Comment articuler cybersurveillance et politique de sécurité informatique en entreprise ?

Réponse courte

La **cybersurveillance** doit s'inscrire dans une politique de **sécurité informatique** formalisée et opposable, fondée sur une finalité légitime parmi celles reconnues par l'article L.261-1 du Code du travail. La politique distingue clairement les outils de protection technique (antivirus, journalisation, pare-feu) des dispositifs de contrôle individuel des salariés, et précise les hypothèses de déclenchement, les périmètres et les habilitations.

L'articulation impose la consultation de la **délégation du personnel** (L.414-9), une charte informatique opposable, une AIPD pour les outils intrusifs (article 35 RGPD), un registre des traitements complet et une transparence sur les durées de conservation. Sans cette documentation, le dispositif est illicite et les données collectées sont irrecevables, indépendamment de la justification technique.

Définition

La **cybersurveillance** regroupe l'ensemble des dispositifs techniques permettant le contrôle de l'utilisation des outils informatiques mis à disposition des salariés (filtrage web, journalisation des accès, monitoring des connexions, DLP, EDR).

Elle constitue un **traitement de données à caractère personnel** au sens du RGPD et doit s'inscrire dans une **politique de sécurité informatique** documentée définissant les règles d'utilisation des ressources numériques, les outils de protection et les hypothèses de contrôle individuel.

Questions fréquentes

Combien de temps conserver les logs de cybersurveillance au Luxembourg ?

Les logs se conservent généralement entre 6 et 12 mois maximum selon la finalité. Au-delà, la conservation doit être justifiée précisément dans le registre des traitements (article 30 RGPD).

Comment articuler cybersurveillance et politique de sécurité informatique en entreprise au Luxembourg ?

La cybersurveillance doit s'inscrire dans une politique formalisée et opposable, fondée sur une finalité légitime de l'article L.261-1 du Code du travail, distinguant les outils de protection technique des dispositifs de contrôle individuel.

Faut-il distinguer outils de sécurité et outils de contrôle individuel ?

Oui, la politique doit clairement séparer les outils de protection automatique (antivirus, pare-feu, journalisation) des dispositifs de contrôle individuel ciblé. Confondre les deux expose l'employeur à voir l'ensemble du dispositif jugé illicite.

Quand la désignation d'un DPO devient-elle obligatoire pour la cybersurveillance ?

La désignation d'un DPO est obligatoire si le traitement est systématique à grande échelle, conformément à l'article 37 du RGPD. Elle s'impose pour la plupart des dispositifs de cybersurveillance permanents.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Que risque l'employeur sans politique de cybersurveillance formalisée ?

Sans politique formalisée, charte informatique ou consultation préalable, le dispositif est illicite et les données inexploitables, y compris en contentieux disciplinaire. Les sanctions RGPD peuvent atteindre 20 millions € ou 4 % du chiffre d'affaires mondial.

Une AIPD est-elle obligatoire pour les outils de cybersurveillance ?

Oui, l'AIPD est obligatoire pour les outils intrusifs comme DLP, EDR ou monitoring continu, conformément à l'article 35 du RGPD. Elle s'ajoute à la consultation de la délégation du personnel (L.414-9).

Conditions d’exercice

La politique de sécurité doit distinguer la protection automatique du système (légitime par défaut) du contrôle individuel ciblé (soumis à motif et proportionnalité) ; confondre les deux expose l'employeur à voir l'ensemble du dispositif jugé illicite.

Condition	Exigence
Finalité légitime	Sécurité du SI, protection des biens, prévention d'actes illicites, conformité réglementaire
Distinction sécurité/contrôle individuel	Outils techniques globaux séparés des contrôles individuels, traçables séparément
Politique formalisée	Charte informatique opposable, signée ou affichée, diffusée à tous les salariés
Consultation délégation	Co-décision pour les entreprises ? 150 salariés (L.414-9) avant déploiement
AIPD	Obligatoire pour les outils intrusifs (DLP, monitoring continu) — article 35 RGPD
Proportionnalité	Mesures graduées, contrôles ponctuels privilégiés, surveillance permanente exclue

Modalités pratiques

Les logs de connexion et de cybersurveillance se conservent pour la durée strictement nécessaire à la finalité, généralement 6 à 12 mois ; au-delà, la conservation doit être justifiée précisément dans le registre.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Démarche	Précision
Politique de sécurité écrite	Document formalisant les outils, finalités et règles de gestion
Charte informatique	Volet salariés de la politique, opposable, diffusée et tracée
AIPD	Pour les dispositifs intrusifs (DLP, EDR, monitoring) — article 35 RGPD
Registre des traitements	Inscription distincte de chaque outil de cybersurveillance (article 30 RGPD)
Habilitations	Liste nominative des accès aux logs avec journalisation des consultations
Durée de conservation	Logs : 6 à 12 mois maximum selon finalité, justifiée dans le registre
DPO	Désignation obligatoire si traitement systématique à grande échelle (article 37 RGPD)

Pratiques et recommandations

Distinguer dans la politique les outils de sécurité globale (antivirus, pare-feu) des dispositifs de contrôle individuel.

Privilégier des contrôles ponctuels et ciblés sur indices objectifs plutôt que des surveillances systématiques.

Former régulièrement le personnel aux règles de sécurité et aux usages autorisés des ressources numériques.

Réviser annuellement la politique de cybersurveillance pour intégrer les évolutions technologiques.

Documenter chaque modification du dispositif dans le registre des traitements avec horodatage.

Prévoir une procédure graduée d'incident incluant l'information du DPO et la traçabilité des accès.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
Art. L.261-2 du Code du travail	Sanctions pénales en cas de violation
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel pour les installations de contrôle
Art. L.312-1 du Code du travail	Obligation générale de sécurité (peut justifier certains outils techniques)
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 30, 32, 35, 37

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

L'absence de politique formalisée, de charte informatique ou de consultation préalable rend le dispositif illicite et les données inexploitables, y compris en cas de contentieux disciplinaire. Les sanctions administratives RGPD peuvent atteindre 20 millions € ou 4 % du chiffre d'affaires mondial.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.