Union syndicale Solidaires

Outils
à l'usage des salariés
et de leurs représentants

Santé au travail | Conditions de travail

n°17
octobre 2015

Surveillance au travail
les droits et recours des salarié-e-s, les obligations des employeurs

L'usage du numérique prend une place grandissante dans les relations de travail. De plus en plus d'entreprises et d'administrations utilisent et multiplient les dispositifs de surveillance des salariés: géo localisation, vidéo-surveillances, contrôle des horaires, des messageries électroniques, écoutes et enregistrement des appels téléphoniques. « *Il est 10H02 et vous n'êtes pas à votre poste de travail* », « *vous avez passé trop de temps avec ce client* », vidéos tournées à l'insu des caissières par des caméras dissimulées, il s'agit là de nombreuses pratiques contraires au droit du travail.
Alors qu'est-ce qui est autorisé ? Quels sont les droits et obligations des employeurs, et quels sont ceux des salarié-e-s ?
L'objet de cette fiche est de faire un point sur les règles applicables en la matière, en tenant compte des évolutions jurisprudentielles ainsi que des positions de la Commission Nationale de l'Informatique et des Libertés (CNIL) qui a édicté un certain nombre de normes et de règles concernant le contrôle des horaires, la vidéosurveillance, la géo localisation, l'utilisation des outils informatiques...
La première partie de la fiche rappelle les obligations des employeurs vis-à-vis des salariés, des représentants du personnel et de la CNIL.
La deuxième partie fait un point sur chacun des systèmes de contrôles et de surveillance : accès aux locaux et contrôle des horaires, vidéo surveillance, géo localisation, utilisation des téléphones professionnels et des outils informatiques.

Quels sont les droits et obligations des employeurs ?

L'employeur dispose de prérogatives certaines dans l'organisation du travail : il a un pouvoir de direction et à ce titre, il peut contrôler et surveiller l'activité des salarié-e-s pendant leur temps de travail.

Toutefois la surveillance mise en place doit être justifiée par la tâche, et proportionnée au but recherché, comme le précise l'article L 1121-1 du code du travail : « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ».

De plus, elle ne peut se faire à l'insu des salariés (*Cass.soc.10 janvier 2012, n°10- 23482*), ni empiéter sur leurs libertés individuelles et leur vie privée. C'est sur ces points que les personnels et leurs représentants doivent exercer la plus grande vigilance car effectivement, des employeurs, tellement obnubilés par la rentabilité, ne vont pas hésiter à franchir la frontière interdite.

- Informer les salariés

C'est un passage obligé en application de l'article L 1222-4 du code du travail : « *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 d'information des salarié-e-s ne sont pas définies par les textes : cela peut se faire par une lettre

recommandée adressée à chaque salarié, une note d'information, ou encore un avenant au contrat de travail.

La CNIL précise que chaque employé-e doit être informé-e des finalités poursuivies, des destinataires des données récoltées, de son droit d'opposition pour motif légitime, de ses droits d'accès et de rectification.

- Consulter les représentants des personnels

- le comité d'entreprise (CE) est informé et consulté avant la mise en place de moyens ou de techniques permettant un contrôle de l'activité des personnels. (L2323-32)

- si la consultation du CHSCT n'est pas prévue expressément, elle semble incontournable. En toute logique, le CHSCT devrait être amené à donner son avis. Le dispositif de surveillance envisagé par vidéo surveillance ou géo localisation peut par exemple induire une pression sur les employés et/ou générer de nouveaux risques professionnels...

Dans la Fonction publique d'État, il n'est pas prévu de consultation obligatoire du comité technique (CT) comme le prévoit le code du travail pour le CE. Toutefois la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique à tout employeur et à toute personne. Il n'y a donc aucune raison de ne pas saisir le CT, ni d'exiger des informations précises des responsables administratifs sur les modes de surveillance des personnels.

- Faire une déclaration à la CNIL

Lorsque le dispositif de surveillance permet de recueil d'informations personnelles sur les salariés, il relève alors de la loi informatique et libertés du 6 janvier 1978 et doit faire l'objet d'une déclaration **préalable** auprès de la CNIL.

La CNIL impose à l'employeur de préciser :
o la finalité du dispositif : contrôle des accès, gestion des temps de présence…
o la nature des données recueillies ;
o les services destinataires ;
o la durée de conservation des données ;
o l'existence d'un droit d'accès, de rectification et d'opposition…

Toutefois, certains fichiers ou traitements automatisés de données sont dispensés de déclaration (paie, déclarations fiscales et sociales, etc.). D'autres font l'objet d'un engagement de conformité s'ils entrent dans le cadre d'une déclaration simplifiée de la CNIL (c'est notamment le cas pour la gestion du personnel, la géo localisation des véhicules, les enregistrements téléphoniques), ou encore font l'objet d'une demande d'autorisation comme ceux qui comportent des données biométriques.

A noter également que la désignation d'un correspondant informatique et libertés au sein de l'entreprise exonère le responsable des traitements informatiques de certaines déclarations.

En cas de non déclaration à la CNIL l'employeur encourt une peine d'emprisonnement de cinq ans d'emprisonnement et une amende de 300 000 €.

Un rôle important pour les représentants du personnel

Au-delà de leur consultation obligatoire les représentants du personnel devront exercer un rôle de contrôle et tout particulièrement vérifier le respect des obligations de l'employeur vis-à-vis des salarié-es, de la CNIL mais aussi pour chacun des systèmes que l'employeur n'outrepasse pas ses droits en terme de surveillance, ce qui figure dans le règlement intérieur, saisir le CHSCT, interroger le médecin du travail, l'inspecteur du travail, faire une enquête...

Les systèmes actuels de contrôle et de surveillance

Quel que soit le système utilisé, il doit au préalable faire l'objet d'une information des salariés, d'une information consultation des représentants du personnel, et d'une déclaration à la CNIL.

Dans le cas contraire, le système de contrôle mis en place ne pourrait pas être opposé à un-e salarié-e.

1 - L'accès aux locaux et le contrôle des horaires

L'employeur peut mettre en place des outils (y compris biométriques) de contrôle individuel pour sécuriser l'accès des bâtiments et la circulation dans les locaux. Ces outils peuvent également être utilisés pour gérer les horaires de travail.

En revanche, il ne doit pas servir à contrôler les déplacements à l'intérieur des locaux, ni à entraver la liberté des représentants des personnels ou à contrôler le respect de leurs heures de délégation.

Une jurisprudence (*Cass.soc 9 juillet 2014, n°13-1615*) a confirmé que l'employeur peut prendre des dispositions pour décider des modalités de déplacement au sein de l'établissement mais à la condition de consulter préalablement les intéressés, et qu'elles n'aient pas pour effet de limiter l'exercice du droit syndical, ni d'entraver leurs fonctions.

Qui accède aux données ?
Les informations ne sont accessibles qu'aux personnes habilitées (ce n'est donc pas n'importe quelle personne dans l'entreprise, l'établissement) qui appartiennent aux services gérant le personnel, la paie ou la sécurité.

Quelle durée de conservation ?
Les données relatives aux accès des bâtiments doivent être supprimées trois mois après leur enregistrement, celles relatives au suivi du temps de travail sont à conserver pendant cinq ans.

Quel recours pour les salarié-e-s ?
Saisir le service des plaintes de la CNIL, l'inspection du travail, le procureur de la République.

2 - La vidéosurveillance

Pour la CNIL, si les dispositifs de vidéo surveillance sont légitimes pour assurer la sécurité des biens et des personnes, « *ils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente* ».

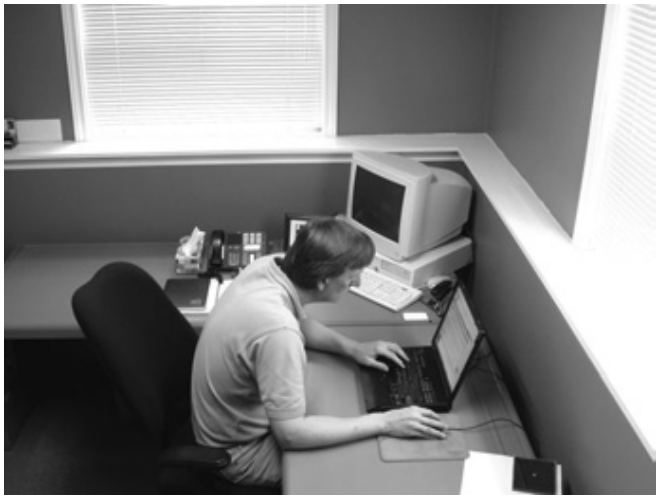
Des caméras peuvent être installées au niveau des entrées et des sorties de bâtiments, des issues de secours et des voies de circulation, dans les zones où sont entreposées des marchandises et des valeurs.

En aucun cas les caméras ne peuvent filmer les salariés sur leur poste de travail, sauf dans des circonstances très particulières comme la manipulation d'argent, mais dans ce cas il faudrait filmer plutôt la caisse que le caissier.

Les zones de pause, de repos comme les toilettes ne sauraient être filmées. Il en est de même pour les locaux syndicaux. Un-e salarié-e ne peut donc pas être filmé-e à son insu. La plus grande vigilance s'impose donc pour les salarié-e-s et pour les instances représentatives du personnel afin de s'assurer que l'employeur n'enfreint pas les règles.

En cas de vidéosurveillance, l'information des employés et des visiteurs passe par la mise en place de panneaux visibles sur lesquels doit être précisé : l'existence du dispositif dans l'établissement, le nom du responsable et la possibilité d'exercer son droit d'accès aux images.

Si dans un certain nombre de situations (magasins, banques, accueil du public...) les caméras de surveillance peuvent être utiles pour sécuriser le personnel ou encore les bâtiments.



Toutefois, la plus grande vigilance s'impose pour empêcher les dérives et les sanctionner. Les abus existent déjà et risquent de se multiplier face à un système de surveillance en voie de généralisation et de banalisation dans nos sociétés. Il faudra savoir réinterroger le travail et son organisation pour trouver, avec les personnels concernés, d'autres solutions moins intrusives qui permettent tout autant d'assurer leur sécurité.

Qui peut consulter les images ?
Le visionnage des images enregistrées est réservé aux personnes habilitées dans le cadre de leurs fonctions comme le responsable de la sécurité. Ces personnes doivent être formées et sensibilisées aux règles entourant la vidéosurveillance.

Quelle durée de conservation ?
Elle ne doit pas excéder un mois.

Quel recours pour les salarié-e-s ?
Saisir le service des plaintes de la CNIL qui peut contrôler tous les dispositifs installés dans des lieux ouverts ou fermés au public ; la préfecture si les caméras filment sur la voie publique, la police ou la gendarmerie ; l'inspection du travail ; le procureur de la République.

Jurisprudence
Après avoir été saisie d'une plainte, la CNIL a mis en demeure un centre commercial (Leclerc) de modifier son système de surveillance aux motifs qu'il était disproportionné, les 240 caméras installées filmaient également l'accès aux toilettes, aux vestiaires, au cabinet médical et aux salles de pause ! De plus, sous couvert de protéger des biens et des personnes, le système plaçait en réalité les salariés sous surveillance permanente à leur poste de travail et surtout de contrôler leurs horaires, les caméras filmant les personnels en train de pointer.

Enfin, la CNIL a souligné plusieurs manquements de la société :
- information insuffisante des personnels ;
- durée de conservation excessive ;
- sécurité insuffisante des données collectées.
CNIL : décision n°2013-029 du 12 juillet 2013

Dans une autre délibération du 16 janvier 2014, la CNIL a de nouveau mis en demeure un autre centre commercial Leclerc de modifier son dispositif biométrique et de vidéosurveillance pour les rendre conformes à la loi informatique et libertés.

D'autres sociétés n'ayant pas donné suite aux mises en demeure ont été condamnées à des amendes.

Dans une autre affaire une entreprise a été condamnée pour avoir licencié un de ses employés sur la base d'un système de surveillance non déclaré.

3 - La géo localisation

La géo localisation des salariés peut se faire par des GPS installés dans les véhicules mis à leur disposition.

Une délibération de la CNIL du 4 juin 2015 a renforcé l'encadrement de la géo localisation pour éviter les abus ; les entreprises ont un an pour se mettre en conformité.

Pour éviter les dérives d'un système particulièrement intrusif, la CNIL en a limité les possibilités aux situations suivantes :
- assurer la sécurité du salarié, des marchandises ou des véhicules dont il a la charge (transports de fonds et de valeurs …) ;
- suivre et facturer une prestation de transport de personnes, de marchandises ou une prestation de services liée à l'utilisation du véhicule (cas des ambulances), ainsi que la justification d'une prestation auprès d'un client ou d'un donneur d'ordre ;
- respecter une obligation légale ou réglementaire en raison du type de transports ou de la nature des marchandises transportées (produits dangereux, produits alimentaires …) ;

- identifier le véhicule le plus proche pour effectuer un dépannage, intervenir après un accident... ;
- le suivi du temps de travail lorsque cela est impossible par un autre moyen avec une réserve importante : la géolocalisation n'est pas justifiée quand le salarié dispose d'une liberté dans l'organisation de son travail comme par exemple un commercial.

Les utilisations exclues de la géolocalisation :
- le contrôle des limitations de vitesse ;
- les temps hors temps de travail : trajet domicile-travail, pauses ;
- le contrôle en permanence d'un employé ;
- le contrôle des kilomètres parcourus sauf en cas d'anomalies ;
- le calcul du temps de travail si un autre dispositif existe déjà ;
- le suivi des déplacements des représentants syndicaux ;
- l'utilisation du véhicule à des fins privées - lorsque le salarié en a l'autorisation- en dehors du temps de travail.

Si le dispositif envisagé par l'employeur ne respecte pas les conditions légales posées par la CNIL ou d'autres textes, les salariés peuvent s'y opposer. En outre, ils ont un accès aux données enregistrées qui les concernent.

Pour garantir leur vie privée, les salariés doivent pouvoir désactiver complètement le système une fois leur travail terminé, pendant leur pause ou pendant l'exercice d'un mandat syndical. Le système « dit de grisage » où les données transmises restent illisibles mais avec possibilité de levée, le grisage par un supérieur n'est pas suffisamment protecteur de la vie privée (*CA Bordeaux 27 novembre 2012 n°11/06565*).

Les règles de sécurité
Le suivi en temps réel ne peut se faire qu'avec un identifiant et un mot de passe, pour éviter que des personnes non autorisées ne surveillent les salariés.

Quelle durée de conservation ?
Les informations obtenues par la géolocalisation sont conservées dans la limite de deux mois, de cinq ans si elles sont utilisées pour le suivi du temps de travail mais dans ce cas seules les données relatives aux horaires du salarié peuvent être conservées pendant cette durée.

Toutefois le délai peut aller jusqu'à un an s'il s'agit d'optimiser des tournées ou de faire la preuve de la réalisation d'intervention en cas d'impossibilité de le faire par un autre moyen.

Quel recours pour les salarié-e-s ?
Saisir le service des plaintes de la CNIL, l'inspection du travail, le procureur de la République.

Jurisprudence
Dans une décision du 17 décembre 2014 (*n°13-23645*), la cour de cassation a confirmé la jurisprudence antérieure : un salarié a toute légitimité pour refuser de se soumettre à un système de géolocalisation, sans encourir de sanction disciplinaire, dès lors qu'il a une relative indépendance dans son emploi du temps. Dans l'affaire jugée le salarié était technico-commercial.

La mise en place d'un système de géo localisation est un projet important et peut donc faire l'objet d'une expertise : un jugement du TGI de Valence a considéré comme important le projet d'équipement progressif de tous les véhicules de la société d'un système de géo localisation en s'appuyant sur l'article L. 4614-12 du code du travail, et sur le fait que la diminution de l'autonomie des salariés en résultant est de nature à modifier leurs conditions de travail. (*TGI Valence 5 décembre 2012 n°12/00632*)

4 - Le contrôle de l'utilisation des téléphones : écoute et enregistrement des conversations téléphoniques

Il faut distinguer :
- le contrôle des relevés téléphoniques : il s'agit pour l'employeur de s'assurer que les salariés « n'abusent » pas du téléphone pour des raisons personnelles mais ce contrôle doit garantir le respect de la vie privée et des libertés des personnes sur le lieu de travail. C'est ainsi que les quatre derniers chiffres des numéros de téléphone sont masqués, le supérieur hiérarchique ne pouvant accéder au numéro complet que de façon exceptionnelle en cas d'utilisation anormale par exemple ;

- de l'écoute des conversations téléphoniques : les règles entourant l'enregistrement des conversations téléphoniques

sont très strictes. Pour la CNIL, il ne peut être réalisé qu'en cas de nécessité et être proportionné aux objectifs poursuivis : ainsi un enregistrement pour des besoins de formation ne pourra se faire que sur une brève période et jamais de manière permanente.

La CNIL exige que la fonction enregistrement puisse être neutralisée en cas d'appels privés.

Les salariés protégés ayant un mandat électif ou syndical doivent avoir à leur disposition un matériel excluant toute possibilité d'interception ainsi que l'identification de leurs interlocuteurs.

Les SMS envoyés depuis un téléphone professionnel sont supposés avoir un caractère professionnel. A ce titre, ils sont consultables par l'employeur et utilisables en cas de sanction disciplinaire, dès lors que leur contenu a un rapport avec l'activité professionnelle.

Leur durée de conservation ne doit pas dépasser un an (six mois pour les besoins de formation).

Jurisprudence

Dans un arrêt du 10 février 2015, la Cour de cassation a confirmé que les « SMS » envoyés d'un téléphone professionnel sont présumés d'ordre professionnel, sauf s'ils sont identifiés comme étant personnels à l'aide notamment de la mention « personnel » au début du message.

Dans cette affaire, une entreprise avait attaqué en justice une entreprise concurrente qui avait débauché une partie de son personnel. Cette entreprise avait été autorisée par ordonnance à consulter les SMS de ses ex salariés. Les juges ont considéré que la production en justice de messages n'ayant pas été identifiée comme étant personnels par le salarié :

- ne constitue pas « *un procédé déloyal au sens des articles 6 du code civil et 6 paragraphe 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales rendant irrecevable ce mode de preuve* » ;
- .... « *qu'ils étaient susceptibles de faire l'objet de recherches pour des motifs légitimes et que l'utilisation de tels messages par l'employeur ne pouvait être assimilée à l'enregistrement d'une communication téléphonique privée effectué à l'insu de l'auteur des propos invoqués...* ».

Cette décision a été prise en dépit de l'argument qu'il était impossible d'identifier un SMS comme personnel, l'envoi d'un tel message depuis un téléphone mobile ne comporte pas d'objet, contrairement à un courriel.

Arrêt n°181 du 10 février 2015 Cour de cassation, chambre commerciale, financière et économique

Cette jurisprudence rejoint celle qui existe déjà concernant les fichiers informatiques et les courriels considérés a priori comme professionnels (voir ci-après).

5 - Le contrôle des outils informatiques

- la messagerie professionnelle

L'employeur peut mettre en place des outils de contrôle et de limitation d'utilisation d'Internet et de la messagerie pour assurer la sécurité des réseaux (virus, filtrages de sites …) et limiter les risques d'abus (fréquence des envois, consultation de sa messagerie personnelle, achats de produits, taille des messages, filtres anti spam…).

Mails personnels et mails professionnels : Selon la jurisprudence, les courriels adressés ou reçus par un-e salarié-e sur son ordinateur professionnel ont un caractère professionnel. A ce titre, l'employeur peut donc les lire même en l'absence du salarié, sauf s'ils sont identifiés comme étant personnels.

Il est donc recommandé aux salarié-e-s de faire figurer la mention « personnel » ou « privé » dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké (la mention mes documents ou de ses initiales n'est pas suffisante). L'employeur ne peut pas consulter les messages personnels.

- l'ordinateur professionnel

Comme pour la messagerie, l'employeur peut accéder aux fichiers et dossiers créés et stockés sur l'ordinateur professionnel, sauf s'ils sont identifiés comme étant personnels. La mention expresse « personnel » ou « privé » est donc essentielle pour préserver toute intrusion de l'employeur.

Mettre un code d'accès à son ordinateur professionnel ne lui donne pas pour autant un caractère privé, il en va de

même pour l'utilisation d'une clé USB sur son ordinateur professionnel.

- les connexions Internet

L'employeur a toute liberté pour fixer des conditions et des limites à l'utilisation d'Internet sur le lieu de travail via le filtrage de sites non autorisés, l'interdiction de télécharger des logiciels…

La jurisprudence a considéré que l'employeur avait le droit de surveiller les connexions grâce à l'historique des sites visités, toutefois il n'a pas les mains totalement libres.

Le Conseil d'État a refusé à l'entreprise Renault Trucks d'installer un logiciel de recherche de fichiers pédopornographiques sur les ordinateurs des salarié-es pour le motif suivant : une entreprise privée ne peut pas mettre en œuvre un traitement des données de données personnelles relatives à des infractions pénales ou destinées à en établir l'existence. Cet arrêt du 11 mai 2015 a confirmé la précédente délibération de la CNIL ayant refusé cette autorisation.

Quelle durée de conservation des données ?

La durée de conservation de ces données est de six mois.

Selon une jurisprudence constante, les dossiers et fichiers créés par un salarié à partir d'un matériel informatique fourni par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, et peuvent être ouverts et consultés par l'employeur en l'absence de l'intéressé dès lors qu'ils n'ont pas été identifiés comme étant « personnel » par l'intéressé.

Cela concerne toutes les technologies : courriels, connexions internet et clé USB et SMS.

Quel recours pour les employé-es ?

Saisir l'inspection du travail, le procureur de la République, et le service de plaintes de la CNIL.

6 - Le contrôle par chronotachygraphe

Le chronotachygraphe est un appareil installé dans les véhicules de transports routiers pour enregistrer des données personnelles relatives à la conduite du salarié : vitesse, temps de pause, temps de conduite.

En application d'un règlement communautaire l'employeur est tenu de mettre en place cet appareil dans tous les véhicules de transports de neuf personnes et dans les véhicules de plus de 3,5 tonnes.

Si l'employeur est dispensé de toute déclaration à la CNIL, il doit toutefois respecter certaines obligations comme celles d'informer les conducteurs de la mise en place de cet appareil, de leurs droits à accéder aux données collectées, de conserver les données pendant au moins un an...

Pour aller plus loin

Consulter le site de la CNIL : ***http://www.cnil.fr/***

Les équipes syndicales ont tout intérêt à consulter régulièrement le site qui est une source essentielle d'informations sur les obligations des employeurs, les recours possibles des salarié-es et notamment.pour obtenir :

- les fiches pratiques relatives à la géolocalisation des véhicules ; la vidéosurveillance ; le recrutement et la gestion du personnel ; l'accès aux locaux et le contrôle des horaires; les outils informatiques au travail.

Ces fiches très synthétiques précisent le but des contrôles mis en place, les obligations des employeurs vis-à-vis des salariés, les recours possibles pour les personnes, les textes de référence ...

- des modèles de plaintes : le site comporte des courriers types en fonction de la nature de la surveillance accessibles en ligne ***http://www.cnil.fr/vos-droits/plainte-en-ligne/***

Il est possible de les adresser également par écrit à l'adresse suivante : Service des plaintes 8 rue Vivienne CSS 30223 75083 Paris cedex 02.

En 2014, 300 plaintes ont été déposées auprès de la CNIL par des salarié-es pour dénoncer des systèmes de vidéo surveillance.

- La CNIL tient également une permanence juridique : 01 53 73 22 22

Outils déjà parus

Outils n° 1
Pression au travail : quand des collègues "pètent les plombs"

Outils n° 2
Le Document Unique : une opportunité pour rendre visible ce que vivent les salariés

Outils n° 3
Le stress : tout le monde en parle...que faire ?

Outils n° 4
Donner la parole aux salariés

Outils n° 5
L'expertise CHSCT

Outils n° 6
Droit de retrait et d'alerte

Outils n° 7
Les cancers professionnels, enjeux syndical

Outils n° 8
Que faire en cas de suicide ou tentative de suicide ?

Outils n° 9
La réforme de la médecine du travail

Outils n° 10
Instance de coordination des CHSCT

Outils n° 11
La pénibilité au travail : quelle compensation et quelle prévention? Le compte pénibilité

Outils n° 12
Pressions et répressions sur les militant-es syndicaux

Outils n° 13
Lien de subordination et représentation du personnel

Outils n° 14
Le droit d'alerte sanitaire et environnemental : un nouveau droit pour les salariés et les représentants au CHSCT

Outils n° 15
La pénibilité au travail

Outils n° 16
Fonction publique d'État : l'impact des réorganisations sur les conditions de travail

Sur notre site :
http://www.solidaires.org/-Les-fiches-Conditions-de-travail-

Appel :

La commission Santé Conditions de travail de Solidaires est preneuse des rapports d'expertises et du matériel syndical associé.

etvoilaletravail@solidaires.org