COMMISSION D'ENQUÊTE SUR LA PROTECTION
DE LA CONFIDENTIALITÉ DES SOURCES JOURNALISTIQUES

SOUS LA PRÉSIDENCE DE
L'HONORABLE JACQUES CHAMBERLAND, Président
Me GUYLAINE BACHAND, Commissaire
M. ALEXANDRE MATTE, Commissaire

AUDIENCE TENUE AU
500, BOUL. RENÉ-LÉVESQUE OUEST
MONTRÉAL (QUÉBEC)

Montréal, le 5 avril 2017

Volume 4

NICOLAS PROVENCHER
Sténographe officiel

COMPARUTIONS :

POUR LA COMMISSION :

Me LUCIE JONCAS, avocate en chef
Me CHARLES LEVASSEUR, avocat en chef adjoint

INTERVENANTS :

Me Mathieu Corbo
Service de police de la Ville de Montréal

Me JULIE CARLESSO
Le Devoir inc.
Québecor Média inc.

Me CHRISTIAN LEBLANC
Me CHRIS SEMERJIAN
CBC/Radio-Canada
Cogeco Média inc.
Médias Transcontinental s.e.n.c.
La Presse ltée
Bell Media
Groupe Capitales Médias
Postmedia Network inc.

Me JEAN-NICOLAS LEGAULT-LOISELLE
Ville de Montréal

Me MATHILDE BARIL-JANNARD
Fédération nationale des communications

Me BENOIT BOUCHER
Procureure générale du Québec

Me RAYMOND DORAY, Ad. E.
Conférence des juges de paix magistrats du Québec

Me GÉRALD SOULIÈRE
Fraternité des policiers et policières de Montréal

Me MOLLY KRISHTALKA :
Canadian Journalists for Free Expression (CJFE)
Reporters sans frontières (RSF)
Committee to Protect Journalists (CPJ)

TABLE DES MATIÈRES

PAGE

LISTE DES PIÈCES

PAGE

EN L'AN DEUX MILLE DIX-SEPT (2017), ce cinquième (5e) jour du mois d’avril :

PRÉLIMINAIRES

LA GREFFIÈRE :

Alors, bonjour. Bienvenue à la Commission. J’aurais une demande particulière à vous faire ce matin. Pour les fins de l’enregistrement, je demanderais à chacun des procureurs de bien penser à ouvrir son micro pour que ce soit capté et faciliter la tâche du personnel aussi.

Alors, veuillez vous assurer que vos cellulaires et autres appareils mobiles soient éteints et notez qu’il y a interdiction d’enregistrer ou de prendre des photos dans la salle d’audience, selon les règles de procédure de la Commission.

LE PRÉSIDENT :

Bonjour, tout le monde. Je demanderais à notre greffière de faire l’appel des avocats présents.

LA GREFFIÈRE :

Avec plaisir. Alors, je demanderais à chaque procureur de bien vouloir ouvrir leur micro afin de s’identifier. Je demanderais d’abord aux procureurs

de la Commission de s'identifier pour les fins de l'enregistrement numérique.

Me CHARLES LEVASSEUR :

Bonjour, Charles Levasseur pour la Commission.

Me LUCIE JONCAS :

Bonjour, Lucie Joncas pour la Commission.

LA GREFFIÈRE :

Et je demanderais maintenant aux procureurs des parties de s'identifier et d'identifier ceux qu'ils représentent.

Me CHRISTIAN LEBLANC :

Bonjour, Christian Leblanc pour La Presse, Radio-Canada, Cogeco, Transcontinental Médias, Postmedia, Groupe Capitales Média et Bell Media.

Me BENOIT BOUCHER :

Bonjour à tous, Benoit Boucher pour la Procureure générale du Québec.

Me MATHILDE BARIL-JANNARD :

Bonjour à tous, Mathilde Baril-Jannard pour la Fédération nationale des communications.

Me MATHIEU CORBO :

Bonjour, Mathieu Corbo pour le Service de police de la Ville de Montréal.

Me JEAN-NICOLAS LEGAULT-LOISELLE :

Bon matin, Jean-Nicolas Legault-Loiselle pour la Ville de Montréal.

Me GÉRALD SOULIÈRE :

Bonjour, Madame, Messieurs, Gérald Soulière, Fraternité des policiers et policières de Montréal.

Me JULIE CARLESSO :

Bonjour, Julie Carlesso pour Le Devoir et Québecor Média.

Me MOLLY KRISHTALKA :

Bonjour, Molly Krishtalka pour Canadian Journalists for Free Expression, Reporters sans frontières et the Committee to Protect Journalists.

Me RAYMOND DORAY :

Bonjour, Raymond Doray pour la Conférence des juges de paix magistrats du Québec.

LA GREFFIÈRE :

Merci.

LE PRÉSIDENT :

Merci beaucoup. Alors, Maître Levasseur, on vous écoute.

PRÉSENTATION

Me CHARLES LEVASSEUR :

Monsieur le Président, Madame la Commissaire,

Monsieur le Commissaire, nous aborderons aujourd'hui le thème de la vie privée. Compte tenu du contexte dans lequel la commission a été créée, compte tenu du mandat qui nous a été confié, il s'agit, je vous le soumets, d'une notion qui est fort pertinente à nos travaux.

Le traitement constitutionnel, le traitement législatif et judiciaire qu'a reçu le concept de vie privée démontre qu'il ne faut pas minimiser l'importance des préoccupations et des problématiques en cette matière. D'ailleurs, depuis près de trente (30) ans, la Cour suprême rappelle l'importance du droit à la vie privée. Entre autres, en mil neuf cent quatre-vingt-huit (1988), le juge La Forest, dans Dyment, mentionnait que :

> La notion de vie privée est au coeur de celle de la liberté dans un État moderne.

En quatre-vingt-dix (99), le juge Cory, dans Edwards, mentionnait que :

> Le droit à la vie privée comporte le droit d'être à l'abri de toute intrusion ou d'ingérence de l'État.

En deux mille neuf (2009), dans Patrick, le juge

Binnie servait un avertissement clair lorsqu'il écrivait, au nom de la Cour suprême :

> Un gouvernement qui fouine de plus en plus dans la vie des citoyens, suscitant ainsi leur méfiance et réduisant leurs attentes quant au respect de leur vie privée, ne parviendra pas de ce fait à restreindre unilatéralement le droit constitutionnel de ceux-ci à la protection de la vie privée.

Plus récemment, en deux mille douze (2012), la Cour suprême, dans Tse, déclarait que :

> Le droit à la vie privée repose sur des valeurs de dignité, d'intégrité et d'autonomie de la personne.

Vu l'importance du droit à la vie privée et en vertu de ce concept découle celui de l'expectative de vie privée. Une notion juridique que nous connaissons et qui balise et limite les pouvoirs de l'État de fouiller, perquisitionner et saisir. Voilà pourquoi ces notions sont pertinentes à nos travaux.

Afin d'élaborer sur cette question, je vous

propose deux blocs de témoignages. Le premier bloc étant composé de membres du Commissariat à la vie privée du Canada, je les laisserai se présenter. Et le deuxième bloc de témoignages sera rempli par le professeur Benoît Dupont, professeur titulaire de criminologie de l'Université de Montréal, détenteur de la Chaire de recherche du Canada en cybersécurité et directeur scientifique du Réseau intégré sur la cybersécurité.

Alors, sans plus attendre, Madame la Greffière.

_____

L'AN DEUX MILLE DIX-SEPT (2017), ce cinquième (5e) jour du mois d'avril, ont comparu :

JULIA BARSS,

PATRICIA KOSSEIM,

CHRISTOPHER PRINCE,

INTERROGÉS PAR Me CHARLES LEVASSEUR :

Q. **[1]** Maître Kosseim, vous vouliez peut-être, d'entrée de jeu, présenter, faire une présentation sur le Commissariat à la vie privée. Je vous invite à présenter l'institution que vous représentez.

Me PATRICIA KOSSEIM :

R. Alors, merci au nom du Commissaire à la protection de la vie privée du Canada, on vous remercie de l'intérêt que vous portez sur ces questions fort importantes. Je suis accompagnée de Christopher Prince, qui est conseiller stratégique en recherche et politique et, comme vous avez constaté, Julia Barss, qui est directrice des services juridiques. Pour moi-même, je suis avocate générale principale au Commissariat à la protection de la vie privée du Canada, et j'occupe ce poste depuis deux mille six (2006). Auparavant j'ai oeuvré dans d'autres institutions fédérales, après avoir pratiqué au

sein d'un cabinet d'avocats privé, ici à Montréal.

Alors, le Commissariat a été créé en mil neuf cent quatre-vingt-quatre (1984) pour protéger et promouvoir le droit à la vie privée des Canadiens. Notre mandat découle de deux lois fédérales en matière de protection des renseignements personnels : l'une dans le secteur privé, et l'autre dans le secteur public.

D'emblée, je tiens à préciser que la cueillette, l'utilisation et la divulgation des renseignements personnels à des fins uniquement journalistiques sont exclues de nos deux lois habilitantes. Donc, si je suis ici aujourd'hui à la demande du procureur de la Commission, c'est pour vous dresser un tableau d'ordre général des lois portant sur la protection de la vie privée au Canada, et plus spécifiquement, sur des questions d'accès légal d'une perspective fédérale.

Comme vous vous souvenez peut-être, le gouvernement fédéral avait amorcé, en deux mille neuf (2009), une série de discussions sur les mesures que devraient prendre les forces policières pour avoir un accès légal aux données commerciales dans le cadre de leurs enquêtes. Il y avait diverses propositions législatives prévoyant une

attribution de nouveaux pouvoirs aux forces policières et d'autres organismes d'application de la Loi qui ont été déposées au Parlement en deux mille neuf (2009), en deux mille onze (2011), et encore en deux mille treize (2013).

Les conditions sous lesquelles les forces policières devraient avoir accès aux données de télécommunications ont suscité un débat animé, notamment en ce qui concernait les divers mécanismes et les seuils proposés. Le législateur se demandait comment moderniser les pouvoirs d'enquête à l'ère numérique, quels organismes pourraient exercer ces nouveaux pouvoirs, et au sujet de quels types d'informations, de crimes ou d'activités.

Au cours des années, les défenseurs des divers projets de loi ont fait valoir une position uniforme. Selon eux, certains identifiants, comme le numéro de téléphone ou les détails relatifs à un appareil mobile, ne présentent aucun risque d'atteinte à la vie privée. S'appuyant sur cette hypothèse, ils ont soutenu qu'il n'y avait aucune attente raisonnable en matière de protection de la vie privée dans le cas d'une métadonnée spécifique technique, par exemple, une adresse IP, une adresse

MAC, ou un numéro d'identification international d'abonné mobile. Selon eux, les enquêteurs gouvernementaux devraient donc pouvoir recueillir ces données sans mandat. Il va sans dire que cette question était controversée à l'époque, et qu'elle l'est encore aujourd'hui.

En deux mille douze (2012) nous avons commencé à mener des recherches approfondies sur ces questions tant du point de vue juridique que technologique. Nous avons produit deux rapports, le premier portant expressément sur ce que les adresses IP peuvent révéler et le second sur les métadonnées et les considérations législatives et juridiques connexes.

En deux mille quatorze (2014), nous avons déposé devant la Cour suprême du Canada un mémoire d’intervenant dans l’affaire R. c. Spencer, une décision significative dont on aura la possibilité de traiter un peu plus longuement ce matin. Et cette même année, en deux mille quatorze (2014), nous avons conseillé le Parlement sur la nature potentiellement sensible des métadonnées dans le cas du projet de loi C-13 qui envisageait rajouter au Code criminel de nouveaux pouvoirs d’accès licites aux données de transmissions. Nous avons

récemment réitéré ces préoccupations dans le cas d'une consultation sur la sécurité nationale, menée par Sécurité publique Canada, qui semblait reprendre bon nombre de ces questions.

Dans nos diverses soumissions, nous avons fait une mise en garde contre l'abaissement des seuils pour autoriser ces nouveaux pouvoirs d'enquête. Nous avons souligné l'absence de reddition de compte s'appliquant à l'exercice de ces pouvoirs et l'absence de conditions à leur utilisation. En bout de ligne, le parlement a adopté le projet de loi sans modification. Les nouveaux pouvoirs sont entrés en vigueur en mars deux mille quinze (2015). Nonobstant, les forces policières ne semblent toujours pas satisfaites de ces nouveaux pouvoirs et ces questions continuent à préoccuper le gouvernement.

Pour parler maintenant brièvement des événements qui ont eu lieu ici au Québec l'an dernier, le Commissaire à la protection de la vie privée du Canada a passé en revue les nouveaux pouvoirs de surveillance dans certaines de ses allocutions cette année. Il a fait paraître dans la presse un texte d'opinion sur l'impact de ses nouveaux pouvoirs de surveillance qui devraient

inquiéter non seulement les journalistes pour des raisons très particulières, reliées à la liberté d'expression et la protection de leurs sources, mais aussi tous les Canadiens et les Canadiennes, même dits innocents.

Alors, ce texte d'opinion me semble particulièrement pertinent à votre étude. Et d'ailleurs, je reprendrais en conclusion certains points sur lesquels le Commissaire a insisté. Au lieu d'élargir les pouvoirs d'accès légal, nous devrions plutôt songer à les resserrer. Surtout à la lueur des risques d'atteinte à la vie privée qui sont beaucoup plus élevés que l'analogie anodine aux annuaires téléphoniques nous laisserait croire. Nous devrions maintenir le rôle crucial des juges dans le processus d'autorisation des pouvoirs d'enquête afin d'assurer l'indépendance nécessaire des corps policiers et ainsi mieux veiller à la protection de nos droits les plus fondamentaux. Et, le Parlement canadien devrait considérer légiférer, plus précisément sur les conditions nécessaires à l'accès légal, et devrait octroyer aux juges la possibilité d'y rattacher des conditions propres à chaque espèce, par exemple, pour protéger des citoyens, les citoyens non visés, mais tout de même

captés par ces mesures, les périodes de rétention de l'information ainsi que la destruction voulue des données non pertinentes. Alors, ça me fera plaisir de répondre maintenant à vos questions.

Me CHARLES LEVASSEUR :

Merci Maître Kosseim. Débutons par vous Maître Kosseim.

Q. **[2]** Pourriez-vous nous entretenir des fonctions que vous occupez au commissariat? Quelles sont vos fonctions en tant qu'avocate générale?

R. Alors, je suis avocate générale principale au Commissariat. Je me rapporte directement au Commissaire à la protection de la vie privée. Je suis aussi directrice générale d'une Direction générale de trente quelques experts, professionnels, une équipe interdisciplinaire qui consiste d'avocats, de conseillers en politique, affaires parlementaires, des chercheurs ainsi que des technologues.

Q. **[3]** Au niveau de la structure du Commissariat à la vie privée, j'ai raison d'affirmer qu'il y a plusieurs subdivisions, il y a plusieurs directions au Commissariat à la vie privée, c'est exact?

R. C'est exact, donc ma direction, en général, comme j'ai pu le détailler tout à l'heure est la

direction qui comporte les aviseurs, les conseillers, si vous voulez, en matière juridique, politique et technologie et recherche. Il y a d'autres directions générales, entre autres, des directions générales qui mènent des enquêtes, et dans le secteur privé, et dans le secteur public. Nous avons une direction générale qui mène des vérifications, direction générale des communications, direction générale des services corporatifs.

Q. **[4]** Maintenant, relativement, vous avez effleuré le sujet dans votre déclaration d'ouverture relativement à la mission du commissaire, du Commissariat, plutôt. Pourriez-vous expliciter un peu plus sur la mission, la raison d'être du Commissariat?

R. Alors, le Commissariat, juste pour expliquer un petit peu, nous sommes un agent du parlement. Donc, nous sommes indépendants du gouvernement, nous ne relevons pas à un ministre tel quel. Le commissaire est nommé par le gouverneur en conseil après consultation et approbation par résolution des deux chambres, la Chambre des communes et le sénat. Il est mandaté pour une période de sept ans et ne peut être déchargé de ses responsabilités que pour

cause. Donc, c'est pour assurer son indépendance. Sa mission... sa mission, essentiellement, est de protéger et de promouvoir les droits à la vie privée des Canadiens.

Donc, d'une part, il reçoit des plaintes des individus ou peut lui-même initier des plaintes quand il y a de quoi, quand il y a des motifs raisonnables et mener enquête ou vérification. Donc, répondre à des problèmes, si vous voulez. Il a aussi le mandat de promouvoir, de façon proactive, la protection des renseignements personnels par le biais de sensibilisation auprès du public, de l'éducation, des entités qui sont, par exemple, assujetties aux deux lois.

Il peut aussi mener des recherches, il peut faire revue des évaluations... des évaluations des facteurs relatifs à la vie privée qui se trouve à être un outil qu'utilise surtout les établissements, les institutions gouvernementales pour gérer les risques vis-à-vis la vie privée.

Il peut aussi, une activité très importante, c'est de conseiller le Parlement. Donc, lorsqu'il s'agit de lois, de projets de lois, plutôt, qui sont déposés au Parlement, il est souvent interpellé à venir témoigner devant des

comités parlementaires pour conseiller les membres, soit du sénat ou de la Chambre des communes de... les enjeux vis-à-vis de la vie privée et porter des recommandations à savoir comment le projet de loi pourrait être amélioré.

Il produit un rapport annuel au Parlement à chaque année. Il peut, au besoin, en situation d'urgence ou lorsqu'il s'agit d'une question d'importance nationale qui ne peut pas attendre le rapport annuel, peut faire rapport spécial au Parlement.

Et je conclurais en disant qu'il collabore beaucoup avec ses homologues provinciaux, territoriaux et surtout à l'échelle internationale étant donné, évidemment, la nature globale des renseignements personnels et les défis à l'échelle mondiale.

Q. **[5]** Vous nous avez mentionné, lors de votre déclaration d'ouverture, que le commissariat a été créé en quatre-vingt-quatre (84) et qu'il a, en quelque sorte, deux lois constituantes. Au niveau de la juridiction, est-ce que je dois comprendre que la juridiction du Commissariat est uniquement auprès des organismes publics ou le Commissariat a également juridiction auprès de l'entreprise

privée?

R. Donc, il y a deux lois habilitantes, justement. Comme toutes les provinces et territoires, nous avons une loi régissant le gouvernement, le secteur public. Donc, nous avons la Loi sur la protection des renseignements personnels, qui a été la première à être adoptée en mil neuf cent quatre-vingt-quatre (1984). Sur... qui régit les institutions gouvernementales et tous les... la cueillette, l'utilisation et la divulgation des renseignements personnels pour des fins de... du gouvernement, du secteur... dans le secteur public. Nous avons... et les institutions sont énumérées explicitement dans l'annexe à la loi. Donc il faut s'y trouver pour être assujetti à la loi fédérale dans le secteur public.

En deux mille (2000) nous avons... le Parlement a adopté une deuxième loi, la Protection des renseignements personnels et des documents électroniques, la LPRPDÉ qui, pour sa part, régit les organisations dans le secteur privé, mais c'est un peu plus compliqué. Alors elle gère... elle régit tous les organismes fédéraux, telles les banques, les sociétés de télécommunications, les lignes aériennes, et caetera. Donc les organismes

fédéraux. Et aussi toute autre organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales, donc... et ça, ceux à travers le Canada, sauf dans les provinces où il existe des lois essentiellement similaires. Dont le Québec.

Alors dans le cas du Québec, par exemple, la loi fédérale ne s'applique pas aux organisations et les activités commerciales, les entreprises par exemple, qui sont régies pour leur part par la loi québécoise. Mais la loi fédérale continue à s'appliquer aux organismes fédéraux et aussi aux communications entre provinces ou à l'échelle internationale.

Q. **[6]** Simplement pour clarifier, pour dites que lorsque... par exemple, au Québec nous avons une loi sur la protection, vous dites que lorsqu'il y a une loi sur la protection qui existe dans une province, la loi fédérale ne s'applique... ne s'applique pas. Est-ce que... par contre, vous nous avez mentionné il y a quelques instants que les entreprises de juridiction fédérale, les banques, les sociétés de télécommunications sont soumises à la Loi sur la protection des documents électroniques. Est-ce qu'une entreprise de

télécommunications qui fait affaire au Québec, donc techniquement qui est de juridiction fédérale, est-ce que la loi fédérale s'applique à ce genre de société-là?

R. Alors quelques précisions. Encore une fois, c'est un peu complexe, mais je veux juste préciser que la loi fédérale ne va pas s'appliquer dans les provinces où il existe une loi, mais qui a été déclarée essentiellement similaire. Donc il y a deux étapes, pas juste l'existence de la loi, mais elle doit être déclarée essentiellement similaire. Et la loi québécoise, en passant, a été la première à avoir cette désignation depuis le début.

Donc pour ce qui est des sociétés de télécommunications, pour prendre l'exemple, au Québec la loi fédérale continue à s'appliquer à cette société, même si elle fait affaire au Québec. Mais j'ouvre une parenthèse importante. Que la loi québécoise aussi s'applique à la société de télécommunication de façon concurrente, et ce, suite à plusieurs décisions de la Commission d'accès à l'information qui a pris juridiction sur ces sociétés. Donc nous avons, jusqu'aux dernières nouvelles, parce que les décisions sont portées en appel à la Cour d'appel du Québec, mais nous avons

essentiellement juridiction concurrente sur ces sociétés. Ce qui fait l'affaire de tout le monde parce que finalement s'il y a une loi qui a un standard plus élevé que l'autre, bien c'est le standard plus restreignant qui va finalement mieux protéger les droits des Canadiens et des Canadiennes.

Q. **[7]** Je vous remercie. Relativement... si on vient, par exemple, au pouvoir que possède le Commissariat. Vous l'avez mentionné tout à l'heure, le Commissariat a un pouvoir d'enquête. Pourriez-vous exposer aux commissaires en quoi consiste ce pouvoir, comment se matérialise-t-il? Comment peut-il être enclenché?

R. Alors les pouvoirs d'enquête existent en vertu des deux lois, et ces pouvoirs sont enclenchés soit par une plainte qui nous est venue d'un individu et qui se trouve à être dans notre juridiction, bien sûr, ou ça peut aussi être une enquête qui est initiée par le commissaire lui-même lorsqu'il y a des motifs raisonnables à croire qu'il y a matière d'enquêter. Comme par exemple, dans les fuites de données. S'il y a des bris importants, bien le commissaire peut, à son propre chef, initier une plainte ou une enquête.

Ses pouvoirs d'enquêter sont assez importants. Donc, il se trouve à être dans les deux lois... dans la loi, et il a une série de pouvoirs. Il peut contraindre la preuve, et caetera. Mais, par contre, nous n'avons pas le pouvoir d'émettre des ordonnances. Donc, contrairement à la Commission d'accès à l'information, nous n'avons pas ce pouvoir d'obliger, ou de contraindre les organismes, dans le secteur privé ou public, à faire, ou à suivre nos recommandations. En bout de ligne, ce ne sont que des recommandations.

Le modèle qui existe au fédéral est basé sur le modèle, je dirais d'ombudsman, donc ils cherchent beaucoup, il passe beaucoup beaucoup d'efforts à essayer de mener et trouver une solution, une résolution entre les parties. Et ça fonctionne dans la grande, vaste majorité des cas. Les enquêtes vont être résolues. Souvent parce que le... il y aura, pas nécessairement un compromis, mais il va y avoir un mouvement des deux parties, et souvent l'organisation va suivre nos recommandations, et des fois il va aussi répondre, en réponse, nous expliquer pourquoi telle et telle recommandation n'est pas réalistique, ou n'est pas faisable, et on va évidemment en tenir compte, et

on va arriver à des recommandations qui sont justes envers la loi, mais aussi faisables et pratiques. Et donc, dans la vaste majorité des cas, les plaintes sont résolues de cette façon.

Elles sont aussi résolues bien avant de mener enquête, nous mettons beaucoup d'emphase au préalable de même ouvrir une enquête. Des fois, juste en discutant avec les parties, on peut résoudre des problèmes à l'amiable, sans avoir à ouvrir une enquête dès le début.

Par contre, là où il n'y a pas de résolution - et comme j'ai dit c'est une très... dans très peu nombre de cas - là le commissaire peut initier ou déposer une demande de révision devant la Cour fédérale. Ou bien une des parties, une des parties qui n'est pas satisfaite peut faire de même. Et donc, la Cour fédérale peut revoir de novo les faits et rendre sa décision au sujet de la plainte, ultimement, qui est évidemment contraignable.

Q. **[8]** Le Commissariat a également un pouvoir de vérification en matière de vie privée. C'est exact?

R. Oui.

Q. **[9]** En quoi consiste ce pouvoir de vérification?

R. Alors le pouvoir de vérification est un pouvoir

encore plus important, je dirais, que le... Pas plus important, mais plus élaboré que le pouvoir d'enquête, donc il va être plus élaboré parce qu'il va revoir, peut-être de façon plus détaillée, mais de façon plus large les systèmes de gouvernance, les systèmes informatiques. Donc il va revoir les mesures de protection, de A à Z, propres à une organisation ou une institution fédérale.

Et les pouvoirs de vérifi... Les vérifications, pour cette raison, bien, elles sont peu... moins nombreuses que les enquêtes, parce qu'elles prennent typiquement plus de temps. Et dans ce cas, dans les cas de vérification, encore une fois, le résultat ultime, ce sont des recommandations qui, dans la grande majorité des cas, sont suivies par soit les institutions, au niveau fédéral, gouvernementales, ou les organismes dans le secteur privé.

Q. **[10]** Au niveau des limites, le Commissariat a une limite juridictionnelle. Pouvez-vous nous... Pouvez-vous expliquer au Tribunal... pas au Tribunal, mais aux Commissaires les limites au mandat du commissariat?

R. Oui. Il y en a plusieurs. Donc, j’ai mentionné tout à l’heure que la loi fédérale ne va pas s’appliquer

dans les provinces où il y a des lois essentiellement similaires, dans le secteur, en ce qui concerne le secteur privé. Du côté du secteur public, la juridiction s'étend uniquement aux entités qui sont listées dans l'annexe, donc ça ne s'étend pas plus large que ça. J'ai mentionné une exclusion importante, par exemple, au sujet des renseignements personnels qui sont recueillis, utilisés ou divulgués pour des fins uniquement journalistiques, qui se trouvent à être extraits de la loi. Et, donc, ça c'est...

LE PRÉSIDENT :

Je m'excuse, Je peux vous poser une question?

R. Oui. Absolument.

Q. **[11]** Quand vous dites, c'est la référence aux données, aux renseignements personnels qui sont exclus lorsqu'ils sont recueillis pour des fins journalistiques. Ça veut dire quoi ça en pratique là, si vous me donniez un exemple concret, là, de ce qui est visé par l'exception?

R. Donc, je vais vous faire une distinction, peut-être qui va éclaircir. Prenons, par exemple, la Société Radio-Canada qui, pour sa part, se trouve maintenant à être assujettie en vertu de la loi dans le secteur public, mais c'est la même

exclusion, grosso modo, qui s'applique dans les deux cas. Pour ce qui est de la Société Radio-Canada, elle va être assujettie à la loi en ce qui concerne, par exemple, l'utilisation ou la cueillette ou la divulgation des renseignements personnels de ses employés. Donc, dans l'administration de la Société, l'administration des données pour fins corporatives ou des employés. Mais par contre, lorsqu'il s'agit de renseignements personnels qui sont recueillis ou utilisés ou divulgués dans le contexte du travail, finalement, journalistique, bien, ça se trouve à être exclu de la loi. Donc, par exemple, toute cette question de sources journalistiques, le travail d'enquête, les recherches que font les journalistes pour préparer leurs travaux, tout ça, c'est évidemment, c'est exclu de la loi. Est-ce que ça vous éclaircit?

Me GUYLAINE BACHAND, Commissaire :

Q. **[12]** Est-ce c'est mentionné, permettez, c'est mentionné dans la loi ou c'est une interprétation de votre Commission?

R. Alors, ce qui est important à soulever, à mentionner, c'est que ça doit être des fins uniquement journalistiques. Donc, c'est une interprétation qu'on fait de cette disposition que

l'utilisation des renseignements personnels pour des fins administratives, par exemple, la gestion des employés, va être couverte par la loi, alors que ce qui relève du travail finalement des journalistes n'est pas couvert et excède le mandat du commissaire.

Me CHARLES LEVASSEUR :

Q. **[13]** Concrètement est-ce qu'il y a une disposition législative...

R. Oui.

Q. **[14]** ... dans soit dans la Loi sur la protection des renseignements personnels ou celle...

R. Oui.

Q. **[15]** Oui?

R. Alors, pour votre information, Julia a les deux dispositions ici...

Me JULIA BARSS :

R. Je pense que vous avez demandé si c'est expressément dans la Loi, donc j'ai voulu juste mentionner que c'est section 69.1 de la Loi sur la protection des renseignements personnels où on voit cette exception. Et, l'autre côté, c'est section 4(2)c) de la Loi sur la protection des renseignements personnels et les documents électroniques, LPRPDE, qui aussi mentionne cette

exception. Merci.

Me CHARLES LEVASSEUR :

Je vous remercie.

Q. **[16]** On y viendra dans quelques instants, mais également, le Commissariat fait des travaux de recherche. La première question que je vous pose, c'est pourquoi?

Me PATRICIA KOSSEIM :

R. Alors, nous faisons la recherche, soit la recherche interne par nos chercheurs à l'interne et on prépare des documents de recherche, des analyses, des rapports de recherche soit à l'interne, comme je l'ai mentionné, ou aussi, on a un programme de contribution qui subventionne des universitaires ou la société civile de mener des projets de recherche qui sont indépendants de nous et qui sont ultimement aussi publiés dans le domaine public. La raison pour laquelle nous faisons ça, bien, il y a en a plusieurs. Premièrement, c'est pour faire avancer les connaissances dans le domaine de la vie privée pour le bénéfice de tout le monde, pour sensibiliser le public, pour éduquer les organisations et les institutions fédérales sur leurs obligations et mener à des meilleures pratiques, par exemple. Et aussi, pour nous aider,

nous-mêmes, à faire avancer nos connaissances, notre expertise et nous éclaircir sur des questions importantes pour que nous, à notre tour, nous puissions mieux conseiller le Parlement, par exemple, sur des questions de vie privée.

Q. **[17]** Et dites-moi, les conclusions, si conclusions il y a, de ces travaux de recherche, est-ce qu'elles sont contraignantes pour le gouvernement ou c'est simplement une constatation qui est faite par le Commissariat?

R. Ce sont essentiellement des constatations, oui.

Q. **[18]** Je vous soumets qu'en deux mille treize (2013), le Commissariat a procédé à une étude sur les adresses IP. Pourriez-vous nous donner un peu le contexte, les objectifs et les motifs qui ont justifié cette étude?

R. Alors oui, bien sûr, le contexte se trouvait à être deux mille douze (2012), lorsqu'il y avait, parmi les projets de loi antérieurs que j'ai mentionnés tout à l'heure, ce qui portait sur l'accès légal, le projet de loi qui existait à l'époque a proposé une disposition qui aurait permis la production de six éléments de métadonnées, si vous voulez, ou de données, qui pourraient être accédées par des organismes chargés de l'application de la loi sans

mandat. Et donc, c'était la proposition qui était faite sous la présomption, encore une fois, que ce sont des données anodines auxquels il n'y a pas vraiment d'expectatives à la vie privée, qui ne sont pas sensibles. Et donc, nous avons... dans ce contexte-là, nous avons pensé, cru bon de faire une analyse plus poussée et effectivement, une analyse technologique pour voir si on pouvait, en partant, prendre deux ou trois de ces éléments, les combiner et en fait, identifier une personne qui était rattachée à ces éléments. Donc, adresse électronique, adresse IP, mais sans le nom de la personne.

Et effectivement, ce projet de recherche a pu constater et documenter que c'était effectivement possible d'identifier une personne avec simplement ces éléments, en combinaison, même sans connaître le nom de la personne.

Q. **[19]** Et les éléments auxquels vous faites référence, vous avez fait référence à six éléments, là, qui avaient été identifiés. Pourriez-vous informer les commissaires sur les éléments qui avaient été identifiés?

R. Dans le projet de loi?

Q. **[20]** Dans le projet de loi, effectivement.

R. Alors, il s'agissait du nom, de l'adresse, le numéro de téléphone, l'adresse courriel, l'adresse de protocole internet, l'adresse IP en question, et l'identifiant du fournisseur de services locaux.

Q. **[21]** Alors, je veux juste être sûr de bien comprendre, dans le projet de loi, il était proposé que les responsables, les organismes responsables de l'application de la loi et de la sécurité nationale pouvaient entrer en possession de ces éléments-là sans mandat?

R. C'était la proposition qui avait été faite à l'époque. Et on s'est fortement questionné sur la nature dite anodine de ces éléments et donc, c'était la raison pour laquelle nous avons entrepris cette recherche. Et nous avons effectivement constaté, comme on le soupçonnait, que ces données n'étaient pas si anodines et qu'elles pouvaient non seulement identifier une personne, mais comme le rapport en fait mention, tracer et énumérer les activités en ligne de cette personne. Donc, les intérêts, les recherches qu'ils avaient faites sur le Web. Ils avaient... les entrées qu'ils avaient faites sur les pages Wikipedia, les commentaires qu'ils avaient faits, croyant que c'était l'anonymat, mais avec l'adresse

IP, ils ont pu tracer et jumeler l'information pour pouvoir constater et dresser un portrait important sur la personne et ses activités en ligne. Les sites Web visités, les intérêts personnels qui pouvaient être inférés ou déduits par le site qu'ils allaient visiter. Et les organisations auxquelles ils appartenaient, par exemple, des forums en ligne, ils pouvaient... si vous participez à des forums en ligne, bien avec l'adresse IP, on pouvait tracer les contributions qu'ils avaient faites, croyant à l'anonymat, mais en fait, qui étaient identifiables avec l'adresse IP.

On fait aussi une revue de l'affaire Petraeus, qui a été l'affaire à l'époque qui avait fait l'objet des articles dans les médias. Il s'agissait de la relation extra-conjugale du directeur de CIA à l'époque. Et il s'agissait d'essayer d'identifier la source de maints courriels qui avaient... menaçants qui avaient été envoyés dans le cadre de cette affaire. Et on explique dans ce rapport comment ils ont effectivement pu identifier la personne, la source qui avait été responsable d'avoir envoyé ces courriels, non seulement en traçant l'activité en

ligne, mais aussi en jumelant cette information avec le lieu physique de la personne, parce qu'ils ont pu identifier de quel hôtel la personne a envoyé ces courriels, même avec une adresse courriel anonymisée, mais en traçant les différents hôtels duquel ils ont envoyé ces courriels menaçants, ils ont pu limiter et déduire un nombre de personnes qui se trouvaient à être à ces hôtels à ces moments donnés. Donc ils ont pu identifier ultimement la personne qui était responsable. Donc les lieux physiques aussi, ils ont pu déduire.

Donc, le but ultime du rapport, c'est de tracer cet exemple, qui était un exemple très public, avec nos propres recherches qu'on avait faites à l'interne, qui confirmaient la même chose, qui arrivaient aux mêmes résultats.

Q. **[22]** Justement, vos recherches à l'interne puis l'affaire Petraeus c'est une chose. Est-ce que vous, est-ce que le Commissariat a fait des recherches à l'interne, des tests, des expériences à l'interne?

R. Oui. Alors, comme je l'ai mentionné tout à l'heure dans ma direction générale, nous avons une équipe de technologues qui sont experts en matière de technologie de l'information et c'est leur

expertise d'ailleurs. Et ils ont fait, ils ont refait cette expérience avec l'adresse du Commissariat, donc tous les utilisateurs qui étaient liés à l'adresse IP du Commissariat, et aussi un de nos technologues s'est porté bénévole pour retracer sa propre adresse IP et pour démontrer ce qui pouvait être déduit de ces activités en ligne qui étaient liées à l'adresse IP qu'il utilisait.

Donc, c'était encore une fois, deux autres exemples qui ont été dressés dans le rapport, mais qui ont fait l'objet d'une analyse technologique à l'interne.

Q. **[23]** Et comme question de fait, vous ne l'avez pas mentionné, mais comme question de fait je comprends que l'expérience a été concluante. Le volontaire, appelons-le comme ça, on a pu le suivre, on a pu identifier ses allées et venues, c'est ce que je comprends.

R. Oui, on a pu tracer un portrait fort intéressant de l'individu en question.

LE PRÉSIDENT :

Probablement moins intéressant que s'il n'avait pas su qu'il était suivi.

R. Ou s'il avait des... des affaires extra-conjugales

aussi.

Me CHARLES LEVASSEUR :

Q. **[24]** Maintenant, le projet de loi dans lequel ce régime-là était prévu, pourriez-vous nous l'identifier?

R. Pardon? Le projet de loi?

Q. **[25]** Oui.

R. Qui existait à l'époque. Le numéro du projet de loi. Le numéro du projet de loi...

Q. **[26]** Oui. Le numéro, oui.

R. ... en deux mille douze (2012)?

M. CHRISTOPHER PRINCE :

R. C-13.

Me PATRICIA KOSSEIM :

R. En deux mille douze (2012)?

M. CHRISTOPHER PRINCE :

R. Oh! non, en...

Me PATRICIA KOSSEIM :

R. Avant. C-13, c'était le dernier. C'était C-30? On peut vous revenir sur la question, le projet de loi qui proposait les six éléments.

LE PRÉSIDENT :

Q. **[27]** Dans votre rapport, c'est mentionné C-30.

R. C-30. Alors, voilà.

M. CHRISTOPHER PRINCE :

R. C’est exact, C-30.

Q. **[28]** Parce que, pour les gens qui nous écoutent ou qui nous regardent, c’est important de dire que ce rapport-là, comme tous vos rapports de recherche, est sur le site Internet, site Web du Commissariat. Alors, ils sont facilement accessibles pour les gens qui s’intéressent aux adresses IP ou aux métadonnées, toutes ces choses-là.

Me PATRICIA KOSSEIM :

R. Absolument. Oui. Dans les deux langues officielles, d’ailleurs.

Me CHARLES LEVASSEUR :

Q. **[29]** Alors, ce ne sont pas des documents secrets, là.

R. Non, non, absolument pas.

Q. **[30]** N’importe qui qui peut aller sur Internet est capable de...

R. Comme vous me l’avez demandé au début, un des objectifs primaires de faire des projets de recherche comme ça, c’est pour sensibiliser le grand public. Donc, ils sont absolument disponibles sur notre site Web. Sans le nom de l’employé, évidemment, pour protéger sa vie privée, mais l’analyse est là.

Q. **[31]** Celui du général Petraeus est là.

R. Oui. Ça, ça a déjà été divulgué par les médias.

Q. **[32]** En octobre deux mille quatorze (2014), vous avez produit un autre rapport qui est pertinent aux travaux de la Commission, c'est celui sur les métadonnées et la vie privée. Je vous repose la même question, quel était l'objet, les motifs, derrière la confection de ce rapport?

R. Alors, ce deuxième rapport, juste pour, encore une fois, préciser, et vous faites bien de me le rappeler, c'est un rapport qui se trouve à être sur notre site Web, public aussi, dans les deux langues officielles, donc disponible pour consultation.

Ce rapport, sur les métadonnées, je vous dresse un petit peu le contexte. C'était deux ans plus tard... ou l'année d'après ou deux ans plus tard, on a commencé à songer à faire ce rapport lors des divulgations d'Edward Snowden. C'était, à l'époque, en deux mille treize (2013), les premières divulgations qui sortaient. Et tout le monde entier se posait ces questions, fort importantes, à savoir, quelle est la nature de ces métadonnées, ces programmes gouvernementaux, qui s'en sert et qui qui y accède, qui cherche à accéder des métadonnées? Quels sont les enjeux au niveau de la vie privée? Donc, c'était la question

du jour, si vous voulez. Et c'est le contexte dans lequel nous avons entrepris ce deuxième rapport de recherche. Qui est moins une recherche technologique qu'une recherche qui dresse les enjeux juridiques plutôt. Mais tout en étant... tout en faisant état de la nature importante des métadonnées et ce qu'elles peuvent divulguer.

Q. **[33]** Hum hum.

R. Donc, c'est une analyse, je dirais, technologique, mais aussi juridique qui cherchait à mieux comprendre les métadonnées et qu'est-ce qui peut être divulgué, si vous voulez, comme renseignements autour d'une communication. Parce qu'une métadonnée, simplement parlant, c'est une donnée qui fournit une information sur une autre donnée. Donc, c'est tous les renseignements qui englobent une communication, par exemple. Et...

Q. **[34]** Est-ce que, par exemple... je vous arrête, je vous arrête ici. C'est une donnée qui... ça peut paraître un peu abstrait, mais au niveau d'une communication cellulaire, avez-vous... sans entrer dans les détails technologiques, là, avez-vous quelques exemples de données qui peuvent être combinées pour donner des données sur des données, finalement?

R. Oui. Alors, les données sur les données, ça répond un petit peu aux questions de qui, de quoi, où, comment et quand? Donc, dans le rapport nous avons un « infographic », très utile, qui prend certaines activités, dont faire un appel téléphonique, je pense que c'était votre question.

Q. **[35]** Hum hum.

R. Et qui dresse, pour chacune de ces activités, toute l'information qui englobe l'activité, donc les métadonnées. Pour ce qui est de l'appel téléphonique, par exemple, il s'agit... il peut s'agir du numéro de téléphone de l'appelant, du numéro de téléphone composé, le destinataire. Le numéro de série unique des appareils téléphoniques utilisés, des deux bords de la communication. L'heure de l'appel. La durée de l'appel. L'emplacement de chaque participant. Le numéro de carte de l'appel. Et, évidemment, si le destinataire se trouve à être une organisation qui a pour mandat quelque chose de très clair, par exemple un centre de toxines, toximanie, ou un centre d'abus des femmes, ou... Donc on peut déduire facilement non seulement qui est le destinataire, mais l'objectif, la raison pour l'appel.

Donc, c'est un petit peu le portrait qu'on peut dessiner autour de l'appel téléphonique.

Q. **[36]** Et, je ne veux pas vous prendre à contre-pied, mais ces données-là, relativement à une communication cellulaire, bon, elles se retrouvent où? On les retrouve... Les policiers peuvent s'en servir à quel escient, et aller les chercher à quel endroit?

R. Ils peuvent aller les chercher auprès des sociétés de télécommunications, par exemple, ou des relevés de compte, par exemple, qui vont dresser les appels qui ont été faits. Donc, en utilisant différentes sources, ils peuvent jumeler et accumuler ces renseignements pour dresser un portrait très important.

Ce qui est intéressant, c'est qu'à l'époque où on a publié ce rapport, il y avait déjà des gens, des experts qui prenaient comme position que les métadonnées étaient tout aussi importantes et révélatrices que la communication elle-même, dont des experts aux États-Unis, par exemple.

Depuis ce rapport de deux mille quatorze (2014), en préparant notre réponse, par exemple, au livre vert du gouvernement, qui est consulté sur les questions de sécurité nationale, il y a même

certains experts, dont au Royaume-Uni, celui qui est responsable de Government Operations, qui maintenant soutient que les métadonnées sont encore plus précieuses et plus importantes que le contenu de la communication, pas seulement parce que, si on compare la donnée, métadonnée à la communication seulement, mais si on regarde la vaste quantité de métadonnées qu'on peut accumuler sur une longue période de temps, de maintes sources.

Donc, avec ce qu'on appelle les données massives, maintenant, et les technologies d'analyse, on peut, pas seulement dresser ce que l'individu a fait, mais encore plus important, on peut prédire ce que l'individu pourrait ou peut faire à la lueur de tous ces renseignements qui dévoilent un portrait ou, on dit en anglais a « pattern », d'activités qui peuvent justement éclaircir sur les activités probables et futures d'un individu.

Donc c'est d'une valeur très significative, qui ne va qu'augmenter avec les technologies d'analyse, qui deviennent de plus en plus puissantes, et la masse, quantité de données qui devient de plus en plus disponible.

Q. **[37]** Vous nous avez entretenus des enjeux, en fait

vous nous avez mentionné qu'il y avait des enjeux juridiques de liés aux métadonnées. On a abordé la question un peu technologique. Au niveau des enjeux juridiques, la première question que j'ai envie de vous poser, c'est comment on traite, au niveau judiciaire, les métadonnées?

R. Alors, les métadonnées ont déjà fait l'objet de plusieurs décisions de la Cour suprême du Canada - vous en avez fait mention, d'ailleurs, dans vos commentaires d'ouverture - où les tribunaux et, entre autres, évidemment, la Cour suprême du Canada, deviennent de plus en plus sensibilisés à la nature des métadonnées, et plus spécifiquement l'expectative de vie privée que les gens ont par rapport au sujet de ces renseignements-là. Donc, il y a deux volets à votre question. Je dirais comment les métadonnées sont traitées par les tribunaux, mais aussi en vertu de nos lois statutaires. Donc, je peux traiter un petit peu des deux.

Q. **[38]** Allez-y.

R. Je vais commencer avec une loi statutaire. Les métadonnées... Pardon. Les lois statutaires définissent un renseignement personnel pas comme étant un renseignement identifié d’une personne, mais identifiable d’une personne. Donc la

définition même permet d'emporter, d'englober les métadonnées, parce que même si on prend certains éléments sans le nom ou l'adresse d'une personne on peut, comme j'ai traité tout à l'heure, on peut déduire l'identité de la personne. Donc les lois statutaires sont déjà, cette flexibilité dans la définition même d'un renseignement personnel pour comprendre les métadonnées. Qu'il s'agisse du nom, mais aussi qu'il s'agisse d'autres données qui sont non identifiées, mais identifiables par le fait que lorsqu'on les combine ensemble on peut ultimement en déduire l'identité de la personne.

En ce qui concerne l'évolution des métadonnées devant les tribunaux et en particulier en vertu de l'article 8 de la Charte, l'évolution des métadonnées a fait en sorte qu'avec le temps les tribunaux reconnaissent de plus en plus l'importance de l'attente raisonnable de la vie privée quand les individus, au sujet de leur ordinateur évidemment. Donc on peut penser à l'affaire R. c. Vu, qui s'agissait de la perquisition de l'ordinateur tel quel, évidemment que la cour a reconnu, renferme des renseignements personnels très importants. L'ordinateur... Et non seulement ce que la personne a pu stocker sur

l'ordinateur, mais ce qui reste sur l'ordinateur même après avoir pensé ou cru qu'il les avait déchu ou détruit. Donc, les ordinateurs retiennent et continuent à stocker les renseignements personnels, même après que l'individu ait pensé qu'il les a bel et bien détruits.

Donc, il y a l'ordinateur tel quel, évidemment il y a la connexion avec le réseau et tout ce que l'Internet, les activités sur le réseau peuvent ouvrir comme portrait des activités en ligne d'un individu qui, elles aussi, sont excessivement sensibles.

Et pour fermer la boucle, dans l'affaire R. c. Spencer par exemple, il s'agissait là de savoir s'il y avait une expectative raisonnable de vie privée dans les simples nom et adresse d'une personne qui effectivement était la clé à l'ordinateur, qui était la clé à l'activité en ligne. Donc, de plus en plus je crois que la cour reconnaît, pas seulement les données telles quelles, mais est de plus en plus sensibilisée à la possibilité de ce que ces données peuvent révéler lorsqu'elles sont combinées avec d'autres ou lorsqu'elles sont effectivement la clé nécessaire pour ouvrir la porte à des données beaucoup plus

sensibles en combinaison.

Q. **[39]** Justement, Spencer c'est une, est-ce que je me trompe en disant que c'est une décision de la Cour suprême qui a été marquante quant au droit à la vie privée des Canadiens? Est-ce que je me trompe lorsque j'affirme ça?

R. Non. Pas du tout. Je pense que c'est un arrêt extrêmement important et significatif au sujet de la protection de la vie privée et c'est une, d'ailleurs, des plus importantes décisions récentes.

Q. **[40]** On y viendra peut-être, bon, pas peut-être, mais on y viendra lorsqu'on abordera la question de l'article 7 de la loi protégeant les documents électroniques, mais peut-être juste nous dresser, vous l'avez fait brièvement, mais peut-être juste nous dresser le portrait de Spencer et comment c'est venu protéger les informations personnelles.

R. Alors, juste pour le bénéfice de ceux qui ne connaissent peut-être pas l'arrêt, il s'agissait d'une affaire où la police avait découvert l'adresse de protocole Internet, donc l'adresse IP, d'un ordinateur d'une personne qui avait utilisé pour accéder à la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de

fichiers. Les policiers ont ensuite obtenu auprès du fournisseur de services internet, sans autorisation judiciaire préalable, les renseignements relatifs à l'abonné qui appartenait à cette adresse IP. Et c'est comme ça qu'ils ont découvert l'appelant, monsieur Spencer, dans ce cas.

Alors, monsieur Spencer avait fait valoir que la police avait effectué une fouille ou une perquisition inconstitutionnelle en n'avoir pas obtenu un mandat au préalable et que la preuve devrait donc être écartée. Ce qui est important dans cette décision, il y a beaucoup de - je peux en traiter longuement, mais je pense que ça vaut la peine juste de mentionner quelques points clés.

Alors, en faisant la revue des facteurs pour évaluer s'il y avait ou non une attente raisonnable en matière de respect de la vie privée, on parle juste du nom et de l'adresse. La Cour a dû passer en revue les facteurs suivants : l'objet de la fouille, donc le nom et l'adresse; l'intérêt du demandeur à l'égard de cette information; l'attente subjective du demandeur; et savoir si l'attente était objectivement raisonnable. Donc, pour ce qui est de l'attente subjective, la Cour en a traité

très brièvement. Évidemment, il y avait une attente subjective.

Mais pour ce qui est des autres facteurs, l'objet de la fouille, pour revenir à l'objet de la fouille, il s'agissait du nom et de l'adresse. Pour monsieur Spencer, il prétendait que le nom et l'adresse comportaient des renseignements personnels d'ordre biographique « core biographical information » parce qu'évidemment, il ne s'agissait pas juste du nom et de l'adresse, mais le lien que ça permettrait avec toutes ses activités en ligne.

Pour sa part, le ministère public avait soutenu que la fouille visait simplement le nom et l'adresse et le numéro de téléphone correspondant à l'abonné qui était lié à l'adresse IP et qui était, donc, une information publique et anodine, encore une fois.

Ce qui est important, c'est dans cette affaire, la Cour a adopté une approche très large et fonctionnelle en examinant non seulement les renseignements personnels qui étaient recherchés, dont le nom et l'adresse, mais en regardant qu'est-ce que ça peut révéler. Donc, ce n'est pas de l'objet en soi qui est recherché, qui devrait faire l'objet de l'analyse, mais comprendre qu'est-ce que

ça pourrait permettre à révéler si on était pour octroyer cette information. Et évidemment, la Cour a trouvé qu'il y avait un intérêt important dans le nom et l'adresse et qu'il s'agissait justement d'un renseignement personnel d'ordre biographique, donc important.

Ensuite, la Cour a regardé la nature de l'intérêt en matière de vie privée. Ce qui est important, dans ce cas, je pense, juste entre parenthèses, je vais ajouter que la Cour a bien dit qu'il ne s'agit pas ici de savoir ou de protéger des activités illicites en ligne, ce n'est pas la nature d'un intérêt qu'on cherche à protéger. Ce qu'on cherche à protéger, c'est le droit des citoyens de façon plus générale dans leurs activités en ligne. Donc, c'est cet intérêt sur lequel on devrait se questionner.

Et donc, pour ce faire, la Cour a rappelé l'aspect informationnel du droit à la vie privée qui englobe trois piliers importants, conceptuels. Le premier, c'est le pilier de la confidentialité. Donc, on pense ici aux dossiers médicaux, évidemment, auxquels on s'attend à ce que les professionnels de la santé maintiennent confidentiels, donc c'est la confidentialité.

Le deuxième pilier, c'est l'aspect de contrôle. Donc l'intérêt d'un individu de contrôler l'utilisation de leurs renseignements personnels et la divulgation à des tiers, à quelles fins et dans quelles mesures et de quelles manières. On pense ici aux transactions commerciales ou l'utilisation par l'État. Vous avez mentionné R. c. Dyment tout à l'heure, c'est un cas classique qui fait valoir le pilier contrôle de la vie privée.

Mais la Cour a aussi dit, et c'est le point le plus important, qu'il existe un troisième pilier, celui de l'anonymat. Et c'est l'anonymat ici qui était l'intérêt en jeu. Où les renseignements en tant que tels n'étaient pas privés, au contraire, on vise expressément à les divulguer, mais c'est le nom de la personne qui est reliée à ces renseignements qui, eux, se veulent protégés. Donc, on pense ici au sondage anonyme, par exemple, où c'est sûr qu'on veut s'exprimer par le biais du sondage, mais on ne veut pas que son nom soit rattaché. Les votes électoraux ou même, je dirais, les sources journalistiques en est un exemple de l'intérêt de ce troisième pilier, de l'intérêt à l'anonymat.

Et c'est ce dernier concept qui rentrait en

jeu dans le contexte de Spencer et dans le contexte de l'Internet de façon plus large et où la Cour a réalisé ou a noté que faire le lien entre le nom d'un abonné et ses activités en ligne peut divulguer l'historique de navigation, les sites de Web consultés, les habitudes de consommation en ligne, les forums consultés. Et là, je rajoute moi-même, à la lumière de notre recherche sur les adresses IP, les commentaires affichés sur Wikipédia, par exemple, parmi une vaste autre quantité de renseignements personnels stockés concernant les internautes.

Et le dernier critère que la Cour a passé en revue, c'est le caractère raisonnable de l'attente à la protection de la vie privée. Donc on a dit tout à l'heure qu'évidemment l'appelant avait un intérêt subjectif. Il s'agissait de savoir si l'attente était aussi objectivement raisonnable.

Et pour ce faire, la Cour a passé en revue le contrat de service du fournisseur de service Internet, dans ce cas c'était Shaw Communications, ainsi que le cadre législatif, pas comme facteur déterminant nécessairement, mais comme des facteurs pertinents. Évaluer la nature objectivement raisonnable de l'attente à la protection de la vie

privée.

Je ne vais pas parler trop de la revue du contrat, bien que c'est fort intéressant parce que le contrat dans ce cas était le contrat de service était avec sa soeur et non pas lui. Donc ici c'était une question importante parce que, lui, il n'était pas partie au contrat d'abonnement, mais ce sera pour un autre jour.

Je vais m'attarder plutôt sur l'analyse du cadre législatif que la Cour a passé en revue, qu'il s'agissait d'être notre loi habilitante, donc notre intérêt d'être là comme intervenant. Alors, la Cour avait fait l'analyse de l'article 7 (3) c.1 .2 de la Loi sur la protection des renseignements personnels et documents électroniques, qui est la loi qui régit le secteur privé, y incluent les sociétés de télécommunications, et sur lequel la police s'est fié comme exception à la règle du consentement pour demander à Shaw Communications de leur fournir le nom et l'adresse de l'abonné associé avec l'adresse IP qu'ils ont suivie en ligne et qu'ils ont identifiés comme client, où ils ont allégué qu'il était identifié avec la pornographie juvénile.

Alors, premièrement, deux points. Je vais

conclure là-dessus. Premièrement, la Cour avait décidé que cette exception au consentement qui existe dans notre Loi ne peut être tenue comme facteur défavorable à l'existence d'une attente raisonnable en matière de vie privée, puisque la disposition elle-même dépend de l'existence d'une attente raisonnable. Le point partant, c'est qu'on parle d'une loi qui existe pour protéger le droit des individus à la vie privée. Donc, le point de départ, c'est que les gens commencent avec une attente en matière de vie privée.

Et le deuxième point, c'est que dans cet article qu'on va revoir peut-être de façon plus détaillée tout à l'heure, la divulgation est discrétionnaire, donc elle doit se distinguer des autres exceptions à l'article 7, dont l'article 7 (3) c. qui, pour sa part, exige la divulgation lorsqu'il y a assignation ou mandat ou ordonnance du tribunal. Donc, là, s'il s'agit d'une divulgation mandatoire, sans le consentement, à la lueur évidemment d'un mandat ou d'une ordonnance d'un tribunal.

L'article 7 (3) c.1, sur lequel la police s'est fiée dans ce cas-ci doit se distinguer. Donc, évidemment, on ne parle pas de cas où il y a

mandat, on parle de cas où il n'y a pas mandat, mais il y avait des conditions rattachées à cette exception. Premièrement, c'est une exception discrétionnaire. Les fournisseurs de service Internet ne sont pas obligés de divulguer l'information, ils peuvent, mais ils ne sont pas obligés. Et, pour le faire, l'institution gouvernementale doit identifier une autorité légitime et ils ne peuvent pas se fier sur 7 (3) c.1 .2, comme autorité légitime. Il faut que cette autorité existe ailleurs. Ce n'est pas dans la Loi même parce que, sinon, ça serait un cercle vicieux. Il faut qu'ils viennent indépendamment avec une source indépendante d'autorité légitime.

Et donc, c'était la responsabilité de la cour de dresser qu'est-ce qui constitue l'autorité légitime dans un tel cas. On ne parle pas de mandat, évidemment, on parle de quelque chose d'autre. Donc, la Cour a dressé trois situations où il y aurait autorité légitime pour la police de demander cette information auprès du fournisseur de service Internet sans mandat. Et ces trois situations sont, là, où il y a une loi raisonnable qui l'autorise, donc il y a une loi habilitante, par exemple, qui autorise l'obtention de ces

données; des circonstances contraignantes, donc urgentes et exceptionnelles, qui ne peuvent pas attendre l'obtention d'un mandat, et qui est bien reconnu dans la Common Law; ou lorsque les renseignements personnels en question n'attirent pas une attente raisonnable en matière de protection de la vie privée, ce qui n'était évidemment pas le cas ici.

Alors, sur ce, je conclus qu'évidemment, dans cette dernière catégorie, c'est plutôt difficile pour une société de télécommunication de voir, juger dans chaque cas d'espèce ou vis-à-vis chaque demande qu'il aurait faite, savoir si, oui ou non, ça attire une attente raisonnable de protection de la vie privée. Et c'est pour ça qu'on a recommandé, dans plusieurs réformes législatives qu'il y ait un encadrement plus spécifique, qui va mieux guider les sociétés, par exemple, de télécommunication à devoir faire cette analyse-là pour faire valoir les leçons de Spencer.

Q. **[41]** Dites-moi, vous avez été intervenants dans... bien, je dis « vous », le Commissariat a été intervenant dans Spencer. Brièvement, pouvez-vous résumer la position que le Commissariat défendait devant la Cour suprême?

R. Alors, évidemment, on a fait valoir le point que les métadonnées étaient sensibles et on a soutenu le point que le nom et l'adresse, ici, n'était pas des renseignements anodins, équivalents à des renseignements qu'on retrouverait dans un annuaire téléphonique, ça, c'en est un, et on se fiait sur nos analyses et nos rapports de recherche qu'on avait faits. On a fait valoir l'argument aussi que l'article 7 (3) c.1 .2 de la loi... notre loi habilitante, de la LPRPDÉ, sur laquelle la police s'est basée pour faire la demande, exige une autorité légitime ailleurs que dans l'article. Donc, il faut vraiment que cette autorité trouve sa source légitime soit dans une loi ou ailleurs que dans la Loi, la LPRPDÉ.

Et nous avons donc soutenu que la Loi, loin de minimiser l'attente raisonnable de vie privée, en fait, renforçait l'attente vu que la Loi a comme objectif principal de protéger les données, et non pas d'en permettre les exceptions.

Q. **[42]** Ça va. Dans le rapport de deux mille quatorze (2014) également, le Commissariat émet des commentaires relativement à la façon dont les entreprises privées qui collectent des données devraient se gouverner quant à la collecte et quant

à la gestion et la divulgation de ces informations. Pourriez-vous informer les commissaires sur la vision du Commissariat au niveau de la collecte de données par les sociétés privées, la gestion de ces données, la divulgation des données?

R. Je m'excuse, j'ai manqué le début. Dans quel contexte?

Q. **[43]** Dans le rapport de deux mille quatorze (2014), il y a des commentaires qui sont faits sur la façon dont les entreprises privées devraient se gouverner quant à la collecte de données, quant à la divulgation de données personnelles. J'aimerais avoir simplement la position du Commissaire à ce niveau-là.

R. Vous parlez du rapport de...

Q. **[44]** Sur les métadonnées.

R. Sur les métadonnées? Et vous parlez plus spécifiquement sur les sociétés de télécommunications, par exemple, qui font l'objet?

Q. **[45]** Allons-y spécifiquement, oui.

R. O.K. Alors nous avons... Évidemment, nous interpellons les organisations à respecter les principes de Spencer. Nous leur rappelons que l'exception à la loi est une exception discrétionnaire, ils ne sont pas obligés de le

faire ou de divulguer l'information. Qu'ils ont la responsabilité, même, de questionner l'autorité légitime pour trouver la source sur laquelle les corps policiers se fient pour demander l'information. Qu'ils devraient songer sérieusement à la nature des renseignements en question, à savoir s'il s'agit de renseignements soient, en soi, sensibles, ou en combinaison avec d'autres renseignements qui pourraient divulguer des informations importantes et sensibles au sujet de leurs abonnés.

Qu'ils devraient aussi - et c'est un point fort important - qu'ils devraient aussi, et ils se doivent, auprès de leurs abonnés, leurs clients, d'être transparents avec les demandes qu'ils reçoivent, et les réponses qu'ils en donnent, en dressant un portrait statistique, dans un rapport annuel, par exemple, qui serait émis une fois par année, pour donner un ordre d'envergure... de gran... un ordre d'envergure, à savoir combien de demandes sont reçues, quelle est la fréquence, quelle est la base aussi des demandes. Est-ce que c'est avec mandat ou sans mandat. Donc, de dresser toutes ces données dans un rapport annuel de transparence, pour mieux éclaircir les clients à

savoir quels sont les risques, quels sont aussi... quelle est leur position vis-à-vis ces demandes vis-à-vis d'autres concurrents, et comment ils les traitent, et quelle est leur politique, leur position vis-à-vis ces demandes. Donc, pour aider aux clients de faire des choix plus éclairés et raisonnables quant à leur fournisseur de service d'internet.

LE PRÉSIDENT :

Q. **[46]** Si vous permettez, ce que vous venez d'exposer, Madame Kosseim, c'est une position institutionnelle du Commissariat, si on veut. Est-ce qu'elle est exprimée aussi clairement dans le rapport de deux mille quatorze (2014), je n'en suis pas certain, et si elle est exprimée clairement à quelque part, où pourrions-nous trouver cette... Évidemment, on va transcrire ce que vous avez dit, alors on va déjà l'avoir sous les yeux, mais si une entreprise, par exemple, voulait agir en bon citoyen corporatif et voulait savoir c'est quoi la position, pour s'aider à prendre une décision devant ces demandes qui peuvent lui être transmises - je ne parle pas des demandes judiciaires, parce que celles-là auront été autorisées par un juge - mais les autres, là, celles qui sont des demandes

non judiciaires, où pourrait-elle trouver l'information?

R. Alors nous avons travaillé sur un volet important sur la production de ces rapports de transparence, pour prendre un exemple, où nous avons à maintes reprises lors d'élaboration de projets de loi ou même dans le cadre de la réforme de notre propre loi, nous avons recommandé qu'il y ait une obligation plus explicite de transparence pour que les organisations, les sociétés de télécommunications puissent publier ces rapporte et on se comprend, ce n'est pas des rapports détaillés qui risquent de mettre en jeu des enquêtes importantes, ce sont des rapports statistiques agrégés qui donnent une idée du nombre et du traitement des demandes qu'ils reçoivent. Nous avons recommandé cela dans le cadre de réformes législatives, nous avons recommandé dans nos lignes, nos communications auprès des entreprises et nous avons publié une analyse de ce que faisaient déjà les sociétés de télécommunications pour faire un inventaire des pratiques courantes. Et nous avons alors à la base de ce qui se faisait déjà par plusieurs, pas tous, mais il y a peut-être cinq compagnies qui produisent ces rapports de

transparence et à la lueur de ces pratiques nous avons pu suggérer les meilleures pratiques. Donc, de tous les rapports qui existaient, on a pu soulever les points les plus forts de certains, d'autres, et c'est un rapport d'ailleurs que mon collègue Chris a élaboré et qui est public sur notre site web pour justement recommander les données statistiques qui devraient être exposées dans ces rapports de transparence.

Nous avons travaillé en étroite collaboration avec ce qui était, à l'époque, Industrie Canada, qui est maintenant Innovation, Sciences et Développement économique Canada, pour développer des lignes directrices. Donc ce ne sont pas nos lignes directrices, ce sont les leurs, mais on a travaillé étroitement en collaboration avec eux et ces lignes directrices qui émettent les données que devraient contenir les rapports de transparence sont disponibles sur leur site web. Et on pourrait vous donner le lien et il existe sur leur site web, encore une fois, dans les deux langues officielles et on y réfère sur notre site également. Donc à la conclusion du rapport de Chris qui est sur notre site web, on fait le lien à ces lignes directrices qui existent en la matière et

qui ont été émises par le gouvernement lui-même.

Q. **[47]** Merci. Est-ce que vous ou monsieur Prince pouvez me donner le nom du rapport, le titre du rapport, est-ce que c'est facilement identifiable dans la liste des rapports disponibles?

R. Ça s'appelle et on peut vous laisser toute cette liste de documents, ça s'appelle les Rapports de transparence des entreprises du secteur privé, une analyse comparée, en date du mois de juin deux mille quinze (2015), et les lignes directrices du gouvernement s'appellent les Lignes directrices concernant la production de rapport sur les mesures de transparence, et je ne vois pas de date, mais ils ont été émis on me dit en même temps, donc en juin deux mille quinze (2015).

Q. **[48]** Les lignes directrices en question, je suppose, je ne devrais peut-être pas supposer, je vous pose la question. Est-ce qu'elles dépassent la confection du rapport de transparence? Est-ce qu'elles vont jusqu'à dire ou à suggérer comment les entreprises devraient agir face à une demande de renseignements?

R. Non. Elles sont des lignes directrices qui portent seulement sur le dernier point que j'ai mentionné qui est que les sociétés devraient être

transparentes quant à la réception et le traitement de ces demandes. Pour ce qui est des autres bonnes pratiques que j'ai mentionnées, je ne peux pas penser à l'instant où nous aurions dressé la liste, aussi explicite que je viens de la faire, mais nous avons dans le cadre de revue de projet de loi, nous avons interpellé le législateur à dresser des considérations plus explicites qui devraient se trouver dans la loi parce qu'évidemment, on peut comprendre la difficulté dans laquelle se trouvent les sociétés de télécommunications à devoir juger d'un cas à l'autre s'il existe une attente raisonnable en matière de vie privée, ce qui est une question tellement complexe qui préoccupe nos tribunaux jusqu'à la Cour suprême du Canada et on ne peut pas imaginer nécessairement une société dans le courant de leurs affaires quotidiennes à devoir peser ces considérations aussi complexes et importantes. Par contre, on essaie de les sensibiliser au fait, comme je l'ai dit, que c'est discrétionnaire, qu'ils se doivent de questionner sur l'autorité légitime et ne pas prendre pour acquis nécessairement qu'ils sont obligés de divulguer l'information. Donc, questionner sur la loi habilitante ou le fondement.

Et comme j'ai dit tout à l'heure, quand même, ils sont des experts en télécommunications et devraient eux-mêmes être sensibilisés à la nature sensible des données et réaliser les enjeux à savoir quels sont les risques d'identification ou de... les risques à divulguer cette information sans mandat.

Maintenant, nous avons aussi souligné à maintes reprises que rien n'empêche les corps policiers à obtenir un mandat. D'ailleurs, dans l'affaire Spencer, la Cour suprême avait souligné qu'avec tout ce qu'ils avaient déjà sur la base des activités en ligne reliée à l'adresse IP, ils avaient de quoi déjà obtenir un mandat. Donc, il n'y avait rien qui les empêchait d'obtenir un mandat avant d'approcher Shaw Communication pour le nom et l'adresse. Donc, ça c'est important aussi à réaliser que rien n'empêche le mandat au préalable. Et Spencer, j'ajouterais, était en deux mille quatorze (2014), donc avant l'introduction des nouvelles dispositions du Code criminel qui, maintenant, permettent une ordonnance sur les données de transmission à un seuil abaissé, pas de motif raisonnable à croire, mais un motif raisonnable de soupçonner. Donc, c'est encore plus

facile maintenant que c'était dans le cas de Spencer d'obtenir un mandat.

Et finalement, je dirais qu'il y a aussi, dans ces nouvelles dispositions du Code criminel, des ordonnances quant à la préservation ou conservation des données. Donc, s'ils ont besoin de plus de temps pour obtenir d'autres informations qui vont soutenir leur demande de mandat ou de perquisition, ils ont la possibilité au moins de faire conserver les données jusqu'à tant à ce qu'ils puissent obtenir le mandat en question. Donc, il y a déjà beaucoup d'évolution depuis l'affaire Spencer qui pourrait faciliter non seulement le traitement de ces demandes par les sociétés, mais aussi le travail ardu des corps policiers qui doivent recueillir cette preuve et soutenir leur demande d'autorisation judiciaire.

Q. **[49]** Je ne veux pas monopoliser le microphone, mais ce seuil abaissé de... est-ce que vous voyez ça, au Commissariat, comme une bonne chose ou une mauvaise chose?

R. Alors, à l'époque, dans le cas du projet de Loi C-13, lorsqu'on a été interpellé devant le comité parlementaire à donner notre point de vue, le commissaire avait exprimé de l'inquiétude quant à

l'abaissement du seuil, du motif raisonnable à croire, au motif raisonnable de soupçonner en raison, justement, d'une nature qui pourrait potentiellement être extrêmement sensible des métadonnées pour toutes les raisons que j'ai traitées tout à l'heure.

Donc, il y avait la question du seuil, mais subsidiairement, si le seuil serait comme finalement, il a été adopté comme étant un motif raisonnable de soupçonner. Si c'était le cas, le commissaire avait recommandé, à l'époque, qu'il y ait d'autres conditions qui soient incluses dans les conditions préalables à l'octroi d'une ordonnance pour, par exemple, limiter les données aux fins de l'enquête et non pas pour d'autres utilisations ou d'autres fins. De... de... songer à savoir si ça devrait exister ou ça devrait être possible pour tout crime ou seulement les plus violents, les plus... les plus importants, les... les plus sérieux. Donc ce sont ce genre de conditions qu'on s'est dit, bien si vous allez abaisser le seuil, bien au moins pensez à d'autres conditions préalables. Ou bien octroyez au juge la possibilité de rattacher des conditions, par exemple, une fois que les conditions préalables

sont rencontrées et les données sont obtenues par les corps policiers, permettre au juge de rattacher des conditions, par exemple à savoir qu'est-ce qui devrait devenir des données captées de façon inattendue sur des gens qui ne sont pas du tout soupçonnés du crime, qui ne sont pas pertinentes. Est-ce que ces données ne devraient pas être détruites immédiatement, par exemple, ou dès qu'ils sont exclus de tout soupçon. Donc ce sont ce genre de... de condition qu'on avait et qu'on... jusqu'à maintenant on aurait voulu voir rattachées à l'octroi de cette ordonnance, ces ordonnances mêmes à un seuil abaissé.

Q. **[50]** Juste une dernière question, probablement la plus facile. Je connaissais les adresses IP, grâce au service de recherche de la Commission, mais vous avez parlé des adresses MAC, M-A-C. Est-ce que c'est... c'est quelque chose d'autre ou c'est la même chose sous un autre nom ou...

R. Alors une chance que j'ai consulté mes technologues hier an anticipation de cette question. Alors effectivement l'adresse IP se trouve à être l'adresse qui est assignée, par exemple, à un « router » dans nos résidences, par exemple. C'est l'adresse qui est associée à l'abonnement de la

résidence. Mais rattaché à l'adresse IP il peut y avoir plusieurs appareils. Et chacun de ces appareils a un numéro spécifique à l'appareil, qui se trouve à être une adresse MAC. Donc ça peut être un téléphone cellulaire, ça peut être un laptop, ça peut être un « game console ».

Q. **[51]** Hum, hum.

R. Un jeu. Donc tous les appareils qui se rattachent au « router », chacun a un numéro spécifique qui identifie l'appareil. Donc c'est l'adresse MAC, qui se distingue d'une adresse IP.

Q. **[52]** Et je vous pose la question, je suppose que l'adresse MAC peut réserver... peut révéler, pardon, autant d'information que l'adresse IP qui a fait l'objet de votre... de votre rapport de deux mille treize (2013)?

R. Et même plus, parce que pour revenir à l'affaire Spencer, il s'agissait de l'adresse IP. Et l'adresse IP était associée à l'abonnement de la résidence, qui était sous le nom de la soeur de monsieur Spencer. Donc même là, la police ne savait pas qui dans la maison utilisait l'ordinateur qui se trouvait à stocker de la pornographie juvénile. Donc il devait aller à un niveau plus loin. Alors qu'une adresse MAC pourrait, je crois, les mener

plus directement à l'utilisateur qui est associé avec l'appareil spécifique. Si ça répond à votre question.

Q. **[53]** Oui, ça répond... ça répond à ma question. C'est... c'est un monde... c'est un monde... je cherche le bon mot pour qualifier le monde dans lequel nous vivons, mais il faut comprendre qu'on vit dans un monde très transparent maintenant. Merci.

R. Merci.

Me CHARLES LEVASSEUR :

J'aurais peut-être suggéré... Il est onze heures cinq (11 h 05), j'aurais peut-être suggéré de prendre la pause, j'allais aborder un autre sujet.

LE PRÉSIDENT :

C'est une bonne idée. Alors quinze (15) minutes, jusqu'à onze heures vingt (11 h 20). Merci.

SUSPENSION DE L'AUDIENCE

REPRISE DE L'AUDIENCE

_____

LE PRÉSIDENT :

Allez-y.

Me CHARLES LEVASSEUR :

Q. **[54]** Alors, Maître Kosseim, nous allons nous attarder à la Loi sur la protection des

renseignements personnels et les documents électroniques. En vertu de la Loi sur la protection des documents électroniques, en vertu de l'article 5, on peut constater qu'une annexe fait partie intégrante de la Loi. J'ai demandé à ce qu'on affiche à l'écran, et vous l'avez à votre droite, l'Annexe 1, qui, comme je le disais, en vertu de l'article 5, fait partie intégrante de la Loi.

Pourriez-vous un peu situer, là, les commissaires sur l'utilité de ces annexes, d'où proviennent les principes, l'effet contraignant?

Me PATRICIA KOSSEIM :

R. Oui. Donc, avec plaisir. Juste pour vous donner un peu le contexte. Cette annexe, qui se trouve, comme vous avez mentionné... qui se trouve à faire partie intégrante de la Loi, en fait, existait bien avait la Loi. C'était un code de pratique qui avait été élaboré par le secteur de l'industrie, qui s'était vêtue de ces lignes directrices et de ces principes, qui sont d'ailleurs basés sur des principes de l'OCDE tels qu'ils existaient à l'époque. Donc, ce sont des principes universels, je dirais, en matière de protection de la vie privée des... la protection des renseignements personnels.

Et lorsque la Loi sur la protection des renseignements personnels et documents électroniques, la LPRPDÉ, a été adoptée, en deux mille (2000), c'était assez inusuel à l'époque, et encore aujourd'hui, que la Loi a, essentiellement, adopté ce code, quand il lui a donné force de loi par le biais de cette annexe.

Donc, les dispositions qui se trouvent à être dans le texte de la loi sont les dispositions qui donnent force de loi à l'annexe et qui sont un peu plus prescrits et qui ressemblent plus à un texte de loi que l'annexe qui est vraiment un code de pratique.

Et là où le législateur a cru bon et a ressenti le besoin, il a qualifié certains de ces principes dans le texte de loi. Donc, par exemple, à certains endroits on dit : « Nonobstant principe untel », et la disposition législative va venir remplacer ou rajouter ou renforcer les principes de l'annexe.

Donc, c'est un peu l'enjeu entre le texte de loi et l'annexe qui fait partie intégrante. Et, d'ailleurs, certains juges, au fil des années, ont commenté sur la nature un peu inusuelle de cette loi, et voilà. Donc, c'est un petit peu

l’historique de l’annexe et comment elle se trouve à être affichée ou intégrée à la Loi telle quelle.

Q. **[55]** Ça, on ne passera pas en revue l’ensemble de l’annexe, mais peut-être je vous suggérerais d’attirer l’attention des commissaires sur certains articles très précis de cette annexe, entre autres, l’article 4.1, qui porte sur la responsabilité relative aux données détenues. Est-ce que vous pourriez un peu expliquer, là, les tenants et les aboutissants de cette annexe?

R. Alors, le principe premier de la responsabilité ou l’imputabilité se trouve, je dirais, à être un des principes les plus importants dans nos... dans le cadre de nos enquêtes, nos vérifications, nos réflexions, et dans le cadre des pratiques des organisations aussi. Parce qu’il se veut être le coeur même, le squelette qui encourage les organisations à adopter des structures et des processus de gouvernance. Donc, c’est vraiment le principe... j’hésite de dire le plus important, mais c'est la toile de fond, finalement. Parce que c'est par le biais de ce principe, et des obligations qui en découlent que les sociétés, les organisations vont faire de quoi pour adopter des procédures; des politiques; vont mettre en oeuvre

ces procédures, ces politiques; vont charger quelqu'un avec la responsabilité de la mise en oeuvre; charger quelqu'un à répondre aux questions des clients, aux plaintes des clients, et qui va adresser les plaintes avant qu'elles aboutissent à des plaintes auprès de notre bureau.

Et le principe veut aussi qu'il y ait un programme de formation des employés quant au traitement des données personnelles, et pas seulement de la formation en début de mandat ou d'emploi, mais une formation régulière et des mises à jour. Et aussi, le principe veut que les organisations rédigent des documents expliquant leurs politiques et les procédures, et je peux dire que de plus en plus, ce principe, sinon explicite, mais implicitement, au Canada et ailleurs dans le monde, cherche à resserrer le principe de responsabilité à ce que les organisations n'aient pas seulement à mettre en place ces mesures de gouvernance, mais aussi être en mesure de les démontrer.

Donc, à la demande d'une autorité en matière de protection des renseignements personnels, les organisations, par exemple, en Europe, doivent être en mesure de démontrer leur

structure de gouvernance. Donc les règles de pratique, ou les bonnes pratiques de coutumes, n'est plus à la hauteur. Il faut vraiment, de plus en plus, que les sociétés en prennent responsabilité, les documents puissent les démontrer à la demande des autorités en question.

Est-ce qu'il y a d'autres choses que je pourrais rajouter? C'est, donc, un petit peu... C'est un petit peu ça. Aussi, rattaché à ce principe de responsabilité, par exemple, on peut voir aussi, de plus en plus, l'importance d'avoir une personne responsable des protections et des renseignements personnels, que ça soit le travail de quelqu'un, peut-être pas à temps plein, mais ça doit être la responsabilité d'une personne. Donc, en Europe, encore une fois, on s'en va de plus en plus à la création de postes mandatoires, « Chief Privacy Officers » pour que vraiment, ces gens-là se relèvent directement à la haute direction, ils font partie, même, de la haute direction, et qu'ils puissent avoir une influence sur les sociétés pour vraiment prendre ces responsabilités à coeur et leur donner l'importance dont ils ont droit.

Q. **[56]** L'article 4.2, qui lui, en vertu de 4.2.1, est lié à l'article 4.8, tout à l'heure on discutait de

transparence, la transparence est prévue à l'annexe, à l'article 4.8, l'article 4.2 sur la détermination des fins de la collecte est lié au principe de transparence. Pourriez-vous nous entretenir brièvement de ce principe?

R. Alors, ça, c'est un principe clé, je dirais, parce que ça ouvre la porte, dans un sens. Tout dépend de la finalité de l'utilisation, ou de la cueillette des renseignements, ou de la divulgation. Donc il faut, le principe interpelle les sociétés à bien définir la fin, la finalité, et la documenter, pour justement les commettre à des paramètres. Donc il faut qu'ils définissent, à prime abord, pourquoi, le pourquoi qu'ils veulent les renseignements personnels ou pourquoi ils vont peut-être, dans certains cas, les utiliser ou les divulguer, parce que c'est le pourquoi qui va informer le consentement. Donc il faut, d'abord et avant tout, qu'eux-mêmes puissent définir le pourquoi, et que le consentement éclairé soit balisé ou soit informé par la fin que veut faire que veut mettre la société, la fin à laquelle la société veut colliger ces renseignements personnels.

Un autre point que j’aimerais rajouter, c’est que lorsqu’une société veut utiliser des

données, par exemple, au-delà des fins qu'ils ont définies au début, bien, ça déclenche l'obligation de retourner obtenir un nouveau consentement. Donc, c'est important de bien définir et de respecter les paramètres de la finalité des données.

Q. **[57]** L'article 4.8 qui traite de transparence, est-ce que j'ai raison de dire que les rapports de transparence proviennent en partie de l'article 4.8 de l'annexe 1 de la Loi?

R. C'est sûr que l'esprit du principe de la transparence mène à encourager les organisations à adopter et publier ces rapports de transparence. Nous ne sommes pas allés aussi loin que certains qui diraient même que c'est une obligation qui découle de ce principe. Nous n'avons pas dit que c'est explicitement requis en fonction du principe de la transparence, mais c'est certainement en ligne avec l'esprit même du principe. Et donc, ça s'aligne très bien avec la volonté du législateur et de l'industrie auparavant en adoptant ce code de pratique que même si tous les renseignements qui pourraient informer le consentement ne peuvent pas nécessairement être dans un formulaire de consentement parce que ça déborderait. Il se faut quand même que ces renseignements soient

transparents ailleurs, que la Société émette leurs politiques, les procédures, soit sur leur site web ou soient en mesure de les produire si quelqu'un les demande ou si la Commission demande de voir les procédures, les politiques, donc il faut que ces... il faut que les sociétés fassent l'effort justement d'être aussi transparentes que possible.

Q. **[58]** Maintenant, on a discuté tout à l'heure de l'article 7, lorsqu'on a discuté de Spencer, on a discuté de l'article 7 de la Loi sur la protection des documents électroniques. Peut-être un commentaire général d'entrée de jeu, là, peut-être un commentaire général sur l'article 7 qui va s'afficher à l'écran dans un instant. Alors, on a effectivement l'article 7. Peut-être un commentaire général en ouverture sur la raison d'être de cet article?

R. Alors, l'article 7 énumère essentiellement les conditions... les exceptions, pardon, aux principes du consentement qui se trouve à être un des principes fondamentaux dans l'annexe. Alors, la Loi par le biais de l'article 7 dresse une liste d'exception que les tribunaux ont déjà jugée, est une liste exhaustive. Donc, si l'exception ne se trouve pas à l'article 7, c'est que l'exception

n’existe pas. Donc, par exemple, dans un des principes, dans un des sous-principes, par exemple, le consentement va être exigé là où... à moins qu’il ne soit pas approprié.

Les tribunaux ont décidé dans des décisions antérieures que la liste de situations où le consentement n’est pas approprié est dressée dans la liste de l’article 7. Donc il n’y a pas de ‘catch all’, il n’y a pas d’autres exceptions, c’est une liste exhaustive.

Deuxième point que je ferais, c’est que toutes les exceptions à l’article 7, aux principes du consentement, demeurent assujetties à un article clé qui se trouve à être l’article 5, alinéa 3. Donc, même s’il y a un consentement, ou même s’il y a exception au consentement, toutes les activités des organisations assujetties à cette loi, la cueillette, l’utilisation et la divulgation doivent être pour des fins qu’une personne raisonnable estimerait acceptable dans les circonstances. Donc, ça vient... c’est le chapeau qui vient se rajouter au-dessus de l’article 7, qu’il y ait ou non consentement.

Troisièmement, pour revenir à ce que je disais tantôt, l’exception au sous-alinéa 7(3)c.1,

par exemple, qui a fait l'objet de l'arrêt Spencer est discrétionnaire. Donc, il y a certaines exceptions qui sont discrétionnaires dans le cadre de la divulgation, par exemple, et d'autres qui sont mandatoires. Donc, ça aussi c'est important à souligner.

Et le quatrième point que je ferais sur le paragraphe 7, ou l'article 7, et comme l'a dit la Cour suprême du Canada dans une affaire récente de la Banque Royale Canada c. Trang, l'article 7 vise à faire en sorte que la loi n'ait pas d'incidence sur les communications légalement requises. Donc, l'objet de la loi n'est pas d'enfreindre des communications qui sont légalement permises ailleurs, c'est d'ailleurs prévu à l'article 7.

Q. **[59]** Mais justement, bien je vais saisir la balle au bond, là, 7(3)c.1, c'est un régime d'exception. J'aimerais que vous nous traciez brièvement le portrait de l'exception, et plus particulièrement, je vous dirais, là, c.1(ii) et (iii).

R. Oui. Alors, 7(3c.1, il s'agit d'une exception au consentement, au consentement, aux principes du consentement lorsqu'il s'agit d'une divulgation à une institution gouvernementale qui a demandé à obtenir le renseignement sur la base d'une autorité

légitime étayant son droit de l'obtenir. Donc, c'est le cas Spencer, justement, où une organisation se fait demander l'information par une instance gouvernementale.

Et il y a des sous-scénarios, si vous voulez, lorsque cette information est demandée parce que l'institution gouvernementale qui a identifié son autorité légitime le demande parce qu'elle... vous voulez (ii) et (iii)?

Q. **[60]** Hum hum.

R. Elle demande la communication aux fins de contrôle d'application du droit canadien, ou provincial, ou étranger de la tenue d'enquête liée à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application. Donc, c'est un scénario.

L'autre, c'est lorsque cette information est demandée pour l'application du droit canadien ou provincial. Donc, (ii) vise le contrôle d'application de la loi et (iii) vise l'application de la loi canadienne ou provinciale. Je peux vous donner un exemple.

Q. **[61]** Allez-y.

R. Alors, le sous-alinéa (ii), c'était le cas de Spencer où la police, les corps policiers

demandaient la communication pour fins de faire avancer leur enquête. Il s'agissait justement d'une exception qui est liée au contrôle d'application de la loi. Le sous-alinéa (iii) est demandé pour l'application du droit canadien ou provincial, donc on peut penser même à notre bureau.

Nous avons, par exemple, le pouvoir, en vertu de notre loi habilitante dans le cadre de notre enquête, nos enquêtes, de demander certains renseignements auprès des sociétés qui font l'objet de notre enquête et de contraindre ces sociétés à produire ces renseignements. On n'est pas responsable pour le contrôle d'application de la loi, mais on administre la loi. Et sous les critères Spencer on est... on demande... notre autorité légitime c'est justement la loi habilitante qui nous donne cette... ce pouvoir explicite. Donc c'est un petit peu la différence entre (ii) et... sous alinéa (ii) et (iii).

Q. **[62]** Et bien que la réponse puisse semble évidente, je comprends que pour avoir accès... instance gouvernementale, j'ai raison de dire que ça peut comprendre une organisation policière à 7(3)?

R. Hum hum.

Q. **[63]** Et je comprends également qu'une autorisation

judiciaire, un mandat n'est pas nécessaire pour contraindre. Parce que c'est ce qu'on appelle le pouvoir de contrainte, pour contraindre une organisation à transmettre de l'information en vertu de cet article-ci.

R. Un mandat n'est pas nécessaire, non, c'est d'ailleurs ce que la Cour suprême du Canada a dit dans Spencer. Parce qu'il faut distinguer cette disposition de la... du paragraphe 7(3)c) qui, elle, prévoit l'existence d'un mandat ou ordonnance d'un tribunal. Donc c'est deux scénarios différents.

Q. **[64]** Dites-moi, est-ce que le Commissariat à la vie privée est avisé de ce genre de demande-là qui sont présentées à des entreprises privées?

R. Non. Et il y a deux raisons pour ça. Alors premièrement, d'emblée il n'y a pas d'obligation à la réception d'une demande, d'aviser notre bureau. Il n'y a pas d'obligation explicite dans la loi. Dans la loi... dans le secteur privé, ni dans la loi sous... ni dans le secteur public. Parce que nous avons souligné ce point, cette lacune quant à nous, au Parlement en vertu des deux lois. Parce que quant à nous, il devrait y avoir une reddition de compte et de la part de la société,

l’organisation qui reçoit, qui traite les demandes, mais aussi la part de l’instance gouvernementale qui fait la demande. Et il n’y a pas de... d’obligation proactive à notifier notre bureau. Ni dans un ni dans l’autre cas.

Q. **[65]** Et est-ce qu’il y a une obligation proactive de tenir un registre, par exemple, de l’information qui est demandée ou de l’information qui est transmise ou...

R. Non, est c’est ce que nous avons recommandé dans le cas de réformes des deux lois habilitantes, que cette obligation soit incluse spécifiquement, explicitement. Et pour les organismes, organisations et pour les instances gouvernementales. Des deux côtés. Pour pouvoir dresser un portrait global de l’envergure de ces demandes, la fréquence, la base juridique, etc. Donc c’est vraiment une lacune que nous trouvons dans les deux lois.

Q. **[66]** Alors au moment où se parle est-ce que j’ai raison d’affirmer qu’il y a aucune traçabilité des demandes qui pourraient être présentées en vertu de 7(3)c.1?

R. Malheureusement, non. Et je vais vous donner un exemple concret. Nous avons sous l’article 37 de la

loi sur la... qui... de la Loi sur La protection des renseignements personnels dans le secteur public, nous avons initié une revue... une revue des pratiques de la GRC justement, pour leur demander parce qu'on voulait être en mesure de... d'avoir, de savoir l'étendue de... et la fréquence de ses demandes, particulièrement des demandes auprès des sociétés de télécommunications pour l'information reliée aux abonnés, sans mandat. Donc c'était l'objectif de la vérification qu'on a initiée.

Et on voulait savoir... et justement combien, la fréquence, auprès de qui? Et malheureusement, la tenue des dossiers à la GRC n'était pas conçue de façon à pouvoir nous donner cette information. Donc malheureusement la vérification... la revue n'a pas mené à grand-chose parce qu'on avait... la GRC elle-même n'était pas en mesure de pouvoir confirmer ni le nom, ni la fréquence, ni auprès de qui toutes ces demandes avaient été faites. Évidemment, une des recommandations qui en est sortie c'est que vous devriez avoir des mesures de documentation, des moyens de documentation en place pour mieux gérer et documenter et connaître l'envergure de ces

demandes.

Me CHARLES LEVASSEUR :

Ça termine. Merci beaucoup.

LE PRÉSIDENT :

Merci, Maître Levasseur.

Alors, vous avez droit à la torture des questions provenant des avocats pour vous remercier. Mais ils sont tous toujours très à propos, alors vous n'avez pas à vous inquiéter.

LE PRÉSIDENT :

Alors, on procède en commençant par maître Battista, aujourd'hui. Maître Corbo, donc.

Me MATHIEU CORBO :

Oui. Pas de questions, Monsieur le Président.

LE PRÉSIDENT :

Très bien. Maître Carlesso?

Me JULIE CARLESSO :

Pas de questions, Monsieur le Président.

LE PRÉSIDENT :

Vous allez me faire mentir. Maître Christian Leblanc?

Me CHRISTIAN LEBLANC :

Je n'aurai pas de questions non plus.

LE PRÉSIDENT :

Merci. Maître Boucher?

Me BENOIT BOUCHER :

Pas de questions.

LE PRÉSIDENT :

Maître Dumais n'est pas ici. Maître Doray?

Me RAYMOND DORAY :

Pas de questions, Monsieur le Président.

LE PRÉSIDENT :

Merci. Maître Soulière?

Me GÉRALD SOULIÈRE :

Je n'ai pas de questions dans le cadre de mon mandat même si, personnellement, j'en aurais beaucoup. C'est un sujet très intéressant. Merci beaucoup, Madame.

LE PRÉSIDENT :

Merci. Maître Crépeau n'est pas ici. Bon. Alors, écoutez, je vous avais promis la torture, mais je ne tiendrai pas ma promesse, bien malgré moi. Il me reste à vous remercier au nom de la Commission, c'était un panel très intéressant. Vous êtes, de toute évidence, très au fait du dossier. Vous nous avez éclairés, à plusieurs égards, sur ce nouveau monde dans lequel nous sommes maintenant. Je suppose que vous êtes tous les trois en poste à

Ottawa.

Me PATRICIA KOSSEIM :

R. Oui.

Q. **[67]** Alors, c’est d’autant plus apprécié que vous vous soyez déplacés pour venir nous rencontrer. Alors, Maître Kosseim, merci beaucoup. Maître Barss, merci beaucoup aussi et, Monsieur Prince, merci beaucoup également.

ET LES TÉMOINS NE DISENT RIEN DE PLUS

LE PRÉSIDENT :

Maintenant, je m’adresse à maître Joncas ou maître Levasseur, est-ce qu’il y a un autre témoin pour ce matin ou le professeur Dupont sera ici cet après-midi.

Me LUCIE JONCAS :

Le professeur Dupont sera ici cet après-midi.

LE PRÉSIDENT :

Alors, écoutez, on va tout de suite ajourner pour quatorze heures (14 h). Merci beaucoup.

LA GREFFIÈRE :

Alors, nous allons suspendre l’audience jusqu’à quatorze heures (14 h).

SUSPENSION DE L’AUDIENCE

REPRISE DE L’AUDIENCE

_____

PRÉLIMINAIRES

LA GREFFIÈRE :

Bonjour, rebienvenue à la Commission. Veuillez vous assurer que vos cellulaires et autres appareils mobiles soient éteints. Et notez qu'il y a interdiction d'enregistrer ou de prendre des photos dans la salle d'audience, selon les règles de procédure de la Commission. Et n'oubliez pas d'ouvrir votre micro pour les fins de l'enregistrement.

LE PRÉSIDENT :

Bonjour. Bon après-midi à tout le monde. Je demanderais à notre greffière de procéder à l'appel des avocats.

LA GREFFIÈRE :

Alors, je demanderais d'abord aux procureurs de la Commission de s'identifier pour les fins de l'enregistrement numérique.

IDENTIFICATION DES PROCUREURS

Me CHARLES LEVASSEUR :

Bonjour, Charles Levasseur pour la Commission.

Me LUCIE JONCAS :

Bonjour, Lucie Joncas pour la Commission.

LA GREFFIÈRE :

Et je demanderais maintenant aux procureurs des

parties de s'identifier et d'identifier ceux qu'ils représentent, et bien ouvrir leur micro.

Me CHRISTIAN LEBLANC :

Bonjour, Christian Leblanc. Je suis accompagné cet après-midi de mon collègue et associé, Chris Semerjian, qui sera parmi nous un peu plus souvent à partir de maintenant. Et tous les deux donc, nous représentons La Presse, Radio-Canada, Cogeco, Postmedia, Transcontinental Médias, Groupe Capitales Médias et Bell Media.

Me BENOIT BOUCHER :

Bon après-midi, Benoit Boucher pour la Procureure générale du Québec.

Me MATHILDE BARIL-JANNARD :

Bonjour, Mathilde Baril-Jannard pour la Fédération nationale des communications.

Me MATHIEU CORBO :

Bonjour, Mathieu Corbo pour le Service de police de la Ville de Montréal.

Me RAYMOND DORAY :

Bonjour, Raymond Doray pour la Conférence des juges de paix magistrats du Québec. Bon après-midi.

Me JEAN-NICOLAS LEGAULT-LOISELLE :

Alors, Jean-Nicolas Legault-Loiselle pour la Ville de Montréal. Bon après-midi.

Me GÉRALD SOULIÈRE :

Bonjour, Gérald Soulière, la Fraternité des policiers et policières de Montréal.

Me JULIE CARLESSO :

Bonjour, Julie Carlesso pour Le Devoir et Québecor Média.

Me MOLLY KRISHTALKA :

Bonjour, Molly Krishtalka pour le Canadian Journalists for Free Expression, Reporters sans frontières and Committee to Protect Journalists.

LA GREFFIÈRE :

Merci.

LE PRÉSIDENT :

Maître Levasseur.

Me CHARLES LEVASSEUR :

Merci. Monsieur le Président, Madame la Commissaire, Monsieur le Commissaire, je vous annonçais ce matin que nous aurions la chance d'entendre le professeur Benoît Dupont cet après-midi, qui viendra nous entretenir des métadonnées et de la surveillance électronique. Je peux laisser à madame la greffière le soin d'assermenter monsieur Dupont et je procéderai ensuite.

_____

L’AN DEUX MILLE DIX-SEPT (2017), ce cinquième (5e) jour du mois d’avril, a comparu :

BENOÎT DUPONT, professeur de criminologie;

LEQUEL, après avoir fait une affirmation solennelle, dépose et dit :

INTERROGÉ PAR Me CHARLES LEVASSEUR :

Q. **[68]** Monsieur Dupont, vous êtes professeur de criminologie à quel endroit?

R. À l’Université de Montréal.

Q. **[69]** Et vous êtes professeur de criminologie depuis combien de temps?

R. Depuis deux mille deux (2002).

Q. **[70]** Depuis deux mille deux (2002). Vous êtes également détenteur de la Chaire de recherche du Canada en cybersécurité, c’est exact?

R. C’est exact, oui.

Q. **[71]** Pouvez-vous expliquer aux commissaires un peu, là, les tenants et les aboutissants de ce qu’est la Chaire de recherche en cybersécurité?

R. Alors, la Chaire de recherche c’est... comment dirais-je, une subvention de recherche qui est destinée à faire vivre un programme de recherche

avec des étudiants, des collaborateurs du secteur industriel et du secteur public, pour mieux connaître les risques numériques auxquels nos sociétés modernes sont confrontées. Ainsi que les réponses qu'on peut y apporter en termes de politique publique, mais aussi de pratique technologique et sociale.

Q. **[72]** En plus d'être professeur à l'Université de Montréal, d'être détenteur d'une chaire de recherche, vous êtes également directeur scientifique du Réseau intégré sur la cybersécurité, c'est exact?

R. C'est bien ça, oui.

Q. **[73]** Pouvez-vous brièvement nous expliquer ce que c'est?

R. Oui. Alors, il s'agit d'un réseau de mobilisation des connaissances qui réunit une vingtaine d'universités canadiennes, des chercheurs du domaine informatique et des sciences sociales ainsi que des agences gouvernementales, une dizaine d'agences gouvernementales des niveaux fédéraux, provinciaux et municipaux, ainsi qu'une dizaine d'entreprises spécialisées dans le domaine de la cybersécurité, pour essayer de mieux diffuser un petit peu les connaissances scientifiques dont nous

disposons à l'heure actuelle sur les risques numériques. Et d'améliorer un petit peu la résilience de la société canadienne face à ces risques-là.

Q. **[74]** Alors, Monsieur Dupont, vous nous entretiendrez aujourd'hui de la surveillance des métadonnées en lien avec les événements qui nous occupent. Je vous cède la parole, et je vous interpellerai sur certains points, là, si le besoin en est.

R. Merci Maître. Monsieur le Président, Madame la Commissaire, Monsieur le Commissaire, Mesdames et Messieurs les participants et intervenants à la Commission, on m'a demandé aujourd'hui d'examiner avec vous le rôle que jouent les métadonnées dans la surveillance contemporaine, et les risques que celles-ci font peser sur la protection de la vie privée, en général, et sur la confidentialité des sources journalistiques en particulier.

Alors, lorsque l'affaire qui a conduit à la nomination de cette commission d'enquête a éclaté, un haut responsable policier qui était interrogé par les médias a déclaré que l'obtention des numéros entrants et sortants d'un cellulaire était parmi les moyens les moins intrusifs à la

disposition de la police. On essaiera donc de voir ce qu'il en est, ce qui a nécessité, pour cela, de comprendre ce que sont les métadonnées, quelle est leur utilisation technique, avant de nous intéresser à leur utilisation à des fins d'enquête et de surveillance.

On sera ensuite amené à comprendre la richesse des informations personnelles qu'elles peuvent révéler au sujet de ceux qui les produisent, et à réfléchir sur les risques qui découlent d'une trop grande dépendance à leur égard pour des fins de surveillance ou d'enquête.

Et je conclurai, enfin, en proposant quelques réflexions additionnelles sur le rôle que les métadonnées jouent dans notre société, ainsi que sur le nouvel environnement technologique dans lequel les journalistes doivent défendre la confidentialité de leurs sources.

Mais avant de plonger plus avant dans ces questions techniques, j'aimerais proposer quelques rappels sur la place centrale qu'occupe la surveillance dans nos sociétés numériques.

La révolution numérique, et toutes les innovations technologiques et sociales qui l'ont accompagnée et qui ont transformé notre vie

quotidienne, nous ont également fait rentrer dans une ère de la surveillance omniprésente à laquelle il nous est virtuellement impossible d'échapper, à moins qu'on choisisse de déconnecter toutes les machines qui nous sont devenues indispensables, aussi bien dans notre vie professionnelle que dans notre vie sociale, et de nous mettre en retrait de la société. On s'entend que ce n'est pas nécessairement une solution qui est très réaliste.

Il ne s'agit pas ici d'un constat qui est alarmiste, ou d'une invitation à voir partout des complots mondiaux portant atteinte à la vie privée, mais d'une analyse qui se veut lucide des nouvelles configurations sociales qui structurent le fonctionnement de nos sociétés contemporaines.

Loin de se présenter comme un bloc monolithique, cette surveillance généralisée s'exerce selon plusieurs modalités et rationalités qui ont toutes en commun la prolifération des traces numériques et des données que chaque individu produit et laisse derrière lui de manière routinière, un petit peu comme le Petit Poucet laissait des petits cailloux et des miettes de pain pour retrouver son chemin dans la forêt.

Ces traces numériques sont utilisées par

toutes les institutions qui nous entourent. Elles sont utilisées par les entreprises de contenu et les services en ligne, qui s'en servent pour mieux comprendre nos intérêts, et ainsi cibler la publicité qu'elles vont pouvoir afficher sur les pages que nous consultons, ou nous faire des offres commerciales auxquelles il nous sera très difficile de résister.

Elles sont utilisées aussi par les entreprises de télécommunications qui vont agréger ces données pour mieux adapter leurs capacités techniques aux besoins de leurs clients, et dans certains cas ralentir l'accès de leurs clients les plus voraces qui utilisent trop de bande passante et qui ralentissent les autres usagers de leur réseau.

Elles sont utilisées par les entreprises d'assurance et de crédit, qui vont tenter d'évaluer le risque posé par des clients potentiels qui désirent souscrire des polices ou des prêts, en essayant de détecter, dans les habitudes de vie qui sont divulguées en ligne, des comportements qui sont perçus comme indésirables.

Elles sont utilisées par les consommateurs, quand ils vont utiliser des services comme Airbnb

ou Uber, et ils vont consulter, en ligne, la fiabilité de leur chauffeur ou de leur hôte potentiel, qui auront été laissées par des usagers qui les auront précédés.

Elles sont utilisées aussi, évidemment, par les agences de renseignements, les Services de police, ou encore les unités de lutte contre la fraude, qui vont accéder à de vastes quantités de données plus ou moins publiques sur des personnes qui sont jugées suspectes.

Mais les délinquants aussi vont pouvoir recueillir des informations très détaillées sur des victimes potentielles, en ligne, qui sont partagées plus ou moins volontairement et qui sont, évidemment, très utiles pour identifier des victimes potentielles.

LE PRÉSIDENT :

Q. **[75]** Professeur Dupont, est-ce que vous permettez qu'on vous...

R. Absolument.

Q. **[76]** ... pose des questions en cours de route?

R. Absolument. Tout à fait.

Q. **[77]** Plutôt que de les garder pour nous et finalement perdre le fil peut-être un peu. Les exemples que vous venez de donner, les compagnies

d’assurances, les corps de police, est-ce que vous dites que c’est utilisé ou ça peut être utilisé?

R. Je dis que c’est utilisé actuellement.

Q. **[78]** Et pour dire que c’est utilisé, on se base sur quoi?

R. On se base sur des enquêtes journalistiques, des recherches effectuées sur le terrain, sur des publications qui sont elles-mêmes divulguées par les utilisateurs, ces entreprises-là qui doivent échanger avec des chercheurs, avec leurs homologues, pour comparer la fiabilité de leurs outils.

Q. **[79]** Donc, le portrait que vous faites, c’est un portrait de la réalité.

R. Tout à fait. Ce qui se passe aujourd’hui. Pas forcément tout au Québec, mais des capacités techniques qui existent dans notre environnement immédiat au Québec ou dans le reste du Canada, en Amérique du Nord ou ailleurs.

Q. **[80]** D’accord. Donc, ce n’est pas un scénario, c’est un documentaire.

R. Exactement, tout à fait. Vous avez tout à fait compris. Et donc, on vit dans une société de verre où les vertus souvent affichées de la transparence, cachent en réalité une explosion de la

surveillance. Et celle-ci va seulement dans l'avenir être amenée à prendre de l'expansion, puisqu'on nous annonce l'Internet des objets dans lequel une multitude d'objets connectés vont diluer les frontières entre le monde en ligne et le monde incarné et va connecter des frigos, des télévisions, des véhicules à Internet et que tous ces capteurs-là vont devenir finalement des outils de surveillance qui vont pouvoir être utilisés par toutes ces institutions que je viens de nommer. On a déjà vu des divulgations, des révélations sur le fait que, par exemple, la CIA arrive à pirater des frigos, des télévisions intelligentes pour espionner ce qui se passe au domicile de certaines de leurs cibles.

Donc, évidemment, je suis tout à fait conscient que cette Commission d'enquête ne porte pas sur la surveillance, mais les thématiques qui l'occupent s'inscrivent dans cette ubiquité de la surveillance de masse qui caractérise nos sociétés numériques et sur les masses de données qu'elles produisent. Donc il y a une connexion quand même entre ce contexte plus large et la thématique de la Commission d'enquête. Et pour que toutes ces masses de données puissent être traitées à très grande

échelle et que leur circulation se fasse de manière fluide, on a recours à un outil indispensable qui sont les métadonnées. C'est pour ça que je tenais à contextualiser un petit peu.

Alors, que sont les métadonnées? Ce sont des données techniques et contextuelles sur les données numériques qui transitent par les réseaux de télécommunications et les réseaux Internet. Donc, ce sont des données sur les données. Elles contiennent des renseignements sur les contenus, sur les machines, sur les activités et parfois, sur les personnes qui prennent part à une transaction en ligne, comme un appel téléphonique, la consultation d'un site Internet ou l'envoi d'un courriel électronique.

Dans notre monde numérique, il est important de comprendre qu'on ne peut pas vivre sans métadonnées, car leur utilité principale n'est pas la surveillance des usagers, mais la localisation des données qui transitent par une multitude de réseaux et de technologies qui sont toutes interconnectées les unes avec les autres. Donc, l'intérêt primaire des métadonnées, c'est de contribuer à l'efficacité du fonctionnement de l'Internet et des réseaux de télécommunications

tels qu'on les connaît aujourd'hui.

Pour illustrer cela, je vais utiliser quelques représentations visuelles de l'architecture d'Internet pour vous aider à comprendre pourquoi on a besoin des métadonnées pour que nos réseaux distribués numériques, électroniques puissent fonctionner. Internet a été conçu dans un contexte de guerre froide pour que les réseaux de communications militaires qui étaient très centralisés puissent survivre en cas de conflit nucléaire, de cataclysme majeur. Parce qu'évidemment, si vous avez un conflit, une catastrophe naturelle, une catastrophe causée par l'homme et que vous avez un réseau centralisé, il suffit que ce réseau soit anéanti pour que vous perdiez votre capacité de communication.

Et donc, le Pentagone a financé des recherches pour essayer de créer un protocole de communications décentralisées qui permettrait de continuer à pouvoir expédier des messages en les découpant en paquets de données qui pourraient prendre des chemins différents et atteindre leur destinataire qui, ensuite, les réassemblerait pour accéder au contenu du message. Donc, on a créé un réseau décentralisé dans lequel vous prenez un

message envoyé par l'émetteur, vous le découpez en petits paquets numériques, vous les envoyez par plusieurs chemins différents et le récepteur va réassembler ces paquets pour pouvoir accéder au contenu de l'intégralité du message. Et donc, évidemment, si vous avez un problème sur l'un des noeuds qui constituent ce réseau, vous avez néanmoins la capacité de pouvoir utiliser des chemins alternatifs et de pouvoir continuer à distribuer les contenus de vos messages numériques. Mais pour que ce protocole puisse fonctionner, que cette décentralisation puisse être efficace, chaque paquet de données doit être étiqueté pour qu'on sache d'où il vient et à qui il est destiné et qu'en cas où un paquet d'un message plus vaste n'est pas distribué, pour une raison X, Y ou Z, le récepteur de ce message puisse renvoyer un message à l'émetteur en disant : « Il me manque une partie du message, veuillez me le renvoyer. » Et donc, les métadonnées sont un petit peu ce mécanisme de protection qui permet de savoir, est-ce que j'ai reçu l'intégralité du message, d'où viennent-ils et qui dois-je contacter s'il me manque des morceaux pour que je puisse le réassembler dans son intégralité.

Q. **[81]** C’est ce que vous avez appelé leur utilité primaire?

R. Exactement. C’est leur utilité technique, c’est-à-dire c’est pour ça qu’elles existent. Et donc, on voit que c’est vraiment cette utilité-là qui justifie leur existence. Donc, cette architecture va permettre à l’ensemble de l’infrastructure de rester opérationnel, comme je l’ai dit, même si certains points de distribution cessent de fonctionner ou s’ils fonctionnent seulement de manière épisodique. Et ça permet aussi au réseau de se développer potentiellement sans limites de temps puisqu’il n’y a plus de goulot d’étranglement et donc, vous pouvez rajouter autant de nouveaux équipements à ce réseau-là puisqu’il va toujours essayer de trouver une façon de distribuer les contenus et d’optimiser la circulation des données à travers les... à l’origine de milliers de machines et aujourd’hui, de milliards de machines sans avoir à changer son architecture sous-jacente.

Donc, ces étiquettes qui permettent de savoir, pour chaque paquet, de quelles machine et réseau ils proviennent, où ils seront et par quel chemin ils transitent s’appellent donc les métadonnées.

Pour être utiles, ces métadonnées doivent pouvoir décrire toute machine qui est connectée au réseau et c'est à travers les adresses IP, dont vous avez, je crois, entendu parler ce matin. Donc les adresses IP sont une catégorie de métadonnées qui vont décrire une machine qui est connectée à un réseau. Ça peut être aussi de décrire le type de navigateur qui est utilisé par un ordinateur pour accéder à internet, ça peut être le système d'exploitation qui est utilisé par une machine. Est-ce que c'est une machine Mac, une machine PC? Les métadonnées vont aussi pouvoir décrire le contenu qui transite par le réseau; quel est le type d'application qui a été utilisé pour envoyer un message ou un contenu particulier; quel est l'identifiant unique pour chaque message qui est envoyé - chaque courriel reçoit un identifiant particulier dès qu'il quitte votre boîte aux lettres électronique et qu'il s'en va sur le réseau - quels sont les serveurs qui sont utilisés pour distribuer ce contenu; quelles sont les données temporelles et géographiques, également, qui sont associées à certaines machines, à l'envoi de certains messages. Et idéalement, les métadonnées vont aussi chercher à décrire quelles sont les

identités des utilisateurs qui expédient certains contenus, donc ça peut être un identifiant, ça peut être une adresse courriel, ça peut être un « cookie » qui est implanté sur votre machine que vous avez préautorisé par un service que vous utilisez régulièrement en ligne, et caetera, et caetera. Donc, les métadonnées c'est cette très grande diversité d'étiquettes qui vont permettre de suivre un petit peu la circulation des données numériques sur ce réseau décentralisé qu'est l'internet.

Et c'est la même chose pour les services de télécommunication cellulaire dont les contenus sont numérisés et qui font aussi appel à une infrastructure distribuée en réseau qui cherche à optimiser en permanence la distribution des ressources pour offrir un service continu à des usagers qui vont bouger en ville et qui, dans les communications, vont devoir être relayés par des antennes à travers une ville comme Montréal, par exemple. Donc, on a besoin des métadonnées pour savoir qui s'en va où et qui est en communication avec qui pour qu'on puisse avoir un passage fluide d'une antenne relais à une autre.

Alors les types, on peut plonger plus en

détail. Les types de métadonnées qui sont recueillies par les différentes entreprises et les différents fournisseurs d'équipements, selon les secteurs d'activités, si on prend, par exemple, les opérateurs télécoms, ce sont les données qui permettent l'identification unique de chaque usager. Donc, chaque usager qui a un téléphone cellulaire a également un numéro IMSI qui contient quinze (15) chiffres et qui est assigné par l'opérateur de télécommunication à chaque client à travers la carte SIM que vous installez dans votre téléphone cellulaire. Donc chaque carte SIM comprend un numéro IMSI de quinze (15) chiffres, unique, qui est assigné par chaque opérateur de télécommunication à chaque usager.

Chaque communication également génère des données qui permettent l'identification des équipements utilisés, donc ça c'est le numéro IMEI, un autre numéro de quinze (15) chiffres que vous retrouvez au dos de votre téléphone cellulaire et qui cette fois-ci n'est pas assigné par l'opérateur de télécommunication, mais par le fabricant de votre terminal.

Donc si vous avez iPhone, c'est Apple qui, selon les conventions internationales, assigne un

numéro unique à votre téléphone cellulaire. Il n'y a pas une autre commande qui utilise le même numéro IMEI. Samsung fait la même chose, tous les fabricants de téléphones cellulaires assignent un numéro unique à chaque appareil qui est connecté au réseau pour qu'on puisse justement l'identifier.

Q. **[82]** Si vous me permettez, donc lorsque je me sers de mon téléphone cellulaire, non seulement mon numéro IMEI va sur le réseau, mais aussi le IMSI de ma carte SIM. Donc il y a deux numéros qui s'en vont sur le réseau de mon fournisseur cellulaire et qui peuvent potentiellement relier la communication à mon cellulaire.

R. Absolument, parce qu'à chaque fois qu'une communication est initiée, les métadonnées sont générées avec le numéro IMEI, IMSI, le début de la communication, le numéro qui est appelé, le numéro d'appel, la géolocalisation également de la communication le plus souvent.

Q. **[83]** Et est-ce que, vous nous l'avez peut-être dit, mais est-ce qu'il existe... est-ce qu'il peut exister deux numéros IMEI, deux numéros IMSI semblables?

R. Non, c'est impossible.

Q. **[84]** Ça va.

R. Donc je viens de le dire, les autres métadonnées générées pour le compte des opérateurs télécoms sont les propriétés... les métadonnées qui concernent les propriétés techniques d'une communication, donc les données géographiques pour aider à déterminer quelles sont les antennes relais qui ont été utilisées pour transmettre une communication. La date d'une communication, son heure, sa durée et le routage de l'appel, c'est-à-dire par quel serveur cette communication-là est passée. Et également toutes les données qui vont permettre l'identification du destinataire de la communication, donc le numéro qui est appelé.

Donc ça, c'est pour les opérateurs de télécommunication. Pour les fournisseurs d'accès Internet, les données... les métadonnées sont les données qui permettent d'identifier les usagers d'un service en ligne, donc l'adresse IP, qui est l'identifiant unique assigné à chaque machine qui est connectée à Internet. Le pseudonyme quand on utilise un identifiant, l'adresse de courriel, le mot de passe et d'autres moyens d'identifier les usagers. Les données techniques d'une connexion, c'est-à-dire la date et l'heure à laquelle toute action est prise sur Internet. Et les données, dans

le cas d'un courriel, qui permettent d'identifier le destinataire, c'est-à-dire l'adresse courriel du destinataire d'un message.

Mais on peut également voir des métadonnées qui sont générées par des équipements et des applications qui ne sont pas connectées à un réseau. Par exemple, quand vous envoyez un document Word, un document Excel, des métadonnées sont générées pour chaque nouveau document que vous créez, notamment votre nom, la machine qui est utilisée. À chaque fois que vous prenez une photo numérique, des métadonnées sont générées aussi. Et donc un appareil numérique ou un téléphone intelligent qui prend une photo aujourd'hui va associer à chaque image des métadonnées qui comprennent des informations techniques sur l'équipement qui a été utilisé, l'heure et la date à laquelle la photo a été prise et dans certains cas la géolocalisation de l'endroit où la photo a été prise. Ce qui veut dire que c'est donc bien plus qu'une photo, ce fichier qui est généré. C'est en quelque sorte une source détaillée d'informations personnelles sur le photographe et sur les personnes qui figurent sur la photo, puisque de plus en plus de services de

renseignements et de police mettent sur pied des bases de données de reconnaissance faciale.

Et on a appris qu'aux États-Unis, par exemple, le FBI dispose d'une base de données, s'est constitué une base de données de reconnaissance faciale qui comprend les visages de la moitié de la population américaine. Donc à partir des photos, à partir des données qui figurent sur ces photos-là et d'autres données qui sont recueillies par ailleurs on peut mettre en place des programmes de surveillance qui peuvent être extrêmement intrusifs.

Alors j'ai dit que les métadonnées étaient... avaient une utilisation primaire qui était technique, mais évidemment quand on commence à comprendre la richesse des informations qui sont véhiculées par les métadonnées, on voit qu'elles peuvent également être utilisées à des fins de surveillance.

Elles sont omniprésentes autour de nous, chaque appareil connecté en notre possession en génère en permanence des quantités considérables au contact de l'infrastructure de télécommunication. Et donc on comprend très bien l'intérêt des services de renseignements, d'autant plus qu'il est

devenu beaucoup plus facile, avec les progrès qui sont réalisés par l'informatique ces dernières années en termes de puissance de calculs et de coûts réduits de stockage de l'information, de pouvoir les traiter de façon complètement automatisée et en temps réel. Et on a appris, par exemple, des géants du web comme Google, LinkedIn, Facebook ou Microsoft, qu'ils ont développé des réseaux de ces métadonnées, des réseaux d'analyse de ces métadonnées, qui contiennent des dizaines de milliards d'informations portant sur des centaines de millions d'usagers.

Donc on comprend que les capacités techniques sont disponibles, qu'elles sont relativement faciles d'usage, et que les technologies informatiques actuelles nous permettent de traiter, de façon routinière, des quantités impressionnantes, considérables, de ces métadonnées-là, que nous produisons en quantité tout aussi impressionnante au quotidien.

Donc, cette démocratisation et cette ubiquité des technologies numériques font en sorte que les métadonnées sont devenues un outil privilégié d'enquête et de surveillance de masse pour les services de police et les services de

renseignements, ainsi que pour les entreprises commerciales, évidemment, mais ce n'est pas l'objet de cette commission d'enquête.

La collecte et l'analyse des métadonnées par les organismes de police et de renseignements permettent de connecter les points entre les activités de suspects impliqués dans des enquêtes criminelles, permettant de reconstituer et d'extrapoler à partir des schémas de communications les réseaux de collaboration entre ces individus suspects, ou entre des individus ciblés, de localiser certains individus recherchés, et d'après - pour vous donner une idée de cette efficacité accrue - un article publié par le New Yorker récemment expliquait que les métadonnées ont permis au Service des U.S. Marshals, qui est le service américain spécialisé dans les enquêtes pour essayer de localiser les personnes en fuite de la justice, ont permis de réduire le temps moyen de capture d'un fugitif de quarante-deux (42) à deux jours. Sur la base d'une utilisation intensive des métadonnées que nous générons, et que les fugitifs aussi, et les criminels génèrent, et ont bien du mal à se passer de tous ces outils numériques.

Q. **[85]** Si vous me permettez, je veux simplement

revenir. Vous avez mentionné que ça permet de reconstituer et d'extrapoler.

R. Oui.

Q. **[86]** Est-ce que vous êtes en train de nous dire que les métadonnées peuvent servir à prédire, en quelque sorte, l'avenir?

R. Pas vraiment à prédire l'avenir, mais à pouvoir formuler un jugement qui est basé sur des données probantes, sur les caractéristiques de certains individus, sans qu'on puisse savoir, avoir cette... obtenu cette information par d'autres biais. Donc, je vais en parler dans un instant, mais on peut déduire le sexe, la taille du réseau social, l'état d'esprit, le profil psychologique, les revenus, le statut d'emploi d'un individu, à partir de la simple analyse de ses métadonnées. Ses opinions politiques, son état de santé, son statut marital, sa fidélité ou son infidélité, à partir d'une simple analyse de ses métadonnées, oui. Tout à fait.

Donc, il ne s'agit pas de prédire l'avenir, mais il s'agit de prédire des choses, de pouvoir se prononcer avec un degré élevé de fiabilité sur certaines caractéristiques d'individus en ayant accès à des données extrêmement fragmentaires.

Q. **[87]** Je vous laisse aller.

R. Donc certains pays, notamment les États-Unis, le Royaume-Uni, Israël, la Chine, la France, la Suède et évidemment le Canada, ont mis en place, au cours des dernières années, des mécanismes de collecte massive des métadonnées auprès des opérateurs de télécommunications qui opèrent sur leur territoire, et ces pays-là vont stocker - les services de renseignements, notamment, de sécurité nationale de ces pays - vont stocker pendant des mois ou des années entières, dans des bases de données, ces métadonnées, qui vont pouvoir être interrogées a posteriori, selon les besoins des services d'enquête et de renseignements.

Et selon, pour vous donner un exemple un peu de la taille, du volume de ces métadonnées, selon les données qui ont été révélées par Edward Snowden, la NSA, par exemple, en deux mille douze (2012) - et deux mille douze (2012), dans le domaine technologique, c'était il y a une éternité - traitait, en un seul mois, à peu près cinq cents millions (500 M) de métadonnées par mois. Donc on voit que ça génère une quantité phénoménale de ces métadonnées. Mais ça n'a pas commencé avec la NSA.

Bien avant, aux États-Unis, la DEA, la Drug

Enforcement Agency, dès dix-neuf cent quatre-vingt-douze (1992), avait mis en place un programme de collecte systématique et d'analyse des métadonnées associées à plusieurs milliards d'appels téléphoniques qui sont passés chaque année par les résidents américains vers une centaine de pays associés à des opérations de trafic de drogue, et un sous-programme de cette initiative, qui a été baptisé ‘Hemisphere’, et qui utilisait les réseaux téléphoniques de la compagnie AT&T aux États-Unis, recueillait chaque jour vers la fin des années deux mille (2000) quatre milliards (4 G) de métadonnées par jour. Évidemment, cette base de données accumulait de façon quotidienne ces quantités phénoménales de données.

Q. **[88]** Et lorsque vous faites référence à ce qu’AT&T connectait, quatre milliards (4 G) de métadonnées, on fait référence aux métadonnées que vous aviez mentionnées tout à l’heure, la date, l’identifiant de l’appelant, l’identifiant du récepteur...

R. Exactement. Pour chaque appel qui était placé vers l’étranger ou en provenance de l’étranger vers des destinataires américains. Et ces métadonnées ensuite, elles étaient fusionnées avec d’autres données qui étaient issues du renseignement

criminel, qui étaient connectées sur le terrain pour essayer de cartographier les circuits et les réseaux de trafic de drogue et de blanchiment d'argent. Et à l'aide, et vous parliez tout à l'heure de prédiction, mais à l'aide d'algorithmes sophistiqués, parce que vous savez que le crime organisé est tout à fait au courant de ce type de pratique, donc change régulièrement, enfin les membres du crime organisé changent régulièrement de téléphone cellulaire et de numéro de téléphone cellulaire, mais la DEA avait développé un algorithme qui permettait de prédire les nouveaux téléphones cellulaires qui apparaissaient sur les réseaux de télécommunications selon qu'ils avaient de fortes chances d'appartenir à des membres connus du crime organisé en se basant sur les schémas d'appels connus du passé et les schémas d'appels de ces nouveaux téléphones cellulaires, de ces nouveaux numéros de téléphone cellulaire. Ce qui permettait de déjouer les tentatives des membres du crime organisé, d'échapper à la surveillance en se procurant à intervalles réguliers de nouveaux appareils et en ouvrant de nouveaux comptes, donc les algorithmes étaient capables de prédire quels étaient les nouveaux numéros qui apparaissaient sur

le réseau qui étaient fort probablement des numéros appartenant à des membres connus du crime organisé.

Et d'ailleurs, ça été utilisé dans une opération canado-américaine puisqu'en deux mille onze (2011) vingt-huit (28) Hells Angels canadiens ont été arrêtés à Seattle sur la base de données produite par ce programme 'Hemisphere' aux États-Unis. Il a été annulé évidemment en septembre deux mille treize (2013) à la suite des révélations faites par Edward Snowden et de la vigilance accrue envers les programmes gouvernementaux de surveillance de masse.

On sait aussi qu'en Italie, la police italienne utilise un logiciel équivalent qui s'appelle 'Log Analysis' pour analyser ces métadonnées et j'ai utilisé une capture d'écran pour vous permettre de visualiser un petit peu comment sont utilisées les métadonnées par les services de renseignements et d'enquêtes. C'est-à-dire, comme je viens de le dire, ces métadonnées souvent il s'agit de centaines de millions, voire de milliards d'informations, et donc on ne peut pas les traiter de façon manuelle. Et on utilise donc des outils informatiques de visualisation qui vont reconstituer des réseaux d'individus qui sont en

contact les uns avec les autres et qui vont être visualisés de façon différentielle, selon leur importance au sein du réseau, qui vont permettre très rapidement de façon visuelle d'évaluer quels sont les acteurs d'intérêt, quels sont les acteurs qui connectent entre eux des réseaux criminels ou des cellules terroristes et quels sont les individus qui sont dignes d'intérêt et qui méritent que des ressources policières ou de renseignements soient affectées à leur surveillance un petit peu plus approfondie.

Q. **[89]** Lorsqu'on regarde la capture d'écran, est-ce qu'on doit comprendre que, ça s'appelle 'Log Analysis', là, est-ce qu'on doit comprendre qu'un simple relevé... un simple, des données de relevés d'appels, provenant de relevés d'appels, peut générer ce genre de graphique-là, ce genre d'analyse-là?

R. Oui, tout à fait. Ça, c'est l'image qui reflète une analyse provenant certainement de plusieurs milliers d'appels qui ont été amalgamés, agrégés ensemble et dont c'est le résultat visuel, la visualisation. Puis ensuite, on peut manipuler pour essayer d'apprendre plein d'autres choses sur quels sont les acteurs centraux, quels sont les acteurs

qui sont déjà connus, qui peuvent être interrogés de façon automatisée aussi, qui peut générer des scores en termes de quantité d'appels, en termes de diversité des appels qui sont émis. Donc qui connaît le plus de membres dans ce groupe criminel, qui reçoit le plus d'appels, qui en émet le plus, ce qui peut nous renseigner sur l'importance sociale que joue cet individu au sein d'un réseau.

Il est certain que quelqu'un qui envoie plus d'appels qu'il n'en reçoit est certainement quelqu'un qui a un poste de commandement ou de coordination au sein d'un réseau, quelqu'un qui reçoit des appels d'un bien plus grand nombre d'individus ou quelqu'un qui reçoit des appels que d'un nombre très réduit d'individus, va nous renseigner sur le statut et le rôle que cette personne-là va jouer au sein d'un réseau de façon extrêmement intéressante.

Q. **[90]** Et est-ce que je comprends bien lorsque, par exemple, là, on est à la police en Italie, mais par exemple, un service policier pourrait acquérir les données, les placer sur un serveur, utiliser le logiciel et c'est ce que ça donne, on n'a pas besoin d'un traitement informatique ou un traitement humain hors du commun pour générer ce

genre de graphique ou d'analyse-là?

R. Non, ces logiciels-là qui sont vendus par un certain nombre d'entreprises, en fait, tout leur intérêt, c'est justement de pouvoir faciliter le traitement sans grande manipulation, sans avoir recours à un grand nombre d'informaticiens de ces métadonnées dans leur état brut, tel qu'elles sont transmises avec une ordonnance de communication ou avec un mandat par les entreprises de télécommunications.

Des statistiques éparses qui nous proviennent du Royaume-Uni et d'Australie nous indiquent aussi que ces gouvernements-là exigent l'accès aux métadonnées des compagnies locales de télécommunications et aux fournisseurs d'accès internet environ cinq cent mille (500 000) fois par an. En Corée du Sud qui semble être le champion mondial, en deux mille onze (2011), deux mille douze (2012), c'était trente millions (30 M) de requêtes de communication de métadonnées qui ont été enregistrées ces années-là, selon 'ONG Privacy International'.

Donc, on voit qu'il y a vraiment des programmes massifs d'acquisition de métadonnées par des agences gouvernementales destinées vers les

opérateurs de télécommunications et les fournisseurs d'accès internet.

Au Canada, puisque c'est la situation qui nous intéresse, au Québec, peu avant la décision Spencer de la Cour suprême, qui a été formulée en juin deux mille quatorze (2014), des statistiques éparses fournies par les principaux opérateurs de télécommunications indiquaient l'usage intensif que les services de police faisaient des métadonnées puisqu'en deux mille onze (2011), l'Association canadienne des télécommunications sans fil a divulgué que ses membres avaient reçu plus d'un point deux millions (1,2 M) de requêtes de la part des services de police et de renseignements concernant leurs clients et qu'ils avaient fourni des informations sur sept cent quatre-vingt mille (780 000) d'entre eux, pour une seule année.

En deux mille treize (2013) également, l'entreprise Rogers a révélé avoir fait l'objet de cent soixante-quinze mille (175 000) demandes similaires. Et on estime aussi que l'Agence canadienne, évidemment ce sont des exemples épars, donc fragmentaires, mais que l'Agence canadienne des services frontaliers aurait émis près de dix-neuf mille (19 000) demandes par an, dont quatre-

vingt-dix-neuf pour cent (99 %) sans mandat particulier. Évidemment, c'était avant la décision Spencer. Et même si la décision Spencer...

M. ALEXANDRE MATTE, commissaire :

Q. **[91]** Me permettez-vous une question. Quand on parle les nombres aussi importants, est-ce que, mettons que je fais une demande pour un numéro de cellulaire et là, ça me donne l'adresse, ça me donne le nom, ça me donne des correspondants, est-ce que tout ça est regroupé dans le cent soixante-quinze mille (175 000) ou si c'est toutes des données qui vont apparaître différemment dans les résultats.

R. Ça, ça serait un des cent soixante-quinze mille (175 000).

Q. **[92]** C'est un sur cent soixante-quinze mille (175 000)?

R. Oui.

Q. **[93]** Tout l'environnement va rentrer avec, mais ça va être une donnée.

Q. **[94]** Bien, tout l'environnement... toutes les métadonnées concernant un numéro, c'est une unité. Si vous... un numéro et qu'ensuite, vous faites une analyse plus approfondie et que là, vous en sortez vingt (20) qui sont associées à ce numéro-là et que

vous revenez avec vingt (20) requêtes supplémentaires, bien là, vous rajoutez vingt (20) à votre N de cent soixante-quinze mille (175 000), et caetera, et caetera.

Q. **[95]** O.K. Donc, ils sont multiplicateurs?

R. Oui, tout à fait.

Q. **[96]** Merci.

R. Donc, comme le rappelle un groupe de travail qui a été nommé par le président Obama justement après les révélations d'Edward Snowden, qui est le moment charnière à partir duquel on avait commencé à se préoccuper de ce que sont les métadonnées et à quoi elles sont utilisées, les services d'enquête et de renseignements affirment que la collecte et l'analyse des métadonnées ne portent pas atteinte à la vie privée, ou du moins, limitent à la nature intrusive de la surveillance puisque le contenu des communications n'est pas concerné. Donc ça, c'est l'explication classique, c'est–à-dire que les métadonnées, c'est moins intrusif que le contenu des interceptions téléphoniques puisqu'on n'a pas accès au contenu des communications.

Mais de l'aveu même des spécialistes de ce groupe de travail, cette affirmation qui résulte d'une distinction juridique traditionnelle entre le

contenu des communications et les données techniques qui sont produites lors de ces communications est tout à fait discutable, voire trompeuse, et ce n'est pas mon jugement, c'est le jugement de ces experts de la Commission qui a été nommé par le président Obama.

En effet, dans une certaine mesure, les métadonnées peuvent quasiment nous en apprendre plus sur une personne que le contenu de ces communications en donnant accès à une quantité considérable de détails qui sont, en apparence, insignifiants, mais qui, une fois réunis et amalgamés avec d'autres renseignements, nous indiquent quels sont ses déplacements, ses habitudes de vie, ses intérêts ainsi que la nature et la structure de son réseau social par les identifiants de ses contacts ou de ses amis à travers les diverses plates-formes et médias sociaux.

Et d'ailleurs, s'inscrivant en faux contre cette affirmation de l'innocuité des métadonnées, dans un rare aveu de leur importance, l'ancien chef de la CIA et de la NSA a affirmé publiquement en deux mille quatorze (2014) que ces services de renseignements-là tuaient des gens sur la base...

la simple base de métadonnées. Donc des programmes ciblés d'exécution de la NSA et de la CIA, avec les drones et les missiles au Moyen-Orient, calculent des probabilités d'identifier et d'éliminer des cibles sur la simple base d'algorithmes qui utilisent les métadonnées à leur disposition.

LE PRÉSIDENT :

Q. **[97]** Pendant que vous y êtes, Professeur Dupont, vous avez fait référence à l'usage intensif en mentionnant des chiffres qui dataient d'avant Spencer.

R. Oui.

Q. **[98]** Est-ce que depuis Spencer deux mille quatorze (2014), est-ce qu'on a des indications de changements de comportements ou au contraire les mêmes attitudes perdurent après l'arrêt Spencer?

R. Alors, comme vous le savez, comme vous l'avez découvert depuis lundi, on n'a pas de statistiques fiables sur ce type de requête, sur leur volume. Mais les informations anecdotiques provenant des fournisseurs d'accès Internet et des opérateurs de télécommunication nous laissent penser que les volumes resteraient similaires et que les organisations d'application de la loi se sont juste adaptées à ce nouvel environnement. Et dans

certains cas, ils essaient également de faire pression pour faire changer la législation pour réintroduire des mécanismes un petit peu moins contraignants que ceux qui ont été imposés par la décision Spencer. Je ne sais pas si ça répond à votre question ou...

Q. **[99]** Oui, mais quelle est la valeur probante de cette évaluation-là?

R. Aucune. Aucune.

Q. **[100]** Parce qu'on n'a pas de données précises.

R. On n'a pas de données. Et on n'a pas de données précises. C'est extrêmement politiquement délicat aussi pour les opérateurs de télécom de divulguer cette information-là. Parce qu'eux... eux ont cette information étant donné qu'ils l'enregistrent, mais on s'est rendu compte... hier, j'ai suivi les activités de la Commission... le système judiciaire n'a pas de traçabilité de ces demandes-là. On n'a vraiment pas de statistiques fiables dont on pourrait se prévaloir pour apporter un jugement définitif et robuste sur cette question que vous venez de poser.

Q. **[101]** Merci.

R. Malheureusement, je dirais. Donc, venons confirmer un petit peut cette estimation de l'importance des

métadonnées. Le principal conseiller juridique de la NSA, donc le service de renseignements électroniques américains, de façon moins dramatique que l'ancien directeur, mais tout aussi informative, a émis le même type de jugement sur l'utilité des métadonnées quand il a souligné que les métadonnées peuvent tout vous dire sur la vie de quelqu'un et que si vous disposez de suffisamment de métadonnées, et là, je le cite : « Vous n'avez pas réellement besoin de contenu. » Les métadonnées, pour eux, sont devenues bien plus intéressantes et bien plus éclairantes sur la vie de quelqu'un et sur son réseau social, que le contenu de ses communications.

Et donc, maintenant, je vais vous citer quelques exemples de recherches universitaires qui démontrent un petit peu la puissance et le pouvoir de ces métadonnées et la manière dont on peut vraiment rentrer dans la vie privée de quelqu'un à partir de l'analyse de ses métadonnées.

En deux mille treize (2013), des chercheurs du MIT, Massachusetts Institute of Technology à Boston, de l'Université Harvard et de l'École normale supérieure ont publié un article dans lequel ils ont démontré qu'il est possible de

prédire la personnalité ou le profil psychologique d'un usager de téléphone cellulaire à partir des métadonnées produites par son appareil de téléphonie cellulaire, avec des taux de fiabilité supérieurs de quarante-deux (42 %) à soixante et un pour cent (61 %) à des jugements qui seraient émis au hasard. Et on voit là un petit peu le résultat de leurs recherches.

Et donc ils ont été capables d'émettre des scores particulièrement fiables d'identification des facteurs psychologiques tels que l'extraversion ou le névrotisme à partir de la simple analyse des métadonnées de ces usagers-là qui avaient donné leur permission pour qu'on analyse leurs métadonnées, mais sans donner plus de renseignements. Et on a pu prédire, à l'aide d'algorithmes très puissants, est-ce qu'ils étaient plutôt névrosés? Est-ce qu'ils étaient plutôt extravertis? Est-ce qu'ils étaient plutôt consciencieux? Avec des scores de prévision extrêmement élevés.

Me CHARLES LEVASSEUR :

Q. **[102]** Et on s'est servi de quelles données?

R. Alors, pour y parvenir les chercheurs ont utilisé des métadonnées qui mesuraient les schémas

d’utilisation des téléphones, c’est-à-dire le nombre d’appels que vous émettiez chaque jour, le nombre de SMS, vos comportements, les comportements des usagers, c’est-à-dire le nombre d’appels émis, le nombre d’appels reçus, les délais entre la réception d’un SMS et la réponse que vous y apportez, donc selon que vous répondiez plus ou moins rapidement, on peut calculer, on peut prédire votre score de... est-ce que vous êtes moins consciencieux? Est-ce que vous oubliez de répondre ou est-ce que vous répondez dans la minute?

La géolocalisation des appels, est-ce que vous vous déplacez beaucoup? Donc, par exemple, la distance moyenne que vous parcourez dans une journée, qu’on peut calculer avec les métadonnées, sont un très bon élément, l’élément principal pour prédire votre degré de névrose. Donc, plus vous voyagez, selon les métadonnées, plus ces outils algorithmiques peuvent renseigner sur votre degré... sur votre profil psychologique sur cette dimension-là.

Également, la régularité des appels. Est-ce que vous appelez toujours au même moment? Est-ce que vous appelez de façon relativement répartie dans le temps ou tout au long de la journée? Est-ce

que vous avez des plages d'appels privilégiées?

Ça peut nous renseigner également sur la façon dont vous vous concentrez sur votre travail, sur votre réseau, sur votre façon de travailler en interaction avec d'autres, en équipe, ou de façon beaucoup plus solitaire. Sur la diversité d'usages, est-ce que vous êtes... tous les jours vous appelez de la même façon ou est-ce que vous changez de façon quasiment quotidienne, la manière...

Donc, oui, les métadonnées, quand on les regarde au-delà des quelques renseignements, nous permettent d'en apprendre énormément sur la vie quotidienne, les habitudes et les pratiques d'individus.

Trois ans plus tard, en deux mille seize (2016), les chercheurs de l'Université Stanford ont publié les résultats d'une étude qu'ils ont menée sur un échantillon de huit cents (800) participants à partir de métadonnées anonymisées. Donc, des métadonnées pour lesquelles ils ne disposaient que du numéro de téléphone et des éléments de géolocalisation issus de téléphones cellulaires. Et il leur a été possible de réidentifier près du tiers des détenteurs des numéros qui auraient émis ou reçus des appels. À l'aide de métadonnées

anonymisées, ils ont réidentifié la moitié des municipalités de résidences des personnes ciblées. Pas les endroits où ils se trouvaient au moment où ils ont placé les appels, leur lieu de résidence, en recalculant l'intégralité de tous les appels placés et reçus. Le statut marital des personnes ciblées. Ils ont réidentifié les partenaires de vie également, des individus qui n'étaient pas ciblés... de façon primaire par ces métadonnées-là.

Les problèmes de santé de la cible. Bien, ils ont juste réussi à réidentifier les numéros de téléphone de destinataires d'appels et selon que vous appelez un oncologue, un psychologue, un gynécologue, un service de 'planning' familial ou un cardiologue, bien, on en apprend un peu plus sur votre état de santé, évidemment.

La religion des personnes visées. Et, dans les deux derniers cas, on voit que c'est très intrusif sur la vie privée, évidemment.

Et d'autres équipes de chercheurs ont réussi à démontrer, avec des méthodologies relativement semblables, qu'on peut utiliser les métadonnées pour déterminer, avec un très haut degré de précision, le sexe de la personne qui est ciblée, son âge, le type d'emploi qu'elle occupe,

son niveau approximatif de revenu. On peut prédire le niveau de revenu de quelqu'un à partir des métadonnées.

Et, dans le cas des métadonnées liées à l'usage d'Internet et des adresses IP visitées, bien, vous pouvez affirmer avec certitude que vous en apprenez énormément sur les opinions politiques des usagers, sur leur religion, leur statut économique, leurs préférences sexuelles et leur personnalité, leurs problèmes de santé physique ou mentale, l'usage de produits stupéfiants qu'ils peuvent éventuellement faire, leurs infidélités amoureuses et bien d'autres informations qui relèvent de la vie privée des individus.

Et tout ça, encore une fois, sur la base de ces simples métadonnées dont on nous dit qu'elles sont finalement peu intrusives.

Q. **[103]** Justement, et tout ça, avec un numéro de téléphone et de la géolocalisation, c'est tout?

R. Et la durée d'appels et un certain nombre d'autres éléments techniques additionnels, que j'ai présentés antérieurement. Tout à fait. Rien de plus. Donc, évidemment, pour traiter ces données, il existe des logiciels et des outils d'analyse qui sont disponibles sur le commerce. Il existe des

logiciels d'interception, de capture et d'extraction structurée des métadonnées. Donc, des entreprises offrent ce type de solution, qui permettent d'utiliser des milliers de critères pour filtrer, pour extraire les métadonnées pertinentes. Parce qu'évidemment, dans une enquête particulière, on va se noyer sous l'information si on n'a pas des filtres qui vont permettre de trier ces informations-là.

Il existe également... Et donc, ces outils-là et ces logiciels-là souvent sont branchés ou utilisent les données qui sont transmises par les opérateurs de télécom. Mais il existe aussi des technologies d'interception des métadonnées qui peuvent se faire à l'insu des opérateurs de télécom. Et c'est ce qu'on a vu, notamment, ces derniers jours dans La Presse, avec les intercepteurs d'IMSI ou les IMSI Catcher, en bon français, qui sont des technologies qui vont s'interposer entre les appareils téléphoniques cellulaires et les infrastructures des grands opérateurs de télécommunications.

Donc je vous ai mis un petit schéma ici pour vous expliquer un petit peu comment ça fonctionne, ces intercepteurs d'IMSI, parce qu'ils

permettent, justement, de contourner, dans certains cas, les autorisations nécessaires pour essayer d'accéder à ces métadonnées auprès des opérateurs de télécom.

Donc cette technique des intercepteurs d'IMSI, elle consiste à imiter les propriétés techniques des antennes-relais de téléphonie cellulaire à l'aide d'un appareil électronique plus ou moins sophistiqué, et j'ai encore vérifié ce matin, mais sur internet, vous pouvez en acheter un en Chine pour mille cinq cents dollars (1 500 $), donc n'importe qui peut s'en pro... Vous pouvez même le fabriquer, il y a des modes d'emploi pour fabriquer votre propre intercepteur d'IMSI, donc, que vous pouvez également télécharger sur internet.

Ensuite, ces appareils-là, électroniques, vont s'interposer entre les téléphones cellulaires et les antennes-relais, et ils vont donc capter les métadonnées qui sont échangées entre ces appareils, puisque chaque protocole de communication qui est initié est lancé par l'échange d'une certaine quantité de métadonnées pour pouvoir authentifier, par exemple, un appareil, l'associer à un client, et caetera, et caetera.

Et donc, les recherches qui commencent à

apparaître sur ces intercepteurs d'IMSI, et dont on a vu certains résultats depuis lundi sur Radio-Canada, montrent que... et qui sont menées aussi auprès, pas uniquement par les journalistes mais par les fabricants et les opérateurs d'équipement de télécommunication, parce qu'eux aussi sont très préoccupés par le fait qu'ils ne peuvent plus garantir l'intégrité des communications téléphoniques cellulaires à leurs clients.

Q. **[104]** Mais, justement. Est-ce qu'on comprend que la compagnie de téléphonie cellulaire n'a aucune idée que quelqu'un intercepte le signal entre son abonné et sa tour?

R. C'est un petit peu plus compliqué que ça. Elle peut avoir une idée de ce qui se passe, mais elle doit, pour cela, déployer des solutions technologiques, qui sont celles offertes par l'un des experts qui a été interviewé par les journalistes de Radio-Canada, donc une entreprise américaine qui a déployé des capteurs qui sont capables, qui sont installés par les entreprises de télécommunications sur leur réseau, mais donc elles doivent donner leur autorisation, et qui va leur permettre, justement, d'identifier des équipements qui ne sont pas les leurs, ni ceux de leurs compétiteurs, mais

qui, néanmoins, se comportent comme des antennes-relais.

Donc elles ont des moyens de le savoir, mais il faut pour ça qu'elles investissent et puis qu'elles travaillent en collaboration avec d'autres entreprises pour essayer, justement, de comprendre la dynamique de ce nouvel environnement électronique et numérique.

Je ne sais pas si je suis très clair, si je me fais bien comprendre, mais elles auraient le moyen de le faire, mais pour l'instant, elles sont un petit peu comme nous tous : elles commencent à découvrir cette nouvelle réalité. Donc...

Me GUYLAINE BACHAND, commissaire :

Q. **[105]** J'ai une petite question. Est-ce que, à votre connaissance, elles le font de façon, ceux qui le font, de façon proactive, ou en réagissant comme les événements auxquels vous référez à Ottawa, là, récemment, c'est en réaction?

R. Bien, elles sont quand même assez proactives, parce qu'elles sont au courant que ça devient de plus en plus répandu, cette technologie des intercepteurs d'IMSI, et elles essaient de comprendre un petit peu quelle est la gravité du problème. Mais en même temps, elles ne peuvent pas faire grand-chose,

parce qu'elles ne contrôlent pas les lieux, ou les autorités, ou les usagers illicites qui déploient ces technologies-là. Donc elles, elles ne peuvent pas forcer qui que ce soit à retirer ce type d'équipement, si ces équipements sont déployés sur des propriétés privées qui sont à proximité de lieux stratégiques.

Donc, elles sont un petit peu pieds et mains liés, parce qu'elles peuvent identifier qu'il y a un problème sur le réseau, elles ne peuvent pas faire grand-chose d'autre. Malheureusement.

Q. **[106]** Merci.

Me CHARLES LEVASSEUR :

Q. **[107]** Et vous dites que IMSI peut intercepter des métadonnées. Est-ce qu'il peut intercepter aussi des données, par exemple, comme la voix, ou, littéralement, le contenu d'un message?

R. Alors oui, dans certains cas oui, mais là on rentre dans des considérations techniques un petit peu plus compliquées, mais vous savez, il y a plusieurs types de protocoles de communications cellulaires, donc LTE, 3G, 2G, et donc, qui font, chacun d'entre eux, référence à des degrés de cryptage de plus en plus robuste. Et donc, certaines technologies d'intercepteurs d'IMSI peuvent effectivement

intercepter des contenus de conversations téléphoniques. Et pour cela, ce qu'elles font, c'est qu'elles forcent les communications et les appareils de téléphonie cellulaire à basculer sur des réseaux qui sont moins encryptés et moins sécurisés, donc plus faciles à intercepter. Donc elles vont jouer un rôle plus actif, mais évidemment le danger c’est qu’elles vont être plus facilement détectables parce qu’elles vont faire basculer sur des réseaux moins sécurisés de grandes quantités d’appareils téléphoniques et on va avoir des anomalies qui vont se produire sur le réseau et qui vont être plus facilement détectées.

Mais effectivement, elles peuvent intercepter des contenus de communications téléphoniques, elles peuvent intercepter de façon routinière des métadonnées, elles peuvent intercepter les contenus de messages textes, de façon également relativement aisée. Après, tout dépend des montants que vous êtes prêts à investir. Pour mille deux cents dollars (1200 $) vous n’allez pouvoir intercepter le contenu d’une conversation téléphonique, mais il y a des solutions qui coûtent plusieurs centaines de milliers de dollars et avec celles-là, oui, vous allez pouvoir intercepter pas

mal tout ce qui se dit sur les ondes à travers les téléphones cellulaires dans une zone géographique avec un diamètre de cinq cents mètres (500 m) autour de l'appareil.

Q. **[108]** Donc à cinq cents mètres (500 m) autour de l'appareil, je suis capable d'intercepter tous les cellulaires en même temps.

R. Oui. Tout à fait. De traiter ces quantités de signaux de façon automatisée, absolument.

Q. **[109]** Ça va, je vous laisse continuer.

R. Donc, évidemment, alors il y a deux utilisations, il y a l'utilisation légale de ces intercepteurs d'IMSI comme les services de police et de renseignement, s'en servent pour, dans le cadre d'enquêtes contre le crime organisé, contre des groupes terroristes. On s'en sert aussi pour essayer de détecter des téléphones cellulaires qui ont été introduits de façon illégale au sein d'établissements pénitentiaires et dans certains cas on a observé également des utilisations lors de manifestations.

Les services de police s'en étaient servis pour identifier des personnes qui étaient connues de leurs services et qui manifestaient sur la voie publique. Donc on interceptait toutes les

métadonnées de tous les gens qui avaient manifesté pour une certaine cause et on traitait ensuite ces informations-là pour essayer de faire apparaître les numéros de téléphone cellulaire d'opposants qui étaient connus, qui étaient considérés comme des personnes d'intérêt.

Et donc, évidemment, ensuite une utilisation illégale de ces intercepteurs d'IMSI puisque n'importe qui peut s'en procurer, que certains services de renseignements étrangers les déploient sur le territoire canadien et on peut imaginer que les services de renseignements canadiens les déploient en territoire étranger. Donc ça, ça fait partie d'activités d'espionnage et de contre-espionnages qui ne sont par régies par le droit et qui se soustraient un petit peu à ces considérations-là.

Ces techniques, évidemment, sont extrêmement intrusives puisqu'elles aspirent l'ensemble des métadonnées générées par des équipements mobiles dans une zone géographique déterminée, même si vous n'êtes pas la cible primaire qu'on cherche à surveiller. Donc, par exemple, si on reprend le reportage de Radio-Canada sur la situation à Ottawa, ce ne sont pas

uniquement les diplomates et les politiciens et les hautes personnalités canadiennes dont les métadonnées sont capturées par ces intercepteurs d'IMSI, c'est tous les gens qui se baladent à proximité de la colline du Parlement dont les métadonnées sont capturées et ensuite peuvent être éventuellement analysées ultérieurement.

Donc ça, ce sont pour les intercepteurs d'IMSI et il existe une troisième catégorie de produits, de logiciels, parce qu'évidemment, encore une fois j'y reviens, le problème c'est le volume et la quantité des données. Donc humainement, on ne peut pas les traiter de façon traditionnelle, donc on doit utiliser des logiciels de visualisation, de traitement automatisé à très grande échelle et donc on peut en acheter sur le commerce. Les services de police et de renseignement en ont.

Ça c'est une capture d'écran de la solution qui est fournie par IBM et en fait vous voyez que ces outils-là, ils cherchent à attirer l'attention des enquêteurs sur les individus ou les appareils qui semblent être les plus importants dans un réseau. Donc selon le nombre d'appels ces logiciels de visualisation vont grossir la taille qui va représenter les personnes suspectes ou les numéros

de téléphone suspects pour qu'ensuite à l'aide d'interfaces graphiques on puisse plus facilement approfondir un petit peu le type d'appels, le nombre d'appels, les destinataires de ces appels sans avoir à passer à travers des centaines ou des milliers de pages de transactions téléphoniques ou d'appels qui ont été échangés.

Il y a d'autres solutions d'entreprises comme Palantir, IBM, une autre entreprise qui s'appelle Xanalys qui offrent ce type de logiciels et qu'on retrouve un petit peu dans tous les salons policiers, les salons de renseignement dans lesquelles des entreprises offrent ce type de services et de produits.

Donc, évidemment il y a quand même un certain nombre de risques et de limites qui sont associés à l'utilisation de ces métadonnées à des fins d'enquête et de renseignements. Moi j'en ai identifié principalement trois. Le premier risque, c'est celui de la culpabilité par association. C'est-à-dire que ces métadonnées vont permettre de récréer de manière quasiment automatisée le réseau de communications d'une personne suspecte afin d'identifier, dans son entourage, des complices, des lanceurs d'alertes ou d'autres personnes dignes

d’intérêt pour les autorités.

Dans le cas des services de renseignements américains, on sait que la NSA peut effectuer des recherches en allant jusqu’à trois degrés de séparation. C’est-à-dire qu’une fois que vous avez une cible, vous pouvez, dans les bases de données des métadonnées de la NSA, aller faire des recherches approfondies jusqu’aux amis des amis des amis de la personne que vous ciblez. D’accord? Donc, si vous utilisez... je ne sais pas qui a utilisé tout à l’heure le terme de ‘coefficient multiplicateur’, peut-être vous, Monsieur le Président?

LE PRÉSIDENT :

Q. **[110]** C’est mon collègue.

R. Votre collègue?

Q. **[111]** Mon collègue, M. Matte.

R. Alors, si vous prenez pour acquis que vous avez... Si vous prenez pour acquis qu’en moyenne, un Nord-Américain a neuf amis, et je ne parle pas des amis Facebook, je parle des vrais amis, bien, les amis des amis des amis d’une personne cible, c’est près de huit cents (800) personnes. Donc, on s’entend qu’une infime minorité va avoir quelque chose à se reprocher parce qu’on est dans un réseau qui s’est

énormément étendu et dans lesquels la majorité des gens n'ont aucune activité illicite, ou n'ont même connaissance des activités illicites de leur contact.

Et donc, ce qui se passe, c'est qu'on instaure un régime de suspicion automatisé qui, à mon avis, me semble un petit peu corrosif parce qu'il est secret, c'est-à-dire que les personnes qui sont concernées par l'analyse de ces métadonnées ne sont jamais averties qu'elles ont été prises dans ce filet d'enquête ou dans ce filet d'analyse de renseignements et quel usage a été fait de leurs métadonnées. Donc ça, pour moi, c'est un petit peu le premier risque. C'est ce risque de culpabilité par association. C'est parce qu'on peut le faire, parce qu'on peut automatiser le traitement de millions ou de milliards de métadonnées, on va considérer qu'on doit examiner les profils d'usage d'internet et de télécommunications de centaines de personnes qui n'ont absolument rien à se reprocher. Parce qu'on peut le faire de façon automatisée à coûts quasiment nuls. Pour moi, c'est le premier risque.

Le deuxième risque, c'est celui de la fiabilité discutable des données, car de l'aveu

même des usagers, du monde du renseignement et du monde policier qui se frottent quotidiennement à ces métadonnées, bien sûr, c'est l'origine technique de ces métadonnées, les liens qu'elles permettent d'établir sont extrêmement utiles, mais elles demeurent d'une fiabilité incertaine tant qu'elles n'ont pas été regroupées et recoupées avec d'autres sources de renseignements. Parce qu'en effet, les comptes téléphoniques peuvent être enregistrés au nom de membres de la famille, au nom d'amis. Des appareils de téléphones cellulaires peuvent être échangés, peuvent être prêtés. Des informations commerciales en possession des compagnies de télécoms peuvent être mal retranscrites. Donc, il y a tout un tas de très bonnes raisons qui font en sorte que ces métadonnées doivent toujours être utilisées avec beaucoup de précautions. Et on a qu'à voir le nombre de révélations concernant les victimes innocentes de frappes ciblées des drones américains au Moyen-Orient pour comprendre qu'il y a beaucoup d'erreurs potentielles et qui peuvent être commises en termes d'analyse et d'inductions qui sont faites à partir de ces métadonnées.

Donc, on doit également ne pas céder aux

sirènes de cette automatisation à très grande échelle et se rappeler que ces métadonnées, elles sont parfois d'une fiabilité qui est douteuse. Ce n'est pas parce qu'elles sont automatisées, parce qu'elles sont produites par les machines et sont cent pour cent (100 %) fiables.

Le troisième risque ou la troisième limite, c'est la quantité des données à traiter, la quantité des données recueillie qui est telle qu'elle peut nuire à leur exploitation parce que les analystes doivent filtrer et interpréter des quantités faramineuses de données. Et même s'ils sont aidés par des algorithmes, il n'en reste pas moins qu'on observe quand même très souvent une dilution des ressources avec des résultats qui s'avèrent très souvent assez décevants. Et à la suite des révélations d'Edward Snowden, le FBI a mené une évaluation de l'utilité de ces métadonnées qui avaient été récoltées avant Snowden et selon eux, entre deux mille un (2001) et deux mille quatre (2004), ils sont revenus un petit peu à l'utilisation qui a été faite des métadonnées par la NSA, la CIA et eux-mêmes et se sont rendu compte que seulement un point deux pour cent (1,2 %) des indices générés par leurs analyses avait produit

des résultats prometteurs. Donc oui, ils avaient beaucoup de métadonnées, oui, ils avaient des manières automatisées de les traiter, mais ce que ça leur avait procuré en termes d'indices concrets et de pistes d'enquête était insignifiant.

Donc, là, également, il y a une autre, je pense, une autre avenue de réflexion importante. Alors, est-ce qu'on peut empêcher ou limiter la collecte des métadonnées? Il existe un certain nombre de solutions technologiques qui sont disponibles aux individus et aux organisations. J'aimerais parler d'abord du réseau TOR, qui est un réseau d'anonymisation des connexions sur Internet qui va vous permettre de surfer, de naviguer de manière plus confidentielle.

Je vais peut-être passer les considérations techniques, mais en gros, c'est un réseau crypté qui est plaqué sur le réseau Internet. Donc, vous installez sur votre machine un logiciel de cryptage et à chaque fois que vous allez naviguer en utilisant ce logiciel-là, vos communications vont être encryptées, elles vont être renvoyées vers tout un tas d'autres serveurs qui appartiennent à ce réseau, qui vont les faire rebondir d'un serveur à un autre, un peu comme quand vous blanchissez de

l'argent. Et ensuite, votre requête va sortir du réseau à un autre point que le point d'entrée vers sa destination finale, et donc il sera beaucoup plus difficile de retracer les métadonnées parce qu'elles auront été offusquées, elles auront été anonymisées, elles auront été encryptées. Et donc ce sera beaucoup plus compliqué à la fois pour les services de police et de renseignements et aussi pour les fournisseurs d'accès Internet, de savoir par exemple, si vous êtes l'un de leurs clients, quels sont les sites que vous avez fréquentés. Parce qu'entre votre machine et le réseau TOR, les communications sont encryptées, donc votre fournisseur d'accès Internet saura que vous avez communiqué avec le réseau TOR, mais il ne saura pas pour quelle destination ultime sur Internet vous avez eu recours à cette technologie-là.

Donc ça, c'est une technologie, d'ailleurs qui a été développée avec le soutien financier de l'armée américaine. Donc, c'est utilisé aussi par les services de renseignements pour eux-mêmes échapper à la surveillance de leurs adversaires étrangers.

Donc, dans le cas de cette technologie, ça permet de masquer les adresses IP. Évidemment, elle

a des points faibles. Il a été démontré ces dernières années que certains services de police et d'enquête avaient réussi à contourner un certain nombre des fonctions d'anonymisation du réseau TOR. Donc, c'est pas du tout une solution parfaite et il y a des moyens techniques justement d'accéder aux métadonnées de leurs usagers.

On peut aussi souscrire sur Internet à des services de proxy ou de VPN qui vont avoir les mêmes fonctions, c'est-à-dire qui vont rajouter un ou plusieurs intermédiaires entre vous et les sites Internet que vous souhaitez consulter en tout anonymat et en toute confidentialité.

Mais évidemment, si ces services VPN, donc réseau privé virtuel sont hébergés dans la même juridiction que celle d'un service d'enquête qui est intéressé par vos activités en ligne, eh bien, ce service d'enquête pourra demander et s'il l'obtient, obtenir la communication des données avec un mandat d'un juge ou avec une ordonnance de communication.

Donc, vous pouvez utiliser cette technologie-là, mais si vous le faites, évidemment, vous devez savoir où sont hébergés les serveurs de ces entreprises si vous voulez réellement échapper

à la surveillance policière. Et je parle de la surveillance légale évidemment, avec les mandats et avec tout cet appareillage juridique-là.

Donc ça, c'est pour Internet, mais évidemment pour la téléphonie cellulaire, le fait que nous ayons pour chaque appareil un IMEI et un IMSI uniques fait en sorte que ne pouvez pas réellement anonymiser vos communications par téléphonie cellulaire avec le même type de technologie. Donc, le seul moyen d'échapper en toute surveillance et à toute capacité d'analyse de vos métadonnées, c'est que pour chaque nouvel appel, vous ayez un appareil de téléphone cellulaire nouveau que vous utilisez, avec un nouveau numéro de téléphone, un nouveau compte auprès d'un opérateur de télécommunication et qu'à chaque fois vous passiez votre appel d'un lieu différent, sans jamais revenir sur un lieu duquel vous avez déjà passé un appel, ce qui est virtuellement impossible.

Donc, pour échapper à la surveillance de vos métadonnées quand vous utilisez un téléphone cellulaire, le meilleur moyen c'est de le laisser à la maison ou de ne pas vous en servir. Et encore même si vous ne vous en servez pas et que vous

l'éteignez vous êtes exposé à l'analyse de vos métadonnées. Il y a un certain nombre de techniques, là, je ne veux pas rentrer dans les détails, mais même de l'éteindre ne suffit pas. On peut le réactiver de façon silencieuse pour continuer à vous surveiller même quand vous l'avez vous-même manuellement éteint, votre téléphone cellulaire.

Alors, ce que j'ai essayé d'indiquer... Ah, oui, évidemment... Avant d'aller plus loin, évidemment, le fait de ne pas... d'essayer d'échapper à l'analyse de vos métadonnées ne va pas vous protéger. Parce qu'évidemment, ça crée un profil atypique de quelqu'un qui essaie de se soustraire à la surveillance, donc ça va probablement encore plus attirer l'attention sur vous, alors que vous cherchez justement à échapper à cette attention-là. Parce que ces capacités d'analyse automatisée sont capables aussi de détecter des gens qui ont très peu d'activités, ou qui ont des activités extrêmement éparses, et donc qui ne correspondent pas à un profil moyen, à un profil typique d'utilisateur d'internet ou de téléphone cellulaire. Donc, là, aussi, vous attirez l'attention sur vous et sur la surveillance.

Alors, comme je l'ai indiqué, ces métadonnées-là peuvent... posent des problèmes assez importants de protection de la vie privée. Elles méritent, à mon avis, un débat public approfondi et éclairé. D'autant plus qu'elles ont aussi une autre utilisation qui est bénéfique. Donc, il ne faut pas uniquement voir les métadonnées comme une source d'oppression et de surveillance de masse. Elles peuvent aussi nous en apprendre énormément sur les habitudes des gens dans des grandes agglomérations urbaines, sur les flux de trafic, donc elles peuvent également avoir une contribution très positive aux politiques publiques, à l'amélioration de la santé des gens, à l'amélioration de la consommation d'énergie. Dans les pays en voie de développement, on s'en sert pour mieux comprendre les schémas de transport urbain, pour savoir où sont les plus grands besoins, comment y répondre. Donc les métadonnées, en fait, sont le reflet de nos activités humaines. Elles ne sont pas uniquement un outil de surveillance de masse, elles ont également tout un tas d'autres utilités qui sont bénéfiques. Donc, je ne voudrais pas non plus vous laisser sur l'impression un peu paranoïaque que les métadonnées

sont le diable incarné et qu'on doit absolument s'en débarrasser, elles ont également des utilisations tout à fait bénéfiques, mais on a encore du mal, dans notre société, à bien comprendre les tenants et les aboutissants de ce qu'elles nous permettent d'apprendre sur la vie privée des individus et sur nos habitudes de société.

Et en conclusion, j'aimerais également attirer l'attention de la Commission sur le fait que même si on pense que l'affaire qui nous concerne est relativement exceptionnelle et unique, c'est-à-dire la surveillance de certains journalistes québécois qui a conduit à la création de cette commission d'enquête, d'autres pays ont déjà été confrontés à cette problématique.

Notamment, en Australie, en deux mille seize (2016), on a appris que la police fédérale avait mené un certain nombre d'enquêtes afin d'identifier les sources de journalistes qui avaient informé ces derniers sur le traitement des demandeurs de statut de réfugié dans le pays, et que donc la police fédérale australienne avait utilisé les métadonnées, la surveillance de ces journalistes à travers les métadonnées qu'ils

produisaient, pour essayer de contourner leur droit de protéger l'anonymat de leurs sources, qui était garanti par le code d'éthique des journalistes australiens.

Donc, concrètement, ce que ça veut dire, c'est que la police australienne a dit : « Effectivement, on reconnaît que vous avez un code d'éthique, vous avez le droit de refuser de nous livrer le nom de vos sources, mais de toute façon, ce n'est plus très important parce qu'aujourd'hui, avec les métadonnées, on n'a plus besoin de vous poser ce genre de question, on peut très bien identifier vos sources. » Tant et si bien que certains journalistes d'investigation de grands médias australiens maintenant laissent leur téléphone intelligent ou téléphone cellulaire au bureau quand ils vont rencontrer des sources confidentielles à l'extérieur, et sont revenus un petit peu à des techniques dignes du Watergate où on va rencontrer les sources dans des endroits un petit peu obscurs.

Mais ce que ça pose surtout comme constat, c'est que maintenant les journalistes australiens, de leur propre aveu, ne se sentent même plus autorisés à pouvoir promettre avec certitude la

confidentialité totale à leurs sources. Ils disent : « Désolé, on va faire ce qu'on peut, mais tant qu'à vous promettre, maintenant, la confidentialité totale, on ne pense plus que techniquement, on est en mesure de pouvoir vous garantir cela. » Ne serait-ce que parce que même si on déploie tout un tas de solutions techniques de communications, le premier contact, il y a toujours un premier contact, celui-là il est extrêmement exposé à une analyse rétroactive qui peut être conduite de façon relativement, je ne dirais pas facile, mais aisée, avec des outils automatisés, dont je viens de vous en présenter certains.

Et donc, ça c'est la question qui se pose : est-il encore possible aujourd'hui, techniquement, pour des journalistes, de pouvoir garantir à leurs sources la confidentialité à laquelle ces dernières sont en droit de s'attendre? Pour les journalistes australiens, c'est devenu quelque chose de quasiment impossible à promettre.

Donc, je vous remercie pour votre attention.

LE PRÉSIDENT :

Q. **[112]** Merci beaucoup, Professeur Dupont.

Me CHARLES LEVASSEUR :

Je n'aurai pas d'autres questions.

LE PRÉSIDENT :

Vous n'avez pas d'autres questions?

Me CHARLES LEVASSEUR :

Non.

LE PRÉSIDENT :

Q. **[113]** Alors, nous allons prendre une pause d'une quinzaine de minutes, et après ça, j'offrirai aux avocats qui sont dans la salle de vous questionner, s'ils ont des questions à vous poser.

R. Parfait.

Q. **[114]** Merci. Quinze (15) minutes.

SUSPENSION DE L'AUDIENCE

REPRISE DE L'AUDIENCE

_____

Me CHARLES LEVASSEUR :

Alors, Monsieur le Président, avant de conclure officiellement, j'aimerais simplement annoncer le dépôt du texte du professeur Dupont. Le texte sera révisé en fonction de la présentation que le professeur Dupont vient de nous donner. Ce que je vous suggérerais ce serait de réserver la cote 9, le texte sera déposé à l'attention de la Commission sous peu. Le professeur Dupont veut le réviser en

fonction des propos qui ont été tenus ici.

LE PRÉSIDENT :

Très bien. Alors, on peut peut-être faire 9E en attendant et, quand on le recevra, on le transformera en 9P pour qu'il soit officiellement public, si on veut.

Me CHARLES LEVASSEUR :

Voilà.

LE PRÉSIDENT :

Ça va?

Me CHARLES LEVASSEUR :

Oui.

LA GREFFIÈRE :

Métadonnées, adresses IP et surveillance policière.

Me CHARLES LEVASSEUR :

Oui.

LA GREFFIÈRE :

Merci.

9E : Texte sur les métadonnées, adresses IP et surveillance policière

LE PRÉSIDENT :

Alors, maintenant je vais demander... inviter les avocats qui le veulent à poser des questions au

professeur Dupont. En commençant par Paul Crépeau pour la Cour du Québec, qui n'est pas ici. Après ça, Maître Soulière.

CONTRE-INTERROGÉ PAR Me GÉRALD SOULIÈRE :

Q. **[115]** Bonjour, professeur Dupont. Gérald Soulière pour la Fraternité des policiers et policières de Montréal. En fait, j'ai trois questions.

La première, quand on parle d'une ligne dure ou une ligne terrestre, est-ce que ça a encore un sens, c'est-à-dire est-ce que deux personnes qui se parlent sur une ligne type dur ne sont pas à risque d'être interceptées?

R. Ça dépend quel sens...

Q. **[116]** Mise à part une autorisation judiciaire, là.

R. Oui, oui. Ça dépend quel sens vous assigné à dure; est-ce que ça veut dire cryptée ou non cryptée? Parce que dans le monde du renseignement, par exemple, une ligne dure c'est une ligne qui est cryptée. Alors, vous pouvez avoir une ligne terrestre non cryptée, une ligne terrestre cryptée, qui est beaucoup plus sécurisée, évidemment, encore mais qui nécessite un équipement particulier.

Q. **[117]** Dans ma tête c'est la ligne...

R. Ligne terrestre ordinaire...

Q. **[118]** C'est ça, résidentielle normale, disons.

R. Résidentielle normale, oui.

Q. **[119]** Est-ce qu'on peut prendre pour acquis que deux personnes qui communiqueraient par ce type de ligne téléphonique ne pourraient pas être interceptées, mis à part avec une autorisation judiciaire qui permet d'intercepter, au niveau du fournisseur, là?

R. Disons que ça serait plus difficile. Ce n'est pas impossible mais ça ne serait pas avec les technologies que j'ai présentées aujourd'hui. Il y a toujours une possibilité mais ça nécessiterait une plus grande proximité physique.

Q. **[120]** Est-ce que c'est une croyance urbaine ou il y a, effectivement, des mots qui, lorsqu'ils circulent sur les réseaux, sont nécessairement... j'allais dire, « interceptés », probablement que le terme n'est pas le bon, mais ils vont lever une espèce de drapeau ou de « warning » qui va attirer l'attention? On pourrait dire des mots comme « drogue » ou je ne sais pas, quoi que ce soit qui aurait rapport avec le terrorisme, par exemple, est-ce que c'est une croyance urbaine, ça?

R. Disons que... je n'ai pas le code de sécurité, donc je ne peux pas me prononcer sur la façon dont travaillent certains services de renseignement et

leur programme de surveillance. Mais il est certain qu'un certain nombre de forums, de sites Internet, dans lesquels il y a beaucoup d'interaction entre des gens qui partagent une certaine idéologie, sont surveillés. Et qu'effectivement, on ne peut pas les surveiller de façon individuelle, donc il y a des outils automatisés qui sont alertés à chaque fois que certains mots particuliers sont utilisés ou certains profils particuliers échangent des informations sur ces réseaux-là.

Alors, je suis conscient que je ne réponds pas tout à fait à votre question mais il faut comprendre qu'Internet, c'est un empilage de plusieurs réseaux, de plusieurs technologies. Alors, votre question, elle porte sur la globalité, là où les programmes de surveillance, en fait, doivent s'adapter à des différences pour chacune des technologies et chacun des modes de communication en ligne et sur Internet.

Donc, oui, il existe, sur certains de ces protocoles, certains de ces réseaux, des mécanismes de surveillance automatisés qui, pour certains d'entre eux, utilisent des mots-clés, mais pas uniquement des mots-clés, c'est-à-dire ces mots-clés revenant à une certaine fréquence, sur

certains types de forum, donc il y a quand même des analyses, des filtrages qui sont effectués, mais il y a effectivement une surveillance automatisée d'un certain nombre de forum et de contenus en ligne, échangés en ligne, oui.

Q. **[121]** O.K. Donc, on peut comprendre de votre réponse que c'est possible. Maintenant jusqu'à quel point c'est fait?

R. Bien, plus que possible parce que...

Q. **[122]** C'est fait.

R. C'est la même technologie qui fait en sorte que si vous utilisez une adresse de courrier électronique gratuite, vous voyez par hasard apparaître des publicités pour certains types de produits qui suivent immédiatement des discussions que vous avez eues avec vos interlocuteurs. Pourquoi? Bien, parce que les entreprises qui fournissent ces services en ligne gratuits ont analysé le contenu de vos conversations à l'aide des mots-clés et vous offre des publicités qu'ils semblent penser être, pour lesquelles vous allez être beaucoup plus réceptifs. Donc, l'analyse par mots-clés des contenus en ligne...

Q. **[123]** Clientèle cible.

R. Ce n'est pas hypothétique, c'est quelque chose qui

fonctionne au quotidien.

Q. **[124]** Vous avez parlé tantôt du risque ou ce que j'ai cru comprendre, en fait bref, d'interception... Je reprends.

Vous nous avez dit que lorsque l'appareil portable cellulaire est inactif, donc par exemple, je le laisse à côté de moi, il peut quand même générer des métadonnées.

R. Oui.

Q. **[125]** C'est exact.

R. Oui.

Q. **[126]** Est-ce qu'il peut servir à une interception de la conversation que les gens ont alors que l'appareil est à côté d'eux? Et si oui, est-ce que ça se fait selon vous?

R. Oui. Ça peut servir. Eh oui, ça se fait.

Q. **[127]** Oui, ça se fait. Donc, même si l'appareil est inactif.

R. Ou même éteint.

Q. **[128]** Même éteint. Je vous remercie. Je n'ai pas d'autres questions.

LE PRÉSIDENT :

Merci beaucoup. Maître Doray?

Me RAYMOND DORAY :

Je n'ai pas de questions, je vous remercie.

LE PRÉSIDENT :

Catherine Dumais n'est pas ici. Maître Boucher?

Me BENOÎT BOUCHER :

Pas de questions, merci.

LE PRÉSIDENT :

Maître Leblanc?

Me CHRISTIAN LEBLANC :

Je n'ai pas de questions, merci.

LE PRÉSIDENT :

Maître Carlesso?

Me JULIE CARLESSO :

Je n'ai pas de questions, mais ce n'est pas par manque d'intérêt, c'était une présentation, un cours parfait sur les métadonnées.

LE PRÉSIDENT :

Vous avez bien raison. Maître Corbo?

Me MATHIEU CORBO :

Pas de questions.

LE PRÉSIDENT :

Très bien. Alors, est-ce que vous avez une...

Me ALEXANDRE MATTE :

Petite question pour moi, Monsieur le Professeur. Dans vos groupes de recherche ou de réflexion, est-ce qu'il y a des policiers?

R. Oui. Tout à fait. Des policiers québécois,

ontariens, fédéraux aussi.

LE PRÉSIDENT :

Q. **[129]** O.K. Ça, ça comprend même dans le réseau dont vous êtes le grand capitaine?

R. Tout à fait. Oui, tout à fait, oui. Tout à fait.

Q. **[130]** Ah! Bon.

R. La Sûreté du Québec, la police provinciale de l'Ontario, la GRC font partie de ce réseau-là.

Q. **[131]** Très bien. Bien, alors écoutez, il me reste, au nom de mes deux collègues et moi-même et en fait, de tous les gens qui nous ont écoutés aujourd'hui de vous remercier. C'était extrêmement bien documenté, bien présenté et juste assez terrifiant pour nous faire réfléchir tout le monde. Alors, merci beaucoup, Professeur Dupont.

R. Merci pour l'invitation.

LE PRÉSIDENT :

Alors, ça complète le programme pour aujourd'hui, Maître Joncas, Maître Levasseur?

Me LUCIE JONCAS :

Oui, effectivement.

LE PRÉSIDENT :

Bon. Alors demain matin, neuf heures trente (9 h 30).

Me LUCIE JONCAS :

Merci.

LE PRÉSIDENT :

Merci beaucoup.

AJOURNEMENT DE L'AUDIENCE

_____

CAUSE CONTINUÉE AU 6 AVRIL 2017, 9 h 30

_____

SERMENT D’OFFICE

Je, soussigné, **NICOLAS PROVENCHER**, sténographe officiel, certifie sous mon serment d'office que les pages qui précèdent sont et contiennent la transcription fidèle et exacte des témoignages et plaidoiries en l’instance, le tout pris au moyen de la sténotypie, et ce, conformément à la Loi.

Et j'ai signé,

_____

NICOLAS PROVENCHER