Résolutions adoptées

à la

112e Conférence annuelle

Juillet 2017

Montréal (Québec)

ASSOCIATION CANADIENNE DES CHEFS DE POLICE

Sûreté et sécurité pour tous les Canadiens grâce
à un leadership policier innovateur

300, promenade Terry Fox, bureau 100, Kanata (Ontario) K2K 0E3
t : 613-595-1101 f : 613-383-0372
c : cacp@cacp.ca w : www.cacp.ca

Table des matières

Résolution 01 - 2017

RÉSOLUTION POUR L'APPROBATION DE LA STRATÉGIE EN MATIÈRE DE GESTION DE L'INFORMATION SUR LA SÉCURITÉ DES COLLECTIVITÉS CANADIENNES (SGISCC)

Soumise par le Comité sur l'information, les communications et la technologie

ATTENDU QUE l'Association canadienne des chefs de police (ACCP) et ses membres échangent des renseignements depuis la création du Centre d'information de la police canadienne (CIPC) en 1972 et de nombreux autres systèmes par la suite;

ET ATTENDU QUE la sécurité, la protection et la prospérité des Canadiens, y compris des agents d'application de la loi et de leurs partenaires, sont tributaires de l'échange efficace de renseignements actuels;

ET ATTENDU QUE de nombreuses enquêtes publiques et études ont désigné le manque d'échange de renseignements et d'interopérabilité, à la fois entre organismes policiers et avec les composantes du système de justice et d'autres organismes gouvernementaux et non gouvernementaux travaillant à la sécurité publique, comme un obstacle à des enquêtes fructueuses et efficaces et à l'efficacité des opérations et du renseignement;

ET ATTENDU QUE le Comité sur l'information, les communications et la technologie (Comité ICT, ancien Comité de l'informatique) de l'Association canadienne des chefs de police encourage l'échange de renseignements entre organismes d'application de la loi et autres intervenants en sécurité publique depuis 1998 en organisant des conférences nationales et en suscitant des progrès comme le Portail d'informations policières (PIP), qui est géré par les Services nationaux de police de la GRC;

ET ATTENDU QU'en 2014, le Comité ICT, avec l'appui financier du Centre des sciences pour la sécurité, du gouvernement du Canada, a réalisé une étude nationale sur la gestion de l'information aux fins de l'application de la loi qui a clairement démontré le manque d'interopérabilité entre systèmes de gestion de l'information aux fins de l'application de la loi au Canada et recommandé l'élaboration d'une stratégie nationale pour améliorer l'échange de renseignements;

ET ATTENDU QUE le Comité ICT de l'ACCP a achevé l'élaboration de la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC), ainsi que le demandait la résolution 2015-05 de l'ACCP;

ET ATTENDU QUE la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) profitera à tous les Canadiens en rehaussant la sécurité des collectivités et en permettant des gains en efficience à l'échelle nationale,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police encourage Sécurité publique Canada à financer et élaborer un cadre national, fondé sur la SGISCC, pour gérer l'information entre les organismes d'application de la loi fédéraux, provinciaux, territoriaux, régionaux et municipaux et d'autres organisations du secteur de la justice;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police encourage Sécurité publique Canada à coordonner et financer, en 2018, un atelier sur la SGISCC à l'intention des organisations fédérales, provinciales et territoriales du secteur de la justice afin de faire mieux connaître les principes de la SGISCC et ainsi accroître l'efficacité des efforts consacrés à la sécurité publique partout au Canada;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police encourage Sécurité publique Canada à assurer le financement d'un soutien à temps partiel à l'élaboration continue de la SGISCC.

Résolution 01 - 2017

RÉSOLUTION POUR L'APPROBATION DE LA STRATÉGIE EN MATIÈRE DE GESTION DE L'INFORMATION SUR LA SÉCURITÉ DES COLLECTIVITÉS CANADIENNES (SGISCC)

Résumé

Tel qu'indiqué ci-dessous, la présente proposition prévoit un soutien en faveur d'une vision élargie de l'échange de renseignements dans le secteur de la justice au Canada. La proposition a pour but d'assurer la communication « ***des renseignements voulus aux personnes voulues et au moment voulu*** » (*voir à l'**annexe A** l'analyse détaillée de la proposition*).

Environnement actuel

L'environnement actuel de l'application de la loi au Canada est dépourvu d'une entité nationale de régie ou de coordination de la gestion de l'information réunissant des représentants fédéraux, provinciaux, territoriaux, régionaux et municipaux. Des renseignements vitaux à une décision judicieuse peuvent se trouver dans un système donné ou être répartis entre divers dépôts d'information cloisonnés.

L'échange de renseignements entre corps policiers et autres partenaires en sécurité des collectivités est limité. Le modèle Hub mis à l'essai en Saskatchewan s'est révélé être une excellente pratique pour la sécurité des collectives, mais les attitudes envers l'échange varient grandement d'une administration à l'autre. De nombreux acteurs de la sécurité publique sont réticents à communiquer des renseignements et ne reconnaissent pas pleinement l'intérêt à le faire[1] [2]. Parfois, il faut y voir la conséquence des lois sur la protection de la vie privée, qui varient d'un ressort à l'autre et qui entravent la volonté d'améliorer l'échange de renseignements.

Les systèmes de données actuels ne se prêtent pas aisément à l'échange de renseignements. Il existe de grands systèmes et des systèmes nationaux, mais ils ne sont pas optimisés en vue de l'échange. Bien que le Modèle national d'échange de l'information (NIEM), d'origine américaine, ait été adopté au Canada, les appels d'offres n'exigent presque jamais qu'il soit utilisé pour l'échange de renseignements.

L'ACCP a déjà constaté ces problèmes et adopté la résolution 05-2015, visant à « définir le cadre et le plan d'action voulus pour réaliser la vision de la SGISCC : une gestion responsable de l'information au service de la sécurité des collectivités ». Le Comité sur l'information, les communications et la technologie, travaillant en collaboration, a élaboré un tel cadre et un plan d'action à l'appui, menant ainsi à bon terme cette phase du projet de SGISCC.

La voie à suivre

Cependant, le travail nécessaire à la création d'un environnement national qui permettra de ***fournir les renseignements voulus aux personnes voulues et au moment voulu*** ne fait que commencer. Comme l'indiquent cette résolution de 2017 et son plan d'action, l'ACCP est appelée à :

- approuver la version actuelle du document sur la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) et charger son Comité sur l'information, les communications et la technologie (Comité ICT) de continuer à faire progresser la SGISCC et son plan d'action;

- encourager les chefs de police à mettre en œuvre et intégrer dans leur organisation la SGISCC et son plan d'action;

- encourager Sécurité publique Canada à appuyer la SGISCC dans le secteur de la justice, et ce, par divers moyens – comprenant un soutien financier mais ne s'y limitant pas.

Résolution 01 - 2017

RÉSOLUTION POUR L'APPROBATION DE LA STRATÉGIE EN MATIÈRE DE GESTION DE L'INFORMATION SUR LA SÉCURITÉ DES COLLECTIVITÉS CANADIENNES (SGISCC)

Contexte

La Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) s'agence avec la Stratégie d'interopérabilité des communications pour le Canada[3], et elle pourra être mise en œuvre grâce aux éléments clés suivants :

- une gouvernance efficace;
- une culture de l'échange responsable de renseignements parmi les organismes de sécurité publique;
- des lois équilibrées favorisant l'échange de renseignements;
- l'établissement et la mise en œuvre de normes nationales sur les données ainsi que de méthodes, modalités et processus connexes fondés sur des normes;
- des outils technologiques facilitant la gestion responsable de l'information aux fins de la sécurité des collectivités.

En somme, la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes vise à tirer parti des personnes, des processus et de la technologie pour fournir les renseignements voulus aux personnes voulues et au moment voulu, pour favoriser un vaste environnement d'échange de renseignements au service de la sécurité des collectivités.

Annexe A

Les renseignements voulus aux personnes voulues et au moment voulu

Environnement actuel

L'environnement actuel de l'application de la loi au Canada est dépourvu d'une entité nationale de régie ou de coordination de la gestion de l'information réunissant des représentants fédéraux, provinciaux, territoriaux, régionaux et municipaux. Des renseignements vitaux à une décision judicieuse peuvent se trouver dans un système donné ou être répartis entre divers dépôts d'information cloisonnés. Le financement d'initiatives de gestion de l'information est fragmentaire, et il n'y a pas de modèle de financement viable en place.

L'échange de renseignements entre corps policiers et autres partenaires en sécurité des collectivités est limité. Le modèle Hub mis à l'essai en Saskatchewan s'est révélé être une excellente pratique pour la sécurité des collectives, susceptible de devenir un modèle national. Cependant, les attitudes envers l'échange varient grandement d'une administration à l'autre; souvent, d'autres intervenants en sécurité publique sont réticents à communiquer des renseignements et ne reconnaissent pas pleinement l'intérêt à le faire[1] [2]. Parfois, il faut y voir la conséquence des lois sur la protection de la vie privée, qui varient d'un ressort à l'autre et qui entravent la volonté d'améliorer l'échange de renseignements. Aujourd'hui, peu de lois en place adoptent une perspective multijuridictionnelle de l'échange de renseignements en faveur de la sécurité des collectivités.

Les systèmes de données actuels ne se prêtent pas aisément à l'échange de renseignements. Par surcroît, les pratiques en matière de conservation et d'archivage de renseignements varient au Canada. Il existe de grands systèmes et des systèmes nationaux, mais ils ne sont pas optimisés en vue de l'échange. Bien que le Modèle national d'échange de l'information (NIEM), d'origine américaine, ait été adopté au Canada, les appels d'offres n'exigent presque jamais qu'il soit utilisé pour l'échange de renseignements. Il serait logique qu'une capacité d'intégrer les fonctions de base du NIEM fasse partie de chaque appel d'offres dans le secteur de la sécurité publique, pour en accélérer l'adoption.

Pour compliquer encore la situation, toutes les répercussions des services à large bande de 700 MHz, de la LTE et du 9-1-1 de prochaine génération ne sont pas bien comprises. Par exemple, les technologies à large bande permettraient de fournir à un agent ou un partenaire en sécurité publique toute l'information susceptible de lui être utile dans une situation donnée, mais il y aurait risque de surcharge d'information. Un effort considérable sera nécessaire pour définir ce qui est important et pertinent pour un agent.

L'ACCP a déjà constaté ces problèmes et adopté la résolution 05-2015, visant à « définir le cadre et le plan d'action voulus pour réaliser la vision de la SGISCC : une gestion responsable de l'information au service de la sécurité des collectivités ». Le Comité sur l'information, les communications et la technologie a assumé la responsabilité d'élaborer un cadre et un plan d'action connexe, et cette phase du projet de la SGISCC a été menée à bon terme avec le

parachèvement de ces documents (quoique les documents doivent être considérés comme des textes vivants, qui évolueront de pair avec les progrès de la technologie). La stratégie et son plan d'action ont été présentés en même temps que la mise à jour annuelle sur la résolution 05-2015.

La voie à suivre

Cependant, ce n'est qu'un début en vue de créer un environnement national apte à ***fournir les renseignements voulus aux personnes voulues et au moment voulu***. Comme l'indiquent la présente résolution de 2017 et son plan d'action, l'ACCP est appelée à :

- approuver la version actuelle du document sur la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) et charger son Comité sur l'information, les communications et la technologie (Comité ICT) de continuer à faire progresser la SGISCC et son plan d'action;

- encourager les chefs de police à mettre en œuvre et intégrer dans leur organisation la SGISCC et son plan d'action;

- encourager Sécurité publique Canada à financer et élaborer un cadre national, fondé sur la SGISCC, pour gérer l'information entre les organismes d'application de la loi fédéraux, provinciaux, territoriaux, régionaux et municipaux et d'autres organisations du secteur de la justice;

- encourager Sécurité publique Canada à coordonner et financer, en 2018, un atelier sur la SGISCC à l'intention des organisations fédérales, provinciales et territoriales du secteur de la justice afin de faire mieux connaître les principes de la SGISCC et ainsi accroître l'efficacité des efforts consacrés à la sécurité publique partout au Canada;

- encourager Sécurité publique Canada à assurer le financement d'un soutien à temps partiel à l'élaboration continue de la SGISCC.

Ces recommandations sont détaillées ci-dessous.

Approbation du document actuel sur la SGISCC

Le Comité ICT a sollicité le concours de nombreuses parties intéressées dans l'élaboration du document de stratégie. Deux réunions nationales ont été tenues pendant ce travail, et le document sur la SGISCC a été raffiné à chaque réunion du Comité ICT depuis 2015. La communauté des forces de l'ordre, la communauté de la justice et le secteur privé ont eu l'occasion de commenter le processus et le produit final. Les membres du Comité ICT croient avoir amené le document et le plan d'action connexe aussi loin qu'ils le pouvaient pour le moment. Pour progresser encore, il faudrait maintenant que l'ACCP approuve le document et le plan d'action sur la SGISCC, étant entendu que le travail sur cette stratégie se poursuivra encore pendant des années. Il faudrait aussi un vif appui de l'ACCP de sorte que son poids et son influence puissent servir à entamer

des conversations avec les décideurs en sécurité publique, partout au pays. Par ailleurs, le Comité ICT aurait besoin d'instructions pour la suite du travail.

Encourager les chefs de police à mettre en œuvre la SGISCC

Si les principes de la SGISCC qui traitent de normes, d'échange de renseignements, de régie et de vie privée ne sont pas mis en œuvre dans les corps de police partout au pays, l'actuel environnement fragmenté et cloisonné de gestion de l'information au Canada ne changera pas. Non plus, il ne deviendra pas plus simple de progresser dans l'échange de renseignements avec d'autres partenaires du système de justice. Par conséquent, l'ACCP est invitée à encourager les services de police membres de mettre en œuvre les principes de la SGISCC. En outre, les membres de l'ACCP devraient s'employer à faire connaître la SGISCC aux associations provinciales, de façon à joindre les non-membres de l'ACCP qui n'auraient pas encore été renseignés sur les concepts de la SGISCC.

Cette mise en œuvre n'exige pas des changements radicaux dans les services de police, mais simplement une approche plus éclairée et plus rigoureuse de la gestion de l'information et de la technologie de l'information. Elle ferait en sorte que les normes de la SGISCC puissent aisément être utilisées dans tout nouveau système acheté ou tout nouveau contrat de service commandé auprès d'un tiers. Le Comité ICT aiderait volontiers l'ACCP (sur demande) à élaborer des documents et des programmes d'information qui favoriseraient l'échange de renseignements au Canada et à l'échelle internationale. Si de telles mesures ne sont pas prises, il est probable que la SGISCC n'obtiendra pas le degré d'acceptation nécessaire pour qu'elle change réellement la donne.

Encourager la participation de Sécurité publique Canada

Si la SGISCC a débuté dans le secteur policier, ses objectifs ont une portée bien plus vaste. Pour accroître la sécurité dans les collectivités, l'échange de renseignements doit se faire aisément, dans le respect des structures juridiques existantes. Par conséquent, il faut que le secteur de la justice et d'autres secteurs du gouvernement prennent connaissance de la SGISCC et adoptent les principes qui leur permettront d'échanger et de gérer une de leurs plus précieuses ressources : L'INFORMATION. Cela étant, l'ACCP a demandé à Sécurité publique Canada d'appuyer la vision de la SGISCC de trois façons.

D'abord, l'Association canadienne des chefs de police encourage Sécurité publique Canada à financer et élaborer un cadre national, fondé sur la SGISCC, pour gérer l'information entre les organismes d'application de la loi fédéraux, provinciaux, territoriaux, régionaux et municipaux et d'autres organisations du secteur de la justice. Un leadership national est nécessaire pour que ces principes soient acceptés partout au pays.

Deuxièmement, l'Association canadienne des chefs de police encourage Sécurité publique Canada à coordonner et financer, en 2018, un atelier sur la SGISCC à l'intention des organisations fédérales, provinciales et territoriales du secteur de la justice. Voilà qui permettrait d'entamer les discussions qui seront nécessaires pour arriver à une concrétisation chez

l'ensemble de nos partenaires. Le Comité ICT, sur demande, aidera à la planification d'un tel atelier.

Enfin, l'Association canadienne des chefs de police encourage Sécurité publique Canada à assurer le financement d'un soutien à temps partiel à l'élaboration continue de la SGISCC.

Renseignements supplémentaires

La Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes (SGISCC) s'agence avec la Stratégie d'interopérabilité des communications pour le Canada[3], et elle pourra être mise en œuvre grâce aux éléments clés suivants :

En somme, la Stratégie en matière de gestion de l'information sur la sécurité des collectivités canadiennes vise à tirer parti des personnes, des processus et de la technologie pour fournir les renseignements voulus aux personnes voulues et au moment voulu, pour favoriser un vaste environnement d'échange de renseignements au service de la sécurité des collectivités.

Notes

1. Article sur les « mythes » concernant la vie privée | *National Post* | Paola Loriggio | 20 janvier 2016 | http://news.nationalpost.com/news/canada/privacy-myths-keep-teachers-police-and-others-from-reporting-suspected-child-abuse-ontario-watchdogs
   Cet article porte sur une nouvelle enquête du coroner sur la mort d'un enfant, Jeffery Baldwin, qui appelait à l'amélioration de l'échange de renseignements entre écoles, sociétés d'aide à l'enfance, police et hôpitaux afin d'empêcher que de pareilles tragédies se reproduisent. L'article s'achève sur cette citation d'Irwin Elman, intervenant provincial en faveur des enfants et des jeunes de l'Ontario : « Il y a souvent des défaillances de points de protection, et nous ne voulons pas que ce soit en raison d'un mythe quelconque au sujet de la communication de renseignements sur les besoins d'un enfant. »

2. Expérience du Service de police de Saskatoon
   Par exemple, une personne fait une chute et se heurte la tête en sortant d'un établissement servant de l'alcool. Elle est emmenée à l'hôpital, évaluée et remise à la police pour d'autres motifs. L'hôpital refuse de communiquer des renseignements sur son état, évoquant des préoccupations de respect de la vie privée. La personne meurt plus tard en cellule. Bien qu'on ne sache pas si la communication de renseignements aurait sauvé sa vie, elle aurait pu aider à comprendre les signes d'une détérioration de son état.

3. La Stratégie d’interopérabilité des communications pour le Canada (SICC) constitue un document stratégique qui vise à fixer des objectifs et à indiquer les grandes priorités nationales en vue d’améliorer la gouvernance, la planification, la technologie, la formation et les exercices pour promouvoir les systèmes interopérables de communication vocale et de données. La SICC et son plan d’action exposent les mesures à prendre, ainsi que des étapes clés, afin d’aider les intervenants d’urgence et les représentants gouvernementaux concernés à apporter chaque année des améliorations mesurables en matière de communications usuelles et d’urgence.

Résolution 02 - 2017

COOPÉRER AVEC LES AUTORITÉS DE CONFISCATION CIVILE

Soumise par le Comité sur les amendements législatifs, au nom des autorités de confiscation civile

ATTENDU QUE l'ACCP reconnaît que la confiscation civile est un moyen efficace de dissuasion et de prévention du crime parce qu'il supprime le profit d'activités criminelles;

ET ATTENDU QUE les autorités provinciales de confiscation civile comptent largement sur les renseignements que les forces de l'ordre ont découverts dans le cadre d'enquêtes criminelles pour déterminer s'il y a lieu d'introduire une demande en confiscation civile [Les renseignements policiers sont disponibles, mais les renseignements financiers sur des personnes affirmant détenir un intérêt dans un bien ne le sont pas nécessairement. Actuellement, les renseignements détenus par des autorités fédérales comme l'Agence du revenu du Canada ou obtenus par l'entremise de CANAFE, qui pourraient être très utiles dans une procédure de confiscation civile, sont souvent disponibles seulement au moyen de demandes adressées au tribunal, ce qui est long et coûteux, ou ne sont pas disponibles en raison de restrictions prévues par la loi.];

ET ATTENDU QUE l'article 490 du *Code criminel* concerne la détention de biens saisis par nécessité aux fins d'une enquête, d'une enquête préliminaire, d'un procès ou d'autres procédures [Il décrit aussi la procédure qui s'impose en cas de demande de remise de biens saisis qui ne sont plus nécessaires à une procédure criminelle. Ces dispositions ont été rédigées bien avant l'avènement des régimes provinciaux de confiscation civile. Par conséquent, il y a des écarts entre ces dispositions visant la remise de biens et les paramètres de la préservation de biens dans le cadre d'une confiscation civile.],

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police incite le Comité de coordination des hauts fonctionnaires à mener à bien rapidement son examen détaillé de la façon dont la confiscation civile est abordée au Canada;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police encourage les gouvernements fédéral et provinciaux à collaborer à des propositions législatives et à des méthodes opérationnelles de sorte que les régimes provinciaux de confiscation civile puissent s'agencer efficacement avec les processus fédéraux et l'application des lois fédérales.

Résolution 02 - 2017

COOPÉRER AVEC LES AUTORITÉS DE CONFISCATION CIVILE

Contexte

La confiscation civile est un processus prévu par des lois provinciales, visant à supprimer le profit du crime et à dissuader les criminels. Le processus de confiscation civile autorisée par un juge peut être un mécanisme utile dans la lutte contre le crime organisé en réduisant ou en éliminant les profits d'une organisation. L'argent et les biens saisis par voie de confiscation civile sont utilisés soit pour aider à indemniser les victimes de crimes, soit à des fins utiles à la communauté.

Au Canada, la confiscation civile a commencé en 2001. L'Ontario a été la première province à adopter une loi en la matière. Depuis lors, huit provinces ont mis en place leurs propres lois et processus pour saisir les instruments et les produits d'activités illégales ainsi que les biens utilisés pour faciliter des activités illégales. L'Île-du-Prince-Édouard et Terre-Neuve-et-Labrador sont les deux seules provinces n'ayant pas de régime de confiscation civile. Parmi les territoires, seul le Nunavut est en voie d'adopter un tel régime.

Il y a deux types de confiscation civile de biens : (i) la confiscation civile où des biens peuvent être confisqués par voie de demande ou de déclaration dans les tribunaux civils, selon les règles et la norme de preuve des tribunaux civils; et (ii) la confiscation administrative où une demande initiale de confiscation peut être introduite au moyen d'un processus administratif. La confiscation civile se fonde sur une procédure *in rem* démontrant que les biens sont soit un instrument, soit un produit d'une activité illégale. La confiscation administrative permet à la province de demander la confiscation sans recourir aux procédures normales des tribunaux civils, en avisant les titulaires d'intérêts de la demande. Si un titulaire d'intérêts souhaite contester la confiscation administrative, il existe un processus lui permettant de le faire.

La Colombie-Britannique, le Manitoba et la Saskatchewan ont mis en œuvre des processus de confiscation administrative. L'Alberta a promulgué les dispositions voulues mais n'a pas encore entamé de procédure.

L'approche provinciale en matière de confiscation civile semble viser à créer le processus de confiscation civile le plus efficace en coopération avec le SPPC (le DPCP au Québec) et les organismes d'application de la loi, de sorte que la procédure civile ne nuise à aucune poursuite mais que la confiscation se fasse aussi rapidement que possible pour que le produit puisse être réinvesti dans la communauté et que les victimes du crime puissent être indemnisées efficacement.

Sans s'allonger indûment sur les détails des dispositions particulières des lois en cause, il est extrêmement important de comprendre que les renseignements sont la clé pour déterminer les paramètres précis d'une richesse illicite. La *Loi de l'impôt sur le revenu*, la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT) et le *Code criminel* contiennent tous des restrictions qui, essentiellement et du moins en partie, excluent l'utilisation de certains renseignements dans une procédure de confiscation civile. Par exemple,

l'article 241 de la *Loi de l'impôt sur le revenu* ne permet pas qu'un procureur général provincial obtienne de l'information fiscale à des fins de confiscation civile. Le paragraphe 241(4) prévoit certes une longue liste des parties auxquelles l'Agence du revenu du Canada peut communiquer des renseignements sur un contribuable, mais les autorités provinciales de confiscation civile n'y figurent pas puisque le processus provincial n'existait pas quand la liste a été établie. Il y a aussi dans la LRPCFAT une restriction interdisant à CANAFE de fournir des déclarations à des autorités de confiscation civile, même si ces autorités lui fournissent des renseignements.

Évidemment, au moment de la rédaction de ces lois fédérales, nul n'entrevoyait la possible interaction future avec le processus de confiscation civile.

Il existe des possibilités éventuelles de renforcer le processus de confiscation civile en modifiant des dispositions pertinentes de la *Loi de l'impôt sur le revenu*, de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* et du *Code criminel* afin de permettre un plus grand échange de renseignements plus tôt dans une enquête.

Le crime organisé pose une menace importante pour la sécurité publique et nuit à la vie quotidienne des Canadiens. Au Canada, l'activité du crime organisé est un problème multidimensionnel exigeant une action vaste et intégrée de la part des organismes d'application de la loi, des poursuivants et des autorités de confiscation civile. Dans son arrêt *Chatterjee*, la Cour suprême a confirmé que des régimes de confiscation civile et pénale peuvent coexister. Faisant œuvre commune pour concrétiser le changement que peut apporter la confiscation civile permettra d'adopter une démarche intégrée et de créer un environnement beaucoup plus complexe et hostile pour ceux qui tirent profit d'activités illégales.

L'ACCP sait que des travaux sont en cours avec le Comité de coordination des hauts fonctionnaires pour améliorer le processus de confiscation civile grâce à des modifications législatives qui permettraient aux autorités de confiscation civile d'obtenir plus rapidement des renseignements issus d'enquête et autres renseignements financiers. Voilà qui augmenterait la capacité de supprimer les avantages financiers des activités criminelles. L'ACCP demande aux gouvernements fédéral et provinciaux de collaborer étroitement en matière de confiscation civile.

Résolution 03 - 2017

VICTIMISATION PAR LE CYBERCRIME au CANADA :
SIGNALEMENT DES INCIDENTS ET COLLECTE DE DONNÉES

Soumise par le Comité de l'ACCP sur la cybercriminalité

ATTENDU QUE l'ACCP et ses membres, par les recommandations qu'ils ont adoptées dans le passé, ont reconnu que tout « cybercrime », quelles que soient ses motivations sous-jacentes, ses sources ou ses formes, est de fait un crime, et que comme tout crime, il crée des victimes qui méritent notre soutien, et que les corps policiers à tous les niveaux ont l'obligation, dans la mesure de leurs capacités, de prévenir le cybercrime, de poursuivre les cybercriminels et de protéger leurs collectivités;

ET ATTENDU QUE l'ACCP reconnaît qu'il y a une Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet (la « Stratégie nationale ») qui prévoit une approche globale et coordonnée visant à renforcer la protection des enfants sur Internet et à poursuivre les personnes qui se servent de la technologie pour s'en prendre aux enfants, comprenant des activités menées par Sécurité publique Canada – y compris par l'entremise du Centre canadien de protection de l'enfance et de sa centrale de signalement Cyberaide.ca, de la Gendarmerie royale du Canada et de son Centre national de coordination contre l'exploitation des enfants – et par le ministère de la Justice;

ET ATTENDU QUE la capacité de mener des actions coordonnées et efficaces de portée nationale, régionale et locale face à toutes les autres formes de victimisation par le cybercrime au Canada reste gravement entravée faute de données fiables;

ET ATTENDU QU'il existe un besoin clair et impérieux de solutions immédiates qui permettraient d'augmenter les taux de signalement par les victimes de toutes les formes d'incidents de cybercrime et de mettre en place d'autres systèmes de collecte de données qui fourniraient à la police et à ses partenaires des données complètes et exactes en vue :

- d'encourager les victimes de cybercrimes à signaler leur victimisation et la portée de ses répercussions;
- d'informer et rassurer les victimes que la police canadienne s'emploie à prévenir, atténuer et réprimer le cybercrime de diverses façons, dans toute la mesure que permet la loi;
- de promouvoir des moyens de prévention qui puissent assurer la résilience des personnes, des collectivités et des institutions;
- de créer une source fiable et constante de données statistiques aux fins d'analyse;
- de déterminer l'affectation des ressources de la police et de ses partenaires;
- d'orienter les décisions stratégiques et tactiques dans la lutte contre le cybercrime,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police demande à ses partenaires, à leurs associations et aux intervenants fédéraux, provinciaux et territoriaux de coopérer avec l'ACCP afin de promouvoir à titre de priorité nationale l'élaboration et la mise en œuvre de méthodes de signalement des cyber-incidents par le public et par les entreprises, ainsi que d'outils innovateurs de collecte de données, pour dresser un bilan continu et global des infractions relevant du cybercrime et des niveaux de victimisation s'y rapportant au Canada. Cette priorité nationale commune appellera le gouvernement du Canada, en coopération avec tous les ordres de gouvernement, à réunir les spécialistes et décideurs voulus pour cerner et mettre en œuvre des méthodes qui soient adaptables en fonction des besoins des acteurs de l'économie tout en accordant la priorité à la sécurité publique et à la protection des Canadiens. (Pour être clair, il est entendu que la présente résolution ne vise aucunement à dévier des activités entreprises dans le cadre de la Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet ou à les entraver.)

Résolution 03 - 2017

VICTIMISATION PAR LE CYBERCRIME au CANADA : SIGNALEMENT DES INCIDENTS ET COLLECTE DE DONNÉES

Résumé

Tel qu'indiqué ci-dessous, la présente proposition prévoit un appui en faveur d'une amélioration du signalement des cybercrimes et de la gestion des statistiques en la matière au Canada, dans l'intérêt des Canadiens.

Environnement actuel

La situation actuelle en ce qui concerne le signalement des cybercrimes au Canada ne procure pas une vue d'ensemble complète des incidents réels de cybercrime. Chaque cas de cybercrime fait une victime, mais notre structure actuelle de signalement ne tient pas compte de bon nombre de ces victimes, ce qui nous empêche de bien saisir l'ampleur et la dynamique changeante du problème.

Statistique Canada, par l'entremise du Comité des informations et statistiques policières (CISP), continue d'actualiser les exigences de signalement du processus de saisie de données utilisé par la police partout au Canada. Cependant, de nombreux événements surviennent en dehors du cadre d'intervention de la police. Par exemple, de nombreux cas de cybercrime concernent l'utilisation frauduleuse de cartes de crédit, et de tels incidents sont souvent gérés entièrement par les banques et les émetteurs de cartes de crédit, de sorte que les statistiques n'apparaissent pas dans le bilan global du cybercrime.

Faute d'une information complète, la situation d'ensemble quant à la nature et à l'étendue du cybercrime n'est pas connue. Il en manque les nombres totaux, les sommes d'argent en cause et les données sur les tendances qui pourraient servir à informer tant les forces de l'ordre que le public.

Par la présente résolution, l'ACCP préconise une vision holistique en la matière.

La voie à suivre

Comme l'indique la résolution elle-même, l'ACCP demande à ses partenaires, à leurs associations et aux intervenants fédéraux, provinciaux et territoriaux de coopérer avec l'ACCP afin de promouvoir à titre de priorité nationale l'élaboration et la mise en œuvre d'un ensemble de méthodes de signalement des cyber-incidents par le public et par les entreprises, ainsi que d'outils innovateurs de collecte de données, pour dresser un bilan continu et global des infractions relevant du cybercrime et des niveaux de victimisation s'y rapportant au Canada, en utilisant des méthodes qui soient adaptables en fonction des besoins des acteurs de l'économie tout en accordant la priorité à la sécurité publique et à la protection des Canadiens.

Nous devons prévoir que le signalement se fasse dans le cadre d'un processus efficace et facile, sans créer une charge de travail indue. Pour assurer la cohérence et l'exactitude du signalement,

nous devons aussi prendre en compte les nuances de cybercrime, déterminer ce qui doit être signalé et établir, de concert avec nos partenaires, des définitions et des seuils.

Nous devons utiliser les capacités actuelles et à venir pour réunir des chiffres et des faits sur les incidents de cybercrime au Canada, et trouver un moyen d'en faire rapport de façon complète et exacte. Ceci doit se faire sans dévier des activités entreprises dans le cadre de la Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet ou les entraver.

Il faudra beaucoup de coordination et de réflexion pour déterminer quelles données sur le cybercrime sont disponibles aujourd'hui, quels renseignements supplémentaires sont nécessaires, et comment il serait possible de saisir les renseignements voulus. Il faudrait aussi examiner ce qui se fait à l'étranger, pour prendre en compte les solutions adoptées par d'autres pays.

Nous sommes face à une vaste présence sur Internet de personnes cherchant à exploiter les autres de nombreuses façons : crime financier, vol d'identité, intimidation. Afin de former convenablement les policiers en techniques d'enquête et affecter judicieusement des ressources à ces nouveaux domaines de criminalité, nous devons disposer d'un moyen de saisir avec exactitude la situation, puis de suivre son évolution alors que des méthodes de cyberattaque sans cesse plus nombreuses apparaîtront à la faveur des innovations technologiques et de leur propagation dans la société.

Cette résolution cerne la tâche énorme mais vitale consistant à dresser un bilan des orientations actuelles et futures du cybercrime, et lance un appel à une action collective.

Renseignements supplémentaires

L'ACCP a déjà adopté des résolutions sur le cybercrime et des enjeux connexes. La présente résolution apporte un plan en vue d'évaluer, de signaler et de réprimer de tels crimes au Canada, dans l'intérêt des citoyens canadiens. Les précédentes résolutions pertinentes se résument comme suit :

> Dans la résolution 03-2012, l'Association canadienne des chefs de police demandait à ses partenaires, à leurs associations et aux intervenants fédéraux-provinciaux-territoriaux de travailler avec elle afin d'accélérer l'élaboration et l'adoption d'une Stratégie nationale de lutte contre la cybercriminalité, y compris des cadres de référence, des mécanismes et une structure qui mèneraient à une meilleure coordination nationale parmi les organismes d'application de la loi ainsi qu'entre eux et les gouvernements, le milieu universitaire et le secteur privé.
>
> Dans la résolution 07-2015, l'Association canadienne des chefs de police demandait à ses partenaires à leurs associations et aux intervenants fédéraux-provinciaux-territoriaux de militer collectivement en faveur de changements dans les lois, la réglementation et les politiques qui accroîtraient l'efficacité et l'efficience des enquêtes, augmenteraient les risques et les conséquences pour les délinquants, et faciliteraient le travail de la police dans divers domaines.

En somme, la résolution actuelle s'appuie sur ces mesures précédentes et reconnaît que pour prévenir efficacement le cybercrime, repérer les cybercrimes, affecter les ressources nécessaires aux organismes d'enquête et informer aussi bien le public que les forces de l'ordre, il faut un signalement complet et détaillé des cybercrimes, comme pour d'autres types de crimes. La présente résolution est un début en vue de déterminer comment le Canada peut plus efficacement mesurer et parer l'étendue véritable du cybercrime et les formes de victimisation qui en découlent.

En somme, pour prévenir efficacement le cybercrime, repérer les cybercrimes, affecter les ressources nécessaires aux organismes d'enquête et informer aussi bien le public que les forces de l'ordre, il faut un signalement complet et détaillé des cybercrimes, comme pour d'autres types de crimes. Cette résolution est un début en vue de déterminer comment le Canada peut intervenir plus efficacement face au cybercrime.