DOI:10.16104/j.issn.1673-1883.2026.01.010

脑机接口数据使用与保护研究

陈庭朗

摘要：对脑机接口数据使用与保护的研究，有助于为脑机接口行业合理利用数据提供明确路径指引。脑机接口设备所采集到的数据来源于使用者的大脑信息，大脑信息涉及使用者的敏感个人信息和隐私信息，脑机接口数据在使用过程中需要厘清使用边界，保障数据来源者的个人信息权益和隐私权利，避免出现数据安全事件。为了平衡脑机接口行业发展与数据保护之间的关系，需要构建脑机接口数据收集动态知情同意机制，合理厘定脑机接口数据限制性使用边界，以及通过外部监管机制保障脑机接口数据处理活动的安全性。

关键词：脑机接口数据；敏感个人信息；隐私权；数据安全

中图分类号：D922.16 **文献标志码：**A **文章编号：**1673-1883(2026)01-0099-11

收稿日期：2025-02-16

作者简介：陈庭朗（2000—），男，广东佛山人，福建师范大学法学研究所研究助理，硕士，研究方向：数字法学、民商法学，E-mail：951331038@qq.com。

一、引言

随着科学技术的飞速发展，人工智能、虚拟现实等技术引发了人们广泛的关注，元宇宙概念的兴起更让人对科幻电影展示的人类在虚拟世界面对面沟通生活的场景有所期待。作为实现元宇宙的核心技术之一的脑机接口（Brain-Computer Interface,BCI）能够将人脑和机器连接起来[1]，在新技术的加持下，人机交互的科幻场景逐步成为现实。脑机接口目前主要在医疗、康复领域使用，最初目的是医治因神经损伤或者神经疾病而导致无法行动、无法交流的人群，使其恢复一定行动和表达能力。尽管脑机接口技术最初旨在用于医疗康复，但逐渐发展到除医疗、康复领域之外的用途，在娱乐、教育以及军事等领域得到开发应用[2]。脑机接口的工作原理是在检测识别大脑神经电活动的特征信号后，通过计算机语言编程转化为命令信号以驱动外部设备，从而能够实现人脑对外部环境的控制[3]。根据与大脑的连接方式，脑机接口可以分为侵入式、半侵入式和非侵入式，前两种脑机接口通过手术将电极植入颅骨以内，所采集的脑电信号质量较高，后者非侵入式脑机接口避免了手术，将设备设置在颅骨外，但是采集到的信号质量较低[4]。

脑机接口设备在运行过程中会收集使用者大脑活动信息，并以数据形式传输给计算机终端进行使用，这些数据也会用于相关解码算法的研究训练。显然，脑机接口必然会涉及使用者大脑信息数据的收集、存储以及使用，这些数据源于使用者的大脑，具有私密性，通过解码这些数据，可以反映出大脑的运作过程与结果，从而“窥探”到使用者的思想、情感态度和意图等私密信息。尽管脑机接口技术目前尚处于发展阶段并没有大规模应用，但是一旦发生数据泄露可能意味着使用者最为私密的大脑信息得以破译。纵观人机交互技术的发展历程，从人工耳蜗（Cochlear Implant）到脑深部电刺激术（Deep Brain Stimulaiton，DBS）再到脑机接口技术，人体和机器的边界愈加模糊[5]，引发了人们关于脑机接口的伦理、法律等相关问题的讨论。如在伦理层面关于脑机接口使用者的自我意志、身份认同等问题的讨论[6]，还有在法律层面关于脑机接口使用者的隐私[7]、知情同意权[8]、神经权利[9]等问题讨论。现有讨论中针对脑机接口所产生的数据使用以及保护问题的讨论较少，本文旨在针对脑机接口数据使用与保护问题进行探讨。

新兴技术的出现，一方面会引起生产方式的变革，带来生产力的飞跃，另一方面也可能带来未知的风险，产生新的法律纠纷。脑机接口技术的出现，无疑对医疗、教育以及娱乐等领域带来新影响，承载着大脑信息的脑机接口数据与一般数据相比较，显然具有特殊性。对于这种特殊的数据该如何使用，其保护限度该如何厘定，现有的法律规制路径是否能在留有新兴技术发展空间与保护数据安全两者之间达到平衡，这一系列的问题都值得进一步思考与讨论，最终为脑机接口技术发展以及数据使用问题提供清晰的路径方向。

二、脑机接口数据的特殊性

（一）脑机接口数据来源的特殊性

大脑信息能映射出个人的心理活动。大脑是人体最复杂的器官，每日需要处理大量信息，人的行为、决策等离不开大脑，在受到不同刺激情况下，大脑会诱发出不同的情绪，这些情绪能够反映出个体的心理活动。在不同的情绪状态下大脑发出的脑电信号不同，通过捕获不同频段的脑电信号形成脑电图（EEG）能够对情绪进行识别[10]。通过分析EEG以识别出的情绪状态并与个体所受到的刺激素材结合进行研究，一定程度上可以解读个体的心理活动、生理状态等。因此，大脑发出的脑电信号能映射出个人的心理活动，通过对大脑所发出的脑电信号进行分析，识别出个人情绪状态，从而揭示出个人的心理活动，利用此类大脑信息能实现电影等艺术作品中所谓的“读心”“读脑”场景。

传统的数据采集难以收集大脑信息。一般的数据采集通过传感器、日志文件以及爬虫等手段采集到设备技术参数、网络服务记录等多种信息，并将这些信息以数字形式聚合，等待存储和分析处理[11]。一般的数据往往来自商业活动、网络服务活动等所产生的信息，这些信息也有可能会涉及个人信息，甚至涉及隐私信息，例如姓名、住址以及肖像等能识别个人身份的信息。传统的数据采集方式下并不会收集到脑电信号这类大脑信息，并且一般数据收集传感器无法直接采集到微弱的脑电信号，只有通过特定的采集装置才能收集到。简而言之，日常生活中个人的大脑信息并不会轻易地被收集并制作成数据，仅在特定场景下才有可能被收集。

脑机接口数据来源于大脑信息。脑机接口通过电极收集脑电信号，以数据形式传输至计算机终端存储，最终由算法解码、分析并处理数据。从脑机接口的运作过程来看，脑机接口数据来源于脑电信号，

这些信号是大脑活动的直接体现，即大脑活动的直接信息。大脑作为人体的控制中枢，其发出的脑电信号通过神经系统向人体各个运动器官发出控制指令，即使神经系统和运动器官受损而丧失功能，只要大脑功能正常，控制指令仍能通过脑电信号从大脑传输，同时脑电信号会根据大脑的思维活动以及受到的外部刺激而呈规律性变化[12]。显然，脑电信号能反映出人的思维活动、情绪状态以及心理活动等多种大脑活动信息，即直接来源于大脑活动信息。这些大脑信息具有个人的唯一识别生物特征，经过筛选、识别以及解读后还可能形成有价值的隐私[13]。因此，来源于大脑信息的脑机接口数据包含着使用者自身可用于生物识别的敏感个人信息以及隐私信息。脑机接口数据与敏感个人信息、隐私信息均涉及人格权益保护，脑机接口数据来源于大脑信息则使其更为特殊，甚至可能触及人类“思想”这一私密领域。

（二）脑机接口数据的应用场景

脑机接口数据在医疗领域的作用。脑机接口技术首次应用是在1963年，英国的格雷·沃尔特（Grey Walter）医生通过外科手术将电极植入一名癫痫病人大脑中，实现了病人通过意念控制幻灯片的“脑控”效果[6]38。该技术最初目的就是用于帮助治疗神经疾病以及帮助瘫痪患者恢复一定的行动能力。目前，脑机接口技术仍主要应用在医疗领域，如马斯克旗下脑机接口公司Neuralink在继帮助患者通过思考控制计算机以实现打电子游戏能力后，其研发的一款名为“盲视（Blindsight）”的实验设备获得美国食品药品监督管理局（FDA）的批准，已用于尝试帮助盲人恢复视力[14]。这些脑机接口设备在运行过程中所收集到的数据，会用于终端算法训练，以提高脑机接口技术的交互准确性，有助于医疗领域的脑机接口设备进一步完善，减少脑机接口带给患者的副作用。其次，在医疗领域产生的脑机接口数据，有助于医生观察患者病理状况，更有针对性地改进疾病治疗、行动力恢复方案。简言之，脑机接口数据在医疗领域无论是用于改进医用脑机接口设备，还是调整治疗康复方案，最终都是反馈到个人身体中，对人的身体健康有明显影响。

脑机接口数据在其他领域的作用。脑机接口技术除在医疗领域应用外，还会在教育、娱乐等其他领域应用，在这些领域中脑机接口技术发挥着监测人体状态、增强人体感官的作用。如在教育领域，脑机接口能对学习者的学习状态、注意力水平进行监测，通过脑机接口设备采集反馈的数据安排学习者进行放松训练、重新集中注意力等等[15]。在娱乐领域，理查德·拉姆恩发布的短片《那一刻》运用了脑机接口技术，观众通过头戴脑电图仪，短片的内容就会在脑海中呈现，观众无须睁开双眼就能观影[16]。显然，无论是在教育领域监测学习状态还是在娱乐领域中增强人体感官，脑机接口技术在其他领域的应用与人体状态密切相关，所产生的脑机接口数据因为来源于大脑信息，对于分析人体状态有着重要作用。

脑机接口数据在应用层面与人体活动密切相关。首先，脑机接口数据的应用意义特殊，通过检视脑机接口数据在应用层面的作用，不难看出脑机接口数据与人体活动密切相关，在各个脑机接口应用场景中用于分析、监测以及调整人体活动，对于人体健康有着重要意义。其次，脑机接口数据的应用场景特殊，一般数据并不会反映人体活动状态，更不会应用于调整人体活动等涉及人身健康的场景，无论脑机接口技术是用于患者治疗康复，还是学习状态监测调整，脑机接口数据在这些场景中对人体活动状态的反映成为脑机接口终端调整的参照，最终参数的调整与使用者的身体健康关系紧密，所产生的数据最终应用也会与人体活动密切相连。简言之，脑机接口技术基础决定了脑机接口数据在应用上与人体活动密切相关，从而导致脑机接口数据的应用场景、应用意义具有特殊性。

(三)脑机接口数据的安全风险

脑机接口数据泄露、篡改会影响使用者生命健康安全。脑机接口技术触及人类最重要的器官——人脑，关乎使用者的生命健康安全，脑机接口数据安全也是保障使用者生命健康安全所无法忽视的问题。部分脑机接口设备除了采集大脑信息外，还具有神经调节功能，对脑部进行刺激，即使是非侵入式脑机接口，也能够通过释放磁信号透过颅骨刺激大脑神经[17]。若发生泄露、篡改脑机接口数据的事件，除了导致脑机接口设备失灵以外，还可能让脑机接口设备终端算法误读数据，从而错误释放磁信号，导致使用者大脑受损，进而危及使用者的生命健康安全。从保障使用者生命健康权益的角度，脑机接口数据安全具有特殊性，一旦数据安全保障措施有所松懈，可能会让使用者遭受难以弥补的身体损害。

脑机接口数据泄露会影响国家安全。传统人工智能通过数据处理技术，进行数据挖掘，能读取出个体的物理隐私和个人信息，而解码脑机接口数据不仅能反观个体的大脑运行，还可以深思大脑的运行结果，凝视个体最私密的意图、思想[18]。脑机接口数据来源于大脑信息，一旦发生数据泄露事件，个体大脑的思想观点可能一览无余，相较于物理外观上的人体隐私信息，个体大脑中承载的隐私信息更为私密，也是个体最不愿意向外界公布的私密信息。随着脑机接口设备应用场景的扩张，部分知悉国家秘密的研究人员、国家工作人员也可能接触到使用脑机接口设备的场景，他们所使用的脑机接口设备产生的数据可能涉及国家秘密，这些数据泄露无疑会给国家带来损失，危及国家安全。

脑机接口数据也存在黑客侵入风险。脑机接口设备需要接入网络进行交流互动，在此过程中存在黑客攻击的风险，在2012年USENIX安全研讨会上，牛津大学的伊万·马丁诺维奇教授等人介绍了一款能够收集脑机接口数据以窃取信息的“脑间谍软件”以验证脑机接口设备的数据安全性，该款软件通过分析脑机接口使用者在观察到特定信息后视觉刺激反应来提取私人信息，如住址、出生日期、信用卡号甚至使用者所知悉的人物[19]。脑机接口数据承载着使用者大量隐私和个人信息，黑客攻击脑机接口设备的直接目的是获取这些信息。其次，脑机接口设备还能通过外部设备实现交互功能，黑客也可能通过篡改脑机接口数据，以改变原有控制指令，从而操控脑机接口外部设备来实现不法目的。黑客侵入脑机接口设备，除了窃取数据以获取私密信息外，还可能通过篡改数据以控制设备，脑机接口使用者便丧失了设备控制权，做出违背其意愿的行为。这不仅仅是数据泄露，还可能借此实施更严重的侵权行为，甚至实施犯罪行为。

三、脑机接口数据规制路径检视

(一)脑机接口数据收集的规制路径检视

用户的知情同意是数据收集的前置机制。根据《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第十四条规定可知，处理个人信息需以个人充分知情且自愿同意情形为前提。知情同意有两方面的要求，首先是知情，即在采集个人信息时应对信息主体进行告知；其次是在个人真正知情的前提下进行“同意”，即个人信息处理者应以明确且易懂的方式告知信息主体处理的信息、目的、储存时间等内容[20]。此外，出于维护信息主体利益的考虑，《个人信息保护法》第十三条设置了个人信息同意的例外情形，其中紧急情况下为维护自然人生命健康或财产安全时可不经过个人同意便可处理个人信息。但脑机接口技术在医疗领域中使用也并非所有应用场景都属于维护生命安全的紧急情况，这并不会影响

用户知情同意作为脑机接口数据收集的前置机制。脑机接口数据来源于大脑信息，大脑信息作为大脑活动的直接记录无疑属于个人信息的范畴，因此，脑机接口用户的知情同意是脑机接口数据收集的前置机制。脑机接口数据的处理者应当遵守知情同意制度，在收集用户大脑活动信息前应告知用户收集大脑信息的方式、目的、储存时间等内容，并在用户真实自愿同意的前提下才能对脑机接口数据进行收集。

普通用户对脑机接口技术存在理解难度。知情是用户做出同意脑机接口数据处理者收集信息的前提条件，即用户对于脑机接口技术有所了解并对脑机接口设备所收集信息内容、用途知悉。首先，脑机接口技术本身就具有复杂性，其综合了神经科学、生物工程以及计算机科学等多个领域的知识，普通人并不能在短时间内充分理解该项技术原理，此外要知悉脑机接口数据安全性问题、泄露风险问题，也需要一定的专门知识作为基础[21]。其次，脑机接口技术目前仍处于发展阶段，离大规模普及还有一定距离，普通人在使用该项技术产品之前较少了解相关技术原理与风险。脑机接口技术的复杂性以及应用层面普及程度低等问题使得普通用户对脑机接口技术存在理解难度，这需要脑机接口数据处理者在收集用户信息前，尽可能地把复杂的技术原理转化为普通用户所能理解的表述，取得用户真实的同意。

部分病患的同意能力受限。脑机接口技术目前在医疗领域应用于运动功能障碍、意识障碍和精神疾病患者的诊疗中[22]，受疾病影响，这三类患者的同意能力有所不同。运动功能障碍的患者通常仅是肢体活动能力受限，能够作出同意脑机接口技术应用以及数据收集的意思表示；意识障碍患者可能处于视物状态和微意识状态，此类患者常处于无法交流的状态，不具备意思表示的能力，更何谈作出同意的能力；精神疾病患者精神健康状态不稳定，若处于发病状态往往欠缺民事行为能力，其民事行为能力取决于其能否辨认自己的行为[23]。因此，精神疾病患者作出同意的意思表示是否有效应取决于其是否具备辨识能力。不同于在娱乐、教育等其他领域使用脑机接口技术的用户，在医疗领域需要使用脑机接口的部分病患，可能意思表示能力受限，难以判断其所作出的同意是否真实有效，这对知情同意制度在脑机接口数据收集规制上产生一定挑战。

（二）脑机接口数据使用的规制路径检视

脑机接口数据在医疗领域的使用规制。在医疗领域，医疗数据的流通使用涉及多个主体，除了患者，还包括医院、医学研究机构、保险公司、政府部门等主体，这些主体出于改善医疗实践、创新治疗方法以及公共卫生管理等目的，对医疗数据都有一定使用需求[24]。脑机接口数据在医疗领域流通使用不免涉及这些主体，这些主体在数据使用过程中需要遵守《个人信息保护法》《中华人民共和国数据安全法》（以下简称《数据安全法》）等法律法规中的相关规定，基于法律法规篇幅和表述形式的局限，相关法律法规难以完全涵盖医疗领域数据使用的规制措施。针对此种情况，有关部门制定了医疗数据使用国家标准《信息安全技术健康医疗数据安全指南》（以下简称《医疗数据指南》），该标准涵盖医生调阅、医疗服务移动应用、商保对接、二次利用等多个场景的数据使用要求，为参与医疗领域数据使用的主体提供指引。相关主体在医疗领域可参照该标准使用脑机接口数据，减少在使用过程中发生危及数据安全事件的可能。

脑机接口数据在其他领域的使用规制。有学者指出，脑机接口技术在使用过程中不免会收集到大脑信息，当算法识别不同用户信息后可为其创设独一无二的标识符，这些标识符可用于身份认证，日后可能会成为身份法律制度的一部分，但仍有待国家统一的技术标准对其推广使用加以规制[25]。不论是身份认证，还是游戏娱乐等其他领域，脑机接口产生的数据在这些领域的使用亟待由国家统一标准加以规制。

除了前述《医疗数据指南》，脑机接口数据在其他领域的使用规制措施并没有可供参考的标准。《医疗数据指南》也仅是针对医疗健康服务的数据，虽能为脑机接口数据在其他领域的使用规制措施提供一定参考，但并不能完全适配娱乐、身份认证等多领域的使用需求。相比较于医疗领域，在资本逐利性驱使下脑机接口数据在其他领域的商业化使用需求更大，对于使用的规制应当更有针对性地调节商业化使用需求和个人信息保护两者之间的关系。

脑机接口数据使用边界有待明晰。脑机接口数据在不同场景中使用需求有所差异，在部分使用场景中，需要未经脱敏处理措施就直接共享、调阅脑机接口数据，如医生制定治疗方案、医学研究以及商保对接等场景；而在部分场景中，脑机接口数据的转让、加工需要在经过脱敏化处理后方能操作，如脑机接口设备研发企业间数据交易等场景。之所以会产生差异化的需求，是因为不同场景下对脑机接口数据所承载的需求信息不同。在直接使用未脱敏脑机接口数据的场景中，需要使用者的身份信息、生物特征以及健康情况这些敏感信息才能完成服务；而在使用脱敏后脑机接口数据的场景中，更多是需要借助脑机接口设备的参数信息对设备研发改进提供参考，此时并不需要使用者的个人信息来完成设备改进。因此，在不同场景下，应从使用需求出发对脑机接口使用边界加以明晰。

（三）脑机接口数据的保护路径检视

脑印唯一性对数据脱敏带来挑战。数据脱敏包括假名化、去标识化以及匿名化，是保护个人信息与隐私的传统方法[26]。数据脱敏措施使得数据所承载的信息通常无法直接识别出信息来源者的身份，这是常规数据脱敏措施被视为数据保护有效路径的根本原因。脑机接口数据来源于脑电信号，脑电信号除了监测人体健康状态、心理状态以外，还被应用于生物特征识别。有研究指出同类型的单一刺激下收集到的脑电信号识别出个人身份准确性近乎能达到100%，此种方式收集到的生物特征信息泄露后，即使采用不同类型刺激依旧可以识别出被收集者的身份[27]。这种来自脑电信号的生物特征，被称为“脑印”，从研究来看脑印如同指纹一样具有唯一性。脑印的唯一性会导致脑机接口数据常规的假名化和匿名化的脱敏措施失灵，因为这两种措施仅仅把直接表明身份的姓名、身份证号等替换，并没有将带有生物特征的脑电信号信息进行脱敏处理，相关主体仍能比对出这些生物特征信息来源者的身份。采取去标识化的脱敏措施，则需要确定相应的标识符，从而选择采取删除、屏蔽、加密等技术措施，去标识化处理还应注意保持数据可用性，而脑机接口数据中能反映脑印特征的脑电信号信息具有一定价值，因此脑印唯一性对去标识化的脱敏措施也带来挑战，对数据处理者的数据保护措施提出更高的要求。

脑机接口数据外部监管机制尚处于初步构建阶段。《数据安全法》的相关规定初步构建起数据外部监管机制，对数据安全监管的主体、数据安全风险监测以及数据安全审查进行规定。这些规定为脑机接口数据的外部监管机制的构建提供了法律依据，但是具体的监管体系措施，仍有待监管法规和政策的补充，从而形成完整的外部监管机制。首先，要解决的是脑机接口数据安全审查范围划分问题。从《数据安全法》第二十四条的表述来看，数据安全审查范围仅仅是数据处理活动，更关注数据流动过程中的动态安全。大数据时代的数据安全要求确保数据全生命周期安全，在数据流动过程中既保护动态安全，又保护处于某一节点数据的静态安全[28]。静态安全则涉及脑机接口设备数据存储安全以及脑机接口企业数据保护技术水平等方面。要实现脑机接口数据全生命周期安全，在划分安全审查范围时要兼顾数据动态与静态双层面安全风险。其次，还要解决数据安全审查机构设置问题。《数据安全法》的相关规定由国家网信部

门负责统筹协调数据安全监管工作，各个行业的主管部门承担该行业的数据监管职责，但没有规定负责数据安全审查的机构。这导致目前数据安全审查职能由多个机构分散承担，如市场监督管理总局直属的中国网络安全审查认证和市场监管大数据中心（以下简称CCRC）开展数据安全管理认证、数据安全人员培训与认证等服务[29]，还有国家互联网信息办公室（以下简称网信办）作为网信部门实际开展数据出境安全评估、个人信息出境合同备案等工作[30]。显然，数据安全审查职能承担过于分散，应将数据安全审查相关职能集中行使。

四、脑机接口数据使用与保护的对策路径

（一）脑机接口数据知情同意路径完善

细化同意能力判断因素。根据《个人信息保护法》第三十一条规定，以年满十四周岁与否作为是否具备同意能力的基本判断标准，处理不满十四周岁未成年人的个人信息，需征得其父母或其他监护人同意。以年龄作为同意能力的判断标准，是由于部分未成年人心智尚未成熟，对复杂的个人信息处理行为难以理解与辨识[31]。除了年龄以外，疾病因素也会改变个人对事物的理解以及辨识能力，从而对个人的同意能力造成影响，因此同意能力判断还应纳入疾病因素进行考虑。首先，在脑机接口设备应用于医疗领域的场景中，部分患者受疾病影响处于微意识或植物状态，这类患者视为不具有同意能力，应征求其监护人的同意来收集脑机接口数据。其次，对于辨识能力受限精神病患者以及因瘫痪而行为能力受阻无法作出同意的患者，只有具有专业知识的主治医生对其辨认事物能力进行判断，因而应当将其主治医生纳入同意能力判断主体中，参考主治医生的意见来判断其是否具有同意能力，不能仅由脑机接口数据处理者进行判断。

丰富告知义务的履行形式。《个人信息保护法》第十七条提出“以显著方式、清晰易懂的语言”来履行告知义务，实践中往往以隐私政策的形式在收集信息前告知信息主体，然而这些隐私政策往往晦涩难懂，信息主体并不会认真阅读。隐私政策是针对不特定群体履行告知义务的形式之一，但由于不同群体的需求、知识结构各异，对隐私政策的详略、专业程度等要求并不一致[32]。在医疗领域的使用场景中，医生会告知使用者脑机接口设备收集的个人信息范围、方式以及数据用途等事项，在这种场景下，即使隐私政策内容专业性很强，使用者也能在医生的阐释下理解相关内容，因而在医疗领域使用场景下，告知内容可以更为详细、专业。而在其他领域使用场景中，并没有类似医生这类专业人员对使用者进行告知，这种场景下，告知义务的履行形式应更加多样，可以通过链接视频讲解数据收集方式、用途等内容，还可以通过简略、通俗版隐私政策推送给普通使用者阅读，确保使用者能够理解告知事项。

构建动态知情同意机制。在传统临床医疗领域的知情同意往往是一次性的，一旦患者在知情同意书上签字即代表着知情同意程序完成，此种一次性的知情同意难以满足对医疗数据长期、反复的研究需求[33]。脑机接口数据在医疗领域的使用，同样具有长期、反复使用的特点，因此需要构建动态知情同意机制。动态知情同意机制应当在《个人信息保护法》相关法条的基础上加以构建，以脑机接口设备使用的不同阶段来划分，结合不同阶段使用者与数据处理者的沟通进行调整。首先，在脑机接口设备使用前，数据处理者应征得使用者或其监护人同意进行数据收集。其次，在设备使用中要重视设备使用者的意愿。部分使用者受疾病影响无法进行沟通交流，其在使用前所做出的同意是由监护人代理完成。当这类使用

者在使用脑机接口设备后恢复了沟通交流能力，数据处理者应再与其进行沟通，由这类使用者选择是否行使《个人信息保护法》第十五条所赋予的撤销同意的权利。最后，当使用者移除脑机接口设备或数据处理者停止提供脑机接口产品与服务时，应视为使用者撤销同意，数据处理者应及时删除承载使用者大脑信息的数据。

（二）脑机接口数据限制性使用边界厘定

大数据时代下，单个数据的价值有限，数据通过流动积累形成数据集从而更好地发挥其最大价值[34]。数据处理者除了将脑机接口设备所收集到的数据存储用于维系产品服务运作、技术研究以外，还能通过数据转让流通以发挥数据最大效用，避免出现数据孤岛现象。此外，数据处理者还能将数据脱敏处理后进行加工成为数据产品，从而出售该数据产品获利。脑机接口数据来源于大脑信息，大脑信息又承载着敏感个人信息和隐私信息，因而脑机接口数据使用涉及敏感信息和隐私信息。受限于技术发展，脑机接口解码算法并不能准确解码所有数据，脑机接口设备所收集到的数据可能超出所需[17]。本文认为，应当根据脑机接口数据所承载信息类型来分类厘定数据使用边界，分为敏感信息数据、隐私信息数据以及无法解码信息数据，并考虑各类型数据对行业发展影响厘定数据使用边界。

敏感信息数据应限制转让、加工等用途。脑机接口的敏感信息数据涉及使用者的生物特征、身体健康信息，这些敏感信息数据在娱乐、教育等其他领域的使用目的最终是为了更好地增强使用者的感官体验，从而获取更大的商业利益。而在医疗领域，无论是医疗器械厂商利用数据完善脑机接口设备，还是部分医疗机构利用数据进行医学研究、完善诊疗方法，均带有维护生命健康的目的。生命权、健康权在民事权益体系中处于最高位阶，理应优先于其他权益进行保护[35]。本文认为，对于敏感信息数据在医疗领域中转让、加工用途使用限制更加宽松，而在其他领域中转让、加工用途使用应严格限制。具体而言，在采取安全加密措施后，允许非营利性质的医疗机构之间对脑机接口敏感信息数据进行转让、加工；对于其他领域的数据处理者，应禁止脑机接口敏感信息数据转让，允许将脑机接口敏感信息数据加工为数据产品，但是相关数据处理者脱敏技术水平应达到法定要求，即经过脱敏处理的数据无法还原且无法识别数据来源者。

隐私信息数据应禁止转让、加工，仅在维系服务、产品运作时存储使用。隐私信息涉及私人生活，是个人不愿意公开的私密信息。隐私信息具有严格的人格权属性，关系到人在社会上自由与人格尊严，其不能自由交易和公开[36]。同理，脑机接口设备所收集的隐私信息数据应当禁止转让和加工成数据产品出售。因为这些数据来源于使用者大脑深处所不愿意为他人所知的信息，如涉及私人情感、性取向等隐私信息，一旦随意被转让、交易，就意味着个人的私密生活被一览无遗，严重侵害个体的人格尊严。本文认为，出于对隐私权的保护，脑机接口隐私信息数据仅限于在维系脑机接口服务、产品运作时可以存储使用，并采取安全措施保护数据。为降低数据泄露风险，若无须用于维系服务、产品运作，数据处理者应及时将隐私信息数据删除。

无法解码的数据仅限研究使用。由于技术发展的局限，脑机接口解码算法并不能准确解码所有收集到的数据。这些无法解码的脑机接口数据用途不明，甚至由于算法黑箱的特征，研究人员难以解释为何无法解码，也不知悉这些数据所承载的具体信息内容。对于这类数据若要求数据处理者直接删除，似乎能避免数据泄露事件的发生，以保护使用者个人信息安全，但是直接删除无法解码的数据也不利于脑机

接口解码算法完善。本文认为，对于无法解码的数据应仅限于研究使用，并设定存储期限，在存储期限内无法完成解码获取信息应删除数据。若在存储期限内解码出数据所承载信息，应根据信息类型分类限制使用。

（三）脑机接口数据外部监管制度的完善

集中数据安全审查职能。随着脑机接口技术在多个行业的应用，出于保障数据安全的考虑，相关部门需要介入对脑机接口数据进行安全审查，但是目前我国数据安全审查工作具有分散性特点，如前文所述由不同部门分别承担数据安全管理认证、数据安全评估等多项工作。近年来，为了更好地组织实施国家大数据战略，推动国家重要数据资源开发利用，在地方层面，各个省份地方政府陆续设立地方数据管理局，作为政府部门的内设机构。在中央层面，国家数据局于2023年10月正式成立，由国家发展改革委直接管理。本文认为，有必要将数据安全审查职能集中，由专门机构行使审查权，构建起央地联动、紧密协作的数据安全审查组织体系。具体而言，在中央层面由国家数据局负责构建数据安全审查处理制度、制定数据安全审查操作和培训标准，以及指导地方数据管理局等工作；在地方层面，由国家数据局和省级地方政府共同管理地方数据管理局，地方数据管理部门负责本地区数据安全审查、数据安全从业人员培训和交流活动等工作，根据当地实际开展审查工作，保障当地数据的安全，及时审查、评估存有安全风险的数据处理活动。

建立行业主管部门和数据安全审查部门协同审查机制。《数据安全法》要求由行业主管部门承担本行业的数据安全监管职责，虽然行业主管部门对行业特点较为熟悉，但是数据安全监管专业要求较高，行业主管部门可能并不具备对数据安全风险进行审查的能力。相较之下，国家数据局与地方数据管理局对于数据安全风险的认知能力与技术能力更强。因此本文认为，应建立由行业主管部门和数据安全审查部门协同审查机制。具体而言，由脑机接口技术涉及卫生健康、科技等行业的主管部门，与以数据局为代表的数据安全审查部门协作，根据不同行业特点协同确定数据安全审查标准，数据安全审查部门对脑机接口数据安全风险进行评估、审查时，还应积极听取相关行业主管部门的意见，力求做出合理、公正的审查结论，妥当平衡数据安全保护与脑机接口行业发展的各方需求。

脑机接口企业的数据保护技术水平应纳入监管范围。脑印的唯一性对传统去标识化的数据脱敏技术产生了冲击，这对脑机接口企业在数据处理活动中数据保护技术水平提出更高的要求。除了动态的数据处理活动，脑机接口数据在静态存储方面的数据安全也应受到重视。因此，应将脑机接口企业的数据保护技术水平纳入数据安全监管范围内，由相关监管部门和数据安全审查部门对脑机接口企业数据保护技术水平进行评估。根据评估结果，允许技术水平达到法定脱敏效果的企业对脑机接口数据进行加工、商业转让等处理活动；技术水平未达到法定脱敏效果的企业仅允许将脑机接口数据用于存储、维系产品服务等用途。

五、结语

在信息化高速发展的时代，数据的价值日益凸显，作为新兴技术的脑机接口，通过算法解码所收集到的数据，实现了人机互动场景。在此场景下，脑机接口数据承载着使用者的敏感信息与隐私信息，需要通过恰当合规的方式进行使用。此外，还要确保脑机接口数据安全可控，数据安全是构建使用者信任

的基础，只有实现数据安全，才能够充分发挥脑机接口数据的价值。为此，应从脑机接口数据收集、使用、保护的全流程入手，平衡好脑机接口行业发展与数据保护的关系。首先，在数据收集过程中，要构建动态同意机制，更好地完善知情同意路径。其次，在数据使用方面，要区分承载不同信息类型的脑机接口数据，厘定合理的使用边界，提高脑机接口数据使用效率。最后，在数据保护方面，完善外部监管制度，保障脑机接口数据安全。

参考文献：

[1] 吉姜蒲.脑机接口合规困境:元宇宙的技术探索和伦理规制[J].湖南行政学院学报,2022(3):116-121.

[2] 肖峰.脑机接口的过去、现在与未来[J].新兴科学和技术趋势,2022(2):193-203.

[3] 杨立才,李佰敏,李光林,等.脑-机接口技术综述[J].电子学报,2005(7):1234-1241.

[4] 葛松,徐晶晶,赖舜男,等.脑机接口:现状,问题与展望[J].生物化学与生物物理进展,2020(12):1227-1249.

[5] SCHERMER M.The mind and the machine:on the conceptual and moral implications of brain-machine interaction.[J]Nanoethics,2009,3(3):217-230.

[6] 李佩瑄,薛贵.脑机接口的伦理问题及对策[J].科技导报,2018(12):38-45.

[7] 张曼.脑隐私法律概念建构:路径、特性与贡献[J].东方法学,2022(5):60-73.

[8] 陶应时,陈巧,刘红玉.治疗型脑机接口的知情同意问题及其应对[J].南华大学学报(社会科学版),2023(1):62-68.

[9] 吴佼玥,李筱永.脑机接口技术视角下神经权利的逻辑生成和规范路径[J].残疾人研究,2022(2):44-53.

[10] 聂聃,王晓韡,段若男,等.基于脑电的情绪识别研究综述[J].中国生物医学工程学报,2012(4):599-606.

[11] 李学龙,龚海刚.大数据系统综述[J].中国科学:信息科学,2015(1):1-44.

[12] 于淑月,李想,于功敬,等.脑机接口技术的发展与展望[J].计算机测量与控制,2019(10):5-12.

[13] 吴佼玥,张博源,任静,等.输入型脑机接口技术临床应用的法律规制研究[J].医学与哲学,2023(4):62-66.

[14] 科技复明新动态:Neuralink 新一代脑机接口产品“盲视”获 FDA 认证[EB/OL].(2024-10-29)[2025-01-12].https://mp.weixin.qq.com/s/0UqfkIaF95nXWPgfcZkdFQ.

[15] 任岩,安涛,领荣.脑机接口技术教育应用:现状、趋势与挑战[J].现代远距离教育,2019(2):71-78.

[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(1):25-32.

[17] 李筱永.脑机接口技术背景下精神完整权的逻辑证成和制度构想[J].政法论丛,2024(3):45-57.

[18] 王高峰,张志领.脑机接口隐私风险治理[J].科技管理研究,2022(5):204-209.

[19] MARTINOVIC I,DAVIES D,FRANK M,etal.On the feasibility of Side-Channel attacks with Brain-Computer interfaces[C]//21st USENIX Security Symposium (USENIX Security 12).2012:143-158.

[20] 申卫星.论个人信息保护与利用的平衡[J].中国法律评论,2021(5):28-36.

[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(9):85-88+93.

[22] 李静雯,王秀梅.脑机接口技术在医疗领域的应用[J].信息通信技术与政策,2021(2):87-91.

[23] 杨代雄.《民法典》第145条评注——限制民事行为能力人实施的法律行为[J].中国应用法学,2022(3):224-238.

[24] 刘士国,熊静文.健康医疗大数据中隐私利益的群体维度[J].法学论坛,2019(3):125-135.

[25] 胡凌.理解技术规制的一般模式:以脑机接口为例[J].东方法学,2021(4):38-48.

[26] 陈怡.健康医疗数据共享与个人信息保护研究[J].情报杂志,2023(5):192-199.

[27] RUIZ-BLONDET M V,JIN Z, LASZLO S."CEREBRE:A novel method for very high accuracy event-related potential biometric identification"[J].IEEE Transactions on Information Forensics and Security,2016,11(7):1618-1629.

[28] 赵丽莉,孙萌.智能可穿戴设备的数据安全审查研究[J].情报杂志,2024(11):181-189.

[29] 中国网络安全审查认证和市场监管大数据中心.中心简介[EB/OL].(2024-10-29)[2025-01-12].https://www.isccc.gov.cn/zxjs/zxjs/index.shtml.

[30] 国家互联网信息办公室.各地省级网信部门受理数据出境安全评估申报、个人信息出境标准合同备案工作的联系方式[EB/OL].(2024-10-29)[2025-01-12].https://www.cac.gov.cn/2023-11/03/c_1700672263791309.htm.

[31] 张素华,尹晓坤.未成年人个人信息同意能力的理论证成及判定[J].财经法学,2023(6):3-17.

[32] 常宇豪.论信息主体的知情同意及其实现[J].财经法学,2022(3):80-95.

[33] 吴梓源.知情同意原则在个体基因信息保护中的适用困境与超越[J].学习与探索,2022(6):91-101.

[34] 高富平.数据流通理论数据资源权利配置的基础[J].中外法学,2019(6):1405-1424.

[35] 王利明.论民事权益位阶:以《民法典》为中心[J].中国法学,2022(1):32-54.

[36] 彭诚信.数据利用的根本矛盾何以消除——基于隐私、信息与数据的法理厘清[J].探索与争鸣,2020(2):79-85+158-159+161.

A Research on the Use and Protection of Brain-Computer Interface Data

CHEN Tinglang

Abstract: Research on the use and protection of Brain-Computer Interface (BCI) data can help provide clear guidance for reasonable utilization of data in the BCI industry. The data collected by BCI devices originates from users′ brain information, which involves sensitive personal information and privacy of users. In the process of using BCI data, it is crucial to clarify usage boundaries, safeguard the personal information rights and privacy rights of data subjects, and prevent data security incidents. To balance the relationship between the development of the BCI industry and data protection, it is necessary to develop a dynamic informed consent mechanism for BCI data collection, reasonably delineate restrictive usage boundaries for BCI data, and ensure the security of BCI data processing activities through external supervision mechanisms.

Keywords: brain-computer interface data; sensitive personal information; privacy rights; data security

责任编辑:周兴涛