

Pouvoir disciplinaire

Sommaire

§§

A Contrôle et surveillance	56020	Entretien préalable	56240
Objet du contrôle	56020	Choix de la sanction	56250
Mise en place des moyens de contrôle	56060	Notification de la sanction	56257
B Sanction disciplinaire	56120	Exécution de la sanction	56270
Définition	56120	D Contrôle judiciaire	56340
Sanctions interdites	56150	Réalité des fautes	56345
Non-cumul des sanctions	56155	Proportionnalité de la sanction	56350
C Procédure disciplinaire	56220	Annulation de la sanction	56355
Date de mise en œuvre	56225		

La surveillance et le contrôle des salariés sur le lieu et pendant le temps de travail ainsi que la possibilité de sanctionner leurs comportements fautifs sont des prérogatives reconnues à l'employeur. Elles découlent directement du contrat de travail et plus spécialement du lien de subordination. Le droit s'attache néanmoins à définir un certain nombre de conditions et de procédures garantissant au salarié la protection de ses droits fondamentaux.

Tout salarié, quels que soient l'activité ou la taille de l'entreprise, son ancienneté ou son statut, même s'il est en période d'essai, doit bénéficier de ces dispositions.

56000

A. Contrôle et surveillance

Objet du contrôle Accès à l'entreprise et déplacements du salarié
A condition de respecter les règles visées nos 56060 s., l'employeur peut mettre en place des **badges électroniques** pour contrôler l'accès à l'entreprise et la durée de travail des salariés.

56020

N-VIII-2900 s
N-VIII-10800 s

Le recours à un dispositif de **géolocalisation** du véhicule de fonction d'un salarié itinérant afin de contrôler la durée de travail n'est licite que si l'employeur n'a pas d'autre moyen d'effectuer ce contrôle et si le salarié concerné ne dispose pas d'une liberté d'organisation de son travail (Cass. soc. 3-11-2011 n° 10-18.036 : RJS 1/12 n° 4).

Sur le contrôle de la circulation des **représentants du personnel** dans et hors de l'entreprise, voir n° 62635.

56040

N-VIII-4900 s

Utilisation du matériel de l'entreprise L'employeur peut contrôler l'utilisation par ses salariés des outils mis à leur disposition pour l'exécution de leur travail. Une utilisation à des fins personnelles est généralement tolérée si elle est raisonnable et ne dégénère pas en abus. Elle peut être encadrée par le règlement intérieur ou, s'agissant du matériel informatique, par la charte informatique de l'entreprise.

56045

N-VIII-5800 s

Les connexions internet établies par le salarié durant son temps de travail sont présumées avoir un caractère professionnel ; l'employeur peut donc librement les contrôler, hors la présence de l'intéressé (Cass. soc. 9-7-2008 n° 06-45.800 : RJS 11/08 n° 1071 ; 9-2-2010 n° 08-45.253 : RJS 5/10 n° 399).

Il en est de même pour les courriels adressés par le salarié à l'aide de la messagerie électronique de l'entreprise, sauf disposition contraire du règlement intérieur (Cass. soc. 26-6-2012 n° 11-15.310 : RJS 10/12 n° 761) ou sauf si le salarié les a identifiés comme étant personnels (Cass. soc. 15-12-2010 n° 08-42.486 : RJS 2/11 n° 92 ; 18-10-2011 n° 10-26.782 : RJS 1/12 n° 3). Dans ce dernier cas, l'employeur ne peut pas librement les consulter, même si l'utilisation non professionnelle de la messagerie a été interdite (Cass. soc. 2-10-2001 n° 99-42.942 : RJS 12/01 n° 1394), sous peine de commettre le délit de violation du secret des correspondances (C. pén. art. 226-15). Mais s'il justifie d'un motif légitime, il peut demander au juge la désignation d'un huissier de justice à cette fin. Le procès-verbal, établi par ce dernier après ouverture du courriel en présence du salarié, est alors admissible comme preuve d'un manquement de l'intéressé à ses obligations contractuelles (Cass. soc. 23-5-2007 n° 05-17.818 : RJS 8-9/07 n° 909 ; 10-6-2008 n° 06-19.229 : RJS 8-9/08 n° 866).

S'agissant des fichiers informatiques enregistrés par le salarié sur son ordinateur professionnel, voir n° 56055.

Précisions

a. L'employeur peut se prévaloir d'un courriel, identifié comme personnel, s'il en a eu connaissance par le fait du salarié (Cass. soc. 2-2-2011 n° 09-72.313 : RJS 4/11 n° 289).

Même valablement consultés, les courriels du salarié ne peuvent être invoqués à l'appui d'une sanction disciplinaire que si leur contenu est en rapport avec son activité professionnelle et ne revêt pas un caractère privé (Cass. soc. 2-2-2011 n° 09-72.449, 09-72.450 et 09-72.313 : RJS 4/11 n° 289).

b. L'utilisation du matériel informatique de l'entreprise à des fins personnelles est en principe abusive lorsqu'elle revêt un caractère systématique ou si le salarié y consacre trop de temps au détriment de son travail. L'abus, s'il est établi, peut justifier une sanction ou un licenciement, le cas échéant pour faute grave comme cela a été admis dans un cas de connexions internet à des fins privées durant 41 h en un mois (Cass. soc. 18-3-2009 n° 07-44.247 : RJS 6/09 n° 508).

c. La faute du salarié peut également résulter de la nature des messages envoyés ou des sites internet consultés. Ainsi, constitue une faute le fait pour un salarié d'envoyer par la messagerie électronique professionnelle, dans des conditions permettant d'identifier l'employeur, un courriel contenant des propos antisémites (Cass. soc. 2-6-2004 n° 03-45.269 : RJS 8-9/04 n° 882), d'installer sur son ordinateur un logiciel permettant le téléchargement illégal d'œuvres musicales à partir de l'adresse IP de l'employeur (CA Versailles 31-3-2011 n° 09-742 ; RJS 10/11 n° 744), ou de recevoir, d'envoyer et de conserver sur son ordinateur des documents à caractère pornographique dont certains présentent un caractère délictueux (Cass. soc. 15-12-2010 n° 09-42.691 : RJS 2/11 n° 111). En revanche, la seule conservation par le salarié sur son ordinateur de 3 fichiers contenant des photos pornographiques sans caractère délictueux ne constitue pas, en l'absence de preuve d'un usage abusif affectant son travail, un manquement justifiant son licenciement (Cass. soc. 8-12-2009 n° 08-42.097 : RJS 3/10 n° 236).

56050

N-VIII-7900 s

La vérification par l'employeur du relevé des communications téléphoniques fourni par l'opérateur ne constitue pas un procédé de surveillance illicite même si les salariés n'en ont pas été avertis (Cass. soc. 15-5-2001 n° 99-42.937 : RJS 7/01 n° 830). Il en est de même de la vérification des relevés des appels passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise (Cass. soc. 29-1-2008 n° 06-45.279 : RJS 5/08 n° 511), si ce dispositif a été régulièrement déclaré à la Cnil : voir n° 56065. En revanche, l'écoute d'une communication à l'insu du correspondant constitue un procédé déloyal (Cass. soc. 16-12-2008 n° 07-43.993 : RJS 2/09 n° 133).

L'usage abusif du téléphone de l'entreprise à des fins privées peut justifier un licenciement (Cass. soc. 29-1-2008 n° 06-45.279 : RJS 5/08 n° 511), le cas échéant pour faute grave comme cela a été admis pour un salarié ayant quotidiennement appelé la métropole depuis la Martinique durant plusieurs mois (Cass. soc. 18-6-2003 n° 01-43.122 : RJS 8-9/03 n° 979).

56055

N-VIII-6200 s

Documents et objets personnels du salarié Les courriers adressés ou reçus par un salarié sur son lieu de travail sont protégés par le secret des correspondances, dont la violation est pénalement réprimée (C. pén. art. 226-15), dès lors que leur caractère

personnel est spécifié (Cass. mixte 18-5-2007 n° 05-40.803 : RJS 7/07 n° 810), ce qui n'est pas le cas s'ils portent la seule mention du nom et du prénom de l'intéressé (Cass. soc. 11-7-2012 n° 11-22.972 : RJS 10/12 n° 763). S'agissant des courriels transmis par le salarié au moyen de la messagerie électronique de l'entreprise, voir n° 56045.

Les **documents détenus par le salarié** sur son lieu de travail, qu'ils soient sous forme papier (Cass. soc. 18-10-2006 n° 04-47.400 : RJS 1/07 n° 7 ; 4-7-2012 n° 11-12.330 : RJS 10/12 n° 759) ou de fichiers informatiques (Cass. soc. 18-10-2006 n° 04-48.025 : RJS 12/06 n° 1241), sont présumés avoir un caractère professionnel et l'employeur peut en prendre connaissance librement. Il en est autrement si le salarié les a identifiés comme personnels. Dans ce cas, sauf risque particulier, l'employeur ne peut y accéder qu'en présence de l'intéressé ou celui-ci dûment appelé (Cass. soc. 17-5-2005 n° 03-40.017 : RJS 8-9/05 n° 799 ; 17-6-2009 n° 08-40.274 : RJS 8-9/09 n° 743). Comme pour l'ouverture des messages électroniques personnels, il peut aussi demander au juge la désignation à cette fin d'un huissier de justice (voir n° 56045).

Précisions a. Le fait pour le salarié d'intituler le disque dur de son ordinateur professionnel « D : /données personnelles » ne confère pas un caractère personnel à l'ensemble des données qui y sont contenues (Cass. soc. 4-7-2012 n° 11-12.502 : RJS 10/12 n° 760). L'**identification personnelle** d'un fichier informatique ne peut pas résulter du seul code d'accès à l'ordinateur du salarié ou de l'intitulé d'un répertoire portant le prénom de l'intéressé (Cass. soc. 8-12-2009 n° 08-44.840 : RJS 2/10 n° 144). Ne sont pas non plus identifiés comme personnels les fichiers dénommés « mes documents » (Cass. soc. 10-5-2012 n° 11-13.884 : RJS 7/12 n° 611) ou « Essais divers » (Cass. soc. 15-12-2009 n° 07-44.264 : RJS 3/10 n° 233).

b. Si l'employeur peut toujours consulter librement un fichier informatique (ou un dossier papier) non identifié comme personnel, en revanche, il ne peut pas se prévaloir de son **contenu** dès lors que celui-ci relève de la **vie privée** du salarié (Cass. soc. 5-7-2011 n° 10-17.284 : RJS 10/11 n° 745 ; 18-10-2011 n° 10-25.706 : RJS 1/12 n° 3).

L'employeur peut écouter les enregistrements réalisés par le salarié sur son **dictaphone personnel** à condition de le faire en sa présence ou après l'avoir dûment appelé (Cass. soc. 23-5-2012 n° 10-23.521 : RJS 8-9/12 n° 673).

Cette condition est aussi exigée, sauf risque ou événement particulier, pour le contrôle de l'armoire ou du **vestiaire** dans lequel le salarié range ses affaires personnelles (voir n° 59970). En revanche, elle ne s'impose pas pour l'ouverture d'un coffre à usage uniquement professionnel (Cass. soc. 21-10-2008 n° 07-41.513 : RJS 12/08 n° 1151).

Quant aux **sacs personnels** du salarié, l'employeur ne peut les ouvrir pour en vérifier le contenu qu'avec son accord et à la condition de l'avoir averti de son droit de s'y opposer et d'exiger la présence d'un témoin (Cass. soc. 11-2-2009 n° 07-42.068 : RJS 4/09 n° 313).

Mise en place des moyens de contrôle Les moyens de contrôle utilisés par l'employeur ne doivent pas apporter de restrictions disproportionnées aux droits et libertés des salariés (voir n° 17030). En outre, ces derniers doivent en être **informés**. A défaut, l'employeur ne saurait leur reprocher un manquement aux règles ainsi mises en place (n° 16940). Le **comité d'entreprise** (CE) doit être informé et consulté sur les moyens et les techniques permettant un contrôle de l'activité des salariés, préalablement à la décision de mise en œuvre dans l'entreprise (C. trav. art. L 2323-32).

En cas de traitement automatisé d'informations nominatives, une **déclaration** préalable doit être faite à la Cnil (voir n° 70740) et les salariés doivent pouvoir obtenir une copie des informations les concernant. A cet effet, la Cnil met en ligne des lettres types sur son site www.cnil.fr.

Ces règles doivent aussi être respectées lors de la mise en place de dispositifs d'évaluation des salariés (n° 17025).

L'institution de règles de caractère général et permanent, disciplinaire notamment, est soumise à la procédure d'établissement du règlement intérieur (n° 60105).

Précisions a. Un **audit ponctuel** visant uniquement à apprécier l'organisation d'un service ne nécessite pas la consultation préalable du CE (Cass. soc. 12-7-2010 n° 09-66.339 : RJS 10/10 n° 719).

b. S'ils sont conformes aux normes simplifiées fixées par la Cnil, les dispositifs de contrôle d'accès aux locaux, de géolocalisation des véhicules et d'écoute téléphonique peuvent faire l'objet d'une **déclaration** de conformité (voir n° 70740, a). Il en est de même des dispositifs d'alerte professionnelle (n° 56070). Dans le cas contraire ou à défaut de norme simplifiée, l'employeur doit effectuer une déclaration normale.

Sont illicites les procédés mis en œuvre sans respect des obligations d'information et de déclaration visées n° 56060. Les éléments ainsi recueillis ne peuvent donc pas servir de **preuve** des fautes commises par un salarié, voir n° 48685. Ainsi jugé pour un auto-commutateur téléphonique non déclaré à la Cnil (CA Paris 3-6-2008 n° 06-11942 : RJS 10/08

56057
N-VIII-16800 s

56060
N-VIII-300 s

56065
N-VIII-2100 s

n° 1056), un dispositif de géolocalisation utilisé à d'autres fins que celles déclarées à la Cnil et portées à la connaissance des salariés concernés (Cass. soc. 3-11-2011 n° 10-18.036 : RJS 1/12 n° 4). A aussi été jugé illicite, faute pour l'employeur d'avoir informé les salariés de la finalité du dispositif, un système de vidéosurveillance de la clientèle d'un magasin, même si les caméras étaient visibles (Cass. soc. 7-6-2006 n° 04-43.866 : RJS 11/06 n° 1143), ou de vidéosurveillance installé sur le site d'une société cliente (Cass. soc. 10-1-2012 n° 10-23.482 : RJS 3/12 n° 212). Par ailleurs, sont des procédés clandestins non valables la filature par un supérieur hiérarchique (Cass. soc. 26-11-2002 n° 00-42.401 : RJS 2/03 n° 149) ou par un détective privé (Cass. soc. 22-5-1995 n° 93-44.078 : RJS 7/95 n° 757 ; 23-11-2005 n° 03-41.401 : RJS 2/06 n° 177) et la surveillance assurée par une société chargée de contrôler l'utilisation par les salariés du distributeur de boissons de l'entreprise (Cass. soc. 15-5-2001 n° 99-42.219 : RJS 7/01 n° 830). Les **délégués du personnel** peuvent agir en justice pour obtenir le **retrait** de tels dispositifs (Cass. soc. 10-12-1997 n° 95-42.661 : RJS 1/98 n° 62). En revanche, sauf recours à un stratagème (Cass. soc. 18-3-2008 n° 06-40.852 : RJS 6/08 n° 649 ; 4-7-2012 n° 11-30.266 : RJS 10/12 n° 848), les faits relevés par l'employeur ou un salarié habilité (Cass. soc. 4-7-2012 n° 11-14.241 : RJS 10/12 n° 764), tel que le supérieur hiérarchique (Cass. soc. 26-4-2006 n° 04-43.582 : RJS 7/06 n° 800), ou par un constat d'huissier (Cass. soc. 10-10-2007 n° 05-45.898 : RJS 12/07 n° 1242), sont des modes de preuve licites, même en l'absence d'information préalable du salarié. L'employeur peut être **pénalement condamné** en cas d'atteinte à la vie privée (C. pén. art. 226-1 et 226-7) ou de violation du secret des correspondances (C. pén. art. 226-15).

Précisions Les règles visées ci-dessus ne sont applicables qu'à la collecte d'informations personnelles. Ne saurait y être assimilé le fait pour une banque de mettre en place un système d'exploitation intégrant un mode de traçage permettant d'identifier les consultants des comptes (Cass. soc. 18-7-2000 n° 98-43.485 : RJS 11/00 n° 1068). De même, l'employeur n'est pas tenu de divulguer l'existence des procédés de surveillance des locaux auxquels les salariés n'ont pas accès (Cass. soc. 31-1-2001 n° 98-44.290 : RJS 4/01 n° 405 ; 19-1-2010 n° 08-45.092 : RJS 4/10 n° 307), y compris lorsque ces procédés ont été mis en place par un client de l'entreprise (Cass. soc. 19-4-2005 n° 02-46.295 : RJS 6/05 n° 595).

56070
N-VIII-13910 s

La loi japonaise « Japanese SOX » du 6-6-2006 et la loi américaine Sarbanes-Oxley du 30-7-2002 imposent aux sociétés cotées sur leur place financière de mettre en œuvre un **dispositif d'alerte éthique** ayant pour objet d'inciter les salariés à signaler les comportements fautifs de leurs collègues ou des dirigeants de l'entreprise susceptibles de nuire à celle-ci ou d'engager sa responsabilité. D'autres le mettent en place volontairement en y associant parfois un code ou une charte éthique. Sur la nature juridique de ce dernier, voir n° 60105. La mise en œuvre d'un système d'alerte est subordonnée aux **conditions** visées n° 56060. Sur la protection du salarié relatant des faits de corruption, voir n° 16945, d.

Précisions a. Seuls peuvent bénéficier du **régime de l'autorisation unique** délivrée par la Cnil les dispositifs d'alerte dont la finalité est limitée aux domaines financier, comptable, bancaire et de lutte contre la corruption (Cass. soc. 8-12-2009 n° 08-17.191 : RJS 2/10 n° 145) ou les pratiques anticoncurrentielles au sein de l'entreprise (Délibération Cnil 369 du 14-10-2010) et qui respectent notamment les règles suivantes : caractère facultatif du dispositif ; identification de l'auteur de l'alerte ; organisation spécifique du recueil et du traitement des alertes ; information de la personne mise en cause ; droit pour cette dernière d'accéder aux données la concernant et de les rectifier (Délibération Cnil 305 du 8-12-2005). L'anonymat doit toutefois pouvoir être conservé, dans le cas de signalements particulièrement lourds ou sensibles (Circ. DGT 22 du 19-11-2008). Les autres systèmes doivent faire l'objet d'une déclaration normale, procédure plus lourde supposant une autorisation préalable de la Cnil.

b. Certains **tribunaux** estiment qu'un dispositif d'alerte n'est pas légal s'il a un **domaine trop étendu**, engendrant des risques de dénonciations calomnieuses et portant ainsi atteinte aux droits des personnes et aux libertés des salariés. Jugé qu'il en résulte dans ce cas un trouble manifestement illicite justifiant la suspension en référé du dispositif (TGI Libourne 15-9-2005 n° 05-143 : RJS 1/06 n° 4 ; TGI Caen 5-11-2009 n° 09-287 : RJS 1/10 n° 3). A en outre été jugée non opposable aux salariés la disposition d'un système d'alerte leur imposant la **consultation** du service juridique de l'entreprise avant toute communication aux autorités ou à la justice (TGI Lyon 19-9-2006 n° 06-2153 : RJS 1/07 n° 6).

B. Sanction disciplinaire

56120
C. trav. art.
L 1331-1
N-VIII-26200 s

Définition Constitue une sanction toute mesure, autre que les observations verbales, prise par l'employeur à la suite d'un **agissement** du salarié considéré par lui comme **fautif**, que cette mesure soit de nature à affecter immédiatement ou non la présence du salarié dans l'entreprise, sa fonction, sa carrière ou sa rémunération.