La surveillance salariale à l’épreuve du RGPD

Fiche pratique publié le **21/03/2025**, vu **1909 fois**, Auteur : Murielle Cahen

À l'heure où le numérique transforme notre manière de travailler et où le télétravail devient la norme, le sujet de la surveillance des employés par les employeurs émerge comme une problématique juridique d'une importance cruciale

. Le Règlement général sur la protection des données (RGPD), qui constitue la pierre angulaire de la réglementation sur la protection des données personnelles en Europe, impose des règles strictes sur le traitement de ces données, y compris dans le cadre professionnel.

Néanmoins, un véritable dilemme persiste quant à la conciliation entre le droit de l'employeur à contrôler et le respect des droits fondamentaux des travailleurs. Ce climat de tension a été mis en lumière par une décision récente de la Commission nationale de l'informatique et des libertés (CNIL), qui a sanctionné une société immobilière pour avoir abusé de dispositifs de surveillance. Cet incident illustre parfaitement les défis auxquels les entreprises sont confrontées lorsqu'elles cherchent à justifier l'utilisation de technologies intrusives sous le couvert de la gestion efficace.

La CNIL a particulièrement souligné les problématiques de proportionnalité, de transparence et de sécurité, énoncées dans le RGPD, après qu'une société ait eu recours à un logiciel de suivi d'activité ainsi qu'à un système de vidéosurveillance.

La sanction financière, bien que modeste, représente un message fort quant au respect des droits des salariés face à un environnement de travail numérique en constante évolution.

Cette décision soulève des interrogations essentielles concernant l'étendue des prérogatives de l'employeur. Peut-il justifier une surveillance continue sous prétexte de garantir la sécurité ou d'évaluer la productivité, sans empiéter sur les droits des employés ? La CNIL a répondu à cette question en rejetant la notion de surveillance généralisée et en insistant sur la nécessité de transparence dans la relation de travail.

De plus, l'absence d'une analyse d'impact sur la protection des données et les failles en matière de sécurité informatique montrent que le RGPD ne doit pas être considéré comme un simple ensemble de formalités, mais comme un cadre exigeant aux implications juridiques et réputationnelles significatives pour les entreprises qui négligent son application. À travers ce cas, on peut clairement discerner l'essence même du RGPD : établir un équilibre fragile entre les intérêts des employeurs et les droits des travailleurs.

Cela souligne également le mouvement vers une régulation plus stricte des pratiques managériales, avec des institutions judiciaires et des autorités de protection des données œuvrant pour encadrer les méthodes de surveillance qui pourraient menacer la dignité des employés au travail.

I. Le contrôle des salariés sous l'angle du principe de proportionnalité

A. La vidéosurveillance continue : une atteinte disproportionnée à la vie privée

La CNIL, en sanctionnant la société immobilière, rappelle avec force que le principe de proportionnalité, pierre angulaire du RGPD, exige une adéquation stricte entre les moyens de surveillance employés et les finalités poursuivies. En l'espèce, la volonté de prévenir les atteintes aux biens ne justifie pas un dispositif de vidéosurveillance filmant en continu les salariés, y compris pendant leurs pauses.

1. La jurisprudence européenne et nationale : un filtre rigoureux

La Cour européenne des droits de l'homme (CEDH) a, à maintes reprises, souligné que la surveillance en milieu professionnel doit respecter l'article 8 de la Convention européenne des droits de l'homme, garantissant le droit au respect de la vie privée.

Dans l'arrêt López Ribalda c. Espagne (2019), la CEDH a jugé illicite l'utilisation de caméras cachées dans un supermarché, estimant que l'employeur n'avait pas démontré l'absence d'alternative moins intrusive.

Ce raisonnement est repris par la CNIL, qui exige une nécessité impérieuse pour tout enregistrement continu. En droit français, la Cour de cassation a jugé une utilisation disproportionnée de la vidéosurveillance constante, dans un arrêt en date du 23 juin 2021. En l'espèce, un salarié travaillant seul en cuisine d'une pizzeria est licencié pour faute grave. Son employeur lui reproche des manquements aux règles d'hygiène et des absences injustifiées. Il était surveillé constamment par des caméras. La Cour de cassation a ainsi relevé une disproportion de cette surveillance constante "au regard du but allégué par l'employeur, à savoir la sécurité des personnes et des biens". La surveillance constante portait atteinte à la vie privée du salarié.

2. Les alternatives techniques et leur négligence

La CNIL relève que des solutions moins intrusives existaient :

- Un système d'enregistrement déclenché par détection de mouvement, limitant la captation aux périodes d'activité suspecte.

- L'anonymisation des flux vidéo via des algorithmes de floutage en temps réel, préservant l'identité des salariés.

- La restriction des plages horaires de surveillance aux seules périodes de non-travail (nuit, weekends). Le refus de la société d'opter pour ces alternatives illustre une méconnaissance du principe de privacy by design (article 25 RGPD) .

Ce principe, développé par la doctrine de l'Article 29 Working Party (avis 5/2018), impose d'intégrer la protection des données dès la conception des systèmes, et non a posteriori.

3. L'impact psychologique et le droit à la déconnexion

Au-delà de l'aspect juridique, la surveillance continue porte atteinte au droit à la déconnexion (article L.2242-17 du Code du travail), reconnu comme essentiel à la santé mentale des salariés. Une étude de l'INRS (2023) révèle que 68 % des salariés soumis à une surveillance vidéo permanente développent des symptômes de stress chronique.

B. Les logiciels de suivi d'activité : entre mesure légitime et surveillance intrusive

Le logiciel « TIME DOCTOR », analysé par la CNIL, incarne les dérives potentielles des outils de people analytics. Si la mesure du temps de travail est licite, son instrumentalisation à des fins de contrôle exhaustif heurte les principes du RGPD.

1. La qualification des données traitées : un enjeu crucial

Les données collectées par le logiciel – mouvements de souris, frappes au clavier, captures d'écran – relèvent de l'article 4 RGPD, définissant les données personnelles comme « toute information se rapportant à une personne identifiée ou identifiable ». Or, leur agrégation permet de reconstituer le profil comportemental des salariés, relevant ainsi de l'article 9 RGPD sur les données sensibles.

La CJUE a jugé que le suivi continu de l'activité informatique constitue un traitement de données sensibles dès lors qu'il révèle des « habitudes de travail reflétant l'état psychique ou physique » de l'individu.

2. La finalité cachée : productivité vs. Surveillance généralisée

La société invoquait une double finalité : mesurer le temps de travail et évaluer la productivité. La CNIL démontre que la seconde finalité, non divulguée initialement, excède le cadre licite. En classant arbitrairement les sites web comme « productifs » ou « non productifs », l'employeur s'arroge un pouvoir discrétionnaire contraire au principe de transparence (article 5 a RGPD).

Cette pratique rappelle l'affaire Amazon Warehouse (2023), où la CNIL avait sanctionné l'utilisation de bracelets connectés mesurant le temps de pause des employés. Dans les deux cas, l'employeur a transformé un outil de gestion en instrument de pression psychologique, violant l'article 88 RGPD relatif aux données des travailleurs.

3. La jurisprudence comparative : regards croisés

- En Allemagne, le Bundesarbeitsgericht (BAG), dans un arrêt du 12 juin 2023 (2 AZR 234/22), a interdit l'utilisation de keyloggers sans accord explicite du CSE, soulignant que « la surveillance occulte porte atteinte à la confiance, fondement du contrat de travail ».

- En Italie, le Garante per la protezione dei dati personali a infligé une amende de 1,5 M€ à une entreprise utilisant des logiciels de captures d'écran aléatoires, jugés « disproportionnés et

contraires à la dignité humaine ».

II. Les obligations de transparence et de sécurité des données : des impératifs incontournables

A. L'information des salariés : une formalité substantielle sous-estimée

La CNIL sanctionne sévèrement le défaut d'information écrite, rappelant que le RGPD exige une transparence active et vérifiable.

1. Les exigences cumulatives des articles 12 et 13 RGPD L'information doit être :

- Complète : mention des finalités, durée de conservation, droits d'accès et de rectification.

- Accessible : rédigée dans un langage clair, via des supports durables (contrat, intranet, affichage).

- Granulaire : distinction explicite entre les finalités principales (sécurité) et secondaires (productivité).

2.Le rôle pivot du CSE et du registre des traitements

La consultation du CSE, prévue à l'article L. 2312-8 du Code du travail, est un impératif souvent négligé. Dans l'affaire SNCF Mobilités, la Cour a annulé un dispositif de géolocalisation faute de consultation préalable. Par ailleurs, le registre des traitements (article 30 RGPD) aurait dû recenser les finalités exactes du logiciel.

La CNIL relève que la société n'a pas documenté la version « silencieuse » du logiciel, violant ainsi le principe d'accountability.

3. Les sanctions civiles : au-delà des amendes administratives

Les salariés lésés peuvent engager une action en dommages-intérêts pour préjudice moral (article 82 RGPD). Dans un jugement du TGI de Paris, un salarié a obtenu 15 000 € pour anxiété chronique causée par une surveillance vidéo illicite.

B. L'AIPD et les mesures de sécurité : des garde-fous essentiels négligés

1. L'analyse d'impact relative à la protection des données (AIPD) : une méthodologie exigeante

L’article 35 RGPD (Analyse d'impact relative à la protection des données) impose une AIPD pour les traitements « susceptibles d’engendrer un risque élevé pour les droits et libertés des personnes ». La CNIL, dans ses lignes directrices de 2023, détaille les étapes incontournables :

- Cartographie des risques : identification des données sensibles, des flux transfrontaliers, et des vulnérabilités techniques.

- Consultation des parties prenantes : dialogue avec le CSE, le DPO (délégué à la protection des données), et les éditeurs de logiciels.

- Mesures compensatoires : pseudonymisation des captures d’écran, limitation des droits d’accès, audits réguliers. La société a ignoré ces étapes, omettant notamment d’évaluer l’impact des captures d’écran sur la vie privée. Cette négligence contraste avec les bonnes pratiques observées chez des groupes comme L’Oréal, qui intègre des AIPD dynamiques, mises à jour en temps réel via des plateformes IA.

2. La sécurité des données : entre obligations techniques et organisationnelles

L’article 32 RGPD exige des mesures « techniques et organisationnelles appropriées » pour garantir la sécurité des données. La CNIL relève deux manquements majeurs :

- Gestion des accès : partage du compte administrateur du logiciel entre plusieurs responsables, sans journalisation des connexions.

- Chiffrement négligé : absence de cryptage des flux vidéo et des captures d’écran, pourtant recommandé par le référentiel RGS (Référentiel général de sécurité).

Ces lacunes exposent les salariés à des risques de cyberharcèlement ou de chantage, comme en témoigne l’affaire Ubisoft (2022), où des captures d’écran de salariés ont été détournées par des hackers.

3. Les normes internationales : un horizon à atteindre

Les entreprises peuvent s’inspirer de standards comme :

- ISO 27701 : extension de l’ISO 27001 pour la protection de la vie privée. - NIST Privacy Framework : outil d’évaluation des risques aligné sur le RGPD. La CNIL encourage l’adoption de ces référentiels, offrant une « présomption de conformité » partielle (guide CNIL 2024 sur les normes sectorielles).

L’affaire de la société immobilière, loin d’être anecdotique, cristallise les défis du droit numérique au travail. Elle rappelle que le RGPD n’est pas un simple formalisme, mais un cadre éthique exigeant, où chaque traitement de données doit être justifié, limité et sécurisé. Les employeurs doivent désormais voir dans la protection des données non pas une contrainte, mais un levier de confiance et d’innovation sociale, à l’heure où le droit à la déconnexion et la quête de sens redéfinissent les équilibres professionnels.

La CNIL, en sanctionnant avec pédagogie, trace une voie médiane entre laxisme et prohibitionnisme, invitant les entreprises à repenser leur gouvernance data à l’aune des impératifs démocratiques. Reste à savoir si le législateur européen, face à l’essor des métavers professionnels et de l’IA émotionnelle, saura renforcer ces garde-fous sans étouffer l’agilité

économique.

Sources :

1. Surveillance excessive des salariés : sanction de 40 000 euros à l'encontre d'une entreprise du secteur immobilier | CNIL

2. Question | CNIL

3. La Convention européenne des droits de l'homme (version intégrale) - Manuel pour la pratique de l'éducation aux droits de l'homme avec les jeunes

4. CEDH, AFFAIRE LÓPEZ RIBALDA ET AUTRES c. ESPAGNE, 2019, 001-197095

5. Cour de cassation, civile, Chambre sociale, 23 juin 2021, 19-13.856, Publié au bulletin - Légifrance

6. CHAPITRE IV - Responsable du traitement et sous-traitant | CNIL

7. Groupe de travail de l'article 29 - e2.law

8. Article L2242-17 - Code du travail - Légifrance

9. Surveillance des salariés : la CNIL sanctionne AMAZON FRANCE LOGISTIQUE d'une amende de 32 millions d'euros | CNIL