

Comment démontrer le caractère excessif d'un dispositif de contrôle ?

Réponse courte

Un dispositif de contrôle est qualifié d'**excessif** s'il dépasse ce qui est strictement nécessaire à sa finalité, en violant les principes de **nécessité**, de **proportionnalité** ou de **minimisation** posés par l'article 5 du RGPD. La démonstration repose sur l'évaluation de la proportionnalité de la cybersurveillance au regard de la nature, de l'étendue, de la durée et de la fréquence du contrôle, ainsi que sur l'existence d'**alternatives moins intrusives**.

Le défaut d'**AIPD**, l'absence de **consultation** de la délégation, le défaut d'information préalable et le dépassement de la durée de conservation des images sans justification sont des indices d'excès. Le salarié ou la délégation peut saisir la **CNPD** ou le tribunal du travail. La charge de la preuve de la conformité incombe au responsable de traitement (**accountability**, article 24 RGPD).

Définition

Le **caractère excessif** d'un dispositif de contrôle s'apprécie au regard des trois critères cumulatifs : la **finalité légitime**, la **nécessité** (aucun moyen moins intrusif disponible) et la **proportionnalité** (équilibre entre objectif et atteinte aux droits du salarié).

L'excès peut résulter du **périmètre** (zones surveillées trop larges), de la **durée** (conservation excessive), de la **technologie** (intrusion injustifiée) ou des **destinataires** (diffusion à des personnes non habilitées).

Questions fréquentes

Comment savoir si un dispositif de surveillance est excessif ?

Un dispositif est excessif s'il dépasse ce qui est strictement nécessaire à sa finalité, en violant les principes de nécessité, proportionnalité ou minimisation (article 5 RGPD). L'analyse porte sur la nature, l'étendue, la durée et la fréquence du contrôle.

L'absence d'AIPD suffit-elle à invalider un dispositif de surveillance ?

Oui, l'absence d'AIPD pour un dispositif présentant un risque élevé constitue à elle seule un manquement sanctionnable jusqu'à 10 M€ ou 2 % du CA (articles 35 et 83 §4 RGPD), indépendamment du caractère excessif du dispositif.

Les keyloggers et l'IA prédictive sont-ils autorisés sur les postes de travail ?

Ces technologies (keyloggers, biométrie, IA prédictive) sont presque toujours disproportionnées sans nécessité avérée. Leur déploiement constitue un indice d'excès et expose à des sanctions RGPD ainsi qu'à l'irrecevabilité des preuves recueillies.

Quels critères doit respecter un contrôle pour être proportionné ?

Le périmètre, la durée et l'intensité doivent être ajustés à l'objectif. Une finalité légitime, l'absence de moyen moins intrusif et une diffusion limitée aux personnes habilitées sont les critères cumulatifs de proportionnalité retenus.

Qui doit prouver la conformité d'un dispositif de surveillance ?

Le principe d'**accountability** (article 24 RGPD) renverse la charge de la preuve : c'est à l'employeur de démontrer la conformité, non au salarié de prouver l'excès. À défaut, la non-conformité est présumée par la CNPD et le tribunal.

Une conservation des images au-delà de 30 jours est-elle excessive ?

Oui, la conservation au-delà de 30 jours sans justification documentée constitue un indice d'excès, contraire à l'article 5 §1 e) du RGPD. La durée doit toujours être strictement proportionnée à la finalité poursuivie.

Une décision automatisée prise sur la base du dispositif est-elle valable ?

Non, sans encadrement humain. L'article 22 du RGPD impose une intervention humaine pour toute décision automatisée. Sa violation constitue un manquement sanctionnable, et la décision peut être annulée par le tribunal du travail.

Conditions d'exercice

Le principe d'accountability (article 24 RGPD) renverse la charge de la preuve : c'est à l'employeur de démontrer la conformité, non au salarié de prouver l'excès en détail.

Critère	Indice d'excès
Périmètre	Zones de vie privée filmées, surveillance généralisée des postes
Durée	Conservation au-delà de 30 jours sans justification documentée
Technologie	Keyloggers, biométrie, IA prédictive sans nécessité avérée
Destinataires	Communication à des tiers non habilités ou non autorisés
Alternatives	Existence de moyens moins intrusifs pour atteindre la finalité

Modalités pratiques

L'absence d'AIPD pour un dispositif susceptible de présenter un risque élevé constitue à elle seule un manquement sanctionnable, indépendamment du caractère excessif du dispositif lui-même.

Manquement	Conséquence
Pas d'AIPD préalable	Sanction RGPD jusqu'à 10 M€ ou 2 % CA (articles 35 et 83 §4 RGPD)
Pas de consultation délégation	Procédure illicite, contestable par la délégation et l' <u>ITM</u>
Pas d'information individuelle	Manquement aux articles 12-13 RGPD, sanction administrative
Conservation excessive	Manquement à l'article 5 §1 e) RGPD
Surveillance généralisée	Disproportion manifeste, irrecevabilité des preuves
Détournement de finalité	Sanction pénale <u>L.261-2</u> + RGPD cumulées
Décision automatisée seule	Manquement à l'article 22 RGPD (encadrement humain)

Pratiques et recommandations

Documenter par écrit chaque finalité, la nécessité et l'absence d'alternative moins intrusive avant déploiement.

Limiter la durée de conservation au strict nécessaire et justifier chaque dépassement par écrit.

Éviter les dispositifs intrusifs (keyloggers, captures d'écran systématiques, biométrie) sauf nécessité impérieuse.

Réviser annuellement la pertinence du dispositif avec la délégation et le DPO.

Saisir la CNPD pour avis préalable en cas de doute sur la conformité d'un dispositif.

Privilégier les contrôles ciblés et ponctuels plutôt que la surveillance permanente et généralisée.

Cadre juridique

Référence	Objet
Art. <u>L.261-1</u> du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
Art. <u>L.261-2</u> du Code du travail	Sanctions pénales en cas de violation
Art. <u>L.414-9</u> du Code du travail	Co-décision de la délégation du personnel pour les installations de contrôle
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Art. 5, 6, 22, 24, 35, 83 du RGPD	Principes, licéité, encadrement humain, accountability, AIPD, sanctions
Lignes directrices CNPD	Surveillance sur le lieu de travail

La charge de prouver la conformité incombe à l'employeur (accountability, article 24 RGPD) : il doit pouvoir produire l'AIPD, le procès-verbal de consultation, les notices d'information et le registre des traitements. À défaut, le tribunal du travail et la CNPD présument la non-conformité. Les preuves issues d'un dispositif jugé excessif sont irrecevables et toute sanction disciplinaire fondée sur ces preuves est annulable.

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.