'hypothèse que certaines organisations policières décident de restreindre l'interactivité parce qu'elles s'inquiètent de la réception de messages non sollicités (*spams*), qu'elles n'ont pas les ressources nécessaires à la surveillance et à l'utilisation des médias sociaux ou qu'elles sont préoccupées par la réception de messages offensants (Brainard et Edlin, 2015). À ce sujet, une étude révélait que les comptes policiers officiels étaient régulièrement victimes d'incivilités de la part de citoyens, amenant ces derniers à faire des commentaires qu'ils n'auraient sans doute pas faits dans la vraie vie (Knop 2018).

Toutefois, des études récentes ayant examiné l'utilisation de Twitter par des organisations policières canadiennes mentionnaient que ces organisations recouraient aux médias sociaux pour promouvoir le professionnalisme du corps de police tout en atteignant les objectifs de la police communautaire (Carpentier-Laberge, 2015, Scheider 2014). Plus spécifiquement, une étude concluait que l'analyse de 3909 messages Twitter du Service de police de la Ville de Montréal démontrait la volonté d'établir un dialogue direct et égalitaire avec la population tout en ouvrant un canal de communication spécifique avec les manifestants (Tuzza et al. 2018). Ceci constituerait une exploitation stratégique et efficace du média.

2. L'utilisation des médias sociaux dans un contexte de renseignement

L'utilisation du cadre 2.0 ne remplace pas les méthodes de recherche et de renseignement plus classiques, mais augmente plutôt les opportunités dans un contexte de vaste plateforme dans laquelle on puise les données (Rathi et Given 2010). Le renseignement en source ouverte est un outil incontournable pour analyser les nouvelles formes de criminalité (Carter 2009), notamment pour comprendre les comportements tels que la radicalisation en ligne (Omand et al. 2012), mais aussi les faits et gestes des activistes de toute nature. La collecte en ligne de renseignements en temps réel fournit non seulement des informations très utiles, mais peut également réduire les risques pour les agents, qui autrement devraient se rendre sur le terrain pour les obtenir (Ivan et al. 2015). L'absence de barrières géographiques est un autre avantage rarement rencontré dans les contextes traditionnels (Rathi et Given 2010).

Au cours des dernières décennies, les policiers ont de plus en plus utilisé le renseignement *open source* (OSINT) et les médias sociaux (SOCMINT) pour recueillir des informations auprès de groupes criminels et d'individus (voir Frank et al. 2011 au Canada). Le modèle

policier axé sur le renseignement (*intelligence led policing*) vise à permettre aux organisations policières de prévoir les crimes en fonction de l'analyse des critères distinctifs de crimes antérieurs. Ce modèle nécessite des informations collectées directement à partir des médias sociaux (Omand et al. 2012), y compris des plateformes qui créent des relations et des interactions entre utilisateurs (Omand 2017). Dans certains cas, la proactivité de l'*intelligence led policing* a amené la police à adapter ses pratiques en réaction à l'utilisation des médias sociaux par les citoyens et à demander proactivement leur collaboration. En faisant circuler des images d'émeutiers à Victoria en 2011 sur les médias sociaux, elle a pu procéder à l'identification des auteurs présumés (Trottier 2012). Deux grandes facettes de l'analyse des médias sociaux peuvent être recensées : l'analyse de contenu et l'environnement virtuel ainsi que l'analyse des groupes criminels (analyse de réseaux criminels).

Analyse de contenu partagé et environnement virtuel. La possibilité d'extraire des messages contenant des termes particuliers de façon massive sur Internet permet non seulement d'identifier les tendances, mais aussi de réduire le temps nécessaire à la collecte de ces données (Cataldi et al. 2010; Petrović et al. 2010). Par exemple, les messages haineux, en particulier en ce qui concerne l'islamophobie (Awan 2014), sont souvent observés sur les médias sociaux. Le racisme en ligne est enraciné dans les stéréotypes (Weaver 2013), et les messages indicatifs de ces représentations peuvent être extraits de grands ensembles de données (Joseph et al. 2017). Certains chercheurs se sont intéressés aux manifestations haineuses en ligne et ont conçu des outils pour aider les chercheurs et les agences d'application de la loi à collecter et analyser ces données (Edwards et al. 2013). En utilisant l'outil créé par COSMOS (Collaborative Online Social Media Observatory), qui détecte les tensions sociales, des chercheurs ont pu construire une typologie de tweets contenant notamment des menaces (Burnap et al. 2015). Les modèles qui classifient le cyberdiscours, en particulier lorsqu'ils sont mis en place après des événements particuliers comme une attaque terroriste, peuvent aider à mettre sur pied des politiques proactives tout en réduisant la victimisation (Burnap et Williams 2016). De plus, une meilleure connaissance des activités se déroulant sur les médias sociaux peut aider à révéler des schémas cachés concernant des processus sociaux et des facteurs déterminants de changements d'humeur dans la société. Obtenir une meilleure connaissance de l'environnement virtuel, par exemple du mécontentement social, pourrait favoriser une évaluation plus juste du niveau de tension sociale (Dochenko et al. 2017) et ainsi contribuer à la prévention du crime.

Suivi de groupes criminels. L'analyse des réseaux sociaux peut aider les organismes d'application de la loi et les organismes gouvernementaux à découvrir des systèmes de liens qui favorisent les activités illégales. Berger et Strathearn (2013) ont évalué les niveaux d'engagement dans l'idéologie de la suprématie blanche sur Twitter en mesurant l'influence, l'exposition et l'interactivité. Les auteurs ont démontré que ces réseaux pourraient être perturbés en ciblant ceux qui semblent les plus influents. Le principe de l'homophilie s'applique sur Twitter : les utilisateurs ont tendance à suivre des comptes qui expriment des opinions similaires aux leurs (Wu et al. 2011). L'existence d'une telle

homophilie peut servir à découvrir les profils similaires d'une population criminogène en utilisant des procédures analytiques pertinentes. C'est de cette façon que certains outils facilitent maintenant l'identification des relations entre membres de groupes criminels, mais aussi permettent la découverte de nouvelles relations. Par exemple, l'examen des *followers* et des *retweets* a été utilisé dans la recherche sur les gangs de rue et a permis de découvrir plusieurs nouveaux membres (Balasuriya et al. 2016).

3. Les manifestations virtuelles et le doxing

3.1. Les manifestations virtuelles

Internet en général, et pas seulement les médias sociaux, a été étudié comme un lieu où des cultures racistes peuvent émerger (Back 2002), car les idéologies extrémistes peuvent facilement être diffusées et toucher de vastes auditoires. Le cas du politicien hollandais d'extrême droite Geert Wilders, qui *tweetait* des contenus incendiaires sur l'islam, en est une illustration (Blanquart et Cook 2013). Alors que les suprématistes blancs, y compris ceux qui encouragent le terrorisme, constituent encore une petite proportion des utilisateurs de Twitter, les stratégies qu'ils utilisent influencent un grand nombre de personnes (Graham 2016). Une telle information est d'une grande importance pour les organismes d'application de la loi, car la propagation d'idées extrêmes est une préoccupation importante à la suite de récents événements survenus à Manchester et Paris.

Plusieurs études se sont intéressées à la façon dont les citoyens utilisent les médias sociaux pour construire la solidarité pour diverses causes (Cabalin 2014, Harlow 2013, Miladi 2011). Sousa et Ivanova (2012) ont conclu que Twitter est souvent perçu comme un lieu d'activisme civique et un lieu d'affirmation des minorités. Howard et Parks (2012) ont examiné les relations entre les médias sociaux et le changement politique. Ces derniers ont conclu qu'Internet en tant que plateforme est devenu un porte-voix pour les communautés marginalisées. Ainsi, l'impact des manifestations en ligne peut avoir un effet d'interaction avec ce qui se passe dans la rue : le Printemps érable au Québec, mais aussi des mouvements comme *#blacklivesmatter* et *#Ferguson*. Ces enjeux constituent des éléments que doivent analyser les agences d'application de la loi puisqu'ils peuvent s'attaquer à la population, à l'État ou même à l'organisation policière elle-même.

Les actions des mouvements comme Anonymous posent de nombreux défis aux agences d'application de la loi et aux administrateurs de services Internet. On assiste de plus en plus à des dérives qui ont des conséquences importantes. Ainsi, les actions du groupe ont entraîné la paralysie de systèmes informatiques d'entreprises critiques comme la banque suisse PostFinance et la compagnie MasterCard (Ludlow 2010). En réponse à l'annonce du projet de loi antiterroriste proposé en 2015, un appel a été lancé par Anonymous afin de protester contre le projet. Le site de la GRC fut paralysé pendant quelques heures. Or, certains gouvernements, dont celui de la Colombie-Britannique, ont affirmé qu'il est

crucial de suivre et de comprendre les tendances observées dans les milieux de l'*hacktivisme* afin de mieux y répondre (Beach 2012). On mentionne aussi que les mouvements comme Anonymous ont transformé la façon de concevoir la participation criminelle (Li 2013). Il s'agit d'un exemple où Internet a bouleversé les processus de transfert de connaissances entre criminels et, par le fait même, la capacité de la police à répondre aux comportements délinquants (Reyns et al. 2011) Au Québec, à la suite d'attaques contre des services policiers, les renseignements personnels de 163 membres de l'Association des directeurs de police du Québec ont été divulgués en guise de représailles aux actions policières durant le Printemps érable. Cette pratique qu'on nomme le *« doxing »* est souvent utilisé par les mouvements d'activistes et sera présenté dans la prochaine partie.

3.2. Médias sociaux et impacts du doxing (dénoncer et condamner 2.0)

Au cours des dernières années, le recours aux médias sociaux a amené une pratique de l'utilisation de l'information à des fins malveillantes. Cette pratique était auparavant connue sous le vocable de *« honte publique »,* une forme de contrôle social déployée lorsqu'une personne enfreint les normes d'une communauté donnée et que les autres réagissent en la critiquant publiquement ou en l'ostracisant (Hawkes 2017). Le terme *« doxing »* vient de l'anglais *« to document »* (*dropping documents* ou *dropping dox*), ou fournir des preuves. Il s'agit d'une forme d'abus en ligne qui survient lorsqu'une partie malveillante en blesse une autre en divulguant des informations d'identification ou sensibles (Snyder et al. 2017). On y associe aussi l'action de rechercher activement de l'information compromettante. Ces données peuvent inclure des noms légaux complets, des adresses résidentielles, des identifiants uniques pour les enregistrements et services gouvernementaux (numéros d'assurance sociale, etc.), des documents professionnels et des photos de la cible et de ses proches (Douglas 2016). La recherche et la divulgation de ces informations se distinguent sous trois formes (Douglas 2016). D'abord, le *deanonymizing doxing*, où on vise à révéler des infos concernant l'identité d'une personne désirant rester anonyme. Ensuite, on a identifié le *targeting doxing*, qui consiste à divulguer des renseignements concernant la localisation géographique de la personne. Finalement, celui ayant le plus d'impact est le *delegitimizing doxing* : révéler des infos privées avec l'intention de déshonorer, d'humilier la personne ou d'entacher sa crédibilité ou sa réputation.

Dans une étude exhaustive sur le *doxing*, des auteurs ont identifié quatre motivations générales associées à cette pratique (Snyder et al. 2017). Premièrement, il peut s'agir de ce que les auteurs appellent « l'esprit de compétition ». Il s'inscrit dans la mentalité de certains pirates informatiques voulant relever une forme de défi, le succès de l'opération leur procurant un sentiment de supériorité, particulièrement si la cible s'est proclamée difficilement atteignable. Deuxièmement, la vengeance constitue une autre motivation importante. Elle peut être par exemple une réponse à un conflit sur un forum en ligne. Troisièmement, l'auteur de la divulgation peut agir au nom de ce qu'il perçoit comme la justice. Il viserait ici une cible ayant commis un acte immoral ou injuste envers un tiers. Les

cibles peuvent avoir escroqué d'autres personnes sur un forum en ligne, ou encore avoir collaboré avec les forces de l'ordre. Finalement, les divulgations peuvent avoir des visées politiques allant au-delà des cibles individuelles pour tenter d'atteindre des groupes, des regroupements d'individus et l'État. Parmi les exemples de divulgations politiques, citons celles de membres de groupes comme le KKK, de groupes de consommateurs de pornographie juvénile ou de personnes travaillant dans des industries que les divulgateurs considèrent comme abusives envers les animaux. À cet égard, on a évoqué que le *doxing* est une tactique de justice sociale faisant partie de l'arsenal des militants antifascistes afin d'aider les communautés vulnérables à contrebalancer les stratégies des groupes haineux de la suprématie blanche (Colton et al. 2017).

Ainsi, on a affirmé que le *doxing* est un spectre qui hante Internet (Douglas 2016) et qui peut toucher plusieurs individus ou groupes. Il est important de souligner que ces informations sont peut-être déjà accessibles au public, mais sous une forme difficile d'accès, ou encore de façon à rendre difficile le croisement de données, occultant ainsi les découvertes fortuites. Dans certains cas, elles pourraient même avoir été obtenues directement de la personne elle-même, de gré ou de force (Douglas 2016). Ce qui a grandement changé la donne est la possibilité que ces informations soient divulguées dans une perspective d'autojustice (Lavoie, Fortin et Ouellet 2013). De nombreux observateurs perçoivent la pratique extrajudiciaire du *doxing* comme une réponse à l'incapacité des institutions d'application de la loi traditionnelles à s'adapter aux besoins et aux réalités du monde numérique en pleine mutation (Ellib 2017). Bien que tout le monde puisse être touché par le phénomène, il semble toutefois que les trois communautés les plus touchées soient les joueurs en ligne, les pirates informatiques et les célébrités (Snyder et al. 2017).

Cette nouvelle problématique entraîne des conséquences dans les pratiques policières. Premièrement, cette pratique pourrait occasionner des plaintes de la part des citoyens. Bien qu'anecdotique, l'événement survenu à Charlottesville est un archétype de ce qui pourrait devenir récurrent dans un monde post-2.0. Lors de cette manifestation anti-immigration, le groupe *Yes You're Racist* (voir annexe 1) invitait les abonnés du compte Twitter à dénoncer les manifestants et à « les rendre célèbres ». Cet appel à l'action a bien fonctionné et plusieurs internautes se sont mobilisés pour faire des « enquêtes d'identification » en exposant les cibles à des représailles. De plus, il faut noter que dans cet exemple, une personne a subi des préjudices puisqu'on l'a confondue avec un manifestant anti-immigration. Les cibles réelles ou mal identifiées ne sont plus en mesure de dissocier complètement leurs noms de cette étiquette (Victor 2017). On constate en effet que dans ce contexte, il n'y a pas de droit de réponse et qu'aucun canal de communication direct ne permet à la personne lésée de se défendre (Ahmed 2004).

Dans certains cas, on constate que la connaissance des informations comme l'adresse personnelle de la cible a permis d'ajouter une autre forme de harcèlement. Une nouvelle pratique appelée le *« swatting »* a commencé à se manifester. Cette pratique consiste à appeler la police en urgence en affirmant qu'il y a eu un incident violent à l'adresse du sujet, ce qui a incité la police à réagir (Mantilla 2015). Plusieurs vidéos sont disponibles sur

les sites de partage où on peut voir les interventions policières puisque la cible utilisait une application pour se filmer en train de jouer à un jeu vidéo.

Deuxièmement, l'actualité a montré que certaines personnes ont utilisé des techniques de *doxing* auprès de policiers. Comme certains l'ont évoqué, la vie privée des agents de police devient de plus en plus publique et pose des risques pour l'intégrité, l'efficacité et la réputation de la police (Goldsmith 2015). Ainsi, deux concepts viennent agir en synergie pour produire l'effet indésirable de divulgation des informations personnelles de policiers. D'une part, on a évoqué l'idée de l'importance de l'indiscrétion policière, l'incapacité à faire preuve de discrétion dans le travail de la police ou dans la vie de policier. Avec l'utilisation des médias sociaux, le dévoilement de certaines informations peut entraîner une baisse d'efficacité opérationnelle et une atteinte à la réputation de l'organisation ou de la personne. D'autre part, certains individus malintentionnés peuvent activement partir à la recherche d'informations personnelles sur le policier. Comme évoqué précédemment, le mouvement Anonymous avait divulgué des informations sur 163 membres de l'Association des directeurs de police du Québec. Au Canada, il a été observé que des groupes Facebook étaient utilisés pour se livrer à du renseignement sur des agents de police (voir annexe 2).

Aux États-Unis, bien qu'aucune étude systématique rigoureuse n'ait été réalisée, une synthèse des affaires récentes a tout de même été diffusée et montre que cette tendance est belle est bien présente :

- Noms, numéros de téléphone et adresses de domicile de 80 policiers de Miami divulgués par le groupe Crackas With Attitude.
- Noms, numéros de téléphone, courriels et les renseigements de 2400 agents fédéraux, policiers locaux, et agences militaires divulgués par le groupe Crackas With Attitude.
- Liste d'agents du FBI divulgués par un groupe revendiquant « free Palestine »
- Publication d'une liste de 2000 noms, numéros de téléphone, courriels d'agents police ou de militaires

(Franceschi-Bicchierai 2017)

Cette nouvelle réalité expose les policiers à des conséquences importantes. En signifiant que la dure réalité est qu'on ne peut retirer les informations qui sont diffusées et partagées sur Internet, Drake (2016) propose une série de mesures allant de la vérification des sites de vente d'informations personnelles jusqu'au retrait des informations personnelles sur différents sites Web. À cet égard, plusieurs mesures doivent être mises de l'avant pour protéger la vie privée des policiers.

4. La demande accrue en formation

La vitesse de l'évolution des nouvelles technologies de l'information entraîne aussi de nombreux défis en termes de formation des policiers. Malgré la reconnaissance généralisée du potentiel des médias sociaux dans les relations avec la collectivité et le désir de tirer parti des médias sociaux, de nombreux organismes d'application de la loi manquent de connaissances, de formation, de temps, mais surtout de ressources financières pour adopter les nouvelles technologies rapidement (Williams et al. 2018). Edlins et Brainard (2016) suggèrent que l'insuffisance des ressources et l'absence de politiques expliquent la lente transformation vers l'utilisation des médias sociaux des dix services de police américains les plus importants. Plusieurs organisations policières ont néanmoins pris l'initiative d'offrir des programmes de formation visant principalement la communication avec le public.

À Toronto, où Twitter est utilisé dans le cadre d'une approche très décentralisée, les changements dans le rôle de communicateurs des agents de police ont poussé les autorités à former un très grand nombre de policiers en communication publique (Meijer et Torenvlied 2016). Cette initiative de la police de Toronto a permis de former près de 200 policiers en trois jours sur l'utilisation des médias sociaux (Meijer et Thaens 2013). Essentiellement, les policiers reçoivent les notions de base du média basées sur l'expérimentation tout en obéissant à certaines règles opérationnelles comme : « ne spéculez pas », « ne parlez pas de l'enquête » et « ne parlez pas d'agents ». En plus de la formation, on mentionne que, pour prévenir les problèmes de communication, les services de police appliquent des contrôles internes sous forme de surveillance et de lignes directrices à suivre (Meijer et Torenvlied 2016). Toutefois, les administrations policières doivent adopter de nouvelles stratégies pour que les agents de police acquièrent une formation sur les médias sociaux qui leur permette d'exercer une surveillance des personnes qui utilisent les médias sociaux pour des activités illégales (Travis 2011).

Annexe 1 : Tweet du groupe Yes, You’re Racist

Annexe 2 : Capture d’écran d’un groupe de renseignements sur des policiers

Références

Ahmed, S. (2004). The cultural politics of emotion. Edinburgh: Edinburgh University Press.

Awan I (2014) Islamophobia and twitter: A typology of online hate against Muslims on social media. *Policy & Internet* 6(2): 133-150.

Back L (2002) Aryans reading Adorno: Cyber-culture and twenty-first century racism. *Ethnic and Racial Studies* 25(4): 628-651.

Balasuriya, L., Wijeratne, S., Doran, D. & Sheth, A. (2016). *Finding Street Gang Members on Twitter.* Article présenté au 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, San Francisco, USA. Repéré à https://arxiv.org/pdf/1610.09516.pdf

Beach, M. (2012). Hacktivism and the government of British Columbia. Official publication. British Columbia.

Berger, J. M. & Strathearn, B. (2013). *Developments in Radicalisation and Political Violence. Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Extremism in Online Social Networks*. Repéré à http://icsr.info/wp-content/uploads/2013/03/ICSR_Berger-and-Strathearn.pdf

Blanquart, G. & Cook, D. M. (2013). *Twitter Influence and Cumulative Perceptions of Extremist Support: A Case Study of Geert Wilders.* Article présenté au 4th Australian Counter Terrorism Conference, Perth, Australia. Repéré à http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1021&context=act

Brainard, L. and Edlins, M. (2015). 'Top 10 US Municipal Police Departments and Their Social Media Usage'. The American Review of Public Administration, 45(6): 728–745.

Brodeur, J. P. (2010). The Policing Web. New York: Oxford University Press.

Burnap P and Williams ML (2016) Us and Them: Identifying Cyber Hate on Twitter Across Multiple Protected Characteristics. *EPJ Data Science* 5(11): 1-15.

Burnap, P., Rana, O. F., Avis, N., Williams, M., Housley, W., Edwards, A., et al. (2015). Detecting tension in online communities with computational Twitter analysis. Technological Forecasting & Social Change, 95(C), 96–108.

Cabalin, C. (2014). Online and Mobilized Students: The Use of Facebook in the Chilean Student Protests. Communicar, 22(43), 25–33. http://doi.org/10.3916/C43-2014-02

Carter, D. L. (2009). *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (2nd ed.). Repéré à https://fas.org/irp/agency/doj/lei.pdf

Carpentier-Laberge, C. (2015) La police et Twitter : l'utilisation des médias sociaux par les services policiers canadiens. Mémoire de maitrise inédit. Repéré à : http://hdl.handle.net/1866/12235

Cataldi, M., Di Caro, L. & Schifanella, C. (2010). *Emerging topic detection on Twitter based on temporal and social terms evaluation.* Article présenté au Tenth international workshop on multimedia data mining, Washington, USA. Repéré à http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.329&rep=rep1&type=pdf

Colton J. S., Holmes, S., & Walwema, J. (2017). From NoobGuides to #OpKKK: Ethics of Anonymous' tactical technical communication. Technical Communication Quarterly, 26(1), 59-75.

Delle Donne, J., & Fortin, F. (2018). Innovation and Policing: Factors Influencing the Adoption of Social Medias by Members of Quebec Police Organizations. Policing: A Journal of Policy and Practice.

Denef, S., Kaptein, N., Bayerl, P. S., and Ramirez, L. (2012). Best Practice in Police Social Media Adaptation. COMPOSITE—Comparative Police Studies in the EU. Repéré à http://repub.eur.nl/pub/40562/

Donchenko, D., Ovchar, N., Sadovnikova, N., Parygin, D., Shabalina, O., & Ather, D. (2017). Analysis of Comments of Users of Social Networks to Assess the Level of Social Tension. Procedia Computer Science, 119, 359-367.

Douglas, D. M. (2016). Doxing: a conceptual analysis. Ethics and Information Technology, 18(3), 199–210.

Drake, T. (2016, Oct 19) How cops can protect themselves from doxing Repéré à https://www.policeone.com/Officer-Safety/articles/233207006-How-cops-can-protect-themselves-from-doxxing/

DynamicMarketing (2017) Taux de pénétration des réseaux sociaux en janvier 2017. Repéré à https://www.dynamicmarketing.eu/statistique-taux-penetration-reseaux-sociaux/

Edlins, M., & Brainard, L. A. (2016). Pursuing the promises of social media? Changes in adoption and usage of social media by the top 10 U.S. police departments. Information Policy, 21, 171–188.

Edwards A, Housley W, Williams M, Sloan L and Williams M (2013) Digital Social Research, Social Media and the Sociological Imagination: Surrogacy, Augmentation and Re-Orientation. International Journal of Research Methodology 16(3): 245-260.

Ellib, E. G. (2017). Whatever your side, doxing is a perilous form of justice. Wired. Repéré à https://www.wired. com/story/doxing-charlottesville/

Franceschi-Bicchierai, L. (2017, 22 janvier) Hackers 'Dox' Miami Police Officers With Data Stolen From Government Database Repéré à https://motherboard.vice.com/en_us/article/bmvze8/hackers-dox-miami-police-officers-with-data-stolen-from-government-database

Frank, R., Cheng, C. and Pun, V. (2011). Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities. Repéré à http://epe.lac-bac.gc.ca/100/201/301/weekly_checklist/2012/internet/w12-05-U-E.html/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf

Graham R. (2016) Inter-Ideological Mingling: White Extremist Ideology Entering the Mainstream on Twitter. *Sociological Spectrum* 36(1): 24-36.

Goldsmith A. (2015) Disgracebook policing: social media and the rise of police indiscretion, Policing and Society, 25:3, 249-267

Harlow, S. (2013). It was a "Facebook revolution:" Exploring the meme-like spread of narratives during the Egyptian pro- tests, Revista de Comunicacion 12, 59–82.

Hawkes, R. (2017). Local Nazis in your area: public shaming and communal disgust in the doxing of white nationalists at Charlottesville. Journal of Undergraduate Research in the Creative Arts and Industries 1 (1).

Howard, P. N., et Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. Journal of Communication, Volume 62, Issue 2, 1 April 2012, p.359–362.

IACP (2013). Social Media Survey Results [PDF]. Repéré à https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=264257

Ivan, A. L., Iov, C. A., Lutai, R. C., & Grad, M. N. (2015). Social media intelligence: opportunities and limitations. CES Working Papers, 7(2A), 505.

Joseph, K., Wei, C. & Carley, K. M. (2017). *Girls Rule, Boys Drool: Extracting Semantic and Affective Stereotypes on Twitter.* Article présenté au ACM Conference on Computer-Supported Cooperative Work and Social Computing, Portland, USA. Repéré à http://www.cs.cmu.edu/~kjoseph/papers/cscw_17.pdf

Knop, J. (2018) 280 insulting characters? An analysis of the content of tweets addressed to the police in Canada and the United States Mémoire de maitrise inédit. Repéré à : http://hdl.handle.net/1866/20964

Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime..” Harvard Journal of Law and Technology 27, 301-587.

Lieberman, J. D., Koetzle, D., & Sakiyama, M. (2013). Police departments' use of Facebook: Patterns and policy issues. Police Quarterly, 16(4), 438-462.

Lavoie, P.E., Fortin, F. et Ouellet, I. (2013). « Usages problématiques d'Internet ». Dans FORTIN, Francis (sous la direction de) Cybercriminalité: entre inconduite et crime organisé, Montréal, Les Presses Internationales Polytechnique, 230 pages.

Ludlow, P. (2010). Wikileaks and hacktivist culture. The Nation, 4, 25-26.

Mantilla, K. (2015). Gendertrolling: How misogyny went viral. Santa Barbara, CA: Praeger.

Meijer, A., & Thaens, M. (2013). Social media strategies: Understanding the differences between North American police departments. *Government Information Quarterly*, 30(4), 343–350. http://doi.org/10.1016/j.giq.2013.05.023

Meijer, A. J., & Torenvlied, R. (2014). Social Media and the New Organization of Government Communications. *The American Review of Public Administration*, 46(2), 143–161. http://doi.org/10.1177/0275074014551381

Miladi, N. (2011). New media and the Arab revolution: Citizen reporters and social activism. Journal of Arab & Muslim Media Research, 4(2&3), 113–119. doi:10.1386/jammr.4.2-3.113_2.

Omand, D. (2017). Social Media Intelligence (SOCMINT). In The Palgrave Handbook of Security, Risk and Intelligence (pp. 355-371). Palgrave Macmillan, London.

Omand D, Barlett J and Miller C (2012) Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security* 27(6): 801-823.

Petrović, S., Osborne, M. & Lavrenko, V. (2010). *Streaming first story detection with application to Twitter.* Article présenté au Human language technologies: The 2010 annual conference of the North American chapter of the ACL, Los Angeles, USA. Repéré à http://homepages.inf.ed.ac.uk/miles/papers/naacl10a.pdf

Rathi, D. & Given, L. (2010). *Research 2.0: A Framework for Qualitative and Quantitative Research in Web 2.0 Environments.* Article presenté au 43rd Hawaii International Conference on System Sciences, Hawaii, USA. Repéré à http://ieeexplore.ieee.org/document/5428434/

Reyns, B. W. & B. Henson & B. S. Fisher. (2011). “Being Pursued Online: Applying Cyberlifestyle- Routine Activities Theory To Cyberstalking Victimization.” Criminal Justice And Behavior. 38(11): 1149-1169.

Schneider, C.J. (2014). Police presentational strategies on Twitter in Canada. Policing and Society : An International Journal of Research and Policy. 1-19

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame (pp. 432–444). Présenté au 2017 Internet Measurement Conference, New York, New York, USA: ACM Press.

Sousa, A., & Ivanova, A. (2012). Constructing Digital Rhetorical Spaces in Twitter: A Case-Study of @BarackObama. Topics in Linguistics, (9), 46-55.

Travis, A. (2011). Riots report to recommend change in police tactics. The Guardian. Repéré le June 7 2018 à http://www.guardian.co.uk/uk/2011/nov/29/riots-report-change-police-tactics.

Trottier, D. (2012) Policing Social Media. Revue Canadienne de Sociologie, 49(4): 411–425.

Tuzza, S., Tanner, S., Carpentier-Laberge, C. (2018). La police face aux outils numériques: Stratégies, pratiques et communication policière sur Twitter lors des manifestations a Montreal. Canadian Journal of Criminology and Criminal Justice 60(3), 354-386.

van de Velde, B., Meijer, A., & Homburg, V. (2014). Police message diffusion on Twitter: analysing the reach of social media communications, Behaviour & Information Technology, 34:1, 4-16

Victor, D. (2017, 14 août). Amateur sleuths aim to identify Charlottesville marchers,but sometimes misfire. New York Times. Repéré à https://www.nytimes. com/2017/08/14/us/charlottesville-doxxing.html

Weaver S (2013) A Rhetorical Discourse Analysis of Online Anti-Muslim and Anti-Semitic Jokes. *Ethnic and Racial Studies* 36(3): 483-499.

Williams, C. B., Fedorowicz, J., Kavanaugh, A., Mentzer, K., Thatcher, J. B., & Xu, J. (2018). Leveraging social media to achieve a community policing agenda. Government Information Quarterly 35 p. 210–222.

Wu, S., Hofman, J. M., Mason, W. A. & Watts, D. J. (2011, March). *Who Says What to Whom on Twitter.* Article présenté au the International World Wide Web Conference, Hyderabad, India. Repéré à http://www.wwwconference.org/proceedings/www2011/proceedings/p705.pdf

Wu, B. (2015). Doxxed: Impact of online threats on women including private details being exposed and “swatting”. Plus Greg Lukianoff on balancing offence and free speech. Index on Censorship, 44(3), 46-49.

Chapitre 5. *Policing*, nouvelles technologies et algorithmes
Anthony Amicelle

« Un nouvel objet a fait son entrée dans nos vies : les algorithmes. Ce terme d'informatique a une signification bien plus large qu'on ne le croit. Comme la recette de cuisine, un algorithme est une série d'instructions permettant d'obtenir un résultat. À très grande vitesse, il opère un ensemble de calculs à partir de gigantesques masses de données (les « *big data* »). […] Il n'est plus beaucoup de gestes quotidiens, d'achats, de déplacements, de décisions personnelles ou professionnelles qui ne soient orientés par une infrastructure de calculs » (Cardon 2015 : 7).

À l'instar de cette observation formulée par le sociologue Dominique Cardon en préambule de son ouvrage intitulé « À quoi rêvent les algorithmes? », force est de constater que ce qu'il est convenu de nommer la « révolution des données » ou encore la « *datafication* » du monde a des implications dans de nombreuses sphères de la société (Cukier et al. 2013). Les enjeux et les usages des algorithmes et de la numérisation massive des données touchent *de facto* à d'innombrables domaines de la vie quotidienne, que ce soit dans le commerce, les campagnes électorales, l'assurance, la finance, le journalisme – via le *data journalism*, la santé et la sécurité pour ne citer que quelques exemples (Campbell-Verduyn et al. 2017, Pasquale 2015). Dans ce cadre, si les algorithmes peuvent être appréhendés comme une série d'instructions permettant d'obtenir un résultat, la notion de *big data* ou de données massives renvoie avant tout à la « capacité de chercher, d'agréger et de recouper de larges ensembles de données » (Boyd et al. 2012). À cet égard, la spécificité des algorithmes à l'ère du *big data* est souvent résumée à la lettre V avec, selon les cas, trois à quatre déclinaisons caractéristiques : Volume; Variété; Vélocité; Véracité.

En tant que première caractéristique, la question du Volume a trait à l'augmentation exponentielle des données numériques ainsi qu'aux nouvelles capacités évolutives de stockage, de traitement et de communications de ces données. À titre d'illustration, la composition de l'univers numérique était estimée en 2016 à « plus de mille-deux-cent milliards de milliards d'octets, dont quatre-vingt-dix pourcents auraient été produits dans les deux dernières années. Ce nombre, qui double tous les deux ans, devrait être multiplié par dix d'ici 2020, pour atteindre 44 zettabytes, ou 44 trillions de gigabytes » (Rouvroy 2016 : 5). Deuxièmement, les données massives analysées se démarqueraient également par leur variété, tant au niveau des sources que des formats (textes, images, sons, etc.), structurés (selon justement un format prédéfini) ou non structurés, par exemple du texte brut tel que le corps d'un message en ligne ou d'un courriel (ibid.). Le troisième V, celui de Vélocité, souligne ensuite la vitesse sans précédent d'accumulation et de traitement des données, souvent en temps réel. Le quatrième et dernier V, celui de véracité, n'est pas systématiquement inclus dans la littérature et pour cause, il concerne davantage un « défi » qu'une réelle spécificité du *big data*, celui de la qualité des données liée notamment au degré de facilité socio-technique des dispositifs en place pour les numériser et les traiter.

Comme l'a résumé Antoinette Rouvroy, « [l]es *big data* signifient donc surtout le franchissement d'un seuil de quantité, de complexité, de rapidité de prolifération des données à partir duquel nous serions contraints d'automatiser et d'accélérer (pour tenir compte de l'accroissement continu, à grande vitesse, des masses de données) les processus de transformation des données numériques en informations opérationnelles. L'expression *Big Data* renvoie donc aux masses de données numériques complexes à accumulation rapide, mais aussi à l'ensemble des nouvelles techniques logicielles (*Data Mining, Machine Learning, Social Network Analysis, Predictive Analytics, "Sensemaking", Natural Language Processing, Visualization*,...) sans lesquelles les données resteraient « muettes », et qui présupposent à leur tour l'utilisation de capacités de stockage et de traitement gigantesques » (Rouvroy 2016 : 11).

D'un côté, la focale sur les *big data* insiste sur l'échelle et la portée des traces numériques laissées par les personnes ainsi que par les flux de capitaux, d'informations et de marchandises en mouvement (Amoore et al. 2015). De l'autre, elle met en lumière la manière dont cette croissance des données numériques va de pair avec l'avènement d'instruments analytiques dits avancés et la promesse de rendre intelligible des *clusters* et des *patterns* – sur des objets et sujets d'intérêt – qui seraient autrement imperceptibles à « l'œil humain ».

Si cette tendance est loin d'être limitée à un secteur d'activités en particulier, il ne faut pas pour autant en inférer des usages, des finalités et des « possibilités de succès » similaires d'un domaine à l'autre. David Lyon rappelle ainsi que « le marketing auprès des consommateurs, les soins de santé, la police urbaine et l'anti-terrorisme – pour prendre quatre sites prépondérants d'application potentiels et actuels du *big data* – n'impliquent pas les mêmes choses et que les pratiques qui peuvent, dans une certaine mesure, être acceptables dans un cas (par exemple, le marketing), peuvent éroder les droits et nier la dignité humaine dans un autre (par exemple, le terrorisme). S'il y a bien des bénéfices ou des inconvénients potentiels, ils ne sont donc pas identiques dans chaque domaine » (Lyon 2016 : 255). Les enjeux et usages des algorithmes et, par extension, des nouvelles technologies dans les domaines du renseignement, du *policing* et de la sécurité nécessitent donc d'être précisés et interrogés, c'est l'objet du présent chapitre.

Dans cette perspective, il convient dans une première section de revenir sur les implications d'une réflexion scientifique sur le rôle et des effets des nouvelles technologies en général, et des instruments algorithmiques en particulier, dans les pratiques de surveillance, de renseignement, de *policing* et de sécurité, entendus au sens large (Andrejevic et al. 2014, Huysmans 2014, Aradau et al. 2015, 2017).

Dans un deuxième temps, il s'agit de mettre concrètement l'accent sur les nombreux changements à l'œuvre en matière de *policing* à la lumière des algorithmes de détection développés et déployés pour contrôler la circulation des personnes, des capitaux et des marchandises (Hannam et al. 2006, Amoore et al. 2017). L'exemple paradigmatique

privilégié pour illustrer ces profonds changements sera celui du « *policing* financier » (Amicelle 2018), à savoir la mobilisation de nouvelles technologies pour surveiller les flux financiers et détecter des activités suspectes au nom de la lutte contre le blanchiment d'argent et le financement du terrorisme. En faisant ce pas de côté vis-à-vis du travail policier *stricto sensu* et en déplaçant le regard analytique sur le *policing* financier, il s'agit aussi d'avoir l'opportunité d'aborder des problématiques clés telles que celles inhérentes au traitement routinier des données massives et des faux-positifs que cela génère.

Une troisième section sera ensuite consacrée à une des grandes promesses associées aux méthodes d'approches automatiques (*machine learning*) dans la sphère policière, à savoir le pouvoir prédictif des algorithmes concernant la localisation des crimes (Nix 2015, Shapiro 2017). Nous reviendrons plus spécifiquement sur les connaissances disponibles au sujet des logiciels – type Predpol – désormais utilisés par des forces de police, notamment aux États-Unis.

Enfin, une quatrième et dernière section conclusive portera sur les réflexions accumulées à propos de l'importance de tenir compte de l'impact des technologies et de leur appropriation quotidienne dans les activités policières. Il s'agira encore une fois de mettre en perspective les promesses technologiques actuelles, cette fois-ci à la lumière des expériences de changement technologique vécues par le passé. Ce recul critique permettra d'en tirer des conclusions générales et des enseignements pratiques utiles pour l'avenir.

1. Penser le rôle et la force d'action des nouvelles technologies

Au cours des dernières années, les instruments socio-techniques et technologies en tout genre ont fait l'objet d'une attention accrue au sein des recherches consacrées aux problématiques de police et de sécurité. En effet, des outils « high-tech » tels que justement les algorithmes mais aussi les outils biométriques, les bases de données, les caméras corporelles, la géolocalisation, sans oublier des outils plus « low-tech » comme les listes et les fichiers papiers, ont été au cœur de nombreuses recherches. Il s'est généralement agi d'examiner les configurations et éventuelles re-configurations des activités de surveillance et de contrôle en concentrant l'analyse sur l'équipement ou l'instrumentation censé faciliter ces pratiques et les stabiliser dans le temps.

Différents sites et domaines d'action ont ainsi été passés en revue pour prendre au sérieux et étudier plus avant le rôle et les effets des technologies largement mobilisées, au point d'être parfois devenues indispensables dans la gouvernance de la sécurité. Dans ce cadre, les chercheurs s'accordent désormais sur l'importance de questionner les technologies choisies, celles-ci ayant chacune leur propre histoire en étant basée sur des standards, des finalités et des fonctionnalités négociés qui sont implicitement porteurs de représentations spécifiques des problèmes à traiter. Ici, les technologies de sécurité ne sont pas des objets statiques puisque leur force d'action dépend de processus de production, de circulation, d'appropriation et éventuellement de résistance de la part de

leurs utilisateurs. La compréhension du processus dynamique de « dialogue » entre un type de technologie et un contexte spécifique d'action – tel qu'un service de police municipal – est d'autant plus importante qu'il se peut que ce processus produise des effets aussi bien inattendus que non désirés.

À cet égard, des études ont été réalisées au sujet de la « technologisation » de la sécurité et les manières dont cette tendance affecte ou reflète les logiques, rationalités ou modes de raisonnement sous-tendant les pratiques de sécurité et l'action de faire la police (Chan 2001, Ceyhan 2008). Dans ces études, la notion de technologie est d'ailleurs souvent employée pour évoquer des outils de collecte, de stockage et de traitement de données numériques.

Plus généralement, l'accent renouvelé sur les technologies a progressivement permis de s'extraire de l'opposition habituelle entre une vision dite instrumentale et une vision dite substantialiste de la technologie. Insistant sur l'importance cruciale des conséquences de l'instrumentation – c'est-à-dire la formulation, la production, le choix et l'appropriation des technologies – pour comprendre nombre de pratiques contemporaines en matière de *policing* et de sécurité, ces travaux s'accordent sur le fait que les instruments socio-techniques sont moins des intermédiaires inertes que des éléments partiellement autonomes contribuant simultanément à habiliter et à contraindre les acteurs qui y ont recours, orientant ainsi les comportements. Chaque technologie est porteuse de connaissances et de représentations particulières concernant les manières d'exercer des formes de contrôle et de gérer les relations entre les représentants de l'autorité étatique et les citoyens.

En cela, chaque technologie, plus ou moins sophistiquée, fournit également une grille d'analyse pour décrire et catégoriser les problèmes à traiter. Par exemple, Georges Kelling a travaillé sur les fondements normatifs des instruments de mesure des performances de la police en montrant comment ils généraient des manières particulières de présenter le travail policier, principalement—si ce n'est exclusivement—sous l'angle de la réduction du crime. Il a ainsi conclu que « mesurer la performance policière seulement au prisme des statistiques criminelles revient simplement à ignorer des éléments essentiels relatifs à la justice, l'intégrité, la diminution de la peur, la satisfaction des citoyens, la protection et l'aide envers celles et ceux qui ne sont pas en mesure de se protéger ou de se venir en aide, entre autres choses » (Kelling 1996 : 32).

Dans cette logique, les technologies ne sont pas neutres ni juste à la disposition des acteurs censés les utiliser. Par ailleurs, une innovation technologique n'est pas non plus la simple et pure matérialisation d'une idée initiale. Les technologies de sécurité sont le résultat de controverses, de rapports de force et donc de débats entre une myriade d'acteurs, de conceptions, d'intérêts, de buts et de valeurs. Autrement dit, le processus par lequel des technologies sont produites pour être associées à des activités de police et de sécurité est autant normatif—voire politique—que technique, si ce n'est plus. Analyser et comprendre la sélection, la construction, l'adaptation et l'articulation de différentes technologies est

donc crucial dans la mesure où ces dimensions vont *in fine* peser sur les comportements policiers et de sécurité.

Il convient ainsi de bien saisir les enjeux et les problèmes posés par l'instrumentation (Halpern et al. 2014 : 17), c'est-à-dire le choix et les usages des technologies qui participent à l'action de faire la police. En effet, les technologies peuvent être amenées à jouer des rôles différents selon les circonstances. Alors que dans certains cas elles peuvent vraiment être de simples intermédiaires qui ne changent pas le cours des pratiques existantes, dans d'autres cas elles vont en partie contribuer à transformer ces pratiques et modifier les façons de faire (Chan 2001). Il s'agit de garder systématiquement en tête la question de savoir si la technologie choisie et à l'œuvre fait ou non une différence dans l'action de faire la police. Les technologies ne doivent pas juste être appréhendées comme des choses puisqu'il s'agit d'instruments enchâssés dans des pratiques sociales et professionnelles, déployés dans des configurations de travail avec des rapports de force spécifiques. En cela, les policiers et les professionnels de la sécurité sont équipés d'une grande variété d'instruments et de technologies qui méritent pleinement d'être étudiées.

2. Le *policing* financier et l'exemple des algorithmes de détection

Dans cette section, il s'agit de commencer à saisir concrètement ce que signifie surveiller et contrôler quotidiennement via des algorithmes à l'ère du *big data* et ce, en s'attardant sur la question des mobilités, et plus précisément d'une mobilité en particulier. « Le concept de mobilités englobe à la fois les mouvements à grande échelle des personnes, des capitaux et des informations à travers le monde, et les processus plus locaux de transport journalier, de mouvement dans l'espace public et de déplacement d'objets matériels dans la vie quotidienne. […] Les peurs soulevées par les mobilités illicites et les risques pour la sécurité qui y sont associés déterminent de plus en plus les logiques de gouvernance et les responsabilités de protection dans les secteurs tant publics que privés » (Hannam et al. 2006 : 1). Au risque de rappeler une évidence, les mobilités ainsi définies sont régulièrement associées à des inquiétudes en termes de sécurité, et les nouvelles technologies sont souvent promues comme une solution, voire la solution, pour sécuriser de telles mobilités.

Les innovations technologiques dans le domaine du numérique et du *big data* jouent un rôle croissant dans la gestion de cette relation entre mobilité et sécurité, autrement dit dans la gestion de cette « tension dynamique entre la liberté de mobilité et la fourniture de sécurité » (Amoore et al. 2008 : 96). En effet, les contrôles de mobilités sont de plus en plus médiés par le biais de nouvelles technologies pour faire face à ce qui est présenté comme le dilemme suivant : comment faciliter les mouvements de personnes, de capitaux et de données tout en faisant respecter les lois contre les mobilités dites illicites ?

Dans ce cadre, les enjeux posés par le choix et les usages des nouvelles technologies devant permettre les contrôles de mobilités sont cruciaux. Pour l'illustrer, nous prenons ici l'exemple paradigmatique de la lutte contre le blanchiment d'argent et le financement du

terrorisme dans laquelle des instruments algorithmiques sont utilisés quotidiennement pour suivre avec attention les flux financiers et détecter les activités suspectes au nom de la sécurité et de la répression de la criminalité et ce, suivant la métaphore de l'aiguille dans la botte de foin.

2.1. Trouver (technologiquement) l'aiguille dans la botte de foin

« Si vous pensez à internet comme à une énorme botte de foin, ce que nous essayons de faire c'est de collecter du foin dans les différentes parties de la botte auxquelles nous avons accès et qui pourraient être profitables en contenant des aiguilles ou des fragments d'aiguille susceptibles de nous intéresser, ce qui nous aiderait dans notre mission » (cité Aradau 2015 : 1). Ces propos sont ceux de Iain Lobban, ancien directeur du GCHQ (service de renseignement britannique), qu'il a tenus en 2013 lors d'une audition publique au Parlement du Royaume-Uni à la suite des révélations d'Edward Snowden sur les pratiques de surveillance et de renseignement aux États-Unis et au-delà (Bauman et al. 2014, Lyon 2015). Cette citation est ici pertinente en ce qu'elle illustre la prégnance de cette métaphore de l'aiguille dans la botte de foin dans les discours touchant à la sécurité, en particulier pour justifier les activités de contrôle, de renseignement et de surveillance réalisées à l'aide d'instruments algorithmiques.

À cet égard, la détection des flux financiers illicites est régulièrement présentée comme étant « la recherche ultime de l'aiguille dans la botte de foin » (Conroy 2015). Au regard de leurs obligations légales de détection et de signalement des transactions financières suspectes (Amicelle et al. 2017), de nombreuses institutions financières - au Canada et ailleurs - sont aujourd'hui équipées d'instruments algorithmiques pour les aider à surveiller des dizaines voire des centaines de millions de transactions mensuelles et à faire face au déluge de données numériques qu'elles génèrent (de Goede 2012). En effet, confrontées à une véritable avalanche d'informations liées à ces millions d'opérations de leurs clients et relations d'affaires, ces institutions financières soumises aux règles anti-blanchiment et de lutte contre le financement du terrorisme n'ont d'autres choix que de se doter de ces nouvelles technologies fondées sur des algorithmes de détection.

2.2. Surveiller et détecter des individus et des comportements suspects à l'ère du big data

Le premier grand investissement technologique qui a été effectué dans le domaine du *policing* financier concerne des instruments algorithmiques automatisés pour explorer et filtrer les bases de données clients et les millions de transactions financières en fonction de seuils monétaires et de listes officielles de suspects. D'un côté, parmi les activités devant être signalées aux autorités étatiques sur la base de seuils monétaires, les banques ont recours à des logiciels afin de détecter et rapporter automatiquement les télévirements « d'une somme de 10 000 $ ou plus vers le Canada ou vers l'étranger en une seule ou plusieurs opérations totalisant 10 000 $ ou plus au cours d'une même période de 24 heures effectuées par une même personne ou en son nom » (Canafe 2018). À la lumière

des derniers chiffres disponibles, les autorités fédérales canadiennes – et plus précisément le Canafe : Centre d'analyse des opérations et déclarations financières du Canada, la cellule canadienne de renseignement financier – reçoivent annuellement plus de 13 millions de déclarations de télévirement (Canafe 2017a).

D'un autre côté, parmi les activités devant être signalées sur la base de sanctions et de listes nominatives officielles de suspects, les banques se sont équipés d'instruments automatisés pour filtrer (en fonction de ces listes de noms) leurs bases de données clients, leurs relations d'affaires et les transactions qu'elles gèrent. À titre d'exemple, l'obligation leur est faite de soumettre des déclarations de « biens appartenant à un groupe terroriste » lorsqu'elles savent ou ont de bonnes raisons de croire que des avoirs financiers sont liés à une organisation qualifiée de terroriste ou à une personne présente sur une liste officielle de suspects associés à des entités telles que les Talibans, Al-Qaïda ou encore l'État islamique.

Hormis cette première catégorie d'investissement technologique, les acteurs du *policing* financier se sont aussi et surtout dotés progressivement de nouvelles technologies de surveillance fondées sur différents types d'algorithmes pour détecter et signaler des « opérations douteuses », c'est-à-dire celles pour lesquelles il existe « des motifs raisonnables de soupçonner qu'une opération financière, qui a lieu ou qui est tentée, est en lien avec la perpétration, ou une tentative de perpétration, d'une infraction de blanchiment d'argent ou de financement d'activités terroristes. Contrairement aux autres types d'obligations en matière de déclaration, il n'y a pas de seuil monétaire pour la déclaration d'opération douteuse » (Canafe 2018).

L'implantation de ces instruments algorithmiques tend aujourd'hui à se généraliser et à transformer la portée et la systématicité de la surveillance et des contrôles effectués en matière de *policing* financier. Ainsi, en plus du filtrage technologique fondé sur des seuils monétaires et des listes officielles de suspects, chaque transaction financière des millions de clients d'une banque équipée d'une telle technologie fait l'objet d'une surveillance quotidienne dans le but de générer des alertes automatiques sur des opérations potentiellement suspectes. Ces alertes automatiques sont produites non pas en temps réel mais au cours de la nuit afin d'être prêtes pour l'analyse humaine dès le matin suivant. Concrètement, ces nouvelles technologies de contrôle et de surveillance reposent sur des algorithmes dits de détection de deux sortes.

2.3. Les formes de détection algorithmiques

Premièrement, la surveillance automatisée est effectuée à l'aide d'algorithmes de détection reposant sur des profils de comportements suspects pré-définis. Pour le dire autrement, l'objectif est de générer des alertes en découvrant des transactions qui correspondent à des scénarios pré-établis. Ces scénarios sont basés sur une combinaison d'indicateurs de soupçons provenant de sources internes et externes, à commencer par Canafe. Le Centre d'analyse des opérations et déclarations financières du Canada fournit

effectivement des indicateurs officiels « dans le but [d'] aider à déterminer si des opérations suscitent en vous des doutes raisonnables. Ces indicateurs, soit communs, soit sectoriels, peuvent s'avérer utiles au moment de juger si une opération, réelle ou tentée, est douteuse ou non. Ils ont été choisis parce qu'ils comportent certaines caractéristiques associées dans le passé à des activités de blanchiment d'argent ou de financement d'activités terroristes » (Canafe 2017b). Avant d'être intégré dans des algorithmes de détection automatique d'activités suspectes, ces indicateurs sont sélectionnés au sein des banques, combinés à d'autres et testés technologiquement pour s'assurer de leur pertinence.

Deuxièmement, la surveillance automatisée de la mobilité financière peut aussi être opérationnalisée à l'aide d'algorithmes de détection qui ne reposent pas sur des scénarios de comportements suspects pré-établis. Dans ce cas, la seconde façon de produire des alertes sur des profils de suspects est basée sur l'historique transactionnel du client ainsi que de son groupe de pairs (clients aux caractéristiques socio-démographiques et/ou aux comportements financiers jugés proches) et la manière dont une ou plusieurs de ses opérations financières dévient de cet historique transactionnel, du groupe de pairs et donc du comportement attendu. Ici, l'alerte automatique de soupçon est la résultante d'algorithmes produisant des profils comportementaux à partir de données individuelles et collectives de transactions et d'activités de comptes bancaires. De plus, des instruments algorithmiques complémentaires sont également utilisés en interne pour faire du *data mining* (exploration de données) et du *link analysis* (analyse de liens) dans les bases de données de la banque afin d'identifier des associations entre clients, comptes bancaires et transactions (transferts électroniques, dépôt d'argent liquide etc.). Cette approche automatisée en termes d'analyse de réseaux est généralement promue pour compléter l'analyse des transactions potentiellement douteuses et déjà détectées ou pour en découvrir de nouvelles. Les instruments algorithmiques de détection (et d'analyse de lien) d'activités douteuses ont finalement la possibilité d'être associés à d'autres analyses également opérationnalisées technologiquement à partir de données numériques non-structurées émanant de sources variées tels que des sites internet et des plateformes de médias sociaux. Cette mise en forme technologique du *policing* dans le monde financier n'est pas sans poser certaines difficultés, à l'instar de la question des faux-positifs.

2.4. Les algorithmes de détection à l'épreuve des faux-positifs

« 5% à 10% de toutes les alertes deviennent des cas d'investigation. Ainsi, 90% à 95% des alertes sont des faux-positifs. Et ensuite, un cas d'investigation qui débouche sur une déclaration d'opération douteuse, c'est moins de 10%... » (entretien réalisé par l'auteur de ce chapitre avec un agent de conformité anti-blanchiment, 2016). Selon ce directeur de l'unité anti-blanchiment d'une grande banque canadienne, c'est au mieux une alerte sur 100 qui donne lieu à un signalement aux autorités étatiques et ce, pour une institution financière qui en envoie des milliers par an. À l'instar du *policing* financier, la question du nombre très (trop) élevé de faux-positifs constitue une des questions centrales dans les pratiques de contrôle et de surveillance réalisées à l'aide de nouvelles technologies et

d'algorithmes de détection fonctionnant sur de grandes masses de données (Benbouzid 2018a).

Dans le cas des banques, une des tâches professionnelles parmi les plus chronophages et coûteuses est celle consistant à « trier » les alertes, de quelques dizaines de milliers à plusieurs millions annuellement pour les plus grandes organisations. La diminution du taux de faux-positif devient dès lors une priorité qui demeure difficile à atteindre de façon satisfaisante avec des enjeux qui transcendent largement le seul cas du *policing* financier : « Cela reste un gros enjeu, il y a beaucoup de faux-positifs, et il y a toujours un équilibre à trouver entre investir pour améliorer ce système [algorithmique] au regard des ressources disponibles, versus passer au travers des faux-positifs et consacrer beaucoup du temps à le faire, donc c'est un enjeu et cela va continuer à l'être. Dans tous les cas, il y aura toujours des faux positifs mais leur volume global, l'objectif est de le réduire à un niveau raisonnable et obtenir davantage d'alertes pertinentes » (entretien réalisé par l'auteur de ce chapitre avec un agent de conformité anti-blanchiment, 2017).

Au regard des dynamiques d'utilisation et d'appropriation des nouvelles technologies et des algorithmes de détection, il va sans dire que les alertes n'apparaissent pas simplement « par magie ». Elles sont le résultat de multiples décisions humaines et d'arrangements sociotechniques préalables. Comme dans bien d'autres configurations actuelles de *policing*, la capacité à produire des alertes de soupçons émerge des relations entretenues entre une série d'équipements technologiques et d'acteurs sociaux allant des créateurs de ces technologies jusqu'à leurs utilisateurs finaux. Dans ce cadre, alors que les caractéristiques (techniques, logiques, cognitives) propres aux technologies permettent et contraignent simultanément l'action de leurs utilisateurs, il est crucial d'insister sur l'importance du processus de paramétrage de ces instruments. Celui-ci dépend en grande partie du degré d'autonomie des institutions équipées vis-à-vis des fournisseurs de technologies, et ceci s'applique aussi bien aux banques qu'aux services de police.

En effet, dans certains cas de figure, les instruments algorithmiques demeurent à l'état de boîtes noires pour leurs utilisateurs, avec très peu de prise pour les paramétrer un tant soit peu en interne sans faire systématiquement appel aux fournisseurs. « Le problème lié au fait de modifier les algorithmes est qu'à chaque fois vous devez faire affaire au vendeur [de la technologie], cela implique des coûts et notre organisation n'est pas prête à payer davantage […]. Et c'est la manière dont le modèle technologique [des fournisseurs] est pensé. Il est pensé pour qu'à partir du moment où vous devenez client, c'est le moment où ils commencent à vous charger des extras car ils savent que vous ne pouvez plus aller voir ailleurs. Et mettre en place un nouveau système technologique c'est très coûteux, particulièrement quand vous avez vraiment besoin de mises à jour car la technologie évolue. Une fois que vous avez décidé de vous engager avec un fournisseur, il y a de fortes chances que vous y restiez sauf en cas de force majeure » (entretien réalisé par l'auteur de ce chapitre avec un agent de conformité anti-blanchiment, 2016).

Dans d'autres cas de figure, les utilisateurs disposent d'une autonomie relative et d'une capacité à mener des opérations de paramétrage sur les algorithmes, ce qui nécessite toutefois des ressources humaines dédiées à l'interne. « Nos personnes TI, c'est chez eux qu'on précise les règles, les scénarios et les seuils [des algorithmes] pour des types d'alertes qui pourraient permettre de donner des cas d'activités suspectes. Ce sont donc eux qui programment nos règles de surveillance, nos algorithmes » (entretien réalisé par l'auteur de ce chapitre avec un agent de conformité anti-blanchiment, 2017). Des personnes disposant de maîtrises ou de PhD en science des données sont ainsi recrutées pour affiner la surveillance automatisée, fondée sur des algorithmes de détection modifiables. Dans un cas de figure comme dans l'autre, la réduction du nombre de faux-positifs tend à devenir une fin en soi.

3. PredPol et l'exemple des algorithmes de prédiction

« Reconnaître des personnes, des objets ou des formes dans des images, classer les pages du web avec un moteur de recherche en fonction des recherches passées de l'utilisateur, recommander un bien culturel, un trajet ou un amant, trier les spams, personnaliser une publicité, etc. Les calculs des services numériques empruntent de plus en plus une forme prédictive s'appuyant sur des méthodes d'apprentissage statistique (*machine learning*). Mais au-delà les mondes numériques *stricto sensu*, la prédiction calculée devient aussi, dans la police, l'assurance, la gestion des entreprises, la surveillance, la justice, l'attribution de crédits et certaines politiques publiques, une technologie de plus en plus fréquemment mobilisée pour promettre la modernisation des services tout en installant un nouveau régime d'anticipation des événements. Technique de calcul profitant du développement des données massives, la prédiction constitue aussi un principe d'intervention inédit dans et sur la société. Sur la base de régularités observées, ces dispositifs calculatoires rationalisent le futur en le rendant disponible à des formes d'action préventives » (Benbouzid et al. 2018 : 12).

3.1. Les spécificités (à nuancer) du « predictive policing »

Alors que différents types d'algorithmes occupent désormais « dans tous les champs de la vie quotidienne une place de plus en plus importante » (Galie-Blanze 2018 : 7), les algorithmes dits de prédiction ont été parmi les plus investis au cours des dernières années pour traiter des données massives, y compris dans le domaine policier avec le développement du « *predictive policing* » (Perry 2013). Cette tendance de fond est particulièrement notable aux États-Unis où des services de police se sont équipés de logiciels et de plateformes d'analyse d'un nouveau genre – « sous la forme de cartographie prédictive et de tableau analytique » (Benbouzid 2018a : 223) – censés contribuer à prédire où et quand les crimes et délits vont avoir lieu (Uchida 2014, Police Executive Research Forum 2014).

Ainsi, le terme de « *predictive policing* » fait référence à toute une série d'instruments analytiques et de pratiques policières ayant pour finalité commune affichée d'user des données massives disponibles et des algorithmes d'apprentissage automatique (*machine learning*) à des fins de prédiction policière. Dans cette perspective, le phénomène de *predictive policing* ne saurait être réduit à de simples instruments socio-techniques dans la mesure où il renvoie aussi et surtout à la défense du postulat selon lequel il est possible d'avoir recours à la technologie pour prédire avec précision la criminalité avant qu'elle ne survienne et ce, afin que ce savoir prédictif puisse être mis au service de la réduction du crime par les forces de police (van Brakel et al. 2011).

« Aux États-Unis, la police prédictive s'inscrit dans un projet ancien de réforme de la police *par la recherche* (Walker 2014) qui vise à créer une police de proaction, plus préventive qu'urgentiste, qui intervient de son propre chef, sans être mobilisée par l'appel des citoyens (Jobard et al. 2015) » (Benbouzid 2017 : 97). Aussi nouveau et inédit qu'il puisse être présenté, le phénomène du predictive policing doit être resitué dans la lignée d'autres approches et réformes policières telles que « l'*intelligence-led policing*, le *data-driven policing*, le *risk-based policing*, le *hot spot policing*, l'*evidence-based policing* et le *premptive-policing* » (Bennett Moses et al. 2018 : 808, Sherman et al. 1989, Eck et al. 1995, Lum et al. 2011, Ratcliffe 2016). Pour autant, malgré des ressemblances et des continuités apparentes, des différences existent bel et bien.

Lyria Bennet Moses et Janet Chan montrent par exemple qu'une différence majeure persiste entre le *data-driven policing* ainsi que le *hot spot policing* d'un côté et le principe du *predictive policing* de l'autre dans la mesure où ce dernier renvoie à une projection explicite vers le futur. « Plutôt que d'assumer une continuité dans les tendances actuelles de criminalité et de *hot spots*, le *predictive policing* modèle explicitement le changement dans le temps, s'appuyant souvent sur la preuve d'un impact géographique statistiquement plus large d'un seul événement criminel » (Bennett Moses et al. 2018 : 808). Sur un autre plan, ces auteures soulignent que le *predictive policing* diffère du *pre-emptive policing* qui, tout en étant aussi tourné vers le futur et le fait d'agir avant l'occurrence d'un événement donné, n'est pas nécessairement fondé sur des prévisions orientées par le traitement de données massives. Si ces variations sont importantes à relever pour saisir la spécificité du *predictive policing*, elles ne doivent encore une fois pas masquer certaines continuités entre ces différents types de *policing* qui s'inscrivent tous dans une évolution plus générale des « stratégies et des technologies de *policing* qui renforcent le rôle du renseignement au sein des agences d'application de la loi » (Bennett Moses et al. 2018 : 808).

3.2. Retour sur le lancement commercial et les promesses du logiciel PredPol

« PredPol a une définition précise du *predictive policing*. Pour nous et nos clients, c'est une pratique consistant à identifier les moments et les lieux où des crimes spécifiques sont le plus susceptibles de se produire, puis de patrouiller dans ces zones pour empêcher ces

crimes d'advenir. Pour le dire simplement, notre mission est d'aider les forces de l'ordre à garder les collectivités en sécurité en réduisant la victimisation » (Predpol 2018).

De par son nom et sa position actuelle de leader sur le marché des technologies de localisation prédictive des crimes, la compagnie PredPol symbolise aujourd'hui plus que toute autre le phénomène du *predictive policing*. Cette start-up a lancé la première version de sa plateforme d'analyse en 2012 après deux années de recherches initiales. Commercialisée sous la forme d'une simple application téléchargeable (sur ordinateur, cellulaire ou tablette) avec les données stockées en infonuagique, cette plateforme – régulièrement mise à jour au cours des dernières années – se présente dès le début comme un « tableau de bord diffusant en temps réel les risques d'occurrence des crimes avec une précision de l'ordre de 200 mètres » (Benbouzid 2017). En cela, PredPol se démarque immédiatement des produits alors concurrents dans le domaine de la cartographie criminelle qui eux se présentaient sous la forme d'installation logiciel sur les ordinateurs de bureau ou l'intranet des services de police.

Au-delà de la forme, la stratégie de lancement (réussi) du produit de PredPol a reposé sur deux autres piliers, à savoir un slogan publicitaire accrocheur pour les dirigeants policiers (*More than Hot Spot tools*) et un « mythe fondateur » (Benbouzid 2016). Tant le slogan que le mythe fondateur ont trait à l'originalité de l'algorithme utilisé par PredPol, à savoir le recours à un modèle de prédiction des séismes pour cette fois-ci prédire le crime. « En matière de crime, il en irait comme pour les séismes : s'il est difficile de prédire l'occurrence d'un premier événement, il est possible d'en prédire les répétitions. PredPol intègrerait ainsi dans son algorithme la dimension contagieuse de la diffusion du crime dans l'espace et dans le temps, d'où le slogan *More Than Hot Spot*. L'idée de la contagion du crime n'est pas nouvelle et ne vient pas de la sismologie. Elle date des années 1980 avec les premières recherches en criminologie autour de la notion de « *repeat victimization* ». Mais sur le plan marketing, la métaphore sismologique a un avantage sur l'explication criminologique : elle fait référence au couplage d'une science dure avec les techniques prédictives des *big data*. Ce marketing scientiste va envoyer un message simple, mais très efficace : « nous avons fait une découverte, le crime serait fongible dans les mathématiques ; nous avons enfin trouvé la solution au problème sur lequel butent l'analyse criminelle depuis des années ». Le succès de Predpol tient en grande partie à ce mythe fondateur, coproduit par la presse et les responsables du marketing, qui présente la start-up comme la contribution de la « vraie science » à la lutte contre le crime » (Benbouzid 2016 : 2).

PredPol a tout de suite bénéficié d'une couverture médiatique largement favorable s'appuyant notamment sur des retours positifs émanant des premières forces de police à s'être équipées. Cette tonalité positive initiale à l'aune de la satisfaction systématique des premiers clients de PredPol a cependant été tempérée à la suite de la révélation d'un document contractuel confidentiel tendant à démontrer que ces clients, comme la police de Modesto, s'étaient engagées à contribuer aux activités promotionnelles de la start-up de Santa Cruz en échange de ristourne sur le coût du logiciel (Benbouzid 2016, Bond-

Graham et al. 2013, Cushing 2013). De plus, les sources rapportant des baisses substantielles de la criminalité ou tout du moins de certaines catégories de crime liées directement au logiciel PredPol n'étaient basées sur aucune preuve ou sans aucune référence à des évaluations publiées ; très peu d'évaluations formelles de technologies de *predictive policing* ont d'ailleurs été menées (Bennett Moses et al. 2018).

Cette absence relative d'évaluation indépendante et publique s'explique en grande partie par le manque de transparence inhérent aux algorithmes de prédiction policière qui, en tant que produits mis en marché, tombent généralement sous le sceau du secret commercial, à commencer par leur code source. La complexité du fonctionnement des algorithmes d'apprentissage automatique peut également être en soi une source d'opacité. Cet élément de complexité indéniable associé au caractère restreint des informations disponibles limite ainsi la capacité des experts indépendants à se prononcer sur les résultats et la performance de ces logiciels, ce qui n'est d'ailleurs pas sans poser question en termes de responsabilité et d'imputabilité des décisions policières prises à partir des algorithmes prédictifs (Bennett Moses et al. 2018, Pasquale 2015). Si la plateforme d'analyse prédictive commercialisée par PredPol n'échappe pas à ces controverses sur la transparence processuelle et l'imputabilité décisionnelle, elle s'avère toutefois plus ouverte que d'autres à l'analyse critique.

3.3. Entre critiques d'efficacité prédictive et de justice sociale

« Comment dès lors évaluer le logiciel, puisque PredPol empêche l'accès au code source ? » (Benbouzid 2016). Dans une démarche originale de questionnement scientifique du logiciel de PredPol, le sociologue spécialiste des machines prédictive Bilel Benbouzid s'est tourné vers le sismologue David Marsan, professeur à l'Université de Chambéry en France et expert international dans l'étude des répliques de tremblements de terre (ibid., 2017). Celui-ci a en effet mis au point l'algorithme de prédiction (sismique) ayant fortement inspiré PredPol comme l'ont d'ailleurs revendiqué publiquement les représentants de la start-up. En collaboration avec le sociologue, David Marsan a accepté de tester son algorithme en utilisant les données de la ville de Chicago, notamment sur la catégorie criminelle des cambriolages. Ses conclusions, critiques, méritent d'être relevées, en voici le résumé ci-dessous :

« David Marsan montre tout d'abord que l'algorithme ne fait guère plus que du *hotspot mapping*. Pour comprendre cette remarque, il faut expliquer que l'algorithme de Predpol calcule l'intensité du risque en fonction de l'espace et du temps en additionnant deux éléments : la part de la concentration et celle de la contagion. La note de David Marsan indique que la contribution de la contagion dans la réalisation du processus existe, mais qu'elle est extrêmement faible. Elle est même négligeable. Ensuite, David Marsan pose le problème de l'absence de stationnarité qui signifie que la structure du processus sous-jacent évolue avec le temps (le crime peut évoluer suivant un processus auto-excitatif en 2013 et d'une autre manière en 2014). Pour le dire autrement, le crime n'a pas la même structure sous-jacente d'une année sur l'autre. Cette absence de stationnarité tient à

l'interaction complexe entre le phénomène lui-même (le cambriolage) et des forces externes (le travail de la police notamment). Ceci faite une grande différence avec l'activité sismologique, dont la structure sous-jacente au XXe siècle est équivalente à celle du XXIe siècle. En toute rigueur, cette absence de stationnarité empêche d'appréhender le phénomène de manière standard, à partir d'un « processus ponctuel auto-excitatif », commercialisable à l'infini. Les phénomènes non stationnaires impliquent de mobiliser d'autres méthodes et d'intégrer des variables externes dans le processus d'apprentissage statistique. Les scientifiques qui ont œuvré au développement de Predpol connaissent évidemment ces limites, qu'ils considèrent comme des questions encore ouvertes (cf. l'article que les chercheurs de la start-up ont spécialement consacré à ce problème, sans qu'ils aient pour autant pu le résoudre entièrement). Les contraintes marketing dans lesquels les chercheurs actionnaires sont pris les empêchent de mettre en avant ces questions, qui sont pourtant cruciales pour que puisse se tenir un débat public sur la commercialisation d'un produit destiné à être utilisé par un service public. Si l'intérêt de Predpol devait être discuté seulement à l'aune son algorithme, la start-up n'aurait pas lieu d'être » (Benbouzid 2016). La question de la réelle pertinence prédictive du logiciel PredPol est ici clairement posée tout en ouvrant celle de son impact plus général au sein de la société.

Si Predpol a pu faire l'objet de critiques récurrentes pointant les risques de discriminations associés à son algorithme de prédiction, les représentants s'en sont toujours défendus en insistant sur le type de données mobilisé pour alimenter leur plateforme d'analyse. « Le type de données que nous utilisons pour nos prédictions est très important. Nous faisons nos prédictions uniquement sur les bases des informations de victimisation, c'est-à-dire les crimes qui ont été signalés à la police » (Predpol 2018). L'algorithme et les analyses qui en découlent ne reposent pas sur les données d'arrestations policières pour éviter de simplement reproduire de manière circulaire l'activité policière, au risque de tomber dans un biais discriminatoire, mais sur les données relatives aux plaintes des victimes. Ce choix et cette réponse apportés par les dirigeants de la compagnie ne sont toutefois pas sans poser problème en ce qu'ils reposent sur un postulat contestable, celui de l'adéquation des données recueillies avec la réalité criminelle. Il s'agit là d'un point bien connu en criminologie, celui de l'écart systémique entre les crimes commis et les crimes rapportés en fonction de différents éléments telles que le type de crime, leur visibilité, les caractéristiques des victimes, leur rapport à la police, etc. (Robert 1977). Ces éléments sont généralement résumés au processus de reportabilité : « [e]ntre la commission d'un acte criminalisable, sa connaissance et sa reconnaissance ultérieure par le système pénal s'intercale un mécanisme intermédiaire complexe, aux multiples facettes, la reportabilité » (Cousineau 1996 : 2).

Les travaux sur la reportabilité ont montré que le renvoi vers la police n'est pas automatique ni distribué de manière homogène au sein de la population, souvent selon la position sociale des victimes et la façon dont elles perçoivent le crime commis ainsi que l'action policière et pénale Dès lors, l'enjeu de justice sociale soulevé par les données alimentant l'algorithme de PredPol est que ce dernier oriente l'action policière vers les

catégories de population qui se tournent formellement vers les autorités. Or, comme l'indique Benbouzid (2016 : 7), « les non-signalements sont des phénomènes sociaux en tant que tels, qui échappent complètement à l'apprentissage statistiques par les données enregistrées par la police. En n'ajustant pas le calcul de l'intensité du risque en fonction de ce taux de non-signalements, l'algorithme de Predpol produit un biais qui peut avoir des impacts sociaux graves : il peut recommander de concentrer l'offre de sécurité sur une partie de la population, au détriment des personnes dont la participation active à la préservation de la qualité de vie de leur quartier est la plus faible. Le problème de l'algorithme de Predpol n'est pas la discrimination policière, comme beaucoup ont pu le craindre, mais celui de l'exclusion d'une partie de la population de l'offre de sécurité publique. Autrement dit, sur le temps long, le strict suivi des recommandations de l'algorithme de Predpol pourrait creuser les inégalités d'accès à la sécurité. C'est à ce prisme qu'il faudrait évaluer la fiabilité des modèles de Predpol ».

3.4. Une finalité gestionnaire ?

Au regard des critiques formulées, il semble que le rôle réel des algorithmes de prédiction comme celui de PredPol se situent finalement moins dans leur dimension prédictive en tant que telle que dans leur dimension de gestion managériale des agents de police, de plus en plus mise en avant par PredPol et sollicitée par les chefs des polices équipées. Dans une de ses dernières publications, Bilel Benbouzid précise que PredPol ne cesse d'innover pour « permettre aux gestionnaires de s'assurer que les officiers, durant leur temps de patrouille font le travail escompté au regard des objectifs de production élaborés au niveau supérieur. Pour ce faire, elle imagine la plateforme […] comme un « tableau de bord » qui permette de contrôler en *temps réel* cette production sous la forme de quantité de travail réalisé par les agents de police sur le terrain. Pour mettre les policiers sous la pression du temps réel, il faut une plateforme de *stream computing* permettant de traiter des flux de données « au fil de l'eau » afin d'enregistrer les trajets des patrouilles. Pour ce faire, PredPol intègre les données des systèmes de suivi GPS placés dans les voitures de police, ce qui permet de suivre les officiers à la trace et de contrôler le temps de la présence des patrouilles selon les secteurs de la ville. Pour organiser la distribution des patrouilles dans l'espace et le temps, les développeurs de PredPol vont proposer un usage astucieux des résultats de leur recherche : ils ont découvert que les patrouilles de police atteignent un niveau d'efficacité suffisant en passant seulement 5 % de leur temps de travail dans les zones identifiées par l'algorithme. Ces résultats sont précieux, car ils permettent de contrôler avec précision le *dosage* des patrouilles, tout en mobilisant *a minima* la part proactive de l'activité policière » (Benbouzid 2018b). Rappelant l'imposition de quotas (sans en être) et de « mise en responsabilité policière » à la manière de dispositifs de management quantitatif tels que *Compstat* (ibid., Didier 2011), cette logique de dosage et d'encadrement de la proactivité policière suppose cependant que les policiers de terrain se conforment passivement voire aveuglément à ces stratégies d'intervention basées sur l'analyse prédictive.

Comme le rappelle à juste titre certains auteurs (Aust et al. 2010), la mise en œuvre dépend beaucoup du degré d'inclusion, d'intérêt, d'enthousiasme et du niveau de confiance des policiers de terrain vis-à-vis de ce qui leur est dit et demandé. « Parfois les policiers ont un savoir qui n'est pas capturé par les données (comme quand ils savent que les données qu'ils ont eux-mêmes entrées dans le système sont erronées ou incomplètes) et peuvent donc être moins enclins à faire confiance aux prévisions ou aux analystes » (Bennett Moses et al. 2016 : 814, Cope 2004). Plus généralement, c'est la question du processus d'appropriation des technologies par les policiers qui est ici posée et sur laquelle il convient de revenir dans la section conclusive de ce chapitre.

4. Propos conclusifs sur les processus crucial d'appropriation des technologies

Dans cette dernière section, il convient de replacer les instruments algorithmiques dans le cadre plus général des technologies en insistant à nouveau sur le fait que les objectifs fixés par les responsables politiques et/ou les supérieurs hiérarchiques ainsi que les préconisations des fournisseurs de technologies n'englobent jamais l'ensemble des effets des technologies dont la force d'action se développe seulement pleinement au contact des acteurs qui les utilisent (Lascoumes et al. 2011). Bien que ces acteurs n'aient souvent pas d'autres choix que de faire avec les technologies qu'on leur demande d'utiliser, il n'en reste pas moins que leur manière d'en faire usage n'est ni passive ni entièrement guidée par des règles pré-établies. Le moment de l'utilisation des nouvelles technologies doit aussi être abordé comme un moment de créativité, au même titre que le moment de production de ces technologies.

Dans cette perspective, prêter une attention accrue aux formes de relations entretenues entre un instrument technologique et ses utilisateurs est central car ces relations renvoient toujours à un processus d'appropriation dynamique. Cette idée fondamentale d'appropriation fait effectivement référence à un « processus dynamique de dialogue et de réflexion entre un objet et un espace d'activités produisant des usages, soit routiniers, soit innovants » (Crespin et al. 2000 : 134). Ainsi, l'enjeu n'est pas de savoir si la technologie détermine les pratiques de ses utilisateurs ou si ces derniers l'instrumentalisent mais plutôt de saisir comment cette relation technologie-utilisateurs déterminent ses termes. Comme l'ont déjà montré plusieurs chercheurs dans le domaine policier, l'appropriation ou la réappropriation des technologies peut s'avérer être si décisive que certaines d'entre elles en viennent à être utilisées quotidiennement comme des technologies de police et de sécurité alors qu'elles n'ont pas été produites, achetées ni même validées à cet effet, à l'instar de l'utilisation policière non-prévue des téléphones portables personnels (Tanner et al. 2015). Un ensemble de contraintes vécues par les agents de terrain stimulent des formes de ré-utilisation de biens de consommation banaux au point que ceux-ci deviennent *de facto* des technologies de police et de sécurité au gré des situations rencontrées. Samuel Tanner et Michaël Meyer mettent ainsi en évidence la créativité quotidienne des policiers de terrain en tant que consommateurs-producteurs de technologies de sécurité.

De plus, les formes d'appropriation ou de domestication (Aas et al. 2009) de ces technologies sont souvent couplées à différents types d'opposition ou de résistance peu visibles à ces mêmes technologies. Par exemple, les cas d'opposition de l'opinion publique à certains instruments tels que de nouvelles bases de données policières représentent probablement un type de contestation plus visible que les formes de réticence voire de résistance plus informelles des utilisateurs supposés de ces technologies (Gilliom et al. 2012). En effet, les contestations publiques de certaines technologies de sécurité ont généralement lieu à l'initiative de groupes de mobilisation ou de personnes qui sont rarement les utilisateurs finaux de ces technologies (Linhardt 200, Bennett 2008). Néanmoins, ces utilisateurs peuvent aussi exercer une influence pour modifier, changer ou abandonner un instrument technologique. Ceci renvoie généralement à des opérations à faible visibilité mais à fort impact telles que des « activités de contournement, de détournement et de neutralisation des instruments, notamment lorsque l'instrument est plus ou moins obligatoire, donc incontournable. Le contournement est un évitement radical ; le détournement est une forme d'appropriation et de réinterprétation qui peut être assimilée à une résistance, généralement de la part des agents chargés de sa mise en œuvre, qui s'en saisissent pour l'asservir à leurs propres fins ; la neutralisation est une appropriation de surface, une simulation d'usage, lorsque l'évitement est rendu impossible » (Lascoume et Le Bouhris 2014 : 507).

De nombreux travaux ont ainsi mis en évidence les marges de manœuvre dont disposent les policiers et autres acteurs de la sécurité pour s'approprier des technologies, à commencer par les nouvelles technologies de l'information et de la communication (Ackroyd et al. 1992, Orlikowski 1996, Ericson et al. 1997). Les agents de terrain ne sont ni totalement subordonnés ni totalement indépendants dans leurs rapports aux technologies. Dans ce cadre, il est important de garder en tête que les nouvelles technologies ne contribuent pas uniquement à réorganiser les relations entre les représentants de l'autorité étatique et les citoyens. Leur introduction a également des conséquences au sein d'une organisation hiérarchique telle qu'un service de police. D'un côté, les technologies sont « travaillées » par les policiers et autres professionnels de la sécurité ainsi que par les organisations auxquelles appartiennent ces derniers. De l'autre, ces technologies, et notamment les nouvelles technologies de l'information et de la communication, ont pu dans le passé récent « déstabiliser des équilibres de pouvoir entre des segments organisationnels en altérant les habitudes de communication, les rôles de chacun dans les relations professionnelles, la division du travail, les formats établis de communication organisationnels, et les différentes routines prises pour acquis » (Manning 1996 : 54).

Tenir compte des processus d'appropriation des nouvelles technologies est crucial pour être en mesure de (mieux) comprendre les pratiques de *policing* et de sécurité. Les politiques de sécurité et les activités de *policing* existent concrètement au travers de ce que les agents de terrain font. Dans ce cadre, l'appropriation des technologies ne renvoie pas seulement à une forme plus ou moins satisfaisante de mise en œuvre de décisions politiques et/ou hiérarchiques pré-existantes. À l'heure actuelle, l'appropriation des

nouvelles technologies, et notamment des instruments algorithmiques à l'ère du *big data*, constituent aussi et surtout une dimension à part entière du processus quotidien de production de sécurité.

Références

Aas, K. F., Gundhus, H. O. and Lomell, H. M. (eds.) (2009), *Technologies of InSecurity: The Surveillance of Everyday Life*, Routledge, New York.

Ackroyd, S., Harper, J. A. and Hugues, D. (1992), *New Technology and Practical Police Work*, Open University Press, Buckingham.

Amicelle, A. (2018), Policing through misunderstanding: insights from the configuration of financial policing, *Crime, Law and Social Change*, 69 (2) : 207-226.

Amicelle, A. and Iafolla, V. (2017), *Reporting Suspicion in Canada: Insights from the Fight against Money Laundering and Terrorist Financing*, *TSAS*, Ottawa.

Amoore, L., Marmura, S., Salter, B. and Mark, B. (2008), Smart Borders and Mobilities: Spaces, Zones,Enclosures, *Surveillance & Society*, 5 (2) : 96-101.

Amoore, L. and Piotukh, V. (2015), Life beyond big data: governing with little analytics, *Economy and Society*, 44: 3 : 341-366.

Amoore, L. and Raley, R. (2017), Securing with algorithms : Knowledge, decision, Sovereignty, *Security Dialogue*, 48 : 3-10.

Andrejevic, M. and Gates, K. (2014), Editorial. Big data surveillance : Introduction, *Surveillance & Society*, 12 (2) : 185-196.

Aradau, C. (2015), The signature of security: Big data, anticipation, surveillance, *Radical Philosophy*, 191 : 1-8.

Aradau, C. and Blanke, T. (2015), The (big) data-security assemblage : Knowledge and critique, *Big Data & Society*, 2 (2).

Aradau, C. and Blanke, T. (2017), Politics of prediction : security and the time/space of governmentality in the age of big data, *European Journal of Social Theory*, 20 (3) : 373-391.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R. B. J. (2014), After Snowden: Rethinking the impact of surveillance, International Political Sociology, 8 (2) : 121-144.

Benbouzid, B. (2016), À qui profite le crime ? Le marché de la prédiction du crime aux États-Unis, *La vie des idées*, accessible en ligne à : https://laviedesidees.fr/A-qui-profite-le-crime.html

Benbouzid, B. (2017), Des crimes et des séismes. La police prédictive entre science, technique et divination, *Réseaux*, 6 (206) : 95-123.

Benbouzid, B. (2018a), Algorithmes prédictifs et droit des algorithmes : contrôler la qualité de faux positifs moralement acceptables, *revue de la gendarmerie nationale*, 261 : 14-18.

Benbouzid, B. (2018b), Quand prédire, c'est gérer. La police prédictive aux Etats-Unis, *Réseaux*, 5 (211) : 221-256.

Benbouzid, B. et Cardon, D. (2018), Machine à prédire, *Réseaux*, 5 (211) : 9-33.

Bennett, C. (2008), *The Privacy Advocates: Resisting the Spread of Surveillance*, MIT Press : Boston, MA.

Bennett Moses, L. and Chan, J. (2018), Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 28:7.

Bond-Graham, D. and Winston, A. (2013), All tomorrow's crimes: The future of policing looks a lot like good branding [online], SF Weekly, accessible en ligne à http://www.sfweekly.com/news/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/

Boyd, D. and Crawford, K. (2012), Critical question for big data, *Information, Communication & Society*, 15 (5) : 662-679.

Campbell-Verduyn, M., Goguen, M. and Porter, T. (2017), Big data and algorithmic governance : the case of financial practices, *New Political Economy*, 22 (2).

Canafe (2017a), *Rapport annuel*, Ottawa.

Canafe (2017b), Ligne directrice 2 : Opérations douteuses, accessible en ligne à : http://fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-fra.asp

Canafe (2018), Opérations financières qui doivent être déclarées, accessible en ligne à : http://www.canafe-fintrac.gc.ca/reporting-declaration/rpt-fra.asp

Cardon, D. (2015), *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Le Seuil, Paris.

Ceyhan, A. (2008), Technologization of security: Management of uncertainty and risk in the age of biometrics, *Surveillance & Society*, 5 (2): 102-123.

Chan, J. (2001), The technological game: How information technology is transforming police practice, *Criminal* Justice, 1 (2): 139-159.

Conroy, J. (2015), Global AML vendor evaluation : Managing rapidly escalating risk, AITE.

Cope, N. (2004), Intelligence led policing or policing led intelligence?: Integrating volume crime analysis into policing, *British journal of criminology*, 44 (2) : 188–203.

Cousineau, M-M. (1996), De la naissance d'une affaire pénale, *Revue du Grapp*, 1 (1) : 1-17.

Crespin, R. et Lascoumes, P. (2000), Régulation de la carrière d'un instrument de santé, *Sociologie du travail*, 42: 133-157.

Cukier, K., and Mayer-Schönberger, V. (2013), *Big data. A revolution that will transform how we live, think and work*, John Murray, London.

Cushing, T. (2013), 'Predictive policing' company uses bad stats, contractually-obligated shills to tout unproven 'successes' [online], Techdirt, accessible en ligne à https://www.techdirt.com/articles/20131031/13033125091/predictive-policing-company-uses-bad-stats-contractually-obligated-shills-to-tout-unproven-successes.shtml

De Goede, M. (2012), *Speculative security. The politics of pursuing terrorist monies*, University of Minnesota Press, Minnesota.

Didier, E. (2011), Compstat à Paris : initiative et mise en responsabilité policière », *Champ pénal/Penal field*, VIII.

Eck, J. E. and Weisburg, D. (1995), *Crime and place*, Criminal Justice Press, New York.

Ericson, R. and Haggerty, K. (1997), *Policing the Risk Society*, Oxford University Press, Oxford.

Galie-Blanze, M. (2018), Algorithmes et protection des données personnelles, *revue de la gendarmerie nationale*, 261 : 5-13.

Gilliom, J. and Monahan, T. (2012), Everyday surveillance, in K. Ball, K. Haggerty and D. Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, pp. 405-411.

Halpern, C., Lascoumes, P. et Le Galès, P. (2014), L'instrumentation et ses effets. Débats et mises en perspective théoriques, in C. Halpern, P. Lascoumes et P. Le Galès (dir.), *L'instrument de l'action publique. Controverses, résistance, effets*, Presses de Sciences Po, Paris, pp. 15-59.

Hannam, K., Sheller, M. and Urry, J. (2006), Editorial: Mobilities, immobilities and moorings, *Mobilities*, 1 (1) : 1-22.

Huysmans, J. (2014), *Security Unbound. Enacting Democratic Limits*, Routledge, London.

Kelling, K. (1996), Defining the bottom line in policing: Organizational philosophy and accountability, in L. T. Hoover (ed.), *Quantifying Quality in Policing*, Police Executive Research Forum, Washington, DC, pp. 23–36.

Jobard F. et de Maillard (2015), *Sociologie de la police. Politiques, organisations, réformes*, Armand Colin, Paris.

Lascoumes, P. et Le Bourhis, J-P. (2014), Les résistances aux instruments de gouvernement. Essai d'inventaire et de typologie des pratiques, in C. Halpern, P. Lascoumes et P. Le Galès (dir.), *L'instrument de l'action publique. Controverses, résistance, effets*, Presses de Sciences Po, Paris, pp. 493–515.

Lascoumes, P. et Simard, L. (2011), L'action publique au prisme de ses instruments, *Revue française de science politique*, 61 (1): 5–22.

Linhardt, D. (2005), La 'question informationnelle': Éléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France (années 1970 et 1980), *Déviance et société*, 29 (3): 259-272.

Lum, C., Koper, C.S., and Telep, C.W. (2011), The evidence-based policing matrix, *Journal of experimental criminology*, 7 (3) : 3-26.

Lyon, D. (2016), Big data surveillance. Snowden, everyday practices and digital futures, in T. Basaran, D. Bigo, E-P. Guittet and R. B. J. Walker (eds.), *International political sociology : Transversal Lines*, Routledge, New York, pp. 254-271.

Lyon, D. (2015) *Surveillance after Snowden*, Polity Press, Cambridge.

Manning, P. K. (1996), Information technology in the police context: The 'sailor' phone, *Informations Systems Research*, 7 (1): 52-62.

Nix, J. (2015), Predictive policing, in R. Dunham and G. Alpert (eds.), *Critical issues in policing : contemporary readings* (7th edition), Waveland Press, Long Grove, pp. 275-288.

Orlikowski, W. J. (1996), Improvising organizational transformation over time: A situated change perspective, *Information Systems Research*, 7 (1): 63-92.

Pasquale, F. (2015), *The black box society: the secret algorithms that control money and information*. Harvard University Press, Cambridge, MA.

Perry W. L. (2013), *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, Rand Corporation.

Police Executive Research Forum (2014), *Future trends in policing*, Office of Community Oriented Policing Services, Washington, DC.

PredPol (2018), PredPol Overview, accessible en ligne à : http://www.predpol.com/about/

Purenne, A. et Aust, J. (2010), Piloter la police par les indicateurs ?, *Déviance et Société*, 34 (1) : 7-28.

Ratcliffe, J. H. (2016), *Intelligence-led policing*, Routledge, New York.

Robert, P. (1977), Les statistiques criminelles et la recherche, *Déviance et Société*, 1 (1) : 3-27.

Rouvroy, A 2016, Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives. VOL. T-PD-BUR(2015)09REV, T-PD-BUR(2015)09REV edn, Conseil de l'Europe, Strasbourg.

Shapiro, A. (2017), Reform predictive policing, *Nature News*, 541 : 458-460.

Sherman, L.W., Gartin, P.R. and Buerger, M.E. (1989), Hot spots of predatory crime: routine activities and the criminology of place, *Criminology*, 27 (1) : 27-56.

Tanner, S. and Meyer, M. (2015), Police work and new 'security devices': A tale from the beat, *Security Dialogue*, 46(4).

Uchida, C. (2014), Predictive policing, In G. Bruinsma and D. Weisburd (eds.), *Encyclopedia of criminology and criminal justice*, Springer, New York, pp. 3871-3880.

van Brakel, R. and De Hert, P. (2011), Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies, *Journal of police studies*, 20 (3) : 163–192.

Walker, S. (2004), Science and Politics in Police Research: Reflections on Their Tangled Relationship, *The Annals of American Academy of Political and Social Science*, 593 : 137-155.