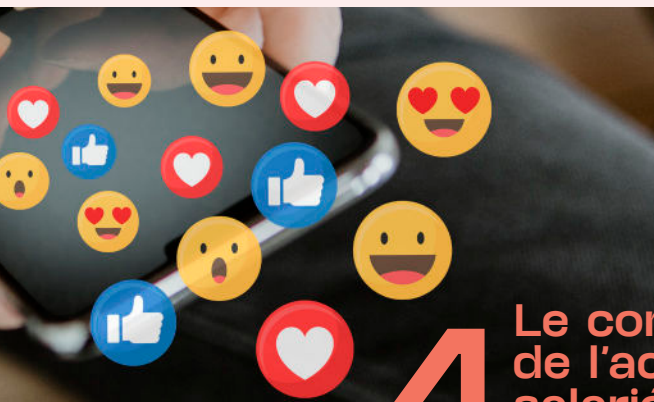


UNIVERCITÉ

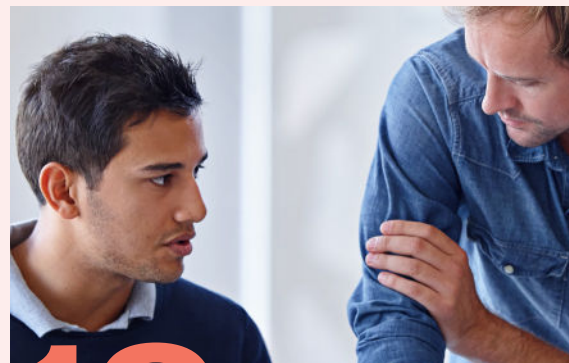
La revue juridique qui crée des ponts entre le monde académique et professionnel

La surveillance des salariés au travail

>9



4 Le contrôle de l'activité des salariés sur les réseaux sociaux



10 Les contrôles « humain »

SOMMAIRE



12 Surveillance des salariés : ce que l'employeur peut (vraiment) faire



20 Interview
Florence CALLENS
Conseillère en droit social à La Cité des Entreprises- Présidente de la section encadrement du Conseil de prud'hommes de Lille-Formatrice agréée EDS.



26 RGPD et surveillance des salariés : les règles essentielles à maîtriser

30 Veille de jurisprudence

Bernard BOSSU
Directeur du Master II Droit social à l'Université de Lille



Michaël MASCRET
Conseiller en droit social
La Cité des Entreprises

La surveillance des salariés au travail

La transformation des organisations de travail, l'essor des outils du numérique et la généralisation du travail hybride ont profondément renouvelé les pratiques de contrôle au sein des entreprises. Caméras, logiciels de traçage, analyse des connexions informatiques, géolocalisation, analyse des connexions informatiques, outils de mesure de la performance et, désormais, recours à l'intelligence artificielle : jamais les employeurs n'ont disposé d'un arsenal technologique aussi vaste pour suivre l'activité de leurs salariés.

Cette évolution ne peut toutefois ignorer un élément essentiel : l'acceptabilité de ces dispositifs par les salariés eux-mêmes. Au-delà du droit, dans un environnement managérial où l'autonomie, la responsabilisation et la confiance sont devenues des valeurs cardinales, de nombreux collaborateurs revendiquent un véritable espace de liberté dans l'accomplissement de leurs missions. Les nouvelles formes d'organisation du travail (travail en mode projet, flex-office, télétravail, horaires modulables, ...) nourrissent cette aspiration et rendent plus sensible toute modalité de contrôle perçue comme intrusive, infantilissante ou disproportionnée.

Parallèlement, les managers font face à une difficulté croissante : comment exercer leur mission de supervision dans un contexte où les attentes d'autonomie s'accroissent et où les environnements de travail se dématérialisent ? Cette tension entre autonomie revendiquée et contrôle nécessaire constitue l'un des enjeux majeurs de l'évolution contemporaine du pouvoir de direction.

La question n'est pas de savoir si un employeur peut surveiller ses salariés. Le droit positif reconnaît clairement que l'employeur peut contrôler l'activité des salariés, prérogative inhérente à son pouvoir de direction. Mais cette surveillance s'inscrit dans un équilibre délicat entre deux exigences également légitimes :

- D'un côté, le pouvoir de direction de l'employeur, qui doit pouvoir organiser, contrôler et sécuriser l'activité de l'entreprise ;
- De l'autre, la protection des droits fondamentaux des salariés, au premier rang desquels figurent le respect de la vie privée, le secret des correspondances, la liberté individuelle et la protection des données personnelles.

La véritable interrogation porte ainsi sur les limites de ce pouvoir. Car ce pouvoir n'est jamais absolu. Il est strictement encadré, notamment par le principe de proportionnalité posé à l'article L. 1121-1 du Code du travail, selon lequel « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » ainsi que par les exigences issues du RGPD et de la loi Informatique et libertés, qui imposent une gouvernance rigoureuse des données collectées.

C'est cette question que les étudiants du Master 2 Droit du travail de l'Université de Lille, dans le cadre du partenariat établi avec La Cité des Entreprises, ont choisi de traiter dans cette nouvelle édition de la revue UniverCité. En consacrant ce numéro au thème « La surveillance des salariés ».

Le contrôle de l'activité des salariés sur les réseaux sociaux



➤ **Anne JALIOSSOLTAN**
Conseiller en droit social La
Cité des Entreprises

À l'ère numérique, les frontières entre vie professionnelle et vie privée se brouillent, en particulier sur les réseaux sociaux. Facebook, X, Instagram, TikTok ou encore LinkedIn sont devenus des espaces où les salariés s'expriment, échangent et parfois critiquent leur entreprise. Cette omniprésence soulève une question centrale : **dans quelle mesure l'employeur peut-il surveiller les réseaux sociaux ?**

Le droit cherche un équilibre délicat entre le pouvoir de direction de l'employeur et les libertés individuelles du salarié.

La jurisprudence s'attelle à la tâche depuis quelques années déjà. Dans les décisions rendues récemment, les juges font preuve d'un pragmatisme certain et tiennent compte de l'évolution des moyens et des pratiques de communication.

Quels sont les enjeux juridiques liés à l'utilisation des réseaux sociaux pour les entreprises ?

Avant d'être appréhendés par l'entreprise, ces risques doivent être connus par celle-ci. Peuvent être mentionnés notamment :

Les « fuites » d'informations : la divulgation d'informations confidentielles, de secrets d'affaires, de secrets de fabrique ou encore la « fuite » du savoir-faire. En effet, des salariés peuvent échanger sur les réseaux sociaux sur des situations rencontrées dans l'exercice de leur activité professionnelle et, ce faisant, potentiellement diffuser, de manière volontaire ou involontaire, des informations sensibles ou encore un savoir-faire.

Les atteintes à l'image et à la réputation : dénigrement, diffamation, injure notamment à l'encontre de l'entreprise ou de ses dirigeants.

Espace public / espace privé sur les réseaux sociaux : une frontière déterminante mais « poreuse »

Les comptes personnels fleurissent sur les réseaux sociaux (Facebook, Instagram, Tik Tok, LinkedIn etc.). Pour vos salariés, la liberté d'expression est limitée s'ils en abusent, et par l'obligation de confidentialité qui pèse sur eux.

Apprécier le caractère public ou privé des propos tenus sur les réseaux sociaux est un exercice délicat. Il est pourtant crucial car, tenu dans un espace public, le contrôle est plus aisé et les sanctions encourues en cas d'abus plus faciles à justifier.

Les critères mis en avant par les juges sont notamment :

- Les **paramètres de confidentialité** du compte ou du groupe (ouvert à tous/limité « aux amis » /groupe fermé) ;
- Le **nombre de personnes** pouvant accéder aux publications (cercle très restreint ou large audience) ;
- L'existence d'une « **communauté d'intérêts** » (groupe fermé de quelques personnes partageant un intérêt commun) ;
- L'**intention** du salarié de rendre ou non ses propos publics (par ex, propos affichés sur l'écran de l'ordinateur de l'entreprise, visibles de toutes les personnes présentes).

Recommandations

- Identifier les enjeux généraux et spécifiques pour l'entreprise concernant l'utilisation des réseaux sociaux ;
- Assurer une veille régulière des contenus relatifs à l'entreprise publiés sur les réseaux sociaux ;
- Adopter une charte « réseaux sociaux » ou inclure des règles dans le règlement intérieur.

Exemples tirés de la jurisprudence :

1. Contrôle par l'employeur des publications publiques d'un salarié qui critique son entreprise sur Facebook ou X (compte ouvert) :

- Lorsque les propos sont diffusés sur un espace public (mur Facebook ouvert, groupe public, compte LinkedIn ou X accessible à tous), l'employeur peut en prendre connaissance sans violer la vie privée ni le secret des correspondances : il ne s'agit pas d'une « correspondance privée » mais d'une publication volontairement rendue accessible à un large public (CA Besançon, 15 nov. 2011, n° 10/02642 ; CA Rouen, 15 nov. 2011, n° 11/01830)
- Si les propos portent atteinte à l'image de l'entreprise ou à l'autorité de la hiérarchie, incitent à la rébellion ou au boycott, ou dénigrent nommément des collègues ou dirigeants, ils pourront caractériser un abus de la liberté d'expression et un manquement à l'obligation de loyauté, justifiant une sanction pouvant aller jusqu'au licenciement disciplinaire, sous réserve de proportionnalité (Cass. soc., 14 déc. 1999, n° 97-41.995 ; CA Lyon, 24 mars 2014, n° 13/03463)

2. Propos tenus sur un « espace privé » (groupe fermé Facebook, compte paramétré en privé, messagerie) et utilisation par l'employeur comme preuve pour sanctionner :

- La Cour de cassation a jugé que des propos injurieux diffusés dans un groupe Facebook fermé de 14 personnes restaient d'ordre privé ; l'employeur ne pouvait pas les utiliser pour justifier un licenciement disciplinaire faute de caractère public (Cass. soc., 12 sept. 2018, n° 16-11.690)
- De même, des propos tenus sur un profil privé accessible à un nombre très restreint de contacts ne constituent pas des injures publiques (Cass. 1re civ., 10 avr. 2013, n° 11-19.530)

Toutefois, la jurisprudence a évolué sur la question de la preuve : la production en justice d'éléments extraits d'un compte privé porte atteinte à la vie privée, mais cette atteinte peut être justifiée par le « droit à la preuve » si trois conditions cumulatives sont réunies :

- la production est indispensable à l'exercice de ce droit,
- elle vise à démontrer un manquement du salarié à ses obligations contractuelles,
- et l'atteinte est strictement proportionnée au but poursuivi (**Cass. 30 sept. 2020, n° 19-12.058 Cass. Ass. plén., 22 déc. 2023, n° 20-20.648**)

Ainsi, ont été admises comme preuves :

- des échanges Facebook privés entre un éducateur et un résident handicapé, révélant un comportement potentiellement maltraitant, compte tenu de l'intérêt légitime de l'employeur à protéger les personnes vulnérables (CA Poitiers, 4 mai 2016, n°15/04170)
- la photo d'une collection de vêtements inédite publiée sur un mur privé, démontrant la violation d'une obligation de confidentialité (Cass. soc., 30 sept. 2020, n° 19-12.058)
- Dans deux arrêts du 4 octobre 2023, des photos en maillot de bain prises sur le lieu et le temps de travail, diffusées dans un groupe privé Messenger, ont pu être produites pour justifier un licenciement, la protection des patients rendant l'atteinte à la vie privée proportionnée (Cass. soc., 4 oct. 2023, n° 21-25.452 et n° 22-18.217)
- En revanche, un licenciement disciplinaire ne peut être fondé sur une conversation strictement privée par messagerie personnelle lorsqu'aucun manquement aux obligations professionnelles n'est caractérisé (Cass. ass. plén., 22 déc. 2023, n°21-11.330)



3. Publication par un salarié, sur LinkedIn ou Facebook, de contenus confidentiels (photos de produits non encore lancés, documents internes, procédés techniques) :

- La jurisprudence a ainsi validé le licenciement pour faute grave d'un salarié ayant publié sur son Facebook privé une photographie d'un défilé de collection de vêtements non encore commercialisée : cette publication violait son obligation contractuelle de confidentialité, d'autant que plusieurs « amis » étaient liés à des sociétés concurrentes, ce qui exposait l'entreprise à un risque concurrentiel (Cass. soc., 30 sept. 2020, n° 19-12.058)
- La cour d'appel de Paris a jugé licite le licenciement d'un responsable R&D ayant publié sur LinkedIn des images de coupes et géométries d'un moteur, issues d'un poster interne, alors que son contrat et le règlement intérieur lui imposaient une stricte discrétion, notamment pour des raisons de défense nationale (CA Paris, 23 févr. 2022, n° 19/07192)

Dans ces cas, l'employeur n'a pas besoin d'un dispositif spécifique de surveillance : il peut constater les publications publiques ou librement accessibles et les produire en justice comme preuves licites, sans violer la vie privée.



CE QU'IL FAUT RETENIR :

L'employeur peut contrôler, dans certaines limites, l'activité des salariés sur les réseaux sociaux, mais ce contrôle est fortement encadré :

Surveiller des contenus publics : OUI

Les informations rendues publiques sur Internet (publications ouvertes, commentaires visibles, profils professionnels) sont accessibles à tout internaute.

Dans ce cas, **l'employeur peut lire ces contenus**, et ils pourront éventuellement servir de preuve en cas de procédure disciplinaire.

Accéder à un compte privé sans autorisation : NON

L'employeur n'a pas le droit :

- de contourner les paramètres de confidentialité,
- d'exiger les mots de passe d'un salarié,
- de se connecter en usurpant une identité,
- d'utiliser un collègue pour espionner volontairement le salarié.

Toute collecte intrusive serait considérée comme une atteinte à la vie privée et rendrait la preuve irrecevable.

Les contrôles « humain »

Par Michaël MASCLET



”Quand la surveillance la plus simple devient la plus difficile”

Lorsqu'on évoque la surveillance des salariés, l'imaginaire collectif se tourne immédiatement vers les outils technologiques : caméras, logiciels de suivi d'activité, géolocalisation, analyse des connexions... Pourtant, le premier mode de contrôle, le plus ancien et le plus répandu, reste celui exercé directement par le manager ou par un service interne de supervision.

Une surveillance si « naturelle » qu'elle en devient presque invisible.

Un contrôle licite tant qu'il reste humain avec une vraie limite : le courage managérial

Ce type de supervision n'a, en principe, rien d'illicite. Il ne nécessite ni information préalable du salarié, ni consultation du CSE, dès lors qu'il ne se transforme pas en dispositif technique dissimulé.

Ainsi, la présence physique du supérieur hiérarchique, l'examen d'une tâche en cours, le contrôle de l'état d'un poste ou l'observation d'un comportement relèvent naturellement de l'organisation du travail. Ils n'entrent dans aucun des régimes juridiques complexes applicables aux outils technologiques de surveillance. Il relève du pouvoir de direction de l'employeur, lequel comprend la faculté d'organiser le travail, d'en vérifier l'exécution et de sanctionner les manquements.

La première limite de ce mode de contrôle n'est ni juridique ni technologique : elle est humaine.

De nombreux managers de proximité hésitent aujourd'hui à exercer pleinement leur rôle de supervision. Plusieurs facteurs expliquent cette retenue :

- La crainte du conflit ou de la contestation ;
- La peur d'être accusés d'harcèlement ou de discrimination ;
- Un sentiment de légitimité affaibli lorsqu'il s'agit d'exprimer un feedback négatif ;
- La peur de ne pas être soutenus si le climat social ou émotionnel de l'équipe se dégrade.

Résultat : le contrôle direct, pourtant le plus simple en théorie, devient le plus complexe à exercer. Les observations informelles s'estompent, laissant place soit à un laisser-faire, soit à une sur-formalisation des échanges, soit encore à l'introduction de dispositifs de surveillance parfois disproportionnés, tels que la géolocalisation.

La conséquence : deux dérives majeures pour l'entreprise

Pour le collectif : la dérive normative

Lorsque les managers ne s'autorisent plus à gérer les situations individuellement, l'entreprise compense par des réponses globales :

- Multiplication des procédures,
- Inflation de règles internes,
- Empilement des circuits de validation.

En somme, faute d'oser cibler les véritables situations individuelles, on légifère pour tout le monde.

Pour les collaborateurs qui dérivent : l'escalade

Lorsqu'un collaborateur dérive sans qu'aucune remarque n'intervienne :

- Les signaux faibles ne sont pas détectés ;
- Les écarts deviennent des habitudes ;
- Les habitudes se transforment en dysfonctionnements structurels.

L'entreprise finit alors par agir... mais trop tard. Les directions des ressources humaines se retrouvent face à des situations anciennes, non documentées, et à des managers épuisés mais déterminés. À ce stade, la logique n'est plus préventive mais corrective : mise en œuvre du pouvoir disciplinaire, retrait de responsabilités, voire rupture du contrat. Faute de recadrages antérieurs traçables et d'une gradation effective des mesures, le salarié est susceptible de percevoir ces décisions comme brutales ou disproportionnées. Le risque contentieux s'en trouve accru, notamment sur la proportionnalité de la sanction et, le cas échéant, sur la cause réelle et sérieuse de la rupture.

Surveillance des salariés :

Ce que l'employeur peut (vraiment) faire

Par Manon BROGNIARD, Aylan BOUSTA, Jeanne DELBE, Alexandre DUBOIS, Camille LAURENT, Julia LELEU, Célia LOISEL



À l'ère du télétravail et du développement du numérique, la surveillance des salariés connaît un essor inédit. Logiciels de suivi d'activité, dispositifs de géolocalisation, reconnaissance faciale ou analyse de données : les moyens techniques de contrôle se multiplient et renforcent le pouvoir de l'employeur.

Pourtant, si le lien de subordination lui confère des prérogatives de direction, de contrôle et de sanction à l'égard du salarié, celles-ci ne sont pas sans limites. Le salarié bénéficie, même au temps et au lieu de travail, du droit au respect de sa vie privée, protégé par les textes

nationaux et internationaux (Art. 8 CEDH, Art. 9 Code civil, Art. 12 DUDH).

Encadrée par l'article L1121-1 du Code du travail, la surveillance doit ainsi être nécessaire, justifiée, et proportionnée, sous peine de basculer dans un contrôle excessif portant atteinte aux droits et libertés des salariés et favorisant une gestion déshumanisée des ressources humaines, source d'anxiété et de désengagement au travail.

L'enjeu réside alors dans la recherche d'un équilibre entre pouvoir de contrôle et protection des droits et libertés du salarié.

L'employeur peut-il contrôler le temps de travail des salariés ?

En vertu des articles L. 3171-1 et suivants du Code du travail, l'employeur doit comptabiliser les heures de travail des salariés selon le régime appliqué afin d'assurer et protéger la santé des salariés en s'assurant du respect des durées maximales de travail et des temps de repos des salariés.

La **directive 2003/88/CE du 4 novembre 2003** encadre, au niveau européen, l'aménagement du temps de travail. Toutefois, **l'obligation pour les États membres d'imposer aux employeurs un système objectif, fiable et accessible permettant de mesurer la durée du travail journalier** ne résulte pas directement du texte de la directive. Elle découle de l'interprétation qu'en a donnée la **Cour de justice de l'Union européenne**, dans son arrêt du **14 mai 2019 (aff. C-55/18, CCOO)**.

S'inscrivant dans cette logique, la **Cour de cassation**, dans un arrêt du **5 juillet 2023 (Cass. soc., 5 juill. 2023, n° 21-24.122, FS-B)**, a jugé que l'absence d'un système fiable et objectif de contrôle du temps de travail est susceptible de constituer un manquement de l'employeur à son obligation de sécurité. Les outils permettant ce suivi du temps de travail peuvent prendre diverses formes (document papier contresigné, document Excel, logiciel, badgeuse, etc). Il est toutefois indispensable de s'assurer que l'outil retenu permette un contrôle effectif du temps de travail. Enfin, tout dispositif de contrôle du temps de travail doit faire l'objet d'une **information des salariés**, ainsi que d'une **information-consultation du CSE** lorsqu'il existe.

L'employeur peut-il géolocaliser les salariés ?

La géolocalisation est une technologie qui permet de connaître en temps réel la position d'un véhicule ou d'un appareil connecté. En pratique, certains employeurs l'utilisent pour suivre les déplacements de salariés travaillant à l'extérieur, comme des chauffeurs, techniciens ou livreurs.

En France, la géolocalisation est autorisée, mais elle est strictement encadrée.

Selon la CNIL, elle ne peut être mise en place que pour des finalités précises :

- Assurer la sécurité du salarié,
- organiser des interventions urgentes,
- facturer une prestation,
- ou encore suivre le temps de travail mais uniquement lorsqu'aucun autre moyen n'est possible.



L'employeur doit également respecter plusieurs obligations. Il doit informer individuellement les salariés, **préciser la finalité du dispositif**, la durée de conservation des données et consulter le CSE avant sa mise en place. La Cour de cassation, le 14 février 2024, a rappelé qu'un système de géolocalisation ne peut pas être utilisé pour d'autres objectifs que ceux annoncés aux salariés.

Il existe aussi des limites à l'usage de la géolocalisation des salariés. En particulier :

- La géolocalisation est interdite en dehors du temps de travail, notamment pendant les pauses ou les trajets domicile-travail, ces périodes relevant de sa vie personnelle.
- Elle ne peut pas non plus être utilisée pour contrôler des salariés qui disposent d'une autonomie dans l'organisation de leur temps de travail, comme l'a jugé la Cour de cassation le 19 décembre 2018 (Cass. soc., 19 décembre 2018, n° 17-14.631).

Enfin, l'utilisation illicite de la géolocalisation a été jugée comme constituant un manquement suffisamment grave justifiant la prise d'acte de la rupture du contrat de travail aux torts de l'employeur.

L'employeur peut-il enregistrer les conversations ? – Droit à la preuve

Le Code pénal sanctionne le fait d'enregistrer des paroles prononcées à titre privé sans consentement. Ainsi, un employeur ne peut enregistrer un salarié à son insu sans porter atteinte à sa vie privée.

La Cour de cassation, le 10 janvier 2012, a rappelé que la surveillance ne doit pas se faire par un procédé clandestin, à l'insu des salariés. De même, l'employeur ne peut pas mettre en place des stratagèmes pour piéger un salarié, tels que l'utilisation de faux clients pour provoquer une faute. Cependant, un dispositif de « client mystère » peut être autorisé lorsqu'il s'agit d'une méthode d'évaluation connue des salariés.

Toutefois, la situation a évolué avec la reconnaissance du droit à la preuve. Dans une décision du 22 décembre 2023, la Cour de cassation a considéré que le caractère illicite ou déloyal d'une preuve ne conduit pas automatiquement à son rejet par le juge. Le juge doit désormais vérifier :

- si la preuve est indispensable pour exercer un droit
- et si l'atteinte à la vie privée est proportionnée au but recherché.

Cette position a été confirmée par la chambre sociale le 10 juillet 2024, dans une affaire relative concernant la preuve d'un harcèlement moral.

Dans la même logique, l'employeur peut produire une photographie issue d'un compte Facebook privé, même obtenue sans autorisation et attentatoire à la vie privée, dès lors que cette preuve est indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi.

L'employeur a-t-il le droit d'utiliser la vidéosurveillance pour sanctionner les salariés ? (CNIL)

L'employeur ne peut pas détourner la finalité d'un système de vidéosurveillance. Selon la Cour de cassation, le 6 décembre 2023, si un employeur installe des caméras pour assurer la sécurité des biens et des personnes, il n'a pas le droit de s'en servir pour contrôler l'activité professionnelle du salarié.

Ainsi une caméra de sécurité ne peut pas servir à vérifier le respect des horaires, la durée des pauses ou la qualité du travail.

Cependant, la vidéosurveillance peut devenir un mode de preuve recevable lorsque les faits reprochés relèvent précisément de la finalité de sécurité pour laquelle le dispositif a été installé. C'est notamment le cas pour la tenue de caisse : les enregistrements focalisés sur une caisse pour vérifier des mouvements d'argent sont parfaitement utilisables pour prouver un vol ou une erreur de caisse répétée.

Pour que l'employeur puisse sanctionner, son dispositif doit respecter la loi « Informatique et Libertés » du 6 janvier 1978, aujourd'hui complétée par le RGPD.

La CNIL veille notamment au principe de proportionnalité : la sécurité ne doit jamais justifier une surveillance permanente ou intrusive des salariés. Elle vérifie notamment si les caméras ne filment pas les écrans d'ordinateur ou les zones de repos ou les vestiaires.



L'employeur peut-il procéder au contrôle des biens du salarié ?

Le contrôle par l'employeur des biens utilisés par le salarié dépend de la finalité du bien mis à disposition : usage partiellement personnel ou usage strictement professionnel.

Les biens mis à disposition à usage partiellement personnel.

Sont concernés notamment :

- les armoires individuelles,
- les véhicules de fonction laissés aux salariés dans leur vie personnelle,
- les téléphones.
- Dans ces situations, le respect de la vie privée impose à l'employeur de respecter les conditions du règlement intérieur et de procéder au contrôle en présence du salarié (sauf risque ou événement particulier).



Les biens mis à disposition à usage exclusivement professionnel relèvent de cette catégorie :

- les courriels professionnels envoyés ou reçus via l'outil informatique fourni par l'employeur,
- les connexions Internet effectuées depuis le poste de travail,
- les SMS envoyés ou reçus sur un téléphone professionnel.

Pour ces biens, l'employeur est en droit de procéder à un contrôle **hors la présence du salarié**, dès lors que l'usage est strictement professionnel.

La Cour de cassation admet 2 limites à ce pouvoir de contrôle. D'une part, si l'employeur peut ouvrir un bien professionnel, il ne peut utiliser son contenu contre le salarié que s'il est d'ordre professionnel, les éléments extra professionnels restant protégés. D'autre part, tout fichier ou message explicitement identifié comme "personnel" par le salarié ne peut être ouvert qu'en présence de ce dernier ou après l'avoir dûment appelé, hormis en cas de risque exceptionnel.

L'employeur peut-il contrôler un salarié en télétravail ?

Le télétravail n'est qu'un mode d'organisation du contrat de travail, de sorte que l'employeur conserve à l'égard des télétravailleurs son pouvoir de direction, de contrôle et de sanction.

Dès lors, il en découle la possibilité pour celui-ci de contrôler l'activité des salariés par le biais d'un système auto-déclaratif, par l'intermédiaire d'un logiciel de suivi du temps de travail rempli par le salarié ou d'un logiciel informatif de badgeage. Toutefois, l'employeur doit informer les salariés et consulter le CSE avant tout dispositif de contrôle, respecter le principe de proportionnalité et garantir la protection des données personnelles, notamment en télétravail.

L'employeur peut-il procéder à des tests de dépistage (alcool / drogue) sur le lieu de travail ?

Le contrôle de la consommation d'alcool et de stupéfiants sur le lieu de travail relève du pouvoir de direction et de l'obligation de sécurité de l'employeur.

En matière d'alcool, l'article R.4428-20 du Code du travail autorise la présence et la consommation de vin, de bière, de cidre et de poiré sur le lieu de travail. Toutefois, depuis 2014, l'employeur est autorisé à édicter dans le règlement intérieur des dispositions plus restrictives concernant la présence et la consommation d'alcool au sein de l'entreprise pour assurer la protection de la santé et de la sécurité des travailleurs. De plus, L'employeur doit empêcher l'accès ou le maintien dans l'entreprise d'une personne en état d'ivresse, sous peine d'engager sa responsabilité.

S'agissant des stupéfiants, leur usage et leur détention sont prohibés par le Code pénal et le Code de la santé publique. L'employeur peut donc prévenir et faire cesser toute consommation créant un risque pour la santé ou la sécurité des biens et des personnes.

Toutefois, les dépistages, alcool ou drogue, constituent une atteinte aux libertés : ils ne sont licites que s'ils sont justifiés par la nature des tâches et proportionnés au but recherché ainsi que s'ils sont prévus par le règlement intérieur (CE, 1er février 1980, n°06361). Un dépistage généralisé et aléatoire est donc illicite (CE, 12 novembre 2012, n°349365). En ce sens, le règlement intérieur doit prévoir des tests ciblés sur des postes à risque, avec des garanties : information du salarié sur la possibilité de contestation et respect de la vie privée.

La jurisprudence admet que certains tests de dépistage, comme le test salivaire ou l'alcootest, puissent être réalisés par l'employeur, sans intervention du médecin du travail, dès lors que les garanties stipulées par le règlement intérieur sont respectées (Cass. Soc., 31 mars 2015, n°13-25.436). Un dépistage positif peut fonder une sanction disciplinaire pouvant aller jusqu'au licenciement pour faute grave, notamment en cas d'ébriété sur le lieu de travail ou de mise en danger d'autrui (Cass. Soc., 24 janvier 1991, n°88-45.022).

” L'employeur doit informer les salariés et consulter le CSE avant tout dispositif de contrôle. ”



Dans quelle mesure l'employeur peut-il contrôler le salarié en arrêt de travail ?

Le contrôle des arrêts de travail par l'employeur est strictement encadré. S'il ne peut contester la prescription médicale de l'arrêt, sauf fraude, il peut en revanche vérifier sa réalité. (Article L1226-1 et R1226-10 du Code du Travail). Ce pouvoir de contrôle doit toutefois respecter la vie privée du salarié et l'interdiction des discriminations fondées sur l'état de santé : seules des vérifications nécessaires et proportionnées sont admises, sans ingérence de l'employeur dans la vie personnelle du salarié.

Ainsi, l'employeur peut diligenter une contre-visite médicale en contrepartie du versement d'indemnités complémentaires. Cette contre-visite est réalisée par un médecin mandaté, au domicile du salarié ou sur convocation. Le salarié doit s'y soumettre et permettre le contrôle, notamment en indiquant son lieu de repos. À l'issue de l'examen, le médecin informe l'employeur du caractère justifié ou non de l'arrêt, ou de l'impossibilité de contrôler le salarié. Si l'arrêt est jugé injustifié ou si le contrôle est rendu impossible, l'employeur peut suspendre le complément de salaire. En revanche, les conclusions du médecin-contrôleur ne peuvent fonder une sanction disciplinaire ou un licenciement, ni remettre en cause le suivi des prescriptions médicales du médecin traitant.

Enfin, le non-respect des obligations envers la sécurité sociale (horaires de sortie) ne constitue pas en soi une faute disciplinaire. De même, le salarié peut continuer à suivre les prescriptions de son médecin traitant sans commettre de faute, même en cas d'avis contraire du médecin mandaté.

Quelle est la place des institutions représentatives du personnel dans le contrôle des salariés ?

Le caractère par nature collectif des dispositifs de contrôle des salariés ne peut que rendre légitime la consultation des représentants de ces salariés préalablement à la mise en œuvre de ces dispositifs. Ainsi, la consultation du CSE doit avoir lieu préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. Pour la Cour de cassation, le 11 décembre 2019, un outil technique constitue un moyen de contrôle dès lors que le but premier n'est pas de surveiller les salariés, mais que les fonctionnalités conduisent accessoirement à une telle surveillance.

Le périmètre des moyens de contrôle n'est pas illimité : mener un simple audit visant à apprécier, à un moment donné, l'organisation d'un service, n'entraîne pas l'obligation de consulter le CSE. Ainsi, si le contrôle accessoire exige une consultation, il n'en va pas de même du contrôle ponctuel.

Enfin, l'usage de l'intelligence artificielle à des fins de contrôle pourrait imposer une double consultation du CSE : au titre de la modification des conditions de travail et des moyens de surveillance.



Quelles sanctions encourt l'employeur qui recourt à une surveillance excessive des salariés ?

Sur le plan pénal, l'atteinte à la vie privée peut entraîner :

- jusqu'à un an d'emprisonnement,
- 45 000 € d'amende

À cela s'ajoutent les amendes de la CNIL pouvant atteindre 10 millions d'€ ou 2% du chiffre d'affaires annuel mondial de l'entreprise.

Sur le plan civil, l'employeur s'expose au paiement de dommages-intérêts et au risque de voir ses preuves rejetées par les tribunaux.

Enfin, un risque majeur d'atteinte à l'image de l'entreprise notamment par la médiatisation des sanctions par la CNIL, peut nuire durablement à l'attractivité et à la confiance de l'entreprise.

➤ CONCLUSION

L'examen des différents dispositifs de surveillance, qu'il s'agisse du contrôle du temps de travail, de la géolocalisation, de l'enregistrement de données ou de conversations, de la vidéosurveillance, du contrôle des outils professionnels, du télétravail ou encore des tests de dépistage et des arrêts de travail, révèle une constante : aucun mode de contrôle n'échappe aux exigences de nécessité, de justification et de proportionnalité.

Derrière la diversité des situations abordées se dessine une même ligne directrice, imposée tant par le législateur que par le juge et la CNIL : le pouvoir de surveillance de l'employeur ne trouve sa légitimité que s'il est encadré, transparent et respectueux des droits fondamentaux du salarié. La multiplication des outils numériques et le recours croissant aux technologies de contrôle renforcent ainsi l'exigence d'une gouvernance juridique rigoureuse, sous peine de voir la surveillance basculer en une source de contentieux, de sanctions et de rupture de la relation de confiance au sein de l'entreprise.



Florence CALLENS

Conseillère en droit social à La Cité des Entreprises -
Présidente de la section encadrement du Conseil de
prud'hommes de Lille-Formatrice agréée EDS.

INTERVIEW

Dans un environnement où les outils numériques, les dispositifs de contrôle et les exigences de cybersécurité se sont profondément ancrés dans le fonctionnement des entreprises, les directions des ressources humaines et les juristes en droit social recourent de plus en plus fréquemment à ces dispositifs comme moyens de preuve dans le cadre des procédures de licenciement. **Mais dès qu'un contentieux apparaît, une question demeure centrale : ces preuves sont-elles licites et recevables devant le conseil de prud'hommes ?** L'équilibre entre droit à la preuve de l'employeur, respect des libertés individuelles du salarié et exigences de loyauté demeure, plus que jamais, au cœur des débats.

Parallèlement, la jurisprudence ne cesse de redessiner les contours du droit de la preuve en droit du travail. Ainsi, une preuve, même obtenue ou produite de manière illicite (violation d'un droit ou d'une règle) ou déloyale (stratagème, dispositif clandestin), **n'est plus automatiquement écartée**. L'année 2026 marque également une étape importante avec la publication, au Journal officiel du 25 février 2026, de la loi consacrant la confidentialité des consultations juridiques des juristes d'entreprise, un texte très attendu qui vient renforcer la sécurité juridique dans la gestion des dossiers sensibles.

Pour éclairer ces évolutions et offrir des repères pratiques aux DRH, responsables RH, juristes, UniverCité donne la parole à Florence CALLENS-HALLOT, Conseillère en droit social à La Cité des Entreprises, Présidente de la section encadrement du Conseil de prud'hommes de Lille, et formatrice agréée EDS. **À travers son double regard de praticienne et de juge prud'homale, elle nous livre les clés d'une gestion maîtrisée de la preuve : depuis la constitution du dossier en amont du licenciement jusqu'à la production des éléments devant le juge.**

UniverCité - **Dans votre pratique, quels sont aujourd'hui les contextes les plus fréquents dans lesquels les employeurs recourent à des éléments de preuve numérique dans le cadre de dossiers disciplinaires ou de licenciement ?**

FC - Aujourd'hui, devant les conseils de prud'hommes, la preuve numérique est devenue omniprésente, et elle est mobilisée aussi bien par les employeurs que par les salariés.

Très concrètement, les premiers éléments produits sont souvent issus des outils de travail : un courriel envoyé trop rapidement, une extraction de logiciel métier, un historique de connexion ou de modification de fichiers. Ces éléments peuvent servir à caractériser une faute, mais aussi, côté salarié, à démontrer qu'il exécutait simplement ses missions dans le cadre des consignes reçues.

Un autre terrain particulièrement fréquent concerne le temps de travail et le télétravail. Connexions VPN très matinales, badge jamais utilisé, messagerie active tard le soir : l'employeur peut y voir le signe d'une fraude ou d'un manquement, quand le salarié s'en sert pour établir qu'il travaillait bien au-delà de ce qui était déclaré ou reconnu.

Enfin, les questions comportementales et de loyauté occupent une place croissante. Publications sur les réseaux sociaux, photos prises sur le lieu de travail, images de vidéosurveillance ou données de géolocalisation peuvent, selon les cas, faire basculer un dossier dans un sens ou dans l'autre, y compris pendant un arrêt de travail.

Le numérique est devenu le témoin silencieux de la vie professionnelle. Il ne crée pas les conflits, mais il en conserve les traces. Et ces traces sont désormais au cœur de la décision prud'homale.

UniverCité - **Lorsque l'on évoque une preuve illicite ou déloyale en entreprise, à quoi cela correspond-il concrètement ? Pouvez-vous en donner des exemples parlants pour les praticiens RH ?**

La preuve illicite ou déloyale est parfois perçue comme un concept très théorique. Dans les faits, elle renvoie à des situations extrêmement concrètes, que les RH et les managers rencontrent régulièrement.

Une preuve est dite illicite lorsqu'elle est obtenue en violation d'une règle légale : droit du travail, droit pénal, ou réglementation relative à la protection des données personnelles. Elle est déloyale lorsqu'elle repose sur un procédé dissimulé ou trompeur, c'est-à-dire lorsque le salarié n'a pas été informé d'un dispositif dont il aurait dû avoir connaissance.

” **Le numérique est devenu le témoin silencieux de la vie professionnelle.** ”

Sur le terrain, les exemples sont bien connus. Une caméra de vidéosurveillance installée officiellement pour des raisons de sécurité, mais ensuite utilisée à des fins disciplinaires sans que cette finalité ait été annoncée. Un entretien enregistré à l'insu de l'autre partie, souvent par précaution ou défiance. Un outil de géolocalisation déclaré pour la protection des véhicules, mais exploité pour contrôler les déplacements ou le temps de travail.

Autre situation fréquente : la récupération de captures issues de réseaux sociaux privés par l'intermédiaire d'un collègue, en dehors de tout cadre transparent.

Mais l'un des angles morts les plus sensibles reste le secret des correspondances. Lorsqu'un employeur prend connaissance, de manière frauduleuse, d'un courrier personnel destiné à un salarié, il ne s'expose pas seulement à l'écartement de la preuve : il encourt une sanction pénale pour violation du secret des correspondances.

Cette protection concerne pleinement les échanges électroniques. Les courriels issus de la messagerie personnelle du salarié sont protégés, même lorsqu'ils sont consultés depuis un ordinateur professionnel. L'employeur ne peut ni les ouvrir, ni les exploiter, ni les produire en justice.

”La preuve n'est jamais neutre.”

La même logique s'applique aux messages provenant d'une messagerie personnelle installée sur un téléphone professionnel. Et point essentiel pour les praticiens RH : même l'interdiction d'usage personnel des outils, prévue par le règlement intérieur, ne permet pas de contourner cette protection. Le caractère personnel de la correspondance prime.

Dans la majorité des cas, il ne s'agit pas d'une fraude consciente, mais d'une mauvaise appréciation des règles, souvent dans un contexte de tension ou d'urgence. Le paradoxe, c'est que la preuve que l'on pense décisive devient parfois la plus dangereuse.

D'où une question essentielle à se poser systématiquement : non seulement *que prouve cette pièce ?*, mais surtout *comment a-t-elle été obtenue ?*



UniverCité – **Sur quels critères les conseillers prud'hommes fondent-ils désormais leur analyse pour déterminer si une preuve collectée de manière irrégulière peut être recevable ?**

FC – Pendant longtemps, une preuve illicite ou déloyale était écartée presque mécaniquement. La jurisprudence a évolué, et cette évolution est aujourd'hui bien intégrée par les conseillers prud'hommes. Elle ne constitue toutefois en aucun cas un blanc-seing.

Le premier critère demeure le caractère indispensable de la preuve. La question centrale est toujours la même : était-il possible d'établir les faits par d'autres moyens licites ? Si la réponse est positive, la preuve irrégulière n'a, en principe, pas vocation à être retenue. Le rejet reste la règle, l'admission demeure l'exception.

Le deuxième critère tient à la gravité des faits reprochés. On ne peut pas tout justifier au nom du droit à la preuve. Une atteinte à la vie privée, aux données personnelles ou au secret des

échanges ne peut être envisagée que si les faits présentent une gravité suffisante : harcèlement, discrimination, violences, atteintes significatives à l'entreprise.

Enfin, les juges examinent la proportionnalité de l'atteinte portée aux droits et libertés du salarié au regard de l'objectif poursuivi. Il s'agit d'un contrôle très concret, au cas par cas. Une intrusion importante dans la sphère personnelle pour un manquement mineur sera systématiquement écartée.

Le message adressé aux praticiens est clair : recourir à une preuve irrégulière revient toujours à franchir une ligne. Cela peut être admis à titre tout à fait exceptionnel, mais jamais par réflexe.

UniverCité – **Le principe de proportionnalité joue désormais un rôle déterminant. Comment est-il mis en œuvre, très concrètement, dans l'examen d'une affaire prud'homale ?**

FC – La proportionnalité est aujourd'hui la clef de voûte du raisonnement judiciaire. Une preuve ne tombe plus automatiquement parce qu'elle est irrégulière, mais elle n'est admise qu'après un examen approfondi.

Très concrètement, le juge procède à un raisonnement en équilibre. Il examine d'abord la gravité des faits reprochés. On n'analyse pas une preuve de la même manière selon qu'il s'agit de simples retards, d'une insuffisance professionnelle, ou de faits graves tels que harcèlement, violences, discrimination ou détournement.

Ensuite, il apprécie l'ampleur de l'atteinte aux droits fondamentaux du salarié : vie privée, données personnelles, secret des correspondances, loyauté des procédés. Une intrusion importante dans la sphère intime sera très difficile à justifier pour un manquement de faible gravité.

Troisième élément décisif : le caractère indispensable de la preuve. Le juge se demande si l'employeur pouvait raisonnablement agir autrement. Une enquête interne, des témoignages ou des échanges écrits auraient-ils permis d'établir les faits ?

Ce n'est que lorsque la preuve est à la fois indispensable et que l'atteinte aux droits est strictement proportionnée à l'objectif poursuivi qu'une admission peut être envisagée.

Pour les praticiens RH, ce changement de logique est fondamental. Il impose anticipation, mesure et traçabilité. Une preuve recueillie dans l'urgence, sans réflexion sur sa proportionnalité, peut rapidement se retourner contre l'employeur.

En pratique, le message est clair : la preuve n'est jamais neutre. Elle doit être pensée non seulement en fonction de ce qu'elle démontre, mais aussi de la manière dont elle a été obtenue, et du prix juridique qu'elle fait payer aux droits fondamentaux.

UniverCité – Dans quelles situations les conseillers prud’hommes peuvent-ils considérer qu’une preuve illicite reste indispensable et donc potentiellement recevable malgré son irrégularité ?

Ces situations existent, mais elles restent rares.

On peut penser, par exemple, à une vidéo non déclarée constituant l’unique moyen de prouver un vol ou une agression, à un enregistrement réalisé dans un contexte de faits particulièrement graves, ou encore à des données de géolocalisation irrégulières révélant une utilisation dangereuse ou frauduleuse d’un véhicule.

Dans ces hypothèses, l’exigence de vérité peut l’emporter, mais toujours avec une grande prudence. Il ne s’agit jamais d’une validation de principe, et encore moins d’un précédent généralisable.

UniverCité – Enfin, au-delà de la gestion des preuves, quels sont selon vous les fondamentaux pour constituer, en amont du licenciement, un dossier solide, loyal et juridiquement sécurisé ?

Un bon dossier ne se rattrape pas à la fin. Il se construit en amont, avec méthode.

Premier pilier : informer et tracer.
Charte informatique, informations sur les dispositifs numériques, documents RGPD : un outil connu et expliqué est un outil exploitable.

Deuxième pilier : vérifier la conformité avant d’agir.
Avant d’utiliser une vidéosurveillance ou un outil de géolocalisation, les finalités doivent être claires et respectées. Sinon, la preuve est déjà fragilisée.

Troisième pilier : privilégier la preuve licite tant qu’elle existe.
Entretiens, alertes, écrits professionnels, témoignages : les dossiers les plus solides reposent d’abord sur du factuel humain, pas sur de la technologie intrusive.

Quatrième pilier : respecter le contradictoire, dès l’interne.
Un salarié qui a pu répondre aux reproches, c’est un dossier qui tient beaucoup mieux devant le juge.

Enfin, dernier point souvent sous-estimé : la cohérence globale.
Délais, proportion des sanctions, pratiques homogènes : tout se regarde, et tout se compare.

Un dossier disciplinaire ou de licenciement n’est jamais une simple pile de preuves. C’est un enchaînement de décisions. Et la moindre rupture de loyauté, même tardive, peut faire tomber l’ensemble.

” Un dossier disciplinaire ou de licenciement n’est jamais une simple pile de preuves. C’est un enchaînement de décisions. Et la moindre rupture de loyauté, même tardive, peut faire tomber l’ensemble. ”



RGPD et surveillance des salariés : les règles essentielles à maîtriser



► **Thomas LAUDE**
Conseiller en droit des affaires – La Cité des Entreprises

► **Entre exigences de sécurité, impératifs organisationnels et respect des libertés individuelles, la surveillance des salariés place l'employeur sur une ligne de crête juridique particulièrement exposée. Si la sécurisation des personnes, des biens et des systèmes d'information conduit de plus en plus d'entreprises à recourir à des dispositifs de surveillance, ces mécanismes ne peuvent être envisagés qu'au prix d'un raisonnement juridique rigoureux.**

Encadrés à la fois par le règlement général sur la protection des données entré en application le 25 mai 2018 (RGPD), le droit du travail et la doctrine constante de la Commission nationale de l'informatique et des libertés (CNIL), ces dispositifs ne constituent jamais un outil de gestion ordinaire. Leur mise en œuvre suppose, au contraire, une vigilance accrue de la part des directions des ressources humaines et des directions juridiques, tant au stade de la conception que dans leur exploitation quotidienne.

Les grands principes du RGPD appliqués à la surveillance

Le RGPD repose sur un socle de principes structurants, au premier rang desquels figurent la finalité, la minimisation des données et la proportionnalité. Appliqués aux dispositifs de surveillance, ces principes imposent à l'employeur de démontrer, de manière précise et documentée, la nécessité du traitement envisagé.

Un dispositif ne peut être licite que s'il répond à un objectif déterminé, explicite et légitime, et s'il demeure strictement limité à ce qui est nécessaire à la poursuite de cet objectif. Toute collecte excessive, redondante ou insuffisamment justifiée expose l'employeur à un risque de remise en cause de la licéité du traitement.

La surveillance au travail : une exception strictement encadrée

La CNIL rappelle de manière constante que la surveillance des salariés ne saurait être ni systématique ni permanente. Elle ne peut être admise qu'à titre exceptionnel, lorsqu'aucune autre mesure moins intrusive ne permet d'atteindre l'objectif poursuivi.

Les dispositifs doivent ainsi être limités à des finalités légitimes, telles que la sécurité des personnes et des biens, la prévention des vols ou la protection de zones sensibles. En revanche, ils ne peuvent avoir pour objet — ni même pour effet — un contrôle individuel et continu de l'activité des salariés.

Certains espaces demeurent, par nature, exclus de toute surveillance, notamment les locaux sociaux, les espaces de repos ou les sanitaires. De même, la surveillance constante des postes de travail n'est admise que dans des hypothèses très spécifiques, par exemple en présence d'un risque particulier et dûment caractérisé.

La détermination de la base légale : un exercice central

Dans le cadre de la relation de travail, la base légale du traitement repose, en pratique, sur l'intérêt légitime de l'employeur. Ce fondement suppose la réalisation préalable d'une mise en balance entre l'objectif poursuivi et l'atteinte potentielle portée à la vie privée des salariés.

Le recours au consentement apparaît, quant à lui, largement inopérant. En raison du lien de subordination inhérent au contrat de travail, la CNIL considère que le consentement du salarié ne peut être regardé comme libre que dans des situations marginales, rarement réunies en matière de surveillance.

L'obligation d'information : une condition déterminante de licéité

La mise en œuvre d'un dispositif de surveillance conforme suppose une information préalable, loyale et complète des salariés. Cette information constitue une condition essentielle de la licéité du traitement.

Les salariés doivent être clairement informés :

- de l'existence du dispositif,
- de ses finalités,
- des données collectées,
- de la durée de conservation,
- des destinataires des données,
- le nom ou la qualité et le numéro de téléphone du délégué à la protection des données ou Data Protection Officer (DPO) ;
- ainsi que des droits dont ils disposent.



En matière de vidéosurveillance, cette information repose sur une combinaison d'affichages visibles et de supports écrits plus détaillés (note interne, charte informatique, règlement intérieur). Un dispositif dissimulé, insuffisamment documenté ou mal expliqué est susceptible d'être qualifié d'illicite, indépendamment de son utilité opérationnelle.

L'articulation indispensable avec le dialogue social

Au-delà des exigences issues du RGPD, la mise en place d'un dispositif de surveillance constitue également un moyen de contrôle de l'activité des salariés au sens du droit du travail. À ce titre, elle requiert la consultation préalable du comité social et économique (CSE).

Cette obligation conditionne non seulement l'opposabilité du dispositif aux salariés, mais également la recevabilité des preuves susceptibles d'être produites en cas de contentieux. Une conformité formelle au RGPD ne saurait donc dispenser l'employeur du respect de ses obligations sociales, sous peine de fragiliser l'ensemble du dispositif.

La durée de conservation : un point de vigilance opérationnel

Le principe de limitation de la conservation impose une gestion rigoureuse des données issues des dispositifs de surveillance. La CNIL considère que les images ou enregistrements ne doivent être conservés que pour une durée courte, généralement limitée à quelques jours et qui ne peut excéder un mois.

Une conservation prolongée ne peut être admise qu'en présence d'un événement particulier, tel qu'un incident de sécurité ou une procédure disciplinaire ou contentieuse en cours. Toute conservation excessive ou systématique expose l'employeur à un risque accru de sanction.

Analyse d'impact et gouvernance des traitements

Lorsque le dispositif est susceptible d'engendrer un risque élevé pour les droits et libertés des salariés, la réalisation d'une analyse d'impact relative à la protection des données (AIPD) s'impose. Cet exercice permet de formaliser l'analyse de proportionnalité, d'identifier les risques résiduels et de définir les mesures de mitigation appropriées.

Même lorsqu'elle n'est pas strictement requise par la réglementation, l'AIPD demeure fortement recommandée. Elle constitue un outil précieux de pilotage de la conformité et de prévention du risque. Dans ce cadre, le DPO joue un rôle central, tant lors de la conception du dispositif que dans son suivi.

Sécurité des données et accès strictement encadré

Les dispositifs de surveillance impliquent la mise en œuvre de mesures de sécurité techniques et organisationnelles adaptées. L'accès aux données doit être strictement limité aux seules personnes habilitées, dans le cadre précis de leurs fonctions.

Une attention particulière doit être portée à la gestion des habilitations, à la traçabilité des accès et à la prévention des consultations non autorisées. Les défaillances en matière de sécurité constituent un terrain récurrent de mise en cause du responsable de traitement.

EN CONCLUSION :

La surveillance des salariés constitue un levier de gestion particulièrement sensible, étroitement encadré par le droit, la réglementation relative à la protection des données personnelles et sous le contrôle attentif de la CNIL. La conformité au RGPD ne saurait se réduire à une information formelle des salariés ou à la production de documents internes. Elle suppose une réflexion approfondie en amont, une gouvernance claire et documentée, ainsi qu'une réévaluation régulière de la légitimité et de la proportionnalité des dispositifs mis en place.

Pour les employeurs, la sécurisation juridique de ces pratiques repose sur un équilibre exigeant entre impératifs opérationnels et respect des libertés fondamentales. C'est dans cette logique de prévention du risque, tant social que contentieux, que les conseillers de La Cité des Entreprises accompagnent leurs adhérents, en les aidant à appréhender de manière globale et cohérente les enjeux liés à la protection des données personnelles, et plus particulièrement à inscrire la conformité au RGPD dans une démarche stratégique, durable et créatrice de sécurité juridique pour l'entreprise.



➤ **Bernard BOSSU**
Directeur du Master II Droit social
à l'Université de Lille

Veille de jurisprudence

1 Droit d'accès aux courriels figurant sur la messagerie professionnelle

Cass. soc., 18 juin 2025, n° 23-19.022

Le règlement européen 2016/679 du 27 avril 2016, dit « règlement général sur la protection des données » (RGPD) prévoit que la personne concernée a un droit d'accès à ses données personnelles (art. 15 du RGPD). Ces dernières se présentent comme toutes informations se rapportant à une personne physique identifiée ou identifiable (art. 4 du RGPD). En conséquence, pour la Cour de cassation, les courriels émis ou reçus par le salarié grâce à sa messagerie électronique professionnelle sont des données à caractère personnel sur lesquelles il peut exercer son droit d'accès. Un salarié licencié pour faute peut donc obtenir de l'employeur non seulement les métadonnées (horodatage, destinataires), mais également le contenu des courriels. Il en va autrement si les éléments dont la communication est demandée sont de nature

à porter atteinte aux droits et libertés d'autrui. La CNIL a ainsi décidé que le respect du droit à la vie privée, le secret des affaires ou encore le secret des correspondances pourraient justifier le refus de communiquer certaines données personnelles (CNIL, 5 janv. 2022, Le droit d'accès des salariés à leurs données et aux courriels professionnels). Cette solution inédite de la chambre sociale est essentielle car elle va permettre au salarié de se constituer des éléments de preuve même si sa messagerie professionnelle a été coupée.

Par ailleurs, le fait pour un salarié de détruire de manière délibérée l'ensemble des données contenues dans sa messagerie professionnelle à la veille d'un entretien préalable à son licenciement s'analyse comme un manquement à l'exécution de bonne foi du contrat de travail (CA Rennes, 13 mars 2025, n° 22 :03.425).

2 Production d'éléments de preuve illicite ou déloyaux par un employeur

Cass. soc., 26 février 2025, n° 22-24.474

Pour démontrer la matérialité des faits, l'employeur peut produire en justice une preuve déloyale ou illicite (atteinte à la vie privée d'un salarié) en espérant que celle-ci soit jugée recevable par le juge. À partir de 2016, la Cour de cassation va affirmer que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie personnelle d'un salarié (Cass. soc., 16 nov. 2016, n° 15-17.163). Le 22 décembre 2024, l'assemblée plénière de la Cour de cassation va décider que le principe de loyauté dans l'administration de la preuve peut aussi s'effacer devant le droit à la preuve (Cass. ass. plén., 22 déc. 2023, n° 20-20.648). En résumé, il est désormais possible de produire des éléments de preuve illicites ou déloyaux dans un procès civil. En d'autres termes, on va mettre en balance le droit à la preuve et les droits antinomiques en présence, tels que le respect au droit de la vie privée.

Mais quelles sont les conditions requises pour admettre une preuve illicite ou déloyale ? La Cour de cassation a identifié trois étapes qui doivent être respectées par les juges du fond (Cass. soc., 8 mars 2023, n° 21-17.802).

Dans une première étape, le juge doit s'interroger sur la légitimité du contrôle opéré par l'employeur et vérifier les raisons concrètes permettant de justifier la surveillance et l'ampleur de celle-ci. Parmi les motifs légitimes, on va trouver par exemple la confidentialité des affaires (se préserver de la concurrence), la sécurité des biens (se protéger contre les vols) ou encore la protection des clients.

Dans une seconde étape, le juge doit rechercher si l'employeur ne pouvait pas atteindre un résultat identique en utilisant d'autres moyens plus respectueux de la vie personnelle. Ainsi le recours à la vidéosurveillance pour prouver les vols commis par une salariée n'est pas justifiée dès lors que les actes fautifs ont déjà été établis dans le cadre d'un audit (Cass. soc., 8 mars 2023, n° 21-17.802).

Enfin, dans une troisième étape, le juge doit apprécier le caractère proportionné de l'atteinte portée à la vie personnelle au regard du but poursuivi. En d'autres termes, on doit s'assurer que l'atteinte portée à la vie privée est aussi mesurée que possible. Ainsi, lorsqu'un employeur produit exclusivement les données professionnelles de la clé USB personnelle du salarié sans ouvrir les fichiers à caractère personnel, l'atteinte à la vie privée est strictement proportionnée au but poursuivi (Cass. soc., 25 sept. 2024, n° 23-13.992).

Cette méthodologie est rappelée par la Cour de cassation dans une affaire où un salarié avait été filmé à son insu dans les locaux de l'entreprise. La haute juridiction relève que « pour établir le grief de divulgation par le salarié de données hautement confidentielles à caractère technique et commercial à une entreprise tierce, l'employeur s'était borné à produire la retranscription des conversations relatives à son activité professionnelle et qu'il n'était pas démontré que l'employeur avait mis en œuvre, avec la complicité d'un autre salarié, un stratagème visant à le piéger et à provoquer la commission d'une faute » (Cass. soc., 26 fév. 2025, n° 22-24.474).

3 Production d'éléments de preuve illicites ou déloyaux par un salarié

Cass. soc., 5 nov. 2025, n° 24-16.208
Cass. soc., 17 déc. 2025, n° 24-18.407

Comme pour l'employeur, la Cour de cassation reconnaît le droit pour le salarié, au nom du droit à la preuve, de produire en justice une preuve déloyale ou illicite. De façon classique, le juge va mettre en balance le droit à la preuve et les droits antinomiques en présence (vie privée ou loyauté). La Cour de cassation a par exemple décidé qu'un enregistrement clandestin réalisé par un salarié ne peut être admis en justice que s'il est indispensable à l'exercice de son droit à la preuve. En conséquence, elle écarte la retranscription d'une conversation téléphonique de l'employeur enregistrée à son insu, dès lors que le salarié disposait d'autres éléments de fait laissant supposer l'existence d'une discrimination (Cass. soc., 5 nov. 2025, n° 24-16.208). Au contraire, dans une autre affaire, la Cour de cassation a admis la recevabilité d'une preuve déloyale pour prouver l'accomplissement d'heures non rémunérées. Selon la haute juridiction, « la production par la salariée de la retranscription d'un enregistrement audio de la conversation avec sa supérieure, obtenu de manière déloyale, était indispensable à l'exercice de son droit à la preuve et proportionnée au but légitime poursuivi, à savoir le paiement des heures travaillées » (Cass. soc., 17 déc. 2025, n° 24-18.407).

4 Messagerie personnelle, secret des correspondances et droit à la preuve

Cass. soc., 26 février 2025, n° 22-18.179

Les courriels reçus ou transmis via une messagerie personnelle du salarié sont couverts par le secret des correspondances. Ce dernier se présente comme une liberté fondamentale dont tout salarié bénéficie, même au temps et au lieu du travail (Cass. soc., 26 janv. 2016, n° 14-15.360). En conséquence, un employeur ne peut se prévaloir des courriels figurant sur la messagerie personnelle du salarié, peu importe que les messages ne comprennent pas un titrage personnel.

Toutefois, comme le précise un arrêt en date du 26 février 2025, « le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie privée du salarié à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi » (Cass. soc., 26 fév. 2025, n° 22-18.179). Dans cette affaire, l'employeur a produit en justice des courriels issus de la messagerie personnelle du salarié pour établir sa déloyauté. Il lui reprochait notamment la divulgation d'informations confidentielles de l'entreprise auprès de professionnels susceptibles de travailler pour des entreprises concurrentes. La Cour de cassation relève que « l'employeur s'était borné à produire des messages échangés par l'intéressé avec ses partenaires pour préparer et négocier le rachat d'une société de ventes de véhicules de même standing que ceux vendus par son employeur et leur faire parvenir des informations confidentielles ». Et, « cette production d'éléments portant atteinte à la vie privée du salarié était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de l'employeur à la préservation de ses intérêts et à la confidentialité de ses affaires ».

5 Messagerie professionnelle et rattachement des courriels à la vie privée ou à la vie professionnelle

Cass. soc., 6 mars 2024, n° 22-11.016
Cass. soc., 25 septembre 2024, n° 23-11.860
Cass. soc., 11 déc. 2024, n° 23-20.716

Lorsqu'un employeur a régulièrement accédé au contenu d'un courriel figurant sur la messagerie professionnelle du salarié, il ne peut pas forcément l'utiliser sur le plan disciplinaire. Le droit de prendre connaissance d'un courriel ne doit pas être confondu avec le droit de se prévaloir de son contenu. Pour la Cour de cassation, si le contenu du courriel se rattache à la vie professionnelle, le salarié pourra être sanctionné sous réserve de caractériser une faute disciplinaire : transmission d'informations confidentielles à des tiers, propos injurieux à l'encontre du supérieur hiérarchique... Ainsi, les messages adressés par un salarié à des collègues de travail et contenant des propos critiques à l'égard de la société et dénigrants vis-à-vis de ses dirigeants sont en rapport avec l'activité professionnelle (Cass. soc., 11 déc. 2024, n° 23-20.716). Au contraire, l'employeur ne peut pas sanctionner le salarié si le message se rattache à la vie personnelle : correspondance amoureuse entre deux salariés, discussion sur le lieu des futures vacances Comme le décide l'assemblée plénière de la Cour de cassation le 22 décembre 2023, une conversation privée qui n'est pas destinée à être rendue publique ne peut caractériser un

manquement aux obligations contractuelles (Cass. ass. plén., 22 déc. 2023, n° 21-11.330). Cette analyse sera reprise par la chambre sociale de la Cour de cassation le 6 mars 2024 dans une affaire où, une salariée d'une caisse de sécurité sociale avait envoyé à des correspondants extérieurs, depuis sa messagerie professionnelle, des messages contenant des propos racistes à l'encontre des assurés d'origine étrangère. La chambre sociale juge que ces messages relèvent de la vie privée car ils s'inscrivaient dans le cadre d'échanges privés à l'intérieur d'un groupe et ils n'avaient pas vocation à devenir publics (Cass. soc., 6 mars 2024, n° 22-11.016). La solution sera réaffirmée par la chambre sociale le 25 septembre 2024 dans une affaire où un cadre dirigeant avait utilisé sa messagerie professionnelle pour adresser des messages à connotation sexuelle à un autre salarié et à des personnes extérieures à l'entreprise (Cass. soc., 25 sept. 2024, n° 23-11.860).



CONTACTS

LA CITÉ DES ENTREPRISES **Campus Entreprises & Cités**

40, rue Eugène Jacquet • 59700 Marcq-en-Baroeul
03 20 99 45 35 • www.lacitedesentreprises.com

Faculté des sciences juridiques, politiques et sociales

1, Place Déliot • 59024 Lille
03 20 90 75 30 • droit.univ-lille.fr