O PROBLEMA DA PROTEÇÃO DA PRIVACIDADE DIANTE DA VULNERABILIDADE DOS DADOS PESSOAIS DIGITAIS: DIAGNÓSTICO SOBRE O PODER DA GOVERNANÇA ALGORÍTMICA E OS VIESES COGNITIVOS

THE PROBLEM OF PROTECTING PRIVACY IN THE FACE OF VULNERABILITY OF DIGITAL PERSONAL DATA: DIAGNOSIS OF THE ALGORITMIC GOVERNANCE POWER AND COGNITIVE BIASES

Alexandre Freire Pimentel [1]
Juliana Montarroyos Lima Nunes [2]

Resumo: *Por meio de uma metodologia exploratório-descritiva, este artigo analisa o direito fundamental da privacidade, do direito à proteção de dados pessoais e do impacto da tecnologia na regulação das relações sociais. Para tanto, examinam-se os conceitos de privacidade, dados pessoais e a importância da Lei Geral de Proteção de Dados brasileira para a tutela desses direitos. São tratados os desafios éticos e jurídicos relacionados ao uso de algoritmos na tomada de decisão, e expostos seus efeitos discriminatórios. Assim, propõe-se a aplicação de princípios éticos e de justiça, por meio de uma governança algorítmica, objetivando-se um cenário tecnológico mais democrático.*
Palavras-chave: *Proteção de Dados Pessoais. Discriminação Algorítmica.*

Abstract: *Through an exploratory-descriptive methodology, this article analyzes of the fundamental right to privacy, the right to protection of personal data and the impact of technology on the regulation of social relations. Therefore, the concepts of privacy, personal data, and the importance of the Brazilian General Data Protection Law for the protection of these rights are examined. This study addresses Ethical and legal challenges related to the use of algorithms in decision-making, and their discriminatory effects. Thus, we propose the application of ethical principles and justice, through an algorithmic governance, aiming at a more democratic technological scenario.*
Keywords: *Personal Data Protecion. Algorithmic Governance Discrimination.*

[1] Professor do PPGD da Universidade Católica de Pernambuco. Professor da FDR-UFPE. Mestre e Doutor em Direito pela FDR-UFPE. Com pós-doutorado pela Universidade de Salamanca (CAPES-FUNDAÇÃO CAROLINA). Juiz de Direito do Tribunal de Justiça de Pernambuco.
Lattes: http://lattes.cnpq.br/6955582727797003.
ORCID: https://orcid.org/0000-0002-8225-6098.
E-mail: alexandrefreirepimentel@gmail.com

[2] Bacharel em Direito pela Universidade Católica de Pernambuco. Pós-graduanda em Direito Digital pela Católica Business School. Pesquisadora da Liga Pernambucana de Direito Digital.
Lattes: http://lattes.cnpq.br/8655170896224566.
Orcid: https://orcid.org/0000-0002-7723-103X .
E-mail: julianamlnunes@gmail.com

Introdução

Estudos sobre inteligência artificial, algoritmos e tecnologia não parecem, *a priori*, temas relacionados ao campo do direito. Entretanto, a velocidade com que as conexões têm sido estabelecidas no atual contexto da "era da hiperconectividade" tem como consequência a imbricação do ramo tecnológico com as diferentes esferas da vida social, cultural e política. Tal interligação ocorre, em especial, na esfera jurídica.

Dessa maneira, o direito, e, mais precisamente, o direito fundamental à privacidade (Art. 5º, X, CF) (BRASIL, 1988), vem sofrendo grande impacto, mediante as novas relações que se estabelecem com o uso de dispositivos eletrônicos. Tal feito possibilitou, sobretudo, uma ampla automação de serviços elementares e decisões, bem como a disponibilização quase irrestrita, aquiescida e compulsória dos nossos dados pessoais. Dessa maneira, esses dados são coletados, tratados e utilizados para interesses não consentidos e, por vezes, indeterminados e ilícitos.

O direito à privacidade surge como um direito subjetivo fundamental, sendo uma espécie de direito relativo à personalidade, que tem por objeto, em síntese, assegurar a integridade e a dignidade da pessoa humana, características basilares para um estado de direito. Por sua vez, o direito à proteção de dados pessoais sucede o direito à privacidade, imbrica-se com este e é produto da chamada sociedade da informação.

O grande contingente de informações associado à imensa quantidade de circulação de dados resultou em uma importante revolução informacional: o Big Data. Os megadados, como também são conhecidos, podem ser definidos como um numeroso conjunto de dados que, ao serem minerados, são capazes de gerar informações de importante relevância socioeconômica. A multiplicidade de sistemas algorítmicos autônomos, agregados à produção em hiperescala de dados, originou uma nova lógica de acumulação, representada pelo capitalismo digital, pela Internet das Coisas (IOT) e, especialmente, pelo aprendizado de máquinas (*machine learning*). Esse conjunto de megadados apresenta-se como uma nova e complexa realidade, gerida por grandes corporações tecnológicas, as quais se tornaram capazes não apenas de predizerem comportamentos humanos, mas, sobretudo, de prescreverem tais comportamentos. Desse modo, grandes corporações se tornaram capazes de influenciar diretamente as escolhas sociais, incluindo as áreas do consumo e da política.

Os algoritmos têm tomado espaços cada vez mais importantes na nossa esfera social, em razão de sua íntima relação com, praticamente, todo nosso comportamento em rede. O simples uso de um buscador como o Google pode nos direcionar para resultados específicos, a partir de rastros de informações que oferecemos ao navegar. Nosso perfil de mercado e até nossas preferências políticas podem ser previstos, correspondendo esse fenômeno, portanto, a uma transformação desses dados em uma estatística preditiva e prescritiva ou ao que pode ser chamado de superpersonalização.

Para analisar esse fenômeno, o presente artigo utiliza uma metodologia exploratória e descritiva, focada no método bibliográfico com revisão de literatura e por meio da análise das legislações pertinentes ao tema. Tem por objetivo estudar o problema da proteção da privacidade sob a perspectiva da vulnerabilidade dos dados pessoais digitais, para, em sequência, oferecer um diagnóstico imparcial sobre o poder da governança algorítmica e os vieses cognitivos que produz.

Referencial Teórico

A garantia da privacidade no ordenamento jurídico brasileiro

A garantia da inviolabilidade da vida privada constitui ponto fundamental em sociedades democráticas e envolve tanto a proteção à privacidade quanto à intimidade das pessoas (DONEDA, 2006). No Brasil, é concebida como um inequívoco direito fundamental, positivado no inciso X, do artigo 5º da Constituição Federal de 1988. Por sua vez, o artigo 21 do Código Civil ratifica que "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". A Lei do Marco Civil da Internet (LMCI - Lei nº 12.965/2014) também referendou

a proteção à vida privada, ao referir, explicitamente, em seu artigo 3º, inciso II, que a disciplina do uso da internet no Brasil deve reger-se pelo princípio da proteção à privacidade**.** No mesmo prumo, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em seu artigo 1º, esclarece que um de seus pilares centrais consiste em proteger o direito à privacidade, expressando, ademais, que este se trata de um verdadeiro direito fundamental.

A proteção à privacidade também é adotada por diversos tratados internacionais, a exemplo da Convenção Americana sobre Direitos Humanos e da Declaração Universal de Direitos Humanos (ONU, 2020), a qual também incluiu o direito o direito à vida privada no âmbito da categoria de direito humano fundamental.

Entretanto, a palavra privacidade detém uma indeterminação conceitual derivada da diversidade de termos utilizados para defini-la, tanto na doutrina como nos dispositivos legais. A propósito, ventilam-se as seguintes proposições: "... vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e até mesmo 'privatividade' e 'privaticidade', entre outros" (DONEDA, 2006, p. 101). Não obstante, a taxonomia do "Esquema de esferas concêntricas", desenvolvida na doutrina alemã, por Hubmann, tem logrado aceitação de parte considerável das doutrinas nacional e estrangeira. A teoria espelha uma representação de graus distintos do sentido conotado pela privacidade, a partir de esferas concêntricas. Assim, a primeira esfera, ou esfera privada, diz respeito a questões excluídas do conhecimento de terceiros. Esta seria, portanto, a esfera mais abrangente da vida privada e envolve outras duas esferas. A segunda delas representa a intimidade, e, por fim, a esfera mais profunda designa a das ações humanas sigilosas (HIRATA, 2017).

No Brasil, Ferraz Júnior (1993) define a privacidade como um direito subjetivo fundamental, que contém, em sua estrutura, três elementos básicos: o sujeito, o conteúdo e o objeto. O sujeito seria o possuidor do direito, seja pessoa física ou jurídica. O conteúdo consiste na capacidade conferida ao sujeito de impor respeito ou de resistir à violação do pertinente apenas a si próprio. O objeto, por fim, é o bem da vida privada, juridicamente protegido e que pode ser traduzido pelo interesse na preservação (FERRAZ JÚNIOR, 1993) de não publicização do que é privado.

Apesar da imprecisão conceitual do termo 'privacidade', é possível afirmar que seu objetivo se resume a alcançar a proteção efetiva e eficaz da tutela do direto fundamental da vida privada da pessoa humana, retratada tanto em seu contexto mais amplo quanto em seus aspectos mais restritos ou sigilosos. No contexto da atual conjuntura dos relacionamentos humanos regidos pela hiperconectividade tecnológica, a proteção sobre a esfera da vida privada se torna cada vez mais necessária. O interesse global sobre a privacidade, devido à influência da sociedade da informação, pôs a privacidade no epicentro da era digital. Nesse cenário, o avanço tecnológico vem provocando um constante conflito entre liberdades e direitos, sobretudo na vinculação entre a proteção da privacidade e os dados pessoais (DOTTI, 1980). Adentra-se, portanto, na análise dessa problemática.

A proteção de dados pessoais no Brasil

A proteção de dados pessoais no Brasil pode ser destacada, do ponto de vista histórico, a partir da promulgação da Constituição Federal de 1988, a qual, em seu artigo 5º, inciso XII, instituiu a garantia da inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas. A Carta Política ainda dispôs, no mesmo artigo 5º, incisos LXIX, LXXII e LXXVII, sobre o direito fundamental ao *habeas data,* cujo suporte fático para seu exercício pressupõe conduta de gestor público responsável pela negação do direito à informação pessoal, cometida com ilegalidade ou abuso de poder por autoridade pública ou agente de pessoa jurídica no exercício de atribuições do Poder Público.

Conquanto a Lei nº 9.507, de 12 de novembro de 1997, tenha regulamentado o direito de acesso à informação e disciplinado o procedimento do *habeas data,* esta regulamentação impôs limites ao direito à informação no setor público. Entretanto foi a Lei nº 8.078, de 11 de setembro de 1990, que instituiu o Código de Proteção e Defesa do Consumidor. Tal lei, de fato, inovou o ordenamento jurídico brasileiro, ao reservar uma seção específica para tratar dos bancos de dados e cadastros de consumidores, propiciando-lhes o direito de acesso às

informações constantes dos cadastros, fichas, registros, bem como aos seus dados pessoais e de consumo, incluindo o direito de saber as respectivas fontes produtoras das informações cadastradas.

Não obstante, a normatização da proteção de dados pessoais em ambiência eletrônica, de modo explícito e específico, só veio à tona no cenário jurídico nacional com o Decreto nº 7.962/2013. Este decreto regulamentou o CDC no pertinente à contratação eletrônica, enquanto, no inciso VII do artigo 4º, teve como finalidade a garantia de atendimento ao consumidor, facilitado nas relações contratuais de comércio eletrônico. O decreto, assim, estabeleceu que o fornecedor de produtos devesse: "utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor".

Em sucessivo, a Lei do Marco Civil da Internet (LMCI), em seu art. 3º inciso III, erigiu à categoria de princípio jurídico a proteção dos dados pessoais no Brasil. Ademais, o art. 7º da LMCI estabeleceu que "o acesso à internet é essencial ao exercício da cidadania". A lei ainda assegurou, aos usuários da rede mundial de computadores, o direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, acrescentando, ainda, que somente poderão ser utilizados para finalidades que justifiquem sua coleta. A LMCI ainda sinaliza que o dado não consista em propósito vedado por lei e que esteja especificado nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. O inciso IX do mesmo artigo 7º da LMCI impôs a exigência do consentimento expresso do titular dos dados como condição para sua coleta, uso, armazenamento e tratamento. Em sequência, o artigo 14 do Decreto nº 8.771, de 11 de maio de 2016, que regulamentou a LMCI, enfim, conceituou os 'dados pessoais' e o respectivo 'tratamento' em ambiência eletrônica, nesses termos:

> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
>
> II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Esse macrossistema de proteção de dados analisado não tratava da matéria de modo exauriente, requerendo complementação legislativa, a qual aconteceu por meio da Lei nº 13.709/2018 (LGPD – Lei Geral de Proteção de Dados), com as alterações procedidas pela Lei nº 13.853/2019. Como revela Gabriel Cavalcanti Neto (2021), a nova lei brasileira foi inspirada no regulamento geral sobre a proteção de dados da União Europeia (GDPR - *General Data Protection Resolution*), o qual é regido pela Regulação nº 2016/679, e passou a vigorar em 25 de maio de 2018.

A adesão do Brasil ao sistema europeu justifica-se, como patenteiam Santiago e Tamba (2018, p. 18) "... entre outros motivos, da intenção de incluir o Brasil no rol de países que proporcionam um grau de proteção de dados pessoais adequados conforme parâmetros internacionais". Não por outra razão, o objetivo e o objeto da LGPD foram enumerados em seu artigo 1º, o qual os especifica da seguinte maneira:

> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os

direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Quanto à definição de dados pessoais, a LGPD seguiu a esteira do Decreto Presidencial nº 8.771, de 11 de maio de 2016, acima citado, o qual, por sua vez, também trilhou a senda do GDPR à medida que o inciso I, do seu artigo 5º, restringiu a "informação relacionada à pessoa natural identificada ou identificável" (LASSALE, 2017, p. 17). Como observa Lassalle (2017), os dados pessoais representam a nova estrutura do mundo, o vetor das mudanças que a revolução digital produz e se consubstanciam como verdadeiras comodities imateriais que estão a deslocar o trabalho humano como unidade de medida e fonte principal da riqueza promovida pelo capitalismo digital.

Mais de uma centena de países possuem legislação de proteção de dados, o que reflete a grande relevância do tema, sobretudo, no atual cenário de ultraconectividade. Autonomia, liberdade e privacidade do indivíduo são alguns dos temas que se relacionam com a tutela dos dados pessoais. Contudo, o tratamento desses dados por procedimentos cada vez mais automatizados, o que, aliás, é permitido tanto pelo GPDR quanto pela LGPD, expõe a ameaça de uso indevido por diversos setores sociais, em especial, pelas grandes corporações do setor tecnológico.

Sob outra ótica, é importante salientar que, apesar de o conceito de privacidade e de dados pessoais apresentarem uma notória conexão, esses não devem ser confundidos. A privacidade diz respeito à proteção individual contra interferências alheias na esfera da vida privada, englobando, inclusive o direito à intimidade, e tem a função de limitar o acesso de informações ao nosso respeito. Já a proteção aos dados pessoais, por sua vez, refere-se a um conjunto mais amplo de garantias fundamentais, não se limitando à tutela da privacidade (DONEDA, 2010; DONEDA; ALMEIDA, 2016). No entanto, essas duas temáticas imbricam-se entre si, ao mesmo tempo em que se entrelaçam com o problema da coleta indevida de informações pessoais e sua sucessiva manipulação e tratamento por potentes sistemas de inteligência artificial. Esses sistemas inauguraram a era da governança algorítmica, por meio de um sistema de vigilância social que se habilitou não apenas a predizer comportamentos, mas, igualmente, a prescrevê-los.

A disruptiva era da vigilância algorítmica

Ao tratarmos da sociedade da informação, não podemos deixar de reconhecer o protagonismo e a centralidade que as tecnologias de comunicação ocupam nos direcionamentos das decisões humanas na contemporaneidade (MATOSO, 2013). Com a evolução tecnológica e dos meios de disseminação de informação, algumas concepções relativas à personalidade e à privacidade tornaram-se alvos frequentes de intervenções indevidas de terceiros, o que impele a sociedade civil organizada a discutir os parâmetros e ferramentas técnicas e jurídicas de proteção da esfera privada dos indivíduos.

As novas dinâmicas de compartilhamento de informações são, com frequência, disponibilizadas para setores públicos e privados, sob a justificativa de eficiência de seu funcionamento. Além disso, novos artefatos tecnológicos já possuem seu funcionamento atrelado à coleta de dados de seus usuários, facilitando, portanto, o armazenamento e a propagação de informações. Tais medidas evidenciam uma violação à tutela da privacidade, uma vez que o indivíduo passa a não possuir o controle de seus dados. Nessa medida, o sujeito se vê impelido a aceitar os termos e condições de aplicações de internet para poder inserir-se nos círculos relacionais sociais (DONEDA, 2006).

No caso das instituições públicas, a lógica é a seguinte: quanto mais informações pessoais a administração pública obtiver, mais eficiente será. As pesquisas estatísticas e censos são alguns exemplos dessa lógica. O efeito prático da concentração de informação é que quanto mais dados armazenados e disponíveis determinado órgão público possui, maior será o poder de controle que deterá sobre os indivíduos. Tal fato, por si só, demonstra a necessidade de se estabelecerem critérios precisos para a coleta desses dados (DONEDA, 2006). No entanto, a

imposição de critérios jurídicos para tal escopo não é tarefa fácil. A violação da privacidade aumenta exponencialmente na medida em que a internet promove a facilidade de disseminação de informações. Como os limites da coleta, armazenamento, tratamento e reprodução informacional não são visíveis, podem ser, consequentemente, facilmente ultrapassados (DONEDA, 2006).

Por um lado, temos a facilidade de comunicação e disponibilidade de serviços que fazem parte do nosso cotidiano, como aplicativos de internet que nos auxiliam nas mais diversas utilidades. Mas, por outro lado, oportuniza-se o controle e vigilância social das corporações tecnológicas, a qual se efetiva por meio de seus algoritmos. Sobre a essa problemática, o sociólogo Sergio Silveira adverte que:

> [...] as tecnologias de informação são tecnologias da inteligência. Elas não ampliam nossa força física, mas aumentam nossa capacidade de armazenar, processar e transferir informações. Elas interferem em nossa cognição e nas possibilidades do nosso pensamento. Podem ampliar, restringir, moldar e limitar nosso modo de comunicar, interagir e organizar informações (SILVEIRA, 2015 *apud* LEIGH; HARDING, 2015. p.12).

Nesse contexto, é também relevante observar a intersecção entre dados e poder econômico. A informação digital coletada com ou sem o consentimento dos respectivos titulares são verdadeiras comodities representativas dessa nova era, designada como 'capitalismo digital'. Nessa era, destacam-se as grandes corporações tecnológicas, que operam em escala global, como o Google, Amazon, Apple e o Facebook. Essas empresas são detentoras de um extenso monopólio econômico nos mais variados setores. São companhias capazes de acumular diversas informações pessoais, tais como: o que gostamos, o que lemos, onde passamos as férias, o que fazemos etc. (SILVEIRA, 2015). Por sua vez, na China, está em curso um intensivo processo de investimentos em pesquisas sobre a Inteligência Artificial (IA) e empreendedorismo digital, envolvendo não só o governo chinês, mas universidades, centros de pesquisa, empresários e corporações tecnológicas. "Dinheiro para o desenvolvimento de IA está chegando de capitalistas de risco, das gigantes de tecnologia e do governo chinês" (LEE, 2019, p. 12). O autor ainda arremata, que "subjacente a essa onda de apoio do governo chinês está um novo paradigma na relação entre a inteligência artificial e a economia" (LEE, 2019, p. 16).

Estamos expostos a uma cultura de vigilância sem precedentes. Porém, a associação entre técnica e tecnologia à vigilância social, em verdade, não é um fenômeno recente. Desde os primórdios do liberalismo, a técnica produzira uma 'consciência vigilante', que passou a interferir incisivamente no mundo dos fatos (SPENGLER; WEBER, 2000). Mais tarde, em meados da década de 1950, Jacques Ellul alertara para o lado vigilante e dominador da governança tecnológica, por meio da sutil criação de "...uma atmosfera, um envolvimento, e mesmo um modelo de comportamento nas relações sociais" (ELLUL, 1968, p. 104). Porém, com a instituição do capitalismo digital, a vigilância social intensificou-se ao ponto de haver o risco de a governança algorítmica transformar o "sujeito humanista" num "indivíduo algoritmicamente assistido", instituindo-se uma "humanidade aumentada" pela assistência algorítmica das tecnologias digitais, as quais tomam decisões para os humanos, passando ao largo da vontade humana (SADIN, 2017, p. 129).

Um caso emblemático de vigilância algorítmica aconteceu no ano de 2013 (REDAÇÃO ÉPOCA, 2013), momento em que o ex-analista da NSA (Agência de Segurança Nacional dos Estados Unidos), Edward Snowden, denunciou programas de vigilância usados pelos Estados Unidos para espionar a população americana e diversos países europeus e latino-americanos, incluindo o Brasil. A vigilância acontecia por meio de empresas como o Google, Apple e Facebook. A então presidenta do Brasil, Dilma Rouseff, e a chanceler alemã, Ângela Merkel, foram vítimas de uma quebra no sigilo de telecomunicações. Como resposta, as líderes apresentaram uma proposta à Organização das Nações Unidas de um projeto referente ao direito à privacida-

de na era digital, intitulada "Privacidade na Era Digital" (MATOSO, 2013).

É inegável que a tecnologia modificou, modifica e modificará padrões do que antes era conhecido como privacidade, intimidade e sigilo. Ainda que os conceitos desses institutos sofram transformações, a sua tutela apresenta-se como uma necessidade premente, devendo, por isso, ser juridicamente assegurada. Para tanto, faz-se necessário associar o direito à privacidade à tutela de outros direitos correlatos, como o direto à igualdade e não discriminação e o direito à liberdade de expressão. Do contrário, o risco de os algoritmos reproduzirem preconceitos sociais é imenso, como descrito a seguir.

Discriminação social e governança algorítmica

No ano de 2015, um programador norte-americano, que é usuário do Google Fotos, descobriu que o programa etiquetava pessoas negras como gorilas. O caso aconteceu quando o programador tirou fotos junto com seus amigos e decidiu fazer o *upload* nessa recém-lançada plataforma digital, e então percebeu que suas fotos estavam organizadas em um álbum nomeado "Gorilas". O sistema, que funciona por meio de Inteligência Artificial, não foi capaz de distinguir a pele humana com a do animal (PASCUAL, 2019). O algoritmo com "viés racista" fez com que o Google se desculpasse pelo erro e prometesse repará-lo. Contudo, dois anos após o ocorrido, a revista Wired resolveu testar o algoritmo, adicionando diversas fotos, inclusive de algumas espécies de macacos. O sistema, no entanto, conseguia identificar imagens quando era buscado por "orangotangos", "babuínos" ou "saguis", mas não respondia quando se buscava por "macacos" ou "gorilas" (PASCUAL, 2019).

Assim, o Google decidiu resolver o problema de uma forma mais simples: apagando as referências. De acordo com um porta-voz do Google, a tecnologia de etiquetar é recente, e, por isso, não é perfeita, admitindo a discriminação como um 'erro'. Problemas semelhantes já se repetiram em plataformas, como Flickr e o Facebook, que permitiam distinguir usuários por raça (PASCUAL, 2019).

Em 2016, a *Red Cross Blood Service*, prestadora de serviços de coleta e de doação de sangue na Austrália, foi vítima de um atentado em seu sistema de segurança de dados e informações, o qual continha cerca de 550 mil doadores. O fato ocorreu devido à transferência indevida de arquivos a uma rede de computadores sem autorização para o tratamento desses dados (MULHOLLAND, 2018). Assim, diversos dados pessoais armazenados entre os anos 2010 e 2016 foram disponibilizados publicamente na internet, como gênero, nome e data de nascimento. Porém, dentre as informações vazadas, uma era especificamente sigilosa. A informação comunicava que, entre os doadores, um deles teria "um comportamento sexual de risco", uma vez que as pessoas tinham se submetido a um questionário em que era perguntado se o doador havia participado de atividades sexuais de risco nos últimos doze meses. A empresa disponibilizou ajuda às vítimas e se retratou pelo erro (MULHOLLAND, 2018).

Em um sistema de recrutamento para novos funcionários, a empresa Amazon precisou remover seu sistema de algoritmos, utilizado para seleção de candidatos, porquanto a inteligência artificial adotada priorizava somente candidatos do sexo masculino. O sistema foi criado a partir de dados de currículos recebidos ao longo de dez anos. A Agência Reuters indicou que a prioridade dada aos homens para as vagas se devia ao fato de o banco de dados ser formado, em sua maioria, por profissionais do sexo masculino. O programa foi desenvolvido em 2014 e já em 2015 foram detectados os indícios de sexismo, quando o algoritmo passou a deletar automaticamente as fichas que continham a palavra "mulher". Sobre isso, a empresa não quis se pronunciar (REDAÇÃO HYPENESS, 2018).

Os casos apresentados nesta seção se referiram a assuntos de natureza racial, de orientação sexual e de gênero, demonstrando, inequivocamente, a violação de dados pessoais sensíveis no tratamento algoritmizado de informações. A utilização não consentida desses dados, tanto pelo setor privado como pelo público, enseja violações a direitos fundamentais e, por isso, representa um alerta para os novos cenários tecnológicos. A propósito, o inciso II do artigo 5º da LGPD define dados pessoais sensíveis, como os relativos à:

> [...]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.

Os algoritmos permeiam a vida social na era digital e o método do aprendizado de máquina está, cada vez mais, envolvido na tomada de decisões importantes. O uso indiscriminado e desregulamentado dessas tecnologias pode acabar hipertrofiando os poderes decisórios artificiais e, por vezes, consentir com deliberações preconceituosas, as quais são previamente adotadas por aqueles que programam os algoritmos. Entretanto, não obstante o fato de o programador ser responsável por alimentar os sistemas computacionais, em se tratando de sistemas autodidatas, os métodos de controle decisórios se tornam cada vez mais complexos e não transparentes.

Racionalidade algorítmica e desigualdade

Embora os algoritmos eletrônicos consistam em fórmulas matemáticas criadas para serem executadas por computadores, e à primeira vista pareçam detentores de uma natureza objetiva e neutra, nada obsta, do ponto de vista informático, que contenham atributos decisórios tendenciosos em sua construção. A racionalidade algorítmica consiste em um modelo específico de logicidade pelos algoritmos, que desempenham um importante papel nos procedimentos de cognição dos fatos e, sobretudo, de tomada de decisão, como explica a professora da Universidade Federal do Rio de Janeiro Fernanda Bruno:

> Um modelo de racionalidade implica simultaneamente produzir conhecimento e intervir sobre um determinado contexto, problema, fenômeno ou realidade. Em nossa sociedade, especialmente em nossas experiências tecnologicamente mediadas, os processos algorítmicos vêm se tornando atores decisivos tanto na captura e análise de dados sobre uma série de setores de nossas vidas privadas e comuns, quanto na tomada de decisão automatizada em diferentes contextos (gestão urbana, políticas públicas, comunicação, trabalho, mercado financeiro, estratégias de marketing e publicidade, segurança etc. (DIGILABOUR, 2019).

Dessa forma, é fundamental que estejamos atentos a essa nova maneira de processar informações, posto que o processo de automação, apesar de sua incontestável utilidade, eficiência e velocidade não é, necessariamente, associado aos valores éticos da sociedade na qual atuam. Prova disso são os inúmeros casos e pesquisas que demonstram a existência de um viés, seja de gênero, raça ou classe, nos processos de tomada de decisão.

Os impactos negativos do uso de algoritmos têm sido tema central de diversos estudos. Exemplo importante, a propósito, é o da matemática CathyO'Neil, que em seu livro, *Weapon Of Math Destruction* (O'NEIL, 2016), demonstrou a maneira pela qual os algoritmos podem incorporar padrões discriminatórios de raça e classe, perpetuando desigualdades existentes na realidade capitalista neoliberal. A autora afirma que as sofisticadas fórmulas matemáticas que orientam atualmente nossas vidas são como verdadeiras armas e, por isso, podem ser direcionadas para prejudicar determinadas pessoas. Ainda, enquanto as armas comuns possuem um alcance limitado, os algoritmos podem atingir milhares de indivíduos ao mesmo tempo. A esse respeito, Shoshana Zuboff denomina uma característica ubíqua dos algoritmos que gerenciam o capitalismo digital, os quais sabem "tudo *sobre nós*, ao passo que suas operações são programadas para não serem conhecidas *por nós*..." (ZUBOFF, 2021, p. 22).

Apontam-se diversos exemplos de sistemas estadunidenses que caracterizam o impacto

negativo desses modelos matemáticos, como consultas realizadas por empresas de concessão de crédito, que verificam a viabilidade de adimplemento por meio de cálculos algoritmos. O sistema funciona a partir de tendências criadas com base nos dados pessoais dos indivíduos, sendo, assim, produzidos perfis, os quais, por vezes, consideram como parâmetro creditício o local em que a pessoa reside ou mesmo critérios de raça (O'NEIL, 2016)

Riscos do uso de algoritmos e os desafios para proteção de dados pessoais

Na medida em que ferramentas computacionais são adotadas em processos decisórios, de maneira total ou parcial, os riscos de vieses nas decisões por elas tomadas são uma realidade já comprovada na prática. Uma abordagem sociológica do uso de algoritmos implica, necessariamente, percebê-los não como um ente abstrato e neutro, mas sim, multifacetado e, por isso, nem sempre imparcial. Um número crescente de problemas de interesse público acontece diuturnamente, os quais são resolvidos no mundo dos dados, reforçando a discussão de seu caráter essencialmente político. Diante disso, a tomada de decisão automatizada pode representar riscos significativos aos direitos e liberdades dos respectivos titulares das informações.

A LGPD propõe-se a resolver a questão, recorrendo, para tanto, a princípios que têm o objetivo de limitar dados coletados, que podem ser utilizadas para compor os algoritmos, a partir de critérios. Esses critérios envolvem elementos como proporcionalidade e transparência, que têm a finalidade de evitar práticas discriminatórias. Além de princípios éticos, a proteção à privacidade e outras liberdades fundamentais também são enfatizadas na lei, como já descrito neste estudo. Contudo, a eficiência em sua aplicação e o acatamento pelas corporações tecnológicas são aspectos de dificílima concretização. Isto ocorre porque, ainda que haja uma intenção de fiscalização ativa pela Autoridade Nacional de Proteção de Dados sobre a conduta dos agentes controladores de dados, a coleta algorítmica de informações pessoais ocorre de modo instantâneo, impossibilitando o controle sobre essa fase. Ademais, há um universo gigantesco de dados que são armazenados em plataformas situadas fora do Brasil, sendo esse também outro fator de impossibilidade de controle efetivo.

É necessário, portanto, indicar alguns aspectos prejudiciais que devem ser atentamente investigados na busca de uma maior precisão no resultado indicado pelo algoritmo.

Neutralidade

As minorias e os grupos mais vulneráveis têm a situação agravada diante dos sistemas automatizados, o que torna distante a ideia de neutralidade. As decisões algorítmicas tendem a reforçar preconceitos e estereótipos que existem em sintonia com a configuração social fora das redes. São inúmeros os casos que envolvem alguma forma de discriminação praticada por algoritmos. Aqui, fala-se em discriminação negativa, quer dizer, aquelas decorrentes de uma distinção arbitrária, normalmente relacionada a dados sensíveis, como raça, classe e gênero. O debate sobre as tendências discriminatórias dos algoritmos tem ganhado repercussão desde que inúmeros casos pelo mundo vieram à tona, reforçando a necessidade de mudanças consistentes na fiscalização no processo de sua criação e atuação na rede.

É importante ressaltar que valores éticos e morais estão embutidos nos próprios algoritmos, uma vez que são construídos por humanos. Assim, a responsabilização não deve ser observada apenas a partir do ângulo jurídico, isoladamente. Uma hipótese a ser considerada é a da responsabilização sobre a técnica em si, ou seja, sobre o processo técnico de criação realizado por engenheiros de *softwares* e programadores. O princípio da não discriminação, que respalda a legislação de proteção de dados brasileira, representa uma orientação para que o tratamento de dados não seja utilizado para fins discriminatórios ou abusivos. Por conseguinte, os dados sensíveis recebem uma camada extra de proteção. Todavia, a captura e o tratamento de dados potencialmente discriminatórios podem ocorrer em situações específicas e previstas em lei.

Devido a "falhas no sistema", o racismo tem sido uma das práticas mais reproduzidas

por sistemas que utilizam tecnologia algorítmica. Exemplos comuns dessa prática são os *softwares* de reconhecimento facial. Segundo os pesquisadores JoyBuolamwini e TimnitGebru, do MIT (Massachusetts Institute of Technology), o reconhecimento obtém melhor desempenho em rostos de pessoas com pele clara. A pesquisa avaliou a tecnologia facial de empresas como a MIT e a Microsoft, e demonstrou que o reconhecimento facial de mulheres negras apresentava o maior índice de erro, o qual atingia a média de 30%, em contraponto a 1% com homens brancos (BRANCO, 2016; QUEIROZ, 2019).

Outro exemplo relevante diz respeito à utilização de técnicas estatísticas preditivas para detectar tendências de reincidência criminal, ou duração de pena. Um relatório investigativo do jornal Pro Publica descobriu que, em um modelo de algoritmo preditivo utilizado por juízes norte-americanos, foram encontradas disparidades de sentenças em relação a pessoas de cor escura, que sofrem penas mais severas do que as de cor branca, consistindo em discriminação racial na justiça criminal. A avaliação algorítmica apresentava tendência para indicar uma possível reincidência por negros, com quase o dobro de chance do que a de réus brancos. Os juízes também não eram capazes de compreender exatamente como o algoritmo chegou a esse resultado (POR REDAÇÃO, 2018).

Ainda sobre o tema, Tarcízio Silva apresenta o conceito de 'microagressões', que constituem "ofensas verbais, comportamentais e ambientais comuns, sejam intencionais ou não intencionais, que comunicam desrespeito e insultos hostis, depreciativos ou negativos contra pessoas de cor" (SILVA, 2019, p. 121), com ênfase em ambientes digitais. Em suma, o autor evidencia que um dos maiores desafios sobre a lógica dos sistemas de aprendizado de máquina diz respeito à reprodução de relações de poder e opressão, que já existem previamente na sociedade. É comum que se reconheça o ambiente virtual como um espaço com pouca ou nenhuma regulação, porém é importante evidenciar que, embora os processos técnicos de funcionamento de algoritmos representem um obstáculo para uma tomada de decisão justa e legítima, as consequências jurídicas dessas decisões merecem maior destaque.

Da necessidade de uma governança de algoritmos

O sociólogo Phillip N. Howard cunhou o termo Pax Técnica, em alusão ao Império Romano, para designar um pacto de defesa mútua a ser realizado entre governo e indústria, que se encontram interligados a partir de arranjos políticos, econômicos e culturais. Nesse sentido, projetos relacionados à mineração e análise de dados, como a Inteligência Artificial, Big Data e Internet das Coisas, devem estar voltados para a consolidação do mercado corporativo, sob pena se colocar em dúvida, inclusive, os processos democráticos (HOWARD apud SILVEIRA, 2017). Com a expansão das tecnologias digitais, é possível compreender que a atual forma de organização da sociedade se dá a partir de um governo de dados. O conjunto de arranjos sociotécnicos no qual estamos imersos são frequentemente responsáveis por moldar nossos comportamentos sociais. Isto ocorre tanto pela presença tecnológica em pequenas atividades do nosso cotidiano, como pela nova ordem político-econômica que vem sendo estabelecida (SILVEIRA, 2017).

As experiências sociais mediadas por processos de tecnologia algorítmica merecem destaque, sobretudo, diante do crescente formato decisório que tem sido desenvolvido. Diante disto, é de suma importância compreender essa nova forma de racionalidade, tornando-se primordial a existência de uma governança específica devido a seu profundo impacto na tutela de direitos individuais e coletivos (SILVEIRA, 2017).

A governança de algoritmos, de maneira ampla, pode ser compreendida a partir de dois ângulos: um normativo e regulatório e outro essencialmente técnico. As discussões podem ser voltadas ao mercado, como a proposta de regulação de empresas privadas, tendo como ponto fundamental o interesse público, ou para a regulação estatal, que teria como foco a análise do nível de transparência de ferramentas utilizadas pelo Estado, por exemplo. Ou seja, o governo de algoritmos envolve um conjunto de atores sociais, tais como governos, organizações não governamentais, empresas e sociedade civil, com o objetivo de discutir caminhos para construção de um espaço digital justo e democrático (SILVEIRA, 2011, 2017).

Observando as implicações jurídicas e sociais que envolvem a internet, foi criado, em

2006, o Internet Governance Forum (IGF), cujo objetivo é fomentar o debate com a participação de diversos governos e entidades da sociedade civil, para enfrentar questões relacionadas à governança da internet. Constata-se, portanto, o crescente interesse da comunidade acadêmica, sociedade e governos sobre questões que entrelaçam justiça, sociedade e internet.

Considerações Finais

A tecnologia pode ser considerada a responsável pelas maiores transformações sociais que a humanidade pôde presenciar. A importância tecnológica atravessou diversas fronteiras, desde o seu surgimento de forma mais rudimentar, nas primeiras revoluções industriais, até o presente momento, com a chegada da sociedade conduzida pela informação. As sofisticadas técnicas de aprendizado e armazenamento de informações, como a Inteligência Artificial e o Big Data, são marcas importantes do atual contexto ultraconectado. Essas tecnologias provocaram um profundo impacto social, com indispensáveis repercussões no plano jurídico.

A internet trouxe novas realidades para o convívio humano, influindo diretamente no comportamento social. É responsável pela reconfiguração de uma infraestrutura informacional e entrega de novas formas de interação social, modelos de trabalho, economia e política. A velocidade das mudanças tornou a regulação dos setores por ela impactados um grande desafio, uma vez que a regulamentação estaria sempre desatualizada em relação às inovações tecnológicas.

Somadas a isso, novas perspectivas econômicas foram lançadas, e o advento do capitalismo digital configurou-se como um sistema ultraliberal e neototalitário. Esse sistema cresceu desregulamentado na esteira dos princípios do 'Consenso de Washington', que, na década de 1990, incentivou a adoção de políticas públicas sem qualquer interferência estatal. Foi nesse contexto que as empresas do setor tecnológico cresceram e se desenvolveram. O setor informacional e tecnológico assumiu um lugar de grande destaque no mercado global. Em razão da natureza ubíqua do Big Data, o controle estatal procedido por um governo de um único país não é capaz de estabelecer mecanismos eficazes de fiscalização sobre o respeito ao direito à privacidade e ao controle dos dados coletados a partir das informações postadas pelos usuários de internet. Assim, o novo cenário exige um controle organizacional supranacional, sendo a via dos tratados a ferramenta adequada para dispor sobre o tema.

A proteção aos dados pessoais e à privacidade, valores constitucionalmente assegurados pelo Brasil e também em tratados internacionais, significa um dos grandes desafios a serem enfrentados no contexto da governança algorítmica. A inteligência artificial e o aprendizado de máquina põem à prova valores éticos e jurídicos que precisam ser tutelados, tendo em vista a possibilidade de discriminação cibernética nos seus processos de desenvolvimento e na sua aplicação em decisões jurídicas.

O uso de algoritmos por meio das novas tecnologias tem tornado estreito o elo entre tecnologia e a segurança de dados pessoais. Seu uso assume posição central, devido ao alcance de decisões de grande impacto social. Desse modo, a regulação dos algoritmos, com uma governança algorítmica regida tanto por tratados internacionais quanto pela legislação interna dos países, apresenta-se como uma alternativa para se colimar o equilíbrio socioeconômico, tendo como finalidade estruturante e essencial o respeito à privacidade e a proteção de dados pessoais.

Nesse sentido, torna-se imprescindível um movimento cooperativo e transdisciplinar de diversos atores sociais e instituições, de forma a utilizar as ferramentas tecnológicas em favor da coletividade, e não contra a ela. A concretização de um ambiente virtual mais democrático exige um esforço para que o protagonismo digital não adquira um caráter nocivo e ilegal. Nessa perspectiva, a não discriminação deve constituir um dos pontos fundamentais da discussão sobre direto, privacidade e tecnologia, uma vez que, se não observada, acarretará a continuidade de graves lesões a direitos fundamentais, com discriminações procedidas a partir da manipulação de dados sensíveis, como raça, sexo, gênero etc.

Referências

BRANCO, Sérgio. Como uma top model ajudou a regular a internet no Brasil. Tradução de Marianna Jardim. In: **Instituto de Tecnologia e Sociedade do Rio**. [S. l.], 19 de out. de 2016. Disponível em: https://feed.itsrio.org/como-uma-top-modelajudou-a-regular-a-internet-no-brasil--4831861d4437. Acesso em: 12 de abr. de 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 de abr. de 2020.

BRASIL. **Lei n. 12.141 de 9 de junho de 2011**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 23 de abr. de 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 de abr. de 2020.

BRASIL. **Lei n. 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 de maio de 2020.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 abr. 2020.

DIGILABOUR. **Tecnopolítica, racionalidade algorítmica e mundo como laboratório: entrevista com Fernanda Bruno**. In: Digilabour. [S.l.], 23 de out. de 2019. Disponível em: https://digilabour.com.br/2019/10/25/tecnopolitica-racionalidade-algoritmica-e-mundo-como-laboratorio-entrevista-com-fernanda-bruno/. Acesso em: 09 de maio de 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. 124 p.

Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 448.

DONEDA, Danilo; ALMEIDA, Virgílio A.F. O que é a governança de algoritmos?*. In: **POLITCS:** Uma publicação do IntitutoNupef. [S. l], 2016. Disponível em: https://politics.org.br/edicoes/o--que-%C3%A9-governan%C3%A7a-de-algoritmos. Acesso em: 26 de abr. de 2020.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: Revista dos Tribunais, 1980. p. 229.

ELLUL, Jacques. **A técnica e o desafio do século**. Rio de Janeiro: Paz e Terra, 1968, p. 104.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**. [S.l.], v. 88, pp. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 26 de abr. de 2020.

HIRATA, Alessandro. **Direito à privacidade**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina ZancanerZockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 30 de abr. de 2020.

LASALLE, José María. **Ciberleviatán: El colapso de la democracia liberal frente a la revolución digital.** Barcelona: Arpa, 2019, p. 17.

LEE, KAI-FU. **Inteligência artificial. Como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos**. Tradução: Marcelo Barbão. 1. Ed. Editora Globo, 2019.

MATOSO, Filipe. **Dilma diz que privacidade na internet deve ter tratamento prioritário na ONU**. In: **G1**. [S. l.], 02 de nov. de 2013. Disponível em: http://g1.globo.com/politica/noticia/2013/11/dilma-diz-que-privacidade-na-internet-deve-ter-tratamento-prioritario-na-onu.html. Acesso em: 26 de abr. de 2020.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 29 dez. 2018.

NETO, Gabriel de Oliveira Cavalcanti. Cybersecurity e Suas Inovações à Luz da Lei Geral de Proteção de Dados. **Simplíssimo**, 2021.

O'NEIL, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. **Denver: Crown**, 2016. p. 272.

ONU, Nações Unidas Brasil. **A declaração universal dos direitos humanos**. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 26 de abr. de 2020.

PASCUAL, Manuel. Quem vigia os algoritmos para que não sejam racistas ou sexistas? In: **EL PAIS**. [S.l.], 17 de marc. de 2019. Disponível em: https://brasil.elpais.com/brasil/2019/03/18/tecnologia/1552863873_720561.html. Acesso em: 03 de maio de 2020**.**

POR REDAÇÃO. Algoritmos contribuem para julgamento de criminosos. In: **itforum**. [S.l.], 22 de nov. de 2018. Disponível em: https://itforum.com.br/noticias/algoritmos-contribuem-para-julgamento-de-criminosos/. Acesso em: 23 de abr. de 2020.

QUEIROZ, Daniela. Os algoritmos replicam as desigualdades de gênero e raça. In: **openDemocracy**. [S.l.], 07 de out. de 2019. Disponível em: https://www.opendemocracy.net/pt/algoritmos-reproduzem-desigualdades-de-genero-e-raca/. Acesso em: 17 de abr. de 2020.

REDAÇÃO ÉPOCA; AGÊNCIA EFE. Brasil e Alemanha levam à ONU projeto contra espionagem. In: Época. [S. l.], 1 de nov. de 2013. Disponível em: https://epoca.globo.com/tempo/noticia/2013/11/brasil-e-alemanha-levam-onu-bprojeto-sobre-privacidadeb.html. Acesso em: 26 de abr. 2020.

REDAÇÃO GALILEU. Arábia saudita torna-se primeiro país a conceder cidadania para um robô. In: **Revista Galileu**. [S. l.], 30 de out de 2017. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2017/10/arabia-saudita-torna-se-primeiro-pais-conceder-cidadania-para-um-robo.html#:~:text=No%20palco%20do%20FII%2C%20ao,uma%20cidadania%20%C3%A9%20algo%20hist%C3%B3rico%22. Acesso em: 20 de març. de 2020.

REDAÇÃO HYPENESS. Inteligência artificial do sistema de recrutamento da Amazon discrimina mulheres. In: **Hypeness**. [S.l.], out. de 2018. Disponível em: https://www.hypeness.com.br/2018/10/inteligencia-artificial-do-sistema-de-recrutamento-da-amazon-discrimina-mulheres/#:~:text=A%20intelig%C3%AAncia%20artificial%20adotada%20pela,apenas%20

candidatos%20do%20sexo%20masculino. Acesso em: 06 de maio de 2020.

SADIN, Eric. **La humanidad aumentada. La administración digital del mundo.** Tradução: Javier Blanco y Cecilia Paccazochi. Buenos Aires: Caja Negra, 2017.

SANTIAGO, Vanessa Cristina TAMBA, Debora Harumi. Proteção de dados no Brasil: novo marco regulatório. In: **Migalhas**, 13 de novembro de 2018. Disponível em: https://www.migalhas.com.br/depeso/290866/protecao-de-dados-no-brasil-novo-marco-regulatorio. Acesso em: 27 de fevereiro de 2020.

SILVA, Tarcizio. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. **Comunidades, Algoritmos e Ativismos Digitais**, 2019.Disponível em: https://tarciziosilva.com.br/blog/racismo-algoritmico-em-plataformas-digitais-microagressoes-e-discriminacao-em-codigo/. Acesso em: 28 de abr. de 2020.

SILVEIRA, Sergio Amadeu da. et al. **Abordagens em ciência, tecnologia e sociedade**. São Paulo: UFABC, 2015. p. 292.

SILVEIRA, Sérgio Amadeu da. **Governo dos Algoritmos**. São Luiz: Revista de Políticas Públicas, v. 21, n. 1, p. 268-281, jan./jun. 2017. Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/rppublica/article/view/6123/0. Acesso em: 30 de abr. de 2020.

SILVEIRA, Sergio Amadeu. Prefácio. In: LEIGH, Davi; HARDING, Luke. WikiLeaks: **A guerra de Julian Assange contra os segredos de Estado**. Tradução de Ana Resende e Marco Leal. ed. 1. São Paulo: Verus, 2011. p. 336.

SPENGLER, Oswald; WERNER, Helmut. **A decadência do ocidente: esboço de uma morfologia da história universal**. Grupo Gen-Editora Método Ltda., 2000.

SUPREMO TRIBUNAL FEDERAL. Inteligência artificial vai agilizar a tramitação de processos no STF. In: **Jusbrasil**. [S. l], 30 de maio de 2018. Disponível em: https://stf.jusbrasil.com.br/noticias/584499448/inteligencia-artificial-vai-agilizar-a-tramitacao-de-processos-no-stf. Acesso em: 20 de març. de 2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira do poder**. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2021, p. 22.

Recebido em 31 de maio de 2021
Aceito em 16 de julho de 2021