Revista de Bioética y Derecho

www.bioeticayderecho.ub.edu – ISSN 1886 –5887

DOSIER MONOGRÁFICO

Segurança digital em interfaces cérebro-computador no contexto ético-jurídico brasileiro

Seguretat digital en interfícies cervell-computadora en el context ètic-legal brasiler

Seguridad digital en interfaces cerebro-computadora en el contexto ético-legal brasileño

Digital security in brain-computer interfaces in the Brazilian ethical-legal context

Margareth Vetis Zaganelli [1], Douglas Luis Binda Filho [2]

[1] Margareth Vetis Zaganelli. Doutora em Direito pela Universidade Federal de Minas Gerais (UFMG). Professora titular da Universidade Federal do Espírito Santo (UFES). E-mail: mvetis@terra.com.br. ORCID: https://orcid.org/0000-0002-8405-1838.

[2] Douglas Luis Binda Filho. Advogado. Graduado em Direito pela Universidade Federal do Espírito Santo (UFES). E-mail: bindadouglas@gmail.com. ORCID: https://orcid.org/0000-0003-0937-6605.

Resumo

As interfaces cérebro-computador funcionam como uma via de comunicação direta entre a atividade elétrica do cérebro e um dispositivo externo, como um computador ou uma prótese. Na atualidade, as interfaces cérebro-computador têm sido utilizadas principalmente para auxiliar pessoas com deficiência ou em pesquisas científicas. Tais interfaces enfrentam desafios significativos em relação à segurança digital, uma vez que ataques potenciais podem comprometer a privacidade, a saúde e a integridade dos usuários. O presente artigo, através de metodologia exploratória, com base em pesquisa bibliográfica e documental, visa a análise das problemáticas referentes à segurança digital em interfaces cérebro-computador no contexto ético-jurídico brasileiro, com o fito de propor o quadro normativo que emerge a partir dessas tecnologias. Inicialmente, o estudo aborda as diferentes categorias de interfaces cérebro-computador. Em sequência, analisam-se as vulnerabilidades de segurança dessas interfaces. Após, realiza-se o quadro normativo aplicado às interfaces cérebro-computador. Conclui-se que é de extrema importância uma abordagem preventiva, colaborativa e multidisciplinar para garantir que essas interfaces permaneçam seguras e protegidas, preservando os direitos e a integridade daqueles que delas dependem.

Palavras-chave: interfaces cérebro-computador; segurança digital; neurosegurança; bioética; direito digital.

Resum

Les interfícies cervell-ordinador funcionen com una via de comunicació directa entre l'activitat elèctrica del cervell i un dispositiu extern, com un ordinador o una pròtesi. Actualment, les interfícies cervell-ordinador s'han utilitzat principalment per ajudar les persones amb discapacitat o en la investigació científica. Aquestes interfícies s'enfronten a reptes importants en relació a la seguretat digital, ja que els possibles atacs poden comprometre la privadesa, la salut i la integritat dels usuaris. Aquest article, a través d'una metodologia exploratòria, basada en la recerca bibliogràfica i documental, pretén analitzar les qüestions relatives a la seguretat digital en les interfícies cervell-ordinador en el context ètic-legal brasiler, amb l'objectiu de proposar el marc normatiu que sorgeix d'aquestes tecnologies. Inicialment, l'estudi aborda les diferents categories d'interfícies cervell-ordinador. A continuació, s'analitzen les vulnerabilitats de seguretat d'aquestes interfícies. Posteriorment, es crea el marc normatiu aplicat a les interfícies cervell-ordinador. Es conclou que un enfocament preventiu, col·laboratiu i multidisciplinari és extremadament important per garantir que aquestes interfícies romanguin segures i protegides, preservant els drets i la integritat dels qui en depenen.

Paraules clau: interfícies cervell-ordinador; seguretat digital; neuroseguretat; bioètica; dret digital.

Abstract

Brain-computer interfaces (BCIs) function as a direct communication channel between the electrical activity of the brain and an external device, such as a computer or a prosthesis. Currently, brain-computer interfaces have been primarily used to assist individuals with disabilities or in scientific research. These interfaces face significant challenges regarding digital security, as potential attacks can compromise the privacy, health, and integrity of users. This article, using an exploratory methodology based on bibliographic and documentary research, aims to analyze the issues related to digital security in brain-computer interfaces in the Brazilian ethical and legal context, with the purpose of proposing the regulatory framework that emerges from these technologies. Initially, the study addresses the different categories of brain-computer interfaces. Next, the security vulnerabilities of these interfaces are analyzed. Then, the regulatory framework applied to brain-computer interfaces is examined. It is concluded that a preventive, collaborative, and multidisciplinary approach is of utmost importance to ensure that these interfaces remain secure and protected, preserving the rights and integrity of those who depend on them.

Keywords: brain-computer interfaces; digital security; neurosecurity; bioethics; digital law.

Resumen

Las interfaces cerebro-computadora funcionan como un medio de comunicación directa entre la actividad eléctrica del cerebro y un dispositivo externo, como una computadora o una prótesis. En la actualidad, las interfaces cerebro-computadora se han utilizado principalmente para ayudar a personas con discapacidades o en investigaciones científicas. Estas interfaces enfrentan desafíos significativos en cuanto a la seguridad digital, ya que posibles ataques pueden comprometer la privacidad, la salud y la integridad de los usuarios. El presente artículo, utilizando una metodología exploratoria basada en investigación bibliográfica y documental, tiene como objetivo analizar los problemas relacionados con la seguridad digital en interfaces cerebro-computadora en el contexto ético-jurídico brasileño, con el fin de proponer el marco normativo que surge de estas tecnologías. Inicialmente, el estudio aborda las diferentes categorías de interfaces cerebro-computadora. A continuación, se analizan las vulnerabilidades de seguridad de estas interfaces. Después, se examina el marco normativo aplicado a las interfaces cerebro-computadora. Se concluye que es de suma importancia un enfoque preventivo, colaborativo y multidisciplinario para garantizar que estas interfaces sigan siendo seguras y protegidas, preservando los derechos y la integridad de quienes dependen de ellas.

Palabras clave: interfaces cerebro-computadora; seguridad digital; neuroseguridad; bioética; derecho digital.

1. Introdução

A história das interfaces cérebro-computador (brain-computer interfaces – BCIs) inicia-se com a descoberta da atividade elétrica do cérebro humano por Hans Berger. Em 1929, o psiquiatra alemão descobriu a eletroencefalografia (EEG) com a introdução de uma inovadora ferramenta de avaliação neurológica e psiquiátrica para a época. Com base nos achados de Caton, Beck, Danilevsky, Prawdicz-Neminsky e outros precursores, Berger efetuou a pioneira gravação de eletrocorticograma em 6 de julho de 1924, durante o decurso de uma cirurgia neurológica em um jovem de 17 anos. Berger apresentou as suas observações em 1929, empregando os termos "ondas alfa" e "ondas beta" para caracterizar os fenômenos identificados (Tudor; Tudor; Tudor, 2005).

Anos mais tarde, no início da década de 1970, a Universidade da Califórnia, através de concessões da Fundação Nacional da Ciência, iniciou as primeiras pesquisas em interfaces cérebro-computador. Conforme pontuado pelo próprio pesquisador à frente do projeto, Jacques J. Vidal (1973, p. 178), tratou-se de uma primeira tentativa sistemática de esclarecer conceitos e de estabelecer as possibilidades e limitações da comunicação cérebro-computador. Inicialmente, as interfaces cérebro-computador (BCIs) foram propostas como uma ferramenta para usar sinais cerebrais a fim de controlar dispositivos externos, como próteses e software de ortografia (Sample et al., 2019, p. 2).

Na atualidade, as interfaces cérebro-computador têm sido utilizadas principalmente como produtos médicos ou em pesquisa, em particular para fornecer serviços de reabilitação a pessoas com deficiência física. Em 2022, um homem com paralisia, sem controle voluntário dos músculos, incluindo os olhos, recuperou a capacidade de comunicar frases completas através de um implante cerebral. O estudo demonstrou que a comunicação em nível de frase é possível usando uma interface cérebro-computador sem depender da visão do paciente, uma vez que ele não tinha um controle do movimento voluntário dos olhos e, consequentemente, não conseguia usar um rastreador ocular para comunicação. O paciente também foi incapaz de usar um sistema de comunicação computadorizado não-invasivo baseado no movimento ocular. Dessa forma, o homem recebeu matrizes de microeletrodos intracorticais em duas áreas do córtex motor (Chaudhary et al., 2022, p. 2).

Em um estudo publicado pela revista Nature em 2023, implantes cerebrais permitiram que um homem de 40 anos caminhasse, doze anos após sofrer um acidente de moto que o deixara paralisado dos quadris para baixo. Os implantes forneceram uma “ponte digital” entre o cérebro do homem e sua medula espinhal, ignorando seções lesionadas. Conseguiu-se capturar os

pensamentos e traduzi-los em uma estimulação da medula espinhal para restabelecer o movimento voluntário (Lorach et al., 2023, p. 126).

Não obstante, para além do uso de tais interfaces em pesquisas científicas, os primeiros produtos de consumo que também fazem uso dessa tecnologia são lançados. Cada vez mais, interfaces cérebro-computador adentram o movimento Quantified Self, com produtos como fones de ouvido que analisam níveis de atenção, foco, engajamento, interesse, excitação, afinidade e níveis de relaxamento e estresse da pessoa (Ijjada et al., 2015, p. 810) ou que digitalizam a saúde do cérebro e recomendam música de acordo com o humor (Park, 2023).

As interfaces cérebro-computador estão sendo cada vez mais visadas como uma forma de aprimoramento humano, o que impacta significativamente a realidade dos seres humanos. Apesar de se tratar de uma tecnologia em desenvolvimento, muito já foi alcançado, de forma que pensar os aspectos ético-jurídicos que envolvem as interfaces cérebro-computador é uma necessidade. O presente artigo, através de metodologia exploratória, com base em pesquisa bibliográfica e documental, visa analisar as problemáticas referentes à segurança digital em interfaces cérebro-computador no contexto ético-jurídico brasileiro. Deseja-se responder ao seguinte questionamento: como seria, a princípio, o quadro normativo aplicado às interfaces cérebro-computador no contexto ético-jurídico brasileiro?

Busca-se, em um primeiro momento, abordar os aspectos gerais das manifestações de interfaces cérebro-computador. Em seguida, realiza-se uma consideração a respeito da vulnerabilidade de segurança dessas tecnologias na área da saúde. Sequencialmente, realiza-se uma análise do quadro jurídico aplicado às interfaces cérebro-computador no contexto ético-jurídico brasileiro. Constatou-se que somente a Lei Geral de Proteção de Dados abordou de maneira substancial a questão das infrações à privacidade com relevância, mas não de forma adaptada para tratar dos riscos específicos de violações às interfaces cérebro-computador.

2. Manifestações de interfaces cérebro-computador

A interface cérebro-computador funciona como uma via de comunicação direta entre a atividade elétrica do cérebro e um dispositivo externo, como um computador ou uma prótese. Tais interfaces fornecem novas formas de interação dos seres humanos com dispositivos externos e o meio ambiente, de modo que ajudam a restaurar, melhorar e modular as funções físicas ou mentais humanas (Sui et al., 2022, p. 1).

Há diferentes formas de categorizar as interfaces cérebro-computador, como, por exemplo, com base no nível de proximidade dos eletrodos ao tecido cerebral. Há as não invasivas, que fazem uso de tecnologias como eletroencefalografia (EEG), magnetoencefalografia (MEG) e ressonância magnética (MRI); as parcialmente invasivas, em que os sensores são colocados dentro do crânio, mas fora da massa cinzenta, por meio da eletrocorticografia (ECoG) (Szafir, 2010, p. 6); bem como as invasivas, que usam microeletrodos e requerem cirurgia para implantá-la.

Leuthardt, Moran e Mullen (2021) propõem, ainda, outra forma de categorizar as BCIs, com base no risco cirúrgico: não invasivo, quando não penetram no corpo; embutidos, quando não mais profundos do que a tábua interna do crânio, e intracranianos, quando os componentes estão localizados dentro da tábua interna do crânio e possivelmente dentro do volume cerebral.

Há igualmente a possibilidade de categorizar as interfaces cérebro-computador com base em suas atribuições. Nesse caso, a princípio, há três grupos diferentes de interfaces cérebro-computador: ativas, passivas e estimulantes. As interfaces passivas restam limitadas a medir a atividade cerebral para posteriormente atribuí-las a um comportamento, estado mental ou enfrentamento cognitivo de uma tarefa. De acordo com Lebedev e Nicolelis (2017, p. 798), essas interfaces poderiam, por exemplo, melhorar as interações humanas com um sistema técnico, monitorizando e decodificando sinais neurais que representam estados cognitivos e emocionais, ao mesmo tempo que fazem ajustes apropriados no sistema técnico.

As interfaces ativas não apenas analisam as atividades cerebrais, mas igualmente desencadeiam uma ação, ou seja, o sujeito modula voluntariamente as ondas cerebrais para controlar um dispositivo externo sem depender de eventos externos (Angrisani et al., 2021, p. 2). A interface decodifica um padrão específico de atividade cerebral e, baseado nisso, resolve o processo desejado.

No caso das interfaces estimulantes são gerados impulsos elétricos a fim de influenciar certas áreas do cérebro, de modo a promover atividades cerebrais específicas, com o objetivo, por exemplo, de prevenir tremores musculares na doença de Parkinson ou convulsões em pacientes com epilepsia. Semelhante às interfaces ativas cérebro-computador, padrões específicos de sinais neurológicos induzem esses impulsos. Faz-se o uso da chamada estimulação cerebral profunda, a qual fornece impulsos eléctricos ao cérebro - semelhantes a um *pacemaker* - para aliviar os sintomas de algumas doenças, como Parkinson, epilepsia ou depressão (Martini; Kemper, 2022, p. 196).

3. Vulnerabilidades de segurança de interfaces cérebro-computador

Assim como existem diferentes tipos de interfaces cérebro-computador, as quais possuem atribuições diversas, há igualmente diferentes formas de ataque a essas tecnologias. Não é apenas o dispositivo em si que oferece pontos de ataque, mas igualmente a infraestrutura digital na qual encontra-se incorporado, como computadores, smartphones e plataformas em nuvem, onde as interfaces são implantadas (Bernal et al., 2020, p. 3).

Quanto mais funções uma interface cérebro-computador combina, maiores são as possibilidades de ataque. Enquanto em ataques ativos terceiros não autorizados podem interferir na função da interface cérebro-computador; em ataques passivos, ataca-se a confidencialidade, a fim de detectar informações privadas dos usuários.

Com a identificação de ameaças potenciais à segurança que podem ser realizadas contra dispositivos neurais implantados, Denning et al. (2009, p. 2) cunharam o termo "neurosegurança", que significa a proteção da confidencialidade, integridade e disponibilidade de dispositivos neurais de partes mal-intencionadas com o objetivo de preservar a segurança de os mecanismos neurais de uma pessoa, a computação neural e o livre arbítrio.

Assim, verifica-se que o invasor poderia prejudicar não apenas o dispositivo, mas também a integridade física e mental do usuário. Um invasor poderia, por exemplo, interferir nos sinais neurais, distorcer os dados gravados ou até mesmo manipular o processamento dos dados brutos captados pelas interfaces cérebro-computador.

Com o intuito de demonstrar a urgência da problemática, Bernal, Celdrán e Pérez (2023), apresentaram uma taxonomia de oito ataques cibernéticos neurais com o objetivo de interromper a atividade neural espontânea, que induziu maliciosamente a estimulação ou inibição neuronal, explorando a possibilidade de recriar os efeitos de condições neurodegenerativas.

Em geral, os ataques podem ser da ordem da confidencialidade, da disponibilidade ou resiliência e da integridade. No caso da confidencialidade, o ataque seria referente aos dados sensíveis coletados pelas interfaces. Em relação à disponibilidade ou resiliência, os ataques afetam a sua funcionalidade, ou seja, uma interface não funciona mais de forma adequada ou então perde a sua capacidade de manter ou restaurar desempenho. Já com relação à integridade, os ataques manipulam as informações e/ou a comunicação com outros dispositivos ou afetam a funcionalidade da interface como um todo (Martini; Kemper, 2022, p. 200-202).

De acordo com Noor e Hassan (2013, p. 704), as redes sem fio são mais suscetíveis e expostas a ataques. No caso dos implantes médicos, muitos dependem de conexão sem fio, de forma que, para

armazenar e analisar informações coletadas por um implante, a interface interage com um PC ou smartphone. Nesse sentido, Kersbergen (2017) afirma que os dispositivos médicos fazem agora parte da Internet das coisas e estão, portanto, expostos às mesmas ameaças de segurança cibernética a que está exposto qualquer coisa ligada à Internet. Portanto, é fundamental não apenas reagir após a ação maliciosa, mas também explorar maneiras de prevenir esses ataques.

4. Quadro jurídico aplicável às interfaces cérebro-computador no contexto brasileiro

A genuína inquietação diante dos ataques cibernéticos dirigidos a interfaces cérebro-computador ressalta a necessidade de haver regulamentações efetivas para assegurar a segurança digital desses dispositivos médicos. Deve-se, assim, refletir o ordenamento jurídico brasileiro e a forma como o direito poderia amparar um usuário em casos de ataque à sua interface cérebro-computador.

Segundo Appazov (2014, p. 50), existem duas estratégias principais para abordar condutas prejudiciais: reagir após tal conduta ter sido cometida, a fim de incapacitar e punir o(s) ator(es); ou impedir a ocorrência da conduta. A princípio, pode-se parecer que o direito penal seria a ferramenta ideal para dissuadir e conter os ataques cibernéticos, contudo, frequentemente revela-se inadequado para tal propósito. Tais ataques podem ser conduzidos de maneira descentralizada, possibilitando que os responsáveis (que atuam internacionalmente ou ocultam sua identidade) frequentemente escapem de ser rastreados ou capturados pelas autoridades policiais (Martini; Kemper, 2022, p. 204).

Durante o último século, tem havido uma ênfase crescente na prevenção de condutas ou crimes indesejáveis, em vez de simplesmente haver uma reação a sua ocorrência. A estratégia preventiva, no entanto, ainda desempenha um papel relativamente menor na abordagem global para lidar com a criminalidade. Uma das razões pelas quais a prevenção constitui uma pequena parte da estratégia atual é o fato de ela consumir muitos recursos, o que implica não apenas um aumento qualitativo e quantitativo no policiamento do ambiente em que podem ocorrer condutas indesejáveis, mas também a colaboração com outros participantes na segurança cibernética, tais como membros da comunidade (Appazov, 2014, p. 50).

Assim, em contextos que envolvem ameaças a bens legais de grande importância, como vida, saúde, integridade física e mental, a abordagem repressiva do direito penal não se mostra adequada como meio de proteção. Desse modo, estratégias e abordagens preventivas tornam-se

imperiosas, com medidas de proteção efetivas que devem tornar o acesso dos agressores impossível ou, pelo menos, consideravelmente difícil (Martini; Kemper, 2022, p. 204).

No Brasil, um quadro jurídico eficiente e aplicável às interfaces cérebro-computador perpassa antes de tudo pela Constituição, uma vez que eventuais violações de segurança podem atingir diferentes direitos fundamentais do indivíduo. Se ataques cibernéticos coletarem informações sobre estado da saúde ou reações emocionais, afeta-se a autodeterminação informativa do indivíduo, sendo uma afronta ao art. 5º, X, da Constituição[1].

Em casos de ataques à disponibilidade ou resiliência e à integridade das interfaces, verifica-se afronta ao *caput* do art. 5º da Constituição[2], porquanto afetar-se-ia a integridade física dos indivíduos e, com isso, o direito à vida. Verifica-se ainda possibilidades de afrontas à liberdade, uma vez que os ataques afetariam a autonomia do indivíduo, bem como à propriedade, pois a destruição da funcionalidade ou o desligamento de uma interface impactaria o usuário igualmente no que diz respeito à interface enquanto sua propriedade.

Para além da Constituição, verifica-se que no quadro normativo aplicado às interfaces cérebro-computador também se encontram a Lei Geral de Proteção de Dados (LGPD), a Resolução da Agência Nacional de Vigilância Sanitária nº 751/2022, a qual dispõe sobre a classificação de risco, os regimes de notificação e de registro, e os requisitos de rotulagem e instruções de uso de dispositivos médicos, e até mesmo o Código de Defesa do Consumidor.

A Lei Geral de Proteção de Dados deve ser aplicada a todos os aspectos das interfaces que envolvam o processamento de dados pessoais, principalmente dos dados sensíveis, bem como àqueles referentes à segurança de dados, como criptografia, requisitos de autenticação e gerenciamento de acesso, detecção de ataque, design de segurança, defesa em profundidade, gerenciamento de incidentes. Igualmente a lei deve auxiliar na identificação dos destinatários dessas obrigações. Trata-se, em tese, da única lei que aborda de forma relevante o tema das violações de privacidade no Brasil. No entanto, a LGPD não está adaptada aos perigos específicos das interfaces cérebro-computador, de forma que não cobre diretamente os requisitos que os fabricantes das BCIs devem cumprir para garantir a efetiva segurança digital dos usuários.

No caso das interfaces cérebro-computador, dados sensíveis são intensamente coletados e armazenados, sendo, em muitos casos, imprescindíveis para o bom funcionamento da tecnologia. Conforme anteriormente apontado pelo estudo, eventuais vazamentos de dados

[1] São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

[2] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade.

podem não apenas comprometer a intimidade e vida privada de um indivíduo, mas igualmente o desempenho alcançado pelo seu usuário.

A Resolução da Agência Nacional de Vigilância Sanitária nº 751/2022 é aplicável às interfaces cérebro-computador, sendo especialmente importante no auxílio da classificação do dispositivo (se médico ou não), bem como para enquadrá-lo segundo o risco intrínseco que representa à saúde do usuário, paciente, operador ou terceiro envolvido, de forma a verificar se estão subordinados a registro ou a notificação.

A referida Resolução traz os requisitos de rotulagem e de instruções de uso, e os procedimentos para notificação, registro, alteração, revalidação e cancelamento de notificação ou registro de dispositivos médicos. A importância é de ordem regulatória e administrativa, sendo especialmente importante que a análise de risco seja criteriosa, face o potencial lesivo da invasão de uma interface cérebro-computador. Tal resolução deve igualmente guiar os fabricantes e as autoridades em casos de emergências, sendo crucial que realizem medidas preventivas e/ou corretivas nessa eventualidade.

O Código de Defesa do Consumidor seria aplicado a todos os aspectos atinentes à matéria consumerista, como os direitos básicos do consumidor, a proteção à saúde e à segurança, a responsabilidade pelo fato do produto e do serviço, bem como a responsabilidade pelo vício do produto e do serviço. Em casos de violações às interfaces cérebro-computador, é importante entender que é possível, em muitos casos, que o dano seja ocasionado devido a uma falha de segurança não observada pelo fabricante ou fornecedor, de modo que, restando configurada a relação consumerista, pode o consumidor requerer a sua devida reparação.

O quadro normativo não necessariamente se esgota, uma vez que, a depender do caso concreto, podem ser verificadas matérias de ordens diversas. No entanto, estudo intentou determinar, a princípio, quais normas seriam imperiosas na maior parte das questões que envolvam interfaces cérebro-computador e violações de segurança. As normas enfatizam a necessidade de adotar uma abordagem preventiva, colaborativa e interdisciplinar para assegurar a segurança contínua dessas interfaces, protegendo assim os direitos e a integridade das pessoas que delas dependem.

5. Conclusões

A cronologia das interfaces cérebro-computador (BCIs) traça uma jornada fascinante desde as descobertas pioneiras de Hans Berger, que revelaram a atividade elétrica do cérebro humano, até os avanços modernos que capacitam as BCIs a desempenharem um papel vital na medicina, na

pesquisa e até mesmo na vida cotidiana com os produtos de consumo que cada vez mais adentram o mercado. Essa evolução tecnológica é verdadeiramente notável e promissora, de forma que proporciona oportunidades sem precedentes para a melhoria da qualidade de vida das pessoas e para a abertura de novos horizontes na exploração do potencial humano.

Contudo, à medida que essa tecnologia se torna mais integrada em nossa sociedade, não se pode ignorar os desafios significativos que ela traz, especialmente no que diz respeito à segurança digital. As BCIs são suscetíveis a uma série de ameaças, desde violações de privacidade até ataques cibernéticos que podem comprometer a saúde e a integridade física dos usuários.

No contexto jurídico brasileiro, várias leis e regulamentos fornecem uma base importante para abordar essas preocupações. A Constituição estabelece direitos fundamentais que podem ser afetados por violações de segurança em BCIs, como o direito à privacidade, à vida e à propriedade. A Lei Geral de Proteção de Dados (LGPD) oferece orientações específicas sobre o tratamento de dados pessoais, incluindo dados sensíveis, e destaca a importância da segurança da informação. Apesar de ser a única lei que abordou de maneira relevante a respeito das violações da privacidade para a segurança a nível geral, não está adaptada aos perigos específicos das interfaces cérebro-computador, de forma que não cobre diretamente os requisitos que os fabricantes das BCIs devem cumprir.

Ainda, a Resolução nº 751/2022 da ANVISA desempenha um papel crucial ao regulamentar dispositivos médicos, incluindo as BCIs, para garantir que sejam seguros e eficazes. Além disso, o Código de Defesa do Consumidor estabelece direitos e responsabilidades em casos de falhas de segurança dos produtos, incluindo BCIs.

Embora o quadro normativo não esgote todas as possíveis questões relacionadas às interfaces cérebro-computador e à segurança cibernética, ele fornece uma base para enfrentar os desafios emergentes. O estudo destaca a importância de uma abordagem preventiva, colaborativa e multidisciplinar para garantir que essas interfaces permaneçam seguras e protegidas, preservando os direitos e a integridade daqueles que delas dependem.

Referências

- Angrisani, L.; Arpaia, P.; Esposito, A.; Gargiulo, L.; Natalizio, A.; Mastrati, G.; Moccaldi, N.; Parvis, M. (2021). Passive and active brain-computer interfaces for rehabilitation in health 4.0. *Measurement: Sensors, 18*. Disponível em: https://www.sciencedirect.com/science/article/pii/S2665917421002099.
- Appazov, A. (2014). Legal Aspects of Cybersecurity. Copenhagen: Justitsministeriet. 70 p. Disponível em:

https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.

- Bernal, S. L.; Celdrán, A. H.; Pérez, G. M.; Barros, M. T.; Balasubramaniam, S. (2020). Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges. *ACM Computing Surveys, 54*, https://doi.org/10.1145/3427376.
- Bernal, S. L.; Celdrán, A. H.; Pérez, G. M. (2023). Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity. *Communications of the ACM, 66*, 68-78. Disponível em: https://cacm.acm.org/magazines/2023/4/271242-eight-reasons-to-prioritize-brain-computer-interface-cybersecurity/fulltext.
- Brasil (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.
- Brasil (1990). *Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências*. Diário Oficial da União, Poder Executivo, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.
- Brasil (2018). *Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União, Poder Executivo, Brasília, DF, 28 jan. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
- Brasil (2022). *Resolução da Diretoria Colegiada nº 751, de 15 de setembro de 2022*. Diário Oficial da União, Poder Executivo, Brasília, DF, 21 set. 2022. Disponível em: http://antigo.anvisa.gov.br/documents/10181/5672055/RDC_751_2022_.pdf/37b2d641-82ec-4e64-bb07-4fc871936735.
- Chaudhary, U.; Ioannis Vlachos, I.; Zimmermann, J. B.; Espinosa, A.; Alessandro Tonin, A.; Andres Jaramillo-Gonzalez, A.; Khalili-Ardali, M.; Topka, H.;Jens Lehmberg, J; Gerhard M. Friehs, G. M.; Alain Woodtli, A.; John P. Donoghue, J. P.; Niels Birbaumer, N. (2022). Spelling interface using intracortical signals in a completely locked-in patient enabled via auditory neurofeedback training. *Nature Communications, 13*. Disponível em: https://www.nature.com/articles/s41467-022-28859-8.
- Denning, T.; Matsuoka, Y.; Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Neurosurg Focus, 27*. Disponível em: https://pubmed.ncbi.nlm.nih.gov/19569895/.
- Ijjada, M. S.; Thapliyal, H.; Caban-Holt, A.; Arabnia, H.R. (2015). Evaluation of Wearable Head Set Devices In Older Adult Populations for Research. *International Conference on Computational Science and Computational Intelligence*, 2015, pp. 810-811, doi: 10.1109/CSCI.2015.158. Disponível em: https://ieeexplore.ieee.org/document/7424202.
- Kersbergen, C. (2017). Patient Safety Should Include Patient Privacy: The Shortcomings Of The FDA's Recent Draft Guidance Regarding Cybersecurity Of Medical Devices. *Nova Law Review, 41*. Disponível em: https://nsuworks.nova.edu/nlr/vol41/iss3/6/.
- Lorach, H.; Galvez, A.; Spagnolo, V.; Martel, F.; Karakas, S.; Intering, N.; Vat, M.; Faivre, O.; Harte, C.; Komi, S.; Ravier, J.; Collin, T.; Coquoz, L.; Sakr, I.; Baaklini, E.; Hernandez-Charpak, S. D.; Dumont, G.; Buschman, R.; Buse, N.; Denison, T.; van Nes, I.; Asboth, L.; Watrin, A.; Struber, L.; Sauter-Starace, F.; Langar, L.; Auboiroux, V.; Carda, S.; Chabardes, S.; Aksenova, T.; Demesmaeker, R.; Charvet, G.; Bloch, J.; Courtine, G. (2023). Walking naturally after spinal cord injury using a brain–spine interface. *Nature, 618*, 126-133. Disponível em: https://www.nature.com/articles/s41586-023-06094-5.

- Lebedev, M. A.; Nicolelis, M. A. L. (2017). Brain-machine interfaces: from basic science to neuroprostheses and neurorehabilitation. *Physiology Review, 97*, 767–837. Disponível em: https://pubmed.ncbi.nlm.nih.gov/28275048/.
- Leuthardt, E. C.; Moran, D. W.; Mullen, T. R. (2021). Defining Surgical Terminology and Risk for Brain Computer Interface Technologies. *Frontiers in Neuroscience, 15.* Disponível em https://www.frontiersin.org/articles/10.3389/fnins.2021.599549/full.
- Martini, M.; Kemper, C. (2022). Cybersicherheit von Gehirn-Computer-Schnittstellen. *Int. Cybersecur. Law Rev., 3*, 191–243. Disponível em https://link.springer.com/article/10.1365/s43439-022-00046-x.
- Noor, M. M.; Hassan, W. H. (2012). Current threats of wireless networks. Barcelona: Communication System and Network (iKohza) Research Group, Malaysia Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia (paper). Disponível em https://core.ac.uk/download/pdf/20081573.pdf.
- Park, K. (2023). Niura's EEG-implemented earbuds scan your brain health and recommend music to your mood. TechCrunch Disrupt 2023, 22 set. 2023. Disponível em: https://techcrunch.com/2023/09/22/niuras-eeg-implemented-earbuds-scan-your-brain-health-and-recommend-music-to-your-mood/.
- Sample, M.; Aunos, M.; Blain-Moraes, S.; Bublitz, C.; Jennifer A; Chandler, J. A.; Falk, T. H.; Friedrich, O.; Groetzinger, D.; Jox, R. J.; Koegel, J.; McFarland, D.; Neufield, V.; Rodriguez-Arias, D.; Sattler, S.; Vidal, F.; Wolbring, G.; Wolkenstein, A.; Racine, E. (2019). Brain–computer interfaces and personhood: interdisciplinary deliberations on neural technology. *Journal of Neural Engineering, 16*. Disponível em: https://pubmed.ncbi.nlm.nih.gov/31394509/.
- Sui, Y.; Yu, H.; Zhang, C.; Chen, Y.; Jiang, C.; Li, L. (2022). Deep brain–machine interfaces: sensing and modulating the human deep brain. *National Science Review, 9*. Disponível em: https://academic.oup.com/nsr/article/9/10/nwac212/6751921.
- Szafir, D. J. (2010). Non-Invasive BCI through EEG: An Exploration of the Utilization of Electroencephalography to Create Thought-Based Brain-Computer Interfaces [Senior Honor Thesis, Boston College]. Disponível em: https://www.bc.edu/content/dam/files/schools/cas_sites/cs/pdf/academics/honors/10Szafir.pdf.
- Tudor, M.; Tudor, L.; Tudor, K. I. (2005). Hans Berger (1873-1941) - Pojivest Elektroencefalografije. *Acta Med Croatica, 59*, 307-313. Disponível em: https://pubmed.ncbi.nlm.nih.gov/16334737/.
- Vidal, J. J. (1973). Toward direct brain-computer communication. *Annual Review of Biophysics and Bioengineering, 2*, 1, p. 157–180. Disponível em: https://www.annualreviews.org/doi/10.1146/annurev.bb.02.060173.001105.

Fecha de recepción: 30 de septiembre de 2023

Fecha de aceptación: 12 de marzo de 2024

Fecha de publicación: 17 de octubre de 2024