fieldfisher

La surveillance des salariés : la clé de voûte du déconfinement au sein des entreprises ?

Juin 2020 / Olivier Proust et Sixtine Crouzet

La surveillance des salariés: la clé de voûte du déconfinement au sein des entreprises?

Pendant de longues semaines, les mesures de confinement ont forcé des millions de salariés à rester à leur domicile. Les entreprises ont alors dû mettre en place les mesures nécessaires pour assurer le télétravail de leurs salariés, lorsque celui-ci était possible.

Comme analysé précédemment[1], le télétravail a entrainé une collecte significative de données personnelles concernant les salariés, pour des finalités diverses et variées, telles que la mise en place de mesures de sécurité pour assurer le travail à distance ou encore l'organisation de vidéo-conférences.

Cependant, à l'heure où certains salariés sont appelés à franchir de nouveau la porte de leur bureau, la reprise de l'activité est susceptible d'entraîner une **surveillance accrue des salariés**.

Cette surveillance concerne de prime abord le recueil et le traitement des données de santé. Considérées comme des données sensibles, ces dernières bénéficient à ce titre d'une protection particulière en vertu du Règlement Général sur la Protection des Données (**RGPD**) : il est ainsi interdit de les traiter, sauf exceptions limitatives. A cet égard, l'autorité française de protection des données (la CNIL) a clairement différencié les pratiques autorisées de celles interdites dans une communication récente[2]. Par exemple, le relevé systématique, au sein d'un fichier, de la température à l'entrée des locaux ou encore l'utilisation de caméras thermiques ne sont pas permis.

Néanmoins, la question de la surveillance des salariés déconfinés va au-delà de la collecte des données de santé des salariés. La reprise de l'activité peut entraîner de *nouveaux* traitements de données personnelles pour garantir la conformité au droit applicable et aux recommandations gouvernementales en matière de déconfinement (1). De nombreux exemples déjà mis en place outre-Atlantique et en Asie témoignent du fait que certains employeurs vont cependant bien plus loin pour lutter contre la propagation du COVID-19 à l'échelle de l'entreprise, se substituant en quelque sorte aux politiques étatiques (2).

Ces nouveaux traitements se doivent de respecter le droit applicable en matière de protection des données personnelles, lequel comprend notamment le RGPD, la Loi Informatique et Libertés et certaines dispositions du droit du travail (3).

Assurer la conformité aux règles énoncées par le gouvernement

Il s'agit dans un premier lieu de se conformer aux règles gouvernementales, dont le Protocole national de déconfinement du Ministère du travail[3]. Ce dernier détaille toute une batterie de mesures à adopter afin de protéger les employés. Des outils innovants sont susceptibles d'apparaître pour assurer leur respect de façon automatisée via un **contrôle renforcé des accès aux locaux, des flux de personnes et du respect des consignes par les salariés**.

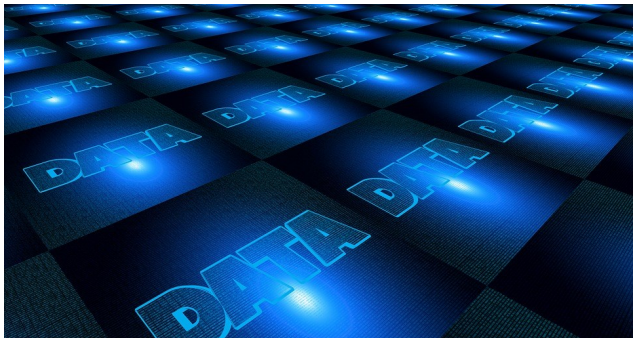
Les entreprises pourraient ainsi envisager d'obliger les salariés à s'enregistrer à l'accueil pour consigner chaque entrée et sortie. En cas d'horaires décalés, l'utilisation des systèmes d'accès préexistants pourrait permettre de vérifier le respect des horaires impartis à chacun (en surveillant par exemple l'historique des badges). Alternativement, la collecte de données de géolocalisation aurait vocation à déterminer si un salarié censé télétravailler reste à son domicile ce jour-là.

La surveillance des salariés: la clé de voute du déconfinement au sein des entreprises?

Afin d'éviter tout contact avec une porte physique, l'installation de portes automatiques pourrait s'accompagner d'un système refusant l'accès à une pièce à une personne, lorsque sa venue rendrait la distanciation sociale impossible (par ex. dans les lieux de pause ou de restauration). De même, un bracelet électronique devant être obligatoirement porté par les salariés émettrait un signal sonore lorsqu'il serait trop proche du bracelet d'un autre salarié.

Si les masques sont obligatoires au sein de l'entreprise, pourquoi ne pas assurer une détection automatique du port de masques, via un système d'intelligence artificielle greffé aux caméras de vidéosurveillance ? Ces mêmes caméras géreraient également les flux de personnes, en repérant tout attroupement dans les espaces communs, et assureraient l'intervention en temps réel d'un agent de sécurité pour disperser les salariés, voire d'un robot pour éviter aux agents d'encourir un quelconque risque d'infection.

La collecte de données comme moyen de lutte contre le COVID -19 à l'échelle de l'entreprise



Certaines structures sont en train d'explorer la mise en place d'outils et de technologies innovants afin de lutter efficacement contre la propagation du virus au sein même de l'entreprise. Les enjeux sont en effet de taille: il s'agit de protéger les salariés et d'éviter la constitution de foyers épidémiques internes et *in fine* la ré-adoption de mesures de confinement.

Les dernières semaines ont vu proliférer les recommandations concernant les applications de suivi des contacts (ou *contact tracing*), émanant à la fois des autorités nationales, comme la CNIL[4], ou des autorités et institutions européennes, comme la Commission européenne[5] et le Comité Européen de la Protection des Données[6] (**CEPD**). Alors que peu d'applications nationales sont à ce jour entièrement opérationnelles en Europe (en France seulement depuis le 2 juin), certains employeurs vont nécessairement vouloir concevoir des méthodes de suivi des contacts en parallèle, en se substituant, en quelque sorte, aux systèmes publics nationaux. Ainsi, des grosses structures qui accueillaient auparavant des centaines voire des milliers d'employés pourraient développer une application mobile interne de suivi, obligatoire pour les salariés, ou s'appuyer sur des badges intelligents. Ceux-ci enregistreraient la localisation des salariés au sein des locaux, la proximité avec leurs collègues ainsi que l'identité de ces derniers.

De plus, un éventuel profilage des employés peut être envisagé en mesurant les risques pour chacun. En fonction d'une note de « déconfinabilité » qui leur serait attribuée, ceux-ci pourraient se voir refuser l'entrée au bureau. Les facteurs suivants pourraient être pris en compte pour attribuer une telle note : nombre de personnes composant leur foyer, présence de travailleurs en première ligne, distance géographique entre le bureau et leur domicile (dont le fait de devoir prendre les transports en commun), l'âge, etc.

Les exemples de nouveaux traitements se trouvent à foison, et certains pourraient devenir notre quotidien.

La surveillance des salariés: la clé de voute du déconfinement au sein des entreprises?

Le nécessaire respect du droit applicable

Pour chaque traitement de données personnelles, les sociétés devront respecter les principes suivants:

Une finalité déterminée, explicite légitime

La finalité de chaque nouveau traitement doit être précise et prédéfinie. Sa légitimité doit faire l'objet d'une analyse attentive, en particulier en vérifiant que la finalité est conforme au droit applicable et notamment au droit du travail.

La proportionnalité et minimisation des données

Ce principe est cardinal en matière de droits à la vie privée et la protection des données des salariés (art. L. 1121-1 du Code du travail). Concrètement, il s'agira d'adopter la technologie la moins vorace en données personnelles et qui ne collectera, par défaut, que les données strictement nécessaires à la finalité prédéfinie. Ainsi, un outil ne nécessitant pas l'identification, directe ou indirecte, des salariés, l'enregistrement des données ou la collecte de données de géolocalisation doit être préféré.

Le choix de la base juridique appropriée

La mise en place de nouveaux traitements nécessite de déterminer au préalable la base juridique la plus appropriée. L'analyse doit s'effectuer au cas par cas, en fonction des spécificités de chaque traitement, de l'atteinte aux droits et libertés des salariés, de leurs attentes raisonnables et des garanties mises en œuvre.

Il est déconseillé en principe de recourir au consentement des salariés, qui est difficilement libre, du fait du déséquilibre présent dans les relations salarié-employeur. On peut envisager la nécessité de se conformer à une obligation légale (par ex. obligation des employeurs d'assurer la sécurité et la santé physique et morale de leurs salariés). La notion de « nécessité » s'entend toutefois strictement. De plus, De plus, selon le CEPD[7], l'obligation légale elle-même doit être « *suffisamment claire à propos du traitement de données à caractère personnel qu'elle requiert* (…) [et] *le responsable du traitement ne devrait pas avoir de marge d'appréciation injustifiée quant à la façon de se conformer à l'obligation légale* ».

L'information des salariés

Au niveau individuel, les salariés doivent être informés des nouveaux traitements, ainsi que de l'évolution de tout traitement préexistant (art. 13 et 14 du RGPD mais aussi art. L 1222-4 du Code du travail). Concrètement, la politique de confidentialité applicable aux salariés doit être modifiée pour informer les salariés des traitements visant à assurer leur sécurité et à accompagner le déconfinement. Ces changements, en fonction de leur importance, doivent être clairement portés à l'attention des salariés via un moyen de communication approprié (par ex. sur l'intranet, par email).

Au niveau de l'entreprise, les sociétés sont tenues d'informer et de consulter préalablement les instances représentatives du personnel concernant « *l'introduction de nouvelles technologies, tout aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail* » (art. L2312-8 du Code du travail) et de les informer « *sur les traitements automatisés de gestion du personnel* » (art. L2312-38).

La surveillance des salariés: la clé de voute du déconfinement au sein des entreprises?

Accountability et documentation de la conformité des traitements

Conformément au principe de responsabilité (*accountability*), l'un des piliers du RGPD, les sociétés doivent être en mesure de démontrer leur conformité aux principes généraux de la protection des données, dont ceux décrits ci-dessus. La documentation de la conception et de la mise en place des traitements permet de justifier, noir sur blanc, leur conformité. Il s'agira par exemple de démontrer que les nouveaux outils protègent par défaut la vie privée.

Le référentiel de la CNIL Gestion des ressources humaines[8], adopté en avril dernier, fournit un cadre de référence pour garantir la conformité des traitements « *courants* » de la gestion du personnel. Or, les traitements précédemment décrits sortent de ce champ d'application. En effet, tel est le cas des traitements entraînant des risques plus importants pour les droits des salariés, dont les traitements ayant recours à des outils innovants, à la vidéosurveillance, au profilage et là 'utilisation des *big data*.

Cette obligation de documentation se matérialise également via la réalisation d'une **analyse d'impact relative à la protection des données** (AIPD). Une telle analyse doit être menée lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes* » (art. 35 du RGPD). En pratique, elle doit être effectuée lorsqu'au moins deux des neuf critères identifiés par le CEPD[9] sont remplis. Or, les critères suivants sont susceptibles d'être remplis par les traitements susvisés: (1) surveillance systématique, (2) données concernant des personnes vulnérables (à savoir, les salariés), (3) usage innovant (utilisation d'une nouvelle technologie), ou encore (4) évaluation/*scoring* (y compris le profilage).

La CNIL considère que ne nécessitent pas l'établissement d'une AIPD les traitements mis en œuvre « *aux seules fins de gestion des contrôles d'accès physiques, en dehors de tout dispositif biométrique, à l'exclusion des traitements qui révèlent des données sensibles ou à caractère hautement personnel* ». Cependant, certains futurs traitements sont susceptibles d'aller plus loin qu'un simple contrôle d'accès à des fins de sécurité des locaux. A ce titre, ils ne pourront pas bénéficier d'une telle dérogation.

Le respect des droits des salariés

En vertu du RGPD, les salariés bénéficient d'un certain nombre de droits sur les données personnelles les concernant (par ex. les droits d'accès et d'opposition). Ces droits s'appliquent aux traitements effectués par les employeurs, mais peuvent varier en fonction de la base juridique retenue pour chaque traitement. L'utilisation d'outils innovants au sein de l'espace public (comme des caméras dans les transports ou l'application StopCovid) a cristallisé le débat public. Par conséquent, les salariés sont nécessairement conscients de l'existence de risques pour leur vie privée, ce qui peut les amener à interroger leur employeur sur l'utilisation de leurs données personnelles, via l'exercice de leur droit d'accès. L'anxiété accompagnant le retour au travail en présentiel est un autre facteur à prendre en compte.

En conclusion, la surveillance des salariés peut être vue par certains employeurs comme la condition nécessaire pour garantir un déconfinement sous contrôle à l'échelle de l'entreprise. La conformité de ces traitements potentiellement intrusifs constituera un défi pour les employeurs et les développeurs d'outils sur lesquels reposent ces traitements.

N' hésitez-pas à contacter notre équipe *Technology, Outsourcing & Privacy* si vous avez des questions sur cette publication.

La surveillance des salariés: la clé de voute du déconfinement au sein des entreprises?

Références

1. Article « La surveillance des salariés en télétravail à l'heure du Covid-19 », Olivier Proust et Sixtine Crouzet, Village de la Justice, 1 avril 2020. Une version anglaise est disponible sur le site de Fieldfisher (« The risks of online employee monitoring during the COVID-19 crisis », 14 avril 2020).
2. Communication « Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs », CNIL, 7 mai 2020.
3. Protocole national de déconfinement pour les entreprises pour assurer la sécurité et la santé des salariés, Ministère du Travail, 8 mai 2020.
4. Communication « La CNIL rend son avis sur les conditions de mise en œuvre de l'application 'StopCovid' », CNIL, 26 mai 2020.
5. Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des donnée, Commission européenne, 16 avril 2020.
6. Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19, CEPD, 21 avril 2020.
7. Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, Groupe de travail « Article 29 » sur la protection des données, 9 avril 2014.
8. Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel, CNIL, 21 novembre 2019.
9. Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, CEPD, adoptées le 4 avril 2017 et dernièrement modifiées le 4 octobre 2017.

Contacts

Olivier Proust
Partner, Technology, Outsourcing & Privacy
+32 2 742 70 15
olivier.proust@fieldfisher.com

Sixtine Crouzet
Associate, Technology, Outsourcing & Privacy
+32 2 742 70 55
sixtine.crouzet@fieldfisher.com