Covid-19. La crise sanitaire favorise l'usage du bossware

written by Françoise Laugée | 3 décembre 2020

L'ONG américaine Public Citizen et l'EFF (Electronic Frontier Fondation) mettent en garde contre le développement, au sein des entreprises, de logiciels de contrôle, voire de surveillance, des salariés.

« La vitesse à laquelle ces nouvelles technologies ont été déployées est préoccupante », s'inquiète Public Citizen, association de défense des consommateurs américains, qui explique cet engouement par la nécessité de faire revenir les salariés sur leur lieu de travail. Dans un rapport intitulé « Workplace Privacy After Covid-19 », publié en août 2020, l'ONG recense au moins cinquante nouvelles applications et technologies de contrôle des salariés, commercialisées depuis le début de la pandémie. C'est sans compter celles qui existaient déjà, et qui sont vendues aujourd'hui comme « outils de veille » de la propagation du coronavirus au sein de l'entreprise. Le nombre de salariés concernés est loin d'être négligeable. L'enquête porte sur 32 entreprises identifiées comme utilisatrices de ces technologies de traçage de santé, ce qui représenterait, selon une extrapolation, 340 000 travailleurs. Cependant ce nombre pourrait atteindre 4 millions de salariés car 14 000 autres entreprises sont déjà équipées d'une technologie que leur fournisseur propose de compléter gratuitement avec un système de veille contre la Covid-19.

Le risque pour les salariés tient au fait que les employeurs n'examinent pas assez scrupuleusement les conditions d'utilisation de ces applications, afin de protéger à la fois la confidentialité des données personnelles et l'intimité de leurs salariés dans l'exercice de leur activité professionnelle. Public Citizen dénonce les atteintes à la vie privée des travailleurs, liées à l'usage d'outils numériques de traçage et de surveillance, alors que l'efficacité de ces technologies pour endiguer la propagation du virus n'a jamais été prouvée. En outre, explique l'association, de nombreux salariés sont contraints d'accepter ces applications, technologies ou vêtements connectés, au risque de perdre leur emploi.

En l'absence d'un cadre réglementaire approprié, les entreprises qui commercialisent ces outils de contrôle et de surveillance font aussi peu de cas du respect de la vie privée des travailleurs que des risques potentiels en matière de cybersécurité. Quant aux employeurs qui les utilisent, ils font preuve d'une grande négligence envers les droits de leurs salariés, en pratiquant le traçage, la collecte et le partage de leurs données personnelles sans leur consentement, notamment les données

sensibles sur la santé.

La plupart des applications de surveillance sur le lieu de travail sont configurées par défaut pour la *« surveillance de masse »*, explique Public Citizen en citant trois exemples : ProtectWell de Microsoft et de la compagnie d'assurance UnitedHealth, Healthcheck de Stratum et COVID-19 Worker Safety and Business Continuity Tracker de Pegasystems qui fonctionnent sur le même principe (ou plutôt absence de principes). Une fois qu'il aura téléchargé une de ces applications sur son téléphone portable, l'employé sera régulièrement sollicité pour déclarer des informations de santé liées à la Covid-19 (symptômes et température). Centralisées sur un tableau de bord en ligne, ces données sont accessibles à l'employeur. Celui-ci pourra ainsi identifier parmi ses employés ceux qui auraient été exposés à d'autres déclarés positifs au virus.

La lecture de la politique de confidentialité montre clairement comment ces applications de contrôle sur le lieu de travail pour cause de pandémie constituent en fait une grave menace pour le respect de la vie privée des travailleurs. ProtectWell, application vendue par Microsoft et la compagnie d'assurance UnitedHealth (242 milliards de dollars de chiffre d'affaires en 2019) envoie le résultat du test de Covid-19 directement à l'employeur, sans passer par le travailleur. Dans sa politique de confidentialité, ProtectWell annonce : *« Nous pouvons obtenir des informations supplémentaires à votre sujet auprès de tiers tels que des spécialistes du marketing, des partenaires, des chercheurs et autres. Nous pouvons combiner les informations que nous recueillons auprès de vous avec les informations vous concernant que nous obtenons de ces tiers et les informations dérivées de tout autre abonnement, produit ou service que nous fournissons. »*

Autre avertissement : *« Toute information qui nous est divulguée en relation avec le site et l'application ProtectWell n'est pas une information de santé protégée, telle que définie par le Health Insurance Portability and Accountability Act de 1996… »*. L'HIPAA, loi sur la portabilité et la responsabilité en matière d'assurance maladie encadre uniquement la confidentialité des informations médicales créées ou conservées par les régimes de santé, les centres d'information sur les soins de santé, les prestataires de soins de santé. Les données collectées par un employeur ne sont donc pas soumises aux règles de protection de la vie privée prévues par la loi fédérale. À l'inverse, le règlement européen sur la protection des données (RGPD) s'applique à l'ensemble des données personnelles de santé d'un employé y compris celles relatives à son « état de santé », présent ou futur.

La société Stratum, qui a conçu l'application Healthcheck indique, quant à elle, que ses propres employés ou agents peuvent consulter les informations personnelles des utilisateurs : *« Si vous accédez à un*

appareil mobile, nous collectons automatiquement des données personnelles, y compris des données relatives à l'appareil, au contenu et à l'utilisation […]. *Nous collectons également l'adresse IP du lieu d'accès pour déterminer votre position actuelle… »*. Selon les informations recueillies par Public Citizen, plusieurs banques, des compagnies d'assurance et de grandes enseignes ont signé ou sont en pourparlers pour utiliser HealthCheck.

Intégrée à une plateforme à laquelle soixante entreprises ont accès, l'application Pegasystems prévoit malgré cela que les informations personnelles des utilisateurs *« peuvent être transférées, traitées et stockées en dehors du pays où elles ont été recueillies »*.

Outre ces applications par lesquelles les employés sont amenés à déclarer eux-mêmes les informations concernant leur santé, Public Citizen présente dans son rapport deux autres catégories de technologies de surveillance sur le lieu de travail en période de Covid-19 : les technologies à porter sur soi (*wearables*) et les équipements (*hardware*). Les informations collectées par ces diverses technologies de contrôle ne sont pas non plus soumises aux exigences de la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA).

Des technologies portables, comme un vêtement ou un bracelet connecté, sont utilisées pour assurer le contrôle du respect de pratiques sanitaires par les employés. Grâce à une puce RFID embarquée, un travailleur qui n'aura pas passé assez de temps près d'un lavabo, sera repéré *a priori* comme ne s'étant pas bien lavé les mains. Des bracelets ou des badges émettent un bip sonore si la distance de sécurité sanitaire n'est pas respectée. Des caméras ou des capteurs vérifient la bonne distance entre les personnes et si les mesures d'hygiène sont pratiquées. La chaîne de restauration rapide CaliBurger a recours à la technologie Pop ID qui permet notamment de remplacer les simples cartes-clés des employés par des portes à déverrouillage automatique par reconnaissance faciale. Dans les usines Ford, les employés portent une montre équipée de la technologie Radiant RFID, qui vibre et change de couleur lorsqu'un salarié se trouve à moins de deux mètres d'une autre personne. La technologie VergeSense, qui compte parmi ses clients les groupes Cisco, Shell, BP et Roche, propose un capteur sans fil pour mesurer la distance entre les employés et la fréquence des interactions, analyse les données et produit un rapport quotidien sur la distanciation sociale.

En conclusion de cet état des lieux, l'ONG Public Citizen établit la liste des points essentiels à considérer avant de recourir à un outil de surveillance sur le lieu de travail. En premier lieu, les entrepreneurs devraient s'interroger sur la pertinence d'un tel système : obtiendraient-ils les mêmes résultats sans collecter des données personnelles ? Le cas échéant, la collecte de données devra être limitée

au strict nécessaire, tout comme la durée de conservation ; l'accès et l'utilisation des données seront limités aux personnes autorisées avec des restrictions imposées au partage avec des tiers ; le cryptage, la pseudonymisation et l'anonymat devront être privilégiés ; tout comme une communication ouverte et transparente avec les salariés, un consentement éclairé étant requis sur la base du volontariat. Des garanties devront être apportées aux travailleurs comme le droit d'accéder aux informations les concernant, de les corriger, de les supprimer, de retirer leur consentement à tout moment, de recevoir une explication lorsque leurs données sont utilisées et de pouvoir éventuellement la contester. Concernant le cas particulier des données biométriques, leur collecte et leur traitement ne doivent être envisagés qu'à la condition qu'il n'existe aucun autre moyen moins intrusif. Public Citizen insiste également sur la nécessité d'élaborer par écrit une politique interne à l'entreprise sur l'ensemble de ces questions et des procédures de confidentialité liées à la Covid-19, et de la partager avec les travailleurs.

De son côté, l'Electronic Frontier Foundation (EFF), ONG de défense des libertés sur internet d'envergure internationale, a baptisé *« bossware »* (matériel du patron) les logiciels de suivi des travailleurs que de nombreuses entreprises ont commercialisé au moment où la Covid-19 a contraint des millions de personnes au télétravail à domicile.

Après examen de la documentation marketing, des vidéos de démonstration, ainsi que des commentaires postés par les clients, l'EFF a établi un classement des variantes du *bossware*, sachant que le point commun de tous ces logiciels, une fois installés sur un ordinateur ou sur un smartphone, est d'avoir un accès privilégié au contenu de cet appareil.

La fonction la plus commune du *bossware* est la « surveillance des activités » qui fournit l'inventaire des applications ou des sites web consultés par l'employé durant ses heures de travail, y compris la liste des destinataires de ses courriers électroniques. De nombreuses entreprises utilisent également des logiciels de « suivi de la productivité » de leurs salariés, outils qui enregistrent le rythme de saisie au clavier ou à la souris. Tous les logiciels du *bossware* étudiés par l'EFF ont une fonction de capture d'écran, certains fournissant même des flux vidéo en direct du terminal de l'employé. Recomposées sous la forme d'un tableau chronologique, ces captures d'écran permettent de revenir sur la journée d'un travailleur et de voir ce qu'il faisait à un moment donné. S'ajoute éventuellement un enregistreur de frappe, lequel ne fera pas la distinction entre les informations relatives à l'activité professionnelle et les données afférentes à des comptes personnels avec un mot de passe privé. Les éditeurs des logiciels Work Examiner et StaffCop recommandent même aux employeurs de lier licenciement ou prime aux mesures de performance dérivées de leurs produits.

Le *bossware* pour appareil mobile inclut presque toujours le suivi de la localisation grâce au GPS. Les logiciels StaffCop Enterprise et CleverControl accentuent encore davantage l'étendue de la surveillance en actionnant à distance, et généralement secrètement, la webcam et le microphone du terminal utilisé par l'employé.

Enfin, comme l'explique l'EFF, le *bossware* pourra être déployé selon deux modes : l'un visible et donc éventuellement contrôlable par le travailleur et l'autre invisible, en arrière-plan. Généralement, le *bossware* est conçu pour proposer cette alternative.

Lorsque le logiciel de surveillance remplit le rôle de pointeuse, il arrive que les salariés puissent l'activer et le désactiver. En revanche, s'agissant des captures d'écran, la possibilité d'en supprimer certaines, avec le logiciel Time Doctor par exemple, a pour effet pervers de décompter le temps de travail correspondant.

Le secteur des logiciels de surveillance des travailleurs existait bien avant le déclenchement de la pandémie mondiale, mais il ne fait aucun doute, selon l'EFF, que le recours accru au télétravail a encouragé leur usage. La Covid-19 est devenue un argument de vente. Awareness Technologies, la maison mère du logiciel InterGuard, déclare avoir augmenté sa clientèle de 300 % dans les premières semaines suivant l'épidémie. Ce même InterGuard vante les mérites de son logiciel pouvant être *« installé silencieusement et à distance, afin que vous puissiez mener des enquêtes secrètes et recueillir des preuves irréfutables sans alarmer le suspect »*.

Si l'activité de certaines entreprises peut justifier un niveau de sécurité sur les ordinateurs et par conséquent un niveau de surveillance sur les appareils des employés en télétravail, la collecte d'informations est souvent excessive. Aux États-Unis, la législation est peu contraignante dans ce domaine, et comme l'explique l'EFF, quasiment rien n'empêche les employeurs de contraindre leur personnel à installer des logiciels sur leurs propres appareils, tant que la surveillance peut être désactivée en dehors des heures de travail.

« Aucune des utilisations, même les moins dérangeantes, ne justifie la quantité d'informations que les logiciels de gestion d'entreprise recueillent habituellement. Et rien ne justifie de cacher le fait que la surveillance a lieu », conclut l'EFF.

Sources :

- « Inside the Invasive, Secretive "Bossware" Tracking Workers », Bennett Cyphers and Karen Gullo, Electronic Frontier Fondation, eff.org, June 30, 2020.
- Workplace Privacy After Covid-19, Digital Rights Program, Burcu Kilic, Scott Hulver, Public Citizen, citizen.org, August 13, 2020.

- « Workplace Surveillance in Times of Corona », Katitza Rodriguez and Svea Windwehr, Electronic Frontier Fondation, eff.org, September 10, 2020.