IMPLANTES CEREBRAIS E A PROTEÇÃO DE DADOS: VULNERABILIDADES CIBERNÉTICAS E O DESAFIO DA SEGURANÇA SOB A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Eduardo Henrique da Silva[1], Perla Savana Daniel[2], e-mail: eduardodasilvahenrique0007@gmail.com

1 INTRODUÇÃO

Os implantes cerebrais são uma subcategoria das interfaces cérebro-máquina (ICMs), que representam uma promissora fronteira da ciência e tecnologia médica contemporânea, já que tais dispositivos, ao permitir a comunicação direta entre o cérebro humano e sistemas computacionais, estão sendo empregados em tratamentos de doenças neurológicas, recuperação de funções motoras e aprimoramento cognitivo.

Em um futuro próximo, podem revolucionar a forma de abordagem das doenças neurodegenerativas e deficiências motoras, expandindo as capacidades humanas, o que introduz a ideia de transumanismo.

Todavia, o desenvolvimento dessas tecnologias não está isento de desafios, pois os dados captados por implantes cerebrais são demasiadamente sensíveis, indo além da esfera dos dados de saúde tradicionais, podendo abranger informações sobre os pensamentos, emoções e estados mentais dos indivíduos.

Esses dados, quando acessados de maneira indevida, podem resultar em violações profundas da privacidade e autonomia do indivíduo, constituindo o que alguns autores já chamam de "privacidade mental" ou "liberdade cognitiva".

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), implementada no Brasil, desempenha um papel central na regulamentação do tratamento de dados sensíveis.

A proteção dos dados gerados por implantes cerebrais se torna, portanto, não apenas uma questão de conformidade legal, mas uma demanda ética e de segurança social.

Este artigo objetiva abordar as vulnerabilidades cibernéticas desses dispositivos e o papel da LGPD na mitigação dos riscos relacionados à segurança e privacidade dos dados neurais.

[1] Pós-graduando lato sensu em Direito Previdenciário e Tributário (FAVENI). Bacharel em Direito, Faculdades Integradas de Jaú (2024).

[2] Mestre em Direito pelo UNIVEM – Marília. Especialista em Direito Civil e Processual Civil pela Escola Superior de Advocacia ESA-SP. Graduada em Direito pela Faculdade de Direito de Jaú (FIJ).

2 METODOLOGIA

Para o desenvolvimento deste artigo, utilizou-se uma abordagem qualitativa e analítica, com ênfase na interpretação da LGPD (Lei Geral de Proteção de Dados) e sua aplicação aos implantes cerebrais.

A pesquisa foi baseada em uma revisão de literatura sobre neurotecnologia, interfaces cérebro-máquina e segurança cibernética em dispositivos médicos conectados.

Concomitantemente, foram analisadas normativas nacionais e internacionais de proteção de dados, envolvendo ainda a análise de incidentes de segurança relacionados a dispositivos médicos conectados e suas implicações para a privacidade e integridade física dos pacientes, em busca de analogias para o contexto dos implantes cerebrais.

3 RESULTADOS E DISCUSSÃO

Os implantes cerebrais geram um tipo de dado extremamente sensível, que transcende as categorias tradicionais de informações de saúde e biometria.

Esses dispositivos, ao captarem dados neurais, podem coletar informações sobre pensamentos, emoções e respostas a estímulos, estabelecendo uma nova dimensão da privacidade que é frequentemente referida como "privacidade mental". Tal natureza dos dados requer uma abordagem rigorosa de proteção, considerando as potenciais consequências da exposição a ciberataques.

Os dispositivos conectados são suscetíveis a diversos tipos de vulnerabilidades, que podem ser exploradas por cibercriminosos. Os ataques podem resultar na interceptação de dados, comprometendo a integridade e a privacidade dos indivíduos, ou na manipulação de comandos neurais, levando a danos físicos e psicológicos significativos.

A possibilidade de um invasor alterar a funcionalidade de um implante cerebral pode afetar diretamente a autonomia do paciente, tornando essencial a implementação de medidas de segurança robustas.

Urge pontuar que, a Lei Geral de Proteção de Dados (LGPD) estabelece um marco jurídico para a proteção de dados sensíveis no Brasil, mas sua aplicabilidade aos dados gerados por implantes cerebrais ainda apresenta desafios.

A LGPD exige o consentimento explícito dos titulares e a adoção de medidas de segurança para proteger dados pessoais, porém a complexidade e a inovação dos dados neurais demandam uma interpretação que se transpõe as diretrizes atuais.

O papel do controlador, que pode ser o fabricante ou o prestador de serviços de saúde, implica na responsabilidade de assegurar que práticas de tratamento de dados estejam em conformidade com a legislação, implementando mecanismos como criptografia e autenticação multifatorial.

Além disso, as lacunas regulatórias existentes indicam a necessidade de desenvolver normas específicas que abordem os riscos inerentes à neurotecnologia. O rápido avanço das tecnologias exige um esforço colaborativo entre legisladores e especialistas para criar um arcabouço que não apenas proteja a privacidade e a segurança dos dados, mas também promova a confiança na adoção de implantes cerebrais.

Dessa forma, é vital que o debate sobre a segurança e a ética no uso de implantes cerebrais avance, garantindo que a inovação não comprometa a dignidade e os direitos fundamentais dos indivíduos.

4 CONSIDERAÇÕES FINAIS

A proteção de dados em implantes cerebrais representa um dos maiores desafios para o direito da proteção de dados no século XXI.

A LGPD, mesmo fornecendo diretrizes valiosas, carece de especificidade para lidar com as particularidades dos dados neurais e as vulnerabilidades associadas a esses dispositivos.

Os riscos de ataques cibernéticos a implantes cerebrais, incluindo a interceptação de dados neurais e a manipulação de funções cerebrais, demandam uma abordagem de segurança cibernética avançada, baseada em criptografia, autenticação robusta e monitoramento contínuo.

Além disso, é necessário que o legislador e as autoridades regulatórias desenvolvam normas específicas para dispositivos neurotecnológicos, a fim de garantir uma proteção adequada dos direitos fundamentais dos indivíduos.

Em última análise, o avanço dessas tecnologias exige um equilíbrio entre o progresso tecnológico e a preservação da dignidade humana, garantindo que os

benefícios trazidos pelos implantes cerebrais sejam acompanhados de salvaguardas jurídicas robustas que protejam a privacidade e a autonomia dos indivíduos.

REFERÊNCIAS

ABREU, K. C. K. **História e usos da internet**. BOCC - Biblioteca Online de Ciências da Comunicação, pg. 1-9, 2009.

CIPRIANO, W. F. **A segurança da informação com o advento da internet das coisas em ambientes hospitalares: uma abordagem bibliográfica**. 2021.

DIAS, F. M. et al. **Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saúde**. Universidade Nove de Julho, 2021.

Lei n. 13.709, de 14 de agosto de 2018. Planalto, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 de setembro, 2024.

MASSOLA, S. C.; PINTO, G. S. **O uso da internet das coisas (iot) a favor da saúde**. Revista Interface Tecnológica, v. 15, n. 2, p. 124-137, 2018.

NUNES, P. F. V. **A definição de uma estratégia nacional de cibersegurança.** Nação e defesa, Instituto da Defesa Nacional, 2012.

SENDIN, I. da S. **Funções de hashing criptográficas**. 1999.

SERAZZI, G.; ZANERO, S. **Computer virus propagation models**. In: SPRINGER. International workshop on modeling, analysis, and simulation of computer and telecommunication systems. [S.l.], 2003. p. 26-50

SILVA, MARCELO. **Segurança cibernética em equipamentos médicos**. Linkedin, 2024. Disponível em: <https://pt.linkedin.com/pulse/seguran%C3%A7a-cibern%C3%A9tica-em-equipamentos-m%C3%A9dicos-marcelo-silva-thmrf>. Acesso em: 25 de setembro de 2024.