TECNOLOGIA DEEPFAKE NO AMBIENTE CORPORATIVO: DESAFIOS ÉTICOS E GOVERNANÇA PARA UMA RESPONSABILIDADE SOCIAL ALINHADA AO ESG

Deepfake Technology in the Corporate Environment: Ethical Challenges and Governance for Social Responsibility Aligned with ESG

Melissa Chanazis Valentini [1]

Universidade Federal de Santa Catarina

Vilson Gruber [2]

Universidade Federal de Santa Catarina

Vladimir Malagues [3]

Faculdade Porto-Alegrense

DOI: https://doi.org//10.62140/MVVGVM5852025

[1] Bacharel em Direito. Pós-graduada em Direito do Trabalho, Direito Tributário e Neurociências Aplicada ao Direito. Mestranda no Programa de Tecnologia Universidade Federal de Santa Catarina – Campus Araranguá. Advogada e Chief Compliance Offcier. Professora da BSSP E CESUSC. E – mail: mcvjuridico@gmail.com – Link: https://orcid.org/0009-0008-8621-3387.

[2] Bacharel em Processamento de Dados pelo Centro Universitário Sant'Anna (1996), mestrado (2007) e doutorado (2010) em Engenharia de Minas, Metalúrgica e de Materiais pela Universidade Federal do Rio Grande do Sul. Atualmente, é professor com dedicação exclusiva da Universidade Federal de Santa Catarina – Campus Araranguá, atuando na graduação e pós-graduação (Stricto Sensu). Lidera o LABTEL (Laboratório de Telecomunicações) e é membro pesquisador do LPA (Laboratório de Pesquisa Aplicada) e do GDER (Grupo de Desenvolvimento em Energias Renováveis). Sua atuação nesses grupos de pesquisa tem sido crucial para o avanço do conhecimento e a aplicação prática de inovações em gestão, tecnologias emergentes e sustentabilidade. E – mail: vilson.gruber@ufsc.br . Link: Orcid: https://orcid.org/0000-0003-4092-8578.

[3] Bacharel em Ciências Contábeis na Faculdade Porto-Alegrense do Rio Grande do sul, Auditor Independente, Signatário do Movimento ODS do Rio Grande do Sul., vladirs@hotmail.com, Link Orcid https://orcid.org/0009-0002-5989-8663.

Sumário: 1. Introdução; 2. Materiais e Métodos; 3. Resultado e Discussão: 3.1. Deepfakes no Ambiente do Trabalho; 3.2. ESG como Estratégia de Proteção aos Direitos Fundamentais e Reputacionais; 4. Legislação Brasileira e o Direito Comparado. 5. Conclusão.

Resumo: O uso de tecnologias avançadas, como deepfakes, está moldando o ambiente corporativo, trazendo tanto novas oportunidades quanto desafios éticos e legais. Este trabalho tem como objetivo investigar os impactos dos deepfakes no contexto empresarial, com foco na gestão de riscos e na responsabilidade social corporativa, alinhando-se aos princípios ESG (Ambiental, Social e Governança). O tema central emerge da potencial utilização dessa tecnologia para manipulação, difamação e outras práticas antiéticas, além de propor estratégias de mitigação de riscos e proteção dos direitos fundamentais dos trabalhadores. Ao final, discute-se a importância de adotar uma abordagem ética e responsável no uso dessas tecnologias, destacando a governança como pilar essencial para a construção de um ambiente corporativo mais seguro e transparente.

Palavra-chave: Deepfake, ESG, Responsabilidade Social Corporativa, Tecnologia.

Abstract: The use of advanced technologies, such as deepfakes, is shaping the corporate environment, bringing both new opportunities and ethical and legal challenges. This paper aims to investigate the impacts of deepfakes in the business context, focusing on risk management and corporate social responsibility, in alignment with ESG principles (Environmental, Social, and Governance). The central theme arises from the potential use of this technology for manipulation, defamation, and other unethical practices, as well as proposing strategies for risk mitigation and protection of workers' fundamental rights. In the end, the paper discusses the importance of adopting an ethical and responsible approach in the use of these technologies, highlighting governance as an essential pillar for creating a safer and more transparent corporate environment.

Keywords: Deepfake; ESG; Corporate Social Responsibility; Technology.

1. INTRODUÇÃO

O avanço das tecnologias disruptivas tem gerado significativos impactos no ambiente corporativo, exigindo uma nova abordagem em relação à governança, à responsabilidade social das empresas e à proteção dos direitos fundamentais

garantidos pela Constituição Federal. Uma das inovações mais controversas é o deepfake, tecnologia que utiliza inteligência artificial para criar ou alterar conteúdos visuais e auditivos, frequentemente de maneira quase indistinguível da realidade.

A tecnologia digital transformou profundamente o ambiente empresarial, introduzindo novas ferramentas que redefinem a forma como as empresas operam e se relacionam com a sociedade. No entanto, essas inovações também trazem vícios, como a manipulação informacional por meio de deepfakes, gerando desinformação. Esses fenômenos podem comprometer a confiança pública, a reputação corporativa e os princípios de responsabilidade social, além de violar direitos fundamentais, como a honra, a imagem e a privacidade, previstos no artigo 5º da Constituição Federal.

No contexto laboral, os deepfakes representam uma ameaça que vai além do entretenimento, podendo ser usados para difamação de colaboradores, manipulação de evidências ou até mesmo sabotagem corporativa. Tais práticas podem ferir o direito à dignidade da pessoa humana, princípio basilar da ordem constitucional brasileira. Em paralelo, o movimento ESG exige que as empresas adotem transparências, posturas éticas e sustentáveis, incluindo o uso responsável de tecnologias.

Este capítulo aborda como os deepfakes desafiam os princípios ESG e como as empresas podem gerenciar esses riscos, protegendo não apenas sua reputação, mas também os direitos fundamentais de seus colaboradores e demais partes interessadas. Incluir esse tema na matriz de risco de uma empresa demonstra maturidade organizacional e compromisso com a proteção de seus ativos, colaboradores e stakeholders, sendo essencial para garantir uma abordagem proativa diante dos desafios trazidos por tecnologias disruptivas.

2. MATERIAIS E MÉTODOS

Este estudo adota uma abordagem qualitativa, fundamentada em pesquisas bibliográficas e em informações disponíveis na internet sobre deepfakes, responsabilidade social corporativa e ESG. Foram considerados casos reais e

iniciativas de governança tecnológica para evidenciar os principais desafios e oportunidades no contexto empresarial.

3. RESULTADOS E DISCUSSÃO

3.1. DEEPFAKES NO AMBIENTE DO TRABALHO

A introdução das tecnologias avançadas, como os deepfakes, no ambiente de trabalho, gerou novos desafios e oportunidades para as empresas. Os resultados discutidos são baseados na análise de casos reais, bem como na reflexão de práticas de governança tecnológica e nas orientações encontradas em fontes de informação confiáveis.

Recentemente o STF publicou um guia ilustrado contra as feepfakes, conceituando em tradução livre que 'as deepfakes nada mais são do que "falsidades profundas", ou seja, conteúdos falsos produzidos com um alto grau de elaboração' (STF, 2024).

As deepfakes são conteúdos falsificados gerados por inteligência artificial, com um nível de realismo tão elevado que podem ser difíceis de identificar como fraudulentos. Essas manipulações envolvem técnicas como substituição de rostos, clonagem de voz e alterações detalhadas, como a movimentação da boca para sincronizar com declarações falsas. Deepfakes têm o poder de nos convencer de que alguém disse algo que nunca diria, fez algo que jamais faria ou esteve em situações que nunca ocorreram. Isso pode resultar em uma ampla gama de consequências, desde golpes financeiros e fraudes diversas até tentativas de manipular agendas públicas e privadas.

Em 2017, pesquisadores da Universidade de Washington desenvolveram um projeto que utilizava técnicas de inteligência artificial para criar vídeos realistas do ex-presidente Barack Obama. O sistema analisava áudios de discursos de Obama e, por meio de redes neurais, gerava movimentos labiais correspondentes, combinando-os com imagens de alta qualidade para produzir vídeos nos quais Obama parecia falar

frases que, na realidade, ele nunca pronunciou (WASHINGTON UNIVERSITY, 2017).

Este projeto destacou o potencial e os riscos associados às tecnologias de deepfake, evidenciando a facilidade com que vídeos falsos, mas altamente realistas, podem ser criados. A pesquisa também serviu como um alerta sobre a necessidade de desenvolver métodos para detectar e combater a desinformação gerada por essas tecnologias.

O Tribunal Superior Eleitoral (TSE) regulamentou, de forma pioneira, o uso de inteligência artificial (IA) na propaganda eleitoral para as Eleições Municipais de 2024. A decisão resultou em alterações na Resolução nº 23.610/2019, redação dada pela Resolução nº 23.732/2024, estabelecendo medidas importantes, como a proibição de deepfakes, a obrigatoriedade de informar sobre o uso de IA na propaganda eleitoral, a restrição do uso de robôs para simular interações com eleitores e a responsabilização das grandes empresas de tecnologia (big techs) pela não remoção de conteúdos como desinformação, discursos de ódio e ideologias nazistas, fascistas, antidemocráticas, racistas e homofóbicas. Essas mudanças buscam promover maior transparência, integridade e segurança no processo eleitoral (TSE, 2024).

De acordo com um levantamento realizado pela empresa de soluções de cibersegurança Fortinet, com dados fornecidos pelo FortiGuard Labs, o Brasil ocupou a segunda posição entre os países mais atingidos por ataques cibernéticos na América Latina em 2022. Foram registradas 103,16 bilhões de tentativas de ataques, representando um aumento significativo de 16% em relação ao ano anterior, quando o total foi de 88,5 bilhões (FORTINET, 2023).

Conforme apontam Santaella e Salgado (2021), "quanto menor for a confiabilidade, por exemplo, de informações obtidas em redes digitais ou mecanismos de pesquisa online, mais grave fica a situação da estabilidade social e mais difícil será recuperar a confiança das pessoas."

Um estudo da University College London revelou que, em 27% dos casos analisados, os participantes não conseguiram identificar se a fala era real ou um

deepfake. No Brasil, a Accenture Technology Vision 2022 mostrou que 100% dos executivos relatam preocupação com fraudes (61%), violações de TI (58%) e danos à reputação (47%) relacionados a deepfakes(UCL, 2021).

O uso de deepfakes para manipulação de imagens, vídeos e áudios, especialmente no ambiente de trabalho tem um impacto profundo nas dinâmicas organizacionais. Sabe-se que além dos danos causados ao empregados e terceiros, escândalos envolvendo tecnologia podem danificar gravemente a imagem das empresas. A manipulação de conteúdo visual e auditivo por meio dessa tecnologia tem se mostrado uma ameaça crescente à confiança nas relações internas e externas das empresas. Em casos de difamação ou manipulação, a empresa e os colaboradores podem ser diretamente prejudicados.

Conforme dados do Instituto de Ensino Superior – ICEV, um exemplo impactante é o caso de um CEO que foi vítima de um ataque de deepfake, onde sua voz foi clonada para autorizar uma transferência financeira de US$ 243 mil para uma conta fraudulenta. O ataque foi realizado de forma tão convincente que os responsáveis pela transação não desconfiaram de nada até que o erro fosse detectado. Esse caso ilustra como deepfakes podem ser utilizados para fraudar e manipular transações corporativas, prejudicando diretamente a segurança financeira e a confiança nas lideranças da empresa (DCIBER, 2023).

Outro caso emblemático de golpe envolvendo deepfake foi relatado pelo Banco do Brasil. A situação ocorreu com um funcionário de uma multinacional em Hong Kong durante uma videoconferência fraudulenta. Convencido de que estava em uma reunião legítima com o diretor financeiro da empresa, o funcionário realizou transferências que totalizaram aproximadamente US$ 25,60 milhões (cerca de R$ 127 milhões) para contas pertencentes a golpistas. Curiosamente, todos os demais participantes da reunião eram falsificações criadas por inteligência artificial, manipulando imagens e áudios autênticos para enganar a vítima (BANCO DO BRASIL, 2023).

A capacidade de deepfakes de prejudicar a reputação de colaboradores é grandiosa, manipulações de vídeos ou áudios podem ser usadas para criar situações comprometedoras, resultando em danos à reputação empresarial e à imagem e à carreira dos indivíduos envolvidos. Isso pode resultar em dipensas indevidas,

mudanças na cultura organizacional e perda de confiança dentro da empresa. Portanto, a utilização de deepfakes de forma maliciosa coloca em risco a integridade das relações de trabalho e compromete os valores de responsabilidade e respeito.

Percebe-se que os deepfakes podem ser usados para criar falsas acusações contra empregados ou empregadores, dificultando a verificação de fatos. Conteúdos manipulados podem ser utilizados para assediar moralmente colaboradores, comprometendo o ambiente organizacional, resultando em prejuízos financeiros e/ou estratégicos.

A governança tecnológica é um aspecto fundamental para mitigar os riscos associados aos deepfakes no ambiente corporativo. Empresas devem adotar práticas de governança robustas, que garantam a implementação de controles internos eficazes e a promoção de uma cultura de responsabilidade social corporativa.

O alinhamento da governança tecnológica aos princípios ESG é essencial para o sucesso dessa mitigação. A responsabilidade social no contexto ESG envolve garantir a transparência, a ética e a proteção dos direitos dos colaboradores. Para lidar com os riscos gerados por deepfakes, é necessário criar políticas internas que garantam a segurança da informação e a veracidade dos conteúdos compartilhados. Ferramentas de monitoramento e validação de conteúdos, como a verificação de vídeos e áudios, podem ser implementadas para detectar e prevenir o uso indevido de tecnologias de deepfake.

Além disso, programas de conscientização são necessários para educar os colaboradores sobre os riscos dessas tecnologias e os métodos usados por golpistas. Isso inclui o treinamento em como verificar comunicações e identificar sinais de manipulação.

A proteção contra deepfakes no ambiente corporativo requer uma abordagem multifacetada. Um exemplo disso é o caso mencionado anteriormente do CEO, onde a falta de verificação da solicitação de transferência foi um dos principais fatores que permitiu que o golpe acontecesse. A implementação de práticas de verificação de múltiplos canais, como a confirmação por telefone ou outras formas de comunicação segura, é uma das maneiras de reduzir os riscos de manipulação.

Além disso, o uso de tecnologias de detecção de deepfakes pode ser uma estratégia eficaz para detectar manipulações em conteúdos compartilhados dentro da empresa. A implementação de algoritmos de IA que identificam alterações em imagens, áudios ou vídeos pode ajudar a detectar e barrar conteúdos falsificados antes que sejam distribuídos.

A educação contínua dos colaboradores é um aspecto essencial para reduzir o risco de fraude e manipulação de conteúdo. Programas de treinamento em segurança digital devem ser realizados com regularidade, ensinando os colaboradores a reconhecer e responder a conteúdos suspeitos. Empresas também podem investir em ferramentas de software que ajudem a verificar a autenticidade de documentos e comunicações.

3.2. ESG COMO ESTRATÉGIA DE PROTEÇÃO AOS DIREITOS FUNDAMENTAIS E REPUTACIONAIS

No Brasil, a temática ESG encontra respaldo na ABNT PR 2030, que, embora não tenha caráter normativo, é amplamente reconhecida como uma prática recomendada aplicável a organizações de diversos portes.

A PR 2030 destaca o ESG como um conjunto abrangente de critérios que integra aspectos ambientais, sociais e de governança, oferecendo uma abordagem estratégica para a sustentabilidade nas empresas. Esses critérios orientam a identificação de riscos e oportunidades, bem como a avaliação dos impactos das atividades empresariais, negócios e investimentos, promovendo a adoção de práticas alinhadas às melhores diretrizes globais (ABNT, 2022).

A PR 2030 destaca como o eixo social (S) um papel significativo na condução do compliance e da governança em uma sociedade cada vez mais ampla e diversificada. A prática recomendada organiza esse eixo em cinco grandes temas, cada um com critérios específicos.

Primeiro Tema (S): **Diálogo Social e Desenvolvimento Territorial**: Este tema aborda critérios como **o investimento social privado,** o **diálogo e engajamento das partes interessadas** e o **impacto social,** reforçando a

importância de parcerias e ações que beneficiem comunidades locais. **Segundo Tema (S): Direitos Humanos:** Enfatiza o **respeito aos direitos humanos** e o combate a práticas abusivas, como o **trabalho forçado ou compulsório** e o **trabalho infantil**, promovendo um ambiente de trabalho ético e responsável. **Terceiro tema (S): Diversidade, Equidade e Inclusão:** Este tema abrange **políticas e práticas voltadas à diversidade e equidade,** bem como a **cultura e promoção de inclusão,** reconhecendo a importância de ambientes organizacionais diversos e justos. **Quarto tema (S): Relações e Práticas de Trabalho:** Focado no bem-estar dos colaboradores, aborda critérios como o **desenvolvimento profissional, saúde e segurança ocupacional, qualidade de vida, liberdade de associação** e **políticas de remuneração e benefícios. Quinto tema (S): Promoção de Responsabilidade Social na Cadeia de Valor:** Enfatiza o **relacionamento com consumidores e clientes,** bem como com **fornecedores,** promovendo uma cadeia de valor ética e socialmente responsável (ABNT, 2024).

Esses temas reforçam a importância de práticas sociais robustas e integradas, alinhadas aos princípios de governança corporativa e compliance, para promover impacto positivo e sustentável na sociedade.

No que tange à sigla (G) governança corporativa, refere-se ao eixo que desempenha um papel crucial na organização dos processos internos e externos, garantindo a integridade da empresa por meio de um compliance adequado.

A PR 2030 aborda o eixo da governança com quatro pilares fundamentais, enfatizando que a governança é a força motriz que garante uma gestão empresarial responsável e ética. Destaca o pilar da **Primeiro tema (G): Governança Corporativa**. Este pilar trata de critérios como a **estrutura e composição da governança corporativa**, bem como o **propósito e a estratégia voltados para a sustentabilidade**, assegurando uma direção alinhada aos princípios éticos e de longo prazo. Segundo tema (G): **Conduta Empresarial**. Aborda aspectos essenciais como o **compliance**, a implementação de **programas de integridade** e **práticas anticorrupção**, além de iniciativas para **combater a concorrência desleal (antitruste)** e promover o **engajamento efetivo das partes interessadas**. Terceiro

tema (G): **Práticas de Controle e Gestão**. Enfatiza a **gestão de riscos do negócio**, os **controles internos**, a realização de **auditorias internas e externas**, a conformidade com o **ambiente legal e regulatório**, e a **gestão da segurança da informação e da privacidade de dados pessoais**, garantindo a proteção e a resiliência organizacional. Quarto tema (G): **Transparência na Gestão**. Destaca a importância da **responsabilização** por meio da prestação de contas e da publicação de **relatórios ESG**, relatórios de sustentabilidade ou relatos integrados, assegurando clareza e confiança nas ações corporativas (ABNT, 2024).

Um dos grandes temas, refere-se às práticas de controle e gestão, desde o compliance, a auditorias internas e externas, como a gestão da segurança da informação e privacidade de dados pessoais.

Valentini (2024), afirma que "o compliance pode ser um aliado poderoso na implementação de práticas ESG, especialmente quando analisado dentro da perspectiva da prática recomendada 2030 da ABNT."

A cartilha adotada pelo IBGC, destaca sobre a identidade da organização, com uma reflexão que é fundamental para se desenhar o sistema de governança, incluindo a elaboração de um código de conduta sobre o qual se desenvolve o sistema de conformidade (compliance). Chama-se atenção que além do código de conduta e ética, a empresa também pode fornecer aos seus colaboradores um ordenamento educativo codificado sobre normas de segurança digital (IBGC, 2023).

Empresas devem implementar práticas de auditoria e transparência em suas tecnologias. Treinamento contínuo das equipes para identificar e mitigar riscos tecnológicos. Comunicação aberta com stakeholders sobre o uso responsável de tecnologias digitais.

De acordo com Freeman (1984, p. 46), os stakeholders são definidos como "qualquer grupo ou indivíduo que pode afetar ou ser afetado pela realização dos objetivos da empresa". No contexto do ESG (Ambiental, Social e Governança), os stakeholders desempenham o papel de um verdadeiro estratégico "guarda-chuva" para as organizações, conforme já abordado por (FREEMAN, 1983). Nesse cenário,

torna-se essencial desenvolver estratégias direcionadas, com foco específico em investidores e fornecedores, que são grupos de alto impacto nas operações e lucros corporativos.

A necessidade de estratégias integradas de curto, médio e longo prazo é evidente, especialmente para fortalecer os planos de continuidade e resiliência da empresa. Esse fortalecimento demonstra a capacidade da organização de se manter competitivo no mercado, mesmo em um ambiente de rápidas transformações tecnológicas. Entretanto, com o avanço exponencial das tecnologias, como os deepfakes, que podem ser usados para fins maliciosos, as estratégias tradicionais precisam evoluir.

Além de adotar os devidos cuidados com investidores e fornecedores que geram impacto significativo nas operações, a empresa deve simultaneamente implementar uma estratégia de responsabilidade social que contemple outras partes interessadas essenciais, como funcionários, comunidades, acionistas e consumidores. É fundamental garantir que o impacto gerado sobre esses grupos seja positivo e alinhado aos princípios do ESG.

É necessário incluir tecnologias de prevenção e detecção no planejamento estratégico. Ferramentas de inteligência artificial e sistemas de monitoramento em tempo real devem ser incorporados para proteger a integridade da empresa e garantir que as práticas de ESG não sejam comprometidas, garantindo a confiança das partes interessadas e a sustentabilidade do negócio.

Embora os conteúdos gerados com deepfake estejam cada vez mais avançados, em muitos casos é possível identificar indícios de manipulação, por isso é primordial a responsabilidade do empregador nos treinamentos, pois há sinais para o reconhecimento de falsificações em que os empregados podem ser alertados, como desalinhamento entre os lábios e a fala; piscar dos olhos pouco natural ou ausente; movimentos corporais rígidos ou artificiais; iluminação irregular entre os quadros, alterações inesperadas na tonalidade da pele, vestígios digitais perceptíveis na imagem.

A chave para enfrentar esse desafio é a implementação de uma abordagem proativa e ética, que inclua a educação dos colaboradores, a verificação de autenticidade dos conteúdos e o fortalecimento das práticas de governança corporativa.

Quando falamos em organizações, inclui-se também instituições que lidam com o público infantil. Conforme Gruber et al. (2020), a eminente tecnologia baseada em dispositivos móveis tem muito a contribuir com a educação, porém, para que a utilização do m-learning como ferramenta didática na segunda infância seja feita de forma eficaz, devem ser superados ou gerenciados alguns desafios sobre a relação da criança com o dispositivo móvel, como a possibilidade de cyberbullying e, principalmente, a dificuldade de monitoramento de conteúdo acessado.

Portanto, integrar a gestão de riscos relacionados aos deepfakes dentro da estratégia ESG é uma abordagem essencial para garantir a sustentabilidade social, ética e organizacional a longo prazo. As empresas que adotarem essas práticas estarão mais bem preparadas para lidar com os desafios tecnológicos do futuro e garantir um ambiente de trabalho mais justo, seguro e transparente para todos os envolvidos.

4. LEGISLAÇÃO BRASILEIRA E O DIREITO COMPARADO

No Brasil, embora ainda não exista uma legislação específica sobre deepfakes, algumas normas já podem ser aplicadas para lidar com abusos relacionados a esse tipo de conteúdo, especialmente no âmbito dos crimes digitais e da proteção dos direitos individuais. Entre essas legislações, destacam-se a Lei Carolina Dieckmann, o Código Penal Brasileiro, enquadrando como crimes de difamação, calúnia ou injúria, conforme as previsões do Código Penal. Caso o conteúdo manipulado cause danos à honra ou à imagem de uma pessoa, ele pode ser punido com penas que variam conforme a gravidade da ofensa. A Lei Geral de Proteção de Dados. O Código Civil Brasileiro que dispõe sobre a Lei de Proteção à Imagem prevista no Código Civil estabelece que qualquer manipulação de imagem que cause danos à honra ou à privacidade de uma pessoa pode ser punida. Deepfakes que envolvem a criação de conteúdo difamatório ou pornográfico podem ser enquadrados como violação da imagem da pessoa.

O Projeto de Lei nº 2.338/2023, em tramitação no Senado Federal, visa estabelecer normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil. O PL tem como fundamentos centrais a centralidade da pessoa humana; o respeito aos direitos humanos e aos valores democráticos e a privacidade, a proteção de dados e a autodeterminação informativa. Embora o texto aborde diversos aspectos relacionados à IA, a questão dos deepfakes — conteúdos falsificados gerados por IA que podem manipular imagens, vídeos ou áudios de maneira realista — não é tratada de forma específica no projeto atual.

Essa ausência abre uma lacuna significativa, considerando o potencial prejudicial dos deepfakes, especialmente em contextos de desinformação e violação de direitos individuais. Há uma expectativa de que futuras discussões legislativas abordem diretamente esse tema, visando criar mecanismos legais para prevenir e punir o uso malicioso de tecnologias de IA na criação de conteúdos falsos.

JOTA (2024), elucidada um estudo comparado de como vários países têm adotado regulamentações para lidar com os desafios impostos pelos deepfakes, especialmente no contexto de abusos digitais e sua disseminação não consensual. Por exemplo, no Reino Unido, o Online Safety Act, aprovado em outubro de 2023, tornou ilegal a disseminação de deepfakes pornográficos não consensuais, mas ainda não criminaliza a criação desses conteúdos. Em 2024, o governo australiano aprovou o Projeto de Lei de Emenda ao Código Penal, que criminaliza o compartilhamento e criação de deepfakes pornográficos. A União Europeia adotou políticas rigorosas para regulamentar a criação e o compartilhamento de deepfakes. O Digital Services Act de 2022 exige que as plataformas removam rapidamente conteúdo não consensual, e o AI Act de 2024 obriga as plataformas a alertarem os usuários sobre a utilização de IA em conteúdos. A Coreia do Sul, uma das pioneiras em legislações rígidas sobre deepfakes, implementou leis para proibir o uso de deepfakes em campanhas eleitorais e punições severas para a criação de conteúdos manipulados com intenções de causar dano. Singapura também adotou medidas rigorosas em

relação ao uso de deepfakes durante as eleições, com leis que proíbem a criação de conteúdos manipulados que possam afetar a integridade das campanhas eleitorais. Nos EUA ainda não foi aprovado uma regulamentação federal abrangente para IA, vários estados, como o Tennessee, já implementaram leis específicas para combater o uso não autorizado de IA em imitações de vozes. Projetos de lei como o Defiance Act e o Shield Act visam proteger vítimas de deepfakes, permitindo que sejam processadas por quem cria ou distribui esses conteúdos.

Essas iniciativas refletem os esforços globais para mitigar os impactos negativos dos deepfakes, com foco em proteger os indivíduos e promover a responsabilidade na utilização de tecnologias emergentes.

5. CONCLUSÃO

As implicações jurídicas do uso de deepfakes no ambiente corporativo são amplas e complexas, trazendo desafios específicos para os empregadores. Entre essas responsabilidades estão a garantia da privacidade e proteção de dados dos empregados, a prevenção de violações aos direitos autorais, a observância da responsabilidade civil por eventuais danos causados por deepfakes e a adoção de medidas eficazes para proteger a integridade das comunicações internas e externas. Nesse contexto, cabe ao empregador implementar políticas robustas e ferramentas tecnológicas que mitiguem riscos, assegurando um ambiente de trabalho ético e seguro.

Integrar a governança tecnológica ao modelo ESG é uma forma estratégica de alinhar inovação com responsabilidade social. Deepfakes não é apenas uma ferramenta, mas também espelha os valores e escolhas das empresas. Uma abordagem consciente e proativa é essencial para transformar os desafios impostos por novas tecnologias em oportunidades de criar práticas mais justas, transparentes e alinhadas aos interesses da sociedade.

No cenário atual, em que a valorização do ESG (Ambiental, Social e Governança) pelos investidores tem ganhado destaque, torna-se fundamental estabelecer procedimentos claros e eficazes para identificar deepfakes promovidos pela concorrência. Essa prática é essencial para proteger a integridade das empresas,

evitando o risco de práticas de greenwashing, já que informações falsas divulgadas na internet podem comprometer iniciativas ESG e causar danos reputacionais.

A desinformação sobre o cenário da empresa torna ainda mais crucial o reforço da transparência e da ética no cumprimento dos princípios ESG (Ambiental, Social e Governança). Informações falsas podem comprometer a continuidade das iniciativas sustentáveis, afetando a confiança dos funcionários e das partes interessadas.

Além disso, o empregador tem o dever de garantir a segurança do ambiente de trabalho, incluindo a prevenção de riscos tecnológicos. A ausência de medidas razoáveis para mitigar ameaças digitais, como deepfakes, pode ser caracterizada como negligência. Embora a Consolidação das Leis do Trabalho (CLT) não trate diretamente do tema, o artigo 157 obriga os empregadores a cumprir e fazer cumprir normas de segurança e medicina do trabalho, o que pode ser interpretado como um fundamento para incluir proteção contra riscos tecnológicos;

Nesse sentido, empregadores podem adotar medidas preventivas, como treinamentos e programas de conscientização, capacitando os empregados a identificar deepfakes e outras ameaças digitais. Essas ações devem ser acompanhadas de políticas claras de segurança da informação e da utilização de ferramentas avançadas para detectar e bloquear conteúdos maliciosos. Essas iniciativas não apenas minimizam riscos, mas também reforçam o compromisso da empresa com a ética, a segurança e o bem-estar de seus trabalhadores.

REFERENCIAS BIBIOGRÁFICAS

ABNT. Prática Recomendada: ABNT 2030-1: Ambiental, social e Governança (ESG) – Conceitos, diretrizes e modelo de avaliação e direcionamento para organizações. Rio de Janeiro: ABNT, 2022. Acesso em 30 dez. 2024.

BANCO DO BRASIL. Segurança Digital. Disponível em: https://blog.bb.com.br//golpes-com-deepfake-saiba-como-se-proteger/ Acesso em: 29 dez. 2024.

BRASIL. Constituição da República Federativa do Brasil. Promulgada em 05 de outubro de 1988. Acesso em: 05 mar. 2024.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União. Acesso em: 05 mar. 2024.

BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Acesso em: 05 jun. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, [2018]. Acesso em: 10 jun. 2022.

BRASIL. Projeto de Lei N° 2.338/2023 - Regulação da Inteligência Artificial no Brasil" - Senado Federal. Acesso em: 29 de dez. de 2024.

DECIBER. Deepfake: entenda o que é e porque é um risco potencial para Empresas. Disponível em: https://dciber.org/deepfake-entenda-o-que-e-e-porque-e-um-risco-potencial-para-empresas/ Acesso em: 29 de dez. de 2024.

FREEMAN, R. Edward. Strategic Management: A Stakeholder Approach. Boston: Pitman,1984.

FORTINET, Fortiguard Labs. O Brasil é o Segundo País mais Atingido por Ciberataques na América Latina. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-ati ngido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em: 23 de março de 2024.

GRUBER, Vilson; GOMES, Nairon Nícolas da Silva; LAVINA, Maria Eduarda; MARCELINO, Roderval; SANTOS, George França dos. M-learning: o novo paradigma educacional na segunda infância: possibilidades e desafios. Disponível em: file:///C:/Users/Usuario/Downloads/2745-Texto%20do%20artigo-10397-2-10-20200616.pdf. Acesso em: 06 de jan. 2025.

JOTA. Regulamentação e políticas globais sobre deepfakes: desafios e avanços legislativos. Disponível em: https://www.jota.info/content/info/deepfakes-uma-tecnologia-de-riscos-e-desafios-legais.Acesso em: 29 dez. 2024.

IBGC. Código das melhores práticas de Governança Corporativa. 6ª edição. Disponível em: https://www.ibgc.org.br/blog/lancamento-sexta-edicao-codigo-melhores-praticas-ibgc. Acesso em: 12 out. 2024.

ICEV. Inteligência artificial imita voz de CEO em roubo de US$ 243 mil. Disponível em: https://www.somosicev.com/blogs/inteligencia-artificial-imita-voz-de-ceo-em-roubo-de-us-243-mil/ Acesso em: 29 dez. 2024.

KASPERSKY. Vídeos falsos e deepfake – Como os usuários podem se proteger. Disponível em: https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake. Acesso em: 29 dez. 2024.

SANTAELLA, Lucia; SALGADO, Marcelo de Mattos. Deepfake e as consequências sociais da mecanização da desconfiança. Revista TECCOGS, São Paulo, v. 11, n. 1, p. 59-73, jan./jun. 2021. Disponível em: https://revistas.pucsp.br/index.php/teccogs/article/view/55981/37929. Acesso em: 29 dez. 2024.

STF. Guia Ilustrado contra DeepFakes. https://portal.stf.jus.br//desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf. Acesso em: 29 dez. 2024.

TSE. TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas- eleições. Acesso em: 30 dez. 2024.

UNIVERSITY OF WASHINGTON. Sincronizando os lábios de Obama: Novas ferramentas transformam clipes de áudio em vídeos realistas. Disponível em: https://www.washington.edu/news/2017/07/11/lip-syncing-obama-new-tools-turn-audio-clips-into-realistic-video/?utm_source=chatgpt.com. Acesso em: 30 dez. 2024.

VALENTINI, Melissa Chanazis. O Compliance como Aliado ao ESG na Perspectiva da Prática Recomendada 2030 da Associação Brasileira de Normas Técnicas. In: 4º Congresso Luso-Brasileiro de Gestão e Conformidade, 2024, Porto Alegre. Porto Alegre: Instituto Ibero-americano de Compliance, 2024. Disponível em: https://iiacompliance.org/wp-content/uploads/2024/08/ANAIS_CLBGC_2024_2.pdf. Acesso em: 29 dez.2024.