

Fiche pratique

Protéger la vie privée des employé·es

“Travailler de chez soi ou depuis un espace partagé pose des problèmes pour la vie privée des employé·es. Alors que les bureaux d’entreprises sont généralement des espaces sécurisés, les conditions de pratique du travail à distance varient drastiquement d’un endroit à l’autre, ce que ce soit en termes d’infrastructure, de sécurité ou de fiabilité du réseau internet.

La vie privée des employé·es comprend leurs activités, relations et communications personnes en dehors de leur lieu de travail (Ranc, 2020). Cette notion est protégée par plusieurs dispositifs légaux, notamment par l’article 8 de la Convention Européenne des Droits de l’Homme, qui garantit le droit au respect de la vie privée et de la vie de famille. Au travail, ce droit s’étend aux communications et activités personnelles ayant lieu durant les horaires de travail, dans la mesure où elles n’interfèrent pas avec les obligations professionnelles (Markham, 2024). La loi française, par exemple, prend en compte cette distinction : elle autorise les employeurs à accéder aux fichiers professionnels des employé·es, mais l’accès aux fichiers personnels ne sont pas accessibles sans consentement préalable ou une raison valable aux yeux de la loi.

Protéger les données personnelles et la vie privée des employé·es est donc primordial, qu’ils et elles travaillent sur site ou à distance. Il apparaît cependant que la protection des données est complexifiée dans les environnements de travail à distance dans la mesure où les organisations manquent parfois d’information ou de visibilité sur la façon dont les employé·es se connectent en ligne.

Dans ce contexte, une étude d'IBM Security (2022) a montré que 83% des organisations avaient connu plus d'un piratage informatique et que la pratique du télétravail faisait augmenter le risque de fuite de données. Ces risques sont liés à des failles dans les réseaux de connexion personnels, des communications non-cryptées et un plus grand usage des appareils personnels, souvent hors de portée des services informatiques. Dans des environnements aussi décentralisés, protéger la vie privée des collaborateurs et collaboratrices devient un impératif technique et éthique.

Les enjeux de protection de la vie privée dans le travail hybride et à distance

Travailler de chez soi ou depuis un espace partagé pose des problèmes pour la vie privée des employé-es. Alors que les bureaux d'entreprises sont généralement des espaces sécurisés, les conditions de pratique du travail à distance varient drastiquement d'un endroit à l'autre, ce que ce soit en termes d'infrastructure, de sécurité ou de fiabilité du réseau internet. Les salarié-es peuvent utiliser des connexions Wi-Fi non sécurisées, omettre de mettre des logiciels à jour, ou partager leur espace de travail, augmentant ainsi le risque de fuite de données.

L'utilisation d'outils de suivi des activités et de la productivité (surveillance via webcam, suivi des touches entrées sur le clavier...) a fait l'objet de nombreux débats. Si ces outils peuvent répondre à des besoins managériaux, ils enfreignent souvent le respect de la vie privée, en particulier lorsque les salarié-es télétravaillent dans des lieux où les sphères privées et professionnelles se confondent.

Les environnements de travail à distance incluent souvent plusieurs appareils, des applications connectées au cloud, et une connexion à des réseaux non sécurisés, et chacune de ces dimensions présentent des risques potentiels pour le respect de la vie privée.

La littérature académique a étudié avec soin l'impact du télétravail sur la vie privée des employé-es. Un des principaux enjeux est le mélange des sphères privées et professionnelles, ce qui met en jeu l'article 8 de la Convention Européenne des Droits de l'Homme.

Selon Ajunwa et al. (2017), la surveillance des employé·es à l'heure du tout-digital soulève de sérieux enjeux concernant l'autonomie et la dignité, en particulier lorsque cette surveillance s'étend en dehors des horaires de travail. De la même façon, les travaux de Nissenbaum (2004) sur la protection des données montrent que les piratages et les fuites de données se produisent lorsque que les flux de données dévient de leur contexte d'origine, ce qui arrive fréquemment dans la pratique du télétravail.

Recommandations pour les managers et les ressources humaines

Protéger la vie privée des employé·es en travail hybride et à distance nécessite de déployer une stratégie équilibrée entre le fonctionnement opérationnel et le respect des libertés et des droits individuels. Voici quelques recommandations :

1

Déployer des politiques claires et transparentes

Assurez-vous que toute collecte ou suivi de données soit explicitement documentée et justifiée, et qu'elles fassent l'objet de communications spécifique. Les employé·es doivent disposer d'informations sur quelles données sont collectées, à quelle fin, où elles sont gardées et qui peut y avoir accès.

2

Minimiser la collecte et le traitement de données

Ne collectez que les données strictement nécessaires à l'atteinte d'objectifs précis. Certaines pratiques intrusives comme la surveillance par webcam ou le suivi GPS ne doivent être utilisées que si elles sont indispensables et font l'objet d'un consentement éclairé.

3

Renforcer la cybersécurité

Mettez en place des VPNs, des authentifications en plusieurs étapes, et encryptez les conversations. Proposez du soutien pour configurer et sécuriser les appareils personnels et ceux utilisés pour le télétravail.

4

Respecter l'équilibre vie pro/vie perso

Restreignez le contrôle aux horaires de travail, et mettez l'emphasis sur l'évaluation des résultats plutôt que sur le fait d'être constamment disponible ou connecté·e. Mettez en place un droit à la déconnexion pour préserver le bien-être des employé·es.

5

Former les managers au respect de la vie privée

Équipez les managers avec les connaissances et les outils pour incarner un leadership basé sur la confiance plutôt que sur le contrôle.

6

Conduire une analyse d'impact relative à la protection des données (AIPD)

Mesurez l'impact des nouvelles technologies ou process sur la protection des données des employé·es avant de ne les déployer. Consultez les salarié·es pour garantir la transparence et la coconstruction.



Pour aller plus loin

Vidéo

- Le droit à la déconnexion au travail, Parlement Européen, 2021
https://multimedia.europarl.europa.eu/fr/video/the-right-to-disconnect-from-work_N01-AFPS-210119-RTDI

Lectures complémentaires

- Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace Through Organizational Commitment and Ethical Environment. arXiv. arxiv.org

Choudhury, P., Larson, B. Z., and Froughi, C., 2021. Is it time to let employees work from anywhere? Harvard Business Review. [online] Available at:
<https://hbr.org/2021/08/is-it-time-to-let-employees-work-from-anywhere>

Bibliographie

- Ajunwa, I., Crawford, K. and Schultz, J., 2017. Limitless worker surveillance. California Law Review, 105(3), pp.735–776.
<https://doi.org/10.2139/ssrn.2746211>
- Ranc, S. (2020). Respect for personal life in the workplace during working hours: the inspection of employee computer files. Revue de droit comparé du travail et de la sécurité sociale.
- Markham, I. (2024). Employee Data: 5 Ways to Tighten Security to Shore Up Trust. The Wall Street Journal.
- Nissenbaum, H., 2004. *Privacy as contextual integrity*. Washington Law Review, 79(1), pp.119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>