MPT

INTELIGÊNCIA ARTIFICIAL, TECNOLOGIA DIGITAL E DISCRIMINAÇÃO NO TRABALHO

DIREITOS E CONCEITOS BÁSICOS

Uma cartilha elaborada pelo
Grupo de Estudos Diversidade e Tecnologia

SUMÁRIO

APRESENTAÇÃO

Atenta aos desafios que o avanço da inteligência artificial e as decisões por algoritmos lançam à tutela dos direitos humanos nas relações de trabalho, a Coordenadoria Nacional de Promoção da Igualdade de Oportunidades e Eliminação da Discriminação no Trabalho (Coordigualdade) do Ministério Público do Trabalho, desenvolveu esta cartilha que reúne os principais direitos e conceitos sobre tecnologia digital no contrato de trabalho.

O intuito desta publicação é oferecer à sociedade brasileira, em particular aos atores sociais do mundo do trabalho, fundamentos para a tomada de decisões individuais e coletivas que envolvam liberdade de empresa e direitos fundamentais à tutela da privacidade, liberdade de expressão, não discriminação e dignidade humana. Esta publicação reúne também iniciativas de ajustes de sistemas informáticos e plataformas digitais para a formação de relações equilibradas entre empresas e particulares.

O material foi idealizado pelo Grupo de Estudos sobre Diversidade e Tecnologia (GE Diversitec), criado em 2020 e composto pelo Procurador do Trabalho Thiago Milanez Andraus (coordenador), pela Procuradora Regional do Trabalho Adriane Reis de Araujo (vice-coordenadora) e pelas Procuradoras do Trabalho Ana Lúcia Stumpf González, Carolina Marzola Hirata, Martha Diverio Kruse e pelos Procuradores do Trabalho Rodrigo de Lacerda Carelli, Patrick Maia Merisio e Guilherme Kirtschig.

Boa leitura!

Abismo digital

O abismo digital é qualquer distribuição desigual no acesso, no uso e no impacto das tecnologias da informação e comunicação entre os grupos sociais. Estes grupos podem ser definidos com base em critérios de gênero, geográficos, geopolíticos, etários, culturais ou de outro tipo. Tradicionalmente se considerava uma questão principalmente de acesso. Na atualidade, com uma penetração global de telefones móveis em mais de 95%, a desigualdade relativa se manifesta entre aqueles que têm mais ou menos banda larga ou mais ou menos habilidades associadas.

Destaque: o relatório "Mensurando o Desenvolvimento Digital: Fatos e Números 2019" sugere que a maioria dos desconectados vive nos países menos desenvolvidos (apenas 20% estão conectados à internet). O estudo indica que mais da metade da população feminina global, 52%, ainda não estão usando a Internet, em comparação com 42% dos homens. A estimativa é de que a proporção de todas as mulheres que usam a Internet globalmente seja de 48% contra 58% de todos os homens. O relatório também aponta que a diferença de acesso entre homens e mulheres acontece em todas as regiões do mundo, exceto nas Américas, que têm quase paridade.

Algocracia

Algocracia corresponde ao estado de coisas em que grande parte de nossas vidas são governadas por algoritmos e decisões automatizadas[1]. Ou seja, decisões automatizadas por meio da

1 DANAHER, John. The threat of algocracy: reality, resistance and accommodation. In: ***Philosophy & Technology***, v. 29, p. 245-268. Disponível

análise de performance de algoritmos. Uma crítica que é feita a essa expressão é que ela atribuiria um valor excessivo ao algoritmo em si, já que o termo "algocracia" traz a ideia de poder exercido pelo algoritmo, e, na realidade, trata-se de poder exercido "através" do algoritmo[2]. Um exemplo de manifestação desse "poder do algoritmo" seria o conteúdo que é sugerido em redes como o YouTube, com tendência a ofertar um segmento de conteúdo que mantém o consumidor em sua "bolha" ideológica, sem apresentar diversidade.

Algoritmo

Algoritmo constitui "uma sequência finita e lógica de instruções executáveis, especificadas em determinada linguagem, que mostram como resolver determinado problema"[3]. Compreendem a entrada de informação, as instruções e a saída de informação[4].

Anonimização e Pseudoanomização de dados

A anonimização é o tratamento de dados pessoais por meio da utilização de técnicas para que um dado perca a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5º, III e

em: https://philpapers.org/archive/dantto-13.pdf. Acesso em: 27 out, 2020.

2 CASTRO, Julio Cesar Lemes de. Redes Sociais como Modelo de Governança Algorítmica. ***Revista Matrizes***, São Paulo, v. 12, n. 2, p. 165-191, maio/ago. 2018.

3 BORATTI, Isaías Camilo. ***Introdução à programação algoritmos***. São Paulo: Vinha de Luz, 2007.

4 https://brasil.elpais.com/brasil/2018/03/30/tecnologia/1522424604_741609.html

XI, LGPD). Com isso, o dado deixa de ser considerado pessoal para fins de proteção da LGPD (art. 12, LGPD). É necessário cuidado, no entanto, com o conceito, pois dados aparentemente anonimizados podem ser identificados em alguns casos, com reversão da informação, por meio do emprego de outros meios (notadamente quando somados a outros dados do indivíduo). Esta é a chamada pseudoanomização. Refere-se geralmente a processo em que dados pessoais são anonimizados, existindo dois arquivos que, ao se complementarem, permitem identificar o titular. Para fins da LGPD, a anonimização somente é válida quando não for revertida por meios próprios ou quando não puder ser revertida com esforços razoáveis, considerando-se o custo e tempo necessários de acordo com as tecnologias disponíveis e a utilização exclusiva de meios próprios (art. 12, § 1º, LGPD). Importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, quer pelo responsável pelo tratamento dos dados, quer por qualquer outra pessoa.

Destaque: o jornal norte-americano New York Times teve acesso, em 2018, a uma amostra de dados de geolocalização de alguns meses coletados por telefones celulares (por aplicativos, por exemplo, de previsão de tempo, comercializados livremente). Os dados se referiam a usuários supostamente anônimos de telefones celulares, revelando apenas localização, horários e trajetos. Um dos trajetos era de uma pessoa que deixava sua casa no norte de Nova Iorque e dirigia 22km até uma escola de ensino médio, lá ficando até o final da tarde. Sucede que a única pessoa a fazer tal trajeto desse modo era a professora de matemática Lisa Magrin. Os dados revelaram igualmente suas visitas aos Vigilantes do Peso, ao médico e uma visita a um ex-namorado, inclusive o tempo gasto em cada local. A amostra também indicava, em relação a outras pessoas, visitas a clínicas

de aborto, presídios, escolas, igrejas, delegacias, hospitais, bases militares, comícios políticos, etc.[5]

Aprendizado de Máquina (*machine learning*)

Corresponde ao aprendizado do computador, por meio de processamento de dados, com técnicas estatísticas sofisticadas[6]. É um tipo de Inteligência Artificial, por meio da qual os computadores aprendem sozinhos a executar tarefas, para as quais não foram explícita ou especificamente programados[7]. É um campo de estudo que confere aos computadores a habilidade de aprender sem terem sido programados especificamente e que explora a construção de algoritmos que podem aprender com seus erros e fazer previsões sobre dados, permitindo produzir decisões e resultados confiáveis e repetíveis. Um exemplo de aprendizado de máquina seria o filtro de ***spams*** (mensagens indesejadas de ***e-mail***, por exemplo).

Em razão do risco de efeitos negativos dos filtros criados pelas máquinas, o art. 22, número 3, do Regulamento Geral de Proteção de Dados da Europa, contempla um conjunto de salvaguardas obrigatórias de titularidade da pessoa natural, dentre as quais se incluem, o direito a "***obter intervenção humana por parte do responsável***". Embora inexistente regramento de idêntico teor no direito nacional, extrai-se do princípio da não

5 www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

6 TAULLI, Tom. ***Introdução à inteligência artificial.*** Uma abordagem não técnica. São Paulo: Novatec, 2020, p. 93.

7 SEJNOWSKI, Terrence J. ***A Revolução do Aprendizado Profundo.*** Tradução de Carolina Gaio. Rio de Janeiro: Alta Books, 2019. Título original: The Deep Learning Revolution.

discriminação (artigo 6º, inciso IX da LGPD), que deverá ser assegurada a revisão humana de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, justamente a fim de evitar efeitos negativos e perpetuadores de discriminação.

Aprendizado Profundo (*deep learning*)

Deep learning pode ser identificada como uma subárea de ***machine learning***, e corresponde à capacidade de processar grandes quantidades de dados para detectar informações e padrões que os seres humanos são, na maioria das vezes, incapazes de perceber. ***Deep*** refere-se ao número de camadas ocultas (TAULLI, 2020, p. 119).

É modalidade de aprendizado de máquina na qual os computadores aprendem conceitos complexos a partir de sua própria experiência, envolvendo conceitos mais simples, por intermédio de redes de sistemas informacionais interconectadas, dispostas como neurônios biológicos, denominadas redes neurais[8]. É impulsionado a partir de algoritmos que, interagindo uns com os outros nas redes neurais, compõem sistemas complexos nos quais há várias "camadas ocultas" de subsistemas interligados, interpondo-se entre os dados da entrada e o resultado da saída da rede[9,10].

8 PEIXOTO; SILVA, 2019, p. 97.

9 SEJNOWSKI, Terrence J. ***A Revolução do Aprendizado Profundo***. Tradução de Carolina Gaio. Rio de Janeiro: Alta Books, 2019. Título original: The Deep Learning Revolution, p. 213-214.

10 PEIXOTO; SILVA, 2019, p. 97; 100.

A tecnologia emula o sistema nervoso humano e consiste em um número elevado de unidades atuando em paralelo, através das quais são detectados padrões e associações com relevância estatística, em um conjunto de dados. O uso da linguagem natural é uma das habilidades que podem ser desenvolvidas pelo aprendizado profundo, daí a interação com a aplicação do Direito.

Sobre o uso da linguagem pelos sistemas de Inteligência Artificial, veja: www.theguardian.com/commentisfree/2020/sep/08/robot-wrote-this-article-gpt-3

Outras aplicações potencialmente problemáticas são o reconhecimento facial e seu uso para detectar, por associação, posicionamentos políticos, características de personalidade, ou ligadas a gênero ou etnia, potencializando formas de discriminação, e prejudicando o funcionamento de sistemas democráticos.

Sobre o assunto, interessante a seguinte notícia: www.otempo.com.br/pampulha/reconhecimento-facial-pode-detectar-orientacao-politica-diz-estudo-1.2434132.

Interessantes alertas sobre a questão constam também da entrevista a seguir, com o autor do trabalho mencionado no link anterior, Michal Kosinski: www.terra.com.br/noticias/tecnologia/profeta-do-escandalo-do-facebook-faz-alerta-sobre-reconhecimento-facial,0ed344cda5d44627eae0c380367eac10wgid36hq.html.

Destaque: o robô Victor, desenvolvido em parceria entre o Supremo Tribunal Federal e a Universidade de Brasília para automatização da verificação do cumprimento dos requisitos de repercussão geral dos recursos extraordinários encaminha-

dos ao tribunal, é um exemplo da utilização de aprendizado profundo de computadores.

Inteligência artificial: Trabalho judicial de 40 minutos pode ser feito em 5 segundos (2018). Disponível em: www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=393522;

STF investe em inteligência artificial para dar celeridade a processos (2018). Disponível em: www.jota.info/coberturas-especiais/inova-e-acao/stf-aposta-inteligencia-artificial-celeridade-processos-11122018.

Registre-se que outros países têm avançado mais na implantação de soluções de Inteligência Artificial no Poder Judiciário: vide SILVA, Rafael Rodrigues da. **Estônia está desenvolvendo o primeiro "juiz robô" do mundo** (2019). Disponível em: https://canaltech.com.br/inteligencia-artificial/estonia-esta-desenvolvendo-o-primeiro-juiz-robo-do-mundo-136099.

Auditabilidade algorítmica

É a possibilidade de que as pessoas afetadas pelos algoritmos e autoridades competentes possam verificar a operação do algoritmo. Ver também "Responsabilidade algorítmica (*accountability*)" e "Explicabilidade".

Autodeterminação informativa

Autodeterminação informativa (art. 2º, inciso II, LGPD) é o poder conferido ao indivíduo de ele próprio controlar a utilização e divulgação de seus dados pessoais. Trabalhadoras e trabalhadores possuem, por exemplo, direito de conhecer a finalidade a

que se destinam os seus dados pessoais coletados pelo empregador, inclusive informatizados.

Destaque: o conceito de autodeterminação informativa é um mecanismo importante de proteção digital. Para ilustrar a importância do tema, vale lembrar que, em 2020, a rede europeia de roupas H&M foi multada em 35,3 milhões de euros por autoridades de proteção de dados alemãs (valor recorde em casos do tipo, à época), em virtude da vigilância ilegal de funcionários. Descobriu-se que a empresa investigava de maneira bastante profunda a vida privada de seus funcionários, mantendo registros amplos sobre assuntos como problemas familiares, crenças religiosas, entre outros[11].

Big data

Big data (data=dados) descreve uma forma de lidar com enormes quantidades de informações (TAULLI, 2020, p. 60). ***Big data*** são grandes e heterogêneas quantidades de dados produzidos rapidamente por uma ampla diversidade de fontes. As inovações tecnológicas vêm permitindo que esses dados sejam coletados e processados, notadamente para conhecimento preditivo. Portanto, o conceito se refere tanto aos dados em si como a sua análise. A crescente mensurabilidade das interações humanas em ambiente digital e o aumento da instalação de sensores em meios físicos (como ocorre na Internet das Coisas) vem permitindo expansão do volume, variedade, velocidade, veracidade e valor dos dados colhidos. A análise de dados nessa escala (viabilizada pelo crescente potencial computacional – ver "Inteligência Artificial") permite extração de informações a partir

11 www.thebritishjournal.com/world/hm-fined-record-e35-million-for-illegal-surveillance-of-employees-thebritishjournal-reports-140422-2020

de relações complexas (não lineares). Com isso, modificam-se produtos, empresas, governos e até o modo como as pessoas se relacionam. O conceito é especialmente sensível porque grande parte do que convencionalmente se denomina ***Big data*** são dados pessoais. Ainda, as grandes estruturas exigidas para sua coleta e processamento leva a sua dominação por grandes corporações (como as chamadas "***Big Five"*** – Facebook, Amazon, Apple, Microsoft e Google), com reestruturação das relações de poder na sociedade (ver "Capitalismo de Dados").

Caixa opaca

Ver "Opacidade Algorítmica".

Capitalismo de Dados

Os dados vêm ganhando papel de destaque no capitalismo contemporâneo, a ponto de estudiosos passarem a utilizá-lo para a qualificação do atual arranjo econômico, embora ainda não haja consenso teórico quanto a tal qualificação (fala-se em capitalismo de dados, dadocêntrico, de plataformas, de vigilância, etc.). Nada obstante a diversidade de expressões ainda existente, fato é que a economia vem se orientando em grau crescente à coleta, ao processamento e à utilização de dados. As organizações mais bem posicionadas para se aproveitar de tal tendência passam a desempenhar papel de destaque nas relações sociais (v. ***Big data***).

Cidadania digital

Trata da necessidade de inclusão e de educação digital, na forma do artigo 4º do Marco da Internet (Lei nº 12.965/2014),

no qual se reconhece o direito do acesso à internet a todas as pessoas, o que compreende o acesso à informação, ao conhecimento, à participação na vida cultural e na condução dos assuntos públicos; a promoção da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso, e, por fim, a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados. Um indivíduo incluído digitalmente é aquele que usa desse suporte para melhorar as suas condições de vida.

Destaque: o Brasil tinha aproximadamente 30 milhões de pessoas acima de 60 anos de idade em 2019 e, de acordo com o IBGE, daqui a 25 anos esse grupo deverá ser de um quarto da população brasileira. Apesar da tendência mundial de crescimento desse grupo, ele ainda é o menor grupo etário de usuários conectados à internet: apenas 31,1% de toda a população idosa do Brasil utiliza a internet. A taxa de **analfabetismo** das pessoas com **60 anos** ou **mais equivale a** 18,0% do total desse grupo etário. Para aquelas pessoas que mal tiveram oportunidade de estudar, num mundo globalizado e repleto de novas tecnologias, envelhecer pode significar exclusão digital e isolamento social. Por isso, o Estatuto do Idoso (Lei nº 10.741/2003) no art. 21 assegura o direito à educação da pessoa idosa, com a inclusão obrigatória de técnicas de comunicação, computação e demais avanços tecnológicos nos cursos especialmente desenhados para ela, com vista à sua integração à vida moderna.

Código-fonte

Corresponde "[...] a um sistema de símbolos utilizados para codificar o programa-fonte em uma determinada linguagem de

programação" (SILVA, 2016, p. 324). Por meio dele, o programa-fonte "[...] é convertido na linguagem de máquina, uma receita de comandos que o computador é capaz de entender" (SILVA, 2016, p. 324).

Consentimento livre

No contexto da proteção de dados, o consentimento é uma das hipóteses taxativas em que o tratamento de dados pessoais é autorizado (conforme art. 7º da LGPD, o tratamento também é permitido para cumprimento de obrigação legal ou regulatória, pela administração pública, para realização de estudos, para execução de contratos, para exercício regular de direitos em processos, para proteção da vida, para tutela da saúde, para atender a interesses legítimos do controlador ou terceiro e para a proteção do crédito). O consentimento para tratamento de dados deve ser dado de forma livre, informada e inequívoca (art. 5º, XII, LGPD) e por meio que efetivamente demonstre a manifestação de vontade do titular (art. 8º, ***caput***, LGPD). Se por escrito, deve constar em cláusula destacada das demais, cabendo ao controlador o ônus probatório de sua obtenção. Ele não pode ser viciado nem genérico (devem ser indicadas as finalidades específicas) e o titular tem direito a sua revogação a qualquer momento (art. 8º da LGPD). No Direito Europeu, entende-se que o desequilíbrio de poder inerente à relação de emprego no mais das vezes não permite consentimento livre, pelo que apenas em situações excepcionais ele é aceito como fundamento para tratamento de dados de empregados (em geral, quando a aceitação ou recusa não gera efeitos à trabalhadora) (***Opinion 2/2017 on data processing at work Adopted on 8 June 2017***). Vale lembrar, no entanto, que o consentimento é apenas uma das hipóteses autorizativas do tratamento de

dados pessoais previstas na LGPD; na relação entre empregado e empregador, certamente outras hipóteses poderão ser mais utilizadas para o tratamento de dados, como do "cumprimento de obrigação legal ou regulatória" e do "exercício regular de direitos em processo judicial" (respectivamente, inc. II e VI do art. 7º da LGPD).

Cookies

São arquivos criados pelos sites que visitamos, teoricamente desenvolvidos para tornar a experiência on-line mais fácil, já que economizam informações de navegação. Cookies permitem que possamos nos manter conectados num determinado site, e que as preferências sejam armazenadas, assim como sugeridos conteúdos relevantes para o local em que estamos logados. Auxiliam no preenchimento de formulários (preenchimento automático com os dados frequentes, por exemplo), na identificação de serviços e produtos em estabelecimentos mais próximos, etc. Contudo, as informações que armazenam precisam ter tratamento adequado para não violar a privacidade do usuário.

Direito à intimidade

O novo contexto social impõe a revisão do conceito do direito à intimidade para que possa manter seu objetivo original de tutela de um espaço reservado a qualquer indivíduo. O direito a se isolar, a não ter interferência externa, dá lugar ao direito de poder controlar toda informação pessoal coletada por outrem, sobretudo quando comparado à possibilidade de gozar de uma série de bens, serviços e ser imerso em um fluxo de relações econômicas e sociais. Portanto, o direito à intimidade ou privacidade em sentido estrito se relaciona com o direito à livre

construção da personalidade, por um consentimento livre e informado, e com a exigência de escolher seu modo de vida de forma coerente com seus próprios princípios. O respeito à intimidade pode ser exercido em face da ação e do conhecimento dos demais, seja pelos poderes públicos ou particulares.

Direito de trabalhadoras e trabalhadores à informação

No contexto da proteção de dados, trabalhadoras e trabalhadores têm direito a ser informados de forma clara, precisa e facilmente acessível acerca das operações de tratamento de dados de que sejam titulares, bem como sua finalidade, forma e duração (art. 6º, I e IV e art. 9º da LGPD). Também têm direito a requisitar confirmação da existência ou de acesso a seus dados pessoais (art. 19 da LGPD) e a obter informações claras e adequadas sobre critérios e procedimentos utilizados para decisões automatizadas (art. 20, § 1º, LGPD).

Direito ao esquecimento

O direito ao esquecimento corresponde à ideia de que a pessoa tem direito a requisitar que seus dados sejam apagados, em certas condições, principalmente quando incorretos, irrelevantes ou excessivos para o propósito de seu tratamento. Trata-se de figura oriunda do Direito Europeu, onde se entende, no entanto, que tal direito não é absoluto, mas, sim, deve ser objeto de ponderação com outros direitos legítimos, como o direito à informação do público em geral. Tais contornos tornaram-se mais evidentes a partir da decisão da Corte de Justiça Europeia em ***Google Spain*** contra ***Spanish Data Protection Agency***, em

2014 (embora ao menos algumas das jurisdições domésticas, como da Alemanha e França, já contassem com decisões reconhecendo de alguma forma tal direito). Sob uma perspectiva mais procedimental, no Brasil, é certo que o titular dos dados tem direito a obter do controlador a eliminação daqueles dados tratados com seu consentimento (exceto quando presente outro fundamento para o tratamento – art. 18, VI, LGPD), bem como a eliminação de dados desnecessários ou ilegalmente tratados (art. 18, IV, LGPD). Em âmbito jurisprudencial, já houve reconhecimento pontual do direito ao esquecimento pelo STJ em 2018 (REsp 1.660.168). O STF analisou o tema frontalmente no RE 1010606, quando decidiu que o direito à liberdade de expressão afasta o direito ao esquecimento no Brasil, fixando tese de que "é incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais ***– especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e as expressas e específicas previsões legais nos âmbitos penal e cível***".

Dados de treinamento

São os dados que servem para a alimentação (***input***) do algoritmo utilizado para o aprendizado de máquina. Assim, vieses e limitações já existentes nesses dados, se não adequadamente considerados, incorporam-se ao modelo produzido no aprendizado de máquina, ocasionando não apenas reprodução

de discriminações subjacentes aos dados de treinamento, mas até mesmo sua amplificação, dada a retroalimentação muitas vezes utilizada no aprendizado de máquina. No jargão da área, é conhecida a expressão ***Garbage in, garbage out*** ("Lixo entra, lixo sai") para designar o conceito de dados de treinamento. Ver Aprendizado de Máquina e Discriminação Algorítmica.

Feminismo por dados (*data feminism*)

O termo foi desenvolvido por Catherine D'Ignazio and Lauren Klein na obra ***Data Feminism***. Ali se apresenta uma nova maneira de pensar a ciência e a ética por dados, realizando a sua intersecção com o pensamento feminista. Essa proposta reconhece que as narrativas em torno do ***big data*** e da ciência de dados são baseadas majoritariamente em masculinidades brancas e em uma concepção heroica da tecnologia (***techno-heroic***). A ciência por dados é uma forma de poder que tem sido utilizada para promover a democracia e os direitos humanos (expor a injustiça, otimizar os resultados de saúde e derrubar governos autoritários), mas que também tem sido usada para discriminar, vigiar e punir.

O feminismo por dados promove essa reflexão por sete princípios: 1. O feminismo por dados analisa o poder ao analisar como ele opera no mundo. 2. O feminismo por dados desafia o poder, na medida em que se compromete a desafiar as estruturas desiguais de poder e a trabalhar pela justiça. 3. O feminismo por dados eleva a autoestima e o empoderamento uma vez que nos ensina o valor das múltiplas formas de conhecimento, incluindo o conhecimento popular sobre modos de vida e a vivência dos corpos no mundo. 4. O feminismo por dados está

repensando o binarismo e as hierarquias, pois nos convida a questionar a divisão binária de gênero, ao mesmo tempo que em repensa outros sistemas de classificação e perpetuação da opressão. 5. O feminismo por dados abraça o pluralismo, quando insiste que o conhecimento mais completo é aquele advindo das perspectivas múltiplas sintetizadas, com prioridade aos saberes indígenas, locais e pragmáticos. 6. O feminismo por dados considera o contexto e assevera que os dados não são neutros nem objetivos, mas, sim, produtos de relações sociais desiguais em que o contexto é essencial para a realização da análise acurada e ética. 7. O feminismo por dados dá visibilidade ao trabalho, pois a ciência de dados, como todos os trabalhos no mundo, é fruto da participação de muitas pessoas.

Discriminação algorítmica

A discriminação algorítmica se configura pela contaminação do banco de dados de ***inputs*** por certos vieses que produzem distorções nos ***outputs,*** oferecendo um resultado em desconformidade ou com efeitos negativos que extrapolam o objetivo do programador.

Padrões algorítmicos podem se revelar enviesados e capazes de produzir uma nova espécie de dano na dinâmica laboral: a "discriminação algorítmica". Quando determinado conteúdo é valorado negativamente ou excluído do ***output*** correspondente ao que o artifício compreende como adequado com base em critérios tidos por injustamente desqualificantes.

As plataformas digitais distribuem o trabalho e a remuneração conforme a produtividade das pessoas engajadas na atividade, sem diferenciar quanto ao gênero e à raça. Essa atitude, porém, desconsidera situações em que a pessoa do traba-

lhador tem dificuldade de acesso à plataforma por questões alheias à sua vontade (***Deliveroo***). Entretanto, um estudo de Stanford constatou que a remuneração das mulheres motoristas da Uber era cerca de 7% menor do que a remuneração dos homens, embora os índices de avaliação e cancelamento fossem bastante próximos. A resposta para a diferença estava na velocidade maior com que os homens dirigiam, o que permitia ter um maior número de viagens e uma melhor remuneração. Além do mais, homens tendiam a identificar mais facilmente os locais com maior demanda.

Destaque: a Amazon abandonou um dispositivo de inteligência artificial desenvolvido para o recrutamento de novos empregados depois de o algoritmo adotado ter apresentado fortes indícios de discriminação de gênero. O sistema para seleção de empregados foi "treinado" com dados de currículos recebidos ao longo de 10 (dez) anos. Como a maioria dos selecionados ao longo do período eram do sexo masculino, o algoritmo, que se baseia em padrões genéricos do passado, priorizou apenas candidatos do sexo masculino porque o banco de dados era composto preponderantemente por profissionais do sexo masculino.

A mesma empresa utiliza algoritmos para controlar a produtividade dos empregados, cujas dispensas são decididas por um ***software*** inteligente que "descarta" os trabalhadores mais "lentos" na execução de suas tarefas. A média do tempo gasto pelos empregados é calculada a partir dos ***scanners*** pessoais que eles usam para a expedição dos produtos de suas prateleiras e esteiras. Todavia, entre os trabalhadores há mulheres grávidas, cujo tempo de execução das tarefas é maior devido à sua condição e à maior frequência de utilização do banheiro, de

modo que o algoritmo as classificou entre as mais ineficientes e as despediu, o que gerou ações trabalhistas por discriminação.

Outro exemplo de discriminação algorítmica é o caso da Uber, cujo sistema de classificação acarretava rendimentos inferiores para as motoristas mulheres.

www.uol.com.br/tilt/noticias/redacao/2018/02/07/mulheres-motoristas-de-uber-ganham-7-a-menos-do-que-homens-diz-estudo.htm

https://olhardigital.com.br/2020/10/28/noticias/uber-esta-sendo-processada-por-seu-sistema-de-classificacao/

Discriminação direta

Ato em que a exclusão ou preferência fundada na raça, na cor, no gênero ou em outros é declarada aberta e diretamente, que tem por efeito destruir ou alterar a igualdade de oportunidades ou de tratamento em matéria de emprego ou profissão. Por exemplo, a contratação apenas de homens para determinado posto de trabalho.

Discriminação indireta

É aquela que se realiza por mecanismos aparentemente neutros, mas que tem por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão para as pessoas do grupo vulnerável. O demandante deve demonstrar a situação aparente de discriminação e pode se valer da utilização de provas estatísticas – sempre que os dados que aportem sejam significativos, superando fenômenos meramente fortuitos e conjunturais. Nessa hipótese, a dinâmica

do ônus da prova requer que o demandado demonstre a proporcionalidade e legitimidade da medida de discriminação impugnada. A atenção do órgão judicante deve se voltar aos resultados da medida, sendo irrelevante a intenção discriminatória.

e-discovery

Procedimento para acesso a informações armazenadas eletronicamente, incluindo documentos, escritos, desenhos, fotografias, áudios, imagens ou qualquer outro dado ou compilação de dados, em qualquer meio a partir do qual tais informações possam ser obtidas, seja diretamente, ou, se necessário, após tradução para uma forma razoavelmente utilizável (Regra 34 da ***Federal Rules of Civil Procedure***, aplicáveis na jurisdição federal dos Estados Unidos da América).

Exemplo: o Tribunal de Bologna concluiu que um algoritmo desenvolvido pelo aplicativo Deliveroo gera efeitos discriminatórios, além de ser indiferente às vicissitudes dos trabalhadores de entrega. Essa conclusão somente foi possível após o exame do algoritmo pelo Poder Judiciário. Vide www.ilmessaggero.it/economia/news/rider_deliveroo_algoritmo_tribunale_bologna_cgil-5677019.html.

Ética digital

É o conjunto sistematicamente organizado de valores e princípios adotados por uma pessoa ou organização em interações digitais com terceiros (e internas, no caso de organizações). Tal sistema pressupõe ponderação entre as possibilidades oferecidas pela tecnologia e o comportamento moral, mediante

incidência do princípio da proporcionalidade (necessidade, utilidade, adequação e proporcionalidade). No âmbito das relações de trabalho, impõe que os empregadores respeitem a intimidade e privacidade dos empregados[12].

Etiqueta digital

É o conjunto de regras de comportamento adotadas por uma pessoa ou impostas por uma organização em interações digitais, a fim de assegurar o respeito à Ética Digital, como por exemplo, definição de horários próprios para que tais interações ocorram (para respeito às normas sobre repousos e direito à desconexão), medidas para evitar intimidações sistemáticas no trabalho, entre outras[13]. (ver "Ética Digital")

Ética da Inteligência Artificial

É o conjunto de valores e princípios que devem ser adotados pelas pessoas responsáveis pelo desenvolvimento e emprego de tecnologias de Inteligência Artificial, bem como devem ser incutidos no próprio algoritmo. Embora nesse campo haja estudo de hipóteses ainda um tanto abstratas (como a da singularidade, ponto em que a evolução da Inteligência Artificial passaria a ser desenfreada), os desafios éticos mais concretos envolvendo a Inteligência Artificial atualmente tratam do respeito à privacidade das pessoas, transparência, respeito à dignidade humana em decisões e gerenciamento automatizados, possibilidade de revisão dessas decisões, entre outros. A inteligência artificial ética pressupõe respeito a princípios como os da intimidade, igualdade, não discriminação, precaução,

12 Fonte: Nota Técnica nº 07/2020.

13 Fonte: Nota Técnica nº 07/2020.

responsabilidade e auditabilidade algorítmica (inclusive no tocante à revisão humana de decisões), explicabilidade, FATE (***fairness, accuracy, transparency, ethics***). Ver explicabilidade, FATE (***fairness, accuracy, transparency, ethics***).

Explicabilidade

Explicabilidade corresponde às técnicas de transparência em modelos complexos de ***deep learning*** (TAULLI, 2020, p. 120). Relaciona-se com a capacidade de identificar os fatores fundamentais que um modelo de Inteligência Artificial utiliza na obtenção de seus resultados. Também pode ser definida como o grau de compreensão humana acerca das decisões de um sistema de Inteligência Artificial. Está relacionada à confiabilidade das ferramentas por usuários e empresas.

FATE (*fairness, accuracy, transparency, ethics*)

Acrônimo de ***fairness***, ***accuracy***, ***transparency*** e ***ethics*** (em tradução literal: justiça, exatidão, transparência e ética), muitas vezes utilizado na área da proteção de dados e ética da inteligência artificial. No geral, são noções derivadas dos princípios regentes das atividades de tratamento de dados, previstos no art. 6º da LGPD (boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas).

Hacker

É uma pessoa que entende muito bem de programação de computadores, e gosta de tentar superar barreiras e limitações. O termo é comumente utilizado pela mídia para descrever como alguém malicioso e intrometido que descobre informações sensíveis ou invade sistemas, obtém senhas, obtém acesso a dados, por vezes tornando-os inacessíveis aos seus titulares. Essa descrição é mais bem representada pelo termo "cracker" (neologismo), pois os hackers criaram seu próprio código de ética e não admitem ser igualados aos "crackers". O cracker seria aquele que adota condutas ilícitas, infringindo a segurança de um sistema, com finalidade de obtenção de vantagens individuais. Já o hacker muitas vezes é movido por um ideal de busca de transparência, de promoção de direitos, ou mesmo de exposição de fragilidades de governos e empresas como forma de apontar erros a serem corrigidos.

Identidade digital

A identidade digital é o conjunto de dados que diferenciam de forma suficiente um indivíduo do resto de pessoas ou entidades na internet. O conceito de pessoa e de identidade é a base para definir a responsabilidade individual e a privacidade. A identidade é caracterizada por ser permanente, mesmo que haja constante evolução e alterações em sua história. Ela representa uma unidade em sua diversidade. Desde um ponto de vista procedimental, "a identidade é uma coleção de características formalizadas, que permitem a identificação e a autenticação necessárias para as relações sociais e econômicas, assim como

para tratar com as autoridades"[14]. Constituem elementos da identidade digital o nome e sobrenome, nome do pai e da mãe, os códigos de identificação que nos são designados, como, por exemplo, a direção de IP[15], o nome do domínio[16] da internet, o e-mail, entre outros. A identidade digital é uma versão digitalizada da identidade procedimental e é um meio onipresente de associação entre dados e indivíduos, por meio da coleta, armazenamento e análise de dados digitais. A digitalização oferece a oportunidade de usar um comportamento como um dado de identificação.

A identidade pode ser pessoal, corporativa ou de clientes. A primeira é aquela que identifica o usuário sem conexão a nenhuma organização. A segunda identifica a pessoa vinculada a uma organização pública ou privada mediante uma relação jurídica e é de uso obrigatório dentro da corporação. Trata-se de uma ferramenta de trabalho. A identidade de cliente é aquela que vincula a pessoa com uma organização pública ou privada com a qual ela estabelece uma relação de negócio de natureza ou vocação contínua, como os programas de fidelidade (por exemplo, das companhias aéreas), as assinaturas de serviços de ***streaming*** (Netflix, por exemplo).

14 Tradução livre, BOGDANOWICZ, Marc. BESLAY, Laurent. ***Ciberseguridad y futuro de la identidad.*** Disponible en: http://vlex.com./vid/ciberseuridad-futuro-identidad-112090.html.

15 IP significa ***Internet Protocol*** e é um número identificador que é dado a um computador ou roteador, ao conectar-se à internet. Por meio desse número o computador pode enviar e receber dados na rede.

16 Domínio corresponde ao endereço dos sites na internet.

Inteligência artificial (IA)

Conjunto de recursos computacionais voltados à solução de problemas, que demandariam o uso da inteligência humana. Compreende um amplo conjunto de métodos, técnicas, atividades e campos de estudo, enfeixados sob uma racionalidade eminentemente prática, voltada à solução de problemas multidisciplinares que, a princípio, demandariam habilidades intelectuais humanas[17].

Uma solução de IA envolve várias tecnologias, como redes neurais artificiais, algoritmos, sistemas de aprendizado, entre outros, os quais conseguem simular capacidades humanas ligadas à inteligência, como o raciocínio, a percepção de ambiente e a habilidade de análise para a tomada de decisões.

O conceito de IA, portanto, está relacionado à capacidade de soluções tecnológicas conseguirem realizar atividades de um modo considerado inteligente. IAs também podem "aprender por si mesmas", graças a sistemas de aprendizado que analisam grandes volumes de dados, possibilitando que ampliem seus conhecimentos.

É também um campo da ciência, cujo propósito é estudar, desenvolver e empregar máquinas para realizar atividades humanas de maneira autônoma. Está ligada à robótica, ao Machine Learning, ou Aprendizagem de Máquina, ao reconhecimento de voz e de visão, entre outras tecnologias[18]. Ver Aprendizagem de Máquina.

17 PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins da. ***Inteligência Artificial e Direito***. v. I. Curitiba: Alteridade, 2019.

18 www.totvs.com/blog/inovacoes/o-que-e-inteligencia-artificial

Internet das Coisas

É o modo como os objetos físicos estão conectados e se comunicando entre si e com o usuário, por meio de sensores inteligentes e softwares que transmitem dados para uma rede. Quaisquer objetos podem integrar a internet das coisas, desde um relógio ou uma geladeira, até carros, máquinas, computadores e smartphones.

Lavagem de dados

Consiste na utilização das tecnologias do ***Big data***, Inteligência Artificial e Caixas Opacas para a prática de atos discriminatórios com aparência de neutralidade[19]. Ver ***Big data***.

Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

Em 15 de agosto de 2018, foi publicada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), com prazo de ***vacatio legis*** alterado diversas vezes: a sua vigência se iniciou em 18/09/2020, exceto no que se refere às sanções administrativas, que entram em vigor em 1º/8/2021. O art. 1º da LGPD aponta como finalidade da lei a proteção dos "***direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural***", sem fazer qualquer distinção quanto ao tipo de relação jurídica em que se dê o tratamento de dados pessoais, abrangendo as relações de trabalho. A disciplina da proteção de dados pessoais tem como fundamentos:

19 AJUNWA, I. ***The "black box" at work***. Big Data & Society. July 2020. doi:10.1177/2053951720938093

I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. No trabalho, a pessoa tem a oposição, acesso, retificação, cancelamento ou bloqueio e, até mesmo, o direito ao anonimização, uso limitado dos dados ou informação sobre as entidades públicas ou privadas que tiveram acesso aos dados. A relação de direitos do titular está enumerada no art. 18 da LGPD e se exerce mediante petição junto ao controlador, que pode responder por meio eletrônico ou sob a forma impressa. Em 9 de julho de 2019, a Lei nº 13.853 criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai editar normas e fiscalizar procedimentos sobre proteção de dados pessoais. Entre as competências da ANPD estão: zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e aplicar sanções em caso de tratamento de dados feito de forma irregular.

Liberdade de expressão

Segundo o art. 13 da Convenção Americana de Direitos Humanos[20], a liberdade de pensamento e de expressão compreende a liberdade de buscar, receber e difundir informações e ideias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro processo de sua escolha. O exercício do direito

20 www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm

não pode estar sujeito à censura prévia, mas é vinculado a responsabilidades ulteriores, observando-se o respeito aos direitos ou à reputação das demais pessoas e a proteção da segurança nacional, da ordem pública, da saúde ou da moral pública. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência. A liberdade de expressão no ambiente de trabalho deve observar as mesmas restrições e cuidados tanto por parte da pessoa que presta o serviço, quanto por parte do empregador.

Malware

Abreviação de "software malicioso" (***malicious software***), o malware é um tipo de software desenvolvido para infectar um computador e causar prejuízos, inclusive na forma de vírus. Ver Ransonware e Vírus.

Metadados

São dados sobre outros dados. Os dados relativos a comunicações entre pessoas são especialmente relevantes para efeitos de proteção, como, por exemplo, quem se comunicou com quem, a que horas, por quanto tempo e localização dos dispositivos utilizados. Apesar de aparentemente serem meramente acessórios, metadados podem ser mais reveladores do que o

próprio conteúdo das comunicações. Com técnicas adequadas, um mapa de relações, por exemplo, pode permitir inferências sobre hábitos, orientação sexual, política, participação em organizações etc. Ver "Inteligência Artificial" e "Big data".

Opacidade algorítmica

Em razão da complexidade dos dados de treinamento e do próprio algoritmo, o processo de decisão do modelo gerado pelo algoritmo pode não ser imediatamente compreendido por terceiros. Ele pode operar como uma "caixa opaca", em que são visíveis a princípio apenas os dados de entrada e saída, mas não seus mecanismos internos de produção do resultado de saída. Assim, é possível que o algoritmo esconda discriminações desejadas ou previsíveis ou mesmo reproduza ou potencialize discriminações originalmente não previstas, de modo que é fundamental exigir transparência. Ver "Lavagem de Dados", "Aprendizado Profundo" "Dados de Treinamento" e "***Big data***".

Destaque: sobre esse item, com especial enfoque no Aprendizado Profundo, ver a seguinte entrevista do Prof. Michal Kosinski: https://diariodosudoeste.com.br/almanaque/nunca-entenderemos-a-inteligencia-artificial/

Pessoa digital

É construída pela atuação direta do indivíduo mais ou menos consciente de suas implicações na internet e é resultado de três forças em permanente tensão: identidade, privacidade e cumprimento da lei. A pessoa digital se configura pela projeção dos direitos da personalidade na internet, mediante a ação dos usuários e sua interação entre si e com os provedores de serviços.

Perfil digital

Resulta da observação das nossas atividades na rede mundial de computadores, combinadas com a mensuração dos registros, em um processo de retroalimentação sobre as identidades digitais que são observadas, captadas, armazenadas e cruzadas pelas empresas.

Phishing

É um tipo de golpe online em que criminosos se passam por organizações legítimas, por e-mail, mensagem de texto, anúncio ou outros meios, a fim de roubar informações confidenciais. São enviadas mensagens (por e-mail ou outros aplicativos) que despertam a curiosidade ou a preocupação do usuário, tais como informações de débitos em instituições bancárias, e são utilizados endereços eletrônicos muito similares aos da real Instituição, justamente para causar a confusão. Assim, o próprio usuário clica em um link e coloca os seus dados, que são "pescados" pelo programa. Geralmente, esses links são enviados para uma grande quantidade de usuários, e cerca de 5% (cinco por cento) dos destinatários efetivamente clicam no link.

Privacy by design

É uma filosofia promovida pela Dra. Ann Cavoukian (anos 1990), que foi representante da comissão de privacidade de Ontário, Canadá, para a construção de sistemas de informação, processos de negócios e sistemas físicos respeitosos com a privacidade. Estabelece que a tecnologia considere, desde o princípio, a privacidade do usuário. Um sistema produzido seguindo

essa filosofia tem como princípios: 1. Ser proativo, não reativo; ser preventivo, não remediador; 2. A privacidade é o modelo padrão; 3. A privacidade é considerada desde o desenho do sistema; 4. Funcionalidade completa (soma positiva, não zero); 5. Proteção em todos os extremos do ciclo de vida do programa ou sistema; 6. Visibilidade e transparência; 7. Respeito à privacidade da usuária e do usuário. Para construir um sistema informático PbD, deve-se responder a cinco perguntas: "Qual será a informação privada a ser manejada?", "quem terá acesso a informação do indivíduo?", "com que medida, granularidade e em que modalidade é necessário o acesso à informação?", "para que deve ser coletada, armazenada e tratada a informação?", e "quando?", trata do período que deve permanecer o acesso à informação e quando perde sua vigência.

Princípio da igualdade

O princípio da igualdade está positivado no art. 5º, ***caput,*** do texto constitucional brasileiro e é expressão do princípio da dignidade humana (art. 1º, III, CRFB). Ele se aplica a nacionais e estrangeiros. O direito à igualdade, associado ao direito à liberdade (art. 5º, ***caput***), configura um valor-chave para a fundamentação e exercício de todos os demais direitos constitucionais, sendo a base do Estado Democrático de Direito. A igualdade formal não esgota e não resolve isoladamente a igualdade material, de maneira que os direitos sociais visam concretizar a igualdade e o Estado é chamado como garantidor das necessidades sociais. O direito à igualdade exerce dupla função na regulamentação da relação de trabalho. De um lado, ele assegura a todos sujeitos laborais, trabalhadoras e trabalhadores ou empregadoras e empregadores, um tratamento igualitário por parte dos poderes públicos no exercício

de suas funções legislativa (igualdade na lei), executiva e jurisdicional (igualdade perante a lei). Esta regra limita a atuação estatal normativa e de aplicação do direito, assim como limita a autonomia coletiva. Toda e qualquer limitação, seja constitucional ou infraconstitucional, ao direito à igualdade necessita responder de forma positiva ao princípio da proporcionalidade. O respeito ao princípio da proporcionalidade exige a comprovação de que a medida de tratamento desigual prevista na norma seja necessária, adequada e proporcional.

Princípio da não discriminação

A Convenção nº 111 da OIT conceitua discriminação como ***toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão;*** bem como, ***qualquer outra distinção, exclusão ou preferência que tenha por efeito destruir ou alterar a igualdade de oportunidades ou tratamento em matéria de emprego ou profissão que poderá ser especificada pelo Membro interessado depois de consultadas as organizações representativas de empregadores e trabalhadores, quando estas existam, e outros organismos adequados.*** O direito se opõe às condutas discriminatórias arbitrárias, que aprofundam ou perpetuam desigualdades históricas e sociais. Segundo Mauricio Godinho, ***discriminação é a conduta pela qual nega-se à pessoa tratamento compatível com o padrão jurídico assentado para a situa***ção concreta por ela vivenciada[21]***.*** O princípio da não discriminação é um desdobra-

21 GODINHO, Mauricio. Proteções contra discriminação na relação de emprego. In: ***Discriminação***. [VIANA; RENAULT] (coords.). São Paulo: LTr, 2000. p. 97.

mento do princípio da igualdade, com um juízo de valor mais severo e consequências mais graves. As normas antidiscriminatórias tutelam em particular as próprias diferenças, físicas ou não, que são alheias à vontade do indivíduo, tais como o sexo, a raça, a etnia, etc., ou advindas da manifestação do exercício de um direito humano, tais como o estado civil, a religião, a origem, etc., a fim de adotar medidas repressivas, compensatórias ou promocionais que minimizem os efeitos jurídicos, sociais e econômicos da diferença.

Princípio da precaução

O princípio da precaução aparece sintetizado no art. 15 da Declaração do Rio de Janeiro sobre Meio Ambiente e Desenvolvimento, pelo qual, ***"quando houver ameaça de danos sérios ou irreversíveis, a ausência de absoluta certeza científica não deve ser utilizada como razão para postergar medidas eficazes e economicamente viáveis para prevenir a degradação ambiental"*** (ONU, 1992). A aplicação nas relações de trabalho pode ser igualmente fundamentada no art. 200, que insere o meio ambiente do trabalho no conceito difuso de meio ambiente seguro e saudável como direito fundamental, e no art. 225, § 1º e § 3º, inciso V, da Constituição da República de 1988, que obriga a adoção de medidas para redução de riscos previsíveis e potenciais, mesmo que ainda não sufragados pela pesquisa científica. A precaução é a cautela antecipada diante do risco ou perigo, ou melhor, do desconhecido. Há necessidade de prevenção do risco quando não é possível saber plenamente qual será o resultado de determinada atividade em relação ao meio ambiente, caso em que a conduta deve ser interrompida. As características do princípio da precaução são: a) a incerteza do dano ambiental e b) risco ou perigo. Há o dever, por parte

dos agentes públicos ou particulares, de agir para eliminá-lo, neutralizá-lo ou ao menos minorá-lo.

Proteção de dados pessoais

Direito fundamental de controle da coleta, armazenamento, tratamento e exatidão dos dados pessoais por terceiros, em arquivos e processos realizados de forma automatizada ou não. O controle sobre a coleta, armazenamento e tratamento dos dados pessoais geralmente é associado ao direito à privacidade, pois o acesso indevido a opiniões políticas, ideológicas, religiosas ou outros dados sensíveis pode ilicitamente ser um critério de seleção de trabalhadora ou trabalhador. Ele se debilita quando associado a um contrato livremente firmado pelas partes, caracterizado por acentuada assimetria de poderes e de conhecimento entre contratantes, como é o contrato de trabalho subordinado.

Destaque: é lei! Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

Em 15 de agosto de 2018, foi publicada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), com prazo de ***vacatio legis*** alterado diversas vezes: a sua vigência se iniciou em 18/9/2020, exceto no que se refere às sanções administrativas, que entram em vigor em 1º/8/2021. O art. 1º da LGPD aponta como finalidade da lei a proteção dos "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", sem fazer qualquer distinção quanto ao tipo de relação jurídica em que se dê o tratamento de dados pessoais, abrangendo as relações de trabalho. A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade

de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Esta norma foi publicada sem a normatização da respectiva autoridade fiscalizadora, o que se concretizou em 9 de julho de 2019, por meio da Lei nº 13.853, que criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai editar normas e fiscalizar procedimentos sobre proteção de dados pessoais. Entre as competências da ANPD estão: zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e aplicar sanções em caso de tratamento de dados feito de forma irregular.

Ransonware

É um software malicioso que infecta seu computador e exibe mensagens que exigem o pagamento de uma taxa para que seu sistema volte a funcionar. Essa classe de vírus (malware) é um esquema criminoso para ganhar dinheiro que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagem instantânea ou site. Ele tem a capacidade de bloquear a tela de um computador ou criptografar arquivos importantes predeterminados com uma senha. Assemelha-se a um “sequestro de dados”. Ver vírus.

Responsabilidade algorítmica (*accountability*)

A LGPD contempla expressamente os princípios da não discriminação (artigo 6º, inciso IX) e da transparência (artigo 6º, inciso VI) para o tratamento de dados pessoais. Assim, as empresas devem adotar, em diálogo com o sindicato obreiro, mecanismos de governança algorítmica, prevendo requisitos e condições específicas para o uso de decisões automatizadas no âmbito trabalhista.

Em observância aos princípios da transparência, da prevenção e da não discriminação, contidos na LGPD, as empresas devem organizar os seus programas de integridade no sentido de prevenir que as decisões automatizadas produzam resultados discriminatórios, bem como oferecer estruturas transparentes que permitam ao titular de dados que se sentir prejudicado por uma decisão tomada de forma exclusivamente automatizada, compreender como ocorreu o tratamento de seus dados.

Como decorrência dos princípios contidos na LGPD, aplica-se às relações de trabalho o princípio da inteligência artificial explicável, pelo qual "***a criação de técnicas de machine learning devem produzir modelos mais explicáveis, mantendo um alto nível de desempenho de aprendizagem; devem ainda permitir que os usuários humanos compreendam, confiem adequadamente e gerenciem com eficácia a geração emergente de agentes artificialmente inteligentes***"[22].

No Direito brasileiro ainda não há um posicionamento pacificado sobre a licitude da utilização exclusiva de sistemas automa-

22 ABRUSIO, Juliana. ***Proteção de dados na cultura do algoritmo***. Belo Horizonte: D'Plácido, 2020. p. 327.

tizados para atos de contratação e dispensa de trabalhadores. De todo modo, é certo que as empresas que optarem pela utilização de sistemas automatizados para contratação e dispensa, dentre outras tomadas de decisões no curso da relação de trabalho, deverão assegurar que os seus algoritmos sejam programados para não reproduzir tratamentos discriminatórios e sejam o mais transparentes possível, informando a empregadas e empregados e a candidata e candidatos a empregos sobre seu direito à explicação diante de decisões automatizadas (art. 20 da LGPD).

Candidatas e candidatos a emprego e trabalhadoras e trabalhadores têm direito a solicitar a revisão, preferencialmente mediante intervenção humana, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem suas condições de contratação, manutenção ou extinção da relação de trabalho (art. 20 da LGPD).

Ver explicabilidade e aprendizado de máquina.

Tecnologias garantidoras de privacidade (PET – *Privacy-enhancing Technologies*)

As tecnologias garantidoras da privacidade transformam tecnologias invasivas em tecnologias garantidoras da privacidade sem que seja necessário renunciar às funcionalidades, permitindo minimizar o uso de dados pessoais, maximizar a segurança da informação e atribuir o controle aos indivíduos. Pode-se citar como exemplo a restrição do acesso às informações, a anonimização ou pseudoanonimização das comunicações, técnicas P2DM (***privacy-preserving data mining),*** entre outros. Ver anonimização e pseudoanonimização.

Tipos de dados pessoais coletados e tratados

Os dados pessoais são classificados em dados pessoais, dados sensíveis, dados biométricos e dados genéticos. A categoria "dados pessoais" engloba todas as informações relativas a uma pessoa identificada ou identificável. Dados sensíveis são os dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual (dados genéticos). Dados relativos à saúde são relacionados à saúde física ou mental de uma pessoa, incluindo a prestação de serviços de saúde, que revelem informações sobre o estado de saúde e eventualmente possibilitem práticas discriminatórias. Dados biométricos são dados pessoais resultantes de um tratamento técnico específico, relativo às características físicas, fisiológicas ou comportamentais, que confirmem a identidade de uma pessoa. Dados genéticos são dados relativos às características genéticas, hereditárias ou adquiridas de uma pessoa singular que deem informações sobre a fisiologia ou a saúde dessa pessoa e que resulta de uma análise de uma amostra biológica proveniente de uma pessoa singular. O reconhecimento facial, por exemplo, é uma tecnologia de tratamento automatizado de imagens digitais, que contém os rostos das pessoas para fins de identificação ou de autenticação em comparação a modelos de rostos. Usar tecnologias de reconhecimento facial para contratar e demitir pessoas com base nos seus níveis de atenção, aparência ou estado de humor deve ser proibido, segundo um conjunto de diretrizes especificas publicadas pelo Conselho da Europa. É irrelevante a autorização de trabalhadoras e trabalhadores, atuais ou futuros, em virtude do desequilíbrio de poderes entre empregados e empregado-

res. Os guias do Conselho da Europa afirmam que a tecnologia de reconhecimento só é **válida** para **propósitos de autenticação** (como para ingresso no local virtual ou presencial de trabalho ou comprovar a identidade de alguém). Ainda assim, deve existir uma alternativa para pessoas que não queiram usar a tecnologia, como uma palavra-passe ou um crachá, e esta alternativa "deve ser de utilização fácil". Caso contrário, os usuários não podem fazer uma "escolha genuína".

Variáveis *proxy*

São variáveis utilizadas em aprendizado de máquina que, embora a princípio neutras, têm uma relação estreita com outras variáveis (inclusive dados pessoais sensíveis) a ponto de poderem ser utilizadas como substitutas destas para efeitos de classificações e decisões, abrindo possibilidade de discriminação velada. Por exemplo, a segregação existente dentro de uma cidade pode criar estreita correlação entre as variáveis CEP e raça, de modo que a primeira pode servir como proxy da segunda e, assim, decisões (para contratação de trabalhadores, por exemplo) baseadas naquela podem equivaler a discriminação racial, tenha ela sido desejada ou não pelo agente de decisão. Ver Opacidade Algorítmica e Lavagem de Dados

Destaque: uma ferramenta de Inteligência Artificial da Amazon utilizada para seleção de candidatos a emprego, uma vez treinada com base em currículos majoritariamente de homens, atribuía pontuação menor a currículos que mencionavam dois colégios exclusivos para mulheres. A empresa descobriu isso em 2015 e deixou de usar o programa[23].

23 www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

Destaque: em 2004, pesquisadores do MIT e da Universidade de Chicago enviaram milhares de currículos falsos a centenas de empresas que anunciavam vagas. Alguns dos supostos candidatos tinham nomes americanos tradicionalmente associados a brancos (como Brendan, Gregg, Emily e Anne) e a outros foram conferidos nomes tidos como típicos de negros (tais como Tamika, Aisha, Rasheed e Tyrone). Os sobrenomes foram escolhidos com o mesmo propósito. O objetivo era verificar se isso alterava o modo como os currículos eram recebidos. Como resultado, currículos com nomes típicos de brancos receberam uma resposta a cada 10 vezes em que enviados, ao passo que aqueles de negros precisavam em média de 15 envios para uma resposta. Além disso, candidatos com "nomes brancos" e credenciais superiores recebiam 30% mais respostas, enquanto para aqueles com "nomes negros" tais credenciais tiveram pouco efeito[24].

Vigilância digital

A importância dos dados no atual arranjo das relações socioeconômicas vem incentivando a vigilância digital para sua coleta massiva, por meio de novas tecnologias de informação e comunicação, com vistas à geração de valor. No âmbito das relações de trabalho, essas novas tecnologias vêm permitindo a intensificação do monitoramento dos trabalhadores, tanto para gestão imediata do trabalho, quanto para acumulação de informações a permitir o refinamento ou a automatização das tarefas (os dados coletados alimentam modelos preditivos sobre compor-

24 BERTRAND, Marianne; MULLAINATHAN, Sendhil. Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination. ***The American Economic Review***, v. 94, n. 4, p. 991-1013, 2004.

tamentos e habilidades do trabalhador e servem, assim, para informar atos de decisão da empresa, muitas vezes automatizados). A vigilância digital, no entanto, é mais intrusiva do que o mero monitoramento, pois capta informações que transbordam o poder empregatício típico, muitas vezes violando a intimidade do trabalhador. Ela é multipropósito e pode levar ou servir a práticas discriminatórias, de intensificação de pressões por intensidade e quantidade de trabalho (com riscos à saúde e segurança), controle de trabalhadores originalmente não considerados empregados, confusão entre as fronteiras de trabalho e vida privada, etc. Note-se que a vigilância digital é viabilizada pelas mesmas tecnologias, genericamente consideradas, que vêm permitindo o aumento de utilização do trabalho remoto. Este, pois, apesar de equivocadamente assimilado anteriormente com um maior grau de autonomia do trabalhador, pode muitas vezes redundar no contrário. A vigilância digital vem se aprimorando a cada dia. Uma tendência recente, por exemplo, é a dos dispositivos vestíveis. Alguns sensores podem ser considerados controversos, pois captam dados de saúde, expressões faciais, voz, impressões digitais e forma da retina. Mas em alguns momentos, as inovações flertam com a distopia. Há notícias da criação de dispositivos para monitoramento neural de trabalhadores[25], assim como implantes de microchips[26]. A prática mais usual de vigilância, no entanto, talvez seja a obtenção de informações de empregados na Internet, como em seus perfis em mídias sociais, notícias, etc., o que vem sendo denominado como ***Cybervetting*** (investigação digital). Ver ***Big data*** e Capitalismo de Dados.

25 https://onlabor.org/neuro-surveillance-and-the-right-to-be-humans-at-work

26 www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin

Destaque: a Amazon obteve recentemente (2018) duas patentes para pulseiras inteligentes que rastreiam de forma permanente a posição das mãos dos trabalhadores de seus centros de distribuição, permitindo monitoramento e ***feedback*** em tempo real (a própria pulseira poderia vibrar, por exemplo, quanto a erros cometidos na separação de encomendas, tempo utilizado nas tarefas e pausas de descanso ou para utilização de instalações sanitárias). Isso, tecnicamente, permitiria que os já sofisticados sistemas automatizados de mensuração e cobrança de produtividade da companhia se aproximassem ainda mais do controle pleno dos próprios corpos dos trabalhadores, como se estes fossem meros robôs. Não há notícia de que tal solução tenha sido efetivamente implementada[27].

Vírus

Vírus é um tipo de software (programa) mal-intencionado. Quando esses programas são executados, o vírus embutido também é executado, propagando assim a 'infecção'. Isso normalmente acontece de forma invisível para o usuário. Há vários tipos de vírus, alguns são espiões, outros são apenas "brincalhões" e executam mensagens jocosas na tela, já outros causam danos que podem ser irreversíveis, como destruir todos os arquivos do usuário. Para se prevenir, é importante ter programas antivírus instalados, realizar atualizações desses antivírus periodicamente, e ter muito cuidado ao instalar programas ou clicar em arquivos executáveis (aqueles que terminam com a extensão ".exe"), principalmente quando recebidos por e-mail. Também é conveniente ter cuidado ao utilizar drives externos (como pendrives, por exemplo), que

27 www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html

podem estar infectados. Ainda, é preciso cuidado ao realizar downloads, buscando sempre sites confiáveis. Ver Ransonware.

Whistleblower (denunciante)

Termo utilizado para se referir a pessoas que detenham conhecimentos privilegiados e reportam, de boa-fé, atos ilícitos às autoridades competentes. Precisam ser protegidas pelo Estado para que a denúncia seja encorajada, o que auxilia o combate às ilicitudes.


MPT