GUIDE SUR LA SURVEILLANCE ÉLECTRONIQUE

AYEZ VOS DROITS À L'ŒIL !

UNE VOIX,
UNE FORCE,
UNE fncc CSN
SOLIDARITÉ
EN ACTION

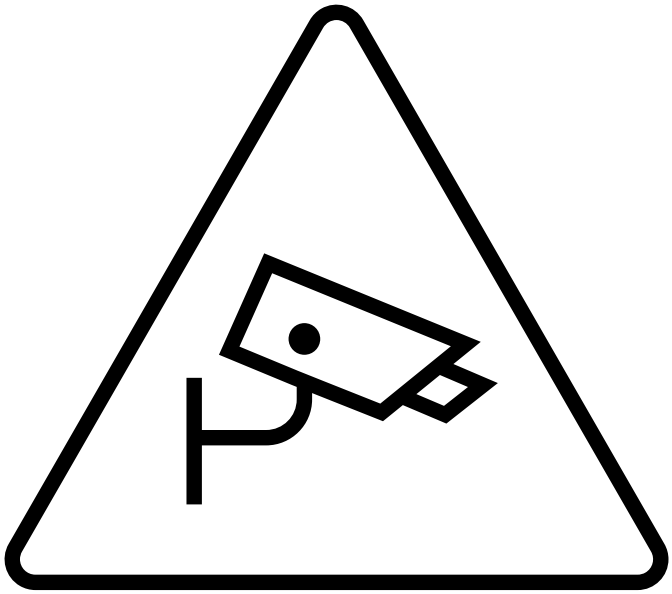
Table des matières

Introduction

La surveillance électronique est souvent associée au télétravail. Toutefois, on observe des formes de surveillance beaucoup plus anciennes que l'ère Covid-19. Force est toutefois d'admettre que la pandémie a accéléré l'avancée technologique des moyens à la disposition des employeurs et que les dernières années semblent être marquées par une croissance du nombre et de l'intensité des moyens de surveillance auxquels sont soumis les travailleuses et travailleurs, parfois même à leur insu. L'intelligence artificielle et la gestion algorithmique y contribuent également.

Cette réalité nous inquiète particulièrement.

C'est pourquoi l'équipe de la FNCC a jugé bon de bâtir le présent guide. Celui-ci se veut non seulement informatif et descriptif, mais il vise également à susciter des réflexions et à permettre aux syndicats d'avoir en main les paramètres nécessaires pour comprendre cette réalité et mieux agir dans leur milieu de travail. Bonne lecture !



Qu'est-ce que la surveillance électronique ?

La surveillance électronique consiste en l'utilisation de tout moyen technologique permettant de connaître, de surveiller, de recueillir et d'enregistrer les activités des travailleuses et travailleurs.

Les outils de surveillance n'ont plus de frontière de temps ni de lieux. Ils permettent de contrôler les travailleuses et travailleurs jusqu'en dehors des heures de travail, le soir, la fin de semaine ou les jours de congés, par exemple, par l'utilisation du cellulaire, d'un ordinateur ou de logiciels fournis par l'employeur. Il en est de même pour le lieu de travail.

Quels sont les enjeux associés à la surveillance électronique ?

Souvent, le réflexe de plusieurs salariées et salariés dans les milieux de travail est de poser la question suivante : « *Je n'ai rien à cacher, je travaille bien. Pourquoi, je devrais m'inquiéter de la surveillance de mon employeur ?* ». C'est donc avec cette prémisse que nous répondons à cette question.

Même si vous n'avez rien à cacher à votre employeur, seriez-vous prêts pour autant à lui permettre de voir ce qui se passe dans votre maison, à lui donner accès à vos courriels personnels ou à vos informations bancaires ?

Permettre à un employeur d'assurer en télétravail une surveillance équivalente à celle qu'il effectue dans un mode de travail présentiel est une chose. Mais là est justement le problème ; le télétravail semble avoir mené à l'augmentation des moyens de surveillance des travailleuses et travailleurs et exacerbé le besoin de contrôle de certains employeurs sur ses employé-es. Et cette surveillance, si elle est exercée, est souvent intrusive et insidieuse.

Même si vous n'avez rien à cacher à votre employeur, trouveriez-vous normal d'avoir constamment un gestionnaire derrière vous qui observe vos activités, qui enregistre chaque message envoyé sur votre ordinateur et à qui, ou qui fait de la filature à chaque fois que vous vous déplacez en voiture dans le cadre de votre travail ?

Généralement, les outils de travail fournis par les employeurs aux travailleuses et travailleurs ne sont pas utilisés en totalité par ces derniers pour des questions liées au travail ou à des fins purement productives. Nous entendons ici l'utilisation pendant les pauses d'applications de divertissement, la consultation occasionnelle des courriels personnels, la connexion à son compte bancaire pour en vérifier le solde, visionner une vidéo drôle transmise par un collègue, etc. Cela ne veut pas dire pour autant que vous êtes malhonnête au travail ou que vous êtes coupable de vol de temps. Toutefois, quand la récolte d'informations est automatique, régulière ou constante, le risque de dérives de toute sorte croît.

Bref, différents enjeux se posent en lien avec la surveillance électronique et reposent principalement sur les éléments suivants :

Le manque de transparence

Sur l'usage ou non de moyens de surveillance.

Sur les autorisations permettant cette surveillance (applications et leurs degrés d'autorisation sur un appareil, accès par l'administrateur réseau, etc.).

Sur l'accès de l'employeur à ces informations (qui a accès, critères pour faire une demande d'accès).

Sur le type d'accès possible (vue ou enregistrement de l'écran en temps réel, décompte du temps inactif d'écran ou de souris, historique de navigation et durée de consultation, etc.).

Sur les salarié-es surveillés (qui ? et combien ?).

Sur la fréquence de la surveillance.

Sur les fins (objectifs) des données récoltées (sécurité de l'entreprise, mesures disciplinaires, etc.).

Sur le stockage des informations personnelles recueillies sur les travailleuses et travailleurs (protection de l'information personnelle).

Sur la durée du stockage de l'information.

Éthique et véracité

Les motifs invoqués par l'employeur pour justifier la surveillance sont-ils véridiques ?

Dissimulent-ils d'autres intentions ?

Les outils de l'employeur sont-ils fiables ? Font-ils la différence lorsque la travailleuse ou le travailleur est en pause et qu'il consulte ses courriels personnels et les autres moments de la journée où il travaille ?

L'intrusion des moyens de surveillance

Les échanges « plus privés » entre collègues ou des membres de sa famille sont-ils révélés à l'employeur ?

Les blagues entre collègues sont-elles lues, entendues par l'employeur ?

Quelles données personnelles sont recueillies ?

Quelles informations sur la vie personnelle, quelles activités de l'employé l'employeur est-il en mesure de recueillir au fil du temps ?

Vulnérabilité des travailleuses et des travailleurs

Instauration de surveillance systématique et continue à l'insu des salarié-es.

Prise en défaut plus facile en contexte de surveillance continue ou régulière.

Quelle est la capacité des travailleuses et travailleurs de réfuter les reproches que l'employeur pourrait faire à leur endroit en utilisant des données recueillies par la surveillance électronique ?

Les salarié-es peuvent-ils se faire reprocher des manquements qui datent de plusieurs années, l'employeur prétextant en avoir eu connaissance seulement lors de la consultation subséquente ?

Sans transparence de la part de l'employeur sur l'exercice de la surveillance, comment un salarié peut-il se sentir en

Exposition de certaines sources journalistiques

La surveillance de travailleuses et travailleurs du milieu journalistique par l'employeur pourrait rendre plus facile l'exposition de certaines sources journalistiques.

Déshumanisation du travail

La travailleuse et le travailleur sont désormais confrontés à des standards automatisés, à des attentes de performance et d'attention éloigné des attentes normales.

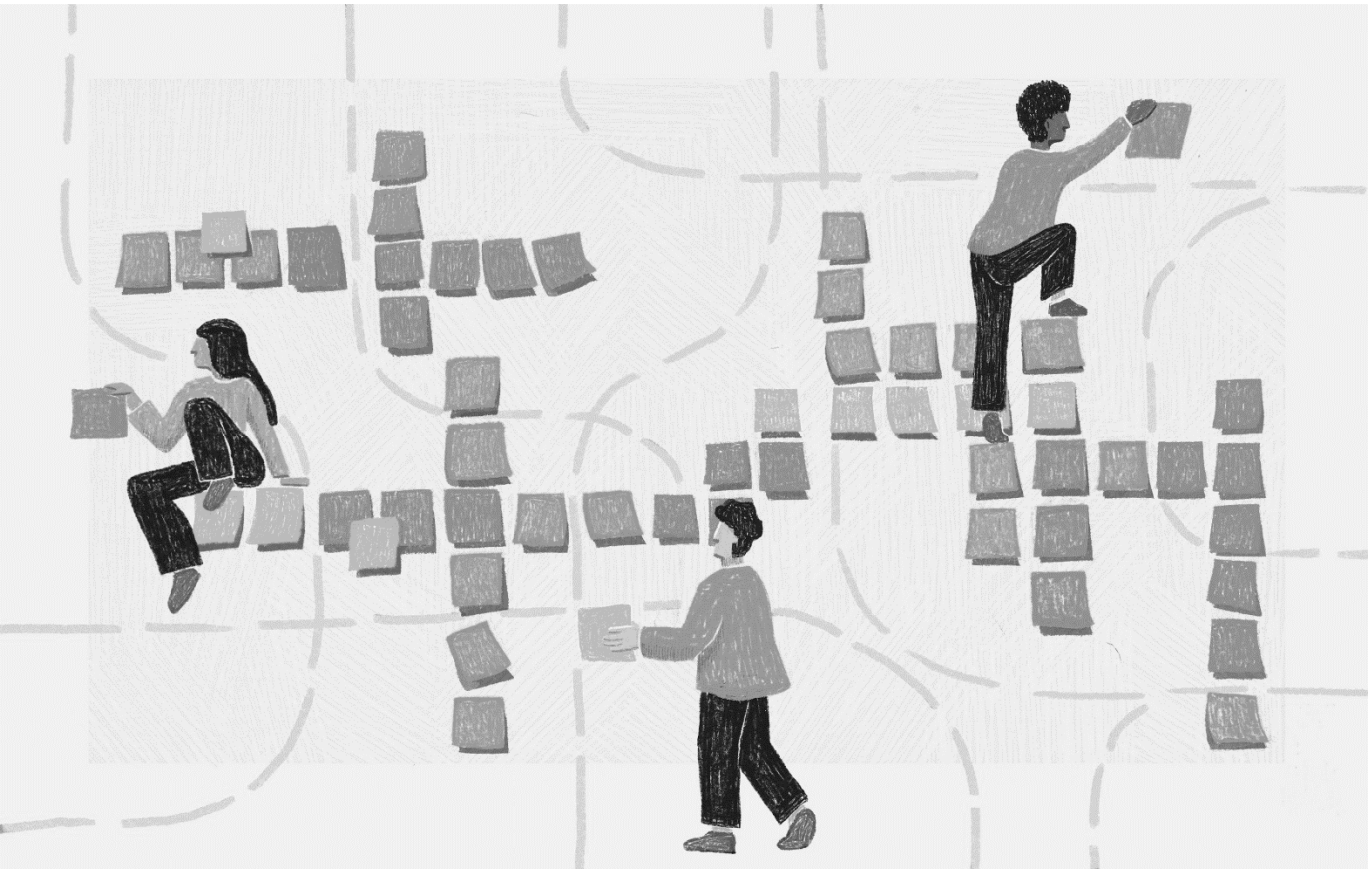
Les comportements deviennent scrutés.

Ce ne sont là que quelques raisons pour lesquelles il est important d'agir et d'encadrer l'utilisation de ces moyens de surveillance électronique.

Les enjeux syndicaux

Nous le répétons souvent. Les activités syndicales ne devraient pas se faire en utilisant les outils et les logiciels fournis par les employeurs. Plus encore, avec la possibilité de surveillance électronique, la vigilance des représentants syndicaux devrait être accrue.

Nous avons répertorié quelques enjeux découlant de la surveillance électronique et auxquels peuvent être confrontés les représentants syndicaux. Ceux-ci portent à réfléchir.



Violation de la confidentialité des conversations privées ou de communications privilégiées

Les conversations entre les représentants syndicaux et leurs membres peuvent être captées ou interceptées.

Même si un employeur ne doit normalement pas obtenir ces conversations, une fois captées, la tentation de les écouter peut être forte.

Accès à des données confidentielles d'enquêtes syndicales.

Accès pour l'employeur à des preuves qui, autrement, il n'aurait pu obtenir :

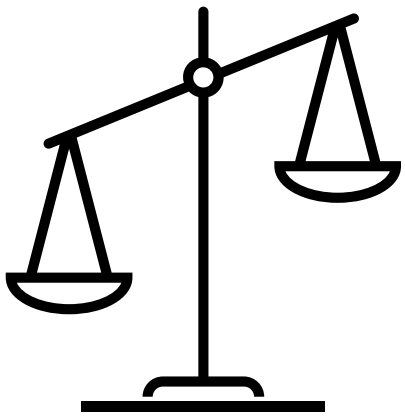
Conversations de groupe sur messageries instantanée (Teams) ;

Extraits de courriels ;

Enregistrement audio de rencontre, etc.

Déséquilibre du rapport de force

Absence ou opacité de l'information transmise par l'employeur au syndicat quant à l'utilisation de la surveillance.



Pas de consultation des syndicats.

Difficulté pour le syndicat de rassurer ses membres.

Difficulté pour le syndicat à cerner les enjeux et à intervenir.

Le syndicat placé constamment en position de défense plutôt qu'en prévention ou en intervention proactive.

Délégitimation du travail syndical.

Difficultés de représentation syndicale

Le manque apparent de littéracie informatique des représentants syndicaux pour bien comprendre les données présentées.

- Peu de représentants semblent maitriser suffisamment l'informatique pour être capables de comprendre, d'interpréter et de confronter le fonctionnement de ces outils.

Difficulté d'assurer une défense adéquate pour les membres

Les données recueillies à l'aide d'outils technologiques et les moyens utilisés pour les recueillir peuvent présenter des enjeux techniques importants et peuvent être difficiles à interpréter.

L'utilisation d'expert pour analyser ou attester des rapports ou données extraites des outils technologiques sera-t-elle nécessaire ?

La difficulté à attester de l'authenticité des données de surveillance utilisées.

Le rapport technique utilisé par un gestionnaire est-il issu d'une collecte automatisée des données ou a-t-il été interprété par un « humain » afin d'y apporter des nuances ?

Utilisation de la preuve en arbitrage

L'arbitre est-il compétent pour comprendre les données qui lui seront présentées ?

La preuve peut être complexe et lourde à administrer.

La nécessité d'exercer des recours pour faire écarter l'utilisation de données.

Discrimination et catégorisation des employé-es

Le risque d'utilisation de la surveillance pour discriminer des travailleuses et travailleurs selon certaines de leurs caractéristiques identifiées par la technologie de surveillance.

La création de profils de salarié-es.

L'analyse des comportements.

Divulgation d'informations lors de travail de nature syndicale

Les représentants syndicaux utilisant les outils technologiques de l'employeur s'exposent à de la surveillance électronique.

La possible surveillance pendant les activités ou heures de libérations syndicales.

- Comment tracer la ligne entre la surveillance électronique pendant le travail et pendant les libérations syndicales ?
- Il n'y a pas de mode « privé » sur les outils de travail lorsque vient le temps de réaliser un travail syndical.

Accès par l'employeur à plusieurs informations :

Qui communique avec les représentants syndicaux ?

À quelle fréquence ?

À quel moment de la journée ?

Pour quels sujets ?

Les stratégies et tactiques de négociation.

Les positions du comité de négociation.

Les actions de mobilisation et moyens de pression qui seront posés.

La possibilité de récupérer le lien de sondage et que l'employeur ait accès aux données ou qu'il puisse y réponde lui-même pour influencer des résultats.

Enjeux de loyauté au sein de l'organisation

Exposition de salarié-es d'une même unité d'accréditation à des conflits de loyauté, de valeurs ou à de la méfiance de collègues s'ils gèrent des outils technologiques et que l'employeur se sert d'eux pour amasser de l'information sur des collègues.

Enjeux de protection des renseignements recueillis

Les données recueillies par l'employeur sont-elles bien protégées ?

a. Qui y a accès ?
b. Quels sont les critères ?
c. Qui juge du bien-fondé des motifs raisonnables de consulter ces renseignements ?

Les données récoltées par l'employeur pourraient-elles se retrouver entre de « mauvaises mains » ?

Certains employeurs pourraient-ils aller jusqu'à vendre, marchandiser les données récoltées ?

Les différents types de surveillance électronique répertoriés

Dans une récente étude réalisée par le Service aux collectivités de l'UQAM[1], les chercheurs associés au dossier ont procédé à une recension complète et exhaustive des différentes catégories de surveillance électronique. Nous vous les reproduisons ici dans certains passages du guide pratique[2] conçu à partir des résultats de l'étude.

Les types de surveillance peuvent se décliner en deux catégories : La surveillance hors ordinateur et celle sur ordinateur.

[1]Ariane Ollier-Malaterre, Sabrina Pellerin, Xavier Parent-Rocheleau, Yanick Provost-Savard. (2024). *La surveillance électronique des employé.e.s au Québec, Recherche partenariale UQAM-CSN-CSQ-FTQ*.
[2] Provost Savard, Y., Pilon, É., Provost-Cardin, É., Ollier-Malaterre, A. et Parent-Rocheleau, X. (2024) *Guide pratique sur la surveillance électronique au travail*, 7 p

La surveillance hors ordinateur

Carte à puce/badge

Description : Suivi de l'emplacement des employé-es, des heures auxquelles ils se trouvent dans le bâtiment, ou de l'usage des appareils ou véhicules.

Exemple : Un machiniste qui doit utiliser une carte à puce afin d'opérer la machinerie

OUI	NON	?
60 %	33 %	7 %

Médias sociaux

Description : Surveillance (ou archivage) des publications des employé-es sur leurs réseaux sociaux personnels.

Exemple : Surveillance (ou archivage) des publications des employé-es sur leurs réseaux sociaux personnels.

OUI	NON	?
22 %	28 %	50 %

Écoute d'appels et microphones

Description : Surveillance des communications orales.

Exemple : Les appels d'un agent de centre d'appels sont écoutés de manière périodique.

OUI	NON	?
15 %	49 %	36 %

Géolocalisation

Description : Localisation des employé-es et suivi de leurs déplacements, sur les lieux de travail ou à l'extérieur.

Exemple : L'utilisation du GPS afin de surveiller la vitesse de conduite d'un livreur

OUI	NON	?
21 %	56 %	23 %

Caméras

Description : Utilisation de caméras pour surveiller les comportements des employé-es en temps réel.

Exemple : Des caméras dans les couloirs d'un hôpital avec surveillance active par des agents de sécurité.

OUI	NON	?
28 %	51 %	21 %

Caméra avec reconnaissance faciale

Description : Identification des employé-es via la reconnaissance faciale.

Exemple : Un employé doit utiliser l'accréditation par reconnaissance faciale pour se connecter à un appareil.

OUI	NON	?
3 %	79 %	18 %

La surveillance sur ordinateur

Sites internet consultés

Description : Enregistrement et suivi actif de toute l'activité de l'utilisatrice ou l'utilisateur sur les navigateurs internet (historique des pages consultées, temps passé sur chaque page, vidéos visionnées, etc.).

Exemple : L'activité numérique d'un employé est enregistrée et surveillée, avec des alertes pour certains sites web consultés, comme un site de recherche d'emplois

OUI	NON	?
38 %	14 %	48 %

Statut d'activité sur Teams ou autre plateforme

Description : Comptabilisation des moments et du temps où l'ordinateur n'enregistre aucune activité sur une application ou plateforme pendant une période donnée.

Exemple : La surveillance du statut sur Teams et l'enregistrement des périodes où le statut est « disponible ».

OUI	NON	?
27 %	25 %	47 %

Transfert et téléchargement de fichiers (Clé USB ou autres)

Description : Suivi et enregistrement des téléchargements de fichiers disponibles sur le réseau (sur des dispositifs USB ou sur d'autres périphériques).

Exemple : Tous les transferts de fichier d'un employé sur le réseau du bureau sont listés et enregistrés.

OUI	NON	?
15 %	49 %	36 %

Contenu des courriels

Description : Stockage et analyse du contenu des courriels, y compris le texte, les pièces jointes et d'autres éléments.

Exemple : La vérification du contenu des courriels d'un employé pour certains mots clés spécifiques.

OUI	NON	?
30 %	16 %	54 %

Captures d'écran

Description : Captures épisodiques de l'écran de l'ordinateur, incluant les onglets ouverts et l'activité en cours.

Exemple : Capture régulière de l'écran d'un employé afin de surveiller les activités non productives, comme les réseaux sociaux.

OUI	NON	?
14 %	28 %	58 %

Surveillance de la messagerie instantanée

Description : Enregistrement et suivi actif du contenu des messages instantanés, y compris le texte, les emojis et d'autres contenus.

Exemple : La vérification du contenu des messages privés entre deux employé-es, pour vérifier le risque de départ.

OUI	NON	?
15 %	19 %	62 %

La surveillance sur ordinateur

Mouvement de la souris

Description : Comptabilisation des moments et du temps où l'ordinateur n'enregistre aucun mouvement de la souris pendant une période donnée (aussi peu qu'une minute).

Exemple : Compilation du temps sans mouvement de souris pour générer un score de productivité pour chaque employé-e.

OUI	NON	?
12 %	37 %	51 %

Nombre de frappes sur le clavier

Description : Comptabilisation des moments et du temps où l'ordinateur n'enregistre aucun mouvement sur le clavier pendant une période donnée (aussi peu qu'une minute).

Exemple : La mesure de la productivité d'un employé basé sur le nombre de frappes sur le clavier.

OUI	NON	?
8 %	39 %	53 %

Photos depuis la caméra de l'ordinateur

Description : Prise de photos des employé-es par la caméra frontale de l'ordinateur.

Exemple : Des photos sont prises durant la journée de travail afin de vérifier qu'une employée est à son poste.

OUI	NON	?
4 %	37 %	59 %

Surveillance des rencontres en visioconférence

Description : Surveillance (enregistrement ou écoute) des réunions virtuelles réalisées sur les ordinateurs de l'employeur.

Exemple : L'enregistrement et la transcription du contenu de la réunion, qui est ultérieurement visionné par un superviseur

OUI	NON	?
28 %	22 %	50 %

Surveillance d'écran en temps réel

Description : Visualisation des écrans de l'ordinateur en temps réel.

Exemple : Une gestionnaire consulte de temps à autre les écrans de ses employé-es pour s'assurer de leur productivité.

OUI	NON	?
11 %	30 %	59 %

Surveillance vidéo constante depuis la caméra de l'ordinateur

Description : Utilisation de la caméra frontale de l'ordinateur pour surveiller les employé-es en continu et en temps réel tout au long de la période de travail (enregistré ou non).

Exemple : Une vidéo est prise durant la journée de travail afin de vérifier qu'un employé demeure à son poste de manière à contrôler sa prestation de travail.

OUI	NON	?
19 %	19 %	62 %

Quelques constats de recherche

La recherche effectuée par le Service aux collectivités de l'UQAM a également permis de dégager des constats alarmants :

82 % des répondants rapportent être soumis à au moins une surveillance électronique ;

71 % des répondants à l'étude ont déclaré avoir au moins une technologie de surveillance sur son ordinateur ;

50 % des répondants ne savent pas si leurs médias sociaux sont surveillés ;

36 % des répondants ne savent pas si leurs appels sont écoutés ;

39 % des répondants pensent que leur employeur pourrait utiliser les technologies pour d'autres raisons que celles annoncées.

63 % des répondants sont inquiets de ne pas pouvoir supprimer les informations que leur employeur recueille sur eux ;

72 % des personnes sondées sont d'avis que leur utilisation des technologies facilite l'intrusion de leur employeur dans leur vie privée.

Le cadre juridique[3]

De manière générale, une surveillance « conventionnelle » et occasionnelle d'un gestionnaire envers un employé, pour, par exemple, vérifier la qualité de la prestation de travail est acceptée. Cette acceptation du droit de gestion de l'employeur est toutefois conditionnelle à ce que celui-ci soit exercé de manière non abusive, discriminatoire ou arbitraire.

Toutefois, les nouveaux moyens technologiques permettent une surveillance étroite, constante, épiant un large spectre d'activités professionnelles, mais aussi personnelles. La surveillance peut maintenant être automatique, à l'aide d'algorithmes ou d'intelligence artificielle.

À titre d'exemple, en novembre 2023, un article[4] de Brigitte Bureau de Radio-Canada mettait en lumière l'utilisation par 13 ministères et agences du gouvernement fédéral d'outils capables d'extraire les données personnelles de téléphones ou d'ordinateurs dans le cadre notamment d'enquête de harcèlement psychologique ou de fraude. Cette réalité ne semble cependant qu'être la pointe de l'iceberg puisque les motifs de cette surveillance sont aussi larges que « des violations des politiques du gouvernement ». Les données recueillies pouvaient aller jusqu'aux contacts, courriels, textos, photos, historiques des déplacements et recherches sur internet et aux contacts.

Devant l'ampleur de la situation, nous pouvons nous poser la question : quel est le cadre de référence juridique concernant la surveillance électronique ?

---

[3] La présente section n'est pas un avis juridique ou une analyse exhaustive, mais seulement un guide d'action pour mieux permettre l'action syndicale en pareilles circonstances.

[4] Brigitte Bureau. *Des outils potentiellement intrusifs utilisés par au moins 13 ministères fédéraux.* 29 novembre 2023 https://ici.radio-canada.ca/info/long-format/2030420/logiciels-espionnage-vie-privee-gouvernement-federal

Un employeur peut-il surveiller ses employés comme il veut, quand il veut ?

Pour mieux comprendre quels sont les principes juridiques encadrant la surveillance électronique, il y a lieu de définir ce qu'elle est. Pourtant, tenter une définition relève de l'exercice de l'équilibriste. En définissant les contours des moyens technologiques servant à encadrer la production des salariés, on se rend vulnérables à une limite définie qui pourrait nous rendre perméables à des technologies non prévues ou qui n'existaient pas au moment où se fixent les contours de notre définition.

Autrement dit, nommer un concept, c'est aussi inclure et exclure ce qui le définit. Maintenant avertis, risquons-nous à définir, de manière perfectible, le concept de surveillance électronique.

Nous nous inspirerons des travaux de certains auteurs[5] pour mieux circonscrire le tout. Ainsi, nous retiendrons que la surveillance électronique peut se définir comme « tout moyen de contrôle technique sur une personne ou un processus, liés aux nouvelles technologies et plus particulièrement aux réseaux numériques de communication[6] ».

[5] Grenon, Camille G et Massé-Lacoste, Catherine, Télésurveillance : le contrôle de la prestation de travail à l'ère du télétravail et ses limites, Développements récents en droit du travail (2022), Barreau du Québec - Service de la formation continue, 2022/08/01 (ci-après « Télésurveillance »)

[6] Hortense Y. EONE, La cybersurveillance des salariés à l'ère du web 2.0, Montréal, Éditions Yvon Blais, 2013, p. 3,

Moyens et utilisation

De manière générale, les employeurs utilisent les outils de surveillance pour différents usages. On peut parler, à titre d'exemple, de protection du matériel, en passant par la propriété intellectuelle, la gestion des informations confidentielles, la protection de son image et de sa réputation,[7] l'accroissement du contrôle sur la production, etc. Ces moyens de contrôle prennent plusieurs formes comme les tableaux l'indiquaient précédemment.

Par conséquent, aux vues de la diversité des formes de surveillance électronique, étudier leur encadrement nécessite que nous nous penchions sur plusieurs concepts. Ainsi seront traités les principes juridiques de base, les principes spécifiques, l'encadrement du contrôle sur les conditions de travail autre que les outils, l'encadrement du contrôle sur les outils de travail ainsi que la question des recours.

Principes juridiques de base

De manière générale, la Charte canadienne[8] et plus particulièrement la Charte des droits et libertés de la personne[9] viennent protéger le droit à l'inviolabilité du domicile, le droit à la dignité ainsi que le droit à protection de la vie privée.

Un employeur qui voudrait surveiller de manière électronique va donc devoir démontrer que la mesure qui viendrait restreindre ces droits fondamentaux ou, autrement dit, qui serait intrusive est faite « dans la poursuite d'un objectif légitime et important et qu'elle est proportionnelle à cet objectif[10] ». Afin de mieux comprendre l'importance accordée à cet équilibre, dans la décision *syndicat des professionnelles et professionnels municipaux de Montréal et Ville de Montréal (grief syndical) 2020 QCTA 358*, le juge rappelle les principaux éléments relatifs au cadre juridique :

« [7] En matière de condition déraisonnable de travail, le syndicat doit démontrer prima facie une atteinte au droit protégé par l'article 46 de la Charte. Lorsque l'atteinte découle d'une surveillance, il doit démontrer que celle-ci est constante ou continue.

[8] En matière d'atteinte au droit à la vie privée, le syndicat doit établir le niveau d'expectative de vie privée auquel l'employé peut s'attendre dans son milieu de travail et en lien avec l'atteinte alléguée. Pour décider s'il y a atteinte à la vie privée de l'employé,

[7] Télésurveillance, ibid p. 11.
[8] Charte canadienne des droits et libertés, partie I de la Loi constitutionnelle de 1982 [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.)], art. n°7 et 8.
[9] Charte des droits et libertés de la personne, RLRQ, c. C-12, art. n°.5
[10] Télésurveillance, ibid p. 15.

le tribunal doit déterminer si l'employé a une attente subjective raisonnable du respect de sa vie privée dans le cas à l'étude. Plus l'expectative de vie privée sera restreinte, moins le risque d'atteinte sera présent.

[9] Dans les deux cas, une fois l'atteinte à la Charte démontrée, il y a renversement du fardeau de preuve et l'employeur doit justifier l'atteinte en établissant qu'il a un motif raisonnable, réel et sérieux, c'est-à-dire rationnel, pour porter atteinte à l'un de ses deux droits fondamentaux et qu'il y a proportionnalité entre ce motif et le moyen utilisé.

[10] La proportionnalité est respectée lorsque l'employeur démontre la nécessité du moyen utilisé et son lien direct avec la problématique soulevée et que ledit moyen est le moins intrusif possible. »

Ces propos ont été repris dans plusieurs autres affaires dont la Cour suprême[11], et de fait, constituent la pierre d'assise avec lesquelles on doit jongler en matière de restriction à un droit fondamental, soit, nommément, le respect de la vie privée.

Motifs sérieux

L'employeur voulant surveiller ses employés devra fournir les motifs au soutien de sa demande. Il ne doit pas prouver la certitude ou la véracité de ces motifs, mais l'existence d'un lien[12]. Le contrôle du travail d'un salarié est un droit reconnu de l'employeur, mais pas celui de la surveillance continue[13].

Ainsi, à titre d'exemple, un employeur pourrait braquer ses caméras sur certains endroits déterminés dans un délai déterminé en cas d'une vague de vols, mais il ne pourrait pas le faire pour contrôler l'exécution du travail.

Comme l'écrivent les auteurs Massé-Lacoste et Grenon, un intérêt économique ne peut pas satisfaire aux critères du motif sérieux. Il faut que la surveillance soit associée au motif visé :

« À ce titre, l'arbitre dans Syndicat de l'enseignement de la région des Moulins et Commission scolaire des Affluents retient qu'une surveillance générale, continue, sans objet précis autre que le fait de pouvoir éventuellement être utilisée pour tout motif disciplinaire, qui est exercée sans justification à l'égard de salariés se trouvant dans leur milieu de travail quotidien et dans l'exercice de leurs fonctions, est inconciliable avec la Charte québécoise (art. 46). »[14]

---

[11] Voir à cet effet R. v. Gomboc, 2010 SCC 55, [2010] 3 S.C.R. 211, R. c. Plant, [1993] 3 R.C.S. 281 et R. c. Jarvis, [2002] 3 R.C.S. 757, 2002 CSC 73.

[12] syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (CSN) c. Trudeau, 1999 CanLII 13295 (QC CA)

[13] Voir à cet effet : syndicat des travailleurs et travailleuses de Sysco-Québec (CSN) et Sysco Services alimentaires du Québec, 2016 QCTA 455 (caméras en continu dans les camions), pourvoi en contrôle judiciaire rejeté (2017 QCCS 3791) ; Société VIA inc. et syndicat des travailleurs unis du Québec, 2017 QCTA 964 (caméras en continu dans l'établissement) ; Ville de Gatineau et Association des pompiers et pompières de Gatineau, 2018 QCTA 730 (caméras en continu à l'extérieur et à l'intérieur).

[14] Télésurveillance, ibid

Lien rationnel

Une fois le motif sérieux démontré, la mesure potentiellement illégale doit faire l'objet d'un autre examen, à savoir si ce moyen utilisé est en lien avec le motif. Ainsi, il ne suffit pas d'avoir un motif sérieux. Il faut que la mesure de contrôle soit appropriée. Il faut que le moyen soit nécessaire pour atteindre les objectifs visés par le motif. Une surveillance généralisée ne serait pas plus appropriée du fait qu'on fournit un motif.

À titre illustratif, si nous devions mesurer les mouvements de souris d'une personne pour évaluer s'il y a vol de temps, il y aurait des écueils majeurs du fait, notamment, qu'un logiciel pourrait simuler le mouvement d'une souris ou le fait qu'on ne peut mesurer le temps de réflexion relatif à l'exécution d'une tâche.

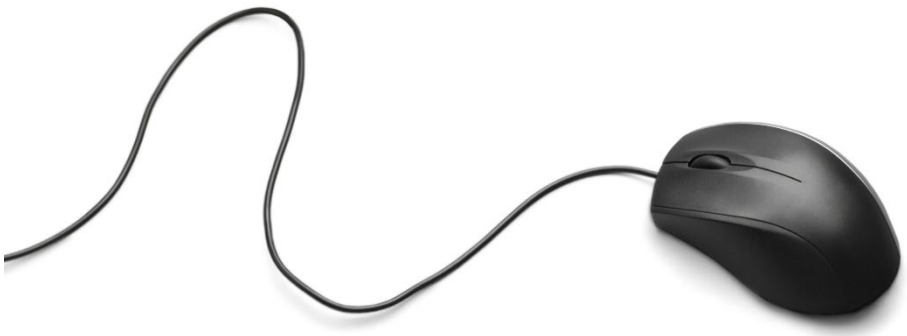
Proportionnalité

Enfin, le test de la proportionnalité s'inspire de la jurisprudence relative à la filature[15] et la surveillance vidéo[16]. Dans ces cas on se pose la question[17] :

- La perte de vie privée est-elle proportionnelle à l'avantage obtenu ?

- La surveillance doit être menée de la manière la moins intrusive possible et le cas échéant, il n'y a pas d'autres moyens moins intrusifs ;

Ce test vient généralement disqualifier plusieurs méthodes systémiques de surveillance puisque la balance de la proportionnalité n'est généralement pas rencontrée.



[15] Note 12 précitée.

[16] syndicat des professeures et professeurs de l'Université du Québec en Outaouais (SPUQO) et Université du Québec en Outaouais, 2016 QCTA 700

[17] Télésurveillance, ibid p.

Principes spécifiques

En plus des principes constitutionnels ou de cette nature, plusieurs lois et règlements viennent également paramétrer les principes de surveillance électronique. Le *Code civil du Québec* vient reprendre les principes jurisprudentiels ci-haut mentionnés en indiquant que la constitution d'un dossier doit avoir un intérêt légitime et sérieux de le faire et l'obligation de protéger la santé et la sécurité au travail en plus de la dignité[18].

Également, la *Loi sur la santé et la sécurité au travail* entraîne des obligations auprès de l'employeur sans égard au lieu de travail de l'employé-e. Ce faisant, l'employeur peut tenter de contrôler la manière dont le télétravail est réalisé, mais il doit le faire de la manière la moins intrusive possible, et ce, même s'il a des obligations légales relatives à la réduction à la source même des risques à la santé. Ainsi, les droits de visite dans le lieu de résidence de l'employé-e ne sont pas acquis et lorsque nécessaire (ce qui est rarement le cas), ils doivent être extrêmement circonscrits. Une présentation numérique du poste de travail devra être privilégiée.

Par ailleurs, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels dans le secteur privé viennent paramétrer la cueillette des informations et renseignements [19]. Seuls les renseignements nécessaires à l'objet du dossier peuvent être recueillis et cette cueillette vient avec l'obligation corolaire de disposer voire détruire ces informations lorsque l'objet du dossier est finalisé. Ces obligations ont été largement renforcées depuis l'adoption le 22 septembre 2023 du projet de loi 25[20]. Ces enjeux restent donc centraux et la protection offerte est d'autant plus vraie que ladite loi vient renforcer les pouvoirs de la Commission d'accès à l'information et les matières pénales incidentes en cas de contravention[21].

Enfin, avec la multiplication des outils technologiques vient parfois l'obligation de disponibilité qui y est incidente. Un employeur qui exigerait d'utiliser un outil personnel pour des fins professionnelles serait, notamment, beaucoup plus restreint dans son droit au contrôle, car le test de la proportionnalité viendrait largement peser en faveur du droit à la vie privée et il devrait également rembourser les coûts de l'outil[22], en plus de payer pour l'obligation de disponibilité au-delà de l'horaire normal de travail.[23]

Il peut être opportun de paramétrer dans les conventions collectives majoritairement de professionnels n'ayant pas d'horaires définis des dispositions de droit à la déconnexion pour faciliter la capacité de décrocher. L'Ontario a une disposition [24] dans la loi équivalant à notre *Loi sur les normes du travail* portant sur ces éléments.

---

[18] Code civil du Québec, RLRQ c CCQ-1991 art. n°36, 37, 2085 et 2087.
[19] Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ p-39.1 art. n°6 et suivants.
[20] Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25
[21] Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ p-39.1 art. n°91 et suivants.
[22] Rassemblement des employés techniciens ambulanciers de l'Abitibi-Témiscamingue (CSN) et Ambulance du Nord inc., D.T.E. 99T-36 (QCTA).
[23] Loi sur les normes du travail, RLRQ, N-1.1 art. n°64
[24] https://www.ontario.ca/fr/document/votre-guide-de-la-loi-sur-les-normes-demploi-0/politique-ecrite-deconnexion-travail

Applications : les conditions de la surveillance par les outils de travail

Nous prendrons dans cette section quelques cas d'espèce pour mettre en relief les cas ci-haut présentés.

Appels 

L'enregistrement systématique des conversations téléphoniques crée un enjeu[25]. L'arbitre Nadeau a retenu que l'enregistrement continu des salarié-es entre eux lors d'une conversation téléphonique avec la liste de rappel était contraire à leurs droits. Notons que l'employeur n'avait pas fait la preuve qu'il n'existait pas d'autres moyens qui pourraient moins préjudicier les salariés.

Cette politique d'enregistrement était contraire « au degré d'autonomie et d'intimité qui va de pair avec le respect de la dignité des salariés. »[26] Elle se différenciait des appels externes avec des clients qui pouvaient avoir certains bénéfices quant à l'enregistrement. Rappelons que la voix est un renseignement personnel[27] et doit être protégé comme tel.

Ordinateur et courriel 

Il faut préciser que c'est l'information contenue dans l'ordinateur et non le matériel qui fait l'objet d'une protection[28]. Ainsi, même si l'ordinateur est la propriété de l'employeur, la protection et le droit à la vie privée subsistent tout de même. Les salarié-es ne renoncent pas à leur droit à la vie privée du seul fait qu'ils utilisent les outils de l'employeur.[29]

Cela étant dit, l'employeur peut toutefois contrôler le temps de travail et l'utilisation de ses outils. Ainsi, en matière de navigation internet, un rapport de journalisation de navigation internet est conforme aux principes de droit s'il s'agit d'un échantillonnage à des fins de supervision[30].

Dans la décision SCFP et AMF[31], concernant un logiciel rappelant Teams dans son fonctionnement, l'arbitre Garneau est venu rappeler que le recours systématique est inconciliable avec les objectifs visés par la Charte, mais que la messagerie, semblable à celle de Teams, peut être utilisée pour des motifs sérieux, comme ce fut le cas en l'espèce.

---

[25] syndicat des travailleurs et travailleuses du CSSS de l'Énergie - CSN catégorie 2 - 3 et Centre de santé et de services sociaux de l'Énergie (CIUSSS de la Mauricie-et-du-Centre-du-Québec) 2017 QCTA 33.
[26] Idem.
[27] C.R. c. Loto-Québec, 2012 QCCAI 300., cité dans télésurveillance, précité p. 40.
[28] Patrick GINGRAS et Éloïse GRATTON, « Accéder ou ne pas accéder au matériel informatique de son employé, telle est la question », Développements récents en droit du travail (2014), vol. 383, Montréal, Éditions Yvon Blais, en ligne : https://edoctrine.caij.qc.ca/developpements-recents/383/368185469
[29] R. c. Cole, 2012 CSC 53, [2012] 3 R.C.S. 34
[30] 2020 QCTA 358 (demande de pourvoi en contrôle judiciaire rejetée : 2022 QCCS 363)
[31] 2019 CanLII 85539 (QC T.A., pourvoi en contrôle judiciaire rejeté : 2021 QCCS 4505).

Enfin, l'arbitre Cléroux dans la décision *La Presse* rappelle que la directive de l'employeur était non contestée par le syndicat en l'espèce et qu'en conséquence, l'utilisation de courriels du photographe pour fins disciplinaires n'a pas été jugée contraire aux droits du salarié.[32]

De manière générale, il est important de se rappeler que de chercher des informations dans l'ordinateur peut s'apparenter à une fouille et qu'en conséquence, ce n'est pas interdit, mais encadré. Ce qui signifie qu'une politique d'employeur intrusive et abusive comme celle de La Presse devrait être contestée par les syndicats.

Vidéo 

Comme indiqué à plusieurs reprises, de manière générale, la télésurveillance et particulièrement la surveillance vidéo en continue est proscrite, car elle est porte atteinte aux droits des personnes. L'article 46 de la Charte des droits et libertés de la personne est venu en effet garantir le droit à des conditions de travail justes et raisonnables et l'article 5 le droit à la vie privée.[33]

Cela dit, un employeur peut avoir des motifs sérieux comme, par exemple du vol de temps, qui surviendrait après une surveillance sporadique moins intrusive et selon certaines circonstances, l'enregistrement vidéo dans un espace-temps ciblé serait permis.

Évidemment, l'enregistrement des renseignements ainsi recueillis doit être traité selon les mêmes paramètres que toute autre information recueillit selon la *Loi sur la protection des renseignements dans le secteur privé* (LPRSP).

Déplacement et biométrie 

D'abord, la géolocalisation est encore plus encadrée que certaines autres cueillettes d'informations. En effet, l'article 43 de la *Loi concernant le cadre juridique des technologies de l'information* requiert une approbation de la part des salarié-es pour prendre ces informations en notes.

La jurisprudence est extrêmement divisée sur le droit à la géolocalisation par l'employeur, notamment sur le fait qu'une géolocalisation peut se faire sans le consentement exprimé des salariés. Ainsi, pour certains arbitres, cette saisie est illégale et contraire à certaines dispositions législatives.

Quant à la biométrie, certains employeurs exigent et recueillent des données, telles que l'empreinte des mains. Ces données assez sensibles font l'objet d'une protection plus grande en vertu de la LPRSP.

[32] syndicat des travailleurs de l'information de la presse c. La Presse (2018) inc., 2021 CanLII 10825 (QC SAT)

[33] Voir la note 10 à cet effet.

Gestion algorithmique 

La question du droit du travail et de la gestion algorithmique en est à leur balbutiement. Cependant, des auteurs notent certains risques associés à l'intelligence artificielle. Ainsi, Élodie Morton, dans le cadre de son mémoire de maitrise[34] indiquait que des biais de discrimination pouvaient se glisser dans certains algorithmes dans la manière de recruter des candidats.

Lorsqu'on met en application ces principes dans le domaine spécifiquement de la surveillance électronique, les algorithmes présentent la difficulté de ne pas se dévoiler ou de s'identifier par eux-mêmes. Tant et aussi longtemps que nous n'avons pas l'information sur l'algorithme, toute forme de cueillette de données va présenter des risques, notamment parce qu'on ne sait pas d'où on tire l'information à quoi va servir l'information si on constitue un dossier ou non combien de temps ça va être conserver, etc.

Ces risques s'appliquent tant du côté de l'évaluation du rendement, le traitement d'une candidature ou, comme indiqué ci-haut, en matière d'embauche. L'accès à l'algorithme[35], mais aussi, sa signification devient donc un enjeu supplémentaire pour contrôler la surveillance électronique faite par l'employeur.

Réseaux sociaux 

Bien que relevant des nouvelles technologies de l'information, les réseaux sociaux peuvent ne pas recevoir le même niveau de protection que d'autres espaces si l'employé-e révèle comme publiques certaines informations. À cet effet, notons que dès 2012, l'usage des réseaux sociaux préoccupait déjà la *Conférence des arbitres* qui tint une journée de formation relativement à ces enjeux[36].

Ce qu'il faut retenir c'est que les conversations privées sur Facebook (Messenger et groupes privés) ne sont pas considérées comme étant du domaine privé entre les destinataires de cette conversation et que l'employeur pouvait donc en faire usage s'il entre en possession de cette information. En effet, dans l'affaire Parc Omega inc. et Ivall[37], la juge Gosselin a estimé qu'il y a absence d'expectative de vie privée pour les auteures d'une conversation sur Facebook.

---

[34] Morton, Élodie, L'intelligence artificielle de recrutement : appréhender les risques de discrimination, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maitrise en Droit des Technologies de l'Information (LL.M), https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/27016/Morton_Elodie_%202021_memoire.pdf?sequence=2&isAllowed=y

[35] Télésurveillance, ibid, p.61-62.

[36] Voir à cet effet : Mes amis facebook, moi et mon emploi : l'arbitrage de grief à l'ère des réseaux sociaux, Les cahiers de la Conférence des arbitres du Québec, Wilson & Lafleur, 2012, 249 p., ISBN 978-2-89689-069-9.

[37] Parc Omega inc. et Ivall 2017 QCTAT 915

Recours

En cas de violation aux principes relatifs à la vie privée, la personne salariée ou le syndicat peut déposer un grief pour réclamer auprès de l'arbitre de grief que cesse l'atteinte au droit ainsi qu'une réparation des préjudices soit faite. Il est à noter qu'en cas de violation reconnue de droits fondamentaux, les arbitres sont généralement plus enclins à ordonner le versement de dommages auprès du plaignant.

Également, la Loi 25 donne également des pouvoirs d'enquête élargis à la Commission d'accès à l'information (CAI). Plus précisément, selon l'article 81 de ladite Loi :

« *La Commission peut, de sa propre initiative ou sur la plainte d'une personne, faire enquête ou charger une personne de faire enquête sur toute matière relative à la protection des renseignements personnels ainsi que sur les pratiques d'une personne qui exploite une entreprise et recueille, détient, utilise ou communique à des tiers de tels renseignements. Une plainte peut être déposée sous le couvert de l'anonymat*. »

Elle dispose pour l'enquête : « des pouvoirs et de l'immunité prévus par la Loi sur les commissions d'enquête (chapitre C-37) sauf le pouvoir d'ordonner l'emprisonnement. [38] »

La CAI peut alors ordonner le versement de pénalités selon les dispositions édictées par la Loi.

Enfin, une contravention à ces droits peut donner ouverture à la reconnaissance d'un accident de travail s'il y a une lésion professionnelle en vertu de la *Loi sur les accidents du travail et les maladies professionnelles*. Il y a alors lieu d'évaluer les faits en l'espèce pour s'assurer que le membre y soit admissible.

[38] Précité note 17, art. 81.

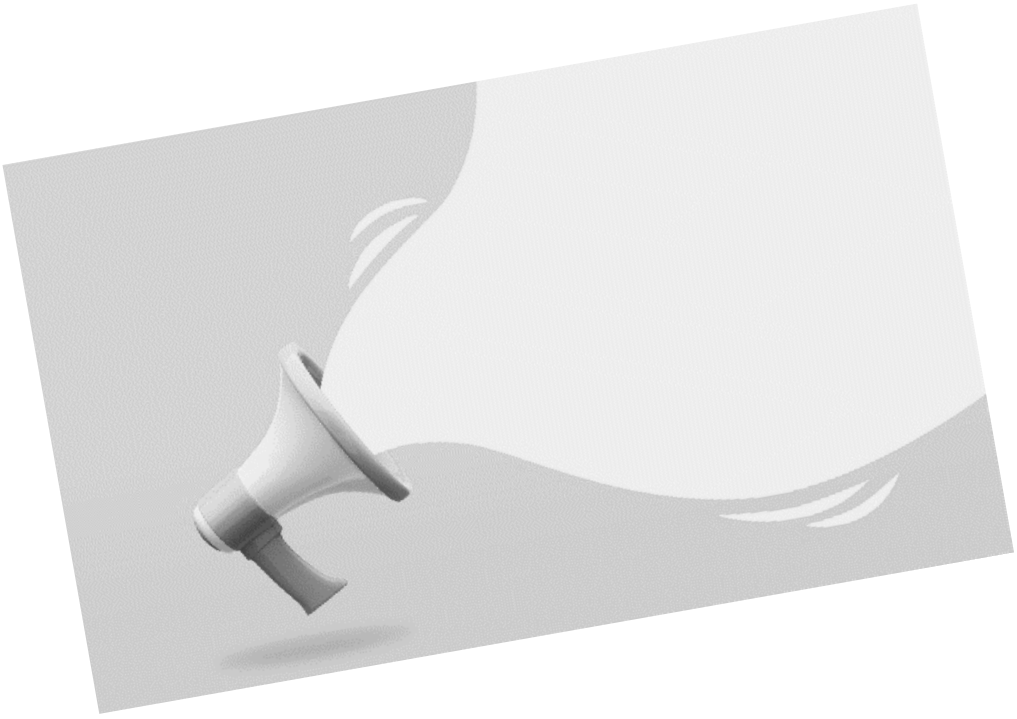
Clauses et éléments à intégrer dans nos conventions collectives ?

Maintenant que certains constats sont posés et que plusieurs inquiétudes sont décelées avec la surveillance électronique, il est maintenant l'heure de se poser la question : que faisons-nous ?

La clé à cette question repose à notre avis sur l'action et la prise en charge syndicales. Souhaitons-nous laisser un sujet si important entre les seules mains des employeurs ? À notre avis, nous ne devrions pas. Ainsi, il est nécessaire d'exiger de la transparence des employeurs. Il est requis d'obliger ces derniers à dévoiler le type de surveillance effectuée de leurs employé-es, sa fréquence et son utilisation. Et également de le limiter.

L'inaction n'est pas une option.

L'annexe I vous présente donc une série de clauses que nous vous invitons à négocier dans le cadre du renouvellement de votre future convention collective. L'accompagnement de votre conseillère syndicale ou conseiller syndical sera précieux pour vous aider à analyser la situation spécifique de l'organisation pour laquelle vous travaillez. Comme dans n'importe quelle négociation, il faut garder en tête que la prise en compte du rapport de force et l'implication des membres du syndicat dans leur mobilisation pour l'atteinte des objectifs fixés est fondamentale.



En guise de conclusion

Plusieurs principes ont été évoqués dans le cadre du présent guide. Les éléments suivants en font une synthèse :

1. La surveillance continue est généralement contraire aux différentes lois en vigueur ;

2. Lorsqu'un employeur souhaite exercer une surveillance électronique, il doit le faire avec les principes développés pour la filature ou la surveillance vidéo et ces principes sont rigoureusement encadrés ;

3. Lorsqu'il y a surveillance électronique, celle-ci doit être pour un motif sérieux, être en lien avec ledit motif et être proportionnelle ;

4. L'encadrement légal ne permet pas de laisser les données choir dans le dossier de l'employeur ;

5. Les formes de surveillance peuvent varier, mais les principes demeurent.

La surveillance électronique n'en est malheureusement qu'à ses débuts avec la gestion des métadonnées et l'intelligence artificielle. Il devient donc névralgique que les syndicats affiliés à la FNCC-CSN s'en saisissent.

Souriez,
vous êtes filmés!

ANNEXE I – Clauses de protection contre la surveillance

1. Définition

La surveillance consiste en l'utilisation de la technologie dans l'objectif d'observer, d'enregistrer et d'analyser l'information reliée aux activités des salarié-es.[39]

2. Interdiction[40]

L'employeur ne peut exercer aucune forme de surveillance que ce soit à l'égard des salarié-es.

3. Principes généraux[41]

3.1 L'employeur utilise une technologie de surveillance uniquement lorsque cela est nécessaire afin d'atteindre un objectif sérieux, légitime et précis. La technologie de surveillance ne peut être utilisée à d'autres fins que celles pour lesquelles elle a été mise en place.

L'employeur s'assure que la surveillance est faite de la façon la moins intrusive possible.

3.2 L'employeur ne peut utiliser les informations recueillies par une technologie de surveillance pour imposer ou justifier des mesures disciplinaires ou administratives.

3.3 L'employeur ne peut utiliser un système de surveillance en continu des salarié-es. Tout consentement à un tel système de surveillance est nul.

3.4 Le syndicat peut contester en tout temps un système de surveillance s'il estime que celui-ci n'est plus nécessaire.

3.5 En cas de contestation, l'employeur a le fardeau de prouver que le système de surveillance était nécessaire pour atteindre un objectif sérieux, légitime et précis.

4. Accord du syndicat[42]

L'employeur avise le syndicat au moins soixante (60) jours précédant toute volonté d'utiliser un système de surveillance.

---

[39] Définition suggérée par l'UQAM dans le Guide pratique sur la surveillance électronique au travail

[40] Si on obtient l'interdiction totale, il n'est plus nécessaire d'avoir d'autres clauses.

[41] Tenter d'insérer un maximum de ces clauses dans les conventions. Ce sont des clauses qui codifient la jurisprudence existante.

[42] S'il n'est pas possible d'obtenir une interdiction totale, tenter d'obtenir un maximum de clauses encadrant la nécessité d'un accord du syndicat et un consentement périodique des salariés.

Dans ce même délai, l'employeur transmet au syndicat des informations sur le système de surveillance qu'il entend mettre en place, notamment :

- Les motifs justifiant l'installation d'un système de surveillance
- Le ou les moyens (à titre d'exemple sans limiter la portée : appareil électronique, le support ou le logiciel) utilisés pour la surveillance ;
- La marque du moyen de surveillance ;
- Les détails techniques du ou des moyens utilisés, notamment les types de données recueillies ;
- Les usages faits par ces moyens ;
- Les modalités de conservation des données ;
- Les modalités de destruction des données ;
- Les modalités de protection de vie privée des salarié-es relativement aux usages ci-haut mentionnées.

L'employeur ne peut utiliser un système de surveillance s'il ne fournit pas l'avis et les informations mentionnées à l'alinéa précédent.

L'employeur avise le syndicat de toute modification aux éléments énumérés dans le deuxième alinéa.

5. Clause statu quo ante

En cas de contestation par grief, l'employeur ne peut utiliser les moyens faisant l'objet d'une contestation tant et aussi longtemps qu'une décision du tribunal ne dispose pas du ou des griefs.

Il incombe à l'employeur de prouver que l'utilisation d'une telle surveillance est conforme aux dispositions de la présente convention collective.

6. Consentement des salarié-es

L'employeur doit informer les salarié-es des modalités de la surveillance afin que ceux-ci puissent fournir un consentement éclairé. Il doit notamment les informer des données qui seront recueillies, de la manière dont elles seront recueillies, de l'utilisation qui en sera faite, de la période de la surveillance, des modalités de conservation et des modalités de destruction des données recueillies.

L'employeur doit requérir le consentement express des salarié-es au minimum une fois par année. Il doit fournir alors les mêmes informations que l'alinéa précédent et attirer l'attention sur toutes modifications apportées à ces éléments.

L'employé-es qui consent à la surveillance peut retirer son consentement à tout moment. L'employeur ne peut effectuer des représailles en lien avec le retrait de ce consentement.

7. **Conservation des données**

L'employeur est tenu de détruire les données relatives aux personnes salariées au-delà d'une période de trente (30) jours à compter de leur collecte à des fins de surveillance électronique.

8. **Santé mentale et prévention**

Le comité paritaire en santé et sécurité au travail (CPSST) doit mettre en place un plan de prévention sur les usages de la surveillance électronique et les répercussions relatives sur la santé mentale desdits moyens.

9. **Protection de la vie personnelle**

L'employeur ne peut d'aucune façon recueillir des informations sur la vie personnelle de l'employé-e par le biais de la surveillance électronique ni exiger la divulgation de son arrière-plan lors d'appels vidéo.

10 **Dossier de l'employé-e**

L'employeur doit informer l'employé-e de l'origine des informations recueillies et ajoutées à son dossier, tout en lui garantissant l'accès à ces données.

11. **Transparence**

L'employé-e peut, en tout temps, demander un relevé des données recueillies par le système de surveillance de l'employeur.

L'employé-e peut demander une copie des données recueillies par l'employeur par l'utilisation d'une technologie de surveillance.

L'employé-e peut demander la modification ou la destruction des données recueillies par l'employeur. L'employeur doit alors procéder à la modification ou la destruction des données.

L'employeur doit énoncer au Syndicat l'ensemble des moyens ou outils de surveillance électronique ou autre qu'il utilise et le type de données et de renseignements qu'ils permettent de recueillir.

12. **Profilage et traitement automatisé**

L'employeur ne donne aucune mesure disciplinaire fondée sur l'utilisation d'une technologie de profilage.

L'employeur ne donne aucune mesure disciplinaire ou administrative fondée sur une technologie de traitement automatisé sans intervention humaine.