

DEEPPAKES E SEGURANÇA DIGITAL: RISCOS DA INTELIGÊNCIA ARTIFICIAL PARA A CONFIABILIDADE DA INFORMAÇÃO NO AMBIENTE DIGITAL

Luan Bernardino Lopes¹; Taís de Cássia Badaró Alves²; Bruna Diniz Pereira³; Marlene Soares Freire Germano⁴

1 Estudante do Curso de Direito da Universidade Iguazu – UNIG, Campus V – Itaperuna, RJ; 2 Docente do Curso de Direito da Universidade Iguazu – UNIG, Campus V – Itaperuna, RJ; 3 Docente do Curso de Direito da Universidade Iguazu – UNIG, Campus V – Itaperuna, RJ; 4 Docente do Curso de Direito da Universidade Iguazu – UNIG, Campus V – Itaperuna, RJ

lopesluanbernardino@gmail.com

Introdução e/ou Fundamento: O avanço da inteligência artificial permitiu a criação de *deepfakes*, conteúdos sintéticos que manipulam imagens, vídeos e áudios para simular pessoas reais. Embora tenham usos legítimos, seu uso indevido pode facilitar fraudes, desinformação e ataques à reputação, representando um desafio à segurança e à confiabilidade das informações no ambiente digital. **Objetivo:** Analisar os riscos associados ao uso de *deepfakes* no contexto da segurança digital e discutir seus impactos para a confiabilidade da informação e para a proteção da identidade digital. **Material e Métodos:** Trata-se de uma pesquisa de natureza qualitativa, de caráter exploratório e descritivo, baseada na análise de dados secundários. Foram examinados estudos acadêmicos recentes, relatórios institucionais e publicações especializadas sobre inteligência artificial, segurança digital e desinformação. A análise buscou identificar tendências relacionadas à disseminação de *deepfakes* e suas implicações para a segurança da informação. **Resultados:** Estudos indicam crescimento acelerado dos *deepfakes*, com a maioria dos conteúdos associada a usos maliciosos, como fraudes digitais, pornografia não consensual e desinformação. Além disso, pesquisas demonstram que a evolução dos algoritmos de inteligência artificial tem tornado essas manipulações cada vez mais realistas e difíceis de detectar, ampliando os riscos para a segurança digital e para a confiança nas comunicações online. Esse cenário evidencia a necessidade de desenvolvimento de tecnologias de detecção e de mecanismos regulatórios capazes de mitigar os impactos negativos dessa prática. A tipificação jurídica dos *deepfakes* no Brasil ainda é complexa. Embora não exista legislação específica sobre essa tecnologia, condutas ilícitas podem ser enquadradas no Código Penal Brasileiro, como no art. 147-B, que trata da violência psicológica contra a mulher, inclusive quando há manipulação de imagem ou som por meios tecnológicos. Quando envolvem crianças ou adolescentes, pode-se aplicar o art. 241-C do Estatuto da Criança e do Adolescente, que criminaliza a simulação de participação de menor em cena sexual por meio de alteração de imagens ou vídeos. Ainda assim, não há lei que regulamente especificamente os *deepfakes* ou as criminalize por si só, existindo apenas projetos de lei em tramitação. **Conclusão:** Conclui-se que o avanço dos *deepfakes* representa um desafio relevante para a segurança digital contemporânea. A proteção da

informação e da identidade digital exige a integração de estratégias tecnológicas, regulatórias e educacionais, voltadas à identificação de conteúdos manipulados e à conscientização da população sobre os riscos associados a essa tecnologia.

Palavras-chave: *Deepfakes*; Inteligência Artificial; Segurança Digital; Tecnologia.