Le profilage algorithmique des salariés peut-il enfreindre le droit pénal ?

Réponse courte

Le profilage algorithmique des salariés peut enfreindre le droit pénal si l'employeur ne respecte pas les obligations légales encadrant le traitement des données à caractère personnel. Sont notamment sanctionnés pénalement la collecte frauduleuse, la conservation illicite, la divulgation non autorisée de données, l'absence d'information individuelle et écrite des salariés, ou le non-respect de leurs droits d'accès, de rectification, d'effacement, de limitation, d'opposition et de portabilité.

Toute utilisation abusive, détournée ou discriminatoire du profilage, ainsi que toute atteinte à la vie privée ou discrimination fondée sur des critères prohibés, constitue également une infraction pénale. Le Code pénal luxembourgeois, la loi du 1er août 2018 et le Code du travail prévoient des sanctions en cas de traitement illicite ou de non-respect des droits des salariés. L'obligation de consultation préalable de la délégation du personnel s'applique à tout dispositif de surveillance ou de collecte automatisée de données.

Définition

Le profilage algorithmique des salariés désigne l'utilisation de procédés automatisés, reposant sur des algorithmes, pour analyser, évaluer ou prédire des aspects relatifs à la performance, au comportement ou à la personnalité des salariés. Cette pratique implique le traitement de données à caractère personnel, parfois sensibles, collectées dans le cadre de la relation de travail.

Au Luxembourg, le profilage algorithmique est encadré par des dispositions spécifiques du Code du travail, de la loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, ainsi que par le Code pénal. Toute collecte de données doit être strictement limitée aux finalités nécessaires à l'exécution du contrat de travail ou à l'exercice des droits et obligations des parties, conformément à l'article L.261-1(2) du Code du travail.

La collecte ou le traitement de données sensibles (état de santé, opinions politiques, convictions religieuses, etc.) est interdit, sauf exceptions strictement prévues par l'article 9 du RGPD et l'article 6 de la loi du 1er août 2018. Toute exception doit être documentée et justifiée.

Conditions d'exercice

Le recours au profilage algorithmique en milieu professionnel est soumis à des conditions strictes. Le traitement doit être justifié par une finalité légitime, proportionnée et transparente. L'employeur doit informer individuellement et par écrit chaque salarié, avant toute mise en œuvre d'un dispositif de collecte automatisée de données, sur :

- l’identité et les coordonnées du responsable du traitement,
- la finalité du traitement,
- la base légale,
- les destinataires des données,
- la durée de conservation,
- l’existence d’un transfert hors UE,
- les droits des personnes concernées (accès, rectification, effacement, limitation, opposition, portabilité).

Cette obligation d’information découle de l’article L.261-1(3) du Code du travail et de l’article 13 du RGPD.

La consultation préalable de la délégation du personnel est obligatoire pour tout dispositif de surveillance ou de collecte automatisée de données concernant les salariés, y compris le profilage algorithmique, conformément à l’article L.261-1(4) du Code du travail. Toute collecte ou traitement de données doit reposer sur une base légale, telle que l’exécution du contrat de travail ou le respect d’une obligation légale.

L’employeur doit garantir l’accès, la rectification, l’effacement, la limitation, l’opposition et la portabilité des données pour chaque salarié, conformément à l’article 15 et suivants du RGPD et à l’article L.261-1(3) du Code du travail.

Modalités pratiques

Avant toute mise en œuvre d’un dispositif de profilage algorithmique, l’employeur doit réaliser une analyse d’impact relative à la protection des données lorsque le traitement est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes concernées.

Une déclaration ou une demande d’autorisation préalable auprès de la Commission nationale pour la protection des données (CNPD) est requise pour certains traitements automatisés, notamment ceux à grande échelle ou présentant un risque élevé (articles 23, 24, 26 et 27 de la loi du 1er août 2018).

L’employeur doit désigner un délégué à la protection des données (DPO) si l’activité principale consiste en des traitements nécessitant un suivi régulier et systématique à grande échelle, conformément à l’article 37 du RGPD et à l’article 38 de la loi du 1er août 2018.

Les salariés doivent être informés de manière claire sur la logique sous-jacente, l’importance et les conséquences du traitement. L’accès aux données doit être limité aux seules personnes habilitées. L’employeur doit garantir la sécurité et la confidentialité des données traitées, conformément à l’article 32 du RGPD.

Il est interdit de prendre une décision automatisée produisant des effets juridiques sans intervention humaine significative, sauf exceptions prévues par la loi (article 22 RGPD). La tenue d’un registre des activités de traitement est obligatoire pour l’employeur, conformément à l’article 30 du RGPD.

En cas de violation de données, l’employeur doit notifier la CNPD sans délai indu et, dans certains cas, informer les personnes concernées, conformément aux articles 33 et 34 du RGPD et à la loi du 1er août 2018.

Pratiques et recommandations

Il est recommandé de limiter le recours au profilage algorithmique aux situations strictement nécessaires et de privilégier la transparence dans la communication avec les salariés. La documentation des traitements, la consultation du délégué à la protection des données et la mise à jour régulière des politiques internes sont essentielles.

L'employeur doit consulter la délégation du personnel avant toute mise en œuvre de dispositifs de surveillance ou de collecte automatisée de données, y compris le profilage algorithmique. Toute utilisation abusive, détournée ou discriminatoire du profilage peut constituer une infraction pénale, notamment en cas d'atteinte à la vie privée, de collecte illicite de données ou de discrimination fondée sur des critères prohibés.

Il est impératif de garantir la sécurité et la confidentialité des données, de tenir un registre des traitements, de respecter l'obligation d'information individuelle des salariés et de permettre l'exercice effectif de leurs droits (accès, rectification, effacement, limitation, opposition, portabilité).

En cas de violation de données, l'employeur doit notifier la CNPD et, si nécessaire, les salariés concernés, conformément à la réglementation en vigueur.

Cadre juridique

Le Code pénal luxembourgeois sanctionne pénalement la collecte frauduleuse, la conservation illicite ou la divulgation non autorisée de données à caractère personnel. L'article 226-1 du Code pénal réprime l'atteinte volontaire à l'intimité de la vie privée par tout moyen, y compris automatisé.

La loi du 1er août 2018 prévoit des sanctions pénales en cas de traitement illicite de données, d'absence d'information des personnes concernées, ou de non-respect des droits d'accès, de rectification, d'effacement, de limitation, d'opposition et de portabilité. Les articles 23, 24, 26 et 27 de cette loi imposent l'obligation d'information de la CNPD et, selon les cas, une déclaration ou une autorisation préalable pour certains traitements automatisés.

L'article L.261-1(2) du Code du travail interdit toute collecte de données en dehors des finalités strictement nécessaires à l'exécution du contrat de travail ou à l'exercice des droits et obligations des parties. L'article L.261-1(3) impose l'information individuelle et écrite des salariés. L'article L.261-1(4) impose la consultation préalable de la délégation du personnel pour tout dispositif de surveillance ou de collecte automatisée de données.

La discrimination résultant d'un traitement algorithmique est également pénalement réprimée par les articles 454 et suivants du Code pénal. L'article 22 du RGPD, applicable via la loi du 1er août 2018, interdit la prise de décision automatisée sans intervention humaine significative, sauf exceptions légales. L'article 32 du RGPD impose la sécurité et la confidentialité des données, et l'article 30 du RGPD impose la tenue d'un registre des activités de traitement.

L'article 9 du RGPD et l'article 6 de la loi du 1er août 2018 interdisent la collecte ou le traitement de données sensibles, sauf exceptions strictement prévues. Les articles 33 et 34 du RGPD imposent la notification des violations de données à la CNPD et, dans certains cas, aux personnes concernées. L'article 37 du RGPD et l'article 38 de la loi

du 1er août 2018 imposent la désignation d’un DPO dans certains cas.

La jurisprudence nationale confirme l’application stricte de ces dispositions en matière de traitement automatisé des données des salariés.

Le recours au profilage algorithmique des salariés expose l’employeur à un risque pénal en cas de non-respect des obligations légales et réglementaires. Il est impératif d’auditer régulièrement les dispositifs utilisés, de documenter chaque traitement, de tenir un registre des activités de traitement et de solliciter un avis juridique spécialisé avant toute mise en œuvre ou évolution significative du dispositif.

L’employeur doit également garantir la sécurité et la confidentialité des données, informer individuellement et par écrit chaque salarié, consulter la délégation du personnel, permettre l’exercice effectif des droits des salariés sur leurs données, désigner un DPO si nécessaire, et effectuer les démarches requises auprès de la CNPD, notamment en cas de violation de données.