Comprendre, sensibiliser et protéger :

Guide pratique sur la surveillance électronique au travail

Février 2024

L'évolution du paysage organisationnel durant les dernières années, marquée par le recours massif au télétravail, a intensifié la tendance vers l'implantation de la surveillance électronique en milieu de travail. Ce guide constitue une synthèse d'information sur la surveillance électronique et résume les résultats d'une consultation sur le sujet réalisée au printemps 2023 auprès de quelque 800 membres de la FTQ, la CSQ et la CSN.

Une définition...

La surveillance électronique consiste en l'utilisation de la technologie dans l'objectif d'observer, d'enregistrer et d'analyser l'information reliée aux activités des employé·es.

Il peut par exemple s'agir de la surveillance par localisation/données biophysiques, de l'activité en ligne et par caméra ou audio.

Ci-dessous, quelques exemples de technologies de surveillance et la fréquence de leur utilisation en contexte de travail :

60% Environ 60% des personnes sondées rapportent l'utilisation de cartes à puces et badges à des fins de surveillance.

25-40% Entre 25-40% des personnes sondées rapportent l'utilisation de caméras sur le lieu de travail, de surveillance des sites web visités, des courriels, des visioconférences, ainsi que du téléchargement de fichiers.

10-20% Autour de 10-20% des personnes sondées rapportent l'utilisation de la géolocalisation, l'écoute d'appels, la surveillance des médias sociaux, de la messagerie instantanée, du mouvement de la souris ainsi que des captures d'écran et de la surveillance d'écran en temps réel.

Les grands constats

82%

82% des personnes sondées rapportent être soumises à au moins une technologie de surveillance électronique.

30%

30% des personnes sondées se sentent constamment surveillées au moyen de technologies, logiciels et appareils au travail.

Les cols bleus, la main-d'œuvre ouvrière et les membres de grandes organisations sont plus nombreux à rapporter qu'ils sont surveillés.

Les pages 2 à 4 présentent la liste complète des technologies de surveillance utilisées en milieu de travail. Les points de couleur représentent la catégorie de technologie : ● surveillance par localisation, ● surveillance de l'activité en ligne et ● surveillance vidéo et audio. **OUI**, **NON** et **?** désignent respectivement le fait d'être soumis, de ne pas être soumis ou la méconnaissance d'être soumis à une technologie de surveillance donnée.

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%

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%

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%

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%

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%

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%

Surveillance sur ordinateur :

Sites internet consultés

Description :
Enregistrement et suivi actif de toute l'activité de l'utilisateur·trice 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%

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%

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%

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%

Transfert et téléchargement de fichiers (Clé USB, autre)

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 enregistrés et conservés.

OUI	NON	?
15%	49%	36%

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 employés, pour vérifier le risque de départ.

OUI	NON	?
19%	19%	62%

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%

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%

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%

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%

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 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 durant ses heures de travail.

OUI	NON	?
19%	19%	62%

Le projet a examiné 5 caractéristiques au cœur des enjeux de la surveillance : 1) sa transparence, 2) sa dénaturation 3), sa persistance, 4) son intrusivité et 5) sa légitimité.

Transparence

Définition : Il s'agit de la mesure dans laquelle les employé·es sont au courant de la surveillance à laquelle ils et elles sont soumi·ses.

Exemple : Nombreux sont les travailleur·ses qui spéculent sur l'étendue de la surveillance auxquels ils et elles sont soumi·ses. Leurs courriels sont-ils surveillés ? Leurs réunions, écoutées ? Leur clavardage sur Teams, enregistré à leur insu ?

Seulement 4% des travailleur·ses jugent que leur employeur est complètement transparent dans son utilisation des technologies de surveillance.

Une proportion importante des travailleur·ses ne sont pas au courant des technologies de surveillance auxquelles ils ou elles sont soumis·ses :

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

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

19% 19% ne savent pas s'ils sont surveillés par caméra.

Dénaturation

Définition : La dénaturation des outils réfère au fait que les données recueillies puissent être utilisées pour d'autres raisons que celles annoncées.

Exemple : Un employeur du secteur de la livraison locale annonce à ses employé·es qu'il implante un outil de géolocalisation sur ses camions à des fins de sécurité des personnes et du matériel. Quelques mois plus tard, on réalise qu'il utilise également cet outil à des fins de surveillance du temps de travail et de localisation des employé·es.

39% 39% des personnes sondées pensent que leur employeur pourrait utiliser les technologies pour d'autres raisons que celles divulguées.

Persistance

Définition : La persistance des données réfère au fait que les informations sur les activités des employé·es sont enregistrées et conservées sur une période prolongée, sans droit à l'oubli.

Exemple : Une gestionnaire a accès à tout ce qui s'écrit sur Teams ou Google Meet étant donné que ce contenu ne s'efface jamais.

63% 63% des personnes sondées s'inquiètent de ne pas pouvoir supprimer des informations que leur employeur recueille ou pourrait recueillir sur eux.

Intrusivité

Définition : Il s'agit de la mesure dans laquelle les technologies de la surveillance électronique s'ingèrent dans la vie privée, affectent l'autonomie et transgressent les frontières personnelles des travailleur·ses.

Exemple : Une employée se préoccupe davantage de ses gestes, de ses paroles et de son arrière-plan durant une visioconférence (p. ex., elle se retient de plaisanter avec ses collègues), sachant qu'elle est enregistrée et sera peut-être visionnée ultérieurement par un.e supérieur.e.

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

Au-delà des conséquences pour soi, les technologies de surveillance intrusives peuvent également affecter négativement les autres.

Exemple : La conjointe d'un télétravailleur sent sa vie privée envahie lorsqu'elle passe dans l'arrière-plan de la caméra de l'ordinateur, car elle sait que des photos sont prises de façon intermittente, puis stockées dans les bases de données de l'organisation.

Caractère intrusif pour d'autres :

54% 54% des personnes sondées sont d'avis que leur utilisation des technologies facilite l'intrusion de leur employeur dans la vie privée de leurs collègues;

42% 42% des personnes sondées sont d'avis que leur utilisation des technologies facilite l'intrusion de leur employeur dans la vie privée de leur famille.

Légitimité

Définition : Il s'agit de la mesure dans laquelle l'utilisation de surveillance électronique par l'employeur est perçue comme justifiée et nécessaire.

Exemple : Un employé avec beaucoup d'expérience en service à la clientèle se questionne sur la nécessité d'être surveillé par caméra durant l'entièreté de son quart de travail, car il estime que sa productivité était la même avant l'introduction de ces technologies sur son lieu de travail.

3% Seulement 3% des travailleur·ses jugent que les technologies de surveillance auxquelles ils et elles sont soumi·ses sont légitimes.

Les usages justifiés de la surveillance électronique?

- **Pour la sécurité :** l'utilisation de caméras peut, par exemple, prévenir les vols d'équipement, le vandalisme et les photocopies abusives.
- **Pour la cybersécurité :** Certains logiciels sont nécessaires afin de contrer les cyberattaques ou le vol d'informations.
- **Pour la santé publique :** En temps de pandémie, les cartes à puces ont été utilisées pour retracer les cas contacts dans les hôpitaux et les CHSLD.

QUELQUES RECOMMANDATIONS PRATIQUES

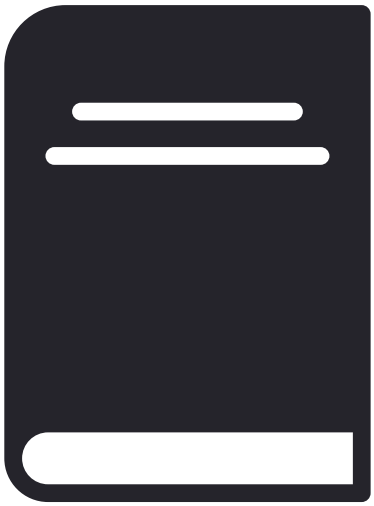
Il est suggéré d'éviter l'utilisation de logiciels de surveillance perçus comme intrusifs et peu légitimes.

- Leur utilisation pourrait être perçue comme un manque de confiance de l'employeur et mener à une variété de comportements défensifs des employé·es.

En cas de recours aux technologies de surveillance électronique, il est recommandé de mettre sur pied un comité qui chapeaute l'implantation des technologies.

- Les conséquences négatives de la surveillance sont limitées lorsque les employé·es ont un pouvoir d'influence sur la façon dont la surveillance est déployée et l'utilisation qui sera faite des données recueillies.

Pour plus d'informations, consultez : https://t.ly/GGVp9



Lectures suggérées

1. La surveillance électronique en télétravail : portrait, enjeux et astuces. Lien: https://t.ly/vnSjl
2. La surveillance en milieu de travail et le travail à distance - En explorer les impacts et les répercussions en pleine pandémie de COVID-19 au Canada. Lien: https://t.ly/WZrMP
3. La protection de la vie privée des employés sur les lieux de travail modernes - Résolution des commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée et des ombuds responsables de la protection de la vie privée. Lien: https://t.ly/PKAn9
4. Surveillance électronique à l'aide d'un logiciel, légale ou non ? Lien: https://t.ly/gHs1v

Ce guide pratique a été produit en partenariat avec la CSN, la CSQ et la FTQ et avec le soutien du Service aux collectivités de l'UQAM, dans le cadre du Protocole UQAM/CSN/CSQ/FTQ.

CONCEPTION DU GUIDE PRATIQUE

- **Yanick Provost Savard**, professeur, Département de psychologie, UQAM
- **Élie Pilon**, étudiant au doctorat, Département de psychologie, UQAM
- **Émilie Provost-Cardin**, étudiante au baccalauréat, Département de psychologie, Université de Montréal
- **Ariane Ollier-Malaterre**, professeure, Département d'organisation et ressources humaines, UQAM
- **Xavier Parent-Rocheleau**, professeur adjoint, Département de gestion des ressources humaines, HEC Montréal

RÉALISATION DE L'ÉTUDE

- **Ariane Ollier-Malaterre**, professeure, Département d'organisation et ressources humaines, UQAM
- **Xavier Parent-Rocheleau**, professeur adjoint, Département de gestion des ressources humaines, HEC Montréal
- **Yanick Provost Savard**, professeur, Département de psychologie, UQAM
- **Sabrina Pellerin**, candidate au doctorat, Département d'organisation et ressources humaines, UQAM