Christine Albiani
Maria Clara Seixas
Organizadoras

ANAIS

III EDIÇÃO DO CONCURSO DE PAPERS SOBRE PROTEÇÃO DE DADOS PESSOAIS

FACULDADE BAIANA DE DIREITO

Editoração Eletrônica: Marília Borges
Diagramação: Jeferson de Jesus
Capa: Marília Borges

Editor Executivo:
Prof. Me. Fernando Caria Leal Neto

Conselho Editorial
Profª. Dra. Claudia Albagli Nogueira
Prof. Me. Diogo Assis Cardoso Guanabara
Prof. Dr. Gabriel Dias Marques da Cruz
Prof. Dr. Geovane de Mori Peixoto
Prof. Dr. Marcus Seixas Souza
Prof. Dr. Maurício Requião
Prof. Me. Roberto de Almeida Borges Gomes
Prof. Dr. Thiago Carvalho Borges

Rua José Peroba, 123, Costa Azul, Salvador/BA. CEP: 41.770-235.
Tel: 3205-7744
Copyright: Faculdade Baiana de Direito
publicacoes@faculdadebaianadedireito.com.br
http://www.faculdadebaianadedireito.com.br

Todos os direitos desta edição reservados a Faculdade Baiana de Direito e Gestão.
É terminantemente proibida a reprodução total ou parcial desta obra, por qualquer meio ou processo, sem a expressa autorização do autor, da Faculdade Baiana de Direito e Gestão. A violação dos direitos autorais caracteriza crime descrito na legislação em vigor, sem prejuízo das sanções civis cabíveis.

C744 Concurso de Papers Sobre Proteção de Dados Pessoais (3. : 2025 : Salvador)
Anais IIII Edição do Concurso de Papers Sobre Proteção de Dados Pessoais / organizadoras Christine Albiani, Maria Clara Seixas. – Salvador : Faculdade Baiana de Direito, 2025.
70 p.

Bibliografia.
Publicação digital (e-book) no formato PDF.
ISBN. 978-65-87051-13-0

1. Proteção de Dados. 2. Direito a Privacidade. I. Título.

CDD 342.0858

Ficha catalográfica elaborada pelo Setor de Processamento da Faculdade Baiana de Direito.

SUMÁRIO

APRESENTAÇÃO

É com enorme satisfação que publicamos os Anais da 3ª edição do Concurso de Papers sobre Proteção de Dados Pessoais da Faculdade Baiana de Direito. Foram meses de preparação para que o nosso alunado pudesse usufruir de um evento de alta qualidade técnica e organização.

Em sua 3ª edição, o Concurso de Papers teve como objetivo estimular as discussões sobre proteção e privacidade em nossa comunidade e a pesquisa e produção científica sobre o tema, como parte do Programa de Privacidade e Proteção de Dados da Faculdade Baiana de Direito e Gestão, dentro do pilar de conscientização e do fomento da cultura de privacidade na instituição.

Os trabalhos foram apresentados em formato de papers, um pequeno artigo científico, e avaliados pelas organizadoras Christine Albiani e Maria Clara Seixas, tendo sido apresentados durante o evento favorecendo o debate dos professores e alunos, um momento muito enriquecedor para todos os participantes.

Publicar os anais do 3º Concurso de Papers não apenas celebra o esforço e dedicação de todos os envolvidos, mas também abre portas para o aprofundamento contínuo do conhecimento e a troca de ideias sobre proteção de dados pessoais.

Os papers aqui reunidos representam valiosas contribuições científicas, que servirão de referência para futuras pesquisas e debates, beneficiando toda a comunidade acadêmica e profissional.

O TRATAMENTO DE DADOS PESSOAIS NA ANÁLISE DE DESEMPENHO: O USO RESPONSÁVEL DA IA COMO O PRESENTE E O FUTURO DO FUTEBOL BRASILEIRO

Thiago Antônio José Moreira Coêlho[1]

RESUMO

Essa dissertação, reconhecendo o papel da IA na análise de desempenho e na profissionalização do futebol brasileiro, visa a instigar o debate acerca do tratamento de dados dos atletas pelos clubes empregadores e da responsabilidade deste pelos danos causados, sem negligenciar, contudo, os interesses dos diversos envolvidos na indústria do futebol.

METODOLOGIA

A pesquisa tem natureza predominantemente qualitativa, consistindo em um levantamento bibliográfico, bem como do exame de dados colhidos da realidade e de legislações pertinentes, a exemplo do Código Civil e da Lei Geral de Proteção de Dados.

Palavras-chave: Dados pessoais; LGPD; tratamento de dados; análise de desempenho; futebol brasileiro.

Preleciona Jaime Barreiros Neto (2010) que o futebol é um esporte capaz de unir povos, produzir sonhos e desejos, gerar euforia e tristeza, impulsionar ou romper guerras e, também, um grande negócio. Hoje se costuma falar em uma "indústria do futebol" e isso não é por acaso. Enxergar o futebol moderno como mero entretenimento ou da mesma forma de outrora, negligenciando a importância do treinamento constante e do trabalho em equipe, é uma visão retrógada, estagnada e rasa. O futebol do século XXI é um esporte mais competitivo, que

1 Graduando em Direito pela Faculdade Baiana de Direito (8º semestre). Categoria: Graduando. Número da matrícula: 202110005.

exige da comissão técnica o ato de extrair o máximo dos seus atletas, e destes um compromisso tático ofensivo e defensivo incomparável na história.

Se por um lado o futebol se torna mais difícil, em uma sociedade cada vez mais interconectada e digital, não demorou muito para que os clubes enxergassem nas novas tecnologias meios de aperfeiçoamento técnico e tático e, como consequência, a importância de um departamento interno: o da análise de desempenho. E foi assim no Brasil. A implementação da tecnologia no futebol pátrio permite o monitoramento de diversos aspectos inerentes aos atletas, a exemplo da corrida nos treinos e durante as partidas, da frequência cardíaca, da impulsão do salto, da velocidade máxima atingida, da distância percorrida, do mapa de calor e da propensão a lesões (Clube Paineiras do Morumby, 2023).

O exercício de análise dos atletas é mais ou menos igual a um professor de academia. Quando o profissional observa a execução do exercício, ele já detecta vários pontos e tem em mente o que corrigir (Cotta, 2020). A análise de desempenho auxilia incisivamente em diversos momentos, a exemplo da melhor escalação para enfrentar o próximo adversário ou da definição do atleta que melhor atenda às carências do elenco, sendo a Inteligência Artificial um mecanismo que facilita o exercício dessa atividade, ainda mais ao se levar em conta o calendário tão apertado como o do futebol brasileiro (Cotta, 2020).

O uso da IA na análise de desempenho foi, como reconhece o técnico Abel Ferreira, um dos fatores determinantes para que o Palmeiras compreendesse as lacunas da equipe do Flamengo e montasse a melhor estratégia que lhe consagraria com o título da Copa Libertadores da América em 2021 (Ferreira, 2022). Não foi outro motivo senão o avanço tecnológico que fez com que o Bahia, já na gestão do Grupo City, desistisse da contratação do meio-campista Christian, do Athlético-PR, pois os seus exames, enviados para a Inglaterra, apontaram que o atleta poderia desenvolver novas lesões no joelho no lapso temporal de quatro ou cinco anos (Ecbahia.com, 2022).

A incorporação da IA na análise de desempenho no futebol brasileiro carrega consigo uma questão delicada a ser tutelada pelo Direito: o tratamento dos dados pessoais dos atletas que aqui atuam pelos clubes de futebol e pelas entidades de administração do desporto. É inegável que a inteligência artificial revolucionou a gestão de dados dos atletas e tem contribuído para a profissionalização do futebol canarinho, no entanto, torna-se crucial o tratamento responsável e transparente das informações coletadas (Meleras; Balsa, 2024). Nesse cenário, devem ser adotados mecanismos de segurança a fim de se evitar vazamentos, já que no ramo esportivo tal falha pode repercutir não somente em consequências judiciais e administrativas, mas também comerciais e financeiras, a exemplo da redução do valor de mercado de determinado atleta (Renatino; Chamelette; 2021)[2].

Destarte, as entidades de prática desportiva enquadram-se no rol disposto

2 O Bahia, aprendendo com os erros do passado, somente anuncia a contratação de jogador após a conclusão de todos os trâmites, sobretudo contratuais. Houve, no entanto, uma negligência quanto à situação envolvendo Christian e o consequente vazamento da informação a respeito dos exames médicos do atleta às mídias independentes. Embora seja difícil de cravar, é possível que o valor de mercado do atleta caia, principalmente no intervalo de quatro a cinco anos e em virtude do vazamento de informações que deveriam ter sido preservadas.

na LGPD[3], estando submetidas a esse diploma. Quanto à base legal que legitima o tratamento de dados dos atletas pelos clubes empregadores, a principal, é, sem dúvidas, o fornecimento do consentimento do titular (art. 7º I), mas há outras duas possíveis de se vislumbrar: a necessidade para a execução do contrato ou de procedimentos preliminares (art. 7º, IV) e a proteção da vida ou da incolumidade física do titular (prevenção e tratamento de lesões do titular) ou de terceiros (evitar a contaminação em série por Covid-19, por exemplo) – o que encontra correspondência no art. 7º, VII do diploma em exame. Vale lembrar que os dados pessoais relacionados à saúde do atleta são considerados sensíveis (art. 5º, II), requerendo, assim, um tratamento especial e ainda mais cauteloso nos ditames do art. 11, com destaque para os incisos I e II, "d" e "e"[4].

Nesse cenário, as entidades de prática desportiva brasileiras sujeitam-se aos princípios listados na LGPD, com ênfase para os da finalidade, adequação, necessidade e prevenção. O tratamento de dados pessoais que exceda essas finalidades ou não seja adequado/necessário para a continuidade do vínculo de emprego poderá culminar na responsabilização do clube empregador (Meleras; Balsa, 2024). O vazamento indevido de dados[5] pode acarretar a responsabilidade objetiva do controlador ou do operador, seguindo a lógica do Direito do Consumidor (Schreiber, 2021), embora comumente ambos os sujeitos se fundam na figura do clube empregador[6]. Essa mesma conclusão se daria ao levarmos em conta a relação de emprego e, portanto, a responsabilidade do empregador por danos ocasionados ao empregado, que é objetiva e admite o direito de regresso, seja com base no art. 932, III, CC ou no descumprimento de obrigações contratuais, em específico a proteção do empregado durante o contrato de trabalho (Schiavi, 2023).

Eis, então, o ponto mais delicado no que tange ao tratamento de dados pessoais dos atletas: o direito à privacidade. Isso porque são muitos os interessados nesses dados, como as federações de clubes, a mídia, os patrocinadores, as empresas de scouting, as casas de apostas e, claro, nós (torcedores) (Meleras; Balsa, 2024). Contam-nos Louis D. Brandeis e Samuel D. Warren (2024), em tradução feita por Maria Clara de Souza Seixas e Marcus Seixas Souza, que o objetivo de uma lei de proteção de dados é salvaguardar aqueles cujos assuntos a comunidade

3 Art. 3º, LGPD. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que (...).

4 Art. 11, LGPD. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...) d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei no 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; (...).

5 A preocupação com a gestão de dados no futebol também se dá a nível internacional. A FIFA adotou o seu próprio regulamento de proteção de dados, denominado Fifa Data Protection (2019), que, fixando diretrizes e princípios, se aplica a todas as associações-membro e às entidades a ela vinculadas, o que inclui os clubes brasileiros.

6 O art. 42 da LGPD expressa que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Além disso, o operador responde solidariamente quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador (§ 1º).

não detém um legítimo interesse, ou seja, a invasão injustificada da privacidade individual. Acontece que os próprios autores admitem que o mesmo conteúdo que pode ser de único interesse de determinado titular pode, no que tange a outro titular, ser igualmente importante aos seus concidadãos (Brandeis; Warren, 2024). Assim, peculiaridades que no "indivíduo comum" devem passar despercebidas pela comunidade adquirem status de matéria de legítima investigação pública em outro cenário.

Apesar de os autores citados utilizarem o exemplo dos políticos, a tese é igualmente aplicável aos atletas de futebol, sobretudo aos que disputam as divisões superiores, uma vez gozarem da condição de figuras públicas. Hoje, enquanto torcedor do Esporte Clube Bahia, tenho rápido acesso a informações sobre o mapa de calor, o número de passes, a quantidade de dribles completos, o tempo de recuperação da lesão de um atleta, mas o clube não me revelou, por exemplo, o conteúdo do laudo psicológico que motivou o tricolor a emprestar Diego Rosa para o futebol belga. Não é uma tarefa árdua entender os dados que podem ser publicizados e aqueles que devem ser mantidVos em sigilo, ou, mais ainda, aquilo que enquanto torcedor tenho o direito de saber daquilo que não se passa de uma mera curiosidade.

Embora recém-positivado na nossa Constituição (art. 5º, LXXIX), o direito à proteção de dados não pode ser concebido de forma absoluta, já que as informações pessoais estão inseridas em um corpo social igualmente digno de proteção (Mendes; Rodrigues Júnior; Fonseca, 2020). A limitação ao direito fundamental à proteção de dados pessoais exige, à luz do caso concreto, (I) uma base jurídica segura, (II) a clareza sobre a necessidade, adequação e proporcionalidade do tratamento de dados e (III) a adoção de providências preventivas mínimas que mitiguem os riscos de dano aos direitos de personalidade do titular (Mendes; Rodrigues Júnior; Fonseca, 2020).

A prevenção, no que tange ao tratamento de dados no ramo do futebol, em não raras ocasiões entra em colisão com a publicidade, princípio importante para a fiscalização e o controle externo (de torcedores e demais stakeholders[7]), ainda mais quando levamos em conta as gestões temerárias que assolam historicamente os clubes brasileiros. Resgatando os ensinamentos de Robert Alexy (2015), não vislumbro outra solução senão a ponderação *in concreto*, de modo que às vezes os anseios do público serão dignos de tutela e, em outras ocasiões, a privacidade do atleta será assegurada, pois, ainda que seja uma figura pública, isso não retira o seu direito à privacidade, mas apenas o relativiza em circunstâncias que tenham justificativa jurídica plausível.

7 A categoria "stakeholders" abrange todos os segmentos que influenciam e são influenciados pelas condutas de uma organização, a exemplo de clientes, imprensa, colaboradores, órgãos governamentais, fornecedores, acionistas, entre outros (Machado; Negrão, 2017).

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2015.

BARREIROS NETO, Jaime. **Direito Desportivo**. Curitiba: Juruá. 2010.

BRANDEIS, Louis D; WARREN, Samuel D. Tradução por: Maria Clara de Souza Seixas e Marcus Seixas Souza. O direito à privacidade. **Revista de Direito Civil Contemporâneo**. vol. 38. ano 11. p. 391-417. São Paulo: Ed. RT, jan./mar. 2024. Disponível em: https://www.ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/1418/1111. Acesso em: 08 set. 2024.

BRASIL. Lei 13.704, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. Brasília, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015 2018/2018/lei/l13709.htm. Acesso em: 05 set. 2024.

_____. Lei 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 08 set. 2024.

CLUBE PAINEIRAS DO MORUMBY. **Tecnologias no Esporte: Benefícios, Tendências e Exemplos**. 2023. Disponível em: https://clubepaineiras.org.br/tecnologias-no-esporte/. Acesso em: 08 set. 2024.

COTTA, Rafael. Aula ministrada no VI Curso de Gestão para o Futebol, Goiânia (Goiás), nov. 2020. Disponível em: IGoDD. Acesso em: 20 nov. 2020.

ECBAHIA.COM. **Bahia desiste da aquisição do volante Christian**. 2022. Disponível em: https://www.ecbahia.com/mercado/nao-vem-mais-bahia-desiste-da-aquisicao-do-volante- christian/. Acesso em: 08 set. 2024.

FERREIRA, Abel. **Cabeça Fria, Coração Quente: Uma viagem pelos bastidores da equipa técnica: segredos, reflexões e métodos de trabalho revelados em primeira pessoa**. São Paulo: Garoa Livros, 2022.

MACHADO; Guilherme Augusto Gonçalves; NEGRÃO, Daniel Lopes. O advogado corporativo e os stakeholders: o advogado e as relações institucionais e com a sociedade. *In*: PERUCCI; Felipe Falcone; LEITE, Márcio de Lima; MAIA, Maria Fernanda Menin, [et al] (org.). **Advocacia corporativa: reflexões e perspectivas**. 2ª ed. Belo Horizonte: D'Plácido, 2017.

MELERAS, Flavia; BALSA, Maria. **Importância da proteção dos dados pessoais dos jogadores de futebol**. 2024. Disponível em: https://www.conjur.com.br/2024-

ago- 04/importancia-da-protecao-dos-dados-pessoais-dos-jogadores-de-futebol/. Acesso em: 08 set. 2024.

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES; Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang [et. al] (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

RENATINO, Renato Santos; CHAMELETTE, Mariana. O tratamento de dados por entidades desportivas do futebol nacionais e internacionais: cuidados e benefícios. **Coluna Jusdesportiva do IBDD**. Rio de Janeiro: IBDD, 2021.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang [et. al] (coord.). **Tratado de Proteção de Dados Pessoais**. 1ª ed. Rio de Janeiro: Forense, 2021.

SCHIAVI, Mauro. **Curso de Direito do Trabalho**. 1ª ed. São Paulo: Juspodivm, 2023.

AS *DEEP FAKES* NO PERÍODO ELEITORAL: COMO A COOPERAÇÃO TÉCNICA ENTRE O TSE E A ANPD PODE CONTER AS AMEAÇAS DA IA AO SISTEMA DEMOCRÁTICO

Milla de Oliveira Gardasevic[1]

RESUMO

Este trabalho analisa as *deep fakes* no período eleitoral e os riscos que essas tecnologias apresentam ao sistema democrático[2]. Utilizando inteligência artificial para criar conteúdos falsos, as *deep fakes* impactam negativamente o processo eleitoral ao difundir desinformação e manipular a percepção pública. A pesquisa foca na parceria entre o TSE e a ANPD, avaliando como a aplicação conjunta da LGPD pode mitigar tais ameaças. Discute os desafios relacionados à identificação e responsabilização dos criadores desses conteúdos falsificados, além de enfatizar a necessidade de uma regulamentação mais clara para punir eleitores comuns[3] que participam dessas práticas. O trabalho destaca a relevância sociojurídica do tema, dado o crescente impacto dessas tecnologias . A pesquisa adota um viés bibliográfico e uma abordagem qualitativa, utilizando o método dedutivo-hipotético.

Palavras-chave: *deep fake*, **inteligência artificial, eleições, TSE, ANPD, LGPD, democracia, dados**

1 INTRODUÇÃO

A presente pesquisa aborda o fenômeno das *deep fakes* e suas implicações no

1 Graduanda em Direito pela Faculdade Baiana de Direito.

2 Para fins deste artigo, trataremos o Sistema Democrático em sentido estrito (oportunidade dos cidadãos de um Estado de participarem das decisões políticas com liberdade de iniciativa) extraído do Dicionário de Ciências Sociais, 2ª ed., FGV, 1987, p.316.

contexto eleitoral, com um foco particular na cooperação técnica entre o Tribunal Superior Eleitoral (TSE) e a Agência Nacional de Proteção de Dados (ANPD). As *deep fakes*, técnicas avançadas de manipulação de imagens e vídeos utilizando inteligência artificial (IA), têm o potencial de comprometer significativamente a integridade do processo democrático.

Este artigo examina como essas tecnologias dificultam a compreensão da verdade, evidenciando que, para mitigar esses riscos, a colaboração entre o TSE e a ANPD é essencial. A ameaça ao sistema democrático figura-se como problemática central e a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) como um desdobramento que salienta a necessidade de uma resposta coordenada. Como identificar os culpados? A quem responsabilizar? Quais são as sanções caíveis?

Destaca-se a relevância sociojurídica do tema, considerando que o impacto direto das *deep fakes* na manipulação de informações durante períodos eleitorais comprometem a percepção dos eleitores, ameaçam a estabilidade política e, consequentemente, a integridade das eleições. Para abordar a temática utilizou-se uma perspectiva bibliográfica e qualitativa, com método dedutivo-hipotético na análise das práticas de fiscalização e sua eficácia na preservação da democracia.

2 AS *DEEP FAKES* E O IMPACTO NO PERÍODO ELEITORAL: A IA COMO AMEAÇA AO SISTEMA DEMOCRÁTICO

Entende-se por *deep fake* uma técnica avançada de manipulação de mídia que utiliza algoritmos de IA para criar, alterar ou sintetizar vídeos e áudios de maneira hiper realista com base em dados biométricos (OMPI, 2022). No Brasil, esses dados são considerados sensíveis e, portanto, são protegidos pela LGPD, que impõe rigorosos controles sobre sua coleta e uso (ANPD, 2024).

No contexto eleitoral, as *deep fakes* podem ser exploradas para disseminar informações enganosas, manipular a percepção pública e influenciar o resultado das eleições de forma indevida. Assim, o Código Eleitoral em seu artigo 323 incrimina a conduta de "divulgar, na propaganda, fatos que sabe inverídicos [i.e., *fake news*]", em relação a partidos ou candidatos e capazes de exercerem influência perante o eleitorado (GOMES, 2020, p. 975).

A capacidade de criar vídeos falsificados que imitam com precisão o comportamento e a fala de candidatos conduz os eleitores a formarem opiniões baseadas em informações falsas (TSE, 2024). Além disso, a disseminação de *deep fakes* pode fomentar a desinformação e aumentar a polarização política, comprometendo a confiança pública no sistema eleitoral e na veracidade das informações apresentadas durante a campanha (NUNES e TRAUMANN, 2023, p.161).

William A. Galston (2020) entende que a IA pode distorcer a natureza do debate político, comprometendo princípios fundamentais do contexto eleitoral como a igualdade de informação e a transparência. O autor americano discorre que as *deep fakes* avançaram tanto, que o ditado "eu só acredito vendo" já não

3 Entendem-se por eleitores comuns, para fins deste artigo, os cidadãos que possuem o direito de voto e exercem esse direito nas eleições, sem ocupar cargos públicos ou funções específicas que os qualifiquem como eleitores de prerrogativa especial.

faz mais sentido, ante um cenário em que é impossível distinguir virtualmente o que é verídico ou não nos vídeos e áudios [Tradução própria].

Como resultado, a capacidade dos eleitores de tomar decisões ponderadas, com base em informações precisas, é gravemente comprometida, minando a eficácia do processo democrático. No contexto brasileiro, a problemática é particularmente preocupante, dada a vulnerabilidade do sistema eleitoral e ao histórico extenso de manipulação dos debates políticos (GOMES, 2020, p. 796).

Perceba-se que até o presente ponto da análise, não foram apontados especificamente os responsáveis pelas *deep fakes*. Isto porque estes podem ser tanto eleitores comuns quanto atores políticos envolvidos diretamente na manipulação de informações. O anonimato e a dificuldade de rastreamento agravam ainda mais o impacto das *deep fakes* no processo eleitoral, pois tornam a responsabilização e a aplicação de medidas corretivas mais complexas.

3 PARCERIA ENTRE ANPD E TSE NA APLICAÇÃO DA LGPD

A eficácia das ações para mitigar a ameaça das novas ferramentas de IA à democracia dependerão da capacidade dos órgãos responsáveis em enfrentar esses desafios e implementar estratégias robustas de fiscalização e controle. O Acordo de Cooperação Técnica nº 4/2021 firmado entre a ANPD e o TSE é vital para a garantia da integridade do processo eleitoral.

A LGPD estabeleceu um marco regulatório para o tratamento de dados pessoais e sensíveis, que se revela importantíssimo na luta contra as *deep fakes*, uma vez que essas tecnologias frequentemente utilizam dados biométricos, como expressões faciais e características físicas, para criar conteúdos falsificados. Os artigos 7º e 11 da LGPD, os quais abordam a necessidade de consentimento e a proteção de dados sensíveis, são especialmente relevantes para coibir o uso indevido de dados pessoais na criação e disseminação de *deep fakes*.

É nesse sentido que as Resoluções nº 23.732/2024 e nº 23.610/2019 do TSE proíbem expressamente o uso de *deep fakes* para prejudicar ou favorecer candidaturas, estipulando que conteúdos sintéticos não podem ser usados para difundir fatos inverídicos ou descontextualizados com o objetivo de causar danos ao equilíbrio do pleito.

As Resoluções supracitadas ainda conseguem complementar perfeitamente a LGPD no que tange à identificação dos responsáveis e a extensão da responsabilidade, pontos que foram levantados na Introdução do presente artigo. As tentativas de identificação dos culpados serão feitas pelas Agências de Checagem, e, uma vez identificados os controladores ou operadores, serão responsabilizados pelos danos decorrentes do uso indevido de dados conforme o art. 42 da LGPD.

Sendo identificados ou não os responsáveis subjetivamente, serão considerados solidariamente responsáveis, civil e administrativamente, os provedores e plataformas de *big techs*, quando não removerem imediatamente conteúdos e contas durante o período eleitoral (TSE, 2024). O artigo 46 da LGPD exige medidas de segurança para proteger dados pessoais, responsabilizando

as plataformas que não implementam controles adequados para impedir a disseminação de *deep fakes*.

Resta evidente o esforço dos órgãos para atuar de maneira colaborativa: uma vez identificados os responsáveis pela criação ou disseminação de *deep fakes*, as sanções previstas tanto pela ANPD quanto pelo TSE são severas.

A LGPD, em seu artigo 52, prevê desde advertências até multas que podem chegar a 2% do faturamento da empresa responsável, limitadas a R$ 50 milhões por infração, além da possibilidade de bloqueio ou eliminação dos dados envolvidos.

No contexto eleitoral, a Resolução nº 23.732/2024 do TSE estabelece sanções adicionais que podem afetar diretamente o candidato infrator, como a cassação do registro de candidatura ou mandato, conforme o impacto da *deep fake* na lisura do pleito. Essas medidas visam coibir o uso indevido de dados pessoais e tecnologias de IA com o propósito de manipular a opinião pública ou favorecer indevidamente candidatos.

Assim, apesar da ANPD e do TSE exercerem papéis fundamentais na aplicação dessas sanções, há uma lacuna significativa na regulamentação relacionada aos eleitores comuns que criam e disseminam *deep fakes* sem estarem diretamente envolvidos no processo eleitoral. Faltam mecanismos claros para punir adequadamente aqueles que, como eleitores, produzem ou compartilham esses conteúdos falsos, influenciando o pleito de maneira indevida. A ausência de normas específicas para esses casos pode enfraquecer os esforços de fiscalização e controle, uma vez que a responsabilidade se concentra majoritariamente nas partes diretamente ligadas à campanha eleitoral.

Outrossim, a atuação conjunta dos órgãos vai além da mera fiscalização, incluindo também a criação de diretrizes técnicas para orientar candidatos, partidos e plataformas sobre o uso correto dos dados, reforçando a necessidade de consentimento explícito, conforme o artigo 7º da LGPD.

Vale menção ao artigo 18 da LGPD, que garante aos titulares de dados o direito de solicitar a correção ou exclusão de dados incorretos ou inadequados. No contexto da eleição, aqueles que tiverem seus dados violados e afetados por *deep fakes* podem invocar esse dispositivo para requerer judicialmente a remoção do conteúdo manipulado e a reparação dos danos causados, com o apoio do TSE e da ANPD na implementação dessas medidas.

Em suma, o TSE, ao garantir a lisura do processo eleitoral, pode, com o apoio técnico da ANPD, monitorar o cumprimento da LGPD e prevenir que o uso indevido de IA comprometa a igualdade de oportunidades nas campanhas eleitorais.

4 CONSIDERAÇÕES FINAIS

Diante do exposto, torna-se evidente que as *deep fakes* representam uma séria ameaça ao processo eleitoral, comprometendo a transparência e a igualdade nas campanhas. A parceria entre o TSE e a ANPD mostra-se essencial para enfrentar os desafios impostos por essas tecnologias, garantindo que as normas

da LGPD sejam aplicadas de maneira eficaz e que os dados pessoais sejam devidamente protegidos.

Ainda que as medidas atuais sejam um passo importante na regulação do uso de IA nas eleições, persiste a necessidade de aprimorar a responsabilização dos eleitores comuns que produzem e disseminam *deep fakes*. Somente com uma regulamentação abrangente e com a cooperação contínua entre os órgãos de fiscalização será possível manter a integridade do sistema democrático.

Além disso, é crucial fortalecer as ferramentas de monitoramento e rastreamento das *deep fakes*, de modo a facilitar a identificação dos responsáveis, sejam eles atores políticos ou eleitores comuns. A criação de normas mais detalhadas para punir aqueles que, mesmo não envolvidos diretamente nas campanhas, manipulam o processo eleitoral por meio da desinformação, se faz urgente. Somente com uma abordagem mais rigorosa e abrangente será possível minimizar os impactos dessas práticas e assegurar um ambiente eleitoral mais justo e transparente.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Radar Tecnológico: Biometria**. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf . Acesso em: 05 set. 2024.

BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins. **Estudos sobre LGPD – Lei Geral de Proteção de Dados – Lei nº 13.709/2018: Doutrina e Aplicabilidade no Âmbito Laboral**. 2022.

SILVA, Benedicto (org.). **Dicionário de Ciências Sociais**. 2. ed. Rio de Janeiro: Fundação Getúlio Vargas, 1987.

BRASIL. Lei nº 4.737, de 15 de julho de 1965. Código Eleitoral. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm . Acesso em: 07 set. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 07 set. 2024.

BRASIL. Resolução nº 23.610, de 18 de dezembro de 2019. Tribunal Superior Eleitoral (TSE). Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019 . Acesso em: 11 set. 2024.

BRASIL. **Resolução nº 23.732, de 27 de fevereiro de 2024.** Tribunal Superior Eleitoral (TSE), 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024 . Acesso em: 08 set. 2024.

GALSTON, William A. **Is seeing still believing? The deepfake challenge to truth in politics.** Brookings, Washington D.C., vol. 2020, jan. 2020. Disponível em: https://www.brookings.edu/articles/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/ . Acesso em: 07 set. 2024.

GOMES, José Jairo. **Direito eleitoral**. São Paulo: Atlas, 2020.

MALDONADO, Viviane Nobrega; BLUM, Renato Opice (coords.). **LGPD: Lei Geral de Proteção de Dados omentada**. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

NUNES, Felipe; TRAUMANN, Thomas. **Biografia do abismo: como a polarização divide famílias, desafia empresas e compromete o futuro do Brasil.** São Paulo:

HarperCollins Brasil, 2023.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL (OMPI). **Inteligência artificial: os deepfakes na indústria do entretenimento.** Revista da OMPI, Genebra, junho de 2022. Disponível em: https://www.wipo.int/wipo_magazine/pt/2022/02/article_0003.html . Acesso em: 09 set. 2024.

RAMAYANA, Marcos. **Direito Eleitoral**. Niterói: Impetus, 2011.

RIEGER, Poliene. **A desinformação e eleições movida a dados: uma ameaça ao sistema democrático e a direitos humanos fundamentais no contexto brasileiro**. Instituto de Direito Público de Brasília (IDP). 2024. Disponível em: http://trabalhoscidhcoimbra.com/ojs/index.php/anaiscidhcoimbra/article/view/59 . Acesso em: 09 set. 2024.

TRIBUNAL SUPERIOR ELEITORAL. **Acordo de cooperação técnica TSE/ANPD LGPD em 23.11.2021**. Brasília, 2021. Disponível em: https://www.tse.jus.br/comunicacao/noticias/arquivos/acordo-de-cooperacao-tecnica-tse-anpd-lgpd-em-23-11-2021/@@download/file/TSE-acordo-cooperacao-tecnica-anpd-lgpd.pdf . Acesso em: 08 set. 2024.

TRIBUNAL SUPERIOR ELEITORAL. **TSE firma acordos para combater discursos de ódio, "deepfakes" e desinformação eleitoral.** Brasília, 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Marco/tse-firma-acordos-para-combater-discursos-de-odio-deepfakes-e-desinformacao-eleitoral?SearchableText=deepfakes . Acesso em: 07 set. 2024.

VIEIRA DE SOUSA, Gustavo; CARVALHO, Isabella Maria Farias. **Análise setorial dos impactos da LGPD no Brasil - Aplicação da LGPD no Direito Eleitoral**. Anuário do Observatório da LGPD da Universidade de Brasília, 2022. Disponível em: https://lirias.kuleuven.be/retrieve/749672#page=116 . Acesso em: 08 set. 2024.

A SOCIEDADE DE VIGILÂNCIA E A PROTEÇÃO DE DADOS SOCIAIS: IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA PRIVACIDADE COLETIVA

Matheus Lobão Costa Caires Novaes

O método de pesquisa utilizado foi o hipotético-dedutivo, baseado nas ideias de Karl Popper. Nesse método, as premissas não são consideradas verdades absolutas. As hipóteses são testadas em diferentes cenários, procurando soluções por meio de tentativas e eliminação de erros. As conclusões resultam da validação das hipóteses mais adequadas para o problema, com o objetivo de gerar o convencimento.

A preocupação com a proteção de dados pessoais é uma característica marcante das sociedades modernas, onde a informação assume um papel central em diversos aspectos da vida humana, desde as relações pessoais até questões políticas, econômicas e sociais. Segundo Laborit, citado por Lojkine, a informação "não é nem matéria nem energia (...) em si, ela é imaterial, representando 'algo que faz com que o todo seja mais do que a soma das partes'" (Lojkine, 2002, p. 113). As tecnologias, por sua vez, permitem não apenas controlar e manipular a informação, mas também transformá-la e utilizá-la para criar novos conhecimentos e produtos. Castells ressalta que, no novo modo informacional de desenvolvimento, a produtividade está fundamentada nas tecnologias de geração de conhecimento, processamento de informações e comunicação de símbolos (Castells, 1999, p. 53-54). Embora o conhecimento sempre tenha sido vital para o desenvolvimento, o que distingue o atual contexto é a aplicação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade, estabelecendo um ciclo contínuo de inovação.

Nesse cenário, a Sociedade da Informação emerge, com a aplicação crescente de tecnologias para processar informações e gerar novos saberes. Isso reforça a importância da proteção de dados pessoais, que ganha reconhecimento jurídico, inclusive nas categorias de direitos humanos e direitos fundamentais. Dados pessoais, que consistem em informações capazes de identificar indivíduos de maneira direta ou indireta, são tratados com especial cuidado. Quando

relacionados a aspectos como ideologia, religião, crença, raça ou saúde, esses dados são considerados sensíveis, exigindo uma proteção ainda mais rigorosa (Lojkine, 2002, p. 113; Castells, 1999, p. 53-54).

A crescente integração entre dados pessoais e o avanço das tecnologias de Inteligência Artificial (IA) tem provocado mudanças profundas na forma como a sociedade encara questões de privacidade e controle da informação. O jurista italiano Stefano Rodotà alerta que o uso indiscriminado da internet, aliado à coleta massiva de dados pessoais e à interconexão entre diferentes bancos de dados, resulta em uma sociedade cada vez mais pautada pelo controle e vigilância. Segundo Rodotà, essa "sociedade da informação" não apenas coloca em risco a privacidade individual, mas também afeta a privacidade coletiva, ao promover uma rede global de vigilância que atravessa fronteiras e ameaça a proteção de direitos fundamentais, como a autonomia e a privacidade (Rodotà, 2008, p. 146).

Contudo, a utilização da IA amplifica ainda mais essa realidade, processando grandes quantidades de dados e permitindo a criação de perfis detalhados de indivíduos e grupos. As implicações disso vão além da esfera pessoal. A sociedade de vigilância descrita por Rodotà emerge como um contexto no qual a privacidade coletiva se esvai, enquanto os dados sociais aqueles originados das interações e comportamentos coletivos são submetidos a monitoramento constante. Esse quadro levanta questões éticas e jurídicas essenciais sobre os limites da vigilância algorítmica e a necessidade de repensar a proteção dos dados sociais. Há uma demanda crescente por uma revisão dos marcos regulatórios que controlam o uso dessas tecnologias. (Rodotà, 2008, p. 146)

O problema central reside no fato de que, ao intensificar a vigilância em massa, a IA compromete não só a privacidade individual, mas também as liberdades coletivas. A capacidade de classificar e monitorar grandes grupos por meio de algoritmos avançados e bancos de dados reforça o que Rodotà descreve como uma tendência irreversível, presente em muitos países (Rodotà, 2008, p. 147). Diante desse novo panorama, torna-se crucial refletir sobre as consequências desse modelo de vigilância para a privacidade tanto individual quanto coletiva, que corre o risco de sofrer transformações irreversíveis.

Byung-Chul Han, filósofo sul-coreano, introduz o conceito de um "pan-óptico digital", caracterizado por uma aparente liberdade e comunicação ilimitada, onde "a transparência e a informação substituem a verdade" (Han, 2018b, p. 56). Para Han, "o novo objetivo do poder não consiste na administração do passado, mas no controle psicopolítico do futuro" (Han, 2018b, p. 56). Essa forma de vigilância digital se distingue do conceito do Grande Irmão de Jeremy Bentham e George Orwell. Enquanto no pan-óptico digital as pessoas não se percebem vigiadas ou ameaçadas, sentindo-se livres, Han ressalta que essa sensação de liberdade é, na verdade, ilusória e mais perigosa do que o modelo de controle explícito retratado por Orwell. "É exatamente essa sensação de liberdade, inexistente no Estado de vigilância de Orwell, que constitui um problema" na sociedade digital (Han, 2018, p. 57).

Para entender melhor a comparação de Han, é importante revisitar a figura do Big Brother criada por George Orwell em seu famoso romance 1984. O Big

Brother representa uma autoridade totalitária que exerce controle absoluto sobre os cidadãos, não apenas monitorando cada movimento e palavra, mas também manipulando a verdade e moldando a percepção da realidade. No mundo de Orwell, o medo da vigilância constante é tangível; as pessoas sabem que estão sendo observadas o tempo todo, o que as condiciona a um comportamento conformista e submisso. A ameaça de punição e o controle da memória onde até o passado é reescrito para atender aos interesses do governo definem a relação entre o Estado e o indivíduo. (Han, 2018, p. 57).

Ao contrário disso, Han sugere que, na sociedade digital moderna, o controle não precisa ser tão explícito. O poder se exerce de maneira mais sutil e psicológica, pois as pessoas, sob a ilusão de liberdade e transparência, voluntariamente compartilham informações, permitindo que o sistema as monitore e controle sem a necessidade de coerção visível. O "pan-óptico digital" que Han descreve é, portanto, ainda mais eficaz que o Big Brother de Orwell, pois a sensação de liberdade encobre a verdadeira extensão da vigilância e do controle. (Han, 2018, p. 57).

Dados é informação, informação é poder, e isso pode ser usado amplamente por países, segundo grandes canais de mídia, levando em conta chefes de governo como do Canadá e dos Estados Unidos que acusam da apropriação de dados por parte de redes sociais chinesas. (Infomoney, 2023)

O chefe do Serviço de Inteligência da Segurança do Canadá, David Vigneault, alertou os cidadãos sobre os riscos de usar o TikTok, afirmando que os dados dos usuários podem ser acessados pelo governo chinês. Em entrevista à CBC, Vigneault destacou que a China tem uma estratégia clara para coletar informações pessoais globalmente. O Canadá está revisando uma proposta do TikTok para expandir suas operações no país, e Vigneault participará desse processo. Nos EUA, o TikTok e sua controladora, ByteDance, estão desafiando uma lei sancionada por Joe Biden que exige o desinvestimento da empresa chinesa na plataforma por razões de segurança nacional, com o prazo final de janeiro de 2025 para cumprimento, sob risco de banimento do aplicativo nos EUA. (Infomoney, 2023)

Em 2018, a Cambridge Analytica foi acusada de coletar e utilizar dados de milhões de usuários do Facebook sem consentimento, gerando um grande escândalo que expôs como a manipulação de dados pessoais pode influenciar decisões políticas e democráticas. A empresa britânica, que atuou em campanhas como o Brexit e as eleições presidenciais dos EUA em 2016, desenvolveu estratégias baseadas em testes de personalidade, direcionando mensagens personalizadas para manipular a opinião pública. (The Guardian, 2018)

Esses dados, coletados sem o consentimento adequado, permitiram que a Cambridge Analytica criasse perfis detalhados dos eleitores, influenciando suas escolhas políticas por meio de campanhas personalizadas, muitas vezes sem que os indivíduos percebessem que estavam sendo alvos de manipulação. A coleta foi inicialmente realizada através de um teste de personalidade criado pelo professor Aleksandr Kogan, que também acessava dados de amigos dos participantes, sem que eles soubessem. (The Guardian, 2018)

O caso veio à tona após denúncias de Christopher Wylie, um ex-funcionário

da empresa, que revelou como a Cambridge Analytica usou esses dados de forma estratégica para influenciar grandes eventos políticos. Esse episódio levantou questões sobre o uso de dados pessoais na política, apontando para a vulnerabilidade das democracias frente a esse tipo de manipulação e a necessidade de regulação para evitar novos abusos que possam distorcer a vontade popular. (The Guardian, 2018)

Ou seja, com dados e com a publicidade certa podemos derrubar ou instaurar governos, por isso essa grande preocupação por parte das potências ocidentais em relação a China, já que nossos dados que fornecemos as Inteligências artificiais, diariamente, são de uma preciosidade incalculável.

Uma solução eficaz para enfrentar os desafios apresentados pela vigilância massiva e pela manipulação de dados pessoais seria a criação de marcos regulatórios globais mais robustos, focados na proteção da privacidade individual e coletiva. Essas regulamentações deveriam estabelecer normas claras sobre a coleta, processamento e compartilhamento de dados, impondo responsabilidades às empresas e governos que fazem uso de informações pessoais. Além disso, é crucial promover maior transparência sobre o uso de tecnologias como a inteligência artificial, exigindo consentimento explícito dos usuários para qualquer tipo de tratamento de seus dados, especialmente no caso de dados sensíveis.

A colaboração internacional seria fundamental para garantir a harmonização dessas regras e evitar a exploração de lacunas jurídicas por empresas ou governos em diferentes países. O fortalecimento de órgãos reguladores e a aplicação de sanções rigorosas contra o uso indevido de dados pessoais também são medidas essenciais para mitigar o impacto da vigilância. Paralelamente, a conscientização pública sobre os riscos e a importância da privacidade digital deve ser promovida, incentivando a sociedade a adotar práticas mais seguras no compartilhamento de informações online. Assim, seria possível equilibrar os avanços tecnológicos com a proteção de direitos fundamentais, como a privacidade e a autonomia.

Por isso a importância do estudo de casos, com o direito comparado e uma análise profunda da nossa própria LGPD, e as normas de direito internacional, sendo um assunto recente, principalmente com a realidade brasileira, sendo um pais pacifico, porém com grande relevância social, não tendo muita jurisprudências sobre, é importante já ter um preparo prévio sobre a temática.

REFERÊNCIAS

THE GUARDIAN. Cambridge Analytica: how did it turn clicks into votes? The Guardian, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook- influence-us-election. Acesso em: 12 set. 2024.

INFOMONEY. Inteligência canadense alerta que China pode usar TikTok para espionar usuários. Infomoney, 23 ago. 2023. Disponível em: https://www.infomoney.com.br/mundo/inteligencia-canadense-alerta-que-china-pode- usar-tiktok-para-espionar-usuarios/. Acesso em: 12 set. 2024.

HAN, Byung-Chul. What Is Power? Cambridge: Polity Press, 2018.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

LOJKINE, Jean. A revolução informacional. Tradução de José Paulo Netto. 3 ed. São Paulo: Cortez, 2002.

CASTELLS, Manuel. A sociedade em rede. A era da informação: economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. 7 ed. São Paulo: Paz e Terra, 1999.

OS PROBLEMAS NO ACESSO ÀS POLÍTICAS REFERENTES AO TRATAMENTO DOS DADOS PESSOAIS

Ana Sofia Medina Gazineo

METODOLOGIA

A pesquisa, que serviu de base para elaboração do paper, adotou uma abordagem qualitativa, utilizando métodos de análise documental e pesquisa survey para investigar como as políticas de privacidade de aplicativos populares são apresentadas e compreendidas pelos usuários. Primeiramente, foi realizada uma análise de conteúdo das políticas de privacidade de 10 aplicativos amplamente utilizados, incluindo WhatsApp, Instagram, TikTok e Gmail, com base na complexidade da linguagem, extensão dos textos e acessibilidade. A análise procurou identificar padrões em relação ao cumprimento dos princípios da Lei Geral de Proteção de Dados (LGPD), como a transparência e o livre acesso à informação. Além disso, foi aplicada uma pesquisa de opinião com 200 usuários de diferentes faixas etárias, a fim de avaliar o nível de compreensão e de leitura das políticas de privacidade desses aplicativos. A pesquisa também incluiu perguntas sobre a percepção dos participantes sobre a clareza das informações e sua disposição para consentir com os termos de uso sem lê-los completamente. A análise dos dados qualitativos foi feita por meio da técnica de análise de conteúdo, enquanto os dados quantitativos foram analisados utilizando estatísticas descritivas para verificar padrões de compreensão e consentimento.

1 INTRODUÇÃO

Segundo a Lei Geral de Proteção de Dados, todos devem ter acesso à política de privacidade de aplicativos, sites ou serviços que utilizam de seus dados pessoais, porém na realidade o que as empresas têm feito é afastar seus clientes dessa realidade, pois mesmo que na teoria respeitem os princípios da lei - como o livre acesso e a transparência - acabam dificultando a compreensão e acesso a

essas informações na forma que é exposta a política de privacidade.

2 DESENVOLVIMENTO

Apesar de muitos controladores de dados afirmarem estar em conformidade com a Lei Geral de Proteção de Dados (LGPD) ao tornar suas políticas de privacidade acessíveis, a realidade é que a compreensão desses documentos ainda é um desafio. Muitas vezes, as políticas de privacidade são apresentadas em linguagem complexa e textos extensos, dificultando a leitura e o entendimento. Exemplos notáveis incluem aplicativos populares como WhatsApp, TikTok, Instagram e Gmail, que possuem termos de uso e políticas de privacidade extensas. O Microsoft Teams, por exemplo, foi apontado em uma pesquisa realizada em 2020 como tendo a maior quantidade de palavras em suas políticas e termos de serviço comparado a outros aplicativos.

Pesquisas realizadas pelo Thinkmoney e pela Deloitte em 2020 destacam essa problemática. Constatou-se que 90% dos britânicos e 91% dos americanos consentem com termos e condições sem ler o conteúdo completo. A pesquisa revelou que a extensão dos documentos é um fator crítico; por exemplo, os 13 aplicativos mais populares da época somavam 128.415 palavras, o dobro da maior parte dos livros de ficção, e levaria aproximadamente 17 horas para uma leitura completa.

Essa realidade explica por que muitos indivíduos não leem os termos e condições, o que pode resultar em consequências graves, como a divulgação inadvertida de dados ou a coleta de informações indesejadas. Muitas vezes, os usuários têm uma falsa impressão de que sabem quais dados serão solicitados, mas acabam surpreendidos por solicitações inesperadas, como acesso a imagens de outros aplicativos ou histórico de navegação. A política de privacidade deve informar sobre a coleta desses dados, mas, se não for lida e compreendida, os usuários não conseguem controlar suas informações pessoais ou reivindicar seus direitos caso haja violação dos princípios estabelecidos no Art. 6º da LGPD. Estes princípios incluem: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilidade e prestação de contas. Somente com conhecimento desses princípios é que os titulares podem fiscalizar e exigir conformidade.

Além disso, a linguagem utilizada nas políticas de privacidade e termos de uso frequentemente não é acessível, dificultando ainda mais a compreensão dos leitores. Esse problema é agravado quando o nível de leitura necessário para entender os documentos é superior à idade permitida para o uso do aplicativo ou site. Isso é especialmente preocupante no contexto do tratamento de dados de crianças, uma vez que o Art. 14 da LGPD exige que as informações sejam adequadas ao entendimento infantil e que o consentimento dos responsáveis seja específico e em destaque. No entanto, muitas vezes as informações não são apresentadas de forma adequada, e a fiscalização do consentimento de crianças é deficiente, permitindo que crianças forneçam consentimento se passando por seus responsáveis.

3 CONCLUSÃO

Para resolver essas questões, as empresas devem adotar métodos mais acessíveis e compreensíveis para a exposição de suas políticas de privacidade. Isso pode incluir o uso de formatos audiovisuais ou outros meios dinâmicos que facilitem a compreensão. Um exemplo positivo é a easyJet, que utiliza vídeos explicativos sobre processos de viagem e termos de privacidade, tornando o acesso e entendimento mais simples e menos demorado. Com essas mudanças, o controle dos titulares sobre seus próprios dados se tornará mais eficaz, e a conscientização sobre as informações relacionadas à privacidade aumentará consideravelmente.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2020.

CAKEBREAD, Caroline. You're not alone, no one reads terms of service agreements. *Business Insider*, 2017. Disponível em: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T. Acesso em: 13 set. 2024.

FAYE, (nome completo não identificado). What Does Your Phone Know About You?. *Thinkmoney*, 2020. Disponível em: https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/. Acesso em: 13 set. 2024.

EASYJET PORTUGAL. Política de Privacidade easyJet. *easyJet Portugal*, 2017. Disponível em: https://youtu.be/HLimolOg0lo?si=bsMfwjfU3nuNrGBp. Acesso em: 13 set. 2024.

KLEINMAN, Zoe. Popular app T&C 'longer than Harry Potter. *BBC*, 2020. Disponível em: https://www.bbc.com/news/technology-54838978. Acesso em: 13 set. 2024.

COHEN, Jason. It would take 17 hours to read the terms & conditions of the 13 most popular apps. *PCMag UK*, 2020. Disponível em: https://uk.pcmag.com/security/130336/it-would-take-17-hours-to-read-the-terms-conditions-of-the-13-most-popular-apps. Acesso em: 13 set. 2024.

TELLES, Fernando. 90% das pessoas não leem termos e condições de apps, revela estudo. *SHOWMETECH*, 2023. Disponível em: https://www.showmetech.com.br/pessoas-nao-leem-termos-e-condicoes-de-apps/. Acesso em: 13 set. 2024.

A CONFLITANTE RELAÇÃO ENTRE A ADI 7276 E OS PRINCÍPIOS DA LGPD

Carlos Henrique Krempser Batista Neves

A Ação Direta de Inconstitucionalidade (ADI) 7276, ajuizada perante o Supremo Tribunal Federal (STF), questiona a constitucionalidade de normas que permitem a quebra de sigilo bancário e fiscal. Essa ação levanta questões significativas sobre como tais normas interagem com os princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Instituída pela Lei nº 13.709/2018, a LGPD estabelece diretrizes rigorosas para o tratamento de dados pessoais, com o objetivo de garantir a proteção e a privacidade dos indivíduos.

Nesse contexto, é fundamental analisar como as normas que autorizam a quebra de sigilo podem entrar em conflito com os preceitos da LGPD, especialmente em relação aos princípios de finalidade e necessidade. O Plenário do STF, em uma decisão tomada na sessão virtual encerrada em 6 de setembro de 2024, validou, por maioria, as regras de convênio do Conselho Nacional de Política Fazendária (Confaz). Essas regras obrigam as instituições financeiras a fornecerem informações aos estados sobre pagamentos e transferências realizados por clientes — tanto pessoas físicas quanto jurídicas — em operações eletrônicas, como Pix, cartões de débito e crédito, quando houver recolhimento do ICMS.

A decisão da ADI 7276 destaca a tensão entre a necessidade de medidas de fiscalização e os direitos de proteção de dados pessoais, enfatizando a importância de equilibrar os requisitos de transparência fiscal com o respeito à privacidade dos indivíduos.

PRINCÍPIOS DA LGPD E QUEBRA DE SIGILO

A Lei Geral de Proteção de Dados (LGPD) é fundamentada em princípios que visam garantir a proteção e a privacidade dos dados pessoais dos indivíduos. Entre os principais princípios da LGPD estão a finalidade, adequação, necessidade e segurança dos dados pessoais.

O princípio da finalidade estipula que os dados pessoais devem ser coletados e utilizados exclusivamente para propósitos específicos e legítimos, os quais devem ser claramente informados ao titular dos dados no momento da coleta. Ou seja, os dados não podem ser utilizados para finalidades diferentes daquelas para as quais foram originalmente obtidos. Nesse contexto, a quebra de sigilo bancário e fiscal, por sua natureza intrinsecamente invasiva, pode ser vista como uma possível violação deste princípio. A divulgação de informações sensíveis, sem um alinhamento claro e justificado com os propósitos legítimos para os quais os dados foram inicialmente coletados, pode comprometer a integridade dos princípios da LGPD.

Adicionalmente, o princípio da necessidade estabelece que apenas os dados estritamente necessários para atingir o propósito específico devem ser coletados e tratados. Esse princípio busca evitar o tratamento de dados excessivos e assegurar que somente a quantidade mínima de informação necessária para cumprir o objetivo declarado seja utilizada. A quebra de sigilo pode resultar na coleta e no tratamento de dados além do que é estritamente necessário, o que pode ser considerado uma violação desse princípio. Ao expandir o escopo de dados acessados ou utilizados para além do inicialmente previsto, a privacidade dos indivíduos pode ser comprometida, contradizendo os preceitos da LGPD.

Em suma, tanto a finalidade quanto a necessidade são princípios centrais da LGPD que buscam proteger a privacidade e garantir a segurança dos dados pessoais. Qualquer prática que envolva a quebra de sigilo e a subsequente divulgação de informações sensíveis deve ser cuidadosamente avaliada para assegurar que não haja uma violação desses princípios, protegendo assim os direitos dos titulares de dados e mantendo a conformidade com a legislação.

IMPACTO DA ADI 7276 SOBRE OS PRINCÍPIOS DA LGPD E A QUEBRA DE SIGILO

A decisão do Supremo Tribunal Federal (STF) na Ação Direta de Inconstitucionalidade (ADI) 7276, que validou as normas do Conselho Nacional de Política Fazendária (Confaz) para a quebra de sigilo bancário e fiscal, ilustra um ponto crucial de tensão entre a legislação fiscal e a Lei Geral de Proteção de Dados (LGPD). Ao exigir que as instituições financeiras forneçam informações detalhadas sobre operações eletrônicas que envolvem o ICMS, a decisão reafirma a necessidade de transparência e controle fiscal. No entanto, essa exigência levanta questões significativas sobre a compatibilidade com os princípios da LGPD, particularmente os princípios da finalidade e da necessidade.

Primeiramente, o princípio da finalidade da LGPD estabelece que dados pessoais devem ser coletados e utilizados exclusivamente para propósitos específicos e previamente informados ao titular. A quebra de sigilo, ao permitir o acesso a dados bancários e fiscais para fins de fiscalização e controle tributário, pode gerar preocupações sobre se tais dados estão sendo utilizados de acordo com os propósitos para os quais foram originalmente coletados. Por exemplo, se informações detalhadas sobre transações financeiras são usadas para verificar o cumprimento fiscal, pode haver uma dúvida sobre se essa utilização está

claramente alinhada com os objetivos legítimos informados aos clientes no momento da coleta dos dados.

Além disso, o princípio da necessidade determina que apenas os dados estritamente necessários para o propósito declarado devem ser tratados. A coleta de informações extensivas sobre todas as operações financeiras que envolvem ICMS pode ser questionada sob a ótica da necessidade. Por exemplo, se dados pessoais são coletados e analisados em um volume muito amplo, isso pode ser visto como um tratamento excessivo de dados, que vai além do necessário para o cumprimento das obrigações fiscais. A necessidade de garantir que apenas a quantidade mínima de dados seja usada para alcançar o objetivo específico é crucial para proteger a privacidade dos indivíduos.

Portanto, o impacto da decisão ressalta a complexidade de equilibrar as exigências fiscais com os direitos à proteção de dados pessoais. A ADI 7276 evidencia como a aplicação das normas de quebra de sigilo pode desafiar os princípios da LGPD, exigindo um ajuste cuidadoso entre a necessidade de transparência fiscal e a proteção da privacidade dos indivíduos.

INTERSEÇÃO ENTRE NORMAS CONSTITUCIONAIS E PROTEÇÃO DE DADOS

A questão central da ADI 7276 é a compatibilidade entre as normas que permitem a quebra de sigilo e os princípios da LGPD. A Constituição Federal garante a inviolabilidade do sigilo bancário e fiscal, exceto em casos específicos, como investigações judiciais e fiscais. No entanto, a LGPD adiciona uma camada adicional de proteção, exigindo que qualquer tratamento de dados pessoais, incluindo aqueles obtidos por meio da quebra de sigilo, esteja em conformidade com seus princípios.

POSSÍVEIS CONFLITOS E SOLUÇÕES

Um dos principais conflitos é a tensão entre o direito à privacidade e a necessidade de investigação e controle fiscal. A quebra de sigilo, embora legítima para fins de investigação e combate à ilegalidade, deve ser realizada com cautela para não infringir os direitos à proteção de dados pessoais estabelecidos pela LGPD.

Uma solução para esse conflito pode ser a harmonização das normas, garantindo que a quebra de sigilo seja realizada de acordo com os princípios da LGPD. Isso pode incluir a definição clara dos limites para o tratamento de dados pessoais e a implementação de medidas adicionais de proteção para garantir que a quebra de sigilo não resulte em um tratamento inadequado ou excessivo dos dados.

CONCLUSÃO

A análise da Ação Direta de Inconstitucionalidade (ADI) 7276 revela a complexa interseção entre as normas que permitem a quebra de sigilo bancário e

fiscal e os princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD). A decisão do Supremo Tribunal Federal (STF) ressalta uma tensão crítica entre a necessidade de transparência e controle fiscal e os direitos fundamentais à privacidade e proteção de dados pessoais. A LGPD impõe princípios rigorosos que visam garantir que dados pessoais sejam tratados com a máxima responsabilidade, respeitando a finalidade e a necessidade do tratamento.

A validação das regras do Conselho Nacional de Política Fazendária (Confaz) para a quebra de sigilo, conforme decidido pelo STF, levanta importantes questões sobre a compatibilidade desses procedimentos com os princípios da LGPD. A quebra de sigilo pode resultar em tratamento excessivo de dados, colocando em risco a privacidade dos indivíduos e potencialmente violando os preceitos da finalidade e da necessidade estabelecidos pela LGPD. Assim, embora a transparência fiscal seja crucial para a eficácia das políticas tributárias, é essencial que essa transparência não ocorra à custa dos direitos de proteção de dados pessoais.

A solução para esses conflitos reside na harmonização cuidadosa das normas que regulam a quebra de sigilo com os princípios da LGPD. É necessário garantir que qualquer medida de quebra de sigilo seja estritamente necessária e proporcional, com limites bem definidos para o tratamento de dados e robustas medidas de proteção. Dessa forma, é possível assegurar que as práticas fiscais e investigativas estejam em conformidade com a proteção dos dados pessoais, equilibrando as necessidades de fiscalização com o respeito à privacidade dos indivíduos. A ADI 7276 destaca a importância de uma abordagem integrada que respeite tanto as exigências fiscais quanto os direitos de proteção de dados, promovendo uma legislação que garanta tanto a justiça fiscal quanto a privacidade.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm. Acesso em: 15 set. 2024.

BRASIL. **Constituição Federal de 1988**. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 set. 2024.

STF. **Ação Direta de Inconstitucionalidade (ADI) 7276**. Decisão do Supremo Tribunal Federal. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6523973. Acesso em: 15 set. 2024.
SILVA, José Afonso da. **Direito Constitucional**. 10. ed. São Paulo: Malheiros, 2020.

BUCCI, Eugenio; FAERMAN, Julio. **Lei Geral de Proteção de Dados: Comentários e Análise Crítica**. São Paulo: Editora X, 2021.
NOGUEIRA, Gustavo R. B. **Direito Digital e Proteção de Dados Pessoais**. Rio de Janeiro: Editora Y, 2022.

A EFICÁCIA DO VISUAL LAW NA TRANSPARÊNCIA DAS POLÍTICAS DE PRIVACIDADE E TERMOS DE USO: UMA ANÁLISE ACERCA DA PROTEÇÃO DE DADOS E O PAPEL DA ANPD NA ERA DO CAPITALISMO DE VIGILÂNCIA

David Sampaio Motta Campos Canario[1]

RESUMO

Este *paper* examina a eficácia do *Visual Law* na melhoria da transparência das Políticas de Privacidade e Termos de Uso em plataformas digitais. Inicialmente, discute-se a natureza jurídica desses documentos como contratos de adesão, destacando a vulnerabilidade dos consumidores diante de cláusulas abusivas e da falta de clareza, que muitas vezes comprometem o consentimento informado. Aborda-se ainda, a importância de adaptar esses documentos à realidade da "sociedade do cansaço" e do "analfabetismo digital", utilizando recursos visuais para facilitar a compreensão dos usuários e promover maior transparência e confiança, conforme incentivado pela Resolução 347/2020 do CNJ. Por fim, discute-se o papel fiscalizatório da ANPD na adequação das empresas à esses tipos de instrumentos. A pesquisa é qualitativa, com levantamento bibliográfico e método dedutivo.

Palavras-chave: Visual Law. Transparência. Dados Pessoais. Plataformas. ANPD.

1 INTRODUÇÃO

A crescente expansão dos serviços *online* têm gerado variadas formas de tratamento de dados pessoais, desembocando em um contexto de capitalismo de vigilância, onde os dados dos usuários são explorados comercialmente para influenciar comportamentos. Nessa senda, a comunicação das Políticas de Privacidade e Termos de Uso tornou-se uma questão basilar para a proteção dos dados pessoais dos usuários. No entanto, a compreensão efetiva e a acessibilidade

1 Graduando em Direito pela Faculdade Baiana de Direito. E-mail: david75239@hotmail.com.

desses contratos de adesão ainda apresentam barreiras para a maioria do seu público, agravado pelo fenômeno da "sociedade do cansaço" do filósofo Byung-Chul, onde os hiperestímulos, a sobrecarga de informações e a complexidade dos documentos legais contribuem para uma sensação de exaustão e desinteresse por parte dos consumidores, frequentemente resultando na aceitação, sem leitura, de cláusulas vagas e abusivas que violam direitos fundamentais, como à privacidade e à informação, demonstrando que o consentimento do usuário, muitas vezes, não é informado (ANJOS, 2023 *apud* HAN, 2017).

Nesse cenário, o *Visual Law* surge como uma alternativa para melhorar a comunicação jurídica, simplificando a apresentação desses documentos e tornando-os mais compreensíveis. Assim, este *paper* busca analisar como essa técnica pode contribuir para a melhoria da relação de consumo, garantindo não só a redução de eventuais litígios, mas principalmente, o pleno cumprimento do princípio da transparência positivado na Lei Geral de Proteção de Dados (LGPD), e assegurando por consequência, direitos previstos no Código de Defesa do Consumidor (CDC), e no Marco Civil da Internet (MCI), os quais também costumam ser flagrantemente violados em razão da falsa sensação de impunidade diante da Autoridade Nacional de Proteção de Dados (ANPD). Por fim, este *paper* adota um método de pesquisa dedutivo, analisando hipóteses com base em premissas jurídicas para formar novas suposições. Trata-se então, de uma pesquisa qualitativa, bibliográfica e sem coleta de dados.

2 A ASSIMETRIA DAS POLÍTICAS DE PRIVACIDADE E TERMOS DE USO

Sabe-se que os Termos de Uso e as Políticas de Privacidade são instrumentos jurídicos utilizados em plataformas digitais para reger a relação entre os usuários e os provedores de serviços *online*, que ao serem aceitos, estabelecem as regras para a utilização dos serviços e o tratamento de dados pessoais dos usuários. Assim, do ponto de vista jurídico, tais documentos podem ser tipicamente classificados como contratos de adesão, que com base no art. 54 do CDC, são aqueles cujas cláusulas são preestabelecidas pelo fornecedor, sem que o consumidor tenha a possibilidade de discutir ou modificar o conteúdo. Dessa forma, ao utilizar uma plataforma digital, o usuário não participa ativamente da elaboração desses documentos, limitando-se a aceitar ou recusar os termos impostos (FALEIROS JÚNIOR, 2021).

Ocorre que, essa natureza dos contratos de adesão pode ser problemática na relação de consumo estabelecida entre o usuário e a plataforma. Isso porque, de um lado, o fornecedor detém um poder contratual significativamente superior, o que pode levar à imposição de condições potencialmente abusivas. De outro, o consumidor, sem pleno conhecimento do conteúdo e das implicações dos termos, é levado a aceitá-los como um requisito para acessar serviços, que hoje, são indispensáveis para a vida cotidiana (LIMA, 2022).

Nota-se então, que a relação de consumo entre usuário e plataforma digital é marcada por uma notável assimetria de poder e informação, uma vez que as plataformas elaboram termos complexos, redigidos em linguagem técnica e

jurídica, que dificultam o pleno entendimento por parte do usuário médio, a qual se agrava quando consideramos consumidores hipervulneráveis, como idosos, analfabetos ou aqueles com menor familiaridade com tecnologia, conhecidos como analfabetos digitais (VENTURI, 2023).

Além disso, o CDC em seu art. 54, §§ 3º e 4º, assegura ao consumidor o direito à informação adequada e clara sobre produtos e serviços em contratos de adesão, de modo que eles devem ser redigidos em termos claros, com caracteres ostensivos e com destaque para aquelas cláusulas que possam limitar algum direito. Contudo, esses documentos costumam falhar em atender a esse requisito, configurando uma situação de vulnerabilidade do consumidor frente à complexidade e à extensão dos documentos. Somado a isso, ao serem aceitos, tais instrumentos podem ainda conter cláusulas que limitam a responsabilidade da empresa ou que impõem obrigações desproporcionais ao consumidor (CARNEIRO, 2020).

Essa obscuridade se relaciona com o princípio da transparência previsto na LGPD, visto que de acordo com o art. 6º, VI, o tratamento de dados pessoais deve ser realizado de forma acessível ao seu titular. Paralelamente, o art. 7º, IX do MCI assegura o consentimento expresso sobre o tratamento desses dados de forma destacada das demais cláusulas. Porém, muitos documentos são redigidos para cumprir apenas uma formalidade, sem de fato proporcionar ao usuário o conhecimento em termos claros, para tomar uma decisão plenamente informada sobre o tratamento de seus dados. Logo, o consentimento por clique pode ser não informado, comprometendo a validade do ato jurídico (CARNEIRO, 2020).

3 A APLICAÇÃO DO VISUAL LAW E O PAPEL DA ANPD

Uma pesquisa da National Privacy Test, conduzida pela NordVPN ao entrevistar 48.063 pessoas de 192 países, mostrou que apenas 38,3% dos brasileiros leem os Termos de Uso (NORDVPN, 2021). Em contrapartida, uma pesquisa da *Bits Academy* feita com 463 voluntários, em 20 estados, apontou que documentos elaborados com técnicas de design, e simplificação do texto, resultam em uma maior interação, sugerindo que tais abordagens podem ser essenciais para aumentar a compreensão desses documentos (BITS ACADEMY, 2020). A fim de superar essas barreiras, surge o conceito de *Visual Law*.

Embora alvo de críticas por juristas conservadores em face da simplificação da linguagem jurídica, essa abordagem inspirada em práticas de *design thinking*, quando aplicada de forma equilibrada, consegue simplificar de forma eficaz, a apresentação de documentos jurídicos por meio de recursos visuais, como gráficos, ícones, fluxogramas e cores, para transmitir informações de maneira acessível, colocando no centro, a experiência do usuário comum, como bem adota a Política de Privacidade do *IFood* (BASEGIO, 2023).

Ademais, corroborando com a eficácia dessa solução, o Conselho Nacional de Justiça (CNJ) através da Resolução nº 347/2020, incentivou o uso do *Visual Law* no âmbito do Poder Judiciário para tornar os documentos jurídicos mais acessíveis. Esse posicionamento influenciou a criação de outros atos normativos,

como o Provimento 45/2021 do Tribunal de Justiça do Espírito Santo, em seu art. 23-D, § 5º, que foi ainda mais específico na produção de avisos de privacidade adotando essa técnica. Diante disso, surge o questionamento sobre o papel da ANPD na fiscalização e garantia da conformidade desses documentos com a lei.

Tal autarquia tem o dever de assegurar que todas as empresas que operam no Brasil, independentemente de seu porte ou setor, estejam em conformidade com a LGPD de acordo com o art. 46, § 1º, sob pena de sofrerem sanções administrativas. Ocorre que, a sensação de impunidade pode ser aflorada em pequenas empresas, que mesmo incentivadas a aplicar o *privacy by design* e ainda sujeitas a um tratamento mais leve com base na Resolução CD/ANPD nº 02/2022, podem acreditar que uma adequação pouco robusta, é apenas uma ameaça para àquelas empresas que lidam com um grande fluxo de dados, especialmente devido às sanções aplicadas contra *big techs*, amplamente noticiadas na mídia. Não só isso, questiona-se ainda a capacidade operacional da ANPD, que em tese, enfrentaria o desafio de monitorar e penalizar todas as violações de dados pessoais, dada a enorme quantidade de serviços digitais, tornando então, o poder de fiscalização ainda mais limitado (LIMA, 2023).

4 CONSIDERAÇÕES FINAIS

Em síntese, a aplicação do *Visual Law* revela-se essencial para alinhar esses documentos tanto às exigências normativas quanto ao padrão de comportamento da sociedade no meio digital. Por fim, sabendo que o papel da ANPD não se limita à punição, mas também ao incentivo na adoção de boas práticas, isso a coloca em uma posição essencial para garantir que o princípio da transparência seja respeitado em sua essência, aliado ao senso crítico dos usuários, que devem estar informados sobre o que estão concordando, bem como, munidos de conhecimento suficiente para denunciar potenciais ilegalidades, o que por si só, pode levar ao aumento de confiança na relação de consumo e o aumento de denúncias, especialmente na era do capitalismo de vigilância, onde os dados pessoais se tornaram uma das mais novas moedas de troca (PEREIRA; MEDEIROS, 2022).

REFERÊNCIAS BIBLIOGRÁFICAS

ANJOS, Pedro Germano. **O Direito na Sociedade do Cansaço: entre o "Ativismo Narcísico" e o "Yes We Canjudicante"**. 2023. Diké Revista Jurídica. Disponível em: https://periodicos.uesc.br/index.php/dike/article/view/3713/2372. Acesso em: 15 ago. 2024.

BASEGIO, Nayara Darabas. **Legal Design: Inovação e Tecnologia da Comunicação.** 2023. In: IV Congresso Internacional de Direito e Inteligência Artificial: Soluções Locais de Inovação e Tecnologia. Disponível em: http://site.conpedi.org.br/publicacoes/s5y6p2k5/490b7s3e. Acesso em: 10 ago. 2024.

BITS ACADEMY. **Legal Design: Pesquisa de análise de comportamento de usuários diante de documentos jurídicos.** 2020. Disponível em: https://pt.slideshare.net/slideshow/pesquisa-sobre-a-aplicao-de-legal-design-e-comportamento-do-usurio/239300827#5. Acesso em: 18 ago. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 ago. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Senado Federal, 1990. Acesso em: 21 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 ago. 2024.

CARNEIRO, Ramon Mariano. **"Li e aceito": violações a direitos fundamentais nos termos de uso das plataformas digitais.** 2020. Revista Internet Lab. Disponível em: https://revista.internetlab.org.br/li-e-aceitoviolacoes-a-direitos-fundamentais-nos-termos-de-uso-das-plataformas-digitais/. Acesso em: 17 ago. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 347, de 23 de abril de 2020.** Dispõe sobre a regulamentação da prática de atos notariais eletrônicos pelos serviços notariais e de registro do Brasil. Diário de Justiça Eletrônico, Brasília, DF, 27 abr. 2020. Acesso em: 19 ago. 2024.

ESPÍRITO SANTO. **Tribunal de Justiça do Espírito Santo.** Provimento TJES nº 45, de 26 de agosto de 2021. Altera a redação do artigo 16 e acrescenta dispositivos aos artigos 32-A, 32-B, 32-C e 32-D do Provimento nº 013/2020. Diário da Justiça Eletrônico, Vitória, ES, 27 ago. 2021. Acesso em: 19 ago. 2024.

FALEIROS JÚNIOR, José Luiz de Moura. **LEGAL DESIGN: A aplicação de recursos de design na elaboração de documentos jurídicos.** Indaiatuba: Foco, 2021. Disponível em: https://vlex.com.br/vid/termos-uso-politica-privacidade-942228598. Acesso em: 14 ago. 2024.

IFOOD. **Política de Privacidade**. Disponível em: https://privacidade.ifood.com.br/privacidade-clientes/. Acesso em: 18 ago. 2024.

LIMA, Cíntia Rosa Pereira de. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos.** 2014. Disponível em: http://www.publicadireito.com.br/artigos/?cod=981322808aba8a03#:~:text=os%20contratos%20de%20ades%c3%a3o%20eletr%c3%b4nicos,espera%20de%20determinada%20rela%c3%a7%c3%a3o%20jur%c3%addica. Acesso em: 19 ago. 2024.

LIMA, Joanan Silva Ribeiro. **Contextualização da Lei Geral de Proteção de Dados para os Pequenos Negócios.** Revista Científica Semana Acadêmica. Fortaleza, ano MMXXIII, Nº. 000229, 2023. Disponível em: https://semanaacademica.org.br/artigo/contextualizacao-da-lei-geral-de-protecao-de-dados-para-os-pequenos-negocios. Acesso em: 13 ago. 2024.

PEREIRA, Maria Marconiete Fernandes; MEDEIROS, Valeria Fernandes. **A IMPORTANCIA DO PAPEL REGULATÓRIO DA ANPD NA SOCIEDADE INFORMACIONAL SOB A PERSPECTIVA DA ANÁLISE ECONÔMICA DO DIREITO.** 2023. Revista de Direito, Economia e Desenvolvimento Sustentável, Florianópolis (SC), e-ISSN: 2526-0057. Disponível em: https://www.indexlaw.org/index.php/revistaddsus/article/view/9575/pdf. Acesso em: 27 ago. 2024.

REVISTA COBERTURA. **Brasileiros têm os piores hábitos digitais, indica levantamento da NordVPN.** 2021. Disponível em: https://www.revistacobertura.com.br/noticias/tecnologia-servicos/brasileiros-tem-os-piores-habitos-digitais-indica-levantamento-da-nordvpn/. Acesso em: 15 ago. 2024.

VENTURI, Thaís G. Pascoaloto Venturi. **Os Termos de Uso, você já leu?** 2023. Disponível em:https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/398919/os-termos-de-uso-voce-ja-leu. Acesso em: 11 ago. 2024.

DESAFIOS ÉTICOS E LEGAIS DO USO DE DADOS BIOMÉTRICOS NO TRANSPORTE PÚBLICO: O CASO DO METRÔ DE SÃO PAULO

Giulia De-gino D'Antonio[1]

1 INTRODUÇÃO

Em que pese a crescente adoção de modelos de negócios em *big data* envolvendo algoritmos de Inteligência Artificial (IA) e Internet das Coisas *(Internet of Things - IoT*) represente um notório avanço tecnológico, a ação civil pública proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em face da empresa Concessionária Da Linha 4 Do Metrô De São Paulo S.A. (Via Quatro), decorrente da coleta e tratamento de imagens e dados biométricos, isto é, dados pessoais sensíveis, sem a devida anuência das pessoas que passavam pelas sete estações que formam a linha Amarela levanta importantes questionamentos sobre privacidade, proteção de dados pessoais e os seus limites.

Em que pese o papel dos dados biométricos no melhoramento de publicidades e propagandas, através da identificação quase instantânea das reações, cabe questionar: como conciliar o uso de dados biométricos com os princípios legais e éticos do ordenamento jurídico, a fim de garantir o crescimento econômico e o avanço da tecnologia sem comprometer a privacidade e os direitos individuais dos cidadãos? A problemática em questão possui uma pertinência extremamente relevante do ponto de vista sociojurídico vez que se trata de uma temática extremamente atual, afinal, o Direito está se habituando à forma com que regula determinadas condutas que tangenciam os dados pessoais e o digital.

No que tange ao procedimento técnico de pesquisa, o presente trabalho se caracteriza como predominantemente bibliográfico. Quanto ao método de pesquisa, a dedução será utilizada visando analisar a veracidade das hipóteses formuladas com base nas premissas jurídicas da doutrina e da legislação no decorrer do artigo. Amparado na metodologia de Popper serão levantados questionamentos acerca dos desafios éticos e legais do uso de dados biométricos,

1 Graduanda em Direito pela Faculdade Baiana de Direito. E-mail: contato@giuliadantonio.com.

os quais buscarão ser respondidos pelo falseamento.

Este estudo busca explorar os desafios da coleta, armazenamento e tratamento de dados biométricos coletados para publicidades em transportes públicos. As implicações éticas e jurídicas decorrentes dessa prática fomentam o debate a respeito do equilíbrio entre inovação tecnológica e o respeito aos direitos fundamentais dos cidadãos, plenamente assegurados pela Constituição Federal e pela Lei Geral de Proteção de Dados .

2 DADOS BIOMÉTRICOS E O ORDENAMENTO JURÍDICO BRASILEIRO

A priori, cumpre destacar que dados biométricos, à luz da Lei nº 13.709/18, art. 5º, inciso II são, inequivocamente, dados sensíveis. Viviane Maldonado e Renato Blum explicam que esses dados pessoais são chamados de "sensíveis" porque podem gerar algum tipo de discriminação, além de implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares, principalmente quando se trata de dados biométricos, dada a sua natureza mais crítica (Maldonado; Blum, 2019, p. 69-70).

A Constituição Federal, por sua vez, esculpe em seu art. 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas como direitos fundamentais (BRASIL, 1988). A disposição constitucional não só faz cristalizar a necessidade e, principalmente, a importância de proteger a esfera pessoal dos cidadãos através da custódia dos seus dados pessoais, sejam eles sensíveis ou não, como também impõe limites ao tratamento desses dados por parte de entidades públicas e privadas.

Ressalta-se, no entanto, que apesar da motivação da conceituação dessa categoria especial de dados pessoais ser fruto de uma observação pragmática da diferença que apresenta o efeito do tratamento desses dados em relação aos demais (Doneda, 2006, p.161), a maior proteção concedida, principalmente a respeito de dados biométricos, não é sinônimo de impossibilidade de tratamento.

Apesar do consentimento inequívoco e da finalidade específica no tratamento de dados sensíveis serem princípios cruciais a serem observados, o art. 11º da LGPD traz em seus incisos oito hipóteses que facultam o seu tratamento, as quais vão além do consentimento, sem deixar de garantir que a coleta e o processamento de informações biométricas sejam realizados de maneira ética e legal.

Nesse ponto, diante da (des)necessidade de consentimento para a coleta de dados biométricos, surge o questionamento: qual seria o fator capaz de impedir a instalação do sistema Portas Interativas Digitais no Caso do Metrô de São Paulo, responsável por captar as emoções dos usuários da Linha Amarela e, ao mesmo tempo, facultar o uso de equipamentos de reconhecimento facial no Carnaval de Salvador?

3 CARNAVAL DE SALVADOR X METRÔ DE SÃO PAULO

A resposta, nada simples, pode ser explicada por uma série de fatores, incluindo questões legais, éticas e de finalidade, que, no caso do Carnaval de

Salvador, versava sobre uma questão de segurança pública[2] e de necessidade de controle de acesso a um eventos de grande aglomeração, subsumindo-se às alíneas b) e e) do art. 11º, inciso II da LGPD[3].

A finalidade evoca também a transparência acerca da maneira em que os dados serão tratados, desde a coleta até o seu armazenamento. No Carnaval de Salvador, a finalidade é quase intuitiva: garantir a segurança do evento. No caso das portas interativas no Metrô de São Paulo, a finalidade de capturar emoções para fins publicitários pode ser vista como menos clara, mais invasiva e abusiva, afinal, o objetivo é a maximização de lucros privados.

Um último ponto de divergência seria a expectativa razoável de privacidade esperada pelas pessoas, isto é, enquanto o Carnaval de Salvador é a festa de rua mais famosa do mundo, estações de metrô são espaços de transporte público e, por isso, instalar portas interativas digitais que, segundo a própria Ré declarou nos autos, é capaz de contar pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, horas de pico de visualizações, captação de expressões e emoções sem o conhecimento ou consentimento desses usuários pode ser vista como uma violação dessa expectativa.

Contudo, é sabido que a mera quebra de expectativa não foi o fator causador da condenação da Requerida ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00 (cem mil reais), mas sim o fato de que o tipo de coleta/tratamento realizado sem consentimento dos usuários não incidia em nenhuma das hipóteses da Lei nº 13.709/18.

4 OS DESAFIOS ÉTICOS ENVOLVIDOS

Ante a improcedência suscitada pela empresa concessionária no sentido de que as portas digitais "não captavam imagem definidas atribuídas a pessoas identificadas, mas apenas detecta rostos e expressões", surgem alguns desafios éticos que demandam análise no contexto jurídico. Não se encaixando nas hipóteses do inciso II do art. 11º, em razão da privacidade e da autonomia individuais é imprescindível que os titulares dos dados pessoais estejam devidamente cientes de que suas emoções estão sendo monitoradas e registradas.

Apesar de não terem provado o que alegam, tomando como se verdadeiros

2 Segundo o Governo da Bahia, as lesões corporais apresentaram queda de 56%.Os roubos e furtos também recuaram, de 1.153 para 898 casos. No acumulado, ações das polícias Militar e Civil prenderam em flagrantes 25 criminosos. No total, somando com os 49 foragidos localizados pelo Reconhecimento Facial, 74 pessoas envolvidas com crimes foram retiradas dos circuitos do Carnaval de Salvador.

3 Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; e) proteção da vida ou da incolumidade física do titular ou de terceiro;

fossem os fatos narrados, a ausência de transparência nesse processo de coleta de dados, por si só, suscitaria questionamentos quanto à legalidade e à ética subjacentes, afinal, é inegável o objetivo de melhoria das publicidades como forma de maximização dos lucros.

Nas palavras de Stefano Rodotá, o cidadão não pode ser visto como simples fornecedor de dados, ele tem que ter poder de controle sobre esses dados, para se estabelecer o equilíbrio na concentração de poder (2008, p. 36). Ressalta-se ainda que os mais diversos perfis passam pelos transportes públicos todos os dias, fazendo com que a questão ética se mostre ainda mais sensível quando diante da vulnerabilidade de grupos como crianças ou pessoas com problemas emocionais, trazendo à tona outras questões dignas de estudo.

5 CONSIDERAÇÕES FINAIS

Diante da análise do Caso do Metrô de São Paulo e das suas portas inteligentes, apesar do inegável papel dos dados biométricos no avanço da tecnologia e na segurança pública, inúmeras são as questões - majoritariamente éticas - postas à prova, sendo um ponto crítico que merece a atenção do Judiciário.

A coleta em massa feita por empresas privadas através da captação das mais diferentes expressões faciais, não só sem consentimento mas visando o lucro através da reação às publicidades exibidas emergem preocupações absolutamente legítimas sobre a eficácia das normas jurídicas que asseguram a privacidade e a proteção de dados pessoais, o que é um direito fundamental reconhecido pelo ordenamento jurídico brasileiro.

Apesar da base sólida oferecida pelo ordenamento jurídico, o caso em tela ratifica como abordagem cuidadosa e atualizada do magistrado diante das inovações tecnológicas é crucial para o bem estar do coletivo e, não por outro motivo, os direitos individuais, como a privacidade e responsabilidade coletiva, são pilares essenciais que devem ser observados para garantir uma abordagem ética e legalmente sólida nesse contexto.

REFERÊNCIAS

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. p. 161.

DUARTE, T. Júlia. **A aplicação da tutela da proteção de dados pessoais no caso das portas interativas digitais do metrô de São Paulo.** 2019. Monografia. (bacharelado em direito) - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, Rio de Janeiro. Prof. Orientador: Flávio Alves Martins.

MALDONADO, N. Viviane.; BLUM, O. Renato. LGPD: **Lei Geral de Proteção de Dados: comentada.** 2ª edição. São Paulo: Revista dos Tribunais, 2019.

Portal Oficial Do Estado Da Bahia. **Reconhecimento Facial alcança 49 foragidos da Justiça no Carnaval.** Disponível em: https://www.bahia.ba.gov.br/2023/02/noticias/reconhecimento-facial-alcanca-49-foragidos-da-justica-no-carnaval/. Acesso em 14 set 2023.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Organização, seleção e apresentação de: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NOS JOGOS ONLINE: UMA ANÁLISE JURÍDICA E SOCIOTECNOLÓGICA

Iasmim Agra Cavalcante

RESUMO

A interseção entre tecnologia e privacidade é cada vez mais proeminente na sociedade digital. A Lei Geral de Proteção de Dados (LGPD) trouxe significativas alterações ao cenário jurídico brasileiro, especialmente no que tange à proteção da privacidade no ambiente digital, impactando diretamente o setor de jogos online. Esta legislação impõe a necessidade de transparência na coleta de dados, consentimento informado dos jogadores e medidas de segurança robustas. Este trabalho analisa os efeitos da LGPD em jogos digitais, abordando desafios jurídicos e tecnológicos, e perspectivas futuras para a indústria.

Palavras-chave: LGPD. Proteção de dados. Privacidade. Jogos online. Regulamentação.

ABSTRACT

The intersection between technology and privacy is increasingly prominent in digital society. The General Data Protection Law (LGPD) has brought significant changes to the Brazilian legal landscape, particularly regarding privacy protection in the digital environment, directly impacting the online gaming sector. This legislation requires transparency in data collection, informed consent from players, and robust security measures. This paper analyzes the effects of the LGPD on digital games, addressing legal and technological challenges, as well as future prospects for the industry.

Keywords: LGPD. Data protection. Privacy. Online games. Regulation.

1 INTRODUÇÃO

A digitalização crescente da sociedade destaca a importância da regulamentação de dados pessoais. A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) visa garantir a privacidade e segurança das informações, impactando significativamente o setor de jogos online, que coleta grandes volumes de dados dos usuários. Essa legislação exige práticas mais transparentes e seguras, adaptadas às novas exigências legais.

Empresas de jogos digitais enfrentam desafios para cumprir a LGPD sem comprometer a experiência dos jogadores. Dados como registros de login, comportamento dos jogadores e transações financeiras devem ser tratados de forma responsável e conforme a lei. Este trabalho analisa as adaptações necessárias, os desafios tecnológicos e jurídicos da implementação da LGPD e as perspectivas futuras para a regulamentação e a privacidade no setor.

A metodologia deste estudo baseou-se em uma análise qualitativa e descritiva, utilizando fontes bibliográficas, jurisprudenciais e relatórios técnicos sobre segurança e privacidade de dados. A abordagem interdisciplinar permitiu explorar os impactos da LGPD no setor de jogos online, considerando aspectos jurídicos e tecnológicos.

2 A LGPD E A COLETA DE DADOS NOS JOGOS DIGITAIS

A aplicação da LGPD no setor de jogos online não se limita à simples proteção dos dados pessoais. A legislação impõe uma série de obrigações às empresas, como o dever de informar claramente os usuários sobre o tratamento de suas informações e de obter o consentimento explícito para tal (BRASIL, 2018). Isso inclui a coleta de dados aparentemente inofensivos, como apelidos (ou "*nicknames*"), que, quando combinados com outros dados, podem identificar o jogador fora do ambiente virtual.

Decisões judiciais recentes reforçam a cautela necessária na divulgação de informações dos jogadores. No caso do Tribunal de Justiça do Estado do Rio de Janeiro, processo n.º 0033863-56.2016.8.19.0203, ficou decidido que os "*nicknames*" utilizados em plataformas de jogos podem ser considerados dados pessoais. Portanto, a exposição pública desses apelidos, especialmente em listas de banimento, pode resultar em danos morais, pois afeta a reputação dos jogadores (COSTA; OLIVEIRA, 2019, p. 202).

A exigência de consentimento também se estende a outros tipos de informações coletadas durante o uso dos jogos. Dados como endereços IP, padrões de comportamento dentro do jogo e transações financeiras são abrangidos pela LGPD, exigindo que as empresas de jogos adotem práticas robustas para assegurar o cumprimento das normas de proteção de dados (MALDONADO, 2019, p. 110).

No cenário global, a regulamentação de proteção de dados como a LGPD e o GDPR (General Data Protection Regulation), está criando um ambiente

normativo mais robusto e integrado. Empresas que operam em múltiplas jurisdições enfrentam o desafio de harmonizar suas práticas para atender às exigências legais de diferentes países. Além disso, a velocidade com que as novas tecnologias são implementadas no setor de jogos, como realidade aumentada e virtual, levanta questões adicionais sobre o tipo de dados que podem ser considerados sensíveis, como expressões faciais e movimentos corporais, os quais podem ser usados para identificar os usuários com precisão ainda maior (MIRAGEM, 2021, p. 150).

3 DESAFIOS JURÍDICOS E TECNOLÓGICOS NA INDÚSTRIA DE JOGOS DIGITAIS

A LGPD impõe desafios significativos à indústria de jogos online, especialmente no tratamento de dados de crianças e adolescentes. A exigência de consentimento explícito dos pais ou responsáveis, bem como a apresentação de informações de forma acessível e clara, demanda medidas específicas que considerem a capacidade de entendimento desse público (PINHEIRO, 2021, p. 76; SENA, 2019, p. 62). Além disso, a conformidade com a LGPD exige revisão estrutural nos sistemas de coleta e armazenamento de dados, com mecanismos que permitam a exclusão de informações a pedido do titular, o que representa uma grande dificuldade para as empresas (PINHEIRO, 2021, p. 89).

A adoção de medidas de segurança, como criptografia e anonimização, surge como uma solução essencial para mitigar os riscos associados à exposição de dados (MALDONADO, 2019, p. 125). No entanto, avanços tecnológicos, como inteligência artificial e algoritmos preditivos, ampliam a complexidade regulatória, pois seu uso inadequado pode infringir a LGPD (TARTUCE, 2022, p. 112). Assim, as empresas devem se adaptar continuamente às inovações, garantindo a privacidade dos jogadores enquanto atendem às normas legais.

As penalidades por não conformidade são severas, com multas de até 2% do faturamento, limitadas a R$ 50 milhões por infração. Além do impacto financeiro, violações podem prejudicar a reputação das empresas, resultando na perda de confiança dos usuários e na migração para concorrentes que adotem melhores práticas de proteção de dados (PINHEIRO, 2021, p. 141). Esse cenário reforça a importância de investimentos constantes em segurança e privacidade.

4 PERSPECTIVAS FUTURAS: CONVERGÊNCIA GLOBAL E PROTEÇÃO DE DADOS

O cenário global de proteção de dados aponta para uma crescente harmonização entre legislações, como a LGPD e o GDPR, refletindo uma tendência de maior rigor na proteção de dados pessoais. Empresas de jogos que operam internacionalmente precisam adequar suas práticas para evitar sanções e atender às demandas de múltiplos mercados (MIRAGEM, 2021, p. 160). A proteção de dados, além de ser uma exigência legal, é uma oportunidade para fortalecer a confiança dos usuários e oferecer experiências mais seguras e confiáveis (PINHEIRO, 2021, p. 130).

No futuro, espera-se que a inovação tecnológica continue a apresentar desafios regulatórios. A inteligência artificial e os algoritmos preditivos,

amplamente utilizados para personalizar a experiência do jogador, podem ampliar as discussões sobre privacidade, especialmente no que tange ao uso de dados pessoais para prever comportamentos. Nesse sentido, a constante adaptação das legislações de proteção de dados será crucial para acompanhar as evoluções tecnológicas e garantir que os direitos dos usuários sejam devidamente resguardados (TARTUCE, 2022, p. 180).

A expansão do metaverso e de tecnologias de rastreamento de dados apresenta novas questões sobre privacidade e propriedade de informações. Perfis detalhados dos jogadores e ambientes imersivos demandam regulamentações específicas para evitar violações de direitos fundamentais. Esse cenário reforça a necessidade de políticas internacionais mais alinhadas, que conciliem inovações tecnológicas com a proteção dos usuários (TARTUCE, 2022, p. 185).

5 CONCLUSÃO

A promulgação da LGPD estabeleceu novos padrões para o tratamento de dados pessoais no Brasil, impactando diretamente a indústria de jogos online. A conformidade com a legislação não é apenas uma exigência legal, mas uma questão de confiança e segurança para os jogadores. As empresas precisam adotar medidas proativas para proteger as informações dos usuários, desde a obtenção do consentimento informado até a implementação de tecnologias de segurança avançadas.

Apesar dos desafios impostos pela LGPD, as empresas que investem em políticas de privacidade transparentes e na proteção de dados estarão mais preparadas para enfrentar as demandas do mercado digital. A proteção da privacidade dos jogadores não apenas assegura a conformidade legal, mas também reforça a reputação das empresas, criando um ambiente de jogo mais seguro e ético. O futuro da indústria de jogos está diretamente ligado à capacidade de adaptação às regulamentações de proteção de dados, tanto nacionais quanto internacionais.

REFERÊNCIAS

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 08 de setembro de 2024.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Apelação Cível n.º 0033863-56.2016.8.19.0203, Relator(a): Des. Alcides da Fonseca Neto, 24ª Câmara Cível, julgado em 04 de dezembro de 2019.** Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rj/791195099/inteiro-teor-791195111. Acesso em: 10 set. 2024.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. **Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais.** Revista brasileira de direito civil em perspectiva, v. 5, n. 2, 2019.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais – Principais repercussões para a atividade empresarial**. Ano 2018. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2018-08-30. Acesso em: 10 de setembro de 2024.

MALDONADO, Viviane Nóbrega (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação.** São Paulo: Revista dos Tribunais, 2019.

MIRAGEM, Bruno. **Responsabilidade Civil: Impactos da LGPD.** 2. ed. Rio de Janeiro: Forense, 2021.

PINHEIRO, Patricia Peck. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)**. 3º edição. São Paulo: Saraiva jur, 2021.

SENA, Sâmara Rodrigues. **A proteção de dados pessoais de crianças no ordenamento jurídico brasileiro.** Revista Caderno Virtual. Brasília: IDP, nº 44, v. 2, abr/jun, 2019.

TARTUCE, Flávio. **Responsabilidade Civil: Impactos da LGPD.** 4º edição. Rio de Janeiro: Forense, 2022.

O USO DE INTELIGÊNCIA ARTIFICIAL (IA) NO ÂMBITO DA FISCALIZAÇÃO TRIBUTÁRIA: ATUAIS PERSPECTIVAS NA UTILIZAÇÃO DE *MACHINE LEARNING* PARA A CONFORMIDADE LEGAL DO ICMS NO ESTADO DA BAHIA

Pedro Lucca Lima Vieira[1]

RESUMO

Este artigo busca explorar o uso da inteligência artificial (IA) em novos procedimentos de fiscalização fazendária do ICMS no Estado da Bahia, analisando as atuais perspectivas para conformidades legais e cumprimentos de obrigações acessórias, visualizando a utilização de ferramentas digitais que aceleram a triagem de dados para o fisco local. A pesquisa busca compreender como ferramentas de IA, como *machine learning*, utilizadas para automatizar processos e aprimorar a detecção de fraudes fiscais. A relevância desse estudo reside no potencial dessas tecnologias para aumentar a eficiência da arrecadação e conformidade tributária sobre o imposto mercantil estadual, além de entender o novo cenário no cumprimento das obrigações e declarações fiscais perante a administração fazendária.

Palavras-chaves: Inteligência Artificial (IA); Fiscalização Tributária; ICMS; Conformidade Legal.

ABSTRACT

This article seeks to explore the use of artificial intelligence (AI) in new ICMS tax inspection procedures in the State of Bahia, analyzing the current perspectives for legal compliance and compliance with ancillary obligations, visualizing the use of digital tools that accelerate screening data for the local tax authorities. The

1 Graduando em Direito pela Faculdade Baiana De Direito. Membro-Ouvinte da Comissão de Direito Tributário da OAB/BA. Membro do Grupo de Estudos de Direito e Negócios – GEDEN. E-mail: pedroluccavl@gmail.com

research seeks to understand how AI tools, such as machine learning, are used to automate processes and improve the detection of tax fraud. The relevance of this study lies in the potential of these technologies to increase the efficiency of tax collection and compliance on state commercial tax, in addition to understanding the new scenario in fulfilling obligations and tax declarations before the tax administration

Keywords: Artificial Intelligence (AI); Tax Inspection; ICMS; Legal Compliance

1 INTRODUÇÃO

O Direito Tributário tem evoluído com base em uma realidade concreta, que vem sendo transformada pelas mudanças sociais impulsionadas pela tecnologia. A crescente digitalização tem impactado diversos setores, inclusive a Administração Pública. Um exemplo disso é o uso de Inteligência Artificial (IA) na fiscalização do ICMS, tributo de grande importância arrecadatória para os Estados.

Assim, a administração tributária enfrenta desafios contínuos, como a evasão fiscal e a complexidade do sistema tributário no que tange ao cumprimento de obrigações acessórias, o que compromete a eficiência arrecadatória e dá nova roupagem a apuração do imposto estadual. Nesse sentido, o problema de pesquisa deste artigo reside na seguinte questão: até que ponto o uso de IA pode aprimorar a fiscalização e aumentar a conformidade do ICMS no Estado da Bahia?

A aplicação de procedimento com intervenção artificial pode trazer maior eficiência ao processo de fiscalização ao reduzir a ação manual, automatizar a detecção de inconformidades e tornar o processo mais célere. Contudo, ao passo inverso, a automação na administração tributária leva a um aumento significativo do contencioso tributário, visto que tais ferramentas ainda não possuem plena interpretação do sistema fazendário estadual (dada sua extrema complexidade), impactando os contribuintes locais com divergências na homologação do imposto estadual e revista equivocada nas prestações de informações.

2 A UTILIZAÇÃO DAS IA's NA ADMINISTRAÇÃO TRIBUTÁRIA E O *MACHINE LEARNING*

O uso da inteligência artificial tem proporcionado maior eficácia na arrecadação de tributos. Isso se dá principalmente devido à capacidade de desenvolver ações de fiscalização dos contribuintes dentro do sistema de lançamento por homologação, como o imposto aqui tratado[2].[3] Dentre as diversas abordagens de IA, uma das mais promissoras é o *machine learning* (aprendizado de máquina), que se destaca por sua capacidade de analisar grandes volumes de

2 ZILVETI, F. A. (2019). **As Repercussões da Inteligência Artificial na Teoria da Tributação**. Revista Direito Tributário Atual, (43), 483–498. Disponível em: https://revista.ibdt.org.br/index.php/RDTA/article/view/1457 . Acesso em 11 set. 2024.

3 JARUDE, Jamile Nazare Duarte Moreno. **O estado da arte da fiscalização tributária federal e o uso de inteligência artificial** / Marília: UNIMAR, 2020.

dados, identificar padrões e, assim, prever comportamentos futuros.

O *machine learning* consiste em algoritmos que, a partir de uma grande quantidade de dados históricos, são treinados para "aprender" a realizar previsões ou classificações[4]. Esses algoritmos podem ser aplicados em diversas frentes na administração tributária, como a detecção de fraudes, auditorias automatizadas, análises de riscos fiscais e monitoramento contínuo de contribuintes.

A incorporação da inteligência artificial pelas administrações tributárias já é uma prática consolidada, abrangendo não apenas um pequeno número de nações, mas sendo utilizada por mais de 40 (quarenta) países, além de integrar debates supranacionais promovidos por organizações como a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e o CIAT (Centro Interamericano de Administrações Tributárias). A capacidade dessas administrações de gerir grandes volumes de dados, juntamente com a diminuição dos custos computacionais e a aplicação prática dos avanços tecnológicos, tem impulsionado a disseminação cada vez maior da IA[5].

A análise do uso da inteligência artificial revela que inúmeras administrações tributárias – assim como a Secretaria da Fazenda da Bahia, como veremos a diante - vêm adotando essa tecnologia para a execução de suas funções. De fato, a IA tem sido empregada amplamente como uma ferramenta de suporte às atividades administrativas, reforçando sua importância nesse contexto, sendo necessário entender sua relevância no atual cenário de conformidade tributária, principalmente quanto ao cumprimento de obrigações acessórias inerentes a apuração de ICMS e os impactos diretos ao contribuinte.

3 INCLUSÃO DE FERRAMENTAS ARTIFICIAIS PARA CONFORMIDADE TRIBUTÁRIA NO ESTADO DA BAHIA

A implementação da inteligência artificial (IA) na administração tributária do Estado da Bahia tem se destacado como um marco no avanço tecnológico da fiscalização e combate a desconformidade contábeis-tributárias quanto ao ICMS.

Nesta linha, com o uso da IA, com base no *machine learning*, a SEFAZ-BA pode monitorar dados fiscais de diferentes fontes, como notas fiscais eletrônicas, transações bancárias e declarações tributárias, identificando padrões de sonegação fiscal de maneira muito mais rápida e precisa. O uso da tecnologia também automatiza processos repetitivos e trabalhosos, liberando os fiscais para se concentrar em investigações mais complexas[6].

Para a administração tributária estadual, dois modelos de previsão foram

4 **O que é Machine Learning?** Disponível em: https://www.oracle.com/br/artificial-intelligence/machine-learning/what-is-machine-learning/ . Acesso em 11 set. de 2024.

5 CALIENDO, Paulo; LIETZ, Bruna (Coords.) **Direito Tributário e Novas Tecnologias**. Porto Alegre, RS: Editora Fi, 2021.

6 SEFAZ/BA. **Pioneiro no país, Cira já recuperou R$ 560 milhões para a Bahia, e adota novas estratégias de combate à sonegação**. **Sefaz BA | Secretaria da Fazenda do Estado da Bahia.** 17 jun. 2024. Disponível em: https://www.sefaz.ba.gov.br/noticias/pioneiro-no-pais-cira-ja-recuperou-r-560-milhoes-para-a-bahia-e-adota-novas-estrategias-de-combate-a-sonegacao/ . Acesso em: 11 set. 2024

desenvolvidos. O primeiro, de curto prazo, busca estimar, já no primeiro dia do mês atual, o montante total de ICMS a ser arrecadado, considerando a atividade econômica do mês anterior, dividido entre 15 (quinze) setores econômicos. Como o ICMS é recolhido no mês seguinte ao da ocorrência dos fatos geradores, esse primeiro dia representa a maior antecipação possível para realizar projeções com base nos dados completos do mês anterior, impactando diretamente na rigidez e analise no cumprimento das obrigações acessórias por parte do contribuinte, como a entrega do GIA/GIA ST-BA (Guia de Informações e Apuração e Substituição Tributária) e EFD ICMS (Escrituração Fiscal Digital).

O segundo modelo, por sua vez, tem a capacidade de gerar estimativas para intervalos de tempo mais longos, permitindo antecipar os cálculos com maior antecedência, abrangendo vários meses correntes.

Os modelos de previsão de arrecadação tributária com o uso de Inteligência Artificial fizeram uso de redes neurais artificiais MLP (*Multilayer Perceptron*) e redes recorrentes LSTM (*Long Short-Term Memory*). Como o princípio básico do aprendizado de máquina é desenvolver algoritmos que aprendam a partir de dados e façam «decisões inteligentes», esses modelos foram ajustados utilizando o histórico de arrecadação tributária de seis anos, combinado com dados diários da movimentação econômica na Bahia, extraídos das notas fiscais eletrônicas emitidas entre empresas (NF-e) e para o consumidor final (NFC-e)[7].

Apesar dos avanços com o uso de tais ferramentas, uma nova forma de administração e conformidade tributária na Bahia, pautada na incrementação exponencial de IA's gera insegurança fiscal aos contribuintes, que agora passam a lidar com um sistema analítico automatizado e com mínima participação humana nas análises tributárias preliminares. Por tal cognição, um dos maiores desafios na utilização de IA em matéria tributária é a falta de transparência nos algoritmos utilizados, elemento formal indispensável quanto trata-se de direito público. Ferramentas baseadas em *machine learning* podem tomar decisões fiscais automatizadas sem que os contribuintes ou os próprios fiscais compreendam completamente o raciocínio por trás dessas decisões, elevando o contencioso administrativo e judicial.

Ainda, os algoritmos das ferramentas utilizadas pela SEFAZ-BA são construídos a partir de dados históricos dos contribuintes, e se esses dados contiverem viés, a IA pode replicar e amplificar esses vieses nas suas decisões sistêmicas. No contexto da Administração Tributária Estadual, isso pode significar que determinados setores ou regiões sejam indevidamente alvo de maior fiscalização. Além disso, a detecção de irregularidades pode ser enviesada, gerando injustiças ao tratar de forma desigual contribuintes que operam em situações similares, o que pode prejudicar a equidade na aplicação das normas tributárias.

4 CONCLUSÃO

7 **COAD - Novas tecnologias da Sefaz-BA resultam em arrecadação de R$ 230 milhões**. Disponível em: https://coad.com.br/home/noticias-detalhe/109790/novas-tecnologias-da-sefaz-ba-resultam-em-arrecadacao-de-r-230-milhoes. Acesso em: 11 set. 2024.

Em resumo, a aplicação da inteligência artificial precisa estar alinhada com os objetivos centrais do Direito Tributário, que ela busca auxiliar. Seu propósito não se limita à simples geração de receitas para o Estado, algo que historicamente tem ocorrido independentemente, ou até em oposição, ao Direito[8].

É difícil identificar grandes mudanças que tenham beneficiado as instituições humanas sem que estejam associadas a conflitos fiscais. Nesse cenário, o uso de algoritmos pelas autoridades fiscais deveria representar um avanço expressivo rumo ao futuro, garantindo tanto a proteção quanto a concretização dos direitos dos contribuintes, em vez de nos remeter a um novo período de instabilidades, o qual se visualiza uma nova era de incertezas informacionais nas operações tributárias.

8 MACHADO SEGUNDO, Hugo de Brito. **Inteligência artificial e tributação: a que(m) os algoritmos devem servir?** Disponível em: https://www.conjur.com.br/2019-fev-13/consultor-tributario-inteligencia-artificial-tributacao-quem-algoritmos-servir/ . Acesso em: 12 set. 2024b.

REFERÊNCIAS

CALIENDO, Paulo; LIETZ, Bruna (Coords.) **Direito Tributário e Novas Tecnologias**. Porto Alegre, RS: Editora Fi, 2021.

COAD - Novas tecnologias da Sefaz-BA resultam em arrecadação de R$ 230 milhões. Disponível em: https://coad.com.br/home/noticias-detalhe/109790/novas-tecnologias-da-sefaz-ba-resultam-em-arrecadacao-de-r-230-milhoes . Acesso em: 11 set. 2024.

JARUDE, Jamile Nazare Duarte Moreno. **O estado da arte da fiscalização tributária federal e o uso de inteligência artificial** / Marília: UNIMAR, 2020.

MACHADO SEGUNDO, Hugo de Brito. **Inteligência artificial e tributação: a que(m) os algoritmos devem servir?** Disponível em: https://www.conjur.com.br/2019-fev-13/consultor-tributario-inteligencia-artificial-tributacao-quem-algoritmos-servir/ . Acesso em: 12 set. 2024b.

O que é Machine Learning? Disponível em: https://www.oracle.com/br/artificial-intelligence/machine-learning/what-is-machine-learning/ . Acesso em 11 set. de 2024.

SEFAZ/BA. **Pioneiro no país, Cira já recuperou R$ 560 milhões para a Bahia, e adota novas estratégias de combate à sonegação. Sefaz BA | Secretaria da Fazenda do Estado da Bahia.** 17 jun. 2024. Disponível em: https://www.sefaz.ba.gov.br/noticias/pioneiro-no-pais-cira-ja-recuperou-r-560-milhoes-para-a-bahia-e-adota-novas-estrategias-de-combate-a-sonegacao/ . Acesso em: 11 set. 2024

ZILVETI, F. A. (2019). **As Repercussões da Inteligência Artificial na Teoria da Tributação**. Revista Direito Tributário Atual, (43), 483–498. Disponível em: https://revista.ibdt.org.br/index.php/RDTA/article/view/1457 . Acesso em 11 set. 2024.

O RISCO DE EXPOSIÇÃO E ABUSO DE DADOS PESSOAIS NO TREINAMENTO DE MODELOS DE INTELIGÊNCIA ARTIFICIAL: ANÁLISE DE PRIVACIDADE E SEGURANÇA A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS

Heitor Monteiro Lobo Freire

1 INTRODUÇÃO

Atualmente, o mundo está sendo transformado por serviços de inteligência artificial (IA) cada vez melhores, como o ChatGPT da OpenAI. Nesse contexto, as grandes empresas como o Google têm demonstrado um interesse gigantesco no desenvolvimento de novas tecnologias de IA. Então a partir de sua base de dados de bilhões de usuários globalmente e oferecendo uma variedade de serviços digitais, essa empresa possui um gigantesco volume de dados pessoais que pode ser facilmente utilizado para treinar suas IAs, parte deles já estão sendo utilizados no treinamento do Gemini. No entanto, o uso desses dados para o treinamento de modelos de inteligência artificial levanta questões sobre várias questões éticas importantes sobre privacidade e segurança, especialmente a partir de uma análise da Lei Geral de Proteção de Dados (LGPD) no Brasil. Este artigo tem como objetivo principal analisar os riscos de exposição e abuso de dados pessoais no treinamento de IAs, principalmente da IA Gemini do Google, destacando as implicações legais e de segurança envolvidas.

2 O CONTEXTO DA LGPD E O USO DE DADOS PESSOAIS PARA TREINAMENTO DE IA

A LGPD vem atuando desde 2020 e estabelece regulações rigorosas sobre a coleta, armazenamento, processamento e compartilhamento de dados pessoais. Segundo esta lei, o tratamento de dados pessoais deve obedecer a alguns princípios fundamentais, a exemplo: transparência, necessidade, segurança e responsabilidade, entre outros. Nesse cenário onde empresas de tecnologia como o Google, a Microsoft e a Meta utilizam quantidades de dados quase imensuráveis para treinar suas IAs, nesse contexto surge uma preocupação frequente sobre

como esses dados estão sendo tratados e se o uso destes está em conformidade com a legislação vigente em nosso país.

O uso de dados pessoais no treinamento de IA tem um grande potencial de acabar violando completamente vários desses princípios estabelecidos pela LGPD. Por exemplo, a norma estabelecida pelo princípio da necessidade exige que apenas os dados estritamente necessários para alcançar a finalidade do processamento sejam coletados e utilizados. Todavia, o treinamento de IAs geralmente utiliza um grande número de dados pessoais, muitos dos quais podem não ser essenciais para o objetivo estabelecido. Ademais, o princípio da transparência exige que os titulares dos dados sejam informados sobre como seus dados serão utilizados, o que nem sempre acontece.

3 RISCO DE ABUSO DE DADOS PESSOAIS PELO GOOGLE NO DESENVOLVIMENTO DA IA GEMINI

O Google, com sua vasta rede tecnológica e sua presença em nivel global, tem acesso a um dos maiores bancos de dados pessoais existentes no mundo. A empresa oferece diversos serviços, como Gmail, YouTube, Google Maps, e o próprio mecanismo de busca, que capturam informações detalhadas e vastas sobre as atividades online de todos seus usuários. Se constata que esse volume massivo de dados representa tanto um ativo econômico extremamente valioso à empresa quanto um potencial risco quando usado para o desenvolvimento de IA, como em exemplo principal o modelo Gemini.

Um dos principais riscos associados ao uso de dados pessoais pelo Google para o treinamento de Gemini é o abuso ou a utilização indevida desses dados. Apesar de a empresa afirmar que adere a princípios rígidos de privacidade e segurança, há uma preocupação crescente de que, dado o histórico negativo do Google em termos de práticas de coleta de dados, a empresa possa usar dados pessoais de maneiras indevidas em benefício próprio.

3.1 COLETA E PROCESSAMENTO EXCESSIVOS DE DADOS

Recentemente, o Google tem sido criticado por suas práticas de coleta massiva de dados, muitas vezes algo muito além do necessário estabelecido na relação com o cliente. No caso específico do Gemini, existem preocupações de que o Google esteja utilizando dados de diversos usuários de maneira excessiva, inclusive as informações pessoais consideradas sensíveis, inclusive sem consentimento claro e explícito. Esse comportamento é extremamente problemático segundo o estabelecido na LGPD, que exige que o processamento de dados seja feito de forma limitada apenas ao mínimo necessário para atingir a finalidade declarada.

3.2 CONSENTIMENTO INFORMADO E TRANSPARÊNCIA

A LGPD exige que o consentimento dos titulares dos dados seja informado, especificado e destacado. No entanto, as políticas de privacidade do Google têm

sido constantemente criticadas por sua complexidade e falta de clareza, o que pode dificultar que os usuários consigam compreender exatamente de que forma seus dados estão sendo utilizados no treinamento do Gemini. Assim, a falta dessa transparência pode levar a uma coleta de dados além do que os usuários precisam, contrariando o estabelecido nos princípios da LGPD.

3.3 USO DE DADOS PARA FINS NÃO DECLARADOS

Existe também a possibilidade de que os dados coletados para um propósito específico sejam usurpados pelas empresas para outros fins no desenvolvimento da IA, sem o devido aviso nem consentimento. Por exemplo, podem ser usados dados de navegação, históricos de localização, preferências de consumo e até mesmo dados de e-mails podem ser utilizados para treinar o Gemini, sendo assim uma grande violação dos princípios de finalidade e necessidade da LGPD.

3.4 PROCESSOS LEGAIS CONTRA O GOOGLE (ALPHABET):

Ao olhar para o passado recente podemos ver que o google foi processado diversas vezes por ter abusado do uso de dados pessoais em treinamentos de IAs, um exemplo é o caso do processo movido pela Clarkson Law Firm, alega que a gigante da tecnologia extrai dados de milhões de usuários sem o consentimento deles e violou as leis de direitos autorais para desenvolver seus produtos de inteligência artificial, o processo também alega que o google tem roubado secretamente tudo o que já foi criado e compartilhado na internet por centenas de milhões de americanos.

3.5 INVESTIGAÇÃO DA UNIÃO EUROPEIA:

O google está sofrendo uma investigação na União Europeia (UE) por conta do uso de informações pessoais no treinamento de suas inteligências artificiais (IA) generativas, o que reflete a preocupação internacional crescente com o cumprimento das legislações de proteção de dados, assim como o crescente preocupação com a possibilidade do google estar cometendo diversos abusos no uso desses dados..

4 OS RISCOS ASSOCIADOS AO TREINAMENTO DE MODELOS DE IA COM DADOS PESSOAIS

Os riscos de exposição e abuso de dados pessoais no treinamento de novos modelos de IA são cada vez mais significativos na sociedade. Esses de IA são baseados no aprendizado do modelo, especialmente aqueles que utilizam técnicas de deep learning, frequentemente requerem enormes volumes de dados para alcançar altos níveis de precisão e desempenho. Esse processo pode envolver dados sensíveis, como informações de saúde, dados financeiros e até mesmo históricos de navegação na internet.

A partir dessa análise podemos identificar riscos frequentes que esses treinamentos podem gerar a sociedade:

4.1 RISCO DE REIDENTIFICAÇÃO

Mesmo quando os dados são anonimizados, há o risco de reidentificação, onde indivíduos podem ser identificados a partir de conjuntos de dados que, à primeira vista, não contêm informações diretamente identificáveis. Estudos mostraram que, combinando dados aparentemente inofensivos com outras fontes de dados disponíveis publicamente, é possível inferir a identidade de um indivíduo.

4.2 RISCO DE VIOLAÇÕES DE DADOS

O treinamento das IAs necessita frequentemente de um armazenamento de grandes volumes de dados nos servidores das empresas que podem ser constantes alvos de ataques cibernéticos. Se as medidas de segurança apropriadas não forem tomadas pelas empresas, essas bases de dados correm serios de serem comprometidas, considerando o avanço cada vez mais dos denominados "hackers" em invadir esses servidores, o que pode levar a outros vazamentos massivos de dados pessoais, como já ocorreu diversas vezes recentemente.

4.3 RISCO DE USO INDEVIDO DE DADOS

Dados devem ser coletados para um propósito específico estabelecido, porém em diversos casos podem ser usados para outros fins, incluindo os maliciosos, muitas vezes sem o consentimento devido explícito dos titulares desses dados, como mostrado anteriormente esse uso indevido vem acontecendo frequentemente nas Big Techs.

5 CONCLUSÃO

A partir do contexto observado, vemos que estamos vivendo uma situação atual extremamente perigosa não só no Brasil como mundialmente em relação ao treinamento de IAs, esse treinamento pode acabar colocando em risco severamente todos os usuários de internet e muitas vezes passa completamente dos limites estabelecidos pela LGPD, por isso é urgentemente necessário que o governo através da ANPD comece a fiscalizar de uma forma muito mais rigorosa o que está verdadeiramente sendo feito com nossos dados nesses treinamentos e que seja apurado o comportamento atual das big techs perante nossos dados, o que só pode ser feito com uma significativa alocação de recursos para essa area e com a coragem necessária para enfrentar gigantes de tecnologia extremamente corruptas que têm os melhores advogados do mercado, a partir disso se deve cumprir o que foi estabelecido na legislação quanto às normas da LGPD e assim multar as empresas em atuação indevida até que a lei seja cumprida integralmente.

REFERÊNCIAS

Autoridade Nacional de Proteção de Dados (ANPD). “Lei Geral de Proteção de Dados Pessoais (LGPD)”. Disponível em: https://www.gov.br/anpd/pt-br.

Nascimento, L., & Braga, D. (2021). “Privacidade e Inteligência Artificial: Desafios da LGPD”. Revista Brasileira de Direito Digital, 3(2), 123-135.

Goodman, B., & Flaxman, S. (2017). “European Union Regulations on Algorithmic Decision-Making and a ‘Right to Explanation’”. AI Magazine, 38(3), 50-57.

Veale, M., & Edwards, L. (2018). “Clarity, Surprises, and Further Questions in the GDPR”. Law, Innovation, and Technology, 10(2), 157-207.

Zuboff, S. (2019). “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”. PublicAffairs.

https://www.cnnbrasil.com.br/tecnologia/google-e-processado-por-rouba r-dados-de-usuarios-para-treinar-suas-ferramentas-de-ia/

https://olhardigital.com.br/2024/09/12/pro/uso-de-dados-para-treinar-ia-c oloca-google-na-mira-da-uniao-europeia/

A TRANSPARÊNCIA E O DIREITO DE SE OPOR NA NOVA POLÍTICA DE PRIVACIDADE DA META E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DIANTE DO USO DE DADOS PESSOAIS DE POSTAGENS EM REDES SOCIAIS PARA TREINAR INTELIGÊNCIA ARTIFICIAL

Heloisa Midlej Cardoso Seixas [1]

RESUMO

O presente trabalho tem como objetivo analisar os riscos e ofensa à lei geral de proteção de dados pessoais no que concerne ao dever de ser transparente acerca de alterações na política de privacidade ao utilizar dados pessoais de contas de redes sociais para treinar inteligência artificial e ao direito de se opor atualização na política de privacidade. Se analisa o fato que a Autoridade Nacional de Proteção de Dados (ANPD), autarquia vinculada ao Ministério da Justiça, em 2024, emitiu uma medida preventiva que determina à empresa Meta que suspenda imediatamente o uso de dados pessoais para treinamento de sistemas de inteligência artificial no Facebook, no Instagram e no Messenger. O presente trabalho busca ser desenvolvido através de uma pesquisa exploratória e qualitativa, de cunho documental e bibliográfico, e se destina a explicar como a nova política de privacidade da Meta desrespeitou a LGPD e como se justificam os atos da ANPD.

PALAVRAS-CHAVE: Inteligência Artificial; Meta; Instagram; Facebook; Messenger.

ABSTRACT

The present work aims to analyze the risks and offenses regarding the duty to be transparent about changes to the privacy policy and the general personal data protection law when using personal data from social media accounts to train

1 Graduanda em Direito. Faculdade Baiana de Direito. https://lattes.cnpq.br/2680926198186989.

artificial intelligence and the right to object to updates to the privacy policy. The work seeks to analyze the fact that the National Data Protection Authority (ANPD), an agency linked to the Ministry of Justice, in 2024, issued a preventive measure that orders the company Meta to immediately suspend the use of personal data for system training of artificial intelligence on Facebook, Instagram and Messenger. This work seeks to be developed through exploratory and qualitative research, of a documentary and bibliographic nature, and is intended to explain how Meta's new privacy policy disrespected the LGPD and how the ANPD's acts are justified.

KEY-WORDS: Artificial Intelligence; Meta; Instagram; Facebook; Messenger.

INTRODUÇÃO

O presente trabalho objetiva analisar a o direito de se opor que dados pessoais de contas de redes sociais sejam utilizados para treinar inteligência artificial, diante do fato que, no ano de 2024, a Meta atualizou a política de privacidade, com novo texto o qual permite que utilize as informações publicamente disponíveis e conteúdos compartilhados pelos usuários para treinamento e aperfeiçoamento dos sistemas de inteligência artificial.

Se traz a hipótese que, de fato, ao atualizar política de privacidade, com novo texto o qual permite que utilize as informações publicamente disponíveis e conteúdos compartilhados pelos usuários para treinamento dos sistemas de inteligência artificial generativa, a Meta, no Brasil, ofendeu a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), observando como teria acontecido tal ofensa em detalhes no que toca a transparência e direito de se opor a ceder dados para treinar a inteligência artificial.

Diante da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), todos aqueles que puderem manipular dados brasileiros devem buscar observar suas normas, estando diante da possibilidade de responsabilidade caso desrespeitem a LGPD. Consequentemente, o presente artigo se justifica na possibilidade tanto de saber mais sobre a política de privacidade da Meta, quanto acerca dos desdobramentos desta atitude diante da possibilidade de ter sido estabelecido um contexto do uso de dados de brasileiros para treinar inteligência artificial sem amplo aviso para os usuários e o modo como decidiram por realizar tal tratamento de dados para treinamento de inteligência artificial em tais redes sociais.

O trabalho, visando ser desenvolvido através de uma pesquisa exploratória e qualitativa, de cunho documental e bibliográfico, se destina a explicar como a nova política de privacidade da Meta desrespeitou a LGPD e como se justificam os atos da ANPD com foco na transparência e direito de se opor ante atualização de política de privacidade, e podendo revogar anuência, a análise documental sendo uma técnica importante na pesquisa qualitativa.

O trabalho adota o tipo de pesquisa bibliográfica e qualitativa, trazendo

como pressuposto básico a utilização de variados fundamentos teóricos da literatura acadêmica, como artigos, lei, entre outras fontes, com a finalidade de atingir uma conclusão adequada sobre os pontos controversos acerca da temática aqui trabalhada, visto que este tipo de pesquisa encontra-se como o mais recomendado dentre o rol existente para realizar essa análise das mais variadas posições voltadas a determinado problema.

Para mais, no que toca a metodologia escolhida, se escolheu o método hipotético-dedutivo, ao levar em consideração as hipóteses que foram levantadas dentro do recorte temático escolhido e a necessidade que se tem de verificação da realidade, o que permite sua validação no campo científico da maneira que se é pretendida.

2 A MEDIDA PREVENTIVA DA ANPD

A Autoridade Nacional de Proteção de Dados (ANPD), autarquia vinculada ao Ministério da Justiça, emitiu, em 2024, uma medida preventiva que determina à Meta que suspenda imediatamente o uso de dados pessoais para treinamento de sistemas de inteligência artificial no Facebook, no Instagram e no Messenger. Ademais, caso a determinação fosse descumprida, haveria uma multa no valor de R$ 50 mil por dia (CNN, 2024).

Em junho de 2024, a Meta atualizou sua política de privacidade, desencadeando os eventos gerados a partir disto, posto que a ANPD identificou partes desta nova política de privacidade as quais não estariam de acordo com a LGPD (Forbes, 2024). Consoante a ANPD, importante destacar que o tratamento de dados aos quais as redes sociais sob controle da Meta adotam pode impactar uma quantidade substancial de pessoas, podendo se citar de modo exemplificativo que, considerando apenas o Facebook, tal rede social possui mais de 100 milhões de usuários ativos, o novo texto permite que a Meta utilize as informações publicamente disponíveis e postagens compartilhadas pelos usuários para treinamento e aprimorar sistemas de inteligência artificial generativa em sistema opt-out (CNN, 2024).

Acerca disto, a autarquia informou que instaurou o processo de fiscalização em virtude de "indícios de violações à Lei Geral de Proteção de Dados (LGPD)". Informou ainda que "Após análise preliminar, diante dos riscos de dano grave e de difícil reparação aos usuários, a Autoridade determinou cautelarmente a suspensão da política de privacidade e da operação de tratamento." A partir disso, se pode buscar saber, diante das palavras da ANPD, quais seriam os riscos de dano grave, bem como qual seria a lista itemizada de desrespeitos a LGPD no caso em pauta os quais justificaram a necessidade que fosse a emitida medida preventiva.

A ANPD cita problemas na nova política de privacidade da meta que teriam justificado a medida protetiva:

> (...) uso de hipótese legal inadequada para o tratamento de dados pessoais; falta de divulgação de informações

> claras, precisas e facilmente acessíveis sobre a alteração da política de privacidade e sobre o tratamento realizado; limitações excessivas ao exercício dos direitos dos titulares; e tratamento de dados pessoais de crianças e adolescentes sem as devidas salvaguardas (CNN, 2024).

Consoante a ANPD, a Meta:

> (...) não forneceu informações adequadas e necessárias para que os titulares tivessem ciência sobre as possíveis consequências do tratamento de seus dados pessoais para o desenvolvimento de modelos de IA generativa" (...). "A Autoridade averiguou, ainda, que, embora os usuários pudessem se opor ao tratamento de dados pessoais, havia obstáculos excessivos e não justificados ao acesso às informações e ao exercício desse direito." (CNN, 2024).

3 A NOVA POLÍTICA DE PRIVACIDADE DA META E A LGPD

Posto que foi apresentado o ocorrido, tendo a ANPD considerado que a LGPD foi desrespeitada, aqui, se vai buscar citar em quais partes da LGPD, especificamente, se pode encontrar os trechos alvo do desrespeito da transparência e direito de se opor os quais a Meta pode ter desconsiderado. Consoante o artigo primeiro da LGPD, tal Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, objetivando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Consoante a ANPD, os problemas com a nova política de privacidade da Meta podem ser listados em uso de hipótese legal inadequada para o tratamento de dados pessoais; falta de divulgação de informações claras, precisas e facilmente acessíveis sobre a alteração da política de privacidade e sobre o tratamento realizado; limitações excessivas ao exercício dos direitos dos titulares; e tratamento de dados pessoais de crianças e adolescentes sem as devidas salvaguardas. Observado a LGPD, se pode observar quais artigos a justificam, neste trabalho, buscando se dar destaque ao requisito da transparência e o direito de se opor.

Para fins de esclarecimento, se busca trazer que o Art. 5º da LGPD considera dado pessoal como informação relacionada a pessoa natural identificada ou identificável. Isto posto, considerando que o Art. 7º O tratamento de dados pessoais somente poderá ser realizado em hipóteses que lista, sendo, uma delas, no inciso I, "mediante o fornecimento de consentimento pelo titular". Neste ponto, cabe trazer os termos opt-in e opt-out.

Considerando que os termos, os quais significam, "opt-in", circunstância na qual o padrão é que o usuário não participe, podendo optar por aderir, e, "opt-out", circunstância na qual o padrão é que o usuário participe, podendo optar por sair, logo, no opt-in, se pode optar por entrar, e no opt-out, se pode optar por sair (Andrade, 2008, p. 35). Assim, se pode concluir que, sendo preciso o consentimento dos usuários para o tratamento de dados pessoais, consoante

a LGPD, deveria ter sido escolhido um sistema opt-in, e não um sistema opt-out para o cumprimento da lei. Ou, pelo menos, maior transparência e aviso de atualização em seus termos e condições para atualizar a anuência dos usuários (Mulholland, 2018, p. 163).

Ainda, consoante Art. 8°, § 3º da mesma lei, consta ser vedado o tratamento de dados pessoais mediante vício de consentimento, o que se pode considerar haver ao não se informar de modo eficaz acerca e, no § 5º do mesmo artigo 8°, se pode ler que "o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado", e, no § 6º, "em caso de alteração" tanto o titular deve ser informado sobre a alteração, quanto pode revogar seu consentimento caso discorde da alteração. Contudo, o modo de se opor ao uso de dados pessoais para treinamento de inteligência artificial por redes sociais da Meta seria dificultoso e contra intuitivo, tendo sido necessário preencher um formulário para se opor ao uso dos conteúdos (Magalhães, 2024).

Em detalhes, seria preciso acessar site específico da rede social da Meta na qual se deseja opor ao uso dos dados pessoais para treinamento de inteligência artificial, ir até a seção "Privacidade e IA generativa", clicar na opção "direito de se opor", destacada em azul, preencher formulário com país de residência, endereço de e-mail e o motivo do pedido, pressionar "enviar", confirmar o envio com um código de seis dígitos recebido por e-mail, e na parte do campo "Contenos como esse processamento afeta você", se poderia informar que não deseja que a Meta use os conteúdos pessoais para o treinamento de IA (Magalhães, 2024). Após o envio, o Instagram, por exemplo, enviaria um e-mail para confirmar o recebimento e informar que deve analisar o pedido. Diante disso, fica evidente o descumprimento à LGPD.

CONCLUSÃO

Finalmente, se pode concluir que os usuários das redes sociais da Meta deveriam ter sido mais amplamente informados acerca das alterações nas políticas de privacidade, consoante artigos da Lei Geral de Proteção de Dados, transparência e adequação ao direito de se opor, tendo havido de fato necessidade de que a Meta mostrasse adequação da política de privacidade consoante aduz a ANPD antes que fosse alterada, devendo ela ser adaptada à lei.

REFERÊNCIAS

ANDRADE, Richarson Lobo de. **A personalização em e-mails promocionais.** 2008. 104f. – Dissertação (Mestrado) – Universidade Federal do Ceará, Departamento de Letras Vernáculas, Programa de Pós-graduação em Linguística, Fortaleza (CE), 2008. Disponível em: http://repositorio.ufc.br/handle/riufc/8773. Acesso em 14 set. 2024.

CNN. Meta é proibida de usar dados de usuários para treinamento de inteligência artificial no Instagram e Facebook. Medida preventiva foi emitida nesta terça-feira (2) pela Autoridade Nacional de Proteção de Dados (ANPD). **CNN**. 02 jul. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/meta-e-proibida-de-usar-dados-de-usuarios-para-treinamento-de-inteligencia-artificial-no-instagram-e-facebook/. Acesso em 14 set. 2024.

FORBES. Brasil suspende nova política de privacidade da Meta. O órgão ligado ao Ministério da Justiça cita o "risco iminente de dano grave e irreparável aos direitos fundamentais dos titulares afetados". **Forbes.** 02 jul. 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/07/brasil-suspende-nova-politica-de-privacidade-da-meta/. Acesso em 14 set. 2024.

LEI nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República,. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 abr. 2021. Acesso em 14 set. 2024.

MAGALHÃES, André Lourenti. Como evitar que a Meta use suas imagens em Inteligências Artificiais. É possível pedir para a Meta não treinar as ferramentas de IA da empresa com seus dados do Instagram ou do Facebook; saiba como. **Terra.** 17 jun. 2024. Disponível em: https://www.terra.com.br/byte/como-evitar-que-a-meta-use-suas-imagens-em-inteligencias-artificiais,f8ae61f3df901362db53540b4b5933bfo89bukrr.html#:~:text=Abra%20o%20menu%20lateral%20e,Envie%20o%20formul%C3%A1rio. Acesso em 14 set. 2024.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8697583. Acesso em 14 set. 2024.

SOBRE AS ORGANIZADORAS DESTES ANAIS

Christine Albiani

Advogada atuante em Compliance Digital e Proteção de Dados. Especialista em Direito Processual Civil e Direito Tributário. Certificada profissionalmente em Visual Law (CPVL) - Opice Blum Academy em parceria com a FGV Projetos. Graduada em Direito pelo Instituto Brasileiro de Mercado de Capitais (Ibmec RJ) com láurea acadêmica Summa Cum Laude. MBA em Gestão Tributária pela USP. Mestra em Direito pela UFBA. Autora do livro "Violação de direitos autorais e responsabilidade civil do provedor diante do Marco Civil da Internet". Integrante do 3º Grupo de Pesquisa do Instituto de Tecnologia e Sociedade (ITS-Rio) sobre Inteligência Artificial e Inclusão. Membra do Instituto dos Advogados da Bahia (IAB).

Maria Clara Seixas

Sócia da 4S Advocacia. Especialista em Direito Digital, IA Law, Proteção de Dados Pessoais, Governança Riscos e Compliance- GRC e Empresarial. Professora do INSPER, da Cubos Academy e Coordenadora do curso de LGPD e Privacidade da Faculdade Baiana de Direito. Pesquisadora em IA, Ética, Direito e Tecnologia e mestranda no tema pela UFBA. PDPP - EXIN Privacy & Data Protection Professional. Premiada como uma das advogadas mais admiradas do país em Direito Digital e Compliance pela Revista Análise Nacional e listada na Revista Compliance OnTop.


FACULDADE
BAIANA DE
DIREITO