I Seminário Internacional
Estado, Regulação e Transformação Digital

O futuro das democracias: hipervigilância, fake news e outras ameaças

LGPD E OS ALGORITMOS DE RECRUTAMENTO DE PESSOAL

BRAZILIAN LGPD AND STAFF RECRUITMENT ALGORITHMS

Luke Henrique Mewes[1]
FAE Business School – Curitiba/PR, Brasil.
lukemewes@gmail.com

RESUMO: A pesquisa engloba os aspectos jurídicos do tratamento de dados pessoais por mecanismos automatizados, especificamente, no contexto dos sistemas de recrutamento de pessoal, à luz da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados. A relevância do tema se dá em razão do crescente uso de ferramentas como a Inteligência Artificial nestes processos, contraposto ao elevado risco discriminatório que estas tecnologias proporcionam, gerando problemáticas jurídicas. Não obstante, a lei estabelece ao titular o direito de conhecer os critérios adotados e obter a revisão das decisões automatizadas, o que poderia muitas vezes inviabilizar o uso da tecnologia. Como objeto central da pesquisa, pretende-se explorar os requisitos para a adequação do tratamento automatizado de dados pessoais, no contexto exposto, ao plano legal. Para responder o problema de pesquisa, será adotado o método de abordagem dedutivo, de procedimento monográfico e a técnica de pesquisa bibliográfica. Partir-se-á dos conceitos gerais encontrados na legislação específica, com o fim de extrair premissas básicas à conformidade legal dos sistemas de recrutamento de candidatos no que tange à proteção de dados pessoais.

Palavras-chave: LGPD; Recrutamento; Discriminação; Algorítimos; Inteligência Artificial.

ABSTRACT: The research encompasses the legal aspects of personal data processing by automated mechanisms, specifically, in the context of staff recruitment systems, in accordance with the Brazilian Law No. 13,709/2018 — General Data Protection Law. The relevance of the topic is due to the growing use of tools such as Artificial Intelligence in these processes, set in contrast to the high discriminatory risk that these technologies cause, generating legal challenges. Nevertheless, the law establishes to the data subject the right to know the criteria adopted and to obtain a reanalysis of the automated decisions, which could often make the use of the referred technology unfeasible. As the central object of the research, it is intended to explore the requirements for the compliance of the automated processing of personal data, in the exposed context, with the legal framework. To answer the research problem, it is adopted the deductive approach method, the monographic procedure and the bibliographical research

[1] Pós-graduando em Direito Digital e Tecnologia pela FAE Business School. Bacharel em Direito pelo Centro Universitário Curitiba. Advogado e Consultor Jurídico.

technique. From the general concepts found in the specific legislation, basic premises are extracted for the legal conformity of the recruitment systems regarding the protection of personal data.

Keywords: LGPD; Recruiting; Discrimination; Algorithms; Artificial Intelligence.

INTRODUÇÃO

A Inteligência Artificial tem representado um paradoxo ao processo da descoberta e do conhecimento. Muito embora sejam desenvolvidos e treinados por mentes humanas, os algoritmos cada vez mais têm demonstrado novas formas de se observar e compreender o mundo. O mais curioso é que as conclusões inéditas não raramente fluem das mesmas informações disponíveis ao olhar humano, ou seja, as máquinas conquistaram a habilidade de enxergar aquilo que o ser orgânico sequer perceberia, ou pelo menos levaria tempos para observar.

O papel dos algoritmos tem sido, pois, permitir o surgimento de insights jamais obtidos. E muitos desses insights são possíveis graças a uma capacidade dos algoritmos: a predição. Por meio da análise massiva de dados, a inteligência artificial é capaz de identificar correlações nem sempre óbvias e, com isso, tem o poder de prever, com algum grau de precisão, a probabilidade de ocorrência de um evento futuro. Um exemplo simples para isso é a estimativa de tempo de viagem que muitos aplicativos de GPS fornecem aos motoristas: através da análise de dados do ambiente, para além da distância até o destino, tais como o horário e dia da semana, o clima, a velocidade média do motorista e obstáculos na pista, é possível prever o horário preciso de chegada.

A capacidade preditiva dos algoritmos, porém, não é infalível, e seus deslizes podem gerar graves danos, em especial quando as premonições versam sobre possíveis qualidades, vícios ou comportamentos de pessoas humanas. Os caminhos da inteligência artificial, muitas vezes são dotados de obscuridade e exaltam desigualdades pré-existentes, penalizando o livre desenvolvimento da personalidade e da vida humana digna, fenômeno observado, infelizmente, em vários ambientes a nível mundial, agora principalmente no mercado de trabalho.

Urge, portanto, a necessidade de avaliar as repercussões jurídicas do uso de ferramentas de inteligência artificial, e de que maneira Sociedade e Estado podem atuar, isolada ou conjuntamente, para coibir os efeitos negativos do uso da citada tecnologia, garantindo o progresso tecnológico que muito beneficia as pessoas, mas mantendo seguros os direitos e

prerrogativas fundamentais dos indivíduos. Em vista deste propósito, a pesquisa se propõe a analisar os aspectos jurídicos relacionados ao processamento automatizado de dados, e de que maneira a legislação dialoga com essa atividade.

No primeiro capítulo, analisa-se o contexto de aplicação dos algoritmos de inteligência artificial, em especial para o auxílio nos processos de recrutamento de pessoas por organizações, observando também os riscos aos indivíduos, atinentes à referida operação. Em seguida, exploram-se as disposições legais acerca do tema, evidenciando-se as balizas levantadas pelo legislador nacional e internacional para conter os perigos atrelados à espécie. Por fim, analisam-se os princípios e condutas ao alcance das organizações, por meio da autorregulação, para conferir legitimidade e legalidade ao tratamento automatizado de dados, mitigando os riscos da atividade.

1 OS ALGORITMOS NO AMBIENTE DE RECRUTAMENTO

A pandemia do vírus Sars-CoV-2 causou profundas mudanças no cenário econômico mundial, especialmente no campo das relações de trabalho. A grande maioria das profissões, em maior ou menor grau, foram afetadas pelas restrições de deslocamento ou pela impossibilidade de aglomeração de pessoas.

De forma reativa, muitos setores da economia se adaptaram para garantir a produtividade e empregabilidade em face do popularmente conhecido "novo normal". Nesse período, a sociedade vislumbrou uma vertiginosa ascensão do teletrabalho. O legislador brasileiro, inclusive, promoveu, nesse tempo, várias alterações na legislação trabalhista com o intuito de contemplar as nuances dessa nova realidade[2].

Porém, o que seria, a princípio, provisório, se tornou permanente para muitos. Uma vez que a sociedade foi compelida a incorporar os meios tecnológicos de forma intensiva no ambiente de trabalho, o trabalho remoto ou *home office* acabou por se consolidar como modalidade principal em diversos setores, especialmente naqueles ligados a atividades intelectuais e artísticas, as quais já eram exercidas em sua grande maioria através de computadores.

[2] Vide alterações à Consolidação das Leis do Trabalho (Decreto Lei nº 5.452, de 1º de maio de 1943) promovidas pela Lei Federal nº 14.442, de 2 de setembro de 2022.

O resultado disso foi, notadamente, o rompimento das barreiras territoriais, pois os profissionais podem, agora, trabalhar em qualquer lugar do planeta, bastando que possuam um dispositivo eletrônico — seja um computador, *tablet* ou *smartphone* — e conexão à internet. Além disso, as organizações ganharam uma facilidade extraordinária em encontrar capital humano, pois a barreira da territorialidade, que antes seria um fator restritivo, já não existe mais.

Atualmente, uma empresa sediada no Brasil, por exemplo, pode contratar um trabalhador que reside no Egito, possuindo o poder de monitorar, sem maiores dificuldades, seu tempo de trabalho e produtividade. A facilidade de construir equipes de alto nível produtivo no contexto atual é incomparável ao período pré-pandemia.

Em contrapartida, a grande facilidade de encontrar talentos gerada pela ampliação massiva do *pool* de possíveis candidatos traz consigo um efeito colateral: a dificuldade em selecionar os candidatos. Se já era difícil encontrar o melhor candidato entre 50 ou 100 candidatos, agora é ainda mais, considerando que, não raro, vagas remotas são disputadas por dezenas de milhares de pessoas.

A situação inédita exige a adoção de medidas inéditas, razão pela qual muito se tem buscado por abordagens mais modernas e mais eficientes, dentre as quais está o uso de sistemas de inteligência artificial, que apesar de existirem há tempos no mercado, têm se popularizado cada vez mais.

Por meio do aprendizado de máquina, que compreende sofisticados métodos de processamento de dados de forma massiva e rápida, os responsáveis pelo recrutamento podem filtrar os melhores candidatos dentre uma ampla gama de currículos, tendo por base critérios objetivos e alinhados ao perfil de colaborador desejado pela organização.

O objetivo precípuo dessas plataformas, é, portanto, conectar os recrutadores aos melhores profissionais. Mas para além disso, os sistemas se propõem a eliminar influências subjetivas que interferem na parcialidade dos programas de seleção de talentos[3].

Através da adoção de parâmetros técnicos de escolha, seriam, em tese, afastados os enviesamentos causados pelos próprios profissionais recrutadores. A experiência prática, porém, revela que essa eliminação é demasiadamente complexa, quando não impossível.

1.1 O risco discriminatório na IA

[3] A Gaia, inteligência artificial desenvolvida pela empresa de recrutamento Gupy, tem por objetivo, segundo sua proprietária, eliminar os vieses inerentes aos processos seletivos comandados por humanos (GUPY, 2021).

Entre os anos 2014 a 2018, a Amazon, empresa estadunidense conhecida por revolucionar o varejo *on-line* através da tecnologia e automatização, tentou implementar internamente um algoritmo de inteligência artificial que pudesse avaliar de forma autônoma os currículos dos candidatos e atribuir a cada um deles uma nota, a qual variava de uma a cinco estrelas. Assim, a empresa conseguiria escolher um número seleto de candidatos dentre um rol de centenas, tendo sempre a certeza da melhor escolha, segundo critérios objetivos.

De início a ferramenta aparentava ser bem-sucedida, mas não levou muito tempo até que se identificassem as primeiras discrepâncias: Durante a implementação da ferramenta de forma interna, identificou-se que o algoritmo privilegiava candidatos homens e dava notas mais baixas às mulheres. A explicação para isso era porque a máquina havia sido treinada por meio da base de currículos dos próprios funcionários da empresa, que por sua vez revelava uma predominância masculina. Deste modo, quando o modelo encontrava nos currículos termos que indicassem que o candidato era mulher, entendia que isso seria um fator negativo e a nota era rebaixada.

Soma-se, também, outro caso envolvendo a discriminação algorítmica:

> O caso de Kyle Behm é paradigmático. Ele teve problemas para encontrar um emprego depois de ser diagnosticado com transtorno bipolar, mesmo com resultados quase perfeitos em seus exames SAT (a versão estadunidense do vestibular). Behm entrou com um processo contra sete companhias pelo uso de um teste de personalidade desenvolvido pela Kronos, uma empresa de gerenciamento de força de trabalho, por entender que o responsável por sua dificuldade de ser recolocado no mercado era o algoritmo. (MENDES; MATIUZZO, 2019, p. 47)

Estes dois grandes exemplos da história da inteligência artificial ilustram o potencial discriminatório de tais ferramentas. Algoritmos que analisam dados e extraem conclusões sem a intervenção humana possuem um alto grau de imprevisibilidade. Além disso, o aprendizado de máquina, nos casos que envolvem dados pessoais, como no contexto do recrutamento de pessoas, estão fortemente suscetíveis a reproduzir discriminações pré-existentes nas bases de dados que os alimentam.

Em verdade, a inteligência artificial sofre de um mal que pode ser descrito como "efeito fotocópia": quando um documento é replicado através de uma copiadora, sua reprodução tende a possuir qualidade inferior, pois o procedimento ressalta as imperfeições constantes no documento original ou na própria copiadora; quando a cópia é submetida ao mesmo processo, depois a cópia da cópia, e assim sucessivamente, chegará um ponto em que o

resultado será um documento completamente desfigurado e distinto do original. Da mesma forma, a cada iteração do modelo de inteligência artificial, os dados vão tomando novas formas, havendo tanto o risco de afastamento do modelo original, quanto da amplificação de incongruências dos dados inseridos, como no exemplo citado, ou mesmo inconsistências do próprio algoritmo.

Sobre esta temática, Marcela Mattiuzzo (In: DONEDA; MENDES; CUEVA, 2020, p. 118) leciona que o termo "discriminação" pode representar, é claro, uma exclusão do indivíduo, mas está atrelada principalmente à generalização dos indivíduos, por intermédio da adoção de máximas nem sempre vinculadas à realidade de cada um, oriundas da observação equivocada de eventos comuns e sua causalidade.

Assim, a tecnologia acaba por seguir o caminho inverso do que se pretende, que é a eliminação de subjetividades, e, consequentemente, a promoção da diversidade e inclusão de pessoas. Isso, portanto, destaca a necessidade e urgência de se instituir diretrizes éticas para o desenvolvimento destas tecnologias, garantindo, sobretudo, a proteção da dignidade humana.

2 A LGPD E AS DECISÕES AUTOMATIZADAS

A Lei Geral de Proteção de Dados Pessoais (LGPD) é, para o Brasil, um marco na defesa dos direitos dos cidadãos na Era Digital. Explorando seu contexto, a norma ganha apoio popular em um momento que as práticas abusivas no ambiente informacional são latentes, quando dados são comercializados irrefreadamente pelas grandes corporações, mas negligenciados pelo ordenamento jurídico.

Escândalos envolvendo a silenciosa, porém massiva, exploração de dados, e vazamento de projetos de manipulação de consciência da coletividade fizeram o pano de fundo da Lei nº 13.709, promulgada em agosto de 2018, e cujo anteprojeto tramitou desde 2010. Assim, o objetivo da lei sempre foi o de combater as condutas abusivas relacionadas a dados pessoais, incluindo aquelas atreladas ao processamento automatizado.

Um dos princípios que norteiam a lei é a não-discriminação, segundo o qual não é possível realizar o tratamento de dados pessoais para fins segregatórios, ilícitos ou abusivos, uma vez que as operações em questão devem sempre resguardar "os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais" (BRASIL, 2018, art. 2º, inc. VII).

Desta forma, com o intuito de garantir os direitos fundamentais dos indivíduos no ambiente cibernético, a LGPD estabelece uma série de balizas à atividade de tratamento de dados pessoais, dentre os quais estão incluídas as hipóteses ou bases legais que autorizam os agentes a tratar dados de pessoas naturais, conforme observado no artigo 11. Em uma análise preliminar, vislumbram-se ao menos três bases sobre as quais poderá se debruçar o tratamento automatizado de dados para fins de recrutamento de pessoas.

2.1 Consentimento

Como preceitua a Lei Geral de Proteção de Dados Pessoais, o consentimento é um ato livre e formal do titular que, ao conhecer dos métodos e das finalidades do tratamento de dados proposto, opta expressamente por conferir aos agentes tal prerrogativa (BRASIL, 2018, art. 5º, inc. XII). Para muitos, o consentimento é a expressão máxima da autodeterminação informativa do indivíduo, que hoje é guarnecida pelo texto constitucional através do novel inciso LXXIX do artigo 5º, incluído pela Emenda nº 115 de 2022.

Por meio do consentimento, é possível fundamentar uma infinidade de atividades de tratamento de dados não previstas em outras bases legais. Com efeito, controladores e operadores possuem no consentimento uma carta branca para tratar dados conforme lhes demanda a criatividade industrial e comercial, salvaguardados, obviamente, os princípios e direitos protegidos pela LGPD.

No escopo em análise, a lógica não seria distinta: a coleta de dados e informações do candidato, incluindo dados sensíveis, para alimentação de sistemas de recrutamento e seleção baseados em inteligência artificial, utilizando-se como base o consentimento, é *a priori* admissível. Sublinha-se, porém, que este consentimento deve ser juridicamente válido, preenchendo as três características listadas pela Lei Geral de Proteção de Dados, quais sejam, que a autorização do titular seja livre, informada e inequívoca, elementos um tanto cinzentos no contexto ora analisado.

2.1.1 Liberdade do Titular

O titular que consente com o tratamento automatizado de seus dados pessoais deve fazê-lo de maneira independente e resguardada de qualquer influência ou enviesamento. Todavia a prática revela que o fluxo de interesses que envolve a atividade obsta referida

imunidade. Ademais, não é imaginável que, no contexto da oferta e procura de vagas de emprego, a manifestação de vontade do titular de dados seja sempre independente.

Nesta senda, é desnecessária a caracterização da coação, ou qualquer forma de manipulação da vontade, para que o consentimento do titular deixe de ser livre. É que a questão do emprego já carrega em si uma enorme influência de elementos subjetivos: a oferta de trabalho, para o candidato, muitas vezes pode representar a diferença entre o sustento e a necessidade, o prestígio e o descrédito social, a concretização e a frustração de aspirações profissionais. Com efeito, o indivíduo que procura emprego acaba se sujeitando a inúmeras condições — inclusive o tratamento abusivo de seus dados — em troca de sua recolocação no mercado de trabalho.

Por esta razão, arrisca-se dizer que não há, na prática, liberdade de escolha dos titulares de dados pessoais quando o tema é o recrutamento de pessoal, sendo este, por consequência, um aspecto que dificulta o reconhecimento da legitimidade do consentimento dado no contexto ora analisado.

2.1.2 Informação acerca do tratamento

Para que o consentimento seja juridicamente válido, o titular precisa ser informado pelo controlador acerca dos propósitos sobre os quais está alicerçado o tratamento de seus dados pessoais. Não obstante, é seu direito conhecer também os procedimentos aos quais seus dados foram submetidos, incluindo o rol de ações descritas no Art. 5º, X, da LGPD, e até mesmo as técnicas e sistemas utilizados. Em outros termos, o titular tem o direito de saber como seus dados entram, como são tratados e como saem das bases do agente de tratamento.

Isso é um desafio para as aplicações que utilizam algoritmos de inteligência artificial, pois nem sempre informações suficientemente claras a respeito do trajeto percorrido pela informação estarão disponíveis. Em vários casos, nem mesmo os desenvolvedores desses sistemas conseguem explicar como eles produziram os resultados, fenômeno que será descrito como “opacidade”.

Por consequência, o consentimento dado ao tratamento automatizado através de inteligência artificial nem sempre poderá se considerar plenamente informado. Embora seja possível ao agente de tratamento expor aos titulares a finalidade do tratamento, que é, obviamente, a seleção de candidatos, a forma do tratamento será não raramente uma incógnita.

2.1.3 Pertinência do Consentimento

O tratamento automatizado de dados com o fim específico de recrutar pessoas possui, como visto, algumas peculiaridades, seja pela falta de transparência nos algoritmos de inteligência artificial, seja pela influência de elementos subjetivos internos e externos ao titular que se candidata a uma vaga de emprego. Estas especificidades, por certo, geram um elevado grau de incerteza em volta do consentimento manifestado.

Nesse sentido, a adoção da referida base legal é problemática, pois ocasiona fragilidades à regularidade do tratamento de dados, colocando em risco a operação pretendida pelo controlador. Com efeito, o agente de tratamento de dados deve se guarnecer de outros permissivos legais, caso queira garantir a segurança jurídica em torno de sua operação.

2.2 Legítimo interesse do controlador

Outra base legal que merece menção é o legítimo interesse do controlador. Trata-se de uma segunda tábula rasa deixada pelo legislador, assim como o consentimento, para resguardar interesses legítimos dos agentes de tratamento de dados pessoais.

Nos casos em que a hipótese de tratamento não se encaixe adequadamente nas demais circunstâncias autorizadas na LGPD, e caso seja impossível ou impertinente obter o consentimento expresso do titular, mas ainda assim as finalidades do controlador sejam legítimas a partir de situações concretas, com o intuito ora de fomentar suas atividades, ora de ofertar serviços que também atendam à legítima expectativa dos titulares, e desde que não se gere maiores riscos à proteção dos dados pessoais, então o tratamento será lícito.

No escopo da presente análise, observa-se que a adoção da referida base pode ser uma alternativa aos sistemas autônomos de recrutamento, no entanto vários cuidados devem ser observados. Requer atenção, neste aspecto, o destaque dado pelo legislador à necessidade de transparência no tratamento baseado no interesse legítimo. Exige o parágrafo 2º do artigo 10 da LGPD que os controladores garantam a clareza e auditabilidade desses processos. Sendo assim, o controlador que baseia o tratamento de dados em seu interesse legítimo deve expor, de modo adequado, e mais do que em qualquer outra hipótese, quais as finalidades que o levam à atividade pretendida, a maneira como os dados serão tratados e, ainda, quais os riscos aos dados pessoais atrelados à operação.

Para corporificar este último, a LGPD instituiu o dever de elaboração de Relatórios de Impacto à Proteção de Dados (RIPD). Sublinha-se, entretanto, a ressalva feita pela lei no sentido de que a obrigação em questão não se sobrepõe à proteção concedida aos segredos comerciais e industriais dos agentes, evidenciando, desta forma, a preocupação do legislador em não causar interferências com outros dispositivos legais, o que, em contrapartida, traz consigo o dever de permitir ser auditado pelas autoridades competentes, neste caso a Autoridade Nacional de Proteção de Dados (ANPD).

Ademais, a organização que recruta seus colaboradores com o auxílio de ferramentas de inteligência artificial, pautando-se por seu legítimo interesse, muito provavelmente o faz sob a justificativa de que o processo seletivo visa alcançar os melhores candidatos, em benefício ao desenvolvimento adequado das atividades da empresa e, também, como forma de escolha mais justa e objetiva em relação aos candidatos mais bem preparados.

Em contrapartida, a empresa, enquanto controladora, deve garantir a transparência dos processos e decisões desenvolvidas por inteligência artificial, explicitando os tipos de dados que servem como *input* para o aprendizado de máquina, assim como a maneira como o algoritmo realiza a filtragem e classificação dos candidatos, ressalvadas, é claro, as operações protegidas por segredos comerciais e/ou industriais.

2.2.1 Utilização de dados mínimos e o Big Data

Há uma ressalva na utilização do legítimo interesse como base para o tratamento automatizado de dados. Como já abordado, as ferramentas de inteligência artificial comumente se utilizam do processamento massivo de dados para produzir suas decisões. Com efeito, por si só essa característica revela um alto risco de tratamento de dados excessivo, pois usualmente os sistemas em questão são alimentados por variadas bases de dados. Em contraste, a lei salienta que, nesta hipótese de tratamento, sejam utilizados apenas os dados estritamente necessários para o fim pretendido, em alusão ao princípio da necessidade, através do qual surge o dever de minimização do uso de dados.

Assim, levantam-se questionamentos: para um modelo de *machine learning* baseado em *big data*, o que de fato poderá ser considerado dado necessário? Seriam todos os dados que contribuem para o processo de aprendizado de máquina? Ou apenas os estritamente necessários para identificar os candidatos? Ainda, é possível minimizar o uso de dados sem prejudicar as funcionalidades da inteligência artificial? Ora, se a intenção do legislador na instituição deste

requisito é reduzir o uso de dados pessoais com base no legítimo interesse, então a hipótese legal pode não ser a mais adequada para o tratamento automatizado.

2.3 Execução de contrato e procedimentos preliminares

Ainda, a LGPD autoriza o tratamento de dados para sustentar relações contratuais: Se duas ou mais pessoas, naturais ou jurídicas, manifestam o *animus contrahendi* e preenchem todos os requisitos para a formação de um ato jurídico válido, então será possível que os dados pessoais dos contratantes, ou de terceiros a eles relacionados, sejam tratados para o fim de formalizar o liame e/ou propiciar a execução de seu objeto.

É possível também que a operação com dados pessoais preceda a realização do contrato, isto é, sirva para alimentar os "procedimentos preliminares" referidos no inciso V do artigo 7º da Lei Geral de Proteção de Dados. O caso em análise é um exemplo: quando uma organização abre vagas para a admissão de novos colaboradores, está-se diante de uma situação precedente ao contrato de trabalho. Com efeito, é possível que os dados dos candidatos sejam tratados com este fim. Independente disso, existem algumas repercussões que merecem ser observadas.

2.3.1 Restrição de finalidades

Quando o Controlador declara ao titular de dados que o tratamento automatizado de dados tem por fim a seleção dos candidatos mais alinhados ao perfil da empresa, a operação deve seguir esta finalidade de maneira estrita, em respeito aos princípios norteadores do sistema de proteção de dados brasileiro. Mas a dúvida que surge é: todas as finalidades estarão englobadas na finalidade declarada? Ou melhor, é possível englobar nesta finalidade todas as respostas que o algoritmo de inteligência artificial trará para a organização?

Quando uma instituição utiliza ferramentas de inteligência artificial para auxiliar na tomada de decisão em processos de recrutamento, por vezes se busca mais do que organizar e triar currículos. Através do *big data* e das técnicas de *deep learning*, os algoritmos podem coletar dados de forma massiva, cruzando diversas bases informacionais, constituídas não somente por dados fornecidos pelos candidatos, mas por dados de redes sociais, de serviços de proteção ao crédito, e assim, é possível traçar perfis mais complexos de cada um desses titulares, sem mesmo que eles tenham conhecimento disso.

Desta forma, para atendimento do princípio da transparência, positivado no artigo 6º, inciso VI da LGPD, é necessário que o controlador exponha suas finalidades ao titular de maneira clara e completa, discriminando, principalmente, se os algoritmos utilizados fazem mais do que simplesmente triar os candidatos com base nos dados informados por cada titular. Nesta linha, comentam Ana Frazão e Carlos Goettenauer (In: BARBOSA, 2021, n.p.):

> Ora, para que se pudesse ter um mínimo de confiança e tranquilidade em relação a tais processos, seria necessário haver algum tipo de controle tanto sobre (i) a qualidade dos dados, a fim de se saber se atendem aos requisitos da veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização e (ii) a qualidade do processamento de dados, a fim de saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis.

Isso, porém, levanta incertezas na medida em que muitos critérios de seleção, tais como a definição de perfis específicos, eventualmente farão parte de estratégias atreladas ao modelo de negócio do controlador de dados, ou mesmo do operador que fornece o sistema de recrutamento, podendo representar segredos comerciais e/ou industriais. Desta forma, há uma aparente dicotomia entre o direito do titular de obter a devida transparência no tratamento de seus dados e os direitos atinentes ao sigilo com relação a informações confidenciais igualmente tuteladas pelo ordenamento jurídico.

2.3.2 Perda do interesse na vaga e revogação da permissão legal

Outro destaque relacionado à base legal dos contratos, especialmente quando o foco são os procedimentos preliminares, está na possibilidade de perda superveniente da legitimidade do tratamento. Isso pois, o candidato que aceitou participar do processo seletivo pode eventualmente desistir da vaga, e, nesta hipótese, não haverá mais respaldo jurídico ao tratamento de seus dados pessoais.

Vislumbra-se, na espécie, uma forma implícita de revogação do tratamento pelo titular, pois ainda que a operação não esteja baseada exclusivamente no consentimento, que por sua vez comporta revogação, o titular tem poder para decidir sobre sua continuidade ou não. Em verdade, o poder de escolha, neste caso, mais está atrelado à potencial relação contratual, e a correspondente liberdade de contratar, do que efetivamente sobre a aplicabilidade da base legal. Em outras palavras, a revogação da base legal é, na verdade, uma consequência da revogação do interesse em ser contratado.

2.4 O direito à revisão das decisões automatizadas

Outro balizamento deixado pelo legislador para a proteção da dignidade humana face ao avanço tecnológico é a instituição do direito à revisão de decisões tomadas exclusivamente com base em processos autônomos, incluindo, é claro, os algoritmos de inteligência artificial. Uma das principais características atribuídas ao tratamento automatizado de dados, portanto, é o rompimento da intangibilidade de suas decisões. Nos termos do artigo 20 da Lei,

> [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.

Isso quer dizer que o titular, sempre que se sentir lesado em razão de uma decisão gerada autonomamente — através, por exemplo, de algoritmos de perfilamento via inteligência artificial — poderá ter uma reavaliação do processo decisório. No caso concreto, se um candidato eventualmente não concorda com o resultado de um processo seletivo, sabendo que a escolha foi feita unicamente por sistemas automatizados, ele poderá, conforme a legislação, obter o reexame da decisão.

É importante desde já frisar que não se incluem nesta hipótese as decisões semiautomatizadas, que seriam aquelas que contém substancial interferência humana, aqui aproveitando o entendimento do Article 29 Working Party (EUROPA, 2017, p. 21) sobre o contexto europeu. Desta forma, se o algoritmo tão somente dá subsídios (dados estatísticos, consolidação e classificação de ocorrências etc.) para que uma pessoa natural efetive a decisão, então não haverá direito à revisão.

Ato contínuo, é interessante, neste aspecto, destacar a distinção entre a legislação brasileira e a equivalente europeia, retratada no Regulamento Geral de Proteção de Dados, quanto às decisões automatizadas. Ao passo em que a LGPD não apresentou óbices à tomada de decisões automatizadas, tão somente definindo critérios (simplificados) de proteção dos interesses do titular de dados, como o direito à revisão, o Regulamento europeu adotou como regra a impossibilidade da operação de forma exclusivamente autônoma, admitindo-a somente em algumas hipóteses, tais como a execução de contratos, pelo consentimento, ou mesmo por autorização legal dos países membros (EUROPA, 2016, art. 22). De todo modo, ambas as jurisdições conferem ao titular o direito de se opor às decisões: a LGPD, como já abordado, no artigo 20, e o RGPD em seu artigo 22(3).

Com efeito, a instituição do direito à revisão é uma tentativa de driblar a discriminação algorítmica sem, com isso, proibir o uso das referidas tecnologias na tomada de decisões, reconhecendo a fundamentalidade das soluções em face das demandas atuais, assim pois, segundo Souza, Perrone e Magrani (In: BIONI, 2020, p. 257), "[e]m um contexto como esse, a proibição do uso de mecanismos que automatizam decisões ou mesmo inteligência artificial, *machine learning* e afins, seria o mesmo que condenar os humanos ao uso de cavalos depois da invenção do motor a combustão".

No texto original do artigo 20 da LGPD, esta nova análise deveria ser realizada "por pessoa natural", todavia a expressão em questão foi suprimida através da Medida Provisória 869 de 2018, posteriormente transformada na Lei nº 13.853 de 2019. Sendo assim, não há a obrigação de que a nova decisão seja proferida por pessoa física, sendo plenamente possível que o próprio sistema a gere novamente.

Isso posto, muito embora a possibilidade de obtenção de uma nova decisão seja clara, há uma omissão da LGPD sobre a maneira que isso deve se operar. Não há menção se a decisão deve ser necessariamente diferente da original, ou se deve haver uma justificativa plausível no caso de manutenção da decisão. De todo modo, é razoável considerar, ao menos, que o controlador deva realizar o ajuste dos parâmetros e variáveis que influenciaram na conclusão do algoritmo, caso contrário não haveria como se caracterizar a revisão.

Há ainda uma lacuna quanto ao prazo para a solicitação da reanálise. Mesmo que anos tenham se passado a partir de uma decisão automatizada, poderia ainda o titular requerer sua revisão? É provável que a Autoridade Nacional de Proteção de Dados intervenha na questão, ou mesmo o legislador, dispondo sobre o procedimento e os limites temporais para o exercício dos direitos atinentes; enquanto isso, adota-se o prazo prescricional geral da legislação civil, que para a espécie é o decenal, nos termos do artigo 205 do Código Civil — o que, em verdade, é completamente incoerente com o contexto, pois a depender do lapso entre a decisão e seus efeitos, eventual revisão se tornará inócua.

Ademais, o direito à revisão de decisões automatizadas traz como corolário o direito do titular de dados pessoais de compreender os critérios e procedimentos realizados pelo algoritmo, conforme disposto no parágrafo primeiro do artigo 20, também denominado por muitos como o "direito à explicação". De modo distinto da legislação europeia, na qual defendem alguns não estar explícito referido direito (FLORIDI; MITTELSTADT; WACHTER, 2017) — embora outros considerem ser o direito à explicação uma derivação lógica do princípio da transparência (JANSSEN, 2019) —, a lei brasileira o trata de forma expressa no parágrafo

1º de seu artigo 20, estabelecendo como dever do controlador "fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada".

A lógica que antecede a disposição legislativa, também presente nos entendimentos do Article 29 Working Party, é no sentido de que não há como garantir ao titular de dados o direito à revisão da decisão automatizada se ele não tem conhecimento de como a decisão foi formada. Em outras palavras, para que o titular tenha efetivamente a prerrogativa de ver reformada a decisão, ele deve deter subsídios para contestá-la.

Aqui, porém, encontra-se um campo de complexidade, visto que os algoritmos de inteligência artificial sofrem muitas vezes com a falta de transparência em sua operação, fenômeno geralmente referido como "opacidade algorítmica" ou *"black box"*. Isso porque, no aprendizado de máquina, apenas a programação inicial do modelo é feita através da intervenção humana, sendo todo o restante desenvolvido autonomamente pela própria inteligência artificial. Em outros dizeres: sabe-se como a informação adentra o algoritmo, mas se desconhece como os dados são tratados em seu interior.

Quanto ao tema, Marcela Mattiuzzo (In: DONEDA; MENDES; CUEVA, 2020, p. 123) traz a seguinte contribuição:

> Exatamente porque permitem algum nível de criatividade não inteiramente controlada por seres humanos, muitos desses sistemas operam de forma não absolutamente compreensível. Em vários casos, mesmo especialistas na área ou até as próprias pessoas que programam o sistema têm dificuldade em entender perfeitamente o passo a passo da tomada de decisão. (

Frazão e Goettenauer (In: BARBOSA, 2021, n.p.), mesmo reconhecendo a vantagem que a autonomia da inteligência artificial proporciona, também comentam que

> [o]s processos decisórios dos algoritmos de inteligência artificial alcançam [...] soluções que superam a expectativa dos humanos, normalmente sujeitos a vieses cognitivos. As vantagens são óbvias. Resolver problemas insolúveis para os seres humanos ou mesmo realizar tarefas de maneira mais eficiente é o próprio objetivo da utilização da inteligência artificial. Contudo, há a significativa possibilidade de a solução criada pelo algoritmo ser de tal forma inesperada que suas consequências não puderam ser mesmo previstas.

De toda forma, atender às exigências legais e fornecer, com o necessário grau de clareza, informações sobre o tratamento de dados realizado por algoritmos autoprogramáveis, apesar de ser um desafio aos controladores, não pode deixar de ser observado, ainda que isso requeira a revisão de todas as etapas do desenvolvimento da tecnologia. A única ressalva ocorre

para os elementos da ferramenta que sejam sigilosos em razão da presença de segredos industriais e comerciais. Nesse sentido, traz segurança jurídica a salvaguarda feita em diversos trechos da LGPD, pois os direitos relativos à transparência do tratamento de dados, via de regra, não se sobrepõem aos segredos empresariais legalmente protegidos.

3 A ADEQUAÇÃO DOS SISTEMAS DE RECRUTAMENTO À LGPD

A LGPD, diferente do que alguns podem pensar, não é uma lei morta. A sistemática da proteção de dados pessoais envolve não apenas a instituição de direitos e deveres, mas um conjunto completo de salvaguardas e medidas ativas que cada vez mais têm se incorporado à rotina de organizações públicas e privadas para a garantia concreta das previsões legais. Trata-se efetivamente do diálogo entre as disciplinas da proteção de dados e do *compliance*, posto que a efetiva proteção de dados pessoais só pode ser exercida através da verificação e administração dos riscos atrelados às atividades exercidas pelos controladores e operadores.

A expressão *"compliance"*, já incorporada ao vocabulário das instituições, representa o estado de conformidade de uma organização à legislação, podendo ou não manter o enfoque em leis específicas, como no caso da LGPD. Conforme Ricardo Simonsen (In: CUEVA; FRAZÃO, 2018, p. 109-110),

> "[a] área de compliance tem como finalidade atuar na prevenção, detecção e na resposta aos atos corporativos que não estejam em conformidade com a legislação, políticas e normas da companhia. Na prevenção, temos as medidas de caráter educativo (treinamento), de engajamento (comunicação), ações da alta administração e a documentação corporativa (código de conduta, políticas, normas e procedimentos). Na detecção, temos a análise, investigação e monitoramento dos riscos. Na resposta, temos as ações de sanção e remediação desses atos, assim como de melhoria de modelos, práticas e produtos"

No mesmo aspecto, Colin Bennett e Charles Raab (2018), na celebrada obra "The Governance of Privacy", trazem para o contexto dos dados pessoais o tema do *"accountability"*, expressão que também remete à assunção de riscos, desta vez vinculada à prestação de contas pela figura dos causadores desse fenômeno. Segundo os autores, a dinâmica do processamento de dados naturalmente produz riscos aos indivíduos. Desta forma, a sociedade deve reconhecê-los e, por meio dessa assunção de responsabilidade, implementar ferramentas de governança para a proteção dos interesses individuais e coletivos. Com efeito, estes instrumentos podem, é claro, se originar da atividade estatal, como no caso das leis e regulamentos, todavia a autorregulação é, na visão de Bennett e Raab, muito bem vinda.

Assim, unindo-se os conceitos, revela-se a necessidade de implantação de medidas pelos particulares, tais como o desenvolvimento de políticas, estruturas de governança e planos de resposta a incidentes, para a mitigação dos riscos e efetivo cumprimento das normas de proteção de dados.

3.1 Mecanismos de mitigação dos riscos

Conforme a norma técnica NBR ISO 31000, o risco é o desvio causado pela incerteza nos objetivos de uma organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006). É dizer, quando o agente não consolida, de forma aplicada, seus objetivos institucionais, exsurge o risco. No cenário da proteção de dados pessoais, o risco está atrelado: a) aos danos que podem ser causados a titulares; e b) ao descumprimento da legislação específica, caracterizando a irregularidade das operações.

Nos programas de *compliance* com as normas de proteção de dados, assim como em qualquer outra modalidade de programa de adequação, os riscos usualmente são mapeados conforme os processos operacionais que utilizam dados pessoais e suas características respectivas, tais como as finalidades, formas de coleta e armazenamento, classificação dos dados com base em suas espécies, entre outros. Assim, cada processo gera riscos próprios e, a partir disso, são adotadas as medidas de mitigação ou eliminação dos elementos de incerteza.

Como analisado, o tratamento de dados de forma automatizada através das técnicas de inteligência artificial como o *machine learning*, e, por conseguinte, a utilização de decisões automatizadas para o recrutamento e a seleção de candidatos a vagas de emprego, gera muitos riscos aos titulares de dados, especialmente em razão do potencial discriminatório atrelado à atividade. Desta forma, existem, para este processo, algumas medidas aparentemente aptas a mitigar ou eliminar seus efeitos negativos.

3.1.1 Adoção de processos semiautomatizados

Como abordado, a LGPD levanta vários requisitos para a atribuição de segurança e legitimidade ao tratamento de dados realizado por máquinas, especialmente quanto às decisões geradas por mecanismos de inteligência artificial. Dentre as medidas estabelecidas pela Lei, está o dever dos agentes de tratamento de rever essas decisões. Entretanto, da leitura do artigo 20 do diploma em estudo, compreende-se que o direito à revisão só terá lugar quando as

deliberações dos agentes forem “tomadas unicamente com base no tratamento automatizado de dados pessoais”. Ou seja, a revisão só será obrigatória quando todo o processo decisório se basear nas informações e *insights* providenciados pela máquina.

É necessário reconhecer que a redação do artigo é um tanto ambivalente, podendo se interpretar que o legislador estaria se referindo tanto a decisões humanas quanto automatizadas, isto é, contanto que fossem baseadas em um tratamento automatizado. Esta compreensão, por óbvio equivocada, se deve ao fato de que a expressão “automatizada” estaria fazendo referência tão somente ao tratamento, e não à decisão. Mas a dubiedade é logo solucionada pelo disposto no parágrafo 1º do referido artigo, o qual faz uso do termo “decisão automatizada”. Logo, compreende-se que quis o legislador aplicar o direito à revisão sobre as decisões exclusivamente automatizadas.

Com efeito, o cenário não será o mesmo quando o conteúdo fornecido pela ferramenta for utilizado de forma acessória, isto é, quando parcela determinante do processo de decisão estiver sob o domínio humano, ainda que pautado por critérios objetivos gerenciados pela inteligência artificial. É o que se denomina, pela lógica, processo semiautomatizado.

Assim, o método pode ser eficaz para mitigar os riscos discriminatórios do tratamento automatizado, uma vez que, embora os subsídios para as decisões sejam fornecidos pela máquina, estas serão, no fim das contas, decisões humanas. Por consequência, não incidirá sobre esse modelo de tratamento de dados o dever de revisão das decisões, dando maior segurança e estabilidade às relações jurídicas envolvidas.

É importante perceber, porém, que o risco é mitigado, mas jamais eliminado. A justificativa disso é o fato de que não há como garantir que a decisão, apesar de proferida por um humano, não se encontrará enviesada pelo próprio algoritmo, pois se a ferramenta é responsável por filtrar os dados para a tomada de uma decisão, então ela possui grande influência na decisão, em uma espécie de direcionamento implícito.

Assim, mesmo com a adoção de processos semiautomatizados, ainda há chances de discriminação indireta dos titulares de dados. Nesse sentido, é importante que a organização que se utilize de tais ferramentas para selecionar talentos mantenha supervisão ativa e contínua sobre o funcionamento dos algoritmos, e viabilize mecanismos de auditoria interna para avaliar os impactos gerados pelo uso da tecnologia, intervindo nos momentos em que surjam discrepâncias ou indícios de tratamento discriminatório abusivo ou ilegal.

Nesta seara, o Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial (GPAN IA), constituído pela Comissão Europeia, publicou, em 2019, um guia

contendo orientações éticas para atribuir confiança às ferramentas de inteligência artificial. Neste guia, foram dispostas várias recomendações técnicas e de governança, dentre as quais a adoção do postulado da supervisão humana. Segundo o corpo técnico,

> [a] supervisão humana ajuda a garantir que um sistema de IA não põe em causa a autonomia humana nem produz outros efeitos negativos. A supervisão humana pode ser realizada mediante mecanismos de governação como as abordagens de intervenção humana (*human-in-the-loop — HITL*), de fiscalização humana (*human-on-the-loop — HOTL)*, ou de controlo humano (*human-in-command — HIC).*

Destaca-se, do excerto, a última abordagem (HIC), pois se trata justamente do que aqui se estuda, assim dizendo, um mecanismo que garanta minimamente o controle sobre os resultados do processo automatizado através da inteligência artificial, evitando que decisões potencialmente injustas sejam levadas a efeito nos processos seletivos, em prejuízo dos direitos e interesses individuais dos candidatos.

O GPAN IA comenta, ainda, sobre o requisito do controle humano:

> A abordagem HIC refere-se à capacidade de supervisionar toda a atividade do sistema de IA (incluindo o seu impacto económico, societal, jurídico e ético mais geral) e de decidir quando e como utilizar o sistema em qualquer situação específica. Tal pode incluir a decisão de não utilizar um sistema de IA numa determinada situação, de estabelecer níveis de apreciação humana durante a utilização do sistema, ou de assegurar a capacidade de anular uma decisão tomada por um sistema. Além disso, deve ser garantido que as autoridades públicas responsáveis pela aplicação da lei têm a possibilidade de exercer a supervisão em conformidade com o seu mandato. (EUROPA, 2019, p. 19).

Assim, deve a organização não apenas propiciar meios para que seja possibilitada a intervenção humana nos processos, sempre que necessário, mas também a auditabilidade do processo como um todo, tanto por seus órgãos internos, quanto por autoridades estatais, a exemplo, no caso brasileiro, da Autoridade Nacional de Proteção de Dados, observado o disposto na parte final do parágrafo 2º do artigo 20 da LGPD, visando sempre a minimização do impacto discriminatório.

Outro fator importante para que esse controle seja materializado recai sobre o mapeamento e documentação dos riscos, também tratado pela doutrina e legislação estrangeira como *"privacy impact assessment"* ou *"data protection impact assessment"*. Quanto ao tema, interessa destacar o disposto no Regulamento Geral de Proteção de Dados da União Europeia - RGPD (Regulamento UE 2016/679), através de seu artigo 35(3), o qual torna obrigatória a elaboração de uma avaliação de impacto sobre proteção de dados quando houver

> "[a]valiação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar"

Sendo assim, o uso de algoritmos para recrutamento de pessoal, ao menos no contexto europeu, exigirá a elaboração dessa avaliação de impactos. Não é o mesmo, porém, com o cenário legislativo brasileiro: apesar de fortemente inspirada na norma europeia, a Lei Geral de Proteção de Dados brasileira definiu de forma distinta e esparsa as situações de obrigatoriedade da avaliação de impacto, denominada pela lei de "relatório de impacto à proteção de dados pessoais", ou simplesmente RIPD.

Para o legislador brasileiro, o RIPD poderá — e não deverá — ser elaborado quando forem tratados dados pessoais: (i) para fins de segurança pública, defesa nacional, segurança do Estado e investigação e repressão de infrações penais; (ii) pela base legal do legítimo interesse; (iii) por agentes do Poder Público. Além disso, a ANPD pode, a qualquer tempo, exigir dos controladores a elaboração do relatório (BRASIL, 2018).

Com efeito, apesar de não tornar a elaboração do RIPD uma regra, a LGPD deixou essa possibilidade a cargo da Autoridade Nacional de Proteção de Dados, que poderá eventualmente exigir dos agentes de tratamento a realização da análise quando do exercício de tratamento automatizado de dados.

Por fim, analisados os seus aspectos, considera-se que a adoção de processos semiautomatizados é senão o principal método de garantir o controle do risco discriminatório gerado pelos mecanismos de inteligência artificial, desde que criadas salvaguardas pelas organizações para garantir a autonomia da decisão humana

3.1.2 Machine Learning e anonimização dos dados pessoais

Outra abordagem que merece ser citada faz menção ao uso de dados anonimizados. Via de regra, dados que passam pelo processo de anonimização, isto é, de eliminação de seu vínculo com o titular, deixam de ser considerados dados pessoais, uma vez que não é mais possível associá-los a uma pessoa natural, fugindo, portanto, da definição legal de informação pessoal. Por consequência, muitos usam dessa técnica para facilitar o tratamento de dados, porquanto os dados anonimizados não se respaldam pelos mesmos critérios de proteção estabelecidos aos dados pessoais, garantindo maior liberdade ao controlador.

Nas ferramentas de Machine Learning, em especial no uso de *Big Data*, o consumo de dados anonimizados é muito praticado, visto que o aprendizado de máquina não necessariamente depende da identificação dos titulares para o desenvolvimento de perfis de usuários ou candidatos. Ao contrário, a informação é fornecida ao algoritmo de forma difusa e as predições são usualmente realizadas com base nos padrões avistados, sem que haja necessidade de identificar o proprietário da informação, mas apenas compreendê-la perante as outras.

Ocorre que o legislador, muito provavelmente ciente desse contexto, e considerando que o potencial discriminatório da tecnologia persistiria muito embora se tratassem dados anonimizados, incluiu uma ressalva na Lei Geral de Proteção de Dados, definindo que "[p]oderão ser igualmente considerados como dados pessoais [...] aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

Sendo assim, o simples fato de a inteligência artificial poder trabalhar com dados anonimizados não se reveste de fator suficientemente apto a mitigar o risco discriminatório atrelado ao tratamento automatizado de dados, porquanto os dados continuam a servir como subsídio para decisões que afetam diretamente os titulares de dados através da generalização, e consequente discriminação, causada pelo algoritmo.

3.1.3 Instituição de procedimentos e prazos pela Autoridade Nacional de Proteção de Dados

A Lei Geral de Proteção de Dados, como já analisado, não estabeleceu quaisquer procedimentos ou prazos para o atendimento dos titulares de dados pessoais no que tange ao exercício do direito à revisão de decisões automatizadas. Neste sentido, para que haja o mínimo de segurança jurídica nesse aspecto, entende-se que a ANPD deverá regulamentar a matéria.

Quanto ao prazo para solicitação da revisão, especialmente, compreende-se que não poderá ser o mesmo da legislação civil, o qual, por exegese do diploma respectivo, seria o prazo decenal. É que, considerando as características do tratamento de dados automatizado, bem como o contexto em que é utilizado, este prazo de solicitação deveria se reduzir a dias, de modo semelhante à sistemática desenhada na legislação consumerista.

Ademais, é prudente que a Autarquia defina as balizas para a efetiva revisão das decisões automatizadas, exigindo dos agentes de tratamento de dados padrões mínimos de atendimento aos titulares, devendo fornecer ao titular informações completas e adequadas

acerca da revisão da decisão, quando deferida, ou de sua impossibilidade, ou mesmo da ausência de diferenças entre a decisão original e a revista.

CONSIDERAÇÕES FINAIS

A observação inicial do fenômeno da discriminação algorítimica poderia levar ao entendimento de que o cerne do problema está no desenvolvimento destas tecnologias. Mas a questão vai além do código, afinal o *machine learning* apenas reproduz o que lhe é apresentado. Neste sentido, é forçoso reconhecer que a inteligência artificial não gera discriminação sobre membros da sociedade, mas apenas escancara aquelas que antes já existiam. Com isso em vista, não é possível condenar a tecnologia por uma questão que dela não se origina.

Por outro lado, é inegável o fato de que o uso massivo de ferramentas de processamento automatizado de dados tem sido um catalisador de desigualdades, promovendo injustiças nos mais diversos setores da sociedade, notadamente sobre as relações de emprego. Em decorrência disso, foi necessário que as organizações, nesse grupo compreendidos os Estados e a iniciativa privada, tomassem providências para reduzir ou eliminar os perigos decorrentes do uso abusivo de dados pessoais.

Os corpos legais, no Brasil e no mundo, trouxeram, nos últimos anos, grandes avanços no que se refere à obrigatoriedade de adoção, pelas diversas organizações, de mecanismos endógenos e exógenos para a salvaguarda dos direitos dos titulares de dados pessoais, possibilitando um cenário de coexistência entre interesses individuais e institucionais. Neste aspecto, a atual legislação pátria, embora esteja apta a receber melhorias, através da atuação da ANPD, trata das decisões automatizadas, buscando compatibilizá-las com os princípios da legislação, ao mesmo tempo em que dialoga com outras normas, a exemplo da proteção garantida ao segredo industrial e comercial.

Sem embargo, o fenômeno da autorregulação ganha papel de destaque em meio às organizações privadas, o que se dá por meio dos programas de *compliance* de dados. A lógica por trás dos referidos sistemas está atrelada à reputação institucional, e daí se evidencia o seu sucesso, posto que cada vez mais as organizações têm buscado parceiros comerciais institucionalmente íntegros para construir suas redes de negócios de forma segura e economicamente próspera.

Ainda no âmbito das práticas de *compliance*, vislumbra-se a importância da observância aos postulados da privacidade e do controle humano, como dirigentes do processo

de desenvolvimento de soluções tecnológicas autônomas, de modo a atribuir eticidade e transparência ao seu uso. Através desses elementos, é possível encontrar vias de convergência entre a utilização destas ferramentas e os princípios da proteção de dados pessoais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de Riscos – Princípios e diretrizes. NBR ISO 31000. Rio de Janeiro, 2009.

BENNETT, Colin. RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. **SSRN Electronic Journal.** Nova Iorque, 2018. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086>. Acesso em 31 jul. 2021.

BIONI, Bruno et al. (Coords.). **Tratado de Proteção de Dados Pessoais**. 1. ed. São Paulo: Forense, 2021.

BIONI, Bruno. **Proteção de dados pessoais: A função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019.

BRASIL. **Lei nº 13.709 de 14 de Agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 31 jul. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 21 de 14 de fevereiro de 2020.** Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Brasília, Câmara dos Deputados, 2020. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em 31 jul. 2022.

CUEVA, Ricardo V. B.; FRAZÃO, Ana. **Compliance: Perspectivas e desafios dos programas de conformidade.** 2. ed. Belo Horizonte: Fórum, 2018.

DONEDA, Danilo. MENDES, Laura S. CUEVA. Ricardo V. B. (Coords.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A caminho da efetividade: contribuições para a implementação da LGPD.** 1 ed. São Paulo: Revista dos Tribunais, 2020.

EDWARDS, L; VEALE, M. Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For. **Duke Law and Technology Review**. v. 16, n. 1, Durham, 2017.

EUROPA. Comissão Europeia. Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias. **Orientações éticas para uma IA de confiança.** Luxemburgo: Serviço das Publicações, 2019. Disponível em: https://data.europa.eu/doi/10.2759/2686. Acesso em 19 out. 2022.

EUROPA. Conselho da Europa. ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***, Convenção 108, de 28/01/1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?_coeconventions_WAR_coeconventionsportlet_languageId=en_GB>. Acesso em 31 jul. 2022.

EUROPA. Grupo de Trabalho do Artigo 29. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2017)**. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>. Acesso em 30 set. 2022.

EUROPA. **Proposta de regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial.** Jornal Oficial da União Europeia. Bruxelas, 2021. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206>. Acesso em 31 de jul. 2022.

EUROPA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,** Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia. n. L119/1. Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679>. Acesso em 31 de jul. de 2022.

FRAZÃO, Ana; GOETTENAUER, Carlos. Black Box e o Direito Face à Opacidade Algorítmica. In: BARBOSA, Mafalda et al. (Coords.). **Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa.** 1. ed. Indaiatuba: Foco, 2021. *E-book.*

GUPY. **Por que (e como) utilizar Inteligência Artificial no combate aos vieses no recrutamento.** Disponível em: <https://www.gupy.io/blog/inteligencia-artificial-no-combate-aos-vieses>. Acesso em 21 out. 2022.

JANSSEN, Janneke H.N. **The right to explanation: means for 'white-boxing' the black-box?**. 2019. 51 f. Dissertação (LL.M. Law and Technology). Tilburg Institute of Law, Technology and Society. Tilburg. Disponível em: <http://arno.uvt.nl/show.cgi?fid=147348>. Acesso em: 30 set. 2022.

MENDES, Laura S; MATTIUZZO, Marcela. Discriminação algorítmica: Conceito, fundamento legal e tipologia. **Revista de Direito Público.** v. 16, n. 90. Instituto de Direito Público: Brasília, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em 31 de jul. 2022.

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.** Rochester, NY, 28 dez. 2016. Disponível em: <https://papers.ssrn.com/abstract=2903469>. Acesso em: 30 set. 2022.