Un audit informatique peut-il fournir une preuve opposable au salarié ?

Réponse courte

Oui, si le dispositif qui a produit les données était régulier — c'est la seule condition qui compte.

Un audit informatique qui analyse l'activité de salariés identifiables constitue un traitement de données à des fins de **surveillance** au sens de l'article L.261-1. Il suppose donc une base de licéité tirée de l'article 6 du RGPD, et surtout l'**information préalable** de la délégation du personnel — ou, à défaut de délégation, de l'ITM. Cette information doit décrire la finalité, les modalités, la durée de conservation, et comporter un engagement de ne pas utiliser les données à d'autres fins.

Un audit conduit pour vérifier la sécurité du système et dont les résultats servent ensuite à sanctionner un salarié illustre exactement ce que l'engagement interdit : le **détournement de finalité**. Si un nouvel usage devient nécessaire, l'information préalable doit être refaite.

Définition

L'**audit informatique** examine les systèmes, les journaux de connexion, les accès et les flux. Il devient un traitement soumis à L.261-1 dès lors qu'il permet d'identifier des personnes et porte sur leur activité.

Le **détournement de finalité** consiste à utiliser des données collectées pour un objectif donné à une fin différente. C'est le manquement le plus fréquent et le plus efficacement invoqué par les salariés.

Questions fréquentes

Comment régulariser un usage nouveau de données déjà collectées ?

En refaisant l'information préalable pour la nouvelle finalité, avant toute exploitation. La régularisation postérieure ne rattrape pas les pièces déjà obtenues.

Les résultats d'un audit informatique peuvent-ils justifier une sanction ?

Oui, si le dispositif qui a produit les données était régulier. C'est la régularité du traitement, non la fiabilité technique, qui décide de la recevabilité.

Que doit contenir l'information préalable exigée avant un tel audit ?

La description de la finalité, des modalités, de la durée de conservation, et l'engagement de ne pas utiliser les données à d'autres fins.

Un audit de sécurité peut-il servir ensuite à sanctionner un salarié ?

Non sans nouvelle information préalable. Utiliser à des fins disciplinaires des données collectées pour vérifier la sécurité du système constitue un détournement de finalité.

Un audit portant sur l'activité de salariés identifiables relève-t-il de l'article L.261-1 ?

Oui. Il constitue un traitement de données à des fins de surveillance et suppose une base de licéité du RGPD ainsi que l'information préalable de la délégation ou de l'ITM.

Conditions d’exercice

La régularité de l'audit conditionne l'usage de ses résultats, non l'inverse.

Élément	Régime
Base de licéité	Article 6, paragraphe 1, lettres a) à f), du RGPD (L.261-1, §1)
Information préalable	Délégation du personnel, à défaut l'ITM (L.261-1, §2)
Contenu de l'information	Finalité, modalités, durée de conservation, engagement de non-détournement
Codécision	Requise pour la sécurité et la santé et le contrôle de production (§3)
Saisine de la CNPD	Dans les quinze jours suivant l'information, avec effet suspensif (§4)
Détournement de finalité	Rend l'usage contestable, même si l'audit était régulier
Sanction pénale	Huit jours à un an d'emprisonnement et 251 à 125 000 euros d'amende (L.261-2)

Modalités pratiques

Un audit exploitable se prépare comme un traitement, pas comme une intervention technique.

Étape	Détail
Définition de la finalité	L'écrire avant l'audit : elle bornera tous les usages ultérieurs
Information de la délégation	Transmettre le document complet et conserver la preuve de sa remise
Délai de quinze jours	Attendre l'expiration du délai de saisine de la CNPD
Périmètre	Limiter l'audit aux systèmes et périodes nécessaires
Anonymisation	Travailler sur données agrégées tant que l'identification n'est pas nécessaire
Traçabilité	Documenter qui a accédé à quoi, quand et à quel titre
Nouvel usage	Refaire l'information préalable avant d'exploiter les données à une autre fin

Pratiques et recommandations

L'audit de sécurité qui devient un audit disciplinaire est le scénario type. Une entreprise mandate un prestataire pour vérifier ses accès, découvre des consultations anormales, et s'en sert pour licencier. La finalité annoncée était la sécurité ; l'usage disciplinaire ne s'y rattache pas, et l'engagement formel de non-détournement exigé par L.261-1 rend la pièce contestable.

Travaillez d'abord sur données agrégées. Un audit qui identifie une anomalie sans nommer personne, puis fait l'objet d'une information préalable spécifique avant l'étape d'identification, se défend beaucoup mieux qu'une analyse nominative d'emblée.

Conservez la preuve de l'information, pas seulement le rapport d'audit. C'est elle que le salarié réclamera, et son absence suffit souvent à faire écarter les conclusions les mieux établies techniquement.

Cadre juridique

Référence	Objet
Art. L.261-1, paragraphe (1)	Surveillance admise dans les seuls cas de l'article 6, §1, a) à f), du RGPD
Art. L.261-1, paragraphe (2)	Information préalable : finalité, modalités, durée, engagement de non-détournement
Art. L.261-1, paragraphe (3)	Codécision pour la sécurité et la santé et le contrôle de production
Art. L.261-1, paragraphe (4)	Saisine de la CNPD dans les quinze jours, avis dans le mois, effet suspensif
Art. L.261-2	Sanction pénale du traitement irrégulier et cessation sous astreinte
Loi du 1er août 2018	Organisation de la CNPD et mise en œuvre du RGPD ; la loi du 2 août 2002 est abrogée

Un audit informatique portant sur l'activité de salariés identifiables est un traitement de surveillance au sens de L.261-1 : sans information préalable, ses conclusions sont contestables. Le détournement de finalité — audit de sécurité exploité à des fins disciplinaires — est le manquement le plus fréquent.