

**XXX CONGRESSO NACIONAL DO  
CONPEDI FORTALEZA - CE**

**DIREITO DO TRABALHO E MEIO AMBIENTE DO  
TRABALHO II**

**ALEXANDRE FERREIRA DE ASSUMPÇÃO ALVES**

**GILMAR ANTONIO BEDIN**

**DALTON TRIA CUSCIANO**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

**Diretoria - CONPEDI**

**Presidente** - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

**Diretor Executivo** - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

**Vice-presidente Nordeste** - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

**Representante Discente:** Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

**Conselho Fiscal:**

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

**Secretarias**

**Relações Institucionais:**

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

**Comunicação:**

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

**Relações Internacionais para o Continente Americano:**

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

**Relações Internacionais para os demais Continentes:**

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

**Eventos:**

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

**Membro Nato** - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

Direito do trabalho e meio ambiente do trabalho II [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Alexandre Ferreira de Assumpção Alves; Dalton Tria Cusciano; Gilmar Antonio Bedin. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-852-3

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito do trabalho. 3. Meio ambiente do trabalho. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34



# **XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE**

## **DIREITO DO TRABALHO E MEIO AMBIENTE DO TRABALHO II**

---

### **Apresentação**

É com júbilo que apresentamos as publicações referentes ao Grupo de Trabalho e Pesquisa (GT) denominado “Direito do Trabalho e Meio Ambiente do Trabalho II”, do XXX Congresso Nacional do CONPEDI, Fortaleza, Brasil, importante evento acadêmico promovido pelo CONPEDI em parceria com a UNICHRISTUS, com enfoque na temática “Acesso à Justiça Soluções de Litígios e Desenvolvimento”, tendo o evento sido realizado nos dias 15, 16 e 17 de novembro de 2023 na UNICHRISTUS - Campus Dom Luís (Av. Dom Luís, 911 - Bairro Meireles).

Trata-se de publicação que reúne artigos doutrinários, oriundos de projetos de pesquisa, artigos de final de disciplina de mestrado ou doutorado e estudos variados de diversos programas de pós-graduação no Brasil e nos Estados Unidos, que colocam em evidência assuntos jurídicos relevantes na seara do Direito do trabalho e meio ambiente do trabalho.

Os debates envolveram a subordinação algorítmica, a tecnologia como modificador do ambiente laboral e das relações de trabalho, o papel das mulheres nas organizações, o Burnout e doenças mentais relacionadas ao trabalho, a LGPD e a privacidade dos trabalhadores, a proteção internacional ao direito do trabalho, a arbitragem na seara trabalhista e os efeitos da pandemia do COVID-19 nas relações laborais e no acesso à justiça.

Os artigos apresentados neste GT DIREITO DO TRABALHO E MEIO AMBIENTE DO TRABALHO II, visaram realizar interfaces entre políticas públicas e grupos vulneráveis no meio ambiente do trabalho, numa perspectiva aberta, interdisciplinar, complexa e polissêmica.

Houve um intercâmbio de experiências entre todos os participantes e os Coordenadores do Grupo de Trabalho, promovendo a integração e aquisição de novos conhecimentos. Cada artigo agora publicado, passou por apresentações, discussões e recebeu contribuições colaborativas das ideias de cada pesquisador(a), visando o aprimoramento de debates que são fundamentais para o desenvolvimento jurídico nacional, especialmente no contexto da pesquisa sobre direito do trabalho e meio ambiente laboral.

Na ocasião, os coordenadores expressam sua homenagem e gratidão a todos que colaboraram para o sucesso do XXX Congresso do CONPEDI. Em particular, destacamos todos(as) os(as) autores(as) que contribuíram para a presente coletânea, reconhecendo o comprometimento e a seriedade evidenciados em suas pesquisas e na elaboração de textos de excelência.

Por fim, os Professores Doutores, Dalton Tria Cusciano, da Fundacentro/Ministério do Trabalho e do Programa de Mestrado da Ambra University, Alexandre Ferreira de Assumpção Alves, Professor da Universidade do Estado do Rio de Janeiro e da Universidade Federal do Rio de Janeiro e Gilmar Antonio Bedin, Professor da Universidade Regional do Noroeste do Estado do Rio Grande do Sul e da Universidade Regional Integrada, agradecem a Diretoria do CONPEDI pelo convite para coordenar o Grupo de Trabalho e externam votos de boa leitura a todos os interessados nos temas abordados.

## **A VIOLAÇÃO DA PRIVACIDADE E INTIMIDADE DO EMPREGADO EM DECORRÊNCIA DO AVANÇO TECNOLÓGICO.**

### **THE VIOLATION OF EMPLOYEE PRIVACY AND INTIMACY AS A RESULT OF TECHNOLOGICAL ADVANCEMENT.**

**Daniel de Almeida Alves  
Lucas Catib De laurentiis**

#### **Resumo**

Este artigo tem como objetivo fulcral investigar um dos maiores dilemas da contemporaneidade do meio ambiente do trabalho, qual seja, realizar uma análise por intermédio do método hipotético-dedutivo em como o crescente avanço tecnológico pode interferir na privacidade e intimidade dos empregados como potencial violador em sua dignidade. Neste sentido, este artigo abordará em como o avanço tecnológico, no qual engloba proteção de dados, geolocalização, tratamento de dados, algoritmos, banco de dados, big data, mineração de dados, elaboração de perfil, autodeterminação informativa, entre outros, são utilizados pelo empregador bem como as consequências negativas que podem advir pelo seu uso imoderado e irrestrito, nos quais culminam, no mais das vezes, em discriminações nocivas ao empregado (tais como discriminações de gênero; ideológicas; maternidade; orientação sexual etc.), obstaculizando o acesso do empregado ao mercado de trabalho ou até mesmo a manutenção de seu contrato de emprego em decorrência do conjunto de práticas denominadas background employment checks, nos quais, infelizmente, são de difícil comprovação pelo empregado, práticas estas cada vez mais utilizadas em conjunto com a Inteligências Artificial e machine learning.

**Palavras-chave:** Privacidade e intimidade do empregado, Avanço tecnológico, Proteção de dados, Autodeterminação informativa, Consequências discriminatórias

#### **Abstract/Resumen/Résumé**

This article aims to investigate one of the greatest dilemmas of the contemporary work environment, which is to carry out an analysis through the hypothetical-deductive method on how the growing technological advance can interfere in the privacy and intimacy of employees as a potential violator in their dignity. In this sense, this article will address how technological advancement, which encompasses data protection, geolocation, data processing, algorithms, database, big data, data mining, profiling, informational self-determination, among others, are used by the employer as well as the negative consequences that can arise from their immoderate and unrestricted use, in which they culminate, more often than not, in harmful discrimination against the employee (such as gender discrimination; ideological; maternity; sexual orientation etc. ), hindering the employee's access to the labor market or even the maintenance of his employment contract due to the set

of practices called background employment checks, in which, unfortunately, it is difficult to prove by the employee, practices that are increasingly used in conjunction with Artificial Intelligence and machine learning.

**Keywords/Palabras-claves/Mots-clés:** Employee privacy and intimacy, Technological advancement, Data protection, Informational self-determination, Discriminatory consequences

## 1 Introdução

O objetivo deste artigo é abordar como o avanço tecnológico pode ser um potencial violador da privacidade e intimidade do empregado uma vez que o avanço tecnológico permite que o poder fiscalizatório e disciplinar do empregador seja cada vez mais crescente, assemelhando-se à sociedade disciplinar foucaltiana.

A maior acessibilidade pelo empregador aos dados pessoais e sensíveis dos empregados permite uma intromissão indevida cada vez mais crescente sobre o comportamento do empregado, tanto em âmbito privado quanto em âmbito público e, o pior, na maioria das vezes sem a ciência ou consentimento do empregado.

Não se quer neste artigo desprestigiar a importância do uso da tecnologia e seus benefícios para a sociedade, mas de tão somente demonstrar que o seu uso exacerbado com a própria utilização de Inteligência Artificial (composta de dados e algoritmos) pode influenciar diretamente no cotidiano do empregado, inclusive de forma disruptiva e negativa, principalmente quando há o controle pelo uso de geolocalização (GPS), sistemas de áudio-videovigilância entre outros.

Neste cenário, a utilização da tecnologia pode acarretar violação da privacidade e intimidade do empregado principalmente quando aliada à Inteligência Artificial, *machine learning* e algoritmos, pois possibilita que haja criação de perfis de cunho homogeneizado e agravando aspectos discriminatórios em face do empregado que não corresponda ao padrão ou preferência social do empregador, obstaculizando a admissão ou até mesmo a manutenção do trabalho, mesmo com a vedação legal neste sentido, conforme se observa pela Lei nº 9.029/1995 (BRASIL, 1995).

Neste sentido, este artigo demonstrará diversos procedimentos adotados pelos empregadores que são intrusivos na vida privada e íntima do empregado, que se denomina como *background employment checks* que podem acarretar até em elaboração de “listas sujas”.

A utilização de algoritmos (algoritmização facilitada pela disponibilidade dos *Big Data* aliadas com a inteligência artificial) colaboram para estas discriminações, principalmente quando estão enviesados, podendo até se demonstrarem racistas, cujas práticas se encontram ocultadas pela possibilidade de manipulação e ocultação pelo segredo comercial envolvido, ou seja, ausência de transparência.

Neste sentido, uma das consequências verificáveis é a própria mineração de dados com o uso destas tecnologias (*Data Mining*) permitindo que haja uma análise preditiva e prescritiva, traçando comportamento e criando perfis dos empregados, em nítido desvio dos princípios da

adequação e finalidade pois sempre realizados sem o consentimento e conhecimento do empregado.

Mesmo os dados pessoais ou sensíveis disponibilizados pelo empregado em redes sociais, não significa que haja uma autorização tácita pela sua utilização pelo empregador, pois estes dados comumente não tem relação direta com as atividades exercidas pelo empregado e, portanto, não podem ser usados em seu desfavor, principalmente ao se levar em consideração que muitas das vezes os dados coletados podem estar desatualizados, falseados ou até mesmo imprecisos, podendo representar algo que não condiz com a realidade.

## **2 O avanço tecnológico como potencial violador da privacidade e intimidade**

O poder fiscalizatório e disciplinar do empregador avançou muito por causa da tecnologia, substituindo a vigilância hierarquizada de estilo militar *in locu* para meios alternativos e informatizados, permitindo fiscalização em tempo real independentemente de onde estiver o empregado e de forma que o trabalhador não consiga identificar quem está o monitorando.

Este tipo de fiscalização e vigilância oriunda da tecnologia, se assemelha à sociedade disciplinar (denominação cedida por Michel Foucault quando aborda a sociedade disciplinar que se originou em decorrência da migração para as cidades com o fim do feudalismo e advento da Revolução Industrial) e ao Panoptismo (idealizado por Jeremy Bentham e posteriormente aprofundado por Michel Foucault (2012)).

Esta analogia é pertinente pelo fato de que o empregado sabe que está sendo vigiado o tempo todo e em tempo real, mas não sabe quem está por trás o vigiando, acarretando maior internalização do medo e garantindo, ao empregador, maior disciplina do empregado, pois mesmo de forma subconsciente acabam agindo da maneira desejada pelo empregador, o que se traduz em gestão totalitária que visa obtenção e maximização do lucro por intermédio de uma coerção sutilmente imposta.

Com o avanço tecnológico e aplicação da inteligência artificial<sup>1</sup> cada vez mais presente na sociedade contemporânea com a conseqüente disseminação do uso desses meios

---

<sup>1</sup> Interessante os conceitos de Inteligência Artificial definidos pela Comissão Europeia e pela OCDE no qual “a IA é um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional” sendo um “sistema baseado em máquina que pode, para um determinado conjunto de objetivos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Usa entradas de máquina e/ou humanos para perceber ambientes reais ou virtuais; para extrair tais percepções em modelos (de forma automatizada, por exemplo com aprendizado de máquina ou manualmente); e para usar o modelo de inferência para formular opções de informação ou ação. Os sistemas de IA são projetados para operar com vários níveis de autonomia” (OECD, 2019b).



tecnológicos, possibilita que haja uma potencial invasão da privacidade dos empregados por diversos mecanismos diferentes, trazendo riscos aos dados pessoais, sendo que muitas das vezes sem a ciência dos empregados, tornando-se de suma importância alçar o direito à privacidade e à proteção de dados dos empregados como direitos fundamentais que devem ser tutelados não só em âmbito formal e dogmático, como no art. 5º, inc. X e LXXIX, da Constituição Federal de 1988, por exemplo (BRASIL, 1988) mas também dotados de aplicabilidade plena e eficácia imediata no ambiente laboral.

O tratamento de dados pessoais que são processados cada vez mais de formas automatizadas, permitem que haja um maior controle de forma unificada das diversas atividades do empregado em suas pormenoridades, possibilitando maior acessibilidade pelo empregador do comportamento do empregado em âmbito privado e público.

A automatização recorrente está atrelada com a própria utilização da Inteligência Artificial, pelo fato de ser composta de algoritmos e dados e sendo dividida comumente de duas maneiras: Inteligência Artificial centralizada e específica com capacidade de inteligência direcionada, utilizada para solucionar problemas normalmente com utilização de computação e matemática; Inteligência Artificial que se amolda e se aproxima com a capacidade intelectual humana, podendo até excedê-la em circunstâncias próprias.

A inteligência artificial pode ser benéfica em diversas áreas da sociedade, tais como na educação, energia, transportes, saúde, serviços públicos etc., porém acentua a potencialidade violadora da privacidade, proteção de dados e a não-discriminação, sendo no ambiente de trabalho ainda mais enaltecida em decorrência de sua transformação disruptiva, afetando a relação entre os empregados e entre estes e as máquinas, com influência direta no cotidiano do trabalhador, pois afeta a produtividade e eficiência em decorrência da própria monitorização e metodologias de aferição.

As inovações tecnológicas conduzem à sensação de controle pleno do empregado, uma vez que a automaticidade oriunda da tecnologia propicia maior controle, suplantando em eficácia a vigilância *in locu* realizada por pessoas. Este controle pode se dar à distância, como a utilização de geolocalização (GPS) e de sistemas com áudio-videovigilância, permitindo que as características fisionômicas, identidade visual do empregado, aparências e conversas sejam vigiadas, atentando também contra a privacidade dos trabalhadores.

Evidentemente que não se enquadra no arcabouço amplo protetivo da intimidade e privacidade do trabalhador quando o seu próprio titular disponibiliza suas informações, como ocorre, por exemplo, na disponibilidade de currículos eletrônicos, como é o caso do *LinkedIn*, que é uma plataforma de disponibilidade de currículos profissionais eletrônicos. Outro

exemplo, é o próprio Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) no qual também disponibiliza elaboração de currículos *lattes* daqueles que se dispuseram em fazê-lo. Nestes exemplos, não há, ao menos *a priori*, invasão da privacidade e intimidade<sup>2</sup>.

O avanço tecnológico também possibilitou que cada vez mais as pessoas disponibilizem informações pessoais na internet, principalmente os trabalhadores, incluindo quando são admitidos, sendo necessário disponibilizar diversas informações pessoais e muitas vezes sensíveis nos quais são organizados e estruturados com logicidade em banco de dados proporcionando ao empregador a maximização de aproveitamento deste conjunto de informações coletadas, desta maneira se potencializa as formas e variedades pelas quais estas informações podem ser utilizadas ou apropriadas uma vez que o banco de dados permite o aumento da comunicação de informações e da capacidade de armazenamento.

Cita-se, como exemplo, os próprios dados biométricos, nos quais, conforme o art. 5º, da Lei Geral de Proteção de Dados Pessoais (LGPD), são considerados dados sensíveis e, mesmo que não haja menção expressa acerca de sua proteção na relação laboral, é evidente e ululante que merece colhida a tutela pretendida aos dados biométricos na relação de trabalho, mormente pelo fato de se saber que o uso da biometria no pacto laboral é muito comum para se ter acesso ao sistema de informática nas empresas, principalmente para o registro de controle de ponto (ou para o acesso às dependências do empregador), consideradas práticas comumente utilizadas por décadas no Brasil, incluindo como outro exemplo a própria videovigilância, que têm impactos significativos no direito à privacidade dos trabalhadores, podendo ter abusos nestas áreas que comprometem a própria privacidade dos trabalhadores (BRASIL, 2018).

Entretanto, não se pode atribuir, aprioristicamente, incompatibilidade dos direitos trabalhistas com o avanço tecnológico em si, sendo necessário buscar equilíbrio entre interesses antagônicos (trabalho e capital) que se traduzem na necessidade do empregador em obter informações sobre as atividades desenvolvidas e dos empregados com o direito à privacidade, considerando principalmente a potencialidade lesiva que as novas tecnologias podem oferecer quanto à violação da privacidade, sendo necessário nesse viés traçar diretrizes e princípios a serem seguidos e observados (GUERRA, 2004).

Sob esta perspectiva há uma nova dimensão do direito do trabalho envolto em novas tecnologias, tais como Indústria 4.0, economia colaborativa, trabalho sob demanda via

---

<sup>2</sup> Diga-se *a priori* pois mesmos nestas situações podem ocorrer violações, tais como invasão por hackers, vazamento de informações sensíveis, pessoais e profissionais, comercialização sem prévia autorização destas informações etc. Cita-se, como exemplo concreto, a seguinte notícia: Justiça condena Catho por furtar dados e empresa faz acordo (VAZ, 2013).

aplicativos etc., modificando as formas de prestar o trabalho, com uso crescente de sistemas inteligentes e de plataformas tecnológicas, criando produtos e serviços em uma verdadeira revolução digital (MOREIRA, 2018).

A revolução digital neste aspecto acarreta fortes impactos no mundo do trabalho, principalmente em relação ao tempo de trabalho, de forma negativa, pois a tecnologia possibilita que o empregado permaneça conectado de forma indefinida e podendo ser demandado pelo empregador a qualquer momento e situação, sendo necessário reafirmar o direito à desconexão do trabalhador (SOUTO MAIOR, 2003), inclusive como uma faceta do direito à privacidade do século XXI.

A própria expansão da tecnologia com sua evolução permite que haja maior tratamento, recolhimento e transmissão de dados, de forma célere e ágil, permitindo que haja um grande potencial de comprometer a privacidade, devendo o Direito buscar o equilíbrio entre os direitos e liberdade das pessoas com o desenvolvimento tecnológico.

Entretantes, o uso indiscriminado e irresponsável da tecnologia, pode ser uma fonte potencial de violação da privacidade e intimidade dos empregados no mercado de trabalho, tanto para a sua admissão quanto durante o pacto laboral, conforme ficará elucidado no próximo tópico.

### **3 Possíveis consequências decorrentes da violação da privacidade e intimidade do trabalhador pelo uso da tecnologia**

O contrato de trabalho no Brasil é caracterizado pelo fato de ser sucessivo no qual abrange diversas fases (pré-contratual, celebração, execução, extinção e pós-contratual) e, diante destas fases, oportuniza-se que se possam ocorrer violações da privacidade e intimidade do empregado em diferentes facetas.

Os direitos e deveres individuais e coletivos insculpidos no art. 5º, da Constituição Federal de 1988, devem ser respeitados em todas as fases do contrato de trabalho, tanto pelo empregador quanto pelo empregado, uma vez que tanto empregador quanto empregado possuem os direitos de convicção política ou filosófica, de associação, de acesso às informações e de consciência, à liberdade de pensamento e expressão, de consciência e crença religiosa, à intimidade e à privacidade além de diversos outros (BRASIL, 1988).

A constante vigilância com o avanço tecnológico têm provocado precarização principalmente em relação ao trabalho, sendo que o uso de inteligência artificial possibilita a criação de “perfis” de cunho homogêneo, possibilitando maior discriminação dos

trabalhadores que não correspondam com o “padrão” socialmente estabelecido e supostamente almejado, estigmatizando e penalizando ainda mais as minorias, criando obstáculos à admissão, manutenção do emprego e ao pleno desenvolvimento da personalidade pois perpetua e acentua, mesmo que de forma velada e mediata, situações discriminatórias, uma vez que os algoritmos podem potencializar diversas espécies de discriminação, apesar da vedação legal de discriminação na admissão, como preceitua o art. 1º, da Lei 9.029/1995 (BRASIL, 1995).

A utilização da inteligência artificial de forma recorrente, principalmente no procedimento de admissão em um emprego que normalmente se denomina como *background employment checks*<sup>3</sup>, pode ocasionar situações discriminatórias, uma vez que este tipo de procedimento tem o condão de verificar aspectos da vida atual e pregressa do empregado, relacionando aspectos da vida privada com o emprego e acaba excluindo candidatos indevidamente pelo fato de se ancorar pelas características pessoais, etnia, domicílio, religião, antecedentes criminais<sup>4</sup>, orientação sexual etc. Isso se dá também porque, a coleta de dados pessoais e sensíveis quando no processo seletivo admissional que não tenha relação com a vaga disponibilizada, também constitui invasão da privacidade pelo potencial discriminatório que pode acarretar.

O procedimento de *background employment checks* acima citado se caracteriza como uma verdadeira investigação intrusiva na vida privada e intimidade do empregado, formando no mais das vezes as denominadas execráveis “listas sujas”<sup>5</sup>, contendo informações acerca de preferências partidárias, políticas, crenças filosóficas e religiosas, hábitos pessoais, situação familiar, filiação sindical, participação de greves e, um dos mais pesquisados, se o trabalhador já ajuizou alguma ação trabalhista em face de ex-empregador, sendo proibidas e ilícitas tais práticas.

A utilização de algoritmos e *machine learning* como forma de gestão do trabalho, apesar de ter sido mais desenvolvida com maior expressão durante o período pandêmico da COVID-

---

<sup>3</sup> Esta prática permite de que empresas especializadas tenham acesso a diversas informações do candidato que vão além da mera análise curricular, analisando o perfil do trabalhador e aspectos privados de sua vida, tais como ideologia, religião, gostos pessoais, orientação sexual, perfil econômico, hábitos de vida etc. (OECD, 2021).

<sup>4</sup> Os antecedentes criminais bem como outras certidões negativas referentes à existência de demandas judiciais em curso ou pretéritas para admissão no emprego, em regra, são consideradas ilícitas por conter dados pessoais e sensíveis. Entretanto, a jurisprudência entende a possibilidade de excepcionalizar este regramento quando a função assim o exigir. Cita-se, como exemplo, a necessidade de se verificar os antecedentes criminais para admissão de vigilante patrimonial de carro-forte para transporte de numerário, sendo crível a exigência de antecedentes criminais neste caso em apreço. Em sentido contrário, caracteriza-se prática discriminatória, cf. a seguinte jurisprudência (exigência de antecedente criminal e exame toxicológico para trabalhar como camareira, prática abusiva) (BRASIL, 2022b; 2023).

<sup>5</sup> Cf. a seguinte jurisprudência temática acerca da proibição e caracterização de dano moral por empregador que se utilizou de “lista suja” (BRASIL, 2022a).

19 em 2020 (ADAMS-PRASSL, 2020) em decorrência da “uberização” do trabalho, fato é que, estes mecanismos também começaram a ser utilizados em diversos outros setores da atividade econômica e empresarial, reforçando o controle do trabalho por intermédio de práticas unilaterais e sem transparência.

A utilização da inteligência artificial com o objetivo de monitorar o desempenho e a produtividade do empregado pode enviesar o procedimento para detecção de supostos comportamentos não desejáveis pela empresa que nem sempre pode corresponder com o padrão comportamental real do empregado, colaborando com a discriminação na admissão (DE STEFANO, 2019), ainda mais quando estes procedimentos não são transparentes, fazendo com que também no ambiente de trabalho seja um local de tensão e pressão, aumentando o estresse e a insegurança do empregado.

Para a necessidade de preservação da privacidade dos empregados perpassa, necessariamente, também à proteção de dados, principalmente os de dados sensíveis pois uma ausência protetiva dos dados possibilita que haja discriminação, tal como pode ocorrer com a opinião política.

Considerando que os dados sensíveis constituem informações da estrutura do próprio trabalhador, estes dados estão adstritos ao “núcleo duro” da privacidade, cuja proteção, por envolver questões de saúde, orientação sexual, religião, raça, gênero, opiniões políticas etc., devem ser enaltecidas ao máximo, com o fito de impedir discriminações entre trabalhadores, inclusive pela elaboração de perfis individuais pelo empregador com o fito de realizar tratamento desigual e ofensivo.

A justificativa da coleta de dados pelo empregador comumente se justifica pela necessidade de embasamento para tomada de decisões, entretanto, o empregado não pode ser considerado uma mera fonte de fornecimento de informação, pois lhe é devido o direito de intervir nesta coleta de dados, principalmente com a finalidade de controlá-la e garantir a exatidão das informações ali constantes bem como ter conhecimento do destino destas informações.

#### **4 O manuseio da tecnologia como possibilidade discriminatória**

É evidente que o avanço tecnológico com a utilização cada vez mais crescente da inteligência artificial carrega consigo diversos benefícios e vantagens, contribuindo para a melhoria social e bem-estar individual bem como para tomadas de decisões aperfeiçoadas mas que, em contrapartida, torna-se uma fonte potencial de violação da intimidade, privacidade,

segurança e distanciamento nas relações de trabalho nos quais, com a utilização em conjunto dos algoritmos, impulsiona na ausência de transparência nos procedimentos decisórios bem como na possibilidade de ocorrer discriminação algorítmica.

A coleta e armazenamento de dados pelo empregador com utilização de algoritmos, com a justificativa de sua neutralidade, também não se sustenta, uma vez que o algoritmo pode enfatizar o racismo (BENJAMIN, 2019) quando os mecanismos de buscas <sup>6</sup> e coletas revelam o padrão da mulher ou do homem branco.

A discriminação algorítmica prioriza determinados grupos em detrimento dos demais, criando privilégios desarrazoados e estabelecendo um procedimento excludente por intermédio da inteligência artificial que deixam os algoritmos enviesados de preconceito, normalizando a masculinidade e a branquitude.

A discriminação algorítmica aliada ao procedimento excludente, está intrinsecamente atrelada com o uso cada vez mais rotineiro dos algoritmos como uma forma de controlar o comportamento humano, influenciando sobremaneira na percepção social da realidade, valores, comportamento individual, opinião pública etc., sendo que, as empresas privadas que as manipulam, comumente não são transparentes e não se submetem ao escrutínio público por não seguirem procedimentos legais formalizados pelo Estado, ensejando assim maior possibilidade de manipulação e discriminação (JUST; LATZER, 2016; LATZER; HOLLNBUCHNER; JUST; SAURWEIN, 2014; ZIEWITZ, 2016), haja vista que, os algoritmos, comumente não precisam de divulgação, sendo tratados, de forma geral, como segredos comerciais (com exceção dos de código aberto – “*open source*”), sendo que deveriam, ao menos, divulgar quais as máximas empregadas na programação de algoritmos e os critérios subjacentes, possibilitando eventual verificação.

Hoje em dia os algoritmos fazem parte constante da vida das pessoas, atuando nos comportamentos e influenciando decisões, sendo que, uma grande parte das atividades rotineiras e cotidianas, incluindo publicidade e consumo midiático, está envolto da presença dos algoritmos, não sendo diferente na vida do trabalhador, sendo os algoritmos utilizados para observar comportamento e interesses, bem como no afã de previsibilidade comportamental futura e das necessidades, guiando as ações e decisões.

---

<sup>6</sup> Mecanismos de buscas são *sites* especializados de busca nas páginas da Internet por intermédio de palavras-chaves, podendo ser conceituado como “um conjunto de programas de computador que executa diversas tarefas com o objetivo de possibilitar a localização de arquivos e *Web sites* que contenham ou guardem relação com a informação solicitada pelo usuário” (LEONARDI, 2012, p. 288).

É neste contexto de “indústria 4.0”, “internet das coisas” e “inteligência ambiente” (ambiente no qual tudo se comunica com tudo) que os empregados estão inseridos e vulneráveis em um sistema computacional no qual cada vez mais as decisões humanas são substituídas (SENDER, 2013).

A algoritmização também é uma consequência da disponibilidade dos *Big Data* que são utilizados, inclusive pelos empregadores, para coletar diversos tipos de dados diversificados, de diferentes fontes, não se restringindo somente aos dados pessoais, residindo aí a problemática de ausência de regulamentação legal aos problemas que surgem do manuseio e utilização dos *Big Data* (EXECUTIVE OFFICE OF THE PRESIDENT, 2014; MAYER-SCHÖNBERGER; CUKIER, 2013; TAEGER, 2014).

Nesta toada, o *Big Data* possibilita aos empregadores possuírem acesso a enormes quantidades de dados de diferentes tipos e qualidade, permitindo armazenamento e acesso devido à alta velocidade do processamento, sendo que as empresas comumente os utilizam em conjunto com outros mecanismos, tais como internet das coisas e computação em nuvem.

A utilização dos *Big Data* pelas empresas aliadas com outras tecnologias, como inteligência artificial, permite que haja uma análise descritiva em procedimentos analíticos dos dados, acarretando em mineração de dados (*Data Mining*); análise preditiva (análise comportamental por intermédio de comparativos de outrem, permitindo colecionar dados com objetivo de reconhecer tendências e padrões comportamentais) e análise prescritiva, desta maneira os algoritmos contribuem para definir o caminho da decisão a ser tomada pelas empresas com perspectiva de governança.

Em relação à mineração de dados, merece uma atenção especial tendo em vista a dinâmica de sua utilização pelas empresas. Objetiva-se com a mineração de dados angariar “novas informações, que podem estar ocultas, a partir de banco de dados” (MARÇULA; BENINI FILHO, 2008, p. 198) e, com estas informações em posse do empregador, traçar comportamentos modais do empregado, descobrindo informações adicionais tais como questões filosóficas, políticas, personalidade, orientação sexual etc.

Outro procedimento de importância salutar em ser mencionado, considerando ser o procedimento mais fácil e o mais utilizado pelos empregadores, levando em consideração a sua facilidade de acessibilidade, trata-se da coleta de dados dos empregados em decorrência de seu uso de perfis alocados em redes sociais. Existem empresas especializadas (DARREL, 2011) em checagens de redes sociais com o objetivo de monitorar as atividades de seu usuário (no caso, empregado) e traçar perfis e um gráfico da pessoa, analisando seus *storys*, *reels*, postagens, fotografias, mensagens etc., revelando um perfil com padrão comportamental que será

analisado para a contratação ou manutenção do contrato de trabalho pelo empregador (RUSTAD, 2009).

É um grande equívoco, por parte dos empregadores, por acharem que a coleta indiscriminada de dados nas redes sociais podem ser utilizados para esta análise pelo simples fato de terem sido disponibilizados pelos empregados, como se o fato de terem criado os perfis, terem concordado com os termos de uso e de privacidade, seria o bastante para consubstanciar um consentimento tácito em desfavor do empregado, todavia, tal prática desvirtua os princípios da lealdade, boa-fé, adequação, transparência e finalidade, constituindo grave ofensa à privacidade e intimidade do empregado.

Os procedimentos acima elencados com objetivo de controle comportamental, inclusive dos trabalhadores, estão relacionados com “tecnocontrol” (“tecnologia normativa” ou “tecnologia prescritiva”) (OERMANN; ZIEBARTH, 2015, p. 257), que são a seleção e o controle do acesso à informação no âmbito dos serviços sociais da internet, como as máquinas de busca por exemplo, servindo como filtragem de busca e ranqueamento algorítmico dos dados pelas empresas, comumente realizados ao arripio do conhecimento dos trabalhadores, permitindo, desta maneira, que sejam criados perfis de usuário (*profiling*)<sup>7</sup> por intermédio de análise comportamental, fazendo com que o empregador tenha acesso indevidamente às informações dos trabalhadores, tais como preferências, valores, orientações sexuais etc., permitindo que o empregador classifique determinado trabalhador pertencente a um determinado grupo em decorrência da padronização comportamental coletada, influenciando no desenvolvimento de emoções, na produtividade, nas decisões etc.

Um das principais formas em se criar perfil de usuário (*online profiling*) é por intermédio dos *Cookies*<sup>8</sup>, que são arquivos que armazenam informações e dados acerca do acesso na internet, possibilitando a coleta e armazenamento de dados, nos quais podem ser usados para monitoramento dos usuários daquele *site* e para elaboração de perfis, tendo em vista o seu uso intensivo (KUROSE; ROSS, 2006).

Para além da utilização dos *Cookies*, outra forma possível de ocorrência de violação de dados trata-se da pirataria digital por intermédio de *hackers*. Salienta-se, primeiramente, de

---

<sup>7</sup> Cf. art. 4º, n.4, do Regulamento de Base da União Europeia acerca desta conceituação, que assim dispõe: “Todo tipo de processamento automatizado de dados personalizados que consiste em que estes dados personalizados sejam usados para avaliar determinados aspectos pessoais que se refiram a uma pessoa física, principalmente para prever e analisar aspectos relacionados a desempenho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, residência habitual ou mudança de endereço desta pessoa física” (BRASIL, 1988).

<sup>8</sup> Não confundir com *Spyware*, que são programas espões que são instalados de forma sub-reptícia, transmitindo todo tipo de informação sem a permissão ou consentimento do usuário (RUSTAD, 2009).



que *hackers* se refere a toda possibilidade que um indivíduo se utiliza para invasão do sistema informático de outrem, inclusive para uso lícito, como se dá quando se faz para aperfeiçoar e testar um sistema e sua segurança para detecção de falhas e vulnerabilidades, pois os que o fazem com intuito ilícito para angariar vantagens indevidas, chama-se de *crackers*, nos quais este sim realiza pirataria digital. Independentemente de *hacker* ou *cracker*, caso o vazamento de dados do empregado tiver sido vazado e facilitado pelo empregador, seja de forma intencional ou não, como descuido da segurança do sistema do empregador<sup>9</sup>, este poderá ser responsabilizado pelos danos ocasionados ao empregado.

Percebe-se de que a formação de perfis que se utilizam de dados sensíveis coletados pelo empregador, pode gerar discriminação, pois mesmo dados não sensíveis *a priori*, caso utilizados para formação de um perfil, se tornam sensíveis, pois pode afetar e prejudicar tanto a esfera individual do trabalhador quanto sua esfera coletiva, caso o trabalhador venha a pertencer a um determinado grupo que tenha sido traçado um perfil com conotações negativas e, diante desta situação, deve-se ter condições muito rigorosas para circulação destas informações, incluindo a proibição da coleta destes dados pelo empregador.

Não se pode olvidar ainda, a possibilidade real e concreta de que os dados coletados possam estar desatualizados, falseados e, até mesmo, imprecisos, no qual pode ocasionar prejuízos ainda maiores, exatamente por não representar a realidade do empregado investigado indevidamente.

Observa-se, portanto, de que os dados pessoais sensíveis coletados e formados pela mineração de dados comumente não tem relação direta com as atividades exercidas pelo empregado, possuindo a serventia tão somente de discriminação (DINIZ, 2008), violando diversos princípios, tais como da adequação, transparência, finalidade, consentimento, boa-fé e lealdade (VIEIRA, 2007).

Diante deste contexto de utilização dos *Big Data* e “*machine learning*” acaba atingindo diretamente os trabalhadores, retirando-lhes no mais das vezes a autonomia e o direito de acesso ao consumo de bens e serviços e, principalmente, na inserção no mercado de trabalho, incluindo os malefícios do “*profiling*” por gerarem tratamento discriminatório.

Não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro,

---

<sup>9</sup> Mesmo que haja terceirização do tratamento de dados para alguma outra empresa especializada, o empregador responderá solidariamente em caso de vazamento e violação daí decorrente (HOWARD, 2008).

da solicitação de um prêmio de seguro especialmente elevado (RODOTÀ, 2008, p. 70).

Com este poderio em mãos, permite que o empregador possa manipular e influenciar no comportamento dos trabalhadores, inclusive com utilização de *bots* sem necessidade de interação direta com os trabalhadores, compartilhando informações e mascarando alguma aprovação, dando a falsa sensação de aparência ampla, estimulando modos de conduta. Cita-se como exemplos possíveis no ambiente de trabalho desta utilização: greve para direitos trabalhistas, com utilização desta tecnologia, pode dar a falsa sensação de que a greve seria pequena ou sem razão de existir, estimulando que demais trabalhadores laborem normalmente sem participarem da greve. Outro exemplo, imagina-se um ambiente no qual o assédio moral é constante, com utilização desta tecnologia, pode mascarar uma realidade dando a falsa sensação de normalidade ou mero exercício e poder diretivo, com práticas de cobranças excessivas e metas inatingíveis.

Veja-se que os exemplos são infundáveis e que não se limitam durante o contrato de trabalho, podendo ocorrer na fase pré-contratual, como na admissão, sendo que a utilização de análise preditiva de dados pode reconhecer determinado comportamento de algum candidato acarretando-lhe a não inserção no mercado de trabalho por esta análise preditiva, portanto, não é aceitável programar previamente em um algoritmo a tomada de decisão de contratação de algum candidato com base em análise preditiva.

Restou demonstrado neste tópico as possibilidades existentes que podem ser potenciais violadoras da intimidade e privacidade do empregado. Todavia, tais práticas discurridas encontram um grande óbice à sua repressão principalmente quando sua disponibilização se encontra de acesso público, como na internet.

Além da dificuldade informada, a produção de prova pelo empregado é considerada de grande dificuldade nesta temática, principalmente a produção de prova acerca do uso de dados ou de consulta a cadastros pelo empregador, sendo considerada pelo viés processual como uma verdadeira “prova diabólica”, ou seja, é uma prova muito difícil ou até mesmo impossível de ser produzida (DIDIER; BRAGA; OLIVEIRA, 2007).

Evidentemente que nestas situações que envolvam discriminação, havendo indícios ou elementos iniciais da conduta violadora, deve-se haver certa presunção de veracidade e atribuindo o ônus probatório ao empregador, de acordo com a teoria dinâmica da distribuição do ônus probatório insculpido nos arts. 373, do CPC e 818, da CLT (BRASIL, 1943) pelo fato do empregador possuir maior aptidão para a produção da prova, inclusive em conformidade com publicação da Organização Internacional do Trabalho (OIT), do seguinte teor:

Probar en uno procedimiento judicial que ha habido discriminación resulta difícil, aunque no se requiera demostrar la intencionalidad del imputado. [...] Así, a fin de ayudar a los demandantes y propiciar la celebración de juicios justos, cada vez son más los países que trasladan al empleador la carga de la prueba en la refutación de los alegatos una vez que el demandante ha manifestado los primeros indicios de discriminación (OIT, 2003, p. 70).

## 5 Conclusão

Conforme desenvolvido e demonstrado neste artigo, as tecnologias que mais podem ser potenciais violadores da privacidade e intimidade do empregado são a biometria, análise de *Big Data*, internet das coisas e inteligência artificial.

As tecnologias acima listadas potencialmente violadoras da privacidade e intimidade do empregado, carrega consigo outro grande desafio referente à sua repressão. Além do mais, muitas práticas ocorrem de forma escondida dos empregados ou candidatos ao emprego, tais como a mineração de dados, buscas online, perfis em redes sociais etc., com total ausência de transparência e sem indicações de critérios precisos, que acabam sendo utilizados no processo de admissão, não sendo raro, no mais das vezes, o empregador se blindar destas práticas alegando parametrização baseada em segredo empresarial aliada às estratégias comerciais ou processo produtivo, tornando eventual reprimenda de difícil detecção e aferição.

Neste sentido, não basta, por si só, a vedação ou proibição da coleta de dados nos moldes apresentados como um ilícito, é necessário que haja procedimento mais incisivo e imediato, mas cuja solução acaba sendo, no mais das vezes, socorrer-se do judiciário.

Entretanto, apesar da complexidade envolvida, em algumas situações é possível identificar os ilícitos acometidos. Cita-se, como exemplo, o próprio hackeamento, no qual caso ocorra a violação da privacidade ou intimidade do empregado, por intermédio da URL (*home page*) é possível identificar o *site* pelo endereço de IP ou pelo domínio que se encontra, uma vez que o IP (Protocolo da Internet) é o que traz a identificação da origem da ilicitude perpetrada. Existem outros *softwares* que colaboram também para esta identificação, incluindo mensagens eletrônicas, país de origem, IP, e-mails etc. (FLORILLO; CONTE, 2013).

Para além de ações afirmativas, é necessário conceder ao empregado, maior controle sobre seus dados, independentemente de ter havido ou não alguma violação, uma vez que ao empregador, ao coletar seus dados, não se sabe ao certo qual será sua finalidade e utilização, inclusive em momento futuro devido ao seu armazenamento.

Normalmente, o consentimento são dotados de informações abstratas e com vagueza sobre seu alcance, não se sabendo ao certo as informações sobre o destino da utilização dos

dados do empregado ou para quem serão transferidos após a coleta e para quais finalidades; não é por outro motivo que o próprio Regulamento Geral de Proteção de Dados da União Europeia qualificou este consentimento de forma mais restrita e rígida, exigindo não só o consentimento expresso, mas também a manifestação consentida livre, inequívoca, explícita, específica e informada.

Diante deste armazenamento pelo empregador, é imprescindível que haja uma fiscalização rígida de como as empresas armazenam os dados pessoais e sensíveis dos empregados, principalmente àqueles relacionados à saúde, mapeando e identificando atos discriminatórios e coletando dados para fins estatísticos acerca da empregabilidade dos trabalhadores nestas circunstâncias.

Ademais, o armazenamento e coleta de dados com utilização de inteligência artificial e algoritmos, necessariamente deve perpassar por uma análise interseccional com conduta ética, já que pela legislação existente, somente o termo de consentimento assinado pelo trabalhador não é o suficiente para dirimir a coleta e armazenamento indiscriminado de dados com a consequente discriminação algorítmica que daí pode advir, pois o consentimento exigido nestas circunstâncias é realizado de forma unilateral pelo empregador, com ausência de paridade em decorrência de assimetria de poder, bem como para que o empregado seja admitido em seu emprego, necessita aceitar as condições que lhe são impostas no momento da contratação. Além do consentimento expresso do trabalhador, é necessário haver respaldo legal com garantia de não discriminação e processamento de dados para fins estatísticos de forma a não ser possível individualizar e identificar o trabalhador.

Em relação ao uso da inteligência artificial<sup>10</sup>, a própria Organização para a Cooperação e Desenvolvimento Econômico (OCDE<sup>11</sup>) estabeleceu alguns princípios a serem seguidos, nos quais a inteligência artificial deve ser “inovadora, de confiança e que respeita os direitos humanos e os valores democráticos” (OECD, 2019a). A União Europeia, por intermédio de seu documento denominado *Orientações Éticas para uma Inteligência Artificial de Confiança*, estabeleceu diretrizes com foco na proteção da pessoa humana por intermédio da necessidade de se haver transparência, respeito a autonomia humana, proteção dos dados pessoais, direito à privacidade com vedação da discriminação. Em âmbito trabalhista, a própria OIT ao alegar de

---

<sup>10</sup> Diversos países (cita-se somente como exemplo os Estados Unidos da América, Canadá, China, Alemanha, França etc.) estão criando estratégias de nível nacional para lidar com a inteligência artificial em decorrência da concorrência desleal que seu uso acarreta em relação às pequenas e médias empresas, uma vez que somente 20% das empresas consideradas de nível mundial (tais como IBM, Facebook, Microsoft, Google, Amazon, Apple etc.) adotam a utilização da inteligência artificial em sua produção ou fornecimento de serviços (SERVOZ, 2019).

<sup>11</sup> Em inglês: *Organisation for Economic Co-operation and Development* (OECD).

que “o trabalho não é uma mercadoria; nem é um robô”, estabelece premissas de uso da inteligência artificial, nos quais se privilegia a tomada de decisões pela autonomia humana em decorrência da inteligência emocional, pois as decisões que afetem o meio ambiente de trabalho, precisa perpassar pelo crivo humano, pois “a gestão de algoritmos, a vigilância e o controle através de sensores e de outras formas de monitoramento, precisa ser regulado para proteger a dignidade dos trabalhadores” (OIT, 2019, p. 13 e 45).

Interessante notar também as recomendações como propostas de solução oriundas do Regulamento (EU) 2016/679 do Parlamento Europeu por intermédio da Recomendação do Comitê de Ministros sobre Tratamento de Dados Pessoais no contexto do emprego, no qual há orientação aos empregadores para que seja evitada intromissão abusiva e injustificada na privacidade dos trabalhadores, sendo estendida esta proteção para todos os mecanismos tecnológicos utilizados pelo empregador, nos quais ao serem utilizados pelos trabalhadores devem ser informados *in totum* acerca da política de privacidade utilizada pelo empregador, sempre de forma periódica e adequada, incluindo na política a finalidade do processamento dos dados e a forma de coleta e armazenamento; orienta-se também para que o acesso das páginas de internet pelo trabalhador sejam adotadas medidas preventivas, tais como utilização de filtros que impeçam o acesso e monitoramento de dados pessoais do trabalhador; os trabalhadores devem ser informados que as comunicações eletrônicas profissionais podem ser acessadas pelo empregador quando necessário, por motivos legítimos ou por segurança; vedação completa de acesso e monitoramento de comunicação privada do trabalhador; orienta-se também para que o empregador adote medidas transparentes quando do desligamento do trabalhador, nos quais os conteúdos podem ser acessados para uso exclusivo da organização da empresa antes da saída do trabalhador, preferencialmente que seja realizado em sua presença.

Percebe-se, desta maneira, diversas obrigações e responsabilidades de que o empregador deve seguir como o responsável pelo tratamento de dados recolhidos e acessados, com adoção de medidas técnicas de segurança e controle suficientemente adequadas para que os dados sejam confidenciais, permitindo o acesso e autorização ao acesso e recolhimento destes dados do trabalhador somente para pessoas devidamente legitimadas e com autorização, sendo que o seu desrespeito, seja proposital ou acidental, deverá acarretar de imediato a notificação e o aviso ao empregado detentor dos dados acerca da ocorrência, devendo o empregador com maior brevidade possível sanar a questão e envidar esforços para mitigar os eventuais prejuízos ocasionados.

Em relação ao empregado titular dos dados, deve-lhe ser concedido diversos direitos, como o direito ao esquecimento, acesso, alteração, retificação, portabilidade e demais direitos

correlacionados aos seus dados, garantindo ainda ao trabalhador a ciência acerca da utilização de seus dados e a sua destinação, mesmo nas situações previstas em leis (como o fornecimento dos dados do trabalhador para o governo), devendo haver na empresa um responsável direto a quem o empregado pode acionar caso queira obter estas informações, bem como alguma instituição governamental onde possa se socorrer caso estes direitos não sejam respeitados.

Neste sentido, é necessário que haja medidas de proteção da privacidade dos dados pessoais do empregado por intermédio de diversos direitos de defesa. Primeiramente, para que seja possível um direito de defesa eficaz, o empregado tem o direito de acesso, conforme se observa nos arts. 5º, inc. LXXII, alínea “a”, da CF/88 (BRASIL, 1988), art. 43, *caput*, do Código do Consumidor (CDC) (BRASIL, 1990), art. 7º, inc. I, da Lei n. 9.507/1997 (BRASIL, 1997) e art. 5º, inc. II, da Lei n. 12.414/2011 (BRASIL, 2011), exemplificativamente.

A clareza e objetividade dos dados pessoais do empregado e sua manutenção, confere-lhe o direito à retificação caso o empregado perceba inexatidão, inveracidade ou necessidade de complementação de seus dados que se encontram em um banco de dados. Engloba-se neste direito também o cancelamento, seja por necessidade de supressão, seja pelo fato de que tais dados não deveriam ter sido colhidos (cita-se como exemplo o art. 5º, inc. I, da Lei n. 12.414/2011 que prevê o direito do consumidor em ter cancelado registro desabonador com a quitação do débito pretérito) (DE LA CUEVA, 1993).

O empregado tem o direito também de compelir o empregador, por intermédio da obrigação de fazer, para que seus dados pessoais coletados sejam tratados e mantidos conforme a finalidade em que o fora autorizado, podendo o empregado restringir seu uso pelo empregador ou até mesmo vedar o seu uso para fins diferentes daqueles originalmente colhidos (VALDÉS, 1996). Compreende-se também neste direito, o resguardo da confidencialidade do empregado e sigilo de seus dados que não estejam em conformidade com o fim que se destina.

Considerando de que com o desvio de finalidade dos dados coletados pelo empregador pode ser caracterizado uma fraude trabalhista, nos termos do art. 9º, da CLT (BRASIL, 1943), é passível de nulidade judicial quaisquer dispensas ou não contratação com base no uso indevido destes dados quando utilizado para criar perfil do empregado e discriminá-lo em decorrência disto, podendo ser readmitido ou indenizado se dispensado ou somente indenizado, caso não contratado (uma vez que não há contratação forçada por causa da livre-iniciativa do empregador).

Importante mencionar de que a proteção que se faz alusão é dos dados pessoais do empregado, uma vez que os dados sensíveis, em regra, nem devem ser tratados e armazenados pelo empregador, seja antes, durante ou após o pacto laboral, podendo ser caracterizado,

inclusive, como tratamento com rigor excessivo pelo empregador, sendo lícito ao empregado invocar a rescisão indireta de seu contrato, nos termos do art. 483, alínea “b”, da Consolidação das Leis do Trabalho (CLT) (BRASIL, 1943).

Diante toda fundamentação, conclui-se de que o avanço tecnológico aumentou, de forma significativa, o poder diretivo, organizacional e fiscalizatório do empregador, sendo necessário criar mecanismos eficazes para que os empregados não tenham a sua privacidade e intimidade violada de forma assídua, nem que seus dados pessoais e sensíveis sejam coletados e utilizados para fins discriminatórios pelo empregador.

### Referências

ADAMS-PRASSL, Jeremias. Algorithmic management and the EU social acquis: opening the black box. **Thematic Working paper for the Annual Conference of the ECE**, 2020.

BENJAMIN, Ruha. **Race after technology**: Abolitionist tools for the new Jim Code. Australia: Polity Press, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Emendas Constitucionais de Revisão. Brasília: Presidência da República, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 04 ago. 2023.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del5452.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm). Acesso em: 04 ago. 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República, 2011. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112414.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm). Acesso em: 04 ago. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 04 ago. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 04 ago. 2023.

BRASIL. **Lei nº 9.029, de 13 de abril de 1995**. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Brasília: Presidência da República, 1995. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9029.htm](https://www.planalto.gov.br/ccivil_03/leis/l9029.htm). Acesso em: 04 ago. 2023.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília: Presidência da República, 1997. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19507.htm](https://www.planalto.gov.br/ccivil_03/leis/19507.htm). Acesso em: 04 ago. 2023.

BRASIL. Tribunal Superior do Trabalho. Dano moral por inclusão do nome do empregado em lista “suja/discriminatória”. **Ag-AIRR - 11192-17.2015.5.18.0053**. 2ª Turma. Relatora: Maria Helena Mallmann. Acórdão, 10 jun. 2022, 2022a.

BRASIL. Tribunal Superior do Trabalho. Exigência de testes da HIV e toxicológico para admissão de camareira – proibição. **ED-RRAg - 1937-62.2017.5.09.0652**. 2ª Turma. Relatora: Maria Helena Mallmann. Acórdão, 11 fev. 2022, 2022b.

BRASIL. Tribunal Superior do Trabalho. Exigência de testes da HIV e toxicológico para admissão de camareira – proibição. **RRAg - 2003-85.2017.5.09.0088**. 1ª Turma. Relator: Amaury Rodrigues Pinto Junior. Acórdão, 14 abri. 2023, 2023.

DARRELL, Keith B. **Issues in Internet law: society, technology, and the law**. 6. ed. Boca Raton-FL: Amber Book Company, 2011.

DE STEFANO, Valerio. Introduction: Automation, Artificial Intelligence, and Labour Protection. **Comparative Labor Law & Policy Journal**, v. 41, n. 1, 2019. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3403837](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3403837). Acesso em: 04 ago. 2023.

DIDIER JR., Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael. **Curso de Direito Processual Civil**. v. 2. Salvador: Juspodivm, 2007.

DINIZ, Ana Paola Santos Machado. Banco de Dados e intimidade informática no trabalho. **Vistos, etc. Revista da Associação dos Magistrados da Justiça do Trabalho da 5ª Região**, Salvador, p. 49 - 53, 2008.

EXECUTIVE OFFICE OF THE PRESIDENT. **Big Data: Seizing Opportunities, Preserving Values**. The White House, 2014.

FIORILLO, Celso Antonio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

FOUCAULT, Michel. **Vigiar e punir**. 40. ed. Petrópolis: Vozes, 2012.

GUERRA, Amadeu. **A privacidade no local de trabalho**. As novas tecnologias e o controle dos trabalhadores através de sistemas automatizados-uma abordagem ao Código do Trabalho. São Paulo: Almedina, 2004.

HOWARD, Christine e. Invasion of privacy liability in the electronic workplace: a lawyer’s perspective. **Hofstra labor & employment law jornal**, Hempstead-nY, v. 25, n. 2, 2008. Disponível em: <https://scholarlycommons.law.hofstra.edu/hlelj/vol25/iss2/5/>. Acesso em: 04 ago. 2023.



JUST, Natascha; LATZER, Michael. Governance by algorithms: reality construction by algorithmic selection on the internet. **Media, Culture & Society**, v. 39, n. 2, 2016. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3871903](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871903). Acesso em: 04 ago. 2023.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LATZER, Michael; HOLLNBUCHNER, Katharina; JUST, Natascha; SAURWEIN, Florian. The economics of algorithmic selection on the Internet. In: BAUER, Johannes; LATZER, Michael (Ed.). **Handbook on the economics of the internet**. Cheltenham, Northampton: Edward Elgar, p. 395-425, 2014. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2710399](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2710399). Acesso em: 04 ago. 2023.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. **Informática: conceitos e aplicações**. 3. ed. São Paulo: Érica, 2008.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution That Will Transform How We Live, Work and Think**. Boston: Mariner Books, 2013.

MOREIRA, Teresa Alexandra Coelho. **Novas Tecnologias e a Questão da Privacidade do Empregado: Experiência em Portugal e na União Europeia**. Braga: Lex Magister, 2018.

OECD - Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. **OECD Legal Instruments**, 2019a. Disponível em: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>. Acesso em: 04 ago. 2023.

OECD - Organisation for Economic Co-operation and Development. Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO). **OECD Publishing**, 2019b. Disponível em: [https://www.oecd-ilibrary.org/science-and-technology/scoping-the-oecd-ai-principles\\_d62f618a-en](https://www.oecd-ilibrary.org/science-and-technology/scoping-the-oecd-ai-principles_d62f618a-en). Acesso em: 04 ago. 2023.

OECD - Organisation for Economic Co-operation and Development. The Impact of Artificial Intelligence on the labour market: what do we know so far? **OECD Publishing**, 2021. Disponível em: <https://www.oecd.org/publications/the-impact-of-artificial-intelligence-on-the-labour-market-7c895724-en.htm>. Acesso em: 04 ago. 2023.

OERMANN, Markus; ZIEBARTH, Lennart. Interpreting code – Adapting the methodology to analyze the normative contents of law for the analysis of technology. **Computer Law & Security Review**, v. 31, n. 2, 2015. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364915000096>. Acesso em: 04 ago. 2023.

OIT - Organização Internacional do Trabalho. **La hora de la igualdad en el trabajo**. Genebra: oficina Internacional do Trabalho, 2003.

OIT - Organização Internacional do Trabalho. **Trabalhar para um Futuro Melhor**, Genebra: OIT, 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUSTAD, Michael L. **Internet Law in a nutshell**. St. Paul-Mn: West-Thomson reuters, 2009.

SENDER, Ulrich. (Ed.). **Industrie 4.0**. Berlim: Springer Vieweg, 2013.

SERVOZ, Michel. **AI, the future of work?** Work of the future! on how artificial intelligence, robotics and automation are transforming jobs and the economy in Europe. European Political Strategy Centre, 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/future-work-work-future>. Acesso em: 04 ago. 2023.

SOUTO MAIOR, Jorge Luiz. Do direito à desconexão do trabalho. **Revista do Tribunal Regional do Trabalho da 15ª Região**, Campinas, n. 23, 2003. Disponível em: <https://juslaboris.tst.jus.br/handle/20.500.12178/108056>. Acesso em: 04 ago. 2023.

TAEGER, Jürgen. (Ed.). **Big Data & Co**: Neue Herausforderungen für das Informationsrecht. OIWR, 2014.

VALDÉS, Julio Téllez. **Derecho informático**. 2. ed. México: McGraw-Hill, 1996.

VAZ, Tatiana. Justiça condena Catho por furtrar dados e empresa faz acordo. **Exame**, 2023. Disponível em: <https://exame.com/negocios/justica-condena-catho-por-furtar-dados-e-empresa-faz-acordo/>. Acesso em: 04 ago. 2023.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antonio Fabris, 2007.

ZIEWITZ, Malte. Algorithms: myth, mess, and methods. **Science, Technology & Human Values**, v. 41, n. 1, 2016. Disponível em: <https://journals.sagepub.com/doi/10.1177/0162243915608948>. Acesso em: 04 ago. 2023.