La cyber surveillance au travail

L'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution énoncent le principe fondamental du droit au respect de la vie privée et familiale de toute personne, droit qui s'étend également au monde du travail selon la jurisprudence de la Cour européenne des droits de l'homme (CEDH).

En effet, dans son arrêt, *Niemietz c. Allemagne*, la Cour a considéré « *qu'il serait trop restrictif de limiter (la vie privée) à un cercle intime où chacun peut mener sa vie personnelle à sa guise* ***et d'en écarter entièrement le monde extérieur à ce cercle.*** *Le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables... Il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciales* ».

Si le droit au respect de la vie privée et au secret des correspondances s'étend aujourd'hui au lieu de travail, ce droit dont jouissent les employés est néanmoins susceptible de connaître des limitations justifiées par le respect d'intérêts légitimes de l'employeur.

En effet, pour des raisons de sécurité notamment, ce dernier peut être amené de manière directe ou indirecte à contrôler ses salariés, grâce à des dispositifs allant de la consultation de la messagerie électronique et de l'enregistrement des conversations téléphoniques à la vidéosurveillance, la géolocalisation ou encore le contrôle des accès aux locaux.

Entrent alors en conflit deux intérêts apparemment contradictoires, mais néanmoins conciliables, entre lesquels il convient de trouver un juste équilibre.

Cette fiche pratique a donc vocation à résumer les droits et obligations des employeurs vis-à-vis de leurs employés lors de la mise en place de dispositifs de surveillance sur le lieu de travail.

La messagerie professionnelle

Aujourd'hui, la messagerie professionnelle est devenue un outil indispensable et bien souvent nécessaire à l'accomplissement, par l'employé, de ses missions de travail. Toutefois, la banalisation d'un tel dispositif de communication électronique n'exonère pas pour autant l'employeur du respect des dispositions relatives à la protection des informations nominatives, et bien qu'il puisse décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie mise à disposition de ses salariés, il est tenu également par l'obligation de respecter la vie privée de ces derniers.

- ***Fonctionnalités autorisées***

La Commission estime que tout traitement automatisé de messagerie professionnelle peut notamment avoir les fonctionnalités suivantes :

- échange de messages électroniques en interne ou avec l'extérieur ;
- historisation des messages électroniques entrants et sortants ;
- gestion des contacts de la messagerie électronique ;
- gestion des dossiers de la messagerie et des messages archivés ;
- établissement et lecture de fichiers journaux ;
- gestion des habilitations d'accès à la messagerie ;
- gestion de l'agenda ;
- mise en place d'une procédure de contrôle gradué ;
- contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants ou sortants ;
- établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

- ***Protection des correspondances privées sur le lieu de travail***

Pour la Commission, le respect du secret des correspondances privées est un principe intangible. Ainsi, l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent, et en soit d'accord.

Toutefois, pour que les messages soient considérés comme personnels, il convient pour les employés de les identifier comme tels, par exemple :

- en précisant dans l'objet du message des mots clés comme « ***privé*** », « ***[PRV]*** » ou encore « ***personnel*** » ;
- en incluant dans l'objet du message une mention laissant manifestement supposer que ledit message est privé, telle que « *vacances au Japon* » ;
- en stockant les messages dans un répertoire intitulé « *personnel* » ou « *privé* ».

La Commission considère donc comme excessive la pratique consistant pour l'employeur à recevoir tous les messages envoyés ou reçus par ses employés puisque cette pratique ne permet pas de distinguer entre les messages professionnels et personnels desdits employés.

Par ailleurs, seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée

à ses intérêts ou à la Loi. Cela peut notamment prendre la forme d'une Ordonnance judiciaire mandatant un huissier de justice aux fins d'accéder, voire d'enregistrer les messages privés litigieux.

- ***Dispositions en cas d'absence ou de départ de l'employé***

Afin d'assurer la continuité des affaires de l'entreprise pendant l'absence d'un salarié (congés, maladie…), la Commission estime que l'employeur pourra avoir accès aux messages professionnels dudit salarié, en utilisant une des méthodes suivantes :

- mise en place d'une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence ;
- désignation d'un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue ;
- transfert à un suppléant de tous les messages entrants.

Dans les deux derniers cas, le salarié devra toutefois être informé de l'identité de son suppléant et ce suppléant ne devra pas lire les messages identifiés comme privés ou personnels.

En outre, en cas de départ définitif de l'entreprise, l'employeur devra avertir l'employé de la date de fermeture de son compte afin de lui permettre de vider sa messagerie de ses messages personnels. Il devra également supprimer l'adresse électronique nominative de l'employé 3 mois maximum après le départ dudit employé.

- ***Modalités d'information des utilisateurs***

Tout employeur doit impérativement responsabiliser les utilisateurs à la protection de leurs informations nominatives. Dans un souci de transparence envers les utilisateurs, ainsi que de loyauté dans la collecte et le traitement des informations nominatives, la Commission recommande donc à l'employeur de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les modalités d'identification des messages privés ;
- la procédure d'accès à la messagerie par des personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

- ***Modalités d'information des tiers destinataires***

La Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant, afin d'informer les tiers destinataires de la finalité du traitement, ainsi que de leurs droits.

Par exemple : **V*os informations nominatives sont exploitées par [Nom de l'employeur] dans le cadre du traitement ayant pour finalité "[Finalité du traitement] ". Conformément à* la Loi n° 1.165 du 23 décembre 1993, *vous disposez d'un droit d'accès, de rectification et de suppression en écrivant [adresse de l'employeur].***

- ***Durée de conservation des données***

Conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, les informations nominatives objets du traitement ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont exploitées.

Ainsi, la Commission demande à l'employeur de prévoir les durées de conservation de données suivantes :

- s'agissant de l'administration de la messagerie électronique (compte individuel et carnet d'adresses) : 3 mois maximum après le départ de l'utilisateur ;
- s'agissant du contenu des messages émis et reçus, la Commission demande qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire ;
- s'agissant des données de connexion (logs, horodatage, fichiers journaux….) : 1 an maximum, en fonction de l'activité exercée.

En tout état de cause, la Commission recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées, conformément à l'article 10-1 susvisé.

Les dispositifs d'enregistrement des conversations téléphoniques

La mise en place de dispositifs d'enregistrements téléphoniques comprend un certain nombre de dangers intrinsèques, et notamment :

- le risque d'atteinte à la vie privée des employés lors d'une utilisation à caractère privé du téléphone ;

- le risque de disproportion entre le dispositif mis en place et les objectifs poursuivis par l'employeur ;
- la déloyauté de la collecte et du traitement des données nominatives d'une personne n'ayant pas les moyens de s'y opposer ou de se défendre.

- ***Fonctionnalités autorisées***

La Commission estime que des dispositifs d'enregistrements téléphoniques peuvent être mis en place pour les finalités suivantes :

- la traçabilité des ordres ;
- le contrôle de la régularité des opérations financières et bancaires effectuées dans le cadre de l'obligation de vigilance ;
- le contrôle qualité par échantillonnage et de manière aléatoire ;
- la résolution des malentendus ;
- l'établissement de preuves en cas de litige.

- ***Garanties pour la vie privée des salariés***

La Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi précise que « *le respect de la dignité humaine, de la vie privée et de la protection des données à caractère personnel devrait être garanti lors du traitement de données à des fins d'emploi, notamment pour permettre aux employés le développement libre de leur personnalité et afin de préserver la possibilité de relations sociales et individuelles sur leur lieu de travail* ».

En conséquence, la Commission appelle l'attention des employeurs sur le fait que les informations nominatives exploitées dans le cadre des traitements qui sous-tendent les dispositifs d'enregistrement des conversations téléphoniques ne sauraient être détournées de la finalité pour laquelle elles ont initialement été collectées.

En outre, ces dispositifs ne sauraient donner lieu à des pratiques abusives portant atteinte aux libertés et droits fondamentaux des collaborateurs, mais également aux droits conférés par la Loi aux Délégués du Personnel et aux Délégués Syndicaux.

Ainsi, l'employeur ne peut pas mettre en place un dispositif d'écoute ou d'enregistrement **permanent ou systématique,** sauf texte légal (par exemple, pour les services d'urgence).

L'employeur ne peut pas non plus enregistrer tous les appels pour lutter contre les incivilités. Il doit choisir un moyen moins intrusif (par exemple opter pour un système permettant au salarié de déclencher l'enregistrement en cas de problème).

Enfin, la Commission préconise que soit instaurée une modalité permettant d'avoir une conversation d'ordre privé non enregistrée, notamment par la **mise à disposition d'un « *téléphone blanc* » non enregistré** ou en laissant **la possibilité aux salariés d'utiliser leurs téléphones personnels**.

- ***Modalités d'information des personnes concernées***

L'enregistrement des conversations téléphoniques étant un traitement particulièrement intrusif dans la vie professionnelle et privée autant de l'appelant que de l'appelé, la Commission insiste particulièrement sur la nécessaire information des personnes concernées.

A ce titre, l'existence d'un tel traitement d'informations nominatives doit être portée à la connaissance desdites personnes, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Les collaborateurs doivent être informés de la manière la plus efficiente possible. Ainsi, à des fins de transparence, il conviendra d'instaurer une procédure écrite décrivant avec précision, notamment, le déroulement de la procédure de contrôle, ses modalités, les appareils téléphoniques concernés (fixes ou mobiles), la finalité des contrôles envisagés et les modalités de droit d'accès.

Concernant les clients et les tiers la Commission demande que ceux-ci soient informés de l'enregistrement : par le biais d'une clause contractuelle, par l'envoi d'un courrier à titre informatif mentionnant la finalité du traitement et les modalités d'exercice du droit d'accès, **ou par un message vocal**.

- ***Données collectées et traitées***

Conformément à l'article 10-1 de la Loi n°1.165 du 23 décembre 1993, la Commission considère que seules les catégories d'informations suivantes peuvent être traitées :

- identité : voix de l'appelant et de l'appelé ;
- contenu de la conversation téléphonique ;
- adresses et coordonnées : numéros de téléphone de l'appelant et de l'appelé ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux enregistrements ;
- données de connexion : logs, traces d'exécution, horodatage, fichiers journaux.

La vidéosurveillance

De nombreuses employeurs ont de plus en plus recours à des systèmes de surveillance afin, par exemple, d'assurer la sécurité des personnes ou des biens ou de contrôler les accès aux locaux.

Ces systèmes utilisent des moyens, plus ou moins complexes, nécessitant le recours à des outils numériques et informatiques, voire à des systèmes de vidéosurveillance.

Ils conduisent souvent à recueillir des informations permettant d'identifier une personne physique déterminée ou déterminable, et soulèvent donc des problèmes particuliers en matière de protection des informations nominatives.

- ***Fonctionnalités autorisées***

La Commission considère que, compte tenu du caractère intrusif des dispositifs de vidéosurveillance traitant les informations nominatives et des informations qui peuvent y être associées, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des impératifs sécuritaires suivants :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- permettre le contrôle d'accès ;
- permettre la constitution de preuve en cas d'infraction.

A ces impératifs peuvent s'ajouter des fonctionnalités propres à l'activité de l'employeur concerné comme, par exemple, l'évaluation du matériel et des effectifs sur le chantier lorsque ledit employeur est une société de travaux publics.

- ***Garanties pour la vie privée des salariés***

Il appartient à l'employeur de démontrer que les droits et libertés des personnes concernées seront protégés.

En conséquence, la Commission demande à l'employeur de préciser que le dispositif de vidéosurveillance mis en œuvre :

- ne permet pas de contrôler le travail ou le temps de travail du personnel ;
- ne conduit pas à un contrôle permanent et inopportun des personnes concernées.

C'est ainsi qu'elle considère que les caméras peuvent filmer :

- les entrées et sorties des bâtiments, en faisant attention toutefois à ne filmer que la surface strictement nécessaire ;
- les issues de secours et les voies de circulation internes ;

- les couloirs ;
- les lieux de stockage de marchandises ;
- les machines de production ;
- les locaux techniques ;
- les archives ;
- les lieux pouvant être considérés comme sensibles (ex : salles serveurs) ;
- le parking intérieur, extérieur et/ou souterrain à condition de ne pas filmer la voie publique ;
- les zones de livraison ou de chargement, les quais de livraison et de déchargement ;
- les caisses.

La Commission estime toutefois que l'installation de dispositif de vidéosurveillance est strictement interdite dans :

- les ateliers (production, montage/démontage…) où travaillent des employés ;
- les vestiaires, les cabinets d'aisance, les bains-douches, les toilettes ;
- les bureaux ainsi que tous lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause déjeuner ;
- les locaux syndicaux et leurs accès lorsque ceux-ci ne mènent qu'à ces seuls locaux.

Par ailleurs, elle rappelle que les caméras ne doivent pas filmer les employés à leur poste de travail, sauf circonstances particulières dûment justifiées. Ainsi, une caméra pourra par exemple filmer un employé manipulant de l'argent mais elle devra être orientée de manière à filmer davantage la caisse que le caissier.

- ***Modalités d'information des personnes concernées***

Conformément à l'article 14 de la Loi n°1.165 du 23 décembre 1993, tout système de vidéosurveillance doit être porté à la connaissance des personnes concernées.

Si l'employeur est libre de choisir le moyen d'information qu'il estime le plus adapté à sa structure ou activité, la Commission demande toutefois que l'information soit dispensée, dans tous les cas, par le biais d'un **panneau d'affichage** mentionnant de manière visible, lisible, claire et permanente l'existence de ce dispositif et comportant*, a minima :*

- un pictogramme représentant une caméra ;
- le nom du service auprès duquel s'exerce le droit d'accès.

- ***Données collectées et traitées***

Conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, les informations collectées doivent être « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement.

La Commission considère donc que les informations suivantes peuvent être collectées et traitées :

- identité : image, visage et silhouette des personnes ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux images ;
- informations temporelles et horodatage : lieu et identification de la caméra, date et heure de la prise de vue.

Concernant la collecte de la voix dans le cas de l'exploitation d'un système de vidéosurveillance, la Commission considère le plus souvent qu'une telle collecte est manifestement excessive au regard des fonctionnalités du traitement. En effet, la collecte de la voix en vue, par exemple, d'assurer la sécurité des biens et des personnes peut conduire à une surveillance pouvant être inopportune à l'égard des personnes concernées. La Commission est donc particulièrement attentive à la justification apportée par l'employeur.

- ***Durée de conservation des données***

Conformément à l'article 10-1 de la Loi n°1.165 du 23 décembre 1993, les données ne doivent être conservées que « *pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées* », à savoir **un mois**.

La géolocalisation

Les dispositifs dits de géolocalisation des véhicules permettent aux employeurs de connaître la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules qui leur sont confiés. Or, si ces systèmes sont susceptibles

d'améliorer les services rendus par les entreprises, leur usage peut donner lieu à des dérives qu'il convient de prévenir.

- ***Fonctionnalités autorisées***

La Commission considère que, compte tenu du caractère intrusif des dispositifs traitant la donnée de géolocalisation des véhicules et des informations qui peuvent y être associées, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des fonctionnalités suivantes :

- la sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge (chauffeurs de véhicules de remise, travailleurs isolés, transports de fonds et de valeurs, etc.) ;
- une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, (interventions d'urgence, flottes de dépannage, etc.) ;
- le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule (ramassage scolaire, nettoyage des accotements, etc.) ;
- le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens.

- ***Garanties pour la vie privée des salariés***

Pour la Commission, l'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent et inopportun de l'employé concerné. Aussi :

- s'agissant des véhicules professionnels pouvant être utilisés par les employés à des fins privées, l'employeur ne doit pas collecter des informations relatives à la localisation d'un employé en dehors des horaires de travail de ce dernier. Dans ce contexte, elle exige que ces derniers aient la possibilité de désactiver la fonction de géolocalisation des véhicules à l'issue de leur temps de travail ;
- concernant les employés investis d'un mandat électif ou syndical, ceux-ci ne doivent pas faire l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat ;
- l'utilisation d'un système de géolocalisation n'est pas justifiée lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.).

- ***Modalités d'information des salariés***

Nonobstant l'information collective prévue par des conventions collectives professionnelles, la Commission demande que l'employé soit clairement et individuellement informé, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 :

- de l'identité du responsable de traitement ;
- de la finalité du traitement ;
- du caractère obligatoire ou facultatif du dispositif ;
- de l'identité des destinataires ou des catégories de destinataires des informations ;
- de l'existence de ses droits d'accès, de rectification et le cas échéant de son droit d'opposition relativement aux informations le concernant.

Les contrôles d'accès par badges

Ces dispositifs utilisent des moyens plus ou moins complexes, nécessitant le recours à des outils numériques et/ou informatiques, voire à des systèmes de communications électroniques. Il peut s'agir de cartes magnétiques ou cartes à puce, avec ou sans contact, combinées à un dispositif de lecture desdites cartes, qui enregistre ou non les informations qu'elles contiennent. D'autres types de dispositifs sont également utilisés, tels que des codes secrets délivrés aux seules personnes habilitées ou des systèmes d'ouverture de portes à distance par le biais d'un poste téléphonique géré par autocommutateur.

Ainsi, l'essence même de tels systèmes repose dans la nécessaire identification des personnes aux fins de surveiller ceux qui pénètrent sur le lieu de travail ou dans certaines zones à accès restreint. Cette surveillance s'étend donc aussi bien à leur identité, qu'à la date, l'heure et la porte par laquelle ils ont pu accéder aux locaux.

- ***Fonctionnalités autorisées***

La Commission considère que la mise en œuvre de dispositifs de contrôle d'accès ne peut avoir d'autres fonctionnalités que :

- de contrôler l'accès aux entrées et sorties de l'entreprise ;
- de contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- de gérer les horaires et les temps de présence des employés ;
- de contrôler l'accès des visiteurs ;
- de permettre, le cas échéant, la constitution de preuves en cas d'infraction.

- ***Garanties pour la vie privée des salariés***

Ces dispositifs ne sauraient être détournés de leur finalité. Ainsi, ils ne peuvent en aucun cas :

- conduire à un contrôle permanent et inopportun des personnes concernées ;
- permettre le contrôle des quotas d'heures que la Loi confère aux Délégués du Personnel et aux Délégués Syndicaux pour l'exercice de leurs fonctions ;
- permettre le contrôle des déplacements à l'intérieur de l'entreprise, exception faite des zones limitativement identifiées comme faisant l'objet d'une restriction de circulation.

- ***Modalités d'information des personnes concernées***

L'existence de tout traitement relatif à un contrôle d'accès par badges doit être portée à la connaissance des personnes concernées, à savoir les employés et visiteurs, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aux termes de cet article, cette information doit porter sur :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'opposition, d'accès et de rectification à l'égard des informations les concernant.

Les modalités de communication de cette information sont laissées au libre choix de l'employeur. Pour les employés, cette communication peut par exemple s'effectuer par voie d'affichage ou par la communication d'une note interne à l'entreprise.

Concernant les visiteurs, cette information pourrait par exemple prendre la forme d'une mention portée sur le formulaire de collecte des informations personnelles qu'ils remplissent, le cas échéant.

Les contrôles d'accès par des dispositifs biométriques

Dans un contexte où se mêlent technologie et sécurité, la biométrie tend à s'imposer dans un certain nombre de pays comme une méthode privilégiée d'identification dans les entreprises.

Pour la Commission toutefois, la donnée biométrique n'est pas une donnée d'identité comme les autres. En effet, elle n'est pas attribuée par un tiers ou choisie par la personne. Elle provient de son corps lui-même et le désigne de façon définitive. Le mauvais usage ou le détournement d'une telle donnée peut alors avoir des conséquences graves. C'est pour cela que le recours à la biométrie doit être strictement encadré.

- ***Traitement reposant sur la reconnaissance du contour de la main***

- **Fonctionnalités autorisées :**

La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main ne peut avoir d'autres fonctionnalités que de :

- contrôler l'accès aux entrées et sorties de l'entreprise ;
- contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- gérer les horaires et les temps de présence des employés ;
- contrôler l'accès des visiteurs ;
- permettre, le cas échéant, la constitution de preuve en cas d'infraction.

- **Données collectées et traitées** :

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : gabarit du contour de la main (résultat du traitement des mesures du contour de la main par un algorithme) ;
- Informations relatives à l'identité de l'employé : nom, prénoms, code d'authentification, photographie ;
- Informations relatives à la vie professionnelle : numéro d'identification interne, service, fonction ;
- Informations sur le temps de présence ou horodatage : date et heure d'entrée et de sortie, plages horaires autorisées, date et heure de passage à une zone à accès restreint, cumul des horaires, heures supplémentaires, absences, autorisations d'absence, congés ;
- Accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage, zones d'accès autorisé ;

- Parking : numéro d'immatriculation du véhicule, numéro de la place de stationnement ;
- Visiteurs : informations d'identité, dates et heures de passage, porte utilisée, organisme ou société d'appartenance, identité de l'employé accueillant le visiteur, gabarit du contour de la main.

- **Durée de conservation** :

- la donnée biométrique et le code d'authentification associé doivent être supprimés dès le départ de l'employé de l'entreprise ;
- les informations relatives à l'identité de l'employé, à la vie professionnelle et à la gestion du parking ne doivent pas être conservées au-delà d'une durée de 5 ans après son départ de l'entreprise ;
- les données relatives à l'accès aux locaux et aux informations sur le temps de présence ou d'horodatage ne doivent pas être conservées plus de 3 mois. Elles pourront être conservées 5 ans dans la seule hypothèse où l'employeur exploite ce dernier à des fins de contrôle du temps de travail et pour les employés uniquement ;
- s'agissant des visiteurs, les informations relatives à la donnée biométrique, à l'identité, à la vie professionnelle, et à la gestion du parking ne doivent pas être conservées au-delà d'une durée de 3 mois à compter de la dernière visite.

➢ ***Traitement reposant sur la reconnaissance du réseau veineux des doigts de la main***

- **Fonctionnalités autorisées** :

La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main ne peut avoir d'autres fonctionnalités que de :

- contrôler l'accès aux entrées et sorties de l'entreprise ;
- contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- contrôler l'accès des visiteurs ;
- permettre, le cas échéant, la constitution de preuves en cas d'infraction.

- **Données collectées et traitées** :

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : Gabarit du réseau veineux du doigt de la personne ;
- Informations relatives à l'identité de l'employé : nom, prénoms, photographie ;
- Informations relatives à la vie professionnelle : numéro d'identification interne, service, fonction ;
- Informations temporelles ou horodatage : date et heure d'entrée et de sortie, date et heure de passage à une zone à accès restreint, plages horaires d'accès autorisées ;
- Accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage, zone d'accès autorisées ;
- Parking : numéro d'immatriculation du véhicule, numéro de la place de stationnement ;
- Visiteurs : informations d'identité, dates et heures de passage, porte utilisée, organisme ou société d'appartenance, identité de l'employé accueillant le visiteur, gabarit du réseau veineux du doigt.

- **Durée de conservation** :

- les informations relatives à l'identité d'un employé, à la vie professionnelle et au parking ne doivent pas être conservées au-delà d'une durée de 5 ans après le départ de l'employé de l'entreprise ou de l'organisme, et les informations relatives aux informations temporelles ou horodatage ne doivent pas être conservées plus de 3 mois à compter de leur collecte ;
- les informations relatives aux visiteurs ainsi que les informations temporelles ou d'horodatage, et celles concernant les accès, ne doivent pas être conservées au-delà d'une durée de 3 mois à compter de la dernière visite ;
- le gabarit de l'empreinte biométrique doit être supprimé dès le départ de l'employé.

➢ ***Traitement reposant sur la reconnaissance de l'empreinte digitale***

- **Fonctionnalités autorisées** :

La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale, enregistrée sur un support individuel détenu par la personne concernée, **ne peut avoir d'autre fonctionnalité que de contrôler l'accès à certaines zones limitativement identifiées au sein de l'entreprise comme faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent**.

Elle interdit par ailleurs les dispositifs :

- enregistrant une image ou une photographie de l'empreinte digitale ;
- reposant sur la reconnaissance de l'empreinte digitale **avec stockage dans une base de données centralisée ou sur un terminal de lecture-comparaison**.

- **Garanties pour la vie privée des salariés** :

Le dispositif reposant sur la reconnaissance de l'empreinte digitale présentant plus de risques pour les individus que celui relatif au contour de la main ou au réseau veineux des doigts de la main, la Commission **exclut l'utilisation de cette donnée à des fins de gestion des horaires et des temps de présence des employés, ou à des fins de contrôle d'accès aux entrées et sorties de l'entreprise**.

Par ailleurs, ces dispositifs ne sauraient être détournés de leur finalité, et notamment ils ne peuvent en aucun cas conduire à un contrôle permanent et inopportun des employés.

Enfin, la Commission estime que les contrôles d'accès aux zones concernées ne doivent pas entraver la liberté d'aller et de venir des salariés protégés dans l'exercice de leurs missions.

- **Données collectées et traitées** :

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : gabarit de l'empreinte digitale ;
- Informations relatives à l'identité de l'employé : nom, prénoms, photographie ;

- Informations relatives à la vie professionnelle : numéro d'identification interne, numéro de carte, service, fonction ;
- Informations temporelles ou horodatage : date et heure de passage à une zone à accès restreint, plages horaires d'accès autorisées ;
- Accès aux locaux à accès restreint : nom et/ou numéro du point de passage à la zone à accès restreint, zones d'accès autorisées ;
- Tiers autorisé : nom, prénoms, dates et heures de passage à la zone à accès restreint, organisme ou société d'appartenance, identité de l'employé accueillant le tiers autorisé.

- **Durée de conservation** :

- les informations relatives à l'identité d'un employé et à sa vie professionnelle ne doivent pas être conservées au-delà d'une durée de 5 ans après le départ de l'employé de l'entreprise ;
- les informations relatives aux tiers autorisés, ainsi que les informations temporelles ou d'horodatage, et celles concernant les accès, ne doivent pas être conservées au-delà d'une durée de 3 mois à compter du dernier passage ;
- le gabarit de l'empreinte biométrique n'est conservé sur le support individuel que le temps durant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones limitativement identifiées de l'entreprise faisant l'objet d'une restriction de circulation.

- ***Modalités d'information des personnes concernées par tout traitement de contrôle d'accès reposant sur des dispositifs biométriques***

L'existence de tout traitement relatif à un contrôle d'accès par un dispositif biométrique doit être portée à la connaissance des personnes concernées, à savoir les employés et visiteurs, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aux termes de cet article, cette information doit porter sur :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'opposition, d'accès et de rectification à l'égard des informations les concernant.

Les modalités de communication de cette information sont laissées au libre choix de l'employeur. Pour les employés, cette communication peut par exemple s'effectuer par voie d'affichage ou par la communication d'une note interne à l'entreprise.

Concernant les visiteurs, cette information pourrait par exemple prendre la forme d'une mention portée sur le formulaire de collecte des informations personnelles qu'ils remplissent, le cas échéant.

Limitation des personnes ayant accès aux informations

Quels ques soient les dispositifs mis en place, la Commission considère que l'accès aux informations objets du traitement doit être limité **aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement ou du but recherché**.

C'est ainsi, par exemple, qu'elle estime que dans le cadre d'un dispositif de contrôle d'accès par badges non biométriques, les catégories de personnel suivantes pourront avoir accès à certaines des informations collectées :

- ✓ service du personnel / ressources humaines : identité des employés, informations relatives à la vie professionnelle, informations temporelles et horodatage, numéro d'identification interne ;
- ✓ service comptable / de paie : identité des employés, informations relatives à la vie professionnelle, informations temporelles et horodatage, numéro d'identification interne ;
- ✓ service gérant la sécurité des locaux : identité des employés, informations relatives aux visiteurs, accès aux locaux, parking, informations temporelles.