论拒不履行信息网络安全管理义务罪

谢望原*

内容提要 “信息网络”包括公用电话网、广播电视网和计算机网；本罪行为主体包括网络接入服务提供者、网络平台服务提供者、网络内容及产品服务提供者；本罪行为事实必须同时满足“不履行信息网络安全管理义务、经监管部门责令采取改正措施而拒不改正、行为符合刑法规定的四种情形之一”。作者主张，本罪主观方面只能是直接故意，同时须有违法性认识；行为人发生违法性认识错误时，不宜以本罪论处。作者还认为：本罪与有关危害国家安全罪的核心区别在于有无危害国家安全的目的；本罪只有既遂而没有未遂；不能以“中立帮助行为”为由否定信息网络服务提供者不履行网络安全管理义务的相应责任。

关键词 网络安全 管理义务 行为要素 心理要素 违法性认识错误

引 言

由于计算机技术的迅速普及并被广泛运用于我们生活的方方面面，今天的社会早已变成了“天网恢恢”的网络世纪。物联网(internet of things)①或“互联网+”大数据时代的来临，更使我们的全部生活与信息网络紧紧联系在一起。网络安全乃是一个关系到国家安全、社会公共安全、国家和公民财产安全、个人生活以及信息安全的极其重大的社会问题，国家必须加大对信息网络安全的保护力度。为了有效地管理网络安全秩序，我国已经先后出台了诸多有关信息网络安全管理的法律、法规，它们多数具有行政法律、法规性质，也包括有关刑法性质的规定。② 但是客观而言，我国原有立法并不足以

* 中国人民大学刑事法律科学研究中心教授，博士生导师。

① 物联网即物物相连的互联网，被称之为继计算机、互联网之后信息产业发展的第三次浪潮。信息来源：载 http://baike.baidu.com，最后访问时间：2016 年 11 月 2 日。

② 根据中央网络安全和信息化领导小组办公室、国家互联网信息办公室政策法规局编写的《中国互联网法规汇编》，我国有关互联网管理的法律有三部、行政法规 10 部、部门规章 28 部、司法解释 13 部、规范性文件 32 件，此外，另有其他 28 部法律规定了有关互联网信息管理的内容，涉及刑事、民事、行政等方面事项。2016 年，全国人大常委会颁布了《中华人民共和国网络安全法》(以下简称《网络安全法》)，国务院发布了第二次修订后的《互联网上网服务营业场所管理条例》，国家网信办发布了《信息网络传播权保护条例》(修订版)、《移动互联网应用程序信息服务管理规定》、《互联网信息搜索服务管理规定》，国家发展改革委等 14 部门联合颁布了《公共资源交易平台管理暂行办法》，国家工商总局发布了《互联网广告管理暂行办法》，等等。

有效地对繁纷复杂的网络违法犯罪进行打击与防范。有鉴于此,作为《刑法》第286条之一,《刑法修正案(九)》第28条新增设了拒不履行网络安全管理义务罪。

所谓拒不履行网络安全管理义务罪,是指网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务,经监管部门责令采取改正措施而拒不改正,符合《刑法》第286条之一第一款规定的四种情形之一的行为。由于本罪尚属新罪,不仅我国刑事司法实践中目前还没有本罪的判例,学术界至今亦未对其展开系统而深入地研究,而国家与公民时时刻刻都处在复杂的网络关系之中,故全面、透彻地研究本罪的相关问题,厘清网络服务提供者的刑事法律责任与界限,从而有效地保护包括网络服务提供者在内的全社会利益和网络安全,这已经是迫在眉睫的问题。

一、行为要素(Actus reus)

在两大法系的刑法理论体系中,行为要素均属于犯罪构成的客观要素,包括行为主体[③]、侵害法益(客体、利益)以及与作为、不作为相关的行为表现要素等。

(一)作为客观要素的行为主体

从立法安排来看,拒不履行信息网络安全管理义务罪被放在《刑法》第286条之一的位置,处在《刑法》分则第6章第一节之中,属于"扰乱公共秩序罪的范畴",它所侵犯的法益乃是社会管理秩序所涵盖的信息网络安全管理秩序。本罪主体仅限于网络服务提供者。那么何谓"网络服务提供者"?世界上有关国家和地区对此有不同的规定和界定。欧洲理事会《网络犯罪公约》(Convention on Cybercrime,2001)曾经将计算机系统"服务提供者"解释为:任何通过计算机系统能够给用户提供交流服务的公共的或私营的实体(entity)和任何为了该交流服务或该服务用户处理或储存计算机数据的其他实体。[④] 而根据1998年美国《数字千禧年著作权法》(The Digital Millennium Copyright Act)第二部分"在线著作权侵权责任限制"的规定,其所指"在线服务提供者(online service provider)"涉及四种行为类型——即时通讯(Transitory communications)、系统缓存(System caching)、按照用户指示存储信息(Storage of information on systems or networks at direction of users)以及信息定位工具(Information location tools)。据此,该法所称的服务提供者是指提供信息传输、路由[⑤],或者提供用户指定的、用户选择素材的点之间数字在线交流链接,而对所传送或接收的素材内容不作修改的当事人,以及在线服务、网络接

③ 在两大法系的刑法学理论中,行为主体均作为犯罪成立的前提要素而不在构成要件中加以研究。但是,在中国占主导地位的"四要件"犯罪构成理论中,一直将行为主体作为一个重要构成要件来看待。考虑到行为主体本质上属于犯罪构成的客观因素,故本文将其纳入行为要素之中。

④ *See* Article 1 c of Convention on Cybercrime. 信息来源:载 http://wenku.baidu.com,最后访问时间:2016年7月22日。

⑤ 路由是指路由器从一个接口上收到数据包,根据数据包的目的地址进行定向并转发到另一个接口的过程。

人的提供者,或者设备运营者⑥。

由于前述欧美法律是 10 多年或近 20 年前的立法,当时它们关于"服务提供者"的规定均以计算机网络系统为依归,并未涉及传统的电话网和电视网。但是就我国的政治与经济政策情况来看,第九届全国人民代表大会第四次会议 2001 年 3 月 15 日通过的《中华人民共和国国民经济和社会发展第十个五年计划纲要》(第六章)已经明确提出了"三网融合"的发展目标,国家开始积极支持电信网、广播电视网、计算机网的发展,促进三网的逐步融通和融合,保证国家信息化建设的健康发展。⑦在此之前,我国通常将信息网络区分为公用电话网、广播电视网和计算机网。虽然这三种网络有各自的形成过程、服务对象和发展模式,其网络功能有所交叉,互为补充,但目前我国已经基本实现"三网融合,互联互通",故"信息网络"包括了公用电话网、广播电视网和计算机网。也就是说,信息网络应当"是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络和系统"⑧。因此,在我国当前的法律语境下,网络服务提供者就不能只局限于早期欧美立法上的"服务提供者"的范围,而是包括了公用电话网服务、广播电视网服务和计算机网络服务的提供者。具体言之,网络服务提供者是指通过信息网络向公众提供信息,或者为获取网络信息等目的提供服务的机构或个人,包括信息网络上的一切提供设备、信息和中介、接入等技术服务的个人、网络服务商以及非营利网络服务提供者。根据其提供的"服务"类型来划分,网络服务提供者具体可分为网络接入服务提供者、网络平台服务提供者、网络内容及产品服务提供者。

何谓网络接入服务提供者(Internet Access Provider)? 关键在于如何准确理解"接入服务"——即为接入信息网络而进行的各种配套服务。"接入"并不仅仅指连接一个宽带光纤等物理接入,也指把一个网站等信息载体成功与互联网连接,为接入互联网而进行的一系列配套增值服务,如空间出租,服务器托管等,因此,接入服务提供者就是所有为信息网络用户提供联通信息网络服务的单位或个人。网络平台服务提供者(Internet Presence Provider)是指提供搜索引擎服务,网络存储、分享服务,电子商务服务平台、社交网络服务平台等平台服务的提供者,包括单位和自然人。网络内容及产品服务提供者即指为网络用户提供网络内容和网络产品服务的单位或自然人。具体言之,网络内容提供者(Internet Content Provider)即向网络用户综合提供网络信息业务和增值业务的运营者,如新浪、搜狐等;至于网络产品⑨提供者,对此关键在于正确把握"网络产

⑥ *See* THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998. 信息来源:载 http://www.copyright.gov/legislation/dmca,最后访问时间:2016 年 8 月 9 日。

⑦ 根据《中华人民共和国国民经济和社会发展第十个五年计划纲要》要求,国家工业和信息化部已经公布一系列的国家三网融合战略计划。根据规划,我国三网融合工作将分两个阶段进行。其中,2010 年至 2012 年重点开展广电和电信业务双向进入试点;2013 年至 2015 年全面实现三网融合发展。

⑧ 《网络安全法》第 76 条第(1)项。

⑨ 网络产品本质上是传统意义上"产品"的延伸,是在信息网络领域产出而用于经营的商品,它是满足信息网络用户需求和欲望的无形载体。

品”。网络产品是指网站为满足用户需求而创建的用于运营的功能和服务，它是网站功能与服务的集成，如腾讯的产品是“QQ”，博客网的产品是“博客”等。网络产品提供者即为用户提供满足其需求的信息网络功能与服务的信息网络运营者。

以上分析表明，自然人和公司、企业等单位均可以成为本罪主体，并且，网络服务提供者作为本罪的主体，与其提供的网络服务是否具有营利性毫无关系。不过，在认定具体责任主体时，应当根据具体情况具体分析，准确认定个案的具体责任人。也就是要查明具体犯罪发生的具体环节，弄清究竟是哪一个或者处在哪个环节的网络服务提供者的不履行义务行为与违法后果具有因果关系，不可任意扩大责任范围，株连无辜。

（二）作为客观要素的行为事实

本罪的具体构成要件行为事实，表现为行为人不履行信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，行为人具有符合《刑法》第286条之一第一款规定的四种情形之一。作为本罪的行为事实，必须同时满足以下三个方面条件：

1. 不履行信息网络安全管理义务

所谓义务，是相对于权利的一个概念，乃指法律上、道义上应尽的责任，包括作为义务与不作为义务。以价值哲学观点来解释，如果说权利是相对于义务的一种价值回报，那么义务则是相对于权利的一种价值付出。而管理义务则是作为具有管理责任的人，因其职务或业务的内在特性，法律所赋予的一种监督管理责任。网络服务提供者作为社会生活中的一员，他们所经营业务的行为必须合乎法律的规范要求，法治国家没有法外之人（包括自然人和法人），任何人及其其经营行为，哪怕是行使权利的行为，都必须保证自己的行为不会危及社会和他人。因此，国家法律赋予网络服务提供者相应的管理义务（责任）当然具有合理性。

从《刑法》第286条之一的规定来看，本罪是一个纯正不作为的义务犯，只能由不作为构成。虽然学界对有关不纯正不作为犯之作为义务来源争议不断，[⑩]但对纯正不作为犯之作为义务来源已有共识，即纯正不作为之作为义务只能是法律、法规有明确规定者。“所谓有明确规定者”是指纯正不作为犯之作为义务只能是法律、法规已有具体规定，且为刑法明确规定公民具有作为义务的情形（如税法规定公民有纳税义务，对于不交税款的情形，刑法规定了逃税罪）。作为一种典型的义务犯，本罪涉及的网络安全管理义务就是信息网络服务提供者[⑪]依法应当履行现行有效的信息网络安全管理法律、法

---

⑩ 不纯正不作为之作为义务来源，我国学界一般认为主要有：（1）法律、法规规定的义务；（2）行为人职务或业务上要求的义务；（3）行为人实施的法律行为引起的义务；（4）由于行为人的先前行为使某种合法权益处在遭受损害的危险状态而产生的防止损害结果发生的义务。参见许成磊：《不纯正不作为犯理论》，人民出版社2009年版，第253页。德国刑法理论上关于不纯正不作为犯之义务来源研究的十分复杂，且深刻细致，但大体上认为有四个来源：（1）法律规定；（2）合同约定；（3）先行行为；（4）其他原因。参见[德]冈特·斯特拉腾韦特、洛塔尔·库伦：《刑法总论I：犯罪论》，杨萌译，法律出版社2006年版，第362-375页。

⑪ 《刑法》第286条之一的开头语句使用的是“网络服务提供者”，但后续语句中使用了“信息网络安全管理义务”，联系全条规定来看，这里的“网络”与“信息网络”应该是同义词，即均指“信息网络”。本文正是在此理解基础上使用“网络”或“信息网络”这两个术语。

规所明确规定的信息网络安全管理的作为和不作为义务。根据《网络安全法》第 21 条的规定,包括网络服务提供者在内的网络运营者⑫的一般安全管理义务是:"国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求,履行下列安全保护义务,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改:(一)制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任;(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;(三)采取监测、记录网络运行状态、网络安全事件的技术措施,并按照规定留存相关的网络日志不少于六个月;(四)采取数据分类、重要数据备份和加密等措施;(五)法律、行政法规规定的其他义务。"至于网络服务提供者的各项具体网络安全管理义务,则散见于大量的有关规范网络运营与管理的法律、法规之中。由于这些法律、法规规定的具体情况十分复杂,为了便于阐释网络服务提供者究竟应当遵守哪些信息网络安全管理义务,笔者将其分为两个类型分别加以说明——禁止性规范为网络服务提供者设定的义务和命令性规范为网络服务提供者设定的义务。

第一,禁止性规范设定的义务。禁止性规范(prohibitive norm)是指规定人们的消极义务(不作为义务),即禁止人们做出一定行为的规范。禁止性规范立法用语的表达范式通常为:"禁止……"、"不准……"、"不得……"、"严禁……"等。禁止性规范设定的义务是指法律、法规明确禁止实施某些行为,⑬行为人(如网络服务提供者)必须约束自己的行为,不得做出超越禁止规范的事项。如果行为人没有遵守禁止性规范或超越了禁止性规范,则构成义务违反。对于此类规范的违反,行为人之行为通常表现为作为的形式。⑭ 例如,《网络安全法》第 12 条第 2 款规定:"任何个人和组织使用网络应当遵守宪法法律,遵守公共秩序,尊重社会公德,不得危害网络安全,不得利用网络从事危害国家安全、荣誉和利益,煽动颠覆国家政权、推翻社会主义制度,煽动分裂国家、破坏国家统一,宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息,编造、传播虚假信息扰乱经济秩序和社会秩序,以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。"又如国家互联网信息办公室《互联网直播服务管理规定》第 15 条第 2 款规定:"互联网直播服务提供者应当建立黑名单管理制度,对纳入黑名单的互联网直播服务使用者禁止重新注册账号,并及时向所在地省、自治区、直辖市互联网信息办公室报告。"这里,法条中的"不得……"、"禁止……"就是禁止性规范,网络服务提供者不得以作为的形式做出法律、法规所禁止的行为。立法者在现行信息网络安全管理的法律、法规中设定了大量禁止性规范,网络服务提供者必须严格遵守这些规范,凡是违背此类禁止性规范设定义务的,就是不履行网络安全管理义务。

---

⑫ 参见《网络安全法》第 76 条第 3 项规定:"网络运营者,是指网络的所有者、管理者和网络服务提供者。"

⑬ *See* Black's Law Dictionary, by Henry Campbell, M. A., 6th Edition, St Paul, Minn. West Publishing Co., 1990, p. 1212.

⑭ 这里,说"行为人之行为通常表现为作为的形式"与前面认为本罪属于纯正不作为犯并不矛盾,因为成立本罪还要求行为人"经监管部门责令采取改正措施而拒不改正"之条件,"拒不改正"当然只能是纯正不作为。

第二,命令性规范设定的义务。命令性规范(rule of order)又称之为强制性规范,是指规定人们的积极义务,即人们必须或应当做出某种行为,不允许人们以任何方式变更或违抗的法律规范。其立法用语的表达范式为:“有……义务”、“应当……”、“必须……”等。命令性规范设定的义务是指法律、法规明确规定行为人必须或者应当积极做出的事项。如果行为人不作为,不按照法律、法规要求积极做出具体作为,则构成义务的违反。例如,全国人民代表大会常务委员会《关于加强网络信息保护的决定》第3条规定:网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密,不得泄露、篡改、毁损,不得出售或者非法向他人提供。再如:《计算机信息网络国际联网安全保护管理办法》第10条第(六)项规定:发现有本办法第4条(危害国家安全等)、第5条(危害国家安全等)、第6条(破坏计算机信息系统)、第7条(侵犯通讯自由)所列情形之一的,应当保留有关原始记录,并在24小时内向当地公安机关报告。这里,“必须……”、“应当……”就是命令性规范设定的义务,网络服务提供者必须或者应当按照法律、法规规定做出具体的积极行为,如果行为人不作为,即不做出有义务做出的行为,就是对义务的违反,必然会招致违法后果。

2. 经监管部门责令采取改正措施而拒不改正

就本罪成立而言,只是满足了前述违反义务条件并不足以构成犯罪,还必须具有行人经监管部门责令采取改正措施而拒不改正行为,才有可能成立犯罪。事实上,本罪作为一个典型的义务犯,其“义务”具有双层次特点:第一层次义务乃是非刑事法律规定的网络服务提供者应当履行的网络安全管理义务;换言之,该层次义务通常是行政法律、法规规定的网络服务提供者所具有的网络安全管理行政义务,前段所述禁止性规范和命令性规范规定的义务即是。但是,考虑到网络服务提供者所从事的业务只是“服务”,无论是从权利义务的合理分配,还是从法律可以期待网络服务提供者的应有能力来看,国家不可以强求网络服务提供者承担网络警察的监管义务与责任。因此,立法者为了避免过分增加网络服务提供者的网络安全管理的法律负担,特别设计了与一般义务犯成立的不同标准——第二层次义务或刑事义务[15],即“经监管部门责令采取改正措施而拒不改正”。只有行为人在已经违反第一层次义务(行政义务)的前提下,进一步违反第二层次义务(刑事义务)时,其行为才可能受到刑法的评价。这里有两点值得注意:

第一,正确理解“监管部门”及其权限。在《刑法修正案(九)》草案征求意见的过程中,曾经有学术机构建议立法机关对本罪法条中的“监管部门”做出明确界定,从而避免因为含义模糊、界线难分而造成司法实践中认定监管主体的混乱。但不知道究竟因为何种原因,立法机关最终没有采纳这一合理建议。尽管目前仍然没有立法与司法解释对哪些部门属于“监管部门”作出解释,但是学术研究上我们仍然可以根据现有法律、法

---

[15] 刑法中规定的绝大多数义务犯都没有第二层次义务要求。如逃避追缴欠税罪、虐待罪、遗弃罪、战时拒不救治伤病军人罪等,只要行为人违反相关法律规定的义务,就有可能受到刑法规范的评价,刑法本身并没有对这些义务犯设定第二层次的义务。

规对“监管部门”做一合理分析与界定。

所谓“监管部门”是指依据法律、法规,具有网络安全监督管理职权的部门。那么,哪些部门具有网络安全管理职权呢?通过对有关法律、法规规定的梳理,考虑到我国政治法律生活的特殊情况,笔者认为以下部门应当属于信息网络安全监管部门:(1)中央网络安全和信息化领导小组;[16](2)国务院互联网信息办公室以及地方政府部门的网络信息办公室;[17](3)公安部门、国家安全部门、国家保密部门专门负责信息网络监管的部门(《中华人民共和国计算机信息系统安全保护条例》6 条);(4)工业和信息化部所属的通讯管理局以及各省、自治区、直辖市通信管理局(《电信互联网用户个人信息保护规定》第 3 条);(5)文化部所属互联网文化监管部门(《互联网文化管理暂行规定》第 6 条);(6)国务院新闻办公室以及省级人民政府的新闻办公室(《互联网新闻信息服务管理规定》第 4 条)。(7)其他依法具有网络监管职权的部门。上述各部门的特点是,有的网络安全管理部门是全国性、全方位的,它们对全国各领域的网络信息安全都具有管辖权,如中央网络安全和信息化领导小组和国务院互联网信息办公室以及公安部网络监管部门;有的则是部门性的,他们只对本部门涉及的网络信息安全有监管职权,如文化部所属互联网文化监管部门,它只对本部门涉及的互联网文化活动具有监管职权;又如国务院新闻办公室只对涉及互联网新闻方面的网络监督管理具有职权。此外,地方各网络信息监管部门只具有对相应地方的网络信息具有监管职权。总之,除了全国性、全方位性的网络信息监管机构外,其他各职能机构只能在各自权限内行使网络信息安全管理职权,不能超越其职权进行网络监督管理。

第二,拒不改正。“拒不改正”乃是立法者为网络服务提供者划定的“红线”(设定的刑事义务),是指网络服务提供者收到法定监管部门责令采取改正措施的通知、指令等而拒绝接受,并且不采取改正措施,继续维持其违反作为义务的不作为状态。这里有几点值得注意:(1)“责令采取改正措施”的主体,限于前一节论及的负有网络安全管理权力的机构,且该权力机构只能在自己的管辖范围内进行网络安全监管。其他非法定的机构或个人,或者超出其监管范围的网络监管部门,无权干预网络服务提供者的运营活动。所以,拒绝接受非法定机构或者超出管辖范围的监管部门提出的所谓“责令改正措施”的通知或指令,不属于本罪构成要件所要求的“拒不改正”。(2)网络监管机构“责令改正”的事项必须是有法律、法规依据的;换言之,监管机构只能对不符合法律、法规的网络服务“责令整改”,如果网络监管机构要求网络服务提供者改正的本来是合法的

---

⑯ 该小组成立于 2014 年 2 月 27 日,该小组的任务之一就是对网络安全的领导和监管。

⑰ 该机构成立于 2011 年 5 月 4 日。2014 年 8 月 28 日《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》明确指出:“授权重新组建的国家互联网信息办公室负责全国互联网信息内容管理工作,并负责监督管理执法。”新近颁布的《网络安全法》第 8 条规定:“国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定,在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责按照国家有关规定确定。”

做法，如批评、监督、检举揭发等，则网络服务提供者有权拒绝。司法实践中，可能会出现对“责令整改”的合法性（正当性）判断上的分歧，即可能出现网络监管部门认为自己的“责令整改”是正当合法的，而网络服务提供者却认为该“责令整改”不具有合法性（正当性），对此，应当由审判机关依据法律、法规的规定和相关刑法学理论作出判断与评价。（3）“责令采取改正措施”一般应当以书面的正式通知送达网络服务提供者，如果情况紧急，来不及以书面形式通知的，可以以电话、电传、电子图片等形式通知，同时记录在案，以备查验。但事后应当及时办理书面通知手续。因此，即使是法定网络安全监管部门，如果不是以合法形式“责令采取改正措施”的，网络服务提供者拒绝接受的，也不成立本罪。（4）网络监管机构的“责令采取改正措施”通知必须确实送达网络服务提供者，如果“责令采取改正措施”的通知或指令虽然发出，但被送达人并没有收到，因而没有采取措施改正的，不属于“拒不改正”。

3. 符合《刑法》第 286 条之一第一款规定的四种情形之一

行为人即使满足了前述两种条件，仍然不能简单地认定其构成了本罪。即只有在满足前述两种条件，同时又具有下列情形之一的，方才成立本罪：

第一，致使违法信息大量传播。“违法信息”是本罪的客观要素之一。所谓“违法信息”是指依法被禁止公开宣扬或传播的信息。具体来讲，应当以现行法律、法规的明确规定来认定传播的信息是否违法。所谓“现行法律、法规”至少应当与《刑法》第 96 条所解释的“国家规定”含义相一致，即违法的“法”应当是指全国人民代表大会及其常务委员会制定的法律和决定；国务院制定的行政法规、规定的行政措施、发布的命令和决定。如国务院发布的《中华人民共和国计算机信息网络国际联网安全保护管理办法》第 4、5 条规定的信息（危害国家安全等违法犯罪信息）就属于违法信息，如果行为人拒不履行信息网络安全管理义务，致使煽动颠覆国家政权、破坏国家法律制度和政治制度的违法信息大量传播就属于“致使违法信息大量传播”。至于各部委、省、直辖市、自治区的地方立法是否属于这里所说的“法”？笔者认为，除了具有全国信息网络安全管理职权的国家级的部、委、办（如公安部、安全部、国家保密局、工信部等）外，一般省部级部门制定的本部门、本地区的行政规范文件不应属于这里“法”的范畴。之所以作这样的理解，是因为刑法的入罪标准必须统一（除非国家有专门规定或者司法解释），如果将地方或者部门制定的有关行政规范文件也纳入这里“法”的范围，就有可能造成入罪标准的混乱，因为各地或者各部门很可能根据本地区、本部门情况来制定行政规范性文件，从而造成全国地方性法规不一致的情况，进而导致认定本罪的标准出现差异。

所谓大量传播应当包括两种情况：一是指众多违法信息被传播出去；所谓“众多”，依照国人“三人为众”的思维习惯，至少是指超过三条或以上的违法信息被传播出去；二是传播的违法信息虽然数量上少于三条，但是传播的受众众多，也可以理解为“大量传播”。比如，行为人致使“煽动民族仇恨、民族歧视，破坏民族团结的”的违法信息在成千上万人中间传播，哪怕是只传播了一条信息，也属于“大量传播”，故足以构成本罪。还要指出，因“致使违法信息大量传播”而成立本罪的，属行为犯（也可以称之为（抽象）

危险犯),并不要求造成特定后果,只要违法信息"大量传播",即构成犯罪。反之,行为人虽然拒不履行信息网络安全管理义务,但是只有少量违法信息传播出去的,则不构成犯罪。

第二,致使用户信息泄露,造成严重后果。所谓"用户信息"是指接受网络服务提供者服务的自然人或者单位的相关信息,包括个人的有关出生、住址、电话、电子邮箱、生活习惯、家庭成员、民族、宗教信仰、价值取向、收入、教育、隐私、QQ 号、身份证号、银行卡号等各种信息,也包括单位不宜公开传播的有关信息,如公司内部掌握的营销计划与策略、客户资料、投资意向、发展规划等。应当注意的是,以"泄露用户信息"形式实施本罪行为的,属结果犯,需要造成"严重后果"才构成犯罪。所谓"造成严重后果",一般是指造成了可以观感的某种负面后果,比如泄露他人隐私等,致使他人严重抑郁或自杀。又如,因为泄露他人经营信息而致使他人遭受重大经济损失,等等。因此,虽然网络服务提供者泄露了用户的信息,不但没有造成"严重后果",而是带来了大量商机的(如产生良好广告效应),当然不能认为是犯罪。

第三,致使刑事案件证据灭失,情节严重。此种情况通常发生在行为人没有履行保存法律、法规要求的固定对处理刑事案件具有证据效力的信息义务。比如,《计算机信息网络国际联网安全保护管理办法》第 10 条第(6)项规定:"发现有本办法第四条、第五条、第六条、第七条所列情形之一的,[18]应当保留有关原始记录,并在 24 小时内向当地公安机关报告。"该项规定专门规定了互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织(包括网络服务提供者)应当履行保留有关涉及危害国家安全等违法犯罪电子证据的义务。因"致使刑事案件证据灭失"而成立本罪的属情节犯。换言之,"情节严重"乃是本罪的构成要件之一,只有行为人拒不履行信息网络安全管理义务,致使刑事案件证据灭失,且情节严重,才会构成本罪。这里,"情节严重"一般是指致使重大犯罪案件(如严重暴力犯罪、恐怖主义犯罪、危害国家安全等犯罪)的证据丢失;多次不履行信息网络安全管理义务,经警告或其他处分后又造成刑事案件证据灭失等情况。

第四,有其他严重情节。这显然是一个兜底性规定,是指除了前述三种情况以外的其他拒不履行信息网络安全管理义务,且情节严重的情形。但应当注意,由于"其他严重情节"语焉不详,在没有明确立法或司法解释之前,一定要慎重适用,必须避免无端扩大解释或类推解释,防止造成破坏罪刑法定原则的严重负面后果。值得注意的是,如果在前述第(三)项"致使证据灭失情形下",行为人没有履行信息网络安全管理义务,致使灭失的乃是特别重大行政案件或者民商事案件证据的,是否可以理解为"有其他严重情节"从而定罪处罚?笔者认为,对此问题,结论应该是否定的。因为,根据《刑法》第

---

[18] 分别涉及危害国家安全、国家秘密,煽动抗拒、破坏宪法和法律及行政法规实施,煽动民族仇恨、民族歧视、破坏民族团结,捏造或者歪曲事实、散布谣言,宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖,教唆犯罪,公然侮辱他人或者捏造事实诽谤他人,损害国家机关信誉,危害计算机信息网络安全,侵犯用户的通信自由和通信秘密。

286条之一第一款第3项的规定，这里作为构成要件之一的只能是“致使刑事案件证据灭失”，如果灭失的不是“刑事案件证据”，即使情节严重，也不符合法条明文规定的构成要件要素。

二、心理要素(Mens rea)

犯罪的心理要素是指行为人行为之时所抱持的心理态度——故意或过失、意图或目的，甚至包括特定的动机[19]。就本罪而言，值得关注的乃是本罪的心理要素只能是直接故意，且本罪故意内容中不要求具有特定目的。所谓直接故意是指行为人在意识上已经认识到其行为必然或者可能发生危害后果，行为人却以积极态度在意志上追求或者希望该危害后果发生。由于本罪法条使用了“经监管部门责令采取改正措施而拒不改正”这样的语句，而“拒不改正”恰恰反映了行为人对危害后果的积极追求或希望态度，故本罪不可能由间接故意(单纯的放任)行为构成。同样道理，过失行为不可能存在“拒不改正”的问题，所以，如果行为人因为工作失误而没有采取改正措施，即使造成了危害后果的，亦不能以本罪论处。关于本罪的心理要素，应当特别注意的问题有二：一是本罪行为人故意的认识程度有何要求？二是发生违法性认识错误时如何处理？

(一)故意的认识程度(范围)

“故意是与实施行为联系在一起的、对犯罪事实的认识”；[20]“故意的认识对象，是构成犯罪的所有客观事实，除了(作为违法类型的)构成要件的该当事实之外，还包括有关违法性与责任的事实。”[21]这虽然是日本刑法学者在论述“故意的认识对象”时所持的立场，但我们不妨将其看作是对故意的认识程度(范围)的描述。如果承认这一见解对于我们正确界定拒不履行信息网络安全管理义务罪的行为人故意的认识程度或范围有重要借鉴意义。那么，本罪行为人至少需要认识到《刑法》第286条之一规定的“构成要件的该当事实”，才能满足本罪故意的认识程度要求。哪些事实属于拒不履行信息网络安全管理义务罪的“构成要件的该当事实”？这就是前文已经阐明的刑法条文规定的“不履行法律、法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正”，且必然或者可能造成四种客观表现之一——(1)致使违法信息大量传播；(2)致使用户信息泄露，造成严重后果；(3)致使刑事案件证据灭失，情节严重；(4)有其他严重情节。换言之，行为人必须认识到自己不履行信息网络安全管理义务、经监管部门责令采取改正措施而拒不改正的行为必然或者可能引起前述四种结果之一，却追求或者希

---

⑲ 学理上一般认为，犯罪动机与犯罪成立无关。但是英国有学者认为，说“动机与刑事责任无关，事实上这并不完全正确。有些犯罪只有在证明被告人的犯罪行为是在特别(坏的)动机驱使下才得以成立。敲诈勒索罪(blackmail)就是一个典型的例子。”参见[英]威廉姆·威尔逊：《刑法理论的核心问题》，谢望原、罗灿、王波译，中国人民大学出版社2015年版，第129页。

⑳ [日]松原芳博：《刑法总论重要问题》，王昭武译，中国政法大学出版社2014年版，第174页。

㉑ 前引⑳，第178页。

望该结果发生,才初步满足本罪故意的认识程度。不过,要成立本罪,还必须是行为人认识到了其行为具有“违法性”,即行为人还需要认识到自己“不履行信息网络安全管理义务”以及“拒不改正”的行为是法律所禁止的。诚如日本学者松原芳博教授所言:“故意中的‘事实认识’,不是‘对物体的认识’,或者‘对裸的事实的认识’,而是必须是‘对含义的认识’。例如,就‘黄色’小说而言,要谓之为对属于‘淫秽文书’存在认识,仅有对有关书籍以及文字组合的‘物体认识’尚不够,这毋庸赘言,而且仅对单纯的语言存在认识也不够,必须认识到属于‘下流的东西’。”[22]由此可见,只有行为人对自己的行为性质有了违法性认识,却在此前提下积极追求或者希望危害后果发生,才满足本罪故意的认识程度。

(二)发生违法性认识错误时如何处理

违法性认识错误是相对于事实认识错误(构成要件错误)而言的一个概念,又称之为“违法性的错误”、“禁止的错误”,是指行为人虽然对涉案的事实存在正确认识,却对该事实的法律评价存在误解,行为人错误地认为自己的行为是法律所允许的(合法的),或者不知道是法律所禁止的,进而实施该行为。违法性认识错误有两种形式:一是不知道法律的存在,二是错误理解法律,把自己不被法律允许的行为错误地理解为法律允许。对于不知法律的情形,一般认为应当遵循“不知法律不成为辩护事由”(Ignorantia juris neminem excusat)的古老格言,除非行为人能够反证自己有合理理由不知道法律的存在,原则上不能因为行为人不知道法律的存在而不负刑事责任。[23] 但是,无论是不知法律还是对法律存在误解,仍然存在诸多争议。

日本大塚仁教授曾经指出:“误解法令的结果,而错误地认识了构成要件要素的意义时,认为它是事实的错误而阻却故意,可以说是判例的基本立场。”[24]此一观点本质上就是“违法性认识必要说”。该观点认为:作为故意的内容,以违法性的意识为必要,不管出于何种理由,违法性的错误均阻却故意责任。换言之,违法性认识错误至少应当排除故意责任。不过,也有学者基于刑法上的犯罪可以分为自然犯与法定犯(行政犯),进而提出了“自然犯、法定犯区别说”的见解,认为:就自然犯而言,行为人对犯罪事实的认识本身就已经反映了行为人的反社会性,因此,成立犯罪不以其具有违法性认识为必要;但对于法定犯来说,只有行为人对其行为受到法律禁止存在认识,才可以认定其反社会性,故若要认定成立行政犯,必须首先认定行为人具有违法性认识。[25] 德国法院的

---

[22] 前引[20],[日]松原芳博书,第 179 页。

[23] 学说史上,持违法性认识不要说者认为,成立故意责任毋需存在违法性认识,也毋需存在违法性认识的可能性,不问是出于何种理由,违法性的错误均不阻却故意责任。日本有判例支持此观点。如关东大地震期间,被告人违反《暴力取缔法》,以高于市价的价格出售石油罐,尽管当时交通中断,被告人并不知道且无从知道三天前刚发布的该法令,但还是被日本法院认定构成《暴利取缔法》规定的犯罪。参见前引[20],[日]松原芳博书,第 197-198 页。

[24] [日]大塚仁:《刑法概说》(第 3 版),冯军译,中国人民大学出版社 2009 年第二次印刷,第 214 页。

[25] 参见前引[20],[日]松原芳博书,第 198-199 页。

判决也体现了这样的立场。[26] 英国刑事司法虽然坚持“不知法不能成为辩护事由”(Ignorance of the law excuses no one)[27]这一原则,但是刑法学家们却强烈主张“个人公平(individual fairness)要求将不知法或法律错误作为辩解事由:那些相信其行为不是犯罪,或者不知道其行为是犯罪的人,不应当被定罪。”[28]英国刑法上关于认识错误适用原则之一就是:如果行为人的认识错误能够否定检察官承担举证责任要证明的犯意(mens rea)中的一个要素(an element),那么行为人的认识错误就会影响刑事责任。[29] 这实际上等于说:如果行为人因为错误认识而不存在犯罪构成所要求的心理要素,如knowledge(明知)、intention(意图)等,那么错误认识就可以排除行为人的刑事责任。例如,贸易与工业大臣诉哈特案(Secretary of State for Trade and Industry v. Hart),因为被告人并不知道1948年《公司法》第161条第(2)项以及1976年《公司法》第13条第(5)项的规定(即法律认识错误),法院接受了被告人不知道有关该犯罪的法律规定之辩解,而明知自己“无资格”是构成该犯罪(无资格而担任审计员罪)的必要条件,故宣告被告人无罪[30]。

通过以上分析可以得出肯定结论:两大法系刑法理论在违法性认识问题上存在某些共通之处,这就是对于一些故意犯罪来说,成立某一犯罪,行为人需要具有违法性认识,亦即行为人需要对其行为性质及其必然或者可能引起的危害结果有认识。在违法性方面发生法律认识错误时,可以排除行为人之行为的犯罪性。之所以如此,其实正如1825年金特诉杰菲里斯案(Gent v. Jefferys)的裁判书所言:“上帝禁止想象检察官或律师甚至法官必然知晓所有的法律。”[31]似此,既然法律专业人士尚且有不知晓的法律,那么要求普通公民知道所有法律就实在有些强人所难了。因此,当行为人确实因为不知道法律禁止或者发生法律错误认识时,应该作出有利于行为人的判断或评价。所以,就作为行政犯的拒不履行信息网络安全管理义务罪而言,当信息网络服务提供者与网络安全监管机构关于违法性认识产生冲突时——比如,针对信息网络上出现的严厉批评国家民族政策、宗教政策失误的信息,网络监管部门认为此批评属于“有损国家形象”的

---

[26] “公民表决案(Volksbefragungs-Fall)”:初级法院(AG)判定被告人违反了1951年5月11日《汉堡警察法令》中禁止推动公民表决反对德国的再军事化,因为被告人1951年6月21日为汉堡的“和平委员会”执行了东德统一社会党组织的公民表决。被告人上诉后,州高等法院将该案提交德国联邦最高法院审理。最高法院后来在裁判理由中评述道:“I. 若被告人当时认识到其行为受到禁止,……则它并不处于禁止错误,而是认识到了其行为之不法。……理由是,行为人也具备违法性认识:行为人知道他所为在法律上是不允许,而是禁止的。”参见[德]克劳斯·罗克辛:《德国最高法院判例·刑法总论》,何庆仁、蔡桂生译,中国人民大学出版社2012年版,第95-96页。

[27] *See* Andrew Ashworth ,Jeremy Horder: Principles of Criminal Law,7th Edition, Oxford University Press,2013,p. 218.

[28] 前引[27],第219页。

[29] 英国刑法理论上认识错误适用的另一原则是:如果行为人的认识错误涉及事实情状,而且该有关事实情状的认识错误能够为行为人提供一个独立的辩护事由,那么行为人的认识错误就会影响(免除)刑事责任。*See* William Wilson, Criminal Law: Doctrine and Theory,3th edition, Pearson Education Limited, 2008,pp. 220.

[30] 本案被告人是一家公司的董事兼秘书长,也是另一家公司的董事。他为两家公司审计截止1979年3月31日的年度账目。他被指控实施了明知自己无资格而担任审计员的犯罪行为。*See* Janet Dine & James Gobert: Cases & Materials on Criminal Law, 3rd Edition, Blackstone Press Limited,2000,p. 648.

[31] *See* Dennis J. Baker: Textbook of Criminal Law, 3rd Edition, Sweet & Maxwell, 2012,p. 641.

违法信息，要求网络服务提供者及时清除，但网络服务提供者在咨询法学教授后得知，这些信息内容仍然属于宪法所保护的言论自由的范围，故行为人拒绝将其清除。对此，笔者认为，应当坚持运用刑法学关于违法性认识错误的通说理论来处理类似案件，不宜认定信息网络服务提供者具有行为故意，因而不应当以犯罪论处。[32] 理由如下：

首先，网络服务提供者在咨询专业人士后确信有关信息内容并不违法，并拒绝接受监管部门的改正意见，即便是与官方的意见发生冲突，这也属于违法性认识错误的范畴，而违法性认识错误至少可以排除行为人的故意责任。考虑到我国《刑法》第 286 条之一明确将本罪规定为故意犯罪（且只能是直接故意），故即便行为人存在过失，也不成立本罪。正如罗克辛教授所言："如果行为人询问（比如问律师）时得到的答复说，计划中的举止属于合法，那他就根本没有可能认识到其举止的违法性了，而这样的举止是没有罪责的。"[33]其次，在现代国家的法律与政治制度设计中，各类媒体（无论是传统的纸质媒体还是当下盛行的网络媒体）的核心功能之一，应该是对政府及其官员的监督与批评，政府及其官员只有时时处在媒体的监督批评之下，才能确保政府及其官员恪尽职守，谨言慎行，奉公守法，全心全意为人民服务。更何况我国《宪法》第 35 条明确规定了我国公民享有言论、出版等自由权利，即便是公民发表的言论与政府及其官员的立场有所不同，国家也应当以宽大为怀的胸襟予以包容。否则，如果公共权力机关动辄运用刑事手段处理涉及言论的问题，那将会造成严重的寒蝉效应。而这样对于国家来说，显然其负面效果远大于正面效果。

三、本罪涉及的相关问题

（一）与有关危害国家安全罪的问题

本罪的表现形式之一乃是"致使违法信息大量传播"，如果这里的"违法信息"包含了分裂国家、颠覆国家政权等危害国家安全犯罪的相关内容时，就可能使本罪与危害国家安全罪中的煽动分裂国家罪（《刑法》103 条第 2 款）以及煽动颠覆国家政权罪（《刑法》第 105 条第 2 款）出现部分重合。因为"违法信息大量传播"在客观上与"煽动分裂国家"、"煽动颠覆国家政权"可能具有客观形式上的类似性。但是它们之间仍然存在明显区别：它们除了侵害法益不同和主体构成不同外，最为应当引起关注的还有主观故意内容不同。本罪行为人的故意内容乃是在有明确认知的前提下，故意不履行信息网络安全管理义务，但行为人主观认知中并无危害国家安全的目的；而后两罪的心理要素方面，恰恰要求行为人具有危害国家安全的目的，行为人之故意内容正是危害国家安

---

[32] 陈兴良教授认为，"径直将违法性认识错误作为责任阻却事由加以讨论，也并不是不可以。"参见陈忠林主编：《违法性认识》，北京大学出版社 2006 年版，第 123 页；黎宏教授亦认为："通说也认为，行为人在没有违法性认识的情况下，也会被作为没有社会危害性认识而排除故意"。参见本注陈忠林主编书，第 389 页。

[33] 前引[26]，[德]克劳斯·罗克辛书，第 101 页。

全。这是因为,虽然现行刑法分则规定的危害国家安全罪没有明确规定成立该类犯罪需要行为人具有危害国家安全的目的,但是从新中国立法传统和学理上来看,认定行为人构成该类犯罪,检察机关仍然必须证明行为人具有危害国家安全的目的。理由在于:首先,危害国家安全罪是由反革命罪演变而来的,而反革命罪在新中国刑法史上从来都是目的犯。[34] 所以,危害国家安全罪自然在历史发展过程中承袭了这一"目的犯"的性质。其次,危害国家安全的目的乃是区分行为人之行为究竟构成普通犯罪还是构成危害国家安全罪的一个关键因素。刑法分则第一章(危害国家安全罪)规定的有关犯罪,如果除去行为人的主观目的,它们就属于普通犯罪。最为典型的就是叛逃罪(《刑法》第109条),当国家机关工作人员擅离岗位出走境外,如果不具有背叛祖国的目的,恐怕很难成立叛逃罪,至多也只能构成偷越国(边)境罪。其三,刑法分则条文中也有其他犯罪没有专门规定特定目的而被普遍认为成立犯罪必须要有特定目的的,诈骗罪、盗窃罪、抢夺罪(《刑法》第266条)、侵占罪(《刑法》第270条)就是其中的适例。虽然法条没有明确规定成立诈骗、盗窃、抢夺、侵占犯罪行为人必须具有非法占有他人财物的目的,但是无论是理论上还是司法实践中,都认为检察官只有证明行为人具有非法占有目的,才能构成诈骗、盗窃、抢夺、侵占犯罪。故不能因为现行刑法分则第一章没有专门规定本章犯罪为目的犯,就认为检察机关不需要证明行为人构成危害国家安全罪必须具有危害国家安全的目的。反之,假如行为人正是以分裂国家、颠覆国家的故意和目的故意致使大量"煽动分裂国家"、"煽动颠覆国家政权"的违法信息得以传播,则构成"煽动分裂国家罪"、"煽动颠覆国家政权罪"(帮助犯),而不成立本罪了。

(二)从一重罪处断[35]

《刑法》第286条之一第3款规定:"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。"所谓"同时构成其他犯罪"可能包括两种情况:一是竞合行为,二是牵连行为。虽然我国刑法中没有关于竞合犯与牵连犯的立法规定,但是,无论是理论上还是司法实践中,我国均认可竞合犯与牵连犯。竞合犯又分为法条竞合犯与想象竞合犯。对于法条竞合犯的处罚,原则上采取"特别法优于普通法"原则;对于想象竞合犯的处罚,则与牵连犯相同,即原则上采取"从一重罪处断"。但是我国立法上,却也有

---

[34] 早在1934年中央苏区公布施行的《中华苏维埃共和国惩治反革命条例》第2条就规定:"凡一切图谋推翻或破坏苏维埃政府及工农民主革命所得到的权利,意图保持或恢复豪绅地主资产阶级的统治者,不论用何种方法都是反革命行为。"后来这一传统一直得到了传承,一直到1979年《刑法》第90条仍然明确规定:"以推翻无产阶级专政的社会主义制度为目的、危害中华人民共和国的行为,都是反革命罪。"参见高铭暄:《中华人民共和国刑法的孕育诞生和发展完善》,北京大学出版社2012年版,第85-86页。

[35] 这里的研究是实然研究,不是应然的研究。从应然的研究来看,该条规定有进一步探讨的必要。

一些刑法条文规定对某些竞合犯或牵连犯按照数罪并罚原则处理。[36] 就本罪的情况来看,只要是行为人实施拒不履行信息网络安全管理义务罪,无论是发生法条竞合、想象竞合还是牵连犯的场合,均不涉及数罪并罚问题,一律按照从一重罪处断原则处理:

第一,实施本罪行为致使违法信息大量传播。如果大量传播的违法信息具有侮辱、诽谤他人的性质,则本罪行为可能与侮辱、诽谤罪的构成要件重合。对此,应当比较该两罪刑罚,按照处罚较重的犯罪论处。由于本罪的法定刑是处 3 年以下有期徒刑、拘役或者管制,并处或者单处罚金,而侮辱、诽谤罪的法定刑是处 3 年以下有期徒刑、拘役、管制或者剥夺政治权利,且侮辱、诽谤罪属于自诉罪(但是严重危害社会秩序和国家利益的除外),故本罪的处罚较侮辱、诽谤罪要重,因此,对于致使大量违法信息传播,造成侮辱、诽谤他人后果的,应当依法按照本罪(拒不履行网络安全管理义务罪)论处。

第二,实施本罪行为泄露的用户信息属于军事秘密的,则应当按照故意泄露军事秘密罪论处。因为故意泄露军事秘密罪的处罚比本罪要重。同理,如果泄露(披露)的信息属于商业秘密,并且造成特别严重后果的,则应当依照侵犯商业秘密罪(《刑法》第 219 条第 1 款后半段,"造成后果特别严重的,处 3 年以上 7 年以下有期徒刑,并处罚金")论处。

第三,实施本罪行为,故意不保留与刑事案件有关的原始证据,"致使刑事案件证据灭失,情节严重的"。此种情况下虽然可能与"帮助毁灭证据罪"重合,但依据前述规定,应当从一重罪处断,比较本罪与帮助毁灭证据罪的刑法规定,依法应对本罪处 3 年以下有期徒刑、拘役或者管制,并处或者单处罚金;而对帮助毁灭证据罪依法应处 3 年以下有期徒刑或者拘役。两相比较,刑法对本罪规定了比帮助毁灭证据罪更重的刑罚,故对于实施本罪行为而同时构成帮助毁灭证据罪的,应当按照本罪论处。

(三)本罪没有未遂

关于既遂、未遂问题,首先要考虑实行行为[37]的着手。因为,在实行行为之前的行为属于预备行为,而在实行行为着手之后,因为客观原因而没有产生行为人预期结果的是未遂;行为人实现预期目标的就是既遂。大陆法系刑法理论关于实行行为着手的时点认定,有客观说(包括形式的客观说与实质的客观说)、主观说(包括主观的客观说)以及折中说。客观说以客观主义刑法思想为根据。形式的客观说主张与构成要件直接密接的行为时间是着手的时间。实质的客观说认为,未遂犯可罚性的实质性根据是着手

---

[36] 如《刑法》第 204 条第 2 款规定:"纳税人缴纳税款后,采取前款规定的欺骗方法,骗取所交纳税款的,依照本法第 201 条的规定定罪处罚;骗取税款超过所缴纳的税款部分,依照前款的规定处罚。"此种情况下,行为人一个骗取出口退税的竞合行为,将可能受到逃税罪和骗取出口退税罪的并罚。又如,《刑法》第 120 条第 2 款规定:"犯前款罪(组织、领导、参加恐怖组织罪)并实施杀人、爆炸、绑架等犯罪的,依照数罪并罚的规定处罚。"一般来说,行为人组织、领导、参加恐怖组织,就是为了进一步实施杀人、爆炸、绑架等恐怖犯罪,因此,"组织、领导、参加"实际上是后续犯罪的原因行为,该款规定实际上是把牵连行为作为数罪处理了。

[37] 按照早稻田大学西原春夫教授的解释,所谓实行行为乃指构成要件中行为人以动词形式表达的行为。"杀人"、"放火"、"窃取"、"通过欺罔取得财物"、"实施猥亵行为"等就属于实行行为。总之,实行行为是构成要件的核心行为。参见[日]西原春夫:《犯罪实行行为论》,戴波、付立庆译,北京大学出版社 2006 年版,第 2 页。

时间的判断基准;发生侵害法益现实危险的时间就是着手的时间。主观说则以主观主义的刑法思想为根据,其代表性的观点认为:着手时间是指犯意的成立根据其行为可以确定地认定之时。折中说认为,根据行为人关于行为的认识,直接开始实施构成要件行为之时是着手。一般认为,主观主义的着手见解较之于客观主义的着手见解其处罚范围要大得多。而客观说属于通说。[38] 但是在笔者看来,折中说可能因为既考虑到了行为人对自己行为性质的主观认识(已有违法性认识),又考虑到了客观方面行为人已经展示自己反法规范的性格,因此,以折中说的标准作为认定着手的时点可能更为合理。

结合拒不履行信息网络安全管理义务罪的构成要件来考察,笔者认为,"经监管部门责令采取改正措施而拒不改正",这里的"拒不改正"一方面反映了行为人对自己的行为性质已有认识,另一方面正好也是行为人"直接开始实施构成要件行为"的开始。正如美国《模范刑法典》所规定的那样,一旦一个人"在实质犯罪方面采取了'实质步骤'",[39]超过这个"临界检测标准"(Rubicon test),"只要行为人'破釜沉舟'并无法回头时",[40]即使没有出现犯罪结果,也已经构成犯罪未遂。但是就本罪而言,依据《刑法》第286条之一的规定,在监管部门"责令采取改正措施"之前,即使行为人存在"致使大量违法信息传播"等事实,却因为监管部门尚没有提出"责令改正"通知而并不构成犯罪;而一旦监管部门提出"责令改正"通知,行为人仍然拒不改正时,就已经成立犯罪(既遂)。虽然在监管部门提出"责令改正"通知与网络服务提供者改正之间可能存在某一时间期间,如监管部门限令网络服务提供者在一定期间内改正,但是这一限令改正的缓冲时间仍然只是向成立犯罪方向发展的一个过渡时间;只有超出这一期间行为人仍然拒不改正才能成立犯罪;如果行为人在此期间内已经改正,则不能成立犯罪。由此可见,本罪根本没有成立犯罪未遂的可能。

(四)网络服务提供者提供的网络服务是否属于不值得处罚的中性行为

有学者认为,作为网络服务商,接入服务提供者、网络内容服务提供者以及网络平台服务提供者所提供的服务具有中性行为的特点,并指出:为互联网提供接入服务的不应构成犯罪;提供网络平台服务的网络经营商通常也不应当承担帮助犯的责任。在该学者看来,似乎只有网络内容服务提供者可能因为提供违法内容服务而可以被处罚。[41] 所谓中性行为,是指就其独立存在的角度来看,具有日常性、职业性等特点的行为。如出租车司机运送客人、五金店老板售卖刀具、铁锤等。但是,当这种行为与其他人的犯罪行为具有某种关系时,如行为人估计到或者认识到他人买刀具用于杀人而卖给他人刀具,他人后来用所买刀具杀人了。刑法理论上将经营者售卖刀具之类的行为称之为"中性帮助行为"。颇具影响力的德国学者罗克辛教授认为:就所谓中性的帮助行为来

㊳ 参见前引㊲,[日]西原春夫书,第6-13页;另见陈子平:《刑法总论》,元照出版公司2015年增修第三版,第378-382页。

㊴ 前引⑲,[英]威廉姆·威尔逊书,第249页。

㊵ 前引⑲,[英]威廉姆·威尔逊书,第252页。

㊶ 参见陈洪兵:《中立的帮助行为论》,信息来源:载 http://www.lawtime.cn,最后访问时间:2016年8月12日。

说,帮助者仅仅是估计到了实行人的犯罪举止,而因为自己的“日常行为”或“职业行为”卖给他人(实行人)刀具的,不应当承担帮助责任;而帮助者已经认识到实行人的犯罪决定,仍然卖给其刀具的,就应当承担帮助责任。[42] 笔者认为罗克辛教授的观点是有道理的。因为,正如著名的阿特金(Atkin)法官首创的相邻原则(neighbour principle),即人们有义务必须保持必要的注意,以免可预见的作为或者不作为伤及四邻所例证的那样,任何人都有不得对他人造成危险的义务,以及不得伤害(或杀害)他人的义务[43]。

不仅如此,考虑到我国现行刑法已经将网络服务提供者拒不履行信息网络安全管理义务的行为纳入了刑法调控范围,因此,在当下我国刑法立法框架下,网络服务提供者拒不履行网络安全管理的行为已经不再具有中立性。所以,再用所谓“中立的帮助行为”来否定网络服务提供者的相应责任就没有任何法律和学理根据了。故网络服务提供者只要经监管部门责令改正而拒不改正,并具有《刑法》第 286 条之一规定的四种情形之一的,就必须承担刑事责任。虽然学者们可以批评将“网络服务提供者明知他人在网络上传播违法信息或实施犯罪,而仍然提供技术支持或者平台服务的要独立追究刑事责任,……这一步跨的有点大也太急”,[44]但是,无论是对于刑事法学研究者还是刑事司法者来说,大家必须而且只能根据《刑法》第 286 条之一规定的犯罪构成要件来认定其犯罪。

余 论

研究至此,有关本罪的实体问题似乎基本上均已论及。但是,还有一个程序性问题:即本罪的管辖权问题有必要略作分析。

由于本罪涉及网络信息问题,又因为网络信息具有跨区域的特点,这就使得本罪的地域管辖与其他传统犯罪有所不同。例如,某网络信息服务提供者的机构与设备均在北京,而其大量传播违法信息的事实在上海的互联网上首先被发现,这就可能涉及两方面问题:其一,是应当由上海的网络信息监管部门直接向网络信息服务提供者提出“责令改正”通知,还是应由上海网络信息监管部门告知北京有关监管部门,然后由北京的网络信息监管部门向网络信息服务提供者提出“责令改正”的通知?其二,如果此种情况下网络服务提供者拒不履行网络安全管理义务,涉嫌构成犯罪,应当由哪一地区的公、检、法进行刑事诉讼?对此,笔者认为,仍然应当根据公安部关于《公安机关办理刑事案件程序规定》(以下简称《程序规定》)和《刑事诉讼法》的有关规定来处理。《程序规定》第 15 条规定:“刑事案件由犯罪地的公安机关管辖。如果由犯罪嫌疑人居住地的

---

[42] 参见[德]克劳斯·罗克辛:《德国刑法学总论》(第 2 卷),王世洲、王锴、劳东燕等译,法律出版社 2013 年版,第 155-192 页。

[43] *See* William Wilson, Central Issues in Criminal Law, Hart Publishing, 2002, p. 141.

[44] “北大车浩关于快播案的精彩点评,新浪司法 2016 年 1 月 11 日。信息来源:载 http://finance.sina.com.cn,最后访问时间:2016 年 8 月 12 日。

公安机关管辖更为适宜的,可以由犯罪嫌疑人居住地的公安机关管辖。"《刑事诉讼法》第24条规定:"刑事案件由犯罪地人民法院管辖。如果由被告人居住地人民法院管辖更为适宜的,可以由被告人居住地人民法院管辖。"由于信息网络互联互通的特性已经打破了行政区域的局限性,所有发现违法信息传播的地区均可以被认为是犯罪地,因此,前述情况下,也可把上海作为犯罪地。此一理解与最高人民法院《关于适用〈中华人民共和国刑事诉讼法〉的解释》第2条规定的精神相一致。[45] 故此,对于前述案例,上海的网络信息监管部门有权直接向违法信息服务提供者提出"责令改正"通知;如果被通知人拒绝接受,则可能构成犯罪,此时可由上海的公安机关和司法机关展开刑事追诉。当然,由于嫌疑人的住址在北京,且北京也是违法犯罪事实发生地,上海的网络信息监管部门也可以将自己掌握的北京网络服务提供者的违法信息和事实告知北京的网络信息监管部门,由北京的网络信息监管部门提出"责令改正"通知;如果被通知人拒绝接受,则进而由北京的公安机关和司法机关展开刑事追诉。

Abstract: "Information network" includes public telephone network, broadcast and television network, and computer network. The subject of the crime of refusing to fulfill the obligation of information network security administration consists of network access provider, network platform provider, network content and product provider. The act of this crime must meet the conditions that "refusing to fulfill the obligation of information network security administration", "refusing to take steps to correct their mistakes according to requirements of supervision authorities" and "acts belong to one of the four conducts stipulated in the Criminal Law". The author points out that subjective aspect of the crime must have direct intention and the recognition of violating the law, and when the actor has wrong recognition of violating the law, his act should not be convicted as this crime. In addition, the author believes that the main distinction between the crime of refusing to fulfill the obligation of information network security administration and crimes relevant to jeopardizing state security is whether there exists the purpose of jeopardizing state security, the crime must be a completed offense, and information network service providers' corresponding liabilities of refusing to fulfill the obligation of information network security administration should not be denied with the reason of neutral help act".

(责任编辑:白岫云)

[45] 该条规定,犯罪地包括犯罪行为发生地和犯罪结果发生地。针对或者利用计算机网络实施的犯罪,犯罪地包括犯罪行为发生地的网站服务器所在地,网络接入地,网站建立者、管理者所在地,被侵害的计算机信息系统及其管理者所在地,被告人、被害人使用的计算机信息系统所在地,以及被害人财产遭受损失地。