

LGPD e inteligência artificial: Um estudo comparado

Brazilian general data protection law and artificial intelligence: A comparative study

Juliano Lazzarini Moretti¹

Milena Maltese Zuffo²

RESUMO

Este artigo analisa a relação entre o uso de dados pessoais e as tecnologias de inteligência artificial (IA), destacando seus desenvolvimentos históricos e desafios regulatórios. O uso de dados pessoais inicialmente focou na privacidade e evoluiu para a proteção de dados, enquanto a IA, surgida no século XX, ganhou relevância comercial na década de 1990, exigindo amplo processamento de dados e gerando tanto benefícios quanto riscos. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleceu um marco jurídico, mas a regulamentação da IA ainda está em discussão, buscando equilibrar inovação com direitos fundamentais e segurança jurídica.

Palavras-chave: Regulamentação de IA. Proteção de Dados Pessoais. Estados Unidos. União Europeia. LGPD.

ABSTRACT

This article analyses the relationship between the use of personal data and artificial intelligence (AI) technologies, highlighting their historical developments and regulatory challenges. The use of personal data initially focused on privacy and evolved into data protection, while AI, which emerged in the 20th century, gained commercial relevance in the 1990s, requiring extensive data processing and generating both benefits and risks. In Brazil, the General Data Protection Law (LGPD) established a legal framework, but AI regulation remains under discussion, seeking to balance innovation with fundamental rights and legal certainty.

Keywords: AI Regulation. Personal Data Protection. United States. European Union. Brazilian General Data Protection Law.

¹ LL.M. pela Columbia University – School of Law (NY); Pós-graduações em Comércio Internacional da UCLA, em Negócios Internacionais da Função Getúlio Vargas (FGV-SP) e em Relações Internacionais da Universidade de São Paulo; e Bacharel em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP).

² LL.M em Direito Marítimo pela University College London, Mestre em Ciências em Direito Internacional Público e Direito Comparado pela Universidade de São Paulo, Bacharela em Direito pela Universidade de São Paulo.

INTRODUÇÃO

O artigo tem como objetivo analisar a interação entre duas matérias distintas, mas, no mínimo complementares: o uso de dados pessoais e a tecnologia de inteligência artificial (IA). Assim, é necessário explicar, inicialmente, que essas atividades existem de forma separada e independente. Por exemplo, há o uso de dados pessoais sem a necessidade de processamento por meio de IA. O início do uso de dados pessoais não está sequer vinculado ao desenvolvimento tecnológico, uma vez que já existia de forma analógica. Contudo, conforme explicou Doneda (2019, p. 14), a discussão anterior era concentrada no direito de privacidade e, na fase tecnológica, houve um avanço do uso de dados com uma intensificação desse uso por entes privados, sendo que a proteção de dados seria um desdobramento da proteção da privacidade na sociedade da informação.

Segundo Mendes, Rodrigues e Fonseca (2023, p. 67), a proteção de dados pessoais se tornou fundamental para conferir segurança jurídica aos setores econômicos que realizavam tratamento de dados em suas atividades e para promover uma sensação de confiança dos titulares de dados pessoais nas estruturas de comunicação e informação, tendo, inclusive, sido declarado um direito fundamental pelo Supremo Tribunal Federal. No Brasil, a Lei Geral de Proteção de Dados Pessoais foi considerada um marco legislativo, uma vez que não existia uma cultura de proteção de dados pessoais anterior e a proteção era realizada com base em artigos esparsos da legislação nacional, como normas gerais de proteção à privacidade ou regras incluídas no Marco Civil da Internet³.

Os Estados Unidos não adotaram uma lei federal sobre a neutralidade da Internet (como o Marco Civil brasileiro, por exemplo) e optaram por reconhecer a autoridade do *Federal Communications Commission* para regulamentar os serviços domésticos de Internet de alta velocidade, que são classificados como serviço de informação (Setenareski *et al.*, 2020, p. 293). Contudo, o debate sobre proteção de dados pessoais é juridicamente relevante no país a ponto de existir um projeto de lei federal sobre o tema, atualmente em discussão, o *American Data Privacy Protection Act*, apresentado em 2022 (US Congress, 2024). Atualmente, os Estados norte-americanos

³ O Marco Civil da Internet se refere à Lei n. 12.965/2014, que estabeleceu princípios, garantias e deveres para o uso da Internet no Brasil. O uso livre da Internet, que alguns apelidaram de “terra sem lei”, gerava uma certa insegurança jurídica, na medida em que não era claro quais normas seriam aplicáveis no espaço digital, como poderia ser realizada a identificação dos usuários e quem poderia ser responsabilizado por eventuais atos ilegais (Tomasevicius Filho, E. 2016, p. 271-273). Os debates legislativos sobre Marco Civil da Internet começaram em 2009 e contou com um processo participativo e democrático, que é celebrado até hoje. Além das discussões moderadas pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa, por meio das quais a população era convidada a comentar as regras propostas e indicar temas relevantes para o debate legislativo, o Ministério das Relações Exteriores solicitou às embaixadas brasileiras no exterior estudos sobre a situação da regulamentação da Internet por outros países (Flumignan, 2018, p. 25).

possuem regras próprias sobre a proteção de dados pessoais, como a *California Consumer Privacy Act*, a *Virginia Consumer Data Protection Act* e a *Colorado Privacy Act*.

As discussões sobre proteção de dados no âmbito dos países membros da União Europeia são mais antigas porque a proteção de dados pessoais é um direito fundamental garantido no artigo 8 da Carta da União Europeia de Direitos Fundamentais. Nesse contexto, em 1995, a União Europeia adotou a Diretiva Europeia sobre Proteção de Dados Pessoais, que foi substituída, em 2016, pelo Regulamento Geral de Proteção de Dados, conhecido pela sigla GDPR. Essa alteração de diretiva para regulamento é relevante em relação à estrutura jurídica da União Europeia. Conforme explicado por Arndt *et al.* (2010, p. 42), o direito europeu é dividido hierarquicamente entre fontes primárias e secundárias, sendo que a Carta da União Europeia de Direitos Fundamentais seria uma fonte primária, enquanto regulamentos e diretivas são fontes secundárias de direito.

A competência da União Europeia para legislar sobre proteção de dados pessoais tem sua base jurídica no artigo 16 do Tratado sobre o Funcionamento da União Europeia. Esse mesmo tratado estabeleceu, no artigo 288, a diferença entre regulamento e diretiva. Enquanto um regulamento tem caráter geral, sendo obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados Membros, a diretiva vincula o Estado Membro quanto ao resultado que se deseja alcançar, mas as instancias nacionais são competentes em relação à forma e meios de implementação. Ou seja, o regulamento não necessita de uma lei nacional para produzir efeitos, enquanto a diretiva dá liberdade legislativa aos Estados Membros (Arndt *et al.*, 2010, p. 45). Na prática, os regulamentos geram um efeito de harmonia jurídica maior do que as diretivas porque não existe uma discricionariedade dos Estados Membros em relação a nacionalização das regras.

Considerando que a matéria começou a ser legislada na União Europeia por meio de uma diretiva, é uma consequência lógica o fato de que os países membros possuem uma tradição na regulamentação da proteção de dados pessoais. Conforme explicado por Custers *et al.* (2018), p. 239-240), a maioria dos Estados Membros adotaram legislações nacionais em 1998, sendo que a França teria sido o último país a adotar uma norma nacional em 2004. O estudo terá como foco o desenvolvimento das normas na União Europeia, motivo pelo qual as discussões nacionais fomentadas pelos Estados Membros não serão analisadas de forma específica.

As discussões sobre IA, por sua vez, tiveram início nos anos 1940, como um exercício matemático que buscava replicar as conexões neurológicas (Shao *et al.*, 2022, p. 2). Os desenvolvimentos tecnológicos ocorreram entre os anos 1950 e 1960, mas a maioria dos resultados

necessários para a popularização comercial da tecnologia foram alcançados apenas nos anos 1990 (Georgiou, 2020, p. 138). Nesse sentido, o gráfico abaixo detalha os principais eventos que possibilitaram o desenvolvimento de tecnologias de IA:

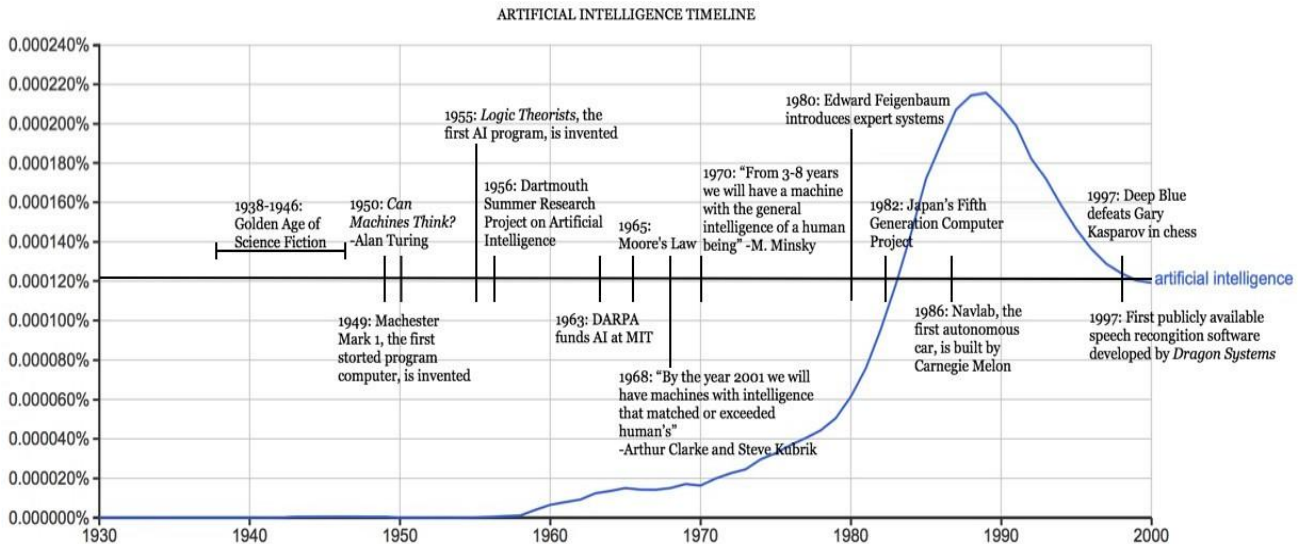


Figura 1: Linha da evolução da inteligência artificial Fonte: Anyoha, 2017.

A IA funciona a partir de uma base de dados, classificando e processando esses dados, sendo que a velocidade e escala com que consegue desempenhar essa atividade foi o que impulsionou a sua utilização em diversas esferas da sociedade (Clother e Doussolin, 2024, p. 5). A IA tem sido vista como uma forma de amplificar as capacidades humanas, como compreensão de texto, análise de dados, emissão de sumários e relatórios etc., e, do ponto de vista estratégico comercial, a IA também pode ser implementada no desenvolvimento de estratégias comerciais. Existem diversos tipos de tecnologia de IA, como robôs, *machine learning*, *large language models*, dentre outros. Essas tecnologias têm sido apresentadas como ferramentas para aumento de eficiência (IBM, 2024). Uma das tecnologias que mais chama atenção, nesse contexto, é a IA generativa, que tem mudado a presunção anterior de que certas atividades só poderiam ser realizadas por humanos, já que ela tem como objetivo gerar conteúdos, como escrever poemas, criar softwares, desenhar (Feuerriegel et al, 2023, p. 111). A IA generativa é baseada em modelagem generativa, que se difere da modelagem discriminativa na medida em que esta classifica dados para auxiliar na tomada de decisão, enquanto a modelagem generativa tenta inferir alguma distribuição real de dados (Feuerriegel et al, 2023, p. 112). As aplicações de AI generativa são apresentadas por Feuerriegel *et al* (2023, p. 116) como

sistemas voltados para resolver problemas de negócios, ampliando as capacidades humanas por meio da integração de tecnologia de IA em tarefas específicas.

Ao mesmo tempo em que essas tecnologias apresentam diversas oportunidades de crescimento e desenvolvimento para o mercado, elas também apresentam riscos que tornam o seu uso uma fonte de insegurança. Segundo a Thomson Reuters (2024), haveria uma demanda do próprio mercado pela regulamentação da IA para ampliar o uso da tecnologia com segurança jurídica sobre as suas responsabilidades, uma vez que a IA generativa pode criar documentos, imagens e vídeos baseados em informações falsas, fazendo com que essas empresas virem, potencialmente, um canal de distribuição de desinformação, dentre outros riscos associados ao uso dessas tecnologias. Essa preocupação não é meramente especulativa, uma vez que há diversos relatos sobre resultados inconsistentes gerados pela IA, fenômeno que tem ficado conhecido pelo termo alucinações (Maleki, Padmanabhan e Dutta, 2024, p. 135).

Esses erros de resultado que podem incluir citações inexistentes representam um risco relevante para as empresas e para quem usa essa tecnologia, já que um número considerável de pessoas não consegue identificar informações falsas ou enganosas geradas pela IA. Em um estudo realizado pela OCDE (2024, p. 23) sobre o tema, apenas a Finlândia apresentou um percentual maior do 80% da população capaz de identificar informações falsas geradas pela IA.

O tema passou a ter relevância jurídica, havendo a intenção de regulamentação da IA no Brasil. Segundo a justificativa do projeto de lei 2.338/2023, há a necessidade de balancear a proteção de direitos e liberdades fundamentais, valorização do trabalho e a dignidade da pessoa humana com a necessidade de criação de novas cadeias de valor, de modo a garantir segurança jurídica para inovação e desenvolvimento tecnológico (Pacheco, 2023, p. 29-30). Considerando que o país já possui uma legislação específica sobre proteção de dados pessoais e a forte interação entre essas duas matérias, é importante compreender quando existiria uma questão a ser abordada por ambas as regulamentações, de modo a buscar uma harmonia legislativa, bem como analisar a experiência estrangeira sobre a regulamentação dessas matérias e a conciliação de pontos controvertidos.

Assim, a partir de uma análise bibliográfica sistemática e não exaustiva, o artigo teve como objetivo realizar uma análise da regulamentação de IA a partir da LGPD, identificando os pontos de convergência entre as matérias e como questões controversas foram endereçadas em outros países que possuem a experiência legislativa ou de discussão sobre o tema. O recorte temático para o estudo comparado foi limitado à União Europeia e aos Estados Unidos, por serem considerados impérios

tecnológicos que possuem abordagens diversas para esses temas (Brandford, 2023, p. 6). Nesse contexto, o artigo foi dividido em três partes. Inicialmente é apresentado como dados pessoais podem ser utilizados por tecnologias de IA, com o objetivo de identificar pontos controversos que costumam gerar discussões sobre a necessidade de regulamentação. Após a identificação desses pontos, foi analisado como eles foram tratados internacionalmente durante os debates sobre a regulamentação da IA e interação com as normas de proteção de dados pessoais. Por fim, os resultados são confrontados com a regulamentação em vigor no Brasil, buscando compreender quais seriam os pontos semelhantes e quando a experiência internacional pode ser benéfica para o contexto nacional.

1. O USO DE DADOS PESSOAIS PELA INTELIGÊNCIA ARTIFICIAL

Existe uma ligação intrínseca entre IA e dados pessoais. As tecnologias de IA funcionam a partir de repositórios de dados. É verdade que nem todos os dados tratados podem ser categorizados como dados pessoais, que segundo o artigo 5º, da LGPD, pode ser entendido como uma informação relacionada a uma pessoa natural identificada ou identificável. Contudo, a depender da finalidade e objetivo da aplicação de IA, ela pode ser utilizada para analisar dados pessoais. Um exemplo geral são as aplicações utilizadas pelo setor de recursos humanos com o objetivo de realizar uma pré-análise de currículos.

A principal questão relacionada ao uso de dados pessoais pela inteligência artificial é tratada como uma questão ética. Em regra, a tecnologia de IA não possui poder cognitivo e funciona como um sistema automático de leitura de dados para a identificação de padrões com o intuito de gerar resultados inteligentes. O processo é realizado a partir da programação de algoritmos. Ocorre que, pela falta de senso crítico na leitura e classificação dos dados, esses algoritmos podem perpetuar vieses discriminatórios por meio da replicação dos padrões identificados (Saeidnia, 2023, p. 1).

Segundo Newstead *et al* (2023), os algoritmos utilizados tendem a replicar padrões discriminatórios enraizados na sociedade. Um exemplo de discriminação realizada por uma decisão automática realizada por tecnologia de AI envolveu o aplicativo Google Fotos (Presse, 2015). Nesse caso, um usuário adicionou algumas fotos pessoais, as quais foram automaticamente lidas, classificadas e incluídas em uma pasta pelo Google Fotos. Ocorre que a pasta foi nomeada pela IA como “gorilas” em razão da cor da pele do usuário. Na época, o Google pediu desculpas e afirmou que trabalharia para melhorar a tecnologia utilizada.

Exemplos do impacto do uso de IA em direitos humanos também são comuns no campo do uso dessa tecnologia para vigilância por vídeo. Segundo Heaven (2020), algoritmos de previsão para policiamento são racistas. Heaven (2020) explicou que existem dois tipos de recursos de previsão para policiamento, sendo um baseado na localização para identificar ligações entre lugares, eventos e taxas criminais para prever os locais em que é mais provável de acontecer um crime, e outro que funciona com base em dados sobre pessoas, como idade, gênero, estado civil, histórico criminal, dentre outros, e que busca prever a chance de uma pessoa estar envolvida em uma atividade criminosa no futuro. O problema dos resultados gerados por essas tecnologias estaria na base de dados utilizada, principalmente por causa de históricos policiais existentes com base em discriminação. Ainda segundo Heaven (2020), uma pessoa preta teria cinco vezes mais chance de ser abordada pela polícia do que uma pessoa branca.

Os casos de discriminação e preconceito nos resultados de tecnologia de IA são diversos e há relatos relacionados a diferentes tipos de tecnologia, desde a *machine learning* até a IA generativa. Considerando que a IA é desenvolvida por uma pessoa, que escolhe desde o tipo de dado que será analisado, o algoritmo utilizado, até a finalidade do tratamento, muitas vezes o fator de discriminação pode ser atribuído ao próprio desenvolvedor. Segundo Varona e Suárez (2022, p. 3-4), há seis tipos de vieses que levam à discriminação: amostral (representatividade comprometida), de medição (erros sistemáticos nos dados), de autorrelato (falta de completude dos dados), de confirmação (preconceito do pesquisador), humano (reflexo de vieses pré-existent) e algorítmico (ampliação de vieses dos dados de treinamento). A discriminação ocorre tanto por algoritmos quanto por dados de treinamento, reforçando decisões e vieses passados em conjuntos futuros.

É dentro desse contexto de falhas nos resultados apresentados pela IA que teve início o debate sobre a necessidade de regulamentação sobre o uso, comercialização e desenvolvimento de IA para preservação de direitos e uso ético da tecnologia. Conforme explicado por Bryson (2020, p. 13) a regulamentação da IA não está relacionada a ideia de estabelecer meio de compensação, mas para manter a ordem social com o intuito de dissuadir as pessoas de realizar algo que abale essa ordem, sendo que esse poder de dissuadir é traduzido no esclarecimento sobre o que deve ser considerado ilegal e na determinação das consequências do descumprimento da legislação, ou seja, no estabelecimento da segurança jurídica. A discussão sobre o uso ético da AI também desencadeou a defesa da necessidade de transparência no uso dessas tecnologias, como defendido por Maranhão, Junquillo e Tasso (2023, p. 151).

Essa necessidade de um uso da IA para tratamento de dados de forma justa, transparente e ética desencadeou uma série de movimentos, cartas abertas e declarações no âmbito internacional. Nesse contexto, chama atenção a Declaração de Montreal (Universidade de Montreal, 2017), que tem como objetivo identificar os princípios e valores éticos que promovem os interesses fundamentais das pessoas e dos grupos. O Professor Russel (2015) também tem escrito uma série de cartas abertas sobre a necessidade de escrever diretrizes para a pesquisa sobre IA, principalmente em relação ao desenvolvimento de armas autônomas com tecnologia de IA. Em 2021, a UNESCO também emitiu uma recomendação sobre a ética na IA. Segundo Díaz-Rodríguez *et al* (2023, p. 3), a abordagem da UNESCO é uma mistura de princípios acompanhados de valores a serem promovidos, como direitos humanos e liberdades fundamentais. A proliferação de diretrizes sobre o uso de IA com ética motivou o estudo de Hagendorff (2020, p. 111), que analisou 22 dessas diretrizes e identificou um impacto limitado, promovendo a discussão sobre como torná-las mais eficazes, o que, na opinião do autor, poderia ser feito por meio da inclusão de explicações técnicas sobre os valores éticos abstratos que são utilizados nos documentos (como Justiça ou centralidade do ser humano em sistemas de IA). Portanto, fica claro que há um grande uso de dados pessoais pela tecnologia de IA e que, apesar do banco de dados utilizados pela IA não ser restrito aos dados pessoais, os principais exemplos de discriminação e preconceito envolvem o tratamento de dados pessoais. Esses problemas encontrados nos resultados de IA desencadearam uma série de publicações sobre diretrizes de ética e IA, como a Declaração de Montreal, as Recomendações da UNESCO sobre Ética da Inteligência Artificial (2021) e os Princípios da Inteligência Artificial da OECD (2019). Essas questões também fomentaram as discussões acadêmicas sobre a eficácia dessas diretrizes (Hagendorff, 2020; Héder, 2020; Klontzas *et al.*, 2023; Bruschi e Diomedea, 2023; Corrêa *et al.*, 2023). Além desse movimento da sociedade, que busca apresentar uma solução para o problema da discriminação e preconceito, também existe uma discussão sobre a necessidade de regulamentação da IA, conforme será analisado no próximo tópico.

2. AS DISCUSSÕES INTERNACIONAIS SOBRE O TEMA: UNIÃO EUROPEIA E ESTADOS UNIDOS

O Brasil está em um processo de discussão sobre a regulamentação da IA, conforme Projeto de Lei n. 2338/2023. As discussões sobre a adoção de um possível marco regulatório tiveram início em 2020, mas o projeto original sofreu alterações e foi reapresentado após o trabalho da comissão de

especialistas jurídicos, formada em 2022. O Brasil teria a intenção de adotar uma legislação que misture as experiências legislativas da União Europeia e dos Estados Unidos (Castro, 2024). Ao mesmo tempo em que deseja garantir direitos fundamentais, os legisladores têm buscado adotar uma lei que promova a liberdade de pesquisa e inovação com desenvolvimento econômico (Senado, 2024).

Nesse sentido, a pesquisa teve como objetivo compreender como as discussões comuns à proteção de dados pessoais e a regulamentação da IA foram tratadas na União Europeia e nos Estados Unidos. Ambos são considerados impérios digitais e, ainda mais relevante para promoção de discussão, possuem abordagens distintas para esses temas. Enquanto os Estados Unidos teriam uma abordagem mais voltada para o mercado, a União Europeia adotou uma abordagem mais voltada para a garantia de direitos (Bradford, 2023, p. 7). Assim, a análise comparada dos atos normativos adotados ou justificativa de eventual ausência legislativa pode ser benéfica para a discussão que ocorre em âmbito nacional e que, ao menos em discurso, busca encontrar um meio termo entre essas abordagens.

2.1. UNIÃO EUROPEIA

A União Europeia se coloca em uma posição de pioneirismo na adoção de normas que regulamentam o espaço digital e as tecnologias. A Autoridade Europeia de Proteção de Dados Pessoais apresenta as normas da União Europeia sobre proteção de dados como um sinônimo de padrão ouro de proteção, atingindo também organizações fora do bloco econômico, mas que ofereçam bens e serviços ou monitorem o comportamento de residentes da União Europeia.

A GDPR foi adotada em 2016 e entrou em vigor em 2018, tendo substituído a Diretiva de Proteção de Dados de 1995. Assim como na legislação brasileira, a GDPR tem como objetivo proteger a conexão entre o dado e um indivíduo identificado ou identificável. Seguindo a estratégia digital da União Europeia (Parlamento Europeu, 2023), a Comissão Europeia começou a discutir a regulamentação de IA em 2021 e, no primeiro semestre de 2024, o Parlamento Europeu adotou e o Conselho Europeu aprovou a *AI Act*, que entrou em vigor em agosto do mesmo ano.

Em um breve resumo, o *AI Act* estabeleceu normas baseadas no risco que o sistema de IA pode representar, considerando a sua finalidade. A União Europeia buscou resolver questões éticas e legais que eram debatidas sobre o tema por meio de proibições no uso dessa tecnologia (Ren e Du, 2024). O regulamento proíbe sistemas de IA que manipulem comportamentos de forma encoberta, explorem grupos vulneráveis ou realizem pontuação social baseada em características pessoais. Além

disso, impõe restrições rigorosas ao uso de identificação biométrica em tempo real (os sistemas de vigilância com uso de IA) por autoridades em espaços públicos, devido aos riscos classificados como inaceitáveis.

A interação entre ambas as normas tem sido muito debatida pela comunidade científica. Ainda assim, antes de apresentar essas análises, é relevante destacar que a interação das matérias não foi ignorada pelas instituições europeias. Em 2020, o Parlamento Europeu publicou o estudo sobre a regulamentação da IA pela GDPR, realizado pelo Painel para o Futuro da Ciência e da Tecnologia. O estudo foi liderado pelo Professor Giovanni Sartor e realizado em coautoria com a Professora Francesca Lagioia. Além de observar que a GDPR não endereçou a IA de forma expressa, o estudo também revelou que diversas questões relacionadas ao uso de dados pessoais em tecnologias de IA não seriam claramente respondidas pelas regras da GDPR (Sartor e Lagioia, 2020, p. III). O estudo aponta que o GDPR se aplica ao processamento de dados pessoais por sistemas de IA, abordando questões como decisões automatizadas, direitos de explicação e impacto ético (artigo 22), mas enfrenta desafios na implementação, como a definição de "riscos elevados" e o equilíbrio entre transparência e a complexidade técnica da IA, e recomenda avaliações de impacto e proteção desde a concepção (artigo 25) para promover conformidade e confiança pública (Sartor e Lagioia, 2020, p. 25-33).

O estudo do Parlamento Europeu está alinhado aos estudos sobre os pontos de intersecção entre a GDPR e a inteligência artificial. O artigo 22 que aborda as decisões automatizadas seria a principal regra de proteção de dados aplicável à IA, uma vez que essas decisões são realizadas com o uso de algoritmos, sendo que a GDPR adota como regra o direito do indivíduo em não se submeter a uma decisão inteiramente baseada em um processo automático, incluindo decisões de perfilamento (Kusmierczyk et al, 2022, p. 9).

Há uma discussão sobre como os direitos do titular de dados pessoais podem ser efetivados no caso do uso de dados pela IA. A GDPR estabeleceu uma série de direitos ao titular de dados pessoais, como o direito à informação, o direito a transparência, o direito ao esquecimento, dentre outros. Quase todos esses direitos foram incluídos na LGPD, que teve forte influência da lei europeia. Nesse contexto, há uma insegurança sobre como os titulares de dados poderão exercer seus direitos, de forma geral, quando houver tratamento de dados em massa (como no caso do *Big Data*).

Segundo a pesquisa de Butt (2024, p. 24-27), parte considerável dessas perguntas é respondida pela interpretação das normas pela Corte de Justiça da União Europeia. Por exemplo, no

caso Österreichische Post, a Corte teria esclarecido que a obrigação dos controladores de informar os titulares de dados pessoais sobre as organizações específicas que recebem os dados pessoais não seria aplicável quando for genuinamente impossível identificá-las. O caso FT v. DW também seria relevante para a matéria, já que teria estabelecido que o titular de dados poderia requerer acesso aos seus dados por motivos que vão além da mera verificação de tratamento legal de dados, tendo o direito de uma cópia integral ou um fiel e inteligível resumo dos dados tratados. O caso Krankenversicherung Nordrhein é relevante por ter estabelecido que o dever de provar o cumprimento das obrigações estabelecidas na GDPR e a exclusão de responsabilidade por danos é do controlador de dados. Todos esses casos serão relevantes para compreender a interação entre as normas de proteção de dados pessoais e os deveres dos desenvolvedores e comercializadores de aplicativos de IA.

A atuação do Comitê Europeu de Proteção de Dados Pessoais também é relevante para a interação das normas. Enquanto a GDPR estabeleceu a criação das autoridades de proteção de dados pessoais, a *AI Act* estabeleceu a atuação das autoridades de monitoramento de mercado. Nesse contexto, o Comitê Europeu (2024) emitiu uma declaração pública sobre a experiência e a expertise que as autoridades nacionais de proteção de dados teriam acumulado lidando com IA e direitos fundamentais e defendeu que essas autoridades deveriam ser indicadas como as autoridades de monitoramento de mercado como meio de garantir uma coordenação regulatória, aumentar a segurança jurídica e fortalecer a supervisão e aplicação de ambas as normas.

2.2. ESTADOS UNIDOS

Os Estados Unidos têm um posicionamento de liberdade de mercado. O país evita a adoção de normas que se sobreponham e criem uma restrição ao mercado que possa ser entendida como excessiva, sob uma perspectiva cultural, e que poderia eventualmente se transformar em obstáculo, mais do que um facilitador. Esse posicionamento ficou muito claro quando a União Europeia adotou a GDPR, que produz efeitos extraterritoriais e exige normas similares em vigor no país em que estiverem estabelecidas as empresas que comercializem ou monitorem residentes da União Europeia.

Foi durante esse período que o Brasil adotou a LGPD, por exemplo, sob o argumento de manter o mercado brasileiro participando do mercado internacional. Nos Estados Unidos, não existe uma norma geral de proteção de dados pessoais em nível federal. O debate sobre a possibilidade de adoção de uma norma federal ainda ocorre nos Estados Unidos e fez com que diversos Estados adotassem suas próprias legislações, como a *California Consumer Privacy Act*.

Nesse contexto, em 2019, o Congresso norte americano realizou um estudo sobre as regras de proteção de dados no país. O estudo é marcado por um entendimento do direito à proteção de dados pessoais como sinônimo do direito à privacidade. Segundo o estudo realizado, não havia uma necessidade inicial de proteção da privacidade na *common law* dos Estados Unidos, sendo que alguns casos e evoluções do direito foram realizados no meio do século XX, mas que nem mesmo as proteções constitucionais seriam suficientes para a proteção do direito de privacidade, motivo pelo qual o país passou a adotar legislações federais específicas que tinham como objetivo garantir os direitos de privacidade dos titulares de dados, como nos casos da *Video Privacy Protection Act* e da *Family Educational Rights and Privacy Act* (Congressional Research Service, 2019, p. 3-21).

Contudo, existe uma diferença em relação ao contexto europeu, que entende haver uma diferença de escopo entre privacidade e proteção de dados pessoais. Segundo Kobott e Sobotta (2013, p. 225-226), privacidade abrange a vida privada, enquanto proteção de dados se aplica a todas as informações pessoais identificáveis. Além disso, os autores defendem que a proteção de dados, conforme o direito da União Europeia, impõe obrigações tanto a autoridades públicas quanto a partes privadas no processamento de informações pessoais, enquanto o direito à privacidade tem um foco mais restrito, endereçando principalmente ações estatais.

Assim, a União Europeia e os Estados Unidos decidiram celebrar um acordo sobre proteção de dados pessoais que garantiu que as relações comerciais entre os países não fossem afetadas pela entrada em vigor da GDPR. O acordo entrou em vigor em 2017, após aprovação e implementação do *US Judicial Redress Act*. Em geral, o Acordo de Proteção de Dados UE-EUA estabelece um quadro para garantir a segurança de dados pessoais compartilhados entre as partes para fins de aplicação da lei, buscando promover cooperação e confiança.

Da mesma forma que ocorreu durante o debate sobre adoção de regras de proteção de dados nos Estados Unidos, o país tem sido palco de uma grande discussão sobre a eventual desnecessidade de adoção de normas de regulamentação da IA. Em 2023, por exemplo, a Câmara de Comércio dos Estados Unidos emitiu uma carta aberta requerendo um estudo parecido com aquele realizado sobre proteção de dados pessoais e com o objetivo de analisar o arcabouço legal norte-americano para concluir sobre a real necessidade de uma nova lei e evitar a adoção de leis em excesso que poderiam, potencialmente, prejudicar o desenvolvimento de novas tecnologias.

Apesar de não ter decidido adotar uma norma federal sobre a regulamentação da IA, os Estados Unidos não estão inertes em relação às discussões sobre ética no uso e desenvolvimento

dessas tecnologias. Nesse contexto, foram adotados dois documentos, o *Blueprint for an AI Bill of Rights*, de 2022 e que não é um documento vinculante, e a ordem do presidente sobre segurança da IA, o *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, adotado em 2023 (White House, 2023). A ordem do executivo não é uma lei propriamente dita, tampouco é vinculante para todos. Essas ordens vinculam somente os empregados do Executivo e podem ser objeto de revisões judiciais. Desde 2022, o Congresso tem analisado a possibilidade de adoção da *Algorithmic Accountability Act*, que não tem o mesmo escopo abrangente das normas da União Europeia, mas buscaria estabelecer requisitos mínimos de responsabilidade por meio de obrigações de emissão de relatórios e análises de impacto.

3. A INTERAÇÃO DAS MATÉRIAS NO BRASIL SOB A ÓTICA DA LGPD E DA PROPOSTA DE REGULAMENTAÇÃO DE IA

Assim como no caso da União Europeia, o Brasil já possui uma norma de proteção de dados pessoais em vigor. Conforme explicou Lorenzon (2021, p. 41), a LGPD nasceu em um contexto normativo em que a norma anterior que deveria ser considerada na sua concepção era o Marco Civil da Internet, uma norma que não tinha como objetivo principal o tema de dados pessoais. Ou seja, não é verdade que a LGPD nasceu de um completo vácuo normativo. Já existia no Brasil, por exemplo, a Lei de Acesso à Informação, de 2011, e que tinha como objetivo efetivar o princípio da transparência no tratamento de informações pessoais, principalmente buscando o respeito aos direitos de intimidade, vida privada, honra e imagem (Nardi e Lutzky, 2023, p. 6). Antes da LGPD, o tratamento de dados pessoais também era discutido no âmbito do Código de Defesa do Consumidor, principalmente em relação aos direitos de informação dos consumidores, o que foi confirmado e intensificado com a Lei do Cadastro Positivo (Nardi e Lutzky, 2023, p. 6).

A LGPD foi altamente influenciada pela GDPR, mas não é uma cópia exata. Nesse sentido, assim como no caso da regulamentação da IA, o espírito do legislador não era inviabilizar o desenvolvimento econômico, mas garantir o balanceamento da liberdade de empreendedorismo com o direito de proteção à personalidade e privacidade (Queiroz, 2021, p. 43). Assim como a GDPR estabeleceu normas sobre a decisão automatizada e os direitos dos titulares de dados, a LGPD também o fez no artigo 20. Até mesmo estudos que têm como objetivo analisar a interação entre a LGPD e o uso da inteligência artificial no âmbito da saúde, como o realizado por Dourado e Aith (2022, p. 4-5) são limitados a análise das decisões automatizadas e o direito de informação.

Segundo Maranhão *et al* (2024), seria importante para a promoção da segurança jurídica a emissão de uma regulamentação desse artigo pela autoridade de proteção de dados nacional. Isso decorreria da forma como o artigo tem sido aplicado no judiciário brasileiro. Em razão da falta de critérios bem estabelecidos, as decisões judiciais têm interpretado o direito de acesso do titular de dados como um direito ao conhecimento do código fonte, subordinação algorítmica, bem como decisões para remover indivíduos de registros (Maranhão *et al*, 2024).

Uma busca na plataforma Painel LGPD nos Tribunais, que consiste em um projeto fácil de identificação de decisões que abordam a aplicação da LGPD no Brasil e foi desenvolvido pelo Jusbrasil e a IDP Privacy Lab (grupo de pesquisa coordenado por Laura Schertel e Danilo Doneda, *in memoriam*), identificou que entre 2020 e 2024, 456 decisões analisaram a aplicação do artigo 20, sendo que houve um pico de decisões em 2023:



Figura 2: Número de decisões sobre o artigo 20 da LGPD nos tribunais brasileiros

Fonte: Painel LGPD nos Tribunais, 2024.

A pesquisa também evidenciou que há poucos julgados no âmbito dos tribunais superiores, sendo que mais de um quarto dos casos foram julgados pelo Tribunal de Justiça do Estado de São Paulo (TJSP). Contudo, o pedido de perícia com a possibilidade de conhecimento do código fonte tem sido mais comum no âmbito dos Tribunais Regionais do Trabalho. Nesse sentido, destaca-se a correição parcial n. 1001223-14.2021.5.00.000, julgada pelo Corregedor-Geral da Justiça do Trabalho em 31 de agosto de 2021, no qual foi determinada a suspensão da perícia computacional determinada nos autos da reclamação trabalhista n. 0102996-92.2021.5.01.0000 pelo perigo de dano irreversível consistente no conhecimento do código fonte. A discussão sobre a subordinação

algoritmia também tem sido realizada na esfera trabalhista, conforme evidenciado pelo recurso de revista em agravo n. 924-88.2022.5.13.0022, julgado em 19 de novembro de 2024, no Tribunal Superior do Trabalho e com voto relator do Ministro Amaury Rodrigues Pinto Júnior. Na decisão, o Ministro relator entendeu que a subordinação algorítmica (pedido de reconhecimento de subordinação trabalhista entre o requerente e a empresa provedora de plataforma digital) não se enquadraria nas hipóteses regulamentadas pela Consolidação das Leis do Trabalho.

Ainda segundo Maranhão *et al* (2024), todas essas decisões estariam aumentando a insegurança jurídica em relação a matérias relevantes como a proteção da propriedade intelectual. Essas decisões também são relevantes para demonstrar que, ainda que o Brasil opte por um modelo muito semelhante ao adotado anteriormente por outro país, os efeitos da legislação não necessariamente serão os mesmos em razão da aplicação e interpretação pelo judiciário nacional.

A IA não é limitada às tecnologias que permitem a tomada de decisão automatizada. Assim, uma regulamentação de IA teria uma abrangência mais ampla e, potencialmente, garantiria uma maior proteção de privacidade e tratamento de dados pessoais por ser aplicável a todas as tecnologias de IA. Como explicado anteriormente, o Brasil ainda não possui uma norma sobre IA e tem tido discussões no Senado sobre a regulamentação da IA. O projeto em discussão propõe a adoção de um modelo de riscos, muito semelhante ao modelo da União Europeia, que levaria a proibição de tecnologias e aplicações que apresentem um risco definido como excessivo ou inaceitável.

Não há uma expectativa da regulamentação brasileira ser uma simples cópia das normas adotadas por outros países. Um exemplo desse ponto é no caso das decisões automatizadas. Existe uma expectativa de legislação dessa tecnologia de forma expressa na regulamentação da IA, em complementação às normas da LGPD. Essa expectativa decorre tanto do fato de haver uma norma semelhante no *AI Act*, quanto das discussões sobre esse ponto que ocorrem no âmbito do Senado. Segundo Almgren (2023, p. 33), existe uma discussão sobre a possibilidade de proibição das decisões automáticas que sejam tomadas sem a supervisão humana por causa do risco de discriminações, o que alteraria a implementação do artigo 20 da LGPD.

Um tema que poderá ser impactado pela regulamentação da IA no Brasil é o uso de reconhecimento facial na segurança pública. Assim como ocorreram diversas discussões no âmbito internacional sobre o balanceamento entre os direitos de privacidade e segurança pública, bem como formas de evitar o viés discriminatório dos resultados, as quais foram devidamente apresentadas anteriormente, há um forte debate no Brasil sobre a possibilidade de uso dessas tecnologias. A LGPD

não foi suficiente para responder a todas as questões que surgem dessa prática, principalmente considerando que o reconhecimento facial consiste no tratamento de um dado biométrico e, portanto, um dado sensível que tem maior proteção legal. Segundo Franqueira *et al* (2021, p. 179-180), o Brasil não adotou regras específicas sobre os limites e padrões a serem seguidos por sistemas de vídeo vigilância. A LGPD seria atualmente o único instrumento possível de ser utilizado para exigir o uso minimamente ético e com respeito aos direitos fundamentais dos usuários. Um exemplo teria ocorrido quando o Tribunal de Justiça do Estado de São Paulo impediu que uma das empresas concessionárias responsáveis pela linha de trens metropolitanos da cidade de São Paulo utilizasse reconhecimento facial para fins publicitários. Ainda assim, a LGPD não seria aplicável quando o tratamento é feito para a manutenção da segurança pública e persecução ou mitigação da prática de delitos, motivo pelo qual a regulamentação da IA pode ser uma oportunidade de trazer segurança jurídica para este ponto.

Independente das decisões que serão tomadas sobre a possível regulamentação da IA, é altamente recomendável que seja seguido os modelos procedimentais adotados na União Europeia e nos Estados Unidos com a análise do arcabouço legal já existente e como as normas têm sido interpretadas pelo judiciário nacional, especialmente em relação às tecnologias de decisão automatizada que já estão regulamentadas em relação aos direitos dos titulares pela LGPD. Ao levar em consideração a realidade nacional de implementação da LGPD e normas de proteção da privacidade, o resultado tende a ser a adoção de uma legislação mais harmônica e que considera a cultura tecnológica nacional.

CONCLUSÃO

A pesquisa evidenciou que existe uma forte interação entre as matérias de proteção de dados pessoais e regulamentação de IA. A tecnologia de IA funciona sob uma lógica que demanda a leitura e classificação de muitos dados, que também é conhecido como *Big Data*. Nesse contexto, a IA não limitada a análise e classificação de dados pessoais, mas, principalmente em razão da finalidade que se deseja alcançar pela implementação do sistema de IA, é possível que seja necessário realizar o tratamento desses dados.

Contudo, a tecnologia não apresenta resultados perfeitos e é marcada pelo risco de discriminação e preconceito nos resultados. Esse risco decorre, novamente, de como o sistema funciona, uma vez que a IA é treinada para encontrar padrões nos dados analisados e são esses padrões

que possibilitam a entrega do resultado desejado. Como a sociedade não é livre de preconceito e discriminação, ao analisar os dados, a IA poderá identificar esses padrões discriminatórios.

As tecnologias de IA também apresentam um erro comum que é chamado de alucinações, consistente em um fenômeno pelo qual a IA generativa pode inventar informações ou basear suas conclusões em premissas falsas. Desse erro decorre o risco de disseminação de desinformação e informações falsas. Como parte considerável da população não tem capacidade de identificar quando uma informação gerada pela IA é falsa ou enganosa, essa situação pode gerar uma insegurança jurídica de mercado, como no caso da incerteza sobre a identificação de quem deveria ser responsabilizado por danos causados. Assim, o debate sobre a necessidade de regulamentação e estabelecimento de valores éticos para uso, comercialização e desenvolvimento da IA se intensificou.

Considerando a intenção nacional de adotar uma norma que tem inspiração em ambos os modelos legislativos (europeu e estado unidense), o estudo demonstrou a necessidade de cautela durante a realização dessa análise e seleção do que será incorporado ao cenário nacional. Além das culturas jurídicas europeia e norte americana serem diferentes, os motivos que levam a União Europeia e os Estados Unidos a tomarem as decisões legislativas é baseado no arcabouço jurídico identificado e as demandas da população. Em síntese, a União Europeia tem uma tradição de adotar normas que buscam garantir os direitos fundamentais dos indivíduos que residem no território europeu, enquanto os Estados Unidos têm uma demanda de mercado e busca compreender as regras já em vigor para evitar um excesso de normas, o que poderia se tornar um obstáculo, ou até um impeditivo para a evolução tecnológica que já se tornou um traço marcante daquela economia. Esse posicionamento estaria alinhado com o tipo de sistema jurídico adotado no país, o *common law*.

Assim como ocorre na União Europeia e nos Estados Unidos, o Brasil também possui normas anteriores à regulamentação da IA cujas regras poderão ter novas interpretações com a entrada em vigor dessa legislação. Nesse contexto, é importante garantir uma abordagem que busque promover a harmonização legislativa, de modo a proporcionar segurança jurídica sobre o tema, mas não se esquecendo das possibilidades quase infinitas que a evolução tecnológica pode proporcionar não só para os negócios de um país, mas para a sociedade como um todo. Em relação à LGPD, existem dois pontos principais de interseção. Primeiro, a regra expressa do artigo 20 atinente às aplicações com tecnologia de decisão automatizada e cujo direito de acesso à informação é previsto na LGPD. A segunda, refere-se aos direitos gerais dos titulares de dados, como transparência e acesso aos dados tratados. Nesse contexto, a pesquisa chamou atenção para a relativa lacuna legal existente em relação

ao uso de câmeras de reconhecimento facial e que poderia ser disciplinada pelas normas de regulamentação da IA, sempre com a preocupação de equilíbrio legislativo e principiológico para que a sociedade como um todo se beneficie dessa evolução tecnológica.

REFERÊNCIAS BIBLIOGRÁFICAS

- ALMGREN, F. *Inteligência artificial e cognição: delegação da atividade cognitiva à máquina*. 2023. Dissertação (Mestrado) - Universidade de São Paulo, São Paulo, 2023. Disponível em: <https://repositorio.usp.br/item/003217248> Acesso em: 03 dez. 2024.
- ANYOHA, R. The History of Artificial Intelligence. *Harvard Kenneth C. Griffin Blog*. 2017. Disponível em: <https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/> Acesso em: 03 dez. 2024.
- BRADFORD, A. *Digital Empires: The Global Battle to Regulate Technology*. Oxford: Oxford University Press, 2023.
- BRUSCHI, D. DIOMEDE, N. A framework for assessing AI ethics with applications to cybersecurity. *AI and Ethics*, v. 3, 2022. Disponível em: <https://link.springer.com/article/10.1007/s43681-022-00162-8> Acesso em 19 dez. 2024.
- BRYSON, J. J. The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation. In: DUBBER, M. D. et al. (coord.). *The Oxford Handbook of Ethics and AI*. Oxford: Oxford University Press, 2020.
- BUTT, J. S. The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans? *Acta Universitatis Danubius Juridica*, v. 20, n. 2, 2024.
- CASTRO, A. IA: relator apresenta proposta alinhada com regulamentos da Europa e dos EUA. *SenadoNotícias*. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/04/24/ia-relator-apresenta-proposta-alinhada-com-regulamentos-da-europa-e-dos-eua> Acesso em: 03 dez. 2024.
- CLOTHER, C.; DOUSSOULIN, J. P. Artificial intelligence: driving force in the evolution of human knowledge. *Journal of Innovation & Knowledge*, v. 9, n. 4, 2024.
- CONGRESSIONAL RESEARCH SERVICE. Data Protection Law: An Overview. Washington: Congress, 2019. Disponível em: <https://crsreports.congress.gov> Acesso em: 03 dez. 2024.
- CORRÊA, N. K. et al. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *CellPress*, v. 4, n. 10, 2023. Disponível em: [https://www.cell.com/patterns/fulltext/S2666-3899\(23\)00241-6](https://www.cell.com/patterns/fulltext/S2666-3899(23)00241-6) Acesso em 19 dez. 2024.
- CUSTERS, B. et al. A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, v. 34, n. 2. 2018.
- DÍAZ-ROGRÍGUEZ, N. et al. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, v. 99, nov. 2023.

- DONEDA, D. *Da Privacidade à Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2019.
- DOURADO, D. A.; AITH, F. M. A. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. *Revista de Saúde Pública*, v. 56, n. 80, 2022. Disponível em: <http://www.rsp.fsp.usp.br/> Acesso em: 03 dez. 2024.
- EUROPEAN DATA PROTECTION BOARD. EDPB adopts statement on DPAs role in AI Act framework, EU-U.S. Data Privacy Framework FAQ and new European Data Protection Seal. 2024. Disponível em: https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en Acesso em: 03 dez. 2024.
- FRANQUEIRA, B. D. *et al.* O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, v. 8, n. 1, 2021. Disponível em:
- FLUMIGNAN, W. G. G. *Responsabilidade civil dos provedores no Marco Civil da Internet (Lei n. 12.965/14)*. 2018. Dissertação (Mestrado) - Universidade de São Paulo, São Paulo, 2018. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2131/tde-21082020-010522/pt-br.php> Acesso em: 03 dez. 2024.
- GEORGIU, K. Tracing the evolution of AI: Conceptualisation of artificial intelligence in mass media discourse. *Information Discovery and Delivery*, v. 48, n. 3, 2020.
- HAGENDORFF, T. The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines*, v. 30, 2020.
- HAGENDORFF, T. The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines*, v. 30, 2020. Disponível em <https://link.springer.com/article/10.1007/S11023-020-09517-8> Acesso em 19 dez. 2024.
- HEAVEN, W. D. Predictive policing algorithms are racist. They need to be dismantled. *MIT Technology Review*, 2020. Disponível em: <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/#:~:text=For%20one%20thing%2C%20predictive%20algorithms,cause%20as%20a%20white%20person> Acesso em 03 dez. 2024.
- HÉDER, M. A criticism of AI ethics guidelines. *Információs Társadalom XX*, n. 4, 2020. Disponível em: https://eprints.sztaki.hu/10069/1/Heder_57_31919577_ny.pdf Acesso em 19 dez. 2024.
- <https://www.revistas.usp.br/rdda/article/view/173903> Acesso em: 03 dez. 2024.
- FUEERRIEGEL *et al.* Generative AI. *Business Information System Engineer*, v. 66, n. 1, 2023.
- KLONTZAS, M. E. *et al.* AI Reporting Guidelines: How to Select the Best One for Your Research. *Radiology: Artificial Intelligence*, v. 5, n. 3, 2023. Disponível em: <https://pubs.rsna.org/doi/full/10.1148/ryai.230055> Acesso em 19 dez. 2024.
- KOBOTT, J.; SOBOTTA, C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, v. 3, n. 4, nov. 2013. Disponível em: <https://academic.oup.com/idpl/article/3/4/222/727206?login=false> Acesso em: 03 dez. 2024.

KUSMIERCZYK, M. *et al.* Algorithmic bias in the light of the GDPR and the proposed AI Act. In: OLEJNIK, M.; MORAWSKA, W. (coord.). *(In)equality. Faces of Modern Europe*. Wrocław: Wydawnictwo Centrum Studiów Niemieckich i Europejskich im. Willy'ego Brandta, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4117936 Acesso em 03 dez. 2024.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, v. 1, 2021. Disponível em: <https://periodicos.fgv.br/rpdue/article/view/83423> Acesso em: 03 dez. 2024.

MALEKI, N. *et al.* Ai Hallucinations: A Misnomer Worth Clarifying. *2024 IEEE Conference on Artificial Intelligence*, 2024. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10605268> Acesso em: 03 dez. 2024.

MARANHÃO, J. S. A. *et al.* Riscos e oportunidades na regulamentação de decisões automatizadas e IA pela ANPD. *Consultor Jurídico*. 2024. Disponível em: <https://www.conjur.com.br/2024-nov-27/riscos-e-oportunidades-da-regulamentacao-de-decisoes-automatizadas-e-inteligencia-artificial-pela-anpd/> Acesso em: 03 dez. 2024.

MARANHÃO, J. S. A. *et al.* Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Revista de Estudos Constitucionais*, v. 3, n. 2, 2024.

MENDES, L. S. *et al.* O Supremo Tribunal Federal, a proteção constitucional dos dados pessoais e a positivação superveniente de um direito fundamental autônomo. In: MENDES, L.

NARDI, L. G.; LUTZKY, D. C. Uma Perspectiva Analítica da Aplicação da Inteligência Artificial (IA) à Lei Geral de Proteção de Dados Pessoais (LGPD). 2023. Dissertação (Graduação). Pontifícia Universidade Católica do Rio Grande do Sul, 2023. Disponível em: <https://repositorio.pucrs.br/dspace/handle/10923/26472> Acesso em: 03 dez. 2024.

NEWSTEAD, T. *et al.* How AI can perpetuate – or help mitigate – gender bias in leadership.

OECD. *The OECD Truth Quest Survey: methodology and findings*. OECD Digital Economy Papers, v. 369, 2024. Disponível em: https://www.oecd.org/en/publications/the-oecd-truth-quest-survey_92a94c0f-en.html Acesso em: 03 dez. 2024.

Organizational Dynamics, v. 52, n. 4, 2023.

PACHECO, R. Projeto de Lei n. 2338, de 2023. *Projeto de Lei*. 2023. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1733154872288&disposition=inline> Acesso em 03 dez. 2024.

PARLAMENTO EUROPEU. *Conclusion of the EU-US Data Protection Umbrella Agreement*. 2024. Disponível em: <https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-conclusion-of-the-eu-us-data-protection-umbrella-agreement> Acesso em: 03 dez. 2024.

PARLAMENTO EUROPEU. *Shaping the Digital Transformation: EU Strategy Explained*. 2023. Disponível em: <https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained> Acesso em 03 dez. 2024.

PRESSE, F. Google pede desculpas por app de foto confundir negros com gorilas. *Portal de Notícias GI*. 02 jul. 2015. Disponível em: <https://g1.globo.com/tecnologia/noticia/2015/07/google-pede-desculpas-por-app-de-foto-confundir-negros-com-gorilas.html> Acesso em 19 dez. 2024

QUEIROZ, R. C. Z. A proteção de dados pessoais: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. 2021. Tese (Doutorado). Universidade de São Paulo, São Paulo, 2021. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-085834/en.php> Acesso em: 03 dez. 2024.

REN, Q.; DU, J. Harmonizing innovation and regulation: The EU Artificial Intelligence Act in the international trade context. *Computer Law & Security Review*, v. 54, n. 2024.

responsable de l'intelligence artificielle. 2017. Disponível em: <https://declarationmontreal-iaresponsable.com/la-declaration/> Acesso em 03 dez. 2024.

RUSSEL, S. Open letter on AI. *Berkeley Engineer Magazine*. 2015. Disponível em: <https://engineering.berkeley.edu/news/2015/11/open-letter-on-ai/> Acesso em: 03 dez. 2024.

S. et al (coord.). *Tratado de Proteção de Dados Pessoais*. 2 ed. Rio de Janeiro: Forense, 2023.
MORGAN, C.; TAYLOR, S. From Bricks to Clicks to AI – the next phase in business Evolution. *Harvard Business Scholl Publishing*. 2023. Disponível em: <https://hbr.org/sponsored/2023/11/from-bricks-to-clicks-to-ai-the-next-phase-in-business-evolution> Acesso em: 03 dez. 2024.

SAEIDNIA, H. R. Ethical artificial intelligence (AI): Confronting bias and discrimination in the library and information industry. *Library Hi Tech News*, 2023.

SARTOR, G.; LAGIOIA, F. The Impact of General Data Protection Regulation (GDPR) on artificial intelligence. Bélgica: European Parliamentary Research Service, 2020.

SHAO, Z. et al. Tracing the evolution of AI in the past decade and forecasting the emerging trends. *Expert Systems with Applications*, v. 209, 2022.

THOMSON REUTERS. Why AI still needs regulation despite impact. 1 feb. 2024. Disponível em <https://legal.thomsonreuters.com/blog/why-ai-still-needs-regulation-despite-impact/> Acesso em: 03 dez. 2024.

TOMASEVICIUS FILHOS, E. Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*, v. 30, n. 86, 2016. Disponível em: <https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN> Acesso em 19 dez. 2024.

UNIVERSITÉ DE MONTRÉAL. *La Déclaration de Montréal pour un développement*

US Congress. *H.R. 8152 – American Data Privacy and Protection Act*. 21 jun. 2022. Disponível em <https://www.congress.gov/bill/117th-congress/house-bill/8152> Acesso em 19 dez. 2024.

VARONA, D.; SUÁREZ, J. L. Discrimination, Bias, Fairness, and Trustworthy AI. *Applied Sciences*, v. 12, n. 5826, 2022.

VAZQUES, C. Q.; GOODWIN, M. What is artificial intelligence (AI) in business? *IBM*. 2024. Disponível em: <https://www.ibm.com/topics/artificial-intelligence-business> Acesso em: 03 dez. 2024.

White House. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. *Briefing Room: Presidential Actions*. 2023. Disponível

em: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> Acesso em: 03 dez. 2024.