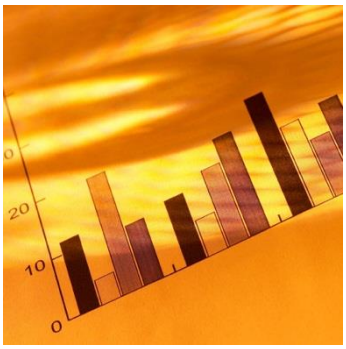
RÉSUMÉ DE RECHERCHE

Crime organisé



2015 – H001

www.securitepublique.gc.ca

BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

NOUVELLES MENACES ET TENDANCES EN MATIÈRE DE BLANCHIMENT D'ARGENT

Selon les estimations, des sommes oscillant entre 5 et 15 G$ CA sont blanchies chaque année au Canada. À l'échelle mondiale, le blanchiment d'argent représenterait des sommes variant entre 500 G et 1 T$ US.

La prévention et l'application de la loi sont les deux piliers de la plupart des régimes de lutte contre le blanchiment d'argent (LBA). La prévention englobe la diligence de la clientèle, le signalement, la réglementation (ou supervision) et les sanctions. Les activités de prévention menées dans le cadre d'un régime de LBA reposent sur la capacité des institutions financières d'exercer leurs fonctions consistant à contrôler l'accès au sein du système, de même qu'à évaluer et à communiquer les risques aux autorités par l'entremise de l'unité du renseignement financier (URF) de l'administration appropriée (42). Quant à l'application de la loi, elle englobe les confiscations (au pénal et au civil), les poursuites, les enquêtes et les infractions sous-jacentes liées à des affaires criminelles (infractions substantielles autres que celles liées au blanchiment d'argent, par exemple les infractions en matière de drogue ou de fraude).

Comme il s'agit d'une activité où les transactions s'effectuent en argent comptant, le trafic de la drogue demeure la principale infraction sous-jacente en ce qui concerne le blanchiment d'argent. Le risque que des sommes soient blanchies varie en fonction de l'ampleur de l'activité de trafic de la drogue. Les petits revendeurs ne manipulent que de petites coupures. Quant aux trafiquants de niveau intermédiaire, ils tentent d'« affiner » l'argent en cherchant à convertir en grosses coupures les grandes quantités de petites coupures qu'ils accumulent. Les cartels mexicains contrôlent 90 % de la cocaïne revendue dans les rues des États-Unis (Simser, 2011) et recyclent les produits de la vente en plaçant de fortes sommes dans des pays où les transactions financières font l'objet d'un examen peu attentif (43).

La fraude représente un type de crime différent dans la mesure où, bien souvent, l'argent ne constitue pas le moyen d'échange. La fraude englobe une kyrielle d'actes illicites allant de la combine à la Ponzi aux escroqueries liées au télémarketing et aux cartes de crédit. Les produits de la fraude sont acheminés vers les institutions financières par les voies conventionnelles, ce qui leur confère un « vernis de légitimité » destiné à berner les victimes (les particuliers et les institutions financières). Le ralentissement de l'économie a eu de graves répercussions sur les institutions financières. Aux États-Unis, plus de 300 institutions de dépôts assurés ont fermé leurs portes depuis 2007 (GAO, 2011). Dès que les marchés ont commencé à manquer de

Dans ce numéro

liquidités, on a assisté à une véritable « ruée » vers les fonds provenant de combines à la Ponzi. Ces combines posent deux types de risques pour les institutions financières : premièrement, le fraudeur utilise les institutions financières pour blanchir l'argent des victimes et l'acheminer vers des destinations étrangères comme l'Europe, le Canada et Antigua; deuxièmement, au-delà des préoccupations relatives à la conformité avec les activités de LBA, il existe un risque en matière de responsabilité civile.

L'auteur passe en revue un certain nombre de nouveaux moyens utilisés afin d'effectuer des paiements : les nouveaux modes de paiement (NMP), les cartes d'accès prépayées, l'argent électronique et les prêts de personne à personne. Ces nouveaux modes de paiement ont été conçus pour combler deux types de besoins présents sur le marché. D'une part, ils visent à faciliter les transactions en ligne, et, d'autre part, ils ont pour but d'aider les personnes sous-bancarisées. Aux États-Unis, quelque 4 millions de prestataires de la sécurité sociale n'ont pas de compte bancaire et utilisent des cartes d'accès prépayées afin de toucher leurs prestations. Le Groupe d'action financière (GAFI) a conclu que les NMP étaient utilisés aux fins malveillantes suivantes : en tant que méthode de financement par un tiers (prête-noms et personnes interposées); en tant que moyen de paiement ne faisant intervenir aucune interaction en personne; et enfin, en vue d'exploiter les fournisseurs de NMP et leurs employés (44).

Les cartes d'accès prépayées représentent un procédé dans le cadre duquel une somme est payée à l'avance et extraite ultérieurement. Elles font office de cartes de crédit prépayées. La carte en tant que telle ne recèle aucune valeur, mais elle donne accès à un bassin de fonds mis en commun. Par exemple, lorsqu'un consommateur utilise sa carte à un point de vente, le terminal détermine si les fonds disponibles permettent de couvrir le coût de la transaction; si l'émetteur de la carte (ou un tiers fournisseur de services de traitement) établit que les fonds sont suffisants, la transaction est approuvée. Une retenue fictive est appliquée au solde de la carte en fonction du montant de la transaction, laquelle est réglée entre le commerçant et l'émetteur.

La monnaie électronique indexée sur les cours des marchandises, par exemple l'argent électronique ou la monnaie numérique, est susceptible de poser un risque pour la LBA. La monnaie numérique est généralement adossée à des actifs (46). Un émetteur obtient de la monnaie métallique et des contrats par l'intermédiaire d'agents à l'échange qui vendent la monnaie numérique aux utilisateurs finaux payant en argent comptant ou au moyen d'un virement électronique. L'utilisateur final peut effectuer des transactions en ligne au moyen de la monnaie électronique. En général, ces transactions – contrairement à celles effectuées avec des cartes de crédit – n'offrent aucune possibilité de recours (les commerçants n'ont accès à aucune procédure de rétrofacturation, et les clients insatisfaits ne peuvent pas être remboursés par le fournisseur de la monnaie). La monnaie électronique peut être échangée contre une monnaie fiduciaire, par exemple le dollar, l'euro ou le yen.

Des plates-formes Internet permettent à des particuliers de prêter de l'argent à d'autres personnes à des fins de bienfaisance ou à des fins lucratives. Le prêt de personne à personne est un segment de marché qui connaît une croissance rapide. En mars 2011, quelque 63 000 prêts non garantis d'une valeur globale de 469 M$ US avaient été consentis par des plates-formes américaines de prêts à but lucratif comme Prosper Marketplace et LendingClub. Un prêteur peut avancer une somme couvrant la totalité ou une partie d'un prêt (cette somme peut même n'équivaloir qu'à 25 $ US) en se procurant des notes de paiement auprès d'une société de prêts de personne à personne. Le prêteur court le risque de ne pas être remboursé. La société de prêts de personne à personne affiche les demandes d'emprunt, les taux d'intérêt et les notes alphabétiques assignées (lesquelles indiquent le risque de crédit). Elle s'adresse ensuite à une banque à charte, par exemple la WebBank of Utah, laquelle lui verse les fonds liés au prêt. L'argent est recueilli par l'entremise d'un virement de fonds électronique, et le prêteur est remboursé (moyennant des frais de service de 1 %). L'auteur souligne que les trois premières notes assignées à des prêts s'assortissent d'un taux de carence de paiement inférieur à 1 %.

En avril 2011, à New York, des accusations ont été portées contre trois des principaux sites de poker en ligne actifs aux États-Unis (Poker Stars, Full Tilt Poker et Absolute Poker). Le département de la Justice des États-Unis soutient que les défendeurs se sont livrés au blanchiment d'argent. En 2006, le gouvernement des États-Unis, préoccupé par le jeu en ligne, a adopté une

loi criminalisant le fait d'accepter un paiement lié au jeu sur Internet (47).

Le jeu pose un risque immense pour la LBA. Un blanchisseur d'argent peut se rendre dans un casino, faire quelques paris puis se faire payer en argent; par conséquent, les casinos soumettent des rapports relatifs aux opérations monétaires et des déclarations d'opérations suspectes au service de renseignement financier partout dans le monde. Cela vaut également pour le jeu en ligne. Une personne qui souhaite accéder à un site de poker doit télécharger le logiciel requis, créer un profil puis verser des fonds dans un portefeuille électronique. En application des dispositions législatives adoptées aux États-Unis en 2006, les entreprises comme Poker Stars doivent verser les fonds gagnés sous forme de chèque. Selon l'auteur, sous l'angle de la LBA, cette façon de faire n'est pas efficace si un joueur verse dans son portefeuille électronique de l'argent « sale » et qu'il reçoit un chèque « propre » d'une société de jeu établie à l'étranger qui se chargera de blanchir l'argent.

Le GAFI s'est penché sur les méthodes de blanchiment d'argent utilisées dans le domaine du sport, plus particulièrement le football. Cet examen lui a permis de déterminer que les équipes de football posent un certain nombre de risques au chapitre de la LBA, notamment les suivants :

- Le football est un domaine où les paiements se font essentiellement en argent comptant (au guichet, au moment de l'achat de produits dérivés et dans les cantines). En outre, ce secteur exige d'importantes entrées de capitaux, lesquels peuvent provenir de divers intervenants, des partisans et des commanditaires. Ceux qui observent le marché des échanges de joueurs savent que l'argent n'est pas toujours dépensé de façon rationnelle.
- La culture du football revêt un caractère important : les propriétaires acquièrent un statut social; les jeunes joueurs peuvent être originaires de milieux sociaux à risque… l'attrait qu'exerce le sport peut conférer aux propriétaires un accès aux personnes exposées à la corruption et leur permettre d'exercer une influence sur elles (GAFI, 2009, p. 36).

Les cartels colombiens ont utilisé des stratagèmes de blanchiment d'argent par voies commerciales afin de blanchir des millions de dollars. Par exemple, ils ont eu recours à la surfacturation d'émeraudes (ils ont expédié des pierres de qualité inférieure injectées d'huile). Aux yeux d'un inspecteur des douanes, les émeraudes « rutilantes » semblaient avoir la valeur qui leur avait été attribuée. De l'argent propre peut être utilisé pour monnayer la valeur des émeraudes, et de l'argent sale, pour assumer le solde.

L'auteur fait observer que les institutions financières sont censées jouer un rôle dans la lutte contre le blanchiment d'argent par voies commerciales, mais elles ne sont pas toujours idéalement placées pour le faire (49). Il ajoute que la plupart des échanges internationaux consistent en des opérations à compte ouvert dans le cadre desquelles l'institution financière verse de l'argent à la demande de son client sans procéder à un examen des documents commerciaux sous-jacents (49).

L'auteur se penche sur la façon dont le blanchiment d'argent infiltre les régimes actuels de LBA. Il mentionne des risques qui ont vu le jour au sein de certains régimes communs qui sont utilisés pour transférer de la valeur, qu'ils soient en ligne ou qu'ils prennent la forme de cartes d'accès prépayées. Il examine également les activités illicites naissantes qui pourraient donner lieu à de nouveaux problèmes, par exemple le blanchiment d'argent par voies commerciales. Il en arrive à la conclusion suivante : pour conserver leur solidité, les régimes doivent constamment demeurer à l'affût des nouvelles tendances et des menaces récentes (51).

SIMSER, Jeffrey. « Money laundering: emerging threats and trends », *Journal of Money Laundering Control*, vol. 16, nº 1, 2013, p. 41-54.

Articles connexes

GAFI. *Money Laundering Through the Football Sector*, Financial Action Task Force, Paris, juillet 2009, p. 42.

GAO. *Bank Regulation: Modified Prompt Corrective Action Would Improve Effectiveness*, GAO-11-612, Government Accountability Office, Washington D.C., juin 2011.

CYBERCRIME ORGANISÉ?

En général, les activités cybercriminelles coordonnées ne sont pas considérées comme relevant du crime organisé, mais certains sites d'échange commercial peuvent être considérés comme des organisations criminelles.

Cette étude repose sur une autre étude composée d'entrevues (auprès de représentants d'entreprises de sécurité Internet, d'agents d'application de la loi en service ou à la retraite et d'anciens pirates informatiques) et d'une analyse de documents de nature juridique. La recherche comprenait des comparaisons entre cybercriminalité et crime organisé; l'étude vient ajouter à ce corpus des études en cours sur la question. L'auteur de l'article se penche sur les définitions de « crime organisé », de « mafia » et de « cybercriminalité » établies par les spécialistes, et il tente de déterminer si les sites cybercriminels d'échange commercial en ligne peuvent être considérés comme relevant de la mafia.

Le crime organisé peut être vu comme une instance qui exerce une certaine forme de gouvernance au sein du milieu criminel, ce qui renvoie expressément à la définition de Varese selon laquelle le crime organisé représente une tentative pour régler et contrôler la production et la distribution illicites d'un produit ou d'un service donné (53). À cette définition, l'auteur ajoute celle selon laquelle la mafia représente un type d'organisation du crime organisé qui tente de gérer l'offre d'une protection (54).

L'auteur définit la cybercriminalité comme une utilisation d'ordinateurs ou d'autres dispositifs électroniques par l'entremise de systèmes d'information comme les réseaux organisationnels ou Internet pour faciliter la perpétration d'actes illicites (54). Il souligne qu'il met l'accent sur les organisations cybercriminelles impliquées dans des activités à but lucratif plutôt que sur celles qui mènent des activités à visée politique (terrorisme ou cyber militantisme) ou malicieuse (pédophilie ou traque furtive en ligne).

Un parallèle a été établi entre les sites d'échange commercial en ligne et la mafia parce que ces sites sont utilisés aux fins d'échange de biens et de services illicites. À titre d'exemple, il mentionne les sites Silk Road et DarkMarket, qui n'existent plus.

Ces sites disposent généralement d'une hiérarchie et d'un programme définis. Une personne est chargée de leur administration, et des modérateurs doivent superviser les échanges et s'assurer que les membres des diverses catégories (dont chacune s'assortit d'un statut et de privilèges distincts) respectent les règles. D'après l'auteur, comme c'est le cas dans d'autres types d'organisations criminelles, une personne monte en grade lorsqu'elle prouve sa fiabilité et ses capacités ou en accordant des faveurs à des membres hauts gradés du site (54). Ce qui intéresse ces sites, ce sont les affaires et le profit, et non pas les questions d'ordre idéologique que les pirates informatiques placent traditionnellement au centre de leurs préoccupations[3].

Au moment d'établir si les sites de ce genre relèvent de la mafia, il faut se demander s'ils tentent de gérer l'offre de la protection (55). Selon lui, vu la quasi-absence d'entraves à la création de sites de ce genre – laquelle n'exige que des compétences relativement élémentaires en matière de programmation – et l'immensité d'Internet, l'établissement d'un monopole dans ce domaine poserait des difficultés (55).

L'article évoque le cas de Iceman, pirate qui assumait les fonctions d'administrateur d'un important site cybercriminel portant le nom de CardersMarket. Il a lancé une campagne visant à unifier les principaux sites de cybercriminalité sous son emprise. Grâce à ses compétences de pointe en piratage, il s'est introduit subrepticement dans chaque site et a subtilisé les renseignements personnels de ses membres et d'autres données. Il a ensuite intégré ces membres cybercriminels à son propre site et supprimé les sites préexistants. Hormis DarkMarket, qui allait entrer en guerre contre CardersMarket, tous les autres sites ont été détruits ou ont vu leur crédibilité compromise de façon irrémédiable (56).

L'auteur souligne que l'une des principales difficultés que pose l'intégration des sites d'échange commercial en ligne à la catégorie des organisations mafieuses tient au fait qu'il est difficile de considérer ces marchés comme des organisations criminelles tout court (56). Il

insiste sur le fait que ces sites doivent être vus comme des marchés, tandis que la mafia n'est pas un marché (56). La mafia peut chercher à exercer un pouvoir sur divers marchés, mais son existence est distincte des diverses entreprises dans lesquelles elle est impliquée.

Le problème que pose la définition des sites en ligne en tant qu'organisations mafieuses tient à ce que leur structure et leur organisation semblent être liées au site en tant que tel plutôt qu'à un groupe autonome (56). L'auteur fait observer que peu d'éléments probants tendent à indiquer que les principaux responsables des sites appartiennent à un groupe organisé et défini extérieur au site lui-même (56). Il souligne que d'importants marchés comme ShadowCrew et DarkMarket mènent leurs activités pendant quelques années et tendent à se désintégrer à mesure que s'accentue la surveillance exercée sur leur site par les organismes d'application de la loi et que leurs dirigeants sont arrêtés. Cela tranche avec les organisations mafieuses, qui peuvent être affaiblies par une surveillance ou des arrestations semblables, mais qui sont en mesure de poursuivre néanmoins leurs activités et de se rebâtir, démontrant ainsi qu'elles sont durables et distinctes de leurs diverses activités et de leurs principaux dirigeants.

Outre les sites d'échange commercial, la majorité des formes attestées de cybercriminalité ne correspondent pas à la définition de « crime organisé ». D'une part, dans bien des cas, les organisations cybercriminelles sont petites et plus ou moins structurées, et elles ne disposent d'aucun plan clair. D'autre part, certaines organisations mieux structurées sont considérées davantage comme des groupes perpétrant des crimes contre la personne plutôt que comme des organisations de gouvernance criminelle.

L'article recense quelques groupes d'apparition récente qui semblent dénoter une appropriation par des organisations présentes en ligne du rôle joué par les groupes criminels organisés classiques, à savoir régler ou contrôler la production ou la distribution d'un produit ou d'un service (57). À titre d'exemple, les activités d'un cybercriminel turc se faisant appeler « Cha0 », qui commercialisait et vendait en ligne des copieurs de cartes et des claviers d'identification personnelle qu'on peut fixer à des guichets automatiques afin d'enregistrer les données et les NIP liés aux cartes (57), pourraient être considérées comme des activités du crime organisé. Cha0 s'est servi de son poste d'administrateur de DarkMarket pour fabriquer des griefs à l'endroit d'un autre vendeur de copieurs de cartes se faisant appeler « Dron » et le faire exclure du site, ce qui lui a permis de devenir le principal fournisseur de copieurs de cartes. Cha0 a ensuite changé son modèle d'affaires et s'est mis à louer plutôt qu'à vendre ses appareils. Les personnes qui louaient le dispositif ne pouvaient que télécharger, à partir des guichets automatiques, des données cryptées que seul Cha0 pouvait déchiffrer. Ainsi, ces personnes étaient contraintes de transmettre les informations à Cha0, qui prenait les mesures requises pour « monnayer » les renseignements liés aux cartes et verser une partie du profit aux personnes à qui il louait ses appareils. L'auteur mentionne que le génie du stratagème de Cha0 tenait à ce qu'il transformait toutes les personnes qui louaient ses copieurs de cartes en membres *de facto* de son organisation (57).

Un autre domaine qui présente des similitudes avec le crime organisé est celui de l'« hébergement inconditionnel », dans le cadre duquel le fournisseur n'exclut pas les clients dont les activités sont contraires à l'éthique ou à la loi (57-8). Ce type d'hébergement est attrayant pour les cybercriminels, et est utilisé aux fins de la prestation de services à des sites pornographiques et à des polluposteurs. À titre d'exemple, le Russian Business Network (RBN) est une organisation de cybercriminels s'étant livrée en 2008 à un racket de protection. On a avancé que la stratégie du RBN consistait à faire surveiller les discussions en ligne de fournisseurs de services de protection Web par des personnes exploitant des sites éventuellement malveillants (58). Le RBN lançait une attaque contre les sites par l'entremise d'un tiers, et offrait ensuite des services de protection contre des attaques de ce genre, moyennant des frais mensuels de 2 000 $ US (58). Les sombres activités de ces sites rendent moins attrayants les services offerts par d'autres fournisseurs de services de protection Web, même si, dans bien des cas, il s'agit d'entreprises légitimes.

Le fait de considérer les groupes cités dans l'étude comme d'authentiques organisations du crime organisé pose un certain nombre de difficultés (58). L'auteur souligne qu'il n'existe au sein d'Internet aucun outil semblable qui permet de contrôler divers marchés. L'exclusion de groupes en ligne et les attaques à l'endroit d'une plate-forme sont utilisées en tant que moyens de contrainte et de contrôle, mais ne causent pas de torts durables. Dans le domaine de la cybercriminalité, le contrôle d'un territoire est plus complexe. L'hébergement inconditionnel semble fournir un certain type d'analogie au sein du cyberespace; toutefois, l'hébergement en question n'est jamais complètement inconditionnel. De surcroît, l'auteur mentionne que des fournisseurs en amont ont mis fin aux activités d'hébergeurs inconditionnels dans le passé, lorsque suffisamment de pression était exercée, et continuent de le faire, ce qui met également fin aux activités de leurs clients (58). Les démarches théoriques classiques et les comparaisons avec les groupes traditionnels du crime organisé demeurent des outils utiles au moment de comprendre quelques-uns des problèmes auxquels se heurtent les organisations cybercriminelles et d'éventuellement expliquer les solutions qu'elles trouvent pour surmonter ces problèmes (59).

LUSTHAUS, Jonathan. « How organised is organised cybercrime? », *Global Crime*, vol. 14, n° 1, 2013, p. 52-60.

Articles connexes

VARESE, Federico. « What is Organized Crime? », publié sous la direction de Federico Varese, New York, 2010, p. 1-33, *Organized Crime: Critical Concepts in Criminology*.

RECOURS AUX DISPOSITIONS LÉGISLATIVES SUR LES ORGANISATIONS CRIMINELLES ET LES COMPLOTS

D'aucuns peignent comme une menace pour les libertés civiles les pouvoirs étendus des policiers et les pouvoirs accrus en matière de poursuites conférés par la législation canadienne visant les organisations criminelles.

L'auteur se penche sur le recours aux dispositions législatives applicables aux organisations criminelles (qu'on désigne également sous l'appellation de « crime organisé ») au Canada et dans d'autres pays occidentaux, et il fait ressortir les avantages et les inconvénients de ces dispositions. En outre, il examine l'utilisation par la Gendarmerie royale du Canada (GRC) des dispositions législatives visant les organisations criminelles et les complots dans le cadre d'enquêtes et en vue d'intenter des poursuites contre des groupes criminels (1). L'auteur se fonde sur des données tirées de documents liés à des affaires précises et sur des entrevues menées auprès de 24 enquêteurs de la GRC et de deux procureurs. Il s'appuie également sur une étude antérieure dans le cadre de laquelle il avait interviewé 70 trafiquants de drogue de haut niveau ayant été condamnés (Desroches, 2005).

En 1997, on a adopté le projet de loi C-95, lequel visait les organisations criminelles, puis le projet de loi C-24, selon lequel une organisation criminelle se définit comme un groupe (1) composé d'au moins trois personnes se trouvant au Canada ou à l'étranger; et (2) dont un des objets principaux ou une des activités principales est de commettre ou de faciliter une ou plusieurs infractions graves qui, si elles étaient commises, pourraient lui procurer, ou procurer à une personne qui en fait partie, directement ou indirectement, un avantage matériel, notamment financier (2).

Ces dispositions législatives ont pour effet d'élargir la portée des infractions qui définissent une organisation criminelle; d'inverser le fardeau de la preuve dans le cadre d'audiences sur la liberté sous caution et en ce qui concerne la saisie de biens et d'actifs; de rendre passible d'une sanction pouvant aller jusqu'à la peine d'emprisonnement à perpétuité toute personne qui incite une autre personne à commettre une infraction au profit d'une organisation criminelle; de faire passer de 60 jours à 1 an la durée maximale des autorisations d'écoute électronique; d'offrir aux victimes et aux témoins une protection contre l'intimidation; et d'offrir une certaine immunité aux policiers en civil qui commettent des crimes afin d'infiltrer des organisations criminelles dans le cadre d'enquêtes à leur sujet (2).

Le texte législatif visant les organisations criminelles confère des pouvoirs accrus à l'État. Les personnes qui, comme l'auteur, ont formulé des critiques à l'égard du texte font valoir que ces dispositions ne

définissent pas de façon précise et exacte la notion de crime organisé (3). L'auteur souligne que bon nombre de dispositions législatives sont fondées sur des stéréotypes, notamment sur l'image classique de l'organisation criminelle de type mafieux dotée d'une structure hiérarchique soumise à un pouvoir centralisé et de membres exclusifs et identifiables assumant des fonctions clairement définies (3). Pourtant, la recherche sur les organisations criminelles impliquées dans la traite de personnes et le terrorisme révèle que les organisations de ce genre sont petites et informelles, et que leur structure est approximative. Des études de nature semblable semblent indiquer que les groupes de trafiquants de drogue de haut niveau sont constitués de petites organisations criminelles autonomes et décentralisées qui se sont regroupées au gré des circonstances, qui ne possèdent aucune structure hiérarchique claire et qui collaborent les unes avec les autres pour leur bénéfice mutuel (3).

L'auteur affirme que les dispositions législatives en vigueur visant les organisations criminelles font qu'il est difficile de prouver l'affiliation, l'association et l'appartenance suivies d'une personne à une organisation (3). À propos d'une affaire concernant le club de motards Hells Angels, l'auteur mentionne ce qui suit : Après que le juge a acquitté le seul accusé reconnu comme membre du gang de motards, les accusations d'appartenance à une organisation criminelle portées contre les autres défendeurs ont été retirées (4).

En outre, l'auteur souligne que, si certains délinquants jouent un rôle central, d'autres agissent en périphérie et participent à des activités de divers réseaux qui se recoupent. Ces interactions peuvent être de nature sporadique et s'effectuer à distance ou par-delà les frontières – il s'agit de réseaux sociaux dynamiques dont la forme et la composition évoluent au fil du temps.

Dans le cadre de l'arrêt (*R. c. Venneri,* 2012), la Cour suprême du Canada a déterminé que le niveau de preuve applicable aux infractions liées aux organisations criminelles devait être plus élevé que celui applicable aux accusations en matière de complot, en faisant valoir que l'application des dispositions sur le crime organisé contenues dans le *Code criminel* était « assujettie à l'existence d'une structure quelconque et d'une certaine continuité » (4).

Les affaires visant les organisations criminelles donnent souvent lieu à des « méga-procès » difficiles à gérer, voraces en temps et en ressources. Les retards qui peuvent en découler sont susceptibles d'aboutir au classement de l'affaire pour des motifs d'ordre constitutionnel (5). Par exemple, au Québec, un juge a rejeté toutes les accusations portées contre 31 membres des Hells Angels en raison du temps déraisonnable mis pour entreprendre leur procès. On a estimé à 11 M$ CA le coût lié à la poursuite, ce qui ne comprend pas les 4 M$ qu'ont exigé les travaux de rénovation du palais de justice entrepris pour répondre aux besoins de ce procès de grande envergure (6).

En 2010, à l'issue d'une enquête visant un réseau de traite de personnes de l'Ontario, la GRC a arrêté 14 personnes et les a accusées de complot visant la traite de personnes (6). La preuve a révélé que les accusés avaient leurré 23 hommes en leur promettant du travail s'ils venaient au Canada. Une fois arrivés ici, ces hommes avaient été contraints de travailler pour rien ou pour un maigre salaire. En raison d'obstacles linguistiques et des menaces que leur avaient proférées leurs ravisseurs, les victimes ont été incapables de chercher à obtenir de l'aide des autorités (6).

En raison de la nature homogène et structurée du groupe se livrant à la traite de personnes, il a été relativement facile pour le procureur de la Couronne de prouver que les accusés appartenaient à une organisation criminelle (6). Tous les défendeurs étaient membres d'une famille étendue de Pápa, en Hongrie. La plupart d'entre eux possédaient un casier judiciaire en Hongrie, et ils avaient tous menti à l'Agence des services frontaliers du Canada au moment de présenter une demande d'asile (6). La preuve a également révélé que tous les membres participaient à des activités de recrutement, de supervision, d'hébergement et de transport de victimes visant à accroître l'ampleur des activités de traite de personnes du groupe.

La GRC a rarement recours aux dispositions législatives visant les organisations criminelles; elle privilégie plutôt le dépôt d'accusations de complot. Un

élément essentiel d'un complot tient à la conclusion d'un accord entre deux ou plusieurs personnes en vue de commettre un acte criminel (7). En vertu de l'article 465 du *Code criminel*, une personne peut être jugée au Canada même si le complot a eu lieu à l'étranger. En outre, le tribunal est autorisé à déduire des actes d'une personne l'existence d'un accord visant la perpétration d'actes criminels (7).

Les enquêteurs de l'escouade antidrogue de la GRC sont conscients du fait que les trafiquants de drogue de haut niveau utilisent des tiers pour éviter de se faire prendre; toutefois, ces revendeurs doivent communiquer et collaborer avec d'autres personnes afin d'acheter et de vendre leurs produits. Par conséquent, les enquêteurs recueillent des éléments de preuve relatifs à des associations et à des réunions de personnes, enregistrent des conversations, rassemblent des documents justificatifs et procèdent à des saisies de drogue afin d'établir l'implication de personnes dans le trafic de la drogue. Par exemple, une étude visant 70 trafiquants de drogue de haut niveau a révélé que la majeure partie d'entre eux avait été déclarée coupable d'accusations en matière de complot. La plupart de ces trafiquants ont déclaré que leur chute était attribuable à un manque de compréhension des dispositions législatives relatives aux complots. L'auteur souligne que ces dispositions sont plus efficaces dans les pays où le contenu des écoutes électroniques est utilisé en tant qu'élément de preuve (7).

Les réseaux de trafiquants forment une chaîne où l'argent monte vers le fournisseur et où la drogue descend vers le distributeur puis l'utilisateur final. Les dispositions législatives en matière de complot permettent aux policiers d'accuser et de faire condamner des délinquants qui assument des fonctions importantes de direction ou jouent un rôle clé au sein d'un réseau, en dépit du fait qu'ils ont évité de commettre des actes criminels manifestes. Cela signifie que la police peut agir de façon proactive et arrêter des suspects avant qu'ils ne commettent une infraction violente (8). L'auteur ajoute ce qui suit : « Un autre avantage des dispositions législatives en matière de complot tient à ce que l'État n'a pas à prouver que les défendeurs sont membres d'une organisation criminelle ou ont commis des crimes pour servir ses intérêts. » (8)

Les lois canadiennes permettent à un juge d'insister sur le fait que la défense n'a pas expliqué la conduite d'un accusé. Si la défense ne présente aucun argument plausible afin de réfuter la thèse d'un complot soutenue par l'État, il est probable que les jurés en arrivent à un verdict de culpabilité.

L'auteur conclut que le Canada a emboîté le pas à d'autres pays occidentaux en adoptant des dispositions législatives conférant des pouvoirs accrus aux organismes d'application de la loi et instituant des sanctions plus sévères, afin de contribuer aux enquêtes et aux poursuites relatives aux crimes. D'aucuns ont fait valoir que les lois canadiennes portaient atteinte aux libertés civiles, s'appuyaient sur des définitions vagues et inexactes de la notion de « crime organisé », et donnaient lieu à des « méga-procès » coûteux. L'établissement de normes de preuve élevées et le rejet d'affaires liées à des méga-procès ont porté un coup dur aux procureurs.

Ainsi, la GRC a rarement recours aux dispositions législatives applicables au crime organisé au moment d'intenter des poursuites contre certaines organisations criminelles, par exemple celles constituées de trafiquants de drogue de haut niveau. Dans la plupart des cas, elle s'en remet à des accusations en matière de complot, dont il est plus facile d'établir le bien-fondé puisqu'elles mettent l'accent sur l'acte criminel plutôt que sur la structure et le fonctionnement d'une organisation. L'auteur s'attend à ce que cette pratique se perpétue, du moins jusqu'à ce qu'on règle les problèmes liés aux définitions et aux normes de preuve applicables.

DESROCHES, Frederick J. « The Use of Organized Crime and Conspiracy Laws in the Investigation and Prosecution of Criminal Organizations », *Policing*, 4 février 2013, p. 1-10.

TENTATIVE D'INTIMIDATION À L'ÉGARD DES SERVICES POLICIERS DU QUÉBEC

Au Québec, les bandes de motards criminalisées se livrent de plus en plus fréquemment à des manœuvres d'intimidation à l'endroit de policiers. L'intimidation a plus d'incidence sur le comportement des patrouilleurs que sur celui des enquêteurs.

L'auteur explique que, au Québec, les organisations criminelles comme les bandes de motards criminalisées (BMC), surtout le chapitre de la côte Est des Hells Angels, usent de l'intimidation afin d'influer sur le comportement de personnes faisant partie du système judiciaire, particulièrement les policiers. Son étude se fonde sur deux sources principales, à savoir la base de données d'un projet sur l'intimidation mené par la police provinciale (la Sûreté du Québec), et des entrevues menées auprès de 20 policiers québécois que des membres de BMC ont tenté d'intimider.

Selon le rapport annuel de 2001 sur le crime organisé du Service canadien de renseignements criminels (SCRC), les BMC du Canada continuent de recourir à la violence – qu'il s'agisse d'actes d'intimidation, de voies de fait, de tentatives de meurtre ou de meurtres – afin de servir et de protéger leurs intérêts (67).

La base de données a été utilisée afin de compiler tous les événements mettant en cause des actes d'intimidation posés par des organisations criminelles d'ici ou d'ailleurs (69). Ces données permettent d'évaluer les tendances en matière d'intimidation et de mesurer la portée du phénomène au Québec. Les critères d'échantillonnage appliqués dans le cadre de l'étude sont les suivants : (i) la période retenue s'étendait de 1999 à septembre 2001 inclusivement; (ii) l'échantillon englobait tous les membres de la police ayant été victimes de tentatives d'intimidation, les personnes ayant une relation avec un policier et des tiers civils impliquant un policier; (iii) tous les actes visant une composante d'une organisation policière (p. ex. des services, des installations ou des véhicules de la police) ont été pris en considération; (iv) les actes retenus devaient avoir été posés par des suspects liés de près ou de loin à une BMC.

L'auteur appuie sa description de la structure hiérarchique des Hells Angels sur les renseignements contenus dans le rapport de 2001 du SCRC. Il mentionne que chaque motard joue un rôle précis et porte un titre distinct au sein de l'organisation. Un « chapitre » renvoie à la bande d'un territoire donné et est dirigée par des « membres en règle » portant les « couleurs » (signes et logos) des Hells Angels sur leur blouson (69). À l'échelon inférieur se trouvent les « *prospects* », qui sont des membres en puissance du chapitre pendant un an. On trouve tout au bas de la hiérarchie les « *hangarounds* », personnes qui gravitent autour du groupe dans l'espoir de devenir des « *prospects* ». Des personnes ayant divers intérêts tournent autour d'eux. Les « clubs-écoles » font partie d'une sous-catégorie; ils occupent un plus petit territoire et partagent une structure organisationnelle composée de « membres en règle », de « *strikers* » et de « *hangarounds* ». Toutes ces personnes portent les « couleurs » du « club-école ». Les « amis » et les « relations » sont souvent des personnes qui brassent des affaires avec le « chapitre » officiel ou le « club-école », et ils ne portent pas les « couleurs ».

Les tentatives d'intimidation à l'égard de policiers prennent rarement la forme d'une agression physique. Il s'agit plutôt de menaces vagues et diffuses, par exemple des allusions à la vie personnelle d'un policier. On cherche à déstabiliser les policiers en évoquant des caractéristiques personnelles de leur épouse ou de leurs enfants. Il arrive que des BMC suivent un policier ou son épouse jusqu'à sa résidence privée ou lui téléphonent à la maison (71). D'autres actes d'intimidation ont pour but de détruire la carrière d'un policier au moyen de poursuites au pénal et au civil ainsi que de plaintes déposées auprès du comité de déontologie, qui examine la nature des obligations et de l'éthique policières. Ces manœuvres ont pour but d'ébranler la volonté d'un policier tout en minant sa crédibilité (71).

Les tentatives d'intimidation se produisent lorsque des BMC dérogent aux règles tacites et tentent d'imposer leur propre méthode (72). Certains policiers sont ciblés en raison de leur comportement excessivement autoritaire et répressif. L'auteur mentionne ce qui suit : « Les actes d'intimidation posés

par les BMC à l'endroit d'enquêteurs sont d'une ampleur et d'une nature différentes de ceux posés à l'égard de patrouilleurs. » (73) L'auteur ajoute que les patrouilleurs n'ont pas reçu la formation qui leur permettrait de composer avec les membres du crime organisé (74). Pour leur part, les enquêteurs possèdent une connaissance approfondie des milieux criminels qu'ils ne partagent pas et perçoivent les règles tacites des interactions entre les BMC et les policiers (74).

Les patrouilleurs réagissent aux tentatives d'intimidation de trois façons différentes. Premièrement, certains policiers tenteront d'éviter le plus possible les rencontres avec des membres de BMC afin d'éviter les problèmes dans leur vie privée ou professionnelle. Deuxièmement, on trouve un noyau restreint de policiers très braves et très actifs qui ont décidé de se spécialiser dans les affaires liées au crime organisé (75). Troisièmement, on trouve des policiers provocateurs qui font fi des normes policières au moment de tenter de mettre le grappin sur des membres de BMC.

En ce qui concerne les résultats de recherche, l'auteur mentionne qu'un entonnoir à trois niveaux a été conçu pour illustrer les effets des tentatives d'intimidation. À chaque niveau, le nombre de policiers disposés à se spécialiser dans la lutte contre le crime organisé diminue. Au premier niveau, on constate que la tentative d'intimidation a de vastes effets et ne touche que les patrouilleurs et leur pouvoir discrétionnaire (76). L'auteur souligne que les craintes relatives à leur vie personnelle et professionnelle découragent les patrouilleurs d'intervenir contre les BMC (76). La peur éprouvée découle d'une menace plus virtuelle que réelle.

Le deuxième niveau de l'entonnoir comprend les patrouilleurs qui ont volontairement choisi de combattre le crime organisé (77). Leurs craintes sont fondées sur des menaces réelles visant des membres de leur famille auxquels des BMC ont tenté de s'attaquer. Quant au troisième niveau, il est constitué des enquêteurs spécialistes des BMC, qui sont moins intimidés en raison du pouvoir qu'ils possèdent et du respect qu'ils inspirent aux criminels (77).

Selon l'auteur, les résultats de recherche révèlent l'existence d'un écart entre la formation des patrouilleurs et les solutions envisagées par les policiers interviewés. Il estime que la prestation d'une formation sur ce type de criminels et leurs réseaux pourrait susciter l'intérêt des patrouilleurs réticents (77). Il ajoute qu'il semble nécessaire de concevoir des méthodes d'intervention efficaces afin d'éviter les écarts de conduite de la part de policiers réagissant à des actes commis par des BMC (77).

L'auteur fait valoir qu'il pourrait être pertinent d'adopter des mesures visant à mieux protéger les policiers faisant l'objet de poursuites inutiles intentées par des BMC, et à veiller à la protection de leurs renseignements personnels (78). De plus, il souligne que les résultats de l'étude indiquent l'existence d'une lacune substantielle au chapitre de la transmission des renseignements au sein des services policiers (78). Il mentionne que l'article 423 du *Code criminel* a été adopté afin de lutter contre l'intimidation à l'endroit de membres d'organismes d'application de la loi (78).

L'auteur conclut que le portrait de l'intimidation semble être plus complexe (78). En raison des répercussions qu'ont les tentatives d'intimidation sur leur vie personnelle et professionnelle, bon nombre de patrouilleurs adoptent une attitude conservatrice. De surcroît, l'auteur avance ce qui suit : « À la lumière des nombreuses arrestations de membres des Hells Angels au cours des dernières années, il est permis de se demander si le phénomène des tentatives d'intimidation ne se déplacera pas vers les endroits où les Hells Angels sont plus présents, à savoir les tribunaux et les pénitenciers. » (79)

GOMEZ DEL PRADO, Grégory. « Outlaw motorcycle gangs' attempted intimidation of Quebec's police forces », *Police Practice and Research*, vol. 12, n° 1, 2011, p. 66-80.

Articles connexes

SCRC. *Annual Report on Organized Crime in Canada 2001* (en ligne), 2001, 55 p. (consulté le 11 avril 2014). Sur Internet : http://www.cisc.gc.ca/annual_reports/documents/2001_annual_report.pdf.

Pour obtenir davantage de renseignements sur la recherche effectuée au Secteur de la sécurité communautaire et de la réduction du crime de Sécurité publique Canada, pour obtenir une copie du rapport de recherche complet, ou pour être inscrit à notre liste de distribution, veuillez communiquer avec :

Pour en savoir davantage :
Division de la recherche
Sécurité publique Canada
269, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
PS.CSCCBResearch-RechercheSSCRC.SP@ps-sp.gc.ca

ISSN : 1927-808x