Les 10 grands principes pour la protection et la confidentialité des données des travailleurs

UNI Global Union

Nyon, Suisse

Les 10 grands principes pour la protection et la confidentialité des données des travailleurs

Introduction

Alors que les données, le "big data" et les jeux de données sont de plus en plus souvent utilises par les entreprises pour alimenter les décisions managériales, il n'existe quasiment pas de règles régissant le respect de la sphère privée et la protection des données des travailleurs. Le présent document présente 10 principes opérationnels qui visent à corriger ce déséquilibre. En proposant des revendications concrètes concernant la collecte et l'utilisation des données par les entreprises, ces principes responsabiliseront les travailleurs et garantiront que leurs données soient utilisées de manière éthique et durable. Il est urgent d'agir sans tarder pour préserver les intérêts des travailleurs et conserver un équilibre sain entre les forces en présence sur les lieux de travail. Les 10 principes énoncés dans le présent document ont été élaborés par UNI Global Union dans ce but.

Les données sont qualifiées de nouvel or. Elles sont négociées, analysées et utilisées dans le marketing, la publicité et la gestion des ressources humaines. Elles constituent également les pièces maîtresses de l'intelligence artificielle et des algorithmes. On estime que d'ici 2030, 15 à 20% du PIB combiné du monde viendra des flux de données. Celles-ci sont le fondement même de la myriade de nouvelles entreprises et de nouveaux services qui individualisent de plus en plus de nombreux aspects de notre économie et de notre société, à savoir les plateformes et l'économie collaborative.

En tant que citoyens, nous laissons chaque jour des pistes de données derrière nous : elles viennent de ce que nous recherchons sur Google, des applications que nous chargeons sur notre téléphone portable, des trajets que nous effectuons en taxi, des appartements que nous louons, des objets que nous achetons, de nos cartes de fidélité, de nos dossiers médiaux, des coups de téléphone que nous passons aux services clients. Sans même parler des endroits où nous nous rendons, des e-mails que nous envoyons, des amis que nous avons sur Facebook ou des tweets que nous écrivons. Toutes ces activités fournissent aux entreprises des données qui nous concernent, nous et notre réseau de connaissances. Les données sont tout simplement le plus grand cadeau que nous puissions offrir gratuitement sans même nous en rendre compte.

Nous fournissons également des données en notre qualité de travailleurs : nos CV, nos données biométriques telles que nos empreintes digitales ou rétiniennes, ainsi que les abondantes données tirées de la surveillance de nos flux de travail par notre employeur. Les données, ou plutôt les jeux de données venant de l'intérieur et de l'extérieur de l'entreprise, sont également utilisées par la direction pour prendre des décisions relevant des ressources humaines. Qui va être recruté ? Qui va bénéficier d'une promotion ? Faut-il licencier untel ou lui donner un avertissement ? Le personnel est-il productif aujourd'hui et sinon, pourquoi ? L'application et l'utilisation au sein des entreprises ont même poussé à se demander si les données ne retiraient pas aux ressources humaines leur volet humain.

Mais en réalité, qui est propriétaire des données que nous fournissons ? Et quels sont les données « en circulation » qui vous concernent, vous et moi ? Voilà deux questions auxquelles il est difficile de répondre. Le CEO de LinkedIn a déclaré que l'écrasante majorité des données du monde était en fin de compte entre les mains des Big Tech : Google, Facebook, Amazon, Microsoft et Apple. Un récent fil Twitter affirme que pour 1000 USD, il est possible de demander à une entreprise toutes

les informations possibles sur une personne. Nous savons que certaines entreprises sont devenues expertes en extraction de données, qu'elles vendent à d'autres pour pouvoir manipuler notre opinion. Nous savons désormais que par l'envoi ciblé de récits spécifiques et le paiement de comptes Twitter et Facebook fictifs pour répandre des points de vue, les élections américaines et le vote sur le Brexit ont été influencés et manipulés à l'aide de données.

Au Japon, le gouvernement se prépare à déployer des « banques de données », nom donné à des institutions publiques qui aideront les citoyens à décider des données qu'ils acceptent de mettre à disposition. En Estonie, un des pays du monde à avoir le système de cybergouvernement le plus poussé et à utiliser le plus les données, les données des citoyens sont régies par des principes juridiques rigoureux qui permettent à l'individu de décider des données disponibles et de la manière de les utiliser. En revanche, de nombreux pays sont à la traîne et sont loin de fournir aux citoyens une manière claire et transparente de savoir quelles informations existent, et a fortiori de leur fournir un moyen de les contrôler.

S'il est vrai que des lois sur la protection des données existent dans de nombreux pays, les données tirées de la surveillance des travailleurs ne sont pas spécifiquement protégées. UNI Global Union coopère avec l'organisation mondiale IEEE en vue de créer une norme mondiale pour la gouvernance transparente des données des travailleurs par les employeurs. Il est également vital que les syndicats cherchent à mettre en œuvre, par le biais de conventions collectives par entreprises ou par secteurs, les droits des travailleurs sur leurs données et les dispositions garantissant leur protection. Sans ces dispositions, l'équilibre des forces au sein des entreprises sera pour toujours biaisé au profit des décisions managériales unilatérales prises à la lumière des données collectées. Vu la relative facilité avec laquelle il est possible de combiner des données venant de sources multiples, les travailleurs peuvent se retrouver extrêmement désavantagés s'ils n'ont pas voix au chapitre et n'ont aucune influence sur le type de données utilisées et la manière dont elles le sont. En fait, on peut affirmer que les droits des travailleurs sur les données et la protection de celles-ci constituent le prochain défi de l'évolution de l'économie numérique.

Vu l'importance des données sur le lieu de travail, UNI Global Union revendique que **les travailleurs et leurs représentants syndicaux aient le droit d'accéder aux données recueillies à leur sujet et par le biais de leur processus de travail, de les influencer, de les modifier et de les supprimer.**

Le présent document concrétise cette revendication clé et la subdivise en 10 points spécifiques.

Table des matières

1. Les travailleurs doivent avoir accès aux données recueillies sur eux et pouvoir exercer une influence sur elles

Les travailleurs doivent avoir le droit d'accéder aux données recueillies sur eux, y compris le droit de faire rectifier, bloquer ou effacer ces données.

Cela inclut les points suivants :

a) Le consentement ne peut pas et ne devrait pas être la base juridique du traitement des données au travail.
b) Un travailleur devrait être en mesure d'obtenir, sur demande, à des intervalles raisonnables et sans retard excessif, la confirmation du traitement des données personnelles se rapportant à sa personne. Cette communication devrait prendre une forme intelligible, inclure tous les renseignements concernant l'origine des données ainsi que toute autre information que le contrôleur est tenu de fournir pour garantir la transparence du traitement.
c) Le travailleur doit bénéficier du droit de portabilité des données, c'est-à-dire du droit de déplacer par ex. les systèmes de notation et de classement d'une plateforme à une autre.
d) Conformément au droit et à la pratique nationaux ou aux modalités des conventions collectives, les données personnelles peuvent être communiquées aux représentants des travailleurs, mais uniquement dans la mesure où ces données sont nécessaires pour leur permettre de défendre correctement les intérêts des travailleurs ou bien dans le cas où ces données sont nécessaires pour accomplir et contrôler les obligations stipulées dans les conventions collectives.

2. Mise en œuvre de garanties durables pour le traitement des données

Pour toutes les formes de traitement des données, les employeurs devraient assurer le respect des garanties suivantes. En particulier :

a) Fournir aux travailleurs des informations claires et complètes avant l'introduction de systèmes et de technologies de l'information permettant la surveillance de leurs activités. Les informations fournies devraient être tenues à jour et devraient tenir compte du principe 3 ci-dessous. Elles devraient inclure le but de l'opération, la conservation ou la période de sauvegarde, ainsi que l'existence des droits d'accès et de rectification des travailleurs et la manière dont ces droits peuvent être exercés. Cette garantie couvre également le moment où les objectifs et les systèmes de surveillance changent.
b) Prendre des mesures internes appropriées relatives au traitement de ces données et avertir les travailleurs à l'avance. Cela inclut de réaliser une étude d'impact sur la sphère privée lorsque les technologies peuvent présenter des risques élevés pour les individus, notamment dans le cas d'un profilage potentiel ou de décisions prises par le biais de systèmes automatisés (voir principe 5 ci-dessous).
c) Consulter les travailleurs dans les circonstances qui font soupçonner un risque de violation du droit au respect de la sphère privée et de la dignité humaine du travailleur. Respecter dans de tels cas le droit des travailleurs à mettre leur veto à la surveillance de ces données jusqu'à ce que l'employeur puisse prouver par écrit que le droit de respecter la sphère privée et la dignité des travailleurs est pleinement respecté et recevoir ultérieurement l'accord des travailleurs (voir principe 5) ;
d) Consulter, conformément au droit national, l'autorité nationale de surveillance sur le traitement des données personnelles.

3. Le principe de minimisation des données doit s'appliquer

Ce principe veut que les employeurs puissent uniquement :

> « recueillir des données appropriées et uniquement celles-ci pour les buts appropriés et uniquement ceux-ci, à utiliser par les personnes compétentes et uniquement celles-ci et pendant les durées appropriées et uniquement celles-ci. »

Les employeurs devraient mettre au point des mesures appropriées pour veiller à respecter dans la pratique les principes et les obligations relatives au traitement des données à des fins d'emploi. Cela inclut les principes de proportionnalité et de subsidiarité : la collecte des données doit être limitée à ce qui est nécessaire pour atteindre les objectifs de la collecte en question, à savoir que le contenu et la forme de l'action doivent être conformes au but poursuivi.

À la demande de l'autorité de surveillance, les employeurs devraient être en mesure de démontrer qu'ils respectent de tels principes et obligations. Ces mesures devraient être adaptées au volume et à la nature des données traitées et au type d'activités entreprises et devraient également tenir compte des implications possibles pour les droits et libertés fondamentales des travailleurs.

4. Le traitement des données doit être transparent

a) Les informations concernant les données personnelles détenues par les employeurs devraient être soit mises à la disposition du salarié concerné directement ou par l'intermédiaire de son ou de ses représentant(s), soit être portées à sa connaissance par d'autres moyens appropriés.
b) Les employeurs devraient fournir aux travailleurs les informations suivantes :
    i. les catégories de données personnelles à traiter et une description des objectifs du traitement ;
    ii. les destinataires ou catégories de destinataires des données personnelles ;
    iii. les moyens donnés aux travailleurs pour exercer le droit énoncé au principe 1 sans préjudice des droits plus favorables accordés par le droit national ou en vigueur dans leur système juridique ;
    iv. toute autre information nécessaire pour garantir un traitement équitable et licite.
c) Une description particulièrement claire et complète doit être fournie des catégories de données personnelles pouvant être recueillies par les TIC, y compris la vidéo surveillance et ses usages potentiels.
d) Ces informations devraient être fournies dans un format accessible et être tenues à jour. En tout état de cause, elles devraient être fournies avant qu'un salarié n'effectue l'activité ou l'action en question, et être aisément mises à disposition par le biais des systèmes d'information normalement utilisés par le salarié.

5. Les lois sur la sphère privée et les droits fondamentaux doivent être respectés dans toute l'entreprise

Cela inclut le respect de toutes les conventions mondiales et régionales sur les droits de l'homme[1], y compris :

- La déclaration universelle des droits de l'homme de l'ONU
- Le Code de pratique de 1997 du Bureau international du travail sur la protection des données personnelles des travailleurs.

L'employeur doit également :

a) Faire preuve de respect pour la dignité humaine et la sphère privée, et la protection des données personnelles devrait être sauvegardée dans le traitement des données personnelles à des fins d'emploi, notamment pour permettre le libre développement de la personnalité du salarié ainsi que les possibilités de relations individuelles et sociales sur le lieu de travail.
b) La communication doit être licite et ne pas inclure de déclarations diffamatoires ou calomnieuses.
c) Les dispositifs de communication dans l'entreprise ne doivent pas être utilisés comme des moyens de harcèlement sexuel ou de diffusion de commentaires choquants poursuivant un but de discrimination.

L'employeur peut exiger un avis de non-responsabilité lorsque les travailleurs communiquent en interne et avec l'extérieur pour dire que les vues exprimées sont celles de l'auteur seul et non celles de l'entreprise.

6. Les travailleurs doivent avoir un droit d'explication exhaustif lors de l'utilisation des données

Ce principe se rapporte aux décisions prises par la direction qui incluent l'obtention de données venant de l'intérieur ainsi que de l'extérieur de l'entreprise. Par exemple, dans les processus de recrutement internes et externes, les travailleurs doivent avoir le droit de savoir sur quelle base une décision a été prise, afin d'être protégés contre les décisions discriminatoires basées sur des prédictions de données, notamment concernant la santé.

Le travailleur doit être informé lorsque des décisions importantes sont prises sur la base de données internes ainsi qu'externes.

7. Les données biométriques et les informations personnelles doivent être protégées

La collecte et la poursuite du traitement de données biométriques ne devraient être entreprises que s'il n'existe aucun autre moyen moins intrusif disponible et uniquement si elles sont accompagnées de garanties appropriées, y compris les garanties supplémentaires prévues au principe 2.

Le traitement de données biométriques et d'autres informations personnelles devrait se fonder sur des méthodes scientifiquement reconnues et être soumis aux exigences d'une sécurité et d'une proportionnalité strictes.

[1] http://www.ohchr.org/Documents/Publications/CoreTreatiesen.pdf

8. Équipements destinés à localiser les travailleurs

Les équipements destinés à localiser les travailleurs ne devraient être introduits que s'ils s'avèrent nécessaires pour atteindre le but légitime poursuivi par les employeurs, et leur utilisation ne devrait pas aboutir à une surveillance permanente des travailleurs. Notamment, la surveillance ne devrait pas être le but, mais seulement une conséquence indirecte d'une action requise pour protéger la production, la santé et la sécurité ou pour garantir le bon fonctionnement d'une organisation. Étant donné le potentiel de violation des droits et des libertés des personnes concernées par l'utilisation de ces dispositifs, les employeurs devraient assurer toutes les garanties nécessaires pour le droit des travailleurs au respect de la sphère privée et à la protection des données personnelles, y compris les garanties prévues au principe 2.

Conformément au principe 3 sur la minimisation des données, les employeurs devraient prêter une attention particulière au but pour lequel ces dispositifs sont utilisés. Les employeurs devraient appliquer des procédures internes appropriées relatives au traitement de ces données et devraient en notifier à l'avance les personnes concernées.

9. Une instance multidisciplinaire et inter-entreprises de gouvernance des données devrait être mise en place

Une instance multidisciplinaire et inter-entreprises de gouvernance des données devrait être mise en place pour régler les questions de formation, de stockage, de manutention et de sécurité des données. Cela inclut des dispositions stipulant que tous les représentants membres de cette instance, y compris les délégués syndicaux, reçoivent une formation appropriée aux données afin d'être équipés à travailler au maintien et à la défense d'une politique durable de protection des données dans les entreprises.

10. Tous les points ci-dessus devraient être mis en œuvre dans une convention collective

Les principes ci-dessus devraient être mis en œuvre et appliqués par le biais de négociations collectives au sein de chaque entreprise ou par secteur. En l'absence de telles négociations, l'employeur devrait établir une instance de gouvernance conformément au principe 9.

Sources :

Le présent document s'est inspiré des principaux documents suivants, sur lesquels il s'appuie :

1) GDPR (http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf)

2) Recommandation CM/Rec(2015) du Conseil de l'Europe (2015) du Comité des ministres aux États membres sur le traitement des données à caractère dans le cadre de l'emploi https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

3) (2017) : GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, avis 2/2017 sur le traitement des données au travail http://ec.europa.eu/newsroom/document.cfm?doc_id=45631