Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica

Paula Cotrim de Abrantes

https://doi.org/10.1590/SciELOPreprints.7141

Submetido em: 2023-10-07
Postado em: 2023-11-16 (versão 1)
(AAAA-MM-DD)

Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica

Challenges and dilemmas of personal data protection in the era of algorithmic culture

Paula Cotrim de Abrantes
Doutoranda em Ciência da Informação
UFRJ/IBICT
ORCID: https://orcid.org/0000-0003-0271-2186

RESUMO: A cultura algorítmica apresenta à sociedade dilemas e desafios que devem ser enfrentados, conhecidos e compartilhados. As pessoas precisam estar cientes de como seus dados são coletados, tratados, armazenados, compartilhados e algoritmizados. Este artigo, sob o ponto de vista da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras legislações, discute questões relativas à proteção de dados pessoais à luz da algoritmização social pela inteligência artificial (IA). Concomitantemente, aborda a transparência algorítmica, soluções tecnológicas para a proteção de dados pessoais e regulamentações sobre o tema. Tecnologias de anonimização de dados também são discutidas e detalhadas. O objetivo é explorar os principais desafios e dilemas relacionados à proteção de dados pessoais no contexto da cultura algorítmica. Por meio de uma metodologia exploratória e dedutiva foi possível destacar algumas tecnologias voltadas para proteger dados pessoais, como também proporcionar maior equidade aos algoritmos de IA.

Palavras-chave: Dado pessoal; LGPD; Cultura algorítmica; Inteligência artificial; Transparência algorítmica.

ABSTRACT: Algorithmic culture presents society with dilemmas and challenges that must be confronted, understood, and shared. People need to be aware of how their data is collected, processed, stored, shared, and algorithmically transformed. This article, from the perspective of the General Personal Data Protection Law (LGPD) and other regulations, addresses issues related to personal data protection in light of social algorithmization by artificial intelligence (AI). Concurrently, it discusses algorithmic transparency, technological solutions for personal data protection, and regulations on the subject. Data anonymization technologies are also elaborated upon and detailed. The aim is to explore the primary challenges and dilemmas associated with personal data protection within the context of algorithmic culture. Through an exploratory and deductive methodology, it was possible to highlight some technologies aimed at safeguarding personal data, as well as to provide greater fairness to AI algorithms.

Keywords: Personal data; LGPD; Algorithmic culture; Artificial intelligence; Algorithmic transparency.

INTRODUÇÃO

O século XXI trouxe à humanidade um novo cenário tecnológico. As Tecnologias da Comunicação e Informação (TICs) agora fazem parte do contexto social decidindo o que as pessoas podem ver primeiro no seu feed do Google, do Instagram, do Tik Tok, dentre outras redes sociais digitais. Essa decisão de que ver primeiro é tomada por algoritmos[1] de *machine learning*[2] (ML) e outros algoritmos de inteligência artificial (IA), que baseados no conteúdo que cada usuário mais vê, o direciona anúncios, perfis e sites quando se acessa um site ou rede social digital (Prado, 2022). Vive-se numa cultura dos algoritmos, onde eles sabem o que é "melhor" para cada usuário. De acordo com Lemos (2021, posição 426-429):

> a cultura dos algoritmos "é hoje a base da cultura digital. Os algoritmos são as novas mídias, pois são formas de plasmar a realidade, sendo ao mesmo tempo uma mensagem, um canal, um emissor e um receptor. Eles não apenas processam informação e realizam tarefas, como essas tarefas nos compelem a fazer algo (Lemos, 2021, posição 426-429).

No entanto, para os algoritmos realizarem essa tarefa de indicação de conteúdo eles se baseiam em dados, e muitos deles, dados pessoais e dados pessoais sensíveis. Isso acarreta grande preocupação quanto à proteção de dados e ao seu tratamento e disponibilização. A Lei Geral de Proteção de Dados Pessoais – LGPD[3]. Foi sancionada no Brasil em 2018 e entrou em vigor em 2020. Ela trouxe uma série de regulamentações que precisam ser seguidas pelos detentores dos dados sob pena de multa e sanções.

É necessário proteger os dados pessoais para se evitar que pessoas sejam identificadas e sofram discriminação por conta deles. Nesse mesmo contexto, algoritmos que usam inteligência artificial podem negar crédito, demitir ou contratar pessoas baseados em seus dados, que muitas vezes nem foram autorizados seu uso para esses sistemas de IA. Em muitos momentos as pessoas nem sabem como esses algoritmos processam seus dados, se existem pesos para eles e que fatores eles levaram em conta. Outras vezes, os indivíduos sequer sabem o que são algoritmos! Nesse sentido, a cultura social de que os algoritmos são verdadeiros

---

[1] "É um conjunto de instruções matemáticas, uma sequência de tarefas para alcançar um resultado esperado em um tempo limitado. Os algoritmos antecedem os computadores – o termo remonta ao século IX ligado ao matemático al-Khwãrizmi, cujo livro ensinava técnicas matemáticas a serem equacionadas manualmente. 'Algorismus' era originalmente o processo de calcular numerais hindo-arábicos" (KAUFMAN, 2018, posição 367).

[2] Subcampo da inteligência artificial, 1959 foi ano da sua criação (KAUFMAN, 2022).

[3] Lei n. 13.709, de 14 de agosto de 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Alterada pela Lei nº 13.853, de 8 de julho de 2019. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1.

oráculos da razão podem então prejudicar as pessoas nos mais diversos aspectos sociais e econômicos.

Algumas abordagens tecnológicas podem minimizar esse problema, como por exemplo, técnicas de anonimização de dados, criptografia, aprendizado de máquina federado e a chamada *Fairness in AI*. A função de algumas dessas técnicas é justamente proteger os dados de cidadãos para não serem expostos a qualquer invasor num banco de dados, além disso, eles podem embaralhar mais os dados para evitar vieses.

Um outro ponto muito importante, se refere à regulação dos dados no que se refere ao seu uso na inteligência artificial (IA). No Brasil foi protocolado o Projeto de Lei (PL) n° 2338, de 2023 (Senado Federal, 2023), que dispõe sobre o uso da Inteligência Artificial. Esse PL traz diversas regulamentações sobre a IA no país, inclusive sobre o uso de dados pessoais por algoritmos de IA. Respostas governamentais regulatórias são importantes quando se pensa numa sociedade dominada pela cultura dos algoritmos e focada somente nos resultados, o aspecto humano também tem que ser considerado.

Nesse sentido, essa pesquisa visa responder a seguinte pergunta: como proteger os dados pessoais na cultura dos algoritmos? Para isso, este estudo usou de uma metodologia exploratória, e dedutiva para selecionar e analisar uma ampla bibliografia, seja em documentos, sites governamentais, relatórios e artigos científicos sobre o tema. Quanto ao objetivo geral da pesquisa, ele se direciona a investigar os principais desafios e dilemas relacionados à proteção de dados pessoais no contexto da cultura algorítmica, tendo como objetivos específicos:

1. Compreender a LGPD;
2. Analisar a era da cultura algorítmica e o uso de dados pessoais;
3. Examinar a transparência e compreensão dos algoritmos;
4. Investigar abordagens tecnológicas de proteção; e
5. Avaliar as respostas regulatórias para sistemas de IA numa perspectiva sobre o Projeto de Lei (PL) n° 2338, de 2023.

Esse trabalho se justifica na medida que se sabe que devido à cultura dos algoritmos, sonhos são comprometidos e vidas modificadas de forma negativa. É preciso fazer uma reflexão como isso pode ser evitado. As pessoas precisam proteger seus dados, saber de seus direitos, compreender como os algoritmos funcionam, como uma possível regulamentação da inteligência artificial pode trazer mais equidade aos resultados dos algoritmos. Já existem tecnologias para essa finalidade, elas precisam ser obrigatoriamente usadas para a proteção de dados do cidadão.

A partir dessa análise, buscou-se estruturar este artigo da seguinte forma: na seção um foi explicada a metodologia do artigo. Na seção dois, a LGPD foi explicada de forma geral para compreensão dos seus principais conceitos. Na seção três foi abordado sobre a era da cultura algorítmica e uso de dados pessoais. A seção quatro examina as questões relacionadas à transparência e compreensão dos algoritmos pelas pessoas. A seção cinco trouxe à tona a existência de técnicas de anonimização para a proteção de dados pessoais. A seção seis analisa aspectos regulatórios do Projeto de Lei (PL) n° 2338, de 2023 relacionados aos algoritmos e suas aplicações, e a seção sete traz os resultados e discussões sobre o estudo.

1 METODLOGIA

A metodologia deste artigo fez uso de uma abordagem exploratória, dedutiva documental e bibliográfica. Foram realizadas análises documentais em leis, regulamentos, manuais e relatórios para prover uma bibliografia ampla e atual sobre o tema da pesquisa. A partir de uma leitura exploratória, o conteúdo foi classificado e categorizado em tópicos para a leitura ficar mais dinâmica e agradável.

O texto foi contextualizado numa linguagem acessível, e dentro do possível, se buscou conceituar e definir os termos que não fazem parte do senso comum para que o entendimento do contexto do estudo seja compreendido de uma forma factível para todos que tenham interesse no tema da pesquisa.

Por conta de uma visão imparcial, abrangente, e específica quando necessária, as informações trazidas neste artigo podem ser proveitosas em várias áreas que discutem sobre os desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica.

2 COMPREENDENDO A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A LGPD é uma importante regulamentação para a proteção de dados pessoais dos cidadãos. Sejam eles dados sensíveis ou não, a Lei traz várias sanções para quem não a cumprir. Ela criou normas para o tratamento dos dados, o que se relaciona com sua coleta e compartilhamento. Essas normativas são válidas para pessoas naturais (vivas). Pessoas físicas ou jurídicas, sejam elas do direito público ou privado, precisam cumpri-las. Sua validade se estende tanto para o meio não digital como para o digital (Brasil, 2018). Logo no seu art. 2º a LGPD já disciplina alguns de se seus fundamentos:

I - o respeito à privacidade;

> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

O respeito à privacidade é fundamental, não é permitido que alguma empresa tenha acesso a dados pessoais se o dono do dado não permitir. Isso só acontece em alguns casos específicos, como por exemplo para fins de pesquisa e de interesse público. A Lei continua garantindo ao cidadão direitos constitucionais fundamentais, como a liberdade de expressão, acesso à informação, e garantia que sua imagem e honra continua invioláveis. A LGPD também não vai contra à inovação e ao desenvolvimento tecnológico, no entanto, os dispositivos inovadores precisam respeitar à Lei.

Toda essa regulamentação é relevante porque com apenas nome, RG e CPF uma pessoa se torna identificada, e com o dado sobre seu emprego, idade, doenças e formação, por exemplo, ela se torna identificável (Lima *et al.*, 2023). Portanto, pessoas físicas e jurídicas responsáveis por esses dados, têm grandes obrigações em suas mãos. Elas serão responsabilizadas se não tratarem os dados com transparência e de forma segura.

Para fornecer essa segurança aos dados, alguns papéis foram definidos pelo artigo 5º da LGPD:

> [...] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...]
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador [...] (Brasil, 2018).

É preciso adequação de quem possua dados pessoais para ativar esses papéis de controlador, encarregado e operador dos dados. Cada um deles na sua função terá que pedir o consentimento ao cidadão do uso do seu dado, anonimizar esse dado, oferecer segurança para ele num banco de dados para que não aconteça acessos indevidos, como também fornecer um relatório de impacto relacionado à proteção desses dados (Brasil, 2018).

No que tange aos dados sensíveis, a LGPD no artigo 5º, inciso II, os descreve como sendo de: “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” (Brasil, 2018).

São considerados dados sensíveis porque qualquer um dos fatores elencados pode ser usado para fazer bullying ou para discriminar uma pessoa. Ela pode sofrer preconceito por possuir uma doença ou por se determinado partido político e devido a isso não conseguir emprego, por exemplo.

A LGPD, no art. 33, define também várias regras específicas para a transferência internacional de dados pessoais, o objetivo é proteger os direitos dos titulares dos dados. Essa transferência é permitida desde que o país ou organização internacional destino forneça proteção adequada aos dados. O controlador também precisa garantir, por meio de cláusulas contratuais, normas globais, selos e certificados, que os direitos de privacidade dos dados do titular estão garantidos.

No entanto, essa transferência acontecerá em algumas circunstâncias, por exemplo: numa cooperação jurídica internacional, para proteção da vida, quando a autoridade nacional autorizar, quando de resultado de um acordo de cooperação internacional; quando a transferência de dados ocorrer por conta de políticas públicas, quando o titular do dado tiver dado permissão para sua transferência, entre outros pontos. Pessoas jurídicas públicas podem solicitar uma avaliação sobre o nível de proteção de dados de determinado país ou organismo internacional (Brasil, 2018). Esse aspecto da LGPD é relevante quando se sabe que as Big Techs[4] atuam no Brasil e coletam, tratam e compartilham dados pessoais.

Vale ressaltar que a Autoridade Nacional de Proteção de Dados (ANPD) tem como missão assegurar que a LGPD seja cumprida. Ela é vinculada à Presidência da República e "regulamentará padrões e técnicas aplicáveis às questões de segurança da informação, interoperabilidade e processos de anonimização" (ANPD, 2033). Também poderá pedir informações relativas ao tratamento dos dados pessoais para os agentes de tratamento.

Por conta de todos os fatores expostos, as regulamentações da LGPD são tão importantes para sociedade. Elas criam um ambiente de segurança para os dados pessoais, os protegendo de qualquer fator que viole a privacidade de uma pessoa sem uma causa justa e amparada legalmente.

3 CULTURA ALGORÍTMICA E O USO DE DADOS PESSOAIS

Na era da cultura dos algoritmos surge um novo paradigma social do culto aos dados, os resultados dos algoritmos calculados por *machine learning*, *deep learning*[5], redes neurais

[4] "As grandes empresas associadas a plataformas de uso intensivo de dados, quase todas situadas na América do Norte, e também cada vez mais na China" (MOROZOV, 2018, posição 1760).

[5] "Aprendizado profundo que introduz representações complexas, expressas em termos de outras representações mais simples organizadas em diversas camadas. Essa estrutura codifica uma função matemática que mapeia conjuntos de valores de entrada (inputs) para valores de saída (outputs)" (KAUFMAN, 2022, p. 11).

profundas[6] entre outras são recebidos como quase inquestionáveis por algumas pessoas. Os dados passaram do paradigma físico[7] onde a preocupação era a eficácia da transmissão da mensagem, ao paradigma social[8], onde são analisados de forma holística.

O dado pessoal é analisado, usado, tratado e compartilhado levantando-se em conta todos os seus "sujeitos". Suas amizades, seu trabalho, seus relacionamentos íntimos e preferências sexuais, sua saúde, educação, cultura, religião, partido político, enfim, absolutamente tudo é analisado, classificado, e categorizado pelos algoritmos. Afinal, cada usuário tem seu próprio ecossistema, ele não é um ser asocial (Frohmann, 1995).

Cunha e Cavalcanti (2008, p. 113) conceituam "dado" como a "menor representação da informação". Capurro (2008) afirma que a origem da palavra "informação" se origina do latim, e busca modelar algo físico para transmitir conhecimento. Quanto a transmitir informação, isso tem a ver com a comunicação de algo a alguém, e precisa ser verdadeira e sem erros para ter utilidade (Machlup, 1983). Dessa forma, pode auxiliar em tomada de decisões sejam pessoais ou organizacionais.

Essa nova era moldada pela cibernética de segunda ordem, onde o usuário faz parte do sistema, tornou-se tão confortável nessa sociedade do século XXI que praticamente tornou real a previsão de Alan Turing onde ele anteviu que "a inteligência da máquina se tornaria tão difundida, tão confortável e tão bem integrada em nossa economia baseada em informações que as pessoas nem a perceberiam" (Kurzweil, 1999, p. 59).

Os mais diversos aplicativos em smartphones coletam os mais variados dados: por onde a pessoa transitou, locais mais frequentes que ela costuma ir, quantidade de passos, controle menstrual, calórico, batimentos cardíacos etc. Como esses dados são tratados e compartilhados? O usuário, dono dos dados, não tem conhecimento, na maioria das vezes concorda com os termos de serviço dos aplicativos sem ler as letras minúsculas com dezenas de páginas que lhe é solicitado aceitar.

O problema dessa nova sociedade acontece quando os avanços computacionais usam dados pessoais para alimentar à máquina e seus prognósticos. Sistemas computacionais fazem uso de uma massiva quantidade dados, os chamados Big Data, com todos os seus 5 Vs – volume, veracidade, variedade, velocidade e valor " (Martínez-Ávila; Souza; Gonzalez, 2019, posição 1584). Todos esses dados, quando se referem às pessoas alimentando às máquinas podem conter

[6] "Redes neurais de aprendizado profundo" (*deep learning neural networks*, dlnn) pela inspiração no funcionamento do cérebro biológico. A técnica é capaz de lidar com dados de alta dimensionalidade, por exemplo, milhões de pixels num processo de reconhecimento de imagem. Além disso, seus algoritmos estabelecem correlações nos dados não perceptíveis aos desenvolvedores humanos, origem do problema da interpretabilidade ou 'caixa-preta'" (KAUFMAN, 2022, p. 11-12).
[7] Numa referência ao texto de Capurro (2003).
[8] Numa referência ao texto de Capurro (2003).

vieses como preconceito e racismo. Decisões financeiras críticas como o deferimento de um financiamento de um imóvel, de um carro, de contratar ou despedir alguém, tudo terá como resposta “desculpe, foi a inteligência artificial que decidiu”.

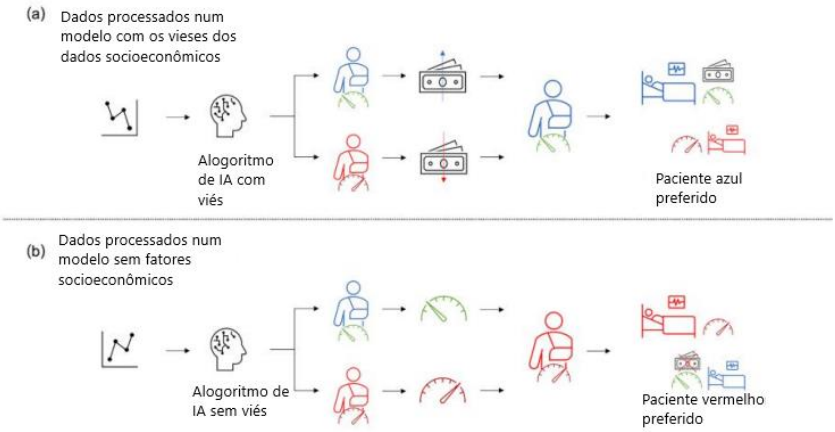
Cavalcanti (2021) explica que os algoritmos dariam uma possível objetividade e eficiência aos dados, tirando os vieses que fazem parte da subjetividade humana. No entanto, segundo a mesma autora, isso não passa de uma falácia, pois os próprios dados fornecidos ao sistema já contêm vieses. A IA irá tornar o sistema ainda mais viciado criando uma base fundamentada em algoritmos falhos.

Morozov (2018, posição 406) cita um exemplo onde o ex-diretor de tecnologia do Google diz que “todos os dados são relevantes para o crédito, ainda que não saibamos como usá-los”. O autor externa grande preocupação com essa frase, pois segundo ele, a privacidade está em grande risco e pode ser inacessível para algumas classes econômicas mais desprotegidas, qualquer clique, telefonema, movimento, poderiam interferir na avaliação de crédito e suas taxas juros. O'Neil (2020), chama atenção que em enquanto as pessoas privilegiadas economicamente, podem ter seus dados avaliados por pessoas, para a grande massa, resta a análise automatizada.

Essa questão de uso dados pessoais e privacidade não é preocupação somente no Brasil, Croll (2012), exemplifica que um cliente norte-americano da American Express teve seu limite de crédito diminuído porque no mesmo local que ele faz compras, outros clientes maus pagadores também faziam. Pessoas estão sendo qualificadas para ter crédito rebaixado somente pelo local onde fazem compras e por conta de fatores que independem de sua vontade.

Hui e colaboradores (2022) explicam como a discriminação dos dados pessoais acontece na saúde numa perspectiva norte-americana. Num sistema de IA com vieses, o paciente azul, que não está em estado grave, mas possui um nível socioeconômico mais alto é favorecido no atendimento por conta de sua capacidade de pagamento. O paciente vermelho, mais desprovido economicamente, ficaria menos tempo internado para liberar mais recursos para o paciente mais rico, mesmo o paciente vermelho precisando de mais tempo de hospitalização. Conforme Figura 1 abaixo:

Figura 1 – Vieses nos dados pessoais de saúde



Fonte: Adaptado de Hui *et al*. (2022, p. 58).

Numa perspectiva de um modelo sem vieses, ele seria imparcial, e a avaliação do paciente seria unicamente pela gravidade e urgência do atendimento. O paciente azul seria liberado mais cedo para a unidade de saúde oferecer mais recursos para o paciente vermelho, mesmo ele sendo mais pobre. Isso daria mais equidade ao sistema de saúde e aumentaria a justiça no atendimento (Hui *et al*., 2022).

No Brasil, a grande preocupação acontece no próprio tratamento dos dados de saúde das pessoas. O artigo 52 da LGPD, normatiza punições como advertência, para quem não cumprir a Lei. Aragão e Schiocchet (2020) se preocupam quanto à transparência do tratamento dos dados de saúde, dizem que não está bem claro como o Sistema Único de Saúde (SUS) fazem a proteção e gerenciamento desse tipo de dado. Entretanto o DataSus possui firewalls; software de proteção antivírus e antimalware entre outras proteções pertinentes (Brasil, 2022b).

Já numa preocupação referente ao próprio uso da internet, uma normativa anterior a LGPD, a Lei nº 12.965, de 23 de abril de 2014[9], estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, em seu art. 7º, diz o seguinte:

O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais [...] (Brasil, 2014).

[9] Marco Civil da Internet.

Percebe-se, portanto, que a Lei nº 12.965, de 23 de abril de 2014 tem grande preocupação quanto a resguardar privacidade e os dados pessoais. Questões como inviabilidade da intimidade são expressamente normatizadas, como o tratamento dos dados. Além disso, a Emenda Constitucional nº 115, de 10 de fevereiro de 2022[10], alterou a Constituição Federal e inseriu a proteção de dados pessoais dentre os direitos e garantias fundamentais.

Sendo assim, compreende-se que o governo brasileiro traz as normativas para a proteção dos dados pessoais, mas a lei precisa ser cumprida. Os dados pessoais precisam estar protegidos e somente usados, esse ou aquele dado, se o usuário permitir. Existe um conjunto de dilemas éticos e morais no uso de dados pessoais. No entanto, a ética e o cumprimento da Lei jamais podem ser afastar dessa questão, independentemente do nível de automação e desenvolvimento tecnológico que a humanidade chegue.

4 TRANSPARÊNCIA E COMPREENSÃO DOS ALGORITMOS

Vive-se na era do século XXI numa verdadeira vigilância algorítmica[11], onde os algoritmos sabem por onde as pessoas circulam, como está sua saúde, relacionamentos, trabalho, até o tipo de filme e comida que mais gostam. Para Xavier e Dantas (2023), os procedimentos de vigilância algorítmica se iniciam na navegação na Web, onde os dados são coletados. Para as autoras, quanto mais dados são capturados, mais eficiente é o processo. Dessa forma, os algoritmos conseguem gerar um padrão comportamental dos indivíduos fazendo uma correlação entre os dados. Nesse sentido, é importante que as pessoas compreendam como esses algoritmos funcionam.

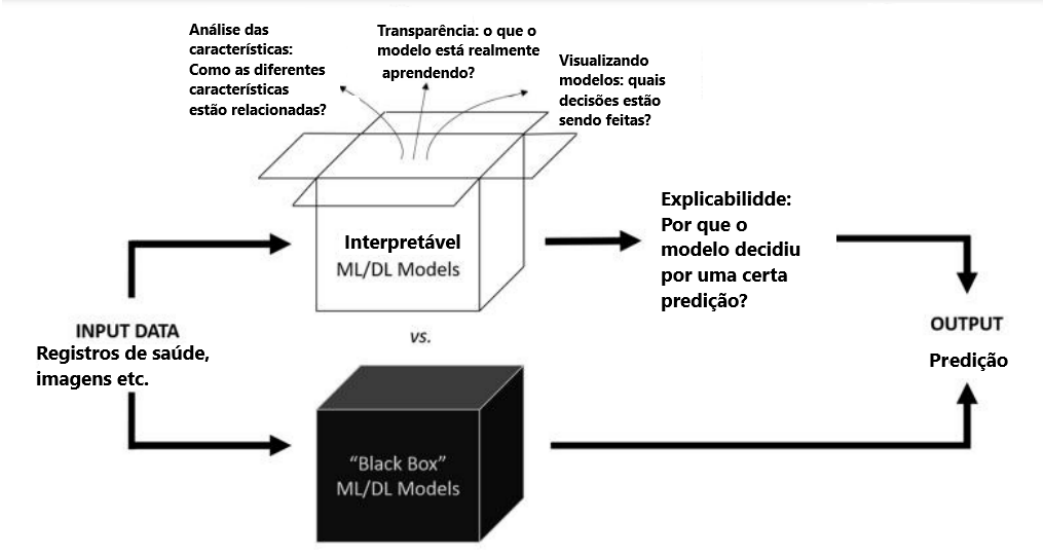
Num primeiro momento é importante reconhecer que tomar decisões sem vieses faz parte da ética. Algoritmos enviesados podem perpetuar as mais diversas desigualdades e preconceitos. Diferenciando o tratamento entre ricos e pobres, pretos e brancos, por conta de sua renda e/ou raça. Para que isso não aconteça é preciso que haja transparência nos algoritmos, ou seja, quais dados eles estão baseados para tomar suas decisões e por quê. Isso traz uma questão relevante, já que em muitos momentos, nem quem inseriu os dados sabem como funcionam os resultados fornecidos pelos algoritmos.

[10] Brasil (2022a).
[11] "Vigilância de dados é a criação e/ou uso sistemático de dados pessoais para a investigação ou monitoramento das ações ou comunicações de uma ou mais pessoas" (CLARKE; GREENLEAF, 2017, p. 3).

Por conta do problema da "caixa preta[12]" (*black box*) dos algoritmos, que realizam milhares de cálculos em funções complexas, se torna difícil entender sua indicação para uma coisa em detrimento da outra. No entanto, Kaufman (2022, p. 41), ressalta que existe o que se denomina "interpretabilidade do sistema de ia", que é entendido como "a tentativa de entender e determinar qual grau de confiança atribuir ao resultado obtido" (Kaufman,2022, p. 41). A autora menciona que existem métodos mais avançados de estudo para essa finalidade. A própria rede como um todo seria observada no que se refere às suas unidades, e não seus resultados (*output*). Isso permitiria a visualização das unidades que fossem mais ativadas e poderia se realizar testes nessas mesmas unidades num modelo de IA.

Hui e colaboradores (2022), esclarecem que é importante perceber a diferença entre a interoperabilidade do sistema e sua explicabilidade. São conceitos diferentes, mas usados como sinônimos às vezes. De acordo com os autores, a interoperabilidade torna possível ver o que acontece dentro da caixa preta, inclui-se os dados, e analisa-se a causa e o efeito. A explicabilidade analisará como o modelo de IA se comporta e a sua racionalidade, além tirar *insights* disso, será compreender seu resultado. No entanto, os dois atuam juntos para tornar todo o processo transparente conforme observado na Figura 2.

Figura 2 – Modelos de IA com transparência



Fonte: Adaptado de Hui *et al*. (2022, p. 61).

Kaufman (2022) destaca assim, que existem esforços no sentido de aumentar a transparência dos modelos de redes neurais em IA. Dessa forma, mesmo sistemas complexos

[12] "Decisões estão sendo tomadas por algoritmos de inteligência artificial, suscitando certo desconforto pelo "problema da interpretabilidade", como os cientistas denominam a caixa-preta desses modelos (desconhecimento de como são gerados os resultados)" (Kaufman, 2022, p. 205).

seriam mais compreensíveis. Uma das rotas possíveis é fornecer exemplos ao sistema e entender como eles fazem a categorização. O objetivo é fazer com que o usuário entenda e sistema e o grau de sua confiabilidade.

Entretanto, conforme O'Neil (2020), nem todos fazem parte desse esforço de tornar os algoritmos transparentes. Algumas empresas simplesmente transformam todo o sistema de IA em segredo coorporativo e não querem estudar sua caixa preta. Nesse sentido, essa dificuldade técnica de compreensão dos dados, fornece uma abertura para manipulação dos dados, discriminação, violações de privacidade, sem falar sobre abuso de poder e censura (Cavalcanti, 2021).

O problema da caixa preta dos algoritmos e sua falta de *accountability* segue sem resolução completamente definida. O'Neil (2020), cujo livro se intitula "Algoritmos de Destruição em Massa", discorre, além de outros temas, sobre a grande falta de transparência dos algoritmos e os danos que isso acarreta para as pessoas.

Cavalcanti (2021) explica que um dos primeiros problemas relacionados à transparência dos sistemas em IA se referem a própria compreensão, pelo usuário, do código matemático que compõem o modelo. Sem falar nas questões relacionadas à propriedade intelectual. A Portaria 411/2020 (INPI, 2020), estabelece que as patentes de invenção implementadas por programa de computador têm condições de receber uma carta-patente de invenção. Por conta disso, técnicas de inteligência artificial que façam uso de algoritmos de IA são entendidas como invenção, caso haja aplicabilidade para resolução de problemas técnicos.

Além disso, pessoas físicas e jurídicas também têm a opção do segredo industrial no que se refere à sistemas de inteligência artificial. O segredo industrial se refere à ativos intangíveis, sua função é garantir o direito de exclusividade. O segredo industrial está citado na Lei de Propriedade Industrial, nº 9.279/96[13]; no que se refere à Programas de Computador, é citado na Lei nº 9.609/98[14], e citado pela Lei nº 10.603, de 17 de dezembro de 2002[15]. Nesse sentido, o possuidor do segredo industrial pode fazer acordos e contratos conforme a Lei assim o permite, inclusive com cláusulas de confidencialidade (Barbosa, 2010). Isso pode fazer com que na prática, sistemas de IA continuem com sua falta de transparência.

Nas patentes de invenção, ao menos existe uma publicação do pedido patente. Nele contém um desenho do modelo que se quer patentear e as reivindicações relacionadas a essa invenção (INPI, 2013). Mesmo que para um leigo seja difícil entender como o sistema irá funcionar, já é algo que se possa ler e pesquisar uma resposta.

[13] Brasil (1996).
[14] Brasil (1998).
[15] Brasil (2002).

Numa tentativa de oferecer mais transparência à coleta de dados, a LGPD em seu art. 20 (Brasil, 2019), disciplina que o titular dos dados tem direito de pedir reavaliação de deliberações realizadas, que usem de forma única, um processamento automatizado de dados pessoais que de alguma forma irão incidir seus interesses. Inclui-se arbitramentos sobre o "perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". No entanto, como visto, ainda existe um longo caminho a se trilhar para tornar os algoritmos mais transparentes e entendíveis.

5 ABORDAGENS TECNOLÓGICAS PARA PROTEÇÃO DE DADOS PESSOAIS

Soluções tecnológicas, podem contribuir efetivamente para anonimizar dados pessoais e evitar que os algoritmos sejam enviesados por conta de fatores econômicos, raça, ou qualquer outro tipo de preconceito. Técnicas de anonimização/pseudonimização, criptografia e aprendizado de máquina federado, são formas de proteger os dados pessoais. Além disso, existem técnicas que possibilitam que a IA consiga prover equidade, transparência em seus algoritmos, conhecido como *Fairness, Accountability, and Transparency in Machine Learning* (FAT/ML) ou somente "*Fairness* in AI". Existe uma organização[16] com eventos anuais para fomentar essa questão.

A LGPD, em seu art. 5º, inciso 11, define anonimização como "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Brasil, 2018). Sendo assim por meio desta técnica um dado pessoal não pode ser mais associado a uma pessoa, impedindo, ou ao menos diminuindo qualquer tipo de viés no tratamento desse dado por um algoritmo.

No que se refere à pseudonimização, a LGPD, em seu art. 13, parágrafo 4º, conceitua da seguinte forma: "é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Brasil, 2018).

Alguns métodos podem anonimizar indivíduos ou ao menos permitem que eles não sejam rapidamente identificados, como por exemplo, o **k-anonimato; l-diversidade** e o **t-proximidade**. Esses métodos, explicados na seção "resultados", trabalham com variáveis que possuem a capacidade de anonimizar dados para impedir que as pessoas sejam identificadas por suas características (Silva, 2015).

No que tange à criptografia, Agner (2017, p. 5-6) a descreve como:

[16] https://www.fatml.org/

> um ramo da matemática que, em sua definição moderna, acolhe toda a tecnologia criada e utilizada para restringir verdades fundamentais da natureza da informação com o intuito de alcançar objetivos como: esconder mensagens, provar a existência de um segredo sem a necessidade de revelar o segredo, provar autenticidade e integridade de dados, provar trabalho computacional etc (Agner, 2017, p. 5-6)

Terada (2008) explica que os algoritmos e protocolos de criptografia possuem alguns eixos fundamentais. A encriptação simétrica tem utilidade para esconder o conteúdo dos dados. A encriptação assimétrica atua em blocos menores de dados, é muito usada em assinaturas digitais. Já os algoritmos de integridade de dados agem em proteger os blocos de dados de potenciais alterações. Por fim, de acordo com o autor, existem os protocolos de autenticação que, juntamente com os algoritmos criptográficos, fazem a análise e conferência da identidade de diversas entidades.

Quanto ao Aprendizado de Máquina Federado, que pode usar técnicas de criptografia, "é uma técnica de *machine learning* (ML) que permite que um grupo de organizações ou grupos dentro da mesma organização treinem e aprimorem de forma colaborativa e interativa um modelo de ML global compartilhado" (Google Cloud, 2022). Nessa forma de tratamento dos dados, somente é compartilhado dados entre as organizações que fazem parte de uma federação pré-formada e que possui várias regras de proteção dos dados pessoais. De acordo com o mesmo autor[17], essas organizações podem ser de diferentes áreas geográficas ou mesmo de setores diferentes numa mesma instituição.

No Aprendizado Federado (*Federated Learning*- FL), os modelos de *machine learning* são treinados com dados homogêneos e distribuídos de forma idêntica. Da mesma forma acontece com dados não independentes e potencialmente não distribuídos de maneira idêntica (Google Cloud, 2022). Nesse tipo de aprendizado são compartilhados pelas organizações somente "os parâmetros dos modelos de ML, que podem ser criptografados para aumentar a privacidade" (Google Cloud, 2022).

No que se refere ao *Fairness* in AI, ela abrange técnicas de pré-processamento, processamento em andamento e pós-processamento de dados. O objetivo é mudar um conjunto de dados que são usados num modelo preditivo de *machine learning* para que nos resultados haja mais imparcialidade. Os algoritmos usados são ajustados para melhor chegar a esse resultado (Hass, 2019). Na seção sete do artigo essa questão será mais detalhada.

[17] Ibidem.

6 RESPOSTAS REGULATÓRIAS PARA A PROTEÇÃO DE DADOS PESSOAIS EM SISTEMAS DE IA – PERSPECTIVAS DO PROJETO DE LEI (PL) N° 2338, DE 2023

A Inteligência Artificial, oficialmente criada em 1956[18], passou por momentos de grandes progressos e investimentos, como também invernos[19] e recuos de injeção de capital (Taulli, 2020). No século XXI, com o aumento da capacidade do processamento computacional, a IA conseguiu o ambiente que precisava para voltar novamente aos grandes investimentos tecnológicos (Bostrom, 2018).

A IA, dessa forma, está incorporada e conectada a sistemas computacionais que oferecem produtos e prestam serviços a partir de suas predições. No entanto, como anteriormente observado, dados tratados por modelos de IA podem conter vieses em seus resultados e terem a possibilidade de vir a prejudicar a vida das pessoas. Existem formas de prover transparência a esses resultados, mas a prática disso no dia a dia ainda está longe do esperado. Técnicas de anonimização precisam ser usadas de forma mais comum para garantir mais segurança para as pessoas no que se refere ao uso dos seus dados.

Uma das principais formas regulatórias relativas à proteção e dados de pessoais quando se pensa numa cultura dos algoritmos é a própria LGPD, como foi observado, ela busca resguardar os dados pessoais dos indivíduos e também é válida para essa nova era algoritmização. Recentemente, o Projeto de Lei n° 2338, de 2023 (Senado Federal, 2023)[20], que dispõe sobre o uso da Inteligência Artificial, também se tornou um agente importante nessa questão da salvaguarda dos dados pessoais. O PL se preocupa com os riscos e benefícios que a IA oferece. Além disso, ele protege os direitos constitucionais do cidadão, mas sem prejudicar o desenvolvimento econômico do país e os incentivos à inovação (Brasil, 2023). No seu art. 5º ele disciplina o seguinte:

> Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo: I – direito à informação prévia quanto às suas interações com sistemas de inteligência artificial; II – direito à explicação sobre a decisão, recomendação ou previsão tomada por sistemas de inteligência artificial; III – direito de contestar decisões ou previsões de sistemas de inteligência artificial que produzam efeitos jurídicos ou que impactem de maneira significativa os interesses do afetado; IV – direito à determinação e à participação humana em decisões de sistemas de inteligência artificial, levando-se em conta o

[18] Por John McCarthy e Marvin Minsky num curso de verão no Dartmouth College (EUA) (RUSSEL, 2021).

[19] O primeiro inverno da IA ocorreu na década de 1970 (TAULLI, 2020). Entre 1980 e 1990 houve grandes investimentos em IA, mas não bons resultados, causando o segundo inverno da IA (KAUFMAN, 2018). As máquinas não eram capazes de processar o grande volume de dados e os investimentos diminuíram (BOSTROM, 2018).

.

[20] Brasil (2023).

> contexto e o estado da arte do desenvolvimento tecnológico; V – direito à não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; e VI – direito à privacidade e à proteção de dados pessoais, nos termos da legislação pertinente (Brasil, 2023).

Como visto, o PL normatiza questões importantes no que se refere à proteção de dados pessoais, cita explicitamente sistemas de IA. Esses modelos precisam garantir que os direitos do cidadão, quanto aos seus dados, sejam cumpridos. Não é permitido discriminar os indivíduos, e se isso acontecer, os vieses precisam ser corrigidos. Ademais, as pessoas podem contestar decisões dos modelos de IA se seus interesses forem afetados.

O art. 7º do Projeto de Lei n° 2338 de 2023, prediz que antes mesmo de usar os modelos de IA as pessoas podem obter informações sobre esses sistemas no que tange: à sua automação, aos dados que foram usados no modelo, qual o papel específico da IA e do agente humano e quais são as medidas de segurança, acurácia e precisão do sistema. O art. 11. do referido PL[21] é importantíssimo, visto que disciplina que decisões por IA que tenham de alguma forma um impacto que não possa ser revertido ou quase impossibilidade de se reverter. Também disciplina situações que gerem decisões que ponham a vida da pessoa em risco. Em ocasiões assim, deve haver um agente humano em grande parte da decisão final.

Na era da vigilância algorítmica, o art. 15 do Projeto de Lei n° 2338 de 2023, normatiza que os sistemas de identificação biométrica em espaços públicos somente são permitidos quando houver previsão de lei federal ou uma autoridade judicial permitir para apuração e repressão penal individual. No entanto, somente nos seguintes casos: “I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos; II – busca de vítimas de crimes ou pessoas desaparecidas; ou III – crime em flagrante” (Brasil, 2023).

O art. 26 do PL n° 2338 de 2023, os segredos industrial e comercial e as conclusões da avaliação de impacto da IA serão públicas. Nessa publicização devem estar incluídas uma descrição da finalidade e contexto do sistema. Medidas de redução de riscos também estão previstas na do Projeto. Já o art. 36 regulamenta que os agentes de IA podem receber sanções por conta de infrações realizadas.

A ANPD (2023) lembra que uma estrutura de regulação recebe críticas por porventura barrar a inovação, no entanto, as normas são elaboradas para que os fomentos à inovação continuem, mas com responsabilidade e proteção aos dados pessoais. O diálogo e interoperabilidade com as instituições inovadoras e os agentes reguladores precisam acontecer.

ANPD (2023) ressalta vários aspectos da LGPD que são preocupações em comum com o PL n° 2338 de 2023, seja na coleta, no tratamento, no compartilhamento dados pessoais ou

---

[2121] Ibidem.

também disciplinando sanções, caso não haja o cumprimento das normativas. A ANPD (2023), por conta disso, cita que as Autoridades internacionais que têm a função de proteger dados pessoais, e têm atuado na normatização da IA, são citados exemplos da Itália, Espanha e Holanda. Esses países atuam contra a discriminação algorítmica e regulam, por exemplo, setores da saúde e telecomunicações.

7 RESULTADOS E DISCUSSÕES

A partir da metodologia descrita na seção anterior, foi possível identificar formas de anonimização e pseudoanonimização dos dados pessoais. As técnicas descritas a seguir buscam proteger esse tipo de dado como forma de garantir a privacidade das pessoas. O objetivo de algumas dessas técnicas é evitar vieses nos resultados gerados por algoritmos de IA, pois o modelo não terá acesso a dados que embutem preconceito e racismo.

Entretanto, é importante ressaltar que mesmo com probabilidade diminuída de conter vieses, os procedimentos técnicos não são infalíveis, e mesmo com todo cuidado, ainda existe a possibilidade de identificação do dado pessoal. Além disso, as técnicas expostas não possuem a intenção de abranger todo o espectro de técnicas de proteção de dados pessoais relativos à IA, esse estudo trouxe apenas alguns para conhecimento do leitor.

O k-anonimato; l-diversidade e o t-proximidade, são técnicas usadas que protegem dados pessoais. No entanto, num modelo de *machine learning*, talvez elas acentuem o viés justamente por homogeneizar dados de determinada doença ou característica financeira, por exemplo, pois quem estivesse nesses grupos, poderia ser discriminado pelos algoritmos de IA. De qualquer forma é válido conhecer como elas funcionam, pois se uma organização informar que apenas usam essas técnicas no modelo de IA, os dados ainda podem conter vieses.

No k-anonimato: O dado pessoal não é identificado se a vaiável k for: $k > l$ (Affonso; Sant'Ana, 2017). Por outro lado, no l-diversidade: Cada conjunto de dados com variáveis-chave compartilhadas terá no mínimo l valores distintos para variáveis sensíveis (Ribeiro-Alves; Franco, 2022). Quanto ao t-proximidade, os dados são distribuídos de tal forma que possibilita assegurar a distribuição dos dados de forma que simetrias ou assimetrias não sejam percebidas (Silva, 2015).

No que tange ao Aprendizado Federado, ele pode usar técnicas da criptografia como a criptografia homomórfica[22]. Ela consegue mitigar riscos de exposição de dados e manter sua

[22] "A Criptografia Homomórfica é uma técnica de criptografia para o processamento de dados criptografados sem a necessidade de decifrá-los. Tal método é indicado para uso em ambientes não confiáveis, como por exemplo as plataformas de computação em nuvem" (GAVINHO FILHO; SILVA; MICELLI, 2015).

privacidade (Silva, Campos, Lucena, 2023). O Aprendizado Federado é uma abordagem de ML colaborativa, diversas máquinas fazem uso do mesmo algoritmo diversas vezes (Yang *et al.,* 2019). Os dados são treinados em equipamentos locais para posteriormente, os resultados serem enviados a uma central. Além disso, somente os resultados que passaram pelo retreinamento são compartilhados. Dessa forma é possível favorecer a privacidade dos dados (Yang *et al.,* 2019).

Para buscar uma maneira de certificar que os dados dos usuários tenham sua privacidade garantida, vários conjuntos de computadores são modelados em conjunto. Assim, espera-se atingir a meta de aperfeiçoar a precisão do modelo (Wang, *et al.,* 2021). Resumidamente o Quadro 1 mostra algumas características do modelo.

Quadro 1 - Aprendizado Federado

Benefícios	Privacidade dos dados num modelo de ML; Possibilita treinamento em diversos equipamentos; Escalabilidade.
Riscos	Atualizações não autorizadas do modelo – comprometimento dos resultados; Vazamentos não propositais; Ataques externos; Comprometimento da acurácia (Vieira; Campos, 2023). Custos altos que inviabilizem o uso do modelo (Khan; Glavin; Nickles, 2023).

Fonte: Elaborado a partir de Google Cloud (2022)

O Aprendizado Federado atua para prover privacidade dos dados na forma de sua constituição. mesmo assim há risco dos dados serem relacionados e prejudicar sua privacidade. A criptografia homomórfica pode inserir ruído aos dados, entretanto isso pode prejudicar a precisão do modelo. A criptografia homomórfica criptografa os dados antes mesmo que os modelos de ML usem. São necessários cálculos posteriores para verificar a eficiência do modelo (Khan; Glavin; Nickles, 2023).

A partir da leitura do trabalho de Vieira e Campos (2023), é possível concluir que, quanto aos vieses no Aprendizado Federado, é importante considerar que os dados são treinados localmente e os resultados desse treinamento é compartilhado, se os dados já tiverem enviesados, é possível passá-lo para o modelo. A variabilidade dos dados é um fator importante, no entanto, se o próprio sistema estiver comprometido, afetará também seu resultado.

O *Fairness in AI* é uma outra abordagem tecnológica para fornecer mais equidade aos algoritmos de IA. Em geral, o modelo é ajustado para que isso aconteça. São realizadas técnicas que podem ser usadas no pré-processamento, processamento em andamento e pós-processamento (Haas, 2019).

Haas (2019) explica que alguns algoritmos de análise preditiva como Árvores de Decisão precisam que os dados de entrada tenham boa qualidade para ter um bom resultado. Se

o padrão do dado já entrar no modelo com viés, isso será reproduzido na sua predição. Sendo assim, técnicas de pré-processamento podem ser abordadas antes mesmo do treinamento no modelo, reduzindo os vieses nos dados. Quanto ao processamento em andamento, os dados seriam alterados durante o processamento dos dados pelos algoritmos (Calders; Verwer, 2010).

No que se refere às técnicas de pós-processamento, após as análises preditivas de um algoritmo é possível ajustar o modelo para ele ser mais justo. De acordo com Haas (2019) é factível alterar a classificação para alguns indivíduos e assim diminuir o preconceito relacionado àquela etiqueta. No entanto, é preciso ter cuidado para que as soluções encontradas não sejam tendenciosas ou imparciais ao extremo, o que seria polos opostos relacionados a *Fairness in AI* (Haas, 2019).

CONCLUSÃO

Este artigo buscou trazer ao leitor as questões relacionadas à cultura da algoritmização num amplo espectro. Primeiramente, o tema foi exposto e os problemas que advém dele: preconceito, racismo, discriminação. Vidas reais sendo afetadas por conta de algoritmos que usam IA. Muito poder tem sido dado a eles, no entanto, sua transparência nos resultados ainda apresenta muitos desafios. A discriminação continua por conta dos resultados dos algoritmos.

No Brasil, a LGPD trouxe muitas normativas que regularam e protegeram os dados pessoais no que se refere à sua coleta, tratamento, armazenamento e compartilhamento. Essa legislação é de suma importância e precisa ser cumprida à risca para que dados pessoais não sejam expostos e prejudiquem pessoas. Em 2023, o PL n° 2338 de 2023, dispõe sobre a inteligência artificial e sua regulação. Se for aprovado, as pessoas poderão reivindicar análise dos resultados, como também, em alguns casos mais sérios, solicitar que um agente humano decida a questão.

Por fim, o estudo expôs também algumas soluções tecnológicas para prover mais proteção e equidade aos dados tratados num modelo que use IA. Espera-se ter respondido à questão principal do estudo: “como proteger os dados pessoais na cultura dos algoritmos?” Da mesma forma, deseja-se que o leitor saia desse texto mais consciente de como seu dado pode ser usado por algoritmos e o que fazer para proteger seu dado pessoal para não ser vítima da discriminação em algum ponto chave da sua vida. Para trabalhos futuros, recomenda-se um estudo mais aprofundado com relação à regulação dos algoritmos de IA na esfera legislativa, e seus perspectivos e desafios.

REFERÊNCIAS

AGNER, Marco. **Bitcoin para programadores**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2017, 90 p. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/bitcoin-para-programadores.pdf. Acesso em: 13 ago. 2023.

ARAGÃO, Suéllyn Mattos; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Reciis – Rev Eletron Comun Inf Inov Saúde**. jul.-set., v. 14, n. 3. p. 692-708. 2020. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012/2391. Acesso em: 13 ago. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD (Brasil). **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial**. Brasília: ANPD, 2023, 31 p. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 11 ago. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD (Brasil). Perguntas Frequentes – ANPD. **Qual é o papel da Autoridade Nacional de Proteção de Dados – ANPD? 2023.** Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c1. Acesso em: 11 ago. 2023.

BARBOSA, Denis Borges. **Uma introdução à propriedade intelectual**. Editora Lumen Juris, 2 ed. ver. atual., 2010. 951 p. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 12 ago. 2023.

BOSTROM, Nick. **Superinteligência:** caminhos, perigos e estratégias para um novo mundo. Rio de Janeiro: DarkSide Books, 2018. 549 p. *Kindle.*

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022a.**
Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 12 ago. 2023.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm#:~:text=LEI%20N%C2%BA%209.279%2C%20DE%2014,obriga%C3%A7%C3%B5es%20relativos%20%C3%A0%20propriedade%20industrial.&text=Art.%201%C2%BA%20Esta%20Lei%20regula,obriga%C3%A7%C3%B5es%20relativos%20%C3%A0%20propriedade%20industrial.&text=V%20%2D%20repress%C3%A3o%20%C3%A0%20concorr%C3%AAncia%20desleal.. Acesso em: 12 ago. 2023.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998.** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 12 ago. 2023.

BRASIL **Lei nº 10.603, de 17 de dezembro de 2002.** Dispõe sobre a proteção de informação não divulgada submetida para aprovação da comercialização de produtos e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10603.htm#:~:text=LEI%20No%2010.603%2C%20DE%2017%20DE%20DEZEMBRO%20DE%202002.&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20de,produtos%20e%20d%C3%A1%20outras%20providências. Acesso em: 12 ago. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 ago. 2023.

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: 10 ago. 2023.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 10 ago. 2023.

BRASIL. Ministério da Saúde. Assessoria Especial de Proteção de Dados. **Programa de Governança em Privacidade**. Brasília: Ministério da Saúde, 2022b. 24 p. https://bvsms.saude.gov.br/bvs/publicacoes/programa_governanca_privacidade.pdf

CALDERS, Toon; VERWER, Sicco. Three naive bayes approaches for discrimination-free classification. **Data mining and knowledge discovery**, v. 21, pp. 277-292, 2010. Disponível em: https://link.springer.com/content/pdf/10.1007/s10618-010-0190-x.pdf. Acesso em: 15 ago. 2023.

CAPURRO, Rafael. Epistemologia e Ciência da Informação. *In*: **V Encontro Nacional de Pesquisa em Ciência da Informação - ENANCIB**. Belo Horizonte, 10 de novembro de 2003. Disponível em: http://www.capurro.de/enancib_p.htm. Acesso em: 11 ago. 2023.

CAPURRO, Rafael. Pasado, presente y futuro de la noción de información. *In:* NAFRÍA, J. M. D. e ALEMANY, F. S. (Ed.). **¿Qué es información? Actas del primer encuentro internacional de expertos en Teorías de la Información - un enfoque interdisciplinar**. León (Spain): Universidad de León. 2008. p.1-26.

CAVALCANTI, Natália Peppi. Transparência e revisão de decisões automatizadas. *In*: VAINZOF, Rony *et al*. **Inteligência Artificial:** Sociedade Economia e Estado. São Paulo: Thomson Reuters Brasil, 2021. p. 175-206.

CLARKE, Roger; GREENLEAF, Graham. Dataveillance regulation: A research framework. **JL Inf. & Sci.**, v. 25, p. 104, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3073492. Acesso em 12 ago. 2023.

CROLL, Alistair. Big data is our generation's civil rights issue, and we don't know it. **Big data now, Atlanta**, p. 55-59, 2012. Disponível em:

https://faculty.cc.gatech.edu/~beki/cs4001/big-data.pdf. Acesso em: 11 ago. 2023.

CUNHA, Murilo; CAVALCANTI, Cordélia Robalinho de Oliveira Bastos da. **Dicionário de biblioteconomia e arquivologia.** Brasília, DF: Briquet de Lemos, 2008. 472 p. Disponível em: https://repositorio.unb.br/handle/10482/34113. Acesso em: 10 ago. 2023.

FROHMANN, Bernd. Knowledge and power in information science: toward a discourse analysis of the cognitive viewpoint. *In***:** R. Capurro, K. Wiegerling, A. Brellochs (Eds.): **Informationsethik. Konstanz,** UVK, pp. 273-286, 1995. Publicado originariamente: The power of imges: a discourse analysis of the cognitive viewpoint *In:* Journal of Documentation, vol. 48, No. 4, 1992, 365-386. Acesso em: 11 ago. 2023.

GAVINHO FILHO, Joffre; SILVA, Gabriel Pereira da; MICELLI, Claudio. Compressão e Otimização de Chaves Públicas usando Algoritmo Genético em Criptografia Completamente Homomórfica. In: **Anais do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2015. p. 225-238.

GOOGLE CLOUD. **Aprendizado federado no Google Cloud**. 2022. Disponível em: https://cloud.google.com/architecture/federated-learning-google-cloud?hl=pt-br#:~:text=O%20aprendizado%20federado%20%C3%A9%20uma,modelo%20de%20ML%20global%20compartilhado. Acesso em: 13 ago. 2023.

HAAS, Christian. **The price of fairness-A framework to explore trade-offs in algorithmic fairness**. 2019. Disponível em: https://web.archive.org/web/20220802070037id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1034&context=icis2019. Acesso em: 14 ago. 2023.

HUI, Aaron T. *et al.* Ethical challenges of artificial intelligence in health care: a narrative review. **Ethics in Biology, Engineering and Medicine: An International Journal**, v. 12, n. 1, 2021. Disponível em: https://www.researchgate.net/profile/Aaron-Hui-3/publication/357757904_Ethical_Challenges_of_Artificial_Intelligence_in_Health_Care_A_Narrative_Review/links/621415714be28e145ca909c1/Ethical-Challenges-of-Artificial-Intelligence-in-Health-Care-A-Narrative-Review.pdf . Acesso em: 13 ago. 2023.

INSTITUTO NACIONAL DE PROPRIEDADE INDUSTRIAL – INPI (Brasil). **Instrução Normativa nº 30**. 2013. 12 p. Disponível em: https://www.gov.br/inpi/pt-br/assuntos/patentes/in_030_in_17_2013_exame_tecnico_versao_final_03_12_2013-1-_1_0.pdf Acesso em: 12 ago. 2023.

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI. **Portaria 411/2020 - diretrizes para o exame de pedidos de patente envolvendo invenções implementadas por computador**. 23 de dezembro de 2020a. Disponível em https://www.gov.br/inpi/pt-br/servicos/patentes/legislacao/legislacao/PortariaINPIPR4112020_DIRPAInvenesImplementadasemComputador_05012021.pdf. Acesso em: 12 ago. 2023.

FAT/ML. **Fairness, Accountability, and Transparencyin Machine Learning**. Disponível em: https://www.fatml.org/. Acesso em: 14 ago. 2023.

KHAN, Mashal; GLAVIN, Frank G.; NICKLES, Matthias. Federated learning as a privacy solution-an overview. **Procedia Computer Science**, v. 217, p. 316-325, 2023.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?** Barueri, SP: Estação das Letras e Cores, 2018. 94 p. *Kindle.*

KAUFMAN, Dora. **Desmistificando a inteligência artificial**. Belo Horizonte: Autêntica, 2022. 331 p. *Kindle.*

KURZWEIL, Ray. Spiritual machines. **Research & Development**, v. 41, n. 7, p. 14-18, 1999.

LEMOS, André. **A tecnologia é um vírus:** pandemia e cultura digital. Porto Alegre: Sulina, 2021. *Kindle*.

LIMA, Ana Paula Canto de *et al.*. **Manual do cidadão:** privacidade, proteção de dados pessoais. Recife: Editora Império, 2023. 242 p.

MACHLUP, Fritz. Semantic Quirks in Studies of Information. *In:* MACHLUP, Fritz. **The Study of Information**, org. F. Machlup e U. Mansfield. Nova York: John Wiley & Sons, 1983. pp. 641-671.

MARTÍNEZ-ÁVILA, Daniel; SOUZA, Edna. Alves de; GONZALEZ, Maria Eunice Quilici **Informação, conhecimento, ação autônoma e big data:** continuidade ou revolução. Marília: Cultura Acadêmica; Unesp, 2019. *Kindle.*

MOROZOV, Evgeny. **Big Tech:** A ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018. 192 p. *Kindle.*

O'NEIL, Cathy. **Algoritmos de Destruição em Massa.** São Paulo: Editora Rua do Sabão. 2020, 252 p.

PRADO, Magaly. **Fake news e inteligência artificial: O poder dos algoritmos na guerra da desinformação**. Digitaliza Conteudo, 2022. 424 p.

RIBEIRO-ALVES, Marcelo; FRANCO, Carolina Mendes. **MANUAL PRÁTICO DE ANONIMIZAÇÃO DE DADOS DE PESQUISA COM O R**. Fundação Oswaldo Cruz, Rio de Janeiro, 2022. 89 p. Disponível em: https://www.arca.fiocruz.br/bitstream/handle/icict/56398/Manual%20Pr%c3%a1tico%20de%20Anonimiza%c3%a7%c3%a3o%20de%20Dados%20de%20Pesquisa%20com%20o%20R.pdf?sequence=2&isAllowed=y. Acesso em: 14 ago. 2023.

RUSSELL, Stuart. **A inteligência artificial a nosso favor:** como manter o controle sobre a tecnologia. Trad, Berilo Vargas. São Paulo: Cia das Letras, 2021. *Kindle.*

SENADO FEDERAL (Brasil). **Projeto de Lei n° 2338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://legis.senado.leg.br/diarios/ver/112653?sequencia=295. Acesso em: 10 ago. 2023.

SILVA. Daniel Fernando Alves da. **Geração Sintética de Microdados utilizando algoritmos de data mining**. 2015. 125f. Dissertação(Mestrado em Economia) Universidade do Porto. 2015, 125 f. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/80015/2/36274.pdf. Acesso em: 13 ago. 2023.

SILVA, Nicolas A. Alves da; CAMPOS, Carlos A. Vieira; LUCENA, Sidney C. de. Inferência da qualidade do serviço em enlaces de rede através de um método baseado em

aprendizado federado. In: **Anais do XXVIII Workshop de Gerência e Operação de Redes e Serviços**. SBC, 2023. p. 71-84. Disponível em: https://sol.sbc.org.br/index.php/wgrs/article/view/24671/24492. Acesso em: 14 ago. 2023.

TAULLI, Tom. **Introdução à inteligência artificial:** uma abordagem não técnica. São Paulo: Novatec, 2020. 276 p. *Kindle.*

TERADA, Routo. **Segurança de dados:** criptografia em rede de computador. trad. Daniel Vieira. São Paulo: Editora Blucher, 2008. 578 p.

VIEIRA, Flávio; CAMPOS, Carlos Alberto V. FedWS: Uma Nova Abordagem para Aprendizado Federado usando Dados Heterogêneos. *In*: **Anais do XXII Workshop em Desempenho de Sistemas Computacionais e de Comunicação**. SBC, 2023. p. 1-12. Disponível em: https://sol.sbc.org.br/index.php/wperformance/article/view/24936/24757. Acesso em: 14 ago. 2023.

XAVIER, Maria Rita Pereira; DANTAS, Alexsandro Galeno Araújo. Dispositivo de vigilância algorítmica: algoritmos rastreadores e coleta de dados. **Simbiótica. Revista Eletrônica**, v. 8, n. 4, p. 94-127, 2021. Disponível em: https://periodicos.ufes.br/simbiotica/article/view/37348/24619. Acesso em: 12 ago. 2023.

WANG, Shibo *et al.* Privacy Protection in Federated Learning Based on Differential Privacy and Mutual Information. In: **2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture**. 2021. p. 428-435.

YANG, Qiang et al. Federated learning: synthesis lectures on artificial intelligence and machine learning. vol, v. 13, p. 1-207, 2019.

Conflito de Interesses

A autora declara não haver qualquer conflito de interesses em relação ao manuscrito, seja ele financeiro, comercial, político, acadêmico ou pessoal.

Este preprint foi submetido sob as seguintes condições:

- Os autores declaram que estão cientes que são os únicos responsáveis pelo conteúdo do preprint e que o depósito no SciELO Preprints não significa nenhum compromisso de parte do SciELO, exceto sua preservação e disseminação.
- Os autores declaram que os necessários Termos de Consentimento Livre e Esclarecido de participantes ou pacientes na pesquisa foram obtidos e estão descritos no manuscrito, quando aplicável.
- Os autores declaram que a elaboração do manuscrito seguiu as normas éticas de comunicação científica.
- Os autores declaram que os dados, aplicativos e outros conteúdos subjacentes ao manuscrito estão referenciados.
- O manuscrito depositado está no formato PDF.
- Os autores declaram que a pesquisa que deu origem ao manuscrito seguiu as boas práticas éticas e que as necessárias aprovações de comitês de ética de pesquisa, quando aplicável, estão descritas no manuscrito.
- Os autores declaram que uma vez que um manuscrito é postado no servidor SciELO Preprints, o mesmo só poderá ser retirado mediante pedido à Secretaria Editorial do SciELO Preprints, que afixará um aviso de retratação no seu lugar.
- Os autores concordam que o manuscrito aprovado será disponibilizado sob licença Creative Commons CC-BY.
- O autor submissor declara que as contribuições de todos os autores e declaração de conflito de interesses estão incluídas de maneira explícita e em seções específicas do manuscrito.
- Os autores declaram que o manuscrito não foi depositado e/ou disponibilizado previamente em outro servidor de preprints ou publicado em um periódico.
- Caso o manuscrito esteja em processo de avaliação ou sendo preparado para publicação mas ainda não publicado por um periódico, os autores declaram que receberam autorização do periódico para realizar este depósito.
- O autor submissor declara que todos os autores do manuscrito concordam com a submissão ao SciELO Preprints.