



► Note d'information de l'OIT

► Renforcer les droits des travailleurs en matière de données

Introduction

Ce dossier traite de l'extraction de données de notre vie privée et de notre vie professionnelle et comment elle peut influencer nos possibilités de travail et l'équilibre du pouvoir entre employeurs et travailleurs; il porte aussi sur les droits que les travailleurs devraient avoir sur ces données pour éviter un rétrécissement des perspectives sur le marché du travail.

Tout ce qui est numérique extrait et/ou produit des données: votre utilisation des réseaux sociaux, vos informations de paiement par carte de crédit, vos habitudes d'achat, les sites web et les applications que vous utilisez et à quel moment, jusqu'aux 14 capteurs de votre téléphone portable qui extraient des données sur votre localisation, le son et la température autour de vous, votre vitesse de déplacement, et bien d'autres choses encore. Toutes ces données sont utilisées pour en déduire des informations sur nous – en tant que citoyens et en tant que travailleurs – pour établir notre profil et faire des prévisions à notre sujet à des fins publicitaires, mais aussi pour la manipulation de pensée, la disponibilité des emplois pour une personne et pour déterminer dans quelle mesure le marché du travail est inclusif et diversifié.

Surtout, ce n'est pas simplement votre vie et votre carrière qui sont affectées par cette extraction de données. Au fur et à mesure qu'elles s'accumulent, les données sont utilisées pour comparer les personnes ou les groupes de personnes selon d'innombrables autres critères. Par exemple, les évaluations des clients en fonction des caractéristiques des travailleurs; les types d'amis et la probabilité de se syndiquer; l'indice de masse corporelle et la vitesse des travailleurs; l'accent, le code postal et la fiabilité perçue. Les systèmes algorithmiques utilisés pour trouver toutes ces corrélations, probabilités, prédictions et différences sont de plus en plus élaborés à mesure que le volume de données croît de manière exponentielle. En d'autres termes, ce que vous faites, sans même que vous le sachiez, affecte la vie des autres.

Les données au travail

Exacerbée par la pandémie de COVID-19, la tendance aux lieux de travail pilotés par les données n'a fait que se renforcer. Tous les services et systèmes numériques sur les lieux de travail extraient des données sur les travailleurs. Nous pouvons identifier 5 façons dont cela se produit:

Data at work



Collecte directe

auprès des candidats à l'emploi, des employés, des clients



Achat de profils/fichiers de données

à des tiers



Extraction de traces de données

à partir des systèmes informatiques et de réseaux



Extraction de traces de données

via des dispositifs, vêtements ou équipements portatifs



Données audio et visuelles

provenant de la vidéosurveillance, des appels téléphoniques et de la reconnaissance faciale

- **Collecte directe:** Votre CV contient une multitude d'informations précieuses. De vos précédents employeurs à votre éducation, peut-être même vos centres d'intérêt et autres activités de loisirs. Les employeurs peuvent également collecter des données directement auprès de leurs clients (ce qu'ils achètent, à quelle fréquence, quels biens ou services ils recherchent sur le site web, etc.) ou de leurs employés actuels (par exemple, à quelle fréquence ils sont malades, combien d'heures ou de jours ils travaillent, etc.).
- **Achat de profils de données:** Ceux qu'on appelle courtiers en données sont nombreux à travers le monde dont tout le modèle d'affaires repose sur l'achat, le regroupement et la revente de bases de données. Il peut s'agir de bases de données agrégées sur la circulation, de données sur la «fiabilité» de certains groupes de personnes, ou de profils sur les scores de crédit, la santé ou le niveau d'études par zone géographique ou statut socio-économique.
- **Extraction de traces de données:** Quand vous vous connectez à votre messagerie ou à votre serveur professionnel, vous laissez une trace de vos activités. A quelle heure vous êtes-vous connecté, à quels documents avez-vous accédé? De même, certains systèmes, tels qu'Office365, créent des rapports sur votre «productivité», votre temps de «concentration», etc. La direction voit-elle ces mesures elle aussi?
- **Données dérivées des capteurs:** Certains bureaux ont des capteurs dans l'ensemble du bâtiment: sous les bureaux pour indiquer à quelle fréquence le bureau est utilisé et libéré; sur les portes pour voir à quelle fréquence une pièce est utilisée ou non. Certains travailleurs sont obligés d'utiliser des scanners portatifs ou des dispositifs portables comme un *Fitbit* ou des systèmes de géolocalisation. Tous ces équipements produisent des données qui sont, ou peuvent être, utilisées par la direction.
- **Données audio et visuelles:** D'autres types de données sont issus des systèmes audiovisuels. Le ton de la voix des travailleurs des centres d'appels et ce qu'ils disent sont mesurés et évalués. La frappe sur le clavier d'un téléphone mobile. La vidéosurveillance ou la reconnaissance faciale est utilisée pour localiser et identifier les travailleurs. Bien que faisant l'objet de vives critiques, certains de ces systèmes ont été utilisés pour détecter l'état émotionnel des travailleurs: sont-ils fatigués, ont-ils l'air tristes, frustrés, heureux ou nerveux?

Quel que soit le moyen d'extraction, les systèmes de contrôle et de surveillance numériques rassemblent des données sur les travailleurs et sur ce qu'ils font et ne font pas. Si le contrôle n'est pas nouveau, la nature numérique des systèmes actuels a des caractéristiques particulières qui ont une influence sur la manière dont les syndicats doivent les aborder. Imaginez un système qui contrôle la productivité des ouvriers d'un atelier d'usine par des caméras de surveillance et des capteurs portatifs. *Premièrement*, le système est impossible à éviter parce qu'il est intégré dans les processus et équipements de travail. *Deuxièmement*, le contrôle est global – il collecte un gros volume de données à partir de sources multiples. *Troisièmement*, la direction reçoit instantanément l'information car les données sont collectées en temps réel. *Quatrièmement*, le système est interactif, permettant une communication et un retour d'information en temps réel – dans notre cas, par l'intermédiaire des écrans de l'atelier montrant la productivité de chacun des ouvriers.

Les employeurs peuvent utiliser ces données pour mesurer la productivité et l'efficacité des salariés (quelle que soit leur définition). Ils peuvent faire de savants calculs sur la probabilité que, par exemple, vous remplissiez vos objectifs, soyez apprécié des clients, ayez un rythme rapide ou soyez dévoué au travail. Ils peuvent par ailleurs les utiliser pour faire des prédictions sur vous: êtes-vous susceptible de quitter l'entreprise bientôt, de tomber malade, de vous ralentir ou d'adhérer à un syndicat?

L'utilisation précise des données par les employeurs dépend de la *finalité* des systèmes qu'ils déploient et de l'analyse des données à laquelle ils procèdent. Dans certains cas, les travailleurs peuvent accepter l'extraction de données. Par exemple, les travailleurs peuvent y être favorables à des fins sanitaires et de sécurité, pour éviter les accidents ou pour mesurer le temps de travail afin d'éviter le stress et l'épuisement au travail. Ce qui est important, c'est que les travailleurs le sachent et aient leur mot à dire quand au fait d'extraire des données, aux objectifs poursuivis, à l'utilisation des données et à leur devenir après coup. Le dossier 2 aborde les avantages et les inconvénients des données et des algorithmes déjà constatés pour les travailleurs.

L'économie politique de l'extraction de données

Bien qu'employeurs et travailleurs pourraient, en principe, s'accorder sur les finalités de l'extraction et de l'analyse de données, une question plus vaste est en jeu: voulons-nous vraiment que nos actions soient quantifiées, transformer notre travail en une multitude de points de

données qui pourront ou non faire l'objet d'un usage abusif? Si les travailleurs sont davantage considérés comme des numéros ou des points par rapport à une norme statistique plutôt que comme des êtres humains, quel sera l'impact sur les droits de l'homme et les droits des travailleurs?

On entend fréquemment dire que les données sont «le nouveau pétrole» – une ressource précieuse à extraire mais qui, à l'état brut, ne peut pas vraiment être utilisée. Les données doivent donc être analysées et regroupées. Elles doivent devenir un actif qui peut être réutilisé pour ajouter de la valeur aux chaînes de production et de services. Selon ce discours, les données sont donc une marchandise qui peut être vendue et achetée. Si l'on suit cette assertion, les données des travailleurs peuvent être monnayées. Cependant, voir la contribution des travailleurs à ces moyens de production en termes monétaires et, comme le font certains, exiger sur cette base une redistribution de la valeur ajoutée aux travailleurs, ne fait que consolider et peut-être même justifier cette marchandisation du travail.

Les critiques de cette perspective économique des données demandent que les données soient considérées sous l'angle du pouvoir et des droits. Ceux qui collectent les données sont ceux qui acquièrent du pouvoir sur les marchés, les concurrents, les citoyens et les travailleurs. Ce sont leurs analyses unilatérales, leurs récits qui dominent et manipulent par conséquent les services, les opinions et les produits qui nous sont révélés à titre individuel, sans tenir compte des droits de l'homme ou autres considérations morales.

L'auteure reconnue de *L'âge du capitalisme de surveillance*, Shoshana Zuboff, est catégorique: nous devrions rendre illégaux ce qu'elle appelle les «marchés des comportements futurs»¹. Elle fait ici référence au commerce des inférences de données qui sont utilisées pour manipuler systématiquement nos personnes sans méfiance. Comme elle le décrit, pour que les collecteurs de données puissent offrir des certitudes à leurs clients, ils ont besoin d'énormes volumes de données et de données variées pour garantir que leurs prédictions et leurs modèles sont aussi exacts que possible. Cela conduit à des économies d'échelle et de gamme – et donc à la concentration du pouvoir entre les mains de quelques entreprises mondiales très riches: Google, Meta, Apple, Amazon, Microsoft, Alibaba et Tencent.

Alors que dans la perspective économique l'extraction des données n'est limitée que par la loi (par exemple, les réglementations sur la protection des données), une approche fondée sur les droits stipule que les données ne peuvent être extraites que si elles respectent l'ensemble des droits de l'homme. En 2018, le Haut Commissariat des Nations Unies aux droits de l'homme (HCDH) a publié² une note d'orientation sur les principes d'une approche des données fondée sur les droits de l'homme. Il y recommande 6 grands principes, chacun renfermant plusieurs sous-principes:

- 1. Participation:** *La participation des groupes de population pertinents aux exercices de collecte des données, notamment à la planification, à la collecte des données, à la diffusion et à l'analyse des données*
- 2. Ventilation des données:** *La ventilation des données permet aux utilisateurs de données de comparer les groupes de population et de comprendre les situations de groupes spécifiques. La ventilation exige que soient collectées des données sur des caractéristiques pertinentes*
- 3. Auto-identification:** *Aux fins de la collecte de données, les populations d'intérêt devraient s'auto-identifier. Les personnes devraient avoir la possibilité de révéler ou de dissimuler les informations concernant leurs caractéristiques personnelles*
- 4. Transparence:** Les collecteurs de données doivent fournir des informations claires, ouvertement accessibles, sur leurs opérations, y compris sur le plan de recherche et la méthodologie de collecte des données. Les données collectées par les organismes gouvernementaux doivent être ouvertement accessibles au public
- 5. Vie privée:** *Les données communiquées aux collecteurs de données doivent être protégées et demeurer privées, et la confidentialité des réponses des personnes et des informations personnelles doit être maintenue*
- 6. Responsabilité:** *Les collecteurs de données ont la responsabilité de faire respecter les droits de l'homme dans le cadre de leurs activités, et les données doivent être utilisées pour tenir les Etats et les autres acteurs responsables de leurs actes pour les questions relatives aux droits de l'homme*

Pour les travailleurs, ces principes impliquent qu'ils ont le droit de participer à la sélection des données à extraire et à quelles fins, que les données sont représentatives et donc non discriminatoires, et que les droits de l'homme

¹ <https://www.project-syndicate.org/onpoint/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01?barrier=accesspaylog>

² https://www.ohchr.org/Documents/Issues/HRIIndicators/GuidanceNoteonApproachtoData_FR.pdf

³ <https://techgdr.com/blog/difference-between-pii-and-personal-data/>

sont respectés à tout moment. Ces droits sont-ils reconnus aux travailleurs dans les réglementations sur la protection des données à travers le monde?

La réglementation sur la protection des données et les travailleurs

Dans le monde entier, les réglementations en matière de protection des données portent sur le traitement des données personnelles d'un individu ou, dans certains cas, également sur les informations personnellement identifiables³. Selon la CNUCED, 19 pour cent des pays dans le monde ne disposent d'aucune réglementation en matière de protection des données⁴. En ce qui concerne plus précisément les données relatives aux travailleurs, les réglementations sur la protection des données dans les autres régions du monde peuvent être classées en trois grandes catégories. Celles qui incluent des articles spécifiques sur les données des travailleurs (comme le Règlement général sur la protection des données de l'Union européenne – le RGPD), celles qui le font implicitement comme la plupart des pays d'Afrique, d'Amérique latine et d'Asie-Pacifique, et celles qui excluent explicitement les travailleurs (telles que la loi californienne sur la vie privée des consommateurs de 2018 – la CCPA, et en partie la loi australienne sur la protection de la vie privée de 1988⁵).

La plupart des réglementations relatives à la protection des données appartiennent à la deuxième catégorie⁶. Dans ce cas, toutes les exigences légales liées à la confidentialité des données s'appliquent à la collecte, au traitement, au transfert et à l'utilisation des données des salariés. En outre, la grande majorité d'entre elles dépendent du «consentement éclairé»⁷ des travailleurs pour l'extraction et l'utilisation de leurs données par les employeurs. C'est contraire au RGPD européen qui stipule explicitement qu'en raison du déséquilibre de pouvoir entre les travailleurs et la direction, les travailleurs ne seront jamais entièrement libres de donner leur consentement. A de mineures exceptions près⁸, le

consentement éclairé n'est donc pas une base juridique pour le traitement des données des travailleurs dans le cadre du RGPD.

La troisième catégorie qui exclut explicitement les travailleurs n'est pas courante bien que plusieurs projets de loi sur la protection des données en cours de négociation aux Etats-Unis cherchent à exclure les travailleurs de cette manière. La CCPA a été amendée par le projet de loi de l'Assemblée n° 25 (AB-25) en 2019, qui supprimait les obligations des employeurs envers les résidents californiens dans leur position de candidats à un emploi, d'employés, de prestataires indépendants, responsables et cadres d'entreprise⁹. Indépendamment des exemptions de l'AB-25, les employeurs sont toujours dans l'obligation de notifier aux consommateurs, y compris aux membres de leur personnel, ainsi qu'aux demandeurs d'emploi, les catégories d'informations personnelles qu'ils collectent et à quelles fins d'utilisation, au moment de la collecte ou avant celle-ci.

En résumé, à l'exception dans une certaine mesure des travailleurs couverts par le RGPD, les droits des travailleurs en matière de données sont mal définis dans les réglementations sur la protection des données dans le monde. Tandis que la majorité de ces réglementations incluent *implicitement* les travailleurs, elles reposent aussi sur le «consentement éclairé» comme fondement du traitement des données personnelles des travailleurs. Cependant, comme le stipule le RGPD, le consentement éclairé ne peut être donné librement par les travailleurs en raison des relations de pouvoir entre la direction et les travailleurs¹⁰. En outre, bien que dans la plupart des protections des données les employeurs soient tenus d'*informer* les travailleurs sur les données collectées et les objectifs de cette collecte, les travailleurs n'ont aucun droit de consultation, de recours, ni de modification ou de suppression des données collectées.

Aucune ne satisfait pleinement aux principes du HCDH, tels que décrits plus haut.

4 <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

5 <https://www.lexology.com/library/detail.aspx?g=0f6d20a7-a6b1-4980-aa0e-a98f1d637d38>

6 Voir cet ouvrage numérique pour un bon aperçu : <https://www.mayerbrown.com/ebooks/A-Global-Guide-to-Employee-Data-Privacy/#/spreads/1>

7 Le RGPD affirme que le consentement doit être «donné de façon libre, spécifique, éclairé et univoque». Cela signifie que la personne concernée accepte le traitement de ses données à caractère personnel et qu'elle ne doit pas être contrainte à donner son consentement, Considérant 32 – Conditions applicables au consentement – Règlement général sur la protection des données

8 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en

9 <https://secureprivacy.ai/blog/ab-25-what-this-ccpa-amendment-means-for-employers-and-employees>

10 Voir: Lignes directrices du groupe de travail «Article 29» sur le consentement au titre du règlement 2016/679, 11, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf

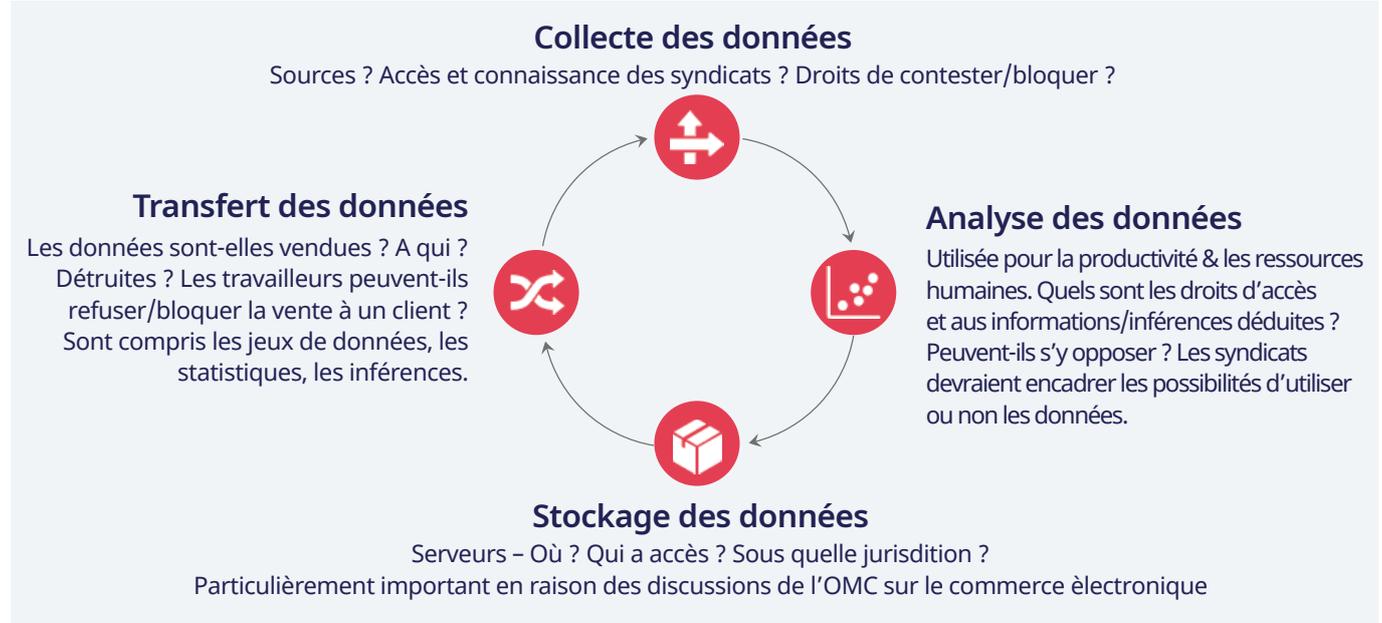
Renforcer les droits des travailleurs en matière de données

Il est clair que les droits individuels et collectifs des travailleurs en matière de données sont mal définis dans la grande majorité des pays et des régions. Le schéma ci-dessous illustre le cycle de vie des données au travail: depuis la collecte des données jusqu'à l'analyse, au stockage et au transfert, il décrit les sujets que les syndicats doivent connaître et sur lesquels ils doivent négocier, ainsi que les droits que les travailleurs doivent avoir. Il s'appuie sur la publication du BIT de 1997 intitulée

«Protection des données personnelles des travailleurs. Recueil de directives pratiques du BIT»¹¹.

Au cours des quatre étapes, certaines demandes, mais c'est loin d'être le cas pour toutes, sont couvertes pour les travailleurs de la zone du Règlement général sur la protection des données de l'Union européenne. Pour les travailleurs de la plupart des autres juridictions, ces droits – s'ils étaient négociés – seraient nouveaux.

Le cycle de vie des données au travail



Collecte des données

La phase de collecte des données couvre les outils de collecte internes et externes, les sources des données, que les délégués syndicaux et les travailleurs aient été informés ou non des outils prévus et qu'ils aient ou non le droit de les contester ou de les rejeter. Une grande partie de l'extraction est cachée au travailleur (ou au citoyen) et la direction doit être tenue responsable.

Dans la région d'application du RGPD, les entreprises sont obligées de réaliser des évaluations d'impact sur l'introduction de nouvelles technologies susceptibles d'impliquer un risque élevé pour les informations

d'autrui. Elles sont aussi tenues de consulter les travailleurs ¹². Pourtant, très peu de syndicats ont accès à ces évaluations, ni même connaissance – les syndicats devraient revendiquer leur droit d'y participer.

Analyse des données

Dans la phase d'analyse des données, les syndicats doivent pallier les lacunes réglementaires qui ont été identifiées – à savoir l'absence de droits en ce qui concerne la création de profils de travailleurs en utilisant les probabilités statistiques basées sur les données collectées. Tandis que les travailleurs de la zone RGPD

11 https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112624.pdf

12 Article 35 du RGPD et Avis 2/2107 sur le traitement des données sur le lieu de travail du Groupe de travail «Article 29» sur la protection des données.

ont un droit à connaître quelles inférences directes sont faites à partir de leurs données personnelles, ils n'ont pas le droit de connaître les inférences dont ils font l'objet si elles n'incluent pas leurs données personnelles¹³.

Ces déductions peuvent être utilisées pour déterminer des emplois du temps ou des salaires optimaux (s'ils sont liés à des mesures de la performance) ou, en matière de ressources humaines, qui embaucher, promouvoir ou licencier. Elles peuvent être utilisées pour prédire les comportements sur la base de schémas historiques, de données émotionnelles et/ou d'activité.. Such inferences can be used to determine an optimal scheduling, wages (if linked to performance metrics) or, in human resources, whom to hire, promote or fire. They can be used to predict behaviour based on historic patterns, emotional and/or activity data.

L'accès aux inférences est essentiel à l'autonomisation des travailleurs et d'ailleurs aux droits humains. Les travailleurs devraient avoir un meilleur aperçu de ces déductions, y avoir accès et avoir le droit de les rectifier, de les bloquer, voire de les supprimer. Sans ces droits, il n'y aura que peu de freins et de contrepouvoirs à l'utilisation par la direction de systèmes algorithmiques ou à la discrimination et aux préjugés induits par les données.

Associés à la phase de collecte des données, les syndicats pourraient ici avantageusement négocier les objectifs de la collecte et de l'analyse des données. Cela suppose notamment de fixer les limites pour ce à quoi les données collectées peuvent servir et ne pas servir.

Exemple:

En Californie, le syndicat des Teamsters a négocié le fait que les données de localisation des routiers collectées pour garantir leur sécurité ne peuvent pas être utilisées dans le cadre des évaluations de performance desdits travailleurs.

Stockage des données

La phase de stockage des données est importante, notamment en ce qui concerne les accords commerciaux et les négociations sur les flux de données. Par exemple, les négociations relatives à la «libre circulation des données» en matière de commerce électronique, au sein de l'Organisation mondiale du commerce, et en marge de l'OMC, ont pour but de supprimer le droit de toute nation à localiser les données sur son territoire. Cela pourrait aboutir au déplacement des données vers des régions de moindre protection de la vie privée, qui présente des risques car les données des travailleurs pourraient alors être vendues, regroupées et revendues sans avoir à respecter les politiques de protection des données du pays d'origine.

Si les données peuvent circuler librement dans le monde entier et que les travailleurs n'obtiennent pas de droits des données beaucoup plus forts par le biais de la législation nationale ou des conventions collectives, leur accès et leur contrôle sur ces données seront encore plus faibles.

Transfert des données

La dernière phase – le transfert des données – est liée à la phase de stockage mais elle a également trait à l'éventuelle vente de données/bases de données, y compris des travailleurs. Les syndicats doivent être vigilants. Il s'agit de la suppression des données mais également de la vente et du transfert à des tiers de jeux de données, avec les inférences et les profils associés. Les syndicats devraient participer aux négociations visant à améliorer nettement les droits de savoir ce qui est transféré et à qui, avec la latitude de s'opposer au processus voire de le bloquer – ce qui est extrêmement important à la lumière des négociations commerciales sur le commerce électronique mentionnées ci-dessus. De la même manière, les syndicats devraient, au minimum, avoir le droit de demander la suppression des jeux de données et des inférences sur les travailleurs quand l'objectif initial a été atteint, conformément au principe de la minimisation des données reconnu par le RGPD (article 5.1.c) 14.

¹³ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

¹⁴ <https://gdpr-info.eu/art-5-gdpr/>

Exemple:

En Irlande, le syndicat du secteur financier a réussi à négocier deux articles essentiels dans la politique du personnel de la banque RBS :

1. Clause anti-marchandisation

La banque s'engage à ne pas transformer les données de ses employés en une marchandise à vendre ou échanger.

2. Respect de la vie privée et des droits de l'homme

La Banque s'engage à respecter la vie privée des travailleurs et les droits humains tels que définis par la loi et surtout par la Déclaration universelle des droits de l'homme des Nations Unies et le Recueil de directives pratiques du BIT sur la protection des données personnelles des travailleurs.

Pour consulter leur communiqué de presse, cliquez [ici](#).

Recommandations

Pour sauvegarder les droits des travailleurs sur les lieux de travail numérisés et éviter que des inférences et des profils de données, souvent obscurs, ne façonnent les perspectives professionnelles des travailleurs, les syndicats devraient commencer à négocier des droits des données nettement renforcés.

Pour y parvenir, les syndicats pourraient:

1. Former les membres et les délégués syndicaux sur le rôle des données dans les lieux de travail numérisés et la société au sens large. Cela comprend des conseils de qualité sur l'utilisation des équipements fournis par l'employeur et de bonnes pratiques concernant la sauvegarde du droit à la vie privée des travailleurs en dehors de leurs heures de travail.
2. Envisager la création d'une cohorte de délégués syndicaux numériques, spécialistes de la «mise en données» du travail et des travailleurs. Voir aussi le dossier 2.
3. Disposer de ressources syndicales (experts juridiques, unités de négociation et organisateurs) qui peuvent faciliter les négociations susmentionnées.
4. Négocier le cycle de vie des données au travail du point de vue des droits de l'homme et des droits des travailleurs et en lien avec eux.
5. Créer un cadre politique sur les droits relatifs aux données à l'échelle des syndicats qui puisse éclairer les délégués syndicaux (numériques) dans leurs négociations. Conformément aux droits humains et au cycle de vie des données au travail, ce cadre pourrait inclure des articles sur:
 - a. Principe général: Garantir la dignité et le bien-être des travailleurs dans l'utilisation sur le lieu de travail de technologies fondées sur les données. Des articles et des normes devraient être établis pour donner aux travailleurs un droit de regard sur les nouvelles technologies et promouvoir la santé et la sécurité, protéger la liberté syndicale et préserver des discriminations et autres effets néfastes sur les travailleurs.
 - b. Les travailleurs et/ou leurs représentants devraient participer à toutes les évaluations de l'impact des données et à leur réévaluation périodique.
 - c. Les employeurs devraient avertir les travailleurs de manière claire et accessible de toutes les technologies basées sur les données en place sur le lieu de travail. Ces notifications devraient intégrer une description compréhensible de la technologie, des types de données collectées, des finalités de ces systèmes et des droits et protections dont disposent les travailleurs.

d. Minimisation des données: Les employeurs ne devraient collecter les données des travailleurs que lorsque cela est nécessaire et essentiel pour que les travailleurs accomplissent leurs tâches. Voir aussi la définition figurant dans le RGPD (<https://gdpr-text.com/fr/read/article-5/>).

e. Les travailleurs devraient avoir le droit d'accéder, de modifier et de télécharger leurs données. Ils devraient recevoir toutes les informations pertinentes en ce qui concerne ces données, y compris pourquoi et comment elles ont été collectées, si des inférences ont été faites sur ces données et, si oui, quelles sont-elles, si les données ont ou non été utilisées pour aider à prendre une décision relative à l'emploi, y compris des décisions d'embauche. Les employeurs doivent être tenus responsables de corriger toute donnée inexacte.

f. Les données des travailleurs doivent être sauvegardées et protégées d'une utilisation abusive. En particulier, les employeurs ne devraient pas être autorisés à vendre ou à accorder des licences ou céder à des tiers l'accès aux données des travailleurs; sinon, l'incitation à violer la vie privée des travailleurs en vendant leurs données contre rémunération est trop forte.

g. Les données biométriques ou relatives à la santé des travailleurs ne devraient jamais être communiquées à des tiers, sauf si la loi l'exige.

h. Les employeurs ne doivent utiliser les systèmes de contrôle et de surveillance que pour des finalités restreintes qui ne portent pas préjudice (directement ou indirectement) aux travailleurs.

i. Les changements apportés aux systèmes de contrôle et de surveillance sur le lieu de travail, en raison de l'évolution technologique, devraient faire l'objet d'une négociation collective.

j. Les technologies fondées sur les données ne doivent pas entraîner de discrimination à l'encontre des travailleurs en raison de caractéristiques protégées telles que le sexe, l'âge, le handicap, le statut matrimonial ou de partenariat civil, la race, la religion ou les convictions. Data minimisation: Employers should only collect worker data when it is necessary and essential for workers to do their jobs. See also definition in GDPR <https://gdpr-info.eu/art-5-gdpr/>

k. La suppression des caractéristiques protégées des technologies fondées sur les données ne devrait pas permettre automatiquement aux employeurs de contourner les autres exigences de ce cadre politique. Par exemple, de nombreux employeurs justifient la vente ou la transmission de jeux de données qui comprennent des données personnelles des travailleurs en revendiquant le fait que ces données sont anonymisées et ne peuvent donc pas être reliées individuellement aux travailleurs. Toutefois, de nombreuses études montrent qu'il est relativement facile de revenir sur l'anonymisation des bases de données¹⁵, ce qui met en danger l'identité et la vie privée des travailleurs.

6. Être prudent et critique face aux tentatives de définir les données comme une marchandise/un bien. Cela passe par la conception de systèmes de redistribution de la valeur ajoutée des données plus favorables aux travailleurs en tant que facteur de production. Les droits ne devraient pas être monnayables.
7. Envisager des moyens pour collecter les données des travailleurs de manière responsable pour contrecarrer l'analyse de la direction (voir dossier 3) et briser ainsi la monopolisation de la «vérité» par l'employeur ou le système.

¹⁵ https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAImZ_o2Up5jda586F714qomIzWnAvy7a3pbaQ4D8vXb7WB3oxaA-ZMJHNpXWZM9W0uCR8aCSvyqd-ZGaCWrugvX_y7GYIwTuv5Cysn4MvhjGmLmVg4uLwMj5pp5cT1epXQCMYLMgIpNizUzEW_MIBPjNEQWiUrQ7tBOTr8VIFXU