[SLATE] Surveillance en télétravail : quels sont vos droits ?

Une entreprise est parfaitement en droit d'installer des logiciels de surveillance sur les ordinateurs du personnel… à condition de l'en avertir.

L'explosion du recours au télétravail en raison de la crise sanitaire a, logiquement, amené les entreprises à penser ou repenser leurs modes d'organisation et de management du travail. Ainsi, la question du contrôle des salarié·es (vis-à-vis du contenu de leur travail, de son suivi, de l'atteinte des objectifs, etc.) dans un contexte d'éloignement physique est devenue encore plus prégnante, du fait de l'impossibilité de vérifier «en vrai», dans les faits, le respect des horaires et/ou des consignes de travail.

En juin dernier, une étude menée aux États-Unis soulignait un intérêt sans précédent des entreprises pour les logiciels de surveillance. Entre janvier et avril 2020, les intentions d'achats pour les logiciels de surveillance à distance des employé·es avaient été multipliés par plus de 50.

Au regard de ces éléments, peut-on considérer que nous sommes désormais dans l'ère de l'hypersurveillance, voire du flicage, des salarié·es en télétravail?

Une capture d'écran toutes les cinq minutes

Le suivi et le contrôle des salarié·es constituent des fonctions majeures de l'activité d'encadrement et de management: la planification et la coordination des activités à réaliser passent par la mise en place de règles de contrôle des tâches à opérer, de l'atteinte ou non des objectifs fixés, de la conformité de ces activités avec les instructions transmises, etc.

La période de télétravail souvent subi a accentué cette tendance au contrôle, jusqu'à donner l'impression d'un surcontrôle, notamment au détriment de la confiance au travail. L'apparition et le développement d'outils et d'équipements digitaux sans cesse plus sophistiqués posent la question de la limite de plus en plus floue entre simple contrôle hiérarchique et surveillance intrusive, voire quasi espionnage, des salarié·es.

Présentés souvent comme de simples outils internes de gestion administrative ou d'aide à l'accroissement de la productivité des salarié·es, ces programmes servent, en théorie, à rationaliser l'organisation de l'activité, notamment en rendant visibles les déséquilibres internes en termes de charge de travail et d'état d'avancement des projets en cours. Ces logiciels assurent également une fonction de sécurité et de filtrage, afin que les salarié·es ne puissent pas naviguer en ligne sur certains sites internet ou extraire des données ou informations sensibles.

Mais leurs fonctionnalités vont beaucoup plus loin: géolocalisation, enregistreur de frappe (*keylogger* traçant la moindre activité au clavier), temps passé en ligne sur des sites «productifs» ou «non productifs», durée de connexion sur les serveurs de l'entreprise, nombre de courriels envoyés, identité des destinataires, etc.

D'autres logiciels opèrent des captures d'écran des ordinateurs toutes les cinq ou dix minutes, ou dressent un véritable portait du «comportement digital» des salarié·es, pour donner à voir leurs éventuelles anomalies. À l'extrême, ce comportement peut même être traité à grande échelle par l'intelligence artificielle, afin d'opérer un contrôle beaucoup plus large. La plupart de ces logiciels de traçage de l'activité sont invisibles pour les salarié·es qui font l'objet d'une surveillance de plus en plus intrusive, ce qui pose logiquement la question de leur légalité.

Que dit la loi?

Tout dispositif de contrôle des salarié·es doit, pour être valable, respecter les libertés et droits fondamentaux des salarié·es, au premier rang desquels se trouve leur vie privée.

Le respect des prescriptions du règlement général sur la protection des données (RGPD), lorsque le dispositif touche à des données personnelles, est également incontournable. De plus, le Comité social et économique (CSE) doit être informé et consulté préalablement, afin d'appréhender en amont le dispositif de contrôle et ses possibles conséquences.

Ainsi, ce contrôle doit être justifié et proportionné, comme l'indique notamment l'Accord national interprofessionnel relatif au télétravail du 19 juillet 2005. De plus, le Code du travail prévoit une obligation de transparence de la part de l'employeur concernant l'usage des données personnelles: *«Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.»*

Les modalités précises du contrôle doivent être établies (type de contrôle, suivi, mesure, etc.) et discutées avec les partenaires sociaux, ainsi que les sanctions prévues. Bien que les messages échangés par le biais d'une adresse ou d'un téléphone professionnels et les fichiers stockés sur les ordinateurs de l'entreprise soient la propriété de cette dernière, cela n'autorise pas les responsables de l'organisation à agir sans limites.

Parallèlement, certain·es salarié·es peuvent développer des stratégies individuelles de contournement des dispositifs de surveillance: recours aux téléphones ou ordinateurs privés à des fins professionnelles, pour sortir ainsi du champ de surveillance, comportements feints, ententes entre salarié·es pour «tromper» ces dispositifs, etc. Ces éléments nous questionnent plus en profondeur sur les défaillances mêmes du management, obligé de recourir à des techniques au mieux *borderline*, au pire illégales.

Un révélateur de la défaillance du management

Ces cas d'espionnage interne témoignent d'une part de la trahison du contrat moral liant supérieur·es et salarié·es, et d'autre part des insuffisances du management, dont certaines pratiques peuvent mener à rompre toute confiance envers les salarié·es.

Cette volonté de compenser l'impossibilité d'une surveillance physique et réelle par des techniques allant du mail ou de l'appel de 9h01 pour analyser le temps de

réponse des salarié·es jusqu'aux logiciels de surveillance et ses abus cristallise une défaillance majeure dans les techniques de management mises en place, et l'incapacité des managers à gérer des équipes à distance.

Cette absence de confiance au travail est, de plus, contre-productive: les salarié·es peuvent développer des stratégies de contournement, mais également avoir tendance à progressivement être démotivé·es, voire à se désinvestir d'un travail dans lequel ils et elles se sentiraient sans cesse suspecté·es d'un potentiel manquement professionnel.

Les conséquences sur la santé des salarié·es ne sont ainsi pas négligeables. Par crainte de ne pas répondre aux attentes des managers et d'être accusé·es de ne pas réellement travailler, les salarié·es se rendent parfois disponibles constamment, induisant une situation de connexion subie, voire d'hyperconnexion.

Dès lors, l'organisation doit être vigilante sur le non-respect de l'équilibre entre vie privée et vie professionnelle, voire à la perméabilité accrue entre ces deux dernières. Ces éléments reposent ainsi la question du droit à la déconnexion et des difficultés à réellement le mettre en place, dans une optique préventive.

Dans ce contexte de crise sanitaire sans précédent, le recours accru au télétravail rebat les cartes du management, encore trop largement orienté vers le contrôle, voire l'hypercontrôle. Cela incite fortement les organisations à développer une nouvelle proposition sur la relation managers-salarié·es, en s'assurant du travail réalisé, sans tomber dans les dérives de l'hypersurveillance, avec la préservation de la frontière entre vie privée et vie professionnelle. Les organisations ont tout intérêt à progressivement passer de la culture du contrôle à la culture de la confiance, et à s'axer moins sur le processus que sur le résultat.

Liens utiles

Surveillance en télétravail : quels sont vos droits ?