Vie privée sur le lieu de travail : de A à RGPD

Votre liberté, votre voix

CGSLB
SYNDICAT LIBERAL

Vie privée sur le lieu de travail : de A à RGPD

Votre liberté, votre voix

CGSLB
SYNDICAT LIBERAL

E.R. : Mario Coppens, Boulevard Baudouin 8, 1000 Bruxelles. 11/2020

TABLE DES MATIÈRES

La vie privée sur le lieu du travail est un thème de plus en plus important. L'importance économique et sociale croissante des technologies (de l'information) n'y est pas étrangère. L'entrée en vigueur du RGPD en 2018 a donné un coup de pouce supplémentaire et placé la vie privée en tête de l'ordre du jour. Cependant, de nombreuses questions subsistent à ce jour sur l'application du droit à la vie privée dans le contexte spécifique de la relation de travail. Dans cette brochure, vous trouverez une réponse aux plus importantes de ces questions.

1. Aperçu historique

1.1 Le droit à la vie privée

Le droit à la protection de la vie privée est un droit immémorial. Sa forme la plus ancienne était liée à l'inviolabilité du domicile. Dans le plus ancien code connu, le Code de Hammurabi (vers 1780 avant JC), la peine de mort était de mise en cas d'accès non autorisé au domicile de quelqu'un. Dans la **Constitution belge** originale de 1831, le droit à la vie privée était initialement exprimé dans le droit à l'inviolabilité du domicile (art. 15) et au secret des lettres (art. 29). Avec la **Convention européenne des droits de l'homme (CEDH)** de 1950 – qui a un effet direct dans l'ordre juridique belge – le droit à la vie privée a pris forme au sens large:

> **ARTICLE 8**
> 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

La même disposition au sens large est incluse dans la Constitution belge depuis 1994:

> **ARTICLE 22**
> Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.
> La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit.

1.2 La protection des données à caractère personnel

Avec l'émergence des premiers outils numériques de communication et d'information accessibles au grand public dans les années 70 et 80, le besoin s'est fait sentir d'une législation spécifique pour l**e traitement des données à caractère personnel**. Après tout, la nouvelle technologie rendait beaucoup plus facile le partage et le stockage des données à caractère personnel, ce qui représentait un risque accru pour la vie privée des personnes auxquelles ces données se rapportaient.
La **Convention 108 du Conseil de l'Europe** de 1981 a jeté les bases de toute législation ultérieure visant à protéger la vie privée lors du traitement des données à caractère

personnel. Les principes de base de cette convention ont été transposés très tôt en Belgique dans la Loi **sur la protection de la vie privée** de 1992.[1] La convention 108 a été précisée au niveau européen en 1995 par la **Directive 95/46/CE**.[2] En 2018, cette directive a cédé la place au **Règlement 2016/679**, plus connu sous le nom de **GDPR** (General Data Protection Regulation) ou **RGPD** (Règlement général sur la Protection des Données).[3] La loi belge sur la protection de la vie privée a été adaptée à ce règlement.[4]

1.3 La notion de « traitement de données à caractère personnel »

Aujourd'hui, le droit à la protection de la vie privée et le RGPD sont souvent mentionnés ensemble. Cependant, le droit à la protection de la vie privée va au-delà du seul RGPD. Après tout, le RGPD ne protège la vie privée que lorsqu'un traitement de données à caractère personnel a lieu. Le RGPD définit le **traitement** comme suit:

> toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Les données à caractère personnel sont définies comme suit:

> toute information se rapportant à une personne physique identifiée ou identifiable (la « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

1 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

2 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

3 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

4 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Si aucun traitement de données personnelles n'a lieu, le RGPD ne s'applique pas. Dans ces situations, le droit à la protection de la vie privée est protégé par les autres sources de droit évoquées ci-dessus.

2. RGPD

2.1 Nouveauté ?

2.1.1 De la prévention à la répression

L'entrée en vigueur du RGPD a placé le thème de la protection de la vie privée en bonne place à l'ordre du jour. Cela s'explique évidemment par les **amendes élevées** qui peuvent être infligées en cas de violation du règlement. Pour les infractions les plus graves, l'autorité de contrôle compétente peut infliger des amendes administratives allant jusqu'à 20 millions d'euros ou, pour une entreprise, jusqu'à **4 % du chiffre d'affaires annuel mondial total** de l'exercice précédent, le montant le plus élevé étant retenu.

Ces amendes élevées s'inscrivent dans un changement de paradigme général qui a été annoncé par le RGPD d'un cadre **préventif** vers un cadre **répressif**. En vertu de l'ancienne Directive, tout traitement (automatisé) de données à caractère personnel devait être notifié à l'avance à l'autorité de contrôle. L'autorité tenait un registre public de traitement. Dans le cadre du RGPD, cette logique a été inversée : les sous-traitants de données à caractère personnel tiennent eux-mêmes un registre de traitement, qui n'est pas public. Ils doivent pouvoir justifier la licéité du traitement, mais il n'y a pas d'obligation de notification. Le risque d'amendes élevées devrait décourager ceux qui traitent des données personnelles de violer la réglementation.

2.1.2 Les principes de base demeurent inchangés

Les principes de base pour un traitement correct des données inclus à l'article 5 du RGPD restent pratiquement inchangés par rapport à ceux énoncés dans la Convention 108 et la Directive 95/46/CE. Les **principes de cet article constituent l'épine dorsale et le cœur du règlement** et serviront également de guide dans cette brochure :

ARTICLE 5

1. Les données à caractère personnel doivent être :

   a) traitées de manière licite, loyale et transparente au regard de la personne concernée **(licéité, loyauté, transparence)** ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales **(limitation des finalités)** ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées **(minimisation des données)** ;

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder **(exactitude)** ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée **(limitation de la conservation)** ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées **(intégrité et confidentialité)** ;

2 Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celuici est respecté **(responsabilité)**.

2.1.3 Autres nouveautés

Néanmoins, le RGPD a introduit quelques innovations plus importantes et moins importantes :

- La définition du **« consentement »** comme motif de traitement licite des données a été renforcée. Désormais, il est défini comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair (NOUVEAU), que des données à caractère personnel la concernant fassent l'objet d'un traitement ».
- Deux nouveaux types de données ont été ajoutés et bénéficient d'une protection spéciale : les données **biométriques** et **génétiques**.
- Le **droit à la portabilité** des données a été introduit. Cela implique le droit pour toute personne concernée d'obtenir les données à caractère personnel la concernant, qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine et le droit de transférer ces données à un autre responsable du traitement.
- Le **droit à une copie** des données à caractère personnel traitées.
- Le droit pour la personne de ne pas faire l'objet d'une **décision fondée exclusivement sur un traitement automatisé, y compris le profilage**, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.
- La préparation obligatoire d'une **AIPD (analyse d'impact relative à la protection des données)** lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physique.
- Pour les traitements de données à une certaine échelle ou lorsque des données à caractère personnel sensibles sont traitées, la désignation obligatoire d'un **délégué à la protection des données (« DPO »)**.
- Sur la base du RGPD, les **sous-traitants**, et pas seulement les responsables du traitement, peuvent aussi être tenus pour **responsables** d'un traitement incorrect s'ils n'ont pas respecté les obligations prévues par le règlement qui incombent spécifiquement aux sous-traitants ou qu'ils ont agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.
- Une **notification obligatoire d'une violation** de données à caractère personnel (par exemple, une fuite de données) à l'autorité de contrôle dans les 72 heures, dans la mesure où la violation présente un risque pour les droits et libertés des personnes physiques.
- Introduction des principes de **protection des données dès la conception (« by design ») et par défaut (« by default »).**

2.2 Licéité, loyauté et transparence

2.2.1 Licéité

Comme première condition, tout traitement doit avoir une base légale. Selon le RGPD, cela peut être trouvé dans l'une des causes suivantes (art. 6):

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

EXEMPLES

- L'autorité espagnole de protection des données (ci-après: APD) a infligé une amende à un employeur qui avait licencié un employé sur la base d›images vidéo de cet employé obtenues illégalement.
- La même APD a infligé une amende à un syndicat qui partageait ses données personnelles avec 400 membres du syndicat sans le consentement de la personne concernée.
- Un employé hongrois avait fait part de ses préoccupations au sujet d'abus dans son entreprise auprès de l'autorité locale. L'employeur en avait entendu parler et lorsqu'il s'est renseigné auprès de la même autorité, cette dernière a informé l'employeur du nom du dénonciateur. Naturellement, l'autorité n'avait aucune raison licite pour cela.

2.2.1.1 Données sensibles

Le traitement de certaines **catégories particulières de données à caractère personnel** (données sensibles) est en principe interdit:

> Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Ce n'est que dans un nombre limité de cas énumérés dans le RGPD que l'utilisation de ces données peut être justifiée.

> **EXEMPLE**
> - L'APD chypriote a infligé une amende à une entreprise pour utilisation injustifiée des données sur la santé des travailleurs. L'entreprise a évalué la durée et la fréquence des absences pour cause de maladie à l'aide dudit « facteur Bradford ». Selon cette théorie de gestion, de courtes absences fréquentes perturberaient l'organisation du travail plus que des absences plus longues moins fréquentes. Le profilage des travailleurs en fonction de la durée et de la fréquence de leur maladie a été considéré comme disproportionné par l'APD compétente.

2.2.1.2 Consentement dans les relations de travail

Le consentement n'est pas une base juridique évidente dans la relation entre l'employeur et le travailleur. Après tout, l'employeur doit être en mesure de démontrer que le consentement était entièrement volontaire. Cela n'est pas évident étant donné le déséquilibre des pouvoirs inhérent à cette relation. Après tout, le considérant 43 du RGPD déclare que:

> (43)
> Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution

Le Groupe Traitement des Données article 29 (aujourd'hui « EDPB », le régulateur européen de la vie privée) l'exprime comme suit (Avis 2/2017):

> « **Les employés sont très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement**, étant donné la dépendance qui découle de la relation employeur/employé. Compte tenu du déséquilibre de pouvoir, les employés ne peuvent donner leur libre consentement que dans des circonstances exceptionnelles, dans lesquelles l'acceptation ou le rejet d'une proposition n'a aucune conséquence »

Les employeurs devront donc dans presque tous les cas rechercher une base juridique autre que le consentement. Ce n'est que lorsque le consentement est donné par **concertation collective/convention collective de travail** que les relations de pouvoir sont équilibrées et le consentement peut-elle être valablement donné.

2.2.2 Transparence

Le traitement des données à caractère personnel n'est autorisé que s'il est communiqué de manière transparente. La collecte de données secrètes n'est jamais autorisée.

La transparence concerne différentes facettes du traitement. Ces informations seront souvent incluses dans une **déclaration de confidentialité** :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
b) le cas échéant, les coordonnées du délégué à la protection des données;
c) les finalités du traitement auquel sont destinées les données à caractère personnel, ainsi que la base juridique du traitement ;
d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;
e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ;
f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
g) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
h) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
i) lorsque le traitement est fondé sur le consentement, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
j) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
k) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
l) l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

EXEMPLE

- Aussi bien l'APD française que grecque a déjà infligé des amendes aux employeurs qui ont installé une surveillance par caméra sur le lieu de travail de manière secrète ou insuffisamment transparente.

2.3 Limitation des finalités

La limitation des finalités est un élément essentiel d'un traitement correct des données. Le traitement n'est valable que si la finalité est explicitement établie et justifiée au moment où les données à caractère personnel sont collectées. Les données ne peuvent être utilisées qu'à cette fin. La réutilisation à d'autres fins pour lesquelles elles n'ont pas été collectées n'est pas autorisée.

EXEMPLE

- Un employeur qui utilise un système de badges comme contrôle d'accès à l'entreprise, ne peut pas utiliser les données d'entrée et de sortie pour vérifier le temps de travail.

2.4 Minimisation des données

Seule la quantité de données strictement nécessaire pour atteindre l'objectif du traitement peut être traitée.

EXEMPLES

- L'APD roumaine a condamné un employeur qui avait placé des caméras dans les vestiaires des employés sur la base de la violation du principe de minimisation des données.
- L'APD espagnole a condamné un employeur qui utilisait des caméras destinées à lutter contre le vol pour surveiller ses employés à d'autres fins.

2.5 Exactitude

Les données traitées doivent être exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour effacer ou rectifier rapidement toute donnée à caractère personnel inexacte.

2.6 Limitation de la conservation

Les données ne peuvent être conservées que le temps nécessaire aux fins pour lesquelles elles sont collectées. Ensuite, elles doivent être supprimées.

EXEMPLES

- Une entreprise allemande a été condamnée à une forte amende pour conservation inutilement longue des données collectées auprès de candidats dans le cadre d'une procédure de recrutement.
- En Hongrie, une entreprise a été condamnée à une amende pour ne pas avoir supprimé les courriels personnels d'un ancien employé.

2.7 Intégrité et confidentialité

Ce principe signifie que le sous-traitant ou le responsable du traitement traite les données à caractère personnel de manière à garantir leur sécurité et qu'elles soient protégées, entre autres, contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. Le sous-traitant ou le responsable du traitement devra prendre les mesures techniques ou organisationnelles appropriées pour ce faire.

EXEMPLES

- Un travailleur espagnol qui s'est plaint d'un cas de harcèlement au travail dans une lettre à la direction de l'hôtel et à la délégation syndicale s'est adressé à l'APD nationale parce que la direction et la délégation syndicale ont violé leur devoir de confidentialité en lisant la lettre lors d'une réunion avec d'autres travailleur.
- Toujours en Espagne, une entreprise a été condamnée à une amende pour violation de la confidentialité en remettant une fiche de paie au mauvais employé.
- Une autorité de sécurité sociale néerlandaise a été condamnée à une amende pour avoir enfreint le principe d'intégrité et de confidentialité pour ne pas avoir correctement sécurisé les données sensibles des employés (informations médicales). Selon l'APD néerlandaise, ces données sensibles nécessitaient une authentification multi-facteur (type « Itsme »).

3. RGPD ou cct ?

3.1 Exception dans le cadre de la relation de travail

Il existe un certain nombre de **conventions collectives de travail interprofessionnelles** importantes qui développent davantage le droit à la protection de la vie privée dans le contexte spécifique de la relation de travail. Ces conventions collectives de travail restent tout aussi importantes qu'avant le RGPD. Dans de nombreux cas, ces conventions collectives de travail offrent une meilleure protection du droit à la vie privée que le RGPD.

L'article 88 du RGPD offre la possibilité d'élaborer des règles spécifiques par convention collective de travail (interprofessionnelle, sectorielle ou au niveau de l'entreprise) :

> Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

3.2 Cct 81: Contrôle des données de communication électroniques en réseau

3.2.1 Principe

Avec cette convention collective de travail, les partenaires sociaux ont voulu créer un cadre dans lequel les employeurs, dans le respect des principes de transparence, de proportionnalité et de finalité, peuvent prévenir et tracer les abus de communication en ligne des travailleurs pendant les heures de travail (c'est-à-dire une utilisation qui va au-delà de l'usage professionnel et de l'usage privé occasionnel normal du réseau). Les garanties les plus importantes pour la protection du travailleur sont la limitation des

finalités (but) pour lesquelles il est autorisé de contrôler et la procédure par étapes en matière d'individualisation.

3.2.2 Information et consultation

Les travailleurs doivent être informés à l'avance (collectivement et /ou individuellement) de tous les aspects du contrôle et de la politique concernant l'utilisation (non) autorisée des moyens de communication en réseau.
Les systèmes de contrôle installés doivent être régulièrement évalués, selon le cas, au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail ou avec la délégation syndicale, de manière à faire des propositions en vue de les revoir en fonction des développements technologiques.

3.2.3 Limitation des finalités

Le contrôle de données de communication électroniques en réseau n'est autorisé que lorsque l'une ou plusieurs des finalités suivantes est ou sont poursuivies :

- la prévention de **faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs** ou **susceptibles de porter atteinte à la dignité d'autrui** ;
- la protection **des intérêts économiques, commerciaux et financiers de l'entreprise** auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (par exemple la divulgation de fichiers, la violation des secrets d'affaires, y compris la recherche et le développement, les processus de fabrication et toutes les données confidentielles) ;
- **la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise**, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;
- le respect de bonne foi des **principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.**

3.2.4 Individualisation

Dans un premier temps, le contrôle n'a lieu **qu'au niveau global**, c'est-à-dire sans pouvoir être lié à un travailleur individuel. Ce n'est que dans une **deuxième phase** que le contrôle peut être **individualisé** lorsqu'une infraction est établie.

L'individualisation des données de communication électroniques en réseau est, en fonction de la finalité que poursuit le contrôle installé par l'employeur, opérée :

- dans le cadre d'une **procédure directe** ;
- dans le cadre d'une **procédure indirecte** (avec procédure de sonnette d'alarme).

3.2.4.1 Procédure directe

L'individualisation directe des données de communication électroniques en réseau est autorisée lorsque le contrôle poursuit l'une ou plusieurs des finalités suivantes:

- la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
- la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (ex : divulgation de fichiers, violation des secrets d'affaires, y compris la recherche et le développement, les processus de fabrication et toutes données confidentielles) ;
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise.

Un employeur qui, dans le cadre d'un contrôle global (anonyme) aux fins énumérées ici, constate une anomalie, a la possibilité d'individualiser directement les données de communication électroniques en réseau à partir des données globales dont il dispose, de manière à retracer l'identité de la ou des personne(s) responsable(s) de l'anomalie.

3.2.4.2 Procédure indirecte

Lorsque le contrôle a pour objet de vérifier le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise, l'individualisation n'est autorisée que sous réserve d'une **phase préalable d'information**.

L'information a pour objet de porter à la connaissance du ou des travailleurs, de manière certaine et compréhensible, l'existence de l'anomalie et de les avertir d'une individualisation des données de communication électroniques en réseau lorsqu'une nouvelle anomalie de même nature sera constatée.

L'information doit revêtir un caractère de rappel ou de mise au point des principes et règles fixées dans l'entreprise de manière à éviter la survenance d'une nouvelle anomalie de même nature.

L'individualisation n'est autorisée qu'en cas de nouvelle violation après la communication de ces informations.

Le travailleur auquel une anomalie d'utilisation des moyens de communication électroniques en réseau peut être attribuée par application de la procédure d'individualisation indirecte, sera invité à un entretien par l'employeur.

Cet entretien a lieu avant toute décision ou évaluation susceptible d'affecter individuellement le travailleur.

3.3 Cct 68 : surveillance par caméras sur le lieu du travail

3.3.1 Information et consultation

Les travailleurs sont informés à l'avance (collectivement et/ou individuellement) de la surveillance par caméras envisagée.

Les informations à fournir concernent au moins :

- La finalité poursuivie ;
- le fait que des images sont ou non conservées ;
- le nombre de caméras et l'emplacement de la ou des caméras ;
- la ou les périodes concernées pendant lesquelles la caméra ou les caméras fonctionnent.

Si, à l'occasion de l'information du conseil d'entreprise, il apparaît que la surveillance par caméras peut avoir des implications sur la vie privée d'un ou de plusieurs travailleurs, le conseil d'entreprise ou, à défaut, le comité pour la prévention et la protection au travail examine les mesures qu'il y a lieu de prendre pour réduire l'ingérence dans la vie privée à un minimum. Après tout, en principe, la surveillance par caméra ne peut pas interférer avec la vie privée de l'employé.

Le conseil d'entreprise ou, à défaut, le comité pour la prévention et la protection au travail doit en outre évaluer régulièrement les systèmes de surveillance utilisés et faire des propositions en vue de les revoir en fonction des développements technologiques.

3.3.2 Limitation des finalités

La surveillance par caméras sur le lieu de travail n'est autorisée que lorsque l'une des finalités suivantes est poursuivie:

- la sécurité et la santé ;
- la protection des biens de l'entreprise ;
- le contrôle du processus de production ;
- le contrôle du travail du travailleur. La surveillance par caméras pour contrôler le travail du travailleur n'a pas pour but de filmer en permanence le travailleur.

3.4 Cct 89: contrôle de sortie

3.4.1 Information

Préalablement à la mise en œuvre d'un système de contrôles de sortie, l'employeur doit informer le conseil d'entreprise sur le système.

À défaut de conseil d›entreprise, cette information est fournie au comité pour la prévention et la protection au travail ou, à défaut d›un tel comité, à la délégation syndicale ou, à défaut, aux travailleurs.

L'information à fournir porte en tout cas sur :

- le périmètre de l'entreprise ou du lieu de travail ;
- les risques de vol dans l'entreprise ou sur le lieu de travail ;
- les mesures afin de prévenir ces risques ou d'y remédier ;
- et les méthodes de contrôle.

3.4.2 Limitation des finalités

Les contrôles de sortie ne sont autorisés que s'ils visent à prévenir ou à constater le vol de biens dans l'entreprise ou sur le lieu de travail.
Les contrôles de sortie des travailleur ne peuvent avoir pour objectif de mesurer les prestations des travailleurs ou de contrôler les présences des travailleurs.
Les contrôles à la sortie des travailleurs par des personnes peuvent (exclusivement) être effectués par des agents de gardiennage, avec ou sans l'aide de moyens électroniques, et de plus uniquement :

- s'il existe des motifs valables de croire que le travailleur a volé des biens à l'endroit qu'il quitte, sur la base du comportement du travailleur, d'indices matériels (par exemple un signal d'avertissement d'un système de détection) ou des circonstances ;
- par voie d'échantillonnage en vue de prévenir les vols.

Les contrôles de sortie systématiques ne sont autorisés que s'ils ont lieu par le biais de systèmes de détection électroniques et/ou techniques (sans l'intervention d'un agent de sécurité).

Le contrôle de sortie peut exclusivement consister en un contrôle des biens présentés par le travailleur contrôlé à l'agent de gardiennage, qu'il porte sur lui ou dans ses bagages à main et/ou qui se trouvent à l'intérieur de son véhicule ou d'un véhicule qu'il utilise.
Le fait de fouiller le travailleur en vue de découvrir des biens dissimulés n'est donc pas autorisée.

Les constatations qui peuvent être utilisées contre le travailleur doivent être communiquées par écrit.

3.5 Cct 38 : recrutement et sélection

La vie privée du candidat doit être respectée lors de la procédure de sélection. Les questions sur la vie privée ne sont justifiées que si elles sont pertinentes en raison de la nature et des conditions d'exercice de la fonction. Ceci s'applique non seulement à l'employeur mais également aux personnes, telles que psychologues et médecins, qui participent, au nom de ce dernier, aux activités de sélection.

Toutes les informations concernant le candidat sont traitées de manière confidentielle par l'employeur.

EXEMPLE

- Un employeur ne peut traiter les extraits de casier judiciaire (ancien « certificat de bonne vie et mœurs ») des candidats, sauf si la candidature concerne un poste pour lequel la loi exige qu›elle ne puisse être exercée que par une personne qui n'a pas été condamnée à certaines peines (voir par exemple l'article 275 de la loi du 2 octobre 2017 réglementant la sûreté privée et spéciale).
- Un employeur ne peut pas rechercher des informations personnelles sur un candidat (par exemple via les médias sociaux) qui ne sont pas directement pertinentes pour le poste proposé (par exemple sur les loisirs, les préférences politiques, etc.).

3.6 Cct 39 : nouvelles technologies

3.6.1 Principe

L'introduction de nouvelles technologies dans l'entreprise s'accompagne souvent de problèmes de protection de la vie privée. C'est pourquoi la convention collective de travail 39 concernant l'information et la consultation sur les conséquences sociales de l'introduction des nouvelles technologies est ici pertinente.

Lorsque l'employeur a décidé d'un investissement dans une nouvelle technologie et lorsque celui-ci a des conséquences collectives importantes en ce qui concerne l'emploi, l'organisation du travail ou les conditions de travail, il est tenu, au plus tard trois mois avant le début de l'implantation de la nouvelle technologie :

- d'une part, de fournir une information sur la nature de la nouvelle technologie, sur les facteurs qui justifient son introduction ainsi que sur la nature des conséquences sociales qu'elle entraine ; et
- d'autre part, de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie.

3.6.2 Champ d'application

La convention collective de travail n° 39 s'applique aux entreprises occupant habituellement en moyenne au moins 50 travailleurs pendant l'année calendrier qui précède la période où l'information doit être donnée.

3.6.3 Information et consultation

L'information écrite à fournir porte sur :

- la nature de la nouvelle technologie ;
- les facteurs économiques, financiers ou techniques justifiant son introduction ;
- la nature des conséquences sociales qu'elle entraine ;
- sur les délais de mise en œuvre de la nouvelle technologie.

L'information est donnée au conseil d'entreprise ou, à défaut, à la délégation syndicale. En l'absence de conseil d'entreprise et de délégation syndicale, l'information est donnée au comité pour la prévention et la protection au travail.

La concertation porte sur :

- les perspectives de l'emploi du personnel, la structure de l'emploi et les mesures d'ordre social projetées en matière d'emploi ;
- l'organisation du travail et les conditions du travail ;
- la santé et la sécurité des travailleurs ;
- la qualification et les mesures éventuelles en matière de formation et de recyclage des travailleurs.

La concertation est réalisée, selon les cas, au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail et avec la délégation syndicale, conformément aux missions dévolues à chacun de ces organes par les dispositions légales ou conventionnelles en vigueur.

4. Geolocalisation

Il n'existe actuellement aucune législation spécifique réglementant la surveillance des travailleurs via des systèmes GPS. Ce n'est qu'au sein de la commission paritaire 219 (organismes de contrôle reconnus) qu'une convention collective de travail sectorielle a été conclue à ce sujet.

La jurisprudence et les avis de l'APD donnent toutefois quelques lignes directrices auxquelles tout système de géolocalisation des travailleurs ou des véhicules qu'ils conduisent doit se conformer.

4.1.1 Limitation des finalités

Un système permettant de rechercher la localisation précise des membres du personnel, doit répondre à des finalités déterminées, explicites et légitimes qui en justifient l'installation et l'utilisation.

Par exemple, en fonction de la sécurité du travailleur, en fonction de la protection du véhicule de service, pour répondre à des besoins professionnels bien définis concernant le transport et la logistique, ou encore, pour surveiller le personnel, afin de contrôler l'utilisation professionnelle du véhicule de service et l'application honnête du régime de travail.

4.1.2 Proportionnalité

Si le système est installé en vue de contrôler l'exécution des missions confiées aux travailleurs, pareil contrôle devrait être ponctuel et justifié par des indices faisant soupçonner des abus de la part de certains employés.

Un contrôle permanent, avec lecture systématique des données enregistrées par le système de localisation, doit en principe être considéré comme disproportionné.

Il existe néanmoins certaines hypothèses dans lesquelles un contrôle plus régulier pourrait être justifié s'il est directement lié à la nature des tâches à accomplir par l'employé, et plus précisément afin d'optimiser la gestion des déplacements de véhicules professionnels (vendeurs, techniciens de terrain). Même dans ce cas, le suivi des véhicules ne doit pas être continu. Le système devrait en tout état de cause pouvoir être désactivé lors de l'utilisation du véhicule en dehors des heures de travail (déplacements domicile-travail, pauses...).

Les autres utilisations interdites comprennent entre autres :

- Le contrôle du respect des la limitations de vitesse ;
- La géolocalisation dans le véhicule d›un travailleur qui est libre d'organiser lui-même ses déplacements ;
- Le suivi des déplacements des représentants du personnel qui ont lieu dans l'exercice de leur mandat ;
- Le calcul du temps de travail des travailleurs lorsqu'un autre système est déjà prévu pour cela.

4.1.3 Information et consultation

Le principe de transparence peut se traduire en prévoyant une information détaillée au profit des personnes dont les données sont traitées, en particulier sur:

- la base juridique du traitement des données. Dans le cas de la géolocalisation, il s'agit vraisemblablement d'un intérêt légitime de l'entreprise ou de tiers ;
- qui est contrôlé ;
- la mesure dans laquelle les contrôles sont effectués ;
- les objectifs poursuivis par le contrôle ;
- la nature des abus qui pourrait mener à un contrôle ;
- la durée du controle ;
- les données traitées ;
- si les données sont envoyées en dehors de l'Union européenne ;
- quels sont les droits du travailleur, tels que le droit de consulter les données, le droit de déposer une plainte auprès de l'Autorité de protection des données, le droit de restreindre le traitement des données etc. ;
- la procédure qui sera suivie après le contrôle.

En outre, les procédures d'information et de consultation de la convention collective de travail 39 doivent également être respectées (voir ci-dessus).
Il est également largement admis qu'une **analyse préalable d'impact relative à la protection des données** (voir 2.1.3 ci-dessus) est nécessaire.

4.1.4 Règlement de travail

Étant donné que l›introduction du suivi GPS implique un pouvoir de contrôle supplémentaire du personnel de surveillance, une adaptation du règlement de travail sera nécessaire.

5. Le secret des communications

5.1 Interdiction

Le secret des communications est garanti, entre autres, par l'article 314bis du code pénal. Sur la base de cet article, il est interdit à l'employeur d'écouter ou d'enregistrer les conversations téléphoniques de ses travailleurs, ou de prendre connaissance du contenu de courriers électroniques (professionnels ou privés) qui ne lui sont pas destinés, à l'aide d'un appareil, sans leur consentement.
La loi relative aux communications électroniques sanctionne également pénalement la prise de connaissance par quelqu'un de l'existence ou de l'expéditeur/destinataire de toute information qui lui est envoyée par voie électronique et qui ne lui est pas personnellement destinée (cette interdiction concerne donc non seulement la prise de connaissance du contenu, mais aussi les métadonnées associées à la communication).

5.2 Exception : preuve des transactions commerciales et les call centers

Il existe une exception à l'interdiction ci-dessus. Cette exception s'applique dans deux cas et aux conditions suivantes :

- l'enregistrement d'une communication électronique et des données relatives au trafic qui s'y rapportent réalisées dans les transactions commerciales licites **comme preuve d'une transaction commerciale ou d'une autre communication professionnelle** (par exemple, banque et investissement), est autorisé à condition que les parties impliquées dans la communication soient informées de l'enregistrement, des objectifs précis de ce dernier et de la durée de stockage de l'enregistrement, avant l'enregistrement.
- la prise de connaissance et l'enregistrement de communications électroniques et des données de trafic, qui **visent uniquement à contrôler la qualité du service dans les call centers** sont autorisés, à condition que les personnes qui travaillent dans le call center soient informées au préalable et de la possibilité de prise de connaissance et d'enregistrement, du but précis de cette opération et de la durée de conservation de la communication et des données enregistrées. Ces données peuvent être conservées maximum un mois.

6. Preuve obtenue par le biais d'une atteinte à la vie privée

Les preuves obtenues en violation des réglementations visant à protéger la vie privée du travailleur doivent-elles être écartées ? Par exemple, un motif grave peut-il être prouvé sur la base d'un enregistrement réalisé avec une caméra de surveillance en violation de la convention collective de travail n° 68 ou sur la base de données de communication électroniques en réseau obtenues en violation de la convention collective n° 81 ?

Tout comme dans les affaires pénales (la doctrine dite d'Antigone), la Cour de Cassation en matière sociale est d'avis depuis un certain temps que, sauf disposition contraire expresse de la loi, il appartient au juge d'apprécier la recevabilité d'une preuve obtenue irrégulièrement, en tenant compte de l'élément ou des éléments de l'affaire prise dans son ensemble, y compris la manière dont les preuves ont été obtenues et les circonstances dans lesquelles l'irrégularité a été commise. A moins qu›une formalité prescrite à peine de nullité n'ait été méconnue, une telle preuve ne peut être refusée que si l'irrégularité commise entache la fiabilité de la preuve ou si l'usage de la preuve est contraire au droit à un procès équitable.

Dans leur jurisprudence récente, plusieurs juridictions du travail se sont ralliées à cette jurisprudence de la Cour de cassation. Toutefois, il existe également une jurisprudence selon laquelle cet arrêt de la Cour de cassation ne s'applique pas aux litiges concernant la fin de la relation de travail entre l'employeur et le travailleur. Les preuves obtenues par le biais d'une violation de la vie privée sont alors exclues des débats.

Compte tenu de cette jurisprudence partagée, un travailleur doit tenir compte du fait qu'il existe toujours un risque que des preuves obtenues par l'employeur en violation de la législation sur la protection de la vie privée puissent encore être utilisées contre lui dans le cadre d'un procès.

7. Droit à l'image

Le droit à l'image est un droit impliquant que pour chaque image d'une personne mais aussi pour l'utilisation de cette image, le consentement de la personne apparaissant sur cette image est requis (art. XI.174 du Code de droit économique) :

> Ni l'auteur, ni le propriétaire d'un portrait, ni tout autre possesseur ou détenteur d'un portrait n'a le droit de le reproduire ou de le communiquer au public sans l'assentiment de la personne représentée ou celui de ses ayants droit pendant vingt ans à partir de son décès.

Ce droit est en fait distinct de la protection de la vie privée. Néanmoins, ce droit est parfois abordé dans le contexte du droit du travail.

La portée du droit à l'image est définie comme suit par la jurisprudence et la doctrine :

- La doctrine et la jurisprudence s'accordent largement sur le fait que lorsqu'une personne sort au grand jour, par exemple dans **un lieu public**, elle donne son consentement tacite. Ce consentement découle des circonstances de fait. Le consentement reste requis pour l'utilisation et la reproduction de la photo ou de la vidéo prise. Dans ce cas, la personne doit cependant en être le sujet principal.
- Si certaines personnes se trouvent **par hasard sur une photo ou une vidéo**, prise dans un lieu public (par exemple, une photo d'un monument où quelques personnes sont représentées), on part du principe qu'une autorisation pour une utilisation ultérieure de cette photo ou vidéo n'est pas nécessaire.
- Lorsque des **images d'une foule** sont prises, aucune autorisation n'est en principe requise (ni pour la prise ni pour l'utilisation par la suite), car ici aussi la représentation de la personne est accessoire. Ce qui relève de la « foule » est évalué au cas par cas.
- Les **personnes publiques** (par exemple les politiciens, les stars du sport, les chanteurs, ...) ne doivent en principe pas non plus donner d'autorisation préalable. Après tout, le droit à l'information (liberté de la presse) s'applique ici, à condition qu'un certain nombre de conditions soient remplies. Certaines personnes ne sont considérées comme une personne publique que lors d'un événement spécifique (par exemple suite à une catastrophe ou à un délit).

www.cgslb.be