Résolutions adoptées
à la
113e Conférence annuelle

Août 2018

Halifax (Nouvelle-Écosse)

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

2018-01
Résolution sur l'élaboration rapide de politiques sur la technologie pour les systèmes des Services nationaux d'information policière (SNIP) pour l'application de la loi au Canada 3

2018-02
Des mesures législatives raisonnables pour faciliter l'accès transfrontalier à des données sur les infractions criminelles au Canada ou détenues par des fournisseurs de services canadiens 7

2018-03
Résolution d'appui en faveur de sensibilisation et de formation sur la cybercriminalité pour les forces de l'ordre canadiennes 13

2018-04
Résolution sur la réglementation des presses à comprimés 16

2018-05
Élaboration d'un modèle d'intervention face à la violence sexuelle 19

Résolution 01 - 2018

RÉSOLUTION SUR L'ÉLABORATION RAPIDE DE POLITIQUES SUR LA TECHNOLOGIE POUR LES SYSTÈMES DES SERVICES NATIONAUX D'INFORMATION POLICIÈRE (SNIP) POUR L'APPLICATION DE LA LOI AU CANADA

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

ATTENDU QUE l'Association canadienne des chefs de police (ACCP) et ses membres ont besoin de technologie fiable, sûre et moderne pour fournir des services efficaces et efficients à leurs collectivités;

ET ATTENDU QUE l'absence de politique facilitant l'adoption d'outils technologiques peut entraîner des retards pour les organismes d'application de la loi qui travaillent à la protection de leurs collectivités;

ET ATTENDU QUE l'adoption de nouveaux outils technologiques exige une politique cadre approuvée pour s'assurer que leur mise en œuvre ne crée pas des risques inutiles;

ET ATTENDU QUE la communauté de l'application de la loi attend depuis des années diverses politiques essentielles en matière de technologie;

ET ATTENDU QUE le Comité sur l'information, les communications et la technologie de l'Association canadienne des chefs de police, lors de son atelier de février 2018 à Vancouver (Colombie-Britannique), a désigné comme premières priorités pour les forces de l'ordre au Canada en matière de technologie de prévoir les moyens les plus rapides pour élaborer une politique sur l'infonuagique et une politique sur l'authentification multifactorielle pour appareils mobiles;

ET ATTENDU QUE le Comité consultatif sur les services nationaux d'information policière (CC SNIP) assure la gouvernance et la surveillance de l'ensemble des Services nationaux d'information policière (SNIP) qui soutiennent les organismes d'application de la loi et rehaussent la sécurité publique en encourageant la mise en commun d'information électronique par le biais du Réseau des Services nationaux de police, de façon rapide et coopérative;

ET ATTENDU QUE le Comité consultatif sur les services nationaux d'information policière (CC SNIP) est en outre chargé d'adopter des politiques sur la technologie élaborées par le sous-comité de la technologie de l'information du CC SNIP et d'assurer la gouvernance en la matière;

ET ATTENDU QUE le commissaire de la Gendarmerie royale du Canada (GRC) est le gardien des systèmes des Services nationaux d'information policière (SNIP) et doit respecter les politiques et les normes du Conseil du Trésor du Canada se rapportant à la gestion de l'information et à la sécurité de la technologie de l'information;

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police travaille avec le Comité consultatif sur les services nationaux d'information policière (CC SNIP) en vue d'améliorer et développer le processus utilisé pour élaborer des politiques sur la technologie, de sorte que les forces de l'ordre au Canada puissent disposer de technologies sécurisées et les mettre en œuvre rapidement;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police communique avec le gouvernement du Canada pour affirmer l'urgent besoin que les forces de l'ordre suivent l'évolution de la technologie, ce qui pourrait exiger l'élaboration de politiques du Conseil du Trésor du Canada.

Résolution 01 - 2018

RÉSOLUTION SUR L'ÉLABORATION RAPIDE DE POLITIQUES SUR LA TECHNOLOGIE POUR LES SYSTÈMES DES SERVICES NATIONAUX D'INFORMATION POLICIÈRE (SNIP) POUR L'APPLICATION DE LA LOI AU CANADA

Contexte

La communauté canadienne de l'application de la loi ne suit pas le rythme des changements dans la technologie et de leurs répercussions sur les politiques. Lors de l'atelier biennal de 2016 du Comité ICT de l'ACCP, l'élaboration d'une politique sur l'infonuagique a été désignée comme une grande priorité. À l'atelier ICT de 2018, il n'y avait toujours pas de politique sur l'infonuagique (il n'y a pas encore de lignes directrices fédérales applicables aux données protégées B dans le nuage), non plus que sur l'authentification multifactorielle pour les appareils mobiles, alors qu'il s'agit d'éléments absolument vitaux pour les efforts stratégiques de nombreux organismes d'application de la loi.

Il ne s'agit pas de critiquer les personnes en cause. Plutôt, il s'agit de viser à prévoir davantage de ressources et d'actualiser le processus d'élaboration de politiques utilisé en matière de technologie. Le but consiste à suivre le rythme et à tirer parti des innovations technologiques à l'avenir. Même s'il n'y a pas eu d'étude approfondie, trois suggestions ont été formulées qui pourraient aider à accélérer la mise au point de politiques sur la technologie. Les éléments décrits ci-dessous ont été discutés à l'atelier ICT à Vancouver; ils pourraient aider à réduire le temps nécessaire à l'élaboration de politiques. L'exemple suivant concerne l'infonuagique, mais il est pertinent aussi pour de nombreuses autres normes.

Participation / ressources de parties externes (milieu universitaire, services-conseils, industrie)

Nous semblons actuellement suivre une démarche plutôt insulaire dans l'élaboration de politiques. Le sous-comité de la technologie de l'information (SCTI) du CC SNIP élabore la politique comme telle grâce à du travail bénévole à mi-temps, en ce sens où des membres de comité qui ont un travail à temps plein auprès de corps policiers sont chargés de rédiger des textes techniques détaillés. Par conséquent, les personnes en cause ont énormément de recherche à faire, et peu de temps à y consacrer. Si le processus bénéficiait de l'apport du milieu universitaire, de services-conseils et de l'industrie, nous pourrions nous attacher à définir les besoins réels des politiques, puis collaborer avec ces intervenants pour cerner des options qui y répondent. Nous devons considérer de tels intervenants comme des experts dans les domaines des nouvelles technologies. Les entreprises de technologie mettent au point la technologie, et ont souvent une vaste expérience de sa mise en œuvre. Nous devrions nous employer à préciser ce que nous tentons d'accomplir. Aux États-Unis, l'industrie fait souvent partie du processus d'approbation avant l'adoption de toute politique. Cette façon de faire est utile, à la fois pour gagner du temps dans l'élaboration des politiques et pour accroître la longévité des politiques (en prévoyant mieux l'avenir).

Travailler avec les normes actuelles

Si nous élaborons nos propres normes pour l'infonuagique :
- il faudra plus de temps pour les élaborer;
- il faudra que le SCTI les révise constamment pour qu'elles restent à jour face à une technologie et des normes qui évoluent sans cesse, ce qui occasionnera encore des délais;
- elles pourraient devenir rapidement périmées, en raison d'imminentes évolutions techniques dont nous ne sommes pas nécessairement renseignés.

Nous devons autant que possible relier nos normes aux normes actuelles de l'industrie (sachant que dans le cas du nuage, le Conseil du Trésor du Canada n'a pas encore publié une politique portant sur les données protégées B). Par exemple, au lieu de rédiger une politique détaillée sur l'infonuagique, nous pourrions relier nos descriptions à des normes généralement acceptées, comme celles de la Cloud Security Alliance (CSA) ou des normes fédérales. La CSA compte parmi ses membres de nombreux fournisseurs du domaine de l'infonuagique ainsi qu'un éventail de spécialistes de la sécurité. Ainsi, au lieu de rédiger une politique très détaillée indiquant que « nous avons besoin des fonctions A, B et C », nous pourrions définir les exigences en fonction des descriptions de la CSA, en disant par exemple qu'il faut « au moins le niveau 4 de la CSA en ce qui concerne l'isolement géographique ». Dès lors, à mesure que les choses évoluent, nous devrions seulement apporter des ajustements mineurs, et non reprendre à neuf des descriptions détaillées.

Créer un environnement de travail approuvé (en infonuagique)

Les États-Unis ont la norme d'infonuagique des Criminal Justice Information Services (CJIS). Il s'agit d'une structure de sécurité préapprouvée qui permet aux organismes d'application de la loi de profiter de services modernes sans avoir à redéfinir tous les détails de la mise sur pied de services d'infonuagique sécurisés. Voilà qui procure aux forces de l'ordre la souplesse et les économies d'échelle qui peuvent réduire leurs coûts sur le long terme. Si un corps policier fait face à un incident majeur où des milliers d'heures de vidéo doivent être sauvegardées et gérées, il aurait un accès rapide et efficace à du stockage de masse dans un environnement infonuagique. On ignore si le Conseil du Trésor du Canada prépare une telle norme acceptée.

Les corps de police du Canada tentent de doter nos organisations de technologies dynamiques et efficaces, mais l'absence de politiques fait qu'ils prennent de plus en plus de retard par rapport à l'évolution de la technologie. Nous devons trouver des façons d'améliorer le processus d'élaboration de politiques sur la technologie en faisant qu'il se rapproche des normes de l'industrie et qu'il exige moins de travail.

Résolution 02 - 2018

DES MESURES LÉGISLATIVES RAISONNABLES POUR FACILITER L'ACCÈS TRANSFRONTALIER À DES DONNÉES SUR LES INFRACTIONS CRIMINELLES AU CANADA OU DÉTENUES PAR DES FOURNISSEURS DE SERVICES CANADIENS

Présentée conjointement par le Comité sur les amendements législatifs et le Comité sur la cybercriminalité

ATTENDU QUE de nombreuses enquêtes criminelles exigent l'accès à des preuves numériques qui se trouvent dans d'autres ressorts, y compris sur le « nuage »;

ET ATTENDU QUE l'accès transfrontalier est un des enjeux les plus pressants pour l'application de la loi partout dans le monde, en particulier en ce qui concerne l'exploitation sexuelle d'enfants, la fraude, le cyberterrorisme et le crime organisé;

ET ATTENDU QUE la procédure actuelle présente des défis à relever en ce qui concerne la collaboration volontaire de fournisseurs de services, la coopération entre corps policiers, la mise en œuvre de certaines techniques d'enquête et l'efficacité de l'entraide juridique internationale en matière pénale;

ET ATTENDU QUE les parties à la Convention de Budapest sur la cybercriminalité ont convenu le 8 juin 2017 d'entamer la préparation d'un protocole fondé sur ce traité pour aider les forces de l'ordre à obtenir des preuves se trouvant sur des serveurs dans des ressorts étrangers, multiples ou inconnus;

ET ATTENDU QUE ce protocole pourrait comprendre des dispositions sur des éléments tels que : (i) une entraide juridique plus efficace; (ii) une plus grande coopération avec des fournisseurs de services dans d'autres ressorts; (iii) un cadre de référence clair et des moyens de protection plus rigoureux pour l'accès transfrontalier à des données; et (iv) des moyens de protection particuliers, y compris des exigences sur la protection des données;

ET ATTENDU QUE le Canada est partie à cette Convention et participe à ce travail;

ET ATTENDU QUE les États-Unis d'Amérique ont adopté le 23 mars 2018 la *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*) (H.R. 4943);

ET ATTENDU QUE cette loi prévoit, entre autres, une procédure accélérée d'entraide juridique par le biais d'accords bilatéraux avec d'autres pays pour la communication à ces pays, selon des modalités simplifiées, de données sur des citoyens, des résidents permanents ou des personnes morales des États-Unis dès lors que le procureur général, en accord avec le secrétaire d'État, est d'avis que le pays présente des moyens suffisants pour limiter l'accès aux données sur ces personnes,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police appuie la participation du Canada aux négociations sur le 2e protocole additionnel à la Convention de Budapest sur la cybercriminalité visant à parer aux difficultés de l'accès transfrontalier à des preuves numériques en matière criminelle;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police exhorte le gouvernement du Canada à négocier un accord bilatéral d'échange de données avec les États-Unis d'Amérique ainsi qu'y autorise la *CLOUD Act*;

IL EST EN OUTRE RÉSOLU QUE l'Association canadienne des chefs de police demande au gouvernement du Canada de s'engager à mener des consultations en bonne et due forme avec l'ACCP dans la mise au point de ces instruments.

Résolution 02 - 2018

DES MESURES LÉGISLATIVES RAISONNABLES POUR FACILITER L'ACCÈS TRANSFRONTALIER À DES DONNÉES SUR LES INFRACTIONS CRIMINELLES AU CANADA OU DÉTENUES PAR DES FOURNISSEURS DE SERVICES CANADIENS

Contexte

Le 23 mars 2018, le Congrès des États-Unis a adopté la *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, et le président l'a sanctionnée. Visant à régler des problèmes liés aux demandes de communication transfrontalière de données aux forces de l'ordre à l'ère du courrier électronique et de l'infonuagique, la *CLOUD Act* autorise les États-Unis à conclure des accords bilatéraux d'échange de données et précise qu'un mandat adressé à un fournisseur de services peut porter sur des données conservées à l'étranger si ces données sont en la possession, sous la garde ou sous le contrôle du fournisseur de données. Le sénateur Orrin Hatch a fait remarquer que « l'accord bilatéral cadre entre les États-Unis et le Royaume-Uni décrit dans la *CLOUD Act* est destiné à servir de modèle pour de futurs accords entre les États-Unis et d'autres pays » et que « la mise en œuvre d'accords semblables avec ... des alliés est vitale pour protéger les consommateurs dans le monde entier et pour faciliter des enquêtes légitimes d'application de la loi ». Le gouvernement du Royaume-Uni et de grandes entreprises technologiques des États-Unis soutiennent la *CLOUD Act*.

Au Canada, les forces de l'ordre sont confrontées aux mêmes défis dans leurs enquêtes, et elles ont besoin de mesures semblables. Par exemple, un grand nombre d'enquêtes sur l'exploitation d'enfants sur Internet exigent l'accès à des preuves numériques conservées dans d'autres ressorts, y compris sur le nuage. Il en va de même pour la fraude, le cyberterrorisme et le crime organisé. Les forces de l'ordre ont besoin de mesures législatives raisonnables, conformes à la Constitution, adaptées au contexte canadien et respectant les règles de bonne entente internationale qui fournissent un cadre de référence permettant à des fournisseurs de services de donner suite à des demandes d'information autorisées par un juge tout en protégeant la vie privée des utilisateurs.

L'infonuagique, l'accès Internet haute vitesse et les appareils mobiles branchés en continu ont des répercussions pour la capacité des forces de l'ordre de reconnaître, recueillir et analyser des preuves numériques. Ces technologies apportent d'innombrables avantages aux Canadiens, mais elles présentent aussi des problèmes. Par exemple, les services de messagerie vocale et par texte sont en voie d'être remplacés par des outils de communication comme WhatsApp et TextMe[1]. Au contraire des entreprises de télécommunication du Canada, la plupart des fournisseurs de services de communication au moyen d'applis conservent leurs données dans divers ressorts.

Le recours croissant des Canadiens à des plateformes en ligne a été souligné dans les consultations que Sécurité publique Canada a menées auprès des Canadiens en 2018. Les participants ont indiqué qu'il est très difficile d'obtenir un accès rapide à des preuves numériques et qu'il faudrait des mesures législatives pour clarifier les rôles et responsabilités, favoriser la rapidité et l'efficacité des enquêtes et permettre l'échange d'information entre organismes

[1] E. Balkovich et coll., *Electronic Surveillance of Mobile Devices – Understanding the Mobile Ecosystem and Applicable Surveillance Law*, RAND Corporation (2015).

d'application de la loi canadiens et transnationaux[2]. L'information fournie pendant ces consultations traduisait la reconnaissance par le gouvernement de la nécessité de méthodes innovatrices, de solutions nouvelles et de collaboration avec des partenaires pour lutter contre des crimes au pays et à l'échelle internationale, par exemple en matière de traite de personnes et d'exploitation sexuelle d'enfants[3].

Les lois et procédures actuelles causent de longs délais et de la confusion

Les forces de l'ordre du Canada recourent souvent à la *Loi sur l'entraide juridique en matière criminelle* pour obtenir l'accès à de l'information conservée à l'étranger ou par des fournisseurs de services établis à l'étranger. Dans son rapport de 2013 intitulé *Liberty and Security in a Changing World*, le groupe d'examen du président des États-Unis sur le renseignement et les technologies de communication indiquait qu'il fallait environ 10 mois pour répondre à une demande de dossiers de courriel présentée au titre de l'entraide juridique. De récents exemples canadiens mettent en lumière les sources d'inefficacité et de retards dans les processus d'entraide juridique :

- Les dossiers de Google demandés pour une enquête sur une affaire de pornographie infantile n'ont été reçus que 14 mois après que la demande a été présentée au titre de l'entraide juridique. Pendant ce temps, la Couronne ne pouvait pas prendre position sur un règlement, et l'avocate de la défense ne pouvait pas évaluer convenablement la responsabilité de son client.

- Au cours d'une vaste enquête sur un cas de fraude, de multiples demandes ont été adressées à Microsoft, Yahoo et Google, et il a fallu 22 mois pour recevoir une partie des dossiers. Le reste de l'information a été fourni 25 mois après que la demande d'entraide juridique avait été présentée.

Comme l'indiquent ces exemples, la lourdeur et la lenteur de la procédure d'entraide juridique sont incompatibles avec les besoins opérationnels des enquêtes et ne tiennent pas compte du fait que tous les États ne disposent pas de services de liaison spécialisés pour faciliter le travail de corps de police étrangers.

Dans l'affaire *Brecknell*, la Cour d'appel de la Colombie-Britannique a récemment fait remarquer que le strict respect de la territorialité est inacceptable à une époque où les criminels et les technologies de communication ne respectent pas les frontières nationales :

> *Le fait est que des activités criminelles telles que trafic de personnes, pornographie infantile, blanchiment d'argent, fraude commerciale et terrorisme international menées par voie électronique peuvent être à l'abri des enquêtes si une ordonnance de communication est considérée comme étant appliquée là où les données sont conservées et est par conséquent inapplicable car extraterritoriale. Un tel résultat équivaut à inviter*

[2] Sécurité publique Canada, *Lutter contre l'exploitation sexuelle des enfants en ligne : Partager les connaissances, renforcer la sécurité – Consultation fermée* (2018). https://www.canada.ca/fr/services/police/servicespolice/consultation-lutter-contre-exploitation-sexuelle-enfants-en-linge.html.

[3] Sécurité publique Canada, *Plan ministériel 2017-2018* (2017).

> *les criminels à dissimuler leur activité visant un ressort en s'assurant que l'information sur leurs communications est conservée dans un autre ressort.*
>
> *Il est notoire que les fournisseurs de services déplacent souvent l'information de leurs clients dans le monde entier, sans doute pour des raisons commerciales parfaitement légitimes, et il semble qu'ils fragmentent souvent les données et les sauvegardent en différents lieux. Le résultat, même s'il n'est pas intentionnel, est parfois effectivement de faire obstacle à des enquêtes sur de graves comportements criminels.*

Certains tribunaux ont permis l'accès à des données conservées à l'étranger quand elles sont « accessibles » à une personne au Canada (p. ex., une section ou une filiale) : *eBay Canada Ltd. c. M.R.N.*, [2010] 1 RCF 145, paragr. 48 à 52. Dans d'autres cas, des sociétés locales ont été contraintes à une divulgation dans un ressort même si les données n'y étaient pas conservées et accessibles. La décision du juge Gorman dans l'affaire *In the Matter of an application to obtain a Production Order pursuant to section 487.014 of the Criminal Code of Canada* souligne l'état incertain du droit :

> [TRADUCTION] *Je ne suis pas en désaccord avec la Cour d'appel. Le crime international crée des difficultés pour les enquêteurs, bien que des accords internationaux visent à les surmonter (voir la* Loi sur l'entraide juridique en matière criminelle*, L.R.C. 1985). Cependant, le raisonnement de la Cour d'appel donne préséance au résultat souhaité par rapport à la juste interprétation de la disposition.*

D'autres problèmes liés à la territorialité ont aussi été constatés, comme la reconnaissance juridique, à l'étranger, de certaines techniques d'enquête clandestines, la notification des personnes dont les renseignements sont demandés, l'absence de réglementation exigeant que les télédiffuseurs aient un bureau dans les pays où ils diffusent, ou que les fournisseurs de services de TI ou de télécommunication obtiennent confirmation de l'identité de leurs clients et conservent cette information pendant une période donnée.

Une solution possible – Des accords bilatéraux et multilatéraux

La *CLOUD Act* évoquée plus haut est un exemple de loi qui respecte la bonne entente internationale, fournit un cadre de référence pour les forces de l'ordre et les fournisseurs de services, et protège la vie privée des utilisateurs. Ainsi, elle autorise les États-Unis à conclure des accords bilatéraux réciproques d'échange d'information avec des gouvernements étrangers admissibles. Les accords réciproques éliminent les obstacles à la divulgation aux forces de l'ordre dans les deux pays. La *CLOUD Act* précise aussi qu'un mandat visant un fournisseur de services de communication aux États-Unis peut englober toutes les données en sa possession ou sous son contrôle où qu'elles se trouvent.

La *CLOUD Act* a créé un processus intégré d'accès à des données. Elle favorise la transparence en autorisant les fournisseurs de services à communiquer au gouvernement d'un pays étranger le fait qu'il a reçu un mandat visant de l'information qui se trouve dans ce pays. Elle donne aussi aux fournisseurs de services la possibilité de contester un mandat visant des données conservées à l'étranger si le fait d'y donner suite constituerait une violation des lois d'un gouvernement étranger.

La *CLOUD Act* constitue un cadre de référence pour un accord bilatéral efficace respectant les garanties constitutionnelles canadiennes. Un tel accord serait un grand progrès pour l'efficacité de la lutte contre la criminalité. Le Canada pourrait donc négocier un accord avec les États-Unis d'Amérique en vertu de la *CLOUD Act*.

Diverses initiatives internationales ont été lancées face au problème de l'accès transfrontalier à des données, y compris la *Convention sur la cybercriminalité* (Convention de Budapest) adoptée par le Conseil de l'Europe. Cette convention sert de référence pour les pays préparant des lois sur la cybercriminalité et pour la coopération entre les 57 États parties.

Le projet de deuxième protocole additionnel à la Convention de Budapest vise à parer aux difficultés de l'accès transfrontalier à des preuves numériques en matière de justice criminelle. Le contenu de ce protocole fait encore l'objet de discussions entre les États parties, mais il pourrait comprendre des dispositions visant à assurer : (i) une entraide juridique plus efficace; (ii) une coopération plus grande ou plus directe avec des fournisseurs de services dans d'autres ressorts; (iii) un cadre de référence clair et des moyens de protection plus rigoureux pour l'accès transfrontalier à des données; et (iv) des moyens de protection particuliers, y compris des exigences sur la protection des données. Le Canada est partie à la Convention et participe au travail du comité. La poursuite de discussions avec les États parties sur des mécanismes pour l'accès transfrontalier efficace à des données qui respectent la souveraineté et les droits de la personne est essentielle pour que les forces de l'ordre disposent des outils voulus pour faire enquête sur la criminalité transnationale.

L'affaire *Microsoft Corp. v. United States* démontre pourquoi des mesures législatives et des accords internationaux sont préférables à l'incertitude et aux litiges. Microsoft refusait de fournir des courriels conservés en Irlande même si un juge américain avait délivré un mandat. Microsoft soutenait que la loi en cause n'était pas applicable en Irlande. La question a été réglée lorsque la *CLOUD Act* a été adoptée.

L'Association canadienne des chefs de police demande une consultation en bonne et due forme avec le gouvernement du Canada relativement au 2^{e} protocole à la Convention de Budapest sur la cybercriminalité, et relativement à la conclusion d'un accord bilatéral avec les États-Unis en vertu de la *CLOUD Act*.

Résolution 03 - 2018

RÉSOLUTION D'APPUI EN FAVEUR DE SENSIBILISATION ET DE FORMATION SUR LA CYBERCRIMINALITÉ POUR LES FORCES DE L'ORDRE CANADIENNES

Présentée par le Comité sur les ressources humaines et l'apprentissage en consultation avec le Comité sur la cybercriminalité

ATTENDU QUE la cybercriminalité est un grand enjeu pour la sécurité publique et l'application de la loi, menaçant les Canadiens et les entreprises, y compris le bien-être sur les plans social et économique, qui, même si elle n'est pas toujours signalée par le public, semble être en hausse puisque près de 24 000 cybercrimes ont été signalés aux services de police canadiens en 2016, 58 % de plus qu'en 2014;

ET 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 ATTENDU QU'en août 2014, le conseil d'administration de l'ACCP a reconnu l'importance croissante de la cybercriminalité, affirmant que le phénomène remet en cause les compétences, les aptitudes, les rôles et les modes d'intervention traditionnels de la police;

ET ATTENDU QU'au moment où les forces de l'ordre du Canada s'adaptent à ce paradigme des services policiers, une formation de pointe doit être assurée pour leur fournir les compétences nécessaires à la détection, aux enquêtes et à la prévention en matière de cybercriminalité, étant entendu qu'une formation efficace sous-tend tous les efforts consacrés à la lutte contre la cybercriminalité, y compris la création de l'Unité nationale de coordination de la lutte contre la cybercriminalité et les équipes d'enquête sur la cybercriminalité que le gouvernement du Canada a annoncées dans le budget de 2018;

ET ATTENDU QUE les forces de l'ordre au Canada, en général, ne reçoivent pas de sensibilisation et de formation adéquates en matière de cybercriminalité, ce qui limite leur capacité de lutter efficacement contre la cybercriminalité et de soutenir les victimes canadiennes;

ET ATTENDU QUE la mesure dans laquelle les organismes d'application de la loi au Canada fournissent de la formation sur la cybercriminalité à leur personnel est variable, nombre d'entre eux comptant surtout, voire entièrement, sur le Collège canadien de police, qui offre en la matière une formation standardisée et uniformisée aux organismes d'application de la loi de tout le Canada[4];

[4] Le Collège canadien de police offre environ 15 différents cours et ateliers abordant la cybercriminalité ou l'expertise judiciaire en informatique, pour environ 820 étudiants chaque année.

ET ATTENDU QUE la capacité du Collège canadien de police de fournir de la formation entièrement à jour et d'offrir des cours a été sensiblement limitée, si bien que l'offre ne satisfait pas à la demande des services de police de l'ensemble du Canada car les cours affichent généralement complet et il y a de longues listes d'attente;

ET ATTENDU QU'il existe un besoin clair et impérieux d'augmenter la capacité du Collège canadien de police d'offrir de la sensibilisation et de la formation en matière de cybercriminalité,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police demande au gouvernement du Canada d'harmoniser à l'échelle nationale la formation sur la cybercriminalité fournie à l'ensemble du milieu canadien de l'application de la loi et d'accroître l'importance accordée à la formation et à la sensibilisation en matière de cybercriminalité au Collège canadien de police, de façon à ce que les forces de l'ordre au Canada aient les compétences et la capacité voulues pour lutter contre la cybercriminalité au 21^{e} siècle.

Résolution 03 - 2018

RÉSOLUTION D'APPUI EN FAVEUR DE SENSIBILISATION ET DE FORMATION SUR LA CYBERCRIMINALITÉ POUR LES FORCES DE L'ORDRE CANADIENNES

Contexte

La cybercriminalité a de grandes répercussions sur la sécurité et le bien-être économique des Canadiens et des entreprises, et elle victimise régulièrement des membres vulnérables de notre société. Aucune organisation ne peut à elle seule vaincre la cybercriminalité. Même si la cybercriminalité semble être largement sous-déclarée, près de 24 000 cybercrimes ont été signalés aux corps de police canadiens en 2016, soit 58 % de plus qu'en 2014.

La cybercriminalité appelle à de nouvelles façons d'aborder les services policiers et la formation. Les forces de l'ordre, partout au Canada et dans le monde entier, sont de plus en plus confrontées à la cybercriminalité, et reconnaissent qu'il faut un changement du paradigme policier pour y réagir. Cependant, il y a de grandes lacunes dans les connaissances et les compétences qui seraient nécessaires pour combattre efficacement la cybercriminalité. Il manque aux forces de l'ordre canadiennes une formation adéquate face à la cybercriminalité et des unités de première ligne pour repérer et poursuivre les cybercriminels.

Dans le budget de 2018, le gouvernement du Canada avait annoncé 201,3 millions de dollars sur cinq ans, et ensuite encore 43 millions par année pour créer, à la GRC, l'Unité nationale de coordination de la lutte contre la cybercriminalité et augmenter le nombre d'équipes d'enquête de la GRC chargées d'enquêtes sur des cybercrimes à l'échelle fédérale. Cet effort accru du gouvernement du Canada consacré à la lutte contre la cybercriminalité a entraîné un besoin urgent d'améliorer et d'étendre la formation sur l'application de la loi face à la cybercriminalité.

En tant que service national de police pour l'ensemble de la communauté des forces de l'ordre du Canada, le Collège canadien de police (CCP) est idéalement placé pour fournir de la formation sur la cybercriminalité à tout le milieu canadien de l'application de la loi. En 2015, le gouvernement du Canada a investi dans une telle formation en finançant quatre nouveaux postes à temps plein à l'Institut d'apprentissage en criminalité technologique (IACT) du CCP. Malgré tout, la capacité du CCP d'offrir la formation la plus à jour et d'organiser un grand nombre de cours sur la cybercriminalité est restée limitée. Actuellement, le CCP ne satisfait pas à la demande des corps de police du Canada. Il faudrait accroître l'effort consacré par le CCP à la formation et la sensibilisation en matière de cybercriminalité, en partenariat avec d'autres écoles de police, pour que les forces de l'ordre du Canada soient prêtes à combattre la cybercriminalité et à répondre aux besoins policiers du 21^{e} siècle.

L'ACCP a déjà adopté des résolutions sur la cybercriminalité et sur des enjeux connexes. La présente résolution s'inscrit dans leur lignée, étant entendu que les connaissances et les compétences pertinentes sont nécessaires à tous les efforts déployés par les forces de l'ordre pour combattre la cybercriminalité. À défaut de solution au déficit de formation et aux problèmes connexes des forces de l'ordre du Canada, la capacité de combattre la cybercriminalité sera entravée.

Résolution 04 - 2018

RÉSOLUTION SUR LA RÉGLEMENTATION DES PRESSES À COMPRIMÉS

Présentée par le Comité consultatif sur les drogues

ATTENDU QUE l'utilisation illicite de presses à comprimés a augmenté l'offre de drogues de rue contenant des opioïdes synthétiques comme le fentanyl;

ET ATTENDU QUE le phénomène cause une crise de santé publique dans des collectivités de toutes les régions du Canada;

ET ATTENDU QUE les modifications de 2017 à la *Loi réglementant certaines drogues et autres substances* (projet de loi C-37) ne fournissent pas des mesures efficaces pour contrer l'importation et la fourniture au pays de presses à comprimés destinées à des fins illicites,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police demande à Sécurité publique Canada de protéger les Canadiens en modifiant encore la *Loi réglementant certaines drogues et autres substances* de façon à soumettre les personnes qui importent des presses à comprimés à des vérifications rigoureuses, à exiger qu'elles précisent l'utilisation qui sera faite des presses à comprimés et à réglementer la vente des presses à comprimés au pays.

Résolution 04 - 2018

RÉSOLUTION SUR LA RÉGLEMENTATION DES PRESSES À COMPRIMÉS

Contexte

En 2018, il y a eu dans l'Ouest canadien une augmentation dramatique des morts par surdose. Cette augmentation peut être attribuée en partie à la reformulation de l'opioïde Oxycontin. En 2012, Oxycontin a été remplacé par OxyNEO, un produit résistant à l'altération. Ce changement visait à réduire le détournement illégal d'Oxycontin à des fins non médicales. La conséquence malheureuse et imprévue du fait que les opioïdes détournés sont devenus plus difficiles à trouver sur la rue a été l'ouverture du marché illicite d'opioïdes à des pilules d'Oxycontin contrefaites – au fentanyl.

Le crime organisé et les revendeurs de rue ont commencé à acheter du fentanyl et des produits analogues, et à fabriquer des comprimés d'« Oxy 80 » à vendre sur la rue. Le matériel industriel nécessaire – presses à comprimés, moules, étampes, instruments d'encapsulation et trieurs de pilules – a été acheté et importé légalement. Nos efforts visant à entraver ce marché illégal ont été minés par la facilité avec laquelle ce matériel peut être acheté et importé. Diverses enquêtes ont révélé la grande quantité de pilules qui peut être produite pour la vente en rue grâce à ces presses à comprimés industrielles.

Malheureusement, la crise des opioïdes continue de produire des effets dévastateurs partout au Canada. En 2016, la Colombie-Britannique a déploré 982 décès par surdose; en 2017, jusqu'au 31 août, il y en a eu 1013. Dans environ 90 % de ces décès, du fentanyl a été détecté. En 2017, partout au Canada, les décès par surdose liés à des opioïdes ont augmenté.

En 2017, le projet de loi C-37 modifiant la *Loi réglementant certaines drogues et autres substances* a reçu la sanction royale. Il a fourni de précieux outils pour aider les forces de l'ordre à entraver l'importation et la production d'opioïdes. Un outil essentiel face à la crise des opioïdes est la réglementation des presses à comprimés et des instruments d'encapsulation, faisant qu'il soit plus difficile pour les trafiquants de produire des pilules contrefaites en grandes quantités. Malheureusement, le projet de loi C-37 n'allait pas assez loin pour empêcher l'importation de presses à comprimés pour des fins illicites. En particulier :

- il ne prévoyait pas de contrôle rigoureux des personnes et entreprises important des presses à comprimés et des instruments d'encapsulation;
- il n'exigeait pas que les importateurs indiquent l'utilisation prévue;
- il ne comprenait pas de moyens de contrôle de la vente de presses au pays ou de la revente de presses importées;
- il ne conférait pas à l'Agence des services frontaliers du Canada la gamme complète des pouvoirs, en vertu de la *Loi réglementant certaines drogues et autres substances*, d'arrestation et d'accusation pour importation illégale de presses à comprimés.

Les pilules contrefaites contenant du fentanyl et des produits analogues continuent d'être offertes sur les marchés des drogues illicites partout au Canada. Les interventions des forces de l'ordre dans des laboratoires de drogues démontrent que des presses à comprimés, des instruments d'encapsulation, des étampes et des moules sont largement utilisés dans la production de pilules contrefaites. Le resserrement de la réglementation aidera les forces de l'ordre à entraver la distribution de pilules contrefaites illicites de fentanyl.

Résolution 05 - 2018

ÉLABORATION D'UN MODÈLE D'INTERVENTION FACE À LA VIOLENCE SEXUELLE

Présentée par le Comité sur la prévention du crime, la sécurité, la santé et le bien-être des communautés et le Comité sur les victimes d'actes criminels

ATTENDU QUE le Comité sur la prévention du crime, la sécurité, la santé et le bien-être des communautés (CPCSSBC) compte parmi ses objectifs stratégiques de repérer de nouveaux modèles de démarches collaboratives et intégrées pour la sécurité, la santé et le bien-être des communautés;

ET ATTENDU QUE le Comité sur les victimes d'actes criminels compte parmi ses objectifs stratégiques de promouvoir des pratiques efficaces et de favoriser l'innovation au service des victimes d'actes criminels;

ET ATTENDU QUE selon les estimations, la violence sexuelle se produit plus de 600 000 fois par année dans les collectivités canadiennes et reste un des crimes qui sont le moins signalés au Canada, entraînant chez les victimes des troubles psychologiques, le syndrome de stress post-traumatique et des idées suicidaires;

ET ATTENDU QUE la violence sexuelle peut être contrée le plus efficacement en appliquant les principes fondamentaux de la police communautaire contemporaine et par la collaboration entre la police et d'autres secteurs (éducation, prévention, intervention, action, soutien, évaluation);

ET ATTENDU QUE le conseil d'administration de l'ACCP a encouragé tous les corps de police à réviser leurs pratiques dans les enquêtes sur la violence sexuelle et que le Comité de l'ACCP sur les victimes d'actes criminels et le CPCSSBC ont formulé des recommandations quant aux pratiques exemplaires et les diffusent dans l'ensemble du milieu policier;

ET ATTENDU QUE le groupe de travail sur l'action face à la violence sexuelle regroupe des dirigeants de corps policiers et d'organisations communautaires possédant une expertise en la matière;

ET ATTENDU QUE le modèle d'intervention face à la violence sexuelle est un programme collaboratif visant à assurer une intervention axée sur la victime dans les cas de crimes de violence sexuelle. Le modèle fait la promotion d'enquêtes recourant à des pratiques exemplaires, fondées sur des données probantes et tenant compte des traumatismes en cause;

ET ATTENDU QUE l'ACCP s'est déjà prononcée en faveur de normes nationales comme moyen de promouvoir des principes communs,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police demande au gouvernement du Canada d'approuver et de soutenir le projet d'élaborer un modèle d'intervention face à la violence sexuelle.

Résolution 05 - 2018

ÉLABORATION D'UN MODÈLE D'INTERVENTION FACE À LA VIOLENCE SEXUELLE

Contexte

En février 2017, le *Globe and Mail* a publié un article sur la façon dont la police traite les allégations d'agression sexuelle. Des données recueillies auprès de plus de 870 corps de police indiquent des lacunes dans le processus d'enquête contribuant à cette malheureuse statistique : une allégation d'agression sexuelle sur cinq est classée comme non fondée.

Le *Globe and Mail* rapportait qu'en moyenne, les corps de police canadiens classent sans suite 19 % de toutes les allégations d'agression sexuelles, les jugeant non fondées (entre 2010 et 2014).

En conséquence, partout au pays, les corps de police ont réexaminé plus de 37 000 dossiers. La codification DUC (Déclaration uniforme de la criminalité) était de toute évidence un facteur important du nombre d'enquêtes aboutissant à une conclusion d'absence de fondement. Ainsi, 6348 dossiers classés comme non fondés avaient en fait été mal classés.

Selon le *Globe and Mail*, 402 dossiers ont été rouverts par suite des examens, et il s'est avéré que des accusations criminelles auraient dû être portées dans une demi-douzaine de cas. Cette constatation a soulevé des préoccupations légitimes, et les corps de police ont approfondi la question pour en trouver la cause dans le processus d'enquête. Parmi les problèmes cernés figurent une formation inadéquate en pratiques tenant compte des traumatismes vécus, des techniques d'entrevue dépassées et la persistance de « mythes au sujet du viol » chez des intervenants du système de justice.

En octobre 2017, un groupe de travail de dirigeants policiers a été mis sur pied pour créer un cadre visant à garantir que la réaction de la police aux plaintes de violence sexuelle soit coordonnée, efficace et axée sur la victime. Le but consiste à mettre au point un cadre provincial cohérent et complet définissant un modèle standardisé d'examen des cas d'agression sexuelle – un modèle canadien. Le groupe de travail s'y emploie, élaborant un modèle qui comprendra des examens trimestriels de tous les dossiers non fondés, un examen de l'ensemble ou d'un échantillon des dossiers qui n'ont donné lieu à aucune accusation, qui sont inactifs (aucune mesure supplémentaire prévue) et qui répondent aux critères du Commissariat à la protection de la vie privée justifiant un examen, y compris tous les dossiers de violence familiale comportant une composante d'agression sexuelle. Il envisage aussi l'examen de toutes les enquêtes sur la traite de personnes.

Il est prévu que le groupe de travail continuera d'élaborer des pratiques exemplaires pour des enquêtes fondées sur des données probantes et tenant compte des traumatismes vécus, et pour améliorer l'aide apportée aux victimes de crimes sexuels. Le cadre comprendra une terminologie et une compréhension communes de la violence sexuelle, qui serviront parmi les corps de police et dans la collaboration avec les partenaires de la communauté. Ce cadre bénéficiera des efforts collectifs d'experts en la matière des milieux policier, universitaire et

communautaire. Le cadre s'appuiera sur les recherches et les pratiques d'avant-garde et sera destiné à servir de guide fondamental permettant aux organismes policiers municipaux, régionaux, provinciaux et nationaux d'élaborer leurs propres politiques.

Le groupe de travail a mené des consultations et des recherches (principalement par sondage) pour évaluer le besoin d'un cadre cohérent. Les faits suivants s'en sont dégagés :

- 68 % des services ont entamé ou envisagent un processus d'examen semblable à celui que propose le groupe de travail;
- 72 % des services interrogés prévoient mener à bien des examens annuels avec des organismes communautaires, mais doivent surmonter des obstacles, par exemple manque de fonds, besoin de pratiques exemplaires uniformisées et l'établissement de protocoles d'entente;
- 62 % ont indiqué que les agents ont besoin de formation supplémentaire sur les pratiques tenant compte des traumatismes dans le cadre de leurs enquêtes;
- 52 % n'avaient pas établi de protocole d'entente, et 79 % étaient au courant des lignes directrices du Commissariat à la protection de la vie privée.

Il est évident qu'une ligne directrice sur les pratiques exemplaires, indiquant le moyen le plus efficace et le plus prudent d'aborder la violence sexuelle, est nécessaire non seulement à l'échelle provinciale, mais à l'échelle du pays. Ce groupe, représentant 18 services de police, a les moyens d'aboutir à un produit qui pourra être adopté aisément par les corps de police.