22 MARS 2024

Des fragments numériques qui tendent à révéler notre identité : la Cour suprême du Canada accorde la protection constitutionnelle aux adresses IP au nom de la vie privée

Auteurs : Léon H. Moubayed, Corey Omer, Alexander Max Jarvie, Alexandra Belley-McKinnon et Amélie Lehouillier

La Cour suprême du Canada a rendu récemment un arrêt de principe sur les droits à la vie privée des internautes dans l'affaire *R. c. Bykovets*. Dans cette affaire, la police a obtenu sans mandat l'adresse de l'*Internet Protocol* (« **IP** ») d'un suspect en s'adressant à un tiers chargé du traitement de paiements dans le cadre d'une enquête pour de prétendues fraudes en ligne. Grâce à l'adresse IP, la police a pu identifier et localiser le suspect, ainsi que demander et exécuter des mandats de perquisition qui ont conduit à l'arrestation du suspect. Le suspect a contesté l'obtention sans mandat des adresses IP, estimant qu'il s'agissait d'une violation de son droit à être protégé contre les perquisitions et saisies abusives prévu à l'article 8 de la *Charte canadienne des droits et libertés* (« **Charte** »).

La majorité de la Cour suprême a statué que les adresses IP font l'objet d'une attente raisonnable au respect de la vie privée et que les forces de l'ordre doivent obtenir un mandat de perquisition pour y avoir accès. La décision de la Cour, qui reconnaît la quantité considérable de renseignements personnels détenus par des entreprises privées et qui rapproche le droit pénal canadien aux attentes des autorités de protection de la vie privée, devrait avoir des conséquences importantes pour le droit à la vie privée en ligne au Canada.

Contexte

L'appelant, Andrei Bykovets, a été reconnu coupable de 14 infractions liées à des achats frauduleux en ligne effectués avec des données de carte de crédit non autorisées après que les policiers aient obtenu les adresses IP associées aux achats auprès de Moneris, une société tierce de traitement qui gérait les ventes en ligne du magasin. Moneris s'est volontairement conformée à la demande de la police et a fourni les adresses IP requises. À l'aide d'informations publiques, la police a pu identifier le fournisseur de services Internet (« **FSI** ») propriétaire des adresses IP pour ensuite obtenir une ordonnance de communication des informations sur les abonnés associées à ces adresses IP. Cette ordonnance de communication a été obtenue conformément aux exigences établies par la Cour suprême dans l'affaire *R. c. Spencer* (« ***Spencer*** »), une décision de 2014 dans laquelle la Cour a reconnu l'existence d'une attente raisonnable en matière de protection de la vie privée couvrant les informations sur les abonnés détenues par les FSI. La police a ensuite utilisé ces renseignements concernant l'abonné pour solliciter et exécuter des mandats de perquisition, qui ont finalement conduit à l'arrestation de Bykovets et à sa condamnation ultérieure.

Bykovets a soutenu que la demande de la police à Moneris pour les adresses IP associées aux achats non autorisés violait ses droits prévus par l'article 8 de la Charte et a demandé que la preuve soit exclue du dossier en vertu de l'article 24(2) de la Charte. Le juge de première instance a estimé qu'il n'y avait pas de violation de l'article 8 et a trouvé Bykovets coupable. La majorité de la Cour d'appel de l'Alberta (2-1) a confirmé la condamnation, estimant que Bykovets n'avait pas d'attente raisonnable en matière de vie privée en ce qui concerne son adresse IP, car une adresse IP ne révèle pas en soi de renseignements biographiques d'ordre personnel. Les juridictions inférieures ont distingué l'affaire en question, où la police ne demandait que l'adresse IP de l'abonné, sans aucune information additionnelle appartenant à ce dernier, des affaires où la police demandait des informations personnelles *associées* à une adresse IP, telles que les informations sur l'utilisateur dans l'affaire *Spencer*. La juge dissidente de la Cour d'appel a estimé que les adresses IP devraient susciter une attente raisonnable au respect de la vie privée, car celles-ci étaient liées à une activité Internet particulière qui était surveillée et susceptible de révéler des informations biographiques.

La décision

La majorité de la Cour suprême (5-4) a infirmé la décision de la Cour d'appel et a estimé que Bykovets avait une attente raisonnable au respect de sa vie privée à l'égard de son adresse IP. Dans son opinion majoritaire, la juge Karakatsanis a souligné qu'Internet avait changé le cadre d'analyse de l'attente au respect de la vie privée et de l'autodétermination informationnelle, allant jusqu'à déclarer qu'Internet avait ajouté les tiers privés à l'écosystème constitutionnel, faisant « de la relation horizontale entre l'individu et l'État une relation tripartite ». Pour la majorité, cela semble justifier un passage à une approche plus téléologique des affaires relatives à la vie privée informationnelle.

En l'espèce, la majorité s'est concentrée sur le potentiel des adresses IP à révéler des détails intimes sur le mode de vie et les choix personnels d'un individu. La majorité a reconnu l'omniprésence de l'Internet dans nos vies modernes et a estimé que les adresses IP sont la clé qui permet de déverrouiller l'activité en ligne d'un internaute, c'est-à-dire « les premiers (...) "fragments numériques" sur la trace cybernétique de l'utilisateur » qui ont le potentiel de révéler des aspects sensibles et personnels de la vie de l'utilisateur. La majorité a estimé que les utilisateurs peuvent avoir un intérêt légitime à garder ces informations privées, comme ils peuvent le faire en utilisant des réseaux privés virtuels (VPN), et que ces informations méritent donc une protection constitutionnelle. La majorité a conclu que les adresses IP donnaient lieu à une attente raisonnable au respect de la vie privée, dans la mesure où elles constituent des liens cruciaux entre les utilisateurs d'Internet et leur activité en ligne pouvant potentiellement révéler d'immenses quantités d'informations personnelles.

La majorité a en outre refusé d'évaluer les intérêts de la vie privée à la lumière de l'intention déclarée de l'État d'utiliser les informations dans un but unique, par exemple pour faire avancer une enquête. À une époque où les sociétés privées peuvent détenir de grandes quantités de données, la majorité a mis en garde contre le fait de laisser à l'entité privée le soin de décider de révéler ou non une adresse IP, et a jugé que les forces de l'ordre devaient obtenir un mandat de perquisition pour obtenir un élément d'information aussi sensible. Par conséquent, la majorité de la Cour suprême a estimé que le droit de Bykovets à la protection contre les fouilles, les perquisitions et les saisies abusives, garanti par la Charte, avait été violé.

Écrivant au nom des juges dissidents, la juge Côté a critiqué l'analyse de la majorité et a soutenu qu'en l'espèce, l'adresse IP de Bykovets, prise isolément, ne révèle guère d'informations privées, et encore moins d'informations très sensibles; elle révélait simplement l'identité du FSI de l'utilisateur. Selon les juges dissidents, les adresses IP pourraient être comparées aux empreintes digitales laissées sur la scène d'un crime, sur lesquelles l'utilisateur n'a aucun contrôle. Les juges dissidents ont également mis en garde contre le fait que la reconnaissance d'une attente raisonnable au respect de la vie privée pour les adresses IP pourrait entraver les enquêtes policières, en particulier celles portant sur des crimes graves, tels que les crimes contre les enfants.

Principaux points à retenir

Cette décision a des conséquences importantes sur le droit à la vie privée des utilisateurs d'Internet au Canada et sur les procédures d'application de la loi à l'ère numérique.

Tout d'abord, la Cour suprême a fait un pas important en reconnaissant qu'une grande quantité d'informations, parfois très personnelles et confidentielles, peuvent être recueillies par des entreprises privées, et en reconnaissant les enjeux de leur disponibilité potentielle pour les autorités gouvernementales. Dans l'affaire *Bykovets*, la Cour suprême envoie un message fort à tous les tribunaux à travers le pays pour qu'ils veillent à ce que l'application de l'article 8 de la Charte reflète la « réalité technologique » moderne afin que les droits fondamentaux soient mieux protégés lors des perquisitions effectuées par les forces de l'ordre.

Ensuite, la décision souligne l'importance de la vie privée en ligne et, en ce qui concerne les adresses IP, elle manifeste une volonté d'arrimer l'application de l'article 8 de la Charte à la position généralement adoptée par les autorités de réglementation de la vie privée dans leur application des lois en cette matière. Les autorités réglementaires adoptent une vision large de ce qui constitue de l'information personnelle, notant fréquemment que les adresses IP peuvent être considérées comme des informations personnelles et qu'elles peuvent constituer un point de départ pour dresser un tableau des activités en ligne d'une personne. Les autorités réglementaires accordent également une attention particulière à la manière dont les informations personnelles peuvent devenir sensibles en fonction du contexte dans lequel elles sont utilisées ou lorsqu'elles sont combinées à d'autres informations. Par exemple, dans son bulletin d'interprétation concernant les renseignements sensibles, un concept clé de la *Loi sur la protection des renseignements personnels et les documents électroniques*, le Commissariat à la protection de la vie privée du Canada (« **CPVP** ») a noté que les renseignements personnels qui, pris isolément, pourraient être considérés comme anodins, peuvent révéler un caractère plus sensible lorsqu'ils sont liés à

des services qui peuvent mettre en évidence les activités et les préférences personnelles des utilisateurs ou lorsqu'ils sont combinés pour créer des profils.

Comme le montre l'interprétation du CPVP, la « sensibilité » des informations personnelles dépend fortement du contexte, de la mesure dans laquelle les informations peuvent être liées à d'autres informations et des conclusions qu'un tiers peut tirer de ce contexte ou de ces liens, ce qui fait écho au modèle des « fragments numériques » que la majorité de la Cour suprême a adopté dans l'affaire *Bykovets*[1].

Enfin, cette décision peut avoir des répercussions plus larges sur les pratiques développées par certaines entreprises qui suivent les données relatives à leurs utilisateurs d'Internet ou établissent des profils, et qui peuvent être disposées à divulguer volontairement les adresses IP aux forces de l'ordre simplement sur demande. L'arrêt *Bykovets* sous-entend que les entreprises privées doivent être prudentes avant de divulguer volontairement des informations personnelles sur les utilisateurs, même des informations qui peuvent à première vue sembler non sensibles ou anodines, en l'absence d'une autorisation judiciaire ou d'un pouvoir clair de le faire en vertu de la législation applicable. Les entreprises ne doivent pas non plus se conformer aveuglément aux demandes des forces de l'ordre et doivent, en cas de doute, demander des précisions ainsi qu'une copie de l'autorisation invoquée.

De manière plus générale, les entreprises devraient envisager d'adapter leurs procédures et leurs formations afin de garantir que les demandes des services de police soient correctement acheminées, examinées et traitées, et devraient envisager la mise à jour de leurs politiques de protection des informations personnelles afin d'assurer un traitement approprié des adresses IP.

[1]Cette vision élargie des informations personnelles et de leur capacité à révéler des informations supplémentaires, potentiellement sensibles, sur une personne a également été reconnue par d'autres législateurs, autorités de réglementation et tribunaux au Canada, aux États-Unis et en Europe. Voir par exemple la *Loi sur la protection des renseignements personnels dans le secteur privé*, RSQ, c. P-39.1, art. 12, quatrième alinéa; la *California Consumer Privacy Rights Act*, qui s'appuie sur le concept de « renseignements personnels sensibles » comme sous-catégorie de renseignements personnels; et au paragraphe 9(1) du Règlement général sur la protection des données de l'UE (RGPD) (titre complet : *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*). Notamment, la Cour de justice de l'Union européenne a interprété les catégories particulières de données à caractère personnel au titre du RGPD comme incluant non seulement les données reflétant directement les catégories sensibles énoncées à l'article 9, paragraphe 1, du RGPD, mais aussi les « données à caractère personnel susceptibles de divulguer indirectement » de telles informations.

Personnes-ressources : Léon H. Moubayed, Corey Omer, Alexander Max Jarvie, Derek D. Ricci et Shari Cohen