

LIBERTÉS INDIVIDUELLES

Faute grave : la preuve issue d'un système de vidéoprotection conforme au RGPD est recevable

Dans un arrêt du 21 mai 2025, la Cour de cassation souligne que **des images issues d'un dispositif de vidéoprotection, n'ayant pas pour finalité première de contrôler l'activité des salariés mais d'assurer la sécurité des personnes et des biens, peuvent être utilisées à des fins disciplinaires en cas de manquement aux règles de sécurité, dès lors que le système répond aux exigences du règlement général sur la protection des données (RGPD).**

Si l'employeur peut recourir aux images issues d'un système de vidéosurveillance pour fonder une sanction disciplinaire, encore faut-il que le dispositif dont est issue cette preuve ne porte pas une atteinte disproportionnée aux droits et libertés des personnes, eu égard aux finalités poursuivies (*C. trav., art. L. 1121-1*) et aux règles imposées par le RGPD. En effet, un tel dispositif doit respecter les principes de finalité, de transparence et de proportionnalité prévus par le RGPD, tout en satisfaisant aux exigences du droit du travail, qui imposent d'informer le salarié de son existence (*C. trav., art. L. 1222-4*) et de consulter le comité social et économique (*C. trav., art. L. 2312-38*). C'est ce que juge la Cour de cassation dans un arrêt du 21 mai 2025, dans lequel elle admet la recevabilité d'une preuve tirée du système de vidéoprotection d'un aéroport, produite pour établir un manquement aux règles de sécurité commis par un agent de sûreté n'ayant pas contrôlé un bagage.

Manquement aux règles de sécurité révélé par la vidéoprotection

L'affaire concernait un agent de sûreté aéroportuaire, licencié pour faute grave. Affecté au contrôle des bagages cabine lors de leur passage sous rayon X, il avait laissé passer deux valises sans procéder à leur inspection, en violation des procédures en vigueur. Pour justifier la sanction, l'employeur s'était appuyé sur des images extraites du système de vidéosurveillance de l'aéroport, sur lesquelles le salarié apparaissait en pleine discussion avec un passager, tandis que le tapis d'inspection des bagages défilait sans qu'aucune vérification ne soit effectuée.

Le salarié avait saisi la juridiction prud'homale en contestant la validité de cette preuve. Il soutenait que le **dispositif de vidéosurveillance, mis en place pour assurer la sécurité des personnes et des biens, avait été utilisé à des fins disciplinaires** sans respect des garanties prévues par le RGPD. Il reprochait notamment à l'employeur de ne pas l'avoir informé des finalités du traitement, ni d'avoir consulté les représentants du personnel. Ses arguments ont été écartés par la cour d'appel. Il a alors porté l'affaire devant la Cour de cassation, en vain.

Traitement de données à caractère personnel soumis au RGPD

Pour apprécier la recevabilité de la preuve, la Cour de cassation rappelle qu'en vertu de l'article 4 du RGPD,

un dispositif de vidéosurveillance constitue un traitement de données à caractère personnel dès lors qu'il permet d'identifier un salarié. Elle précise ainsi qu'en l'espèce : « l'utilisation de constats et attestations réalisés à partir de la captation et du visionnage des images issues du **système de vidéoprotection** de l'aéroport constitue un **traitement de données à caractère personnel** au sens de l'article 4 du RGPD, de sorte que l'**employeur des opérateurs de sûreté** affectés au contrôle des bagages est tenu au **respect** des obligations instituées par les dispositions des articles 5, 6, 13 et 14 du RGPD ». Celles-ci imposent notamment que :

- les données soient **traitées** de manière licite, loyale et **transparente** au regard de la personne concernée, qu'elles soient collectées pour des **finalités déterminées**, explicites et légitimes sans pouvoir être traitées ultérieurement d'une manière **incompatible** avec ces finalités (article 5) ;
- le traitement réponde à l'une des conditions de licéité, dont notamment la sauvegarde des intérêts vitaux des personnes (article 6) ;
- et que la personne concernée soit **informée** des **finalités** du traitement ainsi que de son **droit d'accès** à ses données (articles 13 et 14).

C'est donc à l'aune de ces exigences que la Cour de cassation va examiner le dispositif de vidéosurveillance, et, contrairement à ce que soutenait le salarié, relevé qu'il y était bien conforme.

Dispositif régulièrement mis en place et porté à la connaissance des salariés

La Cour de cassation relève que l'employeur avait respecté les formalités requises lors de l'installation du dispositif de **vidéoprotection**. En effet :

- celui-ci avait été **déclaré** à la Cnil (Commission nationale de l'informatique et des libertés), conformément aux exigences alors en vigueur, et avait été autorisé par **arrêté préfectoral** ;
- installé dans un lieu public et concernant donc tant les clients que les **salariés**, son existence avait été portée à la connaissance des salariés de manière visible et accessible, par un **affichage** sous forme de pictogramme précisant son emplacement et les droits d'accès aux enregistrements ;
- les **représentants du personnel** avaient été informés du recours à la vidéoprotection ;
- l'**accès** aux images issues de la vidéosurveillance était strictement réservé à un **nombre limité** de personnes

habilitées, assurant ainsi la protection et la confidentialité des données personnelles, conformément à l'article 5 du RGPD, qui impose un traitement garantissant une protection appropriée contre tout accès non autorisé ou illicite. Par ailleurs, la **durée de conservation** des enregistrements, limitée à **cinq jours**, était elle aussi conforme à l'article 5, qui interdit de conserver les données plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées.

La Cour en déduit que « les données à caractère personnel concernant le salarié avaient été **collectées** pour des **finalités déterminées et légitimes**, à savoir assurer la **sécurité des personnes** et des **biens** dans l'enceinte d'un aéroport international, et avaient été **traitées** ultérieurement, tant par la société exploitant l'aéroport que par l'employeur, d'une **manière compatible** avec ces **finalités**, le salarié ayant été informé des finalités du dispositif de contrôle et

de son droit d'accès aux enregistrements le concernant ».

Le traitement respectait ainsi les principes de transparence, de proportionnalité et de limitation, tels que l'exige le RGPD. Dans ces conditions, la Cour conclut que « les **moyens de preuve** tirés de l'exploitation des images captées et enregistrées le jour des faits étaient **recevables** ».

Le licenciement pour **faute grave** a également été validé, malgré les 16 années d'ancienneté du salarié : le filtrage systématique des bagages figurait parmi ses **missions** contractuelles essentielles concourant « à **garantir la sécurité** du personnel, des passagers et des installations », et son manquement rendait impossible son maintien dans l'entreprise, même en l'absence d'antécédents disciplinaires. ■

Cass. soc., 21 mai 2025, n°22-19.925 FS-B



CONSULTER LE DOCUMENT SUR :
www.ilsens-sociales.fr