



ÉLÉMENTS DE CONTEXTE

- Le développement des outils numériques permet aujourd'hui aux cadres de travailler à distance de leur entreprise sous différentes formes (télétravail, nomadisme, co-working), dans différents lieux, avec différents outils connectés (smartphone, tablette, ordinateur portable, etc);
- Le cadre peut ainsi acquérir une plus grande autonomie dans l'organisation de son travail, même s'il ne maîtrise toutes les composantes et facteurs influençant le contenu de son travail et les délais;
- L'utilisation de ces formes de travail peut générer des effets pervers :

- une demande implicite de l'entreprise pour une plus grande responsabilité du cadre envers la sécurisation des données de l'entreprise (vol de données ou piratage des systèmes de l'entreprise);
- une exigence de l'entreprise d'une plus grande flexibilité du cadre dans son organisation du travail, accroissant ainsi les risques de perte d'outils de travail ou de données de l'entreprise.

FACE À CES RISQUES LIÉS À LA MANIÈRE DONT ON UTILISE LES OUTILS NUMÉRIQUES À DISTANCE, LES CONDITIONS D'UTILISATION DES TIC DOIVENT ÊTRE CLAIREMENT DÉFINIES ET ENCADRÉES.

PROPOSITIONS

- Négocier dans chaque entreprise une charte d'utilisation des outils numériques, intégrée dans le règlement intérieur, incluant les mesures de protection de la confidentialité et de la sécurité prises par l'entreprise pour protéger les données et les salariés et préciser les conditions d'utilisation des outils ;
- Encadrer strictement la collecte, la durée de stockage et l'usage des données relatives aux salarié-e-s. Elles doivent être adaptées à la finalité recherchée et pas utilisées pour une autre finalité ;
- Exiger que les supports numériques et les outils de connexion soient fournis par l'entreprise et sécurisés sous sa responsabilité ;
- Instaurer des procédures simples à destination de l'encadrement pour signaler tout évènement qui serait susceptible d'être synonyme de fuite des données. C'est bien l'entreprise qui est responsable de la protection de ses données et non le cadre auquel il est demandé parfois de se connecter dans des lieux publics ;
- Former tous les utilisateurs aux réflexes et aux bons usages à avoir pour participer à la protection et à la confidentialité des données.