Chapitre 18

Surveillance électronique

Le télétravail entre confiance et contrôle patronal

M^e Simon Laberge et M^e Deborah Furtado,
Fasken Martineau Dumoulin SENCRL

Table des matières

L'une des conséquences bien connues de la pandémie COVID-19 a été l'essor fulgurant du télétravail. En effet, le « travail de la maison » a été bénéfique durant cette période en ce qu'il a permis à plusieurs employeurs de pouvoir poursuivre leurs activités et opérations, tout en limitant les risques de propagation du virus.

Au Québec, en janvier et février 2020, un peu moins de 7 % de la main-d'œuvre de 15 à 69 ans effectuait la majorité de ses heures de travail à domicile[1]. En mars 2020, soit au moment où la pandémie a été déclarée, cette proportion est passée à environ 23 %, puis à 40 % en avril[2]. En 2022, bien que la pandémie se soit en grande partie résorbée, 35 % de la main-d'œuvre effectuait encore du télétravail, la majorité en mode hybride[3].

Avec l'avènement du télétravail et les défis que celui-ci peut représenter pour les employeurs quant à la gestion de la performance et l'efficacité des employés, l'intérêt de certaines entreprises a également augmenté à l'égard des logiciels disponibles afin, notamment, d'évaluer la productivité de leurs employés à l'aide de la surveillance électronique (également appelés « **patrongiciels** ») a également augmenté.

Par exemple, le logiciel TimeDoctor permet notamment aux employeurs de surveiller le travail des employés en leur permettant de savoir sur quelles tâches précises une équipe travaille, le temps passé sur chaque tâche, les sites et les applications visités par les employés pendant leurs heures de travail, l'heure de connexion et de déconnexion de ces derniers, et plus encore. De plus, cette application offre aux employeurs la possibilité de préparer un rapport de productivité et d'accorder un pourcentage de productivité à chaque employé comportant le nombre de minutes réellement travaillées par chacun. Il comprend également des fonctions d'enregistrement des frappes, de capture d'écran et de suivi de l'utilisation d'Internet.

Hubstaff, quant à lui, est un logiciel offrant aux entreprises la possibilité de prendre des captures de l'écran des employés toutes les cinq minutes. Encore plus intrusif, CleverControl promet sur son site Internet d'augmenter la productivité des employés et d'aider les employeurs à « repérer les fainéants » en surveillant les frappes sur le clavier et les clics sur la souris des employés.

Selon une étude canadienne récente[4], le tiers des employés (33 %) déclare que la surveillance numérique effectuée par leur employeur a augmenté

1. <https://statistique.quebec.ca/fr/document/portrait-du-teletravail-au-quebec>.
2. *Ibid.*
3. *Ibid.*
4. <https://fsc-ccf.ca/fr/projets/suivi-du-teletravail-au-canada-soutien-ou-surveillance/>.

depuis le début de la pandémie. Sept employés sur dix (70 %) affirment qu'au moins un aspect de leur travail fait l'objet d'une surveillance numérique (c'est-à-dire que leurs données ne sont pas simplement stockées, mais qu'elles sont activement contrôlées ou examinées par l'employeur). Les courriels (33 %), les sites Internet (24 %), les séances de clavardage ou les messages (23 %) et les appels téléphoniques (20 %) sont les éléments qui font le plus souvent l'objet d'une surveillance numérique. 32 % des employés ayant répondu ont également affirmé avoir fait l'objet d'au moins l'une des formes de surveillance suivantes par leur employeur : localisation, Webcaméra/enregistrement vidéo, surveillance de la frappe au clavier, capture d'écran ou lecture de caractéristiques biométriques comme les traits faciaux, la voix ou l'iris.

À la lumière de ce qui précède, force est de constater qu'à l'ère du télétravail, où la limite entre la sphère professionnelle et personnelle d'un employé est plus incertaine qu'elle ne l'était auparavant, la surveillance électronique des employés est plus fréquente qu'à une certaine époque, mais surtout que les moyens pour procéder à une telle surveillance se sont multipliés et sont de plus en plus facilement accessibles pour les employeurs. Or, il va de soi qu'une telle surveillance électronique pourrait porter atteinte au droit à la vie privée des employés. En outre, si la surveillance effectuée par un employeur implique la cueillette de renseignements personnels ou sensibles des employés, l'employeur est tenu de respecter plusieurs obligations légales en la matière.

Nous proposons ainsi de dresser un portait de l'état du droit québécois concernant les limites du droit de surveiller électroniquement les outils professionnels utilisés par les employés et, plus précisément, l'historique de leur navigation Internet, leur boîte courriel professionnelle et leur messagerie instantanée.

1. Le cadre législatif applicable

Lorsqu'un employeur effectue de la surveillance électronique, il doit s'assurer de respecter plusieurs obligations législatives, lesquelles se retrouvent à l'intérieur de différentes lois au Québec. La section qui suit vise à dresser un aperçu du cadre législatif le plus couramment analysé par les décideurs québécois[5].

5. La présente section n'est donc pas exhaustive et plusieurs autres articles de loi ou règlement pourraient s'appliquer et être pertinents selon le contexte.

1.1. *La Charte des droits et libertés de la personne*[6] (la « Charte québécoise »)

La Charte québécoise, à son article 5, protège le droit à la vie privée, en plus de prévoir que toute personne qui travaille a droit, conformément à la loi, à des conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique. Selon la jurisprudence, une surveillance constante ou continue en milieu de travail pourrait porter atteinte au droit d'un employé à des conditions de travail justes et raisonnables. La surveillance constante ou continue est celle qui capte en image ou en son le milieu de travail dans lequel un employé effectue son travail, et ce, sans interruption, au point de nourrir une impression d'être épié au moindre geste au cours de la journée de travail[7]. Cette définition a été élaborée plus particulièrement dans un contexte de caméras de surveillance installées en milieu de travail. Dans un contexte où la prestation de travail est rendue à distance, on peut penser qu'une surveillance constante ou continue est celle qui peut permettre à l'employeur de savoir ce que fait un employé sur son ordinateur, par exemple en captant l'écran d'un employé ou sa navigation en ligne de façon constante et continue.

L'article 4 de la Charte québécoise, qui prévoit que toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation, est également souvent analysé par les décideurs afin de déterminer si la surveillance électronique porte atteinte aux droits des employés[8].

La jurisprudence nous a depuis longtemps enseigné qu'au travail, le droit à la vie privée n'est pas absolu puisque l'expectative de vie privée est souvent réduite dans un contexte professionnel, par opposition à l'expectative de vie privée qu'une personne peut avoir dans son domicile et dans sa vie personnelle. Cela est encore plus vrai lorsqu'un employeur dispose d'une politique limitant le droit d'un employé d'utiliser son ordinateur, son courriel professionnel ou un système de messagerie à des fins personnelles, et prévoyant le droit de l'employeur d'accéder à de tels outils. Cela n'a cependant pas pour effet d'anéantir l'expectative de la part d'un employé que son employeur ne consulte pas le contenu de sa boîte courriel sans son consentement. En effet, l'une des décisions de principe visant l'expectative de vie privée qu'un employé

6. RLRQ, c. C-12.
7. *Syndicat des professionnelles et professionnels municipaux de Montréal (SPPMM)* et *Ville de Montréal* (grief syndical), 2020 QCTA 358, par. 19.
8. Pour les employeurs pour lesquels la *Charte canadienne des droits et libertés*, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, ch. 11 s'applique, le droit constitutionnel à la vie privée est prévu à ses articles 7 et 8. L'équivalent de l'article 9.1 de la Charte québécoise se trouve, quant à lui, à l'article 1 de la Charte canadienne (le test d'« Oakes »).

peut avoir eu égard à son ordinateur est le célèbre arrêt de la Cour suprême du Canada *R.* c. *Cole*[9]. Cet arrêt nous rappelle que toute personne peut raisonnablement s'attendre à la protection de sa vie privée à l'égard des renseignements contenus dans son ordinateur de travail, du moins lorsque son utilisation à des fins personnelles est permise ou raisonnablement prévue. Les ordinateurs qui sont utilisés d'une manière raisonnable à des fins personnelles – qu'ils se trouvent au travail ou à la maison – contiennent des renseignements qui sont significatifs, intimes et qui ont trait à l'ensemble des renseignements biographiques de l'utilisateur. Ainsi, les employeurs doivent tout de même se soumettre à certaines contraintes pour accéder aux outils professionnels de leurs employés, et ce, même si l'employeur en détient l'entière propriété.

L'article 9.1 de la Charte québécoise apporte cependant un certain tempérament au droit à la vie privée des employés et permet à un employeur de porter atteinte à certaines libertés et droits fondamentaux, à condition de respecter certains critères. Ainsi, lorsque l'employeur portera atteinte à la vie privée d'un employé, et ce, par sa surveillance électronique – ce qui ne sera pas toujours le cas puisque toute surveillance n'équivaut pas automatiquement à une violation au droit à la vie privée si, par exemple, l'employé n'avait aucune expectative de vie privée quant aux renseignements surveillés – il devra démontrer que sa surveillance « se rapporte à des préoccupations urgentes et réelles ». Autrement dit, l'employeur doit avoir des motifs raisonnables de procéder à une telle surveillance, par opposition à un simple soupçon. Sa surveillance devra également avoir un lien rationnel avec l'objectif qu'il poursuit, devra être de nature à porter le moins possible atteinte au droit à la vie privée, et les effets préjudiciables de sa surveillance devront être proportionnels à la fois à l'objectif poursuivi et aux effets bénéfiques engendrés par son application.

1.2. Le *Code civil du Québec*[10]

Le *Code civil du Québec* prévoit, lui aussi, que toute personne a droit au respect de sa réputation et de sa vie privée[11]. Il indique explicitement que pourra être considéré comme une atteinte à la vie privée d'une personne le fait de surveiller sa vie privée par quelque moyen que ce soit[12].

9. *R.* c. *Cole*, 2012 CSC 53.
10. RLRQ, c. CCQ-1991.
11. Art. 35.
12. Art. 36.

1.3. *Loi sur la protection des renseignements personnels dans le secteur privé*[13] (la « Loi »)

La réforme d'envergure du cadre législatif en matière de protection des renseignements personnels[14] et les nombreux amendements législatifs entrés en vigueur au cours des deux dernières années témoignent, selon nous, d'une volonté du législateur de resserrer les obligations de toute personne recueillant des renseignements personnels. Il est donc essentiel de rappeler brièvement les dispositions de cette Loi qui pourraient avoir une incidence sur la surveillance numérique.

La Loi prévoit que toute personne ne peut collecter que les renseignements personnels qui sont nécessaires à l'objet du dossier[15]. La Cour suprême du Canada[16] a récemment confirmé qu'une personne a une attente raisonnable au respect de sa vie privée face à une adresse IP, puisqu'elle représente un lien crucial entre un internaute et son activité en ligne. Selon le plus haut tribunal du pays, cette adresse est la clé donnant accès à l'activité Internet d'un utilisateur. Cette décision n'est pas étonnante en ce qu'elle est cohérente avec l'interprétation du Commissariat à la protection de la vie privée du Canada qui considérait déjà, depuis plusieurs années, que constituent des renseignements personnels les renseignements sur un utilisateur permettant de dresser un tableau des activités en ligne exercées par celui-ci, par exemple les services en ligne auxquels il est abonné, ses intérêts personnels en fonction des sites Internet visités, les organisations auxquelles il appartient, etc.[17]. Ces renseignements peuvent être sensibles, car ils permettent de déterminer, entre autres, les penchants d'une personne, ses fréquentations et les endroits où elle voyage. En bref, l'activité en ligne d'une

13. RLRQ, c. P-39.1. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 est le pendant applicable pour les organismes publics.
14. Le projet de loi 64 a notamment introduit à la Loi et à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* des règles concernant le traitement des incidents affectant la confidentialité des renseignements personnels par les organismes publics et les entreprises. De plus, il oblige ces organismes et ces entreprises à publier des règles encadrant la gouvernance à l'égard des renseignements personnels et, pour ceux qui recueillent ces renseignements par un moyen technologique, à publier et diffuser une politique de confidentialité. Il y introduit aussi l'exigence qu'une évaluation des facteurs relatifs à la vie privée soit réalisée en certaines circonstances, notamment à l'égard de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Le projet de loi précise diverses exigences relatives au consentement requis préalablement à une collecte, une utilisation ou une communication de renseignement personnel.
15. Art. 5.
16. *R.* c. *Bykovets*, 2024 CSC 6.
17. <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/ip_201305/>.

personne, même pendant ses heures de travail, peut contenir une panoplie de renseignements personnels, et parfois même sensibles.

Sachant que la surveillance électronique pourrait ainsi impliquer la collecte de renseignements personnels, comment s'assurer que leur collecte est « nécessaire » au sens de la Loi ? Selon la Commission d'accès à l'information[18], la nécessité s'évalue par rapport à la finalité de la collecte et à sa proportionnalité. Ainsi, une collecte sera nécessaire si les critères que nous avons énumérés plus haut, pour justifier une atteinte à un droit fondamental sous la Charte québécoise, sont satisfaits.

En outre, lorsqu'une organisation recueille des renseignements en ayant recours à une technologie dont certaines fonctions permettent d'identifier, de localiser ou de profiler les employés, comme certains patrongiciels, la Loi impose une obligation supplémentaire de transparence aux employeurs depuis les amendements législatifs apportés en 2021. En effet, toute organisation doit dorénavant informer les personnes concernées du fait qu'elle a recours à une telle technologie et des moyens offerts pour activer les fonctions d'identification, de localisation ou de profilage[19]. Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels visant à évaluer certaines caractéristiques d'un employé, notamment à des fins d'analyse du rendement au travail ou du comportement de cette personne.

En pratique, ces précisions feront l'objet d'une politique de « vie privée » au sein de l'employeur. D'ailleurs, depuis 2021, la Loi oblige les entreprises à publier des règles encadrant la gouvernance à l'égard des renseignements personnels et, pour ceux qui recueillent ces renseignements par un moyen technologique, à publier et diffuser une politique de confidentialité.

Tout renseignement sensible recueilli par un employeur doit également faire l'objet d'un consentement manifeste et de façon expresse[20]. Un renseignement est sensible lorsque, de par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée[21].

Il existe cependant certaines exceptions à la Loi où le consentement de l'employé à la collecte de renseignements personnels ne sera pas obligatoire. C'est notamment le cas lorsque l'utilisation du renseignement personnel est nécessaire à des fins de prévention et de détection de la fraude. On peut donc

18. <https://cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/collecte-renseignements-personnels_entreprises#evaluer-necessite>.
19. Art. 8.1 de la Loi.
20. Art. 12 de la Loi.
21. Art. 12 (2) de la Loi.

évidemment penser qu'un employeur qui aurait des motifs raisonnables de croire que son employé commet du vol de temps ne sera évidemment pas obligé de demander son consentement dans le cadre d'une enquête impliquant une surveillance électronique et la collecte de renseignements personnels ou sensibles, si celle-ci est par ailleurs justifiée et répond aux autres critères.

2. Analyse des décisions phares rendues en matière de surveillance électronique des outils professionnels

Un constat s'impose de la jurisprudence : maintes décisions ont été rendues concernant l'équilibre entre le droit à la vie privée et à des conditions justes et raisonnables des employés et le droit d'un employeur de procéder à de la filature ou à l'installation de caméras de surveillance en milieu de travail. Il s'agit effectivement des formes de surveillance ayant fait couler le plus d'encre en droit du travail. Par contre, la jurisprudence est encore à un stade embryonnaire eu égard au droit d'un employeur d'accéder aux outils informatiques professionnels d'un employé et de surveiller électroniquement l'usage qui en est fait, à l'aide notamment de patrongiciels, que ce soit pour des motifs disciplinaires, comme le vol de temps, ou pour des motifs administratifs, comme la gestion de la performance à distance.

Il appert des quelques décisions rendues en la matière que les employeurs sont généralement en droit de vérifier l'usage effectué par un employé de ses ressources informatiques, ce qui inclut son ordinateur, son courriel et sa messagerie instantanée, mais à condition d'avoir des motifs raisonnables – ou un objectif réel et urgent, si l'on reprend les termes utilisés – pour justifier une atteinte à un droit protégé par la Charte québécoise. Des motifs raisonnables pourraient impliquer, par exemple, des soupçons objectifs et raisonnables de fraude, de vol de temps ou de concurrence déloyale.

Nous proposons d'analyser les décisions phares en la matière.

2.1. Surveillance des sites Internet consultés par les employés sur leur ordinateur professionnel

Comme mentionné précédemment, bien que les politiques et les pratiques en vigueur dans le milieu de travail puissent réduire l'attente d'un employé en matière de respect de sa vie privée à l'égard de l'usage d'un ordinateur de travail, elles ne la font pas, à elles seules, disparaître complètement : en effet, la nature des renseignements en jeu que comprend un ordinateur expose

généralement les préférences de l'utilisateur, ses intérêts, ses pensées, ses activités et ses idées[22].

Par conséquent, le fait pour un employeur d'imposer des vérifications aléatoires du contenu de l'ordinateur d'un employé pourrait probablement être vu, dans l'état actuel du droit, comme étant abusif et non justifié[23].

De façon plus spécifique, un employeur peut-il surveiller les sites Internet consultés par un employé ?

Comme rappelé par la Cour suprême du Canada dans l'arrêt *Bykovets*[24] précité, les sites Internet consultés par un employé peuvent contenir une foule de renseignements personnels susceptibles de révéler des informations biographiques d'ordre personnel, allant des restaurants qu'il fréquente, aux destinations qu'il visite, à ses passe-temps, aux suppléments alimentaires qu'il utilise, etc. D'autres activités en ligne peuvent révéler des renseignements qui touchent directement à l'ensemble des renseignements biographiques d'un utilisateur. Les sites Internet qui offrent des services de rencontre peuvent, par exemple, donner à l'employeur une description des préférences sexuelles de l'utilisateur, alors que l'historique d'un internaute dans des salons de cyber bavardage médical, politique ou autre, peut révéler ses préoccupations en matière de santé ou ses opinions politiques. Évidemment, si une politique claire de l'employeur interdit l'utilisation d'un ordinateur professionnel à des fins personnelles, l'attente de vie privée de l'employé sera fortement diminuée. Ceci dit, selon la jurisprudence, elle n'est pas nulle, particulièrement si l'employeur tolère l'usage des ordinateurs à fins personnelles ou qu'il n'applique pas sa politique à cet égard avec rigueur.

Dans une affaire récente[25], l'arbitre M^e^ Maureen Flynn devait déterminer si l'employeur effectuait une surveillance électronique illégale en utilisant le logiciel Graylog. Ce logiciel vise à fournir des données générales et brutes sur la consultation de sites Internet effectuée par tous ses employés pendant les heures de travail sur leur ordinateur professionnel appartenant à l'employeur.

Graylog vise avant tout à assurer une utilisation sécuritaire des outils informatiques d'une entreprise. À cette fin, les données d'utilisation des

22. *R.* c. *Cole*, 2012 CSC 53.
23. *Syndicat des professeures et professeurs de l'Université du Québec en Outaouais* et *Université du Québec en Outaouais*, 2016 CanLII 153557.
24. *R.* c. *Bykovets*, 2024 CSC 6.
25. *Syndicat des professionnelles et professionnels municipaux de Montréal (SPPMM)* et *Ville de Montréal (grief syndical)*, 2020 QCTA 358. À noter que cette décision a été confirmée par la Cour supérieure du Québec au terme d'un pourvoi en contrôle judiciaire (voir *Syndicat des professionnelles et professionnels municipaux de Montréal (SPPMM)* c. *Flynn*, 2022 QCCS 363.

22 000 employés de l'employeur, la Ville de Montréal, étaient répertoriées. Une centaine de catégories de sites jugées comme étant non reliées au travail, comme les catégories de voyage, réseaux sociaux, magasinage ou services bancaires, étaient identifiées. Le logiciel retenait par la suite le nombre de connexions pour ces catégories, la fréquence d'utilisation, le pourcentage de ces connexions par rapport à l'ensemble des connexions au sein de l'employeur, et ce, pour une période visée. Il est important de noter que le logiciel ne fournit pas le détail de l'activité menée sur les sites Internet consultés ni la durée de la consultation. Dans cette affaire, la compilation des données était impersonnelle et seuls les codes d'utilisateurs des employés étaient utilisés. Ceci dit, l'employeur pouvait identifier à quel employé appartenait le code d'utilisateur, puisque ce code était fourni par l'employeur lors de l'embauche.

L'employeur avait installé ce logiciel pour éviter un danger de cyberattaque ou réagir rapidement en cas d'attaque. Ceci dit, cette décision est intéressante d'un point de vue de surveillance numérique puisque l'employeur procédait également à une extraction de rapports journaliers des consultations Internet effectuées par les cinquante plus grands utilisateurs d'Internet au sein de ses employés, et ce, en moyenne quatre fois par année. Le rapport contenait un aperçu, par code d'utilisateur, de l'utilisation d'Internet, toutes catégories confondues, un aperçu pour chacune des catégories, la nature des sites visités (et non le site Internet consulté) et la période de consultation. Ces rapports permettaient ainsi à l'employeur de détecter une situation potentielle d'abus.

Après une analyse méticuleuse et prudente de ce rapport journalier, si l'employeur considérait que le temps et le volume de consultation étaient importants et permettaient de douter qu'il puisse y avoir une utilisation d'Internet non conforme au Code de conduite et aux directives en place et connues des employés, une surveillance sur un poste de travail en particulier pouvait être effectuée, en y installant un mouchard afin de débuter une enquête. Selon l'arbitre, c'est à ce moment-là que pourrait survenir une situation potentielle de surveillance constante et continue au sens de la Charte québécoise. Toutefois, cette dernière étape n'était pas visée par le grief, ce qui laisse malheureusement les employeurs et les employés avec peu de réponses eu égard à l'étendue de la surveillance que peut mener un employeur lorsqu'il repère des situations potentielles d'abus. Autrement dit, est-ce que le rapport journalier pourrait amener l'employeur à avoir des motifs raisonnables qu'un employé abuse de ses ressources informatiques (ou à avoir un objectif réel et urgent de surveillance) ? Notre compréhension de la décision favorise une réponse positive à cette question, puisque ces rapports journaliers n'ont pas été vus comme étant illégaux ou non nécessaires.

En effet, l'arbitre en vient à la conclusion que bien que la compilation effectuée par l'employeur couvre toutes et chacune des consultations de sites Internet effectuées par tous les employés de l'employeur à l'aide de ses ordinateurs, cette compilation qui donne lieu à un rapport journalier ne constitue pas une surveillance constante et continue du travail effectué par un employé au sens de l'article 46 de la Charte québécoise, et ce, pour les raisons suivantes :

- le logiciel ne capte pas toutes les activités menées par un employé alors qu'il est à son poste de travail – seules les consultations Internet le sont ;
- le logiciel ne cible pas un employé ou un groupe d'employés en particulier, mais l'ensemble des consultations Internet effectuées par tous les employés ;
- le logiciel compile les données de manière impersonnelle.

En ce qui a trait à la possible atteinte à la vie privée des employés, l'arbitre conclut que les employés ne peuvent avoir d'attente subjective raisonnable eu égard au caractère privé des informations recueillies par l'employeur. En effet, selon l'arbitre, les données analysées par le logiciel et consultées par l'employeur dans les rapports de journalisation ne font pas partie de la sphère privée de l'employé. Dans de telles circonstances, l'employé ne peut avoir une attente subjective raisonnable quant au caractère privé des données générées par sa navigation sur Internet selon les paramètres en cause, considérant qu'il a connaissance des directives en vigueur qui lui indiquent les limites de son droit à la vie privée lorsqu'il utilise les outils informatiques mis à sa disposition par l'employeur.

Même si une expectative à la vie privée existait en pareil cas, l'arbitre indique qu'elle serait minime et justifiée par l'article 9.1 de la Charte québécoise. En effet, l'employeur avait un motif rationnel, légitime et raisonnable d'utiliser le logiciel Graylog et les rapports de journalisation. Ce logiciel assure une utilisation sécuritaire des outils informatiques et permet d'établir les cas d'abus ou de vol de temps.

Cette conclusion est particulièrement intéressante à la lumière de la jurisprudence actuelle. En effet, nous retenons de la décision que le simple fait de produire et consulter un rapport anonymisé des cinquante plus grands utilisateurs d'Internet, comprenant uniquement les catégories de sites Internet visités, ne contrevient pas au droit à la vie privée des employés. Selon nous, considérant que ce rapport anonymisé a été légalement obtenu, il pourrait fonder l'employeur à mener une surveillance additionnelle en raison de « motifs raisonnables » que l'employé abuse de ses ressources. Ceci dit, la surveillance additionnelle suite à cette identification, par exemple par l'installation d'un mouchard sur le poste de travail d'un employé, par l'obtention

de l'historique de navigation d'un employé ou par une capture de l'écran d'un employé à certains intervalles, porterait, selon nous, nécessairement atteinte au droit à sa vie privée. Si la collecte de ces renseignements est jugée nécessaire au sens de la Loi et que cette atteinte peut être justifiée au sens de la Charte québécoise, elle pourrait néanmoins être légale.

En outre, il ne faut pas oublier que si l'employeur collectait le détail des sites Internet visités dans son rapport, plutôt que simplement les catégories de sites visités, la conclusion de l'arbitre quant au fait que les employés n'avaient pas d'attente subjective raisonnable eu égard au caractère privé des informations recueillies par l'employeur n'aurait pu être conciliable avec les enseignements de la Cour suprême du Canada dans l'arrêt *Bykovets*[26]. En effet, selon la Cour suprême du Canada, lorsque les renseignements collectés en ligne tendent à révéler des détails intimes sur le mode de vie et les choix personnels d'un individu (ce qui peut être le cas en analysant les sites Internet visités), ceux-ci sont considérés comme privés.

2.2. Surveillance de la boîte courriel professionnelle d'un employé

Qu'en est-il de la possibilité d'accéder ou de surveiller le contenu de la boîte courriel professionnelle d'un employé ? Bien que l'adresse courriel professionnelle d'un employé ne soit généralement utilisée que pour envoyer des courriels liés à l'exercice de ses fonctions, il peut parfois arriver qu'un employé envoie des courriels personnels à partir de son adresse professionnelle. Cela est d'autant plus vrai si une certaine tolérance existe au sein de l'employeur et qu'aucune directive claire relativement à l'interdiction d'utiliser l'adresse professionnelle pour envoyer des courriels personnels n'est mise en place ou appliquée rigoureusement.

Il appert, encore une fois, que l'employeur doit avoir des motifs raisonnables pour accéder aux courriels professionnels d'un employé et doit tout faire pour éviter les courriels qui pourraient avoir un caractère privé. À titre d'exemple, un arbitre en est venu à la conclusion qu'un employeur était fondé à accéder à la boîte courriel de son employé alors que ce dernier avait envoyé un courriel avec un contenu inquiétant à son supérieur[27]. Dans cette affaire, un conseiller en développement économique travaillant au ministère de l'Économie, de l'Innovation et des Exportations avait partagé avec un directeur son intention de déposer, avec des collègues, une plainte contre un gestionnaire. À la suite du dépôt de la plainte en question, l'employé concerné

26. *R.* c. *Bykovets*, 2024 CSC 6.
27. *Ministère de l'Économie, de l'Innovation et des Exportations* et *Syndicat des professionnelles et professionnels du gouvernement du Québec*, 2017 QCTA 729.

a transmis un courriel au directeur à l'intérieur duquel il a écrit : « le premier missile a été largué ». Inquiet quant à la teneur de ce message et n'ayant obtenu aucune explication de la part du plaignant, le directeur a transmis le courriel au service des ressources humaines, qui a décidé de faire enquête et d'accéder à la boite courriel professionnelle du plaignant. L'arbitre en vient à la conclusion que ce courriel comportait des propos à connotation guerrière et que la référence à l'envoi d'un « premier missile » laissait entendre qu'une action était entreprise et qu'il pourrait y avoir des suites. L'employeur était ainsi fondé à s'interroger sur la loyauté du plaignant et à accéder à ses courriels professionnels. L'arbitre prend notamment en compte les éléments suivants pour en venir à la conclusion que le droit à la vie privée du plaignant n'a pas été violé :

- La surveillance des courriels a été exercée de bonne foi, sans abus et sur une courte période. L'employeur a eu accès aux courriels uniquement pendant deux ou trois jours pour couvrir la période de la mi-janvier à la mi-mai, soit autour du moment où le courriel a été envoyé. Ainsi, la surveillance était limitée à ce qui était nécessaire ;
- L'employeur a ciblé les courriels en fonction de l'objet et du destinataire sur un sujet litigieux en faisant attention de ne pas consulter les courriels touchant à la vie privée du plaignant ;
- L'employeur disposait d'une politique claire précisant qu'il pouvait éventuellement surveiller et même procéder à une vérification de ces courriels. Cela limite ainsi l'expectative de vie privée eu égard aux courriels.

Puis, dans une affaire récente[28], le Tribunal d'arbitrage devait également déterminer si un employeur était en droit d'accéder à la boîte courriel professionnelle de ses employés, et ce, dans un contexte où il craignait que des informations confidentielles aient été transmises à une tierce partie. L'employeur en cause exploite un centre de réadaptation pour jeunes en difficulté et avait été contacté par une journaliste qui souhaitait rédiger un article concernant certaines problématiques vécues dans l'établissement de l'employeur, notamment quant à la stabilité des horaires de travail, la stabilité des équipes et la sécurité au travail. La journaliste référait également à certaines conditions offertes à ses usagers. L'employeur était ainsi convaincu que certains employés avaient communiqué avec la journaliste afin de partager de l'information confidentielle quant à ces sujets, puisque plusieurs de ceux-ci avaient antérieurement fait l'objet de discussions avec le syndicat

28. *Alliance du personnel professionnel et technique de la santé et des services sociaux (APTS)* et *Centre intégré de santé et de services sociaux de la Côte-Nord (grief patronal et grief syndical)*, 2023 QCTA 126.

et les employés. L'employeur a donc fouillé les boîtes courriel de certains employés qu'il jugeait être les plus « revendicateurs » afin d'identifier qui aurait pu transmettre de l'information confidentielle à la journaliste.

L'employeur avait-il le droit de fouiller la boîte courriel de ses employés dans un contexte où il est convaincu que de l'information confidentielle relativement à ses usagers a été communiquée à une tierce partie ? L'arbitre est d'avis que l'atteinte à la vie privée des employés, en l'espèce, n'était pas justifiée, entre autres, pour les motifs qui suivent :

- comme l'employeur autorisait le syndicat à utiliser le système de courriels de l'employeur pour s'adresser à ses membres, l'attente subjective quant au respect de leur vie privée lorsqu'ils s'adressent à leur syndicat par courriel est plus grande ;
- l'employeur n'avait pas de motifs sérieux et raisonnables lui permettant d'avoir accès aux courriels de ses employés : bien qu'une dénonciation de certaines conditions ait été faite à une journaliste, aucune information confidentielle n'avait été révélée par cette dernière (ex. données nominatives des patients, les soins reçus, l'ensemble des données concernant un patient, les échanges entre les intervenants concernant un patient, etc.) ;
- le choix des employés visés par la fouille était plutôt arbitraire : il n'existait pas de lien entre être un « employé revendicateur » et l'action de transmettre de l'information confidentielle ;
- l'employeur a vérifié l'ensemble des courriels des employés visés alors qu'il aurait pu limiter sa fouille aux seuls courriels adressés au syndicat.

Il va de soi que les conclusions de cette décision confirment qu'un employé peut, dans certaines circonstances, avoir une certaine attente quant au respect de sa vie privée relativement aux courriels qu'il envoie de son courriel professionnel. C'est encore plus vrai lorsque les employés sont syndiqués et qu'ils utilisent leur courriel professionnel pour communiquer avec leur syndicat.

En outre, nous comprenons qu'un employeur qui accède à l'ensemble d'une boîte courriel, sans restreindre sa recherche à des courriels spécifiques, comme nous l'avons vu ci-avant, pourra difficilement convaincre un décideur que l'atteinte à la vie privée est justifiée. En effet, des moyens plus proportionnels pour limiter l'atteinte à ce qui est absolument nécessaire par rapport à l'objectif auraient pu être utilisés, et ce, en s'assurant de faire une recherche de courriels limitée à des mots-clés, par exemple, afin d'éviter de consulter des courriels de nature privée.

2.3. Surveillance de la messagerie instantanée professionnelle d'un employé

Plusieurs employeurs donnent accès à leurs employés, dans le cadre de l'exercice de leurs fonctions, à des applications permettant de clavarder de façon instantanée avec des collègues de travail. Nous pouvons penser aux messageries comme Jabber, Microsoft Teams, Lync, Google Chat ou Amazon Chime. Ces applications permettent généralement de connaître le statut d'un employé (disponible, occupé, absent, etc.).

Bien que ces outils soient habituellement fournis par l'employeur, il n'est pas rare que des collègues de travail discutent de sujets non liés au travail sur de telles messageries instantanées. Par conséquent, un employé a-t-il une haute expectative de vie privée face à de telles discussions ?

Récemment, l'arbitre Me Dominic Garneau a eu à se prononcer sur le caractère privé de telles conversations[29]. Dans cette affaire, une agente de secrétariat a été congédiée en raison de fausses déclarations quant à ses heures de travail et absences. Afin de mettre en preuve que l'employée avait volé du temps à l'employeur, ce dernier a, entre autres, accédé et surveillé sa messagerie instantanée Lync, laquelle permet aux employés de discuter avec leurs collègues et de faire connaître leur statut. L'arbitre est d'avis que bien que l'employée ait eu une certaine expectative raisonnable de vie privée à l'égard de ses conversations de nature personnelle, elle savait que son ordinateur pouvait faire l'objet de surveillance en raison de la politique de l'employeur adoptée à cet égard[30].

Dans cette affaire, l'employeur avait été motivé à surveiller la messagerie Lync de l'employée en raison de la réception d'un rapport de dénonciation anonyme à la suite d'un audit interne. Le rapport démontrait en effet que l'employée ne respectait pas son horaire de travail et que, pour pallier ses absences, elle se connectait à distance à l'application Lync afin que son statut soit inscrit comme « présente au bureau », ce qui contrevenait à la politique de l'employeur relative aux médias sociaux et remettait en question la loyauté de l'employée. La dénonciation indiquait également que l'employée prolongeait souvent sa période de repas et ses pauses. Dans le but de vérifier

29. *Syndicat canadien de la fonction publique (SCFP)* et *Autorité des marchés financiers (Mélissa Blais)*, (T.A., 2019-09-16 (décision rectifiée le 2019-09-16)), 2019 QCTA 446. Pourvoi en contrôle judiciaire rejeté (C.S., 2021-10-25) 200-17-030172-191, 2021 QCCS 4505.

30. La politique concernant l'utilisation des médias sociaux prévoyait ce qui suit : « Le membre du personnel doit savoir qu'il n'y a aucune expectative de vie privée par rapport à l'utilisation d'Internet par l'entremise des équipements de l'[Employeur]. En effet, les équipements informatiques de l'[Employeur] font l'objet de surveillance et les utilisations abusives ou inappropriées pourront être rapportées et sanctionnées, comme c'est le cas pour l'ensemble des outils de travail (téléphone, ordinateur, etc.) ».

le sérieux de telles allégations, l'employeur a d'abord procédé à une analyse des données provenant des accès aux portes, à l'ascenseur et au poste informatique de l'employée. Il a ensuite comparé ces données avec les heures déclarées par l'employée et constaté des écarts significatifs. C'est alors que l'employeur a accédé à sa messagerie instantanée.

L'arbitre en vient à la conclusion que l'employeur avait des motifs sérieux et rationnels de croire que l'employée volait du temps, ce qui lui permettait de consulter ses conversations sur Lync. Selon nous, la seule réception d'une dénonciation anonyme, sans avoir tenté de valider le bien-fondé de telles allégations, aurait plus difficilement permis à l'employeur de surveiller sa messagerie. Ceci dit, dans cette affaire, l'employeur avait procédé à une analyse préliminaire permettant de vérifier le bien-fondé des allégations anonymes, comme indiqué ci-haut, avant d'accéder aux conversations de l'employée sur Lync.

Selon l'arbitre, l'accès à la messagerie instantanée lui a permis de démontrer que l'employée utilisait la messagerie pour des conversations personnelles durant son temps de travail de manière abusive. En effet, plus de soixante-et-onze (71) heures avaient été utilisées pour des conversations non reliées au travail. Bien que l'employeur n'interdise pas la tenue de telles conversations, la fréquence et la durée de telles conversations, conjuguées à des prolongations de pauses et absences, étaient abusives. Ses conversations révélaient également que l'employée et son conjoint avaient réservé un local de l'employeur pendant plus d'une heure, pendant les heures de travail de l'employée, afin de discuter d'un dossier personnel sans lien avec le travail.

Selon l'arbitre, aucun autre moyen ou technique n'aurait pu permettre d'atteindre les fins recherchées sans analyser l'ensemble des conversations tenues sur Lync, incluant les conversations de nature privée.

3. Réflexions sur l'avenir

Il est évident que les décideurs auront davantage à se prononcer au cours des prochaines années sur l'utilisation des patrongiciels par les employeurs et les enjeux de vie privée que ceux-ci soulèvent, tant au niveau de la Charte québécoise que de la Loi.

Il sera intéressant de voir comment les décideurs analyseront le critère de « l'atteinte minimale » à la lumière de l'ensemble des logiciels de surveillance disponibles. Par exemple, plutôt que d'utiliser un logiciel permettant d'obtenir une liste de sites Internet consultés ou des captures d'écran à des intervalles spécifiques, la mise en preuve qu'il existe des logiciels permettant à un employeur de produire un rapport qui illustre combien de temps

un employé passe sur des sites Internet non liés au travail, et ce, sans dévoiler la liste des sites Internet consultés, serait-elle suffisante pour démontrer que l'employeur aurait pu atteindre son objectif à l'aide d'un logiciel moins intrusif?

Il est également intéressant de constater que depuis 2023, les employeurs en Ontario assujettis à la *Loi de 2000 sur les normes d'emploi*[31], comptant 25 employés ou plus au 1er janvier de n'importe quelle année, doivent mettre en place une politique écrite sur la surveillance électronique des employés. Les employeurs ontariens doivent maintenant faire preuve de transparence en indiquant s'ils surveillent électroniquement leurs employés ou non. Dans l'affirmative, l'employeur doit décrire comment et dans quelles circonstances cette surveillance a lieu et exposer les objectifs pour lesquels les renseignements obtenus par l'entremise de la surveillance électronique peuvent être utilisés.

Bien que la Loi et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[32] aient été visées par une réforme majeure au cours des dernières années, et que l'obligation d'avoir une politique traitant spécifiquement de la surveillance électronique ne semble pas avoir été mise sur la table, il sera tout de même intéressant de voir si le législateur québécois décidera d'emboîter le pas à notre province voisine en matière de surveillance électronique.

Nous nous questionnons également sur l'importance que prendra le droit de gérance des employeurs dans l'évaluation que les décideurs en droit du travail feront des mesures de surveillance mises en place par les employeurs, et ce, dans un contexte où le télétravail est souvent vu comme étant un privilège octroyé aux employés.

En effet, lorsqu'un employé exerce sa prestation de travail physiquement aux bureaux de son employeur, les représentants de ce dernier peuvent se promener dans les couloirs de l'établissement à tout moment. Par conséquent, l'employeur peut exercer, en quelque sorte, une sorte de surveillance lui permettant de voir si les employés sont bel et bien à leur poste de travail aux heures convenues lors de retours de pauses, repas ou autre. Un simple « tour d'étage » permet également à l'employeur de constater si les employés exercent leur prestation de travail ou s'ils s'adonnent à d'autres activités. Bien qu'il aille de soi que l'expectative de vie privée est diminuée lorsqu'un employé se trouve dans l'établissement d'un employeur, par opposition à celle qu'il peut avoir lorsqu'il se trouve à son domicile, il sera tout de même intéressant de

31. Art. 41.1.1, *Loi de 2000 sur les normes d'emploi*, L.O. 2000, chap. 41.
32. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1.

s'interroger sur l'impact qu'une analyse trop sévère de la part des décideurs pourrait avoir quant aux droits de gérance d'un employeur en matière de surveillance à distance. Il ne fait aucun doute que le télétravail est apprécié par la majorité des employés québécois. Or, celui-ci doit également demeurer profitable pour les employeurs. Des développements jurisprudentiels jugeant trop sévèrement les outils de gestion pouvant être utilisés par les organisations au cours des prochaines années pourraient, selon nous, porter celles-ci à réfléchir quant à l'octroi du privilège de travailler à distance. Rappelons effectivement qu'à moins que le travail à distance ne soit une condition de travail prévue par le contrat de travail d'un employé ou par une convention collective, l'employeur peut généralement y mettre fin.

Par conséquent, une approche conciliant le droit à la vie privée des employés exerçant leur prestation de travail à distance et le droit d'un employeur de gérer efficacement son personnel afin de s'assurer que son entreprise demeure tout aussi profitable que lorsque ses employés sont physiquement présents est, selon nous, la clé du succès pour les deux parties et pour assurer le maintien du télétravail.