10 principais princípios para a proteção e privacidade dos dados dos trabalhadores

UNI Global Union

Sobre a UNI União Global

A UNI União Global está sediada em Nyon, na Suíça e representa mais de 20 milhões de trabalhadores provenientes de mais de 150 países dos mais variados setores em crescimento no mundo – aptidões e serviços. O futuro do mundo do trabalho tem sido uma das principais prioridades da UNI nos últimos anos. Assumindo uma voz de liderança na política global e na indústria, a UNI pretende desenvolver políticas e parcerias inovadoras para potenciar um futuro digital para todos. A UNI entende que, todos os parceiros e governos devem unir-se, com urgência, ao movimento sindical no sentido da criação de uma transição justa para um futuro digno no trabalho. Desde projetos de novas tecnologias, IA e algoritmos, ao impacto nos utilizadores, as considerações ético-sociais devem ser feitas por forma a colocar as pessoas e o planeta primeiro.

UNI Global Union www.uniglobalunion.org
8-10 Av Reverdil www.thefutureworldofwoek.org
1260 nyon
Suiça

Contents

Introdução

Embora os dados pessoais, *big data* e *data sets* sejam cada vez mais utilizados pelas empresas para fundamentar decisões de gestão, as regras sobre a proteção de dados e privacidade dos trabalhadores são quase inexistentes. O presente documento fornece 10 princípios operacionais que permitem lidar com esta questão. Estes princípios permitem às empresas a utilização ética e sustentável dos dados e assegura aos trabalhadores essa mesma utilização, através da imposição de exigências concretas sobre a recolha e uso de dados.

A urgência de atuação imediata é enorme. É necessário adotar medidas que salvaguardem os interesses dos trabalhadores e mantenham um equilíbrio saudável do poder nos locais de trabalho. Os 10 princípios fornecidos neste documento foram desenvolvidos pela UNI com esse propósito.

Os dados têm sido denominados como "*o novo ouro*". São negociados, analisados e utilizados na gestão de marketing, publicidade e recursos humanos. São também a base da construção da inteligência artificial e dos algoritmos. Estima-se, que em 2030, 15-20% do PIB mundial combinado seja baseado no fluxo de dados. São também o alicerce dos novos negócios e serviços que cada vez mais individualizam vários aspetos da nossa economia e sociedade, nomeadamente as plataformas da chamada economia *gig*.

Como cidadãos criamos, diariamente, um rasto de dados: desde as pesquisas no Google às apps nos nossos telemóveis, às corridas de táxi, ao contrato de arrendamento dos nossos apartamentos, compras, cartões de fidelização, registos de saúde, chamadas telefónicas para clientes, para lá dos sítios que visitamos, emails que enviamos, amigos do Facebook e "Tweets" que escrevemos. Ao fazermos tudo isto, fornecemos dados às empresas - não apenas sobre nós, mas sobre a nossa rede de amigos. Os dados são a maior oferta que não nos apercebemos que estamos a entregar.

Também fornecemos dados enquanto trabalhadores – nos CVs, nos nossos dados biométricos (tais como impressões digitais e nos scans oculares), e na quantidade de dados que são extraídos pela monitorização dos nossos processos de trabalho. Os dados, ou melhor, o conjunto de dados, vindo de dentro e de fora das empresas são também utilizados pelos órgãos diretivos para tomarem decisões a nível dos recursos humanos. Quem é contratado? Quem é promovido? Quem deverá ser despedido ou advertido? São os trabalhadores produtivos? E se não são, porque não? A aplicação e uso dos dados nas empresas hoje em dia levanta a questão de saber se os dados estão a retirar a parte humana dos recursos humanos.

Mas quem é, na verdade, proprietário dos dados que fornecemos? E que informação existe espalhada sobre nós? É difícil responder a estas duas questões. O CEO da Linkedin afirmou que a maior parte dos dados mundiais estão nas mãos das grandes empresas de tecnologia: Google, Facebook, Amazon, Microsoft a Apple. Um *feed* recente no Twitter refere que por 1000 USD, uma empresa pode fornecer-nos toda e qualquer informação sobre alguém. Sabemos que algumas empresas são especialistas em minar dados e vendê-los a outras para que essas empresas possam manipular os nossos pontos de vista. Somos bombardeados com histórias particulares e com a subscrição de contas falsas no Twitter e no Facebook para espalhar opiniões. Sabemos agora que as eleições norte americanas e o resultado do referendo do Brexit foram influenciados e manipulados pelo uso de dados.

O governo do Japão prepara-se para implementar os chamados bancos de dados. Escritórios públicos que ajudarão os cidadãos a decidir o tipo de dados que querem disponibilizar. Na Estónia,

um dos países do mundo com um e-governo mais desenvolvido nas matérias do uso de sistemas de dados, os dados relativos aos cidadãos estão sujeitos a princípios legais rigorosos, dando o poder aos cidadãos de decidirem quais os dados a disponibilizar e a forma como serão usados. No entanto, há ainda muitos países que não fornecem aos seus cidadãos uma forma clara e transparente de estes saberem o tipo de informação existente, nem a forma de a poderem controlar.

Embora existam, sob várias formas, normas sobre privacidade e proteção de dados, em vários países, os dados provenientes da monitorização de trabalhadores não estão especificamente abrangidos por essa legislação. A UNI União Global está, em cooperação com a organização global IEEE, a criar um padrão global para a transparência no uso dos dados dos trabalhadores pelos empregadores. É também vital que os sindicados procurem implementar, através das convenções coletivas de trabalho e/ou acordos de empresa, direitos sobre os dados dos trabalhadores e determinações de tutela desses direitos. Sem estas determinações, o balanço do poder nas empresas cairá sempre, unilateralmente, para o lado de que tem a informação e toma as decisões. Dada a relativa facilidade em reunir dados provenientes de várias fontes, sem que os trabalhadores possam dizer que informação pode ser utilizada e como, estes estarão em grande desvantagem. O direito e proteção dos dados dos trabalhadores pode, na verdade, vir a ser classificado como o próximo desafio para os sindicatos á medida que a economia digital toma forma.

“Os trabalhadores e os seus representantes sindicais devem ter direito a aceder, influenciar, editar e apagar os dados que são recolhidos sobre eles através dos seus processos de trabalho”

Devido á importância dos dados no local de trabalho, a UNI União Global exige que os trabalhadores e os seus representantes sindicais tenham o direito de aceder, influenciar, editar e apagar os dados que são recolhidos sobre eles através dos seus processos de trabalho.

Este documento materializa esta exigência principal dividindo-a em 10 pontos de ação específicos.

1. Os trabalhadores devem ter acesso e influência sobre os dados recolhidos sobre eles

Os trabalhadores devem ter o direito de aceder aos dados recolhidos sobre eles, incluindo o direito de retificar, bloquear ou apagar esses dados.

O referido direito determina, nomeadamente:

A. Que o consentimento não pode, e não deve ser a base legal do processamento de dados no trabalho.
B. Que o trabalhador deve poder obter, mediante pedido, com intervalos razoáveis e sem atrasos excessivos, confirmação do processamento de dados a si referentes. A comunicação deve ser feita de forma inteligível, incluindo toda a informação sobre a origem dos dados, assim como qualquer outra informação requerida ao detentor dos dados e que garanta a transparência do processo.
C. O trabalhador deve ter o direito á portabilidade dos dados, i.e., o direito de mover sistemas de avaliação e classificação de uma plataforma para outra.
D. Conforme os usos e a legislação nacional, ou os termos das convenções coletivas de trabalho, os dados pessoais devem ser comunicados aos representantes dos trabalhadores apenas se esses dados forem necessários para uma melhor representação dos interesses dos trabalhadores ou se forem necessários ao cumprimento e supervisão das obrigações constantes dessas convenções.

2. A Implementação sustentável de processos para proteção dos dados

Em todas as formas de tratamento de dados os empregadores devem respeitar as seguintes garantias. Em particular:

A. Informar clara e integralmente os trabalhadores antes da introdução de sistemas de informação e tecnologias que lhes permitam monitorizar as suas atividades. A informação fornecida deve atualizada periodicamente e deve ter em conta os princípios referidos nos três pontos seguintes. A informação deve conter a finalidade da operação, a preservação ou atualização periódica, e os direitos dos trabalhadores de aceder e retificar, contendo também a forma como esses direitos podem ser exercidos. Estas garantias estendem-se a quaisquer alterações às finalidades de tratamento e sistemas de monitorização.
B. Adotar medidas internas adequadas ao processamento da informação e notificar os trabalhadores antecipadamente, realizando uma avaliação de impacto de violação de privacidade quando a utilização das tecnologias possa acarretar riscos elevados para os indivíduos, nomeadamente no caso de criação potencial de perfis ou nos casos decisões tomadas exclusivamente por sistemas automáticos (*vide* principio 5 abaixo).
C. Consultar os trabalhadores sempre que exista uma suspeita de violação dos direitos dos trabalhadores no que respeita á privacidade dos dados e á dignidade da pessoa humana. Nestes casos, deve ser permitido e cumprido o direito de os trabalhadores pedirem um veto à monitorização da informação por parte do empregador até que este logre provar por escrito, e recebendo subsequentemente a aprovação dos trabalhadores, que os direitos do

trabalhador no que respeita á privacidade e á dignidade da pessoa humana são respeitados (*vídeo* principio 5).

3. O princípio da minimalização de dados deve ser aplicado

Segundo este princípio os empregadores apenas podem:

"Recolher informação e apenas a informação adequada para os devidos propósitos e limitada a esses mesmos propósitos, para ser utilizada pelas pessoas autorizadas e apenas por essas pessoas durante o tempo necessário e apenas pelo tempo necessário."

Os empregadores devem desenvolver medidas apropriadas para garantir que, na prática, sejam respeitados os princípios e as obrigações relacionados com o processamento de dados para fins de empregabilidade. Isto inclui os princípios de proporcionalidade e subsidiariedade: a recolha de dados deve ser limitada ao que é necessário para a obtenção dos objetivos da recolha em questão, ou seja, o conteúdo e a forma das condutas adotadas devem manter-se de acordo com o objetivo pretendido.

A pedido das autoridades supervisoras, os empregadores devem demostrar o cumprimento destes princípios e obrigações. Estas medidas devem ser adaptadas à natureza e ao volume do processamento de dados, ao tipo de atividades a realizar e deve também ser tida em conta a possibilidade de implicações nos direitos e liberdades fundamentais dos trabalhadores.

4. Processamento de dados deve ser transparente

A informação respeitante aos dados do pessoal na posse dos empregadores deve ficar acessível ao trabalhador a que diz diretamente respeito ou a um representante deste, ou ser levada ao seu conhecimento por qualquer outro meio adequado.

Os empregadores devem disponibilizar aos trabalhadores a seguinte informação:

A. As categorias dos dados pessoais a serem processados e descrição dos propósitos do processamento;
B. Os recetores ou a categoria dos recetores dos dados pessoais;
C. Os meios que os trabalhadores têm para exercer os direitos descritos no princípio 1, sem prejuízo de outros mais favoráveis fornecidos pela legislação nacional;
D. Qualquer outra informação necessária para garantir um tratamento de dados lícito e leal
E. Deve ser fornecida uma descrição extensivamente clara e completa sobre as categorias de dados pessoais que podem ser recolhidos pelas TICs (Tecnologias de Informação e Comunicação), incluindo a vídeo vigilância e o seu possível uso.
F. A informação deve ser fornecida num formato acessível e deve ser mantida atualizada. Em qualquer caso, tal informação deve ser fornecida antes que o empregado desempenhe a atividade ou ação a que respeita e a sua leitura deve ser disponibilizada através dos sistemas de informação normalmente usados pelo empregado.

5. As normas sobre privacidade e os direitos fundamentais devem ser respeitados por toda a empresa

Isto inclui o respeito por todas as convenções, regionais e globais, sobre os direitos humanos, incluindo:

A. A declaração universal dos direitos humanos da ONU.
B. O código sobre a prática internacional de procedimentos no trabalho de 1997 sobre a proteção dos dados pessoais dos trabalhadores.

O empregador deve ainda:

A. Demonstrar respeito pela dignidade da pessoa humana, pela privacidade e deve salvaguardar a proteção de dados pessoais no processamento de dados para fins laborais, nomeadamente para permitir o livre desenvolvimento da personalidade do trabalhador bem como para possibilitar o relacionamento individual e social no local de trabalho.
B. Garantir que a comunicação é feita de acordo com a lei e que não inclui declarações difamatórias.
C. Garantir que os meios de comunicação empresarial não são usados como meio de assédio sexual, ou para difundir comentários ofensivos com o intuito de descriminação.

O empregador pode exigir um termo de responsabilidade para as situações em que os trabalhadores comuniquem interna e/ou externamente, em que se enuncie as opiniões expressadas são da exclusiva responsabilidade dos autores e não da empresa.

6. Os trabalhadores devem ter direito total a uma explicação aquando do uso dos dados

Este princípio refere-se a decisões tomadas pela administração que envolvam o fornecimento de dados dentro e fora da companhia. A título de exemplo, nos processos de recrutamento internos e externos os trabalhadores devem ter o direito de conhecer os fundamentos da decisão tomada. Esta medida pretende salvaguardar os trabalhadores da tomada de decisões discriminatórias com base em previsões de dados relativamente à saúde.

O trabalhador deve ser informado quando são tomadas decisões importantes fundamentadas em dados quer internos quer externos.

7. Dados biométricos e informações pessoais identificáveis (IPI) devem estar isentos

A recolha e tratamento de dados biométricos só deve ser feita caso não exista outro meio menos intrusivo disponível e só se acompanhado de meios de salvaguarda adequados, incluindo as medidas de proteção adicionais descritas no Princípio 2.

O tratamento de dados biométricos e qualquer outra IPI deve ser baseado em métodos cientificamente reconhecidos e deve estar sujeito a exigências alargadas de segurança e proporcionalidade.

8. Equipamento revelador da localização dos empregados

O uso de equipamento que revela a localização dos trabalhadores só pode ser implementado se se provar necessário para que o empregador atinja propósitos explícitos e determinados; o seu uso não deve servir para a monitorização contínua dos trabalhadores. A monitorização não pode ser a finalidade desse uso, mas apenas uma consequência indireta de uma ação necessária para proteger a produção, a saúde ou a segurança ou para garantir o funcionamento eficiente da organização. Dado o potencial para a violação dos direitos e liberdades de pessoas relacionadas com o uso destes aparelhos, os empregadores devem garantir toda a proteção necessária para garantir o direito á privacidade e proteção de dados pessoais dos trabalhadores, incluindo as medidas de proteção adicionais descritas no Princípio 2.

De acordo com o Principio 3 sobre a minimalização de dados, os empregadores devem ter especial atenção ao fim para o qual estes aparelhos são usados. Os empregadores devem ter procedimentos internos relacionados com o tratamento destes dados e devem notificar antecipadamente a pessoa a quem digam respeito.

9. Deve ser estabelecido um organismo multidisciplinar entre empresas sobre dados

Deve ser estabelecido um organismo multidisciplinar entre empresas para tratar assuntos relativos à formação, armazenamento, tratamento e segurança de dados. Este princípio abrange normas que imponham que todos os representados nesse organismo, incluindo os delegados sindicais, recebam formação apropriada para estarem preparados para trabalharem com empresas na manutenção e preservação de uma política sustentável de proteção de dados.

10.Todos os princípios acima mencionados devem constar num acordo coletivo

Os princípios acima mencionados devem se implementados e reforçados através da contratação coletiva empresarial ou setorial. Na ausência dessas disposições, o empregador deve estabelecer um organismo de governação de acordo com o princípio 9.

Fontes:

Este documento é tem como fonte os seguintes documentos chave:

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