

Coronavirus (COVID-19) : respect des principes communs au droit du travail et au RGPD en situation de télétravail

La CNIL publie une foire aux questions dans laquelle elle met en garde les employeurs sur différents enjeux du télétravail : droit à la déconnexion, porosité des vies personnelles et professionnelles, évolution de la place du collectif dans le travail, etc.

Elle répond aux questions les plus fréquemment posées par le télétravail concernant la protection des données personnelles des salariés mais également des données que le salarié peut être amené à traiter.

- **Conditions de mise en place du télétravail**

Dans le cadre de la pandémie, la CNIL rappelle que le télétravail peut être imposé au salarié par son employeur, même en l'absence d'un accord entre ces derniers.

- **Contrôle de l'activité des salariés en télétravail**

L'employeur conserve son pouvoir d'encadrement et de contrôle de l'exécution du travail en situation de télétravail. La CNIL rappelle cependant que ce contrôle doit respecter certaines règles :

- ce pouvoir ne doit pas être exercé de manière excessive : les dispositifs de contrôle doivent être proportionnés à l'objectif poursuivi et ne pas porter une atteinte excessive au respect des droits et libertés des salariés, notamment au droit au respect de leur vie privée ;
- l'employeur est soumis à une obligation de loyauté à l'égard de ses salariés ;
- les représentants du personnel, s'ils existent, doivent être informés et consultés ;
- les traitements de surveillance de l'activité des salariés doivent être portés au registre des traitements ;
- les traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées devront faire l'objet [d'une analyse d'impact](#).

- **Surveillance des salariés**

La CNIL rappelle que l'employeur ne peut surveiller constamment ses salariés. Un système de contrôle de temps de travail/d'activités reste un traitement de données personnelles, qu'il s'effectue à distance ou sur site. Ce système doit :

- avoir un objectif clairement défini et ne pas être utilisé à d'autres fins ;
- être proportionné et adéquat à cet objectif ;
- nécessiter une information préalable des personnes concernées.

Sauf cas exceptionnels justifiés au regard de la nature de la tâche, l'employeur ne peut pas placer ses salariés sous surveillance permanente. La CNIL liste des exemples de procédés considérés comme invasifs :

- surveillance constante au moyen de dispositifs vidéo (webcam) ou audio. Ex : demande faite par l'employeur de se mettre en visio tout le long du temps de travail pour s'assurer de la présence du salarié derrière son écran ;
- partage permanent de l'écran et/ou utilisation de « keyloggers », logiciels permettant d'enregistrer l'ensemble des frappes au clavier effectuées par le salarié sur son ordinateur ;

- obligation pour le salarié d'effectuer très régulièrement des actions pour démontrer sa présence derrière son écran. Exemple : cliquer toutes les X minutes sur une application.

La CNIL appelle à une réflexion des employeurs concernant l'adaptation des méthodes d'encadrement et d'évaluation des salariés :

- possibilité de mettre en place un contrôle de la réalisation par objectifs pour une période donnée (objectifs raisonnables, quantifiables et contrôlables à intervalles réguliers) ;
- possibilité de mettre en place un compte rendu régulier du salarié.

- **Précaution à prendre en cas d'utilisation de l'équipement personnel du salarié**

Le niveau de sécurité et de confidentialité des données personnelles traitées doit être le même, quel que soit l'équipement utilisé. Dans tous les cas, l'employeur reste responsable de la sécurité des données personnelles de son entreprise.

Le recours aux équipements personnels des salariés est une décision devant être prise après avoir mis en balance les intérêts et inconvénients de cet usage qui brouille la frontière entre vie personnelle et vie professionnelle

- **Visioconférence et obligation d'activation de la caméra**

La CNIL recommande aux employeurs de ne pas imposer l'activation de leur caméra aux salariés en télétravail participant à des visioconférences. Une participation via le micro est suffisante

En effet, l'activation de la caméra peut porter atteinte au droit au respect de la vie privée. Le salarié doit pouvoir être en mesure de refuser la diffusion de son image. Seule des conditions particulières dont il appartient à l'employeur de justifier pourrait rendre nécessaire la visioconférence à visage découvert.

- **Outils spécifiquement dédiés au télétravail**

Certaines entreprises se sont mobilisées pour proposer, le plus souvent gratuitement, leurs solutions numériques pour permettre aux entreprises de faire face à la crise et aidant à la mise en place du télétravail.

La CNIL rappelle que les entreprises ayant recours à de telles solutions doivent évaluer les garanties en matière de protection des données. La CNIL propose donc des conseils pratiques pour [les employeurs](#) et [les salariés](#) et rappelle les [règles et bonnes pratiques](#) en matière de sécurité des données.

- **Compétence de la CNIL en cas de plainte**

La CNIL peut réaliser des contrôles à distance, sur place, sur audition ou sur pièces en cas de plainte d'un salarié ou de sa propre initiative.

En cas de non-respect du RGPD ou du droit du travail, par exemple si l'employeur met en place une surveillance excessive des salariés, la CNIL peut :

- mettre en demeure les organismes de se conformer au RGPD et à la loi ;
- prononcer une sanction financière.

Une publicité peut être décidée en fonction de la gravité des cas.