EN COULISSE : PROCÉDURE POUR LES DEMANDES DES FORCES DE L'ORDRE À LA SUITE DE L'AFFAIRE *R C. BYKOVETS*

Publié le 27 mars, 2024

Catégories: Perspectives, Publications

Dans l'affaire *R c. Bykovets* [1], les juges de la Cour suprême du Canada (CSC) ont conclu, à une majorité de 5 contre 4, que les personnes ont une attente raisonnable en matière de respect de la vie privée en ce qui concerne leurs adresses IP et que, par conséquent, les forces de l'ordre doivent obtenir une autorisation judiciaire préalable (mandat de perquisition ou ordonnance de communication, entre autres) pour y avoir accès [2].

La décision de la CSC a des répercussions évidentes pour les forces de l'ordre, mais ses effets sont susceptibles d'être observés par les entreprises. Celles-ci constateront probablement une diminution du nombre de demandes de divulgation volontaire et une augmentation de celui des ordonnances de communication officielles visant à obtenir des renseignements personnels sur les activités de leurs clients sur Internet.

Dans cet article, nous présentons un survol de la décision de la CSC et nous traitons de considérations importantes, en vertu des lois du Canada, relatives à la protection des renseignements personnels lorsqu'il s'agit de déterminer la mesure dans laquelle une entreprise peut communiquer des renseignements personnels sur ses clients aux forces de l'ordre sans le consentement des personnes visées.

Les faits

Au cœur de l'affaire : une fraude impliquant l'utilisation non autorisée de cartes de crédit pour l'achat de cartes-cadeaux. Au cours de son enquête, l'unité des cybercrimes de la police de Calgary a appris que les paiements par carte de crédit étaient gérés par un tiers fournisseur de services de traitement des paiements. La police a demandé les adresses IP associées aux achats frauduleux, et le fournisseur de services de paiement les a volontairement fournies [3]. Ces adresses IP en main, la police a pu déterminer l'identité du fournisseur de services Internet (FSI) du défendeur grâce à des sources accessibles au public. Elle a ensuite obtenu une ordonnance de communication obligeant le FSI à divulguer le nom et l'adresse du client pour chaque adresse IP [4], ce qui a mené à l'arrestation du défendeur et à l'appel qui s'en est suivi devant la CSC.

L'appelant a contesté en faisant valoir que la demande de la police à la société de traitement des paiements en vue d'obtenir les adresses IP avait violé son droit à la protection contre les fouilles, les perquisitions et les saisies

abusives garanti par l'article 8 de la Charte canadienne des droits et libertés (la « Charte ») [5].

L'arrêt de la CSC

La CSC a conclu, à une majorité de 5 contre 4, qu'il existe une attente raisonnable en matière de protection de la vie privée concernant les adresses IP et que, par conséquent, les forces de l'ordre doivent obtenir une autorisation judiciaire préalable afin d'obtenir l'accès à ces renseignements [6].

Dans leur décision, les juges majoritaires soulignent que, pour que l'article 8 de la Charte protège efficacement la vie privée en ligne de la population canadienne, il doit protéger les adresses IP [7]. Pour parvenir à cette conclusion, les juges majoritaires ont porté leur attention au-delà de l'information que révèle une adresse IP directement sur un utilisateur d'Internet. Ils se sont plutôt concentrés sur la possibilité d'une enquête plus approfondie que ne le permet une adresse IP. En ce sens, les juges majoritaires ont conclu que, au-delà d'une simple chaîne de chiffres, l'adresse IP est une clé qui permet de déverrouiller l'activité d'un utilisateur sur Internet [8]. La CSC a qualifié l'adresse IP de « premier fragment numérique » pouvant mener à l'identité d'un individu et, pour cette raison, cette information suscite une attente raisonnable en matière de protection de la vie privée [9].

L'analyse des juges majoritaires a été motivée par le souci que l'architecture de l'Internet offre aux forces de l'ordre la possibilité de contourner les restrictions de la Charte par l'intermédiaire d'une coopération volontaire avec les entreprises du secteur privé.

La Cour a observé que les entreprises en ligne sont bien placées pour compiler d'importantes données sur l'activité des internautes et que les forces de l'ordre leur demandent souvent de divulguer volontairement ces renseignements afin de faciliter les enquêtes criminelles [10]. Il en résulte que le secteur privé pourrait remplacer la Charte en tant qu'arbitre de la capacité du gouvernement à accéder à des renseignements personnels de nature sensible. En concluant à l'existence d'une attente raisonnable en matière de protection de la vie privée concernant les adresses IP, la police devra plutôt obtenir une autorisation judiciaire préalable avant de demander à des tiers d'accéder à ces renseignements [11].

Que doivent répondre les entreprises auxquelles les forces de l'ordre demandent des renseignements sur leurs clients?

Les entreprises faisant affaire au Canada sont soumises aux lois canadiennes sur la protection de la vie privée dans le secteur privé, telles que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ou les dispositions des lois provinciales essentiellement similaires [12].

Les lois canadiennes sur la protection des renseignements personnels exigent généralement que les entreprises obtiennent le consentement de la personne visée quant à la divulgation de ses renseignements

personnels. Toutefois, la LPRPDE énonce certaines exceptions qui permettent la divulgation sans consentement aux forces de l'ordre dans certaines circonstances. Par exemple, la LPRPDE autorise la divulgation sans consentement si elle est faite en réponse à la demande d'une institution fédérale qui indique son pouvoir d'obtenir ces renseignements, ou encore si la divulgation est nécessaire pour se conformer à une citation à comparaître, à un mandat, à l'ordonnance d'un tribunal ou à une ordonnance de communication [13]. La LPRPDE autorise également la divulgation volontaire de renseignements personnels aux forces de l'ordre s'il existe des motifs raisonnables de croire que les renseignements se rapportent à une question de sécurité nationale ou à la perpétration d'un crime ou d'un délit [14].

L'arrêt *Bykovets* se concentre sur la capacité des forces de l'ordre à obtenir de l'information provenant de tiers et n'aborde pas la question de l'obligation de coopérer volontairement lorsqu'ils reçoivent de telles demandes. Cela dit, on peut s'attendre à ce que la décision entraîne une diminution du nombre de demandes de divulgation volontaire et une augmentation de celui des ordonnances de communication.

Bien qu'il soit essentiel pour la sécurité publique de faciliter les enquêtes des forces de l'ordre, il convient de prendre en juste considération la protection du droit à la vie privée des personnes et les exigences des organisations policières en vertu des lois sur la protection de la vie privée [15]. Les entreprises faisant affaire au Canada doivent donc procéder à une évaluation avant de divulguer des renseignements personnels aux forces de l'ordre afin de s'assurer qu'une exception valable s'applique en vertu des lois sur la protection de la vie privée en vigueur.

[1] *R.* c. *Bykovets*, 2024 CSC 6 [« *Bykovets* »].
[2] *Bykovets*, par. 90 et 91.
[3] *Bykovets*, par. 98.
[4] *Bykovets*, par. 98.
[5] *Loi constitutionnelle de 1982*, Annexe B de la *Loi de 1982 sur le Canada (R-U)*, 1982, c 11.
[6] *Bykovets*, par. 91.
[7] *Bykovets*, par. 28.
[8] *Bykovets*, par. 28.
[9] *Bykovets*, par. 9 et 91.
[10] *Bykovets*, par. 10.
[11] *Bykovets*, par. 89.
[12] Les autres principales lois sur la protection de la vie privée au Canada sont énumérées ci-après. En Colombie-Britannique, la *Personal Information Protection Act*,(en anglais) SBC 2003, c.63; en Alberta, la *Personal Information Protection Act*, (en anglais) SA 2003, c. P-6.5; et au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1.

[13] LPRPDE, 7(3)(c); art. 7(3)(d).
[14] LPRPDE, 7(3)(d).
[15] *Bykovets*, par. 11, 71, 86.

par Robbie Grant, Mitch Koczerginski et Ada Ang (stagiaire en droit)

Mise en garde