

## VIE PRIVEE DES SALARIES ET RESEAUX OUVERTS ET FERMES

Caprioli & Associés  
email : [contact@caprioli-avocats.com](mailto:contact@caprioli-avocats.com)

---

Plan :

### [I\) Protection des données à caractère personnel](#)

#### [1. Le cadre juridique](#)

#### [2. Applications](#)

### [II\) Exercice du contrôle sur l'activité des salariés sur l'Intranet et l'Internet](#)

#### [1. Les fondements légaux de la surveillance des salariés](#)

#### [2. Le contrôle électronique](#)

#### [Notes](#)

---

Dans le cadre d'une utilisation généralisée d'Internet ou d'Intranet par les salariés d'une entreprise (ouverture de compte permettant l'accès des stations de travail informatisées à un réseau ouvert ou fermé), il convient de rappeler un certain nombre de règles juridiques à prendre en compte simultanément notamment celles relatives au respect de la vie privée et à la protection des données personnelles, et celles édictées par le droit du travail.

- La protection des données à caractère personnel (I) ;
- L'exercice du contrôle de l'activité des salariés (II).

### **I) Protection des données à caractère personnel**

Certaines données concernant les salariés figurent de plus en plus souvent sur les sites WEB des entreprises (identité, téléphone, fax, mél, fonctions exercées, photographie, etc...). Mais elles peuvent également se trouver sur l'Intranet de l'entreprise par le biais de la mise en ligne d'informations sur l'activité commerciale, technique, financière, d'organigrammes, de notes de services, de documents administratifs, d'annuaires, de services de messagerie, de forums de discussion, etc...

## 1. Le cadre juridique

La loi du 6 janvier 1978 [\[1\]](#) impose la déclaration préalable auprès de la Commission Nationale Informatique et Libertés (CNIL) de tout traitement automatisé d'informations nominatives, définies comme celles qui permettent l'identification directe ou indirecte d'une personne, ce qui inclut aussi bien des données personnelles du salarié que des données professionnelles (sur Internet et en Intranet). Or, la loi n'établit aucune distinction entre données à caractère personnel ou professionnel ; elle a donc vocation à s'appliquer à tous les traitements !

L'entreprise qui ne respecte pas les obligations légales applicables en la matière s'expose à de sévères sanctions pénales [\[2\]](#), sa responsabilité civile peut en outre être engagée et donner lieu au paiement de dommages et intérêts [\[3\]](#).

Tant qu'un traitement informatisé de données personnelles n'a pas été déclaré auprès de la CNIL, les sanctions sont encourues et maintenues jusqu'à trois années après la fin de son utilisation.

L'article 29 de la loi du 6 janvier 1978 prévoit également une obligation de confidentialité et de sécurité à la charge de la personne qui ordonne ou effectue un traitement d'informations nominatives. Le titulaire du fichier est tenu de prendre « *toutes les précautions utiles pour préserver la sécurité des informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* » ; à défaut, il est passible des sanctions prévues par l'article 226 -17 du Code pénal [\[4\]](#).

## 2. Applications

### **2.1 Sites Web - Intranet**

Avant d'être mis en réseau (Internet), tout site web doit être déclaré auprès de la CNIL.

Si le site web contient des données relatives aux salariés telles que l'identité, la fonction, le téléphone (...), la CNIL recommande de recueillir l'accord des personnes concernées, préalablement à toute diffusion sur Internet et de laisser un délai de réponse.

La CNIL propose sur son site un formulaire type de déclaration pour les traitements automatisés mis en œuvre dans le cadre d'un site web. Ce formulaire mentionne toutes les informations qui doivent être portées à la connaissance des personnes concernées [\[5\]](#).

La diffusion de données personnelles sur l'Intranet doit être mentionnée dans la déclaration auprès de la CNIL ainsi que toutes les mesures permettant d'assurer la sécurité des informations collectées (firewall, cryptographie...).

### **2.2 Annuaire**

Depuis 1995, la CNIL autorise la mise en ligne d'annuaires professionnels sur un réseau international ouvert [\[6\]](#) sous réserve de respecter un certain nombre de conditions strictes [\[7\]](#). L'annuaire doit être déclaré auprès de la CNIL. Au préalable, l'éditeur de l'annuaire est tenu d'obtenir l'accord express des personnes concernées et doit les informer clairement de leur droits (accès, opposition et rectification). Sur le site, les textes français et européens applicables en la matière sont à mentionner ainsi que l'interdiction faite à quiconque de capturer les données à des fins commerciales ou marketing.

### **2.3 L'établissement de profils**

La CNIL autorise l'établissement de profils sur l'Internet par l'employeur à partir de données archivées et relatives à ses salariés sous réserve qu'il soit lié à l'exécution du contrat de travail.

### **2.4 Forums de discussion [\[8\]](#)**

Certains moteurs de recherche permettent d'obtenir l'adresse électronique des participants aux forums de discussion indexée dans la base de données ainsi que l'ensemble des sujets auxquels ils ont contribué et le contenu de leurs contributions. La CNIL recommande que les internautes qui accèdent à ces forums de discussion soient informés des risques de captation de leurs coordonnées et de leur participation et de l'interdiction faite d'utiliser les informations accessibles pour d'autres finalités que celle qui en a justifié la diffusion. En matière de protection des données personnelles, la responsabilité des espaces de discussion pèse sur les responsables des sites.

### **2.5 Les photographies**

En vertu de l'article 9 du code civil, la jurisprudence a consacré le droit à l'image des personnes : toute personne peut s'opposer à la diffusion de son image (sur quelque support que ce soit), considérée comme un attribut de la personnalité.

Partant, pour toute diffusion de photographie sur l'Internet (et Intranet), l'employeur doit avoir obtenu au préalable l'autorisation expresse des salariés concernés et il est tenu de leur indiquer de façon précise les conditions de l'utilisation des photos. L'autorisation doit être consignée par écrit et signée par le salarié.

## **II) Exercice du contrôle sur l'activité des salariés sur l'Intranet et l'Internet**

Sur le lieu et pendant le temps de travail, la surveillance et le contrôle des salariés sont des prérogatives reconnues à l'employeur qui découlent directement du contrat de travail et plus spécialement du lien de subordination. Malgré cette légitimité apparente du contrôle de l'activité des salariés, force est de constater que l'employeur doit respecter des règles identiques à celles qui sont applicables en matière d'écoutes

téléphoniques, de vidéosurveillance et de secret des correspondances. Aussi, le contrôle exercé par l'employeur est conditionnel :

- il ne saurait porter atteinte à la vie privée des salariés (article 9 du Code civil) ;
- il doit faire l'objet d'une information préalable des salariés (et organes représentatifs) ;
- il doit être justifié par un intérêt légitime (tel que prévenir la fraude, assurer la sécurité) ;

## **1. Les fondements légaux de la surveillance des salariés**

### **1.1 Le respect de la vie privée**

L'article L.120-2 du Code du travail prohibe tout contrôle arbitraire en prévoyant que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir, ni proportionnées au but recherché.* »

Cette interdiction est reprise par la loi du 6 janvier 1978 qui interdit la collecte frauduleuse, déloyale ou illicite de données [\[9\]](#).

### **1.2 L'information préalable des salariés et des organes représentatifs**

Principe posé par l'article L.121-8 du Code du travail et repris par la jurisprudence [\[10\]](#), l'information préalable des salariés de la présence d'un système de contrôle est une condition suspensive à son utilisation en toute légalité. Les salariés doivent également être informés de la destination des informations recueillies ainsi que de l'existence d'un droit de rectification pour les données nominatives les concernant.

Le comité d'entreprise doit être informé et consulté préalablement à la mise en œuvre dans l'entreprise d'un système de contrôle de l'activité des salariés [\[11\]](#). En outre, le remplacement de techniques de contrôle utilisées dans une entreprise par un matériel plus performant tel que l'Internet, l'Intranet ou des logiciels spécifiques justifie la consultation du comité d'entreprise [\[12\]](#).

### **1.3 Justification et limites du contrôle**

Le recours à un système de contrôle doit être justifié par un intérêt légitime tel qu'assurer la sécurité des locaux, des salariés ou de la circulation des informations. Comme l'a énoncé la CNIL, et confirmé par la jurisprudence, il ne peut avoir pour seul but de contrôler l'activité professionnelle des salariés.

L'obtention de preuves numériques pour sanctionner les salariés dans le cadre de l'exécution de leur contrat de travail pose problème. En effet, la jurisprudence sociale est réticente à accepter des vidéos ou autres preuves informatiques en raison des possibilités de manipulation, modification ou effacement partiel, volontaire ou non, qu'elles permettent.

## **2. Le contrôle électronique**

La surveillance électronique peut s'exercer par des logiciels de contrôle de l'activité des salariés (sites visités, durée de connexion, archivage des messages électroniques reçus et envoyés...).

Lorsqu'elles existent dans l'entreprise, les procédures de contrôle de l'activité des salariés doivent être conformes aux prescriptions légales, sous peine de constituer un moyen déloyal de collecte de données [\[13\]](#).

### **2.1 Aucune procédure de contrôle n'a été mise en place**

La loi du 10 juillet 1991 qui énonce le principe du secret des correspondances privées émises par la voie des télécommunications s'applique au courrier électronique. Les interceptions et autres lectures (ainsi que l'installation d'appareils conçus pour réaliser de telles interceptions) exposent leur auteur à des sanctions pénales [\[14\]](#).

En principe, toute correspondance émise par le salarié à partir de la boîte aux lettres mise à disposition par l'entreprise est considérée comme professionnelle et à ce titre les procédures de surveillance sont légitimes. En revanche, la jurisprudence a posé des limites franches à la surveillance du courrier électronique reçu par le salarié ou le préposé de l'entreprise [\[15\]](#).

Si le salarié dispose d'une boîte aux lettres personnelle, hébergée par un serveur externe de son choix mais qu'il consulte à partir d'un ordinateur de l'entreprise, la surveillance du courrier électronique risque de poser problème dans la mesure où la distinction entre messages professionnels et privés pourrait s'avérer délicate.

En l'absence de procédure de contrôle spécifique, il paraît opportun de réserver la messagerie électronique à un usage strictement professionnel et de le mentionner dans le cadre de l'information préalable des salariés lors de la mise en œuvre de systèmes de contrôle (spécialement dans une Charte d'utilisation) [\[16\]](#).

### **2.2 Existence d'une procédure de contrôle spécifique**

L'entreprise peut choisir d'adopter une procédure spécifique de contrôle conforme aux dispositions relatives au traitement des données nominatives énoncées par la loi du 6 janvier 1978. (déclaration à la CNIL, information préalable des salariés...) L'employeur pourra en outre prévoir d'informer les salariés sur :

- le lieu d'implantation des moyens de contrôle utilisés ;
- le droit d'accès des salariés contrôlés aux informations les concernant ;
- la nature des informations collectées et leur destinataires ;
- la durée de conservation des données...

### 2.3 Utilisation d'Internet

Des dispositifs de filtrage [17] ou de traçage [18] peuvent être mis en place par l'employeur afin de contrôler (voire limiter) l'utilisation privative d'Internet par les salariés, sous réserve d'avoir déclaré ces dispositifs auprès de la CNIL et informé au préalable les personnes concernées ainsi que les organes représentatifs s'ils existent (art. L. 432-2-1 du code du travail). La durée de conservation des relevés nominatifs doit être mentionnée dans la déclaration (6 mois en général).

L'employeur peut fixer des durées de connexion au delà desquelles les salariés ne sauraient utiliser Internet à des fins privées (20 minutes par semaine ou 1% du temps de travail, par exemple).

En cas de dépassement de ces limites, le temps d'utilisation d'Internet par les salariés n'est pas considéré comme du temps de travail effectif [19]. En conséquence, l'employeur peut opter pour une sanction disciplinaire à l'encontre du salarié fautif, sous réserve d'avoir joint au règlement intérieur de l'entreprise une charte fixant les règles d'utilisation privée d'Internet.

En outre, l'accord collectif peut prévoir l'exclusion du temps de travail effectif des périodes de connexion à Internet à titre privé, ou il peut fixer des limites d'utilisation privative d'Internet. Les salariés qui outrepassent ses limites s'exposent à des retenues sur salaire qui peuvent être proportionnelles à la durée de connexion à des fins personnelles.

La surveillance des salariés sur les réseaux ouverts ou fermés peut être affinée en fonction des systèmes de contrôle utilisés par l'employeur. Toutefois, ces contrôles doivent être effectués conformément aux dispositions relatives à la protection des données nominatives et au droit du travail. Il convient de souligner avec insistance que la rédaction d'une charte d'utilisation des moyens informatiques et de réseaux au sein de l'entreprise peut s'avérer très utile pour résumer les règles de droit, de déontologie et de manière plus générale de sécurité relatives à l'utilisation des ressources informatiques.

#### Notes :

[1] Loi n°78-17 du 6 janvier 1978, Informatique et Libertés, articles 15 et 16. (sous réserves des modifications apportées par la transposition de la Directive 95/46/CE 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)

*Le projet de loi adopté par l'Assemblée nationale le 30 janvier 2002 ( n°780) et le projet de loi adopté par le Sénat le 1<sup>er</sup> avril 2003 (n°96) prévoient des formalités préalables nouvelles. Certains traitements automatisés sont exonérés de toute déclaration (traitements ayant pour objet la tenue d'un registre, destinés à informer le public et à être consultés). Une déclaration préalable ou une autorisation est requise selon le cas pour les autres traitements automatisés.*

[2] Article 226-16 à 226-24 du Code pénal et article 42 de la loi prévoient jusqu'à 5 ans de prison et 300.00 € d'amende.

[3] Cass. Soc., 7 mai 1995 : Gaz. Pal. 1996, somm., p.2, note A. Mole.

[4] Sanction prévue de cinq ans d'emprisonnement et 300 000 euros d'amende.

[5] Notamment, l'exercice du droit d'accès, de modification, de rectification ou de suppression pour les personnes concernées par les données personnelles faisant l'objet d'un traitement.

[6] Délibération de la CNIL du 7 novembre 1995 sur la création d'annuaires de chercheurs.

[7] Délibération de la CNIL du 9 juillet 1996 pour les annuaires des personnels du CNRS,

Délibération de la CNIL du 8 juillet 1997 pour les annuaires en matière de télécommunications.

[8] « Un forum de discussion appelé également groupe de discussion ou encore news groupe est un groupe d'utilisateurs de l'Internet qui échangent par courrier électronique des informations sur un même thème. Il se caractérise en outre par une libre participation et une liberté de parole des intervenants. Pourtant, intervenir dans un forum doit toujours être un acte réfléchi dans la mesure où des milliers de bases de données accessibles à tous peuvent identifier des interventions, les conserver longtemps et profiler les internautes à volonté. Le forum est en lui-même un traitement automatisé de données soumis à déclaration. » Les études du Conseil d'Etat, « Internet et les réseaux numériques », la documentation française, 1998.

[9] Article 25 de la loi du 6 janvier 1978.

[10] Cass. soc. 20 novembre 1991, Bull. civ. V. n°519, p.323.

[11] Article L.432-2-1 du Code du travail.

[12] Article L.432-2 du Code du travail.

[13] Article 25 de la loi du 6 janvier 1978.

[14] Article 226-15 du Code pénal.

[15] Tribunal correctionnel de Paris du 2 novembre 2000, Juris -Data n°139077, confirmé par CA Paris, 11<sup>ème</sup> Ch. A, 17 décembre 2001, JCP 2002, éd. G, II 10087, note J. Devèze et M. Vivant.

[16] V. Cass. soc. 2 octobre 2001, Comm. com. élect. Novembre 2001, p.7 et s.. Cette décision donne tort à l'employeur d'avoir licencié un salarié qui utilisait la messagerie électronique mise à sa disposition à des fins personnelles et en l'absence de Charte d'utilisation.

[17] Techniques de contrôle à priori qui permettent d'interdire l'accès à certains sites et également certaines connexions de l'extérieur.

[18] Techniques de contrôle à posteriori qui permettent par exemple une vérification nominative des sites visités, de la nature des sites, du temps de connexion ...

[19] Article L. 212-4 du Code du travail qui prévoit que la durée du travail s'entend « du travail effectif à l'exclusion du temps nécessaire à l'habillage et au casse-croûte ainsi que des périodes d'inaction dans les industries et commerces déterminés par décret ».