DEEPFAKES: RISCOS, PREVENÇÃO E PROTEÇÃO NA IA

LAURA MARTINS VALENTIM , THEO SOUTO CARDOSO , Mirella Novais Oliveira (orientadora), Talita de Paula Cipriano de Souza (coorientadora)
IFSP, Campus Bragança Paulista.

INTRODUÇÃO

O avanço das tecnologias de Inteligência Artificial (IA), especialmente as *deepfakes*, traz preocupações significativas sobre a privacidade e a autenticidade das informações e pessoas. Nesse aspecto, a legislação do último século precisa ser revisitada, considerando as novas descobertas e os usos ilegítimos que elas provocam como influenciadoras e disseminadoras de informações, cujos métodos antigos de detecção de falsa identidade já não correspondem ao que se encontra em uso na contemporaneidade. Por isso, esta investigação buscou os impactos desse tipo de avanço tecnológico, como nos proteger deles e os riscos que tal tecnologia representa para a sociedade.

Sobre o tema, atualmente está em vigor em todo o território nacional a lei nº 13.709, de 14 de agosto de 2018, que trata sobre proteção de dados pessoais, a LGPD. No seu artigo primeiro, a LGPD "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." Entretanto, desde a sua criação em 2018, diversos avanços tecnológicos que dizem respeito à manipulação de dados pessoais foram criados, que suplantam o texto original e exigem mudanças na redação. A última deles foi realizada em 2019, cujo teor ainda consegue dar conta de alguns casos de *deepfakes*, mas não todos. Por isso, é importante também apresentar outras alternativas legais de proteção, à luz do que se tem utilizado hoje.

OBJETIVO

Objetivo Geral:

Apresentar recursos e legislação de uso nacional de prevenção e proteção contra as *deepfakes*, sobretudo em recursos audiovisuais.

Objetivos Específicos:

1) Conceituar *deepfakes* e os principais recursos tecnológicos utilizados para produzi-las, sobretudo em recursos audiovisuais.
2) Indicar os impactos das *deepfakes* nos direitos à privacidade e à segurança;
3) Descrever a Lei Geral de Proteção de Dados (LGPD) e outros recursos de prevenção e proteção em vigência no Brasil contra as *deepfakes*.

METODOLOGIA

O desenvolvimento da pesquisa se deu à luz do Método Científico: quanto aos procedimentos técnicos, como pesquisa bibliográfica e documental; quanto à natureza, como pesquisa básica; quanto aos objetivos, como pesquisa descritiva; e quanto à abordagem do problema, como pesquisa qualitativa.

Em um primeiro momento, foi realizado uma pesquisa bibliográfica dos principais recursos de *deepfakes* utilizados no Brasil. Posteriormente, foi feita uma tabulação de conceitos e funções dos principais recursos de Inteligência Artificial encontrados para produzir esse tipo de informações. Na etapa seguinte, foram evidenciados os impactos das *deepfakes* em relação aos direitos humanos e de cidadania.

Por fim, foi feita uma análise da LGPD e listagem dos principais meios usuais na proteção e prevenção contra as *deep fakes* no país.

RESULTADOS E DISCUSSÕES

A pesquisa buscou explorar como informações falsas tecnológicas, de recurso audiovisuais são criadas, os riscos envolvidos e quais medidas já existem para prevenir seu uso indevido, considerando o que autores como Chesney e Citron (2019) argumentam sobre a necessidade das políticas claras serem necessárias para controlar o uso malicioso de IA, considerando aspectos técnicos, éticos e legais. Logo, este estudo torna-se crucial para minimizar os danos causados pelas deepfakes, especialmente em situações como disseminação de fake news e difamação, que impactam negativamente o corpo social no campo audiovisual. Apesar de entendermos como elas são criadas e seus potenciais usos prejudiciais, existem lacunas significativas devido ao rápido avanço tecnológico, exigindo o desenvolvimento de métodos mais eficazes de detecção e prevenção.

Portanto, este trabalho se conecta aos debates sobre o avanço da IA, ética tecnológica e a urgência de regulamentação para preservar a privacidade, cujos recursos de autores como Bergesch (2024), ao discutirem a criminalização do uso malicioso de IA, são oferecidos em forma de *insights* cruciais sobre as medidas legais necessárias.

CONCLUSÃO

Espera-se com esse projeto alertar sobre os riscos das *depp fakes*, além de promover alternativas de prevenção e proteção contra elas. Ademais, pretende-se evidenciar que, embora já exista legislação sobre o tema, ainda carece complementar e especificar situações e sanções que acompanhem o rápido desenvolvimento tecnológico das Inteligências Artificiais, em prol de um espaço de progresso com marcas mais positivas do que negativas nas relações interpessoais e na validação de informações.

Em outrossim, cogita-se trabalhar futuramente na catalogação de mecanismos tecnológicos, também produzidos por Ias, para auxiliar e complementar a garantia dos direitos cidadãos de isonomia, autonomia e equidade, evidenciando que também existem inúmeros aspetos benéficos no avanço da tecnologia e que o mesmo não pode ser sempre encarado como ameaça ou influenciador maléfico aos direitos humanos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. 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: jun. 2024.

BERGESCH, Raul. ***Deepfake* é crime? O que é e como se prevenir** (artigo). Bergesch Advogados (Blog, 2024). Disponível em: https://ber.adv.br/deep-fake-e-crime-o-que-e-e-como-se-prevenir/ Acesso em: jun. 2024.

CITRON, Danielle Keats; CHESNEY, Robert**. Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security.** California Law Review. Ed 1. (2019). Disponível em: https://papers.ssrn.com/sol3/papers.cfm? abstract_id= Acesso em: jun. 2024.