

特色专题

脑机接口对情报活动的赋能、现实风险与合规保护

秦长森¹, 刘舒婷²

摘要 脑机接口技术在教育、医疗等领域已经得到了广泛应用,所具有的“非接触式的信息传播”“人体机能的深度强化”“高效的数据传输”等诸多机能对于赋能情报活动开展具有一定的现实意义。通过分析脑机接口技术对于情报活动存在的具体功能,在情报活动中应用脑机接口技术会存在的现实风险,构建了从原则指导到规则锚定的合规保护机制,力求有效保障脑机接口技术在情报领域中的全面应用。此外,在应用过程中还需要坚持预防性利益保护原则、利益位阶保护原则、惩罚与奖励相结合原则,从保护个人自决权、制定隐私合规保护策略、强化情报机构的监督责任、完善数据安全审查制度、制定数据合规保护奖惩机制这5个方面,消解脑机接口技术在情报领域应用中可能面临的风险。

关键词 脑机接口;情报活动;技术赋能;风险预防;合规保护

脑机接口(brain-computer interface, BCI)作为近年来科技行业热门的新兴技术,正逐渐从医学应用延展至教育、商业,甚至是军事领域,随之而来的机遇和挑战也在各个领域中被广泛讨论。不过我国情报界或是关注了宏观层面的人工智能监管问题^[1],或是关注了微观层面的数据要素保障问题^[2],但是在关于脑机接口如何影响情报业发展,如何化解脑机接口的现实风险等中观问题上缺乏必要的学术回应。事实上,脑机接口技术与情报领域存在着紧密的耦合关系。脑机接口技术可以实现不依赖常规的脊髓与外周神经、肌肉系统,而是在脑部与外部环境之间建立一种新型的信息交流与控制通道,通过脑信号

测量隐性心理活动以实现脑部与外部设备之间的直接交互^[3]。这一底层逻辑是通过提取、分析和还原,以实现信息的识别与交互,这在一定程度上改变了情报的来源并能够丰富情报的职能。从信息论的角度来看,情报的目的是实现客体信息对主体的对称性和主体信息对客体的不对称性,进而通过信息优势获得整个对抗过程的主动权;从决策论的角度看,情报的认知对抗本质是确立和保护自己的决策体系能够有效并正确地运行,在最大限度上阻止对方的决策体系以获得正确的认知决策^[4]。由此可见,利用脑机接口技术的信号获取机能可在一定程度上提升信息获取的优势,保证情报人员更加高效地做出决策。基于脑机接口技术对情报发展可能存在的潜在机能,选择从脑机接口如何对情报业进行赋能、脑机接口的情报化发展有何风险、如何

1. 东南大学法学院, 南京 211189
2. 广东省阳春市人民检察院, 阳春 529600

收稿日期: 2024-01-04; 修回日期: 2024-05-18
基金项目: 江苏省高校哲学社会科学重大项目(2022SJZD001); 江苏省研究生科研与实践创新项目(KYCX23_0205); 四川省哲学社会科学重点研究基地——社会治理创新研究中心一般项目(SHZLYB2302)
作者简介: 秦长森, 博士研究生, 研究方向为刑法学、科技法学, 电子邮箱: qinches@seu.edu.cn
引用格式: 秦长森, 刘舒婷. 脑机接口对情报活动的赋能、现实风险与合规保护[J]. 科技导报, 2025, 43(4): 67-74; doi: 10.3981/j.issn.1000-7857.2024.01.00044

对未来的脑机接口产业进行合规保护这3个方面展开讨论。

1 脑机接口如何实现对情报活动的技术赋能

伴随人脑科技的发展,脑机接口已经能够应用于多个情报领域,无论是情报信息的获取,还是情报内容的设计,抑或是情报行动的完善等均具有更为优越的现实功能。

1.1 脑机接口技术在情报领域的具体应用

现代情报的技术发展态势是IT(信息技术)工具和人工智能分析的结合^[5],这与脑机接口以提取人脑信号,再进行数据分析的行为模式十分契合。未来的情报业可以利用脑机接口技术在多个领域展开深入研究。就军事情报而言,脑机接口技术可以创造性地对人类的认知、情感和记忆进行本质性改变,以实现人类能力的跨越式增强。一方面,使用脑机接口的生物介入技术可以直接提高受伤现役军人的生活质量,减少残疾对个人、财政和社会的影响,以便有更多的士兵能够更好地获取有效情报^[6]。另一方面,脑机接口本身也能成为情报传播的工具,促进情报在战场上的有效传播。早在10年前,美国五角大楼的DARPA部门就曾发起“无声语音”计划,通过开发非声学脑机接口传感器,实现战场上用户之间的通信,以便能够消除对任何发声或肢体动作的影响^[7]。美国近年来利用“人机交换技术”促进情报信息的融合化与情报分析的计算化,在不断精进的智能化军事行动中获取了更大的主动权^[8]。可以预见,未来军事领域中将会出现大量脑机接口技术来增强指挥作战的效能从而减少战争带来的伤亡,因此,我国的军事情报发展也需要及时引进脑机接口技术,在伤员救治、信息交换、信息传播等方面促进情报业的进一步发展。

就公安情报而言,我国可以利用脑机接口技术辅助犯罪预防。犯罪问题是影响社会发展的核心问题,若要谋求行之有效的刑事政策,正确把握犯罪形势是不可或缺的前提^[9]。无论是事前的犯罪预防还是事后的犯罪侦查,均需要大量精准有效的情报。事实上,为了有效应对社会精细化发展带来的犯罪问题,我国公安机关已经开始重视建设“信息工作基

础化,基础工作信息化”的工作机制,同时也加重了公安民警信息采集的任务^[10]。但是这种采集信息的方法只是通过对犯罪的事后性反应来阻止犯罪,然而脑机接口技术却可以通过发挥情感的探知功能,在事前实现对犯罪的预防。有研究发现,精神障碍和暴力可能源于个人生活的压力水平,精神失常有可能增加犯罪的概率^[11]。由此,便可以通过应用脑机接口技术对特殊群体的精神状况进行修复,以达到降低犯罪可能性的目的,这种从源头上预防犯罪的办法无疑能够最大程度防止犯罪的发生,同时也能避免适用刑罚措施而带来的惩罚风险。此外,在刑事侦查中使用脑机接口技术,也能更好地辅助侦查人员实现对情报的搜集,以便能够更好地掌握刑事证据。

就竞争情报而言,企业可以利用脑机接口技术分析用户的价值偏好,进一步提高竞争胜出的概率。竞争情报的生命力在于使用性与价值性,竞争情报必须要结合企业的运营特点,帮助企业解决问题,为企业在惊涛骇浪的商海中把握方向,规避风险^[12]。事实上,实务中的一些信息科技公司已经研发出可以对消费者的消费目的进行检测的脑机接口设备。例如,Facebook公司早在2017年就开启了脑机接口研究计划,通过产学研融合制造可穿戴式的脑机接口设备。这些设备可以物联网的形式与其他设备互联,并在用户购物时对不同产品产生的大脑信号进行记录,以便识别用户的情绪和态度^[13]。又如,消费神经技术、电子学习、情感计算、神经营销等均是利用大脑数据作为商品的一些应用领域^[14]。脑机接口的商业化应用使脑机数据置换为商业情报成为可能,通过对这些商业情报进行算法挖掘,无疑能够提高商业情报对企业各方面的决策支持力度,促进业绩改善与加强风险管理^[15]。

1.2 脑机接口技术之于情报发展的现实功能

对于脑机接口技术是否可以全面地应用在情报的各个领域中,有待进一步探索,但仅对上文列举出的军事情报、公安情报、竞争情报中的脑机接口应用展开类型化分析,便可发现其对情报领域的发展至少具有如下功能。

第一,拓宽信息的获取来源。信息与情报有着密切的耦合关系,从某种意义上来看,信息是情报发

挥功能的重要前提,甚至有学者直言“情报就是信息”^[16]。在现代社会中,倘若能够掌握大量信息,特别是精准信息,便能在情报的认知对抗中占据更大的优势,因此收集数据、识别信息、分析信息对获取情报而言至关重要。脑机接口能够改变过去对信息传播媒介的依赖路径,通过提取人脑信息,再进一步识别和分析,就能够实现信息的无声传导、情感的现实测定、机械的远程操控等多功能情报对抗实践,提升情报信息在主客体对抗中的转移效率。如我国学者所言:“情报信息的搜集,在不违反法律和道德的前提下,可以采取一切手段,动用一切能够利用的工具,利用一切能够调用的资源”^[17]。因此,我国情报领域也应当积极引入这一情报信息的搜集方法,力争在全球竞争激烈的国际环境中,实现跨越式的发展。

第二,提升情报行动的安全。保障情报对抗中的安全是情报发展的必要条件,而完整情报活动的核心在于主客体之间的对抗。因此,只有设计出合理的情报行动,才能在一定程度上减少对抗过程中发生的危险。由于脑机接口技术可以实现用户静默表达过程中的信息传播,隔绝主客体之间的直接接触,这无疑能够提升情报主体在主客体之间的对抗优势,在安全保障上实现更好的发展。例如,在反恐情报行动中,情报之间的传递往往需要利用一定的媒介才能开展,物质化的媒介往往具有有形性,一旦被客体发现,不仅情报获取难以实现,对情报主体的生命安全也会造成一定程度的威胁。然而,基于脑机接口介导的读心术或是心脑互译技术,可以通过脑信号解码或是翻译出其心中所想的内容,实现心与心的直接沟通^[18]。这种不依赖物质传播媒介,而直接利用人脑数据实现思想的数据传播,在目标识别、情报搜集、情报分析等相关行动上都能实现静默的表达,由此提升对情报主体更好的保护。

第三,增强情报分析的可信度。情报分析是情报活动的目的,只有提升情报的质量,才能促进情报分析的真实可信度。在大数据时代,数据成为情报分析的主要载体,如何在海量的数据中筛选提炼出所需要的数据,成为增强情报分析可信度的关键。在传统的数据分析模式中,情报人员需要对数据进行入库处理,在此基础上利用算法技术进行情报的提炼。反观脑机接口技术的应用,不仅可以实现人

脑与计算机信息系统的直接相连,在一定程度上避免人工数据处理中可能造成的错误,还能将情报人员从繁重、低级、可重复的数据任务中解放出来,从源头上保证样本数据的真实性,同时也可情报人员提供更多的思考时间。

2 脑机接口技术情报化发展面临的现实风险

科技的发展既是机会的来源,也是风险的来源。尽管脑机接口技术对于赋能情报业的发展具有多重功能,但同样也会带来一些现实的技术风险,只有对这些技术风险进行识别,才能提供更加科学有效的保护方案。具体而言,对脑机接口应用风险的识别可以从伦理风险与法律风险2个层面展开。

2.1 脑机接口技术情报化发展的伦理风险

伦理学是关于道德好坏的价值科学,是关于优良道德的科学^[19]。从伦理学视角审视脑机接口在情报领域的应用风险,就是要考虑脑机接口的情报化发展存在哪些影响社会道德的因素。因此,伦理风险可以说是脑机接口产生的直接风险,主要表现在人体安全风险、自由意志风险和身份认同风险3方面。

就人体安全风险而言,脑机接口应用可能会对人体安全产生不利影响,损害身体健康。按照脑机接口植入人脑深浅的不同,可以将脑机接口分为非侵入式脑机接口与侵入式脑机接口,前者只是将电极与大脑表皮相连,后者则需要将电极通过手术的方式植入到大脑皮层中。显然,后者的手术行为极有可能对人脑造成创伤。有研究表明,医学临床中使用脑机接口,在植入电极之后可能会带来排斥反应,引起大脑的损伤^[20]。目前,脑机接口芯片的寿命最长为1 a左右,如何避免长期安放在人脑内的电极被腐蚀,脱离预定位置等问题仍未得到解决。对于一些由于手术而导致的创伤、出血、感染等问题,尚且可以利用法律手段进行保护,但因脑机接口设备而带来的神经退化、神经衰弱等问题却常常由于因果关系的难以认定,而处于不被保护的状态。

就自由意志风险而言,过度依赖脑机接口技术会控制人类情感的正常表达,是对人的尊严的漠视。一般认为,自由意志是一种个人不受他人控制或干涉,也不妨碍个人做出有意义选择的自由和行为能

力^[21]。囿于脑机接口技术可以通过对大脑的生物电信号进行分析,识别人类的情感,对于一些使用者不愿意透露的情绪,也极有可能通过这种手段被外泄,这无疑是对个人意志的限制。此外,根据医学伦理的基本要求,在对受伤情报人员使用脑机接口医疗技术时,需要获得情报人员的知情同意,而脑机接口技术可以对人类的神经系统进行干预,如何判断知情同意表达的有效性依然是一个悬而未决的难题。如果人类的情绪被脑机接口所主宰,便会犹如机器中的某个零件按照设计好的程序进行运转一样,人类作为具有自由意志的设计者最终将沦为“数据机器的奴隶”。

就身份认同风险而言,脑机接口的过度应用会导致人与机器的区别在实验中逐渐变得模糊,影响人类对自我的了解。脑机接口所连接的人类大脑,是人所存储记忆、预设创造、情感控制的核心,同时也是人类自我认同的来源。无论是利用脑机接口来增强自身的能力,还是利用脑机接口来治疗疾病,都会导致自我同一性的混乱。例如,在康复治疗中,被试者参与治疗的动机是让身体更完整、实现有效沟通和运动,如果治疗在短时间就产生了突出效果,这虽然是理想的变化,但也可能会由于突然的改变而造成身份认同的困难^[20]。这种假设已经在实践中得到了印证,有研究发现,一位使用大脑刺激治疗抑郁症的患者,在后续使用的跟踪报告中对于“我是谁”倍感疑惑,他开始怀疑与其他人交往的方式到底是自己控制的,还是由他所佩戴的设备所实现的^[22]。试想,倘若人类的认知不由大脑控制,而是通过算法反馈进行调节,这必然会影响,甚至破坏人类的自我认知,阻滞人类对自我存在的肯定。

2.2 脑机接口技术情报化发展的法律风险

伦理以人作为主体,而法律则以人类之间的关系为对象^[23]。脑机接口技术的情报化发展除了会带来伦理上的风险外,还会在法律系统中引发诸多问题。根据脑机接口的技术特征,当前技术应用的法律风险主要表现在“隐私泄露风险”和“权利滥用风险”2个方面。

在过去,隐私问题只是一个伦理学层面的问题,但随着社会人口的激增与信息传播的加速,隐私保护逐渐成为一个法律问题。《中华人民共和国民法

典》第1032条之二规定:“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”,脑机接口的情报化应用无疑会对当前的隐私权保护制度带来冲击。一方面,人脑的结构属于人类身体中最私密的空间,人脑的想法通常而言不具有可探知性与可识别性,但脑机接口技术通过采集脑电信号并进行信息分析,能够识别出人类的意识和想法。实践中已经出现通过对大学生脑电信号的采集,来分析是否存在熬夜等相关健康风险的案例^[24]。如此,人脑内部的活动便会被外界所探知,私密性也将不复存在。另一方面,脑机接口技术的过度应用会引发不正当竞争,导致普通民众的隐私权保护受到威胁。情报的核心是运用各种手段和方法获取信息,然后整合知识对信息进行分析、理解、汇总,并形成一定形式的报告,报送给相关人员^[25]。当然,信息的获取需要受到法律的控制,除了要在获取目的、获取行为上具有正当性外,还需要考虑获取信息之后是否会造成不当的后果与影响。脑机接口技术的商业化应用虽然可为企业提供大量的数据,但脑电信号监控的思想读取逐渐将人脑中的隐私透明化,行为性格隐私、健康隐私、神经数据的泄露都将会导致用户的隐私权受到伤害^[26]。

除了“隐私泄露风险”之外,脑机接口技术对人类行为能力的增强也可能沦为不法分子滥用权利的工具。现代法治国家虽然赋予了公民众多的权利,但自我权利的行使不得危及或危害他人的权利,否则就会存在侵权,甚至犯罪的风险。例如,在未告知用户使用脑机接口技术可能存在何种潜在风险的前提下,直接使用该技术就会导致用户的权利无法得到保障,一旦商业领域和政治领域利用脑机接口技术制造虚假的用户体验,就极有可能导致用户被潜意识操控而又无法识别。又如,侦查人员在使用脑机接口技术获取情报时,也可能通过滥用脑机接口技术获取非法证据,导致犯罪嫌疑人的正当权利得不到有效保障。再如,若有人为了获得有效情报而强迫他人使用脑机接口技术,使用者的权利应当如何救济,这在当前的法律体系下仍不明确。除此之外,当脑机接口设备出现故障产生错误的指令,导致使用者出现危害他人的行为时,如何在事后进行追责也成为较为棘手的问题。凡此种种,除了脑机接

口技术本身会产生一定程度的风险外,还在于当前的理论研究与情报实践对脑机接口技术本身缺乏必要的规制策略。

3 脑机接口技术情报化发展的合规保护机制

脑机接口技术的出现在赋能情报活动的同时,也会存在诸多的现实风险,如何消解这些风险便成为未来情报工作研究的重心。就此而言,本文建议引入“企业合规”的预防化思维,从组织体内部克服应用脑机接口技术带来的各种问题。“企业合规”是指企业或者其他组织体在法定框架内,结合自身文化、组织性质以及组织规模等特殊因素,设立的一套违法及犯罪行为的预防、发现及报告机制,并最终形成组织体的守法文化^[27]。在图书馆界,已有学者提出:“依据社会现实的变化需求,建立具有流动性的未成年读者信息隐私权保护机制”^[28]。显然,这是针对图书情报领域中的一个具体维度而建立的专项性合规。对于情报界而言,当务之急是建立整体性的合规保护机制来进行应对在诸多应用场景中展开所带来的潜在风险。因此,本文选择从“原则设定”与“规则厘定”2个维度,对脑机接口情报化发展的合规保护机制进行建设。

3.1 合规机制确立的基本原则

脑机接口技术对情报工作赋能的前提是保障技术应用的安全性与有效性,对于合规机制原则的设计也需要围绕着安全性与有效性来展开。结合脑机接口所产生风险的特点,本文建议在情报组织的合规机制建设中确立如下保护原则。

第一,预防性利益保护原则。合规机制的有效性在于具有对现实风险的预防机能,因而预防性利益保护原则应当成为检验合规保护机制有效性的基本原则。预防性利益保护是指通过在事前建立对风险的预防措施,以防止风险发生时带来的危害后果。虽然目前尚未有实证数据证明脑机接口技术的情报化应用在多大程度上会带来上文所指出的风险,但这些伦理维度与法律维度的风险一旦出现,对于受害者而言便是难以修复的伤害。因此,预防性利益保护原则所针对的对象,一定是在脑机接口情报化应用中处于受害的一方,是以被害方为本位的预防

保护。在此基础上,可以根据被害利益主体的不同,进行区分性的预防保护。对于个人利益的保护而言,脑机接口的制造商、情报获取的需求方应当综合采取一系列必要的措施来保障使用脑机接口主体的合法权益;对于社会利益和国家利益而言,则需要脑机接口制造商、情报获取需求方、脑机接口使用主体采取更加有效的措施,防止由于自身行为不合规所带来的法律问题和伦理问题。

第二,利益位阶保护原则。该原则是指在科技应用中,通过对科技应用所涉及的利益进行识别与衡量,并按照利益的位阶顺序进行平衡保护。因而也可以认为,该原则属于促进合规保护效率的基本原则。根据该原则的要求,在情报活动中应用脑机接口技术时,需要先对技术风险侵害的利益进行衡量,进而将现有的保护措施有针对性地落实到风险预防的每一个实处。不仅如此,当高位阶的利益与低位阶的利益发生冲突时,必须要以高位阶的利益保护为核心,绝不能以牺牲高位阶利益为代价来保护低位阶的利益。一方面,在我国,“以人民为中心”是中国式现代化的核心价值取向^[29]。当脑机接口的应用出现在社会利益与公民个人利益发生冲突的场合,绝不能以保护公共利益为由而牺牲公民个人利益。另一方面,我国的国家利益与公民个人利益息息相关,有机统一,脑机接口的应用也不能以保护商业利益和社会利益为名来牺牲国家利益,否则脑机接口的情报化应用便不具有正当性基础。

第三,有效激励原则。在情报组织体内部建立合规保护机制,必须要提升成员开展合规机制建设的动力,否则上文中的预防性保护与利益位阶保护都将成为空谈。实际上,单纯的奖励与惩罚均不能提升组织体内部实施合规计划的动力,如果没有一定的激励机制,员工就会存在普遍消极怠工的行为,如果单有奖励没有惩罚也会导致组织体内部出现越轨行为。有研究表明:“自愿的惩罚与奖励往往是用来维护合作的机制,而惩罚与奖励往往在生产合作是相辅相成的”^[30]。因此,在该原则的指引下,情报机构应当在组织内部建立一套完整的激励措施体系,对于注重进行合规审查的员工要进行奖励,而对于不注重合规保护,甚至由于故意或过失而出现权益侵害后果的,要采取一定的惩罚措施,促使员工努力

修复被不当使用脑机接口技术而损害的利益。

3.2 合规机制建立的具体规则

情报组织如果想要化解脑机接口技术的应用风险,需要结合上文确立的基本原则,在此基础上审视当前的整体法秩序在脑机接口应用上的着力点,将其融入到组织体内部的合规计划中,从守法的角度实现对技术应用的预防性保护。对此有如下建议。

1) 根据利益位阶保护原则的要求,构建保护使用者个人自决权的具体措施。按照该原则的要求,使用者的个人权益应当属于保护利益的第一位阶,需要受到首要保护。只有在使用者真实、充分了解脑机接口设备的性质、作用、损伤、风险等相关信息的前提下,经过深思熟虑自主做出选择,明确承诺意愿后,才能使用这一设备。据此,可以总结出以下2条具体的规则。第一,如果情报主体在知道使用脑机接口设备可能会带来哪些不利后果后,明确拒绝使用的,便不能以获取情报为由强制使用。第二,企业在出售脑机接口设备时,必须要向消费者明示可能存在的风险,对于消费者拒绝提供的数据信息,不能因为具有竞争情报的价值就违背其意愿进行收集。这便要求情报主体必须要向使用者提供具有可理解性的知情措施,并且只有在接收到使用者明确且肯定的回复后,才能允许其使用脑机接口设备。

2) 立足《中华人民共和国民法典》对隐私权的保护要求,制定预防性隐私合规保护策略。《中华人民共和国民法典》对情报组织提出了隐私保护的要求,该法第1032条明确规定了保障自然人所享有的隐私权,并在第1033条中以“列举+兜底”的方式规定了侵犯隐私权的具体行为类型。然而,脑机接口的使用并不满足“列举类型”的条件,只能通过法律解释将其理解为“以其他方式侵害他人隐私的行为”。根据法律同类解释的要求,只有行为方式具有同质性、利益侵害具有相当性的行为^[31],才能满足“兜底条款”的同类解释规则。因此,对于应用脑机接口技术是否会侵犯公民隐私权的判断,应当着重考察该行为的利益侵害性是否与民法典明示列举的行为类型具有相当性。结合《中华人民共和国民法典》第1032条的明示规定,笔者建议情报组织可在具体的合规计划中至少采取如下策略:第一,情报活动中脑机接口产品不能应用于情报活动之外,否则难以有效保障

使用者的私人生活安宁;第二,在非国家间的竞争情报环境中,脑机接口的应用不能涉及他人的私密空间;第三,对于他人的人脑数据,必须进行去识别化处理。

3) 根据《国家情报法》对情报活动的保障,强化情报机构的监督责任。《国家情报法》是开展国家安全情报工作的总章程,在国家情报活动中应用脑机接口技术必须要满足该法对情报活动的具体要求。事实上,该法第8条已经明示了国家情报工作的核心准则,即尊重和保障人权。这意味着,在国家情报工作中,所有脑机接口技术的应用都必须满足人权保障的要求。本文认为,国家情报机构对于脑机接口使用者人权的保障,需要发挥其基本的监督职能。进一步来说,国家情报机构要充分监督脑机接口生产商的行为,防止在产品使用的源头上出现危及用户基本人权的情形。一方面,国家情报机构需要及时采取对生产商算法优化的监管措施。为了实现技术应用与风险规制的平衡,国家情报机构可在保守商业秘密的情况下,敦促脑机接口生产商对算法的内容进行公开及解释,实现算法的公正透明,保障算法正义^[32]。另一方面,国家情报机构可以引入“专业的第三方”对脑机接口生产商的活动进行监督,并授权其实质地参与到脑机接口生产的全流程监管中,避免因情报机构不懂技术原理而出现生产商的瑕疵性隐患。同时,“专业的第三方”也需要给予情报人员在设备使用上的必要说明和指导,避免因情报人员不懂使用原理而出现利用上的风险。

4) 依据《数据安全法》的要求,完善数据安全预防性审查制度。《数据安全法》是规范数据处理活动的专业法,脑机接口技术的情报化应用离不开对人脑数据的处理,因此也需要吸收《数据安全法》对数据安全审查的要求。该法第24条规定:“国家建立数据安全审查制度,对影响或者可能影响国家安全的数据处理活动进行国家安全审查。”显然,《数据安全法》是站在总体国家安全观的高度对数据安全保障提出的要求,情报机构在开展合规建设时,可以将数据安全审查制度进一步完善,从多个层面保障国家数据安全。相关的合规制度设计可以从以下几个方面展开。第一,在源头上对脑机接口生产商的资质进行审查。情报组织要主动防止出现因企业资质不

健全,而引发的脑机接口产品安全问题。第二,在条件上对人脑数据的储存环境进行审查。对人脑数据进行分析的前提是有效储存人脑数据,情报组织必须加强对数据存储环境的审查,防止出现人脑数据泄露或数据库被黑客攻击的情形。第三,在目的上对使用人脑数据的原因进行审查。通过脑机接口技术提取并分析的人脑数据,必须在目的上有利于情报工作的开展,而不能以其他目的收集或处理。第四,在国际交流中对人脑数据跨境流动的必要性进行审查。当情报机构通过交换人脑数据才能获得情报时,必须要考量人脑数据跨境流动可能带来的后果。亦即,只有在数据不流动会造成重大不利后果时,才能在保障各方利益的前提下,适当地允许人脑数据的跨境流动。

5) 按照有效激励性原则的要求,制定数据合规保护的奖惩机制。在情报组织内部中必须要形成“合规则生,不合规则亡”的文化氛围,保障合规机制的有效运行。否则,即便建立了十分完善的合规机制,倘若不能得到有效遵守,也只能是流于形式。在合规惩罚机制的建立上,情报组织有必要将合规义务的不履行分为合规保障不到位与安全监管职责不履行2个方面。前者是指情报工作人员虽然履行了相关的合规保护义务,但有关做法不够完善,存在继续提升的空间;后者则是指情报工作人员故意不履行合规义务或者怠于履行合规义务,存在巨大的安全漏洞。显然,后者的危害性要远大于前者,对于后者的惩罚力度也须大于前者。本文建议,对于前者的惩处可以通过批判、教育、警示,限期改正的做法来敦促情报人员进一步完善工作机制,对于后者则必须要在职务晋升、奖金评定等方面予以限制,必要时可以采取开除等更为严厉的措施。在合规奖励机制的建立上,情报组织可以通过技术合规竞赛、技术合规保障互评等形式,对表现良好的员工在职务晋升、奖金评定上给予鼓励和优待。总之,一旦将脑机接口技术应用在情报活动中,情报组织便需要采取各种措施,来保障内部合规机制的有效执行。

4 结论

情报工作本身会随着时代的发展发生改变,情

报学理论研究要站在时代的最前沿,审视技术对于情报活动的赋能及其规制。脑机接口技术作为热门技术,在信息的获取、传播以及人体机能的强化等方面有着得天独厚的优势,完全可以引入到情报活动中促进情报工作更好地开展。当然,情报组织也需要理性地审视应用脑机接口技术可能存在的风险,通过研判和审视风险的来源、种类及样态,积极在组织体内部建立体系化的合规机制来应对,如此才能最大程度地实现脑机接口技术在情报领域的全面应用,促进情报工作的科技化、智能化发展。

参考文献(References)

- [1] 刘轩, 陈海彬. 人工智能监管:理论、模式与趋势[J]. 情报理论与实践, 2023, 46(6): 17-23.
- [2] 邹纯龙, 马海群, 王今. 面向全国统一大市场的数据信用体系构建研究[J]. 情报理论与实践, 2023, 46(7): 44-50.
- [3] Lebedev M. A, Nicolelis M A. Brain-machine interfaces: Past, present and future[J]. Trends in Neurosciences, 2006, 29(9): 536-546.
- [4] 赵冰峰. 情报学:服务国家安全与发展的现代情报理论[M]. 北京:金城出版社, 2018: 146.
- [5] 黄斌. 现代情报服务与技术发展趋势[J]. 现代情报, 2013, 33(12): 37-40.
- [6] Kotchetkov I S, Hwang B Y, Appelboom G, et al. Brain-computer interfaces: Military, neurosurgical, and ethical perspective[J]. Neurosurgical Focus, 2010, 28(5): E25.
- [7] Denby B, Schultz T, Honda K, et al. Silent speech interfaces[J]. Speech Communication, 2010, 52(4): 270-287.
- [8] 王天尧, 吴素彬. 迈向智能化的美国军事情报工作发展研究[J]. 情报杂志, 2020, 39(3): 1-7+80.
- [9] 川出敏裕, 金光旭. 刑事政策[M]. 钱叶六, 译. 北京: 中国政法大学出版社, 2016: 7.
- [10] 彭知辉. 论公安情报分析与大数据分析的融合[J]. 情报理论与实践, 2017, 40(10): 36-40.
- [11] Anderz D O, Kanjo E, Amnwar A, et al. The rise of technology in crime prevention: Opportunities, challenges and practitioners perspectives[J]. arXiv preprint arXiv: 2102.04204, 2021.
- [12] 张世平. 走出竞争情报误区 构建企业竞争情报系统[J]. 情报理论与实践, 2010, 33(6): 65-68.
- [13] Ienca M, Fins J J, Jox R J, et al. Towards a governance framework for brain data[J]. arXiv preprint arXiv: 2109.11960, 2021.
- [14] Insel T R. Digital phenotyping: Technology for a new science of behavior[J]. Jama, 2017, 318(13): 1215-1216.
- [15] 李宝虹, 白建东, 张会来. 基于数据驱动的企业商业情报

- 管理[J]. 情报科学, 2014, 32(8): 20-26.
- [16] 程琳. 情报与现代信息关系[J]. 管理观察, 2017(36): 19-21+23.
- [17] 许鑫, 柯健等. 竞争情报分析方法及应用[M]. 北京: 科学技术文献出版社, 2021: 19.
- [18] 肖峰. 脑机接口与他心通达[J]. 哲学分析, 2023, 14(2): 114-127+198.
- [19] 王海明. 伦理学定义、对象和体系再思考[J]. 华侨大学学报(哲学社会科学版), 2019(1): 26-48.
- [20] 李佩瑄, 薛贵. 脑机接口的伦理问题及对策[J]. 科技导报, 2018, 36(12): 38-45.
- [21] 郭华, 田雯, 刘星. 脑-机接口对个人自主的挑战与哲学反思[J]. 中南大学学报(社会科学版), 2020, 26(5): 190-198.
- [22] lein E, Goering S, Gagne J, et al. Brain-computer interfacebased control of closed-loop brain stimulation: Attitudes and ethical considerations[J]. Brain-Computer Interfaces, 2016, 3(3): 140-148.
- [23] 阿图尔·考夫曼. 法律哲学[M]. 刘幸义, 译. 北京: 法律出版社, 2011: 233.
- [24] 曹锦丹, 钟玉骏, 姚艺倍, 等. 健康风险认知过程中的信息框架效应及其神经活动特征分析[J]. 情报科学, 2022, 40(10): 26-32.
- [25] 化柏林. 论情报的本质[J]. 情报理论与实践, 2012, 35(7): 1-5.
- [26] 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.
- [27] 李本灿. 企业犯罪预防中合规计划制度的借鉴[J]. 中国法学, 2015(5): 177-205.
- [28] 秦长森. 数字时代图书馆未成年读者信息隐私权保护路径研究[J]. 西华大学学报(哲学社会科学版), 2023, 42(3): 30-39.
- [29] 余永跃. 以人民为中心: 中国式现代化的核心价值取向[J]. 人民论坛, 2024(4): 46-50.
- [30] Andreoni J, Harbaugh W, Vesterlund L. The carrot or the stick: Rewards, punishments, and cooperation[J]. The American Economic Review, 2003, doi: 10.1257/000282803322157142.
- [31] 俞小海. 论刑法同类解释规则中的“同类”[J]. 法学家, 2023(2): 60-73, 192-193.
- [32] 徐智华, 解彩霞. 算法逻辑下平台从业者权利保护的危机及应对[J]. 西安交通大学学报(社会科学版), 2022, 42(1): 155-162.

Brain-computer interfaces enabling intelligence activities, real risks, and compliance protection

QIN Changsen¹, LIU Shuting²

1. School of Law, Southeast University, Nanjing 211189, China

2. Guangdong Yangchun City People's Procuratorate, Yangchun 529600, China

Abstract As a mainstream technology in new era, brain-computer interface has been widely used in education, medicine, and other fields, and its many functions such as "non-contact information dissemination", "deep reinforcement of human body functions", "efficient data transmission", etc. are of profound practical significance for enabling the intelligence activities. By analyzing the specific functions of brain-computer interface technology for intelligence activities and the real risks of applying brain-computer interface technology in intelligence activities, a compliance and protection mechanism that ranges from the guidance of principles to the anchoring of rules was constructed, to effectively safeguard the comprehensive application of brain-computer interface technology in the field of intelligence. In addition, it is necessary to adhere to the following principles: preventive interest protection, interest level protection, and combination of punishment and reward in the process of application, and the risks that brain-computer interface technology may face in the application of intelligence field can be eliminated from the following five aspects: protection of individual's right to self-determination, formulation of privacy compliance protection strategy, strengthening of the supervision responsibility of the intelligence organization, improvement of data security review system, and the formulation of the rewards and punishments mechanism for the protection of data compliance.

Keywords Brain-computer interface; intelligence activities; technology enablement; risk prevention; compliance protection ●



(责任编辑 卫夏雯)