



**COUR SUPRÊME DU CANADA**

**RÉFÉRENCE : R. c. Mills, 2019 CSC 22**

**APPEL ENTENDU : 25 mai 2018**  
**JUGEMENT RENDU : 18 avril 2019**  
**DOSSIER : 37518**

**ENTRE :**

**Sean Patrick Mills**  
Appelant

et

**Sa Majesté la Reine**  
Intimée

- et -

**Directrice des poursuites pénales, procureure générale de l'Ontario, directeur des poursuites criminelles et pénales, procureur général de la Colombie-Britannique, procureur général de l'Alberta, Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko, Association canadienne des libertés civiles, Criminal Lawyers' Association et Association canadienne des chefs de police**  
Intervenants

**TRADUCTION FRANÇAISE OFFICIELLE**

**CORAM :** Le juge en chef Wagner et les juges Abella, Moldaver, Karakatsanis, Gascon, Brown et Martin

**MOTIFS DE JUGEMENT :** Le juge Brown (avec l'accord des juges Abella et Gascon)  
(par. 1 à 35)

**MOTIFS CONCORDANTS :** La juge Karakatsanis (avec l'accord du juge en chef Wagner)  
(par. 36 à 65)

**MOTIFS CONCORDANTS :** Le juge Moldaver  
(par. 66 à 67)

**MOTIFS CONCORDANTS :** La juge Martin  
(par. 68 à 159)

**NOTE :** Ce document fera l'objet de retouches de forme avant la parution de sa version définitive dans le *Recueil des arrêts de la Cour suprême du Canada*.

---

R. c. MILLS

**Sean Patrick Mills**

*Appelant*

*c.*

**Sa Majesté la Reine**

*Intimée*

et

**Directrice des poursuites pénales,  
procureure générale de l'Ontario,  
directeur des poursuites criminelles et pénales,  
procureur général de la Colombie-Britannique,  
procureur général de l'Alberta,  
Clinique d'intérêt public et de politique d'internet du Canada Samuelson-  
Glushko,  
Association canadienne des libertés civiles,  
Criminal Lawyers' Association et  
Association canadienne des chefs de police**

*Intervenants*

**Répertorié : R. c. Mills**

**2019 CSC 22**

N° du greffe : 37518.

2018 : 25 mai; 2019 : 18 avril.

Présents : Le juge en chef Wagner et les juges Abella, Moldaver, Karakatsanis, Gascon, Brown et Martin.

EN APPEL DE LA COUR D'APPEL DE TERRE-NEUVE-ET-LABRADOR

*Droit constitutionnel — Charte des droits — Fouilles, perquisitions et saisies — Leurre — Opération d'infiltration policière — Interception avec consentement — Accusé inculpé de leurre après avoir eu des communications en ligne avec un policier se faisant passer pour une adolescente de 14 ans — Utilisation par la police d'un logiciel de capture d'écran en vue de créer un relevé de ces communications — La technique d'enquête équivalait-elle à une fouille ou à une saisie des communications en ligne de l'accusé? — La police a-t-elle intercepté une communication privée sans autorisation judiciaire préalable? — Charte canadienne des droits et libertés, art. 8 — Code criminel, L.R.C. 1985, c. C-46, art. 184.2.*

Un policier s'est fait passer en ligne pour une adolescente de 14 ans appelée Leann, avec l'intention d'attraper des cyberprédateurs. Utilisant Facebook et Hotmail, M a envoyé à Leann des messages sexuellement explicites et a organisé une rencontre dans un parc, où il a été arrêté et inculpé de leurre. Le policier en question a, sans avoir obtenu d'autorisation judiciaire préalable, utilisé un logiciel de capture d'écran pour créer un relevé de ses communications en ligne avec M, relevé qui constituerait une preuve pour le procès. M a demandé l'exclusion de la preuve. Le juge du procès a conclu que les messages étaient des « communications privées » au sens de l'art. 183 du *Code criminel*, de sorte qu'à partir du moment où les policiers

déterminaient que M avait un intérêt potentiellement inapproprié à l'égard d'un mineur, une autorisation judiciaire préalable en application de l'art. 184.2 du *Code criminel* était nécessaire pour prendre des captures d'écran des messages. Il a aussi conclu que l'utilisation d'un logiciel de capture d'écran avait entraîné une saisie et que M avait une attente au respect de sa vie privée dans ses communications. Il a donc statué que la police avait violé l'art. 8 de la *Charte*. Il a toutefois estimé que l'utilisation de la preuve n'était pas susceptible de déconsidérer l'administration de la justice et a déclaré M coupable. La Cour d'appel a statué pour sa part que le juge du procès avait commis une erreur en concluant que des autorisations obtenues conformément à l'art. 184.2 étaient requises, et elle a affirmé que l'attente de M au respect de sa vie privée n'était pas objectivement raisonnable. Elle a jugé qu'il n'avait pas été porté atteinte aux droits que lui garantit l'art. 8 et a donc confirmé la déclaration de culpabilité.

*Arrêt* : Le pourvoi est rejeté.

*Les juges Abella, Gascon et Brown* : L'article 8 de la *Charte* n'entrait pas en jeu lorsque le policier a pris des captures d'écran des communications électroniques de M. Pour se réclamer de la protection de cette disposition, l'accusé doit démontrer qu'il pouvait subjectivement, et de façon objectivement raisonnable, s'attendre au respect de sa vie privée à l'égard de l'objet de la prétendue fouille. M ne pouvait pas prétendre qu'il avait une attente au respect de sa vie privée qui était objectivement raisonnable parce que, d'une part, il s'entretenait avec une personne

qu'il croyait être une enfant, et qui était une inconnue pour lui, et, d'autre part, l'agent d'infiltration savait — en raison de la technique d'enquête utilisée — qu'un tel entretien aurait lieu au moment où il a créé cette personne. Eu égard aux faits de l'espèce, et si l'attente en matière de vie privée doit refléter un critère normatif plutôt que descriptif, la sanction judiciaire de la forme particulière de surveillance non autorisée en cause n'empiéterait pas sur l'intimité dont disposent encore les particuliers dans une mesure incompatible avec les objectifs d'une société libre et ouverte. En conséquence, l'opération d'infiltration ne nécessitait pas d'autorisation judiciaire préalable.

Le caractère objectivement raisonnable est apprécié au regard de l'ensemble des circonstances et de quatre considérations. Les trois premières considérations applicables sont l'examen de l'objet de la prétendue fouille, la question de savoir si le demandeur possédait un droit direct à l'égard de l'objet et la question de savoir si le demandeur avait une attente subjective au respect de sa vie privée relativement à l'objet. Ces considérations militent en faveur de l'allégation de M selon laquelle il pouvait s'attendre au respect de sa vie privée. La prétendue fouille vise les communications électroniques, et il n'y a aucune distinction importante sur le plan juridique entre celles-ci et des messages textes. M voulait avoir une conversation seul à seul en ligne. En tant que personne ayant participé aux communications, et à titre de coauteur de celles-ci, M possédait un droit direct à l'égard de l'objet et il s'attendait à ce que les échanges en question soient privés.

La quatrième considération est la question de savoir si l'attente subjective de M au respect de sa vie privée était objectivement raisonnable compte tenu de l'ensemble des circonstances. La détermination du caractère objectivement raisonnable est une question normative du moment où les Canadiens devraient s'attendre au respect de leur vie privée eu égard aux considérations applicables. Suivant un critère normatif, les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas. Le présent pourvoi porte sur un ensemble particulier de circonstances, où la nature de la relation et la nature de la technique d'enquête sont décisives. Bien que l'art. 8 ne soit pas traditionnellement abordé sous l'angle de la relation particulière parce que la protection qu'il offre est neutre sur le plan du contenu, les policiers connaissaient la relation en cause avant qu'il puisse y avoir atteinte à la vie privée. La société considère de nombreuses relations adulte-enfant comme étant dignes de jouir de la protection conférée par l'art. 8, mais il ne s'agit pas d'une relation de ce type en l'espèce. Pour ce qui est de la technique d'enquête, les policiers savaient dès le départ que la relation était fictive et que Leann était véritablement une inconnue pour M. Ils pouvaient donc conclure en toute confiance et à juste titre qu'aucune préoccupation fondée sur l'art. 8 ne découlerait de l'examen des communications en question. La jurisprudence relative à l'art. 8 suppose l'obtention par la police d'une autorisation préalable avant qu'il puisse y avoir atteinte à la vie privée. Il n'y avait aucune possibilité de cette nature dans la présente affaire. L'article 184.2 du *Code criminel* ne s'applique pas en l'espèce parce qu'une communication faite dans des circonstances où il n'y a aucune attente raisonnable au

respect de sa vie privée ne saurait constituer une « communication privée » pour l'application de l'art. 183.

*Le juge en chef Wagner et la juge Karakatsanis* : Il y a accord sur le fait que le pourvoi devrait être rejeté, mais pour des raisons différentes. Lorsque des agents d'infiltration de la police communiquent par écrit avec des individus, il n'y a aucune fouille ou saisie au sens de l'art. 8 de la *Charte*. Il en est ainsi parce qu'un individu ne peut raisonnablement s'attendre à ce que la personne avec laquelle il communique ne prenne pas connaissance de ses propos. En l'espèce, les policiers ne se sont pas ingérés dans la conversation privée d'autres personnes; ils y ont directement participé. Ils n'ont pas non plus contrevenu à l'art. 8 de la *Charte* lorsqu'ils ont communiqué avec M et conservé des captures d'écran de ces conversations. Comme les conversations ont eu lieu au moyen de courriels et de Facebook, elles ont nécessairement pris une forme écrite. Les captures d'écran tirées du logiciel de capture d'écran sont tout simplement une copie d'un relevé écrit déjà existant, et non un relevé permanent distinct créé clandestinement par l'État.

Toute technique d'enquête ne constitue pas une fouille, une perquisition ou une saisie : l'art. 8 n'entre en jeu que dans le cas où la conduite en matière d'enquête empiète sur l'attente raisonnable d'une personne au respect de sa vie privée. Cette disposition n'empêche pas les policiers de communiquer avec des individus au cours d'une opération d'infiltration; il en est ainsi parce que la technique d'enquête qui consiste pour un policier à participer à une conversation — même si



celui-ci est un agent d'infiltration — ne diminue pas l'attente raisonnable d'une personne au respect de sa vie privée. En l'espèce, un agent d'infiltration s'est entretenu avec M par Facebook et par courriel. Cette situation n'est pas différente de celle où un individu parle à un agent d'infiltration en personne. M a clairement voulu que le destinataire (qui était en l'occurrence un policier) reçoive ses messages. Comme il ne pouvait raisonnablement s'attendre à ce que le destinataire visé de ses messages n'en prenne pas connaissance, l'art. 8 n'entre pas en jeu.

L'utilisation du logiciel de capture d'écran par les policiers ne constitue pas non plus une fouille ou une saisie. Il n'y a aucune différence pertinente dans le fait pour l'État de conserver les conversations en prenant des captures d'écran de celles-ci plutôt qu'en utilisant un ordinateur pour les imprimer ou en déposant en preuve un téléphone ou un ordinateur portatif où les conversations sont ouvertes et visibles. Cette utilisation de la technologie ne constitue pas une conduite intrusive ou clandestine de l'État. De plus, le relevé permanent de la conversation résulte du moyen choisi par M pour communiquer. Ce dernier ne peut raisonnablement s'attendre à ce que le destinataire visé de ses communications ne dispose pas d'un relevé écrit de ses propos. Comme les techniques policières utilisées en l'espèce ne faisaient pas intervenir les protections prévues à l'art. 8, une autorisation judiciaire préalable n'était pas requise.

Bien qu'Internet permette aux individus d'échanger entre eux des renseignements très précieux pour la société, il crée aussi davantage d'occasions de

commettre des crimes. Les opérations policières d'infiltration réalisées à la faveur de l'anonymat d'Internet permettent aux policiers d'empêcher de façon proactive les prédateurs sexuels de s'en prendre à des enfants.

*Le juge **Moldaver*** : Les motifs qu'exposent les juges Karakatsanis et Brown sont bien fondés en droit, et chaque série de motifs sert de fondement valable pour rejeter le pourvoi.

*La juge **Martin*** : La surveillance par l'État des communications privées de M constituait une fouille qui violait l'art. 8 de la *Charte*. Il était objectivement raisonnable pour M de s'attendre à ce qu'un agent de l'État ne puisse prendre clandestinement connaissance d'un enregistrement électronique permanent des communications entre lui et le policier sans autorisation judiciaire préalable. L'utilisation par le policier du logiciel de capture d'écran constituait une « interception » au sens de la partie VI du *Code criminel*. Comme il n'a pas obtenu l'autorisation judiciaire préalable, la fouille était déraisonnable. Cependant, la demande d'exclusion de la preuve fondée sur le par. 24(2) de la *Charte* a été rejetée à juste titre. Bien que l'atteinte au droit à la vie privée ait eu des répercussions importantes, la gravité de l'atteinte était minime. L'exclusion d'éléments de preuve pertinents et fiables dans une affaire de leurre d'enfants, lesquels ont été obtenus au moyen de tactiques que la police avait de bonnes raisons de croire légales au moment de l'enquête, aurait pour effet de déconsidérer l'administration de la justice.

La réglementation de l'Internet, lequel est en constante évolution, exige un juste équilibre entre les droits et les intérêts. L'exploitation sexuelle d'un mineur est un acte odieux, et les enfants et les jeunes sont donc particulièrement vulnérables sur Internet. Les acteurs de l'État doivent disposer de pouvoirs d'enquête qui leur permettront d'enrayer l'exploitation sexuelle en ligne. Cependant, de tels pouvoirs d'enquête doivent être contrebalancés par l'obligation de l'État de respecter les droits au respect de la vie privée de ses citoyens. L'attente raisonnable au respect de la vie privée est de nature normative, et non descriptive. La question qu'il faut se poser consiste donc à savoir si le droit à la vie privée revendiqué doit être considéré comme à l'abri de toute intrusion par l'État — sauf justification constitutionnelle — pour que la société canadienne demeure libre, démocratique et ouverte. Dans une société libre et démocratique, il est raisonnable de s'attendre à ce que l'État n'ait accès aux enregistrements électroniques de leurs communications privées que s'il a obtenu l'autorisation de le faire.

Dans *R. c. Duarte*, [1990] 1 R.C.S. 30, il a été conclu que la surveillance électronique participative clandestine par l'État devait être réglementée. La surveillance sans mandat menée à la seule discrétion de la police annihile le droit des individus qu'est le droit de choisir leurs auditeurs et impose le risque de devoir se reporter à des notes écrites de leurs propos. Cela fait en sorte que la notion de liberté de pensée et d'expression se trouve en fait dénuée de sens. En réponse à l'arrêt *Duarte*, le législateur a adopté l'art. 184.2 du *Code criminel*, qui exige l'obtention d'une autorisation judiciaire préalable pour la surveillance électronique participative

menée par l'État. Dans *Duarte*, l'État avait pu obtenir accès à un relevé écrit de communications privées au moyen de matériel d'enregistrement. Or de nos jours, les gens communiquent par le truchement de médias électroniques, de sorte que leurs conversations sont nécessairement enregistrées; pour obtenir un relevé en temps réel d'une conversation, il suffit d'y participer. Une telle évolution des moyens de communication ne devrait pas avoir pour conséquence que l'État n'aurait plus besoin d'autorisation pour prendre connaissance des relevés électroniques de communications privées. S'il en était autrement, il ne nous resterait rien qui vaille du droit de vivre libre de toute surveillance.

Les communications électroniques en cause tiennent à la fois de la conversation de vive voix et de l'enregistrement électronique clandestin de cette conversation qui a suscité une attente raisonnable au respect de la vie privée dans *Duarte*. Cette dualité devrait étayer, et non miner, la protection des droits à la vie privée, puisqu'un enregistrement existe et que l'État dispose d'un accès non réglementé et sans restriction à celui-ci. Les communications électroniques modernes ressemblent aux enregistrements électroniques parce qu'elles ont pour caractéristiques la permanence, la fiabilité probatoire et la transmissibilité qui définissent les enregistrements électroniques et qu'elles constituent un relevé écrit de la conversation. Le fait que les interlocuteurs soient conscients que leurs communications sont enregistrées, et qu'ils créent eux-mêmes sciemment le relevé de celles-ci, ne signifie pas que les communications électroniques doivent être comparées aux conversations de vive voix ou qu'elles réduisent à néant toute attente

raisonnable au respect de la vie privée. La création de relevés électroniques écrits de ses communications privées est pratiquement une condition à laquelle il faut consentir pour participer à la société moderne, et pourtant, les gens ont encore des attentes, subjectives et objectives, au respect de leur vie privée à l'égard de ces communications. La surveillance électronique non réglementée, par l'État, donnera lieu à ce que les gens exercent l'autocensure sur leur expression en ligne et anéantit le sens de la vie privée de la société.

La proposition générale selon laquelle il n'est pas raisonnable que les gens s'attendent à ce que le destinataire visé des messages d'une personne n'en prenne pas connaissance ne peut s'appliquer lorsque l'État a secrètement fait en sorte d'être le destinataire visé. Dans le cas d'une surveillance participative de l'État, la notion de destinataire visé est intimement liée au droit de choisir ses auditeurs. La personne peut raisonnablement s'attendre à ce que l'État n'enregistre une communication privée de façon permanente que s'il a obtenu une autorisation judiciaire. De plus, il existe des distinctions quantitatives et qualitatives entre la surveillance en personne et la surveillance électronique par l'État qui rendent intenable l'analogie entre les « conversations » dont il était question dans *Duarte* et les communications électroniques d'aujourd'hui. Sur le plan quantitatif, les conversations de vive voix avec des agents d'infiltration ne sont pas susceptibles d'exposer le public à une surveillance électronique clandestine à grande échelle en raison de contraintes pratiques liées aux ressources dans le cas des activités d'infiltration policière, tandis que les technologies de surveillance électronique

rendent la surveillance de masse possible comme jamais auparavant. Sur le plan qualitatif, se créer d'autres identités n'a jamais été aussi facile que maintenant, et cet anonymat en ligne permet une surveillance par l'État d'un tout autre ordre à l'aide de fausses identités crédibles. Enfin, les actions de l'État qui vont à l'encontre d'une attente raisonnable au respect de la vie privée doivent être examinées au regard de l'art. 8 de la *Charte*. Exclure les communications de la portée de l'art. 8 parce que l'État destinataire peut obtenir un relevé de la conversation simplement en y prenant part nuit à l'objet des droits à la vie privée, et perturbe le juste équilibre entre la capacité de l'État d'enquêter sur des crimes et les droits des personnes de disposer d'espaces privés pour s'exprimer.

Le fait de décider s'il existe une attente raisonnable au respect de la vie privée en fonction d'une catégorie de relation est un raisonnement relatif à l'analyse de risques qui n'est pas neutre sur le plan du contenu, et qui impose aux tribunaux la tâche d'évaluer les relations personnelles des individus afin de décider lesquelles sont dignes de jouir de la protection conférée par l'art. 8 de la *Charte*, et lesquelles ne le sont pas. La désapprobation par les tribunaux du mode de vie d'un accusé n'a pas sa place dans le cadre d'une analyse du droit à la vie privée au regard de l'art. 8. Enfin, la conclusion qu'il y a attente raisonnable au respect de la vie privée ne signifie pas qu'il est interdit à l'État d'effectuer une fouille; cela signifie simplement que les actions des policiers doivent être validées par un pouvoir qui respecte l'art. 8 de la *Charte*. Le scénario présenté, soit celui où l'État prétend, dans un contexte d'infiltration, être un enfant et communique avec des gens qui cherchent à sexualiser

des enfants, est le type de situation dans laquelle l'État pourrait et devrait obtenir une autorisation judiciaire pour surveiller des communications électroniques privées. Le risque qu'un interlocuteur divulgue une communication privée n'a pas d'incidence sur le caractère raisonnable de l'attente selon laquelle l'État, s'il n'y a pas eu de telle divulgation, ne s'immiscera pas dans cette communication privée. Pour l'application de l'art. 8, l'analyse porte sur le caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi que sur les conséquences de cette dernière pour la personne qui en fait l'objet, et non sur la nature légale ou illégale de la chose recherchée. Il n'est pas raisonnable de supposer que les communications entre des adultes et des enfants qui ne se connaissent pas sont de nature criminelle. Le principe de la neutralité du contenu a été élaboré pour faire en sorte que de telles atteintes injustifiées de l'État à la vie privée ne se produisent pas. L'analyse relative à l'art. 8 n'a jamais supposé que certaines relations sont à première vue criminelles et ne suscitent donc pas légitimement d'attente au respect de la vie privée. Ce n'est pas le rôle des tribunaux d'évaluer les relations personnelles en vue de priver certaines catégories de personnes de la protection que confère l'art. 8 de la *Charte*.

L'utilisation du logiciel de capture d'écran répond aux définitions d'« interception » et de « communication privée » prévues à l'art. 183 du *Code criminel*. Le verbe « intercepter » évoque une interposition entre l'expéditeur et le destinataire dans le cours du processus de communication. Le policier a enregistré le contenu informationnel des communications privées lorsqu'il les a sauvegardées en temps réel aux fins de reproduction à l'intention des tribunaux. L'application de la

partie VI en l'espèce établit un juste équilibre entre la nécessité pour les forces de l'ordre d'enquêter sur les crimes et le droit des individus de ne pas être importunés. Il se peut que, même sans le logiciel de capture d'écran, la technique d'enquête employée par l'État en l'espèce ait constitué une « interception ». En communiquant avec M sur un support qui produit par lui-même un enregistrement électronique, le policier « a pris connaissance » d'un relevé de la communication. Si la surveillance électronique par la police de communications privées n'est régie que par la partie VI dans la mesure où un logiciel externe d'enregistrement est employé, alors le régime n'est plus assez complet. Pour être constitutionnelle, la prise de connaissance en temps réel, par l'État, de communications électroniques privées doit être réglementée.

## **Jurisprudence**

Citée par le juge Brown

**Distinction d'avec les arrêts:** *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Wong*, [1990] 3 R.C.S. 36; *R. c. Duarte*, [1990] 1 R.C.S. 30; **arrêts mentionnés:** *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *R. c. Edwards*, [1996] 1 R.C.S. 128; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Dymont*, [1988] 2 R.C.S. 417; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696; *R. c. Graff*, 2015 ABQB 415, 337 C.R.R. (2d) 77; *R. c. Ghotra*, [2015] O.J. No. 7253; *R. c. George*, 2017 CSC 38, [2017] 1 R.C.S. 1021; *R. c. Morrison*, 2019 CSC 15; *R. c. K.R.J.*, 2016 CSC 31, [2016] 1



R.C.S. 906; *R. c. Budreo* (2000), 46 O.R. 481; *R. c. TELUS Communications Co.*, 2013 CSC 16, [2013] 2 R.C.S. 3.

Citée par la juge Karakatsanis

**Arrêt examiné:** *R. c. Duarte*, [1990] 1 R.C.S. 30; **arrêts mentionnés:** *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Fearon*, 2014 CSC 77, [2014] 3 R.C.S. 621; *R. c. Wong*, [1990] 3 R.C.S. 36; *R. c. Levigne*, 2010 CSC 25, [2010] 2 R.C.S. 3; *R. c. Evans*, [1996] 1 R.C.S. 8; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Orlandis-Habsburgo*, 2017 ONCA 649, 40 C.R. (7th) 379; *R. c. Fliss*, 2002 CSC 16, [2002] 1 R.C.S. 535; *R. c. Oickle*, 2000 CSC 38, [2000] 2 R.C.S. 3; *Rothman c. La Reine*, [1981] 1 R.C.S. 640; *R. c. Mack*, [1988] 2 R.C.S. 903; *R. c. Hart*, 2014 CSC 52, [2014] 2 R.C.S. 544; *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696; *R. c. TELUS Communications Co.*, 2013 CSC 16, [2013] 2 R.C.S. 3; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Alicandro*, 2009 ONCA 133, 95 O.R. (3d) 173; *R. c. Legare*, 2009 CSC 56, [2009] 3 R.C.S. 551; *R. c. Chiang*, 2012 BCCA 85, 286 C.C.C. (3d) 564; *R. c. Bayat*, 2011 ONCA 778, 108 O.R. (3d) 420; *R. c. Babos*, 2014 CSC 16, [2014] 1 R.C.S. 309.

Citée par la juge Martin

**Arrêts examinés:** *R. c. Duarte*, [1990] 1 R.C.S. 30; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; **arrêts mentionnés:** *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *R. c. Patrick*, 2009

CSC 17, [2009] 1 R.C.S. 579; *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *R. c. Reeves*, 2018 CSC 56; *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 320; *R. c. Wong*, [1990] 3 R.C.S. 36; *United States c. White*, 401 U.S. 745 (1971); *R. c. Pires*, 2005 CSC 66, [2005] 3 R.C.S. 343; *R. c. TELUS Communications Co.*, 2013 CSC 16, [2013] 2 R.C.S. 3; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696; *R. c. Fliss*, 2002 CSC 16, [2002] 1 R.C.S. 535; *Holmes c. Burr*, 486 F.2d 55 (1973); *R. c. Wise*, [1992] 1 R.C.S. 527; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *Rothman c. La Reine*, [1981] 1 R.C.S. 640; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211; *R. c. Craig*, 2016 BCCA 154, 335 C.C.C. (3d) 28; *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569; *R. c. Fearon*, 2014 CSC 77, [2014] 3 R.C.S. 621; *R. c. Belnavis*, [1997] 3 R.C.S. 341; *R. c. Dymont*, [1988] 2 R.C.S. 417; *R. c. Collins*, [1987] 1 R.C.S. 265; *R. c. Kwok*, [2008] O.J. No. 2414; *R. c. Blais*, 2017 QCCA 1774, *R. c. Beairsto*, 2018 ABCA 118, 359 C.C.C. (3d) 376; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 R.C.S. 27; *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353; *R. c. Levigne*, 2010 CSC 25, [2010] 2 R.C.S. 3; *R. c. Plant*, [1993] 3 R.C.S. 281.

### **Lois et règlements cités**

*Charte canadienne des droits et libertés*, art. 8, 24(2).

*Code criminel*, L.R.C. 1985, c. C-46, partie VI, art. 172.1, 183 “intercepter”, “communication privée”, 184.2.

### **Doctrines et autres documents cités**

- Fitch, Gregory J. « Child Luring » in *Substantive Criminal Law, Advocacy and the Administration of Justice*, vol. 1, presented to the National Criminal Law Program, Edmonton, Federation of Law Societies of Canada, 2007.
- Haggerty, Kevin D. « Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance » (2009), 17 *Critical Crim.* 277.
- Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, Toronto, Carswell, 1991 (loose-leaf updated 2018, release 7).
- Lyon, David. *Surveillance After Snowden*, Cambridge, Polity Press, 2015.
- MacFarlane, Bruce A., Robert J. Frater and Croft Michaelson. *Drug Offences in Canada*, vol. 2, 4th ed., Toronto, Thomson Reuters, 2015 (loose-leaf updated April 2017, release 2).
- Marthews Alex, and Catherine Tucker, « The Impact of Online Surveillance on Behavior » in David Gray and Stephen E. Henderson, eds., *The Cambridge Handbook of Surveillance Law*, Cambridge, Cambridge University Press, 2017.
- Penney, Jonathon W. « Internet surveillance, regulation, and chilling effects online: a comparative case study » (2017), 6:2 *Internet Policy Review* 22 (en ligne : <https://policyreview.info/node/692/pdf>; version archivée : [http://www.scc-csc.ca/cso-dce/2019SCC-CSC22\\_1\\_eng.pdf](http://www.scc-csc.ca/cso-dce/2019SCC-CSC22_1_eng.pdf)).
- Penney, Steven. « Consent Searches for Electronic Text Communications : Escaping the Zero-Sum Trap » (2018), 56 *Alta. L. Rev.* 1.
- Penney, Steven, Vincenzo Rondinelli and James Stribopoulos. *Criminal Procedure in Canada*, 2nd ed., Toronto, LexisNexis, 2018.
- Pomerance, Renee M. « Flirting with Frankenstein : The Battle Between Privacy and Our Technological Monsters » (2016), 20 *Can. Crim. L. Rev.* 149.
- Stewart, Hamish. « Normative Foundations for Reasonable Expectations of Privacy » (2011), 54 *S.C.L.R.* (2d) 335.
- Westin, Alan. *Privacy and Freedom*, New York, Ig Publishing, 1967.

POURVOI contre un arrêt de la Cour d'appel de Terre-Neuve-et-Labrador (les juges Welsh, Harrington et Hoegg), 2017 NLCA 12, [2017] N.J. No. 55 (QL), 2017 CarswellNfld 58 (WL Can.), qui a confirmé la déclaration de culpabilité prononcée par le juge Orr, 364 Nfld. & P.E.I.R. 237, 1136

A.P.R. 237, 332 C.R.R. (2d) 50, [2015] N.J. No. 97 (QL), 2015 CarswellNfld 79 (WL Can.). Pourvoi rejeté.

*Rosellen Sullivan et Michael Crystal*, pour l'appelant.

*Lloyd M. Strickland et Sheldon B. Steeves*, pour l'intimée.

*Nicholas E. Devlin et Amber Pashuk*, pour l'intervenante la directrice des poursuites pénales.

*Susan Magotiaux et Katie Doherty*, pour l'intervenante la procureure générale de l'Ontario.

*Nicolas Abran et Ann Ellefsen-Tremblay*, pour l'intervenant le directeur des poursuites criminelles et pénales.

*Daniel M. Scanlan*, pour l'intervenant le procureur général de la Colombie-Britannique.

*Christine Rideout*, pour l'intervenant le procureur général de l'Alberta.

*Jill R. Presser and Kate Robertson*, pour l'intervenante la Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko.

*Frank Addario* et *James Foy*, pour l'intervenante l'Association canadienne des libertés civiles.

*Gerald Chan* et *Annamaria Eneajor*, pour l'intervenante Criminal Lawyers' Association.

*Rachel Huntsman, c.r.*, pour l'intervenante l'Association canadienne des chefs de police.

Version française du jugement des juges Abella, Gascon et Brown rendu par

LE JUGE BROWN —

## I. Introduction

[1] Le présent pourvoi soulève deux questions : (1) la technique d'enquête utilisée par un agent d'infiltration équivalait-elle à une fouille ou à une saisie des communications en ligne de l'appelant Sean Patrick Mills au sens de l'art. 8 de la *Charte canadienne des droits et libertés*, et (2) la police a-t-elle intercepté une communication privée conformément à l'art. 184.2 du *Code criminel*, L.R.C. 1985, c. C-46, en l'absence d'une autorisation judiciaire préalable?

[2] Ces questions découlent d'une opération d'infiltration menée par un policier qui s'est fait passer en ligne pour une adolescente de 14 ans, avec l'intention d'attraper des cyberprédateurs. Pendant deux mois, M. Mills a envoyé plusieurs messages par Facebook et Hotmail. Il a finalement été arrêté dans un parc public où il avait organisé une rencontre avec l'« enfant » en question, et il a été accusé de leurre par Internet en vertu de l'art. 172.1 du *Code criminel*. L'ensemble de l'opération s'est déroulée sans autorisation judiciaire préalable.

[3] Utilisant un logiciel de capture d'écran, la police a produit en preuve au procès un relevé contenant les courriels et les messages envoyés. Soutenant qu'il avait été porté atteinte à son droit à la protection contre les fouilles, les perquisitions et les saisies abusives garanti par l'art. 8 de la *Charte*, M. Mills a demandé l'exclusion de la preuve. Bien qu'il ait conclu qu'une autorisation judiciaire était requise à partir du moment où les policiers déterminaient que M. Mills avait un [TRADUCTION] « intérêt potentiellement inapproprié » à l'égard d'un mineur, le juge du procès a néanmoins admis la preuve et a déclaré M. Mills coupable d'un des chefs d'accusation. La Cour d'appel de Terre-Neuve-et-Labrador a confirmé sa déclaration de culpabilité, mais a conclu que l'attente de M. Mills au respect de sa vie privée n'était pas objectivement raisonnable.

[4] Bien que je sois d'accord avec la Cour d'appel pour dire que M. Mills ne pouvait raisonnablement s'attendre au respect de sa vie privée, ma conclusion s'appuie sur des raisons légèrement différentes. Plus précisément, il ne pouvait pas

prétendre qu'il avait une attente au respect de sa vie privée qui était objectivement raisonnable dans les circonstances de l'espèce. Il s'entretenait avec une personne qu'il croyait être une enfant, et qui était une inconnue pour lui, et l'agent d'infiltration savait qu'un tel entretien aurait lieu au moment où il a créé cette personne. En conséquence, comme l'art. 8 de la *Charte* n'est pas en cause, il s'ensuit que l'opération d'infiltration ne nécessitait pas d'autorisation judiciaire préalable. Je rejeterais donc le pourvoi.

## II. Aperçu des faits et des procédures

### A. *Contexte*

[5] En février 2012, l'agent Greg Hobbs du Royal Newfoundland Constabulary a créé un compte de courriel Hotmail afin de se faire passer pour une adolescente de 14 ans du nom de « Leann Power ». Peu après, il a créé un profil Facebook sous le même nom, indiquant que Leann vivait à St. John's et nommant l'école secondaire qu'elle fréquentait. Un mois plus tard, M. Mills (alors âgé de 32 ans) a communiqué avec « Leann » au moyen de Facebook, prétendant être âgé de 23 ans. Dans les deux mois qui ont suivi, il lui a envoyé plusieurs messages et courriels, dont une photo de son pénis.

[6] Les policiers ont conservé un relevé des communications en ligne et des courriels en question au moyen d'un logiciel de capture d'écran appelé « Snagit ».

[7] Le 22 mai 2012, M. Mills a été arrêté dans un parc où il avait organisé une rencontre avec Leann. Il a été accusé de leurre, infraction prévue à l’art. 172.1 du *Code criminel*. Au procès, il a fait valoir que la police — qui avait mené toute l’opération d’infiltration sans autorisation judiciaire — aurait dû obtenir une telle autorisation en application de l’art. 184.2 du *Code criminel*, et que la fouille et la saisie (par Snagit) des communications au moyen du faux profil en ligne portaient atteinte aux droits que lui garantissait l’art. 8 de la *Charte*. Il a donc demandé l’exclusion de la preuve.

B. *Historique judiciaire*

- (1) Cour provinciale de Terre-Neuve-et-Labrador — le juge Orr ((2013), 7 C.R. (7th) 268)

[8] Le juge du procès a conclu que les messages étaient des « communications privées » au sens de l’art. 183 du *Code criminel*. Comme la police participait à celles-ci, leur interception était assujettie aux exigences de l’art. 184.2 (« Interception avec consentement »). Bien que Facebook et Hotmail aient généré automatiquement un relevé des communications, l’utilisation de Snagit a entraîné une saisie additionnelle. De plus, comme M. Mills se servait d’un nom d’utilisateur et d’un mot de passe, il avait une attente au respect de sa vie privée dans ses communications — attente qui, bien que peut-être *limitée* du fait que la destinataire utilisait un pseudonyme ou une fausse identité, n’a pas été *éliminée*.



[9] Le juge a donc conclu qu'il y avait eu violation de l'art. 8 de la *Charte*. Selon lui, une autorisation judiciaire était requise à partir du moment où l'agent Hobbs s'est rendu compte que M. Mills avait un [TRADUCTION] « intérêt potentiellement inapproprié » à l'égard de Leann.

[10] Dans des motifs distincts sur la possibilité d'utiliser les communications au regard du par. 24(2) de la *Charte*, le juge du procès a conclu que l'utilisation de cette preuve n'était pas susceptible de déconsidérer l'administration de la justice (*R. c. Mills* (2014), 346 Nfld. & P.E.I.R. 102) et a déclaré M. Mills coupable.

(2) Cour d'appel de Terre-Neuve-et-Labrador — les juges Welsh, Harrington et Hoegg (2017 NLCA 12)

[11] Bien qu'elle ait confirmé la déclaration de culpabilité de M. Mills, la Cour d'appel a estimé qu'il n'y avait eu aucune « interception » et que le juge de première instance avait donc commis une erreur en concluant que des autorisations obtenues conformément à l'art. 184.2 étaient requises. Se fondant sur les facteurs énoncés dans *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212 (par. 18) — facteurs au regard desquels l'attente raisonnable en matière de vie privée d'une personne est appréciée, elle a conclu (au par. 23) que M. Mills devait savoir qu'[TRADUCTION] « il a[vait] perdu le contrôle à l'égard de toute attente en matière de confidentialité [et] [qu']il a[vait] pris un risque en communiquant volontairement avec une personne qu'il ne connaissait pas ». En conséquence, l'attente de M. Mills au respect de sa vie

privée n'était pas objectivement raisonnable et il n'a pas été porté atteinte aux droits que lui garantit l'art. 8.

### III. Analyse

#### A. *Analyse fondée sur l'art. 8 de la Charte : M. Mills ne pouvait raisonnablement s'attendre au respect de sa vie privée*

[12] Dans l'arrêt *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, notre Cour a réaffirmé que, pour se réclamer de la protection de l'art. 8, l'accusé doit démontrer qu'il pouvait subjectivement, et de façon objectivement raisonnable, s'attendre au respect de sa vie privée à l'égard de l'objet de la prétendue fouille : par. 10; voir aussi *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 34; *Spencer*, par. 16; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 18; *R. c. Edwards*, [1996] 1 R.C.S. 128, par. 45; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 159-160. Je dis « prétendue fouille », car il n'y a pas de « fouille » et « saisie » au sens de l'art. 8 si le demandeur ne peut démontrer l'existence d'une attente raisonnable au respect de sa vie privée : *R. c. Dyment*, [1988] 2 R.C.S. 417, p. 426; voir aussi S. Penney, V. Rondinelli et J. Stribopoulos, *Criminal Procedure in Canada* (2<sup>e</sup> éd. 2018), p. 151-152; H. Stewart, « Normative Foundations for Reasonable Expectations of Privacy » (2011), 54 *S.C.L.R.* (2d) 335, p. 335.

[13] Le caractère objectivement raisonnable est apprécié au regard de l'« ensemble des circonstances » : *Edwards*, par. 31 et 45; *Marakah*, par. 10; *Spencer*,

par. 16-18; *Cole*, par. 39; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579, par. 26; *Tessling*, par. 19. De plus, la Cour a également toujours maintenu que l'examen de l'ensemble des circonstances suppose l'évaluation de tous les aspects de la vie privée : *Edwards*, par. 45; *Patrick*, par. 26. Quatre considérations guident l'application du critère : (1) l'examen de l'objet de la prétendue fouille; (2) la question de savoir si le demandeur possédait un droit direct à l'égard de l'objet; (3) la question de savoir si le demandeur avait une attente subjective au respect de sa vie privée relativement à l'objet; (4) la question de savoir si cette attente subjective au respect de sa vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances : *Cole*, par. 40; *Marakah*, par. 11; *Spencer*, par. 18; *Patrick*, par. 27; *Tessling*, par. 32.

(1) Quel était l'objet de la prétendue fouille?

[14] La prétendue fouille visait les communications électroniques ayant eu lieu lors de séances de « clavardage » sur Facebook, ainsi que par courriel. Je ne vois aucune distinction importante sur le plan juridique entre ces moyens de communication et celui qui consiste à échanger des messages textes sur téléphones cellulaires sur lequel la Cour s'est penchée dans *Marakah*. De nombreux appareils électroniques connectés à Internet donnent accès à chacun d'eux. De plus, dans *Marakah*, la Cour a refusé de faire une distinction entre les différentes applications de messagerie, puisqu'elles sont fonctionnellement équivalentes à un « réseau interconnecté [. . .] [qui] [. . .] permet la transmission rapide de courts messages entre

des personnes » — lesquels échanges, a ajouté la Cour, sont précisément ce que les policiers recherchent : *Marakah*, par. 18-19.

[15] Bien qu'en l'espèce, les policiers aient été les destinataires directs des messages de M. Mills, il n'en demeure pas moins que ce dernier voulait avoir une conversation seul à seul en ligne. Cela tend à étayer la reconnaissance d'une attente au respect de la vie privée à l'égard de ces communications.

(2) M. Mills possédait-il un droit direct à l'égard de l'objet?

[16] Je conviens qu'en tant que personne ayant participé aux communications (et, bien entendu, en tant que coauteur de celles-ci), M. Mills possédait un droit direct à l'égard de l'objet de la prétendue fouille : voir *Marakah*, par. 21; *Spencer*, par. 50; *Patrick*, par. 31.

(3) M. Mills avait-il une attente subjective au respect de sa vie privée relativement à l'objet?

[17] Dans les cas d'allégations de leurre en ligne, il n'est pas difficile pour l'accusé de démontrer une attente subjective au respect de sa vie privée à l'égard des communications en ligne, car éviter d'être repéré constituera dans un tel cas une priorité. Les utilisateurs s'attendent à ce que leurs messages textes ou (comme en l'espèce) leur équivalent fonctionnel demeurent privés : *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696, par. 34. Il n'est donc pas étonnant qu'en l'espèce, la Couronne

ne conteste pas le fait que M. Mills s'attendait à ce que les communications en cause soient privées.

[18] La preuve le démontre amplement, car M. Mills a demandé à Leann de supprimer leurs messages régulièrement et de vider son dossier d'éléments supprimés. Quand Leann a fait un commentaire sur une publication qu'il avait affiché sur Facebook, il a supprimé celui-ci immédiatement et lui a envoyé un message privé pour lui expliquer que sa mère utilisait également Facebook et qu'il [TRADUCTION] « préférerait ne pas entendre ce qu'elle a à dire à propos de notre différence d'âge » : d.a., vol. 2, p. 86. Répondant à un courriel dans lequel l'agent Hobbs avait envoyé à M. Mills des photos prétendument de Leann, M. Mills a promis de garder leur relation secrète. Il a ajouté qu'il s'attendait à la même chose d'elle : d.a., vol. 2, p. 122. De même, lorsqu'il a envoyé à Leann une photo de son pénis en érection, il l'a invitée à effacer toutes leurs conversations. Il lui a écrit ce qui suit : [TRADUCTION] « on n'est jamais trop prudent et tu pourrais, à mon avis, t'attirer des ennuis avec des photos comme celle-ci ». Le titre du courriel, [TRADUCTION] « regarde puis supprime ça!! », montre également qu'il souhaitait que leur relation demeure secrète : d.a., vol. 2, p. 135.

[19] Cette considération milite donc également en faveur de l'allégation de M. Mills selon laquelle il pouvait raisonnablement s'attendre au respect de sa vie privée. Il reste toutefois à se demander si cette attente subjective était objectivement

raisonnable : B. A. MacFarlane, R. J. Frater et C. Michaelson, *Drug Offences in Canada* (4<sup>e</sup> éd. (feuilles mobiles)), vol. 2, p. 24-15.

- (4) L'attente subjective de M. Mills au respect de sa vie privée était-elle objectivement raisonnable?

[20] Pour pouvoir contester une prétendue fouille en vertu de l'art. 8, M. Mills doit démontrer le caractère objectivement raisonnable de son allégation relative au respect de sa vie privée — l'appréciation à cet égard doit tenir compte de l'ensemble des circonstances. Il s'agit non pas d'une question purement descriptive, mais plutôt d'une question normative du moment où les Canadiens *devraient* s'attendre au respect de leur vie privée, eu égard aux considérations applicables. Le présent pourvoi porte sur un ensemble particulier de circonstances — les policiers ont créé l'un des interlocuteurs et ont contrôlé chacun de ses gestes — et deux considérations deviennent décisives : la nature de la technique d'enquête utilisée par la police et la nature de la relation entre les interlocuteurs. De façon plus particulière, en l'espèce, la technique d'enquête utilisée n'a pas réduit de façon importante la sphère d'intimité dont jouissent les Canadiens, parce qu'elle a permis à l'État de savoir dès le départ que l'accusé adulte communiquerait avec une enfant qu'il ne connaissait pas. Comme je vais l'expliquer, en pareilles circonstances, toute attente subjective au respect de la vie privée qu'a pu avoir l'accusé adulte ne serait pas objectivement raisonnable.

[21] Avant de se pencher sur la question normative, il faut, à titre préliminaire, déterminer la nature du droit à la vie privée en cause. En l'espèce, M. Mills fait valoir

un droit à la vie privée d'ordre informationnel. Comme l'a conclu la Cour dans l'arrêt *Spencer*, un tel droit englobe au moins trois facettes qui se chevauchent, mais qui se distinguent sur le plan conceptuel : la *confidentialité*, le *contrôle* et l'*anonymat* : par. 38. M. Mills allègue un droit à la vie privée portant sur le « contrôle » dans le contenu de ses communications, droit représentant le « postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend » : *Spencer*, par. 40. Bien qu'il protège les renseignements que nous communiquons à d'autres personnes, ce droit à la vie privée repose sur le contrôle qu'une personne exerce en choisissant, *de façon sélective*, quelles personnes recevront ces renseignements. En fait, M. Mills soutient qu'il a choisi sa destinataire (en l'espèce une personne qu'il croyait être une enfant et qui était une inconnue pour lui) et que la création par les policiers d'un faux profil en ligne l'a empêché de pouvoir s'entretenir en secret avec celle-ci.

[22] Cependant, élément crucial en l'espèce, M. Mills communiquait avec une personne qu'il croyait être une *enfant* et qui était une *inconnue* pour lui. Celui-ci fait donc valoir que, même lorsqu'il s'entretenait avec une enfant qui était une inconnue pour lui, il avait conservé la possibilité de choisir, *de façon sélective*, à qui il communiquerait certains échanges. Pour les besoins de l'analyse du droit à la vie privée au regard de l'art. 8, cela présuppose qu'il n'y a rien de différent en soi entre une relation mettant en cause un adulte et un enfant qu'il ne connaît pas, et d'autres relations. Je ne suis pas d'accord et, sur ce point, les déclarations faites par le juge Nielsen dans *R. c. Graff*, 2015 ABQB 415, 337 C.R.R. (2d) 77, par. 63 et 65, où

l'accusé a été inculpé de leurre sur Internet à l'égard d'un destinataire qui s'est présenté comme étant une personne âgée de 14 ans, sont, à mon avis, pertinentes :

[TRADUCTION]

En bref, le demandeur a envoyé à une personne qu'il ne connaissait pas du tout des renseignements de nature très personnelle sur Internet, et ce, sans avoir été invité à le faire et sans prendre des mesures raisonnables pour vérifier l'identité du destinataire, pour garantir son propre anonymat ou pour assurer une quelconque confidentialité en ce qui a trait aux renseignements qu'il transmettait.

[. . .]

Compte tenu de l'ensemble des circonstances, je conclus que, bien que le demandeur ait pris des risques ou ait espéré que les messages qu'il envoyait lors de séances de clavardage, ainsi que les autres éléments et renseignements qu'il transmettait en ligne, demeureraient privés, rien ne lui permettait de s'attendre de façon [. . .] objectivement raisonnable au respect de sa vie privée dans les circonstances.

Voir également *R. c. Ghotra*, [2015] O.J. No. 7253 (Q.L.) (C.S.J.), par. 128.

[23] La Cour a reconnu que les enfants sont particulièrement vulnérables aux crimes sexuels (*R. c. George*, 2017 CSC 38, [2017] 1 R.C.S. 1021, par. 2), qu'Internet fournit plus d'occasions d'exploiter sexuellement des enfants (*R. c. Morrison*, 2019 CSC 15, par. 2) et que le fait d'offrir à ceux-ci une protection accrue afin qu'ils ne soient pas victimes d'infractions sexuelles est vital dans une société libre et démocratique (*R. c. K.R.J.*, 2016 CSC 31, [2016] 1 R.C.S. 906, par. 66, citant le juge Laskin dans *R. c. Budreo* (2000), 460 O.R. (3d) 481 (C.A.)).



Cela m'amène à conclure qu'en regard au critère normatif de l'attente en matière de vie privée énoncé par notre Cour (*Tessling*, par. 42), les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas. Le fait que celles-ci aient lieu en ligne ajoute non pas une couche de protection de la vie privée, mais plutôt un élément d'imprévisibilité.

[24] La difficulté, bien entendu, tient à ce que, dans la plupart des cas, il est peu probable que la police connaisse, avant qu'il puisse y avoir atteinte à la vie privée, la nature de la relation entre les interlocuteurs — et sache, par exemple, si l'enfant est véritablement un inconnu pour l'adulte. Il nous faut également garder à l'esprit que la plupart des relations entre adultes et enfants sont dignes de jouir de la protection conférée par l'art. 8, notamment celles avec des membres de la famille, des amis, des professionnels ou des conseillers religieux. Fait important, *et le plus important pour trancher le présent pourvoi*, cette difficulté ne se pose pas en l'espèce. Dans la présente affaire, la police utilisait une technique d'enquête lui permettant de *savoir dès le départ* que l'adulte s'entretenait avec un enfant qu'il ne connaissait pas. Différentes considérations normatives entrent en jeu en l'espèce, tant en ce qui concerne la nature de la relation et la façon dont cela éclaire l'analyse fondée sur l'art. 8, qu'en ce qui concerne la mesure dans laquelle la technique d'enquête réduit la sphère d'intimité dont jouissent les Canadiens.

[25] Si la Cour n'a pas traditionnellement abordé l'art. 8 sous l'angle de la relation particulière entre les parties soumises à la surveillance de l'État, c'est parce qu'elle considère que la protection offerte par cette disposition est neutre sur le plan du contenu. En l'espèce, la technique utilisée a permis aux policiers de connaître cette relation avant qu'il puisse y avoir atteinte à la vie privée. À titre d'exemple, dans *Dyment*, les juges majoritaires de la Cour ont jugé que le fait qu'une personne puisse consentir à donner un échantillon de sang demandé par son médecin ne signifie pas nécessairement qu'il y a eu renonciation à tous les droits à la protection de la vie privée à l'égard de l'échantillon en question une fois que le sang a quitté le corps de cette personne. La Cour a considéré que le droit garanti par l'art. 8 portait non pas uniquement sur *le sang*, mais plutôt principalement sur la relation entre le patient et le médecin. Elle a écrit ce qui suit au par. 28 : « la protection accordée par la *Charte* va jusqu'à interdire à un agent de police [. . .] de se faire remettre [. . .] le sang d'une personne par celui qui l[e] détient avec l'obligation de respecter la dignité et la vie privée de cette personne » (je souligne). En conséquence, bien qu'il ait renoncé au contrôle *matériel* de l'échantillon, le patient a pu — en raison du droit à la protection de la vie privée imprégnant la *relation* — conserver le contrôle *juridique* de celui-ci.

[26] En bref, dans l'arrêt *Dyment*, l'analyse relative à l'échantillon a tenu lieu d'analyse relative à l'objectif visé par l'art. 8, lequel consiste à protéger une relation donnée — que la société juge digne de jouir de la protection de l'art. 8 — contre l'intrusion de l'État. En appliquant cet arrêt en l'espèce, et bien que j'aie affirmé que de nombreuses relations adulte-enfant sont également dignes de bénéficier de la

protection conférée par l'art. 8, je conclus que, si l'attente en matière de vie privée doit refléter un critère normatif (et non purement descriptif), M. Mills et « Leann » n'avaient pas une relation de ce type. Cette conclusion peut s'appliquer ou non à d'autres types de relations, selon la nature de la relation en question et les circonstances entourant celle-ci au moment de la prétendue fouille.

[27] Pour ce qui est de la deuxième considération — la nature de la technique d'enquête utilisée —, ce qui rend objectivement déraisonnable l'attente de M. Mills au respect de sa vie privée est le fait qu'en créant l'enfant fictive, les policiers savaient dès le départ que la relation entre M. Mills et son interlocutrice était elle aussi fictive, et que « Leann » était véritablement une inconnue pour lui. Ils pouvaient donc conclure en toute confiance et à juste titre qu'aucune préoccupation fondée sur l'art. 8 ne découlerait de leur examen de ces communications, parce que les renseignements nécessaires quant à la nature de la relation entre l'accusé et l'« enfant » étaient connus depuis le départ.

[28] Notre jurisprudence relative à l'art. 8 suppose l'obtention par la police d'une autorisation préalable avant qu'il *puisse* y avoir atteinte à la vie privée. Il n'y a toutefois aucune possibilité de cette nature en l'espèce. Les policiers *ont créé* l'enfant fictive et ont attendu que des inconnus d'âge adulte leur envoient des messages. C'est ce qui distingue la présente espèce des affaires *R. c. Wong*, [1990] 3 R.C.S. 36, et *Marakah*, où l'État s'immisciait dans une relation qui (lui) était inconnue. La police avait tout au plus une simple *théorie* quant à la relation entre les interlocuteurs : dans

*Wong*, par exemple, ceux-ci étaient considérés comme des joueurs illégaux. La nature véritable de la relation ne pouvait être connue de façon certaine que par un examen de la conversation. Par contraste, en l'espèce, les policiers connaissaient dès le départ la nature de la relation entre les interlocuteurs. C'est ce qui distingue également le présent cas de l'affaire *R. c. Duarte*, [1990] 1 R.C.S. 30, où la technique employée était celle de l'usurpation d'identité par un indicateur de police.

[29] La technique d'enquête utilisée en l'espèce a permis aux policiers de connaître dès le départ la nature de la relation entre M. Mills et « Leann ». Comme le souligne ma collègue la juge Karakatsanis, cette technique consistait pour les policiers à simplement répondre aux messages qui leur étaient directement envoyés sous le pseudonyme de « Leann ». Il n'y avait aucun risque d'atteinte à la vie privée en l'espèce — ce qui arrive, par exemple, lorsque les policiers passent en revue diverses communications avant d'être en mesure d'établir la relation.

[30] Ma collègue la juge Martin affirme que les présents motifs « impose[nt] aux tribunaux la tâche d'évaluer les relations personnelles des Canadiens afin de décider lesquelles sont dignes de jouir de la protection conférée par l'art. 8 de la *Charte*, et lesquelles ne le sont pas » (par. 110), et « sanctionn[ent] dans les faits l'intrusion injustifiée de l'État dans de grands pans de la vie privée de toute personne en vue d'obtenir quelques communications illégales » (par. 131). Soit dit en tout respect, l'opération d'infiltration fondée sur un pseudonyme utilisée en l'espèce ne constitue pas une première étape vers la mise en place d'une société dystopique

caractérisée par une surveillance de masse non réglementée. Rien dans les présents motifs ne suggère ou ne devrait être considéré comme suggérant que les policiers peuvent simplement surveiller des communications dans l'espoir de tomber sur une conversation qui révèle une activité criminelle. La proposition que j'avance est modeste : je le répète, M. Mills ne peut pas établir une attente objectivement raisonnable au respect de sa vie privée dans les circonstances de l'espèce, où il s'est entretenu en ligne avec *une enfant* qui était *une inconnue* pour lui et où, *élément le plus important*, les policiers savaient qu'un tel entretien aurait lieu au moment où ils ont créé l'enfant en question.

[31] Soit dit en tout respect pour les tenants de l'avis contraire, je ne puis tout simplement pas accepter qu'eu égard aux faits de l'espèce, la « sanction [judiciaire] de la forme particulière de surveillance non autorisée en cause empiéterait sur l'intimité dont disposent encore les particuliers dans une mesure incompatible avec les objectifs d'une société libre et ouverte » : *Wong*, p. 46. Je souscris à la conclusion de la Cour d'appel selon laquelle M. Mills ne pouvait raisonnablement s'attendre au respect de sa vie privée dans les circonstances de l'espèce.

#### B. *Considération additionnelle*

[32] Ma conclusion quant au caractère déraisonnable de l'attente de M. Mills au respect de sa vie privée est déterminante. Cela dit, je ferai l'observation suivante sur la question de savoir si la partie VI du *Code criminel* visait les communications en question du fait qu'il s'agissait de « communications privées ».

[33] À mon avis, l'art. 184.2 du *Code criminel* ne s'appliquait pas en l'espèce parce qu'il n'y a eu aucune « communication privée ». Le paragraphe 184.2(1) prévoit que « [t]oute personne peut [. . .] intercepter une communication privée si l'auteur de la communication ou la personne à laquelle il la destine a consenti à l'interception et si une autorisation a été obtenue conformément au paragraphe (3). » L'article 183 définit « communication privée » et « intercepter » pour l'application de la partie VI :

**183** Les définitions qui suivent s'appliquent à la présente partie.

[. . .]

***intercepter*** S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet.

[. . .]

***communication privée*** Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

...

[34] Si l'on interprète cette définition conjointement avec les précisions apportées par la Cour à l'égard de l'art. 8 de la *Charte*, une communication faite dans des circonstances où il n'y a aucune attente raisonnable au respect de sa vie privée ne saurait constituer une « communication privée » pour l'application de l'art. 183 : *R. c.*

*Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3, par. 32;  
S. Penney, « Consent Searches for Electronic Text Communications: Escaping the  
Zero-Sum Trap » (2018), 56 *Alta. L. Rev.* 1, p. 18.

#### IV. Conclusion

[35] Par conséquent, M. Mills n'a pas réussi à établir qu'il pouvait raisonnablement s'attendre au respect de sa vie privée dans ses conversations avec « Leann ». Je rejetterais donc le pourvoi.

Version française des motifs du juge en chef Wagner et de la juge Karakatsanis  
rendus par

LA JUGE KARAKATSANIS —

[36] Je partage l'avis de mon collègue le juge Brown sur l'issue du présent pourvoi. J'arrive toutefois à cette conclusion pour des raisons différentes. À mon avis, lorsque des agents d'infiltration de la police communiquent par écrit avec des individus, il n'y a aucune « fouill[e] » ou « saisi[e] » au sens de l'art. 8 de la *Charte canadienne des droits et libertés*, et ce, parce qu'il n'est pas raisonnable de s'attendre à ce que le destinataire visé d'un message n'en prenne pas connaissance (même si le destinataire en question est un agent d'infiltration). De plus, la conduite des policiers n'équivaut pas à une fouille ou à une saisie : les policiers n'ont rien pris à l'accusé ni

ne se sont immiscés dans une conversation privée; les agents d'infiltration ont simplement reçu les messages qui leur avaient été directement envoyés.

[37] En l'espèce, les policiers ne se sont pas ingérés dans la conversation privée d'autres personnes; ils y ont directement participé. Comme cette conversation a eu lieu au moyen de courriels et de Facebook messenger, elle a nécessairement pris une forme écrite. Les captures d'écran tirées du programme informatique « Snagit » sont tout simplement une copie d'un relevé écrit déjà existant, et non un relevé permanent distinct créé clandestinement par l'État. En conséquence, les policiers n'ont pas contrevenu à l'art. 8 lorsqu'ils ont communiqué avec M. Mills et conservé des captures d'écran de ces conversations. Je rejeterais le pourvoi.

## I. Analyse

[38] L'article 8 garantit le droit à la protection contre les fouilles, perquisitions et saisies abusives. Lorsqu'ils interprètent cette disposition, les tribunaux tentent d'établir un équilibre acceptable dans une société libre et démocratique entre les intérêts parfois contradictoires que constituent, d'une part, les intérêts en matière de respect de la vie privée nécessaires à la dignité et à l'autonomie de la personne, et, d'autre part, le besoin de vivre dans une société sûre et sécuritaire : voir *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 159-160.

[39] Le droit à la protection contre les fouilles, les perquisitions et les saisies abusives doit évoluer au même rythme que la technologie afin que les citoyens



demeurent à l'abri des atteintes non autorisées de l'État à leur vie privée : *R. c. Fearon*, 2014 CSC 77, [2014] 3 R.C.S. 621, par. 102; voir aussi *R. c. Wong*, [1990] 3 R.C.S. 36, p. 44. Cependant, au fur et à mesure qu'évolue la technologie, les moyens de commettre des crimes — et d'enquêter sur ceux-ci — évoluent également. La présente affaire met en jeu ces deux conséquences. Elle nous oblige à déterminer quelle autorisation judiciaire, s'il en faut une, doit être obtenue au préalable lorsqu'une technique d'enquête policière courante — une opération d'infiltration — se déroule électroniquement en vue « de démasquer et d'arrêter les prédateurs adultes qui rôdent dans l'Internet pour appâter des enfants et des adolescents vulnérables, généralement à des fins sexuelles illicites » : *R. c. Levigne*, 2010 CSC 25, [2010] 2 R.C.S. 3, par. 24.

A. *Conversations électroniques lors d'opérations policières d'infiltration*

[40] À mon avis, il n'y a eu aucune « fouill[e] » ou « saisi[e] » quand l'agent Hobbs, se faisant passer pour une jeune fille, s'est entretenu avec M. Mills par Facebook messenger et par courriel.

[41] Toute technique d'enquête utilisée par les policiers ne constitue pas une fouille, une perquisition ou une saisie sur le plan constitutionnel : l'art. 8 n'entre en jeu que dans le cas où la conduite en matière d'enquête empiète sur l'attente raisonnable d'une personne au respect de sa vie privée : *R. c. Evans*, [1996] 1 R.C.S. 8, par. 11; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 18; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 34. Comme l'a reconnu le juge Doherty,

[TRADUCTION] « [I]orsqu'il s'agit de décider si la conduite de l'État équivaut à une fouille, à une perquisition ou à une saisie, l'attention ne doit pas tant porter sur la nature de la conduite étatique que sur l'incidence de cette conduite sur les intérêts en matière de vie privée du demandeur qui invoque l'art. 8 » : *R. c. Orlandis-Habsburgo*, 2017 ONCA 649, 40 C.R. (7th) 379, par. 39.

[42] Notre Cour reconnaît depuis longtemps que l'art. 8 n'empêche pas les policiers de communiquer avec des individus au cours d'une opération d'infiltration. Il en est ainsi parce qu'un individu ne peut raisonnablement s'attendre à ce que la personne avec laquelle il communique ne prenne pas connaissance de ses propos. L'article 8 ne s'applique pas parce que la technique d'enquête qui consiste pour un policier à participer à une conversation — même si celui-ci est un agent d'infiltration — ne diminue pas l'attente raisonnable d'une personne au respect de sa vie privée. Les affaires *R. c. Duarte*, [1990] 1 R.C.S. 30, et *R. c. Fliss*, 2002 CSC 16, [2002] 1 R.C.S. 535, portaient toutes deux sur des conversations entre des agents d'infiltration et l'accusé. Dans les deux cas, la conversation en soi n'a pas fait intervenir l'art. 8. Comme l'a écrit le juge La Forest dans *Duarte*, à la p. 57, « [u]ne conversation avec un indicateur n'est pas une fouille, une perquisition ou une saisie au sens de la *Charte*. Toutefois l'interception et l'enregistrement électroniques clandestins d'une communication privée en sont » (je souligne). Dans les motifs concordants qu'elle a rédigés dans *Fliss*, la juge Arbour a repris ce point de vue au par. 12, statuant qu'« une conversation avec un indicateur, ou un policier, n'est pas une fouille, une perquisition ou une saisie. Seul l'enregistrement de cette conversation l'est. »

[43] De même, les opérations policières d'infiltration sont reconnues depuis longtemps comme des outils d'application de la loi légitimes et importants. Les policiers n'ont pas besoin d'obtenir une autorisation judiciaire avant d'entreprendre une opération d'infiltration. La Cour a reconnu que ceux-ci peuvent faire appel à la créativité et au subterfuge dans leur travail de prévention du crime et d'enquête en matière criminelle, mais que leur conduite ne doit pas menacer l'intégrité du système de justice pénale : voir *R. c. Oickle*, 2000 CSC 38, [2000] 2 R.C.S. 3, par. 65-67, citant *Rothman c. La Reine*, [1981] 1 R.C.S. 640, p. 697 (opinion concordante du juge Lamer (plus tard Juge en chef)); *R. c. Mack*, [1988] 2 R.C.S. 903, p. 916-917; *R. c. Hart*, 2014 CSC 52, [2014] 2 R.C.S. 544, par. 83.

[44] En l'espèce, un agent d'infiltration s'est entretenu avec M. Mills par Facebook messenger et par courriel. De toute évidence, M. Mills ne s'est pas rendu compte que la personne à laquelle il parlait était un agent d'infiltration. Cependant, cette situation n'est pas différente de celle où un individu parle, sans le savoir, à un agent d'infiltration en personne. L'arrêt *Fliss* établit clairement que les individus qui s'entretiennent de vive voix avec un agent d'infiltration ne font pas par le fait même l'objet d'une fouille ou d'une saisie au sens de la *Charte*, et ce, même si ils n'ont aucune raison de croire qu'ils parlent à la police. Dans la présente affaire, M. Mills a clairement voulu que le destinataire (qui était en l'occurrence un policier) reçoive ses messages. Il ne serait pas raisonnable pour lui de s'attendre à autre chose. Comme il ne pouvait raisonnablement s'attendre à ce que le destinataire visé de ses messages n'en prenne pas connaissance, l'art. 8 n'entre pas en jeu.

[45] Le fait que la conversation ait pris une forme écrite, plutôt qu'orale comme dans les affaires *Duarte* et *Fliss*, ne transforme pas celle-ci en une fouille ou une saisie. À titre d'exemple, si M. Mills avait envoyé une lettre ou remis une note à un agent d'infiltration, l'art. 8 n'exigerait pas que ce dernier obtienne un mandat avant d'en prendre connaissance.

[46] L'appelant soutient que les arrêts *Duarte* et *Wong* ont pour effet combiné d'exiger des policiers qu'ils obtiennent toujours une autorisation judiciaire avant de participer à des entretiens particuliers en ligne dans le cadre d'une opération d'infiltration. À son avis, la conduite des policiers en l'espèce [TRADUCTION] « est impossible à distinguer de » l'enregistrement clandestin dans *Duarte*.

[47] Cependant, le trait commun des affaires *Duarte* et *Wong* était non pas le recours à des agents d'infiltration, mais plutôt la décision unilatérale de l'État d'effectuer clandestinement des enregistrements audio et vidéo de conversations de vive voix, ce qui était troublant, car les policiers avaient transformé une conversation éphémère de vive voix en un relevé permanent à l'insu de la personne qui parlait. La question était de savoir si la capacité technologique nouvelle de « faire l'écoute » de conversations devrait exiger une autorisation judiciaire préalable. Et, en ce qui a trait à la perspective d'enregistrements audio et vidéo de la vie quotidienne, la Cour a conclu que la menace pour la liberté et l'autonomie de la personne l'emportait sur les objectifs valables de l'État en matière d'application de la loi.

[48] Cependant, dans la présente affaire, M. Mills a choisi l'écrit comme moyen de communication avec l'agent Hobbs. Non seulement les utilisateurs du courriel et de Facebook messenger sont au fait de l'existence d'un relevé écrit permanent de leurs communications, mais ils créent en fait eux-mêmes ce relevé. L'analogie avec l'arrêt *Duarte* a trait à la conversation de vive voix, et non à l'enregistrement clandestin de cette conversation. Cet arrêt ne portait pas sur un relevé écrit créé par une personne communiquant avec un agent d'infiltration. Il n'exige donc pas que les policiers obtiennent un mandat avant d'utiliser des moyens de communication modernes, tels les messages textes ou les courriels, au cours d'opérations d'infiltration.

[49] Ma collègue la juge Martin évoque le risque d'une « surveillance électronique clandestine à grande échelle » : par. 103. Cependant, la technique d'enquête utilisée en l'espèce consistait en une conversation seul à seul entre un agent d'infiltration et l'accusé. La Cour a conclu qu'en règle générale, les tentatives des policiers d'obtenir des conversations électroniques écrites sont assujetties à l'art. 8. Ceux-ci sont tenus d'obtenir un mandat avant de pouvoir avoir accès à des conversations par message texte conservées par les fournisseurs de services de télécommunications : *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696, par. 77-81; *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3, par. 12-13 et 48-49. De même, le fait d'examiner une conversation par message texte entre deux autres parties, sans leur consentement, fait également intervenir l'art. 8 de la *Charte* : *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, par. 54-57.

[50] Cette approche ne réintroduit pas l'« analyse fondée sur le risque » rejetée dans l'arrêt *Duarte*. L'article 8 protège les cas où « nous nous attendons à ce que nos propos ne soient entendus que par la personne ou les personnes auxquelles nous les destinons » : *Duarte*, p. 47. C'est précisément ce qui s'est passé en l'espèce — les communications de M. Mills ont été reçues par le destinataire visé, qui était en l'occurrence un policier. En communiquant en ligne avec une personne qu'il n'avait jamais rencontrée auparavant, M. Mills s'est exposé au risque que cet interlocuteur soit un policier. La *Charte* ne peut être invoquée pour « nous protéger si nous choisissons mal nos amis » : *Duarte*, p. 57.

[51] En conséquence, l'art. 8 de la *Charte* n'entre pas en jeu du simple fait qu'un agent d'infiltration discute par voie électronique avec un individu, et ce, pour les motifs suivants : (1) il n'est pas raisonnable de la part de l'expéditeur de s'attendre à ce que le destinataire visé de ses messages n'en prenne pas connaissance (même s'il s'agit d'un agent d'infiltration), et (2) le fait que les policiers communiquent avec un individu n'équivaut pas à une fouille ou à une saisie. D'une manière ou d'une autre, le résultat est le même : il n'y a aucune violation de l'art. 8 quand les policiers ne font que communiquer avec un individu.

[52] L'autre conclusion aurait une incidence importante et négative sur les opérations policières d'infiltration, y compris celles menées électroniquement : voir S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), section 4(c)(v)(B) (portant sur la question de savoir si une communication obtenue

par usurpation d'identité ou par erreur a été interceptée). Je conviens avec l'intervenante l'Association canadienne des chefs de police que le fait d'exiger des policiers qu'ils obtiennent une autorisation judiciaire, surtout une autorisation visée à la partie VI, avant de se livrer à une opération d'infiltration de ce genre [TRADUCTION] « empêchera[it] dans les faits les policiers de [réprimer] de façon proactive [les infractions de leurre] » : m.i., par. 5. Plus particulièrement dans une affaire comme celle qui nous occupe, où il n'y pas de suspect avant l'ouverture de l'enquête, les policiers n'auraient pas de motifs d'obtenir un mandat ou une autorisation visée à la partie VI. Comme l'ont reconnu les tribunaux, les opérations policières d'infiltration sont un moyen important de réprimer les infractions de leurre et de protéger les enfants vulnérables : *Levigne*, par. 25; *R. c. Alicandro*, 2009 ONCA 133, 95 O.R. (3d) 173, par. 38. Exiger que la police obtienne une autorisation judiciaire avant même qu'une opération d'infiltration par voie électronique ne soit lancée ne permet tout simplement pas d'établir un équilibre approprié entre la vie privée des individus et la sécurité de nos enfants.

A. B. *Utilisation de « Snagit » pour faire des captures d'écran d'une conversation électronique*

[53] M. Mills soutient qu'en utilisant « Snagit » pour prendre des captures d'écran des messages électroniques qu'il échangeait avec l'agent d'infiltration, les policiers ont violé de nouveau les droits que lui garantit l'art. 8 de la *Charte*.

[54] Il reste alors à décider si l'utilisation de « Snagit » équivaut par ailleurs à une fouille ou à une saisie qui requiert une certaine forme d'autorisation judiciaire. Bien entendu, même si elle n'était pas autorisée à produire en preuve les captures d'écran imprimées, la Couronne pourrait toujours faire témoigner l'agent au sujet de ce qu'a dit l'accusé et le relevé écrit pourrait servir à rafraîchir la mémoire de ce témoin : *Duarte*, p. 58 et 60; *Fliss*, par. 7, 12 et 43-45. Cependant, la conservation permanente des propos complets et exacts de l'accusé fournit à l'État une preuve convaincante contre l'accusé. L'utilisation par l'État de la technologie de capture d'écran empiète-t-elle sur l'attente raisonnable de l'accusé au respect de sa vie privée de sorte qu'elle constitue une fouille ou une saisie?

[55] À mon avis, la réponse est non. Comme nous l'avons vu, le relevé permanent de la conversation résulte du moyen choisi par M. Mills pour communiquer. Ce dernier ne peut raisonnablement s'attendre à ce que le destinataire ne dispose pas d'un relevé écrit de ses propos.

[56] C'est pour cette raison que l'utilisation de « Snagit » par les policiers ne constitue pas non plus une fouille ou une saisie. Pour ce qui est de la conservation des conversations par l'État, je ne vois aucune différence pertinente entre le fait d'utiliser « Snagit » pour faire des captures d'écran de celles-ci, l'utilisation d'un ordinateur pour les imprimer, et le dépôt en preuve d'un téléphone ou d'un ordinateur portatif où les conversations en question sont ouvertes et visibles. En fin de compte, les captures d'écran obtenues au moyen de « Snagit » ne sont qu'une copie des messages écrits.



Cette utilisation de la technologie ne constitue pas une conduite intrusive ou clandestine de l'État.

[57] Ma conclusion selon laquelle l'art. 8 n'entre pas en jeu en l'espèce ne signifie pas que les opérations policières d'infiltration menées en ligne n'empièteront *jamais* sur une attente raisonnable au respect de la vie privée. Les changements que connaissent la technologie et nos façons de communiquer amènent les tribunaux à jouer un rôle important lorsqu'il s'agit de garantir que les techniques d'infiltration policière n'empiètent pas de façon inacceptable sur la vie privée des Canadiens. En particulier dans le contexte de l'ère numérique, il est important que les tribunaux se penchent tant sur la nature que sur l'étendue de la technique d'enquête utilisée lorsqu'il s'agit de décider si l'art. 8 entre en jeu. Quant à la crainte que les avancées technologiques rendent possible une surveillance plus large, le juge Binnie a fait remarquer dans l'arrêt *Tessling* que « [t]out développement qui pourra survenir devra être examiné par les tribunaux. Les problèmes devraient être analysés au moment où ils se posent véritablement » : par. 55.

[58] Comme les techniques policières utilisées en l'espèce ne faisaient pas intervenir les protections prévues à l'art. 8, une autorisation judiciaire préalable n'était pas requise. Il n'est donc pas nécessaire de se demander si l'une ou l'autre de ces techniques constituait une « interception » au sens de la partie VI du *Code criminel*, L.R.C. 1985, c. C-46.

## II. Conclusion

[59] La question normative qu'il faut finalement se poser au regard de l'art. 8 est de savoir [TRADUCTION] « si, compte tenu de l'incidence d'une technique d'enquête donnée sur des intérêts en matière de vie privée, il est souhaitable que l'État puisse utiliser cette technique sans aucune autorisation légale ou surveillance judiciaire » : H. Stewart, « Normative Foundations for Reasonable Expectations of Privacy » (2011), 54 *S.C.L.R.* (2d) 335, p. 342. Je reconnais que, dans l'arrêt *Duarte*, la Cour n'avait pas prévu l'utilisation généralisée de la communication électronique. Je concède également que beaucoup de gens se livrent à de longues conversations privées en ligne avec des individus qu'ils n'ont jamais rencontrés en personne. Or, bien qu'Internet permette aux individus d'échanger entre eux des renseignements très précieux pour la société, il crée aussi davantage d'occasions de commettre des crimes. L'anonymat de l'univers virtuel permet à certains prédateurs adultes de gagner la confiance d'enfants vulnérables et de les amener par la ruse à se livrer à des activités sexuelles : *R. c. Legare*, 2009 CSC 56, [2009] 3 R.C.S. 551, par. 2; *Levigne*, par. 25.

[60] Les opérations policières d'infiltration réalisées à la faveur de l'anonymat d'Internet permettent à la police d'empêcher de façon proactive les prédateurs sexuels de s'en prendre à des enfants. Les policiers recourent aux opérations d'infiltration depuis des décennies pour enquêter sur des crimes et les prévenir. Le fait que les conversations avec des agents d'infiltration se fassent aujourd'hui sous forme écrite sur Internet ne contrevient pas, en soi, à l'art. 8 de la *Charte*. Toutefois, cette conclusion ne confère aucunement à la police une grande latitude lui permettant de se livrer à une surveillance générale en ligne des conversations privées. Tant l'art. 8 de

la *Charte* —tel que décrit dans les arrêts *TELUS*, *Marakah* et *Jones* — que les doctrines de common law de l’abus de procédure et de la provocation policière limitent les façons dont les policiers peuvent utiliser les communications électroniques au cours d’une enquête.

[61] Les intervenants en l’espèce ont soulevé la préoccupation relative à la mesure dans laquelle les policiers sont autorisés à usurper l’identité d’autres personnes pour favoriser l’atteinte de leurs objectifs d’infiltration. La Criminal Lawyers’ Association intervenante soutient que le fait de ne pas appliquer l’art. 8 en l’espèce ouvre la porte à la possibilité que les policiers se fassent passer pour des fournisseurs de thérapie sur Internet, ou encore créent leur propre service de rencontre, en vue de surveiller les dépendances ou les préférences sexuelles des Canadiens : m.i., par. 4-5.

[62] Ces scénarios ont très peu à voir avec les faits de la présente affaire, où l’agent a créé un seul profil Facebook et n’a pris contact avec personne. Plus important encore, je ne suis pas convaincue que l’art. 8 de la *Charte* ou la partie VI du *Code criminel* constituent les moyens appropriés pour répondre à ces préoccupations. La menace d’opérations d’infiltration menées par des policiers sans scrupules s’apparente davantage à une menace plus large à l’intégrité du système de justice. Comme l’a reconnu le juge Lamer dans *Rothman*, certaines techniques d’infiltration, comme le fait de se faire passer pour un aumônier de prison ou un avocat de l’aide juridique pour soutirer des éléments de preuve incriminants, vont

trop loin et doivent être condamnées par les tribunaux *parce qu'elles menacent l'intégrité du système de justice lui-même* : p. 696-697.

[63] En pareilles situations, soit dans le cas où les tactiques policières d'usurpation d'identité vont à l'encontre de la conception de la décence et du franc-jeu au sein de notre société, les tribunaux devraient invoquer les mécanismes de common law existants pour régir les opérations policières d'infiltration, y compris celles menées en ligne. Ainsi, la doctrine de l'abus de procédure offre une protection contre la conduite coercitive de la police, par exemple dans un cas où l'on miserait sur les points vulnérables de l'accusé, ce qui aurait pour effet de compromettre l'équité du procès et l'intégrité du système de justice : *Hart*, par. 111-118. En outre, si la police fait plus que fournir une occasion de commettre une infraction et qu'elle incite véritablement à sa perpétration, la doctrine de la provocation policière s'applique : *Mack*, p. 964-966. En effet, les tribunaux ont eu recours à cette doctrine pour examiner en profondeur des opérations d'infiltration semblables à celle utilisée en l'espèce : voir *R. c. Chiang*, 2012 BCCA 85, 286 C.C.C. (3d) 564, par. 14-21; *R. c. Bayat*, 2011 ONCA 778, 108 O.R. (3d) 420, par. 15-23. Dans de tels cas, les juges du procès jouissent d'« un grand pouvoir discrétionnaire pour accorder réparation, y compris l'exclusion de la preuve et l'arrêt des procédures » : *Hart*, par. 113; voir également *R. c. Babos*, 2014 CSC 16, [2014] 1 R.C.S. 309, par. 30-47 et 53-57.

[64] Par ailleurs, ma conclusion suivant laquelle la *Charte* ne commande pas d'autorisation judiciaire préalable à la participation d'agents d'infiltration à des

conversations en ligne de ce type n'empêche pas le Parlement d'adopter des dispositions législatives pour régir ces opérations. De fait, compte tenu de l'omniprésence des communications électroniques et de la perspective d'une surveillance policière accrue en ligne, un régime législatif pourrait fournir des indications utiles sur la façon appropriée d'utiliser — et de faire rapport sur — les techniques policières d'infiltration visant à prévenir les cybercrimes et à enquêter sur ceux-ci.

[65] En conclusion, il n'y a eu aucune violation de l'art. 8 lorsque les policiers ont communiqué avec M. Mills et ont utilisé « Snagit » pour conserver le relevé écrit des conversations. Les captures d'écran de celles-ci constituaient donc des éléments de preuve admissibles. Je rejeterais le pourvoi.

Version française des motifs rendus par

LE JUGE MOLDAVER —

[66] Bien que mes collègues les juges Karakatsanis et Brown exposent des motifs distincts pour rejeter le pourvoi, chaque série de motifs est, à mon avis, bien fondée en droit et sert de fondement valable pour confirmer l'ordonnance de la Cour d'appel de Terre-Neuve-et-Labrador ayant rejeté l'appel de M. Mills.

[67] En conséquence, je souscris au résultat auquel ils arrivent et je rejetterais également le pourvoi.

Version française des motifs rendus par

LA JUGE MARTIN —

## I. Introduction

[68] La réglementation de l'Internet, lequel est en constante évolution, présente de nombreux défis pour les législateurs et les tribunaux, et exige un juste équilibre entre les droits et les intérêts.

[69] L'exploitation sexuelle d'un mineur est un acte odieux que dénonce fortement la société canadienne, y compris notre Cour. Dans un contexte numérique, les adultes qui exploitent des enfants et des jeunes dans un but sexuel peuvent gagner leur confiance grâce à des identités anonymes ou fausses et peuvent s'immiscer dans leur domicile plus facilement que jamais, à partir de n'importe où dans le monde. Les enfants et les jeunes sont donc particulièrement vulnérables sur Internet et ont besoin de protection.

[70] Le législateur a pris des mesures pour contrer les risques particuliers que pose la prédation sexuelle en ligne, notamment au moyen de l'art. 172.1 du *Code*

*criminel*, L.R.C. 1985, c. C-46. Les outils de la criminalité deviennent de plus en plus perfectionnés, et il doit en être de même pour les techniques des forces de l'ordre. Les acteurs de l'État doivent disposer de pouvoirs d'enquête qui leur permettront d'enrayer efficacement et en amont l'exploitation sexuelle en ligne des enfants.

[71] Cependant, de tels pouvoirs d'enquête doivent être contrebalancés par l'obligation de l'État de respecter les droits au respect de la vie privée de ses citoyens. Le Parlement a pris des mesures à cet égard en adoptant une loi qui prévoit les situations où l'État doit obtenir une autorisation judiciaire pour avoir accès à certains types de communications privées (voir la partie VI du *Code criminel*, « Atteintes à la vie privée »). Cependant, les dispositions pertinentes de la partie VI ont été adoptées avant l'utilisation massive des moyens modernes de communication électronique, qui peuvent produire un relevé écrit des conversations.

[72] Il s'agit en l'espèce de décider si l'État devrait pouvoir exercer, sans mandat, une surveillance des communications électroniques privées, ou si une telle surveillance par l'État devrait être réglementée. À mon humble avis, la protection des enfants contre l'exploitation sexuelle en ligne, bien qu'elle soit essentielle, n'exige pas que l'État assure une surveillance *non réglementée* des communications électroniques privées des membres du public. Pour les motifs qui suivent, je conclus que les membres de la société s'attendent raisonnablement à ce que l'État ne prenne pas connaissance, à son entière discrétion, de leurs communications électroniques privées. Si la police veut prendre connaissance d'un relevé de ces communications,

dans le but légitime et d'une importance capitale d'empêcher la commission de crimes sexuels contre les jeunes, de telles activités d'enquête doivent être réglementées. C'est au législateur de décider de la nature précise d'une telle réglementation.

[73] Par conséquent, même si l'État devrait avoir pleins pouvoirs pour empêcher les prédateurs sexuels de s'en prendre à des enfants et à des jeunes en ligne, les communications électroniques privées des membres de la société ne doivent pas faire l'objet d'une surveillance non réglementée, par l'État, afin que celui-ci puisse parvenir à ces fins.

## II. Faits pertinents

[74] En 2012, des membres du groupe de lutte contre l'exploitation des enfants de la Royal Newfoundland Constabulary, dont faisait partie l'agent Hobbs, ont mené une opération d'infiltration avec l'intention de mettre la main sur des cyberprédateurs. Le 28 février 2012 et le 12 mars 2012, l'agent Hobbs a créé un compte courriel et un profil Facebook afin de se faire passer pour une adolescente de 14 ans à qui il a donné le nom de « Leann Power ». L'agent Hobbs a déclaré qu'il ne connaissait aucun manuel de politique concernant ce type d'enquête et que le choix de ses tactiques d'enquête était laissé à sa discrétion. Dans le profil Facebook qu'il a créé au nom de « Leann », l'agent Hobbs a indiqué que « Leann » habitait à St. John's et qu'elle fréquentait une école secondaire locale. Il y a ajouté une photo obtenue sur Internet comme photo de profil de « Leann ». Bien que l'agent Hobbs n'ait envoyé



aucune « demande d'amitié », il a reçu et accepté de telles demandes, qui lui ont été faites en raison du lien que « Leann » avait avec l'école secondaire locale (voir (2013), 343 Nfld. & P.E.I.R. 128, par. 3-4 et 40 (« décision relative à l'art. 8 »)).

[75] Le 20 mars 2012, l'agent Hobbs a reçu un message Facebook de M. Mills. Au cours des deux mois suivants, M. Mills a échangé plusieurs messages Facebook et courriels avec « Leann ». Finalement, M. Mills a été arrêté dans un parc public où il avait organisé une rencontre avec « Leann ». Il a été accusé de quatre chefs d'accusation de leurre en vertu de l'art. 172.1 du *Code criminel* (décision relative à l'art. 8, par. 1 et 5-10).

### III. Admissibilité des communications électroniques entre M. Mills et « Leann »

[76] M. Mills a contesté l'admissibilité des communications électroniques échangées entre lui et « Leann » pour deux motifs : d'une part, il a soutenu que la police n'avait pas respecté l'art. 184.2 du *Code criminel* car elle n'avait pas obtenu l'autorisation pour intercepter des communications privées, et d'autre part, que l'action de l'État constituait une fouille et une saisie abusives en contravention de l'art. 8 de la *Charte*.

[77] Mes collègues ont conclu que M. Mills n'avait aucune attente raisonnable au respect de sa vie privée à l'égard de ses communications avec « Leann ». Sans une telle attente, il n'y avait pas de fouille. De plus, le juge Brown conclut que l'art. 184.2

du *Code criminel* ne s'applique pas à l'affaire qui nous occupe, alors que la juge Karakatsanis estime qu'il est inutile d'examiner la question.

[78] Soit dit en tout respect, je ne souscris pas à ces conclusions. M. Mills avait une attente raisonnable au respect de sa vie privée à l'égard des communications en cause, et la surveillance de ces communications privées par l'État constituait donc une fouille. Qui plus est, l'utilisation du logiciel de capture d'écran « Snagit » par la police était régie par l'art. 184.2 du *Code criminel* : l'agent Hobbs a intercepté des communications privées lorsqu'il a utilisé « Snagit » pour enregistrer ses échanges avec M. Mills en temps réel. Il devait donc obtenir l'autorisation prévue à l'art. 184.2. Comme il ne l'a pas fait, l'agent Hobbs a porté atteinte au droit à la vie privée que l'art. 8 de la *Charte* garantit à M. Mills. De plus, même si l'agent Hobbs avait décidé de ne pas utiliser un logiciel de saisie d'écran externe, sa technique d'enquête aurait quand même pu constituer une « interception » pour l'application de l'art. 184.2.

[79] Cependant, l'admission en preuve des communications en cause n'est pas susceptible de déconsidérer l'administration de la justice aux termes du par. 24(2) de la *Charte*. Je serais donc d'avis de rejeter le pourvoi.

#### IV. Attente raisonnable au respect de la vie privée à l'égard des communications électroniques privées

[80] L'attente raisonnable au respect de la vie privée est de nature normative, et non descriptive (*Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 159-160; *R. c.*

*Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 42; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579, par. 14; *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212, par. 18; *R. c. Reeves*, 2018 CSC 56, par. 28). La question qu’il faut se poser consiste donc à savoir si le droit à la vie privée revendiqué doit [TRADUCTION] « être considéré comme à l’abri de toute intrusion par l’État — sauf justification constitutionnelle — pour que la société canadienne demeure libre, démocratique et ouverte » (*R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 320, par. 87).

[81] Pour répondre à cette question dans le contexte du présent pourvoi, il faut commencer par examiner la décision de notre Cour dans *R. c. Duarte*, [1990] 1 R.C.S. 30.

A. *L’affaire Duarte constitue le point de départ*

[82] Il y a de cela tout juste trente ans, notre Cour a conclu que la surveillance électronique participative clandestine par l’État devait être réglementée (*Duarte* et l’arrêt connexe, *R. c. Wong*, [1990] 3 R.C.S. 36). Dans *Duarte*, une conversation de groupe au sujet d’une affaire de cocaïne avait été enregistrée clandestinement avec le consentement de deux des parties à la conversation — un indicateur et un agent d’infiltration. Lorsqu’un participant à une conversation enregistre clandestinement cette conversation ou consent à ce que la conversation soit enregistrée clandestinement, il s’agit de « surveillance participative ». À l’époque, l’al. 178.11(2)a) du *Code criminel* permettait aux parties à une conversation d’exercer une surveillance électronique participative sans mandat. Se fondant sur une analyse

normative du droit à la vie privée, le juge La Forest a conclu que tous les membres de la société ne peuvent pas être exposés au risque que la police exerce une surveillance sans mandat, à sa seule discrétion. Il a en outre conclu que ce principe s'applique tout autant dans le cas de la surveillance participative. Par conséquent, la surveillance électronique participative sans mandat par l'État contrevient à l'art. 8 de la *Charte*.

[83] Essentiellement, l'enregistrement électronique clandestin, par l'État, de communications privées a suscité un droit à la vie privée dans l'affaire *Duarte* parce que l'enregistrement d'une communication transforme les propos éphémères de son auteur en preuve documentaire. Par conséquent, l'enregistrement en tant que tel « annihile le droit extrêmement important [. . .] de choisir nos auditeurs » (p. 51). Le juge Harlan, dissident dans *United States c. White*, 401 U.S. (1971), p. 787-789, et cité dans l'arrêt *Duarte*, p. 54, a exprimé cette inquiétude lorsqu'il a parlé du risque de devoir « se reporter à des notes écrites » de nos pensées privées. Le risque que ces propos éphémères soient consignés par écrit et de façon permanente est évoqué dans deux des plus importants énoncés de principe de l'arrêt *Duarte* :

[l]a réglementation de la surveillance électronique nous protège plutôt contre un risque différent : non plus le risque que quelqu'un répète nos propos, mais le danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos (p. 44, je souligne);

le droit reconnaît que nous devons par la force des choses assumer le risque posé par le "rapporteur", mais refuse d'aller jusqu'à conclure que nous devons en outre supporter, comme prix de l'exercice du choix d'adresser la parole à un autre être humain, le risque que soit fait un enregistrement électronique permanent de nos propos (p. 48, je souligne).

[84] Le problème relatif à l'enregistrement des communications privées soulevé dans *Duarte* tirait son origine de la conviction que, si les membres du public croyaient qu'ils s'exposaient, chaque fois qu'ils ouvrent la bouche, au risque qu'un relevé écrit de leurs communications soit produit afin d'être utilisé par l'État à son entière discrétion, la protection de la vie privée contre l'intrusion de l'État n'existerait plus et la notion de liberté de pensée et d'expression se trouverait en fait dénuée de sens (p. 44). Depuis 1990, il est donc accepté que le fait de laisser l'État libre de procéder à une telle surveillance électronique sans qu'elle soit réglementée reviendrait à renoncer à notre liberté : « la liberté de ne pas être obligé de partager nos confidences avec autrui est la marque certaine d'une société libre » (p. 53).

[85] En réponse à l'arrêt *Duarte*, le législateur a réglementé la surveillance électronique participative menée par l'État (*R. c. Pires*, 2005 CSC 66, [2005] 3 R.C.S. 343, par. 8). Selon l'article 184.2 actuel du *Code criminel*, si l'État cherche à « intercepter une communication privée », il doit au préalable obtenir une autorisation judiciaire, même si l'une des parties à la communication a consenti à son interception.

#### B. *Duarte* à l'ère du numérique

[86] Le présent pourvoi, [TRADUCTION] « c'est l'affaire *Duarte* à l'ère du numérique » (m.a., par. 69). Dans *Duarte*, l'État avait pu obtenir accès à un relevé écrit de communications privées au moyen de matériel d'enregistrement. Or de nos jours, les gens communiquent souvent par le truchement de médias électroniques, de sorte que leurs conversations sont nécessairement enregistrées. Si les technologies

intrusives se trouvaient autrefois entre les mains de l'État, elles se trouvent maintenant dans notre poche arrière.

[87] Comme l'a précisé le juge La Forest dans *Wong*, les principes établis dans *Duarte* ne doivent pas viser seulement le moyen technologique en cause dans cette décision. Au contraire, *Duarte* portait sur « tous les moyens actuels permettant à des agents de l'État de s'introduire électroniquement dans la vie privée des personnes, et tous les moyens que la technologie pourra à l'avenir mettre à la disposition des autorités chargées de l'application de la loi » (*Wong*, p. 43-44). L'atteinte commise à l'aide d'un moyen électronique qui était au cœur de l'arrêt *Duarte* résidait dans la violation du droit de choisir ses auditeurs et, parallèlement, dans le fait que l'État ait entre ses mains des notes écrites de nos pensées privées. L'arrêt *Duarte* a défini ce danger comme étant celui que l'État enregistre et transmette nos propos, mais cette violation de la vie privée peut se présenter sous plusieurs formes.

[88] En l'espèce, nous avons l'occasion d'appliquer les principes normatifs de *Duarte* et de *Wong* au regard de la jurisprudence récente de notre Cour portant sur l'art. 8 de la *Charte* et sur la partie VI du *Code criminel* — plus particulièrement, *Patrick*; *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *Spencer*; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696; et *Reeves*. L'objectif est de parvenir à une position qui, tout en étant solidement ancrée dans la jurisprudence, « évolue[...] au rythme du progrès technologique et, par conséquent,

nous assure[...] une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés » (*Wong*, p. 44).

[89] Le risque dont il était question dans *Duarte* était que l'État puisse prendre connaissance, sans surveillance judiciaire, des relevés reproduisant les pensées privées de citoyens, que ceux-ci n'ont pas choisi de divulguer. À la fin de la guerre froide, pour obtenir un *relevé* en temps réel d'une conversation, il fallait *enregistrer* cette conversation. Aujourd'hui, pour ce faire, il suffit de participer à cette conversation. Notre Cour doit décider si le principal sujet de préoccupation dans l'arrêt *Duarte* — la consignation des conversations — est toujours pertinent, et le cas échéant, de quelle façon il l'est, dans les affaires où a) le mode de communication génère lui-même un relevé de la communication, et b) l'auteur de la communication *sait* que cela se produit. Cette évolution des technologies de communication permet-elle maintenant à l'État d'avoir accès, à son entière discrétion, aux conversations en ligne privées des gens, ce qui menace nos principes les plus chers de protection de la vie privée?

[90] À mon avis, il faut répondre à cette question par la négative. Notre Cour doit définir le droit à la vie privée que l'arrêt *Duarte* et les décisions rendues dans sa foulée visaient à protéger et faire en sorte que ce droit demeure protégé au fil de l'évolution du monde de la communication. Ce droit à la vie privée est le droit d'être protégé contre un accès clandestin de l'État aux relevés de nos pensées privées, sans

aucune supervision judiciaire. Pour que ce droit à la vie privée soit protégé, il a été conclu dans *Duarte* que l'accès de l'État aux enregistrements électroniques de communications privées doit être réglementé. Une évolution des moyens de communication ne devrait pas avoir pour conséquence que l'État n'ait plus besoin d'autorisation pour prendre clandestinement connaissance des relevés écrits de nos communications privées. S'il en était autrement, « il ne nous resterait rien qui vaille de notre droit de vivre libre de toute surveillance » (*Duarte*, p. 44).

C. *Il est objectivement raisonnable de s'attendre à ce que l'État ne prenne pas connaissance, à son entière discrétion, de relevés de conversations privées*

[91] L'accès non réglementé de l'État aux communications électroniques privées fait intervenir l'art. 8 de la *Charte* parce que les communications électroniques modernes ressemblent aux enregistrements électroniques clandestins qui ont suscité une attente raisonnable au respect de la vie privée dans *Duarte*. Bien que les communications électroniques présentent le même caractère informel et immédiat que les conversations de vive voix, elles ont également pour caractéristiques la permanence, la fiabilité probatoire et la transmissibilité qui définissent les enregistrements électroniques. Elles constituent une forme de « notes écrites » (*Duarte*, p. 54, citant *White*, p. 787 à 789) auxquelles l'État cherche à avoir accès. Ainsi, pour que la « liberté de ne pas être obligé de partager nos confidences avec autrui » (*Duarte*, p. 53) conserve un sens, l'accès par l'État aux enregistrements électroniques de nos communications privées doit être réglementé. Par conséquent, il était objectivement raisonnable pour M. Mills de s'attendre à ce que l'État ne prenne



pas connaissance sans mandat des enregistrements électroniques permanents de ses communications privées. L'action de l'État dont il est question en l'espèce constituait une fouille au sens de l'art. 8 de la *Charte*.

[92] Dans l'arrêt *Duarte*, le juge La Forest a établi une distinction entre deux différentes catégories d'activités de l'État : « [u]ne conversation avec un indicateur n'est pas une fouille, une perquisition ou une saisie au sens de la *Charte*. Toutefois, l'interception et l'enregistrement électroniques clandestins d'une communication privée en sont » (p. 57; voir aussi *R. c. Fliss*, 2002 CSC 16, [2002] 1 R.C.S. 535, par. 12). Dans ses motifs, ma collègue la juge Karakatsanis compare les messages échangés entre M. Mills et « Leann » aux « conversation[s] avec un indicateur » dont il était question dans *Duarte* (par. 42 et 48). À son avis, les messages échangés entre M. Mills et l'agent Hobbs sont comparables à une conversation de vive voix, et l'art. 8 de la *Charte* n'entre pas en jeu.

[93] Soit dit en tout respect, j'estime que lorsque l'on considère la distinction qui a été établie entre une « conversation » et un « enregistrement » à la lumière du droit à la vie privée que l'arrêt *Duarte* visait à protéger, il devient évident que, dans l'affaire qui nous occupe, les communications électroniques en cause étaient *à la fois* la conversation *et* l'enregistrement électronique clandestin de cette conversation. Cette dualité devrait étayer, et non miner, la protection des droits à la vie privée, puisqu'un enregistrement existe et que l'État dispose d'un accès non réglementé et sans restriction à celui-ci.

[94] Notre Cour s'est déjà prononcée sur le caractère hybride de la messagerie texte. Dans *TELUS*, la juge Abella a déclaré que la messagerie texte « présente plusieurs caractéristiques de la communication orale traditionnelle : elle se veut un moyen de conversation, la transmission du message est généralement instantanée et l'on s'attend à ce que la communication demeure privée » (par. 1). Plus loin dans ses motifs, la juge Abella a relevé une distinction entre la messagerie texte et les communications orales : « contrairement aux communications orales, les communications textuelles — qui sont, de par leur nature, des écrits — génèrent un document qui peut facilement être copié et conservé » (par. 34). La messagerie texte est donc une « conversation électronique » (*TELUS*, par. 5). Bien qu'elles puissent posséder le caractère immédiat et la spontanéité d'une « simple conversation », les communications électroniques génèrent aussi de par leur nature un relevé écrit permanent<sup>1</sup> de la communication elle-même. Dans ses motifs concordants dans *Marakah*, le juge Rowe a tiré une conclusion similaire : les communications numériques « crée[nt] [...] un historique qui échappe à notre contrôle » et, parallèlement, possèdent une « qualité de conversation » qui font en sorte qu'elles « s'apparentent à une conversation numérique » (par. 86-87). Si la dichotomie établie dans l'arrêt *Duarte* reposait sur la consignation, il s'ensuit que les communications électroniques jouent sur les deux plans. Elles s'entendent à la fois de la conversation de vive voix et de l'enregistrement électronique de cette conversation.

---

<sup>1</sup> Si toutes les communications électroniques génèrent un relevé écrit de la conversation, ce ne sont pas toutes les communications électroniques qui génèrent un relevé écrit *permanent*, p. ex. « Snapchat ». Néanmoins, la nature générale des communications électroniques demeure et il faut en tenir compte : « [l]es différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l'étendue de la protection accordée aux communications privées » (*TELUS*, par. 5).

(1) L'importance de créer l'enregistrement nous-mêmes

[95] Comme le dit la juge Karakatsanis, il ne fait aucun doute que, « [n]on seulement les utilisateurs du courriel et de Facebook messenger sont au fait de l'existence d'un relevé écrit permanent de leurs communications, mais ils créent en fait eux-mêmes ce relevé » (par. 48). Le fait que les interlocuteurs soient conscients que leurs communications sont enregistrées, et qu'ils créent eux-mêmes sciemment le relevé de celles-ci, ne signifie pas que les communications électroniques modernes doivent être comparées à la « conversation de vive voix » dont il était question dans *Duarte* ou qu'elles réduisent à néant toute attente raisonnable au respect de la vie privée à l'égard de ces communications.

[96] Lorsqu'il a établi une distinction entre la communication orale et l'enregistrement, le juge La Forest a cité l'arrêt *Holmes c. Burr*, 486 F.2d 55 (1973), p. 72 : [TRADUCTION] « Peu d'entre nous parleraient franchement si nous savions que tous nos propos sont interceptés par des machines en vue de leur diffusion ultérieure devant un auditoire inconnu et peut-être hostile. Personne ne parle à un magnétophone comme il parle à un être humain » (*Duarte*, p. 50). Si j'adapte l'arrêt *Duarte* à l'ère numérique, il demeure que personne ne parle à un magnétophone comme il parle à un être humain. Pourtant, de nos jours, les gens « parlent à un magnétophone » chaque fois qu'ils envoient un message électronique. Cela signifie-t-il qu'il n'est plus objectivement raisonnable de s'attendre à ce que nos conversations demeurent privées simplement parce qu'elles sont maintenant (la

plupart du temps) enregistrées? Notre Cour a conclu que la réponse est non. La création de relevés électroniques écrits de ses communications privées est pratiquement une condition à laquelle il faut consentir pour participer à la société, et pourtant, les « Canadiens n'ont pas à vivre en reclus du monde numérique afin de pouvoir conserver un semblant de vie privée » (*Jones*, par. 45). En dépit du fait que les technologies modernes peuvent enregistrer des communications électroniques, les gens ont encore des attentes, subjectives et objectives, au respect de leur vie privée à l'égard de ces communications (*TELUS*, par. 32; transcription, p. 59).

[97] De plus, le fait d'avoir conscience que la conversation est consignée n'invalide pas nécessairement le caractère objectivement raisonnable de l'attente selon laquelle l'État n'aura pas accès à ces relevés. Cette attente est de nature normative, non descriptive. Comme l'a écrit la juge Renee M. Pomerance dans son ouvrage « Flirting with Frankenstein: The Battle Between Privacy and Our Technological Monsters », (2016) 20 *Can. Crim. L. Rev.* 149, p. 159 :

[TRADUCTION]

Les citoyens peuvent être prêts à renoncer à leurs libertés civiles s'ils croient qu'ils seront ainsi plus en sécurité. Peut-être sont-ils résignés [à l'absence] de vie privée pour des raisons de commodité. Peut-être sont-ils résignés à l'absence de vie privée parce qu'ils sont conditionnés à croire que nous vivons déjà dans une société de surveillance. Aucune de ces attitudes ne devrait à elle seule dicter notre démarche juridique. Les droits et libertés ne doivent pas être définis en fonction de la peur ou du fatalisme.

[98] Dans *Duarte*, le danger inhérent à la capacité de l'État de créer des enregistrements électroniques de nos propos, n'importe quand et sans aucune justification, était que la société finisse par s'attendre à ce que l'État agisse ainsi. Selon le juge La Forest, une société où nous sommes exposés au risque d'une surveillance électronique non réglementée « chaque fois que nous ouvrons la bouche » (*Duarte*, p. 44) est une société qui n'a plus aucun sens de la liberté (*Duarte; R. c. Wise*, [1992] 1 R.C.S. 527, p. 565, le juge La Forest). L'intervenante, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, a abordé la question de [TRADUCTION] « l'atteinte qui serait portée à la liberté d'expression s'il fallait présumer que l'interlocuteur est un agent d'infiltration de l'État qui crée un relevé de la conversation électronique » (m.i., p. 9), citant le passage suivant de l'ouvrage d'Alan Westin, qui porte sur les débuts de l'ordinateur (*Privacy and Freedom* (1967), p. 349) :

[TRADUCTION]

Le danger que cet essor présentait pour la vie privée et pour les libertés [. . .] était que ceux qui savaient que tous ces renseignements étaient recueillis, stockés dans des machines et faciles d'accès, ne pourraient jamais savoir quand ils seraient utilisés « contre eux » et à quelles fins. Cette conscience du public quant à l'utilisation potentielle des renseignements recueillis se traduirait par des « comportements davantage empreints de "retenue" » et par une moins grande liberté d'action et d'expression. Les gens se soucieraient non seulement du fait qu'ils sont « enregistrés », mais aussi de la façon dont cet enregistrement serait « perçu » par les autorités qui en prendraient connaissance. L'objectif même de la protection de la vie privée [. . .] est de permettre aux gens d'avoir des comportements libérateurs sans contrainte et en toute liberté, et c'est précisément cet exutoire que menace notre système de dossiers informatiques.

Le juge Harlan a exprimé la même idée comme suit : [TRADUCTION] « [c]’est l’évidence même que l’on pèserait bien davantage ses mots et que la communication en serait gênée si l’on soupçonnait que les conversations étaient transmises et transcrites » (*White*, p. 787-789, cité dans *Duarte*, p. 54)

[99] Cinquante ans après l’arrêt *White*, de plus en plus d’auteurs publient des articles à ce sujet qui corroborent l’avis du juge Harlan. De nombreuses études empiriques ont confirmé l’« effet paralysant » de la surveillance gouvernementale sur les comportements en ligne. Ces études indiquent que la surveillance électronique par l’État incite les gens à exercer l’autocensure sur leur expression en ligne (J. W. Penney, « Internet surveillance, regulation, and chilling effects online: a comparative case study » (2017), 6:2 *Internet Policy Review* 22 (en ligne); A. Marthews et C. Tucker, « The Impact of Online Surveillance on Behavior » dans D. Gray et S. E. Henderson, dir., *The Cambridge Handbook of Surveillance Law* (2017) 437.

[100] De savoir qu’à tout moment et pour n’importe lequel de nos propos, il nous faudrait composer avec le fait que l’État ait en sa possession des notes écrites de ces propos aurait pour conséquence rien de moins que l’« anéantissement » (*Duarte*, p. 44) total de notre sens de la vie privée. C’est pourquoi la Cour a décidé, dans l’arrêt *Duarte*, que si l’État voulait prendre connaissance des relevés des pensées privées de ses citoyens, il aurait besoin d’une autorisation judiciaire préalable.

(2) « Destinataire visé »

[101] La juge Karakatsanis affirme qu'« il n'est pas raisonnable de s'attendre à ce que le destinataire visé d'un message n'en prenne pas connaissance » (par. 36). Cette proposition générale ne s'applique pas, et ne peut s'appliquer, lorsque l'État a secrètement fait en sorte d'être le destinataire visé. Il ressort clairement de l'arrêt *Duarte* que, dans le cas d'une surveillance participative de l'État, la notion de « destinataire visé » — ainsi que de la qualification de « la personne ou [d]es personnes auxquelles nous [. . .] destinons [nos propos] » (motifs de la juge Karakatsanis, par. 50, citant *Duarte*, p. 47) — est intimement liée au droit de choisir ses auditeurs. Même si, dans *Duarte*, les « destinataires de la conversation » étaient l'agent d'infiltration et l'indicateur, M. Duarte avait toujours une attente raisonnable au respect de sa vie privée à l'égard du contenu de cette conversation, parce que le recours par la police à du matériel d'enregistrement violait son droit de ne pas avoir à composer avec le risque que des notes écrites soient entre les mains de l'État. Par analogie, la personne qui participe à une conversation électronique privée peut raisonnablement s'attendre à ce que l'État n'ait accès à un enregistrement électronique permanent de cette communication privée que si l'agent de l'État a obtenu une autorisation judiciaire. Les attentes normatives n'ont pas changé. La différence, évidemment, c'est que nous utilisons maintenant des technologies qui font elles-mêmes l'enregistrement.

[102] Je souligne que le présent pourvoi porte sur les communications électroniques et sur la capacité auto-incriminante inhérente à celles-ci de créer un relevé de communications qui seront bien souvent spontanées, informelles. Il ne porte

pas sur les intérêts en matière de vie privée à l'égard d'une note, d'une lettre ou d'autres formes de communication, qui ont leurs propres caractéristiques (motifs de la juge Karakatsanis, par. 45; *Marakah*, par. 86, le juge Rowe; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 24).

(3) Distinctions quantitatives et qualitatives entre la surveillance en personne et la surveillance électronique par l'État

[103] Je me dois de faire deux autres observations sur la nature de la surveillance électronique. D'abord, les « conversations » sur lesquelles notre Cour s'est penchée dans *Duarte* ne sauraient faire l'objet d'une comparaison directe avec les communications électroniques d'aujourd'hui, parce que les conversations de vive voix avec des agents d'infiltration dont il était question dans cette affaire n'étaient pas susceptibles d'exposer le public à une surveillance électronique clandestine à grande échelle.

[104] Dans une société libre et démocratique, les gens ne s'attendent pas à ce qu'un grand nombre de personnes avec lesquelles ils interagissent soient des agents d'infiltration de la police qui les surveillent « à leur guise » (*Duarte*, p. 44 et 49). Si un tel scénario paraît inconcevable dans un contexte d'opération d'infiltration en personne, en raison de contraintes pratiques liées aux ressources dans le cas des activités d'infiltration policière, il devient parfaitement concevable dans le cas des technologies de surveillance électronique : [TRADUCTION] « la surveillance est devenue la principale activité directrice de la nouvelle modernité, et différents



moyens technologiques sont utilisés pour surveiller et gouverner diverses catégories de gens (citoyens, automobilistes, travailleurs, étudiants, consommateurs, voyageurs internationaux, adversaires militaires, prestataires d'aide sociale et autres groupes) » (K. D. Haggerty, « Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance » (2009), 17 *Critical Crim.* 277, p. 277-278; voir aussi D. Lyon, *Surveillance After Snowden* (2015), p. 47 : [TRADUCTION] « les câbles et les conduites de l'Internet [. . .] rendent la surveillance de masse possible comme jamais auparavant »).

[105] Il s'agit, en partie, d'une question de ressources. Alors qu'une opération d'infiltration en personne s'effectue normalement selon un rapport de 1 : 1 (un agent de police qui gagne la confiance d'une cible), la surveillance en ligne peut ratisser beaucoup plus large. Un seul agent de police peut mener plusieurs conversations électroniques à la fois. Par conséquent, le nombre de conversations électroniques que pourraient avoir les agents d'infiltration avec des membres du public, à un moment donné, est susceptible d'être plus élevé que le nombre de conversations que ces mêmes agents pourraient avoir en personne.

[106] L'analogie entre une conversation de vive voix et une communication électronique est intenable non seulement à cause de l'augmentation quantitative de la capacité de surveillance lorsqu'il est question de surveillance en ligne, mais aussi en raison de la distinction qualitative qu'il y a entre la surveillance électronique clandestine et la surveillance en personne. L'agent Hobbs n'aurait pas pu faire ce

travail policier en personne. Se créer d'autres identités n'a jamais été aussi facile que maintenant. Il va de soi qu'à cause de cet aspect de la communication électronique, il est encore plus nécessaire de surveiller le cyberspace en vue de mettre au jour les activités criminelles qui se multiplient en raison de cet anonymat. Or, ce même anonymat permet une surveillance par l'État d'un tout autre ordre, alors que les policiers peuvent créer plus facilement de fausses identités, très élaborées, donc plus crédibles, sous le couvert desquelles ils exercent leur surveillance. Les policiers ont toute discrétion pour exercer une surveillance électronique — vu que « lorsque des agents d'infiltration de la police communiquent par écrit avec des individus, il n'y a aucune “fouill[e]” ou “saisi[e]” » (motifs de la juge Karakatsanis, par. 36) — de sorte qu'ils [TRADUCTION] « pourraient se faire passer pour un fournisseur de services thérapeutiques en ligne en vue de connaître les dépendances d'une personne, ou encore pour un fournisseur de services de rencontre en ligne en vue de découvrir les préférences sexuelles d'une personne — et ce, pendant des semaines ou des mois » (m.i., Criminal Lawyers' Association, par. 4). Lorsque, comme en l'espèce, un policier peut se faire passer pour un enfant et gagner la confiance d'autres enfants — ou lorsque, par exemple, un policier peut prétendre être un fournisseur de services thérapeutiques ou de services de rencontre en ligne sous le couvert d'une fausse identité très élaborée — c'est que la nature de la surveillance a changé. Nos protections en matière de vie privée doivent évoluer au même rythme.

[107] Dans ses motifs, la juge Karakatsanis affirme que « [l]a menace d'opérations d'infiltration menées par des policiers sans scrupules » s'apparente à une

menace à l'intégrité du système de justice en tant que tel (par. 62). Elle s'intéresse à des mécanismes comme l'abus de procédure et la doctrine de la provocation policière afin que les tactiques policières de ce type soient corrigées (par. 62-63). Je suis d'accord pour dire que les mesures policières qui « enfrein[ent] nos valeurs fondamentales » (*Rothman c. La Reine*, [1981] 1 R.C.S. 640, p. 689, le juge Lamer) peuvent et doivent être corrigées de diverses façons, pour le bien de tous. Cependant, lorsque de telles actions de l'État vont aussi à l'encontre d'une attente raisonnable au respect de la vie privée, elles doivent être examinées, notamment, au regard de l'art. 8 de la *Charte*. En l'espèce, ce ne sont pas seulement les actions d'un policier qui sont en litige, mais aussi la règle générale qui devrait régir la façon dont l'État peut avoir accès aux communications privées à l'aide des technologies actuelles. À mon avis, exclure les communications de la portée de l'art. 8 parce que l'État destinataire peut maintenant obtenir un relevé de la conversation simplement en y prenant part nuit à l'objet des droits à la vie privée, et perturbe le juste équilibre entre la capacité de l'État d'enquêter sur des crimes et les droits des personnes de disposer d'espaces privés pour s'exprimer.

[108] Dans l'arrêt *Duarte*, il était question des conséquences sur la vie privée du fait que l'État, à son entière discrétion, avait pris connaissance d'enregistrements électroniques permanents de communications privées. Les communications électroniques s'entendent des conversations qui ont lieu sur des plateformes pouvant, de par leur nature, créer des enregistrements électroniques permanents. Si l'État

souhaite prendre connaissance du relevé de ces communications, il doit obtenir une autorisation.

D. *La question de la relation*

[109] Mon collègue le juge Brown fonde sa décision dans le présent pourvoi sur le fait qu'il n'y a pas d'attente raisonnable au respect de la vie privée lorsque l'État réalise une opération d'infiltration et qu'il sait dès le départ que l'adulte accusé communique avec un enfant qu'il ne connaît pas (par. 22-23). Alors que la conclusion du juge Brown se rattache au contexte d'infiltration, son raisonnement s'appliquerait chaque fois que les facteurs « crucia[ux] » qu'il a établis sont présents, c'est-à-dire que l'accusé « communiquait avec une personne qu'il croyait être une enfant et qui était une inconnue pour lui » (par. 22).

[110] Soit dit en tout respect, je ne peux accepter que cette nouvelle catégorie de « relation » est nécessaire pour limiter les situations où il y a attente raisonnable au respect de la vie privée. De fait, ce concept de « relation » repose sur deux idées qui ont déjà été rejetées par notre Cour. D'abord, le concept de « relation » est en fait un indicateur de « contrôle » et est fondé sur le raisonnement relatif à l'analyse de risques que notre Cour a rejeté. Ensuite, la « relation » est aussi utilisée pour cibler les activités illégales, et n'est donc pas neutre sur le plan du contenu. Au-delà de ces conflits avec la jurisprudence portant sur l'art. 8, il y a, au cœur de ce raisonnement, la position normative selon laquelle une relation entre un adulte et un enfant qui lui est inconnu n'est pas digne de jouir de la protection conférée par l'art. 8 (voir le

par. 26 des motifs du juge Brown). Cette position vise à imposer aux tribunaux la tâche d'évaluer les relations personnelles des Canadiens afin de décider lesquelles sont dignes de jouir de la protection conférée par l'art. 8 de la *Charte*, et lesquelles ne le sont pas. Le point qui est préoccupant ici est que non seulement cela ne s'est encore jamais fait, mais que par principe dans le contexte de l'art. 8, cela ne devrait pas se faire du tout. L'approbation (ou la désapprobation) par les tribunaux du mode de vie d'un accusé n'a pas sa place dans le cadre d'une analyse du droit à la vie privée au regard de l'art. 8.

[111] La Cour ne devrait pas créer de zones soustraites à l'application de la *Charte* à l'égard de certaines communications électroniques privées des gens au motif qu'ils sont peut-être des criminels dont les relations ne sont pas socialement valables. La *Charte* confère expressément à « chacun » les protections garanties à l'art. 8. Les membres de la société s'attendent raisonnablement à ce que l'État ne prenne pas connaissance, à son entière discrétion, de leurs communications électroniques privées.

[112] Enfin, la conclusion qu'il y a attente raisonnable au respect de la vie privée à l'égard d'une chose ou d'un lieu précis ne signifie pas qu'il est interdit à l'État d'effectuer une fouille; cela signifie simplement que les actions des policiers doivent être validées par un pouvoir ou une autorisation qui respecte l'art. 8 de la *Charte*. À mon avis, le scénario présenté, soit celui où l'État prétend, dans un contexte d'infiltration, être un enfant et communique avec des gens qui cherchent à sexualiser des enfants, est précisément le type de situation dans laquelle l'État

pourrait et devrait obtenir une autorisation judiciaire pour surveiller des communications électroniques privées.

(1) La relation comme indicateur de contrôle

[113] Mon collègue le juge Brown affirme qu'il n'est pas raisonnable qu'un adulte s'attende au respect de sa vie privée lorsqu'il communique avec un enfant vulnérable qui lui est inconnu parce qu'espérer qu'une personne qu'on ne connaît pas du tout gardera les communications secrètes est un « pari » qui ne peut être à l'origine d'une attente raisonnable au respect de la vie privée (voir les par. 22-23 des motifs du juge Brown). Autrement dit, M. Mills ne pouvait raisonnablement s'attendre à ce que sa vie privée échappe à la surveillance électronique clandestine et sans mandat par l'État parce qu'il n'exerçait pas un *contrôle* suffisant sur ce que son interlocuteur ferait avec ces communications.

[114] Soit dit en tout respect, cette position réintroduit l'analyse de la « perte de contrôle causée par un risque de divulgation » que notre Cour a récemment rejetée dans *Marakah*. L'analyse relative à une attente raisonnable au respect de la vie privée porte sur l'intrusion de l'État. Le risque qu'un interlocuteur divulgue une communication privée n'a pas d'incidence sur le caractère raisonnable de l'attente selon laquelle l'État, s'il n'y a pas eu de telle divulgation, ne s'immiscera pas dans cette communication privée. Pour cette raison, la théorie de la perte de contrôle causée par un risque de divulgation constitue le genre d'analyse du risque qui, comme l'a maintes fois répété notre Cour, ne devrait pas faire partie de l'analyse fondée sur

l'art. 8 (*Duarte*, p. 44; *Wong*, p. 45-46; *Wise*, p. 563-564, le juge La Forest, dissident, mais pas sur ce point; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211, par. 34, la juge Deschamps, dans ses motifs concordants; *Cole*, par. 58; *Marakah*, par. 45; *Reeves*, par. 50; voir aussi *Ward*, par. 77; *R. c. Craig*, 2016 BCCA 154, 335 C.C.C. (3d) 28, par. 108).

[115] Le rejet de l'analyse du risque par notre Cour n'a jamais été lié à la nature de la relation entre les parties. Dans *Marakah*, par exemple, les juges majoritaires n'ont pas analysé la relation entre MM. Winchester et Marakah, parce que cela n'était pas utile quant à la question de savoir si M. Marakah pouvait raisonnablement s'attendre à ce que l'État n'ait pas accès, sans mandat, à ses messages textes à partir de l'appareil d'un destinataire. Par conséquent, le rejet dans *Marakah* de l'analyse du risque, au par. 40, était un énoncé de principe général applicable à tous les examens concernant les attentes raisonnables au respect de la vie privée à l'égard de communications électroniques, y compris l'examen devant être entrepris dans l'affaire qui nous occupe :

La Couronne prétend que M. Marakah a perdu tout contrôle sur la conversation électronique avec M. Winchester parce que ce dernier aurait pu la divulguer à des tiers. Cependant, le risque que des destinataires divulguent les messages textes qu'ils reçoivent ne change rien à l'analyse (*Duarte*, p. 44 et 51; *Cole*, par. 58). Accepter le risque qu'un interlocuteur divulgue une conversation électronique ne revient pas à accepter le risque différent que l'État s'immisce dans une conversation électronique non divulguée. « La réglementation de la surveillance électronique nous protège contre un risque différent : non plus le risque que quelqu'un répète nos propos, mais le danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos » (*Duarte*, p. 44). En conséquence, le risque qu'un

destinataire divulgue une conversation électronique n'exclut pas une attente raisonnable en matière de respect de la vie privée à l'égard de cette conversation. [Je souligne.]

[116] L'analyse relative à l'attente raisonnable au respect de la vie privée est axée non pas sur la question de savoir si la partie avec laquelle une personne a communiqué est susceptible d'aller voir la police — « [a]ucune législation ne pourrait nous mettre à l'abri de ce risque » (*Duarte*, p. 44). Elle est plutôt axée sur la question de savoir si, faute d'une telle divulgation, il est raisonnable de s'attendre à ce que la police ne s'immisce pas dans ces communications sans mandat ou autre forme d'autorisation.

(2) La relation comme moyen de cibler les actes illégaux

[117] Mon collègue le juge Brown conclut qu'étant donné que notre Cour s'est prononcée sur la vulnérabilité des enfants, sur le fait qu'Internet puisse faciliter la commission de crimes sexuels contre les enfants et sur la nécessité de protéger les enfants contre l'exploitation sexuelle, il s'ensuit que « les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas » (par. 23). Soit dit avec le plus grand respect, je ne peux interpréter cette conclusion autrement que comme visant les activités illégales et privant des droits à la vie privée les personnes qui, pourrait-on croire, sont les plus susceptibles de prendre part à ce type d'activité illégale. Le rôle central que joue le contexte de l'opération d'infiltration dans l'analyse de mon collègue ne fait qu'accentuer ce constat : une opération d'infiltration — par définition



— vise des activités illégales. Par conséquent, la conclusion selon laquelle « les adultes ne peuvent pas raisonnablement s’attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu’ils ne connaissent pas » est contraire au principe fondamental de la neutralité de contenu qui est au cœur de la jurisprudence relative à l’art. 8 de notre Cour.

[118] Pour l’application de l’art. 8, le fait qu’une personne puisse adopter un comportement criminel en ligne ne change pas l’analyse de l’attente raisonnable au respect de la vie privée. Notre Cour a affirmé de façon constante que « [l]a nature de l’intérêt en matière de vie privée ne dépend pas de la question de savoir si, dans un cas particulier, le droit à la vie privée masque une activité légale ou une activité illégale. En effet, l’analyse porte sur le caractère privé du lieu ou de l’objet visé par la fouille ou la perquisition ainsi que sur les conséquences de cette dernière pour la personne qui en fait l’objet, et non sur la nature légale ou illégale de la chose recherchée » (*Spencer*, par. 36; *Hunter*, p. 160; *Wong*, p. 49-50; *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569, par. 72; *Patrick*, par. 32; *Marakah*, par. 48). Pour cette raison, l’analyse relative à l’attente raisonnable au respect de la vie privée doit se faire « en termes plus généraux et plus neutres » (*Wong*, p. 50).

[119] Devant notre Cour, la Couronne reconnaît que, dans l’arrêt *Marakah*, les juges majoritaires ont conclu que l’analyse relative à l’attente raisonnable au respect de la vie privée doit être neutre sur le plan du contenu. Elle a cependant demandé à la

Cour d'écarter cette approche dans tous les cas où les communications électroniques [TRADUCTION] « constituent un acte criminel visant le destinataire » (m.i., par. 56)

[120] En affirmant que « les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas », le juge Brown accède dans les faits à la demande de la Couronne de conclure qu'une « exception limitée » (m.i., par. 50) s'applique à l'analyse neutre sur le plan du contenu qu'utilise notre Cour. En toute déférence, rien ne justifie en l'espèce de déroger à un principe bien établi et à la jurisprudence récente. Ce n'est pas la première fois que la Cour est appelée à élaborer des règles de droit en matière de respect de la vie privée dans le contexte des crimes sexuels commis à l'endroit de mineurs sur Internet ou à l'aide de la technologie numérique (voir p. ex. *Cole, Spencer et Reeves*). La Cour n'a pas jugé bon d'écarter l'analyse neutre sur le plan du contenu dans ces affaires, et il ne convient pas davantage qu'elle le fasse en l'espèce.

[121] Selon le raisonnement habituel qui sous-tend l'importance d'une analyse neutre sur le plan du contenu, la justification d'une fouille en fonction du contenu illégal découvert lors de cette fouille mine le système d'autorisation judiciaire préalable visant à empêcher les fouilles non justifiées avant qu'elles n'aient lieu (voir *Hunter*, p. 160). Le juge Brown cherche à dissiper cette préoccupation en ciblant seulement les personnes qui, selon lui, méritent d'être fouillées parce que leurs relations ne sont pas de celles que notre société souhaiterait protéger d'un examen par

l'État — en l'espèce, les adultes qui communiquent en ligne avec des enfants qu'ils ne connaissent pas.

[122] Cette approche part du principe que les communications entre des adultes et des enfants qui ne se connaissent pas sont de nature criminelle. En réalité, cela n'est pas inévitable. La catégorie générale des « relations entre des adultes et des enfants qui leur sont inconnus » englobe les relations pédagogiques informelles et d'une importance capitale qui peuvent se créer dans le cyberspace. Cette large portée est donc excessive et comprendrait tout un éventail de communications non criminelles : par exemple, les professionnels qui communiquent avec des jeunes pour leur donner des conseils en matière de carrière, ou les adultes qui, parce qu'ils ont vécu des expériences semblables, pourraient fournir du soutien aux jeunes qui sont aux prises avec une dépendance, qui ont des questionnements au sujet de leur identité sexuelle ou qui vivent de l'intimidation. Un adulte qui fait part à un jeune de sa propre expérience, lors de communications électroniques privées entre étrangers, pourrait faire toute une différence dans la vie de ce jeune. S'il n'y a pas d'attente raisonnable au respect de la vie privée à l'égard de telles communications parce qu'un adulte communique avec un enfant qui lui est inconnu, l'État pourrait alors écouter et enregistrer les communications sans que cette surveillance soit réglementée ou limitée, et sans que l'État ait besoin d'une autorisation pour ce faire. Le principe de la neutralité du contenu a été élaboré pour faire en sorte que de telles atteintes injustifiées de l'État à la vie privée ne se produisent pas.

[123] À mon avis, et conformément au raisonnement du juge Binnie dans *A.M.*, la position voulant que « les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas » fait que l'analyse se détourne d'une attente « raisonnable » au respect de la vie privée au profit d'une attente « légitime » au respect de la vie privée. L'opinion selon laquelle certaines relations sont à première vue criminelles et ne suscitent donc pas *légitimement* d'attente au respect de la vie privée suppose à la fois qu'il y a criminalité alors qu'il n'y en a peut-être pas, et qu'il ne peut y avoir aucun droit raisonnable au respect de la vie privée à l'égard des communications illégales. Ces deux postulats sont erronés (*A.M.*, par. 69-73).

[124] Enfin, comme je l'explique en détail plus loin dans les présents motifs, la police a procédé, dans le cas qui nous occupe, à une surveillance en ligne non réglementée d'un nombre inconnu de jeunes qui croyaient parler à une personne de leur âge. Par conséquent, les faits de l'espèce ne dépeignent pas le scénario qu'évoque mon collègue — scénario où seuls les criminels sont privés de la protection de leur vie privée.

[125] Il faut garder à l'esprit que la question n'est pas de savoir si un enfant qui a été victime peut aller voir la police pour lui montrer une communication en ligne qu'il a reçue. Il s'agit plutôt de savoir si l'État peut prétendre être un enfant dans des communications privées en ligne, à son entière discrétion et sans qu'une telle démarche soit réglementée. À mon avis, l'État ne devrait pas être libre de le faire.

- (3) Les tribunaux ne devraient pas avoir la tâche de décider quelles relations personnelles sont visées par l'art. 8 de la *Charte*

[126] Au-delà de mes préoccupations concernant la neutralité du contenu, je signale aussi que la position normative voulant que « les adultes ne peuvent pas raisonnablement s'attendre au respect de leur vie privée dans leurs communications en ligne avec des enfants qu'ils ne connaissent pas » exige que les tribunaux procèdent à une évaluation inutile et non fondée sur des principes des relations personnelles alors que ce facteur n'est pas utile pour l'analyse fondée sur l'art. 8. De plus, même si l'évaluation des relations personnelles par les tribunaux pour décider lesquelles sont dignes d'être protégées contre un examen sans mandat de l'État concorde avec l'analyse fondée sur l'art. 8, les tribunaux sont mal outillés pour réaliser une telle évaluation. Soulever des doutes au sujet d'une catégorie entière de relations humaines ne fait pas que stigmatiser de telles relations; cela expose aussi des communications utiles et socialement valables à une surveillance électronique par l'État, qui n'est pas réglementée. Pour toutes ces raisons, je suis d'avis que les tribunaux ne devraient pas recourir à l'art. 8 pour permettre à l'État de s'immiscer dans certaines relations personnelles qui sont considérées comme n'étant pas dignes de jouir de la protection conférée par la *Charte*.

[127] Je dis cela tout en reconnaissant que les juges majoritaires de notre Cour ont affirmé dans *Patrick* que « [l]'analyse du droit au respect de la vie privée abonde en jugements de valeur énoncés du point de vue indépendant de la personne raisonnable et bien informée, qui se soucie des conséquences à long terme des actions

gouvernementales sur la protection du droit au respect de la vie privée » (par. 14). Cependant, la nécessité d'effectuer des « jugements de valeur » ne permet pas aux tribunaux de procéder à une évaluation libre de toute contrainte des personnes accusées et de leurs relations. La *Charte* a plutôt eu pour effet d'obliger les tribunaux à faire des jugements de valeur *se rapportant aux objets de l'analyse relative à l'art. 8 elle-même*. Ces objets sont « le caractère privé du lieu ou de l'objet visé par la fouille, ainsi que [ . . . ] les conséquences potentielles de la fouille pour la personne qui en fait l'objet » (*Patrick*, par. 32). Sur ce fondement, notre Cour s'est demandé si les membres de la société peuvent s'attendre au respect de leur vie privée à l'égard de leurs sacs à dos à l'école (*A.M.*); de leurs communications par message texte, que ce soit dans le cadre d'une fouille accessoire à une arrestation (*R. c. Fearon*, 2014 CSC 77, [2014] 3 R.C.S. 621) ou dans l'appareil du destinataire (*Marakah*); de leur ordinateur dans leur propre maison (*Vu; Reeves*); d'une voiture dont ils ne sont pas propriétaires (*R. c. Belnavis*, [1997] 3 R.C.S. 341); et de la distribution relative de la chaleur sur la surface de leur résidence (*Tessling*).

[128] L'analyse relative à l'art. 8 n'est pas, et n'a jamais été, axée sur la question de savoir si une relation entre deux personnes qui n'agissent pas au nom de l'État est digne de jouir de la protection constitutionnelle. Par exemple, l'arrêt *R. c. Dymont*, [1988] 2 R.C.S. 417, ne portait pas sur les relations. Dans cette affaire, l'atteinte à la vie privée consistait en « l'utilisation du corps d'une personne sans son consentement, en vue d'obtenir des renseignements à son sujet » (p. 431-432).

[129] La valeur d'une relation personnelle n'est pas non plus un objet ou un aspect pertinent d'une analyse fondée sur l'art. 8. Le législateur a expressément prévu que la protection conférée par l'art. 8 s'applique à « chacun » : « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » Soit dit en tout respect, ce n'est pas le rôle des tribunaux d'évaluer les relations personnelles en vue de priver certaines catégories de personnes de la protection que confère l'art. 8 de la *Charte*. En fait, en tant que protecteurs de la *Charte*, les tribunaux « constituent souvent la seule protection efficace des minorités impopulaires et des individus contre les revirements de la passion publique » (*R. c. Collins*, [1987] 1 R.C.S. 265, p. 282, citant D. Gibson, *The Law of the Charter: General Principles*, (1986), p. 246).

[130] De plus, le fait de créer des zones soustraites au droit à la vie privée pour des relations précises exposera des communications socialement valables à la surveillance non réglementée de l'État. Comme je l'ai déjà expliqué, de nombreuses communications dignes de jouir de la protection conférée par l'art. 8 seraient visées par la catégorie des « adultes qui communiquent avec des enfants qui leur sont inconnus ».

[131] Pour toutes ces raisons, un virage dans notre jurisprudence relative à l'art. 8 qui obligerait les tribunaux à se pencher sur les relations personnelles entre les parties afin qu'ils décident si les droits au respect de la vie privée doivent être respectés ou refusés est en conflit avec l'objet de l'art. 8. Un tel virage sanctionne dans les faits l'intrusion injustifiée de l'État dans de grands pans de la vie privée de

toute personne en vue d'obtenir quelques communications illégales. Cette approche est contraire à la décision qu'a prise notre pays, soit que les communications privées doivent demeurer privées, sauf si l'État a l'autorisation de procéder à une fouille.

(4) Conclusion sur la question de la relation

[132] Notre Cour a toujours rejeté d'adopter la méthode d'analyse fondée sur le risque, et effectue plutôt des analyses fondées sur l'art. 8 qui sont neutres sur le plan du contenu en examinant la conduite de l'État en question. Dans l'affaire qui nous occupe, la question à laquelle il faut répondre lorsqu'on procède à l'analyse de l'attente raisonnable au respect de la vie privée n'est pas de savoir si les adultes qui communiquent en ligne avec des inconnus d'âge mineur au cours d'opérations d'infiltration policières fondées sur un pseudonyme ont une attente raisonnable au respect de leur vie privée à l'égard de leurs communications électroniques privées. Il s'agit plutôt de savoir si les membres de la société peuvent raisonnablement s'attendre à ce que l'État ne prenne pas connaissance, à son entière discrétion, des relevés de leurs communications électroniques privées (voir *Patrick*, par. 32).

E. *Conclusion sur l'attente raisonnable au respect de la vie privée*

[133] Dans une société libre et démocratique, il est raisonnable pour les membres de la société de s'attendre à ce que l'État n'ait accès aux enregistrements électroniques de leurs communications privées que s'il a obtenu l'autorisation de le faire. Il en va de même pour la surveillance participative des communications privées.



D'aucuns peuvent trouver difficile d'accepter que cette attente raisonnable au respect de la vie privée s'applique aussi à M. Mills, mais elle s'applique bel et bien : « [i]l ne faut pas se demander quels risques ont été pris par la personne qui invoque la *Charte*, mais plutôt quels risques devraient lui être imposés dans le cadre d'une société libre et démocratique » (*Reeves*, par. 41; *Duarte*, p. 52; *Spencer*, par. 36; *Patrick*, par. 32; *Wise*, p. 567). En l'espèce, la surveillance policière constituait une fouille au sens de l'art. 8 de la *Charte*.

V. Autorisation visée à la partie VI

[134] Je conviens avec l'appelant que [TRADUCTION] « l'utilisation de “Snagit” pour prendre des captures d'écran des messages répond à la définition d'“interception” prévue à l'art. 183 du *Code criminel*, en ce que ce programme a permis d'enregistrer et de prendre volontairement connaissance de la substance des textos » (m.a., par. 48; voir aussi décision relative à l'art. 8, par. 34). J'examinerai plus à fond la question de savoir si les actions de l'agent Hobbs auraient pu également constituer une interception même sans le recours à « Snagit ». Cette dernière analyse soulève la question de savoir si, compte tenu des nouvelles technologies de communication, il convient de revoir notre régime législatif qui permet l'interception de communications privées. Je laisse cet examen au bon jugement du législateur.

A. *M. Mills avait-il une attente raisonnable au respect de sa vie privée à l'égard de ses communications?*

[135] Pour que l'art. 184.2 s'applique à une technique d'enquête donnée, il faut que l'État cherche à intercepter une « communication privée ». Une « communication privée » est une « [c]ommunication orale ou télécommunication [. . .] qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers » (art. 183 du *Code criminel*). Cette définition prévoit que l'auteur devait avoir une attente raisonnable au respect de sa vie privée à l'égard de ses communications. Pour les motifs exposés ci-dessus, M. Mills avait une attente raisonnable au respect de sa vie privée à l'égard de ses communications. Les communications en cause constituaient donc des « communications privées » au sens de l'art. 183 du *Code criminel*.

B. *L'utilisation de « Snagit » constituait-elle une interception?*

[136] L'article 184.2 du *Code criminel* s'applique aux communications qui ont été « interceptées » au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre. « Intercepter » s'entend « du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet » (art. 183 du *Code criminel*). Avec égards pour l'opinion contraire, je conclus que l'utilisation de « Snagit » dans l'affaire qui nous occupe constituait une interception.

[137] L'agent Hobbs a enregistré ses conversations avec M. Mills à l'aide d'un logiciel [TRADUCTION] « qui permet à son utilisateur de faire des captures d'écran des renseignements apparaissant à l'écran et de les enregistrer » (décision relative à

l'art. 8, par. 6). Interrogé quant aux raisons pour lesquelles il avait utilisé ce logiciel, l'agent Hobbs a répondu : [TRADUCTION] « pour assurer une continuité, pour conserver [les messages] ensemble aux fins de reproduction à l'intention des tribunaux, au besoin » (D.A., vol. II, p. 7). Il a déclaré qu'il n'avait en aucun temps imprimé les messages directement à partir des programmes originaux, mais qu'il « les avait toujours sauvegardés au moyen d'une capture d'écran » (p. 8). L'agent Hobbs a en outre expliqué que : « chaque personne a sa propre façon de faire les choses. C'est simplement celle que je préfère et j'ai toujours trouvé qu'elle était la plus avantageuse. Elle permet de tout conserver au même endroit. Je peux tout stocker dans un même dossier de mon ordinateur » (p. 8). Selon le sens ordinaire du mot « enregistrer », l'agent Hobbs a enregistré le contenu informationnel des communications privées lorsqu'il les a « sauvegardées au moyen d'une capture d'écran » à un seul endroit de son ordinateur « aux fins de reproduction à l'intention des tribunaux » (p. 7-8). Il s'agissait là d'une interception (voir aussi *R. c. Kwok*, [2008] O.J. n° 2414 (QL) (C.J.)).

[138] Dans la présente affaire, l'interception a eu lieu en « temps réel » (*Jones*, par. 69). Il ressort de l'analyse du sens du mot « intercepter » à laquelle notre Cour s'est livrée dans *Jones*, que « la notion d'interception suggère l'idée d'une autorisation prospective visant des communications qui n'existent pas encore. Le verbe “intercepter” évoque une interposition entre l'expéditeur et le destinataire dans le cours du processus de communication » (*Jones*, par. 69; voir aussi *TELUS*, par. 37). Ainsi, la partie VI établit un cadre réglementaire visant à ce que

l'interception en temps réel de communications à venir soit autorisée. Je conviens avec l'appelant que, pour cette raison également, la partie VI s'applique à l'action de l'État en l'espèce (m.a., par. 59). L'agent Hobbs a reçu les communications et les a simultanément enregistrées au moyen d'un logiciel de capture d'écran. On est loin des messages textes existants en cause dans l'arrêt *Jones*. Si l'agent Hobbs avait demandé l'autorisation pour procéder à ces interceptions en temps réel, il aurait demandé l'autorisation pour intercepter des communications non encore existantes. L'action de l'État, en l'espèce, est donc conforme à l'interprétation que notre Cour a donnée au terme « interception » dans *Jones*.

[139] J'ajouterai que, contrairement à ce que la Cour d'appel a conclu (au par. 13) et à ce que certains autres tribunaux d'appel et auteurs ont conclu également (2017 NLCA 12; voir aussi *R. c. Blais*, 2017 QCCA 1774, par. 16-17 (CanLII), *R. c. Beairsto*, 2018 ABCA 118, 349 C.C.C. (3d) 376, par. 25), une « interception » peut se faire sans tiers. Ce que notre Cour a dit au sujet des actes accomplis par un tiers dans l'arrêt *Jones* (par. 72) ne s'applique pas aux cas de surveillance participative ou aux paramètres de l'art. 184.2 du *Code criminel*. Le législateur a adopté l'art. 184.2 actuel en réponse à l'arrêt *Duarte*, qui portait sur une affaire de surveillance participative — l'agent d'infiltration et l'indicateur étaient des *participants* à la conversation. Il y a eu « interception » dans cette affaire non pas parce qu'un tiers avait intercepté la communication, mais parce que le matériel d'enregistrement de l'État l'avait interceptée. C'est l'analyse à laquelle s'est livré à juste titre le juge du procès (décision relative à l'art. 8, par. 17 et 23).

[140] Enfin, la conclusion selon laquelle l'action de l'État en l'espèce constituait une « interception » est compatible avec « l'objectif sous-jacent » de la partie VI (*Jones*, par. 59; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 R.C.S. 27, par. 21). La partie VI vise l'utilisation de moyens technologiques intrusifs en vue de la surveillance des communications privées (*Jones*, par. 73; *Duarte*, p. 43-44). En employant un logiciel de capture d'écran, l'agent Hobbs a utilisé un moyen technologique en vue de surveiller les communications privées de M. Mills, de les enregistrer et d'en prendre connaissance en temps réel et, ce faisant, il a violé le droit de M. Mills de choisir ses auditeurs (*Duarte*, p. 51).

C. *L'utilisation clandestine par l'État de moyens électroniques pour communiquer avec des membres du public dans un contexte privé peut constituer une interception*

[141] Dans le monde actuel des communications, nous nous mettons nous-mêmes sous écoute électronique. Nous transmettons sciemment non seulement aux destinataires prévus, mais aussi aux dépôts de données numériques de sociétés tierces parties, une preuve documentaire de nos communications privées. Pourtant, cela ne nous prive pas du droit d'être protégés contre l'intrusion de l'État dans notre vie privée. S'agissant du régime législatif qui régit les intrusions de l'État dans la vie privée, la partie VI doit tenir compte de ces complexités. Cela comprend ses éléments constitutifs, tels que la définition d'« intercepter » : « [l]a question consiste donc à interpréter le mot “intercepter” à la partie VI. L'interprétation de ce mot doit se fonder non seulement sur les objectifs de la partie VI, mais aussi sur les droits

garantis par l'art. 8 de la *Charte*, lesquels doivent progresser au rythme de la technologie » (*TELUS*, par. 33).

[142] La définition du mot « intercepter » que prévoit la loi est le « fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ». En communiquant avec M. Mills sur un support qui produit par lui-même un enregistrement électronique<sup>2</sup>, l'agent Hobbs « a pris connaissance » d'un relevé de la communication. Il est vrai que, si l'on met de côté la question du logiciel « Snagit », l'agent Hobbs a seulement profité de la technologie dont se servait déjà M. Mills. Or tout comme l'affaire *Duarte* ne portait pas seulement sur l'*enregistrement* de la conversation, mais aussi sur l'acquisition par l'État d'un *relevé d'une communication*, l'art. 184.2 ne vise pas seulement les technologies intrusives qui permettent une *interposition* dans nos communications privées (*Jones*, par. 69); il vise aussi la fonction des technologies intrusives par laquelle elles peuvent *avoir accès* à nos communications privées : « La partie VI reconnaît les dangers inhérents au fait de permettre l'accès aux futures communications privées d'un nombre potentiellement illimité de personnes pendant une longue période » (*TELUS*, par. 42). Les membres du public doivent être protégés contre la collecte clandestine et non réglementée, par l'État, de leurs communications

---

<sup>2</sup> Il convient de noter, cependant, que dans la présente affaire, la preuve documentaire inhérente produite grâce à la communication sur Facebook et Hotmail n'est pas celle qui a été présentée au procès. Les seuls messages copiés par l'agent Hobbs sont ceux qu'il a obtenus à l'aide de « Snagit ». Il avait désactivé le compte Facebook de « Leann » lorsque M. Mills a été accusé des infractions qui sont portées devant notre Cour. Quant aux relevés des conversations produits du côté de M. Mills, la fouille effectuée sur le disque dur de ce dernier n'a permis d'obtenir que des fragments des communications, et la valeur probante de chacun d'eux reposait sur une comparaison avec la capture d'écran intégrale obtenue au moyen de « Snagit ». Les seules communications pouvant être reproduites étaient celles sous forme de capture d'écran.

électroniques privées. Il se peut donc que la surveillance des communications privées en ligne de M. Mills, avec ou sans logiciel de capture d'écran, ait constitué le type de surveillance clandestine, par l'État, au moyen d'une technologie intrusive, que la partie VI vise à interdire.

[143] Si, par ailleurs, la surveillance électronique clandestine par la police de communications privées n'est régie que par la partie VI, dans la mesure où un logiciel externe d'enregistrement est employé, alors notre « régime complet [. . .] en vue de l'interception de communications privées » (*TELUS*, par. 2) n'est plus assez complet. Pour être constitutionnelle, la prise de connaissance en temps réel, par l'État, de communications électroniques privées doit être réglementée.

D. *La partie VI établit un juste équilibre entre la nécessité pour les forces de l'ordre d'enquêter sur les crimes et le droit des individus vivant dans une société démocratique de ne pas être importunés*

[144] Je partage l'avis de l'intervenante, la procureure générale de l'Ontario, pour dire que l'Internet a créé [TRADUCTION] « une plateforme sans précédent pour l'exploitation d'enfants », et qu'il est nécessaire de mener des opérations d'infiltration policières proactives pour lutter contre l'exploitation en ligne des enfants (m.i., p. 7-9; voir aussi G. J. Fitch, c.r., « Child Luring » dans *Substantive Criminal Law, Advocacy and the Administration of Justice*, vol. 1, document présenté au National Criminal Law Program (2007), p. 1 et 3). La partie VI du *Code criminel* a été élaborée à la lumière de ces considérations. À mon avis, son application à l'emploi du logiciel « Snagit » dans l'affaire qui nous occupe établit un juste équilibre entre la nécessité

pour les forces de l'ordre d'enquêter sur les crimes et le droit des individus vivant dans une société démocratique de ne pas être importunés. Si la police souhaite exercer une surveillance électronique clandestine à l'aide d'un moyen technologique intrusif, elle doit faire autoriser sa méthode d'enquête par une cour de justice ou une autre tierce partie indépendante.

[145] Je ne juge pas convaincant l'argument selon lequel les cyberprédateurs passent si rapidement d'une victime à l'autre qu'il serait [TRADUCTION]« inacceptable » de suspendre une enquête le temps d'obtenir une autorisation judiciaire (m.i., Association canadienne des chefs de police, p. 6-8). Notre système judiciaire est en mesure de délivrer les autorisations nécessaires en temps opportun. Chaque jour au pays, des policiers obtiennent des mandats dans des délais serrés. Les mots du juge La Forest dans l'arrêt *Duarte*, p. 52-53, sont ici pertinents :

. . . [I]mposer l'exigence de l'obtention d'un mandat aurait pour seul effet d'obliger la police à limiter la "surveillance participative" aux cas où elle peut démontrer l'existence de raisons plausibles d'obtenir un mandat. Je vois mal en quoi la capacité de la police de combattre efficacement le crime serait diminuée si elle était tenue de limiter le recours à cette pratique aux situations dans lesquelles elle peut convaincre un officier de justice impartial de sa nécessité. Même à supposer que ce soit le cas, la restriction se justifierait par la certitude que la police n'aurait plus le droit [TRADUCTION] "de braquer ces puissants appareils d'écoute sur vous et moi et sur d'autres citoyens respectueux des lois en même temps que sur l'élément criminel", pour reprendre les propos du juge Cirillo dans *Commonwealth v. Schaeffer*, [536 A.2d 354 (Penn. 1987)], p. 367.



Ou encore, comme l'a dit brièvement la juge Karakatsanis au par. 54 de l'arrêt *Reeves* : « Je conviens que rejeter l'approche préconisée par la Couronne pourrait nuire à des enquêtes criminelles, mais c'est souvent ce que font les droits garantis par la *Charte*. »

[146] Je reconnais, cependant, que conclure que la police a « intercepté » les communications même sans l'aide de « Snagit » a des répercussions plus complexes. Il vaut mieux laisser le législateur décider de la norme de raisonabilité qui s'impose en ce qui a trait à l'autorisation judiciaire préalable requise pour procéder à diverses formes d'enquêtes policières proactives. À ce sujet, je tiens à répéter que ma position ne fait pas inexorablement en sorte que la police serait incapable de mener des enquêtes sur les cyberprédateurs, et ne devrait pas avoir cet effet. Elle est plutôt axée sur l'*autorisation* de ces enquêtes par un tiers indépendant. Un régime moins exigeant que celui de la partie VI peut être approprié dans certaines circonstances.

[147] Enfin, concernant les « enquêtes policières proactives » comme celle entreprise dans l'affaire qui nous occupe, je crois qu'une série de lignes directrices uniformisées sur la protection de la vie privée pourraient être utiles. Selon l'agent Hobbs, il n'existait aucune ligne directrice ou politique qui l'aurait aidé à créer une fausse identité la moins attentatoire possible. Il a donc créé lui-même une politique, qui a entraîné des conséquences indésirables. Pour fabriquer son identité virtuelle, l'agent Hobbs s'est servi de photos d'une adolescente qu'il ne connaissait pas, trouvées sur Internet. Cette adolescente a donc participé sans le vouloir à une enquête

policière. Qui plus est, [TRADUCTION] « [i]l y a eu un certain nombre de ce que divers auteurs ont appelé des rencontres “discrètes” entre [l’agent Hobbs] et des personnes innocentes. L’agent s’est servi de leur présence [en ligne] sur sa page Facebook pour donner de la crédibilité à son profil alors que ces personnes lui transmettaient des renseignements, sans savoir qu’il était policier » ((2014), 346 Nfld. & P.E.I.R. 102, par. 10 (« décision relative au par. 24(2) »)). L’agent Hobbs n’a pas tenté d’obtenir ni obtenu le consentement éclairé des personnes qu’il a ajoutées sur sa page Facebook, ces personnes ayant en fait été utilisées comme « appâts » en vue de piéger un cyberprédateur ((2015), 364 Nfld & P.E.I.R. 237, par. 18 (« décision relative à la peine »)). De plus, il n’y avait aucune preuve quant à savoir si, ou comment, la police a conservé les renseignements personnels de l’une ou l’autre de ces personnes (décision relative à la peine, par. 18). Les enquêtes en ligne proactives peuvent être à l’origine d’une surveillance électronique très vaste, de sorte que des personnes innocentes, dont de nombreux jeunes, transmettent sans le savoir des renseignements personnels sensibles à la police. Pour que ces techniques d’enquête soient le moins attentatoires possible, elles doivent être régies par des lignes directrices claires.

#### VI. La fouille constituait-elle une violation de l’art. 8 de la Charte?

[148] Les fouilles, les perquisitions et les saisies sont présumées abusives à moins qu’elles aient été autorisées préalablement par un tribunal. Cependant, la Couronne peut établir, selon la prépondérance des probabilités, que la police a agi de

manière raisonnable, c'est-à-dire que la fouille était autorisée par la loi, que la loi elle-même n'avait rien d'abusif et que la fouille n'a pas été effectuée d'une manière abusive (*Collins*, p. 278). En l'espèce, il n'y a eu aucune autorisation judiciaire préalable, de sorte que la fouille est présumée abusive. La fouille ou la saisie n'était pas autorisée par la loi. Par conséquent, la fouille effectuée à l'égard des communications constituait une violation de l'art. 8 de la *Charte*.

#### VII. La preuve doit-elle être écartée par application du par. 24(2) de la *Charte*?

[149] Après avoir conclu que les droits de M. Mills garantis par l'art. 8 de la *Charte* avaient été violés, le juge du procès a néanmoins rejeté la demande de M. Mills, qui sollicitait l'exclusion de la preuve des communications électroniques par application du par. 24(2). Bien que mon raisonnement diffère à plusieurs égards importants de celui du juge du procès, je conviens avec lui que l'admission de cette preuve n'aurait pas pour effet de déconsidérer l'administration de la justice.

[150] M. Mills soutient que le juge du procès aurait dû aborder la présente affaire comme étant une violation du droit de ne pas s'incriminer. S'il s'agissait là de la position défendue par M. Mills au moment de l'instruction de la demande d'exclusion, alors je conviens que le juge du procès aurait dû se prononcer sur cette question. Or, même s'il s'agissait d'une erreur, celle-ci n'a eu aucun effet sur l'issue de la décision. Dans sa décision relative à la peine, le juge a conclu qu'il ne s'agissait pas d'une affaire de provocation policière (par. 3-8). Ainsi, s'il avait examiné cette

question dans son analyse relative au par. 24(2), le juge du procès aurait conclu que la preuve n'avait pas été obtenue en contravention du droit de ne pas s'incriminer.

[151] Les autres observations de M. Mills concernent le traitement et l'appréciation des facteurs exposés dans l'arrêt *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353, par. 71, qui permettent d'écarter des éléments de preuve en application du par. 24(2). Ces facteurs sont : « (1) la gravité de la conduite attentatoire de l'État [. . .] (2) l'incidence de la violation sur les droits de l'accusé garantis par la *Charte* [. . .] et (3) l'intérêt de la société à ce que l'affaire soit jugée au fond ».

[152] M. Mills soutient que le juge du procès a eu tort de conclure que l'agent d'infiltration avait agi de bonne foi. Il s'agit cependant là d'une conclusion raisonnable que pouvait tirer le juge du procès, après avoir conclu que l'agent [TRADUCTION] « appliquait ce qu'il croyait être une technique d'enquête légitime » (décision relative au par. 24(2), par. 10). Il est préoccupant de constater que l'agent n'a pas cherché à savoir si la technique d'enquête était valide sur le plan constitutionnel, ou s'il devait obtenir une autorisation judiciaire : « il [est] impératif [. . .] de ne pas assimiler la négligence ou l'aveuglement volontaire à la bonne foi » (*Grant*, par. 75). Il est tout aussi préoccupant de constater qu'il ne disposait d'aucune ligne directrice écrite qu'il aurait pu suivre. Je suis cependant d'avis que l'on pardonnera à l'agent Hobbs d'avoir présumé que cette technique était constitutionnelle. L'arrêt de notre Cour *R. c. Levigne*, 2010 CSC 25, [2010] 2 R.C.S. 3, peut être interprété comme une reconnaissance valide de la technique d'enquête

employée en l'espèce<sup>3</sup>. Les parties dans *Levigne* n'ont pas soulevé la question des droits protégés par l'art. 8 de la *Charte* qui est inhérente aux tactiques d'enquête policière employées dans cette affaire, et le silence de notre Cour sur la question dans *Levigne* ne la lie pas maintenant. J'estime néanmoins que, pour cette raison et pour les motifs mentionnés par le juge du procès, ce dernier n'a pas commis d'erreur en concluant que l'agent avait agi de bonne foi. Ce premier facteur milite en faveur de l'admission.

[153] Quant à l'incidence sur les droits de l'accusé garantis par la *Charte*, le juge du procès a conclu que l'attente au respect de la vie privée était réduite parce que [TRADUCTION] « l'accusé communiquait avec un inconnu tout en sachant que ses communications seraient enregistrées sur l'ordinateur de cette personne » (décision relative au par. 24(2), par. 11). C'est pourquoi il a conclu que ce volet de l'analyse militait en faveur de l'admission de la preuve. M. Mills fait valoir que les conclusions du juge du procès vont à l'encontre de la jurisprudence. Je suis de cet avis. Il n'y avait aucune « attente réduite au respect de la vie privée » en l'espèce. Notre Cour a bien précisé que le fait qu'une personne n'ait pas de contrôle sur ses communications ne réduit pas son attente raisonnable en matière de protection contre l'*intrusion de l'État* dans sa vie privée (voir *Duarte*, p. 48; *Marakah*, par. 68). La violation de la *Charte* a eu une incidence importante sur M. Mills : des renseignements biographiques d'ordre privé ont été révélés et soumis à l'examen de la police (*R. c. Plant*, [1993] 3

---

<sup>3</sup> Dans *Levigne*, l'enquêteur a utilisé un logiciel d'enregistrement appelé Camtasia pour enregistrer ses séances de clavardage privées avec l'accusé. Comme l'a déclaré l'agent, Camtasia est [TRADUCTION] « un logiciel qui enregistre essentiellement tout ce qui se passe sur votre écran, comme s'il s'agissait d'une vidéo » (*Levigne*, dossier de l'appelant, p. 113).

R.C.S. 281, p. 293 (un ensemble de renseignements biographiques « pourrait notamment [comprendre des] renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu »); *Cole*, par. 45-46). Ce facteur milite en faveur de l'exclusion.

[154] Quant à l'intérêt de la société à ce que l'affaire soit jugée au fond, le juge du procès a conclu que l'exclusion de la preuve serait [TRADUCTION] « fatale pour la Couronne » et que cette preuve d'« une valeur probante réelle était d'une grande fiabilité » (décision relative au par. 24(2)). En appel devant notre Cour, l'appelant a reconnu que l'infraction reprochée était grave. Toutefois, son avocat demande à la Cour de ne pas accorder [TRADUCTION] « une importance indue » à la gravité de l'infraction (m.a., par. 103-106).

[155] J'estime que l'appréciation des trois facteurs milite en faveur de l'admission de la preuve. En concluant ainsi, je n'accorde pas une « importance indue » à la gravité de l'infraction. Bien que l'atteinte au droit à la vie privée de M. Mills ait eu des répercussions importantes et non réduites, la gravité de l'atteinte à la *Charte* était minime. Je suis d'avis que l'exclusion d'« éléments de preuve pertinents et fiables » dans une affaire de leurre d'enfants, lesquels ont été obtenus au moyen de tactiques que la police avait de bonnes raisons de croire légales au moment de l'enquête, aurait pour effet de déconsidérer l'administration de la justice (*Grant*, par. 81).

[156] Le juge du procès n'a pas commis d'erreur en refusant d'écarter la preuve sur le fondement du par. 24(2), et je confirmerais sa décision selon laquelle la réparation adéquate pour l'atteinte portée à la *Charte* est une réduction de peine de deux mois.

### VIII. Conclusion

[157] Il était objectivement raisonnable pour M. Mills de s'attendre à ce qu'un agent de l'État ne puisse prendre clandestinement connaissance d'un enregistrement électronique permanent de ses communications privées sans autorisation judiciaire préalable. L'utilisation par l'agent Hobbs de « Snagit » constituait une « interception » au sens de la partie VI du *Code criminel*. Qui plus est, il se peut que, même sans « Snagit », la technique d'enquête employée par l'État en l'espèce ait constitué une « interception ». Comme l'agent Hobbs n'a pas cherché à obtenir ni obtenu l'autorisation judiciaire préalable prévue à l'art. 184.2 avant d'utiliser « Snagit », la fouille à l'égard des communications privées en cause était déraisonnable. Toutefois, je n'écarterais pas ces communications sur le fondement du par. 24(2) de la *Charte*.

[158] Le présent pourvoi soulève de sérieuses questions quant à savoir si la surveillance policière de communications électroniques devrait être réglementée et, le cas échéant, de quelle façon elle devrait l'être. Suivant l'abondante série de décisions de notre Cour établissant les principes normatifs de ce qui constitue une attente raisonnable au respect de la vie privée, je conclus que la surveillance non

réglementée, par l'État — en l'espèce, la prise de connaissance non réglementée, par l'État, d'enregistrements électroniques permanents de communications privées — contrevient à l'art. 8 de la *Charte*. Dans la mesure où notre régime législatif qui autorise l'interception de communications privées ne comprend pas les méthodes modernes par lesquelles l'État obtient des enregistrements en temps réel de communications privées, je crois qu'il doit être réexaminé.

[159] Pour les motifs qui précèdent, je suis d'avis de rejeter le pourvoi.

*Pourvoi rejeté.*

*Procureurs de l'appelant : Sullivan Breen King Defence, St. John's;  
Spiteri & Ursulak, Ottawa.*

*Procureur de l'intimée : Department of Justice & Public Safety, Special  
Prosecutions Office, St. John's.*

*Procureur de l'intervenante la directrice des poursuites pénales: Service  
des poursuites pénales du Canada, Toronto.*

*Procureur de l'intervenante la procureure générale de l'Ontario : Crown  
Law Office, Criminal, Toronto.*



*Procureur de l'intervenant le directeur des poursuites criminelles et pénales: Directeur des poursuites criminelles et pénales, Québec.*

*Procureur de l'intervenant le procureur général de la Colombie-Britannique : Ministry of Attorney General, Criminal Appeals and Special Prosecutions, Victoria.*

*Procureur de l'intervenant le procureur général de l'Alberta : Justice and Solicitor General Appeals, Education & Prosecution Policy Branch, Calgary.*

*Procureurs de l'intervenante la Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko : Presser Barristers, Toronto; Markson Law Professional Corporation, Toronto.*

*Procureurs de l'intervenante l'Association canadienne des libertés civiles : Addario Law Group, Toronto.*

*Procureurs de l'intervenante Criminal Lawyers' Association : Stockwoods, Toronto; Ruby, Shiller & Enenajor, Toronto.*

*Procureur de l'intervenante l'Association canadienne des chefs de police : Royal Newfoundland Constabulary Legal Services, St. John's.*