Dernière mise à jour le 23 novembre 2020

Covid-19 : les Questions-Réponses de la CNIL sur le télétravail

En complément de ses recommandations aux employeurs et télétravailleurs, la CNIL a diffusé un questions-réponses sur le télétravail en rappelant certains principes essentiels au droit du travail et au RGPD.

Sommaire

Depuis le 1er confinement, la CNIL a diffusé ses conseils pour mettre en place le télétravail, les bonnes pratiques à suivre par les salariés en télétravail, des conseils pour garantir la sécurité des systèmes et données, et des conseils pour utiliser les outils de visioconférence.

En complément de ses recommandations concernant les outils utilisables, elle répond également aux questions les plus fréquentes concernant le télétravail et rappelle certains principes essentiels communs au droit du travail et au RGPD.

Source de nombreuses opportunités s'il est bien encadré, le recours au télétravail soulève de nombreuses questions qui ne se limitent pas à la protection des données, telles que le droit à la déconnexion et la porosité des vies personnelle et professionnelle, l'évolution de la fonction managériale et de l'évaluation du travail, ou encore la place du collectif dans le travail.

Parmi ces questions figurent celle de la protection des données personnelles des salariés, mais aussi celle des données que les salariés peuvent être amenés à traiter.

Contrôle de l'activité des salariés en télétravail

L'employeur peut contrôler l'activité des télétravailleurs**, si cela ne porte pas atteinte aux droits et libertés des salariés et en respectant certaines règles.**

Le télétravail n'étant qu'une modalité d'organisation de travail, l'employeur conserve, au même titre que lorsque le travail est effectué sur site, le pouvoir d'encadrer et de contrôler l'exécution des tâches confiées à son salarié.

Néanmoins, si le pouvoir de contrôle de l'employeur est une contrepartie normale et inhérente au contrat de travail, les juridictions ont rappelé de manière constante que ce pouvoir ne saurait être exercé de manière excessive.

L'employeur doit donc toujours justifier que les dispositifs mis en œuvre sont strictement **proportionnés à l'objectif poursuivi** et ne portent pas atteinte excessive au respect des droits et libertés des salariés, particulièrement le droit au respect de leur vie privée.

Conformément tant au Code du travail qu'au RGPD, l'employeur est également soumis à une **obligation de loyauté** envers ses salariés.

Il doit à ce titre informer l'ensemble des salariés, préalablement à leur mise en œuvre, des éventuels dispositifs de contrôle de leur activité. Un employeur qui viendrait à manquer à cette obligation pourra voir sa responsabilité engagée ; par ailleurs, les juridictions ont rappelé à maintes reprises que les preuves obtenues à l'aide de tels dispositifs ne peuvent pas, en principe, être invoquées pour justifier une sanction.

L'information et la consultation des représentants du personnel participent à une meilleure transparence et au dialogue social, et constituent des conditions essentielles de mise en œuvre de ces dispositifs.

De la même manière, les juridictions ont eu l'occasion de rappeler qu'il est interdit à l'employeur d'avoir recours à

des stratagèmes visant à « piéger » un salarié.

Par ailleurs, si depuis l'entrée en application du RGPD les traitements de surveillance de l'activité des salariés n'ont pas à faire l'objet d'une formalité préalable auprès de la CNIL, ils **devront cependant 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 doivent faire l'objet d'une analyse d'impact.

Plus particulièrement, la liste des traitements pour lesquels une AIPD est requise rappelle que, dans les cas où ils peuvent être justifiés, les traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés **doivent obligatoirement faire l'objet d'une analyse d'impact relative à la protection des données** (AIPD).

Précautions à prendre en cas d'utilisation par les salariés de leur équipement personnel

L'usage d'équipements informatiques personnels dans un contexte professionnel est connu sous l'acronyme de « **BYOD** » qui est l'abréviation de l'expression anglaise « **Bring Your Own Device** » (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC).

La réglementation en matière de protection des données personnelles veut que **le niveau de sécurité et de confidentialité des données personnelles traitées soit le même, quel que soit l'équipement utilisé**.

L'employeur reste en effet responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

Par ailleurs, si l'employeur est en principe libre d'accéder aux données présentes sur l'équipement professionnel confié au salarié, qui sont présumées avoir un caractère professionnel, ce n'est pas le cas pour les données figurant sur l'équipement personnel de ses employés.

Le recours au BYOD est donc une décision qui doit être prise après avoir mis en balance les intérêts et les inconvénients présentés par cet usage qui brouille la frontière entre vie personnelle et vie professionnelle.

Visioconférence

De manière générale, la CNIL recommande aux employeurs de ne pas imposer l'activation de leur caméra aux salariés en télétravail qui participent à des visioconférences.

Cette recommandation découle du principe de minimisation des données, consacré par l'article 5.1.c du RGPD et selon lequel les données traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » : or, dans la plupart des cas, **une participation via le micro est suffisante**.

Bien que la diffusion de l'image puisse participer à la convivialité dans une période d'éloignement de ses collègues, le télétravail, particulièrement lorsqu'il est subi en raison de la crise sanitaire, peut porter atteinte au droit au respect de la vie privée, tout particulièrement aux autres personnes présentes au domicile.

Dès lors, un salarié doit pouvoir en principe refuser la diffusion de son image lors d'une visioconférence en mettant en avant les **raisons tenant à sa situation particulière**. Seules des circonstances très particulières, dont il appartiendrait à l'employeur de justifier, pourrait rendre nécessaire la tenue de la visioconférence à visage découvert.

Actions 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 de la loi, par exemple si l'employeur met en place une surveillance excessive des salariés, la CNIL dispose une chaîne répressive complète lui permettant de :

- mettre en demeureles organismes de se conformer au RGPD et à la loi ;
- prononcer une sanctionfinancière ou non.

Dans certains cas, une publicité peut être décidée en fonction de la gravité des cas.

Référence

Questions-Réponses de la CNIL du 12 novembre 2020
Retrouvez toutes les questions – réponses de la CNIL dans notre dossier spécifique sur le télétravail :

https://www.legisocial.fr/dossiers-premium/teletravail.html »