

网络信息犯罪归责模式研究

王莹*

摘要 在互联网 2.0 时代,“谁应当为网络信息犯罪导致的法益侵害负责”成为数字时代向传统刑法提出的极具现实性与挑战性的问题。结合网络技术传播原理对我国《刑法修正案(九)》的刑事责任条款进行教义学注疏,理顺其内部逻辑脉络,有助于厘清我国网络服务提供者刑事责任的妥当边界。第一,《刑法》第 287 条之一规定的网络服务提供者是对自己发布信息的刑事责任,为上述行为提供帮助者应以第 287 条之二论处,否则会使得第 287 条之二虚置并产生繁复的竞合问题。第二,第 287 条之二规定的是因他人发布信息而产生的网络服务提供者责任,应抛开共犯框架下中立的帮助犯理论而根据一般的归责原理予以解读,即归责依据在于网络服务提供者对所传输涉罪信息的特殊认知;如此主观不法便会成为归责的唯一依据与本罪的不法重点,因此应对行为人的主观方面采取限制解释,以缓和因客观方面限制的缺乏而带来的责任过度扩张。第三,关于网络服务提供者为他人发布的网络涉罪信息所承担的不纯正不作为犯刑事责任,应当从传统刑法危险源监管保证人地位的教义学资源出发,结合网络传播技术特征,合理界定保证人地位。

关键词 交流犯 非交流犯 帮助犯正犯化 危险源监管保证人地位 风险管辖

在互联网 2.0 时代,用户从信息的被动接受对象转变为主动的内容发布者,传统物理生活空间不断向网络虚拟空间延伸。与之相伴,网络虚拟空间也日益充斥着涉嫌违法犯罪的不良信息。谁应当为这些信息导致的法益侵害负责?网络服务提供者作为网络信息的来源者或者网络信息传输连接者,是否需要为网络信息所导致的法益侵害承担刑事责任呢?我国 2015 年颁布的《刑法修正案(九)》专设三条对网络服务提供者的刑事责任进行规定,分别是第 286 条之一拒不履行信息网络安全管理义务罪、第 287 条之一非法利用信息网络罪与第 287 条之二

* 中国人民大学法学院副教授。本文受国家社科基金项目“信息刑法时代信息犯罪归责与治理模式研究”(项目编号:18BFX101)的资助。

帮助信息网络犯罪活动罪。^{〔1〕} 该如何对上述专门针对网络服务提供者创设的刑事责任条款作出符合网络技术特性与传统刑法教义学原理解释,是《刑法修正案(九)》向当前刑法解释学提出的严峻挑战。

一、归责的逻辑起点:信息网络传播服务行为

在刑法上,探讨刑事责任问题的起点是,存在一个可能被作为犯罪来论处的、具有可罚性的行为,例如盗窃行为、故意伤害行为等;且互联网环境下,网络服务提供者的刑事责任问题也必须从行为这个起点出发。互联网作为虚拟空间,其仅仅是信息或者数据的生成与传播空间,因此引发刑事责任问题的行为不是传统犯罪里的物理有形行为,而是仅局限于在网络空间进行信息传播或者提供信息传播服务的行为。故而,信息网络传播服务行为是探讨网络服务提供者刑事责任的起点。除了第 286 条之一拒不履行信息网络安全管理义务罪这一纯正的不作为犯罪以外,无论是按照共同犯罪原理对用户的犯罪行为成立帮助犯,还是按照第 287 条之二成立帮助信息网络犯罪活动罪,以及第 287 条之一的非法利用信息网络罪,皆离不开信息的发布、传输与存储行为。此外,除该条第二、三项涉及的信息发布行为,第一项所规定的“设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”行为,从网络技术上来讲显然也应归结为信息发布、传输与存储等网络传播服务行为。鉴于网络传播服务行为具有虚拟性与较强的技术性,与现实空间的传统物理行为相比更加不可感知,因此若要将我们基于传统物理世界的经验法则建立起来的教义学原理运用到网络空间,就有必要了解其技术实质与功能,探寻其与现实世界传统犯罪行为连接点并据此对传统教义学予以演绎、细化。

根据网络传播技术的功能特征,可以对信息网络传播服务行为进行如下五种最基本的分类,即信息的发布或上传、网络存储、系统缓存、网络接入(也称为纯粹的信息传输)以及信息定位(或搜索)。而提供上述网络传播服务的网络服务主体则分别称为网络内容服务提供者、网络存储服务提供者、系统缓存服务提供者、网络接入服务提供者以及信息定位服务者(或搜索引擎)。具体而言,网络内容服务提供者(Internet Content Provider)以发布信息为主要网络服务内容,例如互联网新闻服务提供者、企业门户网站等。在个人用户设立个人主页、博客、微博或者在 BBS 上发布信息时,用户也可成为广义上的网络内容服务提供者。网络存储服务提供者(Host Service Provider)是为他人信息提供网络存储空间,例如电子论坛、留言簿运营者,购物网站运营者,以及提供服务器为他人网站提供存储空间的服务提供者。缓存服务提供者

〔1〕 其中第 286 条之一与第 287 条之二的行为主体主要是网络服务提供者,而第 287 条之一的行为主体可以为网络服务提供者,也可以为用户个人。鉴于第 286 条之一拒不履行信息网络安全管理义务罪是对网络服务提供者不履行行政法上的信息安全管理义务而导致的安全管理事故所承担的责任,并非是对网络传播的信息所致法益侵害的责任,其从性质上来说是一种行政犯及纯正不作为犯,而本文仅探讨网络涉罪信息的归责问题,故仅涉及第 287 条之一与第 287 条之二。

(Cache-Service Provider)是指为了有效进行数据传输和节省传输时间而将频繁传输的信息暂时存储在服务器上的服务提供者,以免该信息被访问时每次都需从初始服务器传输到用户在服务器上。〔2〕网络接入服务提供者(Internet Access Provider)则指向终端用户提供网络接入服务的网络服务提供者,比如无线局域网(WLAN)提供者。〔3〕

这种以技术功能为基础的分类广为国际网络立法所采纳,例如美国于1998年10月通过《数字千年版权法》(简称“DMCA”)对网络服务进行了暂时网络传输、系统缓存、根据用户指示在系统或网络中存储信息、信息搜索工具的分类。〔4〕欧盟2000年也通过了《关于共同体内部市场的信息社会服务,尤其是电子商务的若干法律方面的第2000/31/EC号指令》(简称《电子商务指令》),其第12—14条将网络服务分为单纯的网络传输、缓存服务、信息存储服务。德国2007年颁布《电信媒体法》第8—10条也贯彻了欧盟《电子商务指令》的上述分类。〔5〕而与欧盟《电子商务指令》与美国《数字千年版权法》不同的是,德国《电信媒体法》第7条还规定了内容服务提供者的责任。因此,网络服务类型因其具有的不同传播技术特征而直接影响并制约着其对网络传播信息的控制支配程度,上述几部法律均根据不同的服务类型对不同的服务提供者规定了免责条件,也即在符合这些免责条件的情况下,网络服务提供者不对用户利用其网络服务传播的信息承担责任。

我国《刑法》第287条之二规定的网络服务包括互联网接入、服务器托管、网络存储、通讯传输等技术支持以及提供网络广告推广、支付结算等服务,其中“互联网接入、服务器托管、网络存储、通讯传输等技术支持”从网络技术功能角度来看,实际上也可归结为上述五种服务。服务器托管与网络存储皆属于信息存储,而互联网通讯传输服务属于概括式规定,其部分可以归入互联网接入服务,部分可以归入搜索引擎等信息定位服务;至于网络广告推广、支付结算等服务则超出了纯粹网络传播技术服务的范围,并非单纯的网络信息传播,具有附加的服务内容。其中“广告推广”是在中性的网络信息传播之外再加上积极的宣传,而“支付结算”则属于典型的财产或经济类犯罪的帮助行为,鉴于本文仅探讨网络服务提供者对其通过网络路径传播的信息的归责机制问题,故仅限于上述典型的网络传播技术服务,而对上述两种附加功能的网络服务不予探讨。〔6〕

然而值得注意的是,一个网络平台可能同时提供一种以上服务,例如大型网络平台腾讯、

〔2〕 Hoffmann in: Spindler/ Schuster, 3. Aufl., 2015, § 9, Rdn. 1 f.; Sieber/ Höfinger in: Hören/ Sieber/ Holznagel, Teil 18.1, Rdn. 73, 43. Ergänzungslieferung 2016.

〔3〕 德国《远程媒体法》第8条规定,纯粹提供信息传输服务的网络服务提供者包括了提供基础设施服务的主干网络服务提供者(Network provider)和网络接入服务者,参见 Sieber/ Höfinger, Teil 18, Rdn. 64; Hilgendorf/ Valerius, Computer- und Internetstrafrecht, Ein Grundriss, 2. Aufl., 2012, S. 57 f.

〔4〕 U.S.Code Title 17, § 512.

〔5〕 Sieber/ Höfinger(Fn. 2), Teil 18.1 Rdn. 10.关于网络服务提供者的类型区分也可参见王伟伟:“网络服务提供者刑事责任比较研究”,《环球法律评论》2016年第4期,第44—46页。

〔6〕 实际上,广告推广与支付结算服务的提供者往往与被帮助者之间存在意思沟通,运用传统的共同犯罪原理即可解决其责任问题,即应根据第3款以被帮助者构成的犯罪的共犯处罚。故本条对上述两种服务的规定实无必要。

搜狐等门户网都有自己的服务器,因此对于自己发布的信息来说其既是内容服务提供者,又是存储服务提供者;同时,这些网站又运营电子论坛供他人发布信息,针对此种服务其又是存储服务提供者。因此,所谓某种类型的服务提供者,总是针对具体的信息提供服务而言。例如在颇具争议的快播案中,一审判决书认定:“快播公司作为一家流媒体应用开发和服务供应企业,其免费发布快播资源服务器程序和播放器程序,使快播资源服务器、用户播放器、中心调度服务器、缓存调度服务器和上千台缓存服务器共同构建起了一个庞大的基于 P2P 技术提供视频信息服务的网络平台。”从网络技术功能上来看,快播服务应当包括 P2P 缓存服务与信息定位服务(根据用户的指令搜寻视频文件)。

二、信息网络传播服务行为法益侵害的类型:交流犯与非交流犯

信息网络传播服务行为导致法益侵害进入刑法的视野可能有两种方式,第一种是该信息传播行为本身即是刑法所禁止的构成要件行为或构成要件行为的一部分,如传播淫秽物品罪、煽动分裂国家罪、侵犯著作权罪、侮辱罪、诽谤罪等。这类信息本身就是非法的、禁止传播的(如传播淫秽物品罪),或者是禁止向公众表达的(如侮辱罪、诽谤罪),前者在德国刑法上也被称之为传播犯(Verbreitungsdelikt),后者被称之为表达犯(Aeusserungsdelikt),二者的区别在于后者需要行为人内心对所传播内容的认同,而前者则不需要。但其不法构成的实质均是在不特定多数人之间交换或者沟通非法信息,因此二者也被统摄在“交流犯”(kommunikationsdelikt)这个上位概念之下。^{〔7〕}例如德国刑法学者希尔根多夫教授(Hilgendorf)认为鉴于互联网作为现代信息交流与沟通的媒介这一首要功能,大多数网络犯罪都涉及传播法律禁止传播的信息内容。^{〔8〕}在交流犯场合,特定信息的传播本身即是构成要件行为,故信息传播行为本身即可造成法益侵害。且其法益侵害有以下两种情形:交流犯中的表达犯侵犯名誉权这种具体法益;而传播犯中除了侵犯著作权和商标权的犯罪以外,一般都不直接侵犯具体法益,往往只涉及抽象法益的侵犯。例如传播淫秽物品罪、煽动分裂国家罪分别是侵犯社会风化与国家安全这种抽象法益。细言之,我国刑法中规定的交流犯包括第 103 条煽动分裂国家罪,第 105 条煽动颠覆国家政权罪,第 120 条之三宣扬恐怖主义、极端主义、煽动实施恐怖活动罪,第 181 条编造并传播证券、期货交易虚假信息罪,第 217 条侵犯著作权罪,第 249 条煽动民族仇恨、民族歧视罪,第 278 条煽动暴力抗拒法律实施罪,第 291 条之一编造、故意传播虚假信息罪,第 363 条传播淫秽物品牟利罪以及第 364 条传播淫秽物品罪。

〔7〕 Altenhain, Die strafrechtliche Verantwortung für die Verbreitung missbilligter Inhalte in Computernetze, CR 1997, 485; Boese, Strafrechtliche Verantwortlichkeit fuer Verweisungen durch Links im Internet, 2002, S. 2, m.w.N.

〔8〕 只是在术语上 Hilgendorf 教授使用广义的表达犯或内容犯概念(Inhaltsdelikt)代替交流犯,涵盖上文中狭义的传播犯与狭义的表达犯(Hilgendorf(Fn. 3), S. 79.),但由于传统上的表达犯还包含内心倾向要素,故以表达犯作为传播犯的上位概念不甚妥当。内容犯的概念虽然比表达犯的概念更加广泛,但未能体现出这类犯罪信息交流与沟通的不法本质,故笔者更赞同交流犯的概念。

第二种方式是,发布或传播不法信息本身并非构成要件的实行行为,这类信息本身往往也并不会直接造成法益侵害,而是需要与行为人自己或他人在现实世界的行为结合才能造成法益侵害。例如A运营某电子论坛,B为该电子论坛提供网络接入服务,网络用户甲在A的电子论坛上发布诈骗信息,若无现实世界中的进一步行为(例如诈骗账户的开设、被害人的汇款行为等),该信息本身并不会造成财产法益的侵害。再如,用户乙在该电子论坛上发布信息号召他人绑架本地富豪丙,若没有他人在该信息的影响下在现实世界中实施绑架行为,则乙发布的信息本身也并不会造成现实物理世界中生命与财产法益的侵害。^{〔9〕}从理论上讲,第二种不法信息可以指向现实世界中第三人实施的所有传统犯罪行为,从而与后者相结合导致现实世界的法益侵害,因此这种类型的网络服务提供者刑事责任范围比第一种形式要更加广泛。故而,我们可以将第一种网络传播服务行为致损的方式称为交流犯方式,此时非法信息的交流、传播本身是构成要件的实行行为;第二种网络传播服务行为致损的方式为非交流犯方式,此时非法信息的传播本身并非构成要件的实行行为,必须结合信息传播者本人或他人的线下行为才可能造成法益侵害(往往是某种具体的个人法益)。而单纯的信息网络传播,至多是法益侵害的预备,并不会造成法益的现实侵害。显然,因信息网络传播造成法益侵害对网络服务提供者的归责,在交流犯与非交流犯中存在显著区别。在交流犯中,法益侵害是非法信息流通或传播所直接导致的,网络服务提供者或者发起了这种信息传播(正犯),或者参与了他人发布的信息的传播过程(共犯);在非交流犯中,他人的线下行为才是直接的法益侵害行为,一般来说是正犯,网络服务提供者的网络传播服务行为一般来说仅仅是共犯或不作为犯(但此时其是否具有保证人地位,值得探讨,详见下文五(二))。可以说,德国传统刑法中的交流犯与非交流犯概念,为解决网络服务提供者因网络信息而承担的刑事责任问题提供了重要的分析工具,对此将在下文第五部分(即网络服务提供者对他人发布信息的责任部分)予以详细展开。

三、谁发布的信息?——以非法信息来源进行区分的二分法归责逻辑

信息网络传播服务行为本身是技术中立的行为,引起责任的关键问题是其所传播的对象:信息。传播合法信息一般不会引起传播者责任,信息的违法性是引起网络传播服务行为责任的前提。基于互联网信息共享的原理,互联网上的信息是开放的、自由流通的,其信息来源与权属往往被淡化。但是,对于一个科学、合理的责任归属设计来说,确定信息的来源与归属是十分必要的。在现实物理世界,以过错责任为中心的责任归属体系(包括侵权法与刑法)首先会追问“这是谁实施的行为?”,而在虚拟的网络世界,这个体系则首先应该追问“这是谁发布的信息?”。故而,根据信息是由谁发布到网络这一标准对网络服务与网络服务提供者进行区分,也是互联网领域一个最基本的区分。据此可将网络服务提供者分为网络内容提供者(Internet Content Provider,简称ICP)与其他类型的网络服务提供者。

〔9〕《刑法修正案(九)》新增的第287条之一以预备犯正犯化的形式将这种行为规定为犯罪,该条实质上是抽象的危险犯,因此该条的构成要件行为仍然仅是一个法益危险而非非法益侵害行为。

从网络传播技术角度来看,网络内容提供者对其提供的信息具有直接的支配,可以对发布的信息内容进行选择、编辑、删除,而也正是基于这种完全的技术上、权限上的控制,网络内容服务提供者才应对其发布的信息承担完全责任。这一原则也为美国法和德国法所承认。例如美国《通讯端正法》第 230 条(c)(1)中规定“交互式计算机服务的提供者或使用者不应被视为其它信息内容提供者所提供信息的出版者或发表者”,这奠定了网络内容服务提供者与其他类型网络服务提供者的责任区分制,并以此理念为基础对后者进行责任限制。^[10] 在 2009 年 *People v. Gourlay* 一案中,^[11] 被告人 Berry 是一位未成年人,其自创网站发布色情图片, Gourlay 经营的网络公司为这个网站提供网络存储服务。Berry 和 Gourlay 就该网站及其内容进行过几次交流,并合作建立了另外 2 家包含相似内容的网站。一审法院根据该州三部关于儿童色情的法律判决其构成相应犯罪, Gourlay 上诉称其作为服务提供者并未参与发布儿童色情内容,因而不应被视为该内容的发布者。上诉审法院则首先肯定第 230 条免责条款也包括对州法律所规定的刑事责任的豁免,继而认为 Gourlay 的行为并非仅仅提供网络存储空间,而是在知情的情况下积极地参与了网站及其内容的创设,因此是内容服务提供者而非存储服务提供者。由于第 230 条仅对被动的网络存储服务提供者免责,因此对其定罪并不违反该条规定。而德国《远程媒体法》第 7 条第 1 款则开宗明义地规定:“对自己的信息即它所供用户使用的信息按照一般的法律承担责任。”其后的第 8—10 条也分别对网络接入、系统缓存及网络存储服务提供者进行相应的责任限制规定。

无论在侵权法领域还是在刑法领域,个人为自己的行为(在此是自己的信息和信息传播行为)负责都是一个基本原则,因此探讨网络服务提供者的责任首先需要确定信息的来源,即该信息是网络服务提供者发布的还是用户发布的。一方面,网络内容提供者对自己发布的信息独立负责原则在我国侵权法领域得到了体现。比如,2005 年《互联网著作权行政保护办法》中根据信息来源区分互联网内容提供与互联网信息服务提供行为,规定直接提供互联网内容的行为适用著作权法,即构成著作权侵权的完全按照《著作权法》的一般规定进行责任承担;而提供信息服务的行为则适用《互联网著作权行政保护办法》,并对其责任进行了限制规定。2009 年《侵权责任法》第 36 条也分别为网络用户、对自己的信息造成侵权与对他人的信息造成侵权确立了不同的责任类型,网络用户、利用网络侵害他人民事权益的,应当独立承担完全的侵权责任(第 1 款);网络服务提供者在接到网络用户利用其网络服务实施侵权行为的通知或知道

[10] 美国国会 1996 年通过了《通讯端正法案》(Communication Decency Act)作为《电讯法》(Communication Decency Act)的一部分。作为第一部规范网络色情信息的法律,该法案第 230 条(c)规定了广泛的网络服务提供者免责条款:(c)(1)交互式计算机服务的提供者或使用者不应被视为其他信息内容提供者所提供信息的出版者或发表者。Pham(c)(2)交互式计算机服务的提供者或使用者不因下述事由承担民事责任:Pham(A)自愿且善意地限制访问或限制获取其所认定的淫秽、猥亵、色情、下流、暴力、骚扰或其他不当信息。此等材料是否受宪法保护,在所不论。Pham(B)向信息内容提供者或他人提供技术手段,以便其限制访问(A)所规定的材料。

[11] *People v. Gourlay*, No. 278214, 2009 WL 529216, at * 1 (Mich. App. Ct. 2009).

该情形未及时采取必要措施时,与网络用户承担连带责任(第2、3款)。^[12]另外,我国2016年修订的《电信条例》第62条第1款也规定:“使用电信网络传输信息的内容及其后果由电信用户负责。”

另一方面,在刑事责任上也是如此。网络内容服务提供者对于自己所发布信息构成的犯罪承担完全的责任,符合传统犯罪中的一般归责原理;可将发布信息、信息传播、信息导致法益侵害结果视为完整的因果链条,再对网络服务提供者进行主观与客观归责。例如企业门户网站、个人主页、博客博主等在其网站、主页或博客上发布信息,如果发布侵权内容、侮辱、诽谤或者淫秽信息成立侮辱罪、诽谤罪、传播淫秽物品罪等相应犯罪,则根据个人行为个人负责原理,自应对其所传播的信息承担完全的刑事责任。然而在其它类型的网络服务提供者为他人发布的信息提供网络存储、网络接入、缓存等服务时,对该信息导致的法益侵害原则上按照共同犯罪的帮助犯或不纯正不作为犯承担责任。

值得注意的是快播案中快播公司的行为认定。快播P2P缓存技术涉及P2P+CDN技术,即通过快播调度服务器拉拽视频文件存储在缓存服务器中并向客户端提供,这种传输并非限于帮助传输,而是积极地参与了传输过程,即所谓参与传输模式,^[13]因而周光权教授倾向于在“作为的传播”意义上界定快播公司行为,且法官也不否认其中的作为因素。^[14]但是,本文上述五种信息网络传播服务分类中的系统缓存是指一般意义上的web缓存,与快播的网络服务行为不同,其并不主动参与信息传输,而仅是对他人的信息进行以加速访问为目的的存储,因此不符合刑法意义上的“传播”这一概念,不能单独成为传播淫秽物品罪、煽动分裂国家罪等交流犯的正犯行为。而CDN技术的全称Content Delivery Network(内容分发网络)则表明其内容服务提供的身份,可以独立为自己的信息发布行为承担完全责任,因而可以成立传播淫秽物品牟利罪(作为的)正犯。

因此,即使我国2005年《互联网著作权行政保护办法》中使用的“互联网内容提供与互联网信息服务提供行为”这一概念及其区分并未在其后的立法中得到贯彻,我国的网络立法术语也未明确区分网络内容服务提供者与其他类型的网络服务提供者;但这并不妨碍我们在互联网法领域区分自己信息与他人信息,并采用这种责任二分法的责任归属逻辑剖析网络不法信息的归责问题。此外,理解这一归责逻辑脉络,有助于对《刑法》第287条之一与第287条之二进行妥当的教义学注疏,并透过条文规定在整个责任体系中检视网络服务提供者的刑事责任。下文将试图以这一责任二分法的逻辑脉络展开对网络信息归责问题的探讨。

[12] 参见张新宝、任鸿雁:“互联网上的侵权责任——《侵权责任法》第36条的解读”,《中国人民大学学报》2010年第4期,第18—21页;杨立新:“《侵权责任法》规定的网络侵权责任的解释”,《国家检察官学院学报》2010年第2期,第3—4页。

[13] 参见范君:“快播案犯罪构成及相关审判问题——从技术判断行为的进路”,《中外法学》2017年第1期,第33—36页。

[14] 参见周光权:“犯罪支配还是义务违反——快播案定罪理由之探究”,《中外法学》2017年第1期,第53—56页;同上注,第34—36页。

四、对自己发布信息的责任——网络内容提供者责任

例如设立名为“XX 锁业”的网站出售开锁工具和学习光盘传授盗窃犯罪方法,或者设立“如何进行完美绑架”的网站传授绑架方法,或者设立某银行的钓鱼网站进行诈骗,即属此类。从广义来说,网络用户自己发布信息,例如在他人的网站上发布关于“黑炸药制作”的帖子,或者在某狩猎网站上设立 QQ 群进行枪支交易等,本身也属于网络内容服务提供者。因此,第 287 条之一规定的行为可以分为以下两种情形:

一是,设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的(第 1 款第 1 项)。如果这些违法犯罪网站、通讯群组的设立主要是供自己发布上述违法犯罪信息或进行相关信息交流,则属于信息内容服务提供者;如果除了自己发布违法犯罪信息以外,还设置论坛、BBS 等版块供他人发布信息,则还属于网络存储服务提供者。由于第 287 条之二规定了明知他人利用信息网络实施犯罪,为其犯罪提供网络存储的情形,因而在认定上可以包含两种可能,即同时成立第 287 条之一与第 287 条之二的犯罪。对此,按照处罚较重者定罪处罚,但若二罪的法定刑相同,则会带来罪名适用上的困难。因此从信息网络传播技术的角度来看,应对本条进行限制解释,认为仅包括内容服务提供者的情形。这种解释也符合司法实践的情况,例如行为人设立名为“XX 锁业”的网站出售开锁工具和学习光盘传授盗窃犯罪方法,或者设立“如何进行完美绑架”的网站传授绑架方法,或者设立某银行的钓鱼网站进行诈骗,往往是自己发布的信息内容占据网站或通讯群组的大部分。

二是,发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息以及为实施诈骗等违法犯罪活动发布信息的(第 1 款第 2、3 项)。此种情形涉及直接发布违法犯罪信息,行为人既属于网络用户,同时也无疑属于内容服务提供者。而网络服务提供者发布非法信息构成犯罪的,根据个人行为个人负责的原理,应为自己的行为或信息承担完全的责任。在《刑法修正案(九)》出台之前,其承担刑事责任的情况如下:对于交流犯来说,网络服务提供者成立传播淫秽物品罪、煽动分裂国家罪、侮辱罪等交流犯的正犯;对于非交流犯来说,网络服务提供者发布涉嫌诈骗,传授犯罪方法,非法制造、销售枪支、弹药、爆炸物,生产、销售伪劣产品等信息,一般来说成立上述犯罪的犯罪预备或者未遂。而《刑法修正案(九)》增修的第 287 条之一非法利用信息网络罪,实际上是在上述一般的网络内容服务提供者刑事责任之外,又扩展了其责任范围。此后,对于与线下行为配合而发展到既遂阶段的,成立诈骗罪、传授犯罪方法罪等的既遂与本条之罪,并根据 287 条之一第 3 款的规定,依照处罚较重的规定即一般来说按照上述犯罪的既遂来定罪处罚。而对于线下行为未发展到既遂阶段的,则成立本罪和前述犯罪的预备、未遂,以较重的犯罪定罪处罚。

综上,本条规定是对网络内容服务提供者为自己发布的信息承担刑事责任的兜底条款,如果不属于发布信息、设立网站等内容服务,而是为这种内容服务提供接入、存储等服务的,那么其属于内容服务的帮助行为,原则上成立本罪的帮助犯。但是因第 287 条之二同时也为上述网络接入、存储等服务行为专门设立了帮助利用信息网络犯罪活动罪,故而按照法条竞合时特殊法优于普通法的原理,应以第 287 条之二规定的罪名来论处。国内有学者认为,为他人设立

上述网站、通讯群组提供互联网接入、服务器托管、网络存储空间、通讯传输通道等帮助的,也属于设立网站、通讯群组、发布信息的一个环节,也应以此罪论处。^[15] 对此笔者认为,此种理解模糊了为自己发布的信息和为他人发布的信息承担责任的归责界限,使得第 287 条之二形同虚设。因此,设立网站、通讯群组、发布信息应当是针对本人行为而言的,为上述行为提供帮助者,则成立第 287 条之二帮助利用信息网络犯罪活动罪。

五、对他人发布信息的责任

如果我们仅关注网络内容服务提供者的行为,就会发现对其归责与传统犯罪领域并无太大区别。对于网络内容服务提供者利用互联网技术手段或者在互联网这个场域实施的犯罪行为,可以通过扩大解释现有犯罪的构成要件,或者通过创设新的构成要件来加以规制,这并未超越分论个罪而对刑法总论的传统教义学原理带来根本性的冲击。因此,《刑法修正案(九)》出台前关于互联网犯罪的探讨,也多集中在互联网技术手段或场域特征所带来的犯罪规制的技术层面问题,例如非法获取虚拟财产、侵扰网络公共秩序、利用互联网实施著作权侵权等问题而引发的讨论。这些问题虽然借助网络的匿名性、可复制性与广泛传播性获得了新的要素,例如对犯罪损害或犯罪结果的重新定义以及行为方式的扩展理解,但仍然是对传统的加害与被害二元结构的教义学阐释。但是显然,《刑法修正案(九)》不再满足于这个二元结构,而是把目光转向第三方——这一通过提供技术平台而使得犯罪行为得以发生的中间角色,并开始将其纳入整个归责体系。可以说,引入网络服务提供者的刑事责任使得传统的加害与被害二元结构扩展为三角结构(网络犯罪行为人(互联网用户)网络服务提供者——网络犯罪被害人(互联网用户)),这种结构改变给传统刑法教义学的责任理论带来了深远的影响。虽然传统教义学也在共同犯罪场合探讨第三人的刑事责任问题(例如中立的帮助犯问题),但是这在现实世界发生的犯罪中显然仅是一个边缘化的问题。在网络犯罪环境下,内容服务提供者以外的其它类型网络服务提供者提供了犯罪实施必不可少的客观上的条件——信息的网络传输或存储等网络服务,是否或者如何对这种网络服务行为进行归责就成为网络犯罪的一个中心议题。这不仅对传统的共同犯罪理论、不作为犯理论提出了挑战,也对传统罪责原则中的个人责任模式造成了冲击。故而德国刑法学者 Sieber 将其称之为一种新的责任文化。^[16]

如果说传统的物理生活空间是传统犯罪发生的原生空间,随着人类生活空间向网络空间的拓展,犯罪也开始出现在网络空间这一犯罪发生的次生空间。社会生活规则的生成总是来自于人类行为的经验,因而面对网络犯罪问题,我们最初的反应就是将从犯罪发生的原生空间中获得的犯罪规制经验运用于网络空间。在传统刑法教义学资源中,探讨一个人可能为他人

[15] 同上注,第7页。

[16] Sieber, *Aufbruch in das neue Jahrtausend Für eine neue Kultur der Verantwortlichkeit im Internet*, MMR 698, (1999), 690. Sieber 教授在该文中前瞻性地提出“新的责任文化”概念,但遗憾的是并未对这种“新的责任文化”予以进一步的教义学解析。可以说,将传统教义学与互联网的社会结构与技术特征予以结合的深入的“互联网刑法教义学”研究在德国也有待于展开。

行为承担刑事责任的理论主要是共同犯罪理论与不作为犯罪理论,这也是讨论网络服务提供者对他人的信息承担刑事责任时绕不开的两条路径。首先,根据共同犯罪理论,对他人的不法信息所导致的法益侵害可能成立帮助犯或者教唆犯;其次根据不作为犯罪理论,如果其对不法信息所造成的损害具有保证人地位,则对该损害承担不纯正不作为的刑事责任。细言之,如果在用户发布信息之时即认识到该信息是不法信息却仍然提供网络服务,则可能成立用户发布不法信息构成的犯罪的帮助犯(在对用户实施犯罪行为具有支配时成立共同正犯);如果在用户发布信息之后才认识到该信息是不法信息,则之前的服务行为不成立帮助犯,但是如果能够证立其保证人地位,则可能对损害后果具有防止义务,构成相应的(不纯正)不作为犯罪。

(一)共同犯罪路径

网络服务提供者提供的网络服务使得用户得以在互联网发布、传播非法信息因而构成犯罪,客观上来说其为他人的犯罪行为提供了技术上的便利或条件。一方面,根据传统共犯理论可能成立对他人犯罪的帮助犯,此时需要与发布违法犯罪信息的用户具有共同故意;另一方面,根据我国《刑法》第287条之二,即使不存在共同故意,但单方面明知他人发布的信息涉嫌犯罪却仍然提供服务的,可成立帮助信息网络犯罪活动罪。然而,该条规定在我国学界引起了极大争议,对其性质主要存在以下观点。

1.帮助犯正犯化说

多数学者认为本条是帮助犯正犯化的规定,具有对犯罪行为单方面的明知即可成立本罪,因此该条规定扩大了网络共同犯罪成立的范围。持该说的学者又分为激进与保守两个阵营,前者基于严格网络服务提供者责任的立场赞同该立法动向,认为应当跳脱传统共同犯罪理论的框架理解本条。即以网络帮助行为具有“一对多”的严重危害性与主观意思沟通缺乏的常态化为理由,认为传统共犯理论在应对网络帮助行为方面具有滞后性,主张脱离共犯理论框架来理解第287条之二;甚至认为该条正犯化的规定不够彻底,而将其斥为“正犯责任定位的模糊”,提倡将帮助行为单独正犯化,即归责不以被帮助者成立犯罪为限。^[17]而后者则基于传统共同犯罪中立帮助犯理论质疑该条的妥当性,反对将具有中立性与正当职业性的网络服务行为予以正犯化。^[18]

2.量刑规则说

与上述两种观点不同,张明楷教授认为该条规定并非是为帮助犯设立的一个新罪名,即将帮助犯作为正犯加以规定,只是对特定的帮助犯规定了量刑规则,本条并不意味着对共犯从属性原则的放弃和采取扩展正犯概念。^[19]对此笔者有以下两点反驳意见,其一,如果仅是量刑规则,仍然按照帮助犯论处,应该以被帮助的罪名定罪,而不应该以本条所规定的新的罪名定

[17] 参见于志刚:“网络空间中犯罪帮助行为的制裁体系与完善思路”,《中国法学》2016年第2期,第4—9页。

[18] 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18—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5期,第48—50页;周光权:“网络服务商的刑事责任范围”,《中国法律评论》2015年第2期,第175—178页。

[19] 参见张明楷:“论帮助信息网络犯罪活动罪”,《政治与法律》2016年第2期,第2—8页。

罪,这一点是立法明文设定的不可逾越的解释障碍。^[20]其二,如果这种理解仅仅是为了解决被帮助者没有利用帮助者提供的网络服务或者根本没有实施犯罪时不处罚帮助者的问题,则是多余之举。因为法条规定“明知他人利用信息网络实施犯罪,为其犯罪提供……帮助”,实际上就从主观与客观两个方面设定了可罚性的限制,主观上行为人要认识到他人利用其网络服务传输的信息涉嫌犯罪;客观上这种信息应当确实构成犯罪,因而须以被帮助者行为成立犯罪为前提。在此,“他人利用信息网络实施了犯罪”即可以理解为本罪构成要件中所设置的客观处罚条件,旨在处罚网络服务提供者单方提供帮助的情形(片面帮助犯)。因而虽然网络服务提供者须认识到他人利用信息网络实施的行为涉嫌犯罪,但由于不存在共同故意以及共同的行为,故而该行为是否真正成立犯罪,例如是否符合相应犯罪的主体要求或满足其它构成要件符合性的要求,是否达到相应的情节严重程度等,一般来说是行为人(网络服务提供者)无法控制或施加影响的,是独立于行为人本人的行为不法与结果不法之外的,所以相对于本罪的行为人来说客观处罚条件。但是如果被帮助者没有利用帮助者提供的网络服务,则不存在所谓的“帮助”,也因不满足“帮助”这一构成要件要素而不具有构成要件符合性;如果被帮助者没有实施犯罪,即因为客观处罚条件不满足而不具有构成要件符合性,因而不成立本罪。因此,解决被帮助者没有利用帮助者提供的网络服务或者根本没有实施犯罪时不处罚帮助者的问题,并不需要回到共犯的框架下借助共犯从属性原理。

越过上述观点表面的分歧,我们可以从中提炼出第287条之二的两种解释路径。第一条路径是坚持共犯框架的路径,其中包括上述量刑规则说与帮助犯正犯化中的反对说,这两种观点究其实质皆是反对脱离共犯框架对帮助者归责,只是前者将第287条之二直接解释为量刑规则,不承认帮助犯正犯化;而后者虽然忠实于法条原意承认该条性质上是帮助犯正犯化,但却不赞同这种立法上的处理,认为其不符合中立的帮助犯原理,应坚持以传统共同犯罪理论来解决为他人信息负责的问题。第二条路径则是以于志刚教授为代表的脱离共犯框架的路径,基于网络犯罪帮助行为的特殊性要求,跳脱传统共同犯罪理论的框架来理解本条,倡导网络帮助行为的全面单独正犯化。^[21]且这两条解释路径暗含了两种不同的归责思维,分别通向不同的归责结论。第一条路径极力将第287条之二拉回传统共同犯罪理论,甚至不惜通过牵强解释或者否定本条妥当性的代价来达成。但是,如果完全在共犯框架下解释,那么根据共同犯罪部分行为整体归责的思路,其结果应该是他人发布的涉罪信息所对应的犯罪的帮助犯,例如为他人发布的淫秽物品提供网络存储或者网络接入的,成立传播淫秽物品罪的帮助犯;其行为不法是帮助,而结果不法是他人信息所构成的犯罪,即通过帮助犯实现对他人信息的归责,而非第287条之二的帮助利用信息网络犯罪活动罪。至于第二条路径则极力摆脱共犯理论的束缚,朝向单独正犯化方向发展。其背后的逻辑是赋予帮助行为以独立的行为不法与结果不法;行为不法是帮助,结果不法不是他人信息所构成的犯罪(并非是将相应信息构成的犯罪归责给帮助者),而是将对这种犯罪的促进单独评价为结果不法——即帮助利用信息网络犯罪活动罪。

[20] 相同观点参见刘艳红,见前注[18],第20页。

[21] 参见于志刚,见前注[17],第4-9页。

对于第一条解释路径,如上所述,量刑规则说与实在法规定的冲突显而易见,且帮助犯正犯化说中的反对说也由于采取完全的批判态度,根本无法也不欲为本条的解释与适用作任何贡献。相较而言,第二条解释路径似乎更加符合第 287 条之二的归责逻辑。显然,第 287 条之二将帮助行为单独规定为犯罪以后,即切断了把他人信息归责给网络服务提供者的共犯归责逻辑通路——该条不是要求网络服务提供者为他人的(涉罪)信息负责,而是为自己的(帮助)行为负责。但是,笔者却不赞成该观点完全单独正犯化的主张。换句话说,笔者虽依通说承认本条的性质为帮助犯正犯化的规定,但是却认为这种被正犯化了的行为仍然是帮助行为。既然是帮助行为,那么就无法完全脱离对被帮助行为予以单独正犯的理解;他人利用其帮助行为实施的犯罪行为通过主观构成要件与客观处罚条件(他人行为成立犯罪)渗入本罪的构成要件之中,因此被帮助行为成立犯罪是本罪可罚的前提条件。于志刚教授也认识到这一点,即该帮助信息网络犯罪活动罪的构成要件行为是对他人犯罪的帮助行为,需以具体实行行为成立犯罪为前提;其显然不是完全独立的正犯规定,可将之斥为所谓的“正犯责任定位的模糊”。〔22〕

申言之,第 287 条之二帮助网络信息犯罪活动罪作为帮助行为正犯化之规定,具有以下两种性质。其一,其并非共同犯罪规定。该规定表明我国立法者对他人信息的信息责任采取了有别于国际上通行的共犯归责模式,而是独立的归责模式,即因他人信息为自己的帮助行为承担责任。其是一种介于共犯与正犯之间的混合模式,正犯因素在于独立成罪,脱离了部分行为、整体归责的共犯归责模式;而共犯因素则在于本罪的构成要件行为是帮助行为,原本的正犯行为“他人利用信息网络实施犯罪”即作为构成要件要素嵌入本罪的构成要件之中。因此,要求被帮助者的行为构成犯罪并非是因为共犯框架下的共犯从属性原则之要求,而是因为构成要件的明文规定。这种特殊的归责模式提示我们,继续沿用共同犯罪框架下的“中立帮助犯理论”作为本罪的理论分析工具,可能是不合适的。中立的帮助犯理论解决的是因自己日常的或者职业的行为而对利用这种行为的他人行为的归责问题,因此需要解决该日常或者职业行为对他人行为的促进与贡献作用问题。而第 287 条之二解决的是这种帮助行为本身的责任问题,并不关心与他人犯罪的因果联系,只要其主观上存在对他人犯罪行为的明知与客观上提供了网络服务行为,即可构成本条之罪。

因此依据第 287 条之二的归责逻辑思路,可以认为,本罪放弃了对帮助行为客观上的限制,将不法重点放在主观方面,只要存在对他人犯罪行为的明知而提供服务的,即成立帮助。对此应脱离共犯框架下中立的帮助犯理论,根据一般的归责原理予以解读;行为人创设法所不容许的风险是归责的前提,如果正常提供网络存储、网络接入等服务,在一般情形下并未创立法所不容许的风险,但是如果其认识到某信息涉嫌犯罪却仍然提供服务,则属于具有特殊认知的情形,可以对其进行归责。

然而,由于第 287 条之二将主观明知作为归责的唯一依据,因此应对行为人的主观方面采取限制解释,以缓和因客观方面限制的缺乏而带来的责任过度扩张。

第一,应将本罪的明知理解为他人利用信息网络实施犯罪的具体的认识,即存在对他人所传播的涉罪信息内容的具体认识,并谨慎使用明知的推定。原因分述如下:

〔22〕 同上注,第 17 页。

由于归责的合理化说明只有通过客观归责理论中的“特殊认知”才能实现,而“特殊认知”从来都是对法益侵害的具体现实认知。日常生活中虽然到处存在法益侵害或者犯罪行为的可能性,但对这种可能性的认识并不能使自己的行为超越法所不容许的风险。例如,仅仅怀疑可能有恐怖分子炸机而劝被害人登机,并未创设法所不容许的风险。显然,只有针对具体的恐怖分子或恐怖行动的认识才能称得上是行为人的“特殊认知”;一般性的可能性,即使是较高概率的可能性(例如知道某地区局势动荡经常发生恐怖袭击),由于也可能为其他人或者被害人所知悉,因此并未超出日常生活的风险。所以,假使仅一般性地怀疑用户可能滥用其所提供的网络服务传播涉罪信息,则并不构成本罪的明知;其只有在对具体涉罪信息内容具有认识而提供网络服务时,才成立本罪。例如,即使怀疑用户传播的很有可能是淫秽视频(例如点击或播放量异常等),但只要缺乏对所传播信息内容的具体认识,就不符合本罪的主观方面。

另外,也应当对本罪明知的推定进行限制。与传统犯罪不同,网络用户之间的关系是远程的、一对多或者发散型的,网络传播的信息是海量的、动态的,对用户利用信息网络实施犯罪知悉的概率也在客观上远远低于传统物理空间的犯罪。例如当网络信息明显构成犯罪时或者在网络服务收费明显不合理时即认定为具有明知,不符合网络犯罪的现实。因此,2010年《最高人民法院、最高人民检察院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(二)》第8条关于明知的认定,尤其是其中第(三)、(四)项的规定,应谨慎地适用于本条;并有必要对传统犯罪中明知的推定规则结合网络传播技术特征来加以限制。也正是基于网络传播技术与网络空间社会关系结构特征的考虑,无论国际上还是我国主流观点都否定网络服务提供者的主动审查义务;而如果不加限制地使用推定,则等同于向其施加了主动审查义务。从国际上来看,《欧盟电子商务指令》第15条第1款规定:“成员国不得制定普遍的规定向其施加监控传输或存储的信息的义务,或主动寻找表明违法行为之事实的义务。”德国《远程媒体法》第7条第2款也作出了相同规定。^[23]我国相关立法也可作类似推断,比如全国人大常委会2012年颁布的《关于加强网络信息保护的决定》第5条明确规定:“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。”这一规定似乎仅设定了网络服务提供者在认识到违法信息时的行动义务,而并未向其施加主动获取这种认识的审查义务。我国2012年最高人民法院《关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第8条规定:“未对网络用户侵害信息网络传播权的行为主动进行审查的,人民法院不应据此认定其具有过错。”该规定也等于否定了主动的审查义务。

第二,关于本罪的认识内容。由于本条认识对象除了自己的帮助行为,还包括“他人正在利用信息网络实施犯罪”,这原本是共犯框架下帮助犯双重故意的要求,但在第287条之二却成为了正犯的故意要求。此即为本罪故意认识内容的界定带来了难题。“他人利用信息网络实施犯罪”作为本罪的构成要件要素必须为行为人所认识,但是这一构成要件要素显然不是纯粹的事实性要素即描述性构成要件要素,其还包含“他人利用信息网络实施的行为构成犯罪”

[23] Spindler/Schuster (Fn. 2), TMG § 9, Rdn. 33.

这样一个规范的判断在内。于是形成如下嵌套结构,即他人行为是否构成犯罪(A罪)这样一个关于A罪的违法性的认识成为本罪(B罪)的构成要件要素,而针对这一帮助行为是否构成犯罪的认识则是B罪的违法性认识,二者不应混淆。因此,“他人利用信息网络实施的行为构成犯罪”便成为一个特殊的规范性构成要件要素,其由事实性前提与对该事实性前提的规范判断两部分组成;规范判断建立在事实性前提认识基础之上,如认识到事实性前提就可以做出所谓“外行人所处领域的平行评价”,^[24]即对该规范性构成要件要素有认识。而第287条之二的规范性构成要件要素则由以下两部分内容组成:“他人利用信息网络实施了某行为”这一事实、该行为属于刑法上的犯罪(即该行为属于刑法上的构成要件行为(不法类型)并且满足情节等要求)这一规范判断。因此,只要认识到他人利用网络实施了某构成要件行为这一事实性前提,至于该行为事实是否构成犯罪,则属于对这一事实性前提的规范判断,并不需要行为人予以认识。例如,甲宽带公司认识到乙设立淫秽网站而为其提供接入服务,只要其认识到乙的网站涉嫌传播淫秽信息即为已足,不需要甲正确认识到乙的行为在刑法上如何定性以及是否满足传播淫秽物品牟利罪的情节要求。若甲误以为乙的网站仅传播性科普知识及性病预防而为其提供接入服务的,则因未认识到“他人利用信息网络实施的行为构成犯罪”这一规范性构成要件要素的事实性前提而不符合本罪的主观要求。此处也可以看出,必须有对涉罪信息的具体认知,才可能满足该规范性构成要件中对前提性事实的认识要求。这也从另一侧面支持了上文关于本罪主观方面的第一个论点。

(二)不作为犯罪理论路径:义务来源(危险源监管保证人地位)

另一个探讨行为人对他人所实施行为负责的教义学路径是不纯正不作为犯理论。根据该理论,网络服务提供者是否应为他人的行为(即他人的不法信息)所造成的损害结果负责,关键在于其是否具有保证人地位。下文将以传统教义学早期的形式说(形式法律义务理论)与目前通说的功能二分理论为分析框架展开论述。

1. 形式法律义务理论

该说认为保证人地位来源于合同、法律、职业要求以及先行行为,因该说内部的逻辑缺陷逐渐被通说所抛弃。^[25]我国晚近关于作为义务来源的主流话语也基本脱离了形式说而转向实质说。^[26]因此,单纯从网络法规定的网络服务提供者的安全管理义务推导出其保证人地位,继而认为网络服务提供者对于其网络平台上的违法内容或犯罪行为承担不作为刑事责任的观点,因其形式法律义务理论的根基本身就已经受到动摇,是站不住脚的。2000年12月全

[24] Joecks in: Joecks/ Miebach, 3. Aufl., 2017, § 16, Rdn. 70 ff; Roxin, Strafrecht Allgemeiner Teil, Band. I, 4. Aufl., 2006, § 12, Rdn. 101 ff.

[25] Schuenemamm, Zur Garantenstellung beim unechten Unterlassungsdelikt: Dogmenhistorische, rechtsvergleichende und sachlogische Auswegweiser aus einem Chaos, in: Grundlagen des Straf- und Strafverfahrensrechts, FS-Amelung zum 70. Geburtstag, (Hrsg.) Boese /Sternberg-Lieben, 2009, S. 309.

[26] 参见王莹:“先行行为作为义务之理论谱系归整及其界定”,《中外法学》2013年第2期,第325—346页;周光权:“论实质的作为义务”,《中外法学》2005年第2期,第216—225页;陈兴良:“作为义务:从形式的作为义务论到实质的作为义务论”,《国家检察官学院学报》2010年第3期,第70—79页;苏彩霞、肖晶:“作为义务的实质来源:规范支配论之确立与展开”,《浙江大学学报》2015年第4期,第94—108页。

人大常委会《关于维护互联网安全的决定》第7条规定：“……从事互联网业务的单位要依法开展活动，发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告……。”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：“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。”上述规定从法律上确立了对不法信息的停止传输义务，即删除或隔离义务，但这种义务仅是行政法上的或者民法上的义务，违犯之可能导致行政责任或者民事侵权责任，但却未必会导致不纯正不作为的刑事责任。在《刑法修正案(九)》所增修的第286条之一拒不履行信息网络安全管理义务罪之后，这种行为则刚好是本罪的实行行为。例如在快播案中，一审法院以快播公司作为互联网信息服务的提供者对其网络信息服务内容负有网络安全管理义务为由，认为其成立传播淫秽物品牟利罪的不作为犯罪，实际上也反映了司法实务对第286条之一拒不履行信息网络安全管理义务罪这一纯正不作为犯之性质与对不纯正不作为犯保证人地位的误解。^[27]再如，用户甲在某电子论坛上发布诈骗信息，该电子论坛运营者乙发现此诈骗信息但未予以删除，用户丙发现后即与甲联系，将钱汇往甲指定的账户，如果认为乙对丙遭受的财产损失承担不纯正不作为犯罪的刑事责任，即成立不作为形式的诈骗罪，则是不可接受的形式法律义务论的结论。

2. 功能二分理论

功能二分理论根据不同作为义务之间内容与功能上的区别将作为义务的来源分为以下两大类，^[28]即来源于保护保证人地位的作为义务(Obhutsgarantenstellung)与监管保证人地位(Ueberwachungsgarantenstellung)的作为义务。

(1) 保护保证人地位。在功能二分理论框架下分析网络服务提供者的保证人地位，首先可以排除的是保护保证人地位。保护保证人地位证立的基础在于保证人与被害人之间的信赖关系。^[29]法律为何要求父母对于其未成年子女的法益承担保护保证人义务，为何在夫妻之间设定这种义务，原因在于二者之间存在一种稳固的制度化信赖关系。显然在一般情形下，网络服务提供者与其用户之间不存在类似于父母对其未成年子女或者配偶之间的稳固制度化的依赖或保护关系。但除了这种保护保证人地位之外，德国刑法还承认因自愿承担而产生的保护保证人。这种类型的保护保证人是否可以适用于网络服务提供者与其用户呢？对此，德国学者否认了这种可能性，认为即使是以处于弱势的特定法益群体为对象的网站，例如主要以青少年用户为服务对象的青少年娱乐或学习

[27] 相同的观点参见周光权，见前注[14]，第64—65页。

[28] Kaufmann, Die Dogmatik der Unterlassungsdelikte, 1959, S. 282 ff; Kindhäuser, Strafrecht Allgemeiner Teil, 4. Aufl., 2009, § 36, Rdn. 52.

[29] Wohlers/Gaede in: Kindhäuser/Neumann/Paeffgen, 4. Aufl. 2013, § 13, Rdn. 34, n. w. N.; Schuenemann(Fn. 25), S. 344 ff, 350 ff; Rudolphi, Haeuserliche Gemeinschaft als Entstehungsgrund fuer Garantenstellung, NStZ149, (1984), 150 f.

网站,也不能认为其具有因自愿承担而产生的保护保证人地位。^[30]理由是,因自愿承担而产生的保护保证人地位虽然不像普通保护保证人地位那样具有稳固的制度化依赖或保护关系,但是也存在着一种类似的信赖关系,例如保姆与其所照管的儿童、登山队领队与登山队员、游泳池救生员与游泳者之间,皆存在着一种暂时的、替代性的信赖与保护关系。而青少年娱乐或学习网站服务提供者与青少年用户之间则不存在这样一种关系,但这种关系与“网络服务提供者和青少年用户间的关系”究竟是否或者存在何种质的不同呢?德国学说上并未有进一步地论证。在笔者看来,上述保姆、登山领队等因承担而产生的保护保证人地位,是一种对父母与未成年子女、夫妻之间等稳固的制度化关系的拟制,在父母、夫妻一方不在场时提供一种替代性的保护。之所以设置这种替代性的保护责任,是因为上述行为人在其他保护保证人缺席时在场,而能够替代性地避免损害结果发生。但是在网络服务提供者与用户之间的这种匿名性的、远程性的、松散性的关系之中,显然很难进行这种拟制。

(2)监管保证人地位。排除了保护保证人地位之后,在功能二分法框架下尚须探讨网络服务提供者是否具有监管保证人地位。首先检验先行行为引发的监管保证人地位,网络服务提供者提供网络信息服务的行为是否可以被视为先行行为呢?德国学说与判例界定先行行为范围的观点主要有“义务违反标准”“社会相当性标准”以及“义务违反标准+结果发生的紧密危险标准说”,而以罗克辛(Roxin)为代表的学者则基于客观归责理论认为先行行为必须是创设了法所不容许的风险的行为或使得一个业已存在的风险升高的行为。^[31]

显然,无论按照上述哪一种理论,都无法得出网络服务提供者一般性地提供普通网络信息服务的商业行为属于先行行为的结论。在通常的商业模式中,网络服务提供者提供合法的服务行为,即一般性的网络接入、网络存储或者信息定位服务;其是数字时代沟通交流所不可或缺的,属于社会普遍认可的具有社会相当性的行为,或者如互联网领域所称的“技术中立行为”,因而一般说来也未创设法所不容许的危险。即使这种服务导致不法内容或犯罪行为信息的传播,也不能据此即认为该服务是非法服务。^[32]例如网站A上存在他人设置的非法链接,用户点击后进入色情网站B或者宣扬暴力犯罪的网站C,也不能就此认为A网站提供的网络存储服务不属于社会相当性的行为或者包含法所不容许的风险,甚至认定A承担因先行行为引发的不作为刑事责任。因为自互联网技术诞生之初,就难免有被滥用之风险;互联网是由无数网站、主页、链接、BBS、Email、搜索引擎等构建的空间,其信息路径交错纵横,难免最终会通向某个犯罪信息。但是即便如此,它带来的沟通迅捷的利益也远远超过了可能包含的被滥用之风险(传播犯罪信息),因而是法律所容许的风险。

在功能二分法的框架下,接下来尚需探讨的是网络服务提供者是否具有类似危险设备运

[30] Boese, (Fn. 7), S. 157.

[31] 参见王莹,见前注[26],第333—337页。

[32] Derksen, Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt, NJW 1997, 1883; Sieber/ Höfinger (Fn. 2), Teil 19.1, Rdn. 37 ff.

营人或者危险动物的饲主那样的危险源监管的保证人地位。网络技术提供了匿名与远程的传播可能性,P2P平台、BBS网站、搜索引擎等都存在着被用户滥用而传输非法信息的可能。因此,可将互联网视为不法信息的危险源,探讨其危险源监管的保证人地位。德国刑法通说对网络服务提供者保证人地位的论证,也是从这个角度展开的。^[33]

而鉴于网络传播行为的技术性,在借用传统犯罪危险源监管这一教义学资源时,应当充分考量网络技术功能以及网络社会关系结构的特殊性。危险源监管保证人地位的前提是对危险源具有管控或监管职责,例如在分析网络存储服务提供者对其信息存储的服务器管控时,虽然我们可以将这种管控与现实物理空间中房屋所有人对其房屋空间的控制支配进行类比,但仍不应忽视二者之间的差别。前者的控制是在感官可触及的范围之内,因而更加直接与可感,而对服务器上的信息感知却显然不同。因此,有必要在了解网络传播服务行为的技术功能类型与特征的基础之上,对信息传输过程的管控与支配进行分析。^[34]

1)网络存储服务提供者。从技术角度来看,信息存储服务提供者可以在自己的服务器上进行数据存储和删除,因而对其所存储的信息与服务器具有技术上的控制,相应地就具有不对他人造成损害的职责。但与对物理空间的控制与支配不同,其必须结合网络信息传播技术环境来进一步地予以限定。第一,由于信息不断上传与删除,其处于不断的变化更新状态,例如一个较大的信息存储服务提供者的服务器可能存储成千上万个内容服务提供者的主页,每个主页还可能提供大量网页,而这些网页上的大量信息都处于持续的更新变化之中。第二,存储在服务器上的部分信息可能是不开放的,例如,在不开放的用户群组内部传输加密数据,或者一些不法内容提供者对网页设置密码,那么对这部分信息进行控制就会涉及个人信息保护的法律问题。第三,从网络过滤技术来看,目前的网络内容分级、URL过滤、文本内容过滤、图像过滤等技术均存在很大的限制,如存在过滤不精准、易于被规避、执行时间过长而导致无法接受的网络延时等问题。^[35]因此,要求网络存储服务提供者主动审查过滤所有的不法信息,在技术上是现实的,国际上和我国立法者也都否定了的主动审查义务(参见上文五(一)部分论述)。故而这种危险源监管是被动性而非主动性的,只有当信息存储服务者对涉嫌违法犯罪的

[33] Sieber/ Höfinger (Fn. 2), Teil 19.1, Rdn. 43; Hoernle in: Joecks/ Miebach, (Fn. 24), § 184, Rdn. 51.

[34] Sieber教授在论证网络服务提供者危险源监管保证人地位采取的进路是,首先探讨危险源的控制,然后在此基础上进一步予以规范视角的限制。例如如果公众或周围环境形成了一种信任相信不作为者将会控制可能出现的危险时,便具有保证人义务。但是正如Sieber教授自己所承认的,这种规范上的信任期待需要长时间的社会生活才能形成,而网络空间作为次生生活空间恰恰缺乏这种规范期待形成所需要的时间,在这个项下他唯一想到的可能的限制就是“存在具体的明显违法信息的明知”(Sieber/ Höfinger (Fn. 2), Teil 19.1, Rdn. 43),但这一点正是信息网络传输技术环境中判断控制所需考虑的因素之一,因此是一种多余的循环论证。故笔者认为与传统上的危险源监管保证人地位不同,对网络服务提供者危险源监管保证人的论证不需要附加规范上的限制。

[35] Sieber, Verantwortlichkeit im Internet : technische Kontrollmöglichkeiten und multimedienrechtliche Regelungen : Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, 1999, S. 90ff, S. 97; 林建、张帆:“网络不良信息过滤研究”,《情报理论与实践》2007年第4期,第534—539页。

信息有具体的认知或者具体的怀疑时，^[36]才应删除或断开链接，否则即对此承担不纯正不作为责任。

2)系统缓存服务提供者。自动化暂时性的信息缓存服务的性质，介于接入服务与信息存储服务之间，从技术角度来看类似于信息存储服务，但从功能上来看则属于接入服务。^[37]由于缓存服务提供者也将信息存储在自己的服务器上，因此对这部分信息也有监管职责，^[38]但同样基于上述虚拟空间与物理空间的区别，其也仅承担被动的监管职责。即只有存在对所存储的涉嫌违法犯罪的信息有具体认知或者具体的怀疑时，才产生不纯正不作为的刑事责任。

3)网络接入服务提供者。接入服务提供者所传输或以传输为目的临时存储的信息存储在他人服务器上，因此从技术上来看，其不具有类似网络存储服务提供者对信息的监管能力。接入服务提供者所传输的信息数据来自于整个互联网的无数他人服务器，一方面从数量上来说说是浩如烟海，另一方面从状态上来看这些传输中的数据也处于实时变动之中，因此与网络存储提供者相比其发现违法犯罪信息的难度大大增加。^[39]而且即使发现了违法犯罪信息，由于缺乏对他人服务器的支配权限，接入服务提供者也无法对信息进行直接删除，只能尝试阻断通向不法信息的路径，即隔离连接或屏蔽。因此，鉴于网络接入服务的单纯技术性、自动化与被动性特征，^[40]其所传输或以传输为目的短暂存储的信息无法进行控制，因而不具有危险源监管的保证人地位。故而网络接入服务提供者在为用户提供接入服务之后，即使得知所传输的信息涉嫌违法犯罪，也因不具有保证人地位而对用户所发布信息造成的损害不承担不纯正不作为的刑事责任。^[41]

4)信息定位服务。搜索引擎自动、持续、系统地从网络空间搜寻信息，然后将这些信息用其索引程序进行选择、存储与编排，并以搜索结果列表的形式向用户转送或提供，由于搜索引

[36] 在对不法信息的具体怀疑方面《远程媒体法》与《数字千年版权法》表述略有不同，前者将免责条件规定为：“1.其对违法行为或信息没有认识或者在损害赔偿请求情形下也未认识到对其来说可以明显看出违法行为或信息的事实或情状 2.一旦知晓上述情况，立即采取行动删除信息或者断开这些信息的连接”（该法第 10 条第 1 款）。而后者免责条件的规定表述为：“A i 如果其未现实地认识到：材料或使用这种材料的行为构成侵权；ii 在缺乏这种现实认识的情况下，未意识到显然构成侵权的事实；iii 在获得上述认识或者意识到上述情形下，立即删除该材料或隔离对该材料的连接；B.如果服务提供商对侵权行为具有控制权利与能力时，未直接接受来自侵权行为的经济利益；C.在接到第(3)段所述的侵权投诉时立即删除侵权材料或隔离对其的连接”（U.S.Code ,Title 17, § 512 (c)）。

[37] Sieber, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen(I) – Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups des Internet, CR 581(1996), 589.

[38] 德国通说也肯定缓存服务提供者的危险源监管保证人地位, Sieber/ Höfinger(Fn. 2), Rdn. 50.

[39] Sieber(Fn. 37), S. 97.

[40] 参见欧盟电子商务指令立法说明第 42 条: Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr) (ABl. Nr. L178 S. 1) Nr. 42.

[41] 不同观点见 Hilgendorf(Fn. 3), S. 71.

擎也将他人信息(通过索引程序)存储在服务器上,^[42]因而搜索服务提供者也因对服务器具有管控权限,而具有类似于网络信息存储服务提供者的危险源监管保证人地位。^[43]但是,由于搜索引擎对信息的搜索不是通过人类的思维内容进行,而是通过搜索器、索引器的数学计算自动进行;^[44]搜索的网页信息量巨大且处于持久的更新变动之中,因此对搜索的信息进行逐条审查不具有技术上的可能性。此外,过滤软件也同样具有上述导致网络延时、搜索效率降低以及无法精准过滤等问题,故而只有当搜索引擎服务提供者认识到某条信息可能涉嫌违法犯罪时,才有义务将其从搜索结果列表中移除。

其实,上述不同类型的保证人地位也可以在下例中予以更加清晰的说明。

例1:甲女与前男友乙分手,乙出于愤恨将甲的裸照上传到电子论坛丙,引起大量网友围观,丁作为搜索引擎服务提供者通过自动搜索与索引程序将电子论坛丙的图片链接列入搜索结果列表。若丙和丁提供网络服务时即知道该图片内容,则成立第287条之二帮助信息网络犯罪活动罪;若丙、丁不仅具有单方面的认识,还与乙具有共同故意,则此外还成立侮辱罪与传播淫秽物品罪的共同犯罪(若图片点击量达到相关司法解释要求的起刑点),根据287条之二第2款以处罚较重的罪名定罪量刑。若丙、丁提供服务时未认识到图片内容,甲得知自己的裸照在网络上传播后通知了丙与丁删除该链接,但是丙、丁不予删除的,则因丙与丁对自己服务器具有的控制与监管权限,可以肯定其具有危险源监管保证人地位,并进而认定丙、丁构成不作为形式的侮辱罪与传播淫秽物品罪。

值得进一步思考的是,存储型的网络服务提供者,即网络存储、系统缓存与搜索引擎服务提供者是否对所有类型的他人信息均具有危险源监管的保证人地位?网络服务提供者的不纯正不作为犯罪范围又是否存在一定的边界呢?对此,我们需要再次求诸危险源监管保证人地位的教义学分析框架。即功能二分法理论下的危险源监管保证人地位与保护保证人地位的区别在于,阻止损害发生的义务范围不同,前者仅针对危险源可能发生的危险负有防止其实现并导致损害结果发生的义务;而后者的范围更为广泛,对处于弱势地位的法益所有者具有广泛的保护职责,并对来自于法益所有者本人、第三人或者自然界等一切可能的致其法益损害的因素都负有损害防止的义务。因此,危险源监管保证人所防御的风险是危险源所特有的、内在的,而不可能是任何类型的风险,^[45]也即只有危险源所特有的风险才属于保证人的风险管辖范围。而网络空间所特有的风险是违法犯罪信息的高速传输,存储型的网络服务提供者对所存储的信息传播具有技术上的控制与监管,因此其对信息的传播具有风险管辖,对违法信息传

[42] Spindler/Schuster (Fn. 2), Rdn. 33.关于搜索引擎的存储结构也可参见宋聚平、王永成:“搜索引擎中信息存储结构的改进”,《情报学报》2001年第5期,第515—517页。

[43] Sieber/Höfinger (Fn. 2), Rdn. 50.

[44] Reber in: Ahlberg/Götting, 14. Aufl. 2015, (Hrsg.), UrhG § 97 A, Rdn. 78.

[45] 危险源监管保证人地位来自于侵权法上的交往安全义务,即如果物根据其特征可能给他人带来危险,物的所有人或管理人就具有危险防止的作为义务,这种危险主要来自于危险物本身或者危险的技术操作过程。参见 Roxin, Strafrecht Allgemeiner Teil, Band. II, 1. Aufl., 2003, § 32, Rdn. 111 ff.; Schuenemamm (Fn. 25), S. 281.

播这一损害后果也具有保证人地位。但其仅对那些将特定信息的传播规定为构成要件行为的犯罪(即交流犯)承担不纯正不作为责任,而对于超出网络信息传播过程之外的现实世界中的风险与风险实现,不具有危险源监管的保证人地位。

因此,对于信息的传播本身就是构成要件所禁止的内容即交流犯而言,存储类型的网络服务提供者具有保证人地位。而对于非交流犯而言,由于发布或传播信息本身并非构成要件行为,这类信息本身往往并不会直接造成法益侵害,而是与行为人自己或他人的现实世界的行为结合才会造成法益侵害,例如诈骗罪、故意伤害罪、故意杀人罪等传统犯罪。但是这已经超越了网络传播的范围,超越了网络服务提供者的风险管辖范围,因此其对此种损害后果不具有危险源监管的保证人地位。

例 2:某用户 A 在某分类广告网站(类似于 58 同城之类的网站)B 或者在某小区的业主论坛 C 发布了诈骗信息,某宽带公司 D 分别为 A 和 B、C 提供网络接入服务,B 和 C(网络存储服务提供者)的管理员或者版主看到了该信息并向该公司报告,但二公司未要求上述两人对该信息进行删除,D 在进行信息审查检测时发现了 A 发布的信息内容,但是也未采取任何措施,结果 E、F、G 等用户访问该信息后往 A 指定的账户汇入了若干款项。那么,上述行为人应负何种责任呢?

A 属于广义的网络内容服务提供者,成立第 287 条之一非法利用信息网络罪与诈骗罪,按照处罚较重的犯罪论处,如果数额较大则一般按照后者论处;D 作为网络接入服务提供者不具有危险源监管保证人地位,至多仅成立第 287 条之二帮助利用信息网络犯罪活动罪。而 B、C 虽然属于网络存储服务提供者,但对于诈骗罪这种非交流犯不具有风险管辖,对于 E、F、G 等用户访问该信息后的一系列线下行为(如 A 及其同伙开设用于诈骗的账户,E、F、G 等用户访问该信息后果真陷入错误并在该错误作用下往 A 设定的账户中汇钱等等)所导致的被害人财产损失的后果显然不具有危险源监管的保证人地位。若没有被害人与行为人一系列的线下行为,E、F、G 等用户的财产损失后果也不会发生。因此,对于诈骗罪财产损失的后果而言,不承担不作为责任。但若主管机关要求 B、C、D 删除该信息或者断开对其的连接,而其拒不断开的,则仍可成立第 286 条之一规定的拒不履行信息网络安全管理义务罪。

综上,网络服务提供者的不纯正不作为刑事责任存在两重限制。其一,从技术角度来说,要对用户发布的信息具有危险源监管的能力与职责,而一般来说仅存储类型的服务提供者(包括网络存储、系统缓存与信息定位服务提供者)才具有这种技术监管能力。其二,从危险源监管的危险类型或风险管辖角度来说,仅交流犯(即以传播违法犯罪信息为内容的构成要件类型)的风险才属于管辖范围内的风险,而其它犯罪类型的风险则须结合他人在现实世界的线下行为才能实现,不属于网络传播服务行为所固有的危险。区分交流犯与非交流犯,否定网络服务提供者在非交流犯情形下的保证人地位,实际上是在网络世界与现实世界之间设立了一堵界定保证人地位的“防火墙”,以防止超越网络传播行为的风险,并将现实世界传统犯罪行为的风险及其防御也加诸网络服务提供者之上,对其施加过重的责任。而这道划定保证人地位边界的防火墙,只有共同的故意才可以穿透;如果网络服务提供者与发布违法犯罪信息的用户具有共同犯罪的故意,如在例 2

中, B、C 与用户 A 合谋实施诈骗, 由 A 发布信息并实施线下设立账户等行为, 那么根据共同犯罪原理, 显然 B、C 作为共犯对诈骗罪的结果也承担责任。虽然这首先是作为犯罪的问题, 但如果承认作为犯罪也可以引发保证人地位的话, 则理论上也应当肯定其保证人地位。^[46] 另外需注意的是, 网络服务提供者构成相应的不纯正不作为犯罪, 同时其不履行信息网络安全管理义务也可能成立第 286 条之一的纯正不作为犯罪, 此时应根据该条第 3 款的规定“有前两款行为, 同时构成其他犯罪的, 依照处罚较重的规定定罪处罚”, 从一重罪论处。

六、结 语

由于互联网次生空间的规制经验衍生于传统现实世界这一原生空间, 在传统刑法中区分对自己行为和对他人行为(共犯与不作为犯罪领域)的二分法归责逻辑则必然会向网络空间责任进行延伸, 因此自己发布的信息与他人发布信息的归责二分法就成为我们探讨互联网领域责任归属与分配的理论原型。另一方面, 网络技术传播特征与网络用户和网络服务提供者的新型网络社会关系结构决定了不能对这一传统教义学的理论原型进行僵化的理解与套用。笔者提倡根据网络传播技术功能以及与之相联的新型网络社会关系特征对共同犯罪、保证人地位等教义学原理予以新的技术角度的注疏与填充, 构建中国网络涉罪信息归责模式, 探索网络服务提供者刑事责任条款的教义学路径。

第一, 《刑法修正案(九)》第 287 条之一规定了对自己发布信息的责任, 以此对网络服务提供者按照传统刑法教义学对自己发布信息的责任进行补充与无缝化对接, 即将线上预备行为的正犯化排除了这种行为作为预备犯在事实上不被追诉的可能性。因此, 需要明确第 287 条之一规定的是对自己发布信息的刑事责任, 而为上述行为提供帮助者是以第 287 条之二论处, 否则会使得第 287 条虚置并产生繁复的竞合问题。

第二, 第 287 条之二规定了“因他人的信息而对自己(帮助)行为的责任”, 以此对网络服务提供者按照一般的共犯原理来为他人信息(或行为)承担责任进行补充与无缝化对接, 即针对他人信息的归责偏离共犯归责模式, 而引入一种介于共犯与正犯之间的混合归责模式。这种混合归责模式实际上是对传统教义学中区分自己行为 and 他人行为的归责二分法的修正。由于网络用户与网络服务提供者的关系结构具有匿名性、远程性、发散性特征, 后者作为信息的传输者与前者作为信息的发布者之间往往缺乏直接的接触与犯意的沟通; 但是信息传播的损害结果却存在网络空间的放大效应, 因此出于“及时止损”的功利主义考虑, 网络服务提供者更可能被赋予比传统现实空间中的帮助者更加严格的责任。^[47] 这是笔者对第 287 条之二作出的教义学与法律经济学的折衷解读。

[46] 参见王莹:“论犯罪行为人的先行行为保证人地位”,《法学家》2013年第2期,第119—129页。

[47] 刘艳红教授指出网络服务提供者帮助行为正犯化的“类推思维”根源在于管控的便利考量, 参见刘艳红:“无罪的快播与有罪的思维——‘快播案’有罪论之反思与批判”,《政治与法律》2016年第12期,第111—112页。

因此,对于第 287 条之二作为帮助犯正犯化的规定,应当抛开共犯框架下的中立帮助犯理论而根据一般的归责原理予以解读。即归责依据在于对所传输涉罪信息的特殊认知,如此主观不法便成为归责的唯一依据与本罪不法的重点,故而应对行为人的主观方面采取限制解释,以缓和因客观方面限制的缺乏而带来的责任过度扩张。

第三,关于为他人发布的网络涉罪信息所承担的不纯正不作为犯罪刑事责任,应充分挖掘传统刑法危险源监管保证人地位的教义学资源,结合网络传播的技术特征,合理地界定保证人地位。也即,仅承认存储类型的服务提供者(包括信息存储服务提供者、系统缓存服务提供者与信息定位服务提供者)在技术上的危险源监管能力,并且仅对交流犯的法益侵害具有风险管辖,从而在网络世界与现实世界之间设立一堵界定保证人地位的“防火墙”,避免网络服务提供者不纯正不作为刑事责任的泛滥。

Abstract: In Web 2.0, the question who should be responsible for the damage caused by criminal internet information has become the key issue of criminal law in the digital age. To better understand the culpability of Internet service providers, this essay tries to interpret the clauses of criminal liability in Amendment (IX) to the Criminal Law of the PRC and clarify the internal logic according to the principles of network technology communication. First of all, internet service providers who send messages for themselves shall be convicted and punished according to Article 287A. Meanwhile, whoever provides any assistance for the mentioned crime shall be convicted and punished according to Article 287B, which could take full advantage of Article 287B and diminish the chaotic situations of concurrence. Furthermore, Article 287B shall be based on general liability principles rather than neutral-assistance theory as the providers are convicted because of others' behaviors, which means the mens rea—provider's special knowledge of the transmission of criminal information—has become the only and essential foundation of culpability. Thus, in order to decrease the over-expansion of criminal liability, we shall interpret the subjective aspect of the perpetrator restrictively. Ultimately, to identify the guarantor status and omission culpability of internet service providers rationally, the dogmatic resources of guarantor status of danger supervision, combined with the characteristics of internet technology communication, shall become the starting point.

Key Words: Communication Crime; Non-communication Crime; Participation Turning to Perpetration; Guarantor Status of Danger Supervision; Risk Management

(学术编辑:车 浩)

(技术编辑:张晓媛)