

脑机接口技术下神经犯罪的类型及其规制

吴沛泽

摘要: 脑机接口技术的发展催生了神经犯罪这一新型犯罪类型。神经犯罪治理的逻辑起点在于对脑机接口刑事风险的识别。在事实层面,脑机接口的基本分类与运作原理框定了神经犯罪风险的类型、程度与范围,决定了刑法的介入节点;而在价值层面,神经犯罪并未使利益种类发生根本改变,“心理连续”“精神完整”等“神经权利”无法成为刑法的直接保护内容。在刑法的现行框架下,以神经设备、使用者身心安全与神经数据为侵害对象,神经犯罪可以类型化为财产犯罪、计算机犯罪、人身犯罪与数据犯罪四种主要类型。神经犯罪的刑法规制应立足于既有罪名,采取体系性的改良立场。在立法层面,通过对数据干扰行为的确认,对神经数据的分类分级保护以及对健康、自由法益内容的拓展来修正神经犯罪的罪刑规范;在司法层面,应当在复杂的参与主体间,以技术支配为核心标准重塑神经犯罪的归责原则,并在此基础上围绕不法行为的方式、保护对象的重要程度与脑机接口的场景实践构建神经犯罪的罪量评价标准。

关键词: 脑机接口; 神经犯罪; 神经数据; 生命健康; 自由

DOI: 10.19836/j.cnki.37-1100/c.2026.05.017

一、神经犯罪刑事治理的现实困境

脑机接口(brain-computer interfaces)是一种用户与系统进行直接通信的新渠道。与传统键盘、鼠标等输入设备不同,脑机接口可以直接越过肌肉系统与计算机系统进行互动,因此也被认为是未来人机交互的重要方式^①。目前,脑机接口技术已经处在由临床医用向健康个体通用的过渡中。市场上已经存在面向社会公众出售的脑机接口设备,如Neurosky公司公开销售的非侵入式脑机接口设备可以通过佩戴收集包括用户脑电信息在内的各种生理信息,并通过特定的算法规则解码分析,为用户提供情绪监测与健康改进方案。

当下,学界与实务界对脑机接口的法律治理存在广泛争议,其逻辑起点主要集中于是否承认神经权利系一种新兴权利的问题之上,并由此形成了“通过专门立法以保护神经权利”“对现有权利进行适应性解释和应用”与“不需要新的权利、改革或解释”等不同立场^②。与此同时,脑机接口技术也催生了一种异于传统的新型犯罪类型——神经犯罪^③,其本质上属于新技术犯罪。我国学者指出,新技术犯罪是一个犯罪学范畴,指与新兴技术具有高度关联性的犯罪类型^④。而神经犯罪正是在生物科技领域中的特定犯罪现象。神经犯罪的提出并非纯粹的理论建构,也不是缺乏根据的隐忧,而是立足于社会现实基础上的合理展望。正如域外学者指出的:未来的一些黑客可能会毫不犹豫地将神经设备作为攻击目标,利用计算机试图对患者造成身体伤害。例如,在2007年11月和2008年3月,就有人在

基金项目: 云南省哲学社会科学规划年度项目“数据安全风险分类分级的刑法规制研究”(QN202639)。

作者简介: 吴沛泽,云南财经大学法政学院讲师,硕士生导师(昆明 650221; 52650786@qq.com)。

① Abdulkader S. N., Atia A., Mostafa M. M., “Brain Computer Interfacing: Applications and Challenges”, *Egyptian Informatics Journal*, 2015, 16(2), pp. 213-230.

② 韩方序、陈海丹:《做大脑的主人——〈大脑之战:在神经技术时代捍卫自由思考的权利〉评介》,《科学与技术》2024年第3期。

③ 葛向伟:《犯罪学的新兴领域:绿色犯罪学、蓝色犯罪学和神经犯罪学》,《犯罪与改造研究》2025年第9期。

④ 高巍:《新技术犯罪中“故意”判断的客观进路》,《中国社会科学》2026年第1期。

癫痫症公益网站上放置闪烁动画,导致一些患有光敏性癫痫的患者发作^①。

神经犯罪作为新技术犯罪的一种类型,并未得到学界与实务界的足够关注。其一,神经犯罪的内涵并不清晰。有学者指出:神经犯罪(neuro crime)是指为了实现某个犯罪目的,未经授权而访问、干扰、破坏神经设备的正常运作,或者通过神经设备获取、编辑神经信息或神经数据的行为^②。显然,该观点将神经犯罪直接等同于神经数据犯罪,不当缩小了神经犯罪的应有外延。其二,神经犯罪的风险内容缺乏识别标准。在对现有权利体系“重新概念化”的过程中,神经权利能否直接成为刑法的保护内容不无疑问。毕竟,前置法与刑法在立法目的与价值追求层面不可能完全相同。其三,如何在现有的刑法框架中规制神经犯罪缺少明确的操作方案。前置法能够通过创设规范的积极方式来化解神经犯罪风险,但受制于刑法体系的稳固性,刑法立法方法应妥当有序地“顺势而变”^③,直接增设神经犯罪罪名反倒可能衍生出更多的实践难题。

脑机接口技术对人类社会可能造成现实威胁已成不争的事实,其既在观念上打破了“大脑活动是无法触及的”这一固有认知,也在法律治理层面提出了崭新的规制需求。作为一种新技术犯罪,神经犯罪在犯罪结构、危害样态与归责模式等方面体现出了与传统犯罪的显著差异,因此有必要基于技术迭代与刑法治理平衡下的合理时序观,在明确脑机接口的生成原理与风险类型的基础上,有针对性地构建起科学合理的规制路径,以确保脑机接口刑事风险的整体可控。

二、“事实-价值”维度下神经犯罪风险识别路径的检讨

神经犯罪不是特定的刑法罪名,而是对与生物科技(现阶段主要是脑机接口技术)具有高度关联性的犯罪类型与犯罪现象的概括。对于脑机接口技术刑事风险的识别,既要在科技事实层面明确脑机接口的技术原理,也要在价值规范层面明确神经犯罪侵犯的利益种类与内容。

(一)事实维度:基于脑机接口的基本分类与运作机理

目前,学界与实务界主要提出了以下三种脑机接口的分类框架。第一种是以“脑机接口与用户的互动与干预形式”为分类标准所形成的“主动式-被动式-反应式”的脑机接口类型^④。第二种是根据“信号获取模态与安装方法”为分类标准所形成的“侵入式-非侵入式”的脑机接口类型^⑤。第三种是以“功能或促进目标”为分类标准所形成的“情感式-增强式”的脑机接口类型。

不同类型的脑机接口具有不同的功能属性与具体表现形式,其在使用者的联结、对数据的要求以及对医疗技术的依赖层面存在差异。例如,在上述第一种分类中,主动式脑机接口只对用户脑信息进行读取与转译并输出给其他二级设备,居于媒介地位。这种较为典型的中立性质表明,该类脑机接口不仅风险程度普遍较低,而且风险内容也较为单一。被动式脑机接口具有获取用户日常无控制意图的脑电信号,并对其解码分析后以实现日常健康状态、情绪监测、谎言监测等功能。由于该类脑机接口侧重于对数据(信息)的主动获取、处理与分析,所以其保护重心主要在于数据(信息)安全与数据背后的关联性利益。而反应式脑机接口可以通过对用户大脑进行刺激来读取特定脑电信号,从而帮

① Denning T., Matsuoka Y., Kohno T., “Neurosecurity: Security and Privacy for Neural Devices”, *Neurosurgical Focus*, 2009, 27(1), p. E7.

② Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129.

③ 陈伟:《刑法立法方法研究》,上海:上海三联书店,2020年,第15页。

④ Zander T. O., Kothe C., “Towards Passive Brain-computer Interfaces: Applying Brain-computer Interface Technology to Human-machine Systems in General”, *Journal of Neural Engineering*, 2011, 8(2), 025005.

⑤ Maiseli B., Abdala A. T., Massawe L. V., et al., “Brain-computer Interface: Trend, Challenges, and Threats”, *Brain Informatics*, 2023, 10(1), p. 2.

助用户实现控制意图,或者通过对用户神经活动的干预,实现情绪调节、感知增强等功能。反应式脑机接口具有破坏主体感(sense of agency)^①的特征并能够对用户进行潜在的神经引导,从而对自然人的意志主体地位造成威胁。但这种“瓦解”主体性的风险是否具有刑事可罚性仍需要在价值维度进一步验证。又如,侵入式与非侵入式脑机接口的主要区别在于安装方式、信号质量和分辨率方面的差异。因此,二者的规制重心并不在于其风险范围,而是在于人身健康风险程度。正如我国学者所指出的,侵入式脑机接口要将设备植入脑部,因此产生的慢性生物相容性风险与急性风险相比于非侵入式脑机接口产生的神经异常、皮肤接触等风险要更为严重^②。

与此同时,脑机接口设备的基本运作机理可被总体性地概括为“产生—测量—解码—输出”的“四步循环”^③。基于脑机接口技术的运行机理判断不同阶段刑事风险的现实化程度,可以在一定程度上决定刑法的保护侧重与介入时点。具体而言:(1)“产生”阶段是整个脑机接口系统运行的第一个阶段,是指人脑接受外部刺激而产生新想法或任务,其以生物脑电的形式活跃于脑内。显然,该阶段当属脑机接口技术侵害法益流程的起点。在机器与人脑的交互过程中,神经刺激既有可能被视为对人体健康的损伤,也有可能被视为数据犯罪的前置环节或预备阶段。(2)第二阶段的“测量”与第三阶段的“解码”共同构成了神经数据转化成可被理解的神经信息的过程。前者是指脑机接口设备通过对EEG、EMG、fMRI等技术的整合读取生物电信号;后者则是脑机接口设备根据其需要实现的特定功能,制定专项解码规则、信噪比等预设,对脑电信息进行噪声去除并将其解码成为计算机可读语言。单纯获取原始神经数据的违法行为的刑事违法性较低,并不值得刑法评价。例如,域外黑客Cody Brociou破解了由Emotiv生产的面向消费者的脑机接口(称为EPOC)的加密并构建了解密程序。学界与实务界普遍认为:他只是从设备中直接提取原始数据,并没有能力对信号进行过滤或判断传感器所对应的数据流^④。数据的分析与处理是数据风险进一步现实化的必经过程,故“解码”阶段要比“测量”阶段的危险程度更高,处于数据犯罪的重点打击领域。(3)第四阶段被称为“输出”,是指计算机设备(如屏幕、电动轮椅、智能假肢等)按照上一步骤解码的计算机语言作出反应。在这一阶段中,用户脑中的神经计算并未被显著访问或操控,但神经犯罪分子可能攻击与脑信息连接的设备从而限制、修改或干扰其功能。例如,在安装假肢的患者奔跑、开车或上下楼等场景中,犯罪分子可以通过机械性或技术性地破坏假肢系统,致使设备产生错误的运动反馈。

总之,在科技现实主义立场下,立足于脑机接口的分类可以框定刑事风险的基本类型、程度与范围,而明确脑机接口的运作机理则有助于进一步阐释刑事风险的保护侧重与介入时点。

(二)价值维度:基于“神经权利”的刑法规范分析

目前较为主流的研究范式提倡构建神经权利这一新型权利类型来化解脑机接口技术对人类现有权利体系的严重冲击。基于权利束理论,神经权利主要包含认知自由、精神隐私、精神完整与心理连续等内部权利或法益^⑤。对于神经权利的法律保护,在世界范围内形成了以欧洲国家为代表的“现有权利拓展”、以智利等拉丁美洲国家为代表的“神经权利专门化”与以美国为代表的“州级先行”三种路径。刑法不能无视前置法的利益范围,因此厘清神经权利的实质内涵将直接决定神经犯罪侵犯的法

① Serino A., Bockbrader M., Bertoni T., et al., “Sense of Agency for Intracortical Brain-machine Interfaces”, *Nature Human Behaviour*, 2022, 6, pp. 565-578.

② 张红:《脑机接口技术发展中的权利权益保护》,《中国法学》2025年第2期。

③ Gerven M. V., Farquhar J., Schaefer R., et al., “The Brain-computer Interface Cycle”, *Journal of Neural Engineering*, 2009, 6(4), 041001.

④ Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129..

⑤ Ienca M., Andorno R., “Towards New Human Rights in the Age of Neuroscience and Neurotechnology”, *Life Sciences, Society and Policy*, 2017, 13(1), p. 5.

益种类与刑法规制方向。鉴于神经权利的高度抽象性与体系嵌入的障碍性等原因,神经犯罪的刑法规制当下尚不应将“神经权利”作为构建保护体系的理论基底。

首先,神经权利与其他传统权利的实质界限并不清晰,存在对思想、认知等主观内容法律性质的误认。例如,精神隐私权是自然人防止他人非法获取大脑隐私信息的权利,其目的在于保护神经设备所产生的神经数据在整个神经设备系统生态中的私密性。一方面,学理上认为精神隐私在现阶段只能还原为神经数据。既然如此,通过规制既有数据犯罪的方式来保护精神隐私已经足够,无须另设法益。另一方面,精神隐私描绘的是神经数据借助技术呈现出的客观表现形式,与传统隐私并无本质上的差异。有观点将思想作为精神隐私的主要内容,并以此与着眼于行为的传统隐私相区别^①。但是,将自然人的思绪作为精神隐私的内容却不无疑问。这是因为,人类能否控制自己的思想本就是一个悬而未决的问题。更何况,纯粹的思想由于不具备可侵害性,故无法契合刑法的客观主义立场。不难发现,夸大精神隐私与传统隐私对立的观点属于用脑机接口技术特征直接取代权利构建的规范分析,混淆了法律概念事实性与价值性的基本区分。

其次,神经权利无法嵌入刑法的既有框架之中,强行为之有损刑法体系框架的稳定。例如,精神权利中的认知自由权是思想自由的延伸,是指个人控制自己的心理过程、认知和意识的自由^②。在神经权利语境下,脑机接口技术对认知自由的侵犯可能表现为“大脑窃听”“记忆劫持”等不同形式。然而,认知自由风险至多只能被评价为一种伦理风险或在特定情形下的前置性法律风险,而非刑事风险。原因在于:其一,若认为“控制大脑”有构成侵犯自由犯罪之可能,则不仅会对构成要件行为的稳定性形成强烈冲击,更难以说明刑法因果关系的成立依据。其二,若自然人的主观意志在脑部刺激、经颅磁刺激等技术的影响下可以轻易发生改变,这不仅会使实务机关无法提出对认知自由损害的证明标准,还会致使刑事责任体系与追诉程序的全面崩溃。其三,在脑机接口技术尚未完全进入通用阶段的背景下,增设侵犯认知自由的犯罪无助于增进国民对该类犯罪的理解程度,还会遏制技术的创新,不符合不法类型的普遍性与罪名增设的科学性。

最后,神经权利导致刑法防卫阵线的过度前移,不符合刑法的谦抑性特征。人工智能时代的风险似乎无处不在,可能会使刑法的处罚对象从危险变为不安全感,从而形成“泛风险化”的错误观念^③。例如,心理连续权作为神经权利的一个子权利,指向了个人身份感与自我认同。心理连续权的提出旨在防止神经科技对神经功能的改变,反映出了体验的本真性与外部技术塑造之间的矛盾。但是,在神经技术进行有益干预或正向促进时,其对他人心理或人格的改变并非一定属于刑法意义上的损害。正如我国学者所指出的,“基于个人定制算法的加持,脑机接口反倒会开辟一条通往真实的自我感知道路,使用户不断增强自主性并找到他们真正的偏好或内心深处细腻真实的情感状态”^④。与此同时,为了限缩处罚范围,有观点将“造成身体或心理上的伤害”作为心理连续性受损的成立要件之一^⑤。但是,心理伤害的刑法意义并不清晰,对于脑机接口致身心损害的法律评价也只能回归至传统的法律框架中才能得到妥善解决。

(三)简要总结:神经犯罪刑法规制的基本立场

当下,域外对神经权利的理论构建方案对于我国立法与司法的借鉴意义较为有限。在前置法层面,神经权利存在实定法障碍,与我国现行《中华人民共和国民法典》(尤其是人格权编)的内容体系不相兼容。在刑法层面,神经权利内部涵盖了人身风险、数据风险等不同类型,具有一定的权利拼接与

① 童云峰:《脑机接口技术应用背景下神经权利的证立与穿透式保护》,《暨南学报(哲学社会科学版)》2024年第8期。

② 徐娟:《脑机接口技术应用中神经权利的规范构造及其法律保障》,《江汉论坛》2025年第7期。

③ 吴沛泽:《人工智能刑事风险的识别与规制》,《政法学刊》2025年第4期。

④ 王高峰、张志领:《算法伦理视域下的脑机接口伦理问题研究》,《自然辩证法研究》2022年第7期。

⑤ 童云峰:《脑机接口技术应用背景下神经权利的证立与穿透式保护》,《暨南学报(哲学社会科学版)》2024年第8期。

杂糅的色彩。风险间的差异以及风险维度的错位导致了神经权利不仅不具备指导刑事立法之可能,也难以成为刑法文本的直接解释对象。正是因为事实维度下的神经犯罪风险未脱逸出刑法现有的规制框架,因此在现阶段不宜将神经权利作为刑法中的规范概念,更不宜在价值层面将神经权利直接作为刑法的保护法益类型。从神经犯罪刑法规制的基本立场上讲,需谨防先入为主地认为其侵害的利益种类发生了重大变化,而应立足于既有的法益内容,采取解释结论优化与罪名体系修正等缓和路径来应对脑机接口技术对刑事治理的现实挑战。

三、现行刑法体系下神经犯罪的类型分析

有学者指出,神经犯罪作为一种新兴犯罪现象,可以被界定为“通过访问或操纵神经信息、使用神经设备,对个人或群体实施故意的直接或间接身心伤害,以及对受害者的名誉和财产造成损害的犯罪行为”^①。由于脑机接口具有技术关联性、人机交互性与高价值性等基本特征,故根据侵犯对象与法益种类的不同,神经犯罪主要对应了财产犯罪、计算机犯罪、数据犯罪与人身犯罪四种类型。

(一)以神经设备为侵害对象可以构成财产犯罪或计算机犯罪

无论是医用神经设备还是消费级神经设备都兼具财产属性与技术属性,因此,在行为人将神经设备作为侵犯对象的场合中,应视情况认定其构成财产犯罪或计算机犯罪。其一,从财物保护视角看,若行为人故意毁坏脑部刺激装置或脑机接口等神经设备,则其自然构成故意毁坏财物罪。但值得讨论的是,针对病患人群的智能假肢等设备进行攻击的法律认定问题。例如,有学者指出,恶意摧毁运动缺陷者的神经控制机器人手臂可能会显著影响受害者的心理生活,使其行动受到限制和约束并产生恐慌和心理痛苦等情绪反应,从而留下创伤性记忆^②。该观点表明,破坏智能假肢等计算机反应设备具有构成伤害犯罪的可能。这背后的实质考量在于人类躯体不仅限于肉体,还包含机械部分的延展。然而,伤害犯罪保护的是“生理机能的健全”而非“身体的完整性”^③,再加之神经控制设备的损害与患者心理生活的创伤之间缺乏刑法因果关系的成立根据,故在毁损神经控制设备的场合中,行为人仅有构成财产类犯罪与自由类犯罪竞合的可能。

其二,由于神经设备是指能与人体神经系统发生交互并实现采集记录、调控刺激、解码代偿的各类软硬件装置,因此恶意侵犯神经设备的行为完全符合刑法中的计算机犯罪,即刑法第285条第二款的非法控制计算机信息系统罪或刑法第286条第一款的破坏计算机信息系统罪。前者的适例为劫持脑机接口,即监控并改变通信通道,从而削弱甚至取代用户对脑机接口的控制。后者的适例为干扰攻击脑机接口,即以混淆、破坏或延迟脑机接口功能的方式对其发动干扰攻击。

其三,神经犯罪视域下财产犯罪与计算机犯罪的区分标准主要在于行为人针对神经设备的攻击方式。计算机犯罪的保护法益为计算机信息系统的正常运行,即系统本身的功能可以正常发挥,而非系统在实际使用中的预期目的能够实现。因此,只有行为人针对神经设备采取了技术性的攻击方式(如破坏以代码或指令为技术架构的数据处理规则)才可能构成计算机犯罪,而采取物理性的攻击方式只能构成财产犯罪。例如,对脑机接口的干扰攻击可以通过向脑机接口添加噪声的方式予以实现,即在测量层面加入噪声使脑机接口的测量变得不准确,解码过程变得困难。不难发现,上述行为与将计算机设备扔进水中等行为没有本质上的区别,即都是通过物理的方式使计算机设备的外在运行环

① Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129.

② Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129.

③ 张明楷:《刑法学(三)》(第七版),北京:法律出版社,2026年,第1316页。

境发生了改变。因此,对于添加噪声进而干扰脑机接口的案例,不宜将其认定为计算机犯罪。

(二)以使用者身心安全为侵犯对象可以构成人身犯罪

基于脑机接口的使用方法与技术原理,在未来最有可能发生的两种人身犯罪分别是伤害类犯罪与侵犯自由类犯罪。然而,脑机接口技术对使用者造成的不同伤害结果并非都具有刑法评价的意义,因此应准确区分不同结果的形式与内涵,并建立起致损事实与规范评价之间的实质关联。

第一种损害类型属于传统意义上的伤害结果,能够以现行伤害犯罪标准进行准确认定。这种脑机接口引起的损害结果并未脱逸出既有的人体损伤鉴定标准,如侵入式脑机接口所引起的皮肤感染、灼伤、颅内出血、脑膜炎或异物留存等。此类致损结果既可以通过医疗责任制度和产品责任制度提供救济,也在刑法层面存在明确的伤情对应等级。第二种损害类型虽然能够评价为物质性损害结果,但与现行的人体损伤鉴定标准存在脱节,无法直接进行刑法评价。例如,电刺激可能会导致使用者出现神经异常,进而引发意识障碍、头晕、头痛、昏厥等症状。根据《人体损伤程度鉴定标准》,上述神经症状只有基于头部外伤才能进行损伤程度的认定。进言之,“神经系统症状和体征是强调脑实质损伤(包括挫裂伤、梗死)为主引起颅内压增高和脑膜刺激症的一组变化”^①。显然,脑机接口技术产生的电刺激在现行标准下很难被评价为一种实质损伤,故无法实现与伤害犯罪标准的直接对接。第三种损害类型主要体现为精神性损害,已经超出了伤害犯罪的规制范围。例如,攻击锁定综合征(LIS)患者身上的脑机接口将导致其无法执行脑海中正在发出的动作指令,从而产生严重的心理创伤。在刑法视域中,若脑机接口仅对使用者造成心理健康的损害,则无法适用伤害犯罪,只能判断该情形是否符合其他罪名的犯罪构成。比如,通过脑机接口技术对家庭成员进行精神摧残、折磨的,可以认定为虐待罪。第四种损害类型主要体现为身体意象问题或自我认知障碍^②。例如,一名接受了7年脑刺激治疗的抑郁患者就曾对自我的存在产生了深刻的怀疑。该患者说道:“我感到模糊了,以至于我不确定我是谁。”^③类似情形无疑在一定程度上损害了使用者的生命尊严,但基于法益损害确定性与可证明性的要求,上述情形只能依托前置法进行伦理平衡与风险缓解,而无法依靠刑法得到直接规制。

与此同时,脑机接口技术对自由的侵犯也体现出了与传统自由犯罪的显著不同。一方面,脑机接口技术可能以更为新型、隐蔽的强迫形式来侵犯他人的自主性,如通过刺激或改变他人的神经元结构迫使他人以非自愿的方式行动^④。另一方面,传统的自由犯罪主要表现为拘束他人身体或强制被害人实施特定行为,其风险与危害后果在整体上可控。然而,脑机接口技术对人脑的操控可能会导致他人违背自己的意愿而采取一切行动,如强迫他人实施违法犯罪行为甚至是自杀。由此可见,脑机接口技术使得自由法益呈现出一种从外部行动自由向内在意志自由扩张的态势,也在犯罪危害性方面体现出对传统侵犯自由犯罪的超越,有必要优化既有的刑法规制路径。

(三)以神经数据为侵犯对象可以构成数据犯罪或财产犯罪

神经数据是神经设备所处理的人类生理信号,反映自然人大脑的意识活动。域外国家通常不区分神经数据与神经信息,如欧盟数据保护监督局将神经数据定义为,“从大脑和/或神经系统收集到的信息,以及基于这些数据的推断(如情感线索或偏好)”^⑤。但是,在我国刑法明确区分了数据与信息

① 陈林主编:《人体损伤程度鉴定实战指引》,北京:法律出版社,2019年,第76页。

② Satam I. A., Szabolcsi R., “Ethical and Safety Challenges of Implantable Brain-computer Interface”, *Interdisciplinary Description of Complex Systems: INDECS*, 2025, 23(2), pp. 82-94.

③ Klein E., Goering S., Gagne J., et al., “Brain-computer Interface Based Control of Closed-loop Brain Stimulation: Attitudes and Ethical Considerations”, *Brain-Computer Interfaces*, 2016, 3(3), pp. 140-148.

④ Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129.

⑤ European Data Protection Supervisor, *TechDispatch on Neurodata (TechDispatch 2024-1)*, Luxembourg: Publications Office of the European Union, 2024, p.4.

的立场下^①,神经数据犯罪只是神经信息犯罪的前置阶段,二者分别对应不同的罪刑规范。可是,信息总归是对自然人某一类特定属性的记录,而数据却具有承载不同利益的“权利束”特征。人类的思维活动具有复杂性,无法在思维内容上进行单一的类型评价。因此,在大脑生理信号的刑法保护问题上,适用数据类犯罪而非信息类犯罪更能契合人类思维的复杂性特征。

脑机接口技术下的人机交互主要依靠数字计算系统对大脑神经活动的记录、分析、存储以及修改等操作实现。神经数据的处理流程较为复杂,牵涉的风险类型也不尽相同。然而,刑法并无必要为所有数据风险针对性地设置构成要件。例如,安全存储神经数据对防止数据泄露与未授权访问至关重要,但既然刑法中的现有罪名最早只规制到数据的非法获取环节,因此基于刑法的谦抑特质,就不应再次前移刑事防卫阵线去规制数据的非法存储行为。实践中的神经数据不法行为主要表现为三种类型:其一是数据窃取,即行为人侵入神经设备或保存神经数据的服务器以获取用户的脑隐私;其二是数据干扰,即行为人破坏脑机接口各部分之间的正常通信,从而导致数据传输错误或者其他二级设备无法正常运行;其三是数据篡改,既包括行为人针对脑机接口系统测量收集的数据进行篡改,从而导致二级设备按照其意思运行^②,也包括行为人更改脑机接口或其他神经设备的介入治疗方案、刺激模式等^③,从而影响用户神经活动、情绪甚至自主意识。

此外,同神经设备一样,神经数据也具有一定的财产属性。尽管“脑机接口提取的神经信号并不必然构成后续可以财产化利用的数据”^④,但只要能够对神经数据的财产属性进行法律认定,在理论上就具有适用财产犯罪规范的可能。只不过相对于其他数据,神经数据财产的刑法保护更为复杂。一方面,由于神经数据兼具高度人身属性,因此如何为神经数据的财产性权益设计出明确的产权方案仍需进一步的理论与实践探索。另一方面,构建科学合理的财产鉴定体系是虚拟财产刑法保护的重要基础。但与虚拟货币、游戏装备、NFT数字资产等不同,神经数据目前并不存在成熟的市场交易规则。同时,脑机接口技术的科研投入普遍巨大,神经数据刑法价值的认定虽然要以填平损失原则为导向,但也应避免因受害者对神经数据成本价格的举证而间接性地导致刑事处罚过于苛重。

四、神经犯罪刑事归责的标准与路径构建

在明确了神经犯罪的基本类型之后,需围绕上述类型进行体系与内容上的适时革新。在立法上,应对人身犯罪、数据犯罪等现有罪刑规范进行修正以化解传统刑法框架的规制局限;在司法上,应在整体上确立神经犯罪的归责理念与标准以明确刑法的处罚范围,并在此基础上构建多元化的罪量评价标准以适应神经犯罪的新型犯罪结构与危害样态。

(一)立法路径:脑机接口技术下神经犯罪的规范修正

在神经犯罪的四种主要犯罪类型中,我国刑法对计算机犯罪、数据犯罪与人身犯罪具有较为明显的规制局限,应予以适时修正。其一,我国刑法中的破坏计算机信息系统罪既包括了对计算机信息系统的破坏,也包括了对数据的破坏。实际上,行为人通过干扰数据来攻击脑机接口属于神经数据犯罪的常见情形,如通过添加噪声来削弱用户对脑机接口的控制。然而,我国刑法第286条第二款仅将删除、修改与增加作为破坏数据的行为方式,导致其无法周延地规制神经数据犯罪的全部情形。在脑

① 吴沛泽:《数据犯罪规制路径的体系调适:基于双层法益观的确立》,《学术交流》2025年第5期。

② Timo S., “Neurorights: The Debate about New Legal Safeguards to Protect the Mind”, *Issues in Law & Medicine*, 2022, 37(1), p. 95.

③ Denning T., Matsuoka Y., Kohno T., “Neurosecurity: Security and Privacy for Neural Devices”, *Neurosurgical Focus*, 2009, 27(1), p. E7.

④ 张红、叶竞欧:《神经信息的法律保护:个人信息、隐私与数据》,《武汉大学学报(哲学社会科学版)》2025年第3期。

机接口技术下,用户大脑与计算机设备的交互依赖于对神经数据的测量、记录与解码等重要环节,而数据的测量精度、处理速度与可获得性是确保上述环节顺利实现的关键要素^①。如果说删除、修改与增加方式破坏的是数据可获得性的话,那么干扰行为则破坏了数据的测量精度与处理速度。限制脑机接口运行不等同于破坏脑机接口功能,这导致了干扰数据的行为在现阶段无法直接纳入刑法第286条第一款。因此,只有在刑法第286条第二款中增加干扰数据的行为类型才能有效填补刑法的处罚漏洞^②。

其二,在刑法的规制框架内,侵犯脑电信号的不法行为应适用数据犯罪而非侵犯公民个人信息犯罪。之所以如此,不仅是因为数据与信息存在转化顺序上的前后之分,还在于上述行为无法契合侵犯公民个人信息罪的罪量要求。根据刑事司法解释的规定,公民个人信息的计量单位为“条”^③,而数据的计量单位为“组”^④。在数据犯罪的语境中,“组”通常是指用于确认自然人身份信息的数据集合。无论是脑机接口通过EEG、MEG、fMRI等复合技术对特定脑区收集的生物电信号,还是将生物信号解码成可供计算机系统识别的信号,都难以以“条”的形式呈现。我国司法解释对于数据的保护采取了“金融服务身份认证信息”与“其他身份认证信息”二分的简单思路,无法满足数据分类分级保护理念的需求。这是因为,借助脑机接口技术获取人类的大脑活动(包括但不限于记忆、认知、情感等),并将内在神经活动外显化与数据化的过程难免会从内而外地导致私人领域的瓦解。甚至可以说,只要基于特定的技术操作,黑客便可以通过获取脑电信号从而推断出自然人的全部信息。因此,在数据犯罪未来的发展过程中,刑法即使不正面确立神经数据的法定种类,也应通过修正司法解释等操作区隔出神经数据的独立类型,并基于其重要程度进行分类分级的刑法保护。

其三,相比于传统脑损伤,脑机接口技术可以改变人脑的神经元结构,使其产生狂躁、性欲亢奋、冲动控制障碍等病患性格或人格特征的改变^⑤。对于类似的脑机接口损害情形,刑法理应通过伤害类犯罪加以规制。只不过脑机接口技术对神经系统的影响与破坏可能具有隐秘性、持续性与长期性,这对人身损伤的鉴定时机、伤病关系处理原则等提出了严峻挑战。为了回应神经犯罪的规制需求,对于脑损伤的鉴定可考虑突破伤害方式的外部性与物理性限制,将脑电刺激等技术手段也纳入其中。除此之外,在行为人利用脑机接口技术限制他人自主行动能力的场合下(如操控神经设备削弱他人行动能力或通过神经调节、算法认知诱导影响他人自决能力),既有的罪刑规范就不能完美解决类似情形。对此,可以借鉴德、日等国的立法经验,考虑在我国刑法中增设强制罪,以便实现对意思自由与身体自由的共同保护。对于强制罪的罪状与适用可做如下设计:首先,强制罪的法益保护内容是意思决定的自由与意思活动的自由,故只要损害他人自主性的行为都可以被评价为属于强制方式。因此,在行为层面,可以在暴力、胁迫后增加“其他方法”这一开放类型以规制通过脑机接口技术损害他人意志自由的情形。其次,强制罪的结果为“使他人实施并无义务实施的事项”^⑥。但脑机接口技术既能够实现对他人的直接操控,也可能只是单纯干预他人的神经系统(如影响神经元结构)。因此,在行为人导致他人难以正常行使自决权的情形下,只要在鉴定层面存在可测量的神经化学变化,就可以认为行为人满足了强制罪的结果要求。最后,对于行为人未经许可便干扰或终止神经设备的功能来限制或剥夺用户行动能力的行为,可以通过强制罪予以规制,以弥补现有罪刑规范的归责局限。

① Ienca M., Haselager P., “Hacking the Brain: Brain-computer Interfacing Technology and the Ethics of Neurosecurity”, *Ethics and Information Technology*, 2016, 18, pp. 117-129.

② 吴沛泽:《数据犯罪的刑法规制:法益内涵与体系构建》,《中国刑事法杂志》2024年第5期。

③ 参见《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条的规定。

④ 参见《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第1条的规定。

⑤ 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》,《政法论丛》2024年第3期。

⑥ 西田典之:《日本刑法各论》(第七版),王昭武、刘明祥译,北京:法律出版社,2020年,第80—81页。

(二)司法路径:脑机接口技术下神经犯罪的不法认定

1. 神经犯罪的归责原理重塑

从理念上讲,神经犯罪刑事责任的认定就是风险的分配与承担方式在刑法框架中的具体运用。当前端设计者、研发者等主体因未尽到必要注意义务以及后端使用者的不当操作而产生危害结果时,如何在各参与人之间进行责任归属具有重要的讨论价值。因此,有必要对神经犯罪的归责原理进行符合脑机接口技术特点的重新考量,以合理界定各参与人的刑事责任,避免刑法的过度介入。

其一,为了实现神经犯罪风险规制、技术发展与通用普及的整体平衡,应将行为人具有“重大过失”作为确认前端或后端主体刑事责任的必要条件。但是,在新技术诞生初期,对“重大过失”的认定不能过于强调在经验层面上诸如预见可能性等主观要素,而应重视危险创设等客观要素的决定性意义。例如,若脑机接口研发者、设计者的相关行为明显低于一般技术标准的安全阈值,管理者没有履行脑电数据合法收集、储存以及算法备案、审查等法律强制性义务或是后端使用者因严重违反医嘱等专业建议而造成损害时,可以追究上述行为人的刑事责任。

其二,若前端主体与后端主体共同参与导致损害结果发生,应将风险类型的关联作为不同主体间的责任分配依据。一方面,在前端主体与后端主体创设的风险类型高度一致时,宜追究前端主体的刑事责任。新型智能犯罪的因果流程越是复杂,就越应将归责重心放置在危险的开启而非危险的实现之上。即使后端行为对结果的出现具有强化作用,但前端主体优越的技术支配地位可以对应更大的答责范围,再加之人类对新技术的合规使用本就是一个渐进过程,因此在现阶段不宜让后者对损害结果答责。另一方面,在前端主体与后端主体创设的风险类型不一致时,可以分别追究不同主体的刑事责任。例如,虽然脑机接口设计者因算法设计缺陷导致无法正常分析神经信号,但最终的损害结果表现为基于使用者的不当操作而使他人健康受损。由于双方的职责范围与注意义务分属不同类型,此时就应针对性地进行主体间构成要件的判断与罪名的确定。

其三,可以以脑机接口运用环节对结果发生的支配力为依据,在前端主体内部进行二次答责。尽管脑机接口属于一个复杂系统,但并无必要在刑法上将所有责任主体作为“共同犯罪”予以认定。例如,脑机接口的生产需要遵循“工艺设计—微纳制造—生物封装—系统标定—质量出厂”的严密流程。不同的生产主体对脑机接口的安全注意义务及程度并不相同。前端生产主体(工艺整合工程师、精密制造工程师等)决定了脑机接口的性能上限,如数据信号是否清晰等,而后端生产主体(生物封装与测试工程师、质量控制专员等)则决定了脑机接口的安全性,如脑机接口能否安全植入。因此,在脑机接口质量缺陷致损的场合下,应立足于法益侵害的具体类型与流程,“穿透式”地判断责任主体在脑机接口运行环节中的支配程度。比如,同样是脑机接口造成物理性人身损害,若是由于数据传输或信号分析等缺陷而导致他人无法正常操作神经设备,应追究前端生产主体的刑事责任。相反地,若是由于材料本身问题而引发如急性炎症、脑膜刺激等生物损伤,则应追究后端生产主体的刑事责任。

2. 神经犯罪的罪量标准设置

神经犯罪的罪量标准设置应符合脑机接口的技术特点,除结果、数额等传统的可罚要素外,还应考虑到行为方式、保护对象与应用场景等要素对神经犯罪不法内容的影响。其一是行为人的不法行为方式。在传统犯罪中,实务机关对某一行为危害性的判断普遍依托于对结果的考察。换言之,对符合构成要件行为的界定遵循了一种包含结果在内的行为思考方法^①。然而,人工智能犯罪的因果关系并非体现为传统的线性链条,其损害结果在经验上也难以被直观把握。例如,行为人可以通过不同方式攻击受害人的神经网络进而损害其健康:或是神经元扫描(neuronal scanning)攻击,即按顺序刺激神经元,每次只刺激一个单位;或是神经元泛洪(neuronal flooding)攻击,即在特定时间点同时刺

^① 薛铁成:《实行行为与危害行为关系再厘定》,《社会科学研究》2024年第2期。

激多个神经元,改变刺激过程的正常行为并造成过度刺激的影响^①。不难发现,在神经安全领域,两种不法方式的攻击向量与风险类型存在显著差别。前者的主要目标在于窃取大脑信息或窥探隐私,只是会伴随产生受害者的间接性人身风险;而后者可以剧烈刺激大脑神经,使大脑活动趋于瘫痪、崩溃,是一种直接意义上的人身风险。同时,神经攻击行为致损伤后的恢复与进一步影响也决定了攻击行为的不法程度,故相比之下,后者的刑事责任要显著高于前者。因此,在特定场景下,实务机关应基于技术原理与科学法则独立地判断神经犯罪不法行为对刑事归责的具体影响,而不能单纯地面向损害结果进行回溯性的认定。

其二是保护对象的重要程度。学界与实务界倾向于将神经数据作为敏感个人数据(信息)加以保护^②。然而,基于人类大脑思维活动的复杂性,敏感个人数据(信息)的保护模式存在明显不足。这是因为,个人数据(信息)具有描述性特质,记录的是自然人的外部属性,而神经数据捕捉的是身份、意图和体验不断产生的过程。进言之,对神经数据的干预不仅是信息入侵,更是对自我形成的直接性干预^③。国家科技伦理委员会《脑机接口研究伦理指引》第4.4条指出,脑机接口研究过程中采集的神经数据或实验样本反映了被试者的思维精神状态、生理健康信息、性格特征以及财产信息等隐私数据。由此可见,神经数据具有相较于其他类型数据更为开放的特征,需要基于分类分级理念进行差异化的保护。源自大脑的神经数据可能具有“人身”或“人身+财产”等不同的规范结构,所以刑法对神经数据的保护强度必须围绕神经数据与现实利益的实质关联进行综合判定。例如,若神经数据反映出了公民的决策倾向或财产信息等状况,则其与公民的人身安全与财产安全存在较高程度的直接性关联,故可以通过降低入罪标准的方式进行预防性保护。

其三是脑机接口的场景化实践。脑机接口的应用场景包括医疗、教育、娱乐、运动、军事、司法等多个领域。欧盟在2024年通过的人工智能法就将人工智能系统分为禁止性风险、高风险、有限风险和最小风险四类。其中,禁止性风险包含了以刑事执法为目的的风险评估或情绪推断等内容。因此,脑机接口在精神介入治疗与刑事司法(测谎、证据查明)等领域的应用须受到更为严格的制度监管与约束。而用于娱乐或个人目的的系统属于最低风险(不构成风险或风险可忽略)的人工智能系统。欧盟国家对于此类系统通常不设置强制性的规定,而是“在成员国之间收集和分享技术与规制技巧以及最佳实践”^④。因此,基于比较研究的视角,我国对于类似脑机接口的治理也宜置于行业自治或前置法领域调整,而不必诉诸刑事治理。

五、结语

工业社会越是复杂,技术、经济与其他变化对人类的生活环境以及人类自身的改变就越多,法律制度及其理论也就越复杂^⑤。当下,神经犯罪也正以一种超越传统的姿态挑战着既有的刑法框架,倒逼刑事法理与规范进行修正与革新。相比于正如火如荼进行的新兴权利构建运动,刑法对于脑机接口技术的治理还是应当保持必要的克制姿态。一方面,大量的神经犯罪情形在现行的刑法框架下仍可得到妥善解决;另一方面,即使认为现行刑法对神经犯罪存在处罚上的缺漏,也不需要径行创设神经犯罪罪名,而是应回归至更为上层的法益论中,通过对“利益种类是否发生变化”的拷问来实现对

① Bernal S. L., Celdran A. H., Maimo L. F., et al., “Cyberattacks on Miniature Brain Implants to Disrupt Spontaneous Neural Signaling”, *IEEE Access*, 2020, 8, pp. 152204-152222.

② 宁馨:《脑机接口神经数据的场景化归类及法律保护路径——兼评智利“神经数据第一案”》,《天府新论》2025年第6期。

③ Chenier S., Harris M., Kumar R., “Neurotechnology, Cognitive Liberty, and the Law: Building a New Legal Architecture for Mental Autonomy in the Digital Age”, *Legal Studies in Digital Age*, 2023, 2(4), pp. 48-60.

④ 参见欧盟《人工智能法》(AI Act)第66条的规定。

⑤ 伯恩·魏德士:《法理学》,丁晓春、吴越译,北京:法律出版社,2013年,第21页。

既有犯罪体系的优化。传统罪名正在数字技术与生物技术的发展中经历一场严峻的时代考验,神经技术势不可当,而神经犯罪刑法规制的未来发展方向也有待于对科技的持续观察才能得到确定答案。

Types of Neurocrimes under Brain-computer Interface Technology and Their Regulation

Wu Peize

(School of Law and Politics, Yunnan University of Finance and Economics, Kunming 650221,
P. R. China)

Abstract: The development of brain-computer interface technology has spawned neurocrime as a new type of criminal offense. In essence, neurocrime is a conceptual generalization of the criminal types and phenomena closely associated with brain-computer interface technology. Effective regulation of neurocrime is premised on the accurate identification of the criminal risks arising from the application of brain-computer interface technology. At the factual level, the basic classification and operating principles of brain-computer interfaces delineate the type, degree, and scope of neurocrime risks and determine the point at which criminal law should intervene. At the level of values, neurocrime does not fundamentally alter the categories of legal interests protected by criminal law, and neuro-rights—such as the right to mental continuity and mental integrity—cannot be directly protected by China's criminal law. Accordingly, drawing on the inherent connotation of legal interests, China's criminal law should address the practical challenges of criminal governance brought by brain-computer interface technology through optimizing interpretive conclusions and revising the system of criminal charges.

Within the current framework of criminal law, neurocrimes targeting neuro-devices, the physical and mental safety of users, and neural data can be categorized into four major types: property crimes, computer crimes, crimes against the person, and data crimes. The criminal regulation of neurocrime should adopt a systematic approach to reform grounded in existing criminal provisions. At the legislative level, criminal law should introduce the behavioral category of data interference, establish a classified and hierarchical protection system for neural data, and revise the norms governing offenses and penalties for neurocrimes by expanding the connotation of the legal interests pertaining to health and personal freedom. At the judicial level, it is necessary to reconstruct an imputation principle centered on technological dominance among the various participants, and to develop diversified standards for the quantitative evaluation of neurocrimes based on the modes of unlawful conduct, the importance of the objects of protection, and the practical application scenarios of brain-computer interface technology.

Keywords: Brain-computer interface; Neurocrime; Neurodata; Life and health; Freedom

[责任编辑:苏 捷]