



法治日报

星期三
2025年6月11日

法学院

09
专刊

编辑/刘秀宇
主编/李晓军
校对/张胜利

LEGAL DAILY

避风港原则对网络服务提供者刑事责任的限制

前沿聚焦

□ 张燕龙

传统上对网络服务提供者的刑事归责使用“明知+帮助”标准,司法上从严打击、立法上多入罪,给网络服务提供者带来了巨大的刑事责任风险。避风港原则可以发挥责任限定作用,对一味从严的规制模式进行适当调节。然而,避风港原则过时论不绝于耳,其本身也面临巨大挑战。避风港原则在当今时代依然值得坚守,对于其在司法实践中出现的问题,可以通过教义学的方法予以克服,经过升级改造的避风港规则体系作为网络侵权的基石条款,在刑法领域依旧可以发挥重要的责任限制功能。

避风港原则刑事责任限制功能的削弱

(一)适用空间的压缩
避风港原则适用于间接侵权行为,对于网络服务提供者直接侵权的行为并不适用,可以借鉴这一规则来解释网络服务提供者的刑事责任。随着数字技术的发展,网络服务提供者实行行为的边界更加模糊,正犯与共犯、直接侵权与间接侵权的区分愈加困难,司法机关往往倾向于以正犯来认定。司法实践中体现出来的实行行为类型模糊、共犯正犯化解解倾向明显存在问题,不仅直接架空了避风港原则,而且产生出口袋罪嫌疑。

(二)限定规则的异化
网络服务提供者的归责适用过错责任原则,“通知—删除”中的通知与“红旗规则”推定的意义相同,都可以用来证明网络服务提供者主观明知(知道或应知)。同时,网络服务提供者承担间接责任,与此相关的三种行为类型经过我国刑事司法实践的转换,集中体现为帮助行为。然而,传统网络服务提供者的角色随着技术的发展发生变化,参与度提高且参与时间前移,认定其明知的标准难以把握。同时,网络服务提供者对直接侵权事实的明知本是一种具体的明知,但实践中的要求越来越宽泛,成为一种概括、抽象的明知。此外,推定在司法实践中也有异化的倾向,不断呈现出义务化要求的趋势。

(三)平台义务的提升
在网络服务提供者符合一系列较为严苛的

条件之后,免除其赔偿责任,将其从普遍的、主动的审查义务中解放出来,是避风港原则的精髓。如今,随着利益平衡的变化,要求网络服务提供者主动作为的呼声越来越高,作为的标准也水涨船高。这种做法将网络服务提供者作为的时间提前,作为的强度提升,进一步削弱了避风港原则的责任限制功能。

对避风港原则的刑事政策选择

(一)避风港原则面临的质疑

对避风港原则的质疑集中体现在三个方面:一是平台的作用凸显,利益平衡进一步被打破,避风港是否还有“根”。我国民法典原则上认同网络服务提供者不承担审查义务,但又认为需要促使网络服务提供者适当履行监管义务。作为最后手段的刑法究竟要如何平衡各方利益、分配义务,是否还需要维持现有的局面、坚持避风港原则,实属首要难题。二是法律的供给难以满足打击犯罪的效率要求,各方均不堪重负,避风港是否还有“力”。避风港制度的运行效率受到了各方的诟病,避风港制度带有期待网络服务提供者与权利人能够合作共同打击盗版的初衷,但如果在此规则体系下盗版始终得不到遏制,就会逐渐侵蚀避风港原则的根本。三是新的网络服务提供者主体涌现,呼唤新的治理规则,避风港是否还有“货”。随着技术的发展,大量混合型平台开始出现,已经很难将其归入避风港最初设定的四类主体中。此外,全新的网络服务提供者主体开始进场,生成式人工智能成为生成内容的服务提供者,彻底混淆了之前内容与服务的区分标准,导致规则适用的混乱。

(二)我国的刑事政策选择

虽然避风港原则面临重重挑战,但现在提避风港过时论言之过早。首先,无论是从民法典中还是参加的国际条约来看,我国都选择了维持现有的利益平衡局面,继续坚持避风港原则。其次,现有要求变革的理由并不充分。避风港过时论的实质观点认为,平台技术的进步使得网络服务提供者有能力更好地处理在线盗版事宜,因此要进行平衡,加重其责任。但这样会逼迫其出台更高级别的监管技术,不断抬高整个行业的准入门槛,扼杀大量的中小网络服务提供者。此时,权利人反而会更加依靠大型网络服务提供者,要求其承担更大的责任。最后,对网络服务提供者的刑事归责也应当做到宽严相济。“严”主要体现在立法中,从技术改变带来的利益再平衡出发,作出

刑事政策选择;“宽”则主要体现在司法中,通过对避风港原则进行刑法教义学改造来实现。总之,坚持避风港原则就是我国现行法律的基本选择,也是符合国情的应然选择。

对避风港原则的刑法教义学改造

(一)网络服务提供者安全保障义务的限缩
经过避风港原则的梳理,可以将民法与刑法中网络服务提供者的义务条款予以贯通,合理界定打击范围。首先,审查义务的否定是避风港原则及民法典的基本要求。民法典第一千一百九十七条中“必要措施”的规定依旧在避风港原则的框架之内,不能成为要求网络服务提供者履行审查义务的依据。其次,不宜在网络服务提供者的刑事责任中提倡监管义务。应当强调的是其事后、被动的“管”的义务,而不是事前的、主动的“监”的义务。再次,注意义务具有迷惑性,也不宜成为网络服务提供者刑事责任的依据。注意义务容易脱离其原本的应用场景,且缺乏明确性,实践中据以判断注意义务的规范往往层级较低,不宜作为刑法上的义务来源。最后,应当对民法典第一千一百九十八条进行教义学解读,提倡网络服务提供者负有限缩了的安全保障义务。

(二)帮助行为的实质非侵权认定及责任区分

准确界定行为是认定犯罪的前提,对网络服务提供者帮助行为的认定应当遵守以下规则:一是维持二分法的基本框架,在避风港原则设立了间接责任、过错责任之后,直接侵权与间接侵权的二分就成为制度运行的基本前提,对应到刑法上就是正犯与共犯二分的基本框架。二是对帮助行为进行“实质非侵权”认定。对其帮助行为的判断要进行全面考察,只有当违法用途明显大于合法用途时该帮助行为才具有可罚性。三是区分帮助行为的责任类型。民法典第一千一百九十七条中的“知道或者应当知道”在刑法中的应用只包括了明知且主动作为的情形,不包括明知不作为的情形。

(三)网络侵权“必要措施”条款的功能转化
可以在避风港原则的精神下对“必要措施”条款进行刑法教义学的解释,使其承担从宽功能。一是在网络服务提供者过失的情形下承担出罪功能。由于网络服务提供者没有普遍审查的义务,不存在应当预见而没有预见他人直接侵权行为的情形,因此排除疏忽大意过失构成



犯罪的情形。当网络服务提供者预见到了他人直接侵权行为,采取了必要措施后依旧发生犯罪结果的,只构成过于自信的过失,不承担刑事责任。二是在网络服务提供者故意的情形下承担量刑从宽功能。网络服务提供者知道或者应当知道网络用户利用网络服务侵害他人犯罪而提供帮助行为的,应当承担刑事责任。但如果其已经采取了必要措施的,可以从轻或者减轻处罚。

(四)“红旗规则”对刑事推定的限制
以民法典网络侵权责任条款为依据,可以从刑法的角度重新开发“红旗原则”对于推定的限制作用。首先,有无红旗的推定是事实判断而非义务要求。同时,在刑法中应当采用比侵权法更加严苛的标准,用“红旗规则”来提高网络服务提供者“应当知道”的证明标准。其次,准确红旗的推定是行为判断而非能力判断。在推定中将网络服务提供者的“明知”与管理能力、管理义务相挂钩的做法,实质上脱离对行为要件的认定。最后,红旗有多红的推定是程度判断而非有无判断。不能认为只要有犯罪就触发了“红旗规则”,而是要达到“飘扬”的显著性,具体应以网络服务提供者所负的安全保障义务作为底线,且由于每种犯罪的社会危害性不同,这条线也应当根据犯罪类型有所区别。

(原文刊载于《政法论坛》2025年第3期)

法界动态

“涉虚拟货币犯罪的侦查、起诉和证据固定”研讨会举行



本报讯 记者**战海峰** 当前,涉案虚拟货币处置作为数字时代的新兴议题引发广泛关注。面对涉虚拟货币犯罪在侦查、起诉和证据领域带来的新问题、新挑战、新要求,亟须一场跨学科、多维度、深层次的研讨交流。近日,由西南政法大学主办的“涉虚拟货币犯罪的侦查、起诉和证据固定”研讨会举行。

西南政法大学校长林维表示,虚拟货币具有匿名性、去中心化与跨境流动等特性,滋生大量利用虚拟货币进行的新型洗钱、诈骗、贩毒等犯罪,对刑事司法形成系统性挑战,产生侦查溯源难、刑事指控难、证据固定难等难题。这些难题的解决既需要刑事实体法与程序法的协同创新,也需要法学理论与司法实践的深度融合,期待本次研讨会汇聚理论界与实务界专家的智慧,揭示议题中的真问题并提供系统性解决方案。

本次研讨会不仅为涉虚拟货币犯罪的侦查、起诉和证据固定等问题提供了可行方案,也为规范涉案虚拟货币处置程序、防控处置风险、保障处置成效提供了有益启示。

西北政法大学与甘肃政法大学战略合作框架协议签约仪式举行



本报讯 记者**孙立昊** 6月5日,西北政法大学与甘肃政法大学战略合作框架协议签约仪式暨座谈会,在西北政法大学举行。西北政法大学校长范九利、甘肃政法大学校长郑高键出席签约仪式。与会人员规模围绕学科建设、科学研究、人才培养、师资队伍、国际合作等方面展开深入交流。

范九利表示,两校签订并积极落实战略合作框架协议是全面落实立德树人根本任务,加强校际交流,促进两校高质量发展的有效实践。两校将持续深化交流沟通合作,扎实落实合作协议各项内容,互学互鉴,推动西部地区高等教育特别是法学教育高质量发展。

郑高键表示,两校将通过务实举措深度合作,加强资源共享、优势互补,共同探索创新法治人才培养模式,必将为教育强国和法治建设作出新的更大贡献。

A时代法学研究和法律职业创新与发展前沿论坛举行



本报讯 记者**黄洁** 6月7日,AI时代法学研究和法律职业创新与发展前沿论坛在北京举行。本次论坛由北京理工大学法学院、北京理工大学律师学院、北京律师法学研究会、北京市朝阳区律师协会、北京市海淀区律师协会联合主办。与会专家学者围绕“AI时代法学教育的变革”“AI时代律师行业的转型发展”“AI时代司法体系的变革创新”三个主题进行深入研讨。

北京理工大学法学院院长李寿平在总结时表示,AI时代的法学研究、司法实践与科技创新领域须深度协同,共同驱动研究范式转型与法律职业能力升级,共同推动AI发展恪守“科技向善”原则。他强调“善用”人工智能是核心关键:在能力建设上,系统掌握智能技术应用技能;在风险防控上,坚守伦理法律底线,防范技术依赖与滥用风险。必须始终以人本价值为根基,以良知和法治看护AI,引导人工智能发展航向。

本次论坛围绕人工智能背景下法学研究与法律职业的变革进行了深入探讨,有效促进了跨界对话,为智慧法治体系的构建和法律职业模式的创新提供了宝贵的启示。论坛还发布了由“法学+人工智能”本科精英班学生和北京市房山区人民检察院检察官协同打造的“社会治理检察建议智能生成助手”,深度融合法律知识图谱与神经网络算法,这是全国首次由法科在校本科生参与开发的人工智能司法应用系统。

山东政法学院召开思想政治工作和师德师风建设推进会



本报讯 记者**姜东良** 日前,山东政法学院召开思想政治工作和师德师风建设推进会。

山东政法学院党委副书记赵斌强调,思想政治工作是学校各项工作的生命线,师德师风建设是落实立德树人根本任务的重要保证,必须从严抓、长抓不懈。他就推进工作提出:要认清形势、提高站位,深刻把握思想政治工作和师德师风建设的重要性和紧迫性;要系统施策、精准发力,全面推进思想政治工作和师德师风建设提质增效;要压实责任、狠抓落实,凝聚思想政治工作和师德师风建设强大合力。

神经数据开放共享中的个人信息保护

前沿话题

□ 杨嘉祺

近年来,作为未来产业驱动引擎之一的脑机接口技术迅速发展,在医疗领域已落地应用。2025年1月,北京、上海等地接连发布脑机接口行动方案,提出建构神经数据开放共享机制的设想。对于在脑机接口技术医疗应用场景下产生的神经数据,应当采用何种形式进行利用,才能在保护好数据主体权益的前提下推动神经科学研究与技术产品研发,是当前实践与研究中亟待解决的重要问题。

神经数据之性质:敏感且私密个人信息

神经数据是一种特殊的个人数据,即便在医疗场景下产生,也与个人健康医疗数据之间存在区别,自身就应被界定为敏感且私密的个人数据。理由如下:

一是数据自身具有独特构造。神经数据由脑数据与推断数据构成,且由于人类神经系统活动与脑机接口技术系统之间处于实时交互的状态,二者是不可区分的。脑数据因可反映人体

的大脑结构、功能以及神经系统运行模式中高度的个体化差异,属于生物识别信息;经机器学习解码后的推断数据则可能反映个人的财产、性倾向、健康状况等敏感且私密的信息,这些信息的泄露有可能造成人身或财产损失,个人有权决定是否以及在多大程度上进行披露,也享有他人合理使用信息的合理期待。

二是信息内容具有多元特性。一方面,脑机接口广泛且连续地收集在有意识和无意识状态下产生的神经信号,而个人对此控制能力有限。另一方面,神经系统的多功能特性决定了大脑皮层不同功能分区中的神经元或神经元集群以分布式网络的形式参与分析多线并行的任务信息,因此同一脑区的信号可能同时反映了不同的认知状态或者行为过程。尽管脑机接口中的高分辨率传感器能捕捉、提取和转化特定脑区目标信号以取得与特定任务相关的信息,但难以隔离单一任务的神经信号。

开放共享中的个人信息危机与匿名化难题

(一)开放共享中的个人信息危机

从过往的经验来看,有关神经数据开放共享的实践始于神经科学领域。在神经科学研究与脑机接口医疗应用两个场景下,数据主体都可能面临同样的风险,但在程度上存在差别。首先,风险程度上的差别。神经科学研究场景下通过实验任务收集到的数据通常只与给定话题内容相关,但在医疗场景下患者可能与医生、护士、家人朋友或者其他访客交流,基于与人的亲密程度不同,相应的话题内容在私密程度上也存在区别。

其次,风险类型上的共性。一是重新识别风险。在神经科学研究场景下,即便开放数据通常是主题互不相关的数据集,且都已经过去识别化或匿名化处理,但若对已公开数据集进行去匿名化攻击仍可重新识别。在医疗应用场景下,神经数据通常与附加可识别性的一系列相关联的生物医学、临床数据等一起被收集,而神经数据本身具有高度的生物识别能力,导致被重新识别的风险很

高。二是数据滥用风险。在神经科学研究场景下的神经数据可以揭示雇员的健康状况、认知状态或行为特征;在医疗场景下的神经数据也可能被用于实施保险诈骗或敲诈勒索等犯罪行为。在数据利用形式上,开放数据无法限定二次利用的目的,因此已公开数据集是动态的,处于随时被以任何目的进行重新利用的状态。前述数据一旦被滥用将带来的风险至少包括针对个人的不当偏见或歧视。虽然共享数据限定了范围与数据处理目的,但接收数据的第三方可能超出目的范围处理信息或者将数据再次共享,在多次共享所形成的数据分享链条下的数据也同样面临着类似风险。

(二)神经数据的匿名化难题
匿名化是数据合理利用的重要手段,但神经数据的匿名化处理面临以下难题:

一是完全匿名化几乎难以实现。如果将不同匿名化数据集进行整合,通过算法交叉引用可能重新识别个人;如果将匿名化数据集与其他包含身份特征的已公开数据集进行交叉对比,重新识别个人的概率更高。

二是完全匿名化降低数据实用性。目前,我国主要采用去识别化的方法来保证医疗数据的实用性,以满足疾病诊断、医学研究或技术研发的需求,但去识别化技术使重新识别风险更大。

(三)神经数据匿名化难题的破解

一是增加可行的技术保护措施。在数据采集与传输环节使用联邦学习的方法,让机器学习算法在用户本地设备运行,避免因数据集带来的数据泄露与攻击风险。

二是采用动态的匿名化评估方法,对重新识别与数据滥用的潜在风险以及对数据主体造成损害的可能性谨慎地进行定期分析和评估。一旦发现存在风险现实化的可能性,就将匿名化数据转化为未匿名化数据。

神经数据的共享应强化人格权益与经济利益的保护

当匿名化标准未满足,神经数据的分享应当强化患者个人意愿与控制,由个人、医疗机

构、科研机构、产品企业等多个利益相关主体之间通过订立数据共享协议,取得个人的同意与授权许可,而不应采用开放形式。

(一)神经数据不应作为个人健康医疗数据开放共享

第一,神经数据不宜采用开放形式。开放数据无法限定二次利用目的,且极易发生个人信息泄露。第二,神经数据与健康医疗数据开放共享理念不相融。脑机接口医疗应用受众范围较小,所涉及的疾病种类并不具有传染性,不存在公共卫生风险管理的必要。

(二)神经数据共享中应取得个人同意与授权许可

第一,神经数据的共享取得个人单独同意。首先,在神经数据收集阶段应当取得个人同意。一方面,只有处理脑数据以诊断和治疗患者主诉疾病可构成医疗服务合同主要权利义务条款的内容,但处理推断数据不是履行合同所必需的;另一方面,医疗服务合同中与个人自愿使用脑机接口技术产品相关的内容属于合同意思表示,其法律性质与私密信息或敏感个人信息处理中的同意不同。其次,根据个人信息保护法第二十三条的规定,神经数据共享中的同意不同于收集阶段的同意,共享数据应重新取得个人同意。

第二,神经数据的共享若涉及商业化利用,有必要在协议中增加授权许可条款。首先,神经数据中个人信息权益与个人数据中的财产利益无法区分,是一体两面的关系。其次,同意的法律性质是违法阻却事由,而个人的授权是订立合同的意思表示,二者法律性质有别。最后,个人是脑机接口技术产品原始价值的贡献者与形成价值的参与者,有权参与经济利益分配。

需补充说明的是,关于神经数据技术处理中的成本与措施,数据泄露或滥用引发的损害赔偿等问题可通过合同进行明确约定,但对于神经数据的滥用的法律后果,并不是仅通过合同约定就可以解决的,而应考虑通过立法予以明确规制。

(原文刊载于《华东政法大学学报》2025年第2期)

