

神经信息的法律保护:个人信息、隐私与数据

张 红 叶竞欧

摘 要 脑机接口技术能直接探知和反映人类的意识活动,这一划时代的技术变革对自然人的人格权益构成严重威胁。神经信息是由脑机接口设备采集的意识活动信息,现行规范可由神经信息切入,从多个层次应对脑机接口的技术冲击。从整体上看,所有神经信息都构成《中华人民共和国个人信息保护法》第4条第1款所规定的个人信息,其原则上均受《个人信息保护法》调整。具有私密性的神经信息构成《中华人民共和国民法典》第1032条第2款所规定的隐私,自然人可依隐私权人的身份,行使相应的人格权请求权、侵权责任请求权和违约责任请求权。大规模聚合的匿名化神经信息构成神经数据,神经数据持有者可依一般性的数据规范,享有相应的神经数据持有权、加工使用权和产品经营权,并承担神经数据安全的保障义务。

关键词 神经信息;脑机接口;神经信息隐私;神经数据;人格权;生命数字化

中图分类号 D923 **文献标识码** A **文章编号** 1672-7320(2025)03-0039-12

基金项目 国家社会科学基金重大项目(24ZDA009)

脑机接口技术以神经信息为钥,叩开了人类意识活动的大门。作为自然人思维活动的数字化映射,神经信息引发了多层次的法律保护困境。新兴神经技术的冲击,催生了席卷全球的立法热潮,针对神经信息作出专门规定的立法呼号不绝于耳。我国既有规范具备充分的制度张力,经过妥当解释的现行法律足以为神经信息提供全生命周期的保护,不宜过度立法。《中华人民共和国个人信息保护法》(下文简称《个保法》)为神经信息中的人格利益和财产利益提供兜底性保护。《中华人民共和国民法典》(下文简称《民法典》)人格权编重点为神经信息隐私中的人格利益提供周全保障。神经数据持有者可以根据现行的和日后不断完善的一般数据规范,保护其对神经数据享有的财产性权益。

一、问题的提出

神经信息是破解人类心智禁区的密码。1924年,德国精神病学家汉斯·伯格首次记录到大脑的自发电活动^[1](P1437),人类自此得以管窥意识活动的底层生物逻辑,不再单纯倚仗对思维的形而上学分析。在脑电图问世的百年之际,当代学人郑重接过探索人类精神世界的重任,实现了一系列颠覆性的技术突破:Meta 与巴黎的两所高校以脑磁图(MEG)提取神经图像信号,再利用预训练的图像扩散模型进行加工,完成了对受试者脑海中所见画面的初步复现^[2](P8);加州大学戴维斯分校将微电极阵列植入一位渐冻症患者的脑部,实现了对受试者内心语言的解码,让这位有严重语言障碍的患者重新“开口说话”,识别准确率达97%^[3]……在神经技术矩阵的加持下,意识活动首次在人类历史上得以通过直观、生动的方式呈现在脑海之外。

脑机接口技术的运作,以对神经信息的编译为中心,该技术不仅具有空前的医用价值,还具备广阔的商业前景。自2010-2020年,全球政府部门对神经科技的投资已超过60亿美元,民间资本对神经科技

企业的投资更是增长了 22 倍;2021 年,神经技术设备的市场规模已达到 113 亿美元^[4](P26)。

随着神经科技商业版图的急速扩张,神经信息所面临的风险也愈发严峻。消费型脑机接口设备种类繁多,功能各异,其所处理的神经信息既包括大脑传达给各个器官的动作信号,也包括各个器官传达给大脑的感觉信号,还包括大脑本身思维活动的意识信号和情绪信号。神经设备须以这些信号为基础,才能发挥相应的功效^[5]。上述神经信息及其相互之间的组合,直接指向用户的精神与人格,与用户的隐私、人格尊严与人身自由息息相关,理应受到妥善保护。然而,相关企业在实践中并未对神经信息的保护问题给予足够重视。根据“神经权利基金会”(Neurorights Foundation)在全球范围内的调查,有半数以上的神经科技企业在用户协议中没有提到类似于神经数据的概念,有半数以上企业没有在协议中明确提及用户删除神经数据的权利,但有三分之二的企业在协议中载明,企业有权与第三方共享数据。该调查报告认为,神经科技业现有的商业实践与个人信息保护的一般规范差距甚远^[6](P2-4)。

为了应对神经技术革命引发的规范危机,多国政府尝试对神经信息的保护开展专门立法。作为神经权利立法的先锋,智利在 2021 年修改宪法,在基本权利层面明确人民的“大脑活动以及由此产生的信息”应受到特别保护。巴西则专门针对神经数据的保护问题,向立法机关提交了修改通用个人数据保护法的草案。相比之下,美国的地方立法已然靴子落地——2024 年 4 月,科罗拉多州修改了州隐私法,将神经数据纳入敏感数据的保护范围中。

面对域外掀起的立法热潮,我国是否同样需要针对神经信息开展专门立法?对于这一问题,学界应当首先考察,现行规范能否有效调整由神经信息引发的法律问题,能否对神经信息进行有效保护,之后才能得出是否立法和如何立法的结论。具体来说,立法论者需要首先回答三个层面的问题:脑机接口设备采集的神经信号是否构成个人信息,受个人信息保护法调整?脑机接口设备采集的神经信号是否构成隐私,受人格权法调整?脑机接口设备采集的神经信号是否构成数据,受数据法调整?对于上述问题,下文将基于个人信息、隐私和数据的差序格局^[7],对神经信息的保护进行解释论分析,围绕神经信息保护进行规范体系的重构。

二、作为个人信息的神经信息的法律保护

保护新兴神经技术所必须处理的人类信息,已经成为全球性共识。以“神经信息”来指称此类信息,能充分反映它的本质属性,兼顾表达的精准性和全面性。自然人的神经信息要获得现行规范的保护,首先要在法律层面证明神经信息属于个人信息,然后才能对神经信息行使相应的个人信息权益。

(一) 神经信息在个人信息保护法层面的法律属性

如何描述脑机接口技术所处理的人类生理信号,是世界性难题,各国在概念的表达上莫衷一是。在规范层面,西班牙和智利的概念界定从“大脑活动”切入——西班牙的《数字权利纲要》(*La Carta de Derechos Digitales*)将此类信号称为“有关大脑活动的信息”,《智利共和国政治宪法》将其称为“由大脑活动产生的信息”。美国的《科罗拉多州隐私法》和巴西的《神经数据保护草案》则将此类信号称为“神经数据(neural data, 葡萄牙语的表述为 *dados neurais*)”。在学理层面,有观点将此类信号直接称为大脑数据^[5],也有观点将其称为精神隐私^[8]。总体来看,尽管域外诸国的命名尚未达成一致,但它们的构词方式却具有一定的规律性——以一个体现心智能力的形容词(比如“大脑”“脑部”“神经”)去修饰一个名词(比如“数据”“隐私”“信息”)。

与上述诸般称谓不同,本文将脑机接口技术所必须处理的人类信息表述为神经信息,有以下两点理由:其一,以“神经”作为形容词,能周延地框定脑机接口技术所指向的信息范围,以“大脑”或“脑部”来修饰此类信息则并不准确。这一方面是因为,脑机接口设备所提取的信号并不局限于脑部,而是人体的整个神经系统,这其中包括大脑、脊髓与末梢神经等。所以,若把“大脑”或“脑部”作为限定词,脑部以外的神经信号从字义上就不能被涵摄于本概念之内。另一方面,并非所有的大脑信息都是脑机接口设备必

须处理的核心信息,如利用传统神经影像技术(如CR、CT、血管造影等)获得的脑部病理性信息(如是否患有脑瘤、脑卒中等)就属于传统医疗信息,其不必然构成神经技术规制议题项下需要讨论的信息,此议题下所分析的主要是意识活动所产生的信息。

其二,此类信号的本质属性是信息,而非数据或隐私。一方面,由脑机接口提取的神经信号必然构成一种信息,但其不必然构成后续可以财产化利用的数据,例如,在违反强制性规定的情况下,神经信息就无法成为可资利用的数据。虽然复数神经信息组合后可以演变为神经数据,但这要以单个的神经信息被记录为前提。若以“数据”来定义此类信号,则抹杀了它们尚未聚合的原始状态。另一方面,并非所有神经信息都构成隐私,如用户在公共场合抬起手臂,神经设备同时捕捉到这一肌电信号,那么此神经信息显然不是一种隐私,因为它所记录的不过是人在公开场合所作出的一个动作,这个事实与人格尊严并无关联。综上所述,神经信息的定义是,脑机接口技术所必需的,与人类意识活动有关的信息。

神经信息是个人信息吗?有业内观点认为,神经信息不是个人信息。如于神经科技业内领先的心绪公司(EMOTIV公司)^①,其在旗下产品的隐私协议中这样写道:“(我方)也会收集不构成个人信息的信息,如脑电图信号。”“脑电图信号本身不是个人信息,因为它不会也不能识别你的身份。”但实际上,用于表征人类神经信息的EEG信号、MEG信号等,均可以指向特定个人。与指纹类似,每个自然人的脑电波也不尽相同。在固定的测量条件下,不同个体的脑电图将呈现出各异的“脑纹”。因此,脑电图信号是一种有效的生物识别标识符^[9]。也就是说,脑电信息与自然人具有天然的对应关系。因此,神经信息显然具备《个保法》第4条所规定的可识别性,受个人信息保护制度的调整。

《个保法》第28条对敏感个人信息进行了不完全列举,因此,神经信息在规范上具有归属于敏感个人信息的可能性。尽管神经信息具有生物识别性,且在多数情况下构成隐私权的客体,但这并不意味着所有神经信息都是《个保法》第28条所规定的“敏感个人信息”。敏感个人信息的核心构成要件是易致害性,这种风险一般暴露于情感型脑机接口和感官型脑机接口,而非运动型脑机接口中。对于帮助残障人士恢复运动能力的脑机接口设备而言,其采集的脑电信号主要为动作电位信号,如摆臂、伸腿、抓握等信号。此类信息所承载的内容仅为肢体动作,即使被非法泄露或使用,也并不必然侵害人格尊严,故只属于一般个人信息。但具有高度人格性的感官信号和思想内容,则应被认定为敏感个人信息。

(二) 自然人对神经信息享有的个人信息权利

2023年,全球首例“神经信息保护案”——Guido Girardi Lavín诉Emotiv公司案(GIRARDI/EMOTIV INC, Rol N°105065-2023),在智利最高法院宣判。案涉设备是案件被告美国心绪公司生产的脑机接口无线耳机,通过传感器收集用户神经信息。原告主张,设备的用户协议存在强制性条款,迫使用户交出脑数据的处理权限,而设备未能为神经信息提供充分保护。这不仅导致用户数据面临被重新识别、商业化或监控的风险,更可能侵害心理隐私和认知自由等神经权利。智利最高法院认为,智利现行的个人数据保护法无法应对脑数据带来的特殊风险,本案的核心争议在于神经信息是否受宪法保障。法院依据2021年修订的智利宪法第19条,明确“科学技术的发展应以保护大脑活动及其衍生信息为前提”,判决被告心绪公司删除其存储的所有来源于原告的神经信息。

智利以宪法诉讼保护神经信息的创举,具有里程碑式的意义,但此模式显然无法被重复适用。作为根本法,宪法并不能直接有效地对神经技术的治理产生具体的规制作用。如前所述,既然神经信息可以被解释为规范意义上的个人信息,那么我国自然可以直接适用《民法典》和《个保法》来保护神经信息。具言之,自然人对自身的神经信息,享有知情同意权、撤回同意权、信息删除权和损害赔偿请求权。

处理神经信息须以神经信息处理者充分告知个人为前提。依据《个保法》第14条和第17条,个人在知悉以下内容时,方可视为处理者“充分”告知:第一,处理神经信息的具体目的;第二,处理的神经信息

^① 本文提到的神经技术公司目前均无官方中文译名,此处的心绪公司、下文的凝神公司(FocusCalm)和比亚公司(Bía)均为笔者自行翻译。

类别;第三,神经信息的存储方案。放眼当前的技术实践,脑机设备通常分为三类,即输入型、输出型和检测型脑机设备,这三者在处理神经信息的目的、对象和保存措施上各有不同。输入型脑机设备的主要目的是改善用户的意识或情绪,例如用于治疗抑郁症。输出型脑机设备旨在传递用户的动作意图,例如协助高位截瘫患者控制肢体。检测型脑机设备则专注于观察用户特定的脑部状态,如睡眠状态。输入型和检测型脑机设备主要处理涉及心理或思想层面的神经信息,而输出型脑机设备则更侧重处理与动作或行为相关的神经信息。处理者在不同设备的应用场景下,负有相应的具体告知义务。

处理者在明确处理目的的前提下,不得收集超出必要范围的神经信息。例如,针对高位截瘫患者设计的输出型脑机接口设备,其主要功能是解码患者的运动想象,因此,处理者不得随意收集与此目的无关的其他信息,如内心语音信号等。同时,为降低信息泄漏风险,处理者应尽可能将所收集的神经信息局限于设备本地存储,除非确有必要,不应将信息上传至云端进行处理或保存,如神经技术公司凝神公司(FocusCalm)在其隐私协议中规定,所有的脑电图数据都保留在用户智能设备内的FocusCalm应用程序中,其在每次使用结束时会被清除。

处理者对神经信息的保存期限应以实现处理目的所需的最短时间为限,并明确约定数据的处理和保存方式。根据《个保法》第19条,结合《网络数据安全条例》第21条第1款第3项的规定,在保存期限无法预先确定的情况下,处理者不得随意约定无限期的保存时间,而应在用户协议中清晰列明保存期限的具体确定方式,以确保信息处理的透明性和合规性。举例来说,神经技术公司比亚(Bia)的隐私协议中规定Bia在与会员的业务关系存续期间以及之后的无限期期限内将会员数据保留在安全的服务器上,该条款就违反了神经信息保存的最短时限原则。

在处理敏感神经信息时,处理者必须严格遵循“单独同意”规则,并确保处理范围不超过必要限度。根据《个保法》第29条的规定,在脑机接口技术的适用场景下,“单独同意”规则可以细化为三个层面:其一,设备提供方在获得患者同意使用设备的基本意思表示之外,还需额外取得患者同意处理神经信息的明确授权;其二,设备提供方在获得患者同意处理一般性神经信息(如运动想象)的基础上,还需分别单独获得患者对处理敏感神经信息(如内心语音)的具体同意;其三,设备提供方不得泛化或扩展患者对敏感神经信息处理的授权范围。例如,Bia公司在隐私协议的个人信息收集清单中,将大脑活动信息与账户信息和付款信息并列,即违反“单独同意”规则。

根据《个保法》第15条的规定,自然人享有随时撤回对神经信息处理同意的权利,而无需事先征得信息处理者的同意。一旦自然人撤回同意,处理者有义务主动删除其已收集的神经信息。为保障撤回同意权和信息删除权的有效行使,神经信息处理者需依照《个保法》第50条及《网络数据安全条例》第23条的规定,提供简便易行的方式供个人提交申请,并及时处理这些请求。处理者不得以不合理的条件或程序阻碍个人行权。若处理者拒绝相关请求,应当明确说明具体理由。神经信息处理者处理神经信息造成损害,且无法证明自己没有过错的,应按照《个保法》第69条承担过错推定责任。

三、作为隐私的神经信息的法律保护

自然人理应是心灵的最高主权者,是自我精神世界的绝对主宰。在传统技术背景下,个体意识活动的内容是无法被直接探知的存在,因此,它自隐私权制度诞生以来就游离于隐私保护的“光谱”之外^[10](P63)。随着脑机接口技术的蓬勃发展,大脑已不再是绝对私密的精神堡垒,当代隐私法有必要将具有私密性的神经信息纳入隐私的范畴之内,对神经信息隐私实施体系化保护。

(一) 神经信息在隐私法层面的法律属性

在脑机接口技术的冲击之下,个体的心智活动不再是旁人无法染指的禁地,人类的所思所想面临直接暴露的空前危机。无论是出于好奇心还是为了追名逐利,人们总乐于根据蛛丝马迹来推断和揣测他人的心理状态和意识活动。借由以个人数据为基础的智能算法,AI能够以惊人的准确度推算用户的精

神健康状况、政治倾向和宗教信仰。然而,无论人工智能采用何种超级算法深入人类的内心世界,其引发的风险都无法与脑机接口技术对人类精神净土所形成的巨大威胁相匹敌——AI对人类心智的揣度以逻辑推理为线索,以行为科学、心理学、社会学等研究人类外部活动的学科为学理基础,是对人思维活动的主观性、间接性推断;脑机接口技术则是以对大脑神经元的观测为基础,以医学、神经科学等研究人体内部的学科为理论支撑,它的观测结果是对人脑意识活动的客观性、直接性、本质性的反映。申言之,假如脑机接口技术没有得到有效规制,任何人的任何想法都可能赤裸裸地昭显于世人面前,人类作为生命主体者的生命尊严将彻底瓦解^[11](P11),整个世界都将沦为福柯笔下隐私无所遁形的全景监狱。

面对这前所未有的危局,学界涌起一股建构新兴权利的思潮。有观点认为,由脑机接口技术所提取的神经信息,不属于《民法典》第1032条所规定的隐私,因为隐私需要“不愿为他人知晓”,而脑机接口设备的使用,以使用者同意他人读取神经信息为前提。传统隐私权保护的是已经表达出来的,无须外界辅助就可以直接读取的信息,而对个人思想的窥探有较高的技术门槛。故而,应当以一个全新的法律概念——“脑隐私”来保护神经信息,隐私的外延不能涵盖脑隐私^[12](P130-131)。这种理解既过度限缩了“不愿为他人知晓”的内涵,因为隐私不仅包括不与任何人分享的绝对隐私,还包括只有特定人知晓的相对隐私^[13](P497),又片面地压缩了隐私权的调整范围,因为隐私权对利用技术手段刺探隐私的行为同样具有消极的防御权能。还有观点认为应设立精神隐私权^[8],以专门应对新兴神经技术对神经信息探查与监测,从而维护人的自我边界与精神尊严。但是,这种主张并未突破传统隐私权理论的立论基础,也没有提出新的值得保护的利益^[14](P103)。

从规范层面分析,由脑机接口设备读取的神经信息完全可以被涵摄于《民法典》第1032条第2款的范畴之中。《民法典》第1032条第2款规定:隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。首先,大脑的意识活动无须他人的参与,是人类主体性和独立性的来源。所以,它不仅构成一种绝对的“私密活动”,而且在一切私密活动中处于最高位阶。从反证法的角度来说,倘若连最私密的思维活动都不能受到隐私权的保护,那么举重以明轻,其他私密活动又有什么资格忝列于隐私权的保护范围之内?故隐私权在新的技术背景下对神经信息的保护,具有稳定整个隐私谱系的重要作用。其次,如果观测到的私密意识活动被记录于某种载体之上,那么此种记录就属于私密信息,此类信息与私人日记或私人书信没有本质上的区别,它们的曝光都会引致对自然人人格尊严的减损。最后,并非所有神经信息都构成隐私,其承载的内容并不都具有私密性,然而,假如自然人的神经信息在其并非自愿的情况下被持续观测,那么他难免会时刻担心自己的秘密被他人窥探,自己无意识的、不光彩的古怪想法会被公之于众^[15](P30)。这种恐惧势必会搅扰人的正常思维,打破人的“私人生活安宁”。综上所述,借由法律解释的方法,现行隐私权规范在外延上可以周延地囊括神经信息需要保护的各个部分,我国目前不需要对其进行过度立法。

(二) 隐私权人对神经信息隐私享有的权利

当神经信息隐私受到侵害时,隐私权人享有相应的防御型请求权。依据《民法典》第1032条第1款,神经信息隐私受到侵害,是指构成隐私的神经信息,在未经权利人同意的情况下,遭到刺探、侵扰、泄露、公开等行为的侵犯。根据神经信息隐私受到侵害的具体形态,隐私权人可以分别或同时行使人格权请求权、侵权责任请求权或违约责任请求权。在现有的规范体系下,神经信息隐私受到侵害的情形,被《民法典》第1165条划分为两种形态,一是受到侵害但尚未受到损害,二是受到侵害且受到损害。

神经信息隐私受到侵害但尚未受到损害,是指行为人使神经信息隐私陷入泄露或公开的风险,但尚未泄露或公开。在此情形下,权利人可以行使人格权请求权,请求行为人承担停止侵害、消除危险的民事责任。根据《民法典》第995条的规定,受害人有权以隐私权人的身份请求行为人承担一系列民事责任。然而,消除影响、恢复名誉、赔礼道歉以恢复原状为规范目的,以损害的出现为前提,属于侵权责任请求权的范畴,故受害人在未受损害时,只得请求行为人停止侵害、消除危险^[16](P117-118)。如果权利

人的神经信息隐私面临泄露的紧迫风险,还可以依据《民法典》第997条申请人格权禁令,由法院责令行为人停止相关行为。

神经信息隐私受到损害,是指行为人成功刺探或侵扰神经信息隐私,使其泄露或公开。此时,权利人可以行使侵权责任请求权或违约责任请求权进行事后补救。神经信息隐私受到侵害且受到损害时,受害人享有的请求权基础应当根据行为人的身份分类讨论。若为神经信息处理者致使神经信息隐私受损,受害者可向处理者主张违约责任请求权或侵权责任请求权。若受害者主张对方承担侵权责任,须证明处理者有故意或过失。处理者是否有故意较为明显,是否有过失则须考察处理者是否违反必要的注意义务,此处注意义务的具体内容,要根据脑机接口技术的相关国家标准和行业标准来确定。例如,不久前发布的《可穿戴式脑机接口专用脑电采集分析系统技术要求及测试方法(T/CAS 976-2024)》团体标准,就可以用于认定处理者在相应场景下应负担何种注意义务。2024年,中华人民共和国工业和信息化部已经发布了《脑机接口标准化技术委员会筹建方案》,着力打造由基础共性、I/O接口、脑机接口数据、应用、伦理和安全五个部分组成的脑机接口标准体系,此方案将在未来进一步促进责任认定的体系化与规范化。

在责任证立之后,需要进一步明确处理者的责任范围。对于财产损失,受害者可依约定的违约责任请求赔偿,也可依《民法典》第1182条,根据受害者所受损失或处理者所得利益请求赔偿。对于精神损害,受害者可按照《民法典》第995条,要求处理者赔礼道歉。受害者的名誉因神经信息隐私的泄露或公开而受损的,也可依《民法典》第995条,要求处理者消除影响、恢复名誉。受害者遭受严重精神损害的,可依《民法典》第1183条请求精神损害赔偿,此项请求不与处理者违约责任的承担相冲突。

处理者处理神经信息的前提是双方就处理神经信息的相关事项达成协议。若双方在协议中明确约定了处理者的隐私保障义务,能直接判断处理者是否违约,则受害人可径直依《民法典》第577条请求处理者承担违约责任,即继续履行隐私保障义务、采取补救措施或者赔偿损失。若双方在协议中未明确约定相应义务,依《民法典》第510条仍未协商一致的,可依《民法典》第511条第1款第1项,按照国家标准或行业标准来确定具体的隐私保障义务。随着我国脑机接口技术标准化体系的日益完善,当事人可以《民法典》第511条第1款第1项为管道,将相应的国家标准和行业标准引入具体合同义务的判定之中。对于处理者违反隐私保障义务致使不能实现合同目的的情形,受害人还可依《民法典》第563条单方解除合同,合同因违约解除的,受害人仍可依《民法典》第566条第2款请求行为人承担违约责任。

若为神经信息处理者之外的第三人致使神经信息隐私受损,受害者可向第三人主张侵权责任请求权,并在特定条件下向神经信息处理者主张违约责任请求权。脑机接口设备大多依赖网络进行神经信息的传输和加工,这种运行模式包藏着不可避免的隐私泄漏风险。如果第三人利用技术手段侵入脑机接口设备,窃取神经信息隐私,则受害者可依照前文所述主张相应的侵权责任请求权。第三人利用网络损害神经信息隐私的,受害人可以依照《民法典》第1195条通知网络服务提供者(通常是联网神经信息处理者)采取删除、屏蔽、断开链接等必要措施停止侵害、消除危险。处理者明知或应知第三人利用网络损害神经信息隐私,但未采取必要措施的,受害人可依《民法典》第1197条要求处理者和第三人承担连带的侵权责任。处理者未履行或未完全履行隐私保障义务,致使第三人突破隐私防护,造成损害的,受害人也可以向处理者主张违约责任请求权,处理者在承担违约责任后可以向第三人追偿。

侵犯神经信息隐私的行为有作为和不作为两种形态,在这两种形态下,行为人承担民事责任的具体方式各有不同。当行为人以积极的作为侵害神经信息隐私,受害人得请求停止该积极行为。如未获得受害人同意者利用非法技术手段擅自窥探神经信息,或获得受害人授权者,收集在其获得授权范围外、时限外的神经信息,受害人可以请求行为人立即停止其刺探或越权收集神经信息隐私的行为。前文所述的是侵犯神经信息隐私的通常情形,但在例外情形下,行为人也可以通过不作为的方式侵害神经信息隐私。此时,受害人需要请求行为人履行法定或约定的义务——假如处理者处理的神经信息仍有可识

别性,用户可以请求处理者采用多方安全计算^[17]等方法履行必要的隐私计算义务,使信息不可指向具体的用户。

四、作为数据的神经信息的法律保护

作为单一神经信息的集合,神经数据具有空前的科学和商业价值,法律应以确权的形式对其予以周全保护。在数据法层面,要廓清神经信息的法律属性,关键在于确定神经数据权利的权属,将这一财产性权利分配给适当的主体。神经数据权利与自然人的权益存在冲突,权利人在行使相关数据权利时,必须严格履行神经数据的安全保障义务。

(一) 神经信息在数据法层面的法律属性

神经信息和神经数据的关系譬如树木与森林,神经数据从语义上即是对神经信息之集合的统称。与作为个人信息和隐私的神经信息不同,神经信息在数据法层面的难题并不在于神经信息是否构成神经数据,而在于如何理解“持有神经数据”。

神经数据来源于个人,但个人能当然地享有神经数据的持有权吗?神经数据持有权的归属,有三种可能的配置路径:其一是由神经数据的来源者直接享有数据持有权。此方案与神经信息取之于个人的客观事实相符,有利于对神经数据中体现的人格要素提供全面的保障,但它完全无视了神经数据处理者的利益诉求。其二是神经数据来源者与神经数据处理者共享神经数据持有权。在一般数据权属纠纷中,“数据属于个人与平台共有”是一种常见的裁判观点^[18](P74),这种安排看似兼顾了各方的利益,实际将神经数据的财产利益和神经信息的人格利益混为一谈,且持有权共有的比例与权能在现实中很难得到明确,这显然会阻碍数据的利用与流通。其三是由神经数据的处理者享有数据持有权。处理者持有是目前数据权属的通说^[19](P152-153),其论说逻辑在神经数据权利的配置问题上同样适用。

神经数据持有权由神经数据处理者享有,而非个人享有,有如下三点理由:首先,单一的神经信息几乎不具有财产价值。神经信息是人对客观事实的主观映射,是人驱使各个身体部分的生物信号。孤立的神经信息所包含的信息量极低,不具有知识层面的稀缺性,只有聚合起来的神经信息才蕴藏着规律性的价值^[20](P54)。以规模化的神经数据为素材,研究者才能展开分析、比较和归纳工作,从而为识别、预测和干预人的精神活动提供科学指引。上海交通大学建立的情感识别脑电数据集(SJTU Emotion EEG Dataset,以下简称“SEED数据集”)^[21]可以帮助我们直观地理解单一神经信息和神经数据的价值差距。SEED数据集是以感官实验数据为基础的数据集,它收集的是受试者观看不同电影片段时的脑电信号。这些电影片段分为三类,引起积极情绪的片段、引起消极情绪的片段和中性片段。SEED数据集的每个条目由以下信息组成:第一,受试者代号;第二,观看的电影片段类型;第三,受试者自述的情感反应;第四,受试者观看相应片段的脑电信号。所以,该数据集之中每个独立的条目其实平平无奇,它只是这样一条信息——1号受试者观看《唐山大地震》的片段后表示自己感到悲伤,这是他当时的脑电信号。面对这样一条孤立的神经信息,研究者显然无法分析出人类情绪与脑电波之间的对应关系。研究者只有在规模化的数据之中,才能比对各脑电信息的异同,进而推理何种脑电信号表示人类的喜怒哀乐。

其次,神经数据的财产价值来源于神经数据处理者的劳动。神经数据的收集、整理、分析工作是一种数字劳动,它使得零落的、分散的神经信息依照预设的逻辑组合起来,最终指向某一特定的知识或结论^[22](P21)。神经数据的处理既要求专业的程序设计,又需要配置特定的神经数据处理设备,与之截然相反的是,个人在提供神经信息时只需要调动人类的生物本能,这很难被视作一种劳动。从劳动价值论的角度分析,神经数据是处理者的劳动成果,神经数据之财产价值的高低取决于处理者整合神经数据的水平,故神经数据持有权应由神经数据处理者享有。例如,SEED数据集之所以能成为情感脑机接口研究领域使用最为广泛的数据集之一,是因为研究者既选用了恰当的电影素材调动受试者情绪,保证了实验效果,又以适合的通道与频率记录了相应的脑电活动,减少了无关的干扰信息。SEED数据集的成功

要归功于研究者设计实验和执行实验的科研能力,而非个人基础的神经活动。

最后,神经数据持有权由神经数据处理者享有,不影响个人人格权益的保护。作为神经信息集合的神经数据既包含财产利益,也包含人格利益,将其中的财产利益配置给神经数据处理者,既有利于提高数据的使用价值和流通效率,也不至于使其中的人格利益受损^[19](P156-159)。在地方立法中,这一“人财两分”的确权模式已经得到了广泛认同,如《深圳经济特区数据条例》第4条和《上海市数据条例》第12条第2款均强调数据处理者的财产利益受法律保护。对于神经数据的人格利益保护,我们可以根据神经数据是否匿名化进行分类讨论。如果神经数据已经匿名化,其实它就不涉及人格利益保护的问题,因为它已不具有可识别性,其所反映的信息无从指向具体的个人,也就不具有侵害人格利益的可能性。如果神经数据没有匿名化,那么处理者对它的处理须严格遵循《个保法》第13条的个人信息处理规则,且在处理的过程中应依法保障个人查询、复制、携带、删除、修改个人神经数据的权利。

神经数据持有权的权利主体,需要基于具体的使用场景确定。在消费场景下,神经数据的持有人不是消费者,而是脑机接口设备的提供者。所谓消费场景,是指消费者购买脑机接口设备并自行使用,设备提供者处理消费者的神经信息,形成神经数据的应用场景。在此情形下,进行数字劳动的显然是设备提供者,故只要设备提供者有权处理消费者的神经信息,那么由此生成的神经数据就归设备提供者持有。在非消费场景下,神经数据的持有人则相对难以确定。所谓非消费场景,是指设备所有者对不特定多数人使用脑机接口设备的应用场景,如医院购买脑机设备治疗患者,或高校购买脑机设备开展实验。在此情形下,设备的使用者(如患者或受试者)显然不是持有人。但究竟是设备所有者还是设备提供者是神经数据的持有人呢?对于这一问题,应当首先尊重当事人的意思自治,根据约定确定权属。没有约定的,应当根据双方数字劳动的强度和贡献确定权属。

(二)神经数据持有者的权利

2022年12月,中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称“数据二十条”)明确了数据处理者“数据资源持有权”“数据加工使用权”和“数据产品经营权”的三权分置体系。基于处理神经信息的事实,神经数据的持有者享有上述三种数据权利。

神经数据持有权来源于权利主体控制神经数据的事实基础,它是神经数据持有者排他地、自主地管控神经数据的财产性权利。要理解神经数据持有权,首先要廓清它的事实基础。所谓控制神经数据,是指主体以数据基础设施为物质载体控制神经信息之数字副本的状态^[23](P105-107)。神经数据持有权所保护的正是这一状态。从积极的层面来看,持有权保护持有者在事实上支配神经数据的自由,这构成神经数据加工使用权和神经数据产品经营权的确权前提;从消极的层面来看,持有权禁止不特定第三人侵扰持有者对神经数据的控制^[24](P70)。对于行为人非法访问、非法篡改和非法复制神经数据等行为,持有人得主张停止侵害、排除妨害、消除危险等绝对权请求权和损害赔偿请求权。

神经数据加工使用权是持有者对自我持有的进行加工并获取收益的权利。作为人类进入数字空间生存的虚拟原料,神经数据在消费、医疗、娱乐、军事等领域的巨大价值不会凭空显现,它需要由原始数据转换为适用于各个具体应用场景的合成数据,这一转换过程有赖于神经数据处理者的整理、清洗、标注、分析、组合等一系列工作^[25](P167)。持有者对神经数据的加工和使用能实现数据使用价值的增值,为持有者带来更大的经济效益。

神经数据产品经营权是持有者将神经数据及其衍生品投入市场,并获取收益的权利。神经数据没有实体,以神经数据产品为客体的经营权,从本质上是许可他人使用神经数据的权利,这一权利是实现神经数据生产要素化的流通基础。所以,在具体的权能层面,我们不能以传统所有权的占有、使用、处分、收益权能来建构神经数据产品经营权,而是应当以同样具有无形性和可共享性的著作财产权来理解神经数据产品经营权的权能。神经数据持有者不仅可以授权他人访问、检索、复制、分析自己的神经数据,还可以用经营权进行投资入股或质押融资^[26](P169-170)。

作为一项财产权利,神经数据持有权具有明确的权利边界。神经数据持有权的行使,应以保护个人信息权益和隐私权为前提,故此,神经数据持有者负有保障神经数据安全的义务。根据对《个保法》第4条第1款的反面解释,不能直接或间接识别到个人的信息不是受《个保法》保护的个人信息,由于神经数据只能来源于自然人,神经数据持有者的核心义务,实质上是实现和维持神经数据的匿名化。

在理想状态下,一组优秀的神经数据集应当既具有充分的使用价值,又保持完全的匿名化。然而,在神经技术日新月异的迭代趋势下,神经数据的安全性 with 实用性之间的矛盾其实并不容易调和——对匿名化的过度追求会使神经数据沦为无效的随机信号。对于不成像的神经数据(如脑电数据),当下的最新研究采用“字典学习”技术,把复杂的脑电波信号拆解为各个基本构件,再利用机器学习对构件的特征进行分析,就可以像声纹识别、虹膜识别一样识别每个人独特的脑电活动模式^[27]。对于成像的神经数据(如磁共振成像MRI),神经科学家可基于大脑活动的三维图像,对大脑不同区域之间的协同活动进行分析,这一大脑活动的模式被称为“脑连接组”,在数学层面,它可以被表征为一组特征向量。研究者将特定脑连接组的特征向量与已有的特征向量进行比对,就能识别“匿名”神经数据的身份,识别准确率高达94%^[28]。

如果仅考虑神经数据利用中的人格利益保护问题,法律当然可以赋予神经数据处理者这样的义务——抹除神经数据中一切可能表征来源者身份的内容,但神经数据在法律上的绝对匿名化,只会导致它在效用上的绝对低效化。首先,绝对的匿名化会破坏神经数据的基本功能。例如,生成对抗网络等深度学习算法甚至能够从模糊化或部分去标识化的MRI图像中重建面部特征,实现高度精确的再识别^[29],但我们不能因此就移除神经图像数据中的相关面部信息和头部几何信息,因为这会使诸如脑功能分析和脑电源定位的功能性研究,失去最核心的研究素材。再比如,某些神经疾病的诊断和预测完全有赖于精确的脑区连接分析,如果我们因为目前存在用“脑连接组”反匿名化的技术,就要求神经数据处理者剔除所有脑区连接数据,那么其剩余数据的医学研究价值将彻底丧失^[30]。其次,绝对匿名化的神经数据在科学共享中的复用价值极低,难以为跨机构、跨地域、跨学科的协作提供足够支持。例如,在人类连接组计划中,只有保留高分辨率的神经连接图谱才具有可重复性和可验证性。最后,绝对匿名化的工作不仅程序繁杂,而且费时费力,这将严重干扰大规模神经数据集的处理和共享。

如何在神经数据的安全性 with 实用性之间寻求平衡?放眼全球,我们可以根据匿名化的严格程度,将各国提出的匿名化标准划分成三个层次:其一是针对“任何人”的绝对匿名化标准。在该标准下,匿名化的个人信息,应当处于任何人都无法令其与特定个人重新对应的状态。这是最严格的匿名化立法,欧盟《通用数据保护条例》采用了此类标准。其二则是最宽松的“一般人”标准,这一标准的要求是,只要按照一般社会公众的平均水平无法再识别的个人信息,就是完成匿名化的个人信息。显然,这一观点过于宽容,故其仅仅停留在理论层面,未被立法采用^[31](P115-116)。介乎于前述二者之间的是“特定人群”标准,该标准以特定人群通常具备的识别能力为判断基准,只要特定人群以及该水平以下的人群均无法识别某一信息,该信息就实现了匿名化。如美国的《健康保险携带和责任法案隐私规则》规定,若一名对普遍接受的统计和科学原理与方法有适当了解和经验,以使信息不具个人可识别性的人,应用这些原则和方法,以书面结论确定信息被单独或与其他合理可获得的信息结合使用来识别信息主体的风险非常小,则该信息达到了去标识化的要求。英国则以“有动机的入侵者”的识别能力作为匿名化的判断标准。英国对有动机的入侵者的预设是,他不具备任何专业知识,如计算机黑客技术,也不需要使用专业设备或采取入室盗窃等犯罪手段来获取安全保存的数据,但会使用网络搜索、档案检索、图书馆查检等识别方法^[32](P22-24)。显然,此识别能力设定高于一般公众,又略低于专业技术人员。

为了兼顾神经数据的安全与效用,神经数据的匿名化标准应当采用“特定人群”标准。匿名化工作的安全保障效果是边际递减的,但其对神经数据研究价值的损耗是边际递增的^[33]。举例来说,如果法律已经为神经数据的识别设定了一定的技术门槛,那么这一技术门槛每再提高20%,神经数据的研究价值

可能就会损失40%,但其安全性可能只增加了5%。回到规范层面,《数据安全法》一方面在第7条鼓励数据的利用和流动,一方面又在第8条强调数据安全保护义务,意在申明数据的实用性与安全性不可偏废。故此,《数据安全法》第四章规定的神经数据处理者的数据安全保护义务,可以在匿名化问题上被解释为如下内容:神经数据处理者,应确保具有“一定识别能力”的行为人无法还原神经数据来源者的身份。至于何谓“一定识别能力”,则应当视具体的技术场景进行法律解释,立法不宜作机械的规定。同时,鉴于匿名化技术与反匿名化技术的动态博弈,识别能力的判断标准也处于不断的变动之中,神经数据持有者应当遵照《数据安全法》第30条的规定,对其数据处理活动定期开展风险评估,根据实时的神经技术发展水平调整去识别化的技术门槛。

五、结 论

神经信息是人类走向数字化生存的核心要素,法律需要对其妥善规制,但这并不意味着,我国必须制定特别的法律,才能实现对神经信息的完满保护。相反,我国现行规范具有足够的制度张力,既有立法能以个人信息、隐私和数据为切入点,逐一化解脑机接口技术引发的神经信息保护危机,构建神经信息保护的规范体系。

《个保法》是整个规范体系的基础,对神经信息的保护应优先适用《个保法》。其一,尽管《民法典》第1034条第3款规定“个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定”,但该条规定所强调的是隐私权制度在私密信息保护上,而非神经信息保护上的优先适用顺位。前文已述及,神经信息中既包含私密神经信息,又包含非私密神经信息,例如,被记录的内心想法是私密信息,但大脑驱使机械臂拿起水杯的神经信号显然不是私密信息。因此,神经信息并不必然构成私密信息,《民法典》第1034条第3款并不意味着,隐私权制度在神经信息保护上应优先适用。其二,任何被脑机接口处理的神经信息均具有可识别性,都构成个人信息。基于《立法法》第92条的规定,《个保法》相对于《民法典》既是新法,亦是特别法,故在神经信息的保护问题上,《个保法》的适用顺位应优先于《民法典》。准此,任何提供神经信息的个人,都至少享有《个保法》规定的知情同意权、撤回同意权、信息更正、异议、删除权和损害赔偿请求权等权利,神经信息处理者至少要负担《个保法》所规定的相应义务。

神经信息隐私的保护,应优先适用《民法典》有关隐私权的规定,没有规定的,适用《个保法》。神经信息隐私属于私密信息,依照《民法典》第1034条第3款的规定,隐私权制度在神经信息隐私的保护中具有优先适用顺位。但不容忽视的是,神经信息隐私既然能归属于隐私权的“私密信息”之中,就同样能涵摄于《个保法》第28条的“敏感个人信息”之下,盖“私密信息”与“敏感个人信息”的设计均出于对人格尊严的保护。因此,《民法典》第1034条第3款调整规范竞合的方式具有相当的灵活性,对于神经信息隐私的保护,隐私权制度并不凌驾于《个保法》之上^[7](P100)。例如,《民法典》第1033条规定的隐私侵权免责事由为权利人“明确同意”,而《个保法》第29条则要求处理敏感个人信息应当取得个人的“单独同意”,这显然提高了同意的门槛。鉴于《民法典》有关隐私权的规定没有对私密信息的同意条件作出具体阐释,我们可以依据《民法典》第1034条第3款的后半句,直接适用《个保法》第29条的“单独同意”规则。

当自然人的神经信息隐私受到侵害时,其隐私权和个人信息权益将同时受到侵害,人格权请求权、个人信息权益请求权和相关债权请求权构成请求权聚合。对于现存的侵害,停止侵害、消除危险的人格权请求权与删除、更正、补充信息的个人信息权益请求权构成聚合,可以同时行使。对于可以恢复原状的损害,消除影响、恢复名誉、赔礼道歉的债权请求权与相关个人信息权益请求权构成聚合,可以同时行使。对于无法恢复原状的损害,自然人享有损害赔偿请求权,但《民法典》第1165条第1款的过错责任原则与《个保法》第69条的过错责任推定原则不一致,依据《民法典》第1034条第3款的后半句,神经信息隐私受损的自然人,可以要求无法证明自己没有过错的神经信息处理者承担损害赔偿责任。

神经数据的保护,应适用《数据安全法》等一般性数据规范。大规模聚合的匿名化神经信息构成神

神经数据,神经数据持有者所享有的神经数据权益是一种财产性权益,持有者本身不对神经数据享有任何人格权益,持有者对神经数据来源者和神经信息隐私权人承担相应的保护义务。在民事权益的利益衡量中,财产权利劣后于人格权益^[34],故神经数据持有者的核心义务,是实现和维持神经数据的匿名化,避免数据来源者和隐私权人的人格权益受损。

脑机接口技术必然会重塑未来社会的规范体系,但仅就神经信息而言,经过充分解释的现行规范足以对神经信息提供全生命周期的保护。《个保法》为神经信息中的人格利益和财产利益提供兜底性保护。《民法典》人格权编重点为神经信息隐私中的人格利益提供周全保障。神经数据持有者可以根据现行的和日后不断完善的一般数据规范,保护其对神经数据享有的财产性权益。

参考文献

- [1] F. Mushtaq, D. Welke, A. Gallagher et al. One Hundred Years of EEG for Brain and Behaviour Research. *Nature Human Behaviour*, 2024, 8(8).
- [2] Yohann Benchetrit, Hubert Banville, Jean-Remi King. *Brain Decoding: toward Real-Time Reconstruction of Visual Perception*. The Twelfth International Conference on Learning Representations, 2024.
- [3] N.S. Card, M. Wairagkar, C. Iacobacci et al. An Accurate and Rapidly Calibrating Speech Neuroprosthesis. *The New England Journal of Medicine*, 2024, 391(7).
- [4] Daniel S. Hain, Roman Jurowetzki, Mariagrazia Squicciarini et al. *Unveiling the Neurotechnology Landscape: Scientific Advancements Innovations and Major Trends*. Paris: UNESCO, 2023.
- [5] P. Kellmeyer. Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-directed Neurotechnological Devices. *Neuroethics*, 2021, 14(1).
- [6] Jared Genser, Stephen Damianos, Rafael Yuste. *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*. New York: Neurorights Foundation, 2024.
- [7] 申卫星. 数字权利体系再造:迈向隐私、信息与数据的差序格局. 政法论坛, 2022, (3).
- [8] P. López-Silva, A. Wajnerman-Paz, F. Molnar-Gabor. Neurotechnological Applications and the Protection of Mental Privacy: An Assessment of Risks. *Neuroethics*, 2024, 17(2).
- [9] Y.Y. Yang, A.H. Hwang, C.T. Wu et al. Person-identifying Brainprints Are Stably Embedded in EEG Mindprints. *Scientific Reports*, 2022, 12(1).
- [10] Neil Richards. *Why Privacy Matters*. Oxford: Oxford University Press, 2022.
- [11] 张红,叶竞欧. 作为生命权客体的生命尊严. 荆楚法学, 2024, (5).
- [12] 张曼. 脑隐私法律保护的制度建构. 东方法学, 2023, (5).
- [13] 张红. 人格权各论. 北京:法律出版社, 2024.
- [14] 陈鲁夏. 精神隐私可以成为新兴权利吗? 环球法律评论, 2024, (5).
- [15] Jan Christoph Bublitz. Privacy Concerns in Brain-Computer Interface. *AJOB Neuroscience*, 2019, 10(1).
- [16] 温世扬. 人格权请求权的概念构造与适用限制. 政法论坛, 2024, (3).
- [17] A. Agarwal, R. Dowsley, N.D. McKinney et al. Protecting Privacy of Users in Brain-computer Interface Applications. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 2019, 27(8).
- [18] 丁晓东. 数据到底属于谁? ——从网络爬虫看平台数据权属与数据保护. 华东政法大学学报, 2019, (5).
- [19] 张新宝. 论作为新型财产权的数据财产权. 中国社会科学, 2023, (4).
- [20] 曹相见. 个人数据的财产权归属. 法律科学(西北政法大学学报), 2024, (5).
- [21] W. Zheng, B. Lu. Investigating Critical Frequency Bands and Channels for EEG-based Emotion Recognition with Deep Neural Networks. *IEEE Transactions on Autonomous Mental Development*, 2015, 7(3).
- [22] 王利明. 数据权益的民法表达. 荆楚法学, 2024, (1).
- [23] 衣俊霖. 论作为法律关系的数据持有. 法学论坛, 2024, (4).
- [24] 王利明. 数据何以确权. 法学研究, 2023, (4).
- [25] 时诚. 数据权利的模块化设计. 东方法学, 2024, (5).

- [26] 叶敏, 范馨允. 数据产品经营权的生成逻辑与权利架构. 数字法治, 2023, (6).
- [27] T. Nishimoto, H. Higashi, H. Morioka et al. EEG-based Personal Identification Method Using Unsupervised Feature Extraction and Its Robustness Against Intra-subject Variability. *Journal of Neural Engineering*, 2020, 17(2).
- [28] Vikram Ravindra, Ananth Grama. *De-anonymization Attacks on Neuroimaging Datasets*. Proceedings of the 2021 International Conference on Management of Data, 2021.
- [29] David Abramian, Anders Eklund. *Refacing: Reconstructing Anonymized Facial Features Using GANs*. IEEE 16th International Symposium on Biomedical Imaging, 2019.
- [30] D. Eke, I.E.J. Aasebø, S. Akintoye et al. Pseudonymisation of Neuroimages and Data Protection: Increasing Access to Data While Retaining Scientific Utility. *Neuroimage: Reports*, 2021, 1(4).
- [31] 李润生. 个人信息匿名化的制度困境与优化路径——构建“前端宽松+过程控制”规制模式之探讨. 江淮论坛, 2022, (5).
- [32] Christopher Graham. *Anonymisation: Managing Data Protection Risk Code of Practice*. London: Information Commissioner's Office, 2012.
- [33] John M. Abowd, Ian M. Schmutte. An Economic Analysis of Privacy Protection and Statistical Accuracy as Social Choices. *American Economic Review*, 2019, 109 (1).
- [34] 王利明. 论民事权益位阶: 以《民法典》为中心. 中国法学, 2022, (1).

Legal Protection of Neural Information: Personal Information, Privacy and Data

Zhang Hong, Ye Jing'ou (Wuhan University)

Abstract Brain-computer interface (BCI) technology can directly detect and reflect human conscious activities, and this epoch-making technological revolution poses a serious threat to the personality rights and interests of natural persons. Since the conscious activities are collected by BCI devices as neural information, current regulations can address the technological impact of BCI from multiple levels by focusing on neural information. From an overall perspective, all neural information constitutes personal information as stipulated in Paragraph 1 of Article 4 of the *Personal Information Protection Law of the People's Republic of China*, and is in principle subject to regulation under the law. Moreover, neural information with a private nature constitutes privacy as stipulated in Paragraph 2 of Article 1032 of the *Civil Code of the People's Republic of China*. Natural persons, as privacy rights holders, can exercise corresponding personality rights claims, tort liability claims, and breach of contract claims. Large-scale aggregated anonymized neural information constitutes neural data, and holders of neural data can enjoy corresponding neural data holding rights, processing and use rights, and product management rights in accordance with general data regulations, and bear the obligation to ensure neural data security.

Key words neural information; brain-computer interface; neural information privacy; neural data; personality rights; life digitalization

■ 作者简介 张 红, 武汉大学法学院教授, 湖北 武汉 430072;
叶竞欧, 武汉大学法学院博士研究生。

■ 责任编辑 李 媛