

拒不履行信息网络安全管理义务罪： 实质解释与适用检视

黄勇 莫洪宪¹

【摘要】：《刑法修正案（九）》增设拒不履行信息网络安全管理义务罪，是从刑事立法上赋予了网络服务提供者刑事保证人的地位，即直接创设了信息网络安全管理刑法上的作为义务来源。网络安全管理义务的全面、切实履行不能仅依靠网络服务提供者，还需要多个职能部门的联合治理。司法适用过程中，由于对该罪名犯罪主体——“网络服务提供者”的认定不严，导致在量刑上出现自首认定过宽、具体刑罚“畸轻畸重”的刑罚后果。为破解这一问题，刑事司法应当从严格作为义务的主体认定、强化“罪过”的刑法属性，以及规范量刑情节认定及制度的适用方面，确保落实对纯正网络犯罪“宽严相济”的治理理念，兼顾网络空间治理与技术发展保护的双重目标，以推动刑法参与网络社会治理的科学性。

【关键词】：网络服务提供者 刑事保证人 义务来源 管理责任分配 宽严相济

【中图分类号】：D924.3 **【文献标识码】**：A **【文章编号】**：1003-8477（2022）03-0130-09

随着网络信息化时代的不断发展，人们对网络技术与空间的依赖性也越来越强，网络空间已经成为公共空间与私人空间相结合的第二层现实社会。据统计报告，截至2020年6月，我国网民规模已达9.40亿。^[1]与此同时，以5G、工业互联网、卫星互联网等为代表的“新基建”得到国家的高度重视及大力推进。由此可见，互联网时代已经实现了从点对点互联到多领域互通的根本性飞跃发展。而另一方面，不容忽视的是，网络犯罪也呈现出了阶段性转变，即从网络作为犯罪对象，到网络作为犯罪工具，再到网络作为犯罪空间。^{[2]（p1047-1051）}相应地，网络犯罪的危害性与治理难度也与日俱增。在此背景下，如何使刑法适度地、有效地参与网络空间治理成为一个重大挑战。为了强化网络空间的刑法治理，2015年8月29日，第十二届全国人大常委会第十六次会议通过的《刑法修正案（九）》增设拒不履行信息网络安全管理义务罪，本文拟从实质解释论的角度对此罪进行理论与实践上的检视与反思。

一、义务来源：信息网络空间的管理责任人

当前，网络空间已不再是互联网企业占绝对主导地位的领域，国家也在逐步实现政务服务的信息化与社会治理的网络化。因而，网络空间（社会）的治理主体也必须实现多元化，尤其是管理责任主体须摆脱互联网企业（网络服务提供者）唯一义务人的传统思维，而应坚持“政府主导、企业协同”的网络空间管理新模式。对于网络空间犯罪的治理责任也需要结合犯罪本身的特点。一般来说，可将网络犯罪分为三种类型：与传统犯罪本质无异的网络犯罪；较传统犯罪危害“量变”的网络犯罪，主要指信息散布型犯罪；较传统犯罪危害“质变”的网络犯罪，如线下传统犯罪行为转到互联网后反而不构成犯罪的情形。^{[3]（p6-7）}此外，根据《刑法修正案（九）》，还可以延伸出第四类网络犯罪即纯正网络犯罪，也可称之为网络型帮助犯及其关联犯罪，如拒不履行信息网络安全管理义务罪、非法利用信息网络罪及帮助信息网络犯罪活动罪等。对于不同的犯罪类型，治理责任的内容与主体均不相同，就拒不履行信息网络安全管理义务罪而言，其认定重点不仅在于义务来源的明确、合理，更在于义务来源形成的正当

¹作者简介：黄勇（1981—），男，武汉大学法学院博士研究生（湖北武汉，430072）；莫洪宪（1954—），女，法学博士，武汉大学法学院教授（湖北武汉，430072）。

性、合理性与公平性。

（一）形式论与实质论的争议

从拒不履行信息网络安全管理义务罪作为一种纯正不作为犯罪来看，对其司法适用的检视必须回到对义务来源的探讨上，对此，主要存在着形式论与实质论之争。前者坚持了形式四分说的立场，认为作为义务的来源包括：法律法规规定的义务、职务或业务要求的义务、法律行为产生的义务、先行行为引起的义务；后者则认为形式说与罪刑法定原则相抵触，混淆了法律尤其是刑法与伦理的界限，以及存在不当限制处罚范围的可能，因而提出作为义务来源实质说，而具体作为义务来源包括依照法律规定特定的保护义务、事实上承担的保护法益的义务及基于危险共同体关系的保护义务；再如，对危险源的监督义务，也可细分为危险源监控者的义务和危险前行为的义务。^{[4] (p109-113)}实际上，形式论与实质论也并非对立关系，前者是从存在论意义上对作为义务进行形式判断，后者则是从价值论意义上对作为义务所作的实质判断。^{[5] (p78-79)}概括而言，二者之间的争议在于作为义务的来源原因力在于前置规范或行为所设定的义务，还是法律保护近距离原则所内在形成的义务。

鉴于两种学说都存在义务来源主观性强或法律义务范围过大等缺陷，有学者提出“不作为犯义务来源仅为法定义务”，^{[6] (p108)}其目的在于限缩作为义务的来源，更有学者认为还应当进一步细化为刑事法律义务，至于产生依据则包括规范根据与事实根据两个层面，^{[7] (p82)}规范根据是大前提，事实根据是小前提，同时符合则会产生作为义务。由此进一步限缩作为义务的来源与认定，从而合理界定刑事处罚的边界范围。但问题的关键在于，作为事实根据的行为事实是进行形式判断，还是实质判断。换言之，需要结合行为事实所造成的后果来加以认定是否产生事实根据。

综上，对于拒不履行信息网络安全管理义务罪的司法适用，应将重点集中于对其不作为义务的实质性判断。而在这一过程中，一方面，应当明确实质性不作为义务的感受者，另一方面则应当反思当前网络空间治理义务的责任分配，从而预防拒不履行信息网络安全管理义务罪可能存在的扩张适用风险。

（二）刑事保证人义务实质化

确定作为义务的来源只是认定不作为犯的第一步，关键环节在于确定谁来承担作为义务，即作为义务人。在作为义务主体问题上，保证人理论已逐渐为刑法学界所接受。该理论主要分为作为德国刑法理论主流的规范性派和在日本占绝对优势地位的事实性派，前者强调保证人地位确定的规范性，主要学说包括社会群体关系说、期待说、依赖说等，后者则强调对比作为犯与不作为犯因果流程上的事实差异，其代表性学说包括先行行为说和排他支配说，而相对完善的学说主要有排他支配设定说与结果原因支配说。^{[8] (p115-116)}从适用来看，排他支配设定说的“排他性”认定要求过高，且主观性较强；而结果原因支配说则更加强调从具体情形出发，重视对于支配意志的考证但不要求达到“排他”的程度，即支配意志的有无及其强弱对于判断是否“排他”具有重要意义，支配意识与原因结果支配力之间成正相关。总体而言，相比德国的规范性派更加重视宏观的规范地位，事实性派则强调具体的实质作用力，因此，在认定保证人地位时，也更拥有具体而清晰的证成路径及说服力。

以网络空间为例，若赋予网络服务提供者安全管理者的保证人地位，则需要考虑网络空间本身的特点来明确法益侵害的原因究竟是直接行为人的行为，还是网络空间管理者的故意或者过失促成了直接行为人的行为。对此，可以通过对比现实社会中场所管理者的保障义务来源来明确前述区别，即场所对法益侵害的危险来源，是场所本身的缺陷，还是场所本身的特点，若是管理者对场所存在的缺陷负有改善责任而未予排除，则明显具有保证人义务。并且，从支配意志来说，越封闭、越私密，场所管理者的支配意志越强，^{[8] (p115-116)}其保证人义务也越强。相比而言，网络空间已经发展到与社会公共空间高度趋同的阶段，因而，不能将因网络空间自身的特点而存在的违法犯罪隐患过重地附加给网络服务提供者。对此，笔者认为，应当实质性地考察网络服务提供者在违法犯罪发生中的实质性作用。尽管《刑法》第286条之一已将主观上拖延或拒绝主管部门改正要求作为入罪标准，但实际上存在一个悖论：若网络空间发生违法犯罪行为，主管部门会责令网络服务提供者改正，而只要没有“拒不改正”的主观故意，则不会构成本罪。如此，不仅使“责令改正”越来越形式化，无法发挥督促网络服务提供者实质改正的作用，也忽视了网络

服务提供者在违法犯罪行为中的实质性作用而非犯罪化，最终造成该罪名的适用虚化。

综上并结合“限制的实质论”，^{[9] (p31-33)}应当进一步限缩网络服务提供者的管理义务，将其宏观的、形式上的义务予以具体化、实质化，并在作为义务来源法定化的要求下，将作为刑事保证人地位的网络服务提供者的作为义务来源刑法化，以适应网络社会和风险社会双重背景下刑事风险的合理分担。

（三）网络空间治理义务分配

从刑法理论上的不作为犯角度，对于拒不履行信息网络安全管理义务罪应当进行实质解释，即在具有明确法定义务来源的前提下，将网络空间管理者的刑事保证人义务作具体化、实质化的限缩解释。然而，要真正解决该罪在适用过程中可能所出现的扩张适用或者适用空置等倾向，必须从根本上明确网络空间治理的模式与责任分配。

自 20 世纪 90 年代提出“风险社会”理论至今，人文社会科学领域已将风险社会理论发展到将其应用到解释社会现象与作为研究视域阶段。伴随着网络信息时代的不断更迭，“风险社会”给网络空间带来了诸多挑战，其中之一便是网络空间犯罪现象的产生与日益严重。在这种时代大背景下，应从“风险”与“危险”二分的角度来认识网络空间的治理责任，风险与危险之间的区别取决于归因。^{[10] (p47)}对于网络空间自身特点而潜在的风险，应当由社会各主体共担，这也是社会发展所必须付出的代价；而针对网络空间中人为、直接所导致的“危险”则需要判定是否可将其归结为某一主体的责任。当前网络空间治理有三大责任主体：网络服务提供企业、政府及违法犯罪行为人个人。刑法应保持谦抑性，不能一味追求网络空间治理责任承担的犯罪化。换言之，“法律、行政法规规定的信息网络安全义务并不当然产生刑法上的刑事保证人地位”，^{[11] (p11)}单位主体在社会发展中的作用与地位在不断变化，并且国家拥有更加有效、强制性的管理手段。作为技术中立方只有明知行为人进行信息网络违法犯罪活动才能对其科以刑事责任，不能泛化网络服务提供者的管理责任。

二、司法偏差：犯罪认定及刑罚适用的不当

从实质解释论角度来看，拒不履行信息网络安全管理义务罪应当坚持具体的、实质的义务来源认定，并且不能将信息网络空间安全管理义务“企业唯一论”观点带入司法适用。需要说明的是，由于笔者检索到的拒不履行信息网络安全管理义务罪的相关案例有限，因此，对于司法适用方面的审视，主要是从典型案例的角度来进行案件特点的分析。此外，本文认为，之所以该罪名刑事司法适用的案例较少，原因主要在于行政处罚的适用降低了刑事犯罪的案件量，以及适用其他相关罪名如帮助信息网络犯罪活动罪等罪名。

（一）此罪与彼罪：作为犯与不作为犯混同

对于拒不履行信息网络安全管理义务罪而言，除了明确其实质的作为义务内容及其来源之外，最重要的是厘清作为义务的归属，并明确其不作为的行为内容。若在司法适用中将“具有作为义务且能够履行而不履行”作为行为入罪，则偏离了本罪不作为犯的实质危害特征，反而认定为其他相关的作为犯罪更加适宜。这是对司法实践案例进行检视的重点内容。

案例一：上海浦东胡某拒不履行信息网络安全管理义务罪案。¹ 行为人胡某利用网络科技公司从事出租翻墙软件。值得思考的是，首先，行为人胡某是否符合拒不履行信息网络安全管理义务罪中“网络服务提供者”这一主体身份；其次，从案情来看，胡某主动进行非法网络连接的行为已不再是不履行信息网络安全管理义务，而是直接从事违法行为。对于将此种作为犯类型的犯罪认定为不作为犯的本罪，显然不合理。

案例二：云南昆明李某拒不履行信息网络安全管理义务罪案。² 行为人李某在董事长王某的安排下，将三四万张行业卡交给某信息公司挑卡，并安排人员将后者挑选的回收卡进行制卡和发卡工作，后该信息公司将该批回收卡违规实名，且将回收卡卖给

第三方用于盗取回收卡上绑定的用户微信账号，导致绑定的微信号被大量盗取。从案情来看，李某的行为已不属于拒不履行信息网络安全管理义务，而是直接参与了侵犯公民个人信息的犯罪行为，法院将其行为认定为本罪属于将作为犯认定为本罪（不作为犯）的不当认定。

案例三：江苏沭阳孙某拒不履行信息网络安全管理义务罪案。³ 行为人孙某以网络科技有限公司（无公司账户、无财务制度、无财产管理人员，收入归个人所有）为名，在未落实网络日志留存和租户真实身份信息认证的情况下出租远程电脑。本案中，行为人孙某所依托的公司并不具有合法法人地位，其是否属于正当的网络服务提供者也需进一步明确，这直接关系到孙某的行为是不作为的拒不履行信息网络安全管理义务罪，还是作为的非法经营罪。

对三个案例进行详细对比可知，司法适用中首要的突出问题是忽视了适格主体——“网络服务提供者”的认定，导致将属于不作为犯罪范畴的本罪适用于其他作为类型的网络犯罪行为。而产生这一问题的根本原因在于，对拒不履行信息网络安全管理义务罪义务来源及义务主体的认识不清。

2019年10月21日，最高人民法院和最高人民检察院通过的相关司法解释，^[12]对拒不履行信息网络安全管理义务罪的适用标准界定进行了分析。对于“网络服务提供者”的界定，司法解释对三种服务范围进行了概括：第一种服务情形存在的问题是，完整的网络技术存在诸多环节时的局部技术链条作为一个独立的网络服务提供者进行评价不甚合理；第三种服务情形存在的问题是，将网络技术服务的提供者扩张至利用网络技术服务开展公共服务的二次服务提供者认定为“网络服务提供者”并不恰当。（第二种服务情形不存在此处所涉及的问题）概言之，如此扩张的刑事司法态度的原因在于并未将本罪名作为真正的不作为犯加以适用。若网络服务提供者实施的行为直接促成了第三者相关犯罪行为的，则应当认定为作为的共同犯罪，而非拒不履行信息网络安全管理义务罪的不作为犯罪。从这一方面来说，对该罪名的司法适用标准的确立也存在着作为犯与不作为犯混同的解释论层面的困境。综上，问题产生的关键影响因素依旧是未厘清不作为犯行为与帮助犯行为之间的界限，即网络服务提供者的相关行为在第三人违法犯罪行为中所产生作用的程度高低。

对于作为犯与不作为犯的区分，首先，要看某一举止行为是积极的还是消极的，以及该积极身体动作是否具有直接支配性，若是则可以判断为作为犯；其次，无法判断是否具有直接支配性时则要考察规范所确定的期待义务是否得到履行，若没有则可判定为构成不作为犯罪。^{[4] (p109-113)} 但问题的关键在于，司法实践中存在着将作为犯评价为不作为犯罪的情形，这正是前述提到的拒不履行信息网络安全管理义务罪在罪名设计上存在着的适用空置的困境。由此可见，不论是从司法解释的理论角度，还是从实际的司法判例角度，都存在着作为犯与不作为犯认定混同的理论风险与实践问题，而其产生的原因还是实质性作为义务的承担者及其主体身份适当性的不恰当判定。

（二）罪与非罪：技术中立行为绝对正犯化

拒不履行信息网络安全管理义务罪应当是一个纯正不作为犯罪，不仅要有义务来源，而且应当具备能够且可以履行而不履行的客观事实。要判定网络服务提供者可罚的行为到底是作为还是不作为，即可罚的是技术服务研发提供中的风险行为，还是拒不履行信息安全管理义务的消极不作为行为，抑或是深度参与信息网络使用者的违法犯罪行为的积极作为行为，这需要判断“犯罪行为”的性质。对此，将结合“快播案”和前述三个案例进行分析。

一是快播公司案。⁴ 此案主要讨论的是“技术中立行为”的刑事风险以及是否可以作为免责事由，即检视“技术中立行为”正犯化的正当性。从立法上看，对技术中立行为科以刑罚的根据是以不履行信息网络安全管理义务为内容的不作为责任。刑事司法判例也遵循了这一思路。在快播公司案中，法院认为快播公司及各被告人均明知快播网络系统内存在大量淫秽视频并介入了淫秽视频传播活动，因此具备承担信息网络安全管理义务的现实可能但拒不履行网络安全管理义务。^[13] 对于“技术中立”免责事由，法院则认为快播公司属于技术使用者而非技术提供者。对于法院的裁判观点，有学者提出，“避风港”规则强调的是，网络服务提供者不负有事先审查、实时监控网络用户的侵权信息的义务，而只负有事后通知—移除的责任。^{[14] (p141)} 那么，“技术中

立”原则下网络服务提供者的责任究竟是什么？严格意义上来说，网络服务提供者与网络服务使用者之间是民事上的合同关系，而网络服务提供者与行政监管部门之间是被管理与管理的行政关系，因此，行政监管部门不能以行政关系介入前两者之间的民事合同关系之中，要求网络服务提供者监督并制止网络服务使用者的违法犯罪行为，但可以要求网络服务提供者提供安全可靠、保证质量的服务，以符合行政监管的要求。进一步而言，行政监管部门能够要求网络服务提供者提供的担保是技术漏洞完善，还是技术本身所具有的功能或者特征被使用者非法利用的风险规避？对于前者而言，如果尚不具备进行完善的技术能力，则不能认定其构成不作为犯罪；对于后者更加不能因为技术被非法利用而惩罚技术服务提供者。故只能惩罚有漏洞修复能力而故意不修复或者与非法使用者共同从事违法犯罪等行为。

二是本文中的三个案例。这里的探讨，本质上是从另一个侧面即处罚必要性的角度来分析司法实践中对“技术中立行为”正犯化的必要性程度。三个案件中监管部门都进行了两次及以上的监管执法，包括约谈、责令整改及行政处罚，且监管部门最终认定三个案件中的行为人“拒不改正”。值得注意的是，《刑法》第286条之一规定“监管部门责令采取改正措施而拒不改正”及造成法定后果才入罪，但实践中存在着进行行政处罚后，再发生网络服务使用者从事违法犯罪行为时，是否可以认定为“拒不改正”问题。对此，笔者认为，若进行了行政处罚，也采取了纠正措施，网络服务使用者再次做出违法犯罪行为的，不应认定为“责令采取改正措施而拒不改正”，原因有二：其一，已经进行行政处罚再将其置于后续的评价之中属于重复评价；其二，技术漏洞具有潜在性，无法一次性修复完善，即便是同一种网络服务或者技术。对于客观上促进了他人犯罪、主观上也存在认识的中立帮助行为，不能简单运用刑罚进行压制。^{[15] (p208)}即便能够认定存在有漏洞修复能力而故意不修复，也不能一概以刑事责任进行追究。实际上，追究履行信息网络安全管理义务不力的网络服务提供者的行政责任，更能有效地协调技术发展、企业创新与网络空间秩序维护之间的关系。当然，如果企业成立就是出于犯罪目的或者实施犯罪行为是基于整个企业的共同决策，自然应当予以依法惩治。此外，应当重视对于行为主体即“网络服务提供者”身份的认定。不能仅从行为外观就认定其属于“网络服务提供者”，还应当明确其是否具有合法的网络服务提供者主体地位，否则只能以其他罪名进行定罪处罚。对于拒不履行信息网络安全管理义务罪的认定，则应当在明确行为主体具有合法的主体身份的基础上进行。最后，才是对其是否具有“拒不改正”的不作为犯罪事实进行认定。

（三）畸轻畸重：量刑情节及制度适用不当

司法实务中，除了应注意定罪方面的偏差之外，还应当在刑罚的裁量上准确适用量刑情节及制度。总原则是在严把入罪门槛的基础上，对于拒不履行信息网络安全管理义务构成犯罪的行为，应当慎重适用从宽。实践中，该罪名在刑罚裁量环节存在的问题主要有两个：

其一，经过监管部门行政处罚后电话通知到案且如实供述是否可以认定为自首。对比来看，案例一中，行为人胡某先后经监管部门两次约谈责令改正、一次行政处罚后，继续实施犯罪行为被公安机关电话通知到案，且最终认定为自首。一般而言，自首成立的条件是自动投案与如实供述，即自愿性与彻底性。而投案的时间则包括三种情形：“犯罪事实和犯罪嫌疑人尚未被发觉以前、犯罪事实已被发觉而尚未发觉犯罪嫌疑人以前、犯罪事实和犯罪嫌疑人均已被发觉而有关机关尚未对犯罪嫌疑人传讯或者采取强制措施以前。”^{[16] (p376-377)}公安机关电话通知犯罪嫌疑人到案中的“电话通知”的性质会影响自首自动性的认定。但大部分学者及司法判例对此都持肯定态度：一方面司法机关尚未采取实质性措施，另一方面出于鼓励犯罪嫌疑人到案的需要。然而，拒不履行信息网络安全管理义务罪有其特殊性，此罪成立要求的条件之一是“经监管部门责令采取改正措施而拒不改正”，实践中“监管部门”往往是公安机关，且犯罪嫌疑人的系列不履行管理义务的行为具有连续性。换言之，犯罪嫌疑人一直处于监管部门（多为公安机关）的实际控制之下，因此，后续认为构成犯罪后的“电话通知”不属于普通的通知性质，此情形下的“电话通知到案”不应认定为自首，而应将其到案后的如实供述作为坦白认定，从而在刑罚裁量时予以考虑。

其二，刑罚从宽的幅度不统一导致量刑畸重畸轻。案例一中，法院认定成立自首，且退还了全部违法所得并预缴罚金款，故判处有期徒刑6个月，缓刑6个月，罚金人民币3万元。案例三中，法院认为被告人存在自首、认罪认罚、退出违法所得等法定酌定从轻从宽量刑情节，故判处有期徒刑7个月，缓刑1年，并处罚金3万元。而案例二中，法院认定李某到案后如实供述自己的罪

行，认罪认罚、具有悔罪表现，可酌情从轻处罚，故判处有期徒刑1年3个月，并处罚金5000元。对比之下，一方面，案例一从宽的幅度过大，适用缓刑无法实现本罪立法的初衷；另一方面，案例二适用了认罪认罚制度后依旧判处了1年3个月的有期徒刑，相比而言则刑罚过重。此外，在牟利性犯罪中如何协调主刑与罚金刑的关系也是司法适用中需要统一的问题，如案例一和案例三判处的罚金达3万元，而案例二仅为5000元，是否可以通过加重罚金刑来减轻主刑值得反思。

除了理论上要坚持实质解释的进路，实践中也必须处理好从宽与从严的关系。从以上分析来看，拒不履行信息网络安全管理义务罪的不当从严适用主要表现在三个方面：一是作为犯与不作为犯认定的混同；二是消极帮助行为的绝对正犯化；三是刑罚从宽的适用阶段错误及刑罚畸轻畸重。纠正这些错误倾向的基本思路则是犯罪认定从严、刑罚裁量从严，即严把入罪门槛。对于应当追究刑事责任的，鉴于网络空间犯罪的危害性，应当从严科处刑罚。产生上述司法适用中问题的原因在于未厘清网络空间管理义务的责任分配，无法在罪名的司法适用中准确认定义务来源及义务人。因此，在根本的治理理念上，还应当重视协调处理好技术发展与刑法风险防控之间的关系，从而更加理性地立法与执法。

三、纠偏思路：司法适用中的完善对策建议

对网络空间进行刑法治理具有一定的正当性，但要把握合理限度，其路径则是强化对于义务来源的法定化、实质化解释。同时，也要将这种理念贯彻到涉网络刑事司法中，做到宽严相济，实现有责必罚、当罚则罚，避免陷入扩大犯罪圈却又无法实现刑法治理效果的怪圈。

（一）罪名认定上严格作为义务的主体

首先，应当对行为主体是否属于“网络服务提供者”进行实质性的判断。一方面，对于假借“单位”名义作出行为的，由于单位不适格，自然不能认定“网络服务提供者”的单位主体。另一方面，对于由独立自然人实施的网络服务提供行为，应当厘清其到底是网络服务提供者角色下的不作为犯，还是无身份自然人下的作为犯罪，从而排除不符合该罪名适用的行为，避免进行不必要的后续判断。

其次，要界分行为人的行为究竟是未履行义务的不作为，还是积极主动进行犯罪的作为。对于积极实施信息网络违法犯罪行为的，应当进行相应的行政处罚和犯罪认定，不能将其作为拒不履行信息网络安全管理义务罪来定罪处罚，这不仅不利于治理网络犯罪，而且会造成立法本意与司法适用相背离。

再次，对于不积极履行信息网络安全管理义务的，必须进行法定化、实质化认定，义务来源不仅要有刑法上的依据，还应当作实质解释，即作为网络空间的网络服务提供者，其作为义务是不断消除服务存在的技术漏洞刑事风险，还是制止服务使用者利用服务进行违法犯罪？笔者认为，不能将网络空间本身所具有的特点所存在的违法犯罪隐患，过重地附加到网络服务提供者身上，而应当实质性地考察网络服务提供者在违法犯罪发生中的实质性作用。并且，网络服务提供者的安全管理义务是特定的而不是一般的，换言之，对已经显现出来的且可以修复的技术或服务漏洞，网络服务提供者视而不见而被服务使用者利用后也不采取纠正措施的，监管部门才能对网络服务提供者进行行政处罚，并且在初始阶段，监管机关有提醒约谈的义务，而不能一经发现就对其进行行政处罚。

最后，应当慎重认定单位犯罪。对于单位负责人自行决定的，应当认定为个人的单独犯罪或者共同犯罪；对于经过单位内部集体决策的，应当认定为单位犯罪，并对直接负责的主管人员或者其他责任人进行刑事处罚；对于单位成立的目的是进行信息网络违法犯罪的，应当认定为个人犯罪。这样做的目的是，既不影响没有违法犯罪单位的正常经营与长远发展，也依法打击制裁了违法犯罪的单位或个人。

（二）责任判定上强化罪过的刑法属性

刑事责任的本质是行为人对危害结果的发生具有罪过。对于罪过的司法化证明，强化其刑法属性，主要步骤有两个：

其一，对行为之行为性的判断。不作为应当具有行为性，也必须具备危害行为的三个特征，即不作为是行为人危害社会的身体动静，且由行为人的心理态度支配、能够引起外界变化，最终具有损害性和威胁性。^{[16] (p167-168)} 拒不履行信息网络安全管理义务的行为，也应当具备不作为的行为性的三个特征。在拒不履行信息网络安全管理义务罪中，行为人的身体动静究竟是创造技术、提供服务行为本身，还是没有采取措施制止信息网络服务使用人的违法犯罪行为？笔者认为，应当入罪的身体动静应当是，技术或服务存在被利用从事违法犯罪的风险，消除这种风险的措施又是存在的或者可以在短时间内形成的，而网络服务提供者不采取相应的改善措施。值得注意的是，技术或服务本身所固有的特征若被网络服务提供者所利用进行违法犯罪，则属于纯粹的技术中立行为，不应当扩大刑事责任的追究范围。

其二，对具体的、特定的心理态度的认定。在拒不履行信息网络安全管理义务罪的认定上，除了明确作为义务来源之外，第二个关键则是要认定网络服务提供者发生身体动静时的心理态度。通说认为，行为人能够履行而不履行作为义务放任危害结果的发生即构成不作为。具体来说，要证明两点：一是行为人明知自己不履行信息网络安全管理义务的行为会发生危害社会的结果；二是行为人因追求其他目的而放任了不履行信息网络安全管理义务所产生的社会危害。就前者而言，需要根据技术或服务漏洞修复的难度来判定明知的程度，不能泛化网络服务提供者对于服务（或者技术）漏洞可能产生风险的明知范围与程度。对于后者来说，放任是希望的派生意志，就是在追求某种目的的过程中，放任了其他危害结果的发生，而刑法关注的并非从属性，而是放任其他危害结果的可责难性。^{[17] (p42-50)} 然而，拒不履行信息网络安全管理义务罪，相比其他网络犯罪具有特殊性，即危害结果的间接可谴责性，即网络服务提供者不履行作为义务并不直接产生危害结果，而是通过其他行为人积极主动实施违法犯罪而实现。概言之，对于放任的认定，应当强调该作为义务与其他行为人违法犯罪行为的关联性强度，以及是技术本身的功能性特征，还是缺陷性隐患。对于纯技术中立行为，不能认定为网络服务提供者具有放任意志。

（三）刑罚裁量上规范适用情节与制度

实现技术与刑法治理的良性互动，应当坚持宽严相济，为正常的技术创新与发展营造宽松的秩序空间。为了保证刑罚适用的相对统一性，对于拒不履行信息网络安全管理义务罪的刑罚裁量要重视规范化认定及处刑。

首先，要处理好“自首”的认定问题。针对公安机关充当监管部门的情形而言，由于行为主体一直处于公安机关的监控下，若通过通知等形式到案的，不应认定为自首，而可以根据其表现认定为坦白或如实供述等情节，否则，将不利于对此类网络犯罪形成震慑作用。

其次，要处理好认罪认罚制度在“宽严相济”刑事政策下的正确适用。对于“不认罪”者，不能认定为“自首、坦白、立功”。同时要注意，在“认罪”环节上要避免重复评价，即第一次行政处罚后责令采取改正措施的，不能在行政处罚之后再追究刑事责任。此外，不论是认罪，还是认罚，最终都会涉及从宽的具体适用幅度，这关系到刑罚效果与积极功能的实现。对此，有学者提出了层级性理论，即“针对不同案件类型、不同时间节点、不同认罪认罚的具体方式（如自首、立功、退赃退赔等）来设置认罪认罚的从宽幅度”。^{[18] (p62)} 结合该罪名的不作为犯的本质，其要比作为犯的认罪认罚更加注重认罪的主动性与真实性，原因在于拒不履行信息网络安全管理义务罪有着极强的行政犯色彩，需要经过监管部门的前置性认定与处置。可见，认罪认罚从宽制度在该罪名的适用上需要更加重视刑法治理的效果。当然，前提是已经在入罪环节排除了不应当入罪的行为。

结语

网络空间已成为与现实社会公共空间并存的第二大公共空间，其治理的思路应当是共治。不论是网络技术服务的提供者，还是政府监管部门，抑或网络技术服务的使用者，都有相应的责任与义务。换言之，不能对网络技术服务提供者片面附加过重的安全管理义务，也即对于本罪作为义务来源的认定，应当作法定化、实质化的解释，这也是本文问题意识的缘起，以及展开实质解

释与反思司法适用的重要前提。在司法适用方面,虽然本罪名的适用案例较少,但也值得从理论上与立法上反思罪名设置的内在逻辑与可能存在的司法适用风险点。刑法参与网络空间治理需要关注入罪界限与刑罚效果两个方面,既不能使犯罪圈无序扩张,也不能在有限的犯罪圈内消弭刑罚效果。应当特别注意的是,互联网技术的发展与信息社会的形成,使网络空间已成为传统犯罪网络化与纯正网络犯罪的发生场域。相应地,刑法立法与刑事司法对于二者应当坚持不同的应对策略,对前者要保持准确认定与严厉打击,而对后者要保持宽严相济,合理分配刑事责任,以便既维护网络安全,又促进互联网技术的创新发展。

参考文献:

- [1]中国互联网络信息中心(CNNIC).第46次中国互联网络发展状况统计报告[EB/OL].http://www.gov.cn/xinwen/2020-09/29/content_5548176.htm,2020-09-29/2021-03-09.
- [2]于志刚.网络思维的演变与网络犯罪的制裁思路[J].中外法学,2014,(4).
- [3]刘宪权.网络犯罪的刑法应对新理念[J].政治与法律,2016,(9).
- [4]周光权.刑法总论[M].北京:中国人民大学出版社,2016.
- [5]陈兴良.作为义务:从形式的义务论到实质的义务论[J].国家检察官学院学报,2010,(3).
- [6]杨兴培.论不作为犯罪义务来源的法律属性[J].政治与法律,2014,(6).
- [7]段凤丽,李金明.不作为犯罪的作为义务来源新论[J].国家检察官学院学报,2004,(5).
- [8]姚诗.不真正不作为犯的边界[J].法学研究,2018,(4).
- [9]毛玲玲.不作为犯义务的限制实质论[J].东方法学,2014,(3).
- [10][德]尼克拉斯·卢曼.风险社会学[M].孙一洲,译.南宁:广西人民出版社,2020.
- [11]梁根林.传统犯罪网络化:归责障碍、刑法应对与教义限缩[J].法学,2017,(2).
- [12]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[EB/OL].http://www.cac.gov.cn/2019-10/25/c_1573534999086260.htm,2019-10-25/2021-07-30.
- [13]华律网.盘点快播四宗罪[EB/OL].<https://news.66law.cn/a/20161011/9514.html>,2016-09-14/2021-04-13.
- [14]陈洪兵.网络服务商的刑事责任边界——以“快播案”判决为切入点[J].武汉大学学报(哲学社会科学版),2019,(2).
- [15]陈洪兵.论中立帮助行为的处罚边界[J].中国法学,2017,(1).
- [16]马克昌.刑罚通论[M].武汉:武汉大学出版社,1999.
- [17]高铭暄.刑法学原理:第二卷[M].北京:中国人民大学出版社,2005.

[18]陈卫东. 认罪认罚从宽制度研究[J]. 中国法学, 2016, (2).

注释:

1 参见上海市浦东新区人民法院(2018)沪0115刑初2974号一审刑事判决书。

2 参见云南省昆明市盘龙区人民法院(2020)云0103刑初1206号一审刑事判决书。

3 参见江苏省沭阳县人民检察院沭检一部刑诉(2020)827号起诉书。本案判决书尚未公开,但法院采纳了检察机关的所有指控及量刑建议。详见:《全国首例拒不履行信息网络安全管理义务案宣判》,载《江苏法治报》2021年5月20日(06)版。

4 参见北京市海淀区人民法院(2015)海刑初字第512号一审刑事判决书。