· 政策研讨 ·

非侵入式脑机接口数据隐私保护的伦理审思

孟丽君[1] 张海洪[2] 何照楠[1]
[1]中国康复研究中心，北京 100068；[2]北京大学医学部，北京 100191
通信作者：孟丽君，Email：menglydia@126.com，电话：010-87020512

【摘要】 目的 为非侵入式脑机接口技术的数据安全、隐私保护合规发展提供伦理框架。**方法** 通过对数据采集、数据处理和应用生态 3 个层面的过程分析，探讨非侵入式脑机接口全流程中的神经数据安全风险，对数据隐私保护层面所面临的多维伦理困境和现实矛盾进行思考。**结果** 脑机接口数据隐私的保护需构建技术规范、法律约束与伦理治理协同作用的规范框架。**结论** 利用技术手段建立基础防护，通过法律明确各方权利和责任，借助伦理机制平衡技术发展与人的基本权利保护，最终实现对神经数据从获取到使用全过程的全面风险防控。

【关键词】 非侵入式脑机接口； 数据安全； 隐私保护； 伦理审思
【中图分类号】 R197.39；R-05 **【文献标识码】** A DOI：10.3760/cma.j.cn113565-20250829-00216

Ethical reflection on data privacy protection in non-invasive brain-computer interfaces

Meng Lijun[1], *Zhang Haihong*[2], *He Zhaonan*[1]
[1]*China Rehabilitation Research Center, Beijing 100068, China*; [2]*Peking University Health Science Center, Beijing 100191, China*
Corresponding author: Meng Lijun, Email: menglydia@126.com, Tel: 0086-10-87020512

【Abstract】 Objective Establishing an ethical framework to promote the secure, privacy-preserving and regulation-compliant development of non-invasive brain computer interface (BCI) technology. **Methods** Analyzing neural data security risks in data acquisition, data processing and the application and exploring the ethical challenges in data privacy protection of non-invasive BCI. **Results** It was necessary to establish a framework that integrates technical standards, legal constraints, and ethical governance to protect neural data privacy in non-invasive BCI. **Conclusions** Data privacy protection should integrate technical methods, a legal framework that clarifies the rights and responsibilities of all parties, and an ethical guidance that balances technology development with human rights to achieve comprehensive risk prevention covering all stages from data collection to application.

【Key words】 Non-invasive Brain-Computer Interface; Data Security; Privacy Protection; Ethical Reflection
DOI：10.3760/cma.j.cn113565-20250829-00216

脑机接口(Brain-Computer Interface，BCI)是一种在大脑与外部设备之间建立直接信息通道、实现双向信息交互的新型交叉技术[1]。它通过记录装置采集人体颅内或脑外的大脑神经活动，采用机器学习模型等对神经活动进行分析解码，解析出神经活动中蕴含的主观意图等信息，将其转化为可执行的控制指令来操纵外部设备，之后再将设备响应、指令执行结果等过程信息反向传递至脑部，构成一个交互式的信息循环闭环系统。

脑机接口的实现方式主要分为侵入式、半侵入式和非侵入式[2]，其中非侵入式作为脑机接口的一种重要形式，通过无创方式采集头皮脑电信号(EEG)或功能性近红外光谱(fNIRS)信号等，利用机器学习解码转化为指令，从而构建人机交互闭环的脑机接口技术[3]。相较于侵入式脑机接口，非侵入式脑机接口具有无创安全性高、操作便捷、系统成本低及适用场景广泛等显著技术优势。然而，非侵入式脑机接口通过头皮电极捕获的脑电信号(EEG)、功能性近红外光谱信号(fNIRS)等神经数据记录着人的情感波动、疾病预兆甚至脑组织层面潜意识活动，脑机交互数据可能会暴露用户的数据隐私、身份隐私、信息隐私和思想隐私[4]，脑机交互技术看似“能够阅读和监控个人思想，如同探照灯一般使个人隐私无所遁形”[5]，因此，脑机接口的数据隐私泄露正成为脑机接口飞速发展背后的伦理隐忧。

2024 年 2 月，科技部官网发布了由国家科技伦理委员会人工智能伦理分委员会编制的《脑机接口研究伦理指引》(以下简称“《指引》”)，该指引旨在指导脑机接口研究合规开展，防范脑机接口研究与应用过程中的科技伦理风险。《指引》指出，脑机接口研究过程中采集的神经数据或实验样本反映了研究

参与者的思维精神状态、生理健康信息及性格特征、财产信息等隐私数据，应对数据或样本的收集、存储、使用、加工、传输和发布等进行全流程系统性的保障；并严格遵守《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等相关法律法规和标准规范，加强风险监测，防止神经数据或实验样本泄露，保障数据安全和研究参与者的个人隐私保护。

1 神经数据安全风险分析

神经数据是大脑活动的直接映射，既有生理属性，又有精神属性。通过对神经数据进行采集与解码，研究者不仅能了解大脑机理状况，更能借助深度学习模型等技术解析出人的情绪、意识、认知等心理状态信息[6]，例如，大脑特定区域的异常数据能揭示出有抑郁症的倾向，神经数据经过采集、处理与应用等过程，数据的保密性会逐渐弱化。因此，这些数据的隐私保护除了依赖数据加密或访问权限等技术手段外，更要依托使用者的伦理意识，一旦泄露就可能导致个体隐私泄露的风险。在脑机接口研究和应用中，为保护神经数据的安全，需对数据风险的来源、类别和路径进行深入分析，以便为数据保护建立有针对性的框架体系。

1.1 数据采集风险分析

非侵入式脑机接口的数据采集主要通过安装在头皮的电极或传感器来捕捉微弱的神经脑电信号或血氧动力学变化，这种看似无创、安全、便捷的采集技术，却能够成为神经数据隐私泄露的隐患[7]。

首先是环境“噪声”干扰带来的隐私泄露风险。脑电信号由于其信噪比低，在采集过程中较易被无关噪声污染，因此脑电波形中常混有不同程度的伪迹信号。按照产生来源通常可以将脑电伪迹分成两类，一类是由外部环境引起的非生理伪迹，一类是由研究参与者自身生理活动引起的生理伪迹[8]。这些伪迹会掩盖脑电信号中携带的功能信息，使得后续的数据分析或功能执行发生错误。为获取可解读的有效信号，非侵入式脑机接口的采集设备通常需具备增益放大功能，但经增益放大的信号可能被其他第三方设备捕获，通过把这些特征信息与类似于用户的日常活动轨迹数据等辅助信息相结合，便可能推断出用户身份或活动场景，从而形成了隐蔽且易被忽视的隐私安全漏洞。

其次是设备本身的安全问题。脑机接口技术产品本身是一种机械电子装置[9]，消费级的非侵入式脑机接口设备越来越轻便小巧，例如智能耳机或智能头盔，甚至是微型传感器。然而，这些设备一旦落入他人之手，设备里记录的最原始的大脑活动信息，就可能被轻易地非法获取。

另外一个值得警惕的风险是“脑纹”的形成及其唯一性[10]。研究发现，人类大脑的脑电波模式，或者对看图听音乐等特定事件产生的脑电反应波形，是独一无二的。这种独特的脑电波形被称为“脑纹”。利用“脑纹”来识别个人身份，准确率已经接近甚至超过传统的指纹识别[11]。“脑纹”是天生且无法更改的。一旦包含“脑纹”信息的原始脑电数据被盗，意味着这个人大脑的生物识别特征将永久暴露，后果将极其严重且不可逆，它不像泄露了密码可以更改，所以其危害程度远远超过一般的个人信息（如姓名和电话号码）的泄露。

数据采集环节作为神经数据流动的起点，是非侵入式脑机接口数据隐私保护链条中最基础也最易被忽视的薄弱环节，一旦防护不当，还可能为后续数据处理和应用环节的隐私保护埋下难以根除的隐患。

1.2 数据处理风险分析

非侵入式脑机接口的数据处理，是指通过复杂的深度学习模型算法对采集的脑电信号进行特征提取和识别，转化为可解读的情绪或认知状态，最终形成可供外部设备执行的指令[12]。

深度学习模型由于其复杂的算法机制常被视为“黑箱”，所以，学习模型在运行过程中可能存在难以发现的隐性学习路径，提取与目标无关的生物特征，此类特征虽然可以提升模型在特定数据集上的分类性能，却属于与核心任务无关的隐私敏感信息。另外，目前深度学习模型仍存在分辨率不足等问题，导致研发者难以精准定位模型所依赖的关键特征，无法主动识别并消除这类潜在的隐患。而且“黑箱”模型进一步引发了精神隐私边界失控的风险[13]，脑机接口设备使用者无法清晰知晓自身脑电信号中哪些神经表征被模型提取，也难以判断模型基于神经数据所解读的结论是否合理，实质上丧失了对个人精神隐私包括认知、情绪、神经活动规律等核心隐私的掌控权，导致“知情同意”制度逐渐沦为形式，使用者知情同意的有效性与自主性被严重削弱，违背了《脑机接口研究伦理指引》中“研究参与者参与研究之前应当全面获悉手术和相关治疗的风险－受益评估结果”的知情同意原则。

脑电信号的分析与处理需要经过多次迭代逐步实现从原始生理信号到可解释决策结果的转化。为满足迭代需求、支持回溯分析，研发机构往往会对非原始数据进行长期存储，这类数据虽然不是直接采集的原始神经记录，但其保留了可唯一溯源至相应个体的特异性神经模式，数据的隐私泄露风险并未因数据形态的转换而降低，反而可能因“非原始数据＝低敏感数据”的认知偏差而被研发者忽视，形成隐私保护体系中的薄弱环节[14]。一旦此类数据发生泄露，别有用心者可能利用数据中的特异性模式实现个体的身份匹配与神经状态推断，对用户精神隐私构成与原始数据泄露同等程度的威胁。

神经数据的处理往往涉及多个主体，由于不同主体的数据隐私保护权责常常界定不清，一旦发生事故，不同主体可能会互相推诿责任。例如，研发机构以“深度学习模型决策的不可解释性”为借口规避责任，云服务商则以“技术中立”为由，认为其仅提供基础存储服务，不对数据处理的结果负责。另外，现有的伦理审查机制重视审查研究参与者知情同意的合规性、数据采集流程的合理性，缺乏针对神经数据处理算法的专项伦理审查规范，这些因素都导致了数据处理环节的风险隐患，难以发现和消除。

1.3　应用生态风险分析

当神经数据应用于医疗、康复、教育和安防等场景时，由于商业资本的逐利、监管的滞后以及用户认知的不足，导致伦理问题层出不穷。例如，有的企业通过分析用户脑电信号形成“情绪画像”，并通过定向推送算法进行针对性营销，有的企业以“认知优化”为噱头，将非侵入式脑机接口设备包装为提升学习效率的增强型设备[15]。另外，脑机接口技术在职场和教育等场景的应用，可能异化为精神控制工具，例如，有的雇主用脑机接口设备监测员工注意力和疲劳状态，将采集的神经数据与员工的绩效考核体系直接关联[16]，这些做法将员工异化为神经信号可量化的生产机器，构成对员工人格尊严的严重侵害。类似的情形还有使用脑机接口设备评估学生在课堂上的专注度，并将学生的神经数据引入学生学习能力评价体系，忽视学生的学习风格、文化背景、思维习惯等多维差异，对学生的自由发展造成极大损害。

全面介入社会生活的非侵入式脑机接口系统将会让使用者暴露于新型攻击方式中，例如神经指令劫持，攻击者可通过恶意软件侵入用户脑机接口设备，非法篡改输出指令，进行非授权操控外部机械设备。这种攻击行为一旦发生，如操作者控制机械臂作业或是功能障碍者操控轮椅这样的场景，可能导致直接物理伤害甚至致命性安全事故[17]。

通过上述对非侵入式脑机接口在信号采集、数据处理和应用生态 3 个层面多维度、多层级的伦理问题和风险剖析可知，单独依赖技术防护、法律规制或伦理约束中的任何一方都难以实现对数据隐私的有效保障，必须构建技术规范、法律约束与伦理治理协同作用的规范框架。

2　非侵入式脑机接口数据隐私保护治理协同框架的构建

构建非侵入式脑机接口数据隐私保护治理协同框架，需以国家科技伦理委员会人工智能伦理分委员会研究编制的《脑机接口研究伦理指引》为基础，利用技术手段建立基础防护，通过法律明确各方权利和责任，借助伦理机制平衡技术发展与人的基本权利保护，最终实现对神经数据从获取到使用全过程的全面风险防控管理。

2.1　建立神经数据保护的技术规范

首先，在脑机接口技术应用中，要根据数据类别和使用场景，在技术层面对神经数据设置不同的访问权限。例如，原始的脑电信号包含了类似指纹一样独一无二的“脑纹”信息，一旦泄露或滥用将直接威胁个人核心隐私，因此必须使用最严格的加密技术进行数据保护；而经过处理后无法追踪到具体个人的群体统计数据，因隐私泄露风险较低，可降低保护级别。其次，脑机接口硬件设备本身要具备防拆卸、防偷盗的安全机制，软件算法逻辑要可解释，避免因算法黑箱侵犯用户的精神隐私。另外，要建立数据追踪系统，一旦发现异常访问立即阻断，针对异常情况要制订应急预案，尽量减少或遏制信息泄露[18]。

建立技术规范能够为神经数据提供直接有效的保护，也能为法律监管和伦理审查打下坚实的基础。

2.2　制定神经数据保护的法律规范

法律需要明确规定神经数据是个人敏感信息的一部分[6]，研究参与者对自己的神经数据拥有绝对的所有权及自由决定是否授权给他人的权利，任何机构不能利用复杂晦涩的协议文本来达到无限期和超范围占有和使用这些数据的目的。

监管要区分场景，针对医疗诊断、司法鉴定和教育评估等不同的应用领域，遵循“最少必要”的原则，进行差异化监管。“最少必要”原则是指按照合法正

当、目的明确和选择同意等要求，仅收集、存储和使用业务所必需的最少数据，仅授予相关人员工作所需的最小权限，有效防范数据泄露、窃取、损毁、丢失和滥用等风险。第三，处罚措施要更有力，对于滥用神经数据做商业推销，甚至倒卖脑纹信息等行为，要处以重罚。在用户维权时，适当减轻用户的举证负担，使法律规制从形式保护转向实质保护，真正实现对神经数据滥用行为的有效震慑。

2.3 加强伦理治理，规避潜在的伦理隐患

要不断提升科研人员与公众的科技伦理素养，深化跨学科合作，共同推动脑机交互技术伦理的健康发展[19]。首先要革新脑机接口伦理审查机制。审查脑机接口临床研究的伦理审查委员会需加入数据处理专家、算法设计专家等专业技术人员共同参与审查监管[20]，做到临床研究全生命周期、全流程审查。其次，改进研究参与者的“知情同意”过程。用清晰易懂的方式（比如图表和动画）向研究参与者解释清楚非侵入式脑机接口临床研究可能的潜在的风险[21]，知情告知内容除了研究目的、研究内容和流程等知情同意要素以外，还要尽可能充分告知非侵入式脑机接口技术隐藏的一些信息，比如“脑纹”一旦泄露无法更改；脑机接口技术可能推断出研究参与者的情绪状态；非侵入式脑机接口研究大多情况需要长时间的、重复的和高频率的刺激等，这些信息要让研究参与者有充分的时间考虑是否参加研究。即便研究参与者同意参加研究，这个知情同意也应是“动态”的，研究参与者或其监护人可随时查看自己的数据被如何使用，可分别同意或拒绝数据采集、分析和使用等不同环节，并且能随时撤回同意。同时，要告知清楚研究参与者非侵入式脑机接口的相对优势和劣势，例如即便经过长期的刺激治疗研究也可能出现无效的结果，这种情形应由研究参与者充分理解后自主决定是否参加研究[22]。另外，如果数据用途发生改变或者数据发生泄漏，系统必须主动通知研究参与者或其监护人并重新获得其同意。上述措施能让研究参与者或其监护人真正掌握对自己数据的控制权，避免在技术面前处于被动。

3 结论与讨论

神经数据直接关联人类脑活动、认知特征等核心敏感信息，在非侵入式脑机接口（BCI）技术迅猛发展并广泛应用的背景下，其带来的数据隐私风险呈现出前所未有的复杂性与隐秘性，已超越了单一维度的管控范畴。传统的治理模式或因技术迭代过快而滞后，或因伦理情境复杂而失准。因此，构建一个融合技术、法律与伦理的协同治理框架，可以前瞻性地、全方位地及全过程应对 BCI 数据隐私风险，确保脑机接口技术进步始终以尊重和保护人的尊严为前提，实现技术进步与人文关怀的和谐统一，从而保障非侵入式脑机接口技术始终在服务于人类的道路上合规前进。

技术、法律与伦理的协同治理框架不仅强调通过技术构筑底层防线，依靠法律法规划定红线，更注重通过伦理准则内化价值导向，从而形成一个动态调整、正向循环的治理闭环。该治理协同框架优势在于：第一，实现了不同治理方式的相互协同与互补。技术治理提供了坚强的底层保护，弥补了法律规范应对未知风险的滞后性。第二，形成了多层级的治理。法律提供具有强制力的底线约束，伦理则填补法律空白，引导更高阶的“善治”，尤其在应对“意念隐私”和“认知自由”等新型权利诉求时，伦理的审思为法律未来的完善提供了价值基石。第三，激发了多元主体的共治潜能。该框架要求技术开发者、立法者、伦理学家、用户及公众共同参与，促进了治理责任的广泛化与社会化。

当然，与传统的侧重于“技术标准合规”或“严格立法”的框架相比，该框架也存在不容忽视的劣势和挑战：其一，协同成本高昂且可能导致治理冗余。技术手段、法律条文与伦理审查标准之间的协同过程复杂，可能影响创新步伐。其二，存在责任界定模糊的风险。当数据泄露事件发生时，是技术防护的失效、法律监管的漏洞，还是伦理教育的缺位。多元共治在缺乏清晰权责界定的情况下，容易陷入“集体负责实则无人负责”的困境。其三，伦理原则的“软约束”性质，在面对巨大商业利益或军事应用等强驱动时，可能显得无力，仍需依靠法律与技术的“硬杠杆”。

本框架的创新性在于将“伦理治理”贯穿于技术设计、立法论证与公众教育的全过程，与强调“自上而下”集中监管的模式相比，本框架更注重构建一个能够适应技术不确定性的“适应性治理”体系，其中伦理的开放性讨论为法律与技术标准的迭代提供了持续的“负反馈”机制。

本文侧重于框架的理论构建与逻辑论证，对于技术、法律和伦理之间具体的耦合机制、权重分配以及在不同应用场景（如医疗、娱乐和教育）下的差异化配置，尚未能深入展开。非侵入式脑机接口技术

本身仍在快速演进，其数据形态与隐私威胁也在不断变化，文中提出的框架能否经受住未来技术的冲击，仍需持续观察与修正。需要在实证层面进一步探索如何利用人工智能等工具，动态监测与评估协同框架的治理效能，从而在理论与实践的循环互动中，不断完善脑机接口时代的隐私保护范式。

利益冲突　所有作者均声明不存在利益冲突

作者贡献声明　孟丽君负责文章撰写与修改审校；张海红负责文章的修改；何照楠负责查阅文献

参　考　文　献

[1] 肖峰. 脑机接口哲学[M]. 北京：中国社会科学出版社，2023.

[2] Karikari E, Koshechkin KA. Review on brain-computer interface technologies in healthcare[J]. Biophys Rev, 2023, 15(5): 1351-1358.

[3] 邱爽，杨帮华，陈小刚，等. 非侵入式脑—机接口编解码技术研究进展[J]. 中国图象图形学报，2023，28(6)：1543-1566.

[4] 任思腾，周程. 脑机交互中的隐私问题和自主性风险[J]. 自然辩证法研究，2025，41(8)：53-59. DOI：10. 19484/j. cnki. 1000-8934. 2025. 08. 005.

[5] 肖峰. 脑机接口技术的发展现状、难题与前景[J]. 人民论坛，2023(16)：37.

[6] 李筱永，梁恒瑜，任静. 脑机接口技术中神经数据的法律性质探析[J]. 医学与哲学，2024，45(17)：58-62.

[7] Angulo Medina AS, Aguilar Bonilla MI, Rodríguez Giraldo ID, et al. Electroencephalography-Based Brain-Computer Interfaces in Rehabilitation: A Bibliometric Analysis (2013-2023)[J]. Sensors (Basel), 2024, 24(22): 7125.

[8] 赵欣，吴建行，王坤. 脑电信号伪迹去除算法综述：信号处理[J]. 2025，41(6)：1016-1017.

[9] 张喆，赵旭，马艺昕，等. 脑机接口技术伦理规范考量[J]. 生物医学工程学杂志，2023，40(2)：358-364.

[10] 刘泽华. 面向脑纹识别任务的脑电通道选择算法研究[D]. 北京：北京交通大学，2024.

[11] 伍冬睿，涂运禄，付昊天. 一种用于跨会话场景的在线脑纹识别方法：202411691142[P]. 2025-03-14.

[12] Wei X, Narayan J, Faisal AA. The 'Sandwich' meta-framework for architecture agnostic deep privacy-preserving transfer learning for non-invasive brainwave decoding[J]. J Neural Eng, 2025, 22(1).

[13] 王高峰，张志领. 算法伦理视域下的脑机接口伦理问题研究[J]. 自然辩证法研究，2022，38(7)：68-73. DOI：10. 19484/j. cnki. 1000-8934. 2022. 07. 013.

[14] 曾益. 医用脑机接口数据隐私的法律规制：国际比较与启示[J]. 卫生法学，2024，32(4)：73-79. DOI：10. 19752/j. cnki. 1004-6607. 2024. 04. 012.

[15] 金忠星，李东. 消费者偏好预测的深度学习神经网络模型[J]. 计算机应用，2019，39(7)：1888-1893.

[16] 曾睿，何伦凤. 脑机接口技术多领域扩散的外溢风险及其规制[J]. 华南理工大学学报：社会科学版，2023，25(1)：25-32. DOI：10. 19366/j. cnki. 1009-055X. 2023. 01. 004.

[17] Ienca M, Haselager P, et al. Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity[J]. Ethics and Information Technology, 2016, 18(2): 117-129.

[18] 丛杭青. 数据伦理[M]. 北京：高等教育出版社，2025：55-56.

[19] 周程. 脑机接口领域中的伦理问题研究[J]. 人民论坛·学术前沿，2024(16)：44-55. DOI：10. 16619/j. cnki. rmltxsqy. 2024. 16. 005.

[20] 孟丽君，李义庭，孙莹炜，等. 人工智能在康复领域研究应用的伦理审视[J]. 中国医学伦理学，2025，38(2)：166-172.

[21] 曹若愚，瞿骏林. 脑机接口技术应用中知情同意权的伦理与法律规制研究[J]. 天津科技，2024，51(9)：85-88，93. DOI：10. 14099/j. cnki. tjkj. 2024. 09. 023.

[22] 顾心怡，陈少峰. 脑机接口的伦理问题研究[J]. 科学技术哲学研究，2021，38(4)：79-85.

（收稿日期：2025-08-29）

《中华医学科研管理杂志》第六届编辑委员会通讯编委名单