

Article 26

## Surveillance des travailleurs

<sup>1</sup> Il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail

<sup>2</sup> Lorsque des systèmes de surveillance ou de contrôle sont nécessaires pour d'autres raisons, ils doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs.

### 1. Généralités

La protection de la personnalité des travailleurs, déjà ancrée dans l'article 328 CO, s'étend par cet article au droit public du travail. Les travailleurs sont, de ce fait, protégés par une disposition de droit public contre une surveillance de leur comportement. Cela signifie qu'il n'est pas admis de déroger à ces dispositions par un accord de droit privé, par exemple une convention entre l'employeur et les travailleurs ou leurs organisations. L'installation d'un système de surveillance ou de contrôle est admissible uniquement s'il est nécessaire pour d'autres raisons (telles que la sécurité ou le contrôle du rendement). Il faut prendre garde lors de son installation à ce que la protection de la personnalité et de la santé des travailleurs soit préservée le plus possible.

La poursuite de délits commis dans l'entreprise n'est par principe pas l'affaire de l'entreprise, mais exclusivement de la police. Si un employeur n'en tient pas compte, les données de surveillance recueillies de manière illicite ne sont en principe pas exploitables dans une procédure pénale.

On sait par expérience que les installations de surveillance peuvent provoquer des sentiments négatifs chez les travailleurs concernés, voire des atteintes à la santé. A cela s'ajoute le fait que cela peut détériorer le climat dans l'entreprise.

Lorsque le recours à un système de surveillance ou de contrôle est indispensable, il est donc dans l'intérêt de toutes les personnes concernées qu'il soit utilisé avec le plus de retenue possible.

L'une des possibilités est de ne mettre en marche les systèmes de surveillance ou de contrôle qu'en l'absence des travailleurs (p. ex. systèmes de surveillance des vols, utilisation seulement lorsque cela est nécessaire, etc.).

A noter que le comportement et le rendement sont souvent liés. Pour cette raison, une différenciation précise entre la surveillance (autorisée) pour des raisons de sécurité ou de contrôle de rendement et la surveillance (non autorisée) du comportement est souvent difficile, voire impossible.

Exemples de surveillance autorisée dans le but d'optimiser le rendement:

- l'enregistrement automatique du nombre de pièces produits ou de leur qualité;
- l'enregistrement du nombre d'appels pris dans une centrale d'appels;
- l'enregistrement du trajet de véhicules d'entreprise dans un but d'optimisation économique des parcours par la personne chargée de la planification des trajets.

Le principe de proportionnalité est à respecter dans le cadre de l'enregistrement du rendement. Pour savoir si un système de surveillance répond au contenu de l'article 26 de l'OLT 3, il faut d'abord examiner si les trois conditions suivantes sont réunies :

- a) existence d'un intérêt nettement prépondérant autre que la surveillance du comportement des travailleurs (p. ex. sécurité du personnel, de l'entreprise ou optimisation de la production);



- b) proportionnalité entre l'intérêt de l'employeur à recourir à une surveillance et l'intérêt des travailleurs à ne pas être surveillés;
- c) participation des travailleurs à la planification, l'installation et l'emploi des systèmes de surveillance ou de contrôle et concernant la durée de conservation des données ainsi recueillis.

Il faut en outre s'assurer que les législations suivantes soient respectées :

- législation sur la protection des données (loi fédérale sur la protection des données, LPD, RS 235.1 ; ordonnance sur la protection des données, OLPD, RS 235.11). Ces bases juridiques ont pour but la protection de la personnalité et des droits fondamentaux des personnes physiques ou morales au sujet desquelles des privés ou l'administration fédérale traitent des données;
- Code pénal (RS 311.0).

## 2. Alinéa 1

D'une manière générale, on entend par systèmes de surveillance ou de contrôle tous les systèmes techniques (optiques, acoustiques, électroniques, etc.) qui permettent d'enregistrer une ou plusieurs activités ou le comportement des travailleurs.

La surveillance du comportement des travailleurs comprend toute surveillance permettant de vérifier, en permanence (de façon ininterrompue) ou non (par des contrôles périodiques sur de brefs espaces de temps ou par des contrôles par échantillons), certaines activités des travailleurs de façon détaillée.

Exemples:

- les équipements vidéo et les caméras qui enregistrent ce que font les travailleurs et comment ils le font;
- les microphones ou les interphones permettant d'enregistrer les conversations des travailleurs;
- les systèmes de localisation (GPS, RFID, etc.);

- les outils informatiques permettant de connaître les activités des travailleurs à l'ordinateur (logiciels espions, system logs, etc.);
- les systèmes et réseaux informatiques;
- les centrales téléphoniques, les systèmes d'écoute téléphonique;
- les fax et photocopieurs;
- internet (URL, courrier électronique, FTP).

On ne considère pas comme systèmes de surveillance ou de contrôle, notamment:

- les moyens tels que badges électroniques pour l'accès à une entreprise;
- l'enregistrement de l'heure d'entrée dans un bâtiment et de sortie;
- les systèmes électroniques de contrôle de qualité permettant de comptabiliser quotidiennement l'ensemble de la production d'une installation.

## 3. Alinéa 2

S'ils excluent la surveillance du comportement des travailleurs, des systèmes de surveillance et de contrôle peuvent être disposés sur le territoire de l'entreprise à tous les endroits stratégiques pour elle et où les travailleurs accèdent rarement tels que :

- extérieur des bâtiments, parkings extérieurs et souterrains;
- accès, entrées et passages;
- machines et installations dangereuses;
- salles des coffres;
- installations extérieures dangereuses;
- dépôts de produits dangereux.

Les systèmes d'enregistrement du temps de travail (puces RFID, bandes magnétiques, hologrammes, systèmes biométriques, etc.), les contrôles d'accès et les systèmes de suivi des mandats, entre autres, doivent être utilisés de telle manière qu'on ne puisse pas tirer de conclusions sur le comportement des travailleurs.

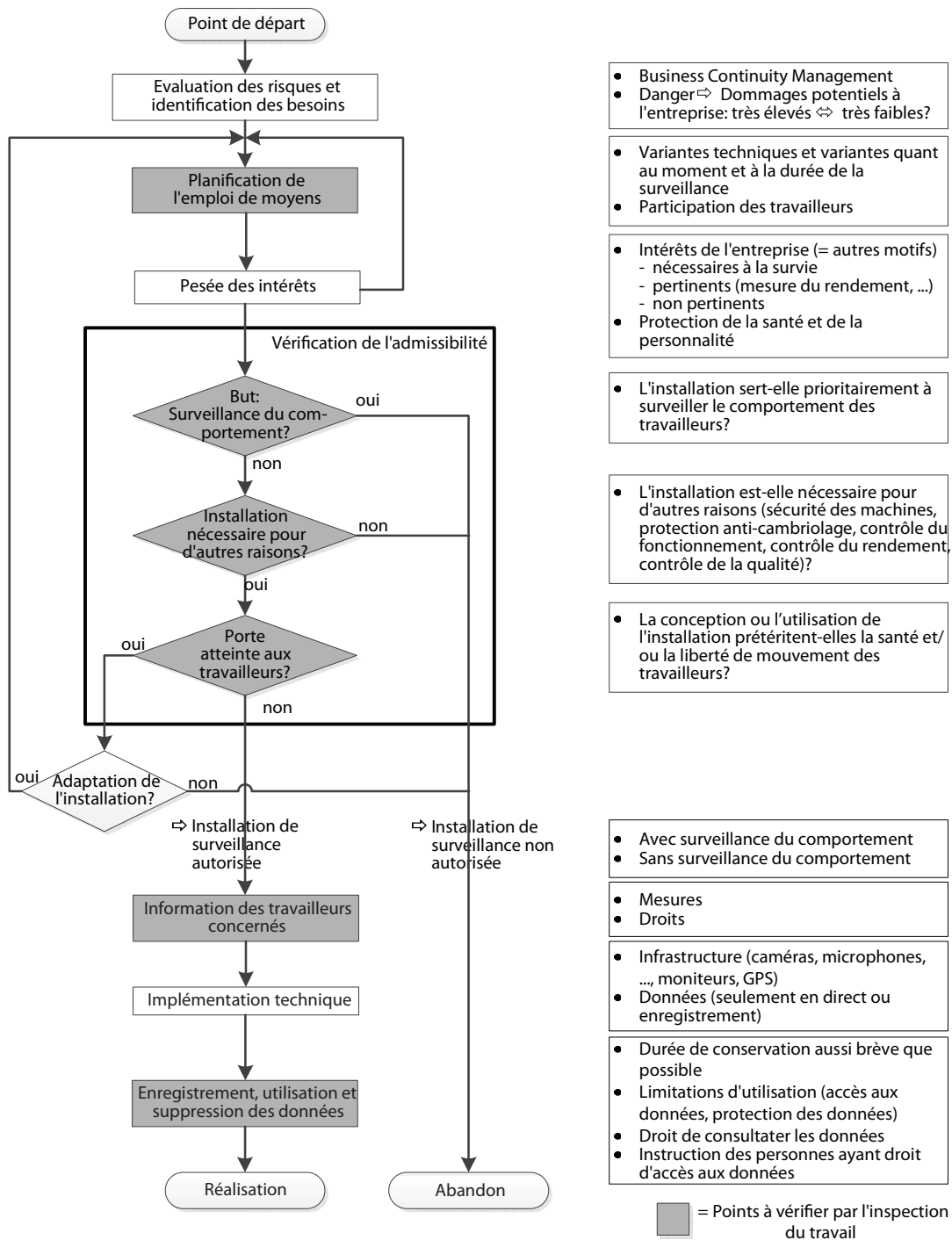
## Commentaire de l'ordonnance 3 relative à la loi sur le travail

Chapitre 2 : Exigences particulières en matière de protection de la santé  
Section 5 : Surveillance des travailleurs  
Art. 26

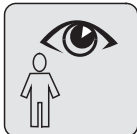


Art. 26

Modèle de planification et de décision concernant la mise en place d'un système de surveillance et de contrôle technique (à l'intention des employeurs, des travailleurs et des inspecteurs)



**Illustration 326-1** : Base de planification et de décision recommandée pour la mise en place d'un nouveau système de surveillance ou de contrôle



Il convient d'évaluer et de décider au cas par cas si un système de surveillance et de contrôle atteint l'objectif défini au début.

### 3.1 Intérêt prépondérant

Il faut procéder dans tous les cas à une pesée d'intérêts (intérêt de l'entreprise versus protection de la personnalité du travailleur).

Parmi les intérêts de l'entreprise figurent en particulier la sécurité des travailleurs, de tiers, de biens d'exploitation nécessaires à la survie de l'entreprise, la sécurité des données et le respect de la loi (p. ex. les casinos, qui ont l'obligation d'être équipés de systèmes de vidéo-surveillance selon l'art. 3 de l'ordonnance du DFJP sur les systèmes de surveillance et les jeux de hasard, RS 935.521.21). Il y a intérêt prépondérant lorsque l'intérêt de l'entreprise est considéré comme supérieur à celui de la protection de la personnalité des travailleurs.

Plus un bien à surveiller est important pour l'existence même d'une entreprise, plus on tendra à considérer la surveillance des travailleurs qui ont accès à ce bien ou qui le manipulent comme acceptable.

Avant de recourir à une surveillance directe par des moyens techniques, l'entreprise doit toutefois clarifier s'il n'est pas possible d'assurer la sécurité du bien d'une manière plus simple (proportionnalité de l'engagement des moyens).

Exemples d'intérêts prépondérants de l'entreprise:

- surveillance d'une salle des coffres dans une banque au moyen de caméras;
- surveillance dans des ateliers d'orfèvrerie / galeries d'art;
- GPS indiquant précisément l'emplacement d'un véhicule (pour des chauffeurs transportant des personnes ou des biens (p. ex substances dangereuses ou périssables), ainsi que pour des prestataires de services tels que les taxis, les services de dépannage, ajusteurs-monteurs d'entretien, etc.).

### 3.2 Proportionnalité (intérêts et moyens)

Le principe de la proportionnalité est respecté lorsque

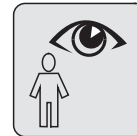
- l'intérêt de l'entreprise l'emporte sur l'intérêt du travailleur à la protection de sa personnalité, et
- le système de surveillance et de contrôle est installé de manière à limiter au maximum l'atteinte à la personnalité du travailleur.

Il est conseillé aux entreprises qui entendent recourir à des systèmes de surveillance ou de contrôle d'établir un dossier comprenant le descriptif du fonctionnement, du mode et du moment des enregistrements; elles pourront ainsi apporter la preuve que ces derniers ne nuisent ni à la santé ni à la protection de la personnalité des travailleurs. Dans ce but, il y a lieu d'évaluer différentes alternatives du point de vue technique et quant au moment et à la durée de la surveillance et du contrôle, en évitant autant que possible la surveillance vidéo.

Après avoir admis qu'il existe un intérêt légitime à la surveillance, on se posera la question suivante sur le choix des moyens : le système de surveillance ou de contrôle respecte-t-il la santé et la protection de la personnalité des travailleurs ? Si tel n'est pas le cas, on recherchera un autre mécanisme, qui remplit cette exigence.

Exemples d'utilisations appropriées des moyens :

- Une localisation des personnes ou régulation de l'accès à certaines parties de l'entreprise au moyen de badges ou d'identification biométrique, par exemple, est préférable à une surveillance vidéo des travailleurs.
- Les systèmes et réseaux informatiques offrent de nombreuses possibilités de surveillance et de contrôle. L'entreprise doit informer leurs utilisateurs de la forme de surveillance employée. L'utilisation d'internet doit être réglementée par l'entreprise.
- Les installations téléphoniques destinées à l'écoute et/ou à l'enregistrement pour le contrôle du rendement lors de ventes par téléphone, sont admissibles si les personnes contrôlées ont don-

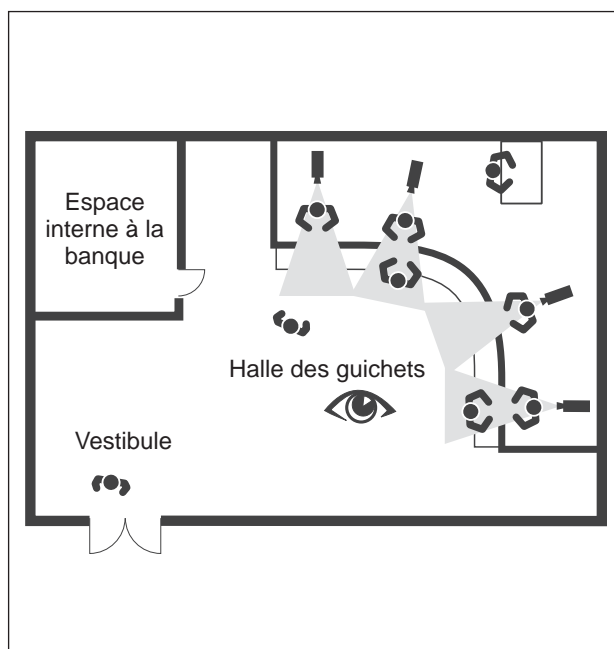


né leur assentiment et sont immédiatement mises au courant de la surveillance, par exemple par un signal optique ou acoustique.

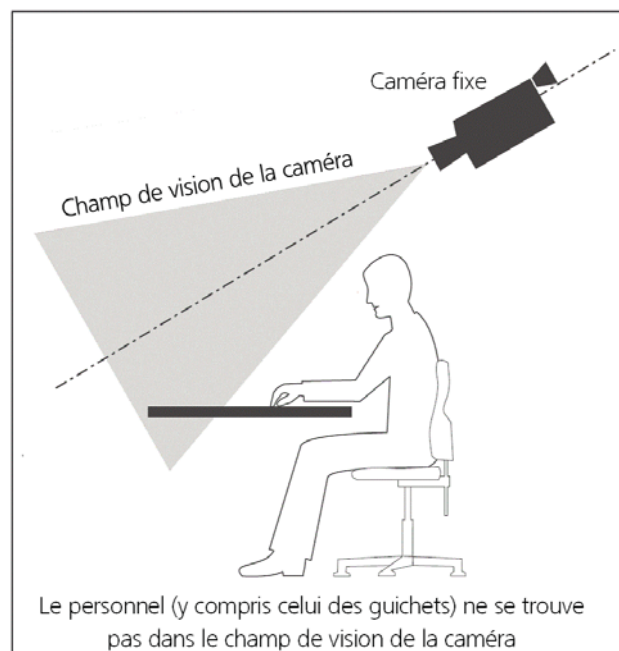
- Si les installations de surveillance et de contrôle lui servent principalement à se prémunir contre les vols, l'entreprise doit informer ses collaborateurs des systèmes de surveillance et de contrôle utilisés (cf. chiffre 3.4 Information et consultation des travailleurs). Les caméras vidéo doivent être placées et réglées de manière que le personnel n'apparaisse pratiquement pas dans leur champ d'observation et ne soit pas enregistré. Les positions et le champ de vision doivent être discutés avec les travailleurs de sorte qu'ils connaissent le secteur d'observation. Les illustrations 326-2 et 326-3 montrent la position de caméras et le champ qu'elles couvrent dans une salle des guichets d'une banque, où le personnel et la clientèle ne sont pas séparés par un vitrage de sécurité. Le personnel bancaire ne se trouve qu'exceptionnellement dans le champ de la caméra.

- Si la surveillance vidéo dans des installations de production complexes sert principalement à la conduite de procédés et à la sécurité, la position des caméras fixes et mobiles et leur champ d'observation sont à choisir de façon que seul le procédé soit surveillé et que les travailleurs n'apparaissent qu'exceptionnellement sur l'image. Si la surveillance des travailleurs eux-mêmes est impérative pour des motifs de sécurité, par exemple pour pouvoir les protéger dans des situations dangereuses dans une centrale de commande, on examinera des solutions de rechange, comme des signaux réguliers à quittancer, faute de quoi une alarme est déclenchée.

On réduira au maximum la durée de fonctionnement du système de surveillance (cf. aussi chiffre 3.3 Protection des données et de la personnalité), en ne l'enclenchant qu'à certaines étapes critiques ou en faisant en sorte que le travailleur puisse l'enclencher lui-même pour se protéger (p. ex. caméras avec microphones dans un magasin de station-service, dans un magasin ou un restaurant, que les travailleurs mettent en marche lorsqu'il y a danger d'agression).



**Illustration 326-2** : Position des caméras et leur champ d'observation dans le cas de guichets de banque « ouverts », sans séparation entre clients et personnel (plan)



**Illustration 326-3** : Surveillance de guichets de banque « ouverts » (coupe)



### 3.3 Protection des données et de la personnalité

La collecte, le traitement et l'enregistrement de données personnelles doit se faire conformément à la législation sur la protection des données (cf. chiffre 1 Généralités).

Le traitement de données personnelles obéit au principe de la bonne foi. La bonne foi signifie ici que le traitement des données doit être effectué de manière transparente pour la personne concernée, c'est-à-dire qu'elle est informée au préalable et de manière détaillée du type et du but du traitement.

Le principe de la proportionnalité doit être systématiquement respecté. Il implique que seules les données pertinentes ou utiles doivent être traitées, puis effacées dans un laps de temps aussi court que possible, déterminé à l'avance. L'accès aux données personnelles traitées doit être réglementé à l'interne. Il doit être limité aux personnes habilitées à procéder à leur dépouillement. Après le contrôle, il est illicite d'archiver des données par souci de sécurité.

L'emploi des technologies de l'information et de la communication, la saisie des données et leur dépouillement doivent être réglementés à l'interne. L'entreprise rédigera un règlement interne, dans lequel elle renseignera les travailleurs de manière transparente sur les droits et les obligations qui leur échoient dans le cadre de l'utilisation de systèmes de surveillance ou de contrôle (p. ex. installations téléphoniques, téléphonie sur internet et informatique) et sur la façon dont le contrôle et la surveillance internes à l'entreprise ont lieu.

- Utilisation des installations téléphoniques de l'entreprise: L'enregistrement de données sur les conversations téléphoniques est soumis à des conditions sévères. Il ne doit pas être utilisé pour contrôler leur comportement des travailleurs. L'interdiction d'appels privés est à faire respecter par d'autres moyens (par exemple obtention des liaisons externes par une centrale ou par certains

appareils uniquement). S'il existe une telle interdiction, on donnera la possibilité aux travailleurs d'effectuer des appels privés à partir d'un appareil non surveillé. Aujourd'hui, l'employeur peut exiger que les appels téléphoniques privés de durée prolongée se fassent pendant les pauses, au moyen d'un téléphone mobile privé. Si les appels privés ne sont pas interdits, les numéros composés par les travailleurs lors de ces appels ne doivent pas être enregistrés. Il est tout au plus admissible d'enregistrer les premiers chiffres des numéros appelés, et cela uniquement pour des raisons de service (p. ex. pour la facturation). Les travailleurs doivent en avoir été préalablement informés.

- Usage de l'informatique: L'entreprise doit communiquer aux travailleurs de manière transparente quelles règles ils doivent observer en matière d'utilisation de l'informatique et dans quels domaines et dans quelles zones elle a le droit de recourir à des systèmes de surveillance ou de contrôle. Les travailleurs doivent en particulier être informés des règles internes concernant l'utilisation d'internet et du courrier électronique (compte de messagerie). Il en va de même des règles selon lesquelles l'employeur peut accéder à la boîte électronique d'un travailleur absent (p. ex. pour cause de maladie ou de vacances).

Il faut rappeler que l'enregistrement de l'environnement sonore ou visuel (p. ex. sur des chantiers, dans la zone d'accès de l'entreprise, dans les locaux de l'entreprise, etc.) sans le consentement des personnes concernées peut constituer une contravention au sens pénal du terme selon les articles 179<sup>bis</sup> à 179<sup>quater</sup> du code pénal. Sont concernés ici, non seulement les travailleurs, mais tout tiers (par ex. client, passant) dont les données auraient été enregistrées sans qu'ils en aient été informés. Les zones surveillées (p. ex. par des caméras ou des microphones) doivent être clairement signalées comme telles.

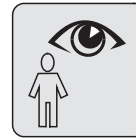


### Commentaire de l'ordonnance 3 relative à la loi sur le travail

Chapitre 2 : Exigences particulières en matière de protection de la santé

Section 5 : Surveillance des travailleurs

Art. 26



Art. 26

#### 3.4 Information et consultation des travailleurs

Lorsque des systèmes de surveillance ou de contrôle qui pourraient être utilisés également pour surveiller les travailleurs sont nécessaires, les travailleurs disposent d'un droit à l'information et à la consultation au sens des articles 5 et 6 OLT 3.

L'employeur doit motiver ses décisions sur des questions touchant à la protection de la santé lorsqu'il ne tient pas compte des objections des travailleurs ou de leur(s) représentant(s) dans l'entreprise ou qu'il n'en tient compte qu'en partie (cf. commentaire de l'art. 48 LTr).

#### 3.5 Accès aux documents et aux données

A leur demande, les autorités d'exécution de la loi sur le travail auront accès à tous les documents relatifs aux installations de contrôle et de surveillance ainsi qu'à toutes les données collectées par les systèmes de surveillance et de contrôle utilisés.

D'entente avec le maître du fichier ou sur proposition de celui-ci, la personne concernée peut également consulter ses données sur place. Si elle y a consenti et qu'elle a été identifiée, les renseignements peuvent également lui être fournis oralement.