

Avec le télétravail, le contrôle a changé d'échelle et de nature. Jusqu'où peut aller la surveillance des salariés sans basculer dans l'intrusion?

BIG BROTHER AU TRAVAIL

Par **Nidal Taibi**

Nathan, 27 ans, est employé dans une PME de marketing numérique. Deux jours par semaine, il reste chez lui. Le matin, il branche son ordinateur professionnel sur la table du salon, ouvre Teams, Slack, trois onglets d'analyse et une *playlist* à bas volume. Depuis quelques mois, un malaise diffus s'est glissé dans sa routine. Son ordinateur ventile plus fort. Certaines fenêtres se figent une fraction de seconde quand il passe d'un document à l'autre. Un manager lui a déjà demandé, presque en passant, pourquoi il avait été «moins réactif» sur une tranche horaire très précise. Nathan n'a aucune preuve d'être espionné. Rien de tangible, rien d'avouable. Seulement cette impression d'être devenu plus lisible, disséqué, décomposé en traces.

Ce soupçon n'est pas une lubie de salarié anxieux. Il raconte un basculement. Comme le résumé ...

GETTY





Surveillance

... Tanguy Mousserion, sociologue du travail: «Avec le télétravail et les technologies numériques, la logique de surveillance, telle qu'on la connaissait dans l'usine, par exemple, ne disparaît pas, elle change de forme. Le rôle, autrefois assuré par un encadrement humain, est désormais de plus en plus pris en charge par des dispositifs techniques.» Le regard du chef n'a pas disparu: il s'est converti en données, en métriques et en interfaces.

A l'usine, le contrôle avait ses pointuses, ses rondes et ses caméras. Dans le travail tertiaire, il tient désormais dans un tableau de bord, un score d'activité, un logiciel de captures d'écran, une webcam qui reste allumée ou un indicateur d'«inactivité» déclenché au bout de quelques minutes sans mouvement de souris. En Belgique, où un salarié sur trois travaille parfois ou habituellement à domicile, la question n'a plus rien d'abstrait. Elle s'est installée dans les appartements, sur les écrans et dans les esprits.

La journée transformée en traces

Le terme *bossware* sert aujourd'hui à désigner cette galaxie d'outils capables d'enregistrer les frappes sur le clavier, d'analyser la navigation Web, de mesurer le temps passé sur des applications, de produire des captures d'écran, de suivre des horaires, voire d'inférer des comportements. Le dernier état des lieux paneuropéen du Joint Research Centre (JRC) de la Commission européenne montre que plus de 90% des travailleurs de l'UE utilisent des outils numériques et que 37% des salariés sont suivis sur leurs horaires de travail. Eurofound, la fondation européenne pour l'amélioration des conditions de vie et de travail, résume la ligne rouge: plus le monitoring, à savoir le suivi de l'activité, ressemble à une surveillance systématique, continue et détaillée, plus le risque d'atteinte aux droits fondamentaux grimpe.

Le chiffre qui a le plus frappé les esprits ces dernières années vient d'un sondage américain mené par l'institut Resume Builder, en 2023, auprès de dirigeants d'entreprises engagées majoritairement dans le travail hybride ou à distance: 96% disaient utiliser au moins une forme de monitoring, 37% imposaient un flux vidéo en direct et près de trois quarts avouaient avoir déjà licencié sur la base de ces outils. C'est un ordre de grandeur spectaculaire, mais qu'il faut lire pour ce qu'il est: une enquête privée, centrée sur des organisations déjà très orientées dans le télétravail massif, et non un baromètre officiel universel. En France, le chiffre souvent repris est celui d'une étude Vanson Bourne pour VMware: 63% des entreprises de plus de 500 salariés y déclarent avoir mis en place ou prévu des outils de supervision du télétravail. Les sources publiques belges, elles, documentent bien mieux le télétravail et le cadre juridique que le volume exact de logiciels déployés.

Car le vrai sujet n'est pas seulement l'existence d'outils de contrôle. C'est leur finesse. Un employeur a toujours eu le droit de vérifier que le travail est bien



«Le risque est de transformer des outils de gestion en instruments de suspicion permanente.»



exécuté. Mais le numérique change l'échelle, la fréquence et l'intimité de ce contrôle. Là où la badgeuse enregistrait une entrée et une sortie, les logiciels contemporains peuvent aspirer une journée entière: temps actifs, temps morts, navigation, disponibilité apparente, rythmes de frappe, ouverture d'applications, échanges écrits, localisation, images.

Le droit rattrape le bossware

En Belgique, le droit n'a pas laissé ce terrain totalement vierge. L'Autorité de protection des données (APD) rappelle que la surveillance sur le lieu de travail passe de plus en plus par des moyens électroniques et que ces possibilités techniques peuvent être particulièrement intrusives. Pour les caméras, la convention collective de travail 68 encadre strictement les finalités

admissibles et impose que le contrôle direct du travailleur reste temporaire. Pour l'Internet et l'e-mail, la CCT 81 pose les trois grands principes: finalité, proportionnalité, transparence. En clair, un employeur ne peut pas tout collecter, tout le temps, pour n'importe quoi, ni individualiser d'emblée n'importe quel signal. Il doit informer, justifier, limiter.

C'est précisément là que se joue la frontière, souligne Tanguy Mousserion: «Lorsque ces conditions disparaissent, la technologie peut basculer vers une surveillance intrusive. Le risque est de transformer des outils de gestion en instruments de suspicion permanente, qui fragilisent la confiance et l'autonomie au travail.» En droit européen aussi, la méfiance est claire. Le Comité européen de la protection des données rappelle qu'en principe les salariés ne sont pas en position de donner un consentement libre à leur employeur, en raison du déséquilibre structurel de la relation de travail. Autrement dit: faire signer une clause n'autorise pas systématiquement la surveillance totale.

Les autorités commencent d'ailleurs à documenter très concrètement les excès. Fin 2025, l'APD a encore examiné un dossier de caméras braquées sur le personnel dans un établissement Horeca, rappelant que la surveillance du travail par caméra n'est admissible qu'à des conditions très strictes. En France, la Commission nationale de l'informatique et des libertés (CNIL) a frappé plus fort. Début 2025, elle a infligé 40.000 euros d'amende à une société immobilière qui utilisait un logiciel paramétré pour comptabiliser des périodes d'«inactivité» de trois à quinze minutes, effectuer des captures d'écran régulières et filmer en permanence des salariés. Un an plus tôt, Amazon France Logistique avait été sanctionnée à hauteur de 32 millions d'euros pour un système de scanners jugé excessivement intrusif, capable de mesurer des temps d'inactivité avec une précision telle que chaque interruption pouvait devoir être justifiée.

La doctrine est tout aussi parlante. La CNIL estime, par exemple, que la capture d'écran couplée à l'enregistrement des conversations téléphoniques est, en principe, ni pertinente ni proportionnée. Le motif est simple: une image figée ne reflète pas fidèlement le travail réel et peut, au passage, capter des éléments privés ou confidentiels. Le fantasme managérial du «voir pour savoir» produit donc souvent l'inverse de ce qu'il promet: beaucoup de données, mais une compréhension déformée de l'activité.

Selon plusieurs observateurs, cette inflation de traces n'ouvre pas seulement un risque juridique, elle crée aussi un risque de sécurité. En 2025, des chercheurs ont révélé qu'un logiciel de surveillance d'employés avait laissé exposés plus de 21 millions de captures d'écran sur le Web. Dans ces images pouvaient apparaître identifiants, documents internes, données personnelles ou conversations privées. Le logiciel censé rassurer le management devenait, d'un coup, une machine à fuite. ...

... Le débat dépasse désormais le seul RGPD (Règlement général sur la protection des données). La directive sur le travail via une plateforme, adoptée à l'automne 2024, est présentée par le Conseil de l'UE comme le premier texte européen à réguler la gestion algorithmique du travail. Quant au règlement européen sur l'IA, il a commencé à produire ses premiers effets le 2 février 2025: certaines pratiques sont désormais interdites, dont la reconnaissance des émotions dans le monde du travail, sauf pour motifs médicaux ou de sécurité. Quant aux systèmes d'IA à haut risque utilisés sur le lieu de travail, l'AI Act prévoit que les représentants des travailleurs et les salariés concernés doivent être informés avant leur déploiement. Le signal politique est limpide: surveiller n'est plus seulement une question d'efficacité managériale, mais de droits fondamentaux.

Ce que le logiciel ne voit pas

Dans sa dernière recherche européenne, le JRC, le service scientifique de la Commission européenne, observe que la «plateformisation» du travail, lorsqu'elle combine monitoring numérique et management algorithmique de façon poussée, est associée à de moins bonnes conditions de travail. Une revue de littérature du JRC montrait déjà que les formes de surveillance excessive s'accompagnent de davantage de stress, d'une baisse de satisfaction au travail, d'un affaiblissement de l'engagement organisationnel et d'une plus forte propension au départ. Tout ce qui fait tenir une équipe se retrouve alors miné par le dispositif même censé la rendre plus performante.

Tanguy Mousserion le formule clairement: «Ces dispositifs peuvent aussi créer un écart important entre le travail prescrit (celui qui est défini par la fiche de poste et le contrat de travail) et celui réellement exigé par les systèmes de pilotage algorithmique. Les indicateurs de performance, les objectifs automatisés ou les logiques d'optimisation peuvent conduire à imposer des rythmes et des exigences qui dépassent ce qui est formellement prévu dans le cadre du travail.» Toute une part de celui-ci devient alors invisible, parce qu'elle ne laisse pas de trace facilement compréhensible: réfléchir, arbitrer, calmer un client, aider un collègue, relire, douter, recommencer, respirer.

Il y a, dans cette logique, une certaine ironie. Les entreprises répètent qu'elles veulent de l'autonomie, de l'initiative, de la confiance. Puis elles achètent des outils qui mesurent la présence. Microsoft a donné un nom à ce décalage: la *productivity paranoia*, cette angoisse managériale qui pousse certains dirigeants à suspecter une baisse de productivité alors même que les salariés se disent productifs. Le *bossware* prospère dans cette brèche: il fournit une preuve, même pauvre, à une inquiétude déjà installée.

En Belgique, les syndicats tentent de faire monter le sujet au bon niveau. La CGSLB (Centrale générale des syndicats libéraux de Belgique) estime que la CCT 39 sur les nouvelles technologies, qui date

Les entreprises répètent vouloir de l'autonomie, de la confiance. Puis achètent des logiciels de surveillance.

de 1983, n'est plus adaptée aux usages actuels de l'IA et de la surveillance numérique. Le syndicat réclame un cadre plus clair, davantage de consultations des représentants des travailleurs, une information précise sur les algorithmes utilisés et l'interdiction des systèmes de surveillance abusive, y compris en télétravail. Le fait même que ces demandes passent aujourd'hui du registre militant au registre programmatique en dit long sur le changement d'époque.

Reste une question simple. Que cherche-t-on à mesurer quand on mesure un salarié? Du temps passé devant un écran? Des mouvements de souris? Une disponibilité apparente? Ou la qualité réelle d'un travail qui, surtout dans les métiers intellectuels, ne saurait se réduire à une suite d'impulsions numériques?

Nathan, lui, continue d'ouvrir son ordinateur le matin avec la même hésitation. Il répond vite, laisse rarement son statut virer au gris et repousse parfois son café pour ne pas «disparaître» trop longtemps. Il n'a toujours aucune preuve. C'est peut-être cela, le plus troublant. Il n'est même plus nécessaire de savoir que l'on est observé, il suffit de le croire un peu pour commencer à se tenir, travailler et respirer autrement. ●