

Garantir les droits collectifs sur les données



LE CYCLE DE VIE DES DONNÉES AU TRAVAIL - UN GUIDE

Le cycle de vie des données est un outil qui vous aide à réfléchir à la manière dont les données sont collectées, utilisées, stockées et éliminées sur le lieu de travail. Des risques pour la vie privée et les droits des travailleurs.euses peuvent apparaître à n'importe quelle étape du cycle de vie des données.

NÉGOCIER

LE CYCLE DE VIE DES DONNÉES AU TRAVAIL

En réfléchissant systématiquement à ces phases, les travailleurs.euses et les syndicats peuvent mieux déterminer quand et comment intervenir. L'intervention est importante à la fois pour atténuer les risques et pour promouvoir les droits des travailleurs.euses.

La notion de « cycle » est un outil discursif utile qui vous encourage à envisager toutes les façons dont les données peuvent être utilisées. Gardez toutefois à l'esprit que le cycle de vie des données n'est pas un processus linéaire. À partir du moment où elles sont acquises, les données peuvent passer à n'importe quelle phase dans n'importe quel ordre, et bon nombre de ces phases se produisent simultanément !



**STOCKAGE &
TRANSFERT DES DO**

1

COLLECTE DE DONNÉES

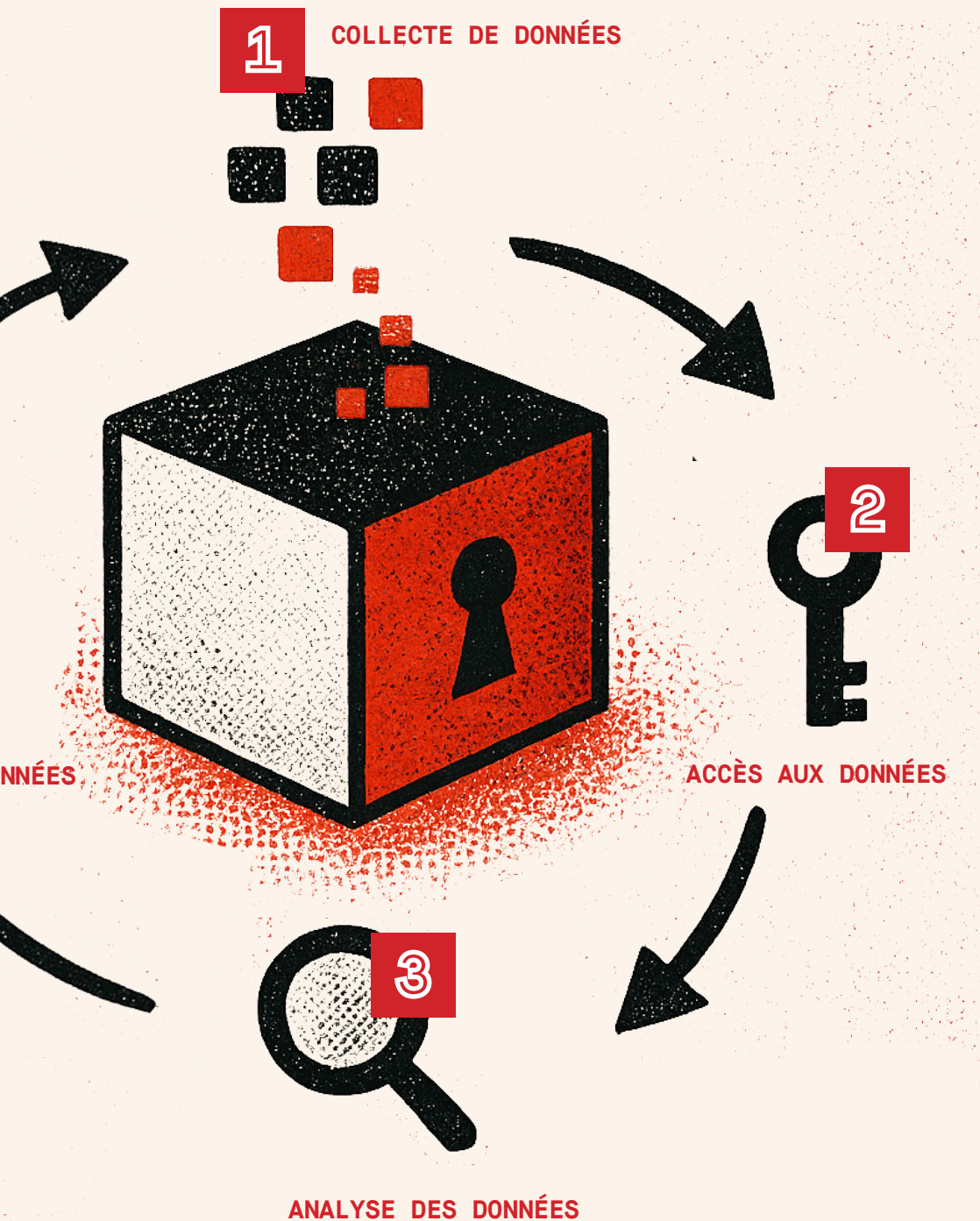
2

ACCÈS AUX DONNÉES

3

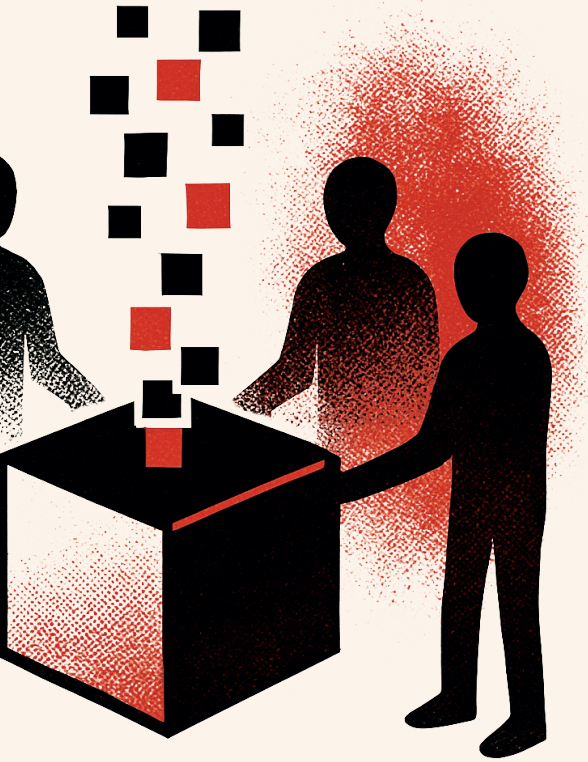
ANALYSE DES DONNÉES

NNÉES



1

COLLECTE DES DONNÉES



La gestion algorithmique et les systèmes d'IA reposent sur des données. Les employeurs peuvent acquérir des données de différentes manières : ils peuvent acheter des données auprès de sources externes; ils peuvent s'appuyer sur les données intégrées dans les systèmes numériques (souvent développés en externe) qu'ils utilisent ; et, le plus souvent, ils peuvent compter sur leurs employé.e.s comme source de données sur le lieu de travail. Même les résultats de données précédemment traitées peuvent constituer de nouvelles sources de données pour les employeurs.

En limitant les types de données que les employeurs peuvent collecter, les travailleurs.euses peuvent protéger leur vie privée et limiter l'efficacité et les types de systèmes d'IA et d'algorithmes utilisés par les employeurs.



2

ACCÈS AUX DONNÉES

L'information est synonyme de pouvoir, et les données sont des informations. C'est pourquoi il est important que la direction prenne les mesures adéquates pour garantir que les informations sont stockées de manière sûre et sécurisée, et que seules les personnes autorisées y ont accès.

Les syndicats et les travailleurs.euses doivent faire la distinction entre les différents types de données et déterminer quelles parties ont besoin d'accéder à quels types d'informations.

L'accès aux données peut être autorisé ou non autorisé, et les travailleurs.euses devraient avoir leur mot à dire sur qui a accès aux informations les concernant. Seules les personnes concernées au sein de l'organisation ont-elles accès aux données pertinentes? Par exemple, l'accès est-il réservé uniquement aux cadres travaillant au sein de l'organisation ? Qu'en est-il des logiciels ou services développés en externe ? Les travailleurs.euses devraient savoir si des tiers ont accès à leurs données. La direction a-t-elle envisagé de limiter ces droits dans les contrats d'approvisionnement/fournisseurs ?



La puissance des données se cristallise lorsque celles-ci sont analysées et utilisées pour prendre des décisions, formuler des recommandations ou faire des prévisions.

Si les travailleurs.euses peuvent consentir à certaines utilisations de leurs données, ils/elles peuvent s'opposer à d'autres. En fin de compte, à moins que des restrictions ne soient mises en place, les données peuvent être utilisées et réutilisées à l'infini et à des fins illimitées.

3

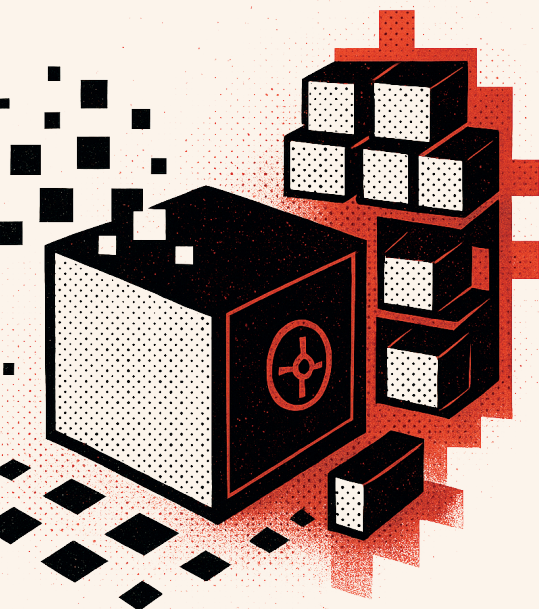
ANALYSE DES DONNÉE



Comment les données des travailleurs.euses sont-elles utilisées et analysées, et à quelles fins? Les travailleurs.euses peuvent-ils/elles accéder aux informations ou aux conclusions tirées à partir de leurs données? Peuvent-ils/elles s'opposer à certaines utilisations de leurs données?

Remarque : les syndicats devraient fixer des limites claires quant à l'utilisation qui peut être faite des données et celle qui ne peut pas l'être. Les syndicats devraient insister pour que toute utilisation des données soit limitée à la raison fournie au moment de la collecte initiale des données.

STOCKAGE & TRANSFERT DE DONNÉES



Une fois les données collectées, les employeurs doivent déterminer où et comment ils vont les stocker. Les données sont des éléments qui peuvent être conservés indéfiniment, et toutes les informations collectées sur les travailleurs peuvent être conservées indéfiniment. Le stockage des données doit rester une préoccupation importante pour les travailleurs tant que leurs données sont conservées.

Lorsque les informations ne sont plus nécessaires, elles peuvent être détruites en toute sécurité, ou données ou vendues à une autre organisation. Ce processus de transfert des données ne doit en aucun cas créer de nouveaux risques pour les travailleurs.euses. Ils/Elles doivent savoir quelles informations sont transférées et à qui, et doivent avoir leur mot à dire dans ces décisions.

En matière de stockage des données, les travailleurs.euses devraient se poser les questions suivantes : la direction prend-elle les mesures adéquates pour stocker les données en toute sécurité ? Dans quelle juridiction les données des travailleurs.euses sont-elles stockées et quel est l'impact de cette situation sur leurs droits ?

Pour le transfert des données, posez-vous les questions suivantes : que deviennent les données après leur utilisation ? Sont-elles supprimées ? Les ensembles de données et les déductions sont-ils vendus/transférés à des tiers à un moment donné ?

LE CYCLE DE VIE DES DONNÉES EN ACTION

EN PRATIQUE VOS CONNAISSANCES

Ce qui suit est une brève activité qui a été développée pour montrer comment le concept de cycle de vie des données peut être un outil conceptuel utile pour réfléchir aux droits des travailleurs.euses en matière de données et les défendre.

Vous allez lire un bref scénario concernant une nouvelle technologie introduite sur le lieu de travail. Imaginez qu'il s'agit de votre lieu de travail et que vous êtes chargé de transmettre les préoccupations et les demandes des employé.e.s à la direction.

En lisant ce scénario, réfléchissez au cycle de vie des données et formulez des questions ou des demandes à l'intention de la direction qui se rapportent à chaque étape du cycle de vie.

Quelles idées vous viennent à l'esprit et quelles protections offriraient-elles aux travailleurs.euses dans cette situation ?



N : METTEZ



LA DIRECTION PRÉSENTE UNE NOUVELLE APPLICATION :

La direction a informé les employé.e.s qu'ils/elles devaient télécharger une nouvelle application sur leur téléphone portable personnel. Cette application servira à modifier les horaires de travail, à signaler les jours de congé maladie et les jours de vacances, et son utilisation est obligatoire. De plus, grâce aux données de géolocalisation, l'application enregistrera automatiquement le temps de travail en vérifiant l'arrivée et le départ des employé.e.s lorsqu'ils/elles se trouvent à moins de 5 mètres de la porte d'entrée.

La direction a informé les employé.e.s que les concepteurs de l'application sont basés en Europe et que les données sont stockées sur un serveur web Amazon en Inde.

Vous avez des questions concernant cette application et souhaitez négocier son utilisation sur le lieu de travail. D'après ce que vous savez, quelles questions, propositions ou demandes avez-vous ?

QU'AVEZ-VOUS TROUVÉ ?

ÉTAPE 1

Une exigence : il devrait être interdit à la direction d'obliger les employé.e.s à télécharger une application sur leur téléphone personnel.



ÉTAPE 2

Une question : étant donné que cette application est utilisée pour modifier les horaires de travail, comment la vie privée des employé.e.s est-elle préservée ?



Il s'agit d'un moyen intrusif d'accéder aux informations personnelles des employé.e.s. Souvent, ce type d'applications peut être utilisé pour collecter davantage de données que ce qui est indiqué. En utilisant un téléphone fourni par leur employeur, les employé.e.s peuvent mieux préserver leur vie privée et leur équilibre entre vie professionnelle et vie privée.

Si un.e travailleur.euse doit souvent changer d'horaire, cela peut être dû à des raisons personnelles, confidentielles ou liées à sa santé. Le système permet-il à l'ensemble du personnel de voir qui a saisi des demandes de changement d'horaire ? Quelles mesures ou précautions sont prises pour garantir la vie privée des travailleurs.euses ?

ÉTAPE 3

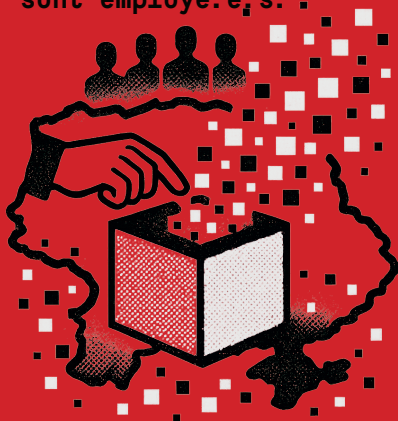
Une exigence : la direction ne devrait pas traiter automatiquement le temps de travail comme elle l'a proposé.



Dans de nombreux lieux de travail, tels que les hôpitaux, les écoles et l'administration publique, le travail peut être principalement effectué à l'intérieur d'un bâtiment, mais les travailleurs.euses peuvent quitter les lieux pour répondre à certaines exigences professionnelles, comme aider les patient.e.s à se rendre à leur véhicule, surveiller les enfants pendant la récréation ou assister à une réunion à l'extérieur. Si la direction traite les données comme proposé, aucune de ces fonctions ne serait considérée comme du temps de travail.

ÉTAPE 4

Une exigence : les données des travailleurs.euses doivent être stockées dans la même juridiction que celle où ils sont employé.e.s.



Les protections des données inscrites dans la loi varient selon les régions. Le meilleur moyen de garantir que les droits des travailleurs.euses soient protégés au moins selon les normes locales consiste à exiger que les données soient stockées localement et à interdire la vente des données du personnel. Cela aidera les travailleurs.euses à garder le contrôle sur leurs informations personnelles.

LE CYCLE DES DONNÉES APPARTIENT AUX TRAVAILLEUR.EUSES

De la collecte au stockage, les données sur le lieu de travail ne sont jamais neutres. Chaque goutte d'information façonne la manière dont le pouvoir circule : qui décide, qui surveille, qui en profite.

Les employeurs et les systèmes numériques chercheront toujours des moyens d'étendre leur contrôle grâce aux données. Les travailleurs.euses et les syndicats doivent y répondre par la vigilance, la créativité et la solidarité :

- **RÉSISTEZ À LA COLLECTE INTRUSIVE.**
- **CONTRÔLEZ L'ACCÈS.**
- **FIXER DES LIMITES À L'ANALYSE.**
- **EXIGEZ UN STOCKAGE LOCAL SÉCURISÉ.**

Ce guide a été élaboré par la Fédération syndicale internationale des services publics en collaboration avec Friedrich-Ebert-Stiftung & Christina Colclough du Why Not Lab pour être utilisé par les syndicats du monde entier.



Pour en savoir plus sur notre travail en matière de digitalisation et accéder à d'autres ressources utiles, consultez notre page consacrée à la digitalisation.