中外法学 Peking University Law Journal
Vol.31, No.6(2019)pp.1446－1468

避风港原则的刑法教义学理论建构

王华伟*

摘 要 我国网络服务提供者的刑法责任存在着结构性失衡问题，这不仅在法理上冲击着法秩序统一原理，在实践中也可能给互联网信息产业的健康发展蒙上阴影。比较研究美国和德国的情况可以发现，形成并发展于民事领域的避风港原则也应当在刑事领域得到转换适用。在我国《刑法》明确扩张网络服务提供者刑法责任的背景下，首先应当以避风港原则为基本依据，建立起网络服务提供者前刑法评价与刑法评价的位阶关系。在此基础上，应进一步将避风港原则的免责规则及其程序构造作为一般性的教义学知识资源引入犯罪论体系，妥善安排其体系性定位，结合具体罪名的构成要件从客观与主观、宏观与微观两个层面限缩网络服务提供者的刑事责任。

关 键 词 网络服务提供者 避风港原则 刑事责任 客观义务 主观罪过

一、问题提出：结构性的缺陷

避风港原则是我国版权法和民事侵权法领域被广泛探讨的问题，它的主旨在于为网络服务提供者划定一个承担侵权责任的边界。在较早期的文献中，学者们便已经开始从比较法的角度对美国《数字千年版权法案》中的避风港原则以及相关的重要判例进行了深入介绍。2006年，在国务院颁布的《信息网络传播权保护条例》中，避风港原则的相关规则被明确加以确立。2009年《侵权责任法》通过，该法第36条实际上在更宽的范围内再次确认了这一基本原则。随着这些相关民事法律规范的施行，避风港原则在民法领域的适用得到了更加深入和全面的

* 北京大学法学院博士后研究人员。本文为司法部2018年国家法治与法学理论研究项目中青年课题“信息刑法的基本原理与理论建构”(项目编号：18SFB3016)的阶段性成果并受中国博士后科学基金第12批特别资助(项目编号：2019T120003)的支持。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

探讨。但是,在刑法领域,近年引起社会广泛讨论的快播案才将网络服务提供者的刑事责任问题推到了前台。从目前的情况来看,不论是理论界还是实务界,对网络服务提供者刑事责任的边界及其认定规则并没有统一看法。与此同时,2015年通过的《刑法修正案(九)》新增加了第286之一拒不履行信息网络安全管理义务罪和第287之二帮助信息网络犯罪活动罪,由此网络服务提供者的刑法责任进一步呈现出扩张化、提前化的趋势。

然而,对于常常以信息技术革新者形象出现的网络服务提供者,一味强调其网络安全管理义务,不仅将给网络服务提供者带来沉重的负担,同时也将阻碍网络技术的发展。〔1〕事实上,以美国、德国为代表的许多西方国家都建立了一套自成体系的网络服务提供者免责模式。而反观我国,虽然民事法律领域的立法规定和理论探讨都就此问题做出了应对,但是在刑事法律领域网络服务提供者的免责事由不仅在立法上处于空白状态,在理论上也缺乏全面性、体系性的深度研究,这造成了一种网络服务提供者刑事责任问题上的结构性缺陷。这种结构性缺陷引发的直接后果在于,网络服务提供者可能在现有的法律框架内承担过重的刑事法律风险。

在传统刑法体系的框架之上,网络服务提供者的刑法责任问题还需要特别地考虑网络空间里的诸多因素,例如网络服务提供者本身的功能特征,网络服务提供者对第三方内容和行为的技术控制可能性,控制措施可能对信息自由和个人隐私带来的侵害等。避风港原则就是综合考虑以上诸多因素之后得出的一种权衡性法律结论,但是它能否以及如何在刑事领域适用,却长期没有得到学界的充分重视。正是在这样的背景下,如何使产生并发展于民事法领域、旨在合理限缩网络服务提供者侵权责任的避风港原则与刑事责任的界定相协调,如何从避风港原则的比较法经验中提炼和总结限定网络服务提供者刑事责任的教义学知识资源,成为亟需加以探讨的问题。

二、避风港原则刑法适用的比较考察

众所周知,避风港原则发源于美国的司法实践,且以成文法的形式在美国被确定下来,它创设了该规则体系的基本模型,在世界范围内产生了深远的影响。此外,早在美国的《数字千年版权法案》正式颁布以前,德国就通过了《电信服务法》,开创性地对网络服务提供者的责任进行了类型化限缩,为欧洲各国提供了立法上的典范。因此,要想清晰地梳理避风港原则的基本内涵和发展脉络,美国法和德国法的实践无疑是极为重要的研究对象。

(一)美国法的实践

1.渊源与基本内容

早在避风港原则出现以前,限制间接侵权责任的思想就已经在“技术中立”原则中被讨论。

〔1〕 参见刘艳红:“网络犯罪帮助行为正犯化之批判”,《法商研究》2016年第3期,第22页;车浩:“谁应为互联网时代的中立行为买单?”,《中国法律评论》2015年第1期,第50页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

1984 年，在著名的索尼案中，美国最高法院确立了“实质性非侵权用途”原则，即如果产品可能被广泛用于合法的、不受争议的用途，能够具有实质性的非侵权用途，即使制造商和销售商知道其设备可能被用于侵权，也不能推定其故意帮助他人侵权并构成帮助侵权。〔2〕1995 年，在著名的 Stratton Oakmont, Inc. v. Prodigy Services 一案中，Prodigy Services 公司的一位用户在其电子布告栏上发表了诽谤 Stratton Oakmont 公司董事长的言论，其后 Stratton Oakmont 公司起诉作为网络服务提供者的 Prodigy Services 公司和那位无法查明的留言者构成诽谤。法院最后认定该案中的网络服务提供者应为其用户在其所提供的虚拟布告栏上的评论承担责任。法院认为，由于网络服务提供者已经安装了监督布告栏上内容的软件，因此他就不再仅仅是内容的分发者，而是属于内容的发布者。〔3〕这一判决造成了一种非常荒谬的局面，即网络服务提供者采取的技术监督措施反倒加重了自身的法律风险。以此案件为契机，1996 年，为了避免让网络服务提供者承担过重的法律责任以及由此可能造成的寒蝉效应，美国国会通过了《通讯端正法》。〔4〕该法第 230 条(c)款第(1)项规定：“交互计算机服务的提供者或使用者，不得被作为其他信息内容提供者所提供信息的出版者或发言者对待。”第(2)项对民事责任的豁免做出规定：“交互计算机服务的提供者或使用者 a)出于善意对他认为属于淫秽、猥亵、肮脏、暴力、骚扰或其他令人反感的内容进行封锁，不论这些内容是否受宪法保护；或 b)为内容提供者或他人提供技术手段来封锁以上内容的，不承担责任。”这些限缩网络服务提供者责任范围的判例规则与责任规范事实上已经为避风港原则奠定了基础。1998 年美国的《数字千年版权法案》第 202 条(《美国法典》第 17 编第 512 条)更为详细和系统地规定了网络接入服务提供者、缓存服务提供者、存储服务提供者以及信息定位工具提供者免于承担救济和侵权责任的条件以及相关程序，这便是避风港原则的由来。〔5〕

2.刑事领域的适用

在 1997 年的 Zeran v. America Online, Inc. 一案中，《通讯端正法》第一次被作为免责事由引入。该案中，原告齐伦(Zeran)认为美国在线(America Online)公司没有及时清除其布告栏上的诽谤言论，应当承担过失责任。但是法院认为交互计算机服务提供者接受大量的帖文，无法轻易地对其加以及时调查，所以基于《通讯端正法》第 230 条予以免责。〔6〕法院的这一

〔2〕 参见王迁：“‘索尼案’二十年忌——回顾、反思与启示”，《科技与法律》2004 年第 4 期，第 62 页。

〔3〕 See Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710, 1, 4 (N.Y. Sup. Ct. 1995).

〔4〕 See Lawrence G. Walters, “Shooting the messenger: an analysis of theories of criminal liability used against adult-themed online service provider”, *Stanford Law & Policy Review*, Vol.23, No.1, 2012, p. 183; Shahrzad T. Radbod, “Craigslist-A Case for Criminal Liability for Online Service Providers”, *Berkeley Technology Law Journal*, Vol.25, No.1, 2010, p.595.

〔5〕 See U.S. Code § 512 Limitations on Liability Relating to Material Online.

〔6〕 See Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

决定开启了《通讯端正法》第230条被广泛适用的历程,〔7〕由于美国《数字千年版权法案》第512条所确立的避风港原则主要适用于版权法律领域,而《通讯端正法》第230条则具有一个非常广阔的适用范围,因此,后者实际成为了网络服务提供者刑事责任认定中的核心条款。〔8〕但是,《通讯端正法》第230条在刑法领域的适用也存在不小的障碍,原因在于,第230条的(e)款直接地限定了该条的适用范围。《通讯端正法》第230条(e)款第(1)项规定:"该条的任何内容都不得被解释为破坏本章第223条或第231条,第18章第71条(关于淫秽内容)或110条(关于对儿童的性剥削),或者任何其他联邦刑事法律的执行。"该条(e)款第(3)项规定:"本条的任何内容都不得被解释为阻碍州实施与本条相协调的州法律。任何州法律或地方法律不符合本条规定的,不得提起诉讼,也不得追究责任。"〔9〕这两项规定意味着,如果网络服务提供者触犯到了联邦刑事法律规定的罪名,或者涉及到那些与本条相一致的州刑事法律所规定的罪名,那么第230条(c)款的免责事由就不能适用。

在2006年的Voicenet Communications v. Corbett中开始真正涉及了《通讯端正法》第230条的刑法适用问题。在该案中,原告Voicenet Communications公司是网络服务提供者,而被告则是法律执行机关。基于可能存在儿童淫秽内容的线索,被告搜查了原告的财产并且没收了相关的计算机设备和文件。原告起诉被告违反了自己的多项宪法性权利,同时也违反了《通讯端正法》第230条所赋予自己的免责权限。〔10〕虽然该诉讼原告最终以失败告终,但是在该案判决中法院明确否定了被告所提出的《通讯端正法》只具有民事免责效力的主张。法院指出,按照《通讯端正法》第230条的语义,这里的免责并不仅限于民法,对第230条(e)款进行整体解读可知,这里的免责事由只是不适用于联邦刑法以及与本条不协调的州刑法。〔11〕

在2009年People v. Gourlay案中,男孩贾斯廷·贝里(Justin Berry)从13岁开始通过摄像头在网络上传播自己的淫秽图像,他还创建了网站来进行这一活动。被告人古尔利(Gourlay)运营一家网络托管公司,他与贾斯廷·贝里取得联系并进行不断密切沟通,后帮助贾斯廷·贝里建立了几个新的网站用来传播其淫秽图像。〔12〕案发后被告人辩称,法庭没有告知陪审团自己享有《通讯端正法》第230条的免责权利,法庭也没有告知陪审团只有他实际地对儿童色情内容的创造做出贡献时才可以被指控触犯了色情类犯罪,而网络服务提供者仅仅提供带宽或技术辅助并没有真正地创造色情内容。对此,控方则认为,被告并不享有这种免责权

〔7〕 See Shahrzad T. Radbod, supra note 4, p.601.

〔8〕 See Lawrence G. Walters, supra note 4, p.183.

〔9〕 See 47 U.S. Code § 230 (e)(1)(3).

〔10〕 See Voicenet Communications, Inc. v. Corbett, No. 04-1318, 2006 WL 2506318, 1, 1 (E.D. Pa. 2006).

〔11〕 Ibid., p.3.

〔12〕 See People v. Gourlay, No. 278214, 2009 WL 529316, 1, 1 (Mich. App. Ct. 2009).

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

利,因为《通讯端正法》仅为民事责任提供的豁免。〔13〕然而,法院认为该条并没有排除对刑法的免责适用,因为第 230 条(e)款第(3)项中的“任何州法律或地方法律”显然包含了刑法。但是,法院另一方面也还是认定,本案中被告已经构成散布或宣传儿童性滥用内容的罪名。〔14〕

在 2009 年的 Dart v. Craigslist 案中,作为网络服务提供者的被告 Craigslist 公司是一个访问量非常大的广告网站,其创建分类,而用户则选择在不同的分类中发布自己的广告。在这个网站上,“情色”版块是最流行的部分,其中包含了“色情服务”的链接。不过,在这里用户也会收到不许发布违法内容的警告和声明。警方控告,尽管存在警告和声明,但是 Craigslist 网站的“色情”版块里存在着大量较为隐晦的卖淫广告,这违反了联邦的、州的以及地方性的禁止促进卖淫的法律。〔15〕在庭审中,Craigslist 公司提出其应当按照《通讯端正法》第 230 条免责,而法院也确认了 Craigslist 公司属于交互计算机服务提供者的身份,且这些广告信息是由其他信息内容提供者所提供。法院认为本案控方对相关罪名条款存在过度解释,按照《通讯端正法》第 230 条(c)款的规定,无法认定 Craigslist 公司创造了那些广告,也不能认为是 Craigslist 提供了那些卖淫的信息,这些信息是它的用户所提供的。因此,被告的免责诉求被法院承认。〔16〕

(二)德国法的实践

1.渊源与基本内容

早在 1997 年,德国国会便通过了一部综合性的《信息与通信服务法》,其中第一部分《电信服务法》第 5 条便已经明确地采取了限缩网络服务提供者法律责任的立场。2000 年,欧盟通过了《电子商务指令》,该指令第 12—15 条进一步详细地规定网络服务提供者的免责条件。此后,为了贯彻实施以上欧盟指令所规定的层级化责任体系,德国联邦议会先后数次修改了《电信服务法》,并最终于 2007 年通过了《电信媒体法》,将《电子商务指令》中的免责规定在国内法中加以转化。

《电信媒体法》第 7 条规定了网络服务提供者责任的一般原则。一方面该条规定了内容提供者按照一般性的法律来承当责任;另一方面该条总体性地规定,第 8—10 条中的网络服务提供者没有义务监督其所传输和存储的信息,也没有义务根据提示违法活动的情形去调查这些信息。此外,与美国的《数字千年版权法案》第 202 条的内容非常类似,该法第 8—10 条分别为接入服务提供者、缓存服务提供者和存储服务提供者规定了具体的免责条件。〔17〕

〔13〕 Ibid., p.2.

〔14〕 People v. Gourlay, supra note 12, pp.3—5.

〔15〕 See Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 961—963 (N.D.lll. 2009).

〔16〕 Ibid., p.967.

〔17〕 Vgl. Telemediengesetz §§ 7—10.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

2.刑事领域的适用

不论是德国《电信服务法》的修订版本,还是2007年通过的《电信媒体法》,其所规定的网络服务提供者免责条款不仅基本承袭了美国避风港原则的核心内容,而且进一步拓展到了几乎所有的部门法领域。德国的立法者清楚明白地阐明,网络服务提供者的免责事由当然适用于刑法领域。〔18〕因此,以避风港原则为基础建立起来的网络服务提供者免责体系在刑法领域同样适用,对此德国学界并无疑义,〔19〕在司法判例上也得到了充分体现。〔20〕

从大体方向上来看,《电信媒体法》第7—10条中责任规则对刑法构成要件解释与适用的影响只能是限缩性的。形象地说,《电信媒体法》只是在网络服务提供者原有的刑事责任基础上做减法。首先,《电信媒体法》第7条第(2)款从一开始就整体地排除了网络服务提供者一般性、主动性的监督和调查义务,而这一规则同样也适用于刑法领域,这就在很大程度上限缩了网络服务提供者的刑事义务范围。其次,该法第8—10条能够进一步对三种具体类型的网络服务提供者的刑法义务发挥一种限缩性的塑造功能。按照《电信媒体法》的规定,接入服务提供者只要没有首先发动信息传输,没有选择信息接收人,没有改变或选择所传输的信息,那么原则上对其传输的外来信息并不负有刑法意义上的保证人义务。〔21〕而缓存服务提供者和存储服务提供者也不承担一般性的主动监督和调查义务,但是,当他们获得相关认知(如信息在源头被删除,或违法信息的存在)后,便负有义务及时地删除或封锁相关信息。〔22〕最后,该法中对违法内容的"认识"需要达到何种程度在德国学界引起了讨论,这也对刑事领域中主观罪责的认定产生了限缩性的影响,原则上过失与间接故意的责任被排除。〔23〕

(三)避风港原则刑法适用的规则提炼

1.美国法的启示

从上述美国刑事司法实践的判例可以看出,一方面,美国1998年《数字千年版权法案》所确定的避风港原则由于其较强的知识产权属性限制并没有在刑事领域得到适用。但是,该法案所设定的网络服务提供者的类型化方案非常经典,其接入服务提供者、缓存服务提供者、存储服务提供者以及信息定位工具提供者的基本分类为之后深入探讨网络服务提供者的责任奠定了基础。这提醒我们的立法与司法实践,不论是网络服务提供者的民事责任还是刑事责任,

〔18〕 Vgl. BT-Drs. 13/7385, S. 20; BT-Drs. 14/6098, S. 23.

〔19〕 Vgl. Hilgendorf/ Valerius, Computer-und Internetstrafrecht, 2. Aufl., 2012, S.59; Malek/ Popp, Strafsachen im Internet, 2. Aufl., 2015, S. 19.

〔20〕 Vgl. AG München: "CompuServe"-Urteil, MMR, Heft 8, 1998, S. 429.

〔21〕 Vgl. Sieber, Teil 19.1 Allgemeine Probleme des Internetstrafrechts, in Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 2014, Rn. 35.

〔22〕 Vgl. Sieber, a.a.O., Rn. 61.

〔23〕 Vgl. Sieber, Verantwortlichkeit im Internet, Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen, 1999, S. 166.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

类型化的处理都是首要的前提。而且,该法案为网络服务提供者所设计的基本免责框架,深深影响了之后欧洲的《电子商务指令》和德国的《电信服务法》,而后者则在刑事法律领域产生了直接的效力。此外,该法案对"通知—删除"规则的程序作出了非常详细的规定,这不仅对我国的民事法律规范产生了直接的影响,而且也为我国网络服务提供者的刑事责任认定带来了重要启发。另一方面,在当下美国法的语境中,限缩网络服务提供者刑事责任的规范依据主要是《通讯端正法》第 230 条(c)款所确立的"善良撒玛利亚人"保护原则。该条的核心内容就是将间接介入争议议题中的网络服务提供者与直接的出版人或发言人区别开来,避免网络服务提供者为他人的内容承担一种直接和同等的责任,这为限定网络服务提供者的刑事责任指明了基本的思考方向。这一规则及其相关判例确立了网络服务提供者的间接刑事责任的特殊性,实际上也为网络服务提供者创设了独立的免责事由。显然,该条款并非专门为处理网络服务提供者的刑事责任"量身定做",但是其法条的表述相对概括与宽泛,因此美国法院通过非常精细的解释,尽量使其免责效力涵盖刑事法律领域。

然而,美国目前这种网络服务提供者的刑事责任限缩模式也存在着相当明显的问题。其一,《通讯端正法》第 230 条的效力范围具有严格的限制,这使得该条款所发挥的对网络服务提供者的责任限缩功能大打折扣。《通讯端正法》第 230 条(e)款第(1)项明确限制了该条对联邦刑事法律的适用效力,而第(3)项则规定了该条不能影响与本条相适应的州法律和地方法律。因此,在可以预见的未来,检察官很可能会将《通讯端正法》第 230 条的限制适用条款作为一个工具,以此来限制交互计算机服务提供者的免责。〔24〕 其二,《通讯端正法》第 230 条(c)款所确立的"善良撒玛利亚人"保护原则,并没有直接规定网络服务提供者在何种特定条件下可以免责,而只是将其与直接的内容出版者和发言者做出区分,其在类型化、体系性与操作性方面仍然存在不足。

2.德国法的启示

与美国的情况不同,德国网络服务提供者的刑事免责规则显然更具明确性、完整性和体系性。首先,按照德国《电信媒体法》的法律效力范围,该法中以避风港原则为蓝本所建构的网络服务提供者免责体系可以几乎完整地适用于刑法领域,因而不会存在免责规则法律效力的局限性问题。其次,这套责任规范详细地规定了网络服务提供者的具体类型与相应的免责条件,不限于仅仅简单区分内容出版者和发言者,更适应信息时代网络服务提供者的独立主体特征,因而也将在刑事司法实践中形成更好的法确定性。最后,在学者们的努力之下,《电信媒体法》中的网络服务提供者免责条款,已经与德国的阶层犯罪论实现了较好的融合,更具体系性与稳定性。

当然,较之于美国法的免责模式,在一些个案中,德国法对网络服务提供者的责任认定可

〔24〕 See Shahrzad T. Radbod, supra note 4, p.615.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

能存在涵盖性不足的问题。因为,在《电信媒体法》对网络服务提供者的类型划分中,并没有对信息定位工具(包括目录、索引、超文本链接等)的提供者做出规定,[25]但美国的避风港原则在程序性规定上更加详细而具有可操作性。

3.教义学规则的提炼

综观美国与德国的法律实践,虽然在具体法律规定和法律适用上存在差异,但是二者通过引入刑法之外的规范来限缩网络服务提供者刑事责任的做法是一致的。在我国的法律语境中,并不存在像《通讯端正法》或《电信媒体法》这样具有统括效力的规范,但是,从上述比较法的经验中,可以提炼出如下网络服务提供者刑事责任的教义学规则:

(1)网络服务提供者的刑事责任属于一种间接责任,其认定应当区别于直接利用网络服务实施犯罪的主体;

(2)网络服务提供者的刑事责任以网络服务提供者的类型化为前提;

(3)网络服务提供者并不具有一般性的主动监督、调查他人违法内容和行为的刑事义务和权力;

(4)网络服务提供者的刑事作为义务,应当结合不同主体类型及其实际的控制可能性分别进行判断;

(5)"通知—删除"的规则和程序限定了网络服务提供者的刑事义务范围和可罚性启动条件;

(6)网络服务提供者的间接刑事责任以对他人违法内容和行为具有明确认知为前提。

上述教义学规则借助于比较法的视角,从避风港原则的法律实践中提炼而来,可以较为妥当地划定网络服务者的刑事责任边界,其虽然没有在刑法明文规定中被确立,但在实际上具有很大程度的普适合理性,因此应当作为一种理论知识资源,结合我国刑法相关构成要件的理解,融入阶层犯罪论体系之中。这套教义学规则既可能涉及传统的刑法罪名,也关乎新设立的网络犯罪罪名,它是框定网络服务提供者刑事责任范围的基础性刑法原理,也构成了互联网刑法总则理论的重要内容。

三、避风港原则在中国刑法中的理论建构

(一)责任结构失衡

关于网络服务提供者的法律责任问题,在中国的法律框架下存在着一种整体性的结构失衡。这不仅体现在我国目前整体的立法架构之中,同时也反映在具体的部门理论建构之内。

首先,从规范的效力层级来看,各种各样的法律规范(法律、行政法规以及部门规章)都不

[25] Vgl. Gercke, Einführung in das Internetstrafrecht, JA, Heft 12, 2007, S. 844.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

同程度地涉及网络服务提供者的责任,其内容各不相同,这就造成了网络服务提供者规则体系的繁杂。在法律层面,全国人大和全国人大常委会先后颁布了《关于维护互联网安全的决定》《关于加强网络信息保护的决定》《刑法修正案(九)》以及《网络安全法》;在行政法规层面,国务院也先后颁布了《互联网信息服务管理办法》《信息网络传播权保护条例》。此外,公安部,国家广电总局,信息产业部,文化部等部委在相关的部门规章中也提及了网络服务提供者的义务和责任,最高人民法院通过一系列的司法解释,在事实上也提供了一些关于网络服务提供者法律责任的规则。这些处于不同效力层级的规范在内容上并不统一,其总体趋势是进一步地明确和扩张网络服务提供者的责任和义务。〔26〕而在基本制度的架构层面,中国的网络治理向来就存在着"九龙治水"的状况,〔27〕这无疑也加剧了规范效力层级的冲突。

其次,从部门法律协调的角度来看,民法与刑法中关于网络服务提供者的责任认定规定明显在朝着两个不同的方向发展。如学者所言,我国的单个部门法并不滞后国际经验太多,但是对那些跨部门的新问题,建立在传统法律部门划分基础上的立法体制在网络环境下面临各种不适应,缺乏整体规划和顶层设计。〔28〕以《信息网络传播权保护条例》第 20—23 条和《侵权责任法》第 36 条为代表的民事法律规范,整体的立法要旨在于限缩网络服务提供者因第三方内容或行为而承担的侵权责任。然而,以《刑法》第 286 条之一和第 287 条之二,以及最高人民法院和最高人民检察院于 2004 年颁布的《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》(以下简称《传播淫秽电子信息解释(一)》)第 7 条和 2010 年颁布的同名司法解释(以下简称《传播淫秽电子信息解释(二)》)第 5—6 条等为代表的刑事法律规范,则越发地扩张网络服务提供者的责任范围。《刑法》第 286 之一属于新增设的纯正不作为义务犯,而《传播淫秽电子信息解释(二)》第 5—6 条以及《刑法》第 287 条之二则被学者视为"共犯正犯化"的典型。换言之,网络服务提供者的民事责任愈发限缩,而其刑事责任反而愈发扩张,这种深层的立法矛盾应当引起法律顶层设计者的注意。〔29〕

最后,在理论层面,这种反差与矛盾同样存在。一方面,目前我国学界不乏大力拥护通过刑事立法来强化网络服务提供者的平台刑事责任的见解。例如有学者认为,网络平台的建立者和管理者有某种"准政府"的身份和责任,对平台上的违法犯罪行为,不允许其视而不见甚至

〔26〕 参见王华伟:"网络服务提供者的刑法责任比较研究",《环球法律评论》2016 年第 4 期,第 52—53 页。

〔27〕 参见方兴东:"九龙治水是中国网络治理的制度创新",载《21 世纪经济报道》2016 年 4 月 6 日,第 004 版;赖早兴:"论拒不履行信息网络安全管理义务罪中的'经监管部门责令改正'",《法学杂志》2017 年第 10 期,第 51 页。

〔28〕 参见周汉华:"论互联网法",《中国法学》2015 年第 3 期,第 30 页。

〔29〕 在刑法领域之外,公法领域也出现了这种令人担忧的现象,有学者称之为"公法阴影下的避风港"。参见姚志伟:"公法阴影下的避风港——以网络服务提供者的审查义务为中心",《环球法律评论》2018 年第 1 期,第 100 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

纵容。〔30〕但是,这种观点没有对过度扩张网络服务提供者刑事义务的消极后果保持应有的谨慎。另一方面,尽管学界部分有识之士已经充分注意到了网络服务提供者刑事责任盲目扩张所带来的弊端,但是,与民事领域学者们对网络服务提供者免责体系的研究相比,刑法学界的研究在体系化程度和理论深度上仍然有待加强。

(二)结构调整依据

以上所描述的网络服务提供者在刑事责任方面的结构性失衡,不论是从理论还是从实务的角度来看,都亟需加以调整。

首先,目前的网络服务提供者的责任结构,与法秩序统一性原理产生了明显的抵牾。〔31〕在我国目前的法律框架中,网络服务提供者的民事责任限缩而刑事责任扩张,法秩序内部出现了定位错乱,部门法规范之间存在着相互冲突的危险。在我国民法学界,尽管对避风港原则也不乏批判省思,〔32〕但是总体来看,不论是法律规定还是理论通说都明确坚持了这一原则的基础性地位,并以此为根据来体系性地限缩网络服务提供者的侵权责任。而遗憾的是,我国目前的刑事立法和理论学说都没有充分地从整体法秩序的高度来审视网络服务提供者的刑事责任问题。在民法领域,通说之所以采纳避风港原则来限缩网络服务提供者的责任边界,其深层次的理由在于,综合权衡了各方利益并最终形成了某种妥当的均衡关系。因此,在刑法领域当中也要充分地考虑和尊重这种民事规范的内部逻辑,至少是在大体方向上不应与其背道而驰。

其次,从刑事政策的角度来看,建立一套体系化的网络服务提供者的刑事免责体系,降低网络服务提供者在经营过程中的刑事法律风险,明确其行为的刑事责任边界,对促进整个信息产业的发展具有至关重要的作用。在互联网和信息产业的发展中,网络服务提供者扮演着先锋者和探路人的角色。纵观近二十年来网络技术给我们生活带来的巨大变化,几乎每个领域的重大变革都是由网络服务提供者直接推动的。信息检索,在线视频,社交网络,电子商务,网络存储,乃至近年来兴起的大数据与云计算等等,通通都离不开网络服务提供者的创新与探索。没有一个相对宽松和明确的法律责任体系,那么这些互联网技术的变革就都无法实现。而如果简单地援用传统法律的规定,将中间平台视为“商场”“传媒”或者“中介”,认为其必须对用户的行为负责,那么中间平台就会疲于应付和生存,难言创新。〔33〕

---

〔30〕 于志刚、吴尚聪:“我国网络犯罪发展及其立法、司法、理论应对的历史梳理”,《政治与法律》2018 年第 1 期,第 76 页。

〔31〕 Vgl. Wang, Die strafrechtliche Verantwortlichkeit von Internet-Service-Provider, Ein deutsch-chinesischer Rechtsvergleich, 2019, S. 115. 与此类似,有学者指出,我国的司法实践在该领域存在“民刑倒挂”的奇怪现象。参见欧阳本祺:“论网络时代刑法解释的限度”,《中国法学》2017 年第 3 期,第 182 页。

〔32〕 例如,有学者认为,在进入人工智能时代和 web 2.0 时代以后,“通知—删除”规则面临诸多挑战,应当对此重新进行制度调整。参见万勇:“人工智能时代的版权法:通知—移除制度”,《中外法学》2019 年第 5 期,第 1260－1263 页。

〔33〕 周汉华,见前注〔28〕,第 23－24 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

最后,从可操作性的角度来看,网络服务提供者法律责任结构的调整也具有现实的可行性和妥当性。尽管我国目前关于网络服务提供者的刑事法律框架明显具有扩张的特征,但这并不妨碍我们借鉴相关国家对此的普遍共识和基本经验,并在一个较为宽泛的法律框架下将其转换为互联网刑法的教义学理论,实现网络服务提供者刑事责任的恰当限缩。在刑事立法强调"主动防御"的同时,刑法理论上的合理出罪机制也应当逐渐完善,只有立法与理论上的"一紧一松"与"一收一放",才能同时顾全网络空间的安全稳定与信息产业的蓬勃发展。

(三)避风港原则的刑法教义学理论建构

1.刑法之前的责任筛除

在德国刑法语境下,由于《电信媒体法》所建构的责任体系可以几乎完整地适用于刑法领域,所以如何处理这一网络服务提供者的责任体系与刑法相关构成要件的关系,就成为了非常现实的问题。对此,德国刑法学界形成了"前置过滤"模式和融合模式两种相对的立场。〔34〕然而,两种模式完全可以在理论上进行恰当地整合,从而使两种模式中各自的优势都得到保留。如齐白(Sieber)所言,原则上可以肯定"前置过滤"模式,但在此基础上仍然可以将《电信服务法》中的免责构成要素与刑法构成要件该当性的认定相融合,形成一种"与构成要件相结合的预先过滤方案"。〔35〕因此,避风港原则发挥着刑法之前的责任筛除功能,其与之后在犯罪论体系的刑法解释中再次发挥限缩作用并不矛盾。

在我国民法领域,已经存在着一系列限缩网络服务提供者侵权责任的规则,从刑法谦抑性的考虑出发,有必要在第一次法(尤其是民法)领域将那些没有刑事当罚性的行为排除出去,以此实现第一次法对网络服务提供者刑事责任的分流;〔36〕同时也保障法秩序统一性原理的贯彻,避免刑法和民法评价的割裂。例如,《信息网络传播权条例》第 22 条就明确规定了存储服务提供者不对他人内容承担赔偿责任的具体条件。再如,《侵权责任法》第 36 条第 2 款规定:"网络用户利用网络服务实施侵权行为的,被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。网络服务提供者接到通知后未及时采取必要措施的,对损害的扩大部分与该网络用户承担连带责任。"该规定意味着,如果网络服务提供者未经提示,或者经过提示之后即采取了必要的措施,那么网络服务提供者就不承担责任。〔37〕因此,在探讨特定网络服务提供者的刑事责任之前,应当充分关注民法领域对其行为的评价。具体来说,首先应当按照网络服务提供者的具体功能对其进行类型归入判断,如内容服务提供者、接入服务提供者、缓存服务提供者、存储服务提供者以及搜索或者链接服务提供者,以便确定其具体适用的免责规

〔34〕 参见王华伟,见前注〔26〕,第 47 页。

〔35〕 Vgl. Sieber (Fn. 23), S. 121－122.

〔36〕 关于第一次法的论述,参见梁根林:《刑事法网:扩张与限缩》,法律出版社 2005 年版,第 34 页。

〔37〕 杨立新:"《侵权责任法》规定的网络侵权责任的理解与解释",《国家检察官学院学报》2010 年第 2 期,第 4 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

则类型。其后,如果按照《信息网络传播权条例》第20—23条以及《侵权责任法》第36条等的规定(网络服务提供者不应承担民事法律责任),那么原则上该网络服务提供者就不应进入刑事诉讼程序,〔38〕即使要对其进行独立的刑事责任分析,也要极为慎重。

此外,避风港原则的实质内涵也可以从我国相关行政性的法律中推导出来。例如,2012年全国人大常委会《关于加强网络信息保护的决定》第5条规定:"网络服务提供者应当加强对其用户发布的信息的管理,发现法律、法规禁止发布或者传输的信息的,应当立即停止传输该信息,采取消除等处置措施,保存有关记录,并向有关主管部门报告。"以及2016年的《网络安全法》第47条也作出了几乎一致的规定。上述条文虽然不像《信息网络传播权条例》和《侵权责任法》那样明确地引入避风港原则,但只要不对其做扩张解释,就仍然可以对网络服务提供者的行政处罚保持克制态度。按照上述规定,网络服务提供者停止传输违法信息(或停止提供服务)、采取消除处置措施、保存有关记录以及向主管部门报告的义务形成于发现违法信息之后;但此处法律只是指出网络服务提供者应当加强用户信息管理(或安全管理),并没有要求网络服务提供者必须主动发现(或调查)违法信息。从法律逻辑来推导,如果网络服务提供者及时履行了上述义务,便不应承担行政处罚的责任。同理,如果按照上述行政性的法律规定,网络服务提供者尚未达到需要予以行政处罚的程度,那么也不应启动刑事处罚机制。长期以来,我国采取了行政处罚与刑事处罚并行的二元制裁模式,两种处罚的区别主要在于法益侵害和不法程度上的差异。较为典型的网络违法犯罪行为,如非法侵入计算机信息系统和破坏计算机信息系统,此前已经分别被规定在《治安管理处罚法》第29条和《刑法》第285、286条。近年来,网络服务提供者拒不履行信息安全管理义务的刑事处罚在《刑法》中被确立,相应的行政处罚也在《网络安全法》等法律中被规定;在这种阶梯性的制裁模式下,司法者在发动刑事制裁之前也应当充分考虑关于网络服务提供者行政处罚条款中所蕴含的责任限制机制。这样一种前刑法责任排除模式的设置,能够在一定程度上避免网络服务提供者刑事责任边界的不当扩张。

2.避风港原则的刑法体系定位

将避风港原则引入刑法的阶层犯罪论体系之中,首先要面临的问题是如何确定其体系性定位。从上文的介绍可以看出,在美国的刑事司法实践中,避风港原则主要是作为一种抗辩事由而存在,这是由美国刑法犯罪构成的双层模式所决定的。而在德国刑法的语境中,学说史上存在着不同的阶层定位。目前,较为主流的学说倾向于认为,避风港原则所承载的免责规则应当在构成要件阶层与刑法归责中实现融合,据此,按照避风港原则被免责的网络服务提供者行为,一开始就不具有相关犯罪的构成要件该当性。〔39〕在我国目前逐步实现阶层犯罪论体系

〔38〕 Vgl. Wang (Fn. 31), S. 137.

〔39〕 Vgl. Sieber (Fn. 23), S. 117 ff; Hilgendorf ua. (Fn. 19), S. 61; Eisele, in Schönke/SchröderStrafgesetzbuch, 30. Aufl. 2019, § 184, Rn 72; Heger, in Lackner/Kühl, StGB, 29. Aufl. 2018, § 184, Rn. 7a.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

转型的背景下,本文认为,避风港原则实际是在考察网络服务提供者技术属性的前提下,为不同类型的网络服务提供者划定作为义务的边界;如果网络服务提供者满足这些免责条件,那么即使他人利用网络服务造成了侵害后果也不应将其归属于网络服务提供者。可见,避风港原则并没有涉及个人可谴责性层面的罪责问题,定位于构成要件该当性阶层是妥当的做法。如果网络服务提供者并没有积极地参与他人的网络违法犯罪活动,而是在发现他人的违法内容与违法行为之后及时地采取必要且合理的技术举措,那么该种行为仍然属于具有积极社会价值的一般服务提供行为,而不具有类型性的刑事不法属性。当然,避风港原则只是网络服务提供者在构成要件该当性阶层所具有的一种特殊免责机制,其他一般主体所具有的出罪事由仍然可以对其适用。此外,在其他犯罪论阶层,一般性的正当化事由如义务冲突、〔40〕被害人承诺,以及一般性的责任排除事由如违法性认识错误、期待可能性〔41〕的判断等等,都同样可能适用于网络服务提供者的刑事责任。〔42〕

更具体地说,避风港原则影响刑事归责的体系连接点首先在于,网络服务提供者不作为犯罪的认定,这是由网络服务提供者的间接责任模式所决定的。如果网络服务提供者直接而积极地参与犯罪谋划和实施,那么他已经成为了共同犯罪的核心组成部分,避风港原则的免责效力就失去了作用空间。除此以外,避风港原则也可以为我国刑法罪名中限制处罚的程序性条件的认定提供指引,如拒不履行信息网络安全管理义务罪中的"监管部门责令采取改正措施而拒不改正",便可以借鉴"通知—删除"规则的合理内涵。同时,主观罪过与客观作为义务之间也存在着紧密的内在关联,主观认识的要求和程度将直接影响网络服务提供者的作为义务的形成时点和范围边界,这也构成了避风港原则塑造网络服务提供者刑事责任的重要方面。与此相关,从定位于构成要件该当性的体系出发,如果网络服务提供者对奠定其刑事义务和责任的事实情况(如封锁某网站的不成文要求)存在着认识错误,那么就是一种构成要件错误,应当阻却故意。〔43〕当然,尽管避风港原则可以在上述方面支撑和补充网络服务提供者的刑事责任认定,但是在刑法领域中引入避风港原则的基本规范目标仍然在于,为网络服务提供者确立一种刑事责任的限缩机制,而非刑事责任的扩张事由。这也意味着,将避风港原则引入刑法犯罪论体系的时候,主要需要借助于目的性限缩的解释方法,以此来协调体系外的教义学知识资源与刑法明文规定之间的关系。

3.刑事责任限缩的具体展开

(1)宏观层面的客观构造与形塑

〔40〕 参见周光权:"拒不履行信息信息网络安全管理义务罪的司法适用",《人民检察》2018 年第 9 期,第 22 页。

〔41〕 参见王文华:"拒不履行信息网络安全管理义务罪适用分析",《人民检察》2016 年第 6 期,第 27 页。

〔42〕 Vgl. Sieber (Fn. 21), Rn. 90 ff.

〔43〕 Vgl. Valerius, in v. Heintschel-Heinegg (Hrsg.), Beck' scher Online-Kommentar, 43. Aufl., 2019, § 185, Rn. 46.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

首先,按照避风港原则的基本精神,在我国网络服务提供者的刑事责任认定过程中,网络服务提供者对其所传输或存储的信息,不应具有一般性和主动性的监督与调查义务。如果要求网络服务提供者对其传输或存储的信息具有一种主动的监督和调查义务,不仅在技术控制可能性、经济运营成本可承受性上存在问题,甚至可能对信息自由、个人隐私、商业秘密造成威胁。〔44〕对此,虽然我国的民事法律没有明确规定,但其在理论上已经成为民法学者的共识。〔45〕基于同样的道理,在刑事责任领域,主动的监督调查义务也应当被否定,这得到了越来越多的刑法学者的认同。〔46〕因此,在网络运营的过程中,并非一旦出现违法传播的侵害性结果就要对网络服务的提供者进行刑事归责,网络服务提供者不是网络的监管者,并不负有防止他人违法内容与违法行为发生的刑事义务与责任。

然而近年来,我国有一些法律规范出现了为网络服务提供者设置主动调查、监督义务的倾向。例如,国家食品药品监督管理总局通过的《网络食品安全违法行为查处办法》第14条规定:"网络食品交易平台提供者应当设置专门的网络食品安全管理机构或者指定专职食品安全管理人员,对平台上的食品经营行为及信息进行检查。"其要求网络平台提供者承担主动的检查、监督义务,这与通行的关于避风港原则的理解完全对立,〔47〕所以有学者称之为网络服务提供者审查义务的"悖论式并行"。〔48〕再如,我国《反恐怖主义法》第19条规定:"电信业务经营者、互联网服务提供者应当依照法律、行政法规规定,落实网络安全、信息内容监督制度和安全技术防范措施,防止含有恐怖主义、极端主义内容的信息传播。"对此,有学者指出,《反恐怖主义法》要求网络服务提供者对传输、存储、处理的恐怖主义、极端主义内容进行内容审查、搜索和过滤,超越了网络服务提供者的管理能力和合理承受能力,如果其已经付出了必要的努力,那么即使出现违法信息被大量传播的情形,也不应追求刑事责任。〔49〕从避风港原则的基本精神出发,为了避免网络服务提供者承担过重的代理监管义务,造成其行动空间萎缩、角色异化,使得网络主体间的关系陷入冲突性紧张,应当对上述规定做限缩性理解,尽量地限定其行政处罚责任。退一步来说,即使网络服务提供者没有履行上述主动检查、监督义务,也不应

〔44〕 Vgl. Sieber, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II), CR, Heft 11, 1997, S. 655 ff; Neal Kumar Katyal, "Criminal Law in Cyberspace", *University of Pennsylvania Law Review*, Vol. 149, No.4, 2001, p.1098.

〔45〕 参见杨立新,见前注〔37〕,第5页;张新宝、任鸿雁:"互联网上的侵权责任:《侵权责任法》第36条解读",《中国人民大学学报》2010年第4期,第24页。

〔46〕 参见涂龙科:"网络内容管理义务与网络服务提供者的刑事责任",《法学评论》2016年第3期,第68页;皮勇:"论网络服务提供者的管理义务及刑事责任",《法商研究》2017年第5期,第19页。

〔47〕 参见赵鹏:"超越平台责任:网络食品交易规制模式之反思",《华东政法大学学报》2017年第1期,第65页。

〔48〕 姚志伟,见前注〔29〕,第102页。

〔49〕 皮勇,见前注〔46〕,第24页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

当承担相应的刑事责任。

需要说明的是,否定网络服务提供者对第三方内容的一般性、主动性监督调查义务,与要求其按照行业标准建立相应的内部安全机制、采纳一定的安全技术措施的做法并不矛盾,因为后者是一种防御性、配合性的安全管理义务。正是在这个意义上,有学者正确地指出,应当区分网络服务提供者的审查义务和注意义务,避风港原则所免除的只是前者而非后者。〔50〕在网络空间里,网络服务提供者仅在非常有限的情形中才具有中立性质。由于网络服务提供者自身的特殊性质,不论是在国外还是我国的立法当中,为网络服务提供者设置一定的行政性法律义务都已经是常态。〔51〕但应当强调的是,不要轻易地将网络服务提供者的一般性法律义务直接上升为刑法义务,否则,很可能会不当地扩张网络服务提供者的刑事责任边界。〔52〕即使是在公法领域中网络服务提供者的作为义务被不断强化的情况下,刑事领域中的归责仍然应当坚守自身的判断逻辑,立足于避风港原则的基本内涵和精神,回归到保证人地位认定之类的实质性考察当中。

(2)微观层面的客观构造与形塑

①主体类型划分。避风港原则可以为相关罪名中主体要件的理解提供指引。例如,虽然拒不履行信息网络安全管理义务罪的主体明确规定为网络服务提供者,但是不同于一般的身份犯,网络服务提供者本身是一个十分宽泛的概念,仍然需要按照避风港原则所划定的主体类型来加以细化。按照避风港原则的规定,网络服务提供者可以大体分为内容提供者、接入服务提供者、缓存服务提供者、存储服务提供者四种类型,其各自对应着不同程度的免责条件,而这一四分法也应当引入到本罪主体要件的解释与认定中来。〔53〕对此,有部分学者主张,网络内容服务提供者应当排除在网络服务提供者的范畴之外。〔54〕笔者认为,虽然内容提供者并不适用避风港原则的免责规范,而是适用一般法律主体的责任规则,但仍然可以将其作为一种区分性概念纳入到网络服务提供者的基本类型的范畴中。因为,属于“自己内容”(Eigene Inhalte)还是“他人内容”(Fremde Inhalte),本身就是需要探讨的重要理论命题。在实务中,常常可能将从理性第三人视角看来属于自己内容的他人内容,也作为自己内容来处理(Sich Zu

〔50〕 姚志伟,见前注〔29〕,第 102 页。

〔51〕 皮勇,见前注〔46〕,第 15－17 页。

〔52〕 参见车浩:《新评快播案:法律无需掌声,也不能嘲弄》,载北京大学法学院,http://www.law.pku.edu.cn/xwzx/pl/26871.htm,最后访问日期:2019 年 8 月 5 日。例如,司法实践中存在将制作、出租翻墙软件的行为认定为拒不履行信息网络安全管理义务罪的做法,这实际上已经把刑法上网络服务提供者的信息网络安全管理义务进行了泛化处理。参见上海市浦东新区人民法院(2018)沪 0115 刑初 2974 号刑事判决书。

〔53〕 王华伟,见前注〔26〕,第 55 页。

〔54〕 参见陈洪兵:“论拒不履行信息网络安全管理义务罪的适用空间”,《政治与法律》2017 年第 12 期,第 40 页;敬力嘉:“论拒不履行网络安全管理义务罪——以网络中介服务者的刑事责任为中心展开”,《政治与法律》2017 年第 1 期,第 55 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

Eigen Machen)。但是,对于具体的标准以及理解仍然存在诸多分歧。〔55〕例如,在为违法犯罪信息提供深度链接的场合,该内容是作为链接提供者的自己内容还是他人内容,采取"服务器标准"或"用户感知标准"就会得出不同的结论,链接提供者的刑事责任也可能随之变化。〔56〕

当然,伴随着信息社会的纵深发展,网络服务的种类越来越繁多,新型网络服务的提供主体也不断涌现,目前学理上对网络服务提供者的类型划定标准仍然存在着诸多讨论。〔57〕2019年最高人民法院、最高人民检察院《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》(以下简称《网络犯罪司法解释》)第1条就对"网络服务提供者"的概念划定了三种大的类型。但即便如此,以上四分法仍然仅具有基础性的意义。一方面,上述司法解释虽然采取多元类型标准,尽可能全面地概括网络服务提供者的主体形态和适用场景,但是在具体评价其刑事责任时,仍然应当回到基本的技术功能类型,否则就无法准确地把握行为的内在性质。另一方面,即便是一些争议较大的网络服务提供者类型,也可以结合其具体的技术原理,比照以上规则对其的保证人地位加以认定。例如,经常引起法律争议的P2P对等网络运营者,虽然并不在上述四分法之列,但是仍然可以通过分析其基本的技术构造,判断其是否具有中心服务器的数据存储能力,以及对违法内容的实际支配控制能力,从而将其归入接入服务提供者或存储服务提供者的范畴。〔58〕再如,对于搜索引擎运营者的刑事责任,也仍然可以根据搜索引擎系统中的多种具体技术功能,以及上述网络服务提供者的基本类型分别加以判断。〔59〕

②作为义务限定。避风港原则可以对网络服务提供者的不作为义务发挥限定性影响。一方面,基于网络服务提供者的技术特征,可能直接涉及的两类传统罪名是传播犯和表达犯。〔60〕网络服务提供者一般性的服务提供行为通常具有社会相当性和有益性,其在一般情

〔55〕 Vgl. Spindler, in Spindler/ Schmitz, Telemediengesetz mit Netzwerkdurchsetzungsgesetz Kommentar, 2. Aufl., 2018, TMG § 7, Rn.7, 18 ff.

〔56〕 参见杨彩霞:"搜索引擎深度链接行为的刑法规制——实然和应然层面的双重思考",《东北大学学报(社会科学版)》2017年第3期,第294-295页;欧阳本祺:"论网络环境下著作权侵权的刑事归责——以网络服务提供者的刑事责任为中心",《法学家》2018年第3期,第160-161页。

〔57〕 李世阳:"拒不履行网络安全管理义务罪的适用困境与解释出路",《当代法学》2018年第5期,第68-70页;陈洪兵,见前注〔54〕,第40页。

〔58〕 相关研究,参见杨彩霞:"P2P软件和服务提供商著作权侵害刑事责任探究——以P2P技术架构为切入点",《政治与法律》2016年第3期,第52-53页。

〔59〕 Vgl. Sieber/ Liesching, Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem Telemediengesetz, MMR-Beilage, Heft 8, 2007, S. 10 ff.

〔60〕 参见王莹:"网络信息犯罪归责模式研究",《中外法学》2018年第5期,第1305页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

况下并不具有犯罪目的,不与用户合意实施违法行为,所以原则上探讨的是不作为犯的构成。〔61〕由于上述两类传统罪名的刑法构成要件通常属于作为犯,因此问题的核心就主要体现为不纯正不作为犯的认定,尤其是基于危险源监督而产生的保证人地位。〔62〕然而,不同类型的网络服务提供者对信息内容的支配程度并不相同,并且这种控制能力受到诸多技术、社会乃至政策条件的限制。在不作为的实质性判断中,发展较为成熟的避风港原则便可以用来形塑监督者保证人义务的形成条件。另一方面,我国《刑法》还专门设立了拒不履行信息网络安全管理义务罪,网络服务提供者的信息网络安全管理义务在刑法中被正式确立,由此实现了从不纯正不作为犯向纯正不作为犯的转型。〔63〕但是,这一规定中的"信息网络安全管理义务"的内容过于模糊,边界也过于宽泛,以至于有学者认为,本罪虽然形式上属于真正不作为犯,但在实质上却变成了不真正不作为犯。〔64〕事实上,对《刑法》第 286 条之一所设定的信息网络安全管理义务,应当通过反向推导该罪明确列举的危害后果来进行类型化的限缩。在该罪中,明确列举的三种危害后果是违法信息大量传播、用户信息泄露(造成严重后果)和刑事案件证据灭失(情节严重),它们实际上对应着网络服务提供者的内容管理义务、用户信息保护义务和信息备份留存义务。所以对这三种义务类型的违反,恰恰就是目前我国司法实践中网络服务提供者不履行网络信息安全管理义务造成社会危害性(法益侵害)的主要体现。〔65〕显然,用户信息保护义务和信息备份留存义务,已经明显越出了避风港原则所勾画的网络服务提供者的第三方间接责任的类型边界。从理论上来看,是否应当在行政法律责任之外继续为网络服务提供者设置如此宽泛的刑法义务,仍然值得反思。〔66〕尽管如此,在对网络服务提供者的信息网络安全管理义务进行类型化处理的情况下,避风港原则仍然可以对其中首当其冲的他人内容管理义务发挥重要的限缩解释功能。

按照避风港原则的内涵,原则上纯粹的接入服务提供者和传输服务提供者对他人的违法内容不应当承担内容管理义务。有学者正确指出,在这种情况下,即使监管部门责令采取改正措施,但如果不具备义务履行可能性,也不能转化为拒不履行网络安全管理义务罪或相关罪名

〔61〕 Vgl. Ceffinato, Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern, JuS, Heft 5, 2017, S. 404.

〔62〕 王华伟:"网络服务提供者刑事责任的认定路径——兼评快播案的相关争议",《国家检察官学院学报》2017 年第 5 期,第 28 页。

〔63〕 参见谢望原:"论拒不履行信息网络安全管理义务罪",《中国法学》2017 年第 2 期,第 241 页。

〔64〕 李世阳,见前注〔57〕,第 70 页。

〔65〕 参见臧铁伟主编:《中华人民共和国刑法修正案(九)解读》,中国法制出版社 2015 年版,第 190－191 页。

〔66〕 皮勇,见前注〔46〕,第 23－24 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

的刑事违法效果。〔67〕而在自己服务器内存储信息的缓存服务提供者和存储服务提供者，则在对违法内容具有明确认知的前提下，例外性地构成监督者保证人地位，因为此时他们具备了删除和封锁信息的技术可能与规范期待。〔68〕值得注意的是，随着网络信息技术的不断深入、渗透以及运营者控制力度的强化，在现实生活中，纯粹的接入服务提供者逐渐变少，而存储服务提供者则越来越多。充斥在虚拟空间的各种网络服务平台，多数都属于存储服务提供者，甚至部分已经转型为内容提供者。此外，如上所述，诸如 P2P 网络运营者、链接设置者、搜索引擎提供者这类具有争议性的法律主体的刑事义务边界却不能一概而论，应结合其提供的具体服务和不同的内部技术构造来分别认定。但是，如果包括接入服务提供者和传输服务提供者在内的网络服务提供者故意与他人共同合作实施犯罪，那么此时网络服务提供的行为即属于积极作为，而不再适用上述不作为犯的原理。原因在于，避风港原则主要处理的是网络服务提供者的间接刑事责任，在网络服务提供者积极参与乃至合谋犯罪的场合，他即丧失了行为的业务性和中立性特征，其行为与一般主体的违法犯罪已然没有实质差异。如学者所言，只有合法平台的运营者才会根据不作为犯原理来探讨其保证人地位，而非法平台的运营者本身就是通过其积极的作为参与了犯罪。〔69〕

③违法内容边界。与作为义务紧密相关联，这里他人的“违法信息”或“违法内容”也应当做相对限缩的理解。一般来说，网络空间的安全管理本属于国家机关的职责，违法信息的性质判定与删除管控也首先是公权力机关的任务。所以，将对违法内容的管理义务转嫁给网络服务提供者，其实是一种代理监管的思路，这不仅会附随性地带来事前审查、事中监控、事后处理等一系列配套管理义务，而且可能会使得作为市场主体的网络服务提供者产生法律主体的身份混乱。〔70〕进一步而言，这种监管义务与责任的转移甚至可能导致一种“刑法的私人化”现象，这一点已经引起了德国学界的批判。〔71〕因为，违法判定和犯罪认定的司法职能本应由公权力机关来执行，将其转交给私有企业并不具有充足的合法性与正当性。而且，我国相关法律、法规、部门规章所划定的违法信息的范围极为广泛，这对违法内容的界定造成了很大困难。

〔67〕参见姜瀛：“‘以网管网’背景下网络平台的刑法境遇”，《国家检察官学院学报》2017 年第 5 期，第 46－47 页。

〔68〕Vgl. Sieber, Die Bekämpfung von Haas im Internet, technische, rechtliche und strategische Grundlagen für ein Präventionskonzept, ZRP, Heft 3, 2001, S. 99；梁根林：“传统网络犯罪的异化：归责障碍、刑法应对与教义限缩”，《法学》2017 年第 2 期，第 12 页；王华伟，见前注〔62〕，第 28－30 页。

〔69〕Vgl. Ceffinato (Fn. 61), S. 408.

〔70〕周光权，见前注〔40〕，第 21 页。所幸的是，有关部门已经认识到了这一问题。2019 年 8 月国务院办公厅发布的《关于促进平台经济规范健康发展的指导意见》第 2 条第（二）项提到，“强化政府部门监督执法职责，不得将本该由政府承担的监管责任转嫁给平台”。

〔71〕Vgl. Liesching, in Spindler/ Schmitz, Telemediengesetz mit Netzwerkdurchsetzungsgesetz Kommentar, 2. Aufl., 2018, NetzDG, § 1, Rn. 8.

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

最早由国务院《互联网信息服务管理办法》第 15 条确立的 9 种禁止性的信息，其范围涵盖“反对宪法基本原则、危害国家安全和统一、损害国家荣誉和利益、破坏民族团结、破坏宗教政策、宣扬邪教和封建迷信”的内容，也包括涉及谣言、淫秽、色情、暴力、恐怖、侮辱诽谤等内容。这种“九不准”的禁止信息类型，其后被多部行政法规、部门规章所吸纳，如此全面宽泛的审查义务为网络服务提供者带来了沉重的负担。〔72〕更成为问题的是，上述禁止信息中有相当一部分内容的边界非常难以认定。例如，并非露骨描述性行为但带有一定淫秽特征的内容，夸大产品功效但尚难认定属于严重虚假宣传的广告，带有贬损性质却未必能够构成侮辱、诽谤等的信息，其是否违法都需要法学专家进行相当专业的判断，一概将这类信息的违法性判断义务科予网络服务提供者是不妥当的。因此，对他人的“违法信息”和“违法行为”也应当通过限制性的解释予以明确，以降低网络服务提供者的间接性刑事责任的不确定性。本罪中的“违法信息”应当仅限于那些在性质上明显违法的信息，而不应包括在性质认定上具有较大争议的内容。在理论上也有学者主张可以将本罪中的“违法信息”与刑法的犯罪构成相关联，以此来进一步地限定处罚范围。〔73〕

④责令改正程序。“监管部门责令采取改正措施而拒不改正”这一要件的理解与适用也应当借鉴避风港原则的“通知—删除”程序予以深化。避风港原则的核心内涵之一是为网络服务提供者的删除、封锁和移除义务附加“获得通知”这一前提条件，通过严密的程序来限定网络服务提供者的责任范围。而我国《刑法》第 286 条之一所规定的“监管部门责令采取改正措施”，实际上也是通过前置的行政通知程序来限制刑罚权的发动，这与避风港原则具有异曲同工之妙。〔74〕在民法领域，理论界和实务界对避风港原则通知程序的各项要件，以及反通知的具体要求，已经做出了相当详尽的研究。但是，刑法学界和司法实践对如何理解“责令改正程序”尚未达成共识，对此，有必要借鉴避风港原则的精神内涵来予以明确。

其一，按照我国目前的法律规定，网络监管部门非常多元，国家网信部门、国务院电信主管部门、公安部门、国安部门、广电总局、新闻出版总署等都具有监管职权，而且对监管机关的行政层级也没有明确限定，这很可能会造成职权冲突或相互推诿的现象。总的来说，应当尽量将监管机构及其职权进行统合，避免网络服务提供者陷入不得不面对“应接不暇”的行政命令的境地。因此，应当对此处的“监管部门”进行目的性限缩解释，将其限定为“网络安全监管部

〔72〕 姚志伟：“技术性审查：网络服务提供者公法审查义务困境之破解”，《比较法研究》2019 年第 1 期，第 33 页。

〔73〕 参见孙禹：“论网络服务提供者的合规规则——以德国《网络执行法》为借鉴”，《政治与法律》2018 年第 11 期，第 55 页；李世阳，见前注〔57〕，第 74 页。

〔74〕 于冲：“‘二分法’视野下网络服务提供者不作为的刑事责任划界”，《当代法学》2019 年第 5 期，第 18 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

门”,〔75〕并控制监管部门的行政级别(如地市级以上)是较为妥当的做法。其二,责令采取改正措施的形式也需要进一步进行限定,应当仅以文书形式发布为宜,否则可能会出现监管机关通知随意性的问题,对此最新的《网络犯罪司法解释》已经予以确认。按照美国避风港原则的规定,通知也应当以书面形式发出,并且载明具体的侵权内容和位置,包括权利人的各项信息等。〔76〕在我国拒不履行信息网络安全管理义务罪的适用中,也应采取严格的程序性条件来控制刑罚的发动。如学者所言,通过书面形式发布通知,不仅可以使责令改正的具体内容更加明确,而且也便于在此过程中保留诉讼证据。〔77〕其三,改正期限也应予以明确,否则“拒不改正”的认定必将陷入争议。例如,2017 年德国通过了《网络执行法》,对大型社交平台运营者规定了违法内容管理义务,对明显违法内容和一般违法内容分别设定了 24 小时和 7 天的删除期限。该法虽然在德国争议非常大,但是这种对义务履行期限做出明确规定的做法却能为法律的适用带来稳定性,仍然值得肯定。其四,在收到责令改正通知以后,网络服务提供者也应当有权提出异议。在避风港原则中,存在着“通知与反通知”规则,即网络服务对象在接到网络服务提供者发来的删除或断开链接的通知后,如果认为自己没有侵权,可以向网络服务提供者提出反向说明与通知(Counter Notification)。〔78〕同理,为了避免行政命令的随意性,保护网络服务提供者的合法权利,尤其考虑到部分网络的第三方内容和信息在违法性认定上的复杂性和争议性,同样也应当明确赋予网络服务提供者向监管机构提出异议(类似于“反通知”)的权利。如果异议成立,那么责令改正的程序失效,刑事追诉程序也应当停止。当然,在异议过程中,不宜停止责令改正通知的执行。〔79〕

(3)主观方面的形态与限缩

避风港原则不仅规定了网络服务提供者对他人违法内容和违法行为所承担的间接责任的边界,其中也包含了网络服务提供者对他人违法内容和违法行为的认识状态要求。一方面,客观义务的范围本身就与主观心态存在直接关联,尤其是在过失犯罪的场合,刑事注意义务无疑被大大扩展。另一方面,避风港原则致力于使网络服务提供者摆脱不确定性的法律风险,进而促进信息服务的蓬勃发展,因此不能让网络服务提供者为他人或然性的违法内容与违法行为承担责任。我国学界关于网络服务提供者刑事责任的探讨主要集中在客观方面,而实际上其主观罪过形式的认定,也可以在避风港原则的规则内涵中得到启示。

目前,学界对《刑法》第 286 条之一拒不履行信息网络安全管理义务罪的主观罪过形式存

〔75〕 王文华,见前注〔41〕,第 25 页。

〔76〕 See U.S. Code § 512 (c) (3)(A).

〔77〕 赖早兴,见前注〔27〕,第 53 页。

〔78〕 See U.S. Code § 512 (g) (2), (3). 我国的类似规定可参见《信息网络传播权保护条例》第 15－17 条。

〔79〕 赖早兴,见前注〔27〕,第 53－54 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

在着较大争议。除了较为典型的故意说之外,〔80〕不乏主张本罪为过失犯的观点。例如,有学者指出,如果将本罪的罪过形式认定为故意,那么拒不履行网络安全管理义务罪中的个别情形也可以构成帮助信息网络犯罪活动罪,如此一来两罪就会出现功能的重合。〔81〕然而,《刑法》第 286 条之一是针对网络服务提供者所设置的纯正的不作为犯和义务犯,而《刑法》第 287 条之二则是为了应对网络共同犯罪难题而设置的帮助行为正犯化罪名,二者虽然在个别情况下存在一定的重合,但是在主体身份、行为内容、结果要件等方面都存在明显区别。因此,以避免二罪的重合为理由来论证犯罪过失是难以成立的。〔82〕更为重要的是,从避风港原则免责效力的刑法转换视角出发,网络服务提供者过失的罪过形式也应被排除。因为,避风港原则排除了网络服务提供者对他人内容和行为进行一般性、主动性监督调查的义务,网络服务提供者对他人违法内容和违法行为的删除与封锁义务,形成于对违法内容和违法行为具有实际认识之后。从过失犯的角度来理解,如果要求网络服务提供者应当掌握他人违法内容或违法行为的情况,则无异于让网络服务提供者事先对他人提供的内容和行为进行提前的主动调查,这在实际上与避风港原则的内涵背道而驰。〔83〕

此外,我国刑法还有一些涉及网络服务提供者刑事责任的传统罪名和相应司法解释,其中也包含了主观罪过要件的规定。例如,《传播淫秽电子信息解释(一)》第 7 条和《传播淫秽电子信息解释(二)》第 6 条都采用了“明知”的表述,立法者在将上述司法解释的规定转化为《刑法》分则第 287 条之二(帮助信息网络犯罪活动罪)的时候,也同样延用了“明知”这一概念。虽然按照构成要件的字面表述,该罪并不是网络服务提供者的身份犯,但是从其规定的行为内容(如提供互联网接入、服务器托管、网络存储、通讯传输等技术支持)来看,却与网络服务提供者有非常密切的关联。基于同样的道理,从避风港原则的责任限缩逻辑出发,上述“明知”不仅应当排除过失的可能性,而且也应当理解为一种明确而具体的认识。〔84〕对此有学者正确地指出,如果正常提供网络存储、接入等服务,行为人在一般情况下并没有创立法所不容许的风险,只有当其具有特殊认知的时候才可以对其进行归责。〔85〕不具有犯罪意图的网络服务者所提供的信息网络服务,本身具有着重要的社会效用,只是在其明确认识到具体的违法内容之后却仍然放任自己的服务提供行为被利用的时候,行为就具有了不法属性。

近年来,网络空间中的共同犯罪不断异化,犯罪参与人的犯意联络逐渐弱化,这促使我国

〔80〕 参见谢望原,见前注〔63〕,第 247 页。

〔81〕 参见李本灿:“拒不履行信息网络安全管理义务罪的两面性解读”,《法学论坛》2017 年第 3 期,第 141－142 页。

〔82〕 Vgl. Wang (Fn. 31), S. 141.

〔83〕 Vgl. Malek u.a. (Fn. 19), S. 25; 欧阳本祺、王倩:“《刑法修正案(九)》新增网络犯罪的法律适用”,《江苏行政学院学报》2016 年第 4 期,第 128 页。

〔84〕 参见王华伟:“网络语境中帮助行为正犯化的批判解读”,《法学评论》2019 年第 4 期,第 137－138 页。

〔85〕 参见王莹,见前注〔60〕,第 1313－1314 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

的立法与司法不断地放宽对行为人主观罪过方面的要求，以此填补可能形成的处罚漏洞。然而，按照避风港原则的基本精神，网络服务提供者的刑事责任属于一种间接责任，它考察的是在何种程度上为他人的违法犯罪行为承担责任，而在主观罪过形式上应当采取更加限定性的立场。一方面，如上所言，按照目前被广泛认可的观点，网络服务提供者不应承担一般性的主动、积极监督调查义务；如果将“明知”的内容降低为认识到其网络服务有被他人用于实施犯罪的可能性，那么就必然会迫使网络服务提供者主动去监督客户的网络活动，从而造成网络服务提供者刑事责任的过度扩大化。〔86〕另一方面，在虚拟空间中，网络用户数量众多且常常处在匿名不确定性状态，用户提供的内容更是数量巨大而变动频繁，网络服务提供者由于技术限制，不可能对其存储信息的具体状况完全掌握。〔87〕正因如此，有学者主张，在对网络服务提供者的“明知”进行推定时，也应当比传统犯罪采取更加严格的标准。〔88〕在《刑法》第287之二已经通过“共犯正犯化”的立法将（共犯语境下）双向的犯意沟通简化为（正犯语境下）单向的主观明知的背景下，至少就网络服务提供者的刑事责任而言，不应再继续放低主观不法要素的构成标准。然而，近期出现的一些案例却让人担忧，在帮助信息网络犯罪活动罪的司法实践中，很多网络服务提供者仅仅是因为个别主体可能利用其提供的呼叫转接服务实施诈骗，〔89〕或可能利用其网络支付接口实施洗钱，〔90〕就被认定构成帮助信息网络犯罪活动罪，这在实际上是对“明知”采取了相当扩张的认定立场。如果仅仅基于网络服务提供者对海量信息中可能存在的违法内容的模糊性、或然性认识就予以刑事归责，必将给网络服务提供者乃至信息产业的发展带来过重的法律风险与负担，而这也正是避风港原则所致力避免的问题。

四、结　语

我国网络服务提供者的刑法责任存在着结构性失衡问题，即网络服务提供者的民事责任限缩而刑事责任扩张，民事免责体系完整而刑事免责体系缺失。这种结构性的矛盾不仅在法理上冲击着法秩序统一原则，在实践中也可能给互联网信息产业的健康发展蒙上阴影。比较研究美国和德国的情况可以发现，避风港原则不应仅限于民事领域的纵深发展，在刑事领域也应当实现体系化的整合与转换。在中国《刑法》通过特别立法明确扩张网络服务提供者刑法责任的背景下，首先应当以避风港原则为基本依据，建立起网络服务提供者“前刑法评价”与刑法评价的位阶关系，以此实现责任分流。在此基础上，我们应当进一步将避风港原则的基本免责

〔86〕 参见皮勇：“论新型网络犯罪立法及其适用”，《中国社会科学》2018年第10期，第146页。

〔87〕 Vgl. Sieber (Fn. 44), S. 654.

〔88〕 参见王莹，见前注〔60〕，第1314页。然而，2019年《网络犯罪司法解释》第11条更为扩张地列举了6种不同的推定方式和1个兜底性条款。

〔89〕 参见浙江省绍兴市越城区人民法院(2016)浙0604刑初1032号刑事判决书。

〔90〕 参见浙江省义乌市人民法院(2017)浙0782刑初1563号刑事判决书。

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

规则与刑法犯罪论体系进行融合，实现避风港原则的刑法转换，从而消除网络服务提供者所面对的不确定的刑事法律风险。具体来说，避风港原则主要应定位于构成要件该当性阶层，将实现网络服务提供者刑事归责的恰当限缩作为基本解释方向。在客观方面，不论是在不纯正不作为犯还是在纯正不作为犯的语境下，避风港原则都可以从宏观和微观两个层面，结合网络服务提供者的类型划分，进一步地限缩、形塑网络服务提供者的刑法义务和刑事责任。同时，避风港原则中的“通知—删除”规则，也可以为拒不履行信息网络安全管理义务罪中责令改正程序的理解与适用提供指引性方案。在主观方面，在涉及网络服务提供者相关罪名及司法解释的适用中，也应当进一步按照避风港原则的深层内涵，将网络服务提供者的过失形态予以排除，并对故意的认识程度进行限定。

网络服务提供者的刑法责任是互联网刑法中一个基础性和总则性的问题。然而，这一问题的妥善处理，已经无法在传统的刑法教义学理论中直接找到答案。因为，在互联网空间里，网络技术催生了新型的社会主体，也重新塑造了各个主体之间的社会关系。避风港原则是综合考虑网络服务提供者不同的主体技术特性、运营成本、信息自由以及产业政策等多重因素后达成的平衡，应当被刑法教义学的理论体系所吸收。网络服务提供者刑事责任理论的建构必须打开学术视野，跨过学科边界，为传统刑法教义学体系注入“活水”，探索建立一种开放式的互联网刑法研究模式。如此，才能实现第一次法与第二次法的协调相处，达到法律制度与技术发展、社会进步的良性互动。

Abstract: There exists the structural problem for the criminal liability of Internet service provider in China, which not only impacts the principle of “unity of legal orders”, but also may cast shadow over the healthy development of the information industry. A comparative study of the United States and Germany reveals that the safe harbor principle, which was formed and developed in civil law, should also be applied in the field of criminal law. In view of the fact, the criminal liability of ISP was explicitly expanded in Chinese Penal Code and we should firstly construct a two-staged process of “pre-criminal law evaluation” and criminal law evaluation for the ISP. On this basis, we should further integrate the basic rules of safe harbor principle into the criminal law theory system, limiting the liability of ISP in both objective and subjective aspects of the crime's components.

Key Words: Internet Service Provider; Safe Harbor Principle; Criminal Liability; Objective Obligation; Mens rea

（责任编辑：车 浩）

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/