Conseil de l'Europe
Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Consultations, 2023

Objet des consultations

- La lutte contre la cybercriminalité est une priorité absolue du gouvernement du Canada.
- Le gouvernement s'adresse aux parties prenantes pour connaître leurs points de vue sur un traité international récemment signé par le Canada : *le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques du Conseil de l'Europe* (Protocole), qui vise à lutter contre la cybercriminalité et à recueillir des preuves électroniques des crimes en général.
- Ce Protocole fournirait aux forces de l'ordre de nouveaux outils pour mieux accéder aux preuves électroniques dans d'autres pays afin de lutter contre la criminalité, tout en prévoyant des mesures de protection des renseignements personnels.
- Les commentaires sont destinés à permettre au gouvernement d'effectuer ce qui suit :
  - mieux évaluer les conséquences possibles de ce Protocole;
  - comprendre les préoccupations relatives aux outils et aux mesures de protection de la vie privée; et
  - envisager l'élaboration de nouvelles lois ou de nouveaux processus pour permettre au Canada de ratifier (d'approuver officiellement) et de mettre en œuvre le Protocole.

Contexte

- Les technologies numériques présentent d'énormes avantages, mais elles sont malheureusement aussi à l'origine de certaines menaces.

- Les criminels et autres auteurs de cybermenaces, dont beaucoup opèrent en dehors de nos frontières, profitent des lacunes en matière de sécurité, du manque de connaissances en matière de cybersécurité et des progrès technologiques pour commettre des crimes.

- Ils volent des renseignements personnels et financiers, de la propriété intellectuelle et des secrets industriels. Ils perturbent et parfois détruisent des systèmes informatiques, des réseaux et même des infrastructures sur lesquels comptent les services essentiels et le mode de vie.

Qu’est-ce que la cybercriminalité?

- La cybercriminalité et les crimes qui s’y rapportent comprennent les infractions qui :
  - visent à endommager un appareil tel qu’un ordinateur (par exemple, un virus, un piratage informatique), un téléphone cellulaire ou un réseau, ou les données de ces appareils (la technologie étant la cible); ou
  - sont commises au moyen d’un appareil tel qu’un ordinateur ou un téléphone cellulaire, et autres (par exemple, matériel d’exploitation sexuelle d’enfants; extorsion au rançongiciel) (la technologie en tant qu’instrument pour commettre des crimes).
- Elle peut être d’origine nationale ou transnationale.

Les défis liés à la lutte contre la cybercriminalité

- Les éléments de preuve électroniques d'une cybercriminalité ou d'une infraction liée à la cybercriminalité sont souvent stockées dans plus d'un pays.
- Il peut être très difficile et lent pour les enquêteurs du monde entier d'utiliser l'outil existant de l'**entraide judiciaire** pour obtenir des éléments de preuve électroniques dans d'autres pays afin de les aider dans leurs enquêtes et leurs poursuites.
- Par conséquent, seule une très faible part des cybercrimes signalés donne lieu à des poursuites.
- C'est pourquoi le gouvernement du Canada cherche à saisir les opportunités, comme le Deuxième Protocole additionnel, pour assurer la sécurité des Canadiens face à la cybercriminalité.

Convention sur la cybercriminalité du Conseil de l'Europe

- Le Canada est partie à la *Convention sur la cybercriminalité* du Conseil de l'Europe (dite « *Convention de Budapest* »).
- Il s'agit d'un traité international qui fournit aux États qui y sont parties des outils pour faciliter les enquêtes et les poursuites en matière de cybercriminalité et de crimes s'y rapportant.
- Le Deuxième Protocole additionnel, récemment signé par le Canada, est une nouvelle partie additionnelle de la *Convention de Budapest* et fournit des outils renforcés pour les forces de l'ordre et les procureurs de la Couronne.

Deuxième Protocole additionnel

- Le Deuxième Protocole additionnel fournit un cadre qui aurait pour but de :
  - permettre aux pays de partager les éléments de preuve électroniques d'un cybercrime et de crimes en général;
  - permettre à un pays de rechercher des renseignements directement auprès d'un fournisseur de services (une entreprise de télécommunications ou de médias sociaux) pour obtenir des renseignements spécifiques (par exemple, des renseignements sur l'abonné, comme le nom ou l'adresse); et
  - protéger les droits de la personne et veiller à ce que des garanties en matière de protection des données à caractère personnel soient en place.
- Le Protocole créerait une procédure plus directe pour demander des éléments de preuve électroniques, offrir des solutions de rechange aux mécanismes d'entraide juridique qui ne sont généralement pas bien équipés pour traiter des volumes élevés de demandes nécessitant une production rapide.

Quelles sont les garanties?

- Le Protocole détermine les pouvoirs et les procédures (« mesures ») destinés à faciliter la prévention, la détection, les enquêtes et les poursuites en matière de cybercriminalité. Ces mesures peuvent avoir une incidence sur les droits.
- Il est important de noter que le Protocole fixe également des conditions et des garanties visant à assurer la protection des droits de la personne et des libertés fondamentales, ainsi que des exigences en matière de protection des renseignements personnels et de la vie privée, notamment en imposant des restrictions quant aux fins auxquelles les données obtenues peuvent être traitées et utilisées, en limitant le partage ultérieur, en veillant à ce que les données à caractère personnel ne soient conservées que le temps nécessaire, en garantissant l'accès de toute personne aux données la concernant, en exigeant une sécurité des données appropriée et en exigeant un contrôle indépendant.
- Les garanties sont parmi les plus robustes que l'on puisse trouver dans un traité international de justice pénale et le Canada pourrait aussi appliquer des garanties supplémentaires.
- Le Protocole comprend des dispositions visant à se prémunir contre les impacts préjudiciables, comme la discrimination illégale.
- Lorsqu'elles sont plus strictes, les lois fédérales et provinciales du Canada sur la protection des renseignements personnels s'appliqueraient également à la possession, à l'utilisation et à la protection des données à caractère personnel dans le cadre d'enquêtes criminelles.

Réserves dans le Deuxième Protocole additionnel

- Le traité permet aux parties d'émettre des **réserves** spécifiques. Les réserves permettent à la partie concernée de se soustraire à certaines dispositions au moment de la ratification.
- Le Canada peut choisir de ne pas autoriser l'**accès direct** par les autorités compétentes (forces de l'ordre) des autres parties aux renseignements sur les abonnés détenus par les fournisseurs de services canadiens (article 7).
- La décision d'appliquer certaines dispositions ou de s'y soustraire aurait des **conséquences réciproques** : si le Canada ne crée pas un régime permettant aux autorités compétentes des autres parties d'obtenir directement ces données au Canada, les forces de l'ordre canadiennes ne seraient pas autorisées à demander directement ces données à des fournisseurs de services étrangers.
- L'approche du Canada à l'égard de cette réserve doit tenir compte du fait que l'administration de la justice est un domaine de compétence partagée.

Signature et ratification

- En signant le Deuxième Protocole additionnel, le Canada manifeste son engagement envers l'esprit et l'intention de cette importante initiative. La signature ne lie toutefois pas le Canada.
- Le Canada n'est *juridiquement lié* que s'il **ratifie le Protocole**, sous réserve des éventuelles réserves spécifiées.
- La décision de ratifier ou non le Protocole sera prise par le gouvernement dans le futur.
- Il est important de consulter les Canadiens pour éclairer les prochaines étapes de la mise en œuvre du traité au Canada.

Quelques autres questions en cours d'examen

- Le gouvernement sollicite des commentaires sur le type d'autorisation (par exemple, judiciaire ou autre) que le Canada devrait exiger pour que les enquêteurs **internationaux et nationaux** obtiennent différents types de données à des fins de justice pénale auprès des fournisseurs de services Internet, notamment :
  - les renseignements sur les abonnés (par exemple, le nom, l'adresse, le numéro de téléphone et l'adresse de facturation), les données relatives à l'enregistrement du nom de domaine, le contenu stocké et les données sur la transmission (le trafic).
- Le gouvernement sollicite également des commentaires sur la question de savoir si le Canada devrait refuser d'autoriser l'**accès direct** par les autorités compétentes (forces de l'ordre) des autres Parties aux renseignements sur les abonnés détenus par les fournisseurs de services canadiens (article 7).

Résultats attendus

- S'il ratifie le Protocole, le Canada devrait faciliter les enquêtes et les poursuites à l'égard de la cybercriminalité et des crimes s'y rapportant, ainsi que d'autres crimes graves, en effectuant ce qui suit :
  - améliorer l'accès en temps opportun aux éléments de preuve électroniques aux fins de leur utilisation dans les enquêtes sur les cybercrimes, les crimes liés à la cybercriminalité et d'autres crimes graves, tout en maintenant des garanties solides en matière de protection des données et de droits de la personne;
  - réduire la pression sur les mécanismes canadiens d'entraide juridique; et
  - contribuer à l'élimination des « refuges » pour les éléments de preuve électroniques et renforcer la capacité du Canada et de ses partenaires mondiaux à tenir les délinquants responsables de leurs actes.

Personnes-ressources – ministère de la Justice

- Gareth Sansom, Directeur-adjoint, Direction de la politique en matière de droit pénal
- Kimberly Burnett, Analyste politique principal, Direction de la politique en matière de droit pénal
- Phaedra Glushek, Avocate, Direction de la politique en matière de droit penal

CSAP-DPA@justice.gc.ca