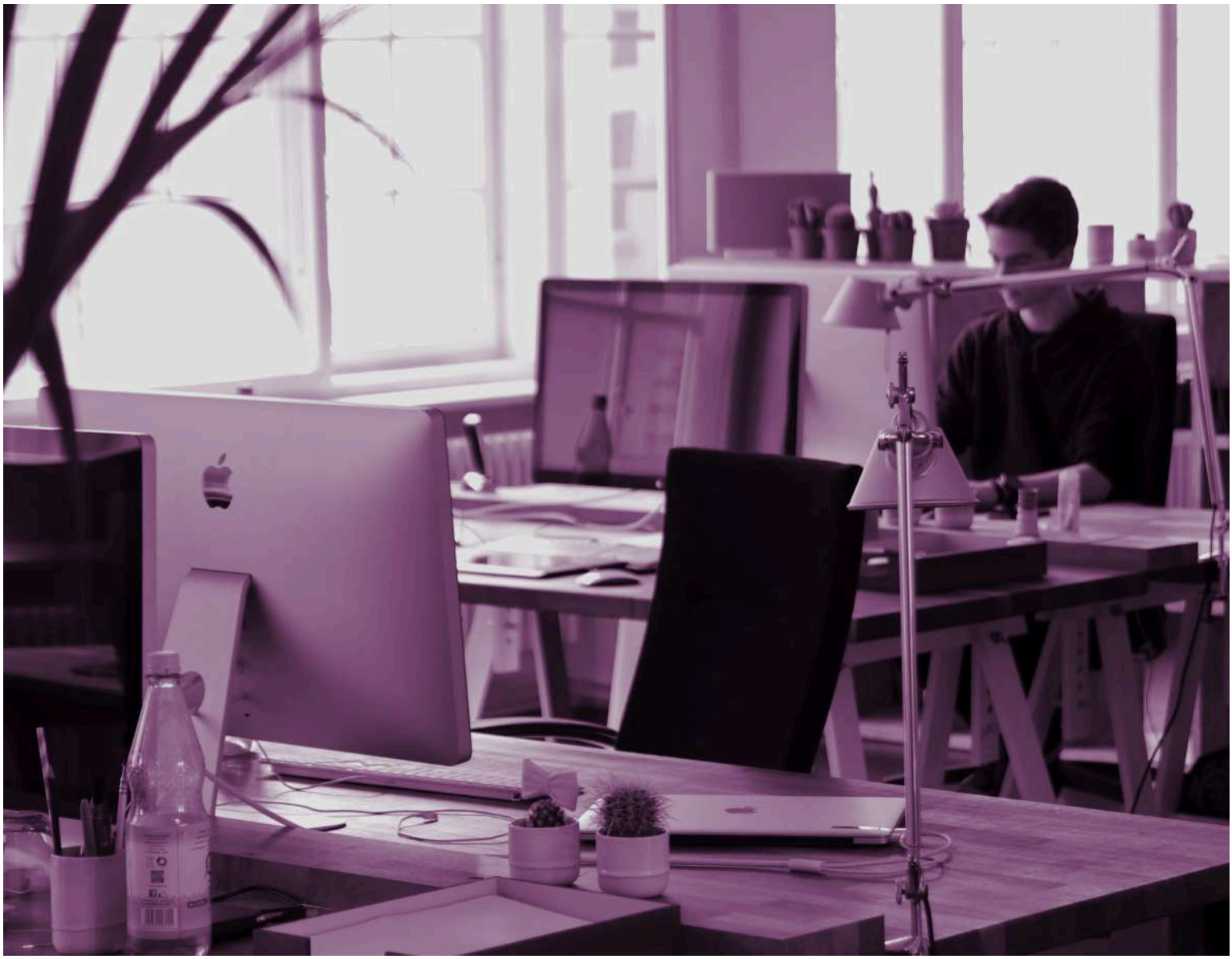
10 PRINCIPI CHIAVE

PER LA PROTEZIONE E LA PRIVACY DEI DATI DEI LAVORATORI



UNI Global Union

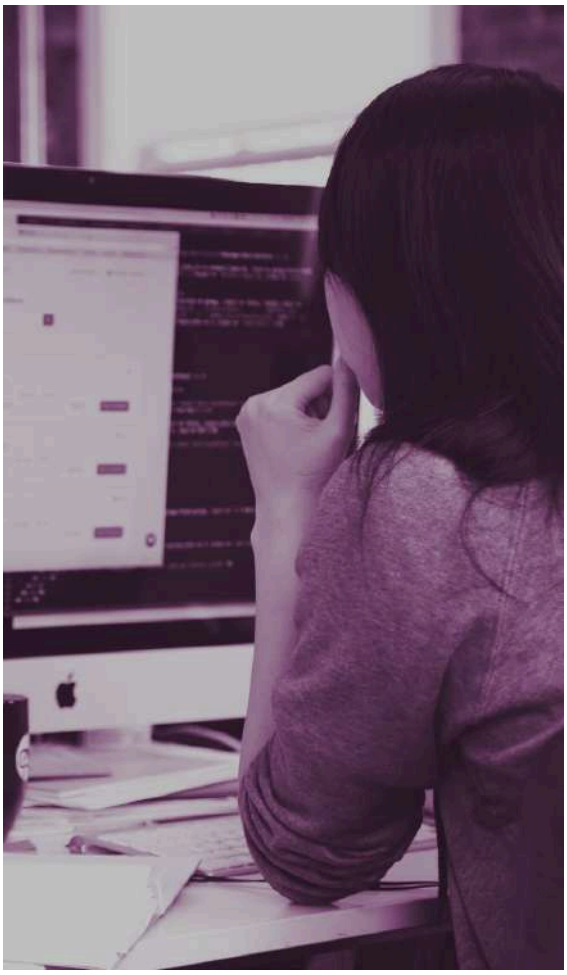
UNI Global Union, con sede a Nyon in Svizzera, rappresenta più di 20 milioni di lavoratori di oltre 150 Paesi nei settori più in crescita nel mondo – competenze e servizi. Il futuro del mondo del lavoro è stata una delle priorità principali per UNI Global Union negli ultimi anni. Con una voce importante sulla politica globale e a livello industriale, UNI cerca politiche innovative e partnership per assicurare a tutti un futuro digitale responsabile. Con urgenza, UNI richiama tutte le imprese e i governi a collaborare con il movimento sindacale, per co-creare una transizione giusta per un futuro del lavoro decente. Dalla progettazione di nuove tecnologie, intelligenza artificiale e algoritmi, all'impatto sugli utenti finali, le considerazioni etiche e sociali devono essere fatte mettendo al primo posto le persone e il pianeta.

UNI Global Union
8-10 Av Reverdil
1260 Nyon
Switzerland

www.uniglobalunion.org
www.thefutureworldofwork.org

INDICE

Introduzione



Mentre dati, big data e set di dati sono sempre più utilizzati dalle aziende per ispirare le decisioni imprenditoriali, la protezione dei dati e le regole sulla privacy difficilmente sono presenti.
Questo documento fornisce 10 principi operativi per affrontare questo squilibrio.
Fornendo concrete richieste sulla raccolta dei dati aziendali e il loro uso, questi principi mettono i lavoratori nelle condizioni di garantire un uso dei dati etico e sostenibile.
C'è una precisa urgenza al momento.
Bisogna agire per salvaguardare gli interessi dei lavoratori e mantenere una buona forza di contrattazione nei luoghi di lavoro.
I 10 principi forniti in questo documento sono stati sviluppati da UNI Global Union con questo scopo.

I dati sono stati definiti come il nuovo oro. È commercializzato, analizzato e usato nel marketing, nella pubblicità nella gestione delle risorse umane. È una delle basi dell'intelligenza artificiale e degli algoritmi.

È stato stimato che entro il 2030 il 15-20% del prodotto interno lordo complessivo mondiale sarà costituito dai flussi di dati. Sta anche alla base delle miriadi di nuove imprese e servizi che stanno costantemente individualizzando molti aspetti della nostra economia e società, cioè le piattaforme della cosiddetta gig economy.
Come cittadini, ogni giorno lasciamo dietro di noi una scia di dati: da ciò che cerchiamo su Google, alle app sui nostri smartphone, dalle corse sui taxi, agli appartamenti in affitto, da ciò che compriamo alle nostre "carte fedeltà", dai registri sanitari alle chiamate al servizio clienti. Per non parlare dei posti che visitiamo, delle e-mail che inviamo, gli amici che abbiamo su Facebook e i tweet che scriviamo.
Così facendo forniamo alle società dati su di noi e la nostra rete di amici. I dati sono il regalo più grande che offriamo senza che ce ne accorgiamo.
Forniamo dati anche come lavoratori – i nostri CV, i dati biometrici come le impronte digitali o la scansione dell'iride, e i numerosi dati raccolti dai datori di lavoro attraverso il monitoraggio dei flussi di lavoro.
I dati, o meglio i set di dati da dentro e fuori l'azienda, sono usati anche dal management nelle decisioni delle risorse umane.
Chi è stato assunto? Chi promosso? C'è qualcuno da licenziare o ammonire? I lavoratori sono produttivi oggi? Se no, perché? L'uso nelle aziende ha persino spinto a domandarsi se i dati stanno prendendo il posto delle risorse umane.

Ma in realtà chi possiede i dati che forniamo? E quali dati esistono "lì fuori" che riguardano me e te? Sono due domande cui è difficile rispondere.
Il CEO di LinkedIn ha dichiarato che la stragrande maggioranza dei dati mondiale è sostanzialmente nelle mani delle big della tecnologia: Google, Facebook, Amazon, Microsoft e Apple.
Una recente comunicazione di Twitter sosteneva che per mille dollari si può avere grazie a una società tutte le informazioni possibili su una persona. Sappiamo che alcune aziende sono esperte nello scovare dati e venderli ad altri così da manipolare i nostri punti di vista. Targetizzandoci con storie specifiche e pagando account Facebook e Twitter fasulli per diffondere opinioni, ora sappiamo che sia le elezioni statunitensi e i risutalti del voto della Brexit sono stati influenzati e manipolati usando i dati.
In Giappone il governo sta preparando il lancio dei cosiddetti "databanks" (banche del dato). Gli uffici pubblici aiuteranno i cittadini a scegliere quali dati vogliono rendere disponibili. In Estonia, uno dei Paesi con l'uso di dati e sistemi di e-government più completi al mondo, i dati dei cittadini sono soggetti a rigorosi principi legali che rafforzano l'individuo nel decidere quali dati rendere disponibili e come possono essere usati. Ancora molti Paesi sono rimasti indietro nell'informare i cittadini in maniera chiara e trasparente sui modi di conoscere quali informazioni esistono e, non meno importante, dare loro gli strumenti per controllarli.
Mentre le leggi sulla privacy e la protezione dei dati esistono in varie forme in diversi Paesi, i dati derivanti dal monitoraggio dei lavoratori non sono strettamente coperti da queste leggi. UNI Global Union sta cooperando con l'organizzazione mondiale IEEE (Institute of Electrical and Electronics Engineers) per creare uno standard globale per una governance datoriale trasparente dei dati dei lavoratori. È altrettanto centrale che i sindacati cerchino di implementare, attraverso accordi collettivi e/o aziendali, i diritti sui dati dei lavoratori e le misure di protezione.
Senza le suddette misure, l'ago della bilancia penderà sempre a favore delle decisioni unilaterali dei manager che possiedono i dati nelle aziende.
Data la relativa facilità di combinare i dati da diverse fonti, senza un intervento sul tipo e su come i dati siano usati, i lavoratori saranno molto svantaggiati. Infatti, i diritti e la protezione dei dati dei lavoratori saranno la prossima frontiera per i sindacati man mano che l'economia digitale prende forma.

> "
> I lavoratori e i loro rappresentanti sindacali devono avere accesso, determinare, modificare e cancellare sia i dati raccolti che li riguardano, sia quelli raccolti durante i processi di lavoro.
> "

Data l'importanza dei dati nei luoghi di lavoro, UNI Global Union chiede che i lavoratori e i loro rappresentanti sindacali debbano avere il diritto di avere accesso, determinare, modificare e cancellare sia i dati raccolti che li riguardano, sia quelli raccolti durante i processi di lavoro.

Questo documento rende operative le richieste principali suddividendole in 10 punti di azione.

1. I lavoratori devono avere accesso e influenza sui dati che riguardano loro

I lavoratori devono avere il diritto di accedere ai dati raccolti che li riguardano, incluso il diritto a rettificarli, bloccarli o cancellarli.

Questo include:

A) che il consenso non possa, e non debba, essere la base legale del processo dei dati a lavoro;
B) che un lavoratore debba avere la possibilità di ottenere, su richiesta, a intervalli ragionevoli e senza eccessivi ritardi, la conferma di un'elaborazione di dati personali che lo/la riguardano. La comunicazione deve essere in forma intelligibile e includa tutte le informazioni sull'origine dei dati, così come le altre informazioni che il dirigente ha richiesto di fornire per assicurare la trasparenza del trattamento;
C) che un lavoratore abbia il diritto alla portabilità dei dati. Per esempio, il diritto a spostare le valutazioni e i sistemi di valutazione da una piattaforma all'altra;
D) che a seconda delle leggi nazionali, o dei termini presenti nei contratti collettivi, i dati personali vengano comunicati ai rappresentanti dei lavoratori, ma solo nel caso in cui questi dati siano necessari per consentire loro di rappresentare al meglio gli interessi dei lavoratori o se questi dati siano necessari per l'adempimento e il controllo degli obblighi previsti nei contratti collettivi.

2. Applicare misure di sicurezza per l'elaborazione di dati sostenibili

Per tutte le forme di trattamento dei dati, i datori di lavoro devono rispettare le seguenti misure di sicurezza. In particolare:

A) informare i lavoratori in maniera chiara e completa prima dell'introduzione di sistemi informativi e tecnologie capaci di monitorare le loro attività. L'informativa fornita deve essere aggiornata e deve prendere in considerazione il principio 3 sottostante. L'informativa deve includere lo scopo dell'intervento, la conservazione o il periodo di back-up, così come la presenza dei diritti dei lavoratori nell'accedere e rettificare i dati e come quei diritti devono essere esercitati. Queste misure di sicurezza includono qualsiasi modifica agli scopi del monitoraggio e i sistemi e le tecnologie suddette;
B) prendere appropriate misure interne relative al trattamento di questi dati e informare i lavoratori in anticipo. Ciò include la realizzazione di una valutazione d'impatto sulla privacy quando le tecnologie possono provocare un alto rischio per gli individui, come nel caso in cui ci si possa trovare di fronte a una potenziale analisi comportamentale o decisioni prese tramite sistemi automatizzati (vedi principio 5);

C) consultare i lavoratori nei casi in cui ci sia il sospetto di una possibile violazione dei diritti dei lavoratori in termini di privacy e dignità umana. Riguardo a questi casi, i lavoratori hanno il diritto di richiedere il veto sul monitoraggio dei dati in questione fino a quando il datore di lavoro possa provarlo per iscritto e di conseguenza ricevere l'approvazione dei lavoratori che il diritto di questi ultimi al rispetto della privacy e della dignità umana sia pienamente preservato (vedi principio 5).

3. Applicare il principio di minimizzazione dei dati

Il principio prevede che i datori di lavoro possano solo:

> "
>
> Raccogliere i dati solo per gli scopi necessari, usarli solo per le persone coinvolte e solo per il tempo necessario.
>
> "

I datori di lavoro devono creare misure appropriate per assicurare, concretamente, il rispetto dei principi e degli obblighi relativi alla gestione dei dati per scopi lavorativi. Sono inclusi i principi di proporzionalità e sussidiarietà: la raccolta dei dati deve essere limitata a ciò che è necessario per raggiungere gli obiettivi della raccolta in questione come, per esempio, il contenuto e la forma dell'azione devono essere coerenti con lo scopo perseguito.

A seguito di una richiesta di controllo da parte delle autorità, i datori di lavoro devono essere capaci di dimostrare la loro conformità a questi principi e obblighi. Tali misure devono essere adattate al volume e alla natura dei dati processati, il tipo di attività svolte, e devono anche essere prese in considerazione possibili implicazioni sui diritti fondamentali e le libertà dei lavoratori.

4. Elaborare i dati in maniera trasparente

A) Le informazioni relative ai dati personali gestite dai datori di lavoro devono essere disponibili anche al lavoratore in questione direttamente o tramite un suo rappresentante intermediario, o notificate attraverso altri mezzi appropriati.

B) I datori di lavoro devono fornire ai lavoratori le seguenti informazioni:

- Le categorie di dati personali processati e una descrizione degli scopi del trattamento
- I destinatari, o le categorie di destinatari dei dati personali
- Gli strumenti che i lavoratori possono usare per esercitare i diritti fissati nel principio 1 senza pregiudizio verso norme nazionali più favorevoli già presenti.

C) Deve essere fornita una descrizione completa e chiara delle categorie di dati personali che possono essere raccolti dal reparto Information and Communications Technologies (ICT), inclusa la videosorveglianza e il loro uso possibile.

D) Le informazioni devono essere in un formato accessibile e aggiornato. In ogni caso, tali informazioni devono essere fornite prima che un dipendente svolga l'attività o l'azione in questione e rese prontamente disponibili attraverso i sistemi informativi usati solitamente dal lavoratore.

5. Rispettare le leggi sulla privacy e i diritti fondamentali in tutta l'azienda

Incluso il rispetto per tutte le convenzioni internazionali e nazionali sui diritti umani, per esempio:

- La Dichiarazione universale dei diritti umani delle Nazioni Unite
- Codice di condotta dell'ILO: Protezione dei dati personali dei lavoratori (1997)

Il datore di lavoro deve anche:

A) mostrare rispetto per la dignità umana, la privacy e la protezione dei dati personali devono essere salvaguardati nella gestione dei dati personali per motivi di impiego, specialmente per consentire il libero sviluppo della personalità del lavoratore e per dare opportunità di relazioni sociali e individuali nel luogo di lavoro;
B) garantire una comunicazione che rispetti le regole e non includa frasi ingiuriose o diffamatorie;
C) assicurare che gli strumenti di comunicazione d'impresa non siano usati come mezzi di molestia sessuale o per diffondere commenti offensivi atti a discriminare.

Il datore di lavoro può richiedere una dichiarazione di non responsabilità quando i lavoratori comunicano internamente ed esternamente così che le comunicazioni espresse siano in capo al solo autore e non all'azienda.

6. Dare ai lavoratori il diritto di spiegazione quando vengono usati i dati

Questo principio si riferisce alle decisioni prese dal management quando si procurano dati da dentro e fuori l'azienda. Per esempio, durante i processi esterni e interni di assunzione, i lavoratori devono avere il diritto di sapere su quale base una decisione sia presa, così da proteggere i lavoratori contro decisioni discriminatorie basate sulla predizione dei dati, così come su quelli riguardanti la salute.

Il lavoratore deve essere informato quando sono prese importanti decisioni sulla base di dati esterni e/o interni.

7. Escludere i dati biometrici e le Personally Identifiable Information (PII)

La raccolta e il successivo trattamento di dati biometrici devono essere svolti solo nel caso in cui non ci siano altri strumenti meno indiscreti disponibili e solo se corredati da corrette tutele, incluse le tutele previste nel principio 2.
Il trattamento di dati biometrici e altri PII si deve basare su metodi riconosciuti scientificamente. E deve essere soggetto ai requisiti di rigida sicurezza e proporzionalità.

8. Dispositivi che rilevano la posizione del lavoratore

I dispositivi che rilevano la posizione dei lavoratori possono essere introdotti solo se si prova la necessità di raggiungere lo scopo legittimo perseguito dai datori di lavoro. Il loro uso non deve portare a un continuo monitoraggio dei lavoratori.
In particolare, il monitoraggio non può essere lo scopo, ma solo l'indiretta conseguenza di un'azione necessaria per proteggere la produzione, la salute e la sicurezza o per garantire lo svolgimento efficiente di un'organizzazione.
Data la potenziale violazione dei diritti e delle libertà delle persone coinvolte dall'uso di questi dispositivi, i datori di lavoro devono assicurare tutte le tutele necessarie relative al diritto alla privacy e alla protezione dei dati dei lavoratori, incluse le tutele previste nel principio 2.
Secondo quanto previsto dal principio 3 sulla minimizzazione dei dati, i datori di lavoro devono prestare particolare attenzione allo scopo per cui tali dispositivi siano usati. I datori di lavoro devono applicare precise procedure interne relative al trattamento di questi dati e devono comunicarlo in anticipo alle persone coinvolte.

9. Creare un ente interaziendale e multidisciplinare per la governance dei dati

Sarebbe utile creare un ente di governance dei dati interaziendale e multidisciplinare per gestire la formazione dei dati, l'archiviazione, il trattamento e i problemi di sicurezza. Ciò include disposizioni in base alle quali tutti i rappresentanti dell'ente, inclusi i delegati sindacali, ricevano un'adeguata formazione sui dati da trattare con le aziende per confermare o rifiutare una policy di protezione dei dati sostenibile.

10. Quanto scritto sopra deve essere applicato nei contratti collettivi

I principi suddetti dovrebbero essere implementati e fatti applicare tramite la contrattazione collettiva o aziendale. In mancanza di tale contrattazione, il datore di lavoro dovrebbe creare un organismo di governance in conformità con il principio 9.

Bibliografia

Questo documento ha tratto ispirazione e idee dai seguenti documenti:

GDPR
(http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT)

COE(2015) Recommendation CM/Rec(2015) of the Committee of Ministers to member States on the processing of personal data in the context of employment
https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

(2017): ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 2/2017 on data processing at work http://ec.europa.eu/newsroom/document.cfm?doc_id=45631