Conservation des données des employés : oui, mais pas Milan

David Dias Matos, le 18 septembre 2025

Le *Garante* italien s'est prononcé sur la conservation des métadonnées de messagerie et des journaux de navigation par la Région Lombardie. L'Autorité a considéré que ces pratiques, en l'absence d'accord syndical et de limitation stricte des durées, constituaient un contrôle illicite de l'activité des employés.

Décision n. 10134221 de la *Garante per la protezione dei dati personali* du 29 avril 2025

Enquête du *Garante*

En avril 2025, l'Autorité italienne de protection des données (*Garante per la protezione dei dati personali*) prononce une mesure contre l'autorité régionale lombarde (Région Lombardie) à la suite d'une enquête. Cette dernière visait l'utilisation d'outils informatiques et la gestion des données personnelles des employés, y compris dans le cadre du télétravail. L'affaire concerne principalement la conservation des métadonnées liées à la messagerie électronique et des journaux de navigation (prosaïquement : l'historique) internet.

L'enquête révèle que la Région conservait les métadonnées de la messagerie électronique (date et heure, expéditeur, destinataire, objet, statut de l'envoi, taille et identifiant) pendant 90 jours. De même, tous les *logs* de navigation internet, y compris les tentatives d'accès à des sites interdits listés dans une « *blacklist* », étaient enregistrés et conservés durant douze mois.

Enfin, ces traitements avaient été mis en œuvre sans la réalisation préalable d'une analyse d'impact relative à la protection des données (AIPD), pourtant exigée par l'art. 35 RGPD.

Réponse lombarde

Suite à l'enquête, la Région Lombardie rétorque en expliquant que ces traitements avaient exclusivement des finalités techniques et de cybersécurité, notamment la détection d'attaques informatiques, la prévention d'intrusions et le maintien du fonctionnement des systèmes de messagerie.

Selon elle, les données n'ont jamais été utilisées pour surveiller ou sanctionner directement

les employés. La Région soutient également que la durée de conservation de nonante jours des métadonnées de messagerie découlent des réglages par défaut de la messagerie et que ces informations sont nécessaires pour garantir une assistance efficace en cas de problème d'envoi des messages.

Pour répondre au reproche que les unions syndicales n'ont pas été consultées, la Région invoque le droit du travail italien qui permet l'utilisation des outils nécessaires à l'exécution du travail sans accord syndical préalable. Elle considère que la messagerie électronique et l'ordinateur constituent de tels outils.

Quant aux logs de navigation, elle fait valoir que l'identification d'un fonctionnaire ne pouvait intervenir qu'à travers la coopération de trois prestataires distincts, chacun détenant une partie de l'information (adresse IP, adresse MAC, identité de l'utilisateur). Cela empêchait tout contrôle direct et continu. Elle justifie enfin la longue durée de conservation par la nécessité d'analyser des attaques persistantes (*APT*, *ransomware*).

Au cours de l'enquête, la Région Lombardie adapte toutefois ses pratiques. Elle signe des accords syndicaux distincts pour le personnel dirigeant et non dirigeant. Elle met à jour sa réglementation interne sur l'utilisation des outils informatiques. Elle amorce des processus d'anonymisation à l'interne. Elle formalise, par un avenant au contrat, la relation avec les prestataires techniques. Enfin, elle procède à la réalisation d'une analyse d'impact, conformément à l'art. 35 RGPD.

Conclusions de l'enquête

Dans son analyse, le *Garante* reconnait les efforts de régularisation mais souligne, à juste titre que, pendant une période prolongée, la Région avait traité les données de ses employés en violation du RGPD et du droit italien de la protection des données. La conservation généralisée des métadonnées de messagerie pendant nonante jours ne peut être justifiée par l'exception contenue dans le droit du travail italien.

Selon le *Garante*, seule une conservation très limitée dans le temps, soit moins de vingt et un jours, peut être considérée comme admissible et nécessaire au fonctionnement des outils de travail au sens strict. Au-delà, il s'agit d'une surveillance à distance (« *controlli in distenza* »), nécessitant un accord syndical ou une autorisation administrative préalable prévue par l'ordre interne italien en lien avec les articles 5, 6 et 88 RGPD.

S'agissant des *logs* internet, l'Autorité rappelle que leur collecte systématique, y compris

celle des tentatives d'accès à des sites interdits, peut révéler des éléments de la vie privée des employés et donc constituer un traitement de données disproportionné.

La conservation de l'historique pendant douze mois est jugée disproportionnée au regard des principes de minimisation et de limitation de la conservation (art. 5 par. 1 let. c et e RGPD). Même si les données sont séparées entre plusieurs prestataires, la possibilité de recoupement permet *in fine* de rattacher les *logs* à un individu identifiable, ce qui engage la responsabilité de la Région en tant que responsable du traitement.

Enfin, le *Garante* relève que l'analyse d'impact faisait défaut, alors que la nature des traitements (surveillance potentielle des employés, conservation étendue, données touchant à la vie privée) remplissait les critères d'un risque élevé au sens de l'art. 35 RGPD conduisant à la nécessité pour le responsable du traitement de procéder à une telle analyse.

En conséquence, le *Garante* conclut que la Région a violé plusieurs dispositions du droit de la protection des données. En font partie, les principes de licéité, loyauté, minimisation et limitation de la conservation (art. 5 RGPD), le principe de licéité pour le traitement des données des travailleurs (art. 6 et 88 RGPD), le principe de protection des données dès la conception et par défaut (art. 25 RGPD) et l'obligation de réaliser une AIPD (art. 35 RGPD).

L'autorité lombarde est mise en demeure, en particulier, de réduire significativement les durées de conservation pour les métadonnées et les *logs*, ainsi que de garantir une information claire des employés conformément à l'art. 13 RGPD.

Leçons à tirer

Cette décision rappelle que la messagerie électronique et la navigation Internet ne peuvent pas être considérées comme de simples outils de travail, car leur utilisation entraîne inévitablement la création de données personnelles. Conservées et analysées, elles permettent un contrôle indirect de l'activité des employés.

Elle met également en évidence que les impératifs de cybersécurité, aussi légitimes soient-ils, ne sauraient justifier une conservation excessive ou indéfinie de ces informations. La durée de conservation doit toujours rester limitée au strict nécessaire et être encadrée par des garanties appropriées afin d'éviter tout risque de surveillance disproportionnée.

Et en Suisse ?

Le travailleur en Suisse est également protégé contre la surveillance de son comportement. Cette protection découle à la fois de l'art. 328 CO, qui garantit le respect de sa personnalité, et de l'art. 26 OLT 3, qui interdit les systèmes de contrôle portant sur le comportement des employés.

L'installation d'un système technique de surveillance ou de contrôle est admissible uniquement s'il est nécessaire pour d'autres raisons (telles que la sécurité, la qualité ou le contrôle du rendement). Lors de sa mise en place, il est cependant nécessaire de prendre en compte l'employé, afin de s'assurer de la protection de sa personnalité et de sa santé.

En définitive, l'implémentation d'un système de surveillance doit se faire avec la participation de l'employé, aussi bien pour satisfaire les obligations légales que morales.

Proposition de citation : David Dias Matos, Conservation des données des employés : oui, mais pas Milan, 18 septembre 2025 *in* www.swissprivacy.law/372