L'employeur peut-il contrôler les connexions VPN des salariés en télétravail ?

Réponse courte

L'employeur peut **contrôler les connexions VPN** des télétravailleurs sous réserve de poursuivre une **finalité légitime** (sécurité du SI, traçabilité des accès aux applications professionnelles), de respecter la **proportionnalité** et de se limiter aux **données techniques** : horodatage, durée, adresse IP source. Il ne peut pas accéder au contenu des communications ni reconstituer une cartographie comportementale du salarié.

L'employeur doit informer individuellement chaque salarié, consulter la délégation du personnel (article L.414-9 du Code du travail pour les entreprises d'au moins 150 salariés), réaliser une AIPD si le risque est élevé et limiter la durée de conservation des logs au strict nécessaire (généralement **6 à 12 mois**). Sans information préalable, le contrôle est illicite et les preuves sont écartées par le tribunal du travail.

Définition

Le **contrôle des connexions VPN** désigne le suivi technique de l'accès distant des salariés au réseau de l'entreprise : horodatage, durée, adresse IP source, applications consultées. Ce traitement constitue un traitement de **données à caractère personnel** au sens du RGPD.

Il s'inscrit dans la cybersurveillance et doit respecter les principes de finalité, de nécessité et de proportionnalité posés par l'article L.261-1 du Code du travail et le RGPD.

Questions fréquentes

Combien de temps conserver les logs de connexion VPN ?

Généralement 6 à 12 mois. Au-delà, la conservation doit être justifiée précisément et inscrite au registre des traitements (article 30 RGPD). La justification doit être documentée par écrit.

Faut-il informer le salarié avant de contrôler ses connexions VPN ?

Oui, l'information préalable individuelle écrite est obligatoire (articles 12-13 RGPD). Sans information, le contrôle est illicite et les preuves sont écartées par le tribunal du travail, même justifié par la sécurité informatique.

L'employeur peut-il contrôler les connexions VPN des télétravailleurs ?

Oui, sous réserve d'une finalité légitime (sécurité du SI, traçabilité des accès), de la proportionnalité et d'une limitation aux données techniques (horodatage, durée, IP source). L'accès au contenu des communications et toute analyse comportementale sont interdits.

Quelles données peut-on collecter lors d'un contrôle VPN ?

Uniquement les métadonnées techniques : horodatage, durée, adresse IP source et applications consultées. La cartographie comportementale, le profilage individuel et l'accès au contenu des communications sont disproportionnés et illicites au regard du RGPD.

Quelles sanctions en cas de contrôle VPN non documenté ?

Amendes administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial et sanctions pénales (article L.261-2 du Code du travail). Les preuves issues d'un contrôle non documenté sont écartées par le tribunal du travail.

Une AIPD est-elle nécessaire pour le contrôle des connexions VPN ?

Oui, si le traitement présente un risque élevé pour les droits des salariés (article 35 RGPD). La consultation de la délégation du personnel (L.414-9) est obligatoire pour les entreprises d'au moins 150 salariés.

Conditions d’exercice

Le contrôle se limite aux métadonnées techniques : tout accès au contenu des communications ou cartographie du comportement est disproportionné et illicite.

Condition	Exigence
Finalité limitative	Sécurité du SI, traçabilité des accès aux applications — exclu : contrôle de la productivité
Métadonnées uniquement	Horodatage, durée, IP source, applications consultées — pas de contenu
Proportionnalité	Pas de profilage individuel ni de cartographie comportementale
Information préalable	Notice individuelle écrite avant la mise en service
Consultation	Délégation du personnel (L.414-9) ou ITM à défaut

Modalités pratiques

Les logs de connexion sont conservés généralement 6 à 12 mois ; au-delà, la conservation doit être justifiée précisément et inscrite au registre des traitements.

Démarche	Précision
Notice individuelle	Finalité, données, durée, destinataires, droits, distinction professionnel/privé
Charte informatique	Encadrement de l'usage du VPN et règles de cybersurveillance
Procès-verbal délégation	Consultation préalable (L.414-9)
AIPD	Obligatoire si risque élevé (article 35 RGPD)
Registre des traitements	Article 30 RGPD
Conservation	6 à 12 mois en principe, justification documentée au-delà
Habilitation	Liste nominative avec traçabilité des consultations

Pratiques et recommandations

Limiter strictement la collecte aux métadonnées techniques nécessaires à la sécurité du SI.

Documenter la base juridique retenue (intérêt légitime ou exécution du contrat) et le test de mise en balance.

Exclure tout accès au contenu des communications et toute analyse comportementale.

Sécuriser les logs par chiffrement, authentification forte et journalisation des consultations.

Anonymiser ou pseudonymiser les logs pour les analyses statistiques globales.

Réviser annuellement la durée de conservation et la pertinence avec la délégation du personnel.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Surveillance des salariés (loi du 1er août 2018)
Art. L.261-2 du Code du travail	Sanctions pénales
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel
Loi modifiée du 1er août 2018	Protection des données personnelles
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 12-13, 30, 32, 35
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

L'absence d'information préalable rend le contrôle illicite, même justifié par la sécurité informatique. L'employeur s'expose à des amendes administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial et à des sanctions pénales (L.261-2). Les preuves issues d'un contrôle non documenté sont écartées par le tribunal du travail.