UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Área de Concentração em Constituição, Sociedade e Pensamento Jurídico

RICARDO ANTONIO MAIA DE MORAIS JÚNIOR

ACCOUNTABILITY E DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS ENQUANTO LIMITES AO USO DA INTELIGÊNCIA ARTIFICIAL NA RELAÇÃO DE EMPREGO

FORTALEZA

2023

RICARDO ANTONIO MAIA DE MORAIS JÚNIOR

ACCOUNTABILITY E DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS ENQUANTO LIMITES AO USO DA INTELIGÊNCIA ARTIFICIAL NA RELAÇÃO DE EMPREGO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito. Área de concentração: Constituição, Sociedade e Pensamento Jurídico.

Orientador: Prof. Dr. Francisco Gérson Marques de Lima.

FORTALEZA
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M826a Morais Júnior, Ricardo Antonio Maia de.
Accountability e direito fundamental à proteção de dados pessoais enquanto limites ao uso da inteligência artificial na relação de emprego / Ricardo Antonio Maia de Morais Júnior. – 2023.
161 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós-Graduação em Direito, Fortaleza, 2023.
Orientação: Prof. Dr. Francisco Gérson Marques de Lima.

1. inteligência artificial. 2. relação de emprego. 3. direitos fundamentais. 4. proteção de dados pessoais. 5. accountability. I. Título.

CDD 340

RICARDO ANTONIO MAIA DE MORAIS JÚNIOR

ACCOUNTABILITY E DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS ENQUANTO LIMITES AO USO DA INTELIGÊNCIA ARTIFICIAL NA RELAÇÃO DE EMPREGO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito. Área de concentração: Constituição, Sociedade e Pensamento Jurídico.

Orientador: Prof. Dr. Francisco Gérson Marques de Lima.

Aprovada em: 05/05/2023.

BANCA EXAMINADORA

_____
Prof. Dr. Francisco Gérson Marques de Lima (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Emmanuel Teófilo Furtado Filho
Universidade Federal do Ceará (UFC)

_____
Prof.ª Dr.ª Ana Virgínia Moreira Gomes
Universidade de Fortaleza (UNIFOR)

FORTALEZA
2023

A Deus.

Aos meus avós maternos, que partiram durante meu Mestrado, mas deixaram um legado imenso e eterno em sua família.

AGRADECIMENTOS

A Deus, pelo dom da vida, por todas as bençãos e pelo sustento espiritual nas horas mais difíceis.

Aos meus pais, Ricardo e Antonia, a quem devo o prazer em estudar e a busca sempre por realizar justiça e propor melhorias à realidade.

À minha noiva, Gabriella, por me suportar nos momentos mais difíceis, por me apoiar nas decisões mais importantes e por comemorar junto a mim os momentos mais felizes.

Ao Professor Dr. Gérson Marques, pela orientação acadêmica na realização desta pesquisa, mas além, na parceria e no apoio ao crescimento pessoal e profissional, sempre com o propósito de buscar a justiça social.

Ao Professor Dr. Emmanuel Furtado Filho e à Professora Dr.ª Ana Virgínia Moreira Gomes, pela participação na Banca examinadora desta dissertação e pelos ricos e valiosos comentários e proposições, visando a melhoria e o aprofundamento da pesquisa.

À Professora Dra. Maria Vital da Rocha, pelos conselhos pessoais e profissionais sempre relevantes, além do apoio na caminhada acadêmica e profissional.

Aos colegas do programa de Pós-Graduação em Direito da Universidade Federal do Ceará, por tornarem os anos dedicados ao Mestrado mais leves e mais proveitosos, proporcionando aprendizados e visões distintas do mundo.

À Faculdade de Direito da Universidade de Lisboa, que me recebeu durante alguns meses para a realização de um período do Mestrado em suas dependências, com o apoio de valorosos professores e professoras, que contribuíram com a abertura da minha visão de mundo e do Direito.

À CAPES, pelo apoio financeiro durante o Mestrado. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

A todos os demais que, direta ou indiretamente, contribuíram com a realização dessa pesquisa e com a conclusão desse ciclo, que marca o início da minha carreira acadêmica.

“Os privilegiados, veremos cada vez mais, serão analisados por pessoas; as massas, por máquinas.”
(O’NEIL, Cathy, 2016, p. 8, traduziu-se).

RESUMO

O estudo se propõe a verificar quais as medidas necessárias para que a utilização de mecanismos de Inteligência Artificial na relação de emprego possa garantir o direito à proteção de dados pessoais do empregado, mitigando os riscos e seguindo os requisitos do princípio da "*accountability*" no tratamento automatizado de dados. Para atingir esse objetivo geral, a presente pesquisa analisa, inicialmente, quais são os principais usos da IA nas relações de emprego, delimitando quais tecnologias devem ser consideradas, qual a influência do *Big Data* para sua difusão na relação de emprego, e quais as principais finalidades a que seu uso é destinado pelo empregador. Em um segundo momento, baseando-se nas peculiaridades da relação de emprego que justificariam uma abordagem diferenciada das demais, ponderam-se os riscos provenientes do uso dessas tecnologias baseadas em IA quanto à proteção de dados do empregado, notadamente quanto aos seus direitos de personalidade, quanto ao direito à privacidade e quanto ao direito à igualdade e não discriminação no local de trabalho. Após isso, apresenta-se o direito fundamental à proteção de dados pessoais como limite ao poder de controle do empregador, verificando-se os requisitos jurídicos para a utilização da IA na relação de emprego, diante do dever de *accountability* (responsabilização e prestação de contas) empresarial. A pesquisa pode ser classificada como básica, explicativa e qualitativa (sob o ponto de vista da forma de abordagem do problema), adotando o método de pesquisa hipotético-dedutivo. A hipótese testada durante toda a pesquisa é de que as medidas hoje previstas na legislação de proteção de dados brasileira não são suficientes para atender ao princípio da responsabilização e prestação de contas (*accountability*), devendo haver outras medidas consideradas boas práticas, inclusive com especificidades voltadas ao âmbito das relações de emprego, diante de suas características próprias. Após testes durante toda a pesquisa, verificou-se, inicialmente, o uso da IA na relação de emprego desde a fase pré-contratual, em processos de recrutamento e seleção; durante o contrato de trabalho, mediante a gestão algorítmica do trabalho; e nas situações excepcionais, a IA é utilizada para premiar empregados em promoções, mas mais ainda em situações visando aplicar sanções àqueles que não desempenhem suas funções apropriadamente. Em segundo momento, indicou-se a existência de algumas características na relação de emprego que a diferenciam das demais quando ao uso da IA pelo empregador, o que permitiu identificar a ocorrência de riscos aos direitos dos empregados que demandam a adoção de medidas pelo empregador para mitigá-los e documentar quais medidas foram eficazes para esse propósito. Por fim, confirmou-se a hipótese inicialmente formulada, de que apenas a adoção do regime legal da proteção de dados não é suficiente, tendo em vista

não haver regulação setorial quanto ao uso da IA na relação de emprego, o que torna necessária a adoção, também, de boas práticas de governança de dados pessoais, baseadas nos riscos envolvidos. Como possíveis boas práticas, sugeriu-se na presente pesquisa os seguintes: (i) a formulação de regras de governança de dados de toda a cadeia de agentes de tratamento de dados; (ii) o mapeamento dos riscos a direitos dos empregados e a aplicação do princípio da precaução; (iii) a adoção de medidas para resguardar a qualidade das bases de dados; (iv) a inclusão da participação humana nas decisões automatizadas como regra; (v) a implementação de medidas de transparência e explicabilidade quanto ao uso da IA na relação de emprego e; (vi) a disponibilização desses sistemas para possíveis auditorias de terceiros, mediante a elaboração e apresentação de relatórios de impacto à proteção de dados pessoais. Verificou-se que as medidas sugeridas são relevantes, mas não são as únicas, devendo os empregadores sempre verificar quais outras boas práticas poderão ser acrescidas, conforme o grau dos riscos mapeados. Para além disso, identificou-se que o presente trabalho deve servir como um guia a partir do qual empregadores possam implementar suas próprias medidas mitigadoras dos riscos provenientes da IA, mas também deverá servir como um guia às autoridades administrativas, judiciais ou sindicais, que busquem a fiscalização das empresas, acompanhando se estas prestarão contas de seus tratamentos de dados; bem como na atividade judicante, em que o Poder Judiciário trabalhista poderá acompanhar se as atitudes do empregador condizem com os comandos legais e com as boas práticas de proteção dos direitos dos empregados, diante de casos concretos.

Palavras-chave: inteligência artificial; relação de emprego; direitos fundamentais; proteção de dados pessoais; *accountability*.

ABSTRACT

The study proposes to verify which measures are necessary so that the use of Artificial Intelligence mechanisms in the employment relationship can guarantee the right to the protection of the employee's personal data, mitigating the risks and following the requirements of the principle of "accountability" in the automated data processing. To achieve this general objective, this research initially analyzes what are the main uses of AI in employment relationships, delimiting which technologies should be considered, what is the influence of Big Data for its diffusion in the employment relationship, and what are the main purposes for which its use is intended by the employer. In a second moment, based on the peculiarities of the employment relationship that would justify a differentiated approach from the others, the risks arising from the use of these technologies based on AI are considered regarding the protection of employee data, notably regarding their personality rights, the right to privacy and the right to equality and non-discrimination in the workplace. After that, the fundamental right to data protection is presented as a limit to the employer's power of control, verifying the legal requirements for the use of AI in the employment relationship, in view of the duty of accountability (responsibility and accountability) business. The research can be classified as basic, explanatory and qualitative (from the point of view of how the problem is approached), adopting the hypothetical-deductive research method. The hypothesis tested throughout the research is that the measures currently provided for in the Brazilian data protection legislation are not sufficient to meet the principle of accountability, and there must be other measures considered good practices, including specificities aimed at to the scope of employment relations, in view of their own characteristics. After tests throughout the research, the use of AI was initially verified in the employment relationship from the pre-contractual phase, in recruitment and selection processes; during the employment contract, through algorithmic work management; and in exceptional situations, AI is used to reward employees for promotions, but even more so in situations aimed at applying sanctions to those who do not perform their duties properly. Secondly, it was indicated the existence of some characteristics in the employment relationship that differentiate it from the others regarding the use of AI by the employer, which allowed identifying the occurrence of risks to the rights of employees that demand the adoption of measures by the employer to mitigate them and document which measures were effective for that purpose. Finally, the hypothesis initially formulated was confirmed, that only the adoption of the legal regime of data protection is not enough, considering that there is no sectoral regulation regarding the use of AI in the employment relationship, which makes the adoption

necessary, and also good governance practices for personal data, based on the risks involved. As possible good practices, the following were suggested in this research: (i) the formulation of data governance rules for the entire chain of data processing agents; (ii) mapping risks to employee rights and applying the precautionary principle; (iii) the adoption of measures to safeguard the quality of databases; (iv) the inclusion of human participation in automated decisions as a rule; (v) the implementation of transparency and explanation measures regarding the use of AI in the employment relationship and; (vi) the availability of these systems for possible audits by third parties, through the preparation and presentation of impact reports on the protection of personal data. It was found that the suggested measures are relevant, but they are not the only ones, and employers should always check which other good practices can be added, according to the degree of mapped risks. In addition, it was identified that the present work should serve as a guide from which employers can implement their own measures to mitigate the risks arising from AI, but it should also serve as a guide to administrative, judicial or union authorities, who seek the supervision of companies, monitoring whether they will be accountable for their data processing; as well as in judicial activity, in which the Labor Judiciary can monitor whether the employer's attitudes are consistent with legal commands and good practices for protecting the rights of employees, in specific cases.

Keywords: artificial intelligence; employment relationship; fundamental rights; data protection; accountability.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CF/88	Constituição Federal de 1988
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
ML	*Machine Learning*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OIT	Organização Internacional do Trabalho
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto à Proteção de Dados
STF	Supremo Tribunal Federal
TST	Tribunal Superior do Trabalho

SUMÁRIO

1 INTRODUÇÃO

O ambiente das relações humanas modificou-se profundamente nas primeiras décadas do século XXI. Por um lado, os dados se intensificaram como a principal matéria-prima para praticamente qualquer atividade empresarial. Nesse contexto, legislações de proteções de dados, já existentes em alguns países europeus desde a década de 1970, passaram a ser mais detalhadas, específicas e disseminadas para outros países, como aconteceu no Brasil em 2018, com a Lei Geral de Proteção de Dados (LGPD).

Por outro lado, o surgimento do *Big Data*, o desenvolvimento de mecanismos de Inteligência Artificial (IA) e o aprimoramento de seus padrões matemáticos – notadamente os algoritmos – possibilitaram o processamento de uma quantidade muito maior de dados em menor tempo, permitindo que a própria IA aprendesse com esses dados e conseguisse, sem uma atividade humana diretamente envolvida, desenvolver habilidades e critérios próprios para, novamente, tratar mais e mais dados (*machine learning*).

O tema da proteção de dados pessoais de empregados não é recente, havendo no Brasil, pelo menos desde a década de 1990, abordagens ligadas principalmente aos direitos à intimidade e à privacidade, assim como, mais recentemente, à desconexão do empregado. Academicamente, mesmo antes da LGPD, muito já se pesquisou acerca da privacidade e da proteção de dados do empregado no Brasil, principalmente diante da existência de um legítimo poder de controle exercido pelo empregador, o que seria capaz de demandar aspectos e discussões que sejam próprios ao âmbito laboral.

A Organização Internacional do Trabalho (OIT) publicou, em 1997, um Código de Práticas abordando o tema da Proteção de Dados Pessoais de Trabalhadores,[1] com o objetivo de orientar e prover boas práticas para que houvesse qualidade no tratamento de dados nas relações de trabalho. Apesar de trazer aspectos de governança acerca da proteção de dados no âmbito laboral, estava situado em um momento em que a internet ainda iniciava seu processo de massificação, sendo ainda distante de um cenário hoje vivenciado, em que é bastante comum que cada cidadão possua um minicomputador (*smartphone*) guardado em seu bolso, podendo trabalhar de qualquer lugar e a qualquer momento.

[1] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Protection of workers' personal data: an ILO code of practice, 1997. **Commentary on the Code of Practice**. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 07 jul. 2020.

Desde aquele período até os dias de hoje, o ambiente das relações de trabalho modificou-se bastante, principalmente nas primeiras décadas do século XXI, principalmente com as já citadas tecnologias baseadas em IA, alimentadas pelo *Big Data* e aprimoradas pelo *machine learning*, os quais trouxeram um tipo de revolução tecnológica que modificou as relações humanas.

No âmbito da Inteligência Artificial, um dos principais desafios discutidos academicamente é o de, a partir da compreensão do funcionamento dos algoritmos, tendo em vista sua capacidade de penetração em diversas áreas da vida humana,[2] desenvolver parâmetros éticos e jurídicos para a governança desses algoritmos,[3] principalmente para evitar violações a aspectos da personalidade dos indivíduos, intrusão na sua privacidade e o fenômeno que se denomina de discriminação algorítmica.

A proteção de dados pessoais implica, dentre outras obrigações a quem realiza tratamento de dados, a responsabilização por esses dados pessoais, assim como a prestação de contas da maneira como esses processos são realizados, assim como em que medida são reduzidos os riscos neles envolvidos. A doutrina internacional convencionou tratar desse tema com a expressão da língua inglesa "*accountability*"[4], já que não há tradução fidedigna para o português e para outras línguas, notadamente latinas. Esse princípio determina, inclusive, que haja boas práticas de mercado para que esses agentes que realizam o tratamento de dados possam demonstrar, de maneira transparente e responsável, quais medidas mitigadoras de risco estariam pondo em prática, bem como deixando-as acessíveis para eventuais auditorias por autoridades de controle.

Mesmo diante de tantas discussões acadêmicas acerca dos limites e dos riscos gerados por esses dispositivos tecnológicos pretensamente inteligentes, pouco ainda se discute acerca dos requisitos jurídicos para aplicação da Inteligência Artificial nas relações de emprego.

E quando se estuda acerca da relação entre Inteligência Artificial e relações de emprego, o foco é direcionado para uma análise quantitativa dos empregos após a interferência da IA, ou seja, a substituição de trabalhadores por máquinas, com a redução de postos de trabalho, pouco ainda sendo tratado acerca de uma análise qualitativa, isto é, como será o

---

[2] MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. Rio de Janeiro: Arquipélago Editorial, 2019.

[3] DONEDA, Danilo; ALMEIDA, Virgílio A. F. What is algorithm governance? **IEEE Internet Computing**, v. 20, n. 4, p. 60-63, 2016.

[4] A palavra traduz, a um só tempo, um conjunto de preceitos como responsabilidade, prestação de contas e transparência em relação às ações de indivíduos ou organizações.

trabalho exercido pelos empregados que serão mantidos diante da influência da Inteligência Artificial, inclusive a íntima relação que haverá entre humanos e máquinas.[5]

É nesse campo de estudo qualitativo, ainda pouco explorado, que se situa a relevância acadêmica do presente trabalho. A motivação acadêmica para a pesquisa que será realizada deriva da necessidade de se analisar mais profundamente a interferência da Inteligência Artificial e os riscos que surgem com seu uso, especialmente no contexto do direito fundamental à proteção de dados pessoais do empregado.

Diante desse cenário, surge um questionamento que perpassa todo o trabalho: quais medidas deverão ser seguidas pelo empregador para que garanta a proteção de dados dos empregados diante do uso de sistemas baseados em Inteligência Artificial e para que preste contas disso para as autoridades competentes?

A hipótese levantada em momento inicial, a qual será testada durante todo o trabalho, é de que as medidas hoje previstas na legislação de proteção de dados brasileira não serão suficientes para atender ao princípio da responsabilização e prestação de contas (*accountability*), devendo haver outras medidas consideradas boas práticas, inclusive com especificidades voltadas ao âmbito das relações de emprego, diante de suas características próprias.

Assim, o objetivo geral do presente trabalho é verificar quais as medidas necessárias para que a utilização de mecanismos de Inteligência Artificial na relação de emprego possa garantir o direito à proteção de dados pessoais do empregado, mitigando os riscos e seguindo os requisitos do princípio da "*accountability*" no tratamento automatizado de dados.

Para atingir esse objetivo, o presente trabalho analisará, inicialmente, quais são os principais usos da IA nas relações de emprego, considerando os motivos preponderantes que levam o empregador a adotar esse tipo de tecnologia na gestão de recursos humanos. Além disso, serão também verificadas as mais diversas aplicações práticas dessas tecnologias baseadas em IA e suas principais implicações jurídicas.

Em um segundo momento, tomando por base as peculiaridades da relação de emprego que justificariam uma abordagem diferenciada, serão ponderados os riscos provenientes do uso de tecnologias baseadas em IA quanto à proteção de dados do empregado. Nesse contexto, serão considerados, em especial os direitos de personalidade, o direito à privacidade e o direito à igualdade e não discriminação no local de trabalho.

---

[5] DE STEFANO, Valerio. 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Artificial Intelligence and Labour Protection (May 16, 2018). **Comparative Labor Law & Policy Journal**, v. 41, n. 1, 2019. p. 2-3.

Após identificados os principais usos da IA na relação de emprego e os riscos quanto à proteção de dados pessoais provenientes deles, será apresentado o direito fundamental à proteção de dados pessoais como limite ao poder de controle do empregador, proporcionando requisitos jurídicos para a utilização da IA na relação de emprego, os quais serão analisados em sua aplicabilidade no ambiente laboral e diante do dever de *accountability* (responsabilização e prestação de contas) empresarial.

Para tanto, a pesquisa, sob o ponto de vista dos procedimentos técnicos, será documental, usando como fonte a Constituição Federal do Brasil de 1988; a Consolidação das Leis do Trabalho; a Lei 9.029/95; a Lei Geral de Proteção de Dados; a legislação estrangeira (notadamente da União Europeia); além de outras normas jurídicas que possam ajudar no atingimento dos objetivos do estudo. A pesquisa também será bibliográfica, pois serão consultadas doutrinas especializadas, nacionais e estrangeiras, acerca do tema, aptas a ajudar na formação da compreensão das principais aplicações de mecanismos de IA nas relações de emprego, quais seus principais riscos à proteção de dados pessoais do indivíduo na relação de emprego e quais medidas de responsabilização e prestação de contas (*accountability*) seriam adequadas para o uso racional e responsável dessas tecnologias pelo empregador.

O método de abordagem científica aplicado será, precipuamente, o hipotético-dedutivo, pois, a hipótese apresentada passa por testes durante a pesquisa, inicialmente para verificar se a IA é aplicada na relação de emprego e de que forma seria sua utilização pelo empregador; em segundo momento, se os riscos derivados do uso dessas tecnologias na relação de emprego seriam capazes de justificar práticas além daquelas já previstas em lei e; em momento final, quais seriam essas possíveis medidas a serem adotadas pelo empregador.

A pesquisa pode ser classificada, ainda, como básica (sob o ponto de vista de sua natureza), explicativa (sob o ponto de vista de seus objetivos) e qualitativa (sob o ponto de vista da forma de abordagem do problema).

2 USO DA INTELIGÊNCIA ARTIFICIAL NAS RELAÇÕES DE TRABALHO E SUAS IMPLICAÇÕES JURÍDICAS

A utilização de ferramentas para o controle do trabalho realizado é inerente à gestão empresarial, que remonta não apenas da revolução industrial, mas desde a criação das primeiras corporações de ofício. A partir do momento em que o empresário delega suas atividades para terceiros exercerem o ofício, possui a necessidade de controlar e verificar se aquelas atividades estão sendo cumpridas a contento e seguindo os direcionamentos empresariais.

No Brasil, assim como majoritariamente nos demais países, o controle dos meios de produção pelo seu proprietário é constitucionalmente legitimado. É possível encontrar fundamento constitucional para o poder de controle do empregador, principalmente nos princípios da Ordem Econômica, previstos no artigo 170 da CF/88, mais especificamente o livre exercício da atividade econômica.

Diante de sua base constitucional, para que se verifique quais as condições que esse controle pode ser realizado, mediante o uso de ferramentas baseadas em IA, no presente capítulo serão apresentados os principais usos desse tipo de tecnologia nas relações de trabalho, conforme apresentado pela doutrina especializada e por estudos sobre o tema.

Antes, porém, será necessário realizar uma delimitação conceitual, de modo a esclarecer quais tipos de tecnologia o presente trabalho abordará, avaliando seus riscos e apontando soluções para seu correto uso pelo empregador. Assim, passa-se, adiante, ao delineamento de conceitos relevantes para o objeto de estudo, notadamente do que pode ser considerado como Inteligência Artificial e de onde ela retira seu principal insumo, os dados.

2.1 Delimitação conceitual: Inteligência Artificial, *Machine Learning* e *Big Data*

Antes de adentrar ao cerne do presente trabalho – que trata da análise dos requisitos para o uso da IA nas relações de trabalho, realizada a partir do direito fundamental à proteção de dados pessoais – será necessário verificar o que esses termos realmente significam, principalmente quando se trata de Inteligência Artificial, que não possui, até hoje, uma definição precisa e definitiva. Por se tratar de um termo que vem sendo cunhado desde, pelo menos, a década de 1950, a probabilidade de confusões terminológicas é imensa, principalmente quando hoje existem diversas metodologias (*Machine Learning*, *Deep Learning*, *Reinforced Learning*, dentre diversas outras) que são inseridas debaixo do mesmo guarda-chuva, que é o termo “Inteligência Artificial”.

É comum que haja empresas oferecendo soluções tecnológicas supostamente baseadas em IA, como ferramentas para triagem e classificação de currículos profissionais em um processo seletivo. No entanto, ao se analisar os aspectos mais particulares daquele instrumento, verifica-se tratar de mera automação ou de tecnologias que se utilizam de planilhas ou de simples códigos que foram previamente programados, com toda a lógica já desenhada e sem muita complexidade.

Por isso, é importante delimitar quais tecnologias efetivamente traduzem instrumentos de IA e que, assim, serão objeto de abordagem deste trabalho. Isso, porque o grau de complexidade que elas possuem é bastante diversificado, assim como o é o grau de risco inerente a cada uma dessas ferramentas, não sendo possível que sejam tratadas de maneira uniforme e sem compreender os limites e as possibilidades (positivas ou nefastas) que elas proporcionam.

O conceito de IA não é unanimidade na literatura especializada, principalmente porque existe uma grande variedade de metodologias aplicáveis a tantos tipos de instrumentos tecnológicos, ao ponto de que, se houvesse algum tipo de delimitação restritiva, não haveria como se ter um único conceito a ser estudado, mas vários deles. Por isso, o termo Inteligência Artificial funciona hoje como um guarda-chuva, embaixo do qual estão diversas categorias tecnológicas, como visão computacional, robótica, processamento da linguagem natural e *machine learning*, dentre diversos outros.[6]

Stuart Russell e Peter Novig[7] apresentam, didaticamente, pelo menos 4 tipos de abordagens acerca da IA. Cada uma dessas abordagens demonstra o foco em algum objetivo almejado: a primeira abordagem consiste na busca por conceber a IA pensando como um humano, exemplificando-se com a criação do GPS por Allen Newell e Herbert Simon, que não pretendia, apenas atingir o resultado de modo correto, mas comparar as etapas tomadas pela máquina em comparação com o raciocínio humano ao resolver os mesmos problemas. A segunda abordagem, por sua vez, entende que a Inteligência Artificial deve agir como um humano, a exemplo do que propunha o pensamento de Alan Turing, cuja teoria afirma que se a IA conseguisse agir como um humano, enganando um jurado, seria considerada inteligente. Ao propor a IA como um instrumento de pensamento racional, os defensores da terceira abordagem buscam ferramentas que possam criar e resolver raciocínios lógicos, é a chamada tradição logicismo da Inteligência Artificial. Por fim, a quarta abordagem, pela qual a IA deveria agir

[6] MAINI, Vishal; SABRI, Samer. **Machine learning for humans**. Online, 2017. p. 9.
[7] RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. trad. Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

racionalmente, propõe-se desenvolver sistemas de IA com características de agentes racionais, ou seja, que agem para alcançar o melhor resultado, sendo a ênfase maior na busca por inferências corretas.

Analisando essas abordagens no campo da Inteligência Artificial, apesar de bastante esclarecedoras sobre quais objetivos podem ser buscados por meio dessas tecnologias, não é possível delimitar exatamente o que ela significaria, já que cada uma delas percebe o fenômeno de uma maneira incompleta, parcelada.[8] No entanto, demonstram que não é possível tratar a IA como uma única tecnologia, mas como diversos tipos de tecnologias e com variados objetivos diferentes, dependendo da abordagem ou metodologia a ser utilizada.

O que as une, provavelmente, é sua estrutura, já que os sistemas de Inteligência Artificial são formados por algoritmos computacionais, os quais podem ser entendidos como instruções e operações matemáticas que apresentam os passos pelos quais um determinado resultado (*output*) será atingido, a partir de informações inseridas inicialmente (*input*).

É bastante comum ver comparações buscando simplificar o termo algoritmo, comparando com simples instruções, tais como uma receita de bolo. Essa afirmação pode ser verídica quando se está tratando do termo algoritmo de uma forma geral, que teve origem na matemática e realmente pode representar qualquer grupo de instruções visando atingir determinada finalidade.

No entanto, ao tratar de algoritmos computacionais, mais especificamente aqueles que são a base para sistemas de IA, Ellis Horowitz e colaboradores destacam, na obra "Algoritmos Computacionais", que é necessário que essas instruções atendam a pelo menos cinco características básicas.[9] A primeira delas é o (i) *input* que o algoritmo deve receber externamente, ou seja, um dado de entrada que lhe seja apresentado como fonte para o resultado esperado. A segunda característica é o (ii) *output*, ou seja, precisa gerar algum resultado ao final a partir das instruções. Em seguida é apresentada a (iii) definitividade (*definiteness*), que traduz a ideia de que cada instrução que dele faz parte deve ser bem definida e clara, sem que haja dubiedade, como a que está presente no exemplo apresentado pelo autor "adicione 6 ou 7 ao número representado por 'x'", pois esse tipo de dubiedade (6 ou 7) não pode ser compreendido por um computador. A quarta característica de um algoritmo é a (iv) finitude (*finitness*), segundo a qual esse processamento algorítmico deve terminar após a realização de um número

[8] FREITAS, Juarez; FREITAS, Thomas Bellini. **Direito e inteligência artificial**: em defesa do humano. Belo Horizonte: Fórum, 2020. p. 28.
[9] HOROWITZ, Ellis; SAHNI, Sartaj; RAJASEKARAN, Sanguthevar. **Computer algorithms**. Nova York: Computer Science Press, 1997. p. 1-2.

finito de etapas. Por fim, a última característica do algoritmo é a (v) efetividade (*effectiveness*), ou seja, cada instrução dele integrante deve ser básica o suficiente para que até mesmo uma pessoa com apenas papel e lápis possa utilizá-lo.

Essas características do algoritmo computacional demonstram o quão matemáticos são os algoritmos, pois seguem uma lógica de precisão e de objetividade, baseada na linguagem da programação, que não pode ser ambígua nem lacunosa. Isso demonstra uma das maiores dificuldades quando se fala no ajuste de algoritmos a preceitos éticos ou jurídicos, como dignidade da pessoa humana, razoabilidade, justiça, proteção ao trabalhador, dentre diversos outros valores que são a base do Estado Democrático de Direito.

Tendo em vista que esses preceitos são todos de conceito aberto, cujo significado dependerá de aspectos casuísticos ou valorativos de quem irá aplicá-los, não serão facilmente transpostos para a linguagem da programação. Isso é especialmente difícil quando se trata dos códigos matemáticos que fazem parte dos algoritmos, pois eles devem eles ser caracterizados com definitividade e efetividade, a ponto de poderem ser reproduzidas pela máquina. Não é simples – pelo menos até hoje – programar um algoritmo para que ele respeite a dignidade da pessoa humana, pois esse valor não pode ser facilmente transposto para a linguagem matemática, o que representa o problema do alinhamento.[10]

Essas características podem, erroneamente, passar ao leigo a impressão de que os algoritmos computacionais são neutros, não favorecendo, portanto, algum resultado enviesado pelos valores de quem o programou ou pelos valores historicamente presentes nos dados recebidos como *input*. Ledo engano, já que a definição dos objetivos a serem atingidos pelos algoritmos é feita por aqueles que os idealizaram ou elaboraram. Dessa forma, se por um lado seus critérios internos de decisão são matemáticos, por outro seus objetivos são externos, definidos por humanos.[11]

Esse problema se intensifica quando se está diante de algoritmos aprendizes, que usam o aprendizado de máquina como metodologia para criação de algoritmos. O aprendizado de máquina é uma metodologia inserida sob o conceito guarda-chuva da IA, que se diferencia bastante da lógica tradicional dos algoritmos computacionais. Enquanto tradicionalmente se obtinha resultados a partir de algoritmos, cujas regras matemáticas seriam previamente definidas pelo programador, com o aprendizado de máquina a lógica inverte: o programador

---

[10] Esse problema é retratado com maior profundidade por Brian Christian, na obra: CHRISTIAN, Brian. **The alignment problem**: Machine learning and human values. Nova York: WW Norton & Company, 2020.
[11] MACHADO SEGUNDO, Hugo de Brito. **Direito e Inteligência Artificial**: O que os Algoritmos têm a Ensinar sobre Interpretação, Valores e Justiça. São Paulo: Editora Foco, 2022. p. 7.

não indica qual o caminho que o algoritmo deve percorrer, ele estabelece um objetivo que quer alcançar (por exemplo, selecionar os currículos profissionais que mais se encaixem em uma vaga de trabalho), fornece, então, ao algoritmo aprendiz, os dados de entrada (*input*) (os requisitos da vaga de emprego ofertada) que o permite produzir um segundo algoritmo, que transforma o *input* no *output*.[12]

Essa metodologia do aprendizado de máquina, ou *machine learning* como se denominou na língua inglesa e se popularizou na literatura científica mundial, revolucionou a forma como a IA é produzida, pois, ao invés de ser programado um algoritmo tradicional, com todos os passos sob o conhecimento e a supervisão do programador, passou-se a ter a criação de um algoritmo que não se sabe bem qual o caminho que vai adotar para chegar ao resultado esperado. No momento em que o algoritmo aprendiz cria uma lógica própria, a partir dos dados que nele foram inseridos para chegar a um resultado, essa forma de decidir nem sempre fica clara aos desenvolvedores, pois pode fugir da lógica de raciocínio humana ou mesmo utilizar critérios que jamais o programador pensou em utilizar para chegar naquele resultado.

Um clássico exemplo é o da IA que foi desenvolvida pela Amazon, para recrutamento de novos desenvolvedores para a empresa. Após um tempo analisando os resultados dos processos seletivos, verificou-se que a IA estava privilegiando homens em detrimento de mulheres nas seleções, porém os programadores não tinham inserido nenhum comando direcionado para isso, muito menos havia nos currículos a informação do gênero dos candidatos.

O que se percebeu depois é que o algoritmo, ao analisar os dados históricos de contratações da mesma empresa e do mercado de tecnologia como um todo, criou uma lógica em que aquelas pessoas que haviam estudado em determinada escola, quando contratadas para cargos ligados a tecnologia, não chegavam com tanta frequência a cargos elevados quanto os candidatos que haviam estudado em outras escolas, assim privilegiando estes em detrimento daqueles. O problema, no entanto, é que a escola preterida era destinada ao público feminino.

Assim, o algoritmo cometeu discriminação quanto ao gênero (baseado em um dado aparentemente inofensivo e em uma lógica já discriminatória, historicamente presente no mercado de tecnologia) e assumiu que seria uma lógica válida a ser aplicada, pois seu único objetivo era chegar ao resultado esperado: candidatos que se encaixassem bem nos critérios da vaga proposta.

---

[12] DOMINGOS, Pedro. **O algoritmo mestre**: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec Editora, 2017. p. 29.

São os algoritmos de aprendizado de máquina que o presente trabalho abordará com maior foco, tendo em vista que são eles que geram maiores riscos aos direitos fundamentais, inclusive o direito à proteção de dados pessoais. Os algoritmos tradicionais (que, por vezes, não são sequer denominados IA, mas simples automação[13]) possuem um grau de risco muito menor, já que os erros na programação poderão ser mais facilmente consertados por quem os programou, pois estes saberão o caminho percorrido pelo algoritmo para atingir o resultado.

No contexto de algoritmos de aprendizado de máquina, por outro lado, os próprios desenvolvedores enfrentam uma verdadeira "caixa preta". Esse termo é utilizado para descrever a opacidade dos critérios utilizados por essas ferramentas. Muitas vezes, inclusive, as empresas não buscam sequer investigar seus critérios, nem mesmo revelá-los para eventuais auditorias, albergando-se no segredo de negócio.[14]

O avanço tecnológico da IA até a difusão do aprendizado de máquina no cotidiano empresarial somente foi possível a partir do início do século XXI, após pelo menos 50 anos de pesquisas sobre o tema. Isso aconteceu por consequência de diversos fatores, como bem descrito por Hugo de Brito Machado Segundo no livro "Direito e Inteligência Artificial". O referido autor constata que, nos anos 1960 e 1970, a empolgação com a possibilidade de se ter máquinas inteligentes convivendo com humanos era tamanha que já se imaginava esse cenário como possível no final do próprio século XX.[15] No entanto, acrescenta o autor, o desenvolvimento tecnológico nessa área se deu com menor velocidade do que o esperado, resultando em um período que ficou conhecido posteriormente como "inverno da IA". Chegando ao final do século XX, verificou-se que não havia sido concretizada a expectativa quanto à existência de máquinas inteligentes convivendo com seres humanos, tendo o foco da tecnologia se direcionado mais para o desenvolvimento de máquinas como ferramentas de comunicação entre os indivíduos, ou seja, como "terminais a partir dos quais os humanos

---

[13] Deve-se diferenciar os algoritmos de IA com simples automação. Esta representa os códigos matemáticos computacionais elaborados com a finalidade de atingir determinado resultado, já esperado. Enquanto isso, os algoritmos de IA dependem de treinamento e de aprimoramento para que seus resultados sejam atingidos de maneira aprimorada a partir da automação, gerando situações em que mesmos dados de entrada podem produzir resultados diferentes em um mesmo algoritmo, pois isso dependerá do treinamento e não apenas dos passos que foram programados originalmente. Para maiores explicações sobre essa diferenciação conceitual, conferir: ALBUQUERQUE, Adriana Reis de. **Poder artificial de tributar?** limites e requisitos à utilização (adequada) da inteligência artificial pela administração tributária. 2022. 40 f. Tese (Doutorado em Direito) - Faculdade de Direito, Programa de Pós-Graduação em Direito, Universidade Federal do Ceará, Fortaleza, 2022. p. 115-116 (nota de rodapé nº 240). Disponível em: http://www.repositoriobib.ufc.br/0000c3/0000c394.pdf. Acesso em: 14 mar. 2023.

[14] PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

[15] MACHADO SEGUNDO, Hugo de Brito. **Direito e Inteligência Artificial**: O que os Algoritmos têm a Ensinar sobre Interpretação, Valores e Justiça. São Paulo: Editora Foco, 2022. p. 8.

poderiam trocar mensagens, enviar e-mails ou pesquisar informações inseridas na rede por outros seres humanos".[16]

Ainda para Hugo Machado Segundo, essa difusão de tecnologias voltadas para a comunicação e troca de informações entre seres humanos proporcionou o armazenamento e o processamento de uma grande quantidade de dados – de forma ainda mais organizada – o que veio a ser denominado de *Big Data*, podendo ser explicada como "uma quantidade absurda de informações, cujo crescimento é exponencial, e que podem ser processadas e trabalhadas por computadores de uma maneira impossível aos humanos".[17] Diante dessa massiva quantidade de dados disponíveis como *inputs*, as ferramentas de IA no século XXI puderam sofrer uma verdadeira revolução, já que seus resultados (*output*) tinham agora um leque imenso de possibilidades, e com maior complexidade do que os algoritmos utilizados até os anos 1990, que sofriam de uma "pobreza do *input*", apontada por Hugo Machado Segundo como a possível causa do relativo insucesso dessas tecnologias naquele período.[18]

O primeiro e mais evidente aspecto presente no *Big Data* que o torna um fenômeno tão relevante para o desenvolvimento dos sistemas de IA certamente é o já mencionado elevado volume de dados. No entanto, outras características são intrínsecas ao *Big Data*, cujas repercussões impactam diretamente o direito fundamental à proteção de dados pessoais.

De acordo com Mayer-Schönberger e Cukier,[19] em obra intitulada "*Big Data"*, embora não haja uma definição precisa para o termo, é possível caracterizá-lo por meio de três tendências. Primeiramente, trata-se de uma quantidade imensa de dados que, estatisticamente, aproxima-se da totalidade das informações, tornando a conexão dessas informações algo inimaginável. Em segundo lugar, a grande quantidade de dados pode gerar imprecisão devido à desorganização, não havendo compromisso com o certo, mas com o resultado mais provável. Por fim, o *Big Data* permite a conversão da causalidade em correlação, o que abre possibilidades de uso prático nunca vistas anteriormente.

Essa abordagem contrasta com a concepção clássica de que o conhecimento científico deve ser baseado em causalidades, ou seja, procurar as situações que produzam determinados efeitos. Em vez disso, as decisões baseadas em estatísticas permitem a previsão de eventos futuros com base em correlações, como acontece no raciocínio que infere,

---

[16] MACHADO SEGUNDO, Hugo de Brito. **Direito e Inteligência Artificial**: O que os Algoritmos têm a Ensinar sobre Interpretação, Valores e Justiça. São Paulo: Editora Foco, 2022.
[17] Ibid.
[18] Ibid., p. 8-9.
[19] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: A revolution that will transform how we live, work, and think. Nova York: Houghton Mifflin Harcourt, 2013. p. 13-14.

estatisticamente falando, a probabilidade de ocorrência de um evento "x", quando um evento "y" for verificado.[20] A tomada de decisão com base em *Big Data* pode resultar em maior acurácia e eficiência econômica. No entanto, também deve-se considerar o efeito social disso, especialmente o risco de discriminação com base em decisões tomadas usando *Big Data*.

Em uma análise ainda mais aprofundada, Mira Burri sistematiza o *Big Data* como um fenômeno que comporta diversas outras características, que geralmente são catalogadas como "5V's"[21]: (i) volume, devido à grande quantidade de dados produzidos pela sociedade atualmente, seja em e-mails, mensagens em redes sociais, fotos, vídeos e até mesmo as curtidas em uma rede social, seja a partir de dispositivos como *smartwatches* ou *smartphones*; (ii) velocidade, considerando a rapidez na geração desses dados, mas também na sua distribuição, análise – muitas vezes, em tempo real – e, frequentemente, sem a necessidade de armazenamento local dessas informações em bases de dados; (iii) variedade, pois os dados são produzidos de diversas formas, ainda mais a partir do fenômeno da digitalização da vida, em que todos os aspectos da personalidade de um indivíduo são disponibilizados no meio digital, causando um desafio decorrente de os dados estarem desestruturados, mas com o *Big Data* seria possível estruturar todos esses dados, mesmo diante de tamanha variedade; (iv) veracidade, tendo sido aumentado o grau de confiança das análises feitas a partir desses dados, mesmo que não atingindo uma certeza quanto a determinado assunto, mas a maior probabilidade possível de se predizer um resultado; e (v) valor, a partir da habilidade humana em transformar os dados em algo com um propósito específico, ajudando organizações (públicas ou privadas) a performarem melhor.

Com o *Big Data*, os algoritmos de IA, notadamente aqueles baseados em aprendizado de máquina, conseguem robustecer seu processamento de dados, a tal ponto que podem produzir inferências sobre algum indivíduo, a partir de dados que possam não ter qualquer relação direta com aquilo. É o exemplo já citado, em que o algoritmo de seleção da empresa Amazon – que privilegiava homens em detrimento de mulheres – identificou como critério para sua decisão o local de estudo dos candidatos (que, no caso, era destinado ao público feminino), algo que aparentemente não faria sentido para uma análise curricular feita por um ser humano.

---

[20] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 44.

[21] BURRI, Mira. Understanding the implications of big data and big data analytics for competition law: an attempt for a primer. **New Developments in Competition Law and Economics**, p. 241-263, 2019. p. 2-5.

Isso reforça a dificuldade de se obter transparência das decisões algorítmicas hoje, já que com o *Big Data* e com o aprendizado de máquina as inferências podem adotar critérios jamais imaginados pelos programadores, pelas empresas que os estão utilizando e, ainda menos, pelos titulares dos dados. Diante desse cenário, o presente trabalho busca verificar exatamente quais requisitos seriam necessários para tornar responsável o uso dessa IA, diante da incerteza quanto aos riscos, especialmente à proteção de dados pessoais.

Por isso, a partir do tópico seguinte serão analisados alguns usos mais comuns da IA nas relações de trabalho, visando exatamente identificar em quais situações são mais utilizadas essas tecnologias, além de verificar como são aplicadas e quais riscos poderão gerar. Diante daquilo apresentado até então, a categoria de sistemas de IA que demandam maior atenção quanto aos riscos envolvidos aos direitos dos titulares de dados – neste caso, dos empregados – é aquela representada pelas metodologias de aprendizado de máquina (*Machine Learning*), não se devendo confundir com a mera automação de processos, a qual não implicaria, prima facie, riscos suficientes para os requisitos que serão verificados ao final do presente trabalho.

Nas relações de trabalho, algumas fases podem ser destacadas para fins didáticos, pois fazem parte da cronologia de um contrato dessa natureza (seja ele de uma relação de trabalho *lato sensu*, seja de uma relação de emprego na qual se verifica mais propriamente a subordinação do trabalhador).

Assim, antes de se firmar um contrato de trabalho, a empresa deve estabelecer um processo de recrutamento ou seleção para ocupar seus postos de trabalho. Isso ocorre por meio do uso de mecanismos para encontrar o melhor candidato dentre os disponíveis, para que a vaga disponível possa ser adequadamente preenchida. Após a contratação, o desempenho profissional daquele trabalhador é monitorado, seja para fins de remuneração – naquelas atividades que pressupõem remuneração conforme a tarefa –, seja para manutenção da qualidade do serviço, seja, ainda, para o monitoramento da execução de suas atividades. Por fim, aqueles trabalhadores que se destacam ou, de outro lado, aqueles que não apresentam um desempenho profissional adequado poderão sofrer consequências positivas – promoções ou bonificações – ou negativas, ocasiões em que o empregador deverá avaliar o grau de lesividade da conduta do trabalhador para aplicar a penalidade que mais se adeque ao caso, por vezes utilizando ferramentas tecnológicas e, até mesmo, automatizadas para essa finalidade.

2.2 Recrutamento e seleção automatizados

Na fase pré-contratual, ou seja, aquela em que ocorre a preparação para que o contrato de serviço seja efetivado, o contratante já se utiliza de diversas ferramentas tecnológicas, buscando encontrar o melhor perfil profissional para cada vaga ofertada e, assim, dentre as pessoas que se encaixem naquele perfil, atingir seu objetivo maior naquele momento (contratação de profissional), tudo isso com o menor esforço e custo possível.

Em 2018, a Comissão Global sobre o Futuro do Trabalho, vinculada à OIT, encomendou um estudo, que foi realizado por um grupo de pesquisadores liderados por Ekkehard Ernst.[22] Nesse estudo, identificou-se que a IA é utilizada pelas empresas, principalmente, para 03 finalidades: a combinação de resultados, a classificação de perfis e a otimização na gestão de processos internos. Na metodologia adotada, os autores apresentavam o cenário e ressaltavam que essas atividades eram perfeitamente aplicáveis tanto para o mercado consumidor externo (aqueles indivíduos que buscavam consumir os serviços ou produtos da empresa) quanto para os consumidores internos, aqueles empregados ou prestadores de serviços da empresa.

Nesse sentido, a combinação de resultados é aquela finalidade que mais se encaixa com o processo de recrutamento e seleção de novos trabalhadores para a empresa, já que geralmente a procura por vagas de emprego é muito maior do que a quantidade de vagas ofertadas. Assim, diante de centenas, ou milhares, de candidatos, a empresa deverá possuir ferramentas tecnológicas que garantam eficiência na combinação de resultados, encontrando o par perfeito para aquele perfil de vaga ofertado.

A necessidade de usar ferramentas baseadas em IA nos processos de recrutamento e seleção é evidenciada pela falta de eficiência em muitos processos ainda existentes no mundo empresarial, que acabam se tornando grandes gargalos para as organizações. Em estudo realizado pela PWC, uma das maiores empresas de consultoria empresarial do mundo, identificou-se que cerca de 75% das organizações contratantes não fornecem um retorno avaliativo (*feedback*) para os candidatos que não tenham passado em seus processos seletivos, enquanto 18% desses candidatos reprovados deixam de ser consumidores dessas mesmas empresas que os rejeitaram.[23]

Isso demonstra a grande necessidade de maior eficiência nessa fase pré-contratual, para que se possa, inclusive, proporcionar maior e melhor contato com as pessoas rejeitadas

---

[22] ERNST, Ekkehard et al. The economics of artificial intelligence: Implications for the future of work, **ILO Future of Work Research paper Series**; ILO, 2018.

[23] PWC. **Artificial Intelligence in HR**: a no-brainer? Disponível em: https://www.pwc.nl/nl/assets/documents/artificial-intelligence-in-hr-a-no-brainer.pdf. Acesso: 10 out. 2022.

nos processos seletivos. Além dessa necessidade, essa fase preliminar apresenta uma peculiar vantagem para o uso dessas tecnologias baseadas em IA, que é a grande quantidade de dados envolvida. Como ressalta Michel Servoz,[24] em estudo encomendado pela Comissão Europeia em 2019, para que uma IA baseada em *Machine Learning* possa ter realmente alguma contribuição, ela precisa de uma grande quantidade de dados disponível, já que é a partir desse *Big Data* que ela poderá aprimorar seus usos de maneira própria, sem a necessidade de intervenção humana.

A fase de recrutamento pode ser considerada como aquela em que a empresa mais obtém informações externas que ela não vai utilizar em momento posterior. Afinal, quando centenas de inscritos em processo seletivo enviam seus currículos (às vezes até mesmo por vídeos de apresentação), preenchem formulários com informações profissionais e pessoais, participam de entrevistas, relatando mesmo rotinas diárias ou aspectos familiares, a empresa poderá contratar apenas alguns poucos candidatos, deixando as informações dos demais sem qualquer uso futuro, nem mesmo para lhes passar um retorno quanto ao motivo pela não contratação, como visto supra. Por essa grande quantidade de dados, existe tanta proliferação de ferramentas de IA aplicadas nesse momento pré-contratual.

No entanto, as coisas nem sempre foram assim. Ao apresentarem o cenário histórico, Stewart Black e Patrick Van Esch[25] demonstram que com o início do século XX até a década de 1980, o que mais gerava valor às empresas eram aqueles ativos tangíveis, ou seja, a estrutura empresarial, os bens produzidos, as máquinas necessárias para produção e propriedade empresarial. A partir do início do século XXI, esse estado de coisas mudou, já que os ativos intangíveis (recursos humanos, propriedade intelectual etc.) passaram a valer muito mais para as empresas do que os ativos tangíveis, tanto que as empresas mais valiosas do mundo hoje são aquelas que não possuem grandes máquinas, mas propriedade intelectual sobre tecnologias e grandes bases de dados estruturadas. Por esse motivo, as técnicas de seleção de pessoas mais qualificadas passaram de práticas importantes para objetivos estratégicos de CEOs das empresas, tendo a seleção de novos empregados recebido o status de decisão estratégica para o negócio.

---

[24] SERVOZ, Michel. The Future of Work? Work of the Future! **European Commission**, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/future-work-work-future. Acesso em: 18 mar. 2023.

[25] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020.

Outro estudo, este encomendado pelo Parlamento Europeu em 2022,[26] analisa amplamente a difusão dessas novas tecnologias baseadas em IA nas relações de trabalho, sendo que na fase de recrutamento são apresentadas 04 principais usos que possuem implicações jurídicas, sendo eles: (i) o direcionamento das vagas que serão apresentadas para cada pessoa ou grupo de pessoas em redes sociais profissionais; (ii) a filtragem de currículos antes mesmo do início do processo seletivo; (iii) a seleção por ferramentas com base em características pessoais; e (iv) a realização de entrevistas com candidatos por meio de ferramentas baseadas em IA.

O uso da IA na fase pré-contratual trabalhista pode ser sistematicamente dividido em 04 (quatro) principais finalidades, sendo elas (i) a oferta das vagas aos candidatos, (ii) a triagem dos candidatos por seus currículos ou aplicações, (iii) a avaliação dos candidatos pós análise curricular e (iv) a facilitação de etapas do processo seletivo[27].

Quanto ao primeiro uso, a oferta de vagas aos candidatos, é bastante comum nos dias de hoje que as empresas procedam com o direcionamento das vagas que serão visualizadas apenas por determinados grupos de pessoas, tratando-se de uma prática que é tecnicamente possível pela tendência cada vez maior de perfilização (*profilling*), pela qual a empresa consegue mapear perfis de pessoas, a partir de uma base de dados da qual dispõe, e alimenta os algoritmos de IA, os quais poderão aplicar o *Machine Learning* e definir quais pessoas mais se enquadram nos perfis propostos.

Black e Van Esch explicam que esse uso da IA ocorre também por meio da mineração dos dados que estão disponíveis em redes sociais (tais como LinkedIn, Facebook, Instagram, Twitter, Pinterest), processo tornado possível pelas ferramentas baseadas em IA que conseguem encontrar os perfis ideais de candidatos com base em análises estatísticas de dados já publicamente disponíveis. Empresas como Pandologic, Talenya e Hirescore divulgam suas ferramentas baseadas em IA com capacidade para realizar essas análises, sem as quais o direcionamento das vagas não seria possível.[28]

Além de direcionar o conteúdo das vagas a determinados grupos, até mesmo o meio mais efetivo para determinado grupo de pessoas é identificado pela IA. Por exemplo, se para determinado público o ideal é um anúncio predominantemente por escrito em um e-mail, mas

---

[26] DE STEFANO, Valerio; WOUTERS, Mathias. AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (European Parliament, 2022). **Commissioned Reports, Studies and Public Policy Documents**. Paper 219, 2022.

[27] Adota-se a mesma divisão proposta em BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020.

[28] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020, p. 219.

para outro público um anúncio via imagens em redes sociais seria mais efetivo. Assim, as empresas conseguem buscar seu público exatamente com o conteúdo e a forma mais adequados, servindo para afunilar os candidatos para somente aqueles buscados, bem como para promover políticas sociais.

Esse tipo de aplicação de ferramentas de IA – para direcionamento de resultados a determinados grupos de pessoas – permite que sejam realizadas políticas afirmativas, para que as vagas sejam mais divulgadas entre públicos mais marginalizados ou que tenham menor representatividade naquela empresa,[29] por exemplo mulheres, negros, povos originários, pessoas trans, dentre diversos outros usos benéficos dessa tecnologia.

Um exemplo apresentado por Black e Van Esch é da empresa Textio, que oferece serviços de adequação de textos e formatos de anúncios de vagas, com a finalidade de reduzir vieses discriminatórios ou inadequados. No site da empresa, são apresentados alguns exemplos, sendo o principal deles quando a plataforma analisa um texto de vaga e sugere a substituição da expressão *driven by* pela expressão *inspired by*, pois esta tenderia a ressoar melhor com mulheres. Dessa maneira, o que a plataforma realiza uma adaptação de textos, por meio de sugestões probabilísticas obtidas por IA, para determinados públicos esperados naquela vaga.

Figura 1 – Divulgação de funcionalidades da IA da empresa Textio

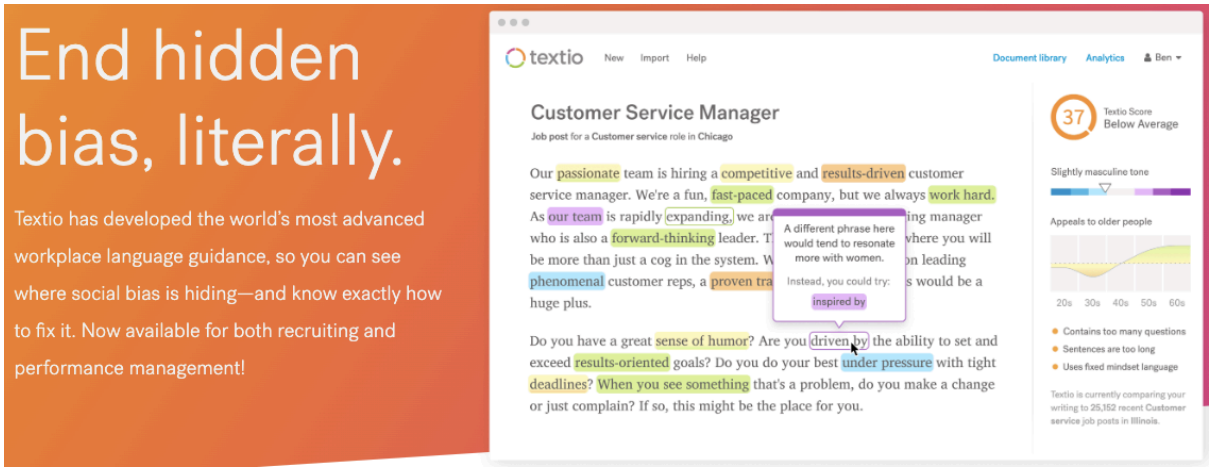

Imagem retirada do site da empresa Textio, demonstrando como a plataforma sugere ao recrutador a mudança da linguagem conforme o público que pretende atingir.[30]

[29] Black e Van Esch apresentam diversos casos de sucesso, em que organizações aplicaram ferramentas baseadas em IA para reduzir vieses discriminatórios nos textos de suas ofertas de vagas, bem como aumentar a diversidade de participantes e contratados por essas empresas, cf. BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020.
[30] TEXTIO. End hidden bias, literally. Disponível em: https://textio.com/. Acesso 30 mar. 2023.

De acordo com Black e Van Esch[31], empresas como Johnson & Johnson e L'Oréal já tiveram sucesso em reduzir vieses discriminatórios e aumentar a participação de mulheres em seus processos seletivos, notadamente para cargos mais elevados. A primeira atingiu um aumento de 15% mais mulheres interessadas por suas vagas, enquanto a segunda conseguiu até mesmo igualar a quantidade de homens e mulheres participando de seus processos seletivos, utilizando a ferramenta Textio para direcionar o conteúdo de maneira mais assertiva.

Outro exemplo citado pelos autores é da empresa Unilever, que contratou a ferramenta baseada em IA da empresa Pymetrics para direcionar suas vagas de estágio estratégico não a um grupo específico de candidatos, mas, sim, para ampliar a participação de outras universidades que não eram tão bem representadas em seus processos seletivos. Assim, a Unilever conseguiu duas vezes mais candidatos do que em seleções anteriores, aumentando também a diversidade racial, socioeconômica e com relação às universidades às quais esses candidatos estavam vinculados, passando de 800 universidades para 2.600 universidades alcançadas por seu processo seletivo.[32]

Não se pode esquecer, no entanto, que a possibilidade de direcionar anúncios de vagas para determinados grupos poderia, ao revés, privilegiar pessoas e grupos que já são super-representados, aprofundando ainda mais cenários de discriminação e acesso ao trabalho. Os riscos dessas tecnologias serão mais bem abordados na seção seguinte, já que no momento será privilegiado apresentar os diversos usos concretos dessas tecnologias nas relações de trabalho.

A IA pode ser utilizada não apenas no direcionamento de vagas a grupos de pessoas conforme seu comportamento social, mas também relativamente à sua busca por emprego. Segundo Black e Van Esch, a empresa L'Oréal contratou ferramenta baseada em IA para buscar não só candidatos ativos no mercado, ou seja, aqueles que estivessem efetivamente à procura empregos, mas também os candidatos passivos, que não necessariamente estão em busca de recolocação imediata. A medida possibilitou a participação de 2 milhões de candidatos para cerca de 5 mil vagas, representando 400 candidatos por vaga.[33]

Não apenas as empresas com ferramentas próprias baseadas em IA estão sendo eficazes no recrutamento de candidatos, sobretudo no que diz respeito à fase de anúncio de vagas. As próprias redes sociais profissionais estão buscando formas de facilitar as

---

[31] BLACK, J. Stewart; VAN ESCH, Patrick. *Op. Cit.*, p. 219.
[32] FELONI, Richard. Consumer-goods giant Unilever has been hiring employees using brain games and artificial intelligence — and it's a huge success. **Insider**, 28 jun. 2017. Disponível em: https://www.businessinsider.com/unilever-artificial-intelligence-hiring-process-2017-6. Acesso em: 02 abr. 2023.
[33] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020. p. 219.

contratações, como forma de agregar valor a seus usuários (aqueles em busca de contratação ou com vagas em aberto e querendo preenchê-las). Por exemplo, o LinkedIn, rede social profissional mais difundida na atualidade, apresenta sua funcionalidade "Carreiras" como sendo um auxiliar para seus clientes recrutadores e para candidatos a vagas. Segundo a própria empresa:

> Quando você anuncia uma vaga, usamos os dados e insights do LinkedIn para combinar seus critérios com as competências, experiência e objetivos de um usuário. A segmentação personalizada exibe sua vaga a profissionais relevantes para facilitar as candidaturas.[34]

Ao explicar como funciona a seleção dos perfis de candidatos, a rede social informa que, ao selecionar um candidato pelo qual teria interesse em entrevistar, o recrutador receberá indicações de perfis de pessoas semelhantes:

> Conforme você recebe as candidaturas, você poderá visualizá-las e organizá-las em um só lugar. Filtre, classifique e avalie os candidatos para concentrar seus esforços e interagir apenas com os melhores. **Quando você classifica um perfil como qualificado, o LinkedIn entende o que você está buscando e recomenda sua vaga a pessoas semelhantes** (grifou-se).[35]

No entanto, não apresenta maiores detalhes sobre como esses perfis são construídos, quais dados utilizam, quais inferências produzem, quais critérios são empregados para classificar as pessoas, nem mesmo se utilizam tecnologias baseadas em IA para chegar a essas conclusões.

Ao consultar a Política de Privacidade do LinkedIn, a empresa informa que utiliza "sistemas automáticos" para fornecer conteúdo e recomendações aos usuários, não explicando quais seriam esses sistemas automáticos (se seriam simples automações ou se utilizariam metodologias mais profundas de aprendizado de máquina), nem de que forma eles ajudam efetivamente os usuários a receberem indicações precisas de serviços da rede social:

> Usaremos seus dados para recomendar vagas ou pessoas que possam se beneficiar da sua orientação profissional, além de mostrar para você e para terceiros contatos profissionais relevantes (ex., quem trabalha em uma empresa, setor, função, localidade ou que tem determinadas competências e conexões). Você pode indicar o seu interesse em mudar de emprego e compartilhar informações com recrutadores. Podemos usar os dados do seu perfil e atividades para recomendar vagas e recomendar você para os recrutadores. **Podemos utilizar sistemas automáticos para fornecer**

[34] LINKEDIN. Talent Solutions. Disponível em: https://business.linkedin.com/pt-br/talent-solutions/post-jobs. Acesso em: 18 mar. 2023.
[35] Ibid.

> **conteúdo e recomendações para ajudar a tornar os nossos Serviços mais relevantes para nossos Usuários, Visitantes e clientes**. Manter seu perfil atualizado e correto pode ajudar você a se conectar melhor com outras pessoas e com oportunidades através dos nossos Serviços. (grifou-se)[36]

Para além da busca por candidatos, personalizando anúncios de vagas a eles, a IA pode ser útil – ainda na fase de divulgação da vaga – para reaproveitar candidatos passados e verificar se eles se enquadram ou não nas novas vagas ofertadas pelas empresas. É o exemplo da empresa Engage Talent, que busca exatamente reavaliar os candidatos passados para que a empresa contratante dessa ferramenta possa reutilizá-los em seus demais processos seletivos ou não.[37]

O segundo tipo de uso da IA na fase de recrutamento e seleção é para triagem de currículos. Nessa fase, as empresas buscam mais do que tudo reduzir o tempo despendido na análise curricular. Principalmente em mercados mais concorridos e com maior rotatividade, a agilidade em responder aos candidatos pode ser crucial para garantir sua adesão ao processo seletivo e, posteriormente, à sua contratação por aquela empresa.

Existem algumas ferramentas baseadas em IA que apresentam soluções bastante revolucionárias para as empresas. A empresa Ideal oferece uma ferramenta baseada em IA que, segundo ela, já encurtou o tempo de análise curricular de um de seus clientes de 25 dias para apenas 10 dias, garantindo uma redução de 60% de tempo.[38] Outros exemplos que podem ser citados são da rede de hotéis e resorts Hilton, que abreviou o tempo de análise curricular de 42 dias para apenas 5 dias com a implementou de uma ferramenta baseada em IA, o que representa uma redução de 88% do tempo.[39] Há, ainda, o caso da empresa L'Oreal, que também usou ferramenta baseada em IA para reduzir o tempo de análise de um currículo de 40 minutos para apenas 4 minutos, alcançando 90% de redução no tempo despendido.[40]

A velocidade pela qual os algoritmos realizam análises curriculares e triagem de candidatos, antes mesmo de suas entrevistas, pode trazer certo assombro aos recrutadores, já

---

[36] LINKEDIN. Política de Privacidade. Disponível em: https://br.linkedin.com/legal/privacy-policy?trk=d_checkpoint_lg_consumerLogin_cap_ft_privacy_policy#use. Acesso em: 17 mar. 2023.
[37] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020. p. 220.
[38] IDEAL. S&P Data Increased Retention By 20%. Disponível em: https://ideal.com/customer/sp-data/. Acesso em: 02 abr. 2023.
[39] MCLAREN, Samantha. How Hilton, Google, and More Have Dramatically Reduced Their Time to Hire. **Linkedin**, 24 maio 2018. Disponível em: https://www.linkedin.com/business/talent/blog/talent-strategy/how-these-companies-reduced-time-to-hire. Acesso em: 02 abr. 2023.
[40] SHARMA, Anushree. How AI reinvented hiring practice at L'Oréal. **People Matters**, 16 ago. 2018. Disponível em: https://www.peoplematters.in/article/technology/how-the-worlds-largest-cosmetic-company-transformed-its-hiring-practice-with-ai-19006. Acesso 02 abr. 2023.

que até mesmo a qualidade das análises curriculares pelas máquinas aparenta ser superior quando comparadas aos humanos. Esse argumento é apresentado nos estudos de Nathan Kuncel e colaboradores, que apontam que uma simples automação pode alcançar um desempenho até 25% melhor na análise curricular do que recrutadores humanos.[41]

Afinal, como apontam Black e Van Esch, os algoritmos de IA passaram de uma atividade meramente de análise de palavras-chave para produção de inferências quanto aos candidatos, até mesmo a partir do uso da linguagem por eles em seus currículos, permitindo inferir se serão mais persistentes ou não apenas com base nessa informação.[42]

O terceiro tipo de aplicação da IA no recrutamento é quando esses sistemas são utilizados como ferramentas de avaliação de candidatos, por exemplo na realização de entrevistas. Em muitas dessas situações, o uso da IA acontece quando são aplicadas ferramentas "gamificadas" de entrevista com candidatos, ou seja, por meio da aplicação de jogos os candidatos serão avaliados. Por exemplo, a empresa Unilever contratou a ferramenta baseada em IA da empresa Pymetrics para aplicar cerca de 12 jogos (com base na neurociência) com seus candidatos a vagas de emprego, com duração de 20min cada. Um desses jogos buscava identificar se o candidato teria a capacidade de assumir riscos, funcionando da seguinte maneira:

> Um dos jogos mediu a tomada de riscos. Candidatos tinham 3 minutos para coletar tanto dinheiro quanto eles poderiam clicar em 'bombear' para inflar um balão com ar e dinheiro. Cada clique adicionava 5 centavos. A qualquer momento, o candidato poderia optar por coletar dinheiro para adicionar o valor ao seu total e começar com um novo balão. No entanto, se o candidato esperou demais e o balão estourou, o candidato não arrecadava dinheiro com esse balão. Os candidatos podiam arrecadar dinheiro tão rápido clicando cedo e com frequência ou esperando desde que não esperem muito. O ponto do jogo não era realmente sobre a quantidade de dinheiro coletado, mas identificar a propensão de risco do indivíduo.[43] (tradução livre).

Como resultado, a ferramenta identificava que aqueles candidatos que assumiam risco de forma moderada ou moderadamente alta teriam maior probabilidade de melhor desempenhar suas funções, enquanto aqueles com menor capacidade de assumir riscos ou capacidade muito alta de assumir riscos não estariam de acordo com os padrões da empresa.

---

[41] KUNCEL, Nathan R. et al. Mechanical versus clinical data combination in selection and admissions decisions: a meta-analysis. **Journal of applied psychology**, v. 98, n. 6, p. 1060, 2013.

[42] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020. p. 220.

[43] FELONI, Richard. Consumer-goods giant Unilever has been hiring employees using brain games and artificial intelligence — and it's a huge success. **Insider**, 28 jun. 2017. Disponível em: https://www.businessinsider.com/unilever-artificial-intelligence-hiring-process-2017-6. Acesso em: 02 abr. 2023.

Em uma etapa posterior do processo seletivo da Unilever, os candidatos seriam convidados a participar de entrevistas, as quais ocorreriam por meio eletrônico, gravadas e, posteriormente, analisadas por ferramentas baseadas em IA. Assim, as imagens captadas pelas câmeras (de celular ou de computador) revelariam à IA aspectos como palavras-chave utilizadas, linguagem corporal, reações micro faciais e o tom de voz do candidato. Essas informações seriam utilizadas como fonte para que a IA designasse inferências sobre o indivíduo, as quais seriam confrontadas com as características dos melhores empregados da Unilever, resultando em combinações positivas (candidatos seriam encaminhados para a próxima fase) ou negativas (candidatos teriam sua nota rebaixada, permanecendo ou não nas etapas seguintes).[44]

Outra empresa que adotou uma estratégia parecida foi a L'Oréal, que contratou a ferramenta baseada em IA da empresa Mya Systems para analisar os candidatos que passaram da fase de triagem curricular (cerca de 10% do total de candidatos do processo seletivo). Essa ferramenta era um *chatbot* que fazia perguntas aos candidatos e analisava suas respostas. Os dados obtidos eram, então, comparados às respostas obtidas dos melhores empregados da L'Oréal, tomando como base os seguintes critérios: o conteúdo das respostas e a estrutura das sentenças e o vocabulário utilizados. Em seguida, foi criada uma nota para cada candidato, e aqueles que atingiram uma nota satisfatória foram selecionados para a próxima etapa: uma entrevista com um recrutador humano.[45]

Por fim, a última finalidade do uso da IA no recrutamento e seleção de novos empregados, analisada neste trabalho, é facilitar o processo seletivo e oferecer uma experiência agradável ao candidato, assemelhando-se à experiência de um consumidor. Isso ocorre em razão de as empresas enxergarem a necessidade de garantir, cada vez mais, uma experiência satisfatória aos candidatos a emprego. Alguns elementos favorecem isso, como a possibilidade de que o candidato possa se concorrer em outras seleções, como a possibilidade de ele comentar sobre suas impressões para família e amigos e, também, a necessidade de que os candidatos que forem aprovados precisarem ter tido uma experiência satisfatória, ao ponto de que, ao final, aceitem a contratação.

Primeiramente, a IA já é utilizada para facilitar a participação de candidatos em processos seletivos, pois não é mais exigido o envio de um currículo em formato específico. As ferramentas de IA conseguem minerar os dados presentes nas redes sociais dos candidatos, que

---

[44] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020. p. 221.
[45] Ibid.

muitas vezes só precisam informar suas redes sociais para que elas se tornem a base inicial de triagem pela empresa recrutadora.[46]

O segundo uso é quando os *chatbots* são utilizados para facilitar a participação do candidato no processo seletivo, especialmente: (i) ao fazerem a atualização das fases do processo seletivo e respondendo as dúvidas do candidato sobre as etapas que virão; (ii) ao proporem perguntas para os candidatos poderem completar as informações ausentes em seus currículos ou redes sociais; e (iii) ao responderem as perguntas dos candidatos sobre as características da empresa ou da vaga buscada, de maneira ininterrupta, todos os dias do ano.[47]

2.3 Gestão algorítmica do trabalho

A seleção de um candidato para o preenchimento da vaga de emprego não o torna livre da influência de sistemas baseados em IA no seu ambiente de trabalho. Em realidade, diante de uma relação de emprego, o patrão alicerça-se no seu legítimo poder de controle, decorrente da livre iniciativa e do poder empregatício, para adotar diversas ferramentas de vigilância e comando do trabalho humano.

Cada vez mais os empregadores, principalmente ligados à indústria, à logística e às cadeias de suprimentos, lançam mão do uso de dispositivos vestíveis (*wearables*). Esses dispositivos são ligados diretamente ao corpo do trabalhador, coletando dados (inclusive dados pessoais sensíveis, ligados à saúde) de maneira constante, permitindo que o empregador consiga identificar alguns indicadores sobre o desempenho profissional.

Dispositivos como relógios inteligentes (*smartwatches*) ou pulseiras que captam informações sobre atividades físicas desempenhadas pelos usuários, além de vários outros tipos, são utilizados pelo empregador, o qual apresenta essas ferramentas como uma vantagem ao empregado, já que este poderá livremente medir seus próprios batimentos cardíacos, a quantidade de passos durante o dia, bem como ter estimulada a prática de exercícios físicos, já que esse instrumental possui a função primordial de estímulo a atividades físicas e hábitos saudáveis.[48] Para além das vantagens quanto ao estilo de vida saudável, empregadores apresentam diversos outros benefícios para a utilização desses dispositivos vestíveis, como

---

[46] Ibid.
[47] BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020. p. 221-222.
[48] MANOKHA, Ivan. Why the rise of wearable tech to monitor employees is worrying. **Independent**, 04 jan. 2017. Disponível em: https://www.independent.co.uk/tech/why-the-rise-of-wearable-tech-to-monitor-employees-is-worrying-a7508656.html. Acesso em: 04 abr. 2023.

alertar ao trabalhador quando ele esteja desempenhando alguma atividade perigosa, monitorar os momentos em que ele esteja trabalhando com má postura corporal[49], além de acompanhar a fadiga de determinado empregado que trabalha, por exemplo, por longas horas na direção (caminhoneiros, motoristas de ônibus, dentre outros)[50].

Para além das vantagens ergonômicas e relacionadas à saúde dos trabalhadores, seu uso é também observado para que o desempenho profissional dos trabalhadores de determinada empresa possa ser fiscalizado, não apenas quanto ao resultado entregue, mas também sobre como o trabalho está sendo realizado e como o corpo do empregado está reagindo às atividades propostas a ele. Valerio De Stefano[51] elenca três principais formas de controle do desempenho profissional através desses dispositivos vestíveis, sendo eles: (i) o registro de movimentos e a localização dos empregados, pois assim o empregador poderá monitorar seu ritmo de trabalho e verificar em quais momentos o empregado realizou pausas; (ii) o monitoramento do desempenho físico dos empregados durante determinadas atividades que demandem mais esforço, assim o empregador conseguirá avaliar a produtividade e a capacidade física dos seus trabalhadores para determinadas tarefas; e (iii) apresentação de alertas aos empregados, para que possam deixar de realizar determinada atividade e passar para outra, dentro de uma cadeia de etapas que ele deverá seguir, impondo, assim, o tempo dentro do qual cada atividade pode ser executada.

Além dos dispositivos vestíveis, diversas empresas utilizam ferramentas de comunicação interna ou externa como forma de monitoramento do desempenho profissional.

---

[49] O dispositivo desenvolvido pela empresa UpRight Go é colado às costas do trabalhador e propõe-se a monitorar a postura corporal, provendo respostas (feedback) quando houver uma postura inadequada, para que o próprio trabalhador a corrija. ALLISON, Conor. The Upright Go aims to solve your back pain and screen slouch. **Wareable**, 31 jan. 2017. Disponível em: https://www.wareable.com/wearable-tech/upright-go-release-date-price-specs-3850. Acesso em: 04 abr. 2023.

[50] O SmartCap representa um paradigma emergente de vestimenta inteligente que vem sendo introduzido ao ambiente laboral, apesar de ainda não estar plenamente inserido em escritórios convencionais. Em sua versão atual, o SmartCap se apresenta como uma opção de uso na forma de bonés de beisebol, gorros ou faixas para a cabeça e se destina, em particular, aos operadores de veículos pesados. Seu objetivo primordial é o monitoramento da fadiga por meio do emprego de tecnologia de eletroencefalografia (EEG). PLUMMER, Libby. Wearables in the workplace: The tech taking over your office in 2017. **Wareable**, 21 fev. 2017. Disponível em: https://www.wareable.com/wearable-tech/wearables-in-the-workplace-office-235. Acesso em: 04 abr. 2023.

[51] DE STEFANO, Valerio. 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Artificial Intelligence and Labour Protection (May 16, 2018). **Comparative Labor Law & Policy Journal**, v. 41, n. 1, 2019. p. 10.

Sistemas como o Slack[52] ou o Microsoft Teams,[53] cujas funcionalidades permitem que determinada empresa possa gerenciar sua equipe, por meio de interações virtuais, por *chat*, por reuniões à distância, ou por e-mail, em algumas situações são utilizadas por empregadores também para monitorar o desempenho profissional de seus empregados. A ferramenta "*My Analytics*", da Microsoft, utiliza sistemas de IA que rastreiam o uso das demais ferramentas oferecidas pela empresa (Teams, Outlook, Skype, OneDrive) para identificar se o trabalho está sendo realizado de forma adequada ou se necessita de maior produtividade.[54] Algumas das métricas que são analisadas podem incluir o tráfego de e-mails diários enviados ou recebidos, o tempo de resposta a eles e o tempo dedicado a reuniões, tudo isso com o objetivo de otimizar as rotinas profissionais dos empregador.[55]

As redes sociais profissionais também são mecanismos que auxiliam o empregador a verificar se as atividades desempenhadas por seus empregados estão sendo realizadas e devidamente divulgadas, a fim gerar mais engajamento para a empresa e, assim, fortalecer sua marca. Um exemplo emblemático foi citado por Cathy O'Neil,[56] envolvendo a empresa americana Cataphora que, em 2008, comercializou um software que classificava empregados de acordo com uma série de métricas, dentre as quais sua geração de ideias. Na prática, o software acessava os e-mails e as mensagens corporativas dos empregados, classificando-os de acordo com sua capacidade de criar ideias ou de conectá-las.

Esses tipos de controle do desempenho profissional por meio de equipamentos vestíveis, ferramentas de comunicação e redes sociais profissionais podem ser categorizadas como fontes de dados para o *Big Data* no local de trabalho. Antes da difusão do *Big Data*, o empregador apenas tinha como fonte de dados de seus empregados aquelas informações coletadas no local de trabalho fisicamente (por exemplo, câmeras de vigilância, observações de fiscais ou gerentes, relatos de clientes ou de terceiros). Nas últimas décadas, entretanto, o

---

[52] "O Slack oferece uma nova forma de comunicação para a sua empresa. Ele substitui os e-mails por algo mais rápido, mais organizado e mais seguro. Em vez de conversas independentes por e-mail, toda a comunicação é organizada em canais, que são fáceis de criar, participar e pesquisar. Quando há um canal para cada detalhe da empresa, todos sabem exatamente onde consultar para fazer o trabalho." SLACK. Aqui acontece. Disponível em: https://slack.com/intl/pt-br/solutions. Acesso em: 04 abr. 2023.

[53] MICROSOFT. Microsoft Teams. Disponível em: https://www.microsoft.com/pt-br/microsoft-teams/teams-for-work. Acesso em: 04 abr. 2023.

[54] MICROSOFT. O MyAnalytics, o controlador de eficiência no trabalho, agora está mais amplamente disponível. **Microsoft**, 02 jan. 2019. Disponível em: https://www.microsoft.com/pt-br/microsoft-365/blog/2019/01/02/myanalytics-the-fitness-tracker-for-work-is-now-more-broadly-available/. Acesso em: 04 abr. 2023.

[55] DE STEFANO, Valerio; WOUTERS, Mathias. AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (European Parliament, 2022). **Commissioned Reports, Studies and Public Policy Documents**. Paper 219, 2022. p. 15.

[56] O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016. p. 132-133.

empregador passou a contar com diversos instrumentos de coleta de dados do empregado, incluindo ferramentas que originalmente não tinham esse objetivo, mas que acabam sendo utilizadas para fiscalização e gestão do trabalho. Diante dessas e inúmeras outras fontes de informações, o empregador consegue unificar uma base de dados sobre seus empregados, de modo que utilize ferramentas de IA para análise dessas informações e, assim, possa tomar decisões sobre cada um deles, predizer comportamentos prováveis de acontecer ou prescrever quais atitudes deveriam ser desempenhadas por suas equipes de trabalhadores.

Esse fenômeno gerou grandes oportunidades de mercado para consultorias e analistas de dados, que puderam oferecer metodologias que eram originalmente aplicadas para análise de dados de consumidores e clientes e passaram a utilizá-las para o ambiente interno da empresa, formando uma disciplina denominada *HR Analytics* ou *People Analytics*. Trata-se de uma metodologia de trabalho que alia estatística, análise de dados, Inteligência Artificial e relações trabalhistas, tendo como objetivo retirar observações e lições a partir dos dados disponíveis e, possivelmente, predizer o que pode acontecer ou prescrever o que acontecerá com maior probabilidade no ambiente dos recursos humanos empresariais.[57]

Com isso, diversas empresas passaram a focar em adotar ferramentas estatísticas e de análise de dados de seus empregados, buscando atingir maior eficiência de suas tarefas, bem como entender as melhores métricas de desempenho profissional. No entanto, distintamente de outras áreas das empresas (como a área financeira ou a área comercial), a área de recursos humanos não apresentou tanta proeminência quanto ao conhecimento aplicado dessas tendências, provavelmente em razão da falta de treinamento dos gestores de RH quanto a essas temáticas, o que gerou um movimento muito grande de terceirização, culminando com a contratação de softwares e ferramentas de terceiros para realização dessas análises de dados.[58] Com a crescente geração e análise de grandes volumes dados, essas ferramentas são equipadas com algoritmos de inteligência artificial, que operam com base nas informações coletadas a partir dessas diversas fontes de dados.

Exemplos não faltam de aplicações de ferramentas de IA para o controle do desempenho profissional nas empresas. Um dos casos de destaque é o da IA pertencente à IBM, empresa que dispõe de um supercomputador denominado “Watson”, famosa também pelas suas tecnologias baseadas em IA. Nesse caso em particular, foi lançada no mercado uma ferramenta

---

[57] DE STEFANO, Valerio; WOUTERS, Mathias. AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (European Parliament, 2022). **Commissioned Reports, Studies and Public Policy Documents**. Paper 219, 2022. p. 13.

[58] CAPPELLI, Peter; TAVIS, Anna. HR Goes Agile. **Harvard Business Review**, mar./abr. 2018. p. 52.

de IA chamada "programa de predição de atrito" (*predictive attrition program*), criada com base no supercomputador Watson, capaz de prever com até 95% de precisão quando os empregados estariam mais propensos a pedir demissão em uma empresa nos próximos seis meses. Essas previsões são formuladas com base em reações e comportamentos identificados a partir de um padrão previamente definido. Então, se o empregado sai do seu padrão, demonstrando comportamentos que frequentemente são associados a pedidos de demissão, é indicado a ele que participe de cursos e treinamentos estimulantes e propondo a ele mudanças de comportamento laboral.[59] Apesar de bastante atrativa, segundo a própria empresa a tecnologia analisa critérios que não foram apresentados publicamente, já que ela se recusa a fornecer o "tempero secreto" de sua tecnologia.[60]

Outra ferramenta de IA aplicada na gestão do desempenho laboral foi desenvolvida pela empresa Percalota, que se propõe a promover maior eficiência na gestão de escalas de trabalho, principalmente coletando dados de vendas e de resultados individuais ou em grupos de vendedores. Primeiro, a ferramenta promete determinar com qual colega de trabalho o indivíduo mais se identificaria, tarefa realizada tomando por base os dados sensoriais e informações sobre as vendas desses empregados quando em dupla com uma ou outra pessoa.[61] Além disso, com base nas mesmas informações coletadas, a ferramenta da Percolata estima as pontuações de produtividade de vendas de cada empregado e as usa para criar cronogramas de trabalho.[62]

Não apenas o trabalho na indústria ou no varejo têm campo fértil para a aplicação de ferramentas baseadas em IA, mas também o trabalho remoto. Durante e após o período de pandemia pela Covid-19, este tornou-se muito mais comum e aplicado em diversos setores da economia. Alexandra Mateescu[63] analisa o uso de sistemas denominados *Electronic Visit Verification* na gestão e fiscalização do trabalho de cuidadores em formato *home care*, que atendem seus pacientes nas próprias residências destes. Segundo a pesquisa realizada com cerca de vinte trabalhadores nessa modalidade, percebeu-se que esses sistemas, instalados nos seus

---

[59] SCHRAGE, Michael et al. Performance management's digital shift. **MIT Sloan Management Review**, 2019. p. 3-5.
[60] ROSENBAUM, Eric. CNBC WORK IBM artificial intelligence can predict with 95% accuracy which workers are about to quit their jobs. **CNBC**, 03 abr. 2019. Disponível em: https://www.cnbc.com/2019/04/03/ibm-ai-can-predict-with-95-percent-accuracy-which-employees-will-quit.html. Acesso em: 07 abr. 2023.
[61] DE STEFANO, Valerio; WOUTERS, Mathias. AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (European Parliament, 2022). **Commissioned Reports, Studies and Public Policy Documents**. Paper 219, 2022. p. 15.
[62] BERNHARDT, Annette; SULEIMAN, Reem; KRESGE, Lisa. **Data and algorithms at work**: the case for worker technology rights. 2021. p. 9.
[63] MATEESCU, Alexandra. Electronic Visit Verification: the weight of surveillance and the fracturing of care. **Data & Society Research Institute**, 2021.

smartphones, exigiam que constantemente fossem registradas fotografias do empregado e de seus pacientes para confirmar que esses trabalhadores estariam mesmo onde diziam estar.

Além disso, no trabalho realizado em casa, popularmente denominado *home office*, igualmente fortalecido após o período pandêmico, ao ter o empregado trabalhando fora de sua visão, passou-se a adotar nas empresas a utilização de mecanismos de fiscalização do trabalho, notadamente por meio de tecnologias – e, inclusive – baseadas em IA.

Ainda em 2021, surgiram relatos de que a Teleperformance, uma grande empresa colombiana de atendimento telefônico que presta serviços para importantes empresas de tecnologia, como Apple, Amazon e Uber, teria solicitado que seus funcionários em trabalho remoto concordassem com a instalação de câmeras em seus computadores. De acordo com as informações, essas câmeras estariam vinculadas a um sistema de inteligência artificial que identificaria possíveis violações às normas internas de troca de turno, tirando uma fotografia dessas infrações e enviando automaticamente para a empresa investigar.[64] Outros casos de uso da IA para monitoramento e direção de atividades laborais são apresentados por Antonio Aloisi e Valerio De Stefano,[65] com maior detalhamento e refletindo sobre seus riscos, demonstrando de que maneiras essas tecnologias se apresentam de forma intensificada na relação de emprego.

A empresa Amazon, já referida em outros trechos, está situada na vanguarda dos avanços tecnológicos quando o assunto é controle e gestão de pessoas. Tanto no processo de recrutamento de novos empregados quanto no controle das atividades desempenhadas pelas equipes, essa empresa adota ferramentas baseadas em IA, tanto que passou a ser denominada em um estudo realizado pela *Uni Global Union* (federação sindical mundial) como um panóptico, fazendo referência à ferramenta de vigilância idealizada por Jeremy Bentham, que permitiria um fiscal ao centro ter uma visão geral de todas as salas de um prédio, que hoje representa um símbolo da falta de privacidade.

Nesse estudo, foram apontadas diversas práticas violadoras da privacidade e dos direitos humanos dos trabalhadores na Amazon, dentre eles o uso de câmeras de vigilância e escâneres corporais que contavam com sistemas baseados em IA com tecnologia de

---

[64] SOLON, Olivia. Big Tech call center workers face pressure to accept home surveillance. **NBC News**, 08 ago. 2021. Disponível em: https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227. Acesso em: 01 set. 2021.

[65] DE STEFANO, Valerio, 'The EU Proposed Regulation on AI: a threat to labour protection?', **Regulating for Globalization**, 2021.

reconhecimento de padrões de comportamento, para continuamente vigiar os empregados e evitar que houvesse aproximação de mais de 2m entre eles nos depósitos.[66]

Além desse controle espacial, os empregados nos depósitos da Amazon tinham de usar leitores de código de barras e computadores instalados em locais estratégicos para, ao início do dia, informarem ao sistema que estariam iniciando a jornada de trabalho. Dessa forma, o sistema, por meio de uma decisão algorítmica, passaria suas atividades paulatinamente, conforme a atividade anterior seria realizada.[67] Portanto, um algoritmo iria continuamente repassar as atividades, com base no rastreamento do ritmo de trabalho coletado pelos equipamentos, por meio de um monitoramento ininterrupto, em tempo real.

Para além do uso interno, a Amazon comercializa seus softwares baseados em IA com outras empresas, de modo que soluções que possam vir a comprometer direitos serão espalhadas e potencializadas de forma alarmante. Um exemplo desse tipo de tecnologia é a *Amazon Web Services Panorama Appliance*, que faz parte do pacote AWS. Segundo informa a fabricante em seu site: "o *AWS Panorama Appliance* é outra opção de dispositivo de *hardware* que pode se integrar perfeitamente à sua rede local e pode executar vários modelos de visão computacional (CV) em vários fluxos de vídeo simultâneos."[68] (tradução livre). Trata-se, portanto, de uma ferramenta que permite a empresas acessarem os vídeos obtidos por câmeras de vigilância em sua própria rede interna, sem a necessidade de armazenamento dessas informações em servidores externos. Além disso, durante o período de pandemia pela Covid-19, a Amazon divulgava essa tecnologia como forma de os empregadores em fábricas utilizassem sistemas de aprendizado de máquina (ML) para permitir que os vídeos registrados fossem analisados continuamente com a finalidade de garantir o distanciamento entre os empregados, o que consequentemente permitiria a programação desses dispositivos também para outras finalidades, como monitoramento do desempenho profissional.[69]

2.4 Avaliações, sanções e dispensas aplicadas pelo algoritmo ou a partir dele

[66] DELFANTI, Alessandro; RADOVAC, Lilian; WALKER, Taylor. The Amazon Panopticon: A Guide for Workers, Organizers & Policymakers, **UNI Global**, 2021. Disponível em: https://uniglobalunion.org/wp-content/uploads/amazon_panopticon_en_final.pdf. Acesso em: 07 abr. 2023. p. 8.
[67] Ibid., p. 6.
[68] AMAZON. AWS Panorama Devices. Disponível em: https://aws.amazon.com/pt/panorama/appliance/. Acesso em: 08 abr. 2023.
[69] DELFANTI, Alessandro; RADOVAC, Lilian; WALKER, Taylor. The Amazon Panopticon: A Guide for Workers, Organizers & Policymakers, **UNI Global**, 2021. Disponível em: https://uniglobalunion.org/wp-content/uploads/amazon_panopticon_en_final.pdf. Acesso em: 07 abr. 2023. p. 9.

Para além do processo de contratação e do processo de acompanhamento de um contrato de trabalho, igualmente nas suas situações excepcionais, sejam elas avaliações, sejam sanções ou dispensas, são aplicadas pelo empregador tecnologias baseadas em IA.

Um ramo empresarial em que é bastante comum a utilização de dispositivos de IA para monitoramento do desempenho laboral, visando a avaliação dos trabalhadores, é aquele relacionado a *telemarketing* ou *Call Center*, setor marcado por violações aos direitos dos trabalhadores, notadamente quanto à invasão de privacidade e outras medidas empresariais questionáveis. O caráter reservado da atividade desempenhada pelo trabalhador, que o faz mediante ligações telefônicas com os consumidores daquele serviço, aliado à dificuldade que se tem de medir a qualidade das |tarefas realizadas por maneiras que não sejam a escuta das ligações, são fatores que incentivam empresas a buscarem cada vez mais acessar os conteúdos dessas conversas.

Mais recentemente, com a difusão de tecnologias baseadas em IA, esse setor despontou como um dos que mais as aplicam, como acontece com o uso de softwares que, de maneira automatizada, a partir das vozes nas ligações, detectam os estados emocionais (tristeza, felicidade, raiva, desmotivação etc.) tanto de trabalhadores quanto de consumidores, com o intuito inicial de prover mensagens motivacionais, buscando melhorar a eficiência do trabalhador.[70]

No entanto, nada impediria que essa ferramenta fosse utilizada para avaliar as emoções dos seus empregados e consumidores e, assim, verificar se o trabalho está sendo executado a contento ou não, se os consumidores estão satisfeitos ou não com as ligações e a forma com que são tratados, dentre diversas outras métricas possíveis. Essas análises de emoções ocorrem por meio do tratamento de dados pessoais sensíveis, que no caso seriam os dados biométricos obtidos a partir da voz.

Para além do tratamento automatizado de dados pessoais, outros tipos de dados pessoais também podem ser utilizados com o propósito avaliativo. É o exemplo dos metadados,[71] aqueles tipos de informações que, digitalmente, estão presentes em dispositivos

---

[70] SIMONITE, Tom. This Call May Be Monitored for Tone and Emotion. **Wired**, 19 mar. 2018. Disponível em: https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/. Acesso em: 08 abr. 2023.

[71] O termo "metadados" não é exclusivo dos meios digitais, já que desde há muito se utiliza esse conceito para áreas como biblioteconomia, tendo um significado geral mais próximo de "informações que oferecem detalhes a respeito das características de um determinado recurso. Via de regra, eles propiciam um conjunto de funcionalidades que abrangem desde a localização, documentação, descoberta, avaliação, seleção, até outras. Cabe destacar que essas operações são suscetíveis de serem realizadas por meio de usuários finais humanos ou por seus representantes automatizados" (tradução do autor), em DEMPSEY, Lorcan et al. A review of metadata: a survey of current resource description format. [S.l.] Specification for resource description methods. v.1, 1997. p. 5. Disponível em: https://archive.ifla.org/documents/libraries/cataloging/metadata/d32p1.pdf. Acesso em: 09 abr. 2023.

conectados à internet e que registram, por exemplo, o local, o horário ou o endereço de IP com os quais uma pessoa está acessando determinada página da internet. Na relação de emprego, principalmente durante e após a pandemia da Covid-19, quando se intensificou o trabalho remoto, os empregados passaram a gerar cada vez mais metadados para análise de seus empregadores.

Quando o empregador possui acesso a essas informações – aparentemente inofensivas e sem valor prático – por meio de dispositivos de IA, ele consegue identificar padrões de comportamento e criar inferências acerca de seus funcionários e do rendimento deles no trabalho. Paul Leonardi explica um pouco de como esse tratamento de dados pode ocorrer:

> Por exemplo, se um trabalhador começar a trabalhar tarde um dia (conforme registrado pelos horários de login da VPN), passar um tempo excepcionalmente curto trabalhando com informações em um portal (conforme registrado pelos carimbos de data/hora do lado do servidor) e estiver excepcionalmente quieto em uma reunião (conforme registrado pelo total de segundos de conversação em uma sessão de Zoom), nenhum desses metadados digitais por si só nos diz muito. Mas quando essas informações são combinadas, examinadas ao longo do tempo para qualificar um padrão de comportamento e comparadas com os padrões de outros funcionários, elas podem começar a criar inferências de que um funcionário está, por exemplo, se desconectando da organização. (tradução livre).[72]

Dessa forma, mesmo quando o empregado esteja trabalhando diariamente, poderá ser surpreendido com alguma sanção decorrente do rastreio de suas atividades diárias, a partir de informações que não seriam de maneira racional conectadas com a inferência produzida pelo empregador, de modo automatizado.

Um estudo realizado pela *Oxford Internet Institute* analisou, dentre várias ferramentas, uma que foi desenvolvida pela empresa americana NexLP, com mais de 50 clientes espalhados no mundo. A tecnologia possui um algoritmo que consegue detectar a possibilidade de *bullying* ou assédio em conversas corporativas, seja por e-mail, seja por *chat* ou documentos corporativos. Assim, ela continuamente monitora as comunicações corporativas e, caso encontre algo que siga o padrão agressivo, aciona uma etiqueta de alerta na mensagem, encaminhando automaticamente para o jurídico ou para a gestão de pessoas daquela empresa.[73]

---

[72] LEONARDI, Paul M. COVID-19 and the new technologies of organizing: digital exhaust, digital footprints, and artificial intelligence in the wake of remote work. **Journal of Management Studies**, v. 58, n. 1, p. 249, 2021. p. 250.

[73] NEFF, Gina et al. AI @ Work: Artificial Inteligence in the workplace. Disponível em: https://cdn.futuresays.org/content/uploads/2020/08/14084038/FS_PDF_GINA_V4.pdf. Acesso em: 09 abr. 2023.

Diante de tantas possibilidades de utilização da IA nas relações de emprego, alguns riscos jurídicos devem ser apontados, principalmente quanto ao direito à proteção de dados pessoais. Esse cenário é agravado diante da subordinação inerente às relações trabalhistas, que podem resultar em um estado de coisas de continua violação de direitos. Assim, considerando que a análise sobre as limitações ao uso da IA na relação de emprego, impostas pelo direito fundamental à proteção de dados pessoais, depende da análise de riscos a esse direito, passar-se-á, a seguir, a abordar os referidos riscos.

3 PRINCIPAIS RISCOS DA INTELIGÊNCIA ARTIFICIAL PARA A PROTEÇÃO DE DADOS DO TRABALHADOR

Apesar de o uso massivo das tecnologias baseadas em IA pelo empregador terem como principais objetivos a promoção da eficiência econômica, a melhoria da gestão do trabalho e a fiscalização do trabalhador por meios mais eficazes, persistem diversas situações de risco aos direitos dos empregados, especialmente quando se fala em riscos à proteção de dados pessoais.

Segundo estudo encomendado pela OCDE, muitos dos riscos gerados pela IA no ambiente de trabalho não são exclusivos dessas tecnologias, já que, por exemplo, a vigilância invasiva poderia ser gerada por qualquer tecnologia digital, guiada ou não por um algoritmo. No entanto, o grande diferencial da IA é a sua capacidade de intensificar e sistematizar essas falhas e riscos, mudando radicalmente as relações existentes entre empregadores e empregados.[74]

As propostas de regulação da IA na União Europeia baseiam-se no critério do risco, classificando as tecnologias de acordo com o risco que geram e, assim, estabelecendo critérios de aplicação, regras aplicáveis e requisitos a serem seguidos. Os demais países que possuem discussões legislativas sobre regulação da IA igualmente usam algum tipo de avaliação dessas tecnologias baseada no risco, ainda que não necessariamente adotem o mesmo formato discutido no âmbito da União Europeia, que é a classificação das tecnologias em "baixo risco", "médio risco", "alto risco" e "risco proibitivo".

Essa tendência europeia de vincular o grau de regulação, assim como o detalhamento e as especificações dos mandamentos regulatórios, ao grau de risco existente em cada demanda ou situação a ser regulada, é conhecida como regulação de risco (*risk-based approach*).[75]

Diante disso, levando em conta a inexistência de regulação brasileira sobre a temática, mas ainda assim considerando a relevância da abordagem *risk-based approach*, a seguir serão analisados os riscos trazidos pela aplicação da IA na relação de emprego, visando apurar quais medidas de *accountability* seriam mais adequadas para cada cenário, com o

---

[74] SALVI DEL PERO, Angelica; WYCKOFF, Peter; VOURC'H, Ann. Using Artificial Intelligence in the workplace: What are the main ethical risks? **OECD Social, Employment and Migration Working Papers**, n. 273, 2022. p. 17. Disponível em: https://ideas.repec.org/p/oec/elsaab/273-en.html. Acesso em: 07 nov. 2022.

[75] ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **I Encontro da Rede de Pesquisa em Governança da Internet**, Novembro de 2017 pesquisa sobre esse tipo de regulação, na Europa, e a proteção de dados pessoais, principalmente baseando-se nos estudos de Raphaël Gellert.

objetivo de evitar uma proposição genérica para todo tipo de tecnologia. Para além de considerar os riscos decorrentes do uso dessas tecnologias de modo amplo, o presente trabalho ponderará os riscos à proteção de dados pessoais especialmente na relação de emprego, a qual possui contornos diferenciados em relação às demais relações jurídicas, principalmente diante do seu elemento principal: a subordinação do empregado ao empregador.

3.1 Peculiaridades das relações de emprego que proporcionam mais riscos e justificam uma abordagem diferenciada

O grande ponto distintivo da relação de emprego, em relação às demais, é que existe uma situação desigual entre empregador e empregado, legitimamente alicerçada em preceitos constitucionais e celetistas. Assim, enquanto uma das partes possui muitos (senão todos) os meios decisórios, a outra deve seguir as decisões exaradas pela primeira, de maneira subordinada e limitada, prestando um serviço de natureza personalíssima.

O uso das ferramentas tecnológicas pelo empregador acentua o grau de desigualdade na relação empregatícia, principalmente porque essas tecnologias são utilizadas para rastrear condutas realizadas pelos empregados, aferindo sua produtividade e os submetendo à constante vigilância.

Nas seções seguintes, portanto, serão analisados os caracteres presentes na relação entre empregador e empregado que acentuam as situações de risco proveniente do uso da Inteligência Artificial. Dar-se-ão destaque à subordinação, como aspecto presente que evidencia a fragilidade do empregado diante do empregador, e ao poder de controle eletrônico do empregador, que evidencia uma intrusão legítima à privacidade do empregado, resultando na denominada “nudez tecnológica” deste.

3.1.1 Subordinação e poder empregatício enquanto elementos de fragilidade do empregado

A relação de emprego tem seu destaque dentre as relações de trabalho tendo em vista ser baseada na subordinação entre empregado e empregador. Assim, o grande traço distintivo e peculiar da relação de emprego é o fato de que o empregado está subordinado ao empregador, o qual, por consequência, detém o poder empregatício em relação ao empregado.

Trata-se de uma relação de complementariedade, já que a subordinação somente existe vinculada ao poder do empregador, ao passo em que este poder gera no empregado o

dever de submeter-se aos comandos lícitos passados por seu contratante, o qual é o proprietário daquela atividade economicamente organizada.

Ressalte-se que o desequilíbrio entre as partes é decorrente do poder empregatício, o qual não deve ser compreendido como um direito potestativo do empregador, ou como um mecanismo hierárquico na empresa, pois tais concepções não refletem as conformidades democráticas da empresa, vivenciadas a partir do século XX.[76]

Para Maurício Godinho Delgado,[77] o poder intra-empresarial (poder empregatício) deve ser considerado como uma relação jurídica contratual complexa, pois comporta a união de vontades do empregador e do empregado, mas com variações de intensidade quanto ao peso dos indivíduos dessa relação, gerando uma assimetria variável, "mediante a qual se preveêm [sic], se alcançam ou sancionam condutas no plano do estabelecimento e da empresa".[78]

Essa concepção demonstra que o poder empregatício não se traduz como apenas uma relação de hierarquia, em que todos os comandos do empregador devem ser verticalmente aceitos sem qualquer participação do empregado, que também possui pretensões, liberdades e interesses naquela relação jurídica.

O poder empregatício legitima, ao empregador, as atividades ligadas à direção, à punição e ao controle. Essas atividades refletem as dimensões do poder empregatício, pois são componentes necessários para a boa gestão do empreendimento. Uma das dimensões do poder empregatício é o poder de controle, o qual é considerado por Alexandre Agra Belmonte como "prerrogativa de fiscalização da execução das tarefas conforme as diretrizes, métodos, metas e fins estabelecidos no contrato de trabalho".[79]

O poder de controle do empregador era considerado por parte da doutrina clássica do direito do trabalho como inerente à possibilidade de poder acompanhar continuamente a prestação do trabalho e de vigiar o espaço empresarial interno.[80] Existia, ainda, que, visse tal prerrogativa como decorrente da subordinação presente na relação de trabalho.[81]

Bruno Lewiki[82] traça um histórico do controle do empregador, sistematizando-o em 3 (três) principais fases: o controle pessoal, o controle técnico e o controle total. As fases

---

[76] DELGADO, Mauricio Godinho. **O poder empregatício**. São Paulo: Ltr, 1996. p. 185.
[77] Ibid., p. 191.
[78] Ibid.
[79] BELMONTE, Alexandre Agra. **O monitoramento da correspondência eletrônica nas relações de trabalho**. LTr, 2004. p. 61.
[80] DELGADO, op. cit., p. 178.
[81] SÜSSEKIND, Arnaldo; MARANHÃO, Délio; VIANNA, Segadas. **Instituições de direito do trabalho**. v. 1. 22. ed. São Paulo: LTr, 1991. p. 237.
[82] LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003.

apontadas pelo autor demonstram que, historicamente, as mudanças no tipo de controle refletem-se pelos avanços tecnológicos e pela contínua necessidade de descentralizar as formas de controle do trabalho humano.

Inicialmente, havia um controle do tipo pessoal, já que desde os primeiros artesãos e produtores rurais do fim da idade média havia o controle da produção, sendo que naquelas situações o controle era feito pelo próprio profissional, o qual era detentor da produção e controlava a sua produtividade. Mesmo com o surgimento de pequenas oficinas e firmas, o controle permaneceu com seu aspecto pessoal, haja vista a horizontalidade que havia naquele momento, pois um trabalhador fiscalizava o outro, sem que houvesse uma relação hierarquizada entre eles. Mesmo quando surgiram empresas com maior quantidade de trabalhadores, o controle permanecia com um aspecto pessoal, a despeito de já haver uma verticalidade no controle, com a presença de fiscais trabalhando especificamente para monitorar o que era feito pelos trabalhadores e se estaria sendo executado o trabalho a contento do contratante.

Em uma segunda fase, instaurada somente com o surgimento de grandes fábricas, houve a primeira mudança de paradigma no controle da atividade empresarial, quando, no século XX, por meio do taylorismo, passou-se a adotar maior controle do tempo despendido em cada atividade, o que valeria como critério para aferir a produtividade daquela atividade. O controle do tempo despendido para a atividade representava, então, o controle dos empregados, que precisavam cumprir com as determinações de tempo para cada uma das funções a eles delegadas.

Além do controle do tempo, a visão panóptica, teorizada por Jeremy Bentham, foi buscada em sua implementação como uma forma de que o empregador pudesse, sem muito esforço, ter a vigilância de todos os trabalhadores ao mesmo tempo.

No período pós-guerra, as indústrias automobilistas tiveram uma proeminência na mudança estrutural do modelo de trabalho, encontrando em Henry Ford a doutrina (fordismo) responsável por incentivar o controle da produtividade dos trabalhadores com base na subordinação destes ao ritmo das máquinas, por meio da divisão estanque de tarefas. Esse novo modelo permitiu o controle do tempo de trabalho e, consequentemente, do desempenho do trabalhador. Além disso, adotava-se, com base no fordismo, uma estrutura fabril de posições fixas, em que os empregados deveriam estar estáticos em seus locais, para economizar movimentos, encurtando os momentos de não-trabalho.

Mudança significativa houve com a chegada da terceira fase. Após a recessão de 1973 e a crise do petróleo, houve uma nova mudança paradigmática quanto ao controle

empresarial, culminando em um modelo de trabalho iniciado nas indústrias automobilistas japonesas que ficaria conhecido como toyotismo.

Esse modelo de trabalho não eliminou os modos do fordismo, por isso não pode ser denominado pós-fordista, mas neofordista, porque adotou um controle multifacetado, imiscuindo elementos presentes tanto no controle técnico quanto no controle pessoal. Assim, utilizando-se da ideia de flexibilidade no trabalho, incentivava os empregados a se autocontrolarem, por meio da cobrança de resultados e de uma visão de autoprodutividade. Dessa forma, denomina-se "envolvimento participativo" o fato de que, segundo Bruno Lewicki: "a pessoa precisa parecer perfeita; os mínimos detalhes de sua personalidade têm que corresponder à imagem que a corporação tem de um trabalhador de comportamento irretocável".[83] Essa busca por fazer parte do padrão esperado pelo empregador gera no trabalhador a necessidade de abrir mão até mesmo de sua privacidade para atingir a eficiência na empresa, ao passo em que se verifica um verdadeiro "panóptico descentralizado",[84] mediado por dispositivos tecnológicos que não foram feitos para vigilância, mas atingem essa finalidade de alguma forma. Pondera Lewicki que "esse novo controle abrange todos os aspectos e momentos da vida da pessoa, minando a separação entre o trabalho e a vida externa".[85]

É esse poder de controle do empregador que o permite instalar câmeras de segurança no local de trabalho, restringir acesso a alguns sites pelos empregados, apresentar e monitorar alguns detalhamentos da rotina de trabalho que deve ser seguida, enfim, tudo aquilo que diz respeito à verificação do que está sendo realizado no ambiente de trabalho.

Apesar de facilitar o estudo sistemático do tema, a doutrina mais tradicional do Direito do Trabalho considera que o poder de controle não passa de uma das manifestações do poder diretivo, além de ser ligada ao poder disciplinar, do qual geralmente é o pressuposto.[86] Ainda assim, não se deve confundir com o poder disciplinar, pois não necessariamente o controle será realizado com a finalidade única de disciplina do local de trabalho, mas, como visto na seção anterior, também buscando maior eficiência na execução das atividades, gerando maior produtividade.

O poder de controle eletrônico, no entanto, tem a aptidão de trazer mais desequilíbrio ainda à relação de emprego, principalmente com a utilização das novas tecnologias do século XXI. Teresa Coelho Moreira considera que, com o uso das Novas

---

[83] LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003. p. 107.
[84] WHITAKER, Reg. **The end of privacy**. New York: New York Press, 1999. p. 40.
[85] LEWICKI, op. cit., p. 107.
[86] DELGADO, Mauricio Godinho. **O poder empregatício**. São Paulo: Ltr, 1996. p. 178.

Tecnologias da Informação e Comunicação (NTIC), esse poder de controle é atualizado, aumentado e, mesmo permanecendo como legítimo, poderá impactar direitos fundamentais do empregado, sobretudo aqueles mais ligados aos direitos de personalidade.[87]

Portanto, a própria existência de um legítimo poder de controle na relação de emprego, que já permitiria a vigilância ser executada no local de trabalho, diferencia a relação de emprego das demais relações jurídicas.

3.1.2 Poder de controle eletrônico do empregador enquanto legitimador de uma nudez tecnológica do empregado

O poder de controle é potencializado quando exercido por meio de NTIC. Nesse contexto, sobretudo considerado uma realidade digital, a vigilância no local de trabalho ocorre de maneira imperceptível.[88]

Essa característica da vigilância laboral, obtida por meio das novas tecnologias, reflete o que se denomina hoje de um poder de controle eletrônico, novo pois remodela a relação de vigilância tradicional. Enquanto tradicionalmente o empregador utilizava sua estrutura hierárquica para impor algum tipo de controle centralizado (revista íntima ou monitoramento por câmeras), com as novas tecnologias, o controle se dá de maneira muito mais sutil e descentralizada.

Teresa Coelho Moreira destaca duas características do poder de controle eletrônico do empregador. A primeira delas diz respeito à coleta de dados ilimitada que deriva dessa nova dimensão do poder de controle, pois o uso de novas tecnologias permite e estimula que sejam utilizados cada vez mais dados pessoais dos empregados, de modo que aparenta não ter limites sua coleta pelo empregador. A autora ressalta que "através do recurso à Inteligência Artificial é possível seguir os trabalhadores para, praticamente, todos os locais, controlar sua produtividade, o que fazem nos seus tempos de não trabalho e até, eventualmente, despedi-los".[89]

A segunda característica apontada é a de que essa nova modalidade de controle (eletrônico) é impessoal e invisível. Em sua forma tradicional, a utilização das tecnologias pelo

---

[87] MOREIRA, Teresa Coelho. **A Privacidade dos Trabalhadores e as Novas Tecnologias de informação e comunicação**: contributo para um estudo dos limites do poder de controlo electrônico do empregador. Coimbra: Almedina, 2010. p. 32-33.
[88] MOREIRA, Teresa Coelho. **A Privacidade dos Trabalhadores e as Novas Tecnologias de informação e comunicação**: contributo para um estudo dos limites do poder de controlo electrônico do empregador. Coimbra: Almedina, 2010. p. 62.
[89] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 179.

empregador para vigiar e monitorar os trabalhadores era claro, não havendo tanta discrição quanto à sua aplicação, já que sua finalidade era somente voltada ao gerenciamento e monitoramento dos funcionários. Além disso, o controle era realizado de maneira espacial, ou seja, limitado ao ambiente de trabalho. Ao passo em que as mesmas tecnologias que são utilizadas pelo empregado para a realização de seu trabalho se tornam mecanismos para sua vigilância, ou, ainda, diante do fato de que até mesmo o trabalho realizado em casa pode ser monitorado, a autora comenta que "através dessas tecnologias há um esbatimento das fronteiras espácio-temporais, alterando-se profundamente a relação de proximidade que existia entre empregador e trabalhador e que havia caracterizado o poder de controlo no passado".[90]

Não existe mais a prevalência do controle de um ser humano por outro. O que há, agora, são mecanismos que podem monitorar, vigiar e, até mesmo, tomar decisões sobre os monitorados. Segundo a professora portuguesa,

> [...] a monitorização digital pressupõe um salto qualitativo já que se está perante um controlo à distância, frio, incisivo, sub-reptício, aparentemente infalível, tornando possível um controlo total, ou quase total, de todos os movimentos da vida dos trabalhadores, o que origina que o trabalhador se torne transparente e sempre conectado - *homo connectus* - com os empregadores, deixando de ser livre.[91]

Diante desse novo poder de controle, a situação de fragilidade do empregado é aprofundada pela superexposição perante seu empregador, de maneira que quaisquer informações, seja da vida pessoal seja da experiência profissional, serão analisadas detidamente pelo empregador, ao ponto de formar perfis profissionais e pessoais daquele empregado.

Um evento que ilustra bem esse novo estado de coisas do poder de controle ocorreu em 2008, envolvendo a empresa Cataphora, como mencionado no item 2.3. O caso tratava de um *software* utilizado pela empresa que, como critério de avaliação, acessava os e-mails e mensagens coorporativas de seus funcionários para verificar o quão criativos costumavam ser.

Ao tratar do tema, Cathy O'Neil[92] aponta como problema o fato de que as empresas podem preferir demitir empregados que tenham menores classificações nesses critérios (presumindo que tais empregados seriam menos criativos), porém eles poderiam estar gerando excelentes ideias sem compartilhá-las com os colegas, ou mesmo poderiam ter contribuição em

---

[90] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 182.
[91] Ibid., p. 180.
[92] O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016.

outros aspectos, por exemplo melhorando o clima corporativo com piadas ou comentários úteis aos demais, características igualmente valorizadas no ambiente de trabalho.[93]

A produção desse tipo de inferências sobre os empregados ocorre visando melhores resultados, selecionando aqueles empregados mais ajustados aos critérios pretendidos pela empresa, porém podem gerar impactos discriminatórios, pois esses empregados podem sequer saber que estão sendo objeto dessas inferências, muito menos de maneira automatizada, por exemplo com uso de Inteligência Artificial.

Então, diante do legítimo poder de controle, atualizado pelas novas tecnologias, tem-se um monitoramento eletrônico ocorrendo nas relações de emprego, que acontece de maneira imperceptível, sutil e descentralizada, fragilizando o empregado nesse tipo de situação.

Para além da fragilidade própria gerada pelo poder de controle, outra repercussão mais evidente é a ampla gama de informações fornecidas ao empregador. Ao ser contratado, um empregado já precisa apresentar diversos dados pessoais, seja por meio de envio de documentos, seja por meio do preenchimento de algum tipo de formulário.

Esses dados pessoais são utilizados para diversas finalidades, sendo a principal delas permitir que haja o poder diretivo do empregador, permitindo que ele possa identificar seus empregados, direcioná-los para o exercício de suas atividades, prestar contas de suas obrigações legais ou sindicais, portanto, para fazer com que o contrato de trabalho se efetive.

No entanto, esses não são os únicos dados acessíveis pelo empregador, principalmente quando são utilizadas novas tecnologias, a exemplo de algoritmos de IA. O empregador tem acesso às trocas de mensagens dos empregados, quando utilizando alguma ferramenta de comunicação interna, a registros de horários dos empregados, algumas vezes a dados de geolocalização, ao desempenho profissional perante situações de estresse (incluindo emoções e reações a essas situações), dentre diversos outros.

Ao buscar uma gestão de pessoas mais efetiva, o empregador terá de inferir algumas conclusões a partir dos dados dos empregados, já que os dados básicos não serão suficientes. O empregador poderá ter acesso aos dados pessoais sensíveis dos empregados, àqueles dados ligados a saúde, ou mesmo àquelas informações dos familiares do empregado.

Todo o acesso do empregador a essas informações, não apenas àquelas estritamente necessárias para a finalidade principal do contrato de trabalho, mas que são importantes para a melhoria da gestão empresarial, demonstram que o empregado está cada vez mais desnudado

[93] Ibid., p. 132-133.

pelo empregador. Sempre mais, o empregador tem acesso a quem seu empregado é, faz ou deixa de fazer.

Teresa Coelho Moreira afirma que se trata de uma nudez tecnológica do empregado, pois essas novas tecnologias aumentam desmesuradamente a capacidade de acumulação de informações, permitindo criar um perfil do empregado com base em informações aparentemente inofensivas.[94]

Mais especificamente quanto à Inteligência Artificial, algumas peculiaridades são apontadas pela doutrina como especificamente sensíveis para as relações de emprego. Antonio Aloisi e Elena Gramano sistematizam essas peculiaridades, listando-as em quatro principais.[95] Primeiro, esses mecanismos de IA geralmente coletam informações de diferentes fontes (mesmo fora da relação de emprego), além de coletar mais dados do que estritamente necessários. Segundo, esses algoritmos criam inferências não intuitivas e não verificáveis, gerando um *HR Analytics* baseado na predição. Terceiro, os algoritmos podem causar impacto não só na liberdade e na privacidade dos empregados, mas também na sua autonomia e nas decisões morais, conectando cada vez mais a vida pessoal com a vida profissional. Quarto, esses mecanismos, associados a uma cultura de automonitoramento e gamificação, podem gerar o fornecimento de dados pessoais pelo empregado de maneira consensual, mas em troca de pequenos benefícios supérfluos.

Os impactos desse tipo de tratamento de dados, de maneira automatizada, pelo empregador, são pouco discutidos e menos ainda regulados. No Brasil, a LGPD traz um regramento sobre decisões automatizadas, porém permite que a empresa deixe de proativamente apresentar os critérios para a tomada de decisão automatizada, devendo aguardar a solicitação do titular de dados.[96]

Especificamente na relação de emprego, não há legislação que trate do tema, abrindo a possibilidade de que o empregador utilize mecanismos de IA, sem que o empregado saiba que está sendo monitorado por eles, quais as finalidades daquele monitoramento ou, ainda, quais as consequências que vai resultar.

---

[94] MOREIRA, Teresa Coelho. **A Privacidade dos Trabalhadores e as Novas Tecnologias de informação e comunicação**: contributo para um estudo dos limites do poder de controlo electrônico do empregador. Coimbra: Almedina, 2010. p. 27.

[95] ALOISI, Antonio; GRAMANO, Elena. Artificial intelligence is watching you at work. Digital surveillance, employee monitoring and regulatory issues in the EU context. **Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection"**, 2019, p. 105-106. Disponível em: http://salus.adapt.it/wp-content/uploads/2020/07/Gramano-Alois_AI-is-Wathching-you_2019.pdf. Acesso em: 07 set. 2020.

[96] O artigo 20, parágrafo primeiro da LGPD prevê a obrigação do controlador de dados fornecer informações sobre o tratamento automatizado de dados pessoais, porém condiciona à solicitação do titular de dados, além de excepcionar essa obrigação quando envolver segredo industrial ou comercial.

Diante disso, e da peculiaridade da relação de emprego quanto ao uso da IA pelo empregador, a seguir serão identificados os principais riscos provenientes dessas tecnologias para o direito à proteção de dados do empregado, primeiro em relação aos direitos de personalidade, em segundo momento em relação ao direito à privacidade, por último serão abordados os riscos à igualdade e à não discriminação no ambiente de trabalho. A partir do entendimento dessas situações de risco, será possível, em seguida, observar de que maneira o direito fundamental à proteção de dados pessoais limita o uso da IA na relação de emprego.

3.2 Personalidade em perigo: imagem e identidade pessoal

A LGPD (Lei Geral de Proteção de Dados) é o instrumento normativo que fornece a proteção dos dados pessoais aos titulares desses mesmos dados, principalmente resguardando o direito à privacidade. No entanto, não se limita a ele, já que garante diversos outros direitos aos indivíduos, inclusive com fundamentos em outros institutos jurídicos. Como evidência, o artigo 1º da LGPD deixa claro os objetivos da lei: "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Em outro trecho da lei, no artigo 2º, são listados os fundamentos da disciplina da proteção de dados, dentre os quais se encontra o respeito à privacidade (inciso I), a inviolabilidade da intimidade, da honra e da imagem (inciso IV), a autodeterminação informativa (inciso II) e o livre desenvolvimento da personalidade (inciso VII, b).

A simples análise da legislação demonstra que, para além da privacidade, a proteção de dados pessoais também busca instrumentalizar outros direitos de personalidade, tais como a honra, a imagem, o livre desenvolvimento da personalidade (bastante associado à autodeterminação informacional e ao direito à identidade pessoal). Portanto, ao buscar a análise sobre os riscos à proteção de dados pessoais, decorrentes da aplicação da IA na relação de emprego, não haveria como deixar-se de falar dos riscos implicados aos direitos de personalidade do empregado, enquanto pessoa no trabalho.

Os direitos de personalidade são institutos jurídicos tradicionalmente vinculados ao Direito Civil, já que oriundos da proteção da pessoa e de seus aspectos mais intimamente ligados com o simples fato de existir. Assim, o Código Civil, nos artigos 11 e seguintes, dispõe sobre a tutela dos direitos de personalidade, diante dos seus contornos específicos e de sua proteção pelo Direito.

Muitos, inclusive, confundem os direitos de personalidade com os direitos fundamentais, previstos na Constituição Federal, tradicionalmente existentes para proteger os

indivíduos do poder emanado do Estado. No entanto, tal confusão não se sustenta, mesmo que haja elevado grau de semelhança e interseção entre essas duas categorias de direitos.

Em Portugal, a doutrina sobre os direitos de personalidade é vasta e muito rica, sendo bastante assente dentre os juristas portugueses que não há coincidência entre esses direitos, inclusive porque há direitos de personalidade que não se qualificam como direitos fundamentais e há direitos fundamentais que não se igualam aos direitos de personalidade.[97]

Já na doutrina alemã, recorre-se à dignidade humana como fundamento para os direitos de personalidade, mas por aspectos históricos que lhes fazem seguir por esse caminho, inclusive diante da estreita relação entre público e privado quando de sua primeira teorização naquele país (um caso envolvendo o direito de imagem do ex-Chanceller Otto Von Bismarck, às vésperas da entrada em vigor do novo Código Civil alemão).[98]

No caso do Brasil, estando previstos e fundamentados no Código Civil, os direitos de personalidade encontram seu real fundamento no Direito Privado, o que, segundo Otávio Luiz Rodrigues Júnior, "implica o reconhecimento de que as normas do Código Civil fornecem os meios de vinculação dos particulares, sem necessidade de recursos permanente ao texto constitucional para sua concretização".[99]

Carlos Alberto Bittar[100] expressa essa distinção existente na doutrina, colocando de um lado os "direitos do homem" ou "direitos fundamentais", sendo "objeto de relações de direito público, para efeito de proteção do indivíduo contra o Estado" e, de outro lado, os "direitos de personalidade", sendo "os mesmos direitos, mas sob o ângulo das relações entre particulares, ou seja, da proteção contra outros homens".

No entanto, apesar de se tratar de direitos com substrato no Direito Privado, não se deve considerar que haja separação estanque entre eles e os direitos fundamentais, oriundos de uma dimensão do Direito Público. Afinal, o que os diferencia é a lógica de aplicação, já que nas relações privadas, geralmente, a relação entre as partes é mais equilibrada juridicamente – mesmo que não o seja econômica ou socialmente –, enquanto no Direito Público a relação sempre será de desigualdade, entre o particular e o público.

---

[97] CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra Editora, 1995. p. 581-582.
[98] RODRIGUES JUNIOR, Otavio Luiz. Direitos fundamentais e direitos da personalidade. *In*: TOFFOLI, José Antonio Dias (org.). **30 anos da constituição brasileira**: democracia, direitos fundamentais e instituições. Rio de Janeiro: Forense, 2018, p. 679-703. p. 681.
[99] Ibid., p. 683.
[100] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., ver., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015. p. 67.

Está igualmente presente, nas relações de emprego, a tutela dos direitos de personalidade. O empregado que se encontra prestando serviços de maneira subordinada não deixa de ser uma pessoa por isso, mantendo o traço distintivo desses direitos. Pode-se arguir, ainda mais, que nesse tipo de relação jurídica a proteção a esses direitos deve ser reforçada, diante do fato de que existe uma relação de desigualdade jurídica entre as partes, legitimada pelo próprio Direito.

Além da desigualdade existente por padrão na relação de emprego, o caráter da pessoalidade implica em uma prestação de serviços personalíssima, o que leva o empregado a estar praticamente "inserido" no próprio objeto do contrato de trabalho, já que a prestação do serviço é contratada de maneira insubstituível, portanto, implicando na inserção de aspectos físicos e psíquicos do empregado naquela relação contratual.[101]

Como já explicado na subseção anterior, a relação de emprego implica na subordinação jurídica do empregado ao empregador, o qual possui o Poder Empregatício, que lhe permite dirigir o empreendimento, fiscalizar se as orientações estão sendo bem cumpridas e, inclusive, controlar os meios pelos quais o trabalho é realizado. Esse Poder é capaz de invadir diversos aspectos da personalidade do empregado, revelando mais ainda a perspectiva da proteção dos direitos de personalidade do empregado.

Dentre os direitos de personalidade, encontram-se o direito à imagem, o direito à identidade pessoal, o direito à honra, o direito à privacidade, o direito à integridade física, os direitos morais de autor, dentre vários outros. Na relação de emprego, a proteção a esses direitos encontra-se geralmente direcionada para o direito à imagem, para o direito à privacidade e para o direito à identidade pessoal. Diante do escopo do trabalho, atendente ao direito à proteção de dados pessoais, estes serão os direitos de personalidade a serem analisados, diante dos riscos impostos pelo uso dos mecanismos de Inteligência Artificial.

O direito à imagem do empregado é impactado pelo uso da IA, principalmente quando se percebe o uso dessas tecnologias para captação de imagens dos empregados, gerando dados pessoais biométricos, seja com a finalidade de verificação da identidade, seja com a finalidade de análise de padrões comportamentais ou emocionais.

A proteção à imagem, tradicionalmente, é referida como o mais evidente direito da personalidade, já que a imagem é a representação corpórea dos aspectos visíveis da personalidade de um indivíduo. Se o ser humano possui uma representação externa de sua personalidade, o faz primeiramente por meio da imagem que reflete nos demais.

---

[101] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 187.

Para Carlos Alberto Bittar, o direito à imagem é aquele:

> […] que a pessoa tem sobre a sua forma plástica e respectivos componentes distintos (rosto, olhos, perfil, busto) que a individualizam no seio da coletividade. Incide, pois, sobre a conformação física da pessoa, compreendendo esse direito um conjunto de caracteres que a identifica no meio social.[102]

Esses caracteres identificadores da pessoa no meio social variam de acordo com a evolução das formas de representação da imagem. Se, à época de Pontes de Miranda, os caracteres identificadores em da imagem de uma pessoa seriam as formas, a voz ou os gestos,[103] com o avanço tecnológico e dos meios de reprodução da imagem humana, tem-se um leque mais amplo de caracteres identificadores da imagem humana.

Hoje incorporada aos *smartphones*, grandes câmeras fotográficas já representaram uma tecnologia inovadora de reprodução da imagem. Dessa mesma forma, a imagem humana deixou de ser uma mera fotografia e passou a ser identificada por caracteres mais sofisticados, principalmente com o uso de mecanismos mais invasivos de vigilância e reprodução de imagens. Isso acontece, por exemplo, com a identificação da impressão digital, o mapeamento da retina, o reconhecimento de padrões faciais, dentre outros que estão na categoria dos dados pessoais biométricos.

Com a difusão dessas tecnologias de captação de imagens, hoje muitos estabelecimentos empresariais possuem mecanismos de vigilância do local de trabalho, por exemplo câmeras de videomonitoramento, controles de acesso a estabelecimentos por meio de identificação facial ou por impressão digital, dentre outros, legitimamente instalados para garantir a segurança dos locais de trabalho e, portanto, baseados em hipóteses legais válidas.[104]

No entanto, a partir do momento em que esse monitoramento se propõe a captar dados pessoais biométricos dos empregados, por meio de tratamento automatizado, as finalidades desse tratamento devem ser sempre verificadas de maneira legítima e respeitando os direitos dos empregados.

Neste ponto, é relevante destacar o que seria categorizado como "dado pessoal biométrico" para fins da análise de seu tratamento pelo empregador. Biometria é um termo que representa "a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de

---

[102] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., ver., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015. p. 209.
[103] MIRANDA, Pontes de. **Tratado de Direito Privado**, Tomo VII: Direito de personalidade. Direito de família: direito matrimonial (existência e validade do casamento). Atual. Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Editora Revista dos Tribunais, 2012. p. 111.
[104] A LGPD exige que o tratamento de dados ocorra com base em alguma hipótese legal, de acordo com o tipo de dados pessoais, sejam eles ordinários (art. 7º), sejam sensíveis (art. 11).

seus atributos fisiológicos ou comportamentais mensuráveis".[105] Assim, informações relativas a atributos fisiológicos que possam ser mensurados – tais como a altura, a geometria da mão, a identificação por retina, a delimitação dos traços do rosto – e os atributos comportamentais mensuráveis – a forma como digita, o jeito como anda, gestos peculiares, os atributos da voz, por exemplo – são considerados dados biométricos.

O artigo 5º, II da LGPD reconhece os dados biométricos na categoria de dados pessoais sensíveis, os quais gozam de proteção diferenciada pela lei, com bases legais de tratamento próprias e, diante do risco de seu processamento, demandando medidas de minimização de risco específicas.

O tratamento de dados biométricos na relação de emprego é usual e antigo, antes mesmo de qualquer preocupação com o uso de Inteligência Artificial. O controle de jornada de trabalho de empregados é muitas vezes realizado por meio da captação dos dados biométricos presentes nas impressões digitais deles, validando sua identidade perante o sistema de marcação do ponto, visando prevenir a fraude no registro dos horários de entrada e saída no trabalho.

Outro exemplo comum de tratamento de dados biométricos de empregados ocorre no acesso às dependências do estabelecimento empresarial, em que muitas vezes os empregados devem proceder ao reconhecimento, não apenas de sua impressão digital, mas, por vezes, ao reconhecimento facial.

O reconhecimento facial se apresenta como um dos tipos de reconhecimento biométrico, mas que possui inúmeras vantagens em comparação aos demais. Chiara de Treffé e Elora Fernandes apontam os principais benefícios desse tipo de reconhecimento biométrico:

> (i) o reconhecimento facial é uma tecnologia não intrusiva muito baseada na maneira como os próprios seres humanos se reconhecem mutuamente; (ii) devido à existência de um sistema burocrático já consolidado de identificação por intermédio de fotos, seria possível criar facilmente uma interação entre ele e o reconhecimento facial aos cidadãos; (iii) o reconhecimento facial é baseado na capacidade de memória dos computadores, compensando a falibilidade perceptiva dos seres humanos; (iv) ao ser integrada aos sistemas de vídeo para vigilância, essa tecnologia permite a identificação à distancia, sem que as pessoas saibam ou tenham de cooperar com a identificação; (v) pelo reconhecimento facial é possível saber, também, as emoções de uma pessoa (por exemplo, felicidade ou raiva), bem como suas informações biográficas (como sexo, etnia e idade); (vi) em comparação com as outras características biométricas, as pessoas, nos dias atuais, mostram-se mais passíveis de compartilhar imagens de seu rosto (como em mídias sociais, por exemplo, utilizando, inclusive, ferramentas de marcação - tags).[106]

[105] TREFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo Guia da. **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, p. 283-315. p. 292.

[106] TREFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo Guia da. **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, p. 283-315. p. 294.

No entanto, apesar dos inúmeros benefícios proporcionados por esse tipo de tratamento de dados pessoais baseado no reconhecimento facial, os riscos inerentes ao uso da IA para essa finalidade na relação de emprego pede amplo cuidado. Isso, porque as tecnologias de IA baseadas no *machine learning* possuem capacidade de aprender com os próprios dados a elas disponibilizadas. No entanto, mesmo sendo considerados aprendizes, os algoritmos dessas tecnologias podem produzir resultados incorretos e discriminatórios.

O tratamento automatizado desses dados biométricos deve ter atenção ainda maior, principalmente considerando as características básicas dos dados biométricos que, segundo Teresa Coelho Moreira, são a *universalidade*, já que todas as pessoas as possuem, a *singularidade* ou *unicidade*, tendo em vista que cada um possui atributos biométricos únicos, a *permanência*, pois esses dados raramente se modificam, mantendo-se para sempre com aquele indivíduo, além da *mensurabilidade* e *acessibilidade*, pois está na própria natureza da biometria que os dados sejam capazes de medição.[107]

Pelo fato de serem permanentes durante toda a vida, por vezes até ultrapassando o término da vida, seu tratamento pode impactar uma pessoa eternamente, registrando para sempre determinada informação ocorrida em um certo momento de sua vida, impossibilitando que haja o esvaimento dessas informações, caracterizando verdadeira pena perpétua para determinados atos cometidos preteritamente.

Importante destacar que o reconhecimento facial ou biométrico, principalmente de empregados, pode levar a uma objetificação dessas pessoas,[108] já que serão substituídas por simples caracteres biométricos, sem qualquer tratamento individual sobre a pessoa, apenas sobre suas informações. Em uma época que cada vez mais se busca a pessoalidade no trato entre empregador e empregado, objetivando maior humanização e interação humana, considerar que um empregado poderia ser resumido ao modo ou a velocidade com a qual digita em seu computador, utilizando apenas essas informações como forma de premiação ou punição trabalhista, seria esquecer-se completamente da natureza humana daquele trabalhador.

Além disso, na análise de candidatos em processo seletivo, o reconhecimento automatizado de dados biométricos, notadamente faciais e de padrão de comportamento, pode implicar em critérios de seleção que desconsiderem as peculiaridades dos candidatos, levando

---

[107] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 233.
[108] TREFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo Guia da. **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, p. 283-315. p. 300.

o contratante a selecionar não indivíduos, mas padrões de comportamento e de reações que, talvez, pertençam a um arquétipo de bom candidato à vaga de emprego. Essa substituição da pessoa por resultados analisados matematicamente reflete uma verdadeira "algoritmização" dos indivíduos, que são tratados como verdadeiros algoritmos digitais.[109]

Outro risco a ser destacado diante do tratamento automatizado de dados pessoais biométricos diz respeito à falta de acurácia desses dispositivos de IA no reconhecimento facial, principalmente de grupos já discriminados. Diversos casos de reconhecimento facial que não funcionavam, por exemplo, com pessoas negras, com mulheres – especialmente com mulheres negras –, com pessoas asiáticas, dentre outros grupos, demonstram que as máquinas, assim como os humanos, podem cometer erros.[110] Esses erros são geralmente ocasionados pela falta de representatividade na construção dos algoritmos de IA, já que geralmente as bases de dados utilizadas, assim como os testes prévios, são de pessoas brancas do sexo masculino.

Outro risco do uso do reconhecimento facial automatizado no local de trabalho diz respeito ao reconhecimento de emoções e reações, notadamente em processos seletivos e em avaliações de desempenho de empregados. O reconhecimento facial ou de outros dados biométricos, como a voz, permite ao empregador avaliar se, em determinados momentos de estresse ou de uma demanda exigente no trabalho, aquele indivíduo reage de maneira serena ou estressada; se mantém uma imagem cordial perante os clientes ou se destempera-se diante de um cliente insatisfeito; se responde educada ou rispidamente a uma ligação de cliente que seja mais agressivo e incompreensivo.

Diversos casos de reconhecimento facial identificando padrões de emoções ou reações foram aplicados, por exemplo o caso do Metrô de São Paulo, em que a concessionária da Linha Quatro Amarela buscou utilizar uma ferramenta para avaliar as reações dos usuários do transporte público, diante de painéis publicitários. O propósito inicial poderia ser interessante, avaliar a satisfação dos indivíduos com as propagandas disponibilizadas perante os locais públicos, proporcionando a análise de sua efetividade e permitindo a melhoria para a população. No entanto, diversos questionamentos foram feitos diante disso, por exemplo aqueles indivíduos que apenas estivessem passando pela estação de metrô, de maneira anônima,

---

[109] NAKAR, Sharon; GREENBAUM, Dov. Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. **Boston University Journal of Science & Technology Law**, v. 23, n. 1, p. 88-123, 2017. p. 119.

[110] Sobre esse tema, Virginia Eubanks (EUBANKS, Virginia. **Automating inequality**: How high-tech tools profile, police, and punish the poor. Nova York: St. Martin's Press, 2018) e Safiya Umoja Noble (NOBLE, Safiya Umoja. **Algorithms of oppression**: How search engines reinforce racism. Nova York: NYU Press, 2018) apresentam, de maneira estruturada, diversos casos de discriminação racial derivada do uso de algoritmos de reconhecimento facial, igualmente a Joy Buolamwini, no documentário "Coded Bias".

teriam seus dados coletados sem qualquer medida de obtenção do consentimento ou possibilidade de recusa do tratamento.[111]

O reconhecimento facial para identificação de emoções e reações encontra maiores barreiras ainda na Europa, em que muitos Tribunais e Autoridades de controle quanto à proteção de dados pessoais já se posicionaram contrários ao uso indiscriminado dessas tecnologias. Um desses exemplos mais marcantes vem do ICO (*Information Commissioner's Office*), a Autoridade de proteção de dados pessoais do Reino Unido, que recentemente publicou alguns documentos que alertam as empresas quanto ao uso de algoritmos de reconhecimento facial e tratamento de dados biométricos para análise de reações e emoções, notadamente para contratação em processos seletivos de emprego. Isso, porque, segundo o ICO, essas tecnologias não possuem evidências científicas suficientes para serem utilizadas de maneira ampla, além do que poderem gerar impactos no acesso a emprego, a crédito e outros direitos e serviços públicos, com base em informações sensíveis e, até mesmo, sem confiabilidade científica.[112]

Além disso, principalmente no local de trabalho, os riscos inerentes ao aumento da vigilância podem ser intensificados quando se fala do reconhecimento facial por empregadores, já que essas bases de dados podem ser eventualmente compartilhadas com outras empresas, até mesmo com o Poder Público, de maneira que a interconexão desses dados perante bases diferentes pode trazer prejuízos quanto aos direitos de liberdade e igualdade.

Teresa Coelho Moreira ressalta, inclusive, que o empregador não deveria utilizar diversos dados biométricos em conjunto, por exemplo vigilância eletrônica e geolocalização, pois isso poderia trazer inferências perigosas quanto aos direitos do empregado e à sua intimidade[113].

Diante disso, percebe-se que o direito à imagem se encontra perante inúmeros riscos pelo uso da IA na relação de emprego, notadamente quando se fala em reconhecimento facial automatizado e no tratamento desses dados pessoais biométricos de maneira desproporcional e sem qualquer base legal adequada.

---

[111] O caso foi objeto de Ação Civil Pública, ajuizada pelo IDEC (Instituto Brasileiro de Defesa do Consumidor) perante o Tribunal de Justiça de São Paulo, sob o número 1090663-42.2018.8.26.0100 e foi julgado procedente, para condenar a empresa ao pagamento de indenização por danos morais coletivos de R$ 100.000,00 (cem mil reais), além da abstenção de captação de imagens por esses equipamentos.

[112] Recentemente, foram publicados informativos do ICO sobre esse tema, que podem ser acessados nos links a seguir: "*Biometrics insight report - 26 October 2022"* (ICO: Biometrics: insight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf. Acesso em: 07 abr. 2023) e "*Biometrics foresight report - 26 October 2022"* (ICO: Biometrics: foresight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf. Acesso em: 07 abr. 2023).

[113] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 235.

Outro direito à personalidade que se encontra diante de riscos nessas situações é o direito à identidade pessoal. Adriano de Cupis foi o pioneiro a destacar a importância do bem jurídico da identidade pessoal no Direito Civil, baseando-se na necessidade do ser humano de afirmar sua própria individualidade, para que seja conhecido por quem ele realmente é.[114]

Por isso, para o referido autor, a identidade consistiria "no distinguir-se das outras pessoas nas relações sociais".[115] E continua, sobre a identidade pessoal, entendendo que "o homem atribui grande valor, não somente ao afirmar-se como pessoa, mas como uma certa pessoa, evitando a confusão com os outros".[116] Essa necessidade de identificar-se não se limita a diferenciar-se de outros, vai além, representando a possibilidade de o indivíduo decidir a forma como gostaria que os demais lhe enxerguem.

Quanto ao conteúdo do direito à identidade pessoal, Adriano de Cupis ressalta que sua configuração é, essencialmente, ocupada com o direito ao nome. No entanto, assume que o nome é apenas um dos elementos – apesar de ser o principal – de identificação da pessoa, destacando outros como a imagem, a voz e os acontecimentos da vida.

Carlos Alberto Bittar considera o direito à identidade pessoal como aquele que "constitui o elo entre o indivíduo e a sociedade em geral".[117] Para ele, a identidade se apresenta por meio dos sinais identificadores da pessoa (por exemplo, o nome), por meio dos quais o público em geral consegue manter um relacionamento normal nos diversos ciclos (familiar, sucessório, negocial, comercial e outros). Seguindo na mesma linha de Cupis, considera que tais sinais identificadores (ou elementos de identificação) possuem 02 (duas) funções essenciais: (i) individualizar a pessoa e (ii) evitar a confusão entre uma pessoa e outra.[118]

Ainda que haja outros elementos de identificação, Bittar ressalta que o nome apresenta uma identificação mais precisa, enquanto a imagem e a voz o fariam em um âmbito mais restrito, pois demandariam a prévia fixação de quem seria aquela pessoa e, também, um maior esforço associativo.[119]

Acerca da identidade como bem jurídico tutelado, considera-o um atributo ínsito à personalidade humana, mas o autor também destaca que o direito essencial ligado à identidade

---

[114] CUPIS, Adriano de. **Os Direitos da Personalidade**. 2. ed. Trad. Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008. p. 179.
[115] Ibid.
[116] Ibid.
[117] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., ver., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015. 265.
[118] Ibid.
[119] Ibid., p. 266.

é o direito ao nome,[120] diante de sua concepção de que ele é o sinal identificador que mais facilmente distingue um indivíduo.

Pontes de Miranda já se referia à identidade pessoal como um direito, mas não um direito específico, trata-se de uma categoria da qual fazem parte o direito ao nome, direito ao registro da identidade, direito ao retrato e outros meios de identificação, inclusive testemunhais. Segundo o autor, esses direitos à identidade pessoal seriam direitos imediatos, dos quais derivariam direitos mediatos – como o direito ao nome –, exemplificando ele que mesmo o nascituro já é identificado por sua mãe, apesar ainda não possui nome que lhe seja garantido pelo Direito.[121]

Percebe-se, portanto, que a doutrina civilista dos direitos de personalidade aborda, tradicionalmente, o direito à identidade como intrinsicamente relacionado com o nome da pessoa, sendo este o sinal identificador mais relevante para a identidade pessoal, como maneira de se identificar um indivíduo e diferenciá-lo de outro.

Não se estranha quando, ao preencher algum cadastro, seja o indivíduo questionado inicialmente sobre seu nome, para só então serem dele questionados outros atributos, que variam de acordo com a necessidade daquele receptor das informações. O nome recebe sua relevância mesmo no nascimento, quando do ato inicial de identificação da criança, pois o seu próprio nome é a ele associado, visando evitar confusão com outra.

No entanto, não se pode confundir o direito ao nome com o direito à identidade pessoal. O nome possui proteção jurídica específica, como expressão do direito a ter um nome e do direito à proteção do nome. Mas a identificação pessoal a ele não se limita.

Há, porém, outros sinais identificadores da pessoa, como sua imagem, sua voz, seus atributos pessoais, os quais podem igualmente ter proteção específica dos direitos de personalidade – direito à imagem, direito à voz.

Ricardo Luis Lorenzetti remete à doutrina italiana para a construção de um direito à identidade pessoal com autonomia, refletindo-se mediante duas espécies, a identidade estática e a identidade dinâmica. Enquanto a identidade estática representaria o nome, a identificação física e a imagem – atributos que, *a priori*, seriam estáveis, sem muitas possibilidades de mudança radical –, a identidade dinâmica diria respeito a "uma verdade biográfica, uma

---

[120] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., ver., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

[121] MIRANDA, Pontes de. **Tratado de Direito Privado**, Tomo VII: Direito de personalidade. Direito de família: direito matrimonial (existência e validade do casamento). Atual. Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Editora Revista dos Tribunais, 2012. p. 64.

história, um estilo individual e social do sujeito; é aquilo que diferencia o indivíduo, que o faz diverso".[122]

A concepção da identidade pessoal como um bem jurídico complexo, com a distinção entre sua dimensão estática e sua dimensão dinâmica, permite que seja atualizado conforme sejam modificados os meios de expressão da personalidade. Assim, mostra-se possível distinguir os diferentes sinais identificadores do indivíduo, tornando o nome apenas um desses sinais, não mais essencial para a identidade pessoal, como o era antigamente.

Essa distinção entre o direito à identidade pessoal e o direito ao nome encontra maior relevo e, ao mesmo tempo, maior necessidade, quando se fala do contexto digital. Ao buscar sua identificação no âmbito digital, os indivíduos não o fazem apenas com o seu nome, pelo contrário, o nome é cada vez menos utilizado para a identificação digital.

De modo crescente, a vida é refletida digitalmente por meio dos dados pessoais, sejam eles representados pelo próprio nome da pessoa, sejam eles também representados por um número de IP (*Internet Protocol*), ou outros elementos que possam identificar o indivíduo, direta ou indiretamente, como avatares virtuais, apelidos em redes sociais, nomes socialmente reconhecidos, dentre outros. Exemplo típico dessa nova forma de identificação ocorre nas redes de relacionamento (Facebook, Instagram, Twitter) ou em jogos eletrônicos, em que os usuários por vezes sequer conhecem os nomes uns dos outros, reconhecendo-se por seus apelidos ou *nicknames*.

Esse fenômeno, conhecido como "datificação", traduz o processo de formação de um corpo digital de informações que representem e, mais do que isso, confundam-se com o próprio indivíduo.

Os dados pessoais tornaram-se mais um tipo de sinal identificador da pessoa, refletindo a personalidade de uma pessoa para os demais em sociedade. Afinal, a identificação (mesmo que potencial) do sujeito é o critério distintivo para caracterizar um dado pessoal, tanto pela LGPD[123] (Lei Geral de Proteção de Dados brasileira) quanto pelo RGPD[124] (Regulamento Geral de Proteção de Dados europeu).

---

[122] LORENZETTI, Ricardo Luis; **Fundamentos do direito privado**. Trad. Vera Maria Jacob de Fradera. São Paulo: Revista dos Tribunais, 1998. p. 483-484.

[123] LGPD. Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

[124] RGPD. Artigo 4º. Definições. Para efeitos do presente regulamento, entende-se por: 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

O termo "datificação" foi trazido por Viktor Mayer-Schönberger e por Kenneth Currier como um dos elementos inerentes ao fenômeno do *Big Data* (inclusive, o nome de sua obra). Segundo os autores, o Facebook datificou as relações pessoais, o Twitter datificou a expressão de ideias, o LinkedIn datificou as experiências profissionais.[125]

Nessas plataformas, a simples informação de que o indivíduo clicou em um botão de seu computador ou *smartphone* e marcou que "curtiu" um determinado conteúdo virtual já é capaz de revelar as preferências e tendências de comportamento daquela pessoa. Ainda, o fato de aceitar um convite virtual para tornar-se "amigo" de outra pessoa na rede social já traduz algum aspecto identitário, no sentido de que aquelas pessoas nutrem algum tipo de relação, seja próxima ou mais distante, de admiração ou algo nesse sentido.

Mas não apenas nas redes sociais esse fenômeno está presente, também quando um indivíduo utiliza um dispositivo inteligente (por exemplo, um *smartwatch*), que contabiliza a quantidade de calorias gastas em um dia, ou quantas horas permaneceu em pé ou em movimento. Nessa situação, os dados, ainda mais analisados em uma escala macro, podem refletir se a pessoa é ou não sedentária, ou se possui uma vida agitada de exercícios predominantemente pela manhã ou à noite. São inferências obtidas a partir de dados pessoais, identificando diversos aspectos da personalidade, sem que esteja necessariamente presente o nome da pessoa, sua imagem ou outro elemento identificador.

É por isso que o direito à identidade pessoal precisa sustentar-se na sua concepção dinâmica, abrindo espaço para que seja reconhecido e garantido mesmo quando o que está em exposição são os dados pessoais e as inferências que as outras pessoas (ou algoritmos) produzem a partir deles.

Essas inferências são utilizadas com base nos dados pessoais que estão presentes no âmbito digital e formam as grandes bases de dados integradas (*Big Data*). Por isso, Mayer-Schönberger e Currier sustentam que a datificação não se limita à produção desses dados como sinais identificadores, mas porque hoje são usados para gerar valor comercial, principalmente por meio das inferências que se pode obter a partir do comportamento nas redes sociais.[126] Seria a "datificação de tudo" a tendência a partir do *Big Data*, para a qual a sociedade deve estar preparada e, conforme se sustenta neste trabalho, o Direito deverá estar atento e pronto para regular.

---

[125] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: A revolution that will transform how we live, work, and think. Nova York: Houghton Mifflin Harcourt, 2013. p. 91.
[126] Ibid., p. 93-94.

Reforçando essa ideia da datificação de tudo, retomando o que dizem Mayer-Schönberger e Currier sobre a transição da causalidade para a correlação causada pelo *Big Data*, (item 2.1), dessa forma é que são produzidas inferências acerca dos indivíduos, apenas com base nos dados pessoais que são gerados no meio digital. A junção dessa grande quantidade de informações de diversas bases de dados diferentes, mesmo que não se saiba o nome do indivíduo a que esses dados se referem, permite produzir conclusões sobre sua personalidade, por exemplo sua sexualidade, suas preferências ideológicas ou mesmo suas condições de saúde.

Um estudo realizado em 2017, por pesquisadores da Columbia Business School, da Universidade de Nova York e da Northeastern University, constatou a facilidade com a qual o Facebook seria capaz de identificar se um indivíduo é gay com base em apenas três curtidas naquela rede social.[127] Outro estudo, esse realizado no MIT em 2009, identificou que a partir da análise dos amigos no Facebook, a plataforma seria capaz de identificar homens gays.[128]

Diante desses exemplos, é possível suscitar hipóteses de risco levadas ao ambiente de trabalho. Por exemplo, se um empregador monitora as redes sociais de candidatos em processo seletivo ou de seus empregados (mesmo que sejam apenas dados disponibilizados ao público), poderá ter conhecimento de diversas preferências e características daquele indivíduo, levando a eventuais situações de discriminação ou mesmo de punição, no caso de haver interação em redes sociais de modo que não agrade ao empregador.

Outro caso, que teve maior repercussão, é aquele comentado por Charles Duhigg,[129] quando a empresa norte-americana Target realizou uma campanha de publicidade direcionada a seus consumidores, utilizando algoritmos de Inteligência Artificial para identificar perfis comportamentais baseados nos padrões de consumo. Uma dessas clientes era uma jovem que passou a receber em casa publicidade relacionada a gestação, como se ela estivesse realmente precisando daqueles produtos, causando desconfiança em seu pai. Ao dirigir-se a uma loja Target, o pai da jovem questionou a situação, porém alguns meses depois descobriu que sua filha estava realmente grávida, situação já prevista pela Target antes mesmo do conhecimento pela família.

Nessa situação, aumenta-se mais ainda o risco perante o ambiente de trabalho, notadamente porque saber se uma empregada está grávida antes mesmo da própria gestante é

---

[127] CHEN, Daizhuo et al. Enhancing transparency and control when drawing data-driven inferences about individuals. **Big data**, v. 5, n. 3, p. 197-212, 2017.
[128] MOORE, Matthew. Gay men 'can be identified by their Facebook friends'. **The Telegraph**, 21 set. 2009. Disponível em: https://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html. Acesso em: 07 abr. 2023.
[129] DUHIGG, Charles. **O poder do hábito**: por que fazemos o que fazemos na vida e nos negócios. Trad. Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

uma grave invasão de sua intimidade, caracterizando desrespeito ao direito à identidade pessoal, ou seja, de naquela situação poder apresentar seu estado gravídico à família apenas quando lhe aprouver, ou mesmo ao seu cônjuge. Mesmo que seja importante que essa informação seja comunicada a seu empregador de maneira imediata, para que possa iniciar o cômputo de sua estabilidade no emprego, a empregada deverá ter o direito de escolher o melhor momento e a melhor forma de fazê-lo. Além disso, o conhecimento antecipado pelo empregador poderia levar a uma dispensa (ou recusa na contratação), de modo injustificado, mesmo que depois descubra-se que aquela mulher estaria grávida.

Caso houvesse a utilização do mesmo tipo de tecnologia pelo empregador ou contratante em processo seletivo, seria possível que ele soubesse outras condições de saúde de seus candidatos a emprego, inferindo a essas pessoas a tendência a determinadas doenças ou condições de saúde, ocasionando possível discriminação por uso de informações sensíveis. Bruno Bioni exemplifica algumas possibilidades de deturpação dessa atividade, desrespeitando o direito à identidade pessoal, da seguinte forma:

> Processos seletivos na área de recursos humanos, para a concessão de crédito, para a estipulação de prêmios nos contratos securitários e até mesmo o risco de não embarcar em um avião, porque seus hábitos alimentares podem ser coincidentes com o perfil de um terrorista. Essas são amostras de que a categoriza o da pessoa, a partir de seus dados pessoais, pode repercutir nas suas oportunidades sociais, no contexto de uma sociedade e uma economia movidas por dados.[130].

Percebe-se, portanto, que os riscos apresentados diante da utilização desses algoritmos de IA refletem diretamente nos direitos de personalidade no local de trabalho, dentre os quais a privacidade é um dos mais destacados, razão pela qual será em seguida apresentado de maneira mais debruçada.

3.3 Vigilância desenfreada e privacidade relativizada

Diante do uso da IA, o empregado encontra-se com sua privacidade frontalmente em risco, por diversos aspectos diferentes, alguns deles já mencionados durante o presente trabalho. Importante destacar que o poder de controle eletrônico do empregador, que permitiria (em tese) a aplicação dessas tecnologias na relação de emprego, pode levar o empregador a buscar mais e mais invasão na intimidade e na vida privada do empregado.

---

[130] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 88.

No entanto, deve haver limites a esse poder empregatício. Esses limites devem ser os direitos fundamentais e os direitos de personalidade do empregado, de maneira que possa haver uma equivalência entre o direito do empregador de acompanhar a boa execução do seu empreendimento e os direitos do empregado, dentre os quais o de não ter sua privacidade violada em razão disso.

Esses riscos à privacidade do empregado se destacam bem quando analisados os princípios previstos na LGPD – os quais representam a carga valorativa necessária para se garantir a proteção da privacidade do titular de dados – notadamente quando se abordam os aspectos complexos na compatibilização entre o uso da IA e os comandos principiológicos da proteção de dados pessoais. Tendo isso em vista, passa-se a analisar, objetivamente, alguns riscos que o uso da IA na relação de emprego pode gerar aos princípios da LGPD, já que esse direcionamento metodológico seria capaz de demonstrar os riscos à privacidade do empregado.

Os incisos I, II e III do artigo 6º da LGPD[131] expressam a tríade de princípios que se relacionam mais diretamente, sendo eles indispensáveis para a compreensão da licitude de um tratamento de dados. O princípio da finalidade (inciso I) enumera que todo propósito de tratamento de dados deve ser específico e não pode haver tratamento posterior de forma incompatível com essa finalidade inicialmente estabelecida. O princípio da adequação (inciso II) prevê que o tratamento de dados deve ser compatível com a finalidade informada ao titular de dados. Já o princípio da necessidade (inciso III) prega que o tratamento de dados deve se limitar ao mínimo de dados possível, proporcionalmente ao que se deva alcançar com a finalidade previamente determinada.

O uso da IA pode impactar diretamente esses três princípios. Pincipalmente pois o funcionamento dos mecanismos baseados em IA depende do uso do *Big Data*. Por meio deste, os algoritmos de IA buscam mais fontes de informações úteis para seus propósitos e, dessa forma, podem produzir um resultado mais assertivo e mais fiel ao resultado esperado. No entanto, para isso os dados que serão utilizados não podem ter sua finalidade limitada, devem sempre estar disponíveis para reutilização em outros tipos de inferências ou resultados da máquina.

---

[131] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Em seu livro, que aborda especificamente o fenômeno do *Big Data* e suas consequências econômicas, sociais e epistemológicas, Viktor Mayer-Schönberger e Kenneth Cukier explicam que o *Big Data* implica em uma mudança de mentalidade quando se trata de utilização de dados, já que antes eles eram considerados de maneira estática, ou seja, atingido seu objetivo seriam descartados; porém, a partir do *Big Data*, os dados se tornaram matéria-prima dos negócios, servindo para criar valores além do seu propósito inicial.[132] Os autores citam os dados referentes ao modo como o motorista de carro se posiciona em seu assento, que seriam dados completamente sem utilidade. Contudo, com o *Big Data* e a grande capacidade de processamento de dados, essas informações são úteis, por exemplo, para que automóveis inteligentes possam alertar o motorista quando ele demonstra sinais de cansaço ao volante, evitando acidentes de trânsito e salvando milhares de vidas.

Porém, diante da quantidade de dados pessoais de empregados que o empregador já possui, se esses eles forem usados para finalidades diversas daquelas necessárias para a execução do contrato de trabalho, estar-se-iam sendo contrariados os princípios da finalidade, da adequação e da necessidade. Além disso, no caso tecnologias que sejam utilizadas pelo empregador, com base nos dados de empregados, para sugerir publicidade na rede interna da empresa, ou ainda para verificar sua situação de crédito, utilizando isso como critério para contratação ou manutenção do contrato de trabalho, essas situações violariam a privacidade do empregado, por utilizarem dados a mais do que os necessários e para finalidades diversas das inicialmente determinadas.

Outros princípios previstos no artigo 6º da LGPD[133] são o princípio da transparência (inciso VI) e o princípio do livre acesso (inciso IV), que conjuntamente revelam a necessidade de que o tratamento de dados seja feito com base na visibilidade dos dados pelo titular, bem como da realização do tratamento de dados e dos agentes de tratamento.

No entanto, diante do uso da IA na relação de emprego, as decisões são tomadas não de maneira explicada ou justificada, já que as decisões automatizadas carecem de muito da transparência que deveria ocorrer enquanto tratamento de dados pessoais. Não à toa que os algoritmos são denominados, muitas vezes, de caixas pretas (*black boxes*),[134] pois, dependendo

---

[132] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: A revolution that will transform how we live, work, and think. Nova York: Houghton Mifflin Harcourt, 2013. p. 5.

[133] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

[134] PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

da metodologia utilizada para o aprendizado de máquina, será praticamente impossível verificar seus critérios ou sua árvore de decisão.

Dessa opacidade do algoritmo surgem diversos questionamentos sobre se eles deveriam, juridicamente, incorporar em suas programações a transparência, ou seja, não apenas permitir que as regras do jogo sejam apresentadas ao titular de dados, mas também que o próprio algoritmo seja construído de maneira explicável.

Claramente, a exigência de transparência sempre que haja o uso de algoritmos de IA protegeria os direitos dos indivíduos. Mas alguns grandes problemas podem surgir desse tipo de pensamento amplo e genérico. Primeiramente, deve-se considerar que o proprietário do algoritmo precisaria mantê-lo em segredo para diferenciar-se de seus concorrentes, pois poderá desenvolver inovação ao ponto de realizar algumas atividades que não sejam executáveis por outros. Assim, como garantir o segredo do negócio, se terá de ser plenamente transparente em relação a seu algoritmo de IA?

Diante desse questionamento retórico, a LGPD flexibilizou o princípio da transparência (o qual já resguarda os segredos comercial e industrial), permitindo que o agente de tratamento que realize decisões automatizadas somente tenha de revelar informações sobre critérios caso seja solicitado pelo titular de dados. E, mesmo assim, poderá recusar-se a prestar maiores detalhes sobre a tecnologia, resguardados pela proteção do segredos comercial e industrial.[135] No entanto, havendo a recusa, a Autoridade Nacional de Proteção de Dados poderá realizar auditoria, buscando exatamente verificar se haverá aspectos discriminatórios naquela decisão automatizada.[136]

Diante da falta de transparência dos algoritmos, Ana Frazão e Carlos Goettenauer apontam alguns riscos dessa falta de transparência, inclusive para aspectos discriminatórios ou equivocados:

> [...] sem a devida transparência, é muito provável que a programação possa estar permeada de vieses e preconceitos dos programadores, intencionais ou não, que podem levar a erros de diagnóstico ou a graves discriminações. Mais do que isso, é

[135] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

[136] Art. 20. [...] § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

> possível que as correlações encontradas no processamento sejam consideradas equivocadamente causalidades, fator que pode reforçar discriminações.[137].

Isso, porque as decisões de muitos desses algoritmos de aprendizado de máquina são tomados com base em correlações, mas são considerados pelo mercado – e pelo empregador, no caso da relação de emprego – como se fossem razões certas de causa e efeito. Mesmo com a falta de correspondência entre as correlações e as causalidades, como explicam Mayer-Schönberger e Cukier, o *Big Data*, grande combustível das decisões tomadas pela IA, promove uma alteração muito relevante na epistemologia, considerando o grande valor da correlação, não para encontrar certezas nos fenômenos sociais, mas para buscar probabilidades e, assim, proporcionar uma tomada de decisão estatisticamente mais próxima do adequado:

> Como seres humanos, fomos condicionados a procurar causas, embora a busca de causalidade seja muitas vezes difícil e possa nos levar a caminhos errados. Em um mundo de big data, por outro lado, não teremos que nos fixar na causalidade; em vez disso, podemos descobrir padrões e correlações nos dados que nos oferecem insights novos e inestimáveis. As correlações podem não nos dizer precisamente por que algo está acontecendo, mas nos alertam de que está acontecendo.[138] (tradução livre).

Essa busca por correlações pode trazer grandes acertos e levar a decisões muito ajustadas, principalmente quando visualizadas a um nível mais amplo, por exemplo quando a Google identificou o aumento de pessoas com doenças gripais nos Estados Unidos apenas pelas buscas realizadas, ou seja, quanto mais pessoas geograficamente localizadas em um determinado local estivessem pesquisando sobre gripe, sintomas ou remédios para gripe, mais provavelmente teria havido um aumento de casos gripais naquele local.[139] No entanto, quando se trata de decisões individuais, a exemplo da contratação de um candidato em processo seletivo ou da demissão de um empregado por atitudes que provavelmente ainda tomará, o risco de uma decisão desse tipo ser tomada injustamente é muito maior, podendo levar a graves violações a direitos fundamentais.

A falta de transparência nessas decisões não permite ao empregado, aos órgãos de controle e fiscalização ou à própria sociedade civil identificar se os critérios utilizados para se chegar naquela decisão estão corretos ou não. Ana Frazão e Carlos Goettenauer apresentam,

---

[137] FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica *In*: BARBOSA, Mafalda Miranda et al. (coord.). **Direito Digital e Inteligência Artificial**: Diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 29.
[138] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: A revolution that will transform how we live, work, and think. Nova York: Houghton Mifflin Harcourt, 2013. p. 14.
[139] Ibid., p. 1-2.

inclusive, que o mínimo de confiabilidade nessas decisões automatizadas somente poderia existir se houvesse informações claras sobre a qualidade dos dados que estão sendo utilizados e a qualidade do processamento desses dados, para que se verifique se os meios pelos quais essas decisões estão sendo tomadas se encaixam nos conceitos de justiça estabelecidos pelo Direito.[140]

Em seu estudo acerca das repercussões da Inteligência Artificial nas relações de emprego, Valerio De Stefano ressalta que o uso de algoritmos para avaliar a performance no trabalho deveria ser acessível para que os critérios de decisão sejam sempre transparentes e permitam aos próprios empregados evitarem ser alvo de decisões arbitrárias ou discriminatórias.[141] No entanto, na relação de emprego, a falta de transparência é maior ainda do que nas demais, já que nela existe maior assimetria informacional entre empregador e empregado, que acentua esses riscos de falta de esclarecimentos para os empregados sobre os critérios e a utilização dessa IA.

Outros princípios que serão destacados, para evidenciar o risco do uso da IA, são os princípios da segurança dos dados (art. 6º, VII), da qualidade dos dados (art. 6º, V), da prevenção (art. 6º, VIII) e da responsabilização e prestação de contas (art. 6º, X).[142] Todos eles fazem referência aos deveres que os agentes de tratamento devem adotar perante um tratamento de dados, minimamente garantindo que os dados sejam mantidos com confidencialidade, integridade e disponibilidade (pilares da segurança da informação) e sempre atualizados e corretos (qualidade dos dados). Além de garantir essa segurança dos dados, deverão os agentes de tratamento demonstrar que o fazem, de maneira preventiva e prestando contas de maneira responsável.

Ao utilizar sistemas de IA na relação com o trabalhador, o empregador acaba por contratar serviços de terceiros, já que as áreas internas ligadas ao RH geralmente não são tão

---

[140] FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica *In*: BARBOSA, Mafalda Miranda et al. (coord.). **Direito Digital e Inteligência Artificial**: Diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 28.

[141] DE STEFANO, Valerio. 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Artificial Intelligence and Labour Protection (May 16, 2018). **Comparative Labor Law & Policy Journal**, v. 41, n. 1, 2019. p. 29.

[142] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

desenvolvidas ao ponto de, internamente, desenvolverem ferramentas próprias de gestão de pessoas.[143] Assim, na contratação de empresas terceiras, as quais comumente são grandes empresas multinacionais, com recursos suficientes para o desenvolvimento dessas ferramentas mais avançadas, existe dificuldade do empregador em cobrar-lhes medidas de segurança adequadas, ou mesmo exigir que demonstrem cabalmente as medidas de segurança dos dados que aplicam nos seus sistemas, para cumprir o que é estabelecido nos princípios da LGPD.

É difícil compreender que um empregador de médio porte conseguiria exigir de empresas como a IBM ou a Microsoft que demonstrem quais as medidas técnicas e administrativas que adotam para a proteção dos dados pessoais, bem como que elas apresentem comprovações de proatividade e de prestação de contas sobre os tratamentos de dados que elas realizam, se elas compartilham esses dados com terceiros ou, mesmo, se reutilizam essas informações para propósitos diversos dos originais.

Trata-se, portanto, de mais um risco para a privacidade do empregado, já que ele confere seus dados pessoais ao empregador, o qual contrata serviços e sistemas de terceiros, os quais receberão esses dados pessoais dos empregados e, eventualmente, compartilharão com servidores espalhados em outros países, buscando formar bases de dados cada vez mais estruturadas e capazes de seus propósitos econômicos. Dificulta-se, portanto, a autodeterminação informativa, ou seja, o controle que o empregado deveria ter sobre o que está acontecendo com seus dados pessoais que foram compartilhados com seu empregador.

Assim, identificados os principais riscos envolvidos quanto à privacidade do empregado, passam-se a analisar os riscos que a adoção desses mecanismos de IA podem gerar diante dos aspectos ligados à igualdade e à não discriminação no ambiente de trabalho.

3.4 Discriminação algorítmica do trabalhador

Reduzir a discriminação nas decisões empresariais geralmente é a justificativa adotada por quem defende o uso de uma IA para auxiliar ou para tomar aquele tipo de decisão. Afinal, decisões empregatícias podem ser muito enviesadas e podem gerar graves situações discriminatórias.

No entanto, de grande objetivo a ser evitado, a discriminação pode ser reforçada e potencializada pelo uso da IA. A utilização da IA para tomada de decisões, notadamente quando se tratando de gestão de pessoas, pode trazer aspectos discriminatórios, por vezes de forma

[143] Vide o que foi abordado na Seção 2.3, *supra*.

consciente, mas também de forma inconsciente. Geralmente, assume-se que a decisão que seja tomada por um mecanismo de IA será mais objetiva do que uma decisão tomada por um ser humano. Essa é a visão que pessoas comumente possuem em seu cotidiano, já que se imagina que uma máquina não terá emoções e, portanto, não decidirá tendendo para favorecer ou prejudicar alguém deliberadamente.

Não se deve considerar, para o propósito do direito à igualdade e à não discriminação, qualquer tipo de desigualdade existente entre os indivíduos. Afinal, decisões que aceitam alguns e rejeitam outros são comuns na sociedade e, inclusive, fazem parte da lógica normal dos seres humanos que vivem em comunidade. Durante um processo seletivo de emprego, será escolhido um dentre vários candidatos, provavelmente aquele mais qualificado para a vaga a ser preenchida, com maiores aptidões para aquelas funções esperadas pelo contratante, deixando os demais candidatos enquanto rejeitados naquela seleção. Não se trata, necessariamente, de uma decisão discriminatória. O critério definidor sobre uma decisão ser ou não discriminatória deve envolver, dentre outros aspectos, os motivos que levaram àquele resultado.

Seguindo nessa linha, Gérson Marques de Lima, em análise detida da igualdade de tratamento nas relações de trabalho, considera que:

> Não há incompatibilidade ou contradição alguma em o Direito reconhecer situações de desigualdade e, ao mesmo tempo, vedar discriminações. Ao contrário, quando ele proíbe as discriminações está reconhecendo a existência de desigualdade (natural ou artificial), pois, assim não fosse, não precisaria estabelecer vedação. De fato, nas situações de igualdade é despicienda norma que a estabeleça. Não é necessário a lei afirmar aquilo que já é.
> É justamente vendo as desigualdades (mormente as artificiais), como fonte de discriminação, que o ordenamento, segundo um juízo axiológico de pertinência, procura revolver o quadro, para restringir ou extirpar as diferenciações injustas, até o limite do tolerável.[144]

Essas situações de discriminação reprovadas pelo Direito são, portanto, aquelas que saem dos contornos da legislação ou que extrapolam o razoável. Isso representa um filtro útil para a identificação daquelas condutas que sejam juridicamente inadequadas, em contraposição a condutas que diferenciem indivíduos, sem que haja necessariamente discriminação.

O direito da proteção de dados pessoais encontra a não discriminação como um de seus princípios, conforme previsto no artigo 6º, inciso IX[145]. Não por acaso inseriu-se na LGPD

---

[144] LIMA, Francisco Gérson Marques. **Igualdade de tratamento nas relações de trabalho**. São Paulo: Malheiros, 1997. p. 45.

[145] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;"

esse princípio, mesmo que a discriminação seja um fenômeno presente em inúmeras relações jurídicas, de formas variadas e por quaisquer tipos de indivíduos. Geralmente a discriminação ocorre quando existe o conhecimento, pelo discriminador, de informações pertencentes ao discriminado. Assim, a proteção dessas informações pertencentes ao potencialmente discriminado possui grande relevância e efetividade quando da proteção em face da discriminação.

Na relação de emprego, a discriminação ocorre de maneira ampla, devendo ser coibida igualmente em todos os campos de ocorrência prática. Principalmente pelo fato de que a relação de emprego existe mediante uma desigualdade patente entre empregador e empregado, legitimado mediante o poder diretivo do empregador e, complementando-o, a subordinação do empregado à direção a ele determinada. Outro ponto que levanta maior atenção a esse aspecto na relação de emprego é a assimetria informacional patente entre as partes nessa relação, já que mesmo que uma decisão seja tomada com base em critérios discriminatórios, será difícil ao empregado entender quais motivações foram essas e, mais difícil ainda, recorrer desse julgamento discriminatório pelo empregador.

Tão relevante é esse tema da não discriminação na relação de emprego que, ainda em meados da década de 90, foi sancionada a lei nº 9.029/95, que dispõe em seu artigo 1º a proibição de "qualquer prática" discriminatória e limitativa, para acesso ou manutenção na relação de trabalho.[146] Gérson Marques de Lima, ao comentar sobre a amplitude da expressão "qualquer prática", acrescenta:

> Como a lei vem atender a escopo constitucional, insculpido na parte referente aos direitos fundamentais, ela há de ser interpretado extensivamente, e o preceito há de alcançar as formas mais inimagináveis possíveis de atitudes que importem *discrímen* em razão do sexo, da raça, do estado civil, da situação familiar e da idade. E isto de modo a abranger os vários estágios do contrato de emprego, vale dizer, tanto a fase pré-contratual (ou admissional), como a contratual propriamente dita (aquela insurgente no curso da relação empregatícia), bem ainda a fase dispensatório (aquela expurgada no momento da ruptura contratual).[147].

Portanto, ao analisar aspectos discriminatórios, deve-se ter em atenção todos os tipos de decisões empregatícias, desde a fase pré-contratual até o término do contrato e mesmo

---

[146] Art. 1º É proibida a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, reabilitação profissional, idade, entre outros, ressalvadas, nesse caso, as hipóteses de proteção à criança e ao adolescente previstas no inciso XXXIII do art. 7º da Constituição Federal.

[147] LIMA, Francisco Gérson Marques. **Igualdade de tratamento nas relações de trabalho**. São Paulo: Malheiros, 1997. p. 29-30.

após esse período, enquanto houver dados pessoais do ex-empregado registradas perante o ex-empregador.

Quando se trata da discriminação gerada por algoritmos de IA, é necessário ressaltar que uma decisão tomada por um ser humano pode ser enviesada, tanto implícita quanto dolosamente. No entanto, o julgamento por uma máquina dificilmente conterá o dolo em discriminar, por evidente ausência de consciência da máquina, restando a discussão sobre o eventual dolo do programador.

Reforçando essa ideia, Laura Mendes e Marcela Mattiuzzo consideram que, realmente, os seres humanos são tendenciosos, ao passo que o uso de algoritmos de IA, por exemplo no recrutamento de novos empregados, poderia reduzir os vieses discriminatórios. Contudo, diversos efeitos adversos da utilização exclusiva dessa tecnologia poderiam ocorrer, já que, mesmo racionalizando os critérios pretendidos pela empresa, poderia considerar que os candidatos "fora do padrão" não desempenhariam tão bem determinadas atividades, haja vista que suas capacidades seriam outras, diferentes dos demais colegas de setor.[148]

Para o pretendido estudo, é necessário o entendimento de que os dispositivos de Inteligência Artificial – utilizando métodos de tomada de decisões baseadas em algoritmos, ou seja, em cálculos matemáticos – foram pretensamente desenvolvidos para facilitar as tomadas de decisões, pois evitariam o caráter enviesado que a atuação humana poderia ter, baseada nas preferências e opiniões de cada indivíduo.

Esses sistemas automatizados poderiam, por exemplo, facilitar a contratação ou demissão de um empregado sem que isso fosse feito a partir de uma impressão, opinião ou preconceito do empregador. Porém, apesar de terem sido popularizados como provedores de decisões racionais e objetivas, sem vieses, são desenvolvidos por seres humanos, os quais inserem critérios e regras de decisão para seu funcionamento.[149]

Dessa forma, tais critérios podem estar imbuídos das preferências e das opiniões de seus desenvolvedores, o que tornaria o algoritmo – pretensamente neutro – em uma replicação de um posicionamento humano. Vale destacar, aqui, que mesmo que se sustente a possibilidade de criação de uma Inteligência Artificial sem critérios influenciados pelas opiniões de seus desenvolvedores, ainda assim a própria máquina pode levar a decisões que gerem algum tipo de discriminação, pois elas têm como base padrões historicamente construídos e a presunção

---

[148] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 46.
[149] PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

de que eles se repetirão.[150] Em outras palavras, "os algoritmos poderiam absorver padrões discriminatórios presentes na sociedade e replicá-los como uma verdade objetiva".[151]

Isso se dá, muitas vezes, corroborando um adágio popular entre os programadores e desenvolvedores, que é o "*garbage in, garbage out*", que, traduzido livre e literalmente, quer dizer que quando entra lixo, também sai lixo. Essa célebre frase expressa uma lógica de que, caso os dados analisados pelo algoritmo sejam errados, ou até mesmo enviesados ou discriminatórios, os dados que resultarão desse tratamento serão igualmente errados, enviesados ou discriminatórios.[152]

Essa situação é o que se denomina de discriminação algorítmica, fenômeno do qual derivam diversas discussões acadêmicas, voltadas principalmente ao estudo dos conflitos éticos da IA, dos parâmetros de regulação apropriados e de medidas para resguardar a proteção dos dados pessoais.

Diversos casos de discriminação gerada por algoritmos ocorrem, sendo que nem todos acontecem de maneira uniforme, tanto que uns são causados por fatores diversos dos outros, ou então geram impactos de maneiras diferentes, razão pela qual a doutrina elaborou a tipologia da discriminação algorítmica, sendo sistematizada por Laura Mendes e Marcela Mattiuzzo em quatro principais tipos.

O primeiro tipo de discriminação algorítmica seria aquele gerado por um erro estatístico.[153] Assim, ocorre quando há algum erro de contabilização dos dados disponíveis, seja pela incorreção na base de dados, por exemplo dados incorretamente coletados, seja por problemas no código do algoritmo. Nessa situação, o erro decorre da programação que teria sido mal calibrada, fugindo de seu propósito pretendido.

As autoras ilustram esse tipo diante da grande quantidade de erros que ocorrem nos casos de identificação de *score* de crédito nos Estados Unidos, baseadas em parecer formulado pela FTC (*Federal Trade Commission*) ao Congresso daquele país, apresentando uma margem de erro entre 10% e 21%, dependendo da natureza do erro.[154]

O segundo tipo de discriminação por algoritmo é aquele gerado por uma generalização,[155] ou seja, todas as variáveis estão matematicamente corretas, mas por algum

---

[150] O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016. p. 38.
[151] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 41.
[152] BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, p. 671-732, 2016. p. 683-684.
[153] Ibid., p. 51-52.
[154] Ibid., p. 53.
[155] Ibid., p. 52.

motivo o indivíduo é relacionado automaticamente a um grupo de outros indivíduos, a partir do que o algoritmo entende que ele possui as mesmas categorias do grupo no qual está inserido. Assim, a generalização ocorre quando é retirada a individualidade das características de uma pessoa, passando ela a ser analisada como um todo em seu grupo estatístico.

É certo que todo modelo é uma generalização e que nem toda generalização gera algum tipo de prejuízo. No entanto, há de se considerar os casos em que a generalização possa afetar os direitos dos titulares de dados. Por exemplo, se o indivíduo possui boas condições financeiras, mas reside em um local em que a maioria das pessoas não o possuem, poderá ele (pela análise do seu CEP) ter algum tipo de prejuízo, diante da generalização feita com base nos dados possuídos pelos demais indivíduos do grupo.[156]

Um terceiro tipo de discriminação diz respeito àquelas hipóteses em que, para que o algoritmo chegue a uma conclusão, deverá haver o tratamento de dados pessoais sensíveis do indivíduo.[157] A Lei Geral de Proteção de Dados (LGPD) classifica como dados pessoais sensíveis aqueles que expressam diretamente as informações mais íntimas do ser humano, por exemplo dados relativos a origem racial ou étnica, convicção religiosa, preferência política, filiação a sindicato, referentes à saúde ou biométricos.[158]

Poder-se-ia questionar por que tais decisões podem levar a discriminação, mesmo que não haja risco aparente. Ocorre que esses dados sensíveis, além de serem mais protegidos pela lei, podem ser mascarados por outras informações (*proxies*) que vão indicar os dados sensíveis do indivíduo sem que ele saiba desse tratamento. Nesse sentido, grupos que são historicamente marginalizados (negros, mulheres, alguns grupos religiosos) podem permanecer marginalizados pelo uso de informações que mascararam o tratamento de dados sensíveis.[159]

O quarto tipo de discriminação por algoritmo é aquele em que há limitação de direitos.[160] Nesse caso, todos os cálculos estatísticos podem estar corretos, mas seu resultado será a limitação de um direito previamente estabelecido. Essa limitação não precisa ser ativa, pode ser também passiva.

Um exemplo apresentado pelas autoras ocorreu na Alemanha, quando os *bureaus* de crédito disponibilizavam uma ferramenta de consulta ao *score* de crédito dos cidadãos, sendo

---

[156] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 52-53.
[157] Ibid., p. 52.
[158] Art. 5º Para os fins desta Lei, considera-se: [...]
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
[159] MENDES; MATTIUZZO, op. cit., p. 54.
[160] Ibid., p. 52-53.

que aqueles que buscavam saber mais vezes o seu *score*, consultando à própria empresa, tinham sua nota de crédito reduzida, pois seria considerada uma atitude típica de um indivíduo que não possui condições financeiras saudáveis. Na prática, os indivíduos tinham limitado seu direito de acessar sua nota de crédito, pois poderiam sofrer consequências discriminatórias pelo algoritmo – redução da sua pontuação de crédito.[161]

Diante dessa tipologia, fica claro que a discriminação não ocorre apenas porque o programador inseriu conscientemente algum viés discriminatório naquela aplicação de IA. Além disso, mesmo que uma empresa utilize um mecanismo de IA que produz discriminação, não necessariamente esse efeito será intencional, pois é muito comum que seja resultado de um dos tipos citados, alguma falha nos dados que foram processados pelo algoritmo; algum erro de programação; alguma generalização automaticamente realizada que desconsidere outros aspectos; algum tratamento de dados sensíveis de maneira mascarada, ou limitando algum direito do indivíduo.

Por outro lado, a falha ocasionada pela máquina não quer dizer que não haja responsabilidades ou mesmo salvaguardas que devam ser adotadas pelas empresas. Em realidade, quando há a utilização de alguma dessas tecnologias, deverá haver bastante cuidado e respeito a medidas de proteção da pessoa titular dos dados, garantindo que haja a devida diversificação nos critérios utilizados, a transparência desses critérios, além de uma periódica revisão dos resultados gerados pelos algoritmos.

O uso de tecnologias baseadas em IA, com a finalidade de análise de uma enorme quantidade de dados (*Big Data*), gera riscos à qualidade dessas análises, já que os resultados de decisões algorítmicas nem sempre reproduzem a realidade como ela é, pois, como ressalta Hugo de Bruto Machado Segundo, apesar de serem coletados a partir do mundo fenomênico, são apenas fragmentos dessa realidade, existindo no mundo numênico, o que lhes traz características como parcialidade, precariedade e falibilidade, não podendo ser entendida como uma decisão certa e inteiramente real.[162]

Juridicamente, há diversas implicações relevantes que advêm da utilização de mecanismos de IA, principalmente quanto à transparência de seus critérios, haja vista a grande variedade de casos concretos em que se pôde verificar a ocorrência de discriminação algorítmica. Essas repercussões jurídicas serão, a seguir, abordadas.

---

[161] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 54-55.
[162] MACHADO SEGUNDO, Hugo de Brito. **Direito e Inteligência Artificial**: O que os Algoritmos têm a Ensinar sobre Interpretação, Valores e Justiça. São Paulo: Editora Foco, 2022. p. 9.

A literatura, nacional e internacional, apresenta diversos exemplos de discriminação gerada pelo uso de algoritmos de IA. Um dos exemplos apresentados por Cathy O'Neil[163] é o do IMPACT, sistema baseado em algoritmo de avaliação de professores, que foi utilizado pelas escolas públicas de Washington, D.C. Esse sistema avaliava os professores de acordo com critérios que incluíam as notas dos alunos em testes ao final de cada ano escolar. Os resultados desse algoritmo geravam uma nota para os professores, os quais seriam dispensados caso tivessem uma nota baixa. Afinal, a intenção da escola era que o professor gerasse bons resultados nas notas de seus alunos.

Ocorre que, após diversos casos de descontentamento de professores, passou-se a investigar o algoritmo e percebeu-se que ele estava incentivando os professores a diminuírem o rigor em seus testes, já que isso provavelmente poderia impactar em sua continuidade no emprego. Um outro resultado notado foi que aqueles que não adotavam tais práticas acabavam sendo dispensados, pois a nota parecia refletir, de algum modo, as notas dos alunos.

O ponto que mais chama a atenção é que, quando um professor se sentia injustiçado, como foi o caso da professora Sarah Bax, não haveria a quem recorrer. No caso dela, após questionar a um superior, ficou sem resposta sobre uma pergunta simples: qual critério foi utilizado para a elaboração daquela nota. Após tentativas frustradas buscando que técnicos esclarecessem esses critérios, outro questionamento foi elaborado pela autora: como é possível recorrer de uma decisão cujo critério ninguém tem conhecimento?[164]

Outro caso também citado reflete mais diretamente como os algoritmos podem ser discriminatórios, além de não serem transparentes. A autora relata o caso de Kyle Behm, um jovem estadunidense que teve problemas em ser admitido em algumas seleções de emprego. Ele não conseguia entender o motivo dessas reprovações, se todas as suas notas nos exames SAT (algo como o vestibular brasileiro) eram elevadas. Ao reparar bem nos testes de personalidade em que ele participava nessas seleções, percebeu que se pareciam demais com um exame que havia feito, o qual o diagnosticou com transtorno bipolar.

Depois que descobriu que provavelmente estava sendo recusado em oportunidades de emprego por causa de sua condição, ajuizou ações contra sete empresas pelo uso desse teste e contra a sua desenvolvedora, a empresa Kronos, por considerá-la responsável pela sua dificuldade de recolocação em emprego.[165]

---

[163] O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016.
[164] Ibid., p. 8.
[165] Ibid., p. 105-107.

Esses exemplos demonstram que alguns critérios utilizados em processos de automação, quando se utilizam mecanismos de IA, podem ser utilizados para buscar menores tendências pessoais ou reduzir vieses, porém esses próprios algoritmos de IA podem perpetuar discriminação baseada em vieses.

Esse tipo de situação ocorre, principalmente, pois os dispositivos de IA são tendencialmente obscuros, sem critérios de transparência que demonstrem os motivos de se chegar àquela decisão específica. Regra geral, algoritmos de aprendizado de máquina (*machine learning*) possuem essa dificuldade, pois o algoritmo passa a aprender com a própria prática decisória dele e com os dados a que é submetido. No entanto, essa base de dados pode estar enviesada.

A opacidade desses algoritmos é uma grande barreira à verificação da ocorrência de discriminação algorítmica. Segundo Danilo Doneda e Virgílio Almeida, a obscuridade do processo decisório do algoritmo é um grande problema para toda a sociedade, principalmente para as autoridades reguladoras, pois a verificação de uma possível discriminação somente será realizada se for possível saber qual o *input* ou qual o método estatístico utilizado.[166]

Ressalta-se, inclusive, a previsão do princípio da transparência na LGPD, que exige das empresas a apresentação de informações claras, precisas e acessíveis quanto tratamento de dados, inclusive automatizado. Mas o debate gira não apenas sobre a possibilidade jurídica de transparência, também quanto à possibilidade técnica, pois é discutível a transparência plena dos critérios de um algoritmo de IA.

Para Laura Mendes e Marcela Mattiuzzo, o algoritmo sendo obscuro tornaria bastante difícil verificar eventual discriminação que tenha ocorrido, sendo complicado também antecipar-se a possíveis discriminações.[167]

Kroll e colaboradores asseveram que a transparência não seria tão efetiva quanto aparenta ser, tendo em vista que poderá ser inatingível juridicamente, seja em razão de algum argumento de ordem pública, seja por razões privadas, bem como porque saber os métodos que foram adotados não seria suficiente se o algoritmo já não tivesse sido construído para permitir sua prestação de contas. Além disso, as aleatoriedades criadas pela IA seriam imprevisíveis em algumas metodologias, ainda mais quando se utiliza o *machine learning*.[168]

---

[166] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What is algorithm governance? **IEEE Internet Computing**, v. 20, n. 4, p. 60-63, 2016. p. 6.
[167] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. p. 47.
[168] KROLL, Joshua A. et al. Accountable algorithms. **University of Pennsylvania Law Review**, v. 165, p. 633-705, 2017. p. 633.

Assim, mais do que exigir transparência, os autores sustentam que a prestação de contas (em inglês, *accountability*) poderia ser uma forma de garantir que a própria empresa deixe registrado seu tratamento de dados, para posterior auditoria ou verificação.[169]

Diante dos tipos de discriminação algorítmica e dos riscos gerados por eles, o princípio da não discriminação, entabulado no artigo 6º da LGPD, dispõe ser proibido o tratamento de dados para fins discriminatórios ilícitos ou abusivos. Um destaque inicial é que, enquanto a lei nº 9.025/95 trata de proibir práticas discriminatórias que tenham determinados motivos (com uma lista exemplificativa e específica), a LGPD determina dois critérios apenas, ambos com um caráter mais genérico e baseados na finalidade do tratamento dos dados pessoais.

Em outro artigo científico, Laura Mendes, Marcela Mattiuzzo e Mônica Fujimoto explicitam o significado e as implicações desses termos (discriminação ilícita e abusiva) na LGPD. Para as autoras, a LGPD traz um avanço na tutela da não discriminação, pois apresenta dois tipos de discriminação que, baseados no tratamento de dados, são recriminados.[170] No artigo 6º, inciso IX, da LGPD, é apresentado o princípio da não discriminação, caracterizando-se pela impossibilidade de realização do tratamento de dados pessoais para fins ilícitos ou abusivos.

A lei, portanto, estabelece critérios finalísticos, ou seja, o que importa para definir a conduta como discriminatória e inaceitável é sua finalidade. A discriminação ilícita, segundo as autoras, seria aquela que já possui vedações legais expressamente direcionadas a determinada conduta, portanto independe de qualquer critério quanto à sua relevância ou quanto a algum erro estatístico que possa ter ocorrido.[171]

Diversos podem ser os exemplos de discriminação ilícita, especialmente na relação de emprego. No caso hipotético referido por Jon Kleinberg e colaboradores, de um empregador que tenha aplicado um algoritmo para selecionar seus vendedores e o referido algoritmo, ao analisar os dados dos atuais vendedores e seus resultados, conclui que os clientes compram mais produtos a partir de vendedores brancos, em comparação com vendedores negros.[172] Caso esse empregador utilizasse esse critério para a seleção de novos vendedores, estaria cometendo

---

[169] KROLL, Joshua A. et al. Accountable algorithms. **University of Pennsylvania Law Review**, v. 165, p. 633-705, 2017.
[170] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. *In*: DONEDA, Danilo et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.
[171] Ibid., p. 432.
[172] KLEINBERG, Jon et al. Discrimination in the Age of Algorithms. **Journal of Legal Analysis**, v. 10, p. 113-174, 2018. p. 148-149.

discriminação algorítmica por generalização ilícita, pois desrespeitou o disposto nos artigos 1º cominado com o artigo 4º da lei nº 7.716/89[173][174].

Na hipótese citada, a discriminação ocorreu e foi considerada pelo fato de existir previsão legal expressa vedando a conduta de negar uma vaga de emprego com base em raça ou cor. Segundo concluem as autoras, quanto à discriminação ilícita:

> [...] a lógica de tal proteção é evitar que a discriminação limite direitos básicos como acesso ao trabalho, saúde, educação, transporte, convívio social e exercício da cidadania, exatamente por uma compreensão do legislador de que tais direitos são de particular relevância para todos os indivíduos e que determinados grupos são negativa e desproporcionalmente afetados quando comparado a outros grupos.[175]

Já a discriminação abusiva não representa, diretamente, o descumprimento a um preceito legal que veda conduta discriminatória específica. Em verdade, a conduta aparentemente é lícita, mas seus efeitos produzem algum tipo de discriminação, que igualmente não é aceita pelo ordenamento jurídico, não por expressa vedação legal, mas por violação ao princípio da igualdade.

Para Bandeira de Mello, "por via do princípio da igualdade, o que a ordem jurídica pretende firmar é a impossibilidade de desequiparações fortuitas ou injustificadas".[176] Dessa forma, aquelas decisões que diferenciam indivíduos de maneira fortuita ou sem qualquer justificação razoável deverão igualmente ser recriminadas, juntamente com aquelas expressamente vedadas na legislação.

O referido autor propõe critérios para aferição de quais condutas que implicam em diferenciação não poderão ser admitidas, em razão da quebra da isonomia.[177] Primeiro, identificar qual foi o fator de diferenciação. Em seguida, analisar se há uma correlação lógica e racional para o critério adotado como fator diferenciador. Por fim, confrontar essa correlação lógica com os valores e interesses absorvidos no sistema constitucional e jurisprudencial.

Assim, esse teste de isonomia proposto por Bandeira de Mello demonstra que deve ser utilizado o critério da razoabilidade a partir do motivo que levou àquela diferenciação,

---

[173] Lei nº 7.716/89: Art. 1º Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. [...] Art. 4º Negar ou obstar emprego em empresa privada. Pena: reclusão de dois a cinco anos.

[174] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. *In*: DONEDA, Danilo et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 434.

[175] Ibid., p. 435.

[176] BANDEIRA DE MELLO, Celso Antônio. **Conteúdo jurídico do princípio da igualdade**. São Paulo: Malheiros, 3. ed., 8ª Tiragem, 2008. p. 18.

[177] Ibid., p. 21.

cotejando com os valores fundamentais existentes no ordenamento jurídico vigente. Caso seja verificado que a conduta em análise procedeu com diferenciação com base em critério que vai de encontro aos preceitos constitucionais, legais e jurisprudenciais, estar-se-á diante de uma discriminação abusiva.

Gérson Marques de Lima[178] contribui com a discussão considerando que atitudes como essas podem igualmente ser caracterizadas como abuso de direito. Segundo esse autor, mesmo que haja um direito de diferencias as pessoas, por exemplo, quando o empregador decide por contratar aquele indivíduo que mais lhe pareça adequado ao trabalho, não poderia utilizar-se dessa faculdade para imprimir uma discriminação persecutória ou a título de revanche.

Diante desse cenário, em que a discriminação abusiva é identificada quando o critério utilizado como motivo para a diferenciação vai de encontro a valores jurídicos, essa aferição pode encontrar dificuldades ainda maiores quando se trata de uma decisão algorítmica.[179]

Como já ressaltado, esses algoritmos de IA, principalmente aqueles que utilizam metodologias baseadas em aprendizado de máquina (*Machine Learning*) ou aprendizado profundo (*Deep Learning*) produzem resultados de forma semiautônoma, com pouca interferência humana na valoração dos critérios que são aplicados para chegar a uma conclusão. As decisões tomadas por esses algoritmos são baseadas em cálculos matemáticos, derivados de operações de 1 (um) e 0 (zero), não em valores humanos de igualdade ou isonomia.

A dificuldade de se identificar esses resultados nas decisões algorítmicas é um desafio para o Direito, já que qualquer decisão deve ser passível de clarificação e de revisão pelo indivíduo que está sendo julgado. A título de exemplo, em um processo seletivo de emprego que seja realizado com uso de ferramentas de IA para triagem de candidatos para determinada vaga, ao ser recusado para a vaga, o candidato não necessariamente terá indicados os critérios que foram relevantes para sua reprovação. Poderá ter sido alguma incompatibilidade física ou motora, a exemplo da vaga de emprego se destinada a um motorista no caso em que o candidato possuía algum tipo de condição que lhe impedia de exercer essa atividade. No entanto, revisitando o caso Kyle Behm,[180] o candidato pode ter sido reprovado para uma vaga

---

[178] LIMA, Francisco Gérson Marques. **Igualdade de tratamento nas relações de trabalho**. São Paulo: Malheiros, 1997. p. 31.

[179] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. *In*: DONEDA, Danilo et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 435.

[180] O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016.

de emprego como vendedor de loja pois seu perfil comportamental, criado pela IA, pode ter traços de transtorno bipolar, condição esta que não lhe impossibilitaria de exercer a profissão, podendo ser considerada uma discriminação algorítmica abusiva.

Diante desses riscos envolvendo a aplicação da IA nas relações de emprego, seja na fase pré-contratual, seja durante a vigência do contrato de trabalho, bem como na extinção dessa relação, cabe verificar de que maneira a legislação adota mecanismos protetivos aos trabalhadores, para evitar ou mitigar os riscos apontados, ainda que não haja expressamente regulamentação brasileira quanto ao tema da Inteligência Artificial na relação de emprego.

4 REQUISITOS LEGAIS E BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS PARA UTILIZAÇÃO DA INTELIGÊNCIA AARTIFICIAL NAS RELAÇÕES DE EMPREGO

Diante dos riscos envolvendo a aplicação de mecanismos de IA pelo empregador, surgem instrumentos para limitar o seu poder, dentre eles o mais importante sendo o direito fundamental à proteção de dados pessoais do empregado.

No presente capítulo, então, serão abordados os aspectos relacionados à proteção de dados pessoais mesmo antes da LGPD, tendo em vista que a prévia existência de disposições sobre privacidade e intimidade na própria Constituição Federal – uma vez que, inclusive, foi reconhecido pelo STF um direito fundamental à autodeterminação informativa. Na legislação trabalhista, contudo, quase nenhuma referência ao tema havia, apesar de decisões do TST já versando sobre proteção da privacidade do empregado; e no Marco Civil da Internet, no qual já se falava de proteção da privacidade, com medidas concretas vinculadas ao uso da internet, e de proteção de dados pessoais, deixando para lei específica regular esse ponto. Após identificar-se como se constituía o referido direito à proteção de dados pessoais do empregado antes da LGPD, passar-se-á a analisar quais os requisitos legais previstos na LGPD que tocam ao uso da IA pelo empregador. Por fim, serão apresentadas diretrizes de boas práticas que vão além da previsão legal, mas que podem contribuir com a conformidade empresarial quanto à proteção de dados pessoais do empregado diante do uso da IA pelo empregador.

4.1 Primórdios do direito fundamental à proteção de dados pessoais na relação de emprego

A LGPD foi um grande marco na proteção desse direito no Brasil, trazendo princípios basilares, requisitos legais a partir dos quais seja possível efetuar o tratamento de dados pessoais, deveres e responsabilidades para aqueles que executem esse tratamento, além de sanções decorrentes do descumprimento legal. No entanto, antes mesmo de sua aprovação, em 2018, o ordenamento jurídico brasileiro já possuía estruturas jurídico-legais que garantiam diversas proteções, ainda que parciais, ao direito à proteção de dados pessoais. Tanto que diversas contendas entre empregador e empregado já se resolviam perante os tribunais trabalhistas – e mesmo no STF –, girando em torno do direito à intimidade, à reserva da vida

privada, ao sigilo das correspondências e, em última argumentação, à dignidade da pessoa humana.

Por tais motivos, a seguir serão apresentados alguns pontos anteriores à LGPD, os quais já garantiam alguma proteção ao empregado, mesmo que não com todos os detalhes e com toda a extensão que fez a referida lei. Em seguida, analisar-se-ão especificamente as previsões existentes na referida lei que toquem mais diretamente no uso da IA pelo empregador para que, nos dois últimos tópicos, sejam discutidas a proposta de regulamentação da IA ainda em trâmite perante o Congresso Nacional, e a estrutura de *enfforcement* quanto à auditabilidade da IA na relação de emprego.

4.1.1 Constituição Federal

O rol dos direitos fundamentais, previsto no artigo 5º da Constituição Federal de 1988, preceitua a inviolabilidade da intimidade e da vida privada (inciso X) e do sigilo de dados (inciso XII). Da maneira como previsto no texto constitucional, o texto da norma expressa que ninguém poderá violar a intimidade ou a vida privada de outrem, proteção essa que também se estende ao sigilo de dados.

A realidade social e econômica acompanhando o restante do mundo, modificou-se radicalmente desde a promulgação da Constituição Federal, principalmente com a proeminência de tecnologias que conectam indivíduos de diversos lugares simultaneamente, por vezes com o uso de um simples celular.

A intimidade e a privacidade, na sua concepção original, apresentam-se como direitos de status negativo, impondo a abstenção de alguém em invadir a intimidade ou vida privada de terceiros. Essa dimensão revela-se incompatível com a atual realidade tecnológica, em que se deve considerar um direito à proteção de dados, de natureza positiva, que exige a proposição de medidas aptas a proteger aquelas informações que deixarem de ser privadas, além de conter um aspecto procedimental, por meio da criação de mecanismos institucionais com o objetivo de concretizar o referido direito, seja na via administrativa seja na judicial.

Quanto ao indivíduo em sua relação de emprego, igualmente se deve promover a proteção de dados, não mais apenas a intimidade ou a privacidade clássica, diante de suas peculiaridades e fragilidades. Isso, porque o poder de controle eletrônico exercido pelo empregador, que se vale de meios tecnológicos para tanto, torna-se muito mais efetivo do que o tradicional, porém muito mais intrusivo e que demanda por grandes quantidades de informações do empregado.

A proteção do direito à intimidade e do direito à privacidade, notadamente do empregado, mostram-se insuficientes para a ressignificação do poder de controle pelo empregador, devendo-se promover a proteção de dados, de maneira ativa, do empregado. Não que se desconsidere totalmente a noção clássica de privacidade, já que o valor da vida privada merece ainda o respeito e a proteção pelo Direito, principalmente quando se fala em relação de emprego, já que o empregado é fiscalizado pelo seu empregador durante o trabalho, mas deve ter reservada sua vida privada do poder de controle dele, uma vez que os aspectos íntimos da vida do empregado não importam para a boa execução do empreendimento do empregador.

Cada vez mais se torna difícil não estar sujeito a um tratamento de dados, já que a sociedade da informação demanda que toda e qualquer atitude seja baseada nessas operações, o que limita sobremaneira um direito de status negativo.

O direito à intimidade teve sua origem bastante ligada ao direito à propriedade, no contexto da criação dos Estados modernos, em que se intensificavam as hierarquias e os nobres passavam a priorizar suas propriedades separadas dos demais. Nessas situações, passou-se a ter maior interesse pela separação do nobre em seus momentos de sono, refeições, rituais religiosos e sociais, bem como de reflexão ou pensamento.[181]

Sandra Lia Simón apresenta o histórico desse direito, para então conectá-lo à relação de emprego, apontando que "a vida privada aparece, portanto, como um direito à solidão, à reserva, ao isolamento".[182]

A privacidade clássica constitui-se, assim, como uma faculdade pertencente às classes mais privilegiadas, que possuem a capacidade de separar-se dos demais para atingir determinados momentos sozinhos, sem a interferência de terceiros. Essas situações são possíveis, sobretudo, pelas mudanças de estruturas causadas pela Revolução Industrial,[183] momento em que também surgem as preocupações sobre os direitos trabalhistas.

No entanto, o direito à privacidade apenas passou a ter sua teorização na doutrina jurídica com o ensaio produzido por Samuel Warren e Louis Brandeis, em 1890. Nesse estudo, os autores buscam identificar, na análise das decisões dos tribunais ingleses e norte-americanos, um direito autônomo à privacidade, concebida na forma de um direito de estar só (*right to be let alone*).[184]

---

[181] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar. 2008. p. 26.
[182] SIMÓN, Sandra Lia. **A proteção constitucional da intimidade e da vida privada do empregado**. São Paulo: LTr, 2000. p. 71.
[183] RODOTÀ, op. cit., p. 26.
[184] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

Nessa concepção do direito, bastante característica do Estado Liberal, em que os indivíduos apenas precisariam ser resguardados de arbítrios quanto à sua esfera individual, nota-se que não há proteção para os casos em que o indivíduo efetivamente consente em não estar sozinho. Afinal, se o consentimento serviria para resguardar o direito à intimidade e à vida privada, estando em uma situação de compartilhamento de informações com terceiros, não teria mais o direito à sua privacidade.

Por isso, surge uma nova concepção de direitos ligados à privacidade, remodelada de acordo com a evolução de tratamento de dados pessoais, em um contexto em que o indivíduo compartilha suas informações com terceiros.

Nessa perspectiva, deve-se resguardar a privacidade do indivíduo não apenas até a sua permissão para tratamento dos dados, mas, durante o referido tratamento, haverá de ser resguardado ao indivíduo o controle, o acompanhamento e a informação sobre o que está acontecendo com eles. Seria, assim, necessário considerar a privacidade como um status positivo, em que o indivíduo consiga ter um controle ativo sobre o fluxo dessas suas informações.[185]

Essa visão foi corroborada por Danilo Doneda, que apresentou um apanhado histórico da evolução das normas de privacidade, principalmente no âmbito europeu, onde essa dimensão da privacidade ficou conhecida como autodeterminação informativa (ou informacional). Essa dimensão da privacidade mostrou-se capaz de proteger os dados também após seu compartilhamento com terceiros, principalmente na garantia do controle dos dados. Nesse sentido, afirma o autor que:

> A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração [...]. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.[186].

Essa atualização do entendimento, do que seria considerado privacidade, trouxe diversas implicações, notadamente porque os mecanismos existentes até então apenas protegiam o indivíduo de ações que invadissem sua esfera individual, mas não permitiam que

---

[185] COPETTI, Rafael; MIRANDA, Marcel Andreata de. Autodeterminação informativa e proteção de dados: uma análise crítica da jurisprudência brasileira. **Revista de Direito, Governança e Novas Tecnologias**, v. 1, n. 2, p. 28–48, 2015. p. 32.

[186] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

o cidadão tivesse a capacidade de acompanhar o que estaria ocorrendo com suas informações, se estariam sendo compartilhadas com terceiros ou, ainda, se estariam sendo utilizadas com finalidades ilícitas.

O direito à autodeterminação informativa, enquanto dimensão da privacidade, traz aspectos relevantes para o debate das relações jurídicas, haja vista que permite o acompanhamento e a fiscalização dos agentes de tratamento de dados – sejam particulares, sejam entes públicos. O indivíduo poderia, assim, utilizar-se de seus próprios meios para requisitar acesso a suas informações, buscar explicações acerca do uso de seus dados, bem como fiscalizar diretamente aqueles a quem seus dados foram compartilhados.

Ainda assim, percebe-se que a esfera de proteção da autodeterminação informativa é limitada ao âmbito individual, ainda com resquícios da primeira fase histórica, em que a privacidade estaria intimamente ligada à esfera do indivíduo, que teria de buscar meios próprios para exercer seus direitos. O questionamento que se fazia a doutrina é que aqueles indivíduos que não tinham condições de exercer seus direitos de privacidade, ou ainda aqueles que sequer sabiam da existência desse direito ou da necessidade de garanti-lo, ficariam à mercê da boa vontade dos agentes de tratamento,[187] já que lhes faltaria uma proteção mais ostensiva, saindo da esfera privada.

Com isso, a privacidade não estaria satisfatoriamente protegida enquanto não fosse acessível a todos, principalmente àqueles que não teriam acesso facilitado a seus dados, a exemplo do empregado, que fornece dados pessoais para tratamento por seu empregador, mas que, por diversos fatores, incluindo-se a subordinação, ficaria sem muitos mecanismos aptos a fiscalizar o bom uso deles.

Diante dessa necessidade, surge na doutrina mais uma fase do direito à privacidade, que avança além da esfera individual e parte para a proteção coletiva. Além disso, essa nova fase garante mecanismos procedimentais para a efetivação da privacidade, não apenas indicando o direito, mas também proporcionando estruturas de concretização. Trata-se da proteção de dados pessoais, dimensão da privacidade que não dispensa as fases anteriores, mas que eleva o padrão coletivo de proteção.[188]

---

[187] Segundo o artigo 5º, IX da LGPD, são agentes de tratamento o controlador e o operador de dados. Esses termos são explicitados nos incisos VI e VII do mesmo artigo: "VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; "VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador";

[188] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011. p. 98.

Essa nova ideia de proteção da privacidade – não mais baseada na vida privada ou na intimidade, não se limitando à esfera individual, mas focando principalmente nos dados pessoais (enquanto elementos a partir dos quais o indivíduo constrói e expressa sua personalidade) – traz diversos avanços protetivos. O foco nos dados pessoais é a grande reviravolta de entendimento, já que permite a rastreabilidade das condutas dos agentes de tratamento, assim como tornam mais objetiva a proteção, saindo de conceitos mais abstratos como a vida privada e a intimidade, e passando para um conceito objetivo, o de dados pessoais.

O acréscimo de medidas garantidoras desse direito, inclusive de iniciativa estatal, também demonstra um grande avanço protetivo nesse sentido. O Estado, que antes era considerado o possível violador da intimidade e da vida privada, passou a ser considerado um garantidor desses direitos, responsável até mesmo pela fiscalização e pela normatização dos limites de tratamento de dados, resguardando ativamente a privacidade dos indivíduos e da coletividade.

Resumindo o que caracteriza a fase da proteção de dados, Laura Mendes explica o seguinte:

> Quanto aos efeitos gerados por essa proteção, alinhando-a ao conceito de autodeterminação informativa, é possível pensá-los a partir de uma dupla dimensão. De um lado, essa proteção se desdobra como liberdade negativa do cidadão oponível perante o Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro lado, ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).[189]

Como ressaltado pela autora, passou-se a ter um direito em dupla dimensão, tanto aquela subjetiva, ligada à proteção do sujeito potencialmente alvo de violações à intimidade ou à privacidade, quanto a dimensão objetiva, que expressa a proteção quanto à existência de mecanismos, inclusive estatais, de promoção da privacidade, ativa e coletivamente.

Um desses mecanismos ativos de proteção estatal à proteção de dados é a existência de uma Autoridade de proteção de dados, que seja independente e que possua atuação fiscalizatória e acessível aos cidadãos, independentemente de sua condição financeira, social ou política. O mais comum é que tais Autoridades estejam previstas nas próprias normas de

[189] MENDES, Laura Schertel. STF reconhece direito fundamental à proteção de dados: Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**. vol. 130/2020 | p. 473 | Jul - Ago / 2020.

proteção de dados, as quais disponham de possibilidades de atuação e detalhes sobre seu funcionamento.[190]

Dessa forma, na era da privacidade enquanto proteção de dados pessoais, não mais basta que a proteção seja limitada à intimidade ou à vida privada – aspectos subjetivos e de status negativo de abstenção de conduta –, ou, ainda, limitada à autodeterminação informativa – que, apesar de avançar para aspectos de controle das informações e dos dados, restringe-se à esfera individual –. Trata-se de um dever da coletividade proteger a privacidade e o uso dos dados da coletividade, criando-se uma cultura protetiva, boas práticas empresariais e normas que concretizem esses direitos.

Tanto é que o STF reconheceu a existência de um direito fundamental à autodeterminação informativa, antes mesmo da aprovação da Emenda Constitucional que expressamente incluiu o inciso LXXIX ao artigo 5º da Constituição, estabelecendo o direito fundamental à proteção de dados pessoais. Em julgamento ocorrido em 07 de maio de 2020, com relatoria da Ministra Rosa Weber, perante uma discussão sobre a possibilidade de compartilhamento de dados pessoais entre operadoras de telefonia e o IBGE no período pandêmico, a Corte Suprema decidiu que esse compartilhamento irrestrito, sem o estabelecimento de limitações ao uso dos dados e sem medidas técnicas e administrativas que comprovassem a segurança desses dados pessoais, violaria um direito fundamental à autodeterminação informativa, implicitamente vigente na Constituição Federal.[191]

Em seu voto, a Ministra Rosa Weber ressaltou que o direito à proteção de dados pessoais pode ser reconhecido como um direito fundamental, a partir da compreensão do direito fundamental à dignidade humana, do direito fundamental à intimidade, considerando a renovação da sua força normativa diante dos novos riscos decorrentes do avanço tecnológico, além do papel do *Habeas Data* como mecanismo de tutela material do direito à autodeterminação informativa.[192]

Portanto, diante da decisão proferida pelo STF, é possível considerar que o direito à proteção de dados pessoais já estaria previsto na Constituição Federal ainda que não

---

[190] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 307-309.

[191] BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC/DF**. Relator: Min. Rosa Weber. Data de julgamento: 24/04/2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629 Acesso em: 25 abr. 2023.

[192] Segue trecho do voto da Relatora: "A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.", p. 109.

expressamente, mas diante de um arcabouço de direitos fundamentais que, como resultado do avanço espraiado de novas tecnologias invasivas da personalidade humana, foi remodelado, passando de um direito à intimidade para um direito à autodeterminação informativa.

Mesmo com o reconhecimento do direito fundamental de modo implícito, a proteção de dados pessoais recebeu esse status de maneira expressa, a partir da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que incluiu o inciso LXXIX ao artigo 5º da Constituição Federal.[193] Dessa forma, deixando sua natureza implícita para trás, agora de forma expressa a proteção de dados pessoais passa a ser um grande balizador para as relações jurídicas, dentre elas a relação de emprego, cuja legislação própria faz poucas referências a esse tema, mesmo diante de jurisprudência dos tribunais do trabalho, dentre eles do Tribunal Superior do Trabalho.

4.1.2 Legislação e jurisprudência trabalhistas

A legislação trabalhista brasileira não possui previsão expressa resguardando o direito à privacidade, à intimidade ou à proteção de dados do empregado. A CLT, consolidada em 1943, não tinha em sua origem qualquer menção a esses direitos, mesmo que fossem direitos de personalidade, intimamente conectados com a dignidade humana no trabalho.

Apesar disso, algumas referências poderiam ser, hoje, indiretamente, entendidas como um reforço à previsão constitucional desses direitos. Por exemplo, o artigo 5º da CLT[194] prevê o direito à isonomia salarial independente do gênero, o que de alguma maneira oferece proteção aos dados pessoais dos indivíduos que, simplesmente pelo seu gênero, fossem discriminados pelo empregador, recebendo um salário menor do que outras pessoas na mesma empresa. Essa previsão reforça a não discriminação no local de trabalho, preceito que é inerente ao direito do trabalho e, a partir da LGPD, representa também um dos princípios fundamentais dessa disciplina.[195]

Outra disposição da CLT que possui relação indireta com a privacidade, notadamente sua proteção diante de dispositivos tecnológicos pelo empregador, é o artigo 6º,

---

[193] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[194] CLT. Art. 5º - A todo trabalho de igual valor corresponderá salário igual, sem distinção de sexo.

[195] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

parágrafo único,[196] que iguala o trabalho vigente sobre o controle eletrônico do empregador à relação de trabalho tradicional, sem que essa peculiaridade lhe retire a subordinação jurídica. Assim, mesmo que haja controle empregatício por meios telemáticos e informatizados, ainda assim prevalecerão os direitos trabalhistas básicos, principalmente diante da subordinação existente entre empregador e empregado.

Já o artigo 41 da CLT[197] traz previsão de registro dos empregados pela empresa, seja por meios físicos seja por sistemas eletrônicos. Esse dispositivo traz legitimidade para o empregador tratar os dados de seus empregados de modo estruturado, mesmo em bases de dados, com a finalidade de gerenciá-los em seu empreendimento. O parágrafo único do referido artigo descreve quais são os dados do empregado que deverão ser registrados pelo empregador.[198] Essa norma abre margem para que o empregador possa livremente decidir por utilizar ferramentas de IA para registro e tratamento de dados pessoais do empregado, utilizando como motivação a necessidade de registrar dados referentes duração e efetividade do trabalho, já que essas ferramentas tecnológicas teriam a capacidade de mais fielmente registrar horários de trabalho ou estabelecer métricas de resultados do trabalho realizado pelo empregado.

A título exemplificativo, ferramentas tais como as citadas na seção 2.3, que registram dados pessoais e, muitas vezes, dados pessoais sensíveis dos empregados para monitoramento do trabalho e apoio à gestão pelo empregador, são sistemas eletrônicos que poderiam ser justificadas pelo empregador como previstas no artigo 41 da CLT, estando confiante de sua legitimidade. Ocorre que o parágrafo único do referido artigo, em sua parte final, deixa bem claro qual o filtro ético-jurídico para a utilização dessas ferramentas para registro de dados pessoais dos empregados, que é a proteção do trabalhador. Somente os dados que interessem à proteção do trabalhador poderão ser utilizados no registro, o que quer dizer que nem todos os interesses do empregador legitimarão o tratamento desses dados pessoais por ferramentas tecnológicas, demandando sempre o balanceamento do interesse empresarial com os interesses e direitos do indivíduo trabalhador. Para além disso, o requisito não vale apenas para quais dados devem ser registrados, mas também de quais tratamentos podem ser realizados

---

[196] Art. 6º Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego. Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio.

[197] Art. 41 - Em todas as atividades será obrigatório para o empregador o registro dos respectivos trabalhadores, podendo ser adotados livros, fichas ou sistema eletrônico, conforme instruções a serem expedidas pelo Ministério do Trabalho.

[198] Art. 41 – [...] Parágrafo único - Além da qualificação civil ou profissional de cada trabalhador, deverão ser anotados todos os dados relativos à sua admissão no emprego, duração e efetividade do trabalho, a férias, acidentes e demais circunstâncias que interessem à proteção do trabalhador.

com esses dados, havendo igual necessidade de ponderação quanto à legitimidade dos meios utilizados pelo empregador, sempre privilegiando os direitos do trabalhador.

Da mesma forma, pode-se fazer referência ao artigo 41 da CLT,[199] que prevê a anotação dos horários de trabalho no registro de empregados, o qual pode estar em sistemas manuais, mecânicos ou eletrônicos. Essa disposição legitima o tratamento de dados pessoais pelo empregador, mas com a finalidade de comprovação dos horários de trabalho efetivamente cumpridos pelo trabalhador. Mesmo quando o trabalhador exerce sua função fora do estabelecimento, como no teletrabalho ou no trabalho externo, haverá anotação dos horários, ainda que o registro esteja em poder do empregado.[200]

Ressalte-se que a legitimação celetista para que o empregador possa exigir o registro dos horários do empregado decorre, diretamente, do poder de controle do empregador, o qual deve dirigir seu empreendimento e controlar como o trabalho é realizado, afinal reflete a subordinação existente na relação de trabalho. No entanto, o propósito da lei é exatamente garantir que os horários realizados pelo empregado sejam computados e não sejam ocultados em seu desfavor. Na complementariedade a isso, também permitir ao empregador saber quando houver trabalho em horário extraordinário, para que possa remunerá-lo.

Mesmo que o empregador adote ferramentas tecnológicas para controle de jornada do empregado, deverá ele respeitar os limites da intimidade, da vida privada e da proteção de dados pessoais do trabalhador, já que esse controle de jornada é apenas um instrumento, cujo propósito é, além de permitir o controle pelo empregador, proteger os direitos e interesses do empregado.

Há de se ressaltar, também na CLT, o artigo 373-A da CLT, que prevê algumas condutas vedadas ao empregador para garantir os direitos específicos para a mulher no trabalho. Esse dispositivo veda condutas do empregador que tenham por base critérios como sexo, idade, cor, situação familiar ou estado de gravidez. Por exemplo, não poderá o empregador utilizar esses critérios para anunciar vagas de trabalho, para recusar empregar ou promover, bem como motivar a dispensa, para determinar a remuneração, formação ou ascensão profissional e para seleção em concursos. Outros dois incisos trazem vedações específicas ao empregador, como

---

[199] Art. 74. O horário de trabalho será anotado em registro de empregados. [...] § 2º Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso.

[200] Art. 74. [...] § 3º Se o trabalho for executado fora do estabelecimento, o horário dos empregados constará do registro manual, mecânico ou eletrônico em seu poder, sem prejuízo do que dispõe o caput deste artigo.

exigir comprovação de esterilidade ou gravidez na admissão ou permanência no emprego e proceder com revistas íntimas nas empregadas ou funcionárias.

Próxima desse artigo da CLT, a Lei nº 9.029/95 também consiste em legislação trabalhista, mesmo que não consolidada, já que apresenta condutas vedadas no emprego que sejam relacionadas a discriminação. De acordo com sua previsão normativa, são vedadas condutas como as descritas no artigo 373-A da CLT, mas com aprofundada proteção, pois prevê punições para os indivíduos que a descumpram.[201]

Outro ponto relevante, presente na CLT, que reflete indiretamente algum cuidado com a proteção dos dados pessoais do empregado, é a garantia de estabilidade provisória. Essa prerrogativa encontra previsão em algumas situações, como é o caso do artigo 165, que protege os membros da CIPA (Comissão Interna de Prevenção de Acidentes) da despedida arbitrária e do artigo 391-A[202], que garante a estabilidade provisória para a gestante. Essas disposições se coadunam com o princípio da não discriminação, previsto na LGPD, como já referido anteriormente, já que o empregador não poderá dispensar o empregado pela condição que possua ou pelo cargo que ocupe.

Diante da análise dessas previsões celetistas, percebe-se que não há referências diretas à privacidade ou à proteção de dados pessoais. O que há são disposições trabalhistas que, de alguma maneira, se associam a alguns valores ligados à privacidade e à proteção de dados pessoais, tais como o princípio da não discriminação. Além disso, algumas disposições legitimam o uso de ferramentas tecnológicas pelo empregador, para tratamento de dados pessoais do trabalhador, o que não quer dizer que não haja limites a esse tratamento de dados, o qual deve sempre seguir o respeito aos interesses e aos direitos do empregado.

Na seara trabalhista, o TST, por ser o Tribunal uniformizador dos entendimentos jurisprudenciais, historicamente possui decisões sobre alguns temas relevantes ligados à proteção da privacidade do trabalhador.

Em diversos casos o Tribunal já teve de apreciar situações em que o empregador exerceu seu poder de controle ao fiscalizar e realizar revistas em pertences dos empregados. A finalidade, segundo os empregadores, seria evitar furtos de objetos pertencentes à empresa ou

---

[201] Art. 1º É proibida a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, reabilitação profissional, idade, entre outros, ressalvadas, nesse caso, as hipóteses de proteção à criança e ao adolescente previstas no inciso XXXIII do art. 7o da Constituição Federal.

[202] Art. 391-A. A confirmação do estado de gravidez advindo no curso do contrato de trabalho, ainda que durante o prazo do aviso prévio trabalhado ou indenizado, garante à empregada gestante a estabilidade provisória prevista na alínea *b* do inciso II do art. 10 do Ato das Disposições Constitucionais Transitórias.
Parágrafo único. O disposto no caput deste artigo aplica-se ao empregado adotante ao qual tenha sido concedida guarda provisória para fins de adoção.

aos demais empregados. Enquanto isso, alegando violação da privacidade, bem como a disposição do artigo 373-A da CLT, os empregados pedem a condenação do empregador em indenização por danos morais.

Ocorre que o TST já firmou entendimento de que essa revista não pode ser íntima, porque violaria a intimidade dos empregados, bem como deve ser feita de forma moderada, sem que invada caracteres da personalidade do indivíduo. Assim, como ressaltado em alguns casos exemplificativamente cotejados, o TST entende que a revista em objetos pessoais – como bolsas ou mochilas – não enseja violação aos direitos de personalidade, por caracterizarem um caso de moderação.[203] No entanto, quando se trata de revista íntima, junto ao corpo do trabalhador, ou mesmo com a exposição do empregado a situação vexatória, por exemplo com desnudamento para verificação visual do empregador, o entendimento judicial é de que violaria a direito à intimidade.[204]

Outra temática, ligada à privacidade do empregado, que está sempre presente em julgados do TST envolve o videomonitoramento dos locais de trabalho e sua possível invasão de privacidade, quando diz respeito ao monitoramento do empregado e de seus aspectos pessoais.[205] Mais uma temática decorrente do direito à privacidade aparece na jurisprudência do TST, que é a exigência pelo empregador de certidões de antecedentes criminais em processos de seleção de emprego.[206]

Mais um ponto de destaque na jurisprudência do TST que envolve a proteção de dados do empregado diz respeito ao acesso do empregador às comunicações trocadas pelos seus empregados, seja em meios corporativos seja em meios privados.[207]

Vê-se que o tema da privacidade sempre esteve presente nos debates legais e jurisprudenciais trabalhistas, pelo menos nas últimas décadas, mas sempre vinculadas ao direito

---

[203] Alguns precedentes da SBDI-1 podem ser destacados nesse sentido: E-ED-RR - 2189500-50.2009.5.09.0005, SBDI-1, Relator Ministro Guilherme Augusto Caputo Bastos, *in* DEJT 12.2.2016; E-RR - 200900-33.2013.5.13.0009, SBDI-1, Relator Ministro João Oreste Dalazen, *in* DEJT 12.2.2016.

[204] Nesse sentido: E-ARR-1493-54.2012.5.18.0102, Subseção I Especializada em Dissídios Individuais, Relator Ministro Guilherme Augusto Caputo Bastos, DEJT 28/09/2018; E-ED-RR-90340-49.2007.5.05.0464, Subseção I Especializada em Dissídios Individuais, Relator Ministro Alberto Luiz Bresciani de Fontan Pereira, DEJT 01/03/2013.

[205] Alguns precedentes do TST evidenciam os critérios para que a utilização de câmeras no local de trabalho seja válida, como o TST RR 169000-71.2009.5.02.0011. Outros julgados apresentam invalidação do uso de videomonitoramento em banheiros e vestiários, vide RR-1793-64.2016.5.12.0030 e RR-24457-06.2017.5.24.0003.

[206] Julgados nesse sentido evidenciam que a exigência dessa documentação, quando não relevante para o cargo a ser ocupado, viola os direitos de personalidade, por exemplo o seguinte julgado do TST: RR-2249-12.2017.5.07.0032.

[207] Reforçando que o acesso do empregador a e-mails profissionais é permitido, tendo em vista considerar-se ferramenta de trabalho, porém não sendo possível o acesso a e-mail pessoal do empregado, vide julgado do TST: RR - 1347-42.2014.5.12.0059.

à privacidade e ao direito à intimidade, os quais fazem parte da categoria direitos da personalidade. Estão previstos os comandos normativos na Constituição Federal, em seu artigo 5º, porém trazem disposições abertas, suscetíveis de interpretação e dosagem pelos atores. Assim, não há requisitos práticos ou mesmo medidas recomendadas para adoção de tecnologias no trabalho com a finalidade de tratar dados pessoais dos trabalhadores. Além disso, em momento algum a legislação trabalhista faz referência à IA ou a ferramentas automatizadas de tratamento de dados.

Alguns desses entendimentos beiram ao casuísmo, pois cada situação concreta apresentará os parâmetros a partir dos quais uma análise judicial poderá verificar se os direitos em questão – de um lado, o poder diretivo do empregador, do outro lado, o direito à privacidade e intimidade do empregado – estão sendo ou não bem aplicados e ponderados. O julgador somente poderá delimitar se uma conduta de videomonitoramento está sendo bem realizada pelo empregador se ele tiver os elementos concretos daquele caso específico, não podendo, conforme a legislação anterior à LGPD, aplicar critérios para aferição do quão certa ou quão errada terá sido aquela decisão empresarial.

4.1.3 Marco Civil da Internet

Em 2014, foi aprovado o Marco Civil da Internet (MCI), instrumento normativo que trouxe regras sobre o uso dos meios digitais, privilegiando a liberdade de expressão como fundamento, mas também reconhecendo outros valores, tais como os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, dentre vários outros valores que caracterizam alguma limitação à liberdade de expressão.

Ainda em 2014, antes mesmo da edição da LGPD, já havia previsão no MCI acerca do direito à proteção de dados pessoais dos indivíduos, quando se relacionando no ambiente digital. O artigo 3º do MCI previu os princípios regentes ao uso da internet do Brasil, sendo um deles a proteção dos dados pessoais, na forma da lei.[208] Portanto, a LGPD não inovou ao trazer o direito à proteção de dados pessoais ao ordenamento jurídico brasileiro. O que ela fez foi expandir esse direito para os meios não digitais, além de trazer regras mais claras de sua procedimentalização, já que no MCI ele estava previsto pontualmente, mas com a ressalva de ter de ser complementada por lei própria, que veio a ser a própria LGPD.

---

[208] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] III - proteção dos dados pessoais, na forma da lei;

Alguns autores, antes mesmo da aprovação da LGPD, afirmavam que separar privacidade e proteção de dados – como foi feito pelo MCI – não possuía lógica, já que não haveria como se conceber privacidade sem proteção dos dados e porque não havia substrato legal ou constitucional expresso sobre o tema da proteção de dados, é o que afirmava Victor Hugo Gonçalves:

> Conceitos esses que, em tempos de tecnologias de informação e comunicação, são conexos e altamente interligados, pois todas as proteções e ferramentas de ação para a defesa da privacidade nada mais são do que dados pessoais. Teoricamente, tal divisão de proteção à privacidade da proteção dos dados pessoais são constitucionalmente insustentáveis.[209]

Apesar dessa remissão a lei própria, o artigo 7º do MCI[210] prevê alguns direitos dos usuários da internet, sendo alguns principais o direito à inviolabilidade da intimidade e da vida privada; a inviolabilidade tanto dos fluxos de comunicações quanto dos conteúdos dessas comunicações, feitas pela internet, salvo por ordem judicial; a garantia de não fornecimento de seus dados a terceiros sem que houvesse consentimento ou uma hipótese prevista em lei; informações claras e completas sobre o tratamento de dados pessoais realizado na internet, inclusive suas finalidades; necessidade de consentimento para tratamento de dados pessoais; dentre diversos outros.

Esses direitos já fazem parte de um arcabouço introdutório ao que se instaurou como disciplina da proteção de dados no Brasil, com a LGPD. Afinal, diversas dessas previsões estão contidas na nova lei, mesmo que de forma mais aprofundada e muito mais estruturada para sua aplicação práticas pelos agentes de tratamento de dados pessoais.

Uma discussão relevante advinda do MCI na relação de emprego diz respeito à possibilidade de o empregador se utilizar de ferramentas tecnológicas aplicadas no trabalho

---

[209] GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. São Paulo: Grupo Gen-Atlas, 2017, p. 24-25.

[210] MCI. Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;.

para rastrear os passos de seus empregados e, de alguma forma, produzir provas digitais em um processo judicial. Por exemplo, o empregador poderia se utilizar de algum aplicativo disponibilizado para seus empregados para uma finalidade diversa e, em eventual processo judicial, verificar se as horas extras alegadamente trabalhadas pelo ex-empregado teriam sido realmente cumpridas na empresa ou se os dados de geolocalização presentes nesse aplicativo diriam o contrário, que naquele momento ele estaria em casa ou em outro local desvinculado ao trabalho.

Ou ainda, em um exemplo apresentado por Ana Cláudia de lima e João Paulo Albino,[211] em um processo buscando o reconhecimento de vínculo trabalhista, no qual o autor alegue que trabalhava todos os dias da semana, sendo que a empresa argumenta que ele apenas prestava serviços em torno de duas vezes por semana. Nessa situação o juiz poderia determinar que houvesse diligências necessárias para esclarecer os fatos, com base no artigo 765 da CLT. Essa busca de provas poderia ocorrer da seguinte forma:

> Para dirimir provas frágeis ou contraditórias, o juiz poderá determinar que o próprio trabalhador que utilize celular com sistema operacional Android® apresente seu histórico de localização gravado na conta da plataforma Google® ou expedir ofício à Operadora de Celular, requisitando o mapa Estágio Rádio Base, no período em que o vínculo empregatício é postulado e exclusivamente quanto à jornada informada na petição inicial, para que não se alegue invasão de privacidade quanto aos horários fora do mencionado horário de trabalho.[212]

Antes do MCI, talvez não houvesse a possibilidade de se obter desses aplicativos ou ferramentas tecnológicas os registros passados de seus ex-empregados, já que as empresas de tecnologia possuam a necessidade de constantemente apagar seus dados antigos, por limitações de armazenamento de dados em seus servidores. No entanto, o artigo 15 do MCI[213] trouxe a previsão de que os provedores de aplicações na internet,[214] ou seja, aqueles que

---

[211] DE LIMA, Ana Cláudia Pires Ferreira; ALBINO, João Pedro. Técnicas de captura de geolocalização para produção de prova judicial. **Revista Direito das Relações Sociais e Trabalhistas**, v. 8, n. 1, p. 216-233, 2022.
[212] Ibid., p. 15-16.
[213] Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
[214] A definição de aplicações de internet se encontra no artigo 5º, inciso VII do MCI: Art. 5º Para os efeitos desta Lei, considera-se: VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

disponibilizem sistemas tecnológicos com aplicação direcionada aos próprios usuários, mantenham os registros de acesso a essas aplicações pelo prazo de 6 (seis) meses.

O Código de Processo Civil pode conter a legitimação do uso das provas digitais pelo empregador em determinado processo judicial, já que o artigo 369[215] prevê o direito das partes de utilizarem todos os meios legais, bem como moralmente legítimos, para provar a verdade dos fatos.

Apesar da previsão legal, ainda deverão ser respeitados os direitos à intimidade, à vida privada e, principalmente, à proteção dos dados pessoais. Se o empregador busca se utilizar de registros feitos em aplicações da internet por ele fornecidas pelo seu empregado (ou ex-empregado) para uma finalidade meramente lúdica ou que não gere naquele indivíduo alguma expectativa de que pudesse ser usado contra si em algum processo judicial, deve-se considerar a necessária transparência, prevista no artigo 6º, inciso VI[216] da LGPD, sendo ele um dos princípios fundantes dessa legislação.

Além disso, o uso indiscriminado dessas tecnologias para a finalidade de rastrear a vida do empregado, mesmo que durante o horário de trabalho, torna o meio ambiente de trabalho de alguma maneira desconfortável, com um sentimento de constante vigilância dos mínimos detalhes de onde o empregado está ou vai durante seu intervalo para descanso. Da mesma forma, naqueles casos em que o empregador proíbe ou limita a ida de empregados ao banheiro, temática amplamente já debatida perante o TST, esse tipo de ferramenta poderia servir como auxiliar do empresário para acompanhar quais os trabalhadores que estejam indo mais vezes ao banheiro ou outros locais de descompressão física ou psicológica.

4.2 Lei Geral de Proteção de Dados

Após bastante influência gerada a partir da evolução legislativa da União Europeia de promover seu próprio Regulamento Geral de Proteção de Dados (RGPD), o Brasil viu-se incentivado a elaborar legislação própria sobre o tema. Afinal, grande parte dos países pertencentes à OCDE e, também, aqueles que buscavam maior integração com esses países já

[215] Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.
[216] Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

possuíam legislação própria, sendo necessário que o Brasil providenciasse essa medida, para atingir maior integração entre os países por meio do fluxo transfronteiriço de dados pessoais.

Assim, em 2018, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (LGPD), que inovou trazendo diversas disposições principiológicas sobre o tema, complementando a matéria que já vinha sendo superficialmente abordada em legislações anteriores, além de prover os agentes de tratamento[217] de dados com medidas práticas necessárias a implementar, de modo a cumprir com os preceitos da legislação.

Para Eduardo Magrani e Paula Guedes, a LGPD se apresenta como um quadro regulatório fundamental, por ter apresentado uma estrutura positiva em prol do controle do titular sobre seus dados, diante dos inúmeros riscos da IA aos direitos humanos, notadamente porque os dados são motor dessa tecnologia.[218]

4.2.1 Princípios da proteção de dados pessoais

Quando se analisou os riscos que o uso da IA na relação de emprego gera à privacidade do empregado (seção 3.3), viu-se que diversos princípios da LGPD são postos em xeque diante das características tanto da IA quanto do *Big Data*, que é o grande combustível que alimenta esses sistemas inteligentes. Destacou-se também que o poder de controle eletrônico do empregador poderia servir como uma justificativa legítima para que ele pudesse invadir cada vez mais na vida privada do empregado, violando sua dignidade e seus direitos de personalidade.

No entanto, Teresa Coelho Moreira sugere que sejam aplicados os princípios da proteção de dados pessoais como limites diretos ao poder de controle do empregador.[219] Assim, seguindo a sugestão da professora portuguesa, cabe verificar de que maneira os princípios da proteção de dados pessoais, dispostos na legislação própria da matéria, poderiam ser de grande valia para limitar o poder do empregador, diante do uso da IA.

O artigo 6º da LGPD dispõe de dez princípios, que são a base valorativa da proteção de dados pessoais no Brasil. No RGPD europeu são igualmente citados princípios da proteção

---

[217] A LGPD classifica como agentes de tratamento o controlador e o operador dos dados (art. 5º, IX). O controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI). O operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII).

[218] MAGRANI, Eduardo; GUEDES, Paula. Inteligência Artificial: desafios éticos e jurídicos. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 89.

[219] MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021. p. 189.

de dados pessoais, sendo eles bastante similares aos princípios vigentes na lei brasileira. Aqueles princípios mais relevantes de um estão presentes, em alguma medida, também no outro, podendo citar-se os princípios da finalidade, necessidade, adequação, qualidade dos dados, dentre vários outros.

A similaridade entre os princípios presentes nessas normas não é obra do acaso, nem mesmo apenas alguma falta de criatividade do Legislador brasileiro. Em verdade, esse rol de princípios é anterior mesmo ao RGPD e à Diretiva 95/46/CE[220]. Esse conjunto de comandos principiológicos a respeito do tratamento de dados pessoais decorre de acordos e arranjos internacionais e transnacionais, datados da década de 1970, com o que se denominou FIPPs (*Fair Information Practice Principles*).[221]

Nesse período, os Estados Unidos da América, com o "Relatório sobre Registros, Computadores e Direitos do Cidadão", o Reino Unido, com o Relatório emitido pelo Comitê de Privacidade e a Alemanha, com a Lei do estado de Hesse, apresentaram princípios bastante similares entre si. Esses princípios dispunham sobre condições para que as organizações pudessem realizar tratamento de dados, mantendo-se uma finalidade determinada, utilizando apenas os dados necessários, garantindo acesso e transparência aos indivíduos, medidas técnicas de segurança dessas informações e cuidados desde o design dos sistemas.[222]

Essa coincidência de princípios, desde o início das primeiras leis de proteção de dados, demonstram a equivalência de preocupações enfrentadas pelos indivíduos de maneira generalizada. Além disso, representou um passo importante para que houvesse maior capacidade de circulação dessas informações de um país para o outro diante da equivalência de parâmetros principiológicos existente. Essa origem baseada nos princípios dos FIPPs pode ser considerada como um grande pilar de similaridade entre LGPD e RGPD, os quais possuem princípios fundantes bastante similares.

Além dessa influência, os princípios fundantes da proteção de dados pessoais derivam também das Diretrizes propostas pela OCDE em 1980 e atualizadas em 2013, para possibilitar a proteção da privacidade e o fluxo transfronteiriço de dados pessoais. Nessas Diretrizes, é apresentada uma lista de 8 (oito) princípios que deveriam nortear a proteção dos

---

[220] Norma da Comunidade Europeia, anterior ao RGPD, que tinha um caráter sugestivo aos Estados-membros, para que cada um deles adotasse leis nacionais de proteção de dados, seguindo os parâmetros previamente estabelecidos na referida Diretiva.

[221] MENDES, Laura Schertel. BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, ano 28, p. 157-180, jul.-ago. 2019. p. 165.

[222] Ibid., p. 167.

dados pessoais, sendo eles os mesmos utilizados pela Diretiva nº 95/46/CE e, posteriormente, pelo RGPD e pela LGPD.

A primeira categoria de princípios, presentes na LGPD, diz respeito aos princípios que limitam o tratamento de dados, exigindo do agente que o tratamento realizado seja adequado e necessário a atingir um propósito determinado, lícito e informado ao titular de dados. Portanto, estão incluídos nessa categoria os princípios da finalidade, da adequação e da necessidade.

O princípio da finalidade, previsto no artigo 6º, inciso I da LGPD,[223] prevê expressamente que o tratamento de dados somente pode ocorrer se tiver um (ou mais) propósito previamente definido. A prévia definição da finalidade para o tratamento de dados deve considerar diversas características, as quais são previstas na redação legal.

A primeira dessas características é que o propósito do tratamento de dados deve ser legítimo, assim considerado aquele propósito que atende aos parâmetros jurídicos e, também, éticos, não se admitindo que o propósito do tratamento de dados seja ilícito, contrário à boa-fé, fora da expectativa do titular de dados e, menos ainda, contrário a seus direitos. Por exemplo, não poderá o empregador definir que pretende realizar um processo seletivo por meio de rede social profissional, apontando que todos os candidatos deverão apresentar certidões de antecedentes criminais, já que essa exigência, para uma função que não a exige, é descabida e viola direitos fundamentais, portanto é ilegítima.

A segunda característica dos propósitos do tratamento de dados é que eles devem ser específicos, devendo, então, possuir a determinação daquilo que se pretende, de forma a evitar uma previsão genérica ou abstrata da intenção e do resultado esperado pelo agente de tratamento de dados naquele momento. Portanto, quando o empregador decidir que tratará dados do empregado, deverá definir exatamente qual o resultado que buscará atingir, não podendo simplesmente registrar que se trata de um tratamento de dados pessoais visando melhoria da prestação de serviços. Deverá, ao revés, especificamente indicar que o tratamento dos dados pessoais se dará para que se compare os resultados de um empregado com o do outro, por meio de métricas A, B ou C.

A terceira e a quarta características podem ser agrupadas, já que a finalidade deve ser tanto explícita quanto informada ao titular de dados. Assim, não basta que haja a informação da finalidade ao titular, mas essa informação tem de ser explícita ao ponto de não deixar dúvidas

[223] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

e garantir que, proativamente, o agente de tratamento de dados fez sua parte para que o titular saiba o que realmente acontecerá, de modo finalístico, com seus dados. Portanto, mesmo que o empregador conste em seu regulamento empresarial que poderá utilizar ferramentas baseadas em IA para monitorar os resultados do trabalho de seus empregados, essa informação não deve apenas ser repassada, mas explicitamente apresentada, com cláusula apartada e, inclusive, destaque das demais, podendo até mesmo utilizar-se de mecanismos visuais e baseados em uma linguagem simples.

A quinta característica do princípio da finalidade é que, após definido o propósito desse tratamento de dados, mesmo que haja outro propósito buscado pelo agente de tratamento para aqueles dados, ele deverá ser buscado apenas se guardar compatibilidade com o propósito original, haja vista evitar a confusão no titular de dados, o qual teria frustrada sua expectativa caso o segundo propósito fosse diverso e incompatível com o primeiro. Assim, sendo de interesse do empregador fornecer dispositivos vestíveis aos seus empregados, com a finalidade de estimulá-los a realizar mais exercícios, não seria compatível com esse propósito inicial (estímulo aos exercícios) que o empregador armazenasse os registros de atividades e de batimentos cardíacos de seus empregados e os compartilhasse com empresas de plano de saúde, as quais poderiam aumentar os valores do plano, com base no histórico de saúde realmente exercido pela pessoa.

O segundo princípio, que possui ligação direta com o primeiro, é o princípio da adequação, previsto no artigo 6º, inciso II da LGPD.[224] Segundo esse princípio, escolhido o tratamento de dados pessoais e delimitado o propósito que se pretende atingir, ambos devem ser compatíveis e adequados entre si. Portanto, se o propósito determinado pelo empregador for o de selecionar um candidato em processo seletivo automatizado, não será adequado que ele armazene todos os dados pessoais dos demais candidatos por muito tempo, por exemplo 10 anos, ou indistintamente. Será incompatível pois o armazenamento dessas informações não tem o condão de efetivar o propósito buscado, o que fere contrariamente o princípio da adequação.

Como terceiro princípio dessa categoria, a necessidade, prevista no artigo 6º, inciso III da LGPD,[225] representa a lógica presente na disciplina da proteção de dados pessoais, que é a de minimização do tratamento de dados. Segundo estabelece o princípio da necessidade, o

[224] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

[225] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

agente de tratamento somente poderá utilizar aqueles dados que sejam estritamente necessários ao propósito por ele estabelecido.

Para cumprir com esse princípio, o agente deverá avaliar primeiramente a pertinência dos dados pessoais para aquela finalidade, em segundo momento selecioná-los conforme seja proporcional para o resultado esperado e, por fim, remover aqueles dados que sejam excessivos para seu desiderato. No caso da relação de emprego, se o empregador tiver o propósito de confirmar se um determinado empregado esteve ou não trabalhando durante seu horário designado, deverá se limitar ao tratamento apenas daqueles dados estritamente necessários, por exemplo os registros de jornada ou os acessos do empregado a algum sistema específico, caso se trate de um trabalho à distância.

No entanto, com a vasta utilização de sistemas baseados em IA que tratam dados provenientes do *Big Data*, não apenas essas informações triviais são utilizadas pelas empresas, mas também os dados de geolocalização do empregado, que pode revelar o local onde o empregado esteja realizando seu trabalho remoto; ou ainda, como relatado no caso Teleperformance[226], o rastreio da vida privada do empregado, com a possibilidade de ter sua câmera do computador ligada esporadicamente durante alguns momentos do dia, para confirmar se aquele empregado está ou não à frente do computador.

Tratamentos de dados dessa natureza violam o princípio da necessidade, haja vista que abrangem o tratamento de dados que são, além de invasivos, desnecessários à obtenção daquele propósito, já que haveria outros caminhos possíveis, menos invasivos, de se chegar ao mesmo objetivo.

Outro grupo de princípios da proteção de dados pessoais é aquele relacionado com o acesso à informação pelo titular dos dados. Um dos valores mais caros à proteção de dados pessoais é a noção de autodeterminação informativa, a partir da qual o indivíduo tem o direito de determinar os meios pelos quais seus dados pessoais serão tratados, as finalidades de tratamento e, inclusive, com quem essas informações são compartilhadas, de modo que o titular esteja no controle dos dados que o digam respeito.

Diante disso, um dos princípios que concretiza a autodeterminação informativa é o princípio do livre acesso, previsto no artigo 6º, inciso IV da LGPD.[227] Segundo esse princípio, deve ser proporcionado ao titular dos dados o acesso, facilitado e gratuito, aos dados pessoais

---

[226] Caso apresentado no capítulo 2, nota de rodapé nº 55.

[227] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

de maneira integral, à forma do tratamento que esteja sendo realizado e à sua duração. Nesse sentido, quando o empregado deseje saber quais dados pessoais são tratados pelo seu empregador, deverá este fornecer essas informações de maneira facilitada e gratuita, inclusive informando se o tratamento de dados se dá de forma automatizada. O princípio do livre acesso soma-se ao princípio da transparência (a seguir explicitado), para robustecer a necessidade de o empregador informar ao empregado quando este estiver sendo submetido a um tratamento automatizado de dados pessoais.

O segundo princípio que diz respeito à facilitação do controle dos dados pelo titular é o princípio da transparência, previsto no artigo 6º, inciso VI da LGPD.[228] De acordo com esse princípio, não basta que haja o acesso do titular aos dados pessoais, à forma e à duração do tratamento realizado, mas também deverão ser a ele disponibilizadas informações sobre a realização do tratamento e sobre quais os agentes que realizam tratamento desses dados pessoais.

Trata-se de disposição de ainda maior relevância na sociedade da informação, já que a facilidade com que as tecnologias conseguem realizar o tratamento de dados torna-o cada vez mais invisível, dificultando ao titular de dados saber quando exatamente estará havendo um tratamento ou não. Ainda mais, quando se fala em aplicação de mecanismos de IA, o mais comum é que ocorram diversos julgamentos algorítmicos com base nos dados pessoais, mas os indivíduos sequer sabem que estão sendo avaliados por máquinas, muito menos as finalidades ou as peculiaridades desse tratamento.

Outro motivo que traduz a maior relevância desse princípio é a complexa rede de compartilhamentos de dados existente, notadamente quando se fala de uma relação de emprego, em que apenas o empregador deveria ter acesso àqueles dados pessoais de seus empregados, mas, por contratarem softwares e serviços (muitos deles, baseados em IA) de empresas terceiras, acabam aceitando compartilhar com elas os dados de seus empregados. Essas empresas terceiras conseguem reutilizar essas informações recebidas do empregador para efetuar novas análises de dados dos titulares, por vezes para finalidades completamente incompatíveis com o propósito original, já descumprindo o princípio da finalidade, supra discutido.

No entanto, não basta que sejam apenas disponibilizadas informações ao titular dos dados, elas devem ser claras, precisas e facilmente acessíveis. A clareza nas informações

[228] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

demanda que elas revelem o que está ocorrendo, sem que se obscureça nenhum detalhe relevante ao titular. A precisão reflete o intuito da lei de exigir dos agentes de tratamento que confirmem a veracidade dessas informações, evitando respostas desatualizadas ou descoladas da realidade.

A terceira característica é que as informações devem estar facilmente acessíveis, o que significa que o agente de tratamento não pode impor limitações ao acesso pelo titular, que deverá ser informado de maneira acessível e gratuita. Ressalte-se, no entanto, que a transparência encontra limitações quando prevaleça o direito empresarial de manutenção do segredo comercial ou industrial (espécies de segredo de negócio), tendo em vista o respeito à propriedade e ao desenvolvimento econômico. Assim, mesmo que sejam solicitadas informações sobre determinado tratamento de dados, poderá o empregador recusar seu fornecimento, caso sua revelação pudesse violar seu direito de manter informações confidenciais em sigilo.

E quando se trata de algoritmos de IA que devem seguir o princípio da transparência, não há como se considerar esse princípio apenas em um aspecto formal, ou seja, que seja satisfeito tão somente pela apresentação de documentação ao titular de dados e que informe qual o tipo de tratamento realizado e quais os agentes que realizam esse tratamento. A necessidade de transparência dos algoritmos é maior, haja vista que os processos de tomada de decisão que se baseiam nessas tecnologias podem não ser conhecidos nem mesmo por seus programadores ou pela empresa que contratou a referida solução tecnológica.

Tendo em vista a lógica envolvida nesses algoritmos de IA para chegar às suas decisões, que não se utilizam da causalidade, mas da correlação probabilística, os passos adotados até se chegar naquela decisão podem ser obscuros. Até mesmo quando os passos são conhecidos, os critérios utilizados podem não estar tão claros para aquela tomada de decisão. Ainda que se saiba os passos e os critérios, o peso que foi dado a cada um dos critérios considerados pela IA não é demonstrado com clareza, às vezes nem mesmo para os programadores.

Por esse motivo, Frank Pasquale[229] conclui que esses algoritmos, que cada vez mais são difundidos nas relações humanas, podem ser obscuros ao ponto de serem comparados com "caixas-pretas", que possuem características guardadas sob diversas camadas de proteção, o que, ao mesmo tempo, faz com que percam sua transparência e não se tornam acessíveis pelos que mais precisariam de informações: os titulares de dados pessoais.

---

[229] PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

Assim, apresenta-se a explicabilidade como possível atenuante do funcionamento obscuro dos algoritmos de IA. Essa capacidade de explicar detalhes sobre o algoritmo vai além da transparência, pois enquanto essa se limita, pela definição legal, a apresentar informações sobre o tratamento e os agentes que o realizam, a explicabilidade exige do agente de tratamento que sua tecnologia efetivamente seja capaz de revelar parâmetros racionais que o fizeram chegar àquela conclusão, seja pela apresentação dos critérios que foram utilizados, o peso de cada um deles ou, ainda, pela racionalidade envolvida naquela decisão.

Para este trabalho, far-se-á a diferenciação entre explicabilidade e direito à explicação, termos distintos mas correlatos, já que um é a consequência lógica do outro, porém vistos de óticas distintas. A explicabilidade será entendida enquanto dever do agente de tratamento em tornar sua tecnologia em algo explicável, permitindo revelar os detalhes envolvidos em uma decisão tomada por algoritmo.

Já o direito à explicação pode ser entendido como a posição mantida pelo titular de dados que, caso deseje manifestá-lo, pode solicitar e obter a explicação sobre os aspectos daquela decisão algorítmica. A explicabilidade algorítmica e o direito à explicação quanto a decisões automatizadas serão abordados com maiores detalhes no tópico relativo aos direitos dos titulares de dados, pois poderá abordar em conjunto os princípios da transparência e livre acesso (previstos no artigo 6º, incisos IV e VI da LGPD) e o direito à explicação (previsto no artigo 20, §1º da LGPD).

Outro grupo de princípios da LGPD que merece destaque quando se aborda o uso da IA engloba tanto o princípio da qualidade dos dados (previsto no artigo 6º, inciso V da LGPD) quanto o princípio da não discriminação (previsto no artigo 6º, inciso IX da LGPD). Esses princípios dizem respeito à necessidade de que o tratamento de dados ocorra de maneira justa e exata, quanto aos propósitos a que ela se destina.

O princípio da qualidade dos dados[230] exige que o agente de tratamento não implique na modificação dos dados pessoais fornecidos pelo titular, já que este tem a garantia de que suas informações serão mantidas *exatas*, ou seja, não estarão incorretas; *claras*, portanto de fácil compreensão; *relevantes*, já que somente poderão ser tratadas caso sejam necessárias; e *atualizadas*, para que se evitem decisões equivocadas ou que possam ocasionar prejuízos ao titular dos dados. Assim, o empregador que se utilize de ferramentas baseadas em IA para avaliar o desempenho profissional de seus empregados deverá sempre manter atualizada a base

[230] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

de dados que alimenta essa tecnologia, caso contrário poderá incorrer em injustiças ou alimentar resultados espúrios produzidos pelo algoritmo.

Já o princípio da não discriminação,[231] abordado com maiores contornos na seção 3.4, enuncia que o tratamento de dados não pode ter finalidades que resultem em tratamento discriminatório, seja ele ilícito, portanto contrário à lei e ao Direito, ou abusivo, que extrapole os limites de razoabilidade. Assim, o empregador que utilizar um sistema de IA para contratação de novos empregados não poderá estabelecer critérios seletivos que violem a legislação ou que excedam a razoabilidade. Esse cuidado não deve ser apenas quanto a critérios explícitos, mas os critérios utilizados implicitamente pelo algoritmo devem ser verificados, já que a lógica da correlação, em que se baseiam essas tecnologias, pode levar a situações em que um critério aparentemente inofensivo (por exemplo, qual a escola que a pessoa estudou) pode levar a uma decisão discriminatória, baseada em uma ilicitude (tendo em vista que todas as pessoas que estudam em uma escola para o público feminino são mulheres, a decisão eventualmente pode ocorrer com base no gênero[232]).

O conjunto final de princípios da proteção de dados pessoais destaca a importância dos agentes de tratamento adotarem uma atitude proativa. Isso significa que eles devem tomar medidas para prevenir incidentes envolvendo dados pessoais, garantindo a segurança e a prevenção de problemas. Além disso, é fundamental que realizem o tratamento de forma adequada e transparente, evidenciando que estão cumprindo suas responsabilidades e prestando contas de suas ações.

O princípio da segurança[233] exige que sejam adotadas medidas aptas a proteger os dados pessoais, sejam medidas técnicas (por exemplo, antivírus, firewall, tecnologias que limitem o acesso aos dados apenas a quem deva realmente acessá-los), sejam medidas administrativas (desenho de processos gerenciais internos, capacitações para os empregados, políticas internas se segurança da informação, dentre outras). Esses mecanismos de segurança possuem como finalidade evitar que ocorram incidentes de segurança dos dados, os quais são exemplificados na lei como destruição, perda ou alteração dos dados, além de comunicação ou difusão dessas informações, se feitas de maneira ilícita ou acidental.

---

[231] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
[232] Foi o que houve com a IA utilizada pela Amazon para recrutamento, já abordado no capítulo anterior,, que logo foi descartada pela empresa, pois estava selecionando candidatos com base no gênero e discriminando mulheres, mesmo que esta informação não estivesse claramente na base de dados, pois o critério que era utilizado como substituição (*proxie*) era a escola em que as candidatas haviam estudado.
[233] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

A necessidade de segurança dos dados pessoais intensifica-se conforme mais se utiliza tecnologia no âmbito do tratamento de dados, afinal as tecnologias são vetores computacionais que podem conter falhas de programação ou lacunas que fragilizem o sistema para acesso não autorizado de terceiros. Portanto, diante do uso de sistemas de IA, os quais conseguem tratar uma imensa quantidade de dados, mas também podem produzir dados em escala e variedade também imensas, as consequências advindas de uma falha de segurança na IA pode gerar prejuízos muito maiores do que um simples registro estático de dados.

Mais preocupante ainda do que os riscos provenientes de falhas de segurança de dados nos sistemas de IA é que esses sistemas possuem também a capacidade de atenuar riscos de segurança da informação, afinal um sistema de IA não deveria cometer erros que sejam tipicamente humanos. Estudo promovido pelo Fórum Econômico Mundial em 2022 constatou que cerca de 95% dos incidentes de segurança da informação ocorrem por condutas humanas, não por falhas tecnológicas.[234] Diante disso, algumas metodologias de IA podem realmente ser uma excelente forma de mitigar essas falhas de segurança da informação, atuando de forma similar ao sistema imunológico do corpo humano, pois quando um empregado descumpre (ou está em vias de descumprir) uma regra de segurança da informação, a IA instantaneamente reage e bloqueia aquela ação ou seus efeitos indesejados, similar ao que fazem os glóbulos brancos.[235]

Embora o uso da IA pareça benéfico ao reduzir os riscos de segurança da informação, ele também aumenta o uso dessas ferramentas no ambiente de trabalho, o que pode intensificar o tratamento de uma quantidade crescente de dados pessoais dos próprios empregados. Afinal, se uma ferramenta de IA possa estar sempre à disposição para intervir em um possível incidente de segurança causado por um empregado, este deverá ter seu trabalho constantemente monitorado, não havendo espaço para privacidade do indivíduo, já que sua máquina terá de estar sempre em constante fiscalização do empregador (ou de sua IA).

Diante do uso da IA, por meio de sistemas complexos e, muitas vezes, fora do alcance de conhecimento até do próprio empregador, essas tecnologias devem possuir mecanismos de garantia da segurança dos dados, assim como deverão ser elaborados relatórios prévios acerca do impacto que seu uso pode gerar tanto na proteção dos dados, quanto nos demais direitos fundamentais e humanos. É o que traduz o princípio da prevenção, delimitado

---

[234] WORLD ECONOMIC FORUM. The Global Risks Report 2022, p. 52. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Acesso em: 20 abr. 2023.
[235] MANKY, Derek. O uso da inteligência artificial e a segurança cibernética. **itforum**, 04 abr. 2020. Disponível em: https://itforum.com.br/noticias/o-uso-da-inteligencia-artificial-e-a-seguranca-cibernetica/. Acesso em: 20 abr. 2023.

no artigo 6º, inciso VIII da LGPD,[236] que exige conduta proativa empresarial na busca por evitar a ocorrência de danos decorrentes do tratamento de dados pessoais. A elaboração de relatórios, a capacitação frequente das equipes relacionadas ao tratamento de dados e, ainda, a realização de testes de aderência da IA aos resultados esperados e juridicamente permitidos deve ser a tônica sempre presente na rotina empresarial.

Um dos princípios fundantes que mais se destaca na disciplina da proteção de dados pessoais é o princípio da responsabilidade e prestação de contas, previsto no artigo 6º, inciso X da LGPD,[237] que encontra direto paralelo com o princípio da responsabilidade, previsto no art. 5(2) do RGPD europeu. Comumente denominado de *accountability*, esse princípio configura o cerne do presente capítulo, haja vista que os limites impostos pela proteção de dados pessoais ao uso da IA pelo empregador podem ser pragmaticamente analisadas conforme as medidas que ele deve seguir, baseando-se nos princípios da LGPD, atendendo aos direitos dos titulares de dados e cumprindo com os deveres de elaboração documental, apresentados na referida legislação.

Segundo apontam Bruno Bioni e Laura Mendes, isso representa o segundo dos três pilares de maior conexão entre essas normas,[238] que é o modelo *ex ante* de proteção.[239]

O princípio da responsabilidade e da prestação de contas tem como objetivo exigir, dos agentes de tratamento de dados, que eles próprios estejam aptos a comprovar sua adequação ao que diz a norma, sem necessidade de uma validação prévia. Assim, sempre que houver algum tipo de fiscalização por órgãos administrativos ou judiciais, ou ainda quando houver a solicitação de informações pelo titular de dados, deverá o agente de tratamento comprovar que está adotando as medidas legais.

Esse mecanismo apresenta um grande diferencial para o modelo de proteção de dados europeu, já que na Diretiva 95/46/CE, anterior ao RGPD, era permitido que os Estados-Membros pudessem ter legislações exigindo a validação prévia das Autoridades nacionais de proteção de dados para que determinadas operações de tratamento de dados pudessem

---

[236] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

[237] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[238] O primeiro deles é a coincidência entre os princípios, pois tiveram a mesma origem a partir dos FIPPs, já tratada no início do presente tópico.

[239] MENDES, Laura Schertel. BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, ano 28, p. 157-180, jul.-ago. 2019. p. 165.

acontecer. No entanto, o modelo anterior – de validação prévia de tratamento de dados pelas Autoridades de proteção de dados – era dificultoso na prática, pois elas não possuíam recursos suficientes para validar todos os pedidos a tempo e com a qualidade necessária, bem como passava a impressão de que bastaria a notificação para que aquela operação de tratamento estivesse autorizada.[240]

A inovação trazida pelo artigo 5(2) do RGPD representa um avanço do *Compliance* para um lugar de destaque no Direito da proteção de dados contemporâneo, tendo em vista que não havia, na Diretiva 95/76/CE, essa previsão expressa de que os agentes de tratamento deveriam demonstrar, proativamente, que cumpririam os princípios nela elencados. Portanto, o princípio da responsabilidade assume uma função nuclear na estrutura e na aplicação do RGPD.[241]

O terceiro pilar de maior conexão entre LGPD e RGPD, no entendimento de Laura Mendes e Bruno Bioni, é exatamente o papel central desempenhado pela noção de *accountability*.[242] Segundo os autores, ambas as normas de proteção de dados fornecem um "voto de confiança" nos agentes de tratamento de dados, permitindo que eles realizem suas atividades, desde que demonstrem que estão cumprindo a legislação.[243] Assim, diversos mecanismos são apresentados para que isso ocorra, tais como relatórios de impacto à proteção de dados, medidas de *privacy by design*, avaliações sobre o legítimo interesse, dentre outros.

O princípio da prestação de contas (*accountability*) e as boas práticas dele decorrentes serão abordados a partir do tópico seguinte, notadamente quanto ao uso empresarial da IA na relação de emprego.

4.2.2 Limitação a uma hipótese (ou base) legal de tratamento de dados

Outra característica relevante da LGPD é a previsão de que o tratamento de dados somente pode ocorrer se estiver dentro de uma das hipóteses legalmente previstas. Essas hipóteses autorizativas estão segmentadas de acordo com o tipo de dados pessoais que será tratado. Se forem tratados dados pessoais ordinários, aqueles sem alguma peculiar

---

[240] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation**: A Commentary. Oxford: Oxford University Press, 2020. p. 560.
[241] CORDEIRO, António Barreto Menezes. **Direito da proteção de dados à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020. p. 161-162.
[242] Previsto no RGPD no art. 5(2) e no art. 24. Previsto na LGPD no art. 6º, X.
[243] MENDES, Laura Schertel. BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, ano 28, p. 157-180, jul.-ago. 2019. p. 172.

sensibilidade, seguir-se-á o rol de hipóteses previsto no artigo 7º da LGPD.[244] Por outro lado, se o tratamento de dados envolver uma categoria especial denominada de dados pessoais sensíveis,[245] então o rol de hipóteses autorizativas será aquele previsto no artigo 11 da LGPD.[246]

Para as relações de emprego, no âmbito dos dados pessoais ordinários, as hipóteses legais mais utilizadas são: o consentimento (para a realização de processo seletivo, por exemplo); a execução de contrato (quando da contratação e durante os expedientes comuns e obrigatórios à relação de emprego); obrigação legal ou regulatória (por exemplo, quando os dados do empregado são registrados em sistema vinculado ao Poder Executivo Federal); exercício regular de direitos em processo judicial, administrativo ou arbitral; e o legítimo interesse (por exemplo, quando o empregador deseje realizar um tratamento de dados além do que seja necessário para execução do contrato de trabalho ou obrigação legal, por exemplo alguma pesquisa interna para verificar a representatividade de gênero na empresa).

---

[244] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[245] Art. 5º Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[246] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Para utilizar sistemas de IA na relação de emprego, o empregador não poderá utilizar da obrigação legal ou regulatória, por não haver exigência legal ou regulatória de uso da IA na relação de emprego. Também não lhe é autorizado fundamentar-se na execução de contrato, já que o uso da IA não é necessário para essa finalidade, que poderia ser atingida sem a aplicação dessas tecnologias (vide todas as demais empresas que executam seus contratos de trabalho sem o uso da IA). Por fim, o empregador não poderá se utilizar do exercício regular de direitos, já que processos judiciais, administrativos ou arbitrais não exigem esse tipo de tecnologia, pelo menos até hoje. Assim, restam apenas o consentimento e o legítimo interesse, para análise mais detida quanto ao uso da IA.

Ressalte-se que o consentimento não é a base legal mais indicada para a relação de emprego, tendo em vista que se trata de uma relação de hierarquia e que é dotada de subordinação do empregado pelo empregador. Portanto, não haverá como considerar o consentimento passado pelo empregado como válido, já que um dos requisitos exigidos por lei é que o consentimento seja livre, característica que se perde diante da subordinação. Ainda assim, em situações específicas, poder-se-ia admitir o registro dessa hipótese legal, por exemplo, para um processo seletivo ou alguma situação em que não haja prejuízo diante da recusa ao fornecer o consentimento pelo empregado.[247]

Ao utilizar a IA, caso o empregador fundamentasse esse tratamento de dados no consentimento (considerando uma situação hipotética em que em que o consentimento seja livre), teria de seguir diversos requisitos. O primeiro deles seria que o consentimento deve ser uma manifestação livre de vontade, portanto, demanda que as partes não tenham, naquele momento, relação de subordinação ou, caso tenham algum vínculo empregatício (por exemplo), que a recusa em fornecer o consentimento não lhe gere qualquer prejuízo. O segundo requisito é que a manifestação livre de vontade pressupõe informação, portanto deverá o titular de dados ter acesso facilitado às informações que estão previstas no artigo 9º da LGPD,[248] de forma clara,

---

[247] Nesse mesmo sentido, apontando como critério da liberdade do consentimento a análise acerca do "poder de barganha" que tem o titular de dados naquele tratamento de dados específico: BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 197.

[248] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

adequada e ostensiva. O terceiro requisito para o consentimento é que este deve ser inequívoco, devendo estar adstrito à finalidade do tratamento de dados que foi informada ao titular antes de ele formalizar a manifestação de vontade. Ainda, um quarto requisito é que esse consentimento deve ter sido fornecido para uma finalidade determinada, além do que cada nova finalidade para tratamento de dados deverá ser informada ao titular de dados, mesmo que o novo tratamento ocorra com base no legítimo interesse.

Diante desses requisitos, conclui-se que, ao se basear no consentimento como hipótese legal autorizativa do tratamento de dados, há um dever de informar ao titular de dados quando se está utilizando uma IA, tendo em vista que essa é uma das informações previstas no artigo 9º, inciso II (forma e duração do tratamento, observados o segredo comercial e industrial).

Quanto ao legítimo interesse, por se tratar de uma hipótese legal muito ampla, já que a lei não esclarece exatamente qual a finalidade do tratamento de dados nela baseado, o empregador poderia pensar em utilizá-la para todas as possíveis situações de tratamento de dados além do que já fora previsto inicialmente. Por exemplo, no caso de utilização de sistemas de IA em qualquer das fases da relação de emprego – mesmo na fase pré-contratual – (conforme exemplificado no capítulo 2 deste trabalho). O empregador poderia pensar que, já tendo havido consentimento para o processo seletivo ou já havendo justificativa com base na hipótese da execução de um contrato, para a relação de emprego em si, o legítimo interesse poderia fundamentar o tratamento de dados ordinários pela IA. Esse pensamento não está inteiramente equivocado, já que a lei não proíbe a fundamentação do uso da IA com base no legítimo interesse, mas é importante destacar que essa hipótese legal demanda um teste de proporcionalidade para que seja validada, previsto no artigo 10 da LGPD.[249]

Conforme previsão do referido artigo, o tratamento de dados pessoais baseado no legítimo interesse deverá ser realizado para finalidades legítimas, legitimidade essa que deverá ser analisada em cada situação concreta, desde que sirva para, por exemplo, apoiar ou promover as atividades do controlador de dados, para proteger o exercício regular de direitos do controlador em face do titular ou, ainda, para prestação de serviços que beneficiem o titular de

[249] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

dados. Nessas duas últimas situações, o inciso II do artigo 10 exige que sejam respeitadas as legítimas expectativas do titular de dados, bem como seus direitos e liberdades fundamentais. Para além dos requisitos ligados à finalidade, os dados que serão utilizados para esse tratamento o devem ser apenas aqueles estritamente necessários para a finalidade pretendida. Por fim, deverá o agente de tratamento adotar medidas que garantam a transparência do tratamento de dados.

Percebe-se que o teste de proporcionalidade, baseado nos requisitos acima elencados, deve sempre considerar o respeito aos direitos e liberdades fundamentais do titular, os princípios da proteção de dados pessoais (finalidade, necessidade, transparência, dentre outros), assim como a legítima expectativa do titular de dados. Caso seja essa a hipótese legal utilizada para justificar a aplicação da IA pelo empregador, deverá este reforçar as medidas de transparência para com o empregado – nos termos do parágrafo 2º do artigo 10 da LGPD –, o que demanda, por consequência lógica, o dever de informar ao titular de dados quando este estiver sendo submetido a tratamento automatizado de dados (por exemplo, quando estiver sendo utilizada uma IA).

Já no âmbito dos dados pessoais sensíveis, as hipóteses legais mais aplicáveis às relações de emprego são o consentimento (regra, nessas situações) e, excepcionalmente, para cumprimento de obrigação legal ou regulatória, para exercício de direitos em contrato ou processo judicial, administrativo ou arbitral ou para garantia da prevenção à fraude e à segurança do titular. No caso de aplicação de sistemas de IA na relação de emprego, exclui-se a obrigação legal ou regulatória, pois até o presente momento não há lei ou regulação que exija do empregador a utilização desse tipo de tecnologia. Exclui-se também o exercício de direitos em contratos ou processo judicial, administrativo ou arbitral, já que em nenhuma dessas situações o uso da IA é mandatório, restando apenas o consentimento e a garantia da prevenção à fraude e à segurança do titular como hipóteses legais assumíveis para análise mais detida a seguir.

O consentimento nas relações de emprego, como já mencionado supra, não pode ser a regra, já que dificilmente o requisito da manifestação livre de vontade será atendido, diante da presença de uma subordinação entre empregado e empregador, o que pode macular sua liberdade de manifestação. Ainda assim, considere-se a eventualidade de que o empregador consiga comprovar que a manifestação de vontade foi livre, por meio da demonstração de um "poder de barganha"[250] do empregado. Nesse sentido, a exigência da LGPD para o

[250] Novamente fazendo referência ao requisito sugerido por Bruno Bioni, referenciado na nota de rodapé nº 67.

consentimento no tratamento de dados pessoais sensíveis é mais rigorosa do que com os dados pessoais ordinários, tendo em vista que essa categoria de dados pessoais é especialmente suscetível "de utilização para fins discriminatórios, como estigmatização, exclusão ou segregação, de modo que seu tratamento atinja a dignidade de seu titular, lesionando sua identidade pessoal ou privacidade".[251]

Diante do necessário aumento da proteção a essa categoria de dados pessoais, o consentimento se torna diferenciado do que é previsto no artigo 7º da LGPD, pois deverá ser – diante do artigo 11 da LGPD – um consentimento específico e destacado. Grande parte da doutrina acompanha Bruno Bioni na crítica à redação contida nesse artigo, tendo em vista que os adjetivos que poderiam melhor endurecer o rigor quanto ao consentimento seria "expresso", ao invés de simplesmente "específico", tendo em vista que a primeira é a nomenclatura que também se utiliza no RGPD europeu e no Marco Civil da Internet brasileiro.[252] Ainda assim, a doutrina considera que os sentidos das expressões "específico" e "destacado" devem ter as seguintes acepções:

> Específico deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações de granularidade. Destacado pode ser interpretado no sentido de que é importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento, devendo tais disposições virem destacadas para que a expressão do consentimento também o seja. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento.[253]

Portanto, o consentimento como hipótese legal de tratamento de dados pessoais sensíveis, notadamente quando do uso de sistemas de IA pelo empregador, deve preceder a informação ao empregado, por meio de documentação sobre todos os fatos relevantes acerca do tratamento, destacando a ele que uma IA será utilizada para tratamento de seus dados sensíveis e dele colhendo o consentimento especificamente para tanto. Mais uma vez, o dever de informação ao empregado é reforçado.

---

[251] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 455.

[252] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 202-203.

[253] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, ano 9, n. 1, 2020. p. 34.

A outra hipótese legal autorizativa para um eventual uso de IA na relação de emprego para tratamento de dados pessoais sensíveis é aquela direcionada à garantia da prevenção à fraude e à segurança do titular, a qual se assemelha bastante à hipótese do legítimo interesse (que não é permitida para o tratamento de dados pessoais sensíveis), porém com finalidades bem mais restritivas, sendo elas garantir que aquele tratamento prevenirá a fraude ou garantir que o tratamento garantirá a segurança do titular de dados. Como exemplos, Chiara de Teffé e Mario Viola citam:

> [...] instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária por meio de um caixa eletrônico, por exemplo.[254]

Diante disso, o empregador poderia entender que, em determinada situação daquela relação de emprego, um sistema de IA que monitora os empregados por meio de reconhecimento facial (tratamento de dados biométricos) seria o instrumento adequado para garantir que não haverá fraude diante do registro de presença, baseando-se na hipótese legal ora referida.

Necessário pontuar que o parágrafo primeiro do referido artigo 11 da LGPD apresenta uma cláusula de abertura, já que mesmo aqueles dados pessoais ordinários, mas cujo tratamento revele dados pessoais sensíveis e possa causar dano ao titular de dados, também terá o mesmo tratamento dos dados sensíveis. Um exemplo dessa situação é ressaltado por Teffé e Viola, quando supõem um empregador que não trata ativamente dados de saúde de seus empregados para saber se estão doentes, mas que os rastreia por meio de dados de geolocalização (dados ordinários).[255] Esse tratamento tem o potencial eventualmente de demonstrar que o empregado encontra-se dirigindo muitas vezes ao mesmo hospital, que é especializado em doenças contagiosas ou estigmatizantes. Diante da possibilidade de revelar dados pessoais sensíveis, bem como de causar um dano ao empregado, aquele tratamento deverá seguir os mesmos requisitos de hipótese legal que os dados pessoais sensíveis.

Vistas as possíveis hipóteses legais autorizativas de tratamento de dados pessoais, ordinários e sensíveis, com as quais o empregador poderia se legitimar para o uso de sistemas de IA na relação de emprego, veja-se a seguir os direitos dos empregados, enquanto titulares de

---

[254] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, ano 9, n. 1, 2020. p. 32.
[255] Ibid., p. 35.

dados, que deverão ser atendidos pelo empregador, com especial destaque para o artigo 20 da LGPD, que trata dos direitos em face de decisões unicamente automatizadas.

4.2.3 Atendimento aos direitos dos titulares

Além dos princípios da proteção de dados pessoais e das hipóteses legais autorizativas do tratamento de dados, a LGPD trouxe aos agentes de tratamento alguns direitos dos titulares de dados que deverão ser respeitados e promovidos. O artigo 17 da LGPD[256] traduz os direitos fundantes da proteção de dados pessoais, sendo eles o direito à titularidade dos dados pessoais, o direito à liberdade, o direito à intimidade e o direito à privacidade. Eles podem ser considerados direitos fundantes pois é a partir deles, e com vistas à sua concretização, que se desenvolvem os demais direitos, previstos nos artigos 18, 19 e 20 da LGPD.

O artigo 18 da LGPD[257] traz um rol de comandos, apresentados como direitos dos titulares de dados, mas que encontram discussão doutrinária sobre sua real natureza jurídica. A

---

[256] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

[257] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

esse respeito, Eduardo Nunes de Souza e Rodrigo da Guia Silva se esses elementos seriam, de fato, "direitos" ou se seriam "remédios jurídicos", ou seja, instrumentos por meio dos quais os direitos serão realizados.[258] No entender dos autores, todos os incisos do artigo 18 da LGPD não refletem direitos propriamente ditos, mas, sim, remédios para a tutela da privacidade, na concepção já atualizada pela autodeterminação informativa. Isso, porque o conteúdo desse dispositivo não inova no rol de direitos, sendo possível verificar que já existiam vinculados à noção de privacidade, e que agora foram consagrados na forma de "medidas e procedimentos que podem ser adotados pelo titular de dados ou que devem ser implementados pelo agente de tratamento, com vistas a efetivar a tutela da privacidade e, mais do que isso, mensurar a extensão da tutela desse direito".[259] Essa delimitação jurídica dos incisos do artigo 18 é necessária para que se evite dotar a eles um valor em si mesmo ou tratá-los como poderes absolutos, já que são prerrogativas instrumentais que visam o direito à privacidade.[260] Apesar de serem remédios, não direitos em si mesmos, como a nomenclatura utilizada pela lei foi essa, seguir-se-á denominando-os como "direitos", mesmo com o cuidado de não os entender como um fim em si mesmo, mas como instrumentos para o atingimento do direito à privacidade e dos direitos expressamente elencados no artigo 17.

Mais detidamente sobre cada uma desses direitos, cumpre destacar que todos possuem relevante influência sobre a proteção de dados durante o uso da IA na relação de emprego, tendo em vista que todos esses comandos se associam diretamente ao cumprimento dos princípios da proteção de dados pessoais, já abordados na seção 4.2.1. Assim, sempre que se faça uso da IA na relação de emprego, o empregador deve atentar para a garantia dos mecanismos previstos no artigo 18 da LGPD, por exemplo, com medidas adotadas na própria arquitetura dos sistemas de IA ou, mesmo, com canais de comunicação direta com o titular de dados e diversas iniciativas de informação sobre os detalhes do tratamento automatizado de dados.

Sistematicamente, o presente trabalho dividirá os direitos (ou remédios) em sete grupos distintos, de acordo com similaridades entre eles e sua aplicação conjunta. O primeiro grupo de direitos diz respeito a ter o titular de dados a confirmação da existência de um

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.
[258] SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. **Pensar–Revista de Ciências Jurídicas**, Fortaleza, v. 24, n. 3, p. 2, 2019.
[259] Ibid., p. 10.
[260] Ibid., p. 11.

tratamento de dados (artigo 18, I) e ter acesso aos dados, objeto desse mesmo tratamento (artigo 18, II). Nessa categoria, deverá o empregador fornecer a seus empregados a possibilidade de confirmar quando seus dados serão tratados pelo empregador e saber que dados são esses. Sabe-se que, durante toda a relação de emprego, diversos dados pessoais do empregado serão tratados, para finalidades diversas, mas todas com um propósito maior: cumprir o contrato de trabalho.

Mesmo diante do poder diretivo do empregador, que lhe permite tratar dados como horário de entrada e saída, eventuais doenças que justifiquem uma falta ao trabalho, dentre outros tipos de tratamento, aquele que seja realizado com auxílio de uma IA deverá mais ainda prover esse direito aos empregados. Afinal, se o rendimento do trabalho do empregado será monitorado continuamente, por meio de dados sobre a quantidade de cliques no mouse ou da velocidade de digitação no teclado do computador, ao produzir um documento ou e-mail, deverá estar ciente de que ali está sendo alvo de um tratamento de dados e quais os dados que estão sendo considerados para avaliação de seu rendimento. Ou quando o candidato a uma vaga de emprego estiver submetido a uma etapa do processo seletivo em que, por meio de uma gamificação, a IA analisará suas reações e poderá ou não decidir por sua contratação com base nisso, deverá também o indivíduo ter ciência de que está sendo avaliado por uma máquina e quais dados estão sendo utilizados como critério para esse tratamento automatizado.

O segundo grupo de direitos diz respeito à retificação dos dados (artigo 18, III), pelo qual o empregador deverá sempre atender ao pedido do empregado que busque corrigir seus dados que estejam incompletos, inexatos ou desatualizados. Esse direito é relevante pois todo o funcionamento da IA na gestão de pessoas demandará análise de dados dos empregados e, se esses dados estiverem em alguma dessas três situações, o resultado provavelmente será equivocado e, potencialmente, prejudicial ao titular de dados. Portanto, até mesmo para reduzir a ocorrência de vieses discriminatórios, deverá sempre o empregador estimular que haja a atualização dos dados dos empregados, bem como disponibilizar a eles a possibilidade de alertar quando houver alguma incorreção ou incompletude. Ressalte-se, porém, que alguns autores afirmam não estarem incluídos nesse direito (como também não no direito de acesso, de oposição, de exclusão e de explicação) as inferências produzidas a partir do tratamento de dados, por exemplo, quando uma empresa avalia o candidato por meio de um jogo (gamificação) e cria um perfil comportamental a partir disso. Esse perfil e suas características (mais proativo, mais avesso ao risco etc.) podem ser consideradas inferências. Nesse sentido, Sandra Wachter e Brent Mittelstadt (pesquisadores do Alan Turing Institute, vinculado à Universidade de Oxford), analisaram, por meio de análise de dispositivos do RGPD, guias

orientativos do WP-29 e decisões dos tribunais europeus, se as inferências estariam ou não abarcadas pelos direitos nele previstos (similares aos previstos no artigo 18 da LGPD) e concluíram que será necessária a criação, pela jurisprudência do Tribunal de Justiça da União Europeia, de um direito às inferências razoáveis ("*right to reasonable inferences*"), ampliando o conceito de dados pessoais para que abarque também essas inferências criadas sobre os titulares de dados, mesmo que a partir de dados anonimizados.[261]

Outro grupo de direitos diz respeito ao cancelamento, o qual inclui o direito à eliminação dos dados pessoais tratados com o consentimento (artigo 18, VI), o direito à anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a lei (artigo 18, IV) e o direito à revogação do consentimento (artigo 18, IX). Segundo esses direitos, o titular de dados poderá, sempre que identificar alguma situação anômala, exercê-los, visando reduzir ou encerrar um tratamento de dados. Por exemplo, um tratamento de dados que esteja sendo realizado com base no consentimento, mas o titular queira revogar esse consentimento, terá ele esse direito e, caso queira, também a eliminação desses dados que foram tratados naquela situação.

Mais um exemplo ocorre quando o empregado verifique que seu empregador está efetuando o tratamento de dados sem conformidade com a lei, situação em que poderá solicitar e obter a eliminação desses dados, o bloqueio (temporariamente, enquanto não se regulariza o tratamento de dados) ou, ainda, a anonimização, procedimento pelo qual um dado pessoal (que identifica o titular de dados) será transformado em um dado anonimizado (incapaz de identificar o titular de dados, considerando meios técnicos de irreversibilidade).

Ainda há o direito à oposição (artigo 18, §2º), segundo o qual, diante de um tratamento de dados, que não seja baseado no consentimento, o titular que identificar alguma situação em desconformidade com a lei, poderá opor-se a esse tratamento, o qual deverá ser cessado e o titular será informado sobre as consequências dessa oposição. Por exemplo, quando o empregador esteja utilizando uma ferramenta de IA baseada no legítimo interesse, caso não haja mais a legítima expectativa do titular de dados e este deseje encerrar o tratamento, deverá ser a ele disponibilizado algum canal de comunicação pelo qual poderá opor-se a esse tratamento, mesmo que resulte em sua dispensa do trabalho ou não participação de algum benefício contratual, consequências essas que deverão ser informadas ao titular.

Também, o direito à informação, que abrange informações sobre compartilhamento de seus dados e com quem foram eles compartilhados (artigo 18, VII) e o direito à informação

[261] WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI. **Columbia Business Law Review**, v. 2019, n. 1.

sobre as consequências na negativa de fornecer consentimento (artigo 18, VIII). Nesse ponto, o direito de ter o controle dos dados pessoais (autodeterminação informativa) adquire ferramentas importantes, pois para que o titular de dados possa fornecer seu consentimento ou mesmo que forneça dados pessoais com base em outra hipótese legal, deverá estar ciente sobre quem quem terá acesso a essas informações. Ainda, caso o titular possa negar-se a fornecer o consentimento, deverá saber as consequências dessas escolhas, pois ainda que possa considerar não tão favorável transferir seus dados para aquele agente, a recusa em fornecer pode lhe trazer consequências até piores.

Por sua vez, o direito à portabilidade dos dados (artigo 18, V) representa fidedignamente a autodeterminação informativa, tendo em vista que permite ao titular de dados transferir seus dados para outro fornecedor de serviço ou produto, mediante requisição expressa, porém ainda sendo necessária a regulamentação pela ANPD sobre o tema. Apesar de carecer de regulamentação, o direito à portabilidade dos dados permite que o empregado adquira, do seu empregador, algum histórico funcional, informações sobre seu comportamento no local de trabalho, sobre seu rendimento profissional e assiduidade.

Há de se ressaltar, porém, que a lei prevê expressamente o resguardo aos direitos do agente de tratamento (no caso em comento, do empregador) em manter seu segredo comercial ou industrial, já que não será obrigado a revelar, a terceiros, informações que lhe sejam caras ao ponto de prejudicar a concorrência e o desenvolvimento de seu negócio. Da mesma forma, quando o empregador houver já anonimizado os dados pessoais do empregado, não haverá obrigatoriedade de portabilidade, já que não mais indicará o titular de dados (artigo 18, §7º).

Como dito anteriormente, os direitos relacionados mais diretamente ao uso da IA estão previstos no artigo 20 da LGPD, que abordam tanto o direito à explicação de uma decisão automatizada, quanto o direito de revisão dessa decisão e, até mesmo, uma eventual auditoria no algoritmo. Trata-se do sétimo grupo de direitos previstos na LGPD, sendo estes aqueles que mais possuem peculiaridades, segundo as quais o tratamento de dados realizado por sistemas de IA deverá respeitar. Por isso, o tema será abordado com maior profundidade.

4.2.4 Direitos em face de decisões automatizadas: o art. 20 da LGPD

Quando se trata de limites impostos pelo direito fundamental à proteção de dados quanto ao uso da IA na relação de emprego, o ponto crucial se dá no bojo do artigo 20 da LGPD,[262] o qual trata especificamente das decisões automatizadas.

O artigo 20 da LGPD consigna alguns direitos que podem ser utilizados pelos titulares de dados quando da ocorrência de tratamento automatizado. Esses direitos são aplicáveis às relações de emprego. No entanto, precisam ser analisados em seus detalhes. Dispõe o art. 20 da LGPD que "o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

A primeira parte do *caput* do artigo 20 apresenta o direito do titular de dados em solicitar a revisão da decisão automatizada, desde que ela afete seus interesses. Então, deve-se observar que não são todas as decisões automatizadas que gerarão o direito de solicitar revisão, mas apenas as decisões que impactem nos interesses do titular de dados. A expressão "afete seus interesses", contida no texto legal, parece ser um tanto abstrata, por não identificar claramente a possibilidade de uma decisão favorável ao titular de dados ser revisada. Deixa, ainda, dúvida se apenas as decisões contrárias aos interesses do indivíduo é que possam ser revisadas.

No caso da relação de emprego, uma decisão desfavorável ao empregado certamente afetará seus interesses. Outras decisões automatizadas que sejam, aparentemente, indiferentes podem gerar impactos também, principalmente porque, como já foi abordado, alguns dados aparentemente inofensivos podem ser base para um tratamento de dados que crie um perfil de conduta e, assim, gerar algum tipo de tratamento invasivo à privacidade ou mesmo discriminatório.

Mas, até mesmo as decisões que sejam favoráveis ao empregado podem guardar certas limitações, afetando ainda seus interesses. É de se questionar o seguinte: em um processo seletivo, ao ser selecionado para um cargo específico, se a decisão fosse tomada por um ser humano, poderia o candidato ter sido contratado para um cargo mais elevado na empresa? Será

---

[262] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

que outros critérios, como empatia, capacidade de interação com outras pessoas, não seriam considerados pelo entrevistador humano mais do que por uma máquina? Portanto, o simples uso da IA para tratamento de dados em um processo seletivo já aparenta ter aspectos que afetam os interesses daquele candidato em processo seletivo.

Em outras situações, como gestão algorítmica do trabalho realizado, quando o empregador aplica essas ferramentas baseadas em IA para verificar se um empregado está ou não em frente ao computador durante seu horário de trabalho, ou quando realiza análise de dados colhidos a partir de dispositivos vestíveis (*wearables*) para avaliar o rendimento e as capacidades físicas de seus empregados, questiona-se: não haveria outras formas de se atingir o mesmo objetivo, com meios menos invasivos ou com o tratamento de menos dados pessoais? Aparentemente essas situações também levam a efeitos que afetam os interesses do empregado.

Ainda, na avaliação do desempenho profissional, se um sistema de IA estiver analisando o comportamento profissional daquele empregado, estará este sempre à mercê de alguma decisão (positiva ou negativa) quanto à sua relação de emprego, seja considerando que o desempenho foi inferior, podendo gerar sanções, seja deixando de considerar resultados muito positivos gerados pelo empregado, portanto limitando-o em algum tipo de promoção de carreira. Assim, nessas situações aparentemente o uso da IA também é capaz de afetar os interesses do empregado.

O uso da IA na relação de emprego, considerando as peculiaridades como o poder diretivo e de controle do empregador, a subordinação jurídica, a nudez tecnológica do empregado, levam a considerações próprias e diferenciadas das demais relações jurídicas. Assim, uso dessas ferramentas pelo empregador sempre afetará os interesses do empregado, que se vê diante de um tratamento automatizado de dados realizado por quem possui um legítimo poder de controle sobre o seu trabalho, que se submete a um regime de subordinação jurídica e, além disso, para o qual fornece dados pessoais diariamente, pela simples realização do trabalho.

Continuando na análise do *caput* do artigo 20 da LGPD, algumas decisões automatizadas, mesmo que não afetem os interesses do titular de dados, poderão ser revisadas. São as decisões que definem seu perfil pessoal, profissional, de consumo e de crédito ou, ainda, que defina os aspectos de sua personalidade.

A criação de perfis pode ser bastante útil para finalidades relacionadas à eficiência do negócio e para atingir melhor o público desejado, porém apresentam diversos riscos à personalidade dos indivíduos. Na relação de emprego, o empregado, já fragilizado em decorrência do poder de controle pelo empregador e da grande quantidade de dados pessoais

compartilhados com aquele, encontra-se em situação de ainda maior vulnerabilidade com a criação de perfis comportamentais.

Como ressaltado por Teresa Coelho Moreira, a utilização de tecnologias de informação e comunicação nas relações laborais deverá sempre seguir alguns limites, sendo o mais importante deles a consideração de que o empregado é um sujeito, não mero objeto.[263]

Dessa forma, quando o empregador utiliza IA para a definição de perfil profissional do seu empregado, ou mesmo de um candidato à vaga de emprego, deverá sempre respeitar as características individualizadas, não sendo permitido que o indivíduo seja tão somente um instrumento para atingir uma finalidade econômica. Para tanto, não poderá basear-se tão somente no resultado algorítmico para tomar decisões acerca do empregado, sendo necessário que haja a participação de um ser humano na tomada daquela decisão.

Enquanto isso, o § 1º do art. 20 da LGPD prevê o direito à explicação de decisões automatizadas na LGPD, já que o agente de tratamento deverá fornecer informações sobre aquela decisão. No entanto, essa previsão legal apresenta uma mitigação do princípio da transparência, já que, nos casos envolvendo decisões automatizadas, o agente de tratamento apenas deverá fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados caso seja dele solicitado.

A preferência do legislador, na referida norma, deu-se para resguardar o segredo comercial e industrial, ou seja, em manter intocáveis as informações mais estratégicas por trás do desenvolvimento daquela aplicação de Inteligência Artificial.

Por outro lado, essa mitigação pode ser prejudicial, tendo em vista que o direito à revisão de decisões automatizadas somente ocorrerá caso se saiba que o tratamento automatizado esteja ocorrendo, o que, muitas vezes, pode ser mascarado, principalmente nas relações de emprego, diante do poder de controle e da subordinação inerentes a essa relação.

Ainda que se preveja essa mitigação da transparência pela necessidade de solicitação de informações pelo titular de dados (no caso, o empregado), o direito à explicação de decisões automatizadas representa relevante mecanismo para buscar o respeito à proteção de dados pessoais. Se os algoritmos são considerados verdadeiras "caixas pretas", deverá o agente de tratamento (nesse caso, o empregador) promover meios pelos quais seja possível apresentar informações sobre aquela decisão automatizada e, portanto, tornar a IA de algum modo explicável.

---

[263] MOREIRA, Teresa Coelho. Novas tecnologias: um admirável mundo novo do trabalho? **Revista de Direitos e Garantias Fundamentais**, n. 11, p. 15-52, 2012. p. 32.

Já no § 2º, é explicitado que a auditoria nesses critérios, pela ANPD, somente ocorrerá caso o agente de tratamento se recuse a fornecer tais informações, o que limita ainda mais o poder fiscalizatório dessa Autoridade, fragilizando o exercício dos direitos do titular. Nesse contexto, a ausência de referência a algum mecanismo efetivo na legislação brasileira atua como fator de aprofundamento dessa deficiência de auditoria nos mecanismos tecnológicos utilizados pelo empregador..

Outros países encontraram, além da legislação de proteção de dados, regramentos específicos para proteção de trabalhadores, principalmente considerando sua especial fragilidade. Na França, por exemplo, os direitos dos trabalhadores em face de tecnologias intrusivas são expressamente garantidos na legislação. O Código Civil francês, ao tratar da coleta de dados de empregados, baseia-se em três princípios básicos: transparência ou lealdade; proporcionalidade; e relevância. Com base na transparência, os empregados devem sempre ser informados sobre utensílios de vigilância antes mesmo de sua instalação. A partir da proporcionalidade, qualquer restrição imposta a empregados deve ser devidamente justificada e comprovadamente proporcional à finalidade pretendida. Baseando-se na relevância, toda tecnologia implementada deverá ser relevante ao propósito de melhoria de suas habilidades profissionais.[264]

Em Portugal, como explica Teresa Coelho Moreira, o artigo 25º, n. 1, do DL 260/2009, estabelece o direito do candidato a emprego de ser informado, por escrito, sobre os métodos e técnicas de recrutamento aos quais será submetido, além das regras relativas a eles, o que poderia ser considerado um caminho para a redução de preconceitos sociais resultantes das tecnologias nas relações de trabalho.[265]

No RGPD europeu, há grande debate doutrinário acerca da existência ou não de um real direito à explicação de decisões automatizadas. Grande parte do debate iniciou entre professores ligados à Universidade de Oxford, ao analisarem os contornos iniciais do RGPD e sua possível aplicação após o início da vigência.

O primeiro artigo que chamou a atenção sobre o tema foi produzido por Bryce Goodman e Seth Flaxman.[266] Os autores trouxeram ponderações de que o RGPD estaria prevendo um direito à explicação de decisões automatizadas, principalmente baseando-se nos

---

[264] DE STEFANO, Valerio. *Op. Cit*., p. 117.

[265] MOREIRA, Teresa Coelho. Principais repercussões da utilização de sistemas de inteligência artificial por agentes empresariais no âmbito do direito do trabalho – algumas questões. *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019. p. 412.

[266] GOODMAN, Bryce; FLAXMAN, Seth. European union regulations on algorithmic decision making and a "right to explanation". **AI Magazine**, v. 38, n. 3, p. 50–57, 2017.

deveres dos responsáveis pelo tratamento em informar aos titulares de dados sempre que houvesse a utilização de decisões automatizadas, bem como da lógica subjacente e das consequências previstas para esse tratamento automatizado de dados, previstos nos artigos 13(2), f e 14(2), g. Além disso, também reconheceu o direito à explicação no artigo 15(1), h, que prevê o direito de acesso do titular de dados a informações sobre essas decisões automatizadas, nos mesmos termos dos artigos que tratam sobre o dever de informar do responsável pelo tratamento. Para esses autores, o ponto chave desses dispositivos estaria no significado de "informações úteis" *meaningful information*), o que garantiria um real direito à explicação da lógica envolvida nas decisões automatizadas.

Em resposta a esse artigo inicial, Sandra Wachter, Brent Mittelstadt e Luciano Floridi[267] desenvolveram um artigo bastante provocativo, propondo, em seu título, que não haveria um "direito à explicação" no RGPD. Apesar do título, os autores buscam diferenciar o direito à explicação (não previsto no RGPD) de um direito de ser informado, este, sim, segundo eles, presente no RGPD. A premissa básica do artigo é a diferenciação entre a explicação das funcionalidades do sistema (envolvendo a lógica, o grau de significância de certas informações, as consequências previstas e a funcionalidade geral daquele algoritmo) e a explicação sobre uma decisão específica (incluindo as razões da decisão e as circunstâncias individuais ponderadas para que aquela decisão específica tenha sido gerada). O que os autores defendem é que o direito a ser informado (previsto nos artigos 13 a 15 do RGPD) apenas garante a explicação das funcionalidades do sistema, mas não garante que o titular de dados tenha explicado os motivos e critérios para que aquela sua decisão específica tenha sido tomada daquela forma. Apontam, ainda, que mesmo o considerando 71 do RGPD prevendo a explicação dos critérios de uma decisão automatizada específica, pelo fato de que considerandos[268] não possuem caráter vinculativo, não haveria esse direito expressamente garantido, apenas sugerido pelo RGPD.

Em resposta a esse debate inicial, Andrew Selbst e Julia Powles apresentaram uma terceira visão sobre o tema,[269] criticando a ideia proposta por Wachter e os demais, de não haver um direito à explicação no RGPD (inclusive, apontando que os autores do segundo artigo

---

[267] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017.

[268] "Considerandos", no RGPD europeu, são disposições preliminares, que contextualizam e fornecem informações de caráter mais aberto do que as normas, com o propósito de também auxiliar as partes a melhor entender as disposições do RGPD.

[269] SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, p. 233-242, 2017.

prometem algo no título, mas não cumprem o prometido no decorrer do seu artigo), mas também indicam que a ideia inicialmente proposta por Goodman e Flaxman não foi bem fundamentada. Sobre o assunto, os autores do terceiro artigo consideram que a distinção entre a explicação de funcionalidades do sistema e de uma decisão específica pode ser relevante, mas na prática é inviável separar as informações de ambas, tendo em vista o caráter determinístico dos modelos de decisão automatizada (se os mesmos dados forem apresentados ao mesmo algoritmo, para os autores, a decisão deverá ser a mesma, não havendo essa separação tão distante entre uma explicação da funcionalidade ou da decisão específica). Assim, os autores propõem que o termo "informações úteis sobre a lógica" da decisão, previsto nos artigos 13 a 15 do RGPD, seriam equivalentes a informações que poderiam explicar também a decisão específica, não apenas a lógica geral de uma decisão automatizada.

Esse debate foi travado antes mesmo do início da vigência do RGPD (2017), mas encontra relevo desde então. Acadêmicos de diversas posições associam-se a um ou outro posicionamento, criticando ou defendendo a redação do RGPD quanto ao direito à explicação de decisões automatizadas. O que esse debate demonstra é que o texto do RGPD, mesmo sendo mais descritivo e detalhista do que a LGPD, também contém pontos lacunosos, que mereceriam uma redação mais objetiva e que pudesse esclarecer melhor seu âmbito de aplicação.

Ao contrário do RGPD, a LGPD possui apenas um parágrafo de um artigo falando especificamente sobre esse tema (art. 20, §1º). Apesar de sua objetividade, referido parágrafo diz expressamente que, ao ser solicitado, o controlador de dados possui o dever de fornecer "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada". Adotando uma visão analítica do dispositivo, percebe-se que está previsto não apenas uma informação sobre as funcionalidades do sistema (direito a ser informado, na visão de Watcher e outros[270]), mas também informações sobre os critérios e os procedimentos que levaram àquele resultado específico (direito à explicação proposto pelos referidos autores).

Renato Leite Monteiro, que rejeita a interpretação de Wachter e de seus coautores, afiliando-se ao entendimento proposto por Selbst e Powles, chega à mesma conclusão, pontuando que, na lei brasileira, "a explicação deve incluir não somente informações sobre os

[270] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017. *passim*.

dados pessoais que serviram de substrato para o algoritmo, mas também sobre a lógica por trás de tais decisões".[271]

Assim, mesmo que se considere a visão mais restritiva do direito à explicação, na forma proposta por Wachter e os demais, a LGPD deixa bem claro que o direito à explicação de decisões automatizadas, no Direito brasileiro, envolve também as informações que levaram àquele resultado, incluindo critérios e procedimentos.

Seguindo na análise do direito à explicação, Monteiro ressalta que esse direito no contexto brasileiro é ainda mais alargado, permitindo até mesmo que se verifique o direito à explicação de uma decisão automatizada que seja baseada em dados anonimizados (segundo o artigo 5º, III seriam aqueles dados que não permitem a identificação do titular de dados), os quais tenham como finalidade a formação de perfis comportamentais,[272] conforme previsão do artigo 12, *caput* e §2º, da LGPD.[273]

Outro mecanismo relacionado ao direito à explicação que possui previsão na LGPD, mas não no RGPD, é quando a explicação dos critérios e procedimentos que levaram até aquela decisão automatizada encontra óbice quanto ao segredo comercial e industrial, limitação essa prevista expressamente pelo artigo 20, §1º da LGPD.[274] Conforme previsto no parágrafo segundo, caso o controlador de dados se recuse a fornecer tais informações, com base no segredo comercial ou industrial, poderá a Autoridade Nacional de Proteção de Dados realizar auditoria, visando verificar a ocorrência de aspectos discriminatórios naquele tratamento automatizado de dados.

No RGPD europeu, é prevista, no considerando 63, a proteção do segredo comercial e da propriedade intelectual, não especificamente nos casos de explicação de uma decisão automatizadas, mas quanto ao direito de acesso aos dados pessoais. É também previsto no RGPD, como um dos poderes das Autoridades de Proteção de Dados, a realização de auditorias sobre a proteção de dados. No entanto, não há previsão expressa sobre a possibilidade de auditoria das Autoridades de Proteção de Dados quanto a essa situação, o que já se revela uma

---

[271] MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, v. 39, p. 1-27, 2018. p. 13.
[272] Ibid., p. 10.
[273] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
[274] Art. 20. [...] § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

fragilidade, pois não expressamente autoriza que a auditoria seja realizada mesmo ultrapassando o segredo comercial e industrial.

Esse mecanismo é relevante, principalmente considerando que algoritmos também podem gerar decisões automatizadas que sejam discriminatórias, seja pela generalização das decisões com base em perfis comportamentais, pela baixa qualidade dos dados utilizados, pela utilização de dados pessoais sensíveis ou mesmo pela limitação do exercício de outros direitos.[275] Diversos casos de discriminação gerada por algoritmos são citados na doutrina,[276] sendo que a opacidade desses algoritmos, ou seja, sua dificuldade de entendimento dos critérios e procedimentos utilizados para atingir uma decisão, são os maiores impasses para que o titular de dados e as Autoridades de Proteção de Dados possam efetivamente garantir o princípio da não discriminação, nesses casos.

Nada obsta, no entanto, que as Autoridades de Proteção de Dados dos Estados-Membros possam ampliar o escopo de aplicação do direito à explicação, até mesmo da realização de auditorias ou outros mecanismos de garantia da transparência das decisões automatizadas. Em estudo realizado sobre esse tema, Bryan Casey, Ashkon Farhangi e Roland Vogl analisam o debate traçado em torno do direito à explicação no contexto europeu, mas superam-no com uma visão pragmática do assunto: se não há uma clareza no texto do RGPD, as Autoridades de Proteção de Dados, por outro lado, debruçaram-se sobre esse objetivo de tornar as decisões automatizadas mais explicáveis, indicando diversas medidas que são mais efetivas para tanto.[277] Afinal, se o grande debate traçado entre os acadêmicos de Oxford era em torno do que significariam as "informações úteis" sobre a lógica das decisões automatizadas, tratando-se de um conceito aberto, caberia a essas Autoridades definir tais informações e de que maneira os responsáveis pelo tratamento poderiam explicá-las aos titulares de dados.

De modo prático, essa dificuldade em tornar as tecnologias algo explicável demanda esforço não apenas dos agentes de tratamento, mas também dos órgãos reguladores. No Brasil, a ANPD está em sua agenda regulatória 2023/2024,[278] na qual estão inseridos planos de regulamentar os direitos dos titulares de dados, dentre os quais está implícito o direito à

---

[275] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, v. 16, n. 90, p. 39-64, 2019. *passim*.

[276] Diversos exemplos de discriminação algorítmica são citados por O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016. Sobre a opacidade dos algoritmos, vide: PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

[277] CASEY, Bryan; FARHANGI, Ashkon; VOGL, Roland. Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. **Berkeley Tech. LJ**, v. 34, p. 143, 2019.

[278] BRASIL. Autoridade Nacional de Proteção de Dados. ANPD publica Agenda Regulatória 2023-2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024. Acesso em: 20 abr. 2023.

explicação, e regulamentar a IA, regulação esta que demandará preocupações com a explicabilidade dos sistemas algorítmicos.

4.2.5 Relatório de Impacto à Proteção de Dados

Outra previsão da LGPD que possui conexão direta ao uso de sistemas algorítmicos pelo empregador para tratamento de dados pessoais do empregado diz respeito à realização de Relatório de Impacto à proteção de dados (RIPD). Essa ferramenta, cuja definição encontra-se expressa no artigo 5º, XVII da LGPD,[279] representa uma medida que pode ser exigida do controlador de dados, caso o referido tratamento ocorra de modo a eventualmente gerar riscos às liberdades civis e direitos fundamentais dos titulares. Nesse documento deverão constar os riscos envolvidos naquele tratamento assim como as medidas, salvaguardas e mecanismos para mitigação desses riscos.

Quando se fala em uso da IA na relação de emprego, estão envolvidos diversos riscos à proteção de dados pessoais, seja aos direitos de personalidade, com especial risco à privacidade, seja aos direitos à igualdade e não discriminação no local de trabalho. Assim, diante da aplicação dessas tecnologias pelo empregador, este poderá elaborar Relatório de Impacto à proteção de dados, visando apresentar quais os riscos envolvidos naquele tratamento automatizado, especificamente, assim como demonstrar quais medidas o empregador adota, para mitigar os riscos e, assim, legitimar o uso desses sistemas de IA. Em complemento, o parágrafo único do artigo 38 da LGPD[280] acrescenta algumas informações que também deverão fazer parte do RIPD, como a descrição do tipo de dados pessoais coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, além da análise, pelo controlador de dados, acerca das medidas, salvaguardas e mecanismos que sejam adotadas para mitigar o risco.

No entanto, a previsão da LGPD quanto à obrigatoriedade do RIPD é alvo de divergências doutrinárias, já que a previsão no texto da lei é lacunosa. Segundo dispõe o *caput*

---

[279] Art. 5º Para os fins desta Lei, considera-se: [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

[280] Art. 38. [...] Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

do artigo 38 da LGPD,[281] a elaboração do RIPD poderá ser determinada pela ANPD, reforçando-se que a lei utiliza o verbo "poderá", que indica uma possibilidade, não uma obrigatoriedade. Assim, a interpretação literal pode levar o leitor a considerar que a elaboração do RIPD não é obrigatória a todos os agentes de tratamento de dados, passando a ser obrigatório apenas quando a ANPD determinar que o seja.

Em complemento, o parágrafo terceiro do artigo 10 da LGPD indica que a ANPD poderá (novamente utilizando o verbo que indica possibilidade) solicitar (diferentemente do artigo 38, que fala "determinar") Relatório de Impacto à proteção de dados quando o tratamento de dados tiver como fundamento o legítimo interesse. Nessa situação, além da dúvida também gerada pelo verbo poderá (que poderia representar uma faculdade de ação da ANPD), ainda há o complemento com um verbo, que a ANPD poderá "solicitar" esse relatório, dando a impressão de que o agente de tratamento poderá recusar-se a apresentar esse documento, já que apenas será solicitado, não determinado ou requisitado.

A ANPD, mesmo já tendo indicado que regulamentará a matéria em sua agenda para o biênio 2023/2024, ainda não apresentou algum guia orientativo ou resolução sobre a matéria. Ainda assim, em 06 de abril de 2022, apresentou uma página em seu site[282] com perguntas e respostas sobre o tema Relatório de Impacto à proteção de dados, no qual esclarece alguns dos questionamentos suscitados pela doutrina desde a edição da LGPD. Por exemplo, a ANPD explica que quando houver a "solicitação" pela ANPD, conforme previsto no artigo 10, parágrafo terceiro da LGPD, o agente de tratamento deverá (ressaltando o verbo que indica obrigatoriedade) elaborar o RIPD.

Mesmo diante de tantas lacunas, Maria Cecília Gomes ressalta que o RIPD não pode significar apenas um documento, gerado para apresentar conformidade com a lei, mas deve ser entendido como uma forma de demonstrar uma avaliação prévia (avaliação de impacto à proteção de dados), que deve ser feita pelo controlador de dados antes de implementar qualquer novo produto, serviço ou tecnologia, visando avaliar os impactos que estes poderão gerar aos direitos dos titulares de dados.[283] Gabriel Hayduk complementa que a "estrutura do RIPD poderá ajudar a alcançar o ponto ótimo do balanceamento entre os diferentes elementos

---

[281] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

[282] BRASIL. Autoridade Nacional de Proteção de Dados. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais. Acesso em: 25 abr. 2023.

[283] GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista da AASP,** (144), 2019. p. 180.

envolvidos" na análise de riscos e benefícios da utilização de determinada tecnologia pelas empresas.[284]

Tendo isso em vista, antes mesmo de aplicar algum sistema de IA na relação de emprego, uma análise de risco poderá identificar quais as possíveis situações prejudiciais ou violadoras aos direitos dos empregados. Ao identificar quais os riscos envolvidos, o empregador poderá propor medidas, salvaguardas ou mecanismos, com vistas a reduzir o impacto desses riscos ou, até mesmo, evitar que ocorram. Caso o empregador verifique que as medidas sugeridas não serão suficientes para mitigar os riscos envolvidos, não poderá aplicar aquela tecnologia, caso contrário estará violando os princípios da LGPD, mais especificamente o princípio da prevenção (pois não estará adotando medidas para evitar o risco), o princípio da segurança (pois não adotará medidas de segurança capazes de proteger os dados pessoais) e da responsabilização e da prestação de contas (pois as medidas não são eficazes para o cumprimento das normas de proteção de dados pessoais).

O RIPD, além de uma ferramenta para documentar uma avaliação que busca mitigar os riscos possíveis em um tratamento de dados, pode ser considerada como uma forma de documentação das medidas adotadas pelo empregador, servindo para cumprimento do que estabelece o princípio da prestação de contas (*accountability*). O RIPD não é a única forma de evidenciar esse princípio, tendo em vista que a LGPD dispõe de diversos elementos capazes de viabilizar o tratamento de dados, conforme já foram abordados os requisitos no presente tópico. Diante dos requisitos impostos pela LGPD, o empregador deverá cumpri-los, sob pena de desrespeitar as normas de proteção de dados pessoais.

No entanto, para além das obrigações legais, a LGPD também propõe, no artigo 50,[285] que os próprios agentes de tratamento formulem regras de boas práticas e de governança de dados, inclusive regras específicas para os envolvidos no tratamento de dados. Diante dessa previsão, assim como pela ausência de normas específicas quanto à proteção de dados na relação de emprego e, menos ainda, quanto ao uso da IA, o presente trabalho proporá algumas das medidas de boas práticas que possam ser aptas a demonstrar que o empregador esteja

---

[284] HAYDUK, Gabriel. Requisitos do relatório de impacto à proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 571-572.

[285] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

cumprindo as normas de proteção de dados diante do uso da IA, cumprindo com o princípio da *accountability*.

4.3 *Accountability*: boas práticas de governança de dados diante do uso da IA pelo empregador

Na concepção de Caitlin Mulholland e Rodrigo Gomes, algumas características da LGPD influenciam mais diretamente as regras, especialmente quanto ao uso da IA e a proteção de dados pessoais. A primeira dessas características é a estrutura principiológica nela prevista, que traduz uma gama de valores a serem promovidos pelos agentes de tratamento, permitindo que haja o controle de novas tecnologias (tais como a IA), de uma forma mais atualizável do que regras mais fechadas.[286] A segunda característica relevante da LGPD para esse propósito é o reconhecimento da lei de que os próprios agentes de tratamento devem formular regras de boas práticas e de governança de dados, conforme previsto no artigo 50.[287] Ainda segundo os autores, a soma desses fatores contribui para que os agentes de tratamento possam mitigar riscos no tratamento de dados, promovendo transparência e afastando a responsabilização por eventuais danos causados aos titulares.[288]

Por tal razão, o dever de prestação de contas pelo empregador deve ser o grande guia para buscar a efetivação do direito fundamental à proteção de dados do empregado. Somente a exigência legal de cumprimento das normas não proporciona o mesmo grau de efetividade, já que a aplicação desses sistemas de IA e as regras de seu funcionamento poderão ser, como geralmente são, mascaradas dos titulares de dados (empregados), de terceiros interessados (sindicatos, Ministério do Trabalho e Emprego, Ministério Público do Trabalho) e do Poder Judiciário. Quando se exige do agente de tratamento, para além do cumprimento da norma, a apresentação de evidências de que ele está cumprindo a norma, bem como a formulação de boas práticas para melhor evidenciar isso, surgem algumas situações favoráveis, como o engajamento empresarial advindo da necessária criação de um programa de governança de dados, a possibilidade de fiscalização pelo titular de dados a partir da documentação que presta contas e a auditabilidade daquele agente de tratamento por terceiros interessados e órgãos fiscalizadores.

---

[286] MULHOLLAND, Caitlin; GOMES, Rodrigo Dias de Pinho. Inteligência Artificial e seus principais desafios para os programas de *compliance* e as políticas de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 162.
[287] Ibid.
[288] Ibid., p. 162.

Dentre as medidas concretas, necessárias para que os agentes de tratamento de dados pudessem efetivamente utilizar os dados pessoais, encontra-se uma linha norteadora mestra, que é o princípio da responsabilização e da prestação de contas. Previsto no artigo 6º, inciso X da LGPD,[289] esse princípio dispõe expressamente que qualquer organização, pública ou privada, ou mesmo pessoa natural, que trate dados pessoais com finalidade econômica, deverá demonstrar que adota medidas eficazes e capazes de comprovar que observa e cumpre as normas de proteção de dados, comprovando inclusive sua eficácia.

Esse princípio decorre de um movimento internacional em torno do termo "*accountability*", que não possui tradução direta ao português, mas que representa essa responsabilização de agentes em realizar determinada atividade com proatividade e demonstração ativa de que cumpre com as normas de forma responsável.

No entender de Nelson Rosenvald e José Faleiros Júnior, a LGPD faz parte de uma tendência regulatória mundial de superação do modelo de regulação baseada no comando e controle, em que a lei possui comandos objetivos e os agentes devem segui-los fidedignamente, sob pena de medidas de controle. Caminha-se, assim, para um modelo de estruturas mais abertas, aprimoradas pelos preceitos do *compliance*.[290]

Percebe-se essa abertura maior da regulação quando a LGPD, em regra, não proíbe o tratamento de dados, mas proporciona princípios, que deverão ser considerados; requisitos legais para tratamento de dados (ou bases legais), que deverão ser registrados; e direitos dos titulares de dados, que deverão ser respeitados. Diante desse cenário, cumpridos esses pontos principais, a lei possibilita que os agentes de tratamento procedam com o tratamento dos dados pessoais, depositando neles a confiança para que possam controlar os riscos envolvidos em suas atividades e buscar sua mitigação.

No entanto, mesmo diante da confiança recebida da lei, os agentes de tratamento recebem um ônus de responsabilidade e prestação de contas, previsto no artigo 6º, inciso X, outrora referenciado. Nessa previsão legal, percebe-se que o conceito jurídico

---

[289] Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[290] ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. *Accountability* e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 772.

"responsabilidade" é dotado de relevante polissemia, derivada da nova tendência regulatória (mais aberta e voltada ao *compliance*), e reflexo da sua ampliação conceitual no mundo.[291]

Após pesquisa realizada com base nos quase dez anos de tramitação de projetos de lei sobre a proteção de dados no Brasil, até culminar na aprovação da LGPD em 2018, Bruno Bioni constata que o grande fio condutor dessa evolução de propostas normativas é "a progressiva delegação de uma série de competências decisórias aos agentes de tratamento de dados".[292] Por isso, continua o referido autor, os agentes de tratamento ganharam maior discricionariedade para significar conceitos jurídicos indeterminados e para escolher as medidas adequadas para cumprir a lei,[293] sendo possível concluir que "o princípio da *accountability* na LGPD é o que melhor ilustra o processo de mutação pelo qual o texto da lei sofreu ao longo das nove fases mapeadas ao longo de quase dez anos".[294]

Na língua inglesa, existem pelo menos quatro acepções para o conceito jurídico "responsabilidade". A primeira delas é a "*liability*", que representa mais diretamente o que no Brasil se entende pela "indenização haurida pelo nexo causal que conecta conduta e dano, acrescida por outros elementos aferidos em conformidade com o nexo de imputação concreto, tendo em conta as peculiaridades de cada jurisdição".[295] A segunda acepção é "*responsibility*", que "denota o sentido moral de responsabilidade, voluntariamente aceito e jamais legalmente imposto".[296] A terceira acepção é a "*answerability*", que pode ser traduzida como "explicabilidade", impondo "mais uma camada da função preventiva da responsabilidade, materializada no dever recíproco de construção da fidúcia a partir do imperativo da transparência".[297] Por fim, a "*accountability*", concepção ampliada da responsabilidade, pois derivada da tendência de "inclusão de parâmetros regulatórios preventivos, que promovem uma interação entre *liability* do Código Civil e a regulamentação voltada à governança de dados, seja em caráter *ex ante* ou *ex post*".[298]

Assim, segundo constatam Nelson Rosenvald e José Faleiros Júnior, a LGPD fez a escolha de privilegiar, como princípio da proteção de dados pessoais, uma junção entre *liability*

---

[291] ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. Accountability e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.
[292] BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais**: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 52.
[293] Ibid.
[294] Ibid., p. 70.
[295] Ibid., p. 774.
[296] Ibid., p. 775.
[297] Ibid., p. 776.
[298] Ibid., p. 777.

(responsabilização) e *accountability* (prestação de contas).[299] Dessa forma, o agente de tratamento deverá resguardar-se quanto às medidas adotadas no tratamento de dados pessoais, visando evitar a ocorrência de danos e, portanto, evitar sua responsabilização civil (*liability* ou responsabilização), por meio da prestação de contas sobre as medidas e boas práticas adotadas, demonstrando que elas são aptas a mitigar os riscos envolvidos no tratamento de dados (*accountability* ou prestação de contas).

Corroborando essa tendência regulatória mais aberta, Eduardo Magrani e Paula Guedes entendem que a regulação dos sistemas de IA não será suficiente se for restrita ao Direito, tendo em vista a progressiva e constante complexidade desses sistemas, devendo haver também atenção para normas sociais, para questões mercadológicas e para a própria forma como se constrói a arquitetura dos sistemas, ou seja, os códigos de programação.[300]

Por isso, os referidos autores sugerem algumas boas práticas que podem aprimorar a já existente regulação sobre o tema. Primeiramente, que o próprio design das ferramentas baseadas em IA seja construído alinhado com diretrizes éticas e com a doutrina dos direitos humanos. É o movimento denominado "design sensível a valores", que demanda desses sistemas não apenas o cumprimento do quadro regulamentar vigente, mas também deve haver preocupação dos desenvolvedores com os valores humanos, na fase de concepção da IA e por padrão, na usabilidade pelos usuários.[301] O segundo grupo de boas práticas é relacionado à implementação de relatórios de impacto, já que a LGPD prevê, em seu artigo 38, caput e parágrafo único, a obrigatoriedade de elaboração do RIPD (Relatório de Impacto à Proteção de Dados), mas os autores sugerem como boa prática sua realização sempre que houver desenvolvimento e utilização de sistemas de IA para decisões automatizadas.[302] Um terceiro grupo de boas práticas sugeridas pelos autores é a garantia de maior transparência e explicação da IA, para que os sistemas possam incorporar arquiteturas e códigos "projetados para explicar seu raciocínio e permitir que os humanos interpretem seus resultados".[303] Outro grupo de boas práticas é relacionado à autorregulação, por meio da qual as empresas também possam criar suas próprias regras e códigos de conduta para que insiram em suas estruturas padrões éticos que possam auxiliar sua conformidade com a lei.[304]

---

[299] BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais**: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 778.
[300] MAGRANI, Eduardo; GUEDES, Paula. Inteligência Artificial: desafios éticos e jurídicos. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 83.
[301] Ibid., p. 84.
[302] Ibid., p. 85.
[303] Ibid., p. 86.
[304] Ibid., p. 87.

Como forma de contribuir com o debate, o presente estudo sugere um rol de boas práticas que possam ser utilizadas pelo empregador, visando cumprir com a legislação de proteção de dados na utilização de sistemas de IA na relação de emprego, assim como prestando contas desse cumprimento da legislação.

A primeira medida de boas práticas é a necessária governança de dados que envolva toda a cadeia de tratamento de dados. Quando um empregador contrata um sistema de IA pertencente a terceiros, por exemplo, alguma empresa de tecnologia como a Amazon, a Microsoft ou alguma empresa de âmbito nacional, não apenas o empregador deve responder pela regularidade do tratamento de dados, igualmente a empresa proprietária e/ou desenvolvedora daquele sistema deverá ser responsabilizada pelas medidas de adequação à proteção de dados pessoais e à mitigação de riscos. Ambas as empresas serão consideradas agentes de tratamento, sendo possível que se enquadrem como controladores de dados (aqueles que tomam decisões acerca do tratamento de dados pessoais) e/ou operadores de dados (aqueles que seguem as orientações do controlador quanto ao tratamento de dados pessoais).

O artigo 42 da LGPD estabelece a responsabilidade civil dos agentes de tratamento em caso de danos ocasionados por descumprimento da legislação. Especialmente o parágrafo primeiro estabelece a responsabilidade solidária do operador de dados quando este descumprir as orientações lícitas do controlador. Já o parágrafo segundo dispõe que os controladores que estejam diretamente envolvidos no tratamento responderão também solidariamente pelos danos ocasionados. Assim, diante de qualquer das situações (operadoria ou controladoria), as empresas responderão em conjunto. Se uma das empresas dessa cadeia de tratamento de dados for apenas operadora, deverá sempre realizar um filtro para avaliar se as determinações do controlador de dados serão lícitas, caso contrário será responsabilizada solidariamente. Se o controlador de dados – que, provavelmente, será o empregador, por ser parte da relação jurídica com o titular de dados, empregado – contratar uma empresa que será operadora dos dados e utiliza a plataforma dessa empresa para tratamento de dados pessoais que gera riscos aos direitos dos empregados, deverá a empresa proprietária da tecnologia também responder por danos ocasionados, já que deveria ter validado se o uso daquela tecnologia o seria para fins lícitos. Para além da preocupação com responsabilização por possíveis danos, também deverá estar dotada de mecanismos que assegurem que aquela tecnologia não causará danos ou violações aos direitos dos titulares de dados, notadamente direitos fundamentais, sociais e trabalhistas.

Em um cenário em que o uso da IA pelo empregador gera mais e mais terceirização de responsabilidades, por reduzidas iniciativas de desenvolvimento de tecnologias pelos

próprios setores de RH das empresas, estas, ao contratarem suas fornecedoras de tecnologia baseadas em IA, deverão sempre realizar uma fiscalização prévia dessas empresas e tecnologias, denominada comercialmente como *due diligence*. Esse procedimento deve ocorrer, por meio da cobrança pelo empregador de relatórios de impacto, políticas de segurança da informação e mecanismos presentes na própria arquitetura do sistema de IA que garanta sua explicabilidade. Afinal, se um titular de dados exigir do empregador uma explicação daquela decisão automatizada, deverá este saber responder-lhe a contento, dependendo assim da cooperação da empresa terceira.

Uma segunda medida de boas práticas que se sugere neste trabalho é o mapeamento de riscos a direitos dos empregados e a adoção do princípio da precaução pelo empregador. O princípio da precaução pode não estar previsto textualmente na LGPD, mas advém do Direito Ambiental e propõe que, diante de condutas que tenham alto grau de incerteza quanto aos riscos e danos, deve-se possuir uma razão amplamente justificada para tomar determinadas decisões sobre aquele tema[305]. Dessa forma, sugere-se que os empregadores adotem sempre decisões baseadas no princípio da precaução, por meio da categorização dos sistemas de IA que serão utilizados conforme o grau de risco.

Esse tipo de metodologia (categorização das tecnologias de IA com base no risco) está contida na proposta de regulação da IA pela União Europeia e na proposta de regulação da IA, produzida pela Comissão de Juristas do Senado brasileiro[306]. Em ambos, a utilização da IA nas relações de trabalho figura como tendo alto risco, demandando sempre os maiores cuidados e mais relevantes obrigações e limitações pelos agentes de tratamento[307]. Assim, o mapeamento dos riscos pelo empregador se torna imperioso, diante do potencial de alto risco gerado pelos

---

[305] Para esse propósito, Bruno Bioni e Maria Luciano realizam um apurado de diversas aplicações do princípio da precaução no Direito Ambiental internacional, culminando com o entendimento de que o referido princípio tem por foco determinar as razões para a tomada de uma decisão regulatória. BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019. p. 214.

[306] Essa metodologia dispõe que cada tipo de tecnologia ou finalidade de uso da tecnologia será categorizado de acordo com alguns critérios e estratos, entre baixo risco, risco moderado, alto risco ou risco proibitivo. Assim, para cada um dos estrados haveria tratamentos e regulações diferentes.

[307] Na proposta europeia (denominada "AI Act"), consta do Anexo III, item 4 (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206). Na proposta brasileira (Minuta aos Projetos de Leis nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, proposta no substititutivo produzido pela CJSUBIA), encontra-se no artigo 17, inciso III (BRASIL. Senado Federal. Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4&_gl=1*1dq78qd*_ga*MTkwMjcxOTY4Ni4xNjgyNDg0MjYw*_ga_CW3ZH25XMK*MTY4MjQ4NDI2MC4xLjEuMTY4MjQ4NDI4MS4wLjAuMA. Acesso em: 26 abr. 2023).

sistemas de IA, que podem impactar aspectos da personalidade do empregado e limitar direitos e liberdades individuais, tais como os direitos sociais e direitos trabalhistas.

Uma terceira medida de boas práticas para o empregador que deseje utilizar sistemas de IA é reforçar os cuidados com as bases de dados que alimentarão esses algoritmos. Como já relatado no capítulo 3, muitos dos casos de discriminação algorítmica e erro de decisões automatizadas são gerados por falha nas bases de dados, seja dos algoritmos que tomarão as decisões automatizadas, seja nos modelos de algoritmos, que criarão outros algoritmos por meio do *machine learning*. Assim, deverá o empregador sempre buscar que sua base de dados esteja fidedigna e atualizada, seja por meio da minimização dos dados (decorrência dos princípios da finalidade, necessidade e adequação – respectivamente artigo 6º, incisos I, II e III da LGPD), seja por atualização constante, inclusive disponibilizando para que os próprios titulares de dados possam realizar sua verificação (decorrência dos princípios do livre acesso, da qualidade dos dados e da transparência – respectivamente, artigo 6º, incisos IV, V e VI da LGPD).

A quarta medida que se sugere aos empregadores, no uso da IA, é a necessária participação humana nas decisões que envolvam relações de emprego e, mais ainda, possíveis limitações a direitos de acesso ou manutenção ao trabalho. Apesar de o artigo 20 da LGPD não deixar expresso que o pedido de revisão das decisões automatizadas deva ser analisado por um ser humano, sabe-se que a proposta original previa essa exigência, tendo sido alvo de veto pelo Presidente da República por questões ligadas à logística disso quanto a empresas que tenham esse modelo de negócios. No entanto, quando um empregador busca adotar esse tipo de ferramenta para tomar decisões automatizadas sobre seus empregados, não está aí a realizar um modelo de negócios próprio, em verdade estará em uma situação excepcional, que não é a regra prevista na legislação trabalhista ou no contrato de trabalho.

Então, a inclusão de um ser humano na revisão dessas decisões, até mesmo sem necessariamente haver a solicitação pelos titulares, mas proativamente (reflexo do princípio da prevenção – artigo 6º, inciso VIII da LGPD), demonstrará boas práticas adotadas pelo empregador. Além disso, mesmo que haja a participação humana, deverá ser garantido que essa pessoa, ou grupo de pessoas, seja capacitada e treinada, para que não recaia sobre ela o denominado "viés da automação", pelo qual o ser humano inclina-se a manter uma decisão que já foi validada por uma máquina, pela inconsciente visão de que a decisão da máquina tende a ser correta, mais do que uma decisão humana. Por fim, o revisor humano deverá ter poder para influir nas decisões, rejeitando-se situações em que se trate de tão somente algum preposto para cumprir uma formalidade, devendo haver real análise dos casos e sua revisão efetiva.

A quinta medida de boas práticas é relacionada à transparência e explicabilidade das decisões automatizadas, mesmo diante do segredo de negócio (expressamente protegido pela LGPD). Ao escolher por adotar mecanismos de IA na relação de emprego, o empregador deverá optar por aqueles que garantam sempre maior explicabilidade. Ou seja, os próprios sistemas contratados deverão ter condições técnicas de demonstrar a racionalidade das decisões automatizadas, nem que seja por meio dos critérios utilizados e o peso que cada critério teve naquele resultado. Ainda, é necessário estabelecer um padrão de que sempre os empregadores informarão aos seus titulares de dados quando estes estiverem sendo alvo de uma análise ou decisão algorítmica, afinal, será uma concretização do princípio da transparência, que garante ao titular informações claras, precisas e facilmente acessíveis sobre a realização daquele tratamento de dados. Quanto ao segredo de negócio, mesmo diante de sua proteção, poderá o empregador seguir algumas regras nacionais ou internacionais de boas práticas para apresentação dessas informações que lhes sejam solicitadas, a exemplo de regulações sobre o tema na União Europeia.

Alguns exemplos podem ser citados, como iniciativas de clarificar o entendimento do que seriam essas "informações úteis" sobre a lógica envolvida nessas decisões automatizadas. O Grupo de Trabalho do artigo 29 (WP29 ou A29WP, na sigla em inglês) é um comitê consultivo encarregado de auxiliar a implementação do RGPD. Hoje, esse órgão passou a se chamar Comitê Europeu de Proteção de Dados (*EDPB*) e sua atuação encontra relevo na coordenação das Autoridades de Proteção de Dados dos Estados-Membros, mantendo o alinhamento destas com o RGPD.

O funcionamento do Comitê Europeu de Proteção de Dados (EDPB) encontra-se previsto no artigo 68 e seguintes do RGPD, que atribui a ele o objetivo principal de assegurar a aplicação coerente do RGPD, bem como diversas atividades específicas, dentre as quais a de emitir diretrizes, recomendações e melhores práticas sobre tratamentos de dados. No próprio texto do RGPD, diversas são as menções à atuação desse órgão, inclusive no considerando nº 72, que prevê que o EDPB elaboraria Orientações sobre a definição de perfis e, portanto, o tratamento automatizado de dados pessoais.

Uma de suas Orientações (*Guidelines*), emitida em 2018, foi sobre esse tema, em que foi clarificado o sentido desse termo "informações úteis" sobre a lógica envolvida, como sendo:

> - as categorias de dados que foram ou serão utilizadas no processo de definição de perfis ou de tomada de decisão;
> - o motivo pelo qual essas categorias são consideradas pertinentes;

- o modo como é elaborado qualquer perfil utilizado no processo de decisão automatizada, incluindo eventuais estatísticas utilizadas na análise;
- o motivo pelo qual esse perfil é relevante para o processo de decisão automatizada; e
- o modo como é utilizado para uma decisão relativa ao titular dos dados.[308]

As sugestões apresentadas acima são razoáveis, considerando que não violam o segredo de negócio, além de possuírem o condão de esclarecer a lógica envolvida na decisão automatizada ao titular de dados, portanto poderão ser compartilhadas pelo empregador de maneira transparente e explicável, configurando-se boas práticas para cumprimento do direito à proteção de dados pessoais do empregado.

Outra medida de boas práticas, a última apresentada neste trabalho, diz respeito à necessidade de o empregador ajustar suas tecnologias baseadas em IA à auditabilidade, ou seja, promovendo que elas estejam disponíveis para que possam ser averiguadas e, caso estejam adequadas, sejam validades, caso não, que sejam rechaçadas.

A elaboração de Relatórios de Impacto representa excelente exemplo de ferramenta capaz de disponibilizar a terceiros se as medidas adotadas pelo empregador são eficazes e adequadas para mitigar os riscos envolvidos naquele uso da IA. Mesmo que não sejam documentos que obrigatoriamente devam ser públicos, sua disponibilização para terceiros representa uma boa prática de governança de dados, pois representa disposição para auditabilidade e, assim, demonstra não haver ilícitos ocorrendo naquela operação.

Além disso, segundo Maria Cecília Gomes, o RIPD "deve ser visto não apenas como uma documentação do controlador gerada após um processo de conformidade, mas sim como um instrumento de apoio nas atividades de tratamento de uma organização para que ela possa fazer sua governança de dados e demonstrar conformidade com as obrigações legais previstas".[309]

As auditorias nos algoritmos de IA poderiam ser realizadas pelos órgãos de controle, tais como a ANPD, que possui essa como uma de suas competências, estabelecida no artigo 55-J, inciso XVI da LGPD.[310] Complementando sua competência, no caso de recusa ao fornecimento de informações sobre as decisões automatizadas, o controlador (no caso,

---

[308] UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29º para a Proteção de Dados. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. Adotadas em 3 de outubro de 2017. Bruxelas: UE, 2016.

[309] GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista da AASP**, (144), 2019. p. 176.

[310] Art. 55-J. Compete à ANPD: [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

empregador) poderá ser solicitado pela ANPD para realização de auditoria ao algoritmo, para verificar possíveis aspectos discriminatórios.

Além de auditorias administrativas, judicialmente algumas tentativas de auditorias em algoritmos já foram tentadas, inclusive relacionadas às relações de trabalho, mas não lograram êxito diante da amplitude dos critérios suscitados na ordem judicial, assim como por argumentos de que a auditoria não seria hábil para o objetivo pretendido, no caso, comprovação de eventual vínculo de emprego entre empresas proprietárias de plataformas de transporte urbano com profissionais parceiros dessas plataformas.

No entanto, apesar dessa discussão, auditorias que sejam realizadas com propósitos claros e adequados, tais como a possível identificação de vieses discriminatórios, ou para verificar os aspectos sugeridos no presente tópico, quando se tratou sobre os critérios para explicabilidade de uma decisão automatizada, aparenta-se como algo positivo o controle judicial dessas decisões.

Também, pode-se considerar auditorias realizadas por terceiros particulares interessados, a exemplo de entidades sindicais, haja vista serem aqueles legitimados para fiscalizar as condições de trabalho dos empregados. Ainda, órgãos administrativos que não sejam propriamente ligados à proteção de dados pessoais, tais como Ministério Público do Trabalho e Ministério do Trabalho, por meio das Superintendências Regionais do Trabalho e Emprego – SRTEs.

A atuação sindical para acompanhamento e fiscalização do uso de algoritmos pelo empregador deve ser ressaltada, principalmente porque sua presença é bem mais descentralizada do que os demais órgãos supracitados. Enquanto os órgãos estatais precisam fiscalizar todas as empresas indistintamente, as entidades sindicais são especialmente destinadas a fiscalizar as empresas que atuem em suas categorias profissionais. No entanto, com a reforma trabalhista de 2017 (Lei nº 13.467), a atuação sindical foi enfraquecida, notadamente pela diminuição de sua renda, causada pela não obrigatoriedade do pagamento de contribuição sindical pelos empregados.

Ainda assim, os sindicatos devem ter papel central nessa discussão, seja em fase prévia à adoção de ferramentas de IA, devendo ser cientificada quando o empregador intente utilizá-la, seja durante seu uso, devendo o empregador garantir mecanismos de transparência também aos sindicatos, para que possam fiscalizar seu cumprimento ao que determinam os direitos fundamentais dos trabalhadores[311]. Como medida concreta para se atingir essa

[311] MARQUES, Fabíola; MARTINEZ NETO, Aldo Augusto. Vieses algorítmicos, direitos fundamentais e os sindicatos. **Revista Direito do Trabalho e Seguridade Social**, v. 222, p. 201-219, 2022.

participação sindical, os Relatórios de Impacto à proteção de dados produzidos pelo empregador devem ser disponibilizados aos sindicatos, como forma de estarem cientes dos riscos envolvidos e das medidas adotadas, visando mitigá-los.

Diante das boas práticas apresentadas, é perceptível que não se trata de uma totalidade de normas que feche lacunas inteiramente, quanto ao uso da IA na relação de emprego. Medidas de boas práticas podem ser criadas e ajustadas pelos particulares, de acordo com o que prevê o artigo 50 da LGPD, desde que sigam sempre o sentido trazido pela legislação sobre o tema.

Assim, a *accountability* apresenta uma dupla funcionalidade: *ex ante*, como um guia para os agentes de tratamento, os quais terão à sua disposição – e deverão elaborar novas – "regras de governança e boas práticas que estabeleçam procedimentos, normas de segurança e padrões técnicos, tal como se extrai do artigo 50 da LGPD [...]", mediante adoção de um programa de *compliance* de dados pessoais; e *ex post*, como um guia para as autoridades, judiciais e administrativas, que poderão identificar melhor quando as diretrizes da proteção de dados pessoais estão sendo descumpridas e poderão quantificar melhor as responsabilidades de cada um dos agentes de tratamento, além de poderem estabelecer melhor os remédios necessários para sanção desses agentes.[312]

Portanto, o presente trabalho, ao propor critérios legais e boas práticas de governança de dados pelo empregador que utiliza sistemas de IA na relação de emprego, propõe-se a munir particulares, tais como empregadores que tenham esse interesse de utilizar essas ferramentas ou empregados, que estejam sendo alvo dessas tecnologias, mas não sabem quais critérios utilizar para avaliar sua correção. Busca-se, também, auxiliar órgãos administrativos e judiciais, no sentido de fiscalizar ou julgar se determinadas práticas de empregadores estejam adequadas ou não à proteção de dados pessoais, conforme disposições cogentes ou sugestivas de boas práticas. Por fim, o presente trabalho pretende contribuir com o debate público quanto à regulação da IA, notadamente quando se trata de especificidades relacionadas à relação de emprego, que possui peculiaridades que a fragiliza, demandando medidas próprias e adequadas, visando evitar riscos e danos que possam violar seus direitos fundamentais, dentre eles o direito à proteção de dados pessoais.

---

[312] ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. *Accountability* e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 778-779.

5 CONSIDERAÇÕES FINAIS

Diante do que foi apresentado, podem-se chegar a alguns resultados relevantes para os propósitos delineados no início da pesquisa. Inicialmente, constatou-se que, dentre as diversas concepções de Inteligência Artificial, aquela que mais encontra usabilidade perante as relações de emprego e, também, que proporciona maior probabilidade de riscos aos direitos dos empregados é aquela baseada nas metodologias de aprendizado de máquina (*Machine Learning)*. Portanto, mesmo diante de simples sistemas de automação de processos internos, não se mostra adequado estabelecer parâmetros jurídicos e de boas práticas tais quais o que se apresentou neste trabalho.

Foi identificado que os usos da IA na relação de emprego ocorre nas suas diversas fases, desde a fase de ingresso ao emprego, quando as vagas são direcionadas para determinado público, por meio de algoritmos das redes sociais profissionais, e quando os candidatos se submetem a processos seletivos altamente tecnológicos e que medem aspectos de suas personalidades a partir do uso de ferramentas associadas a jogos e *chatbots* conversacionais.

Após a contratação do empregado, foi verificado que a gestão do trabalho é subsidiada por diversos tipos de sistemas de IA, dentre eles aqueles que monitoram os dados pessoais sensíveis dos empregados – notadamente ligados à saúde – por meio de dispositivos vestíveis (*wearables*), com vistas a analisar suas capacidades de realizar as atividades laborais. Também se constatou que as ferramentas de comunicação interna de algumas empresas são imbuídas de algoritmos de aprendizado de máquina, que permitem ao empregador rastrear – por vezes, contínua e ininterruptamente – o uso de dispositivos eletrônicos pelos empregados, seja para quantificar sua produção seja para medir a qualidade e assiduidade daquele trabalhador.

Mantendo-se perante a gestão algorítmica do trabalho, verificou-se, também, o uso da IA na predição de empregados que estejam mais propensos a tomar alguma decisão, por exemplo de sair da empresa, o que poderia levar a duas consequências distintas: o empregador auxiliar aquele empregado a continuar na empresa, por meio da motivação; ou o empregador antecipar-se e já punir aquele empregado, diante de características que possam ser a ele imputadas como faltosas. Ainda, analisou-se que existem diversas ferramentas baseadas em IA que são aplicadas em contextos de fábricas, propondo melhoria da ergonomia e da qualidade do trabalho, mas que rastreiam dados pessoais ininterruptamente dos empregados, até mesmo influenciando no aumento do ritmo de trabalho. Constatou-se que a maior parte dessas ferramentas de IA na relação de emprego pertencem a terceiros, não sendo comum o

desenvolvimento interno dessas tecnologias pelas empresas, o que leva a implicações jurídicas relevantes, quando se trata de responsabilização dos agentes.

Chegando a uma terceira fase da relação de emprego, identificou-se que premiações e sanções são largamente aplicadas a empregados com auxílio da IA, seja quando a decisão é subsidiada por dados coletados por essas tecnologias seja quando elas próprias tomam as decisões que afetam os interesses do empregado. Assim, constatou-se que tecnologias de reconhecimento facial e detecção de expressões faciais e corporais dos empregados – mesmo sem comprovações científicas robustas sobre sua eficácia – são utilizadas para medir seus humores e emoções, o que gera resultados positivos ou negativos no âmbito do trabalho.

Também, destacou-se que os metadados, aquelas informações eletrônicas geradas pelos empregados quando utilizam determinados dispositivos, permitem ao empregador rastrear aspectos como localizações passadas, tempo de uso daquele dispositivo, quantidade de interações (cliques, letras digitadas ao teclado etc.), proporcionando ao empregador a capacidade de rastreio ininterrupto até mesmo de micro etapas do trabalho, que podem levar a premiações ou sanções, a depender dos dados coletados.

Seguindo após analisados os principais usos da IA na relação de emprego, buscou-se verificar os mais relevantes riscos que esses usos poderiam implicar nos direitos dos empregados, notadamente aqueles que estejam sob o conceito da proteção de dados pessoais. Assim, indicou-se a existência de algumas características na relação de emprego que a diferenciam das demais, sendo elas a existência de um legítimo poder de controle eletrônico pelo empregador, que ainda mais estabelece uma relação jurídica baseada na subordinação do empregado a seu contratante, ainda mais quando a relação de emprego proporciona ao empregador uma quantidade imensa de dados pessoais do empregado, caracterizando verdadeira “nudez tecnológica” deste.

Assim, os riscos especialmente relacionados ao direito à proteção de dados do empregado, diante do uso da IA, foram pormenorizados. A primeira categoria de riscos foi relacionada aos direitos de personalidade, tendo em vista as violações que podem ocorrer quanto à imagem do empregado, diante de tecnologias de reconhecimento facial, de detecção de sentimentos e humores; quanto ao direito à identidade pessoal, já que os algoritmos de IA produzem perfis comportamentais sobre os empregados, os quais não possuem acesso a essas inferências produzidas pelo empregador, muitas vezes encobertas pelo segredo de negócio.

A segunda categoria de riscos envolve o direito à privacidade, o qual é impactado pelo uso da IA principalmente quando do contínuo rastreamento de atividades realizadas pelo empregado, sem que muitas vezes seja ele informado, utilizando ainda de dados pessoais que

foram fornecidos para uma finalidade, mas serão utilizados para uma outra, dificultando a autodeterminação informativa pelo titular de dados.

Foi identificada, ainda, uma terceira categoria de riscos à proteção de dados do empregado, relacionada à igualdade e à não discriminação no local de trabalho, já que esses algoritmos de IA possuem o propósito de tomarem decisões mais isentas e sem vieses, no entanto, algumas situações podem leva-los a decisões discriminatórias, como erros estatísticos ou de programação, como generalizações indevidas, como uso de dados pessoais sensíveis e, também, a produção de decisões que limitem direitos do empregado.

Percebeu-se que muitos dos riscos advindos do uso da IA na relação de emprego decorrem do não atendimento aos princípios previstos na legislação de proteção de dados pessoais, notadamente limitação do tratamento a uma finalidade, minimização dos dados, transparência e livre acesso, além da não discriminação. Buscando identificar na legislação o amparo teórico-prático para as medidas necessárias, encontrou-se a necessidade de o empregador privilegiar o direito fundamental à proteção de dados pessoais, fortalecer o atendimento aos princípios da LGPD, condicionar o tratamento automatizado de dados a uma das hipóteses legais autorizativas de tratamento, proporcionar o exercício dos direitos dos empregados enquanto titulares de dados e produzirem relatórios de impacto à proteção de dados, mesmo que não lhes seja exigido *prima facie*.

Por fim, para além das exigências legais para garantir o direito à proteção de dados pessoais do empregado, concluiu-se que o empregador deverá formular e seguir boas práticas de governança de dados pessoais, com espeque no princípio da prestação de contas (*accountability*), adotando medidas tais como a inclusão de todos os agentes de tratamento às regras de governança de dados pessoais, para garantir que, mesmo nos casos em que os sistemas são de terceiros, haverá garantia da regularidade e adequação às normas; o mapeamento dos riscos aos direitos dos empregados, decorrentes do uso da tecnologia baseada em IA, adotando ainda o princípio da precaução como balizador de condutas empresariais; o reforço com cuidados quanto às bases de dados que alimentarão o aprendizado de máquina e o seu uso na relação de emprego, visando evitar situações de erro de julgamento ou de discriminação algorítmica; a inclusão da participação humana nas decisões, jamais deixando apenas para dispositivos tecnológicos a definição de critérios e situações que afetem os interesses dos empregados, portando esses indivíduos com poderes e capacitação suficientes para a função; promover a transparência e a explicabilidade das ferramentas de IA, buscando decifrar as "caixas pretas", disponibilizando para os empregados, ou quem os represente, respostas sobre critérios e forma de decisão automatizada; Por fim, promover a auditabilidade dos sistemas de

IA, disponibilizando informações úteis para acompanhamento de órgãos administrativos e judiciais, além de possibilitar a participação sindical nas auditorias, principalmente por meio da elaboração e divulgação de relatórios de impacto à proteção de dados pessoais.

Ao final, conclui-se que as medidas legalmente exigidas e as boas práticas de prestação de contas em governança de dados pessoais não são exaustivas, havendo amplo campo para propostas de novos critérios, que se somem aos já apresentados, na busca pelo respeito à proteção de dados pessoais pelos empregadores ao utilizarem sistemas baseados em Inteligência Artificial.

Confirmou-se, portanto, a hipótese inicialmente formulada, de que apenas a adoção do regime legal da proteção de dados não é suficiente, tendo em vista não haver regulação setorial quanto ao uso da IA na relação de emprego, o que torna necessária a adoção, também, de boas práticas de governança de dados pessoais, baseadas nos riscos envolvidos. Como possíveis boas práticas, sugeriu-se na presente pesquisa os seguintes: (i) a formulação de regras de governança de dados de toda a cadeia de agentes de tratamento de dados; (ii) o mapeamento dos riscos a direitos dos empregados e a aplicação do princípio da precaução; (iii) a adoção de medidas para resguardar a qualidade das bases de dados; (iv) a inclusão da participação humana nas decisões automatizadas como regra; (v) a implementação de medidas de transparência e explicabilidade quanto ao uso da IA na relação de emprego e; (vi) a disponibilização desses sistemas para possíveis auditorias de terceiros, mediante a elaboração e apresentação de relatórios de impacto à proteção de dados pessoais.

Verificou-se que as medidas sugeridas são relevantes, mas não são as únicas, devendo os empregadores sempre verificar quais outras boas práticas poderão ser acrescidas, conforme o grau dos riscos mapeados.

Para além disso, identificou-se que o presente trabalho deve servir como um guia a partir do qual empregadores possam partir, quando buscarem referências de medidas necessárias a proteger os direitos dos empregados diante de dispositivos de IA, mas também deverá servir como um guia às autoridades administrativas, judiciais ou sindicais, que busquem o intuito fiscalizatório das empresas, acompanhando se estas prestarão contas de seus tratamentos de dados; bem como na atividade judicante, em que o Poder Judiciário trabalhista poderá acompanhar se as atitudes do empregador condizem com os comandos legais e com as boas práticas de proteção dos direitos dos empregados, diante de casos concretos.

REFERÊNCIAS

ALBUQUERQUE, Adriana Reis de. **Poder artificial de tributar?** limites e requisitos à utilização (adequada) da inteligência artificial pela administração tributária. 2022. 40 f. Tese (Doutorado em Direito) - Faculdade de Direito, Programa de Pós-Graduação em Direito, Universidade Federal do Ceará, Fortaleza, 2022.

ALLISON, Conor. The Upright Go aims to solve your back pain and screen slouch. **Wareable**, 31 jan. 2017. Disponível em: https://www.wareable.com/wearable-tech/upright-go-release-date-price-specs-3850. Acesso em: 04 abr. 2023.

ALOISI, Antonio; GRAMANO, Elena. Artificial intelligence is watching you at work. Digital surveillance, employee monitoring and regulatory issues in the EU context. **Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection"**, 2019, p. 105-106. Disponível em: http://salus.adapt.it/wp-content/uploads/2020/07/Gramano-Alois_AI-is-Wathching-you_2019.pdf. Acesso em: 07 set. 2020.

AMAZON. AWS Panorama Devices. Disponível em: https://aws.amazon.com/pt/panorama/appliance/. Acesso em: 08 abr. 2023.

BANDEIRA DE MELLO, Celso Antônio. **Conteúdo jurídico do princípio da igualdade**. São Paulo: Malheiros, 3. ed., 8ª Tiragem, 2008.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, p. 671-732, 2016.

BARROS, Alice Monteiro de. **Proteção à intimidade do empregado**. São Paulo: LTr, 1997.

BELMONTE, Alexandre Agra. **O monitoramento da correspondência eletrônica nas relações de trabalho**. LTr, 2004.

BERNHARDT, Annette; SULEIMAN, Reem; KRESGE, Lisa. **Data and algorithms at work**: the case for worker technology rights. 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais**: o princípio da *accountability*. Rio de Janeiro: Forense, 2022.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., ver., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BLACK, J. Stewart; VAN ESCH, Patrick. AI-enabled recruiting: What is it and how should a manager use it? **Business Horizons**, v. 63, n. 2, p. 215-226, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. ANPD publica Agenda Regulatória 2023-2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024. Acesso em: 20 abr. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais. Acesso em: 25 abr. 2023.

BRASIL. Senado Federal. Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4&_gl=1*1dq78qd*_ga*MTkwMjcxOTY4Ni4xNjgyNDg0MjYw*_ga_CW3ZH25XMK*MTY4MjQ4NDI2MC4xLjEuMTY4MjQ4NDI4MS4wLjAuMA. Acesso em: 26 abr. 2023.

BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC/DF**. Relator: Min. Rosa Weber. Data de julgamento: 24/04/2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629 Acesso em: 25 abr. 2023.

BURRI, Mira. Understanding the implications of big data and big data analytics for competition law: an attempt for a primer. **New Developments in Competition Law and Economics**, p. 241-263, 2019.

CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra Editora, 1995.

CAPPELLI, Peter; TAVIS, Anna. HR Goes Agile. **Harvard Business Review**, mar./abr. 2018.

CASEY, Bryan; FARHANGI, Ashkon; VOGL, Roland. Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. **Berkeley Tech. LJ**, v. 34, p. 143, 2019.

CHEN, Daizhuo et al. Enhancing transparency and control when drawing data-driven inferences about individuals. **Big data**, v. 5, n. 3, p. 197-212, 2017.

CHRISTIAN, Brian. **The alignment problem**: Machine learning and human values. Nova York: WW Norton & Company, 2020.

COPETTI, Rafael; MIRANDA, Marcel Andreata de. Autodeterminação informativa e proteção de dados: uma análise crítica da jurisprudência brasileira. **Revista de Direito, Governança e Novas Tecnologias**, v. 1, n. 2, p. 28–48, 2015.

CORDEIRO, António Barreto Menezes. **Direito da proteção de dados à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020.

CUPIS, Adriano de. **Os Direitos da Personalidade**. 2. ed. Trad. Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

DELGADO, Mauricio Godinho. **O poder empregatício**. São Paulo: Ltr, 1996.

DELFANTI, Alessandro; RADOVAC, Lilian; WALKER, Taylor. The Amazon Panopticon: A Guide for Workers, Organizers & Policymakers, **UNI Global**, 2021. Disponível em: https://uniglobalunion.org/wp-content/uploads/amazon_panopticon_en_final.pdf. Acesso em: 07 abr. 2023.

DE LIMA, Ana Cláudia Pires Ferreira; ALBINO, João Pedro. Técnicas de captura de geolocalização para produção de prova judicial. **Revista Direito das Relações Sociais e Trabalhistas**, v. 8, n. 1, p. 216-233, 2022.

DEMPSEY, Lorcan et al. A review of metadata: a survey of current resource description format. [S.l.] Specification for resource description methods. v. 1, 1997. p. 5. Disponível em: https://archive.ifla.org/documents/libraries/cataloging/metadata/d32p1.pdf. Acesso em: 09 abr. 2023.

DE STEFANO, Valerio. 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Artificial Intelligence and Labour Protection (May 16, 2018). **Comparative Labor Law & Policy Journal**, v. 41, n. 1, 2019.

DE STEFANO, Valerio; WOUTERS, Mathias. AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework (European Parliament, 2022). **Commissioned Reports, Studies and Public Policy Documents**. Paper 219, 2022.

DOMINGOS, Pedro. **O algoritmo mestre**: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec Editora, 2017.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. What is algorithm governance? **IEEE Internet Computing**, v. 20, n. 4, p. 60-63, 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

DUHIGG, Charles. **O poder do hábito**: por que fazemos o que fazemos na vida e nos negócios. Trad. Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

ERNST, Ekkehard et al. The economics of artificial intelligence: Implications for the future of work, **ILO Future of Work Research paper Series**; ILO, 2018.

EUBANKS, Virginia. **Automating inequality**: How high-tech tools profile, police, and punish the poor. Nova York: St. Martin's Press, 2018.

FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica *In*: BARBOSA, Mafalda Miranda et al. (coord.). **Direito Digital e Inteligência Artificial**: Diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021.

FELONI, Richard. Consumer-goods giant Unilever has been hiring employees using brain games and artificial intelligence — and it's a huge success. **Insider**, 28 jun. 2017. Disponível em: https://www.businessinsider.com/unilever-artificial-intelligence-hiring-process-2017-6. Acesso em: 02 abr. 2023.

FREITAS, Juarez; FREITAS, Thomas Bellini. **Direito e inteligência artificial**: em defesa do humano. Belo Horizonte: Fórum, 2020.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista da AASP**, (144), 2019.

GOODMAN, Bryce; FLAXMAN, Seth. European union regulations on algorithmic decision making and a "right to explanation". **AI Magazine**, v. 38, n. 3, p. 50–57, 2017.

HAYDUK, Gabriel. Requisitos do relatório de impacto à proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

HOROWITZ, Ellis; SAHNI, Sartaj; RAJASEKARAN, Sanguthevar. **Computer algorithms**. Nova York: Computer Science Press, 1997.

ICO: Biometrics: foresight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf. Acesso em: 07 abr. 2023

ICO: Biometrics: insight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf. Acesso em: 07 abr. 2023

IDEAL. S&P Data Increased Retention By 20%. Disponível em: https://ideal.com/customer/sp-data/. Acesso em: 02 abr. 2023.

KLEINBERG, Jon et al. Discrimination in the Age of Algorithms. **Journal of Legal Analysis**, v. 10, p. 113-174, 2018.

KROLL, Joshua A. et al. Accountable algorithms. **University of Pennsylvania Law Review**, v. 165, p. 633-705, 2017.

KUNCEL, Nathan R. et al. Mechanical versus clinical data combination in selection and admissions decisions: a meta-analysis. **Journal of applied psychology**, v. 98, n. 6, p. 1060, 2013.

KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation**: A Commentary. Oxford: Oxford University Press, 2020.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003.

LEONARDI, Paul M. COVID-19 and the new technologies of organizing: digital exhaust, digital footprints, and artificial intelligence in the wake of remote work. **Journal of Management Studies**, v. 58, n. 1, p. 249, 2021.

LIMA, Francisco Gérson Marques. **Igualdade de tratamento nas relações de trabalho**. São Paulo: Malheiros, 1997.

LINKEDIN. Política de Privacidade. Disponível em: https://br.linkedin.com/legal/privacy-policy?trk=d_checkpoint_lg_consumerLogin_cap_ft_privacy_policy#use. Acesso em: 17 mar. 2023.

LINKEDIN. Talent Solutions. Disponível em https://business.linkedin.com/pt-br/talent-solutions/post-jobs. Acesso em: 18 mar. 2023.

LORENZETTI, Ricardo Luis; **Fundamentos do direito privado**. Trad. Vera Maria Jacob de Fradera. São Paulo: Revista dos Tribunais, 1998.

MACHADO SEGUNDO, Hugo de Brito. **Direito e Inteligência Artificial**: O que os Algoritmos têm a Ensinar sobre Interpretação, Valores e Justiça. São Paulo: Editora Foco, 2022.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. Rio de Janeiro: Arquipélago Editorial, 2019.

MAGRANI, Eduardo; GUEDES, Paula. Inteligência Artificial: desafios éticos e jurídicos. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance*** **e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

MAINI, Vishal; SABRI, Samer. **Machine learning for humans**. Online, 2017.

MANKY, Derek. O uso da inteligência artificial e a segurança cibernética. **itforum**, 04 abr. 2020. Disponível em: https://itforum.com.br/noticias/o-uso-da-inteligencia-artificial-e-a-seguranca-cibernetica/. Acesso em: 20 abr. 2023.

MANOKHA, Ivan. Why the rise of wearable tech to monitor employees is worrying. **Independent**, 04 jan. 2017. Disponível em: https://www.independent.co.uk/tech/why-the-rise-of-wearable-tech-to-monitor-employees-is-worrying-a7508656.html. Acesso em: 04 abr. 2023.

MARQUES, Fabíola; MARTINEZ NETO, Aldo Augusto. Vieses algorítmicos, direitos fundamentais e os sindicatos. **Revista Direito do Trabalho e Seguridade Social**, v. 222, p. 201-219, 2022.

MATEESCU, Alexandra. Electronic Visit Verification: the weight of surveillance and the fracturing of care. **Data & Society Research Institute**, 2021.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**: A revolution that will transform how we live, work, and think. Nova York: Houghton Mifflin Harcourt, 2013.

MCLAREN, Samantha. How Hilton, Google, and More Have Dramatically Reduced Their Time to Hire. **Linkedin**, 24 maio 2018. Disponível em: https://www.linkedin.com/business/talent/blog/talent-strategy/how-these-companies-reduced-time-to-hire. Acesso em: 02 abr. 2023.

MENDES, Laura Schertel. BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, ano 28, p. 157-180, jul.-ago. 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, p. 39-64, 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. *In*: DONEDA, Danilo et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

MICROSOFT. Microsoft Teams. Disponível em: https://www.microsoft.com/pt-br/microsoft-teams/teams-for-work. Acesso em: 04 abr. 2023.

MICROSOFT. O MyAnalytics, o controlador de eficiência no trabalho, agora está mais amplamente disponível. **Microsoft**, 02 jan. 2019. Disponível em: https://www.microsoft.com/pt-br/microsoft-365/blog/2019/01/02/myanalytics-the-fitness-tracker-for-work-is-now-more-broadly-available/. Acesso em: 04 abr. 2023.

MIRANDA, Pontes de. **Tratado de Direito Privado**, Tomo VII: Direito de personalidade. Direito de família: direito matrimonial (existência e validade do casamento). Atual. Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Editora Revista dos Tribunais, 2012.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, v. 39, p. 1-27, 2018.

MOORE, Matthew. Gay men 'can be identified by their Facebook friends'. **The Telegraph**, 21 set. 2009. Disponível em: https://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html. Acesso em: 07 abr. 2023.

MOREIRA, Teresa Coelho. **A Privacidade dos Trabalhadores e as Novas Tecnologias de informação e comunicação**: contributo para um estudo dos limites do poder de controlo electrônico do empregador. Coimbra: Almedina, 2010.

MOREIRA, Teresa Coelho. **Direito do Trabalho na Era Digital**. Coimbra: Almedina, 2021.

MOREIRA, Teresa Coelho. Novas tecnologias: um admirável mundo novo do trabalho? **Revista de Direitos e Garantias Fundamentais**, n. 11, p. 15-52, 2012.

MOREIRA, Teresa Coelho. Principais repercussões da utilização de sistemas de inteligência artificial por agentes empresariais no âmbito do direito do trabalho – algumas questões. *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin; GOMES, Rodrigo Dias de Pinho. Inteligência Artificial e seus principais desafios para os programas de *compliance* e as políticas de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

NAKAR, Sharon; GREENBAUM, Dov. Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. **Boston University Journal of Science & Technology Law**, v. 23, n. 1, p. 88-123, 2017.

NEFF, Gina et al. AI @ Work: Artificial Inteligence in the workplace. Disponível em: https://cdn.futuresays.org/content/uploads/2020/08/14084038/FS_PDF_GINA_V4.pdf. Acesso em: 09 abr. 2023.

NOBLE, Safiya Umoja. **Algorithms of oppression**: How search engines reinforce racism. Nova York: NYU Press, 2018.

O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. New York: Crown, 2016.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Protection of workers' personal data: an ILO code of practice, 1997. **Commentary on the Code of Practice**. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 07 jul. 2020.

PAVELSKI, Ana Paula. **Os direitos da personalidade do empregado**: em face do exercício abusivo do poder diretivo do empregador. Curitiba: Juruá, 2009.

PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

PLUMMER, Libby. Wearables in the workplace: The tech taking over your office in 2017. **Wareable**, 21 fev. 2017. Disponível em: https://www.wareable.com/wearable-tech/wearables-in-the-workplace-office-235. Acesso em: 04 abr. 2023.

PWC. **Artificial Intelligence in HR**: a no-brainer? Disponível em: https://www.pwc.nl/nl/assets/documents/artificial-intelligence-in-hr-a-no-brainer.pdf. Acesso: 10 out. 2022.

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

RODRIGUES JUNIOR, Otavio Luiz. Direitos fundamentais e direitos da personalidade. *In*: TOFFOLI, José Antonio Dias (org.). **30 anos da constituição brasileira**: democracia, direitos fundamentais e instituições. Rio de Janeiro: Forense, 2018, p. 679-703.

ROSENBAUM, Eric. CNBC WORK IBM artificial intelligence can predict with 95% accuracy which workers are about to quit their jobs. **CNBC**, 03 abr. 2019. Disponível em: https://www.cnbc.com/2019/04/03/ibm-ai-can-predict-with-95-percent-accuracy-which-employees-will-quit.html. Acesso em: 07 abr. 2023.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. Accountability e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. trad. Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

SALVI DEL PERO, Angelica; WYCKOFF, Peter; VOURC'H, Ann. Using Artificial Intelligence in the workplace: What are the main ethical risks? **OECD Social, Employment and Migration Working Papers**, n. 273, 2022. Disponível em: https://ideas.repec.org/p/oec/elsaab/273-en.html. Acesso em: 07 nov. 2022.

SERVOZ, Michel. The Future of Work? Work of the Future! **European Commission**, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/future-work-work-future. Acesso em: 18 mar. 2023.

SCHRAGE, Michael et al. Performance management's digital shift. **MIT Sloan Management Review**, 2019.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, p. 233-242, 2017.

SHARMA, Anushree. How AI reinvented hiring practice at L'Oréal. **People Matters**, 16 ago. 2018. Disponível em: https://www.peoplematters.in/article/technology/how-the-worlds-largest-cosmetic-company-transformed-its-hiring-practice-with-ai-19006. Acesso 02 abr. 2023.

SIMONITE, Tom. This Call May Be Monitored for Tone and Emotion. **Wired**, 19 mar. 2018. Disponível em: https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/. Acesso em: 08 abr. 2023.

SIMÓN, Sandra Lia. **A proteção constitucional da intimidade e da vida privada do empregado**. São Paulo: LTr, 2000.

SLACK. Aqui acontece. Disponível em: https://slack.com/intl/pt-br/solutions. Acesso em: 04 abr. 2023.

SOLON, Olivia. Big Tech call center workers face pressure to accept home surveillance. **NBC News**, 08 ago. 2021. Disponível em: https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227. Acesso em: 01 set. 2021.

SOUTO MAIOR, Jorge Luiz. Do direito à desconexão do trabalho. **Revista do TRT da 15ª Região**, Campinas, n. 54, 2003.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. **Pensar–Revista de Ciências Jurídicas**, Fortaleza, v. 24, n. 3, p. 2, 2019.

SÜSSEKIND, Arnaldo; MARANHÃO, Délio; VIANNA, Segadas. **Instituições de direito do trabalho**. v. 1. 22. ed. São Paulo: LTr, 1991.

TEXTIO. End hidden bias, literally. Disponível em: https://textio.com/. Acesso 30 mar. 2023.

TREFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo Guia da. **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, p. 283-315.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, ano 9, n. 1, 2020.

UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29º para a Proteção de Dados. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. Adotadas em 3 de outubro de 2017. Bruxelas: UE, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI. **Columbia Business Law Review**, v. 2019, n. 1.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017.

WHITAKER, Reg. **The end of privacy**. New York: New York Press, 1999.

WORLD ECONOMIC FORUM. The Global Risks Report 2022, p. 52. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Acesso em: 20 abr. 2023.

ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **I Encontro da Rede de Pesquisa em Governança da Internet**, Novembro de 2017 pesquisa sobre esse tipo de regulação, na Europa, e a proteção de dados pessoais, principalmente baseando-se nos estudos de Raphaël Gellert.