武汉大学法学院40周年院庆系列学术活动

第一届信息犯罪防控论坛

智慧社会环境下网络平台犯罪治理

论

文

集

主办：中国犯罪学学会信息犯罪防控专业委员会

承办：武汉大学法学院

武汉大学刑事法研究中心

武汉大学网络治理研究院

协办：武汉大学马克昌法学基金会

广州华多网络科技有限公司

武汉鲲鹏智法科技有限公司

中国　武汉

二〇一九年三月

内部资料注意保密

目 录

论网络服务提供者的协助管理义务及相关刑事责任

——从快播案判决切入……皮 勇 1

网络直播平台犯罪之治理……谢昊轩 郭泽强 23

网络服务平台的类型及其监管责任探讨……叶良芳 应家赟 38

网络平台犯罪的政策调适与刑法应对……魏 东 悦 洋 57

政府数据开放的刑事风险及治理

——基于刑法解释学的进路……柳 洁 82

网络直播平台犯罪风险的企业防控对策……齐守明 王若琪 93

非典型网络开设赌场行为的刑法适用……王 刚 101

我国彩票销售网络平台犯罪治理……宫步坦 钟佳佳 114

犯罪经济学视野下的网络平台数据泄露治理对策探究……王启欣 126

数字经济培育与网络黑产治理……吴沈括 144

论远程视频取证模式的构建……张启飞 虞纯纯 148

智慧社会语境下的网络犯罪情势与治理对策……崔仕绣 崔文广 156

电商法颁布背景下利用网络直播进行犯罪的现状及规制……陈奕屹 174

附 录：主题发言人讲稿……188

网络平台犯罪及其治理对策……皮 勇 188

利用第三方支付平台犯罪及其治理……汪恭政 193

利用网络直播平台进行犯罪的现状及成因分析……陈奕屹 202

利用网约车服务平台犯罪基本情况及现状……吴 勃 207

论网络服务提供者的协助管理义务及相关刑事责任

——从快播案判决切入

皮勇*

摘要：对网络服务提供者设立协助管理义务是各国立法的趋势，国内外立法规定的义务内容基本相同，主要是协助执法、内容信息监管、用户数据保护，我国相关立法在协助管理义务的类型化、区别化方面与国外立法的差距较大。我国网络服务提供者可能构成作为犯形式的单独犯、帮助犯、帮助他人利用信息网络犯罪活动罪和拒不履行信息网络安全管理义务罪，前二者与国外相关立法相似，国外网络服务提供者违反协助管理义务的法律责任主要是民事责任和行政责任，我国刑法中的拒不履行信息网络安全管理罪存在过度犯罪化的缺憾。

关键词： 网络服务提供者 信息网络安全管理义务 中立的帮助行为 刑事责任

在信息化网络化社会中网络服务提供者处于枢纽地位，网络社会活动高度依赖于网络服务，同时，与网络服务相关的违法犯罪数量迅速增长，给网络社会治理带来新的严峻挑战。网络服务提供者协助网络安全管理是治理网络社会的关键，“网上信息管理，网站应负主体责任”，[①]新通过的《网络安全法》和《刑法修正案（九）》明确规定了网络服务提供者的信息网络安全管理义务和法律责任，包括刑事责任。在网络服务提供者的信息网络安全管理义务及刑事责任问题上，刑法理论界对相关立法和司法判决的看法存在严重分歧，影响着网络社会治理路径的选择。网络服务的法治化是各国立法面临的共同课题，我国应当从本国社会信息化网络化实际出发，借鉴国外立法的成功经验，适当设定网络服务提供者的信息网络安全管理义务，合理划定其承担刑事责任的边界。

一、“快播案”引出的问题

2016 年 9 月“快播案”审结宣判，“快播案”的事实认定和判决理由引起刑

* 武汉大学法学院教授、博士生导师。
基金项目：国家社会科学基金重点项目（项目号 13AFX010）“全球化信息化社会环境中的新型恐怖活动及其整体法律对策研究”

① 习近平：《在网络安全和信息化工作座谈会上的讲话》，《人民日报》2016 年 4 月 26 日第 2 版。

法学者的热议，存在支持和批判有罪判决的两种对立观点。

在批判有罪判决的观点中，又有基于案件事实和基于判决理由而提出批判意见的两种不同情形。例如，有学者认为，“快播既不是一个淫秽信息的内容提供者，也不是一个专门供用户发布淫秽信息的平台，但是作为一款可以播放各种视频信息的播放器软件，客观上为那些分享淫秽信息的用户提供了帮助和便利，这就是其涉嫌犯罪的事实基础。”[①]进而提出快播公司不应承担刑事责任的观点，就属于前者情形。而海淀区人民法院审理查明的事实是：快播公司不只是向用户提供资源服务器程序（QSI 软件）和快播播放器程序（QVODPlayer 软件），其网络系统按其设计目标抓取访问量大的文件放入快播公司的缓存服务器中，将从用户到用户的信息传播渠道改变为从公司的缓存服务器到用户，以加快文件的传输速度；为了规避版权和淫秽视频带来的法律风险，该系统将被抓取的文件由单服务器传输完整文件改为多服务器协作传输打散的文件，最后在用户端集合播放；快播公司盈利受益于大量用户的点播；快播公司因涉及传播淫秽视频资源受过两次行政查处。因此，前者情形观点缺乏事实基础。但是，该案判决书认定，“快播公司具备承担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”，“放任其网络平台大量传播淫秽视频，因而构成传播淫秽物品牟利罪。”[②]将拒不履行管理义务与构成传播淫秽物品的行为关联在一起，一定程度上误导了学者的判断。

属于后者情形的论述以中立帮助行为理论为立论基础。例如，有学者提出“网络中立帮助行为”的概念，“尽管网络中立帮助行为具有上述特殊性，但其只是在中立帮助行为的内核之外披上了网络化的外衣，在刑事法理上并没有彻底脱离中立帮助行为的基本范畴，因此对其进行分析仍然应当运行在中立帮助行为的理论基础之上。”[③]“网络中立帮助行为的案件的处理走向了“变通化”，即对于存在正犯但难以抓获的情形以及没有正犯的情形，实务部门往往会避开帮助犯的探讨，在刑法规范中寻找“既有”的罪名，对其进行扩张解释，直接将网络中立帮助行为作为分则罪名的正犯行为处理。……快播案最终在网络服务提供者的网络

① 车浩：《谁应为互联网时代的中立行为买单？》，载《中国法律评论》2015 年第 3 期。
② 《吴铭等制作、复制、出版、贩卖、传播淫秽物品牟利罪一审刑事判决书》，北京市海淀区人民法院（2015）海刑初字第 512 号。
③刘艳红：《网络中立帮助行为可罚性的流变及批判——以德日的理论和实务为比较基准》，载《法学评论》2016 年第 5 期。

安全管理义务的牵引下以传播淫秽物品牟利罪论。”[①]中立帮助行为理论研究的是外观上无害、客观上对正犯行为或结果起到促进作用的行为，德国刑法理论称之为“外部的中立的行为”，[②]希望提出区别于应当处罚的帮助犯的不处罚标准，该理论以存在具体的实行犯为前提，通常以传统社会环境中的不负有法定义务的日常行为或者业务行为为研究对象。将该理论用于分析网络服务提供者的所谓“中立的帮助行为”，实质上否定其负有信息网络安全管理义务，这与事实相矛盾，[③]而且，网络服务提供者“客观上帮助”的并非具体的正犯，而是在概括的故意和盈利目的驱动下为包括违法犯罪人在内的大量不特定的用户提供网络服务，理论适用的条件和对象不同，故以上观点值得商榷。

支持该案判决的代表性观点认为，“快播公司拉拽淫秽视频文件存储在缓存服务器里，并且向用户提供缓存服务器里的淫秽视频文件的行为，则不是中立的帮助行为，而是传播淫秽物品的正犯行为，……一审判决还从快播公司负有网络视频信息服务提供者应当承担的网络安全管理义务，并且具备管理的可能性但没有履行网络安全管理义务的角度，论证了快播公司构成传播淫秽物品牟利罪。……快播公司拉拽淫秽视频文件存储在缓存服务器之后，就有义务防止用户观看该视频文件，但快播公司却同时向用户提供缓存服务器里的淫秽视频文件。所以，从作为与不作为相结合的角度，也能说明快播公司的行为属于传播淫秽物品。”[④]该观点中有两点值得商榷：一是将包括单纯的缓存服务在内各类网络传输缓存服务一概认定为应负刑事责任的传播行为；二是将他人提供的淫秽信息进行有规避法律目的的分解、分散传输和整合行为定性为不履行信息网络安全管理义务行为，并类比于砍伤人后继续砍杀来说明其既是作为犯又是不作为犯。[⑤]《网络安全法》和其他互联网管理法规规章禁止任何人传播违法信息，按照前述学者的观点，该类禁止性规范也可以认为是设立了不得传输违法信息的义务，但是，它不等同于信息网络安全管理义务，后者不可能由传播淫秽物品牟利罪的法条推

① 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。
②Vgl. Marcus Wohlleben, Beihilfe durch aeusserlich neutrale Handlungen,1996,S.4.
③ 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。
④ 张明楷：《快播案定罪量刑的简要分析》，《人民法院报》2016 年 9 月 14 日第 3 版。
⑤ 张明楷教授的这种观点未获得广泛的认同，部分学者认为，禁止规范和命令规范不可能同时存在于一个刑法规范中，规定禁止性规范的刑法条文不能成为作为义务的来源。参见肖中华：《论不作为犯罪的几个问题》，载王作富主编：《刑事实体法学》，群众出版社 2000 年版，第 81 页；林亚刚：《刑法学教义（总论）》，北京大学出版社 2014 年版，第 114-115 页。

导出。从文义上讲，管理义务是指对服务或管理对象依法管理的义务，自身违法犯罪行为不在“管理”的含义范围内，否则，网络服务提供者故意传播自己制作、整理、编辑的淫秽信息也可以按拒不履行信息网络安全管理义务罪定罪处罚，这明显是对犯罪性质的错误认识。

“快播案”判决及相关评论争议的焦点是网络服务提供者的信息网络安全管理义务及其刑事责任，网络服务提供者是网络社会的核心单元，信息网络安全管理义务的范围及相关刑事责任的边界直接影响网络服务提供者的行为，进而传导影响整个网络社会活动乃至我国社会信息化发展，其合理设立具有重要的社会意义。当前我国刑法被认为向“功能性、积极性”转变，[①]积极介入网络社会治理，除了前述判决体现的司法趋势外，《刑法修正案（九）》设立了拒不履行信息网络安全管理义务罪，从刑法上确立了网络服务提供者的信息网络安全管理义务，将其与刑事责任直接联系。刑法是一把双刃剑，过度介入网络社会治理会损害社会的公正和发展，应使之不超出良性、适度的范围，关键是适度设定网络服务提供者的信息网络安全管理义务，合理划定其刑事责任的边界。

二、网络服务提供者的协助管理义务范围

网络服务提供者是社会服务提供者，本来不具有社会管理的权力和义务，信息网络安全的义务“是国家向网络服务提供者(服务商) 施加的义务———从另一个角度看， 这也是一种授权， 服务商有权删除网络信息———法律要求他们这么做，否则将承担法律责任。”[②]这种法律责任是在特殊的网络社会环境中产生。当前网络违法犯罪数量巨大且具有跨区域性，仅靠以条块架构组织起来的传统国家管理部门难以管控，而网络服务提供者能够在第一时间管控信息网络空间的违法犯罪活动，实时管理能力超过专门的社会管理部门，而且，它们构建网络信息活动空间、设定网络活动规则、直接管理网络信息活动，与包括违法犯罪者在内的服务接受者共生互利，具有特殊的社会地位和能力，应当是“网络社会重要的组织力量，对维护网络信息安全负有重要社会责任。”[③]为了有效治理网络社会，信息发达国家普遍对网络服务提供者设立信息网络安全管理义务，适度设定该义务的范围成为立法的关键。

[①]参见周光权：《积极刑法立法观在中国的确立》，载《法学研究》2016 年第 4 期。
[②]秦前红、李文才：《网络公共空间治理的法治原理》，《现代法学》2014 年第 6 期。
[③]李源粒：《网络安全与平台服务商的刑事责任》，载《法学论坛》2014 年第 6 期。

（一）国外网络服务提供者的信息网络安全管理义务

目前国外立法对网络服务提供者规定的信息网络安全管理义务主要是协助执法、信息内容监管和个人数据保护义务。

1. 协助执法义务

协助执法义务是指网络服务提供者协助犯罪侦查部门以技术手段获取他人通信内容或通信相关数据，包括通信监视、数据留存及其附随义务。协助执法义务不仅多见于外国刑事立法中，也是国际组织的重要立法内容。协助执法义务通常是要求公共电信服务提供者承担，随着互联网通信的发展，提供公共通信服务的网络服务提供者也是该义务的承担者。[①]

协助通信监视义务，是指网络服务提供者依照法律规定和调查机关的要求，利用通信技术主动对被监控对象的通信数据与通信内容进行实时获取和记录。代表性的立法包括欧盟理事会《关于合法拦截通信的决议》、[②]欧洲理事会《关于网络犯罪公约》、[③]德国《电信法》和《电信监控法令》、[④]美国《通信协助执法法》等。[⑤]协助执法义务的内容，通常是要求网络服务提供者具备一定的通信监控能力，提供通信监控接口或称交换接口，具备及时响应能力、实时监控能力、监控数据传输和安全保障能力，以及承担协助解密和信息保密义务。批评者认为以上立法导致网络服务提供者成本大增，影响自身运营和发展，也必然侵犯公众隐私，削弱与客户的信任关系。对此国外立法采取两种限制方法：一种是限制协助监控能力，避免强制网络服务提供者过度投入。如欧洲理事会《关于网络犯罪的公约》第 20 条、第 21 条规定的协助，限于“服务提供商在其技术能力范围内”；另一种是提供协助监控的费用或者补偿，如美国 1994 年《通信协助执法法》第 109 条、[⑥]德国 2004 年《电信法》的相关规定。[⑦]

数据留存义务，是指网络服务提供者采取一定技术手段保存用户使用通信网络所产生的通信数据，在有关部门调查刑事犯罪、恐怖活动等时予以提供。例如《美国法典》第 2704 条规定了数据保护备份，第 2703 条规定了按要求披露用户

[①]德国《2005 电信监控条例》第 3 条规定，协助通信监控义务适用于提供公共电信服务的电信运营商，公共通信服务、互联网接入服务和其他互联网服务的提供者都被纳入“服务提供者”的范围。
Vgl. Telekommunikations-Ueberwachungsverordnung, 2005, §3.
[②]See Council Resolution of 17 January 1995 on the lawful interception of telecommunications, §3. §8. §9.
[③]See Council of Europe Convention on Cybercrime, 2001, §20. §21.
[④]Vgl. Telekommunikationsgesetz, 2004, §110，Telekommunikations-Ueberwachungsverordnung, 2005.
[⑤]See Communication Assistance for Law Enforcement Act,1994, Chapter I, §103.
[⑥]See Communication Assistance for Law Enforcement Act, 1994, Chapter I, §109.
[⑦]Vgl. Telekommunikationsgesetz, 2004, §110-9.

通信或者记录。[1]根据 2006 年欧洲议会和欧盟理事会《关于存留因提供公用电子通信服务或者公共通信网络而产生或处理的数据及修订第 2002/58/EC 指令的第 2006/24/EC 指令》，2008 年德国对多部法律进行了修改，要求德国公用电信和公共通信网络服务提供者承担存储数据、保护数据安全的数据留存义务。前述指令和立法遭受广泛的批评和反对，2010 年德国联邦宪法法院以侵犯通信秘密与违背比例原则为由判决数据留存的法律违宪，2014 年欧洲法院判定前述指令无效，认为，留存的数据作为一个整体可能提供相关人的确切信息从而侵犯人身相关权利，数据留存对所涉基本权利所造成的广泛、严重的干涉不能充分限制在绝对必要的情形下，未要求数据必须在欧盟境内留存，不能确保对独立机构的保护和安全要求的符合性。[2]2015 年德国通过《通信数据的存储义务与最高存储期限引入法》，对网络服务提供者的数据留存义务进行了若干限制，包括限制存储的数据类型、存储期限、政府机关使用数据的范围。

除了以上两项主要的执法协助义务外，国外立法还规定网络服务提供者承担相关附随义务，如按照有权机关的要求提供所持有的数据、报告违法信息和活动、[3]提供相关技术协助、保密等义务。[4]

2. 信息内容监管义务

信息网络空间存在海量的违法内容信息，执法部门仅靠自身的力量难以有效监控，欧美立法规定网络服务提供者承担内容信息监管义务。

欧盟 2000 年《电子商务指令》（以下简称《指令》）中规定了信息社会服务提供者的义务，[5]包括：（1）一般性非监管义务和特殊情况下法律或命令规定的监督义务；[6]（2）信息服务提供者在知晓非法活动后迅速删除、阻止他人访问非法信息义务；[7]（3）信息存储服务提供者对非法信息活动的注意义务。[8]该指

[1]See 18 U.S.C. §2703, §2704.

[2]See"The Court of Justice declares the Data Retention Directive to be invalid", http://europa.eu/rapid/press-release_CJE-14-54_en.html.

[3]美国法典第 2258A 条规定了网络服务提供者报告其系统中的涉及儿童色情或者儿童性滥用的视频材料的违法信息和活动的义务，并规定了罚金。See 18U.S.C. §2258A.

[4]See Council of Europe Convention on Cybercrime, 2001, §18. §19.

[5] See Directive 2000/31/EC of the European parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

[6]欧盟《指令》序言第 47 段规定，"欧盟成员国不应当对服务提供者强加监督义务，所规定的义务应当为一般性的。此规定不涉及特殊情况下的监督义务，特别是不得影响各成员国官方根据国内立法发布的命令。" See preamble of Directive on electronic commerce, (47).

[7]欧盟《指令》序言第 46 段规定，"为了可以适用限制责任的条款，信息服务提供者包括存储服务提供者在被通知或知晓非法活动时，必须迅速删除涉及的信息或者阻止他人访问该信息；……本指令不影响成员国规定在删除信息或者阻止他人访问该信息前必须迅速履行的特别要求。"See preamble of Directive on

令还对提供"纯粹传输"、"缓存"、"存储"服务的三类中间服务提供者规定了共同免责条件和普通监督义务的排除，[1]该共同免责条件是"不得修改传输的信息，但不包括在传输过程中进行的技术性处理，因为这些处理不改变所传输信息的完整性。……只是使该传输更有效率，……是纯技术性的、自动的和被动的，这表明其既不知道也无法控制传输或存储的信息内容。"[2]缓存、存储服务提供者在知晓非法活动后，必须迅速移除或者阻止他人访问涉及的信息，才能免责。以上免责的规定"不应影响法院或者行政机关根据成员国的法律制度，要求服务提供者终止或者预防侵权行为的可能性。"[3]也不适用于"服务提供者故意与服务接受者合作实施超越'纯粹传输服务'或'缓存'活动的非法行为。"[4]

德国早在 1997 年就在《电信服务法》规定了服务提供者的信息内容管理义务，承担一般法律要求的封锁他人提供的违法内容信息的义务，但是，除非同时满足"知晓内容"、"技术上有可能阻止"、"阻止不超过其承受能力"三个条件，免除其法律责任，此外，对自己提供的内容信息应承担责任。[5]在服务提供者仅"提供（违法内容信息）利用途径"或者"自动缓存（违法内容信息）"时，不负有监管义务。[6]在前述欧盟指令生效后，德国 2007 年《电信媒体法》承袭了前述两部法律文件的立场，对提供"作为信息的传输通道"、"为加速信息的传输的临时存储"、"信息存储"三种中间网络服务的服务提供者规定，除非同时满足前述三个条件，对他人提供的违法信息不承担责任，但是，包括以上三类中间网络服务提供者在内的所有服务提供者都必须承担法律规定的移除或者拦阻对违法信息的访问的义务，同时，对自己提供的信息依照一般法律承担责任。[7]

electronic commerce, (46).

[8]欧盟《指令》序言第 48 段规定，"本指令不影响成员国为了发现和阻止一定类型的非法活动，要求为用户提供存储服务的服务提供者承担注意责任和义务，该注意义务对服务提供者应当是合理的，并有相应的国内立法规定。"See preamble of Directive on electronic commerce, (48).

[1]See Directive on electronic commerce, §12-15.

[2]See preamble of Directive on electronic commerce, (42), (43).

[3]See Directive on electronic commerce, §12-14.

[4]See preamble of Directive on electronic commerce, (44).

[5] 德国 1997 年《电信服务法》第 5 条规定，"（1）服务提供者根据一般的法律对自己提供的内容负责；（2）如果所提供的内容是他人的，那么只有在服务提供者知晓这些信息的内容，并且在技术上有可能阻止且进行阻止不超过其承受能力的情况下，才承担责任；……（4）如果服务提供者在不违反《电信法》第 85 条关于保守通信秘密规定的情况下知晓信息内容，有技术可能加以阻止，且阻止不超过其承受能力的，那么，根据一般的法律产生的对于违法内容信息的封锁义务不受影响。"Vgl. Teledienstegesetz, 1997, §5.

[6]德国 1997 年《电信服务法》第 5 条第（2）项规定，"服务提供者对只由自己提供利用途径，而由他人提供的内容不负责任。基于用户的要求，自动、短时间地提供他人的内容信息，该行为被视作介绍通道。"Vgl. Teledienstegesetz, 1997, §5.

[7]德国 2007 年《电信服务法》第 7 条至第 10 条规定，"（1）服务提供者应当根据一般的法律对自己提供的信息承担责任。（2）第 8 条至第 10 条意义内的服务提供者无需监控他们传输或者储存的信息，或者搜索

美国法典第 17 章第 512 条、第 47 章第 230 条规定了服务提供者不承担民事责任的条件。美国法典第 17 章第 512 条规定了提供短时间的数字网络通信、系统缓存、根据用户指令在系统或者网络中寄存信息、信息地址工具服务的四类服务提供者免除民事责任的条件，其共同免责条件是服务提供者：（1）不是信息的提供者，不能对信息内容进行修改，也不能对信息进行选取；（2）不知晓目标信息是侵权材料，或者没有认识到明显存在侵权行为的事实或者情况，或者在认识到后或者得到侵权通知后，迅速予以移除该信息或者阻断、屏蔽对其的访问；（3）服务提供者没有在其络用户的侵权行为中直接获得经济利益。[①]美国法典第 47 章第 230 条是对私人拦阻或审查可能对未成年人造成损害的淫秽、下流、骚扰等冒犯性信息的保护，规定网络服务提供者不因拦阻和审查内容信息而承担发布信息的民事责任。[②]需要注意的是，以上 2 条规定只免除了服务提供者的民事责任，服务提供者仍然会因违反美国法典其他法条而承担行政、刑事法律责任。[③]

3.用户数据保护义务

欧美国家重视保护个人数据，明确规定网络服务提供者承担保护和管理用户个人数据的义务。德国 2007 年《电信媒体法》第 4 章“数据保护”规定了服务提供者承担保护用户数据的义务，[④]服务提供者只能在相关法律许可或者用户同意的范围内，为了提供电信多媒体服务或者为了其他目的而收集和使用个人数据。[⑤]除了法律规定的可以不告知用户的情形，服务提供者在收集、存储、传输和使用个人数据前，必须将相关情况告知用户并获其同意。有权机关可以依法要求网络服务提供者提供个人数据，协助相关部门履行法定职责。

显示存在违法行为的事实。即使根据第 8 条到第 10 条的规定服务提供者不承担责任，也不得影响根据一般的法律规定的移除或者拦阻对信息的访问的义务。必须保护电信法第 88 条规定的隐私。”Vgl. Telemediengesetz, 2007, §7-10.

[①]See 17 U.S.C. §512 (a), (b), (c), (d) (2006).

[②]美国法典第 47 章第 230 条(c)规定：“（1）任何服务提供者或者交互式计算机服务使用者不应当被当做其他内容信息提供者提供的信息的发布者或者演讲者；（2）任何自愿的以善良动机的限制访问、获取以上冒犯性信息的，以及为限制以上信息而采取的行动或者技术手段，不承担民事责任。”See 47 U.S.C. §230 (c) (2006).

[③]美国第 47 章第 230 条（e）“对其他法律的影响”款明确规定，“本条不应被解释为修改本节第 223 或者第 231 条、关于淫秽的第 71 条、关于儿童性利用的第 18 章第 110 条或者其他联邦刑事法律的执行。”但是，美国法院的判决确认网络服务提供者没有义务监控他人上传的内容信息，这是因为“考虑到一般情况下需要大量的人力来审查上传到互联网的数以百万的文件，附加此义务将会使对互联网的访问戛然而止。”参见[美] Lawrence G.Walters,《美国网络服务提供者的刑事责任——基于网上色情信息的视角》，《刑法论丛》2015 年第 4 卷（总第 44 卷），杨新绿、涂龙科译，第 467 页。

[④]Vgl.Telemediengesetz, 2007, §11-15.

[⑤]这里的“其他目的”，根据德国《电信媒体法》第 14 条“库存的数据”之（2）的规定，是“根据有权机关的命令，服务提供者可以在具体案件中提供库存的数据相关信息，其范围以起诉犯罪、州警察当局预防危险、联邦和州机构履行保护宪法、联邦情报机构和军队反情报机构或者保护知识产权的法定职责的需要限。” Vgl. Telemediengesetz, 2007, §14（2）.

美国法典第 121 章“存储的有线和电子通信和交易记录访问”规定了保护用户个人数据的义务，第 2702 条“自愿披露用户通信或者记录”、第 2703 条“按照要求披露用户通信和记录”、第 2704 条“备份保护”规定了通信服务提供者披露、备份用户通信数据和内容信息的义务，禁止电子通信服务提供者违反法律规定和未经用户同意，故意披露存储的或者服务中他人的通信的内容数据，同时，规定了服务提供者披露数据的免责事由，如服务提供者非故意获取的内容信息看似与犯罪活动相关、出于善意相信出现了涉及死亡或者严重伤害的紧急事件等情况。[①]政府部门可以依法要求披露用户通信和记录，[②]服务提供者负有依照政府部门的要求备份保护用户电子通信内容的义务。[③]

前述欧美立法对网络服务提供者规定的信息网络安全管理义务具有以下特点，有必要研究和借鉴。

（1）网络服务提供者原则上应承担一般法律规定的管理义务，单纯技术服务类型的网络服务提供者在一定条件下不承担民事责任。不同类型的服务提供者承担的管理义务有一定差别：第一，协助执法机关进行通信监控、数据留存和保护用户数据是各类公共通信服务提供者的共同义务；第二，网络服务提供者不承担审查用户上传信息的义务，如果没有同时满足“知晓内容”、“技术上有可能阻止”、“阻止不超过承受能力”等条件，提供纯粹传输、缓存、数据存储服务等所谓中间服务提供者不对用户提供的非法信息承担责任，否则，与其他网络服务提供者一样要承担一般法律规定的移除或者拦阻访问非法信息的管理义务；第三，网络服务提供者收集、存储、传输和使用个人数据，必须符合相关法律或者经用户同意，在法律规定的情况下，可以向政府部门、执法机关提供用户个人数据。

（2）在一定程度上体现了适当性和利益平衡原则。网络服务提供者履行法定的管理义务受技术、成本等因素限制，欧美前述立法体现了适当性原则，如对提供执法协助的公共电信服务提供者规定了补偿或支付费用，对所谓中间服务提供者规定免责条件，对数据留存的范围和使用条件进行限制。信息网络安全管理义务是国家管理权的延伸，过度扩展必然侵犯公众的网络表达和言论自由等权利，前述立法体现了维护法秩序和保障公民权利的平衡，如将网络服务提供者协

[①]See 121 U.S.C. §2702 (a), (b), (c).

[②]See 121 U.S.C. §2703.

[③]See 121 U.S.C. §2704.

助收集通信内容数据限定在严重犯罪的范围内，限制网络服务提供者收集、使用用户数据等。

（3）规定了义务冲突解决机制。网络服务提供者履行协助执法与保护用户数据两种义务时可能发生冲突，政府部门和执法机关要求网络服务提供者披露用户数据，会导致后者违反与用户之间的保密约定，如果不规定义务冲突解决机制，将会使网络服务提供者处于两难境地。前述欧美立法规定，网络服务提供者应当根据有权机关的要求提供、披露用户个人数据，免除其违反服务协议的法律责任，避免了义务冲突。

（二）我国网络服务提供者的协助管理义务及国内外相关立法比较

我国互联网的发展与电信业有着紧密的关系，公众使用的互联网接入服务是从起初的拨号上网发展到当前的光纤上网和无线网络服务，主要由中国电信、中国移动和中国联通等电信企业提供，公共电信服务提供者和互联网服务提供者被合称为网络服务提供者。[①]目前我国关于网络服务提供者的协助管理义务的立法具有以下特点：

第一，网络服务提供者协助管理义务立法的多层级化。相关法律法规规章有《刑法》、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》、《反恐怖主义法》、《网络安全法》等法律以及大量的行政法规和部门规章。

第二，法律和行政法规对网络服务提供者简单类型化，[②]部门规章进行了更细致的类型化。[③]以上法律法规规章将网络服务提供者分为中间服务提供者（包括网络接入、服务器托管、网络存储、虚拟空间租用、通信传输等纯粹的网络技术服务提供者）、互联网信息服务提供者、网络交易服务提供者（包括为网络商

[①]我国《网络安全法》第 76 条规定，“网络运营者，是指网络的所有者、管理者和网络服务提供者。”第 24 条规定，“网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。”这里办理固定电话、移动电话等入网手续的只可能是公共电信服务提供商，故我国法律中的网络服务提供者包括公共电信服务提供者和互联网服务提供者。

[②]《反恐怖主义法》区分电信业务经营者和互联网服务提供者，《刑法》、《网络安全法》和《关于加强网络信息保护的决定》将二者统称网络服务提供者或者网络运营者，除了《刑法》第 287 条之二规定了“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”的犯罪主体，其他法律未对网络服务提供者进行分类，而规定网络服务提供者的协助管理义务的行政法规仅有国务院《互联网信息服务管理办法》，规定了互联网信息服务提供者和互联网接入服务提供者。

[③]《互联网直播服务管理规定》、《即时通信工具公众信息服务发展管理暂行规定》、《互联网用户账号名称管理规定》、《互联网信息搜索服务管理规定》、《移动互联网应用程序信息服务管理规定》、《网络出版服务管理规定》、《通信短信息服务管理规定》、《规范互联网信息服务市场秩序若干规定》、《电信和互联网用户个人信息保护规定》、《网络交易管理办法》等部门规章将网络服务提供者分为互联网直播服务、即时通信服务工具公众信息服务、信息搜索服务、移动互联网应用程序信息服务、网络出版服务、短信息服务、第三方交易平台服务提供者。

品交易、网络金融服务等市场交易活动提供第三方交易平台的服务提供者）。

第三，各类网络服务提供者的协助管理义务差别小。现行立法对各类网络服务提供者规定的协助管理义务见图中的 A-G 项义务。《刑法》只概括提出信息网络安全管理义务，但未明确其内容，而《网络安全法》、《反恐怖主义法》、《加强网络信息保护的决定》三部法律交叉规定了各类网络服务提供者承担图中的 A、C、D、E、F、G 项义务，国务院《互联网信息服务管理办法》规定了互联网信息服务和接入服务提供者提供者承担 B 项义务，各类网络服务提供者承担几乎完全相同的协助管理义务。其中，互联网信息服务提供者和互联网接入服务提供者承担的协助管理义务最宽，而第三方交易平台服务提供者只承担与中间服务提供者相同的义务。

协助管理义务的种类 / 网络服务提供者的种类		A. 技术支持与协助[①]	B. 数据留存[②]	C. 保护个人信息[③]	D. 管理发现的违法信息[④]	E. 主动审查含有恐怖主义、极端主义内容信息[⑤]	F. 真实身份验证[⑥]	G. 对不提供实名认证者拒绝服务[⑦]
1. 中间服务提供者		有	有[⑧]	有	有	有	有	有
2. 互联网信息服务提供者[⑨]	2.1 互联网直播服务提供者	有	有	有	有	有	有	有
	2.2 即时通信服务工具公众信息服务提供者	有	有	有	有	有	有	有
	2.3 互联网信息搜索服务提供者	有	有	有	有	有	有	有
	2.4 移动互联网应用程序信息服务	有	有	有	有	有	有	有
	2.5 网络出版服务提供者	有	有	有	有	有[⑩]	有	有
	2.6 短信息服务提供者	有	有	有	有	有	有	有
	2.7 其他互联网公共信息服务提供者	有	有	有	有	有	有	有
3. 第三方交易平台服务提供者		有	有[⑪]	有	有	有	有	有

我国网络服务提供者承担以上立法规定的多种信息网络安全管理义务，而非“只具备中立义务”，[⑫]“不再是纯粹的商业活动经营者。因而，在法律上都兼具

[①]见《网络安全法》第 28 条、《反恐怖主义法》第 18 条。
[②]见《互联网信息服务管理办法》第 14 条、《网络交易管理办法》第 30 条和第 35 条。
[③]见《网络安全法》第 41 条、第 42 条、第 43 条和第 44 条以及《关于加强网络信息保护的决定》第 2 条。
[④]见《网络安全法》第 47 条、《反恐怖主义法》第 19 条、《关于加强网络信息保护的决定》第 5 条。
[⑤]见《反恐怖主义法》第 19 条。
[⑥]见《网络安全法》第 24 条、《反恐怖主义法》第 21 条、《关于加强网络信息保护的决定》第 6 条和《网络交易管理办法》第 35 条。
[⑦]见《网络安全法》第 24 条、《反恐怖主义法》第 21 条。
[⑧]见国家工商行政管理局颁布的《网络交易管理办法》第 35 条。
[⑨]见《互联网信息服务管理办法》第 13 条、第 14 条、第 15 条。
[⑩]见《网络出版服务管理规定》第 23 条。
[⑪]见《网络交易管理办法》第 30 条。
[⑫]刘艳红：《网络时代言论自由的刑法边界》，载《中国社会科学》2016 年第 10 期。

网络服务提供者与网络安全管理者双重主体形象。”[①]从社会地位和作用上分析，网络服务提供者是网络社会生态环境的主要创建者、网络活动规则的主要制定者，有责任向社会平衡提供便捷和安全产品，当前“重便捷、轻安全、缺信用”的网络服务状况是网络违法犯罪状况严峻的基础环境和重要条件。在网络社会环境下，只有网络服务提供者才能在及时、直接管控网络违法犯罪活动，如果不要求其承担必要的安全管理义务，其社会作用实际上偏向于网络违法犯罪，因此，在法理上网络服务提供者也不应当“中立”。

比较国内外相关立法，二者规定的协助管理义务内容基本相同，都包括协助执法、数据留存、保护用户信息、管控违法信息和违法活动，但是，差别也比较明显，主要表现在以下方面：

1. 不同网络服务提供者的管理义务的类型化、区别化差异大。前述欧美立法根据网络服务提供者的业务活动类型和义务承受能力，规定了类型化、区别化的协助管理义务，中间服务提供者的义务要明显轻于互联网信息服务提供者。我国对网络服务提供者的类型化立法不充分，仅前述行政法规和部门规章对网络服务提供者进行了分类，[②]其管理义务几乎没有区别。

2. 管理义务立法的适当性差别大。法治国原则不仅要有法可依，立法内容还应适当，[③]前述欧美立法在一定程度上体现了适当和利益平衡原则，而我国相关立法存在义务设置不当等问题：（1）各类网络服务提供者的管理义务基本无差别，特别是要求提供互联网接入、信息存储和缓存等中间服务的提供者承担前述 D、E 项义务，不符合该类服务提供者的业务活动性质和承受能力，也必然阻碍我国社会的信息化；（2）对第三方交易平台服务提供者的义务加载不足。在网络交易活动中，网络违法犯罪人能直接侵害公众的人身、财产权益，相比于中间服务和互联网信息服务，第三方交易平台活动服务提供者如淘宝网等电商网，掌握巨量的用户信息，控制交易的能力更强，本应承担更高程度的管理义务，而当前立法仅由部门规章规定其留存用户信息和交易信息，且法律规范的层级低、效力弱，难以保障相关法律责任的落实；（3）保护用户信息的义务设置不完善。网络服务提供者可以依法向国家相关部门和调查机关披露用户信息，欠缺披露的实体和程序方面的规定；（4）数据留存义务设置不适当。用户数据留存义务不仅会严重影响网络服务提供者的经营活动，也会被用于侵犯公众的合法权利，我国相关立法对该项义务设置得过于宽泛；（5）义务设置没有体现利益平衡原则。我国立法不仅没有规定网络服务提供者协助管理的补偿或者支付费用，反而将其协助义务范围设置得过于宽泛，对用户权利的保障也不充分。

[①]梁根林：《传统犯罪网络化：归责障碍、刑法应对与教义限缩》，载《法学》2017 年第 2 期。
[②]有学者批评我国关于网络服务提供者的立法存在“类型化缺失”，这不符合立法的实际情况。参见王华伟：《网络服务提供者的刑事责任比较研究》，载《环球法律评论》2016 年第 4 期。
[③]王利明：《法治：良法与善治》，载《中国人民大学学报》2015 年第 2 期。

信息网络安全管理义务是网络服务提供者承担法律责任包括刑事责任的基本前提，我国相关立法在网络服务提供者的类型化、义务的区别化和适当化等方面存在不足，加重了网络服务提供者的法律责任，还使部分网络服务提供者承担刑事责任的范围泛化。我国应当借鉴国外相关立法，适度设立信息网络安全管理义务，推进前述类型化、区别化和适当化立法。同时，也要注意的是，当前我国网络交易平台服务提供者的管理义务严重不足，网络经济活动因缺失网络交易平台服务提供者的安全管理，是当前互联网经济、金融领域的诈骗犯罪泛滥的重要原因之一，未来应对网络交易平台服务提供者加载与其社会地位和能力相适应的网络安全管理义务。

三、网络服务提供者的刑事责任

前述欧美立法规定网络服务提供者承担的法律责任分为三类：（1）对自己提供的内容信息，网络服务提供者应当承担一般法律规定的责任。前述欧盟和德国立法规定，网络服务提供者的身份或业务活动性质不是豁免法律责任的依据，如果其实施了法律规定的违法犯罪行为的，应当承担法律责任包括刑事责任。这类刑事责任与网络服务提供者的管理义务无关，因网络服务提供者自身违反了法律的禁止性规定而负担；（2）对于他人提供的内容信息，前述欧美立法规定网络服务提供者应承担内容信息监督义务，同时设定了排除法律责任的条件，只有同时满足法律规定的“知情”、“技术上有可能阻止、阻止不超过其承受能力”等条件的，网络服务提供者才承担一般的法律规定的责任包括刑事责任。网络服务提供者承担这类刑事责任并非因为构成违反相关网络管理义务的犯罪，而是因为符合传统犯罪立法的规定；[①]（3）违反协助执法、用户个人数据保护相关管理义务的，网络服务提供者要承担相关立法规定的法律责任，主要是民事责任和行政责任，如美国法典第 2252 条、第 2258A 条规定违反协助执法或报告违法内容信息义务的法律责任是民事罚金，也有国家如英国《调查权管理法案》第 11 条第（7）款对违反协助执法义务的行为规定了监禁、罚金等刑事处罚。

与国外立法相似，根据网络服务提供者的行为过程中是否涉及他人的违法活动，我国刑法规定网络服务提供者承担刑事责任的情况分为三种，第一种是构成作为形式的单独犯、第二种是构成帮助性质的犯罪，第三种是构成违反信息网络安全管理义务的不作为犯。与国外立法不同之处有两点：第一，网络服务提供者违反用户个人信息保护、协助执法等信息网络安全管理义务的，不仅要承担行政法律责任，还可能构成拒不履行信息网络安全管理义务罪而承担刑事责任；第二，针对他人提供的违法信息或实施的违法活动，网络服务提供者在知晓违法信息或

[①] 美国司法判例显示，网络服务提供者可能因为知晓他人上传的儿童色情、诈骗等内容，被认为触犯共同犯罪条款、美国法典第 18 章第 1952 条、第 2252 条、第 2257 条、第 1961~1968 条等而受到刑事处罚。参见[美]Lawrence G.Walters,《美国网络服务提供者的刑事责任——基于网上色情信息的视角》，《刑法论丛》2015 年第 4 卷（总第 44 卷），杨新绿、涂龙科译，第 468-484 页。

违法行为的内容时，既可能构成传统犯罪的共同犯罪，也可能构成帮助信息网络犯罪活动罪，还可能因拒不履行阻断违法信息传播的管理义务而构成拒不履行信息网络安全管理义务罪。以上应负刑事责任的行为表现出与网络服务相同的技术特性，且与正常业务活动紧密联系，新近刑法立法追究后两种情形中网络服务提供者的刑事责任，被批评在网络服务领域刑法过度扩张。[①]因此，有必要研究和合理划定网络服务提供者承担刑事责任的边界。

（一）作为犯形式的单独犯

随着社会网络化发展，不仅出现了新型网络犯罪，传统犯罪也向网络化发展，这两类行为都可以由网络服务提供者实施。网络服务提供者单独构成作为犯，类似于前述德国立法规定的对自己提供的信息“承担一般法律规定的责任”的情形，如互联网信息服务提供者故意传播自己制作、编辑整理的恐怖主义内容信息的可能构成宣扬、煽动恐怖主义罪。

网络服务提供者自己制作并传播违法内容信息，当然构成相应的传播违法内容信息的犯罪，对于他人制作的违法内容信息，网络服务提供者在知晓内容的情况下故意进行了编辑、整理等改变并通过自己的网络服务器传播的，也应构成犯罪。“快播案”中快播公司并非只是为用户分享视频信息提供传输通道或者不对信息进行加工的交流空间，而是对视频信息进行了基于自身经营利益考虑的筛选、促进快速传播，对违法视频信息进行了分散传输和整合方式的编辑处理，应视为传播自己提供的违法内容信息，因此，“快播案”判决对其行为按照传播淫秽物品牟利罪认定是有事实和法律依据的。根据前文对前述国外立法的分析，该案如果发生在境外，也不会被免于承担法律责任。张明楷教授认为，“快播公司拉拽淫秽视频文件存储在缓存服务器里，并且向用户提供缓存服务器里的淫秽视频文件的行为，则不是中立的帮助行为，而是传播淫秽物品的正犯行为”，该观点将缓存服务一概视为正犯的传播行为是不妥当的，会严重扩大互联网信息服务提供者的刑事责任范围，进而阻碍互联网应用和网络社会的发展，前述国外立法将未同时满足前文提及的三个条件的缓存服务免除法律责任的模式，值得我国借鉴。除了构成传播内容信息相关犯罪外，网络通信接入、主机托管、数据存储服务提供者非法获取用户的通信内容的可能构成侵犯通信自由罪或侵犯公民个人信息罪，非法获取、非法提供用户的个人信息的可能构成侵犯个人信息罪等。

在第一种情形下网络服务提供者承担刑事责任，与其信息网络安全管理义务无关，学者们对其适当性不存异议。而且，由于网络服务提供者具有技术、业务活动优势，侵犯的对象更广泛，危害更严重，隐蔽性更强，在一定情况下有必要从重处罚，[②]不少学者也支持比传统形式的犯罪处罚更重。[③]

[①]参见刘宪权：《论信息网络技术滥用行为的刑事责任——<刑法修正案（九）相关条款的理解和适用>》，载《政法论坛》2015年第6期。陈洪兵：《中立行为的帮助》，法律出版社2010年版，第233页。
[②]最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》

（二）具有帮助性质的犯罪

网络服务提供者明知他人利用信息网络实施犯罪而为其提供帮助的，我国按照两种方式追究刑事责任：第一种是按帮助犯处理。由于网络服务提供者的帮助犯罪行为与其业务活动相关，容易与其正常业务活动相混淆，其主观心态成为犯罪成立的关键要件。根据我国刑法通说，帮助犯与实行犯之间必须存在共同犯罪故意，可以为共谋的故意或片面帮助的故意；[①]第二种是按新设立的帮助利用信息网络犯罪活动罪独立定罪处罚。学者们对该罪的设立和适用争议较大。在国内外立法中，网络服务提供者构成具有帮助性质的犯罪都不以其信息网络安全管理义务为犯罪成立的前提条件，司法实务也不将其违反信息网络安全管理义务作为影响刑事责任程度的因素。

按帮助利用信息网络犯罪活动罪追究网络服务提供者的刑事责任，需要符合刑法第287条之二规定的构成条件。该罪的危害行为应当为具有计算机、网络技术服务性质的技术支持和帮助，否则，无法对利用信息网络实施的犯罪起到帮助作用，或者因其与普通的帮助犯罪没有区别，不需要予以独立犯罪化。该罪行为还受法条所列举行为方式的特性的限制，该罪法条采用了兼有列举式和概括式的行为描述方式，列举的“提供互联网接入、服务器托管、网络存储、通讯传输”涵盖前文分析的中间网络服务行为，利用互联网“提供广告推广、支付结算”涵盖前文分析的第三方交易服务平台服务行为，因此，网络服务提供者可以构成该罪。

1. 帮助信息网络犯罪活动罪不是帮助犯的量刑规则

有学者认为，“我国《刑法》第287条之二所规定的帮助信息网络犯罪活动罪，并不是帮助犯的正犯化，只是帮助犯的量刑规则”，[②]否认其独立犯罪化的价值，同时，意味着构成该罪必须符合共同犯罪的构成条件，客观上限制了该罪的适用。当网络服务提供者仅为某一个具体的下游犯罪提供帮助时，的确可以按照传统的帮助犯定罪处罚,但是，追究其刑事责任要依附于实行犯的查证和追究责任，在网络犯罪产业链态势下，“被帮助的正犯作为犯罪行为的直接实行行为人，不仅服务器可能设置在境外，而且其人可能也躲避在境外。对网络共同犯罪进行刑事归责时，经常面临提供网络服务的帮助犯被追诉而正犯却逍遥法外的困境”，[③]同时，收集、审查、认定网络犯罪案件中的电子数据仍然是追诉网络犯罪案件的重大司法实务难题，案件办结的困难大，实际上可能最终无法追究其刑事责任，而且，按其他犯罪处理也往往缺乏事实和法律依据。事实上网络服务

第2条规定，对利用网络技术手段实施电信网络诈骗的，酌情从重处罚。
[②] 例如，张明楷教授认为“网络诽谤的特点， 决定了其本身就是值得处罚的情节严重的行为。”诽谤犯罪网络化应比传统诽谤犯罪危害更大，处罚应更重。参见张明楷：《网络诽谤的争议问题探究》，《中国法学》2015年第3期。
[①]参见高铭暄、马克昌主编，赵秉志执行主编：《刑法学》，北京大学出版社、高等教育出版社2013年版第165-166页。
[②]张明楷：《论帮助利用信息网络犯罪活动罪》，载《政治与法律》2016年第2期。
[③]梁根林：《传统犯罪网络化：归责障碍、刑法应对与教义限缩》，载《法学》2017年第2期。

提供者从来就不是为了某一个或者少数人而是服务于公众，将其按照帮助犯定罪处罚没有反映网络服务的产业链行为特征，不能做到罚当其罪和有效遏制犯罪。因此，笔者不同意这种观点，这种观点是以传统物态社会的视角观察网络社会，共同犯罪理论建立在“一人对一人”或者“一人对少数人”传统社会活动基础上，不适分析“一人服务于人人、人人服务于一人”网络社会活动。该罪行为不同于传统的帮助犯，其技术支持和帮助行为具有明显的犯罪产业链行为特征，是整个网络犯罪链的重要环节，它并非为帮助某一个具体下游犯罪而单独存在，而是为了谋求自身独立的经济利益为众多下游网络犯罪提供服务。它具有不同于帮助犯的独立性，“网络空间中某些犯罪的帮助行为的社会危害性已经远远超过了实行行为的危害性”，[①]这种比实行行为更严重的社会危害性不可能为从属性行为所具有，而只能是因其自身所具有的独立犯罪性质。

将该罪行为按照方式行为独立犯罪化，[②]给予兜底性刑罚处罚，可以与按照帮助犯模式处理相互补充，例如，该罪行为人明知相互独立的多人实施网络犯罪而给与技术支持与帮助，按照帮助犯处理可能都不能成立犯罪，但是，其帮助多人的行为可以被评价为“情节严重”，可以按照该罪处理；当按照帮助犯处罚更重时，如构成贩卖毒品罪的帮助犯，仍然应按照贩卖毒品罪定罪处罚。至于该罪是否过度扩展刑法的边界，笔者认为，构成该罪不仅要求行为人明知他人犯罪，还必须满足“情节严重”的要件，在规范层面避免了过度犯罪化。该罪立法具有必要性和合理性，有利于全面、全程遏制网络犯罪，是我国刑法顺应网络社会发展的适应性调整，而不是所谓的积极主义的刑法立法。[③]

2. 帮助信息网络犯罪活动罪不是帮助犯的正犯化

还有学者认为，该罪立法是帮助犯的正犯化，“完全可以脱离正犯去评价共犯行为，共犯行为的独立属性为这种刑法评价预留了足够的理论空间，对共犯正犯化的立法规定在共同犯罪理论体系中不存在障碍。”[④]笔者也不同意这种观点，理由是：（1）我国刑法学通说认为，仅教唆犯具有从属性和独立性的双重属性，认为帮助犯也具有独立性缺乏法律依据和刑法理论支撑；（2）帮助犯的正犯化的基础是行为在性质上仍然属于帮助犯，只是因为存在新的犯罪立法，其定罪脱离原来的正犯，但是，这种立法“弱化了正犯责任应有的独立性，也造成了正犯责任和片面共犯责任的适用冲突，一旦通过总则性司法解释将片面共犯全面引入后，帮助利用信息网络犯罪活动罪就会被空置。”[⑤]可见，对该罪作帮助犯正犯化的解读面临立法与帮助犯理论相互排斥的问题；（3）受限于刑事责任的从属性。

[①]于志刚：《论共同犯罪的网络异化》，载《人民论坛》2010年第29期。
[②] 我国刑法第285条、第286条规定的犯罪行为都是按照犯罪手段行为设立的犯罪，与按照侵犯的犯罪客体设立的犯罪形成了相互补充的关系。
[③]参见周光权：《积极刑法立法观在中国的确立》，载《法学研究》2016年第4期。
[④]陆旭：《网络服务提供者的刑事责任及展开——兼评<刑法修正案（九）>的相关规定》，载《法治研究》2015年第6期。
[⑤]于志刚：《网络空间中犯罪帮助行为的制裁体系与完善思路》，载《中国法学》2016年第2期。

如果该罪在性质上仍然定位为帮助犯，则其刑事责任必然要从属于正犯，或者依附于正犯的刑罚，或者只能规定较轻的刑事责任。有学者提出“必要帮助犯的主犯化”、[①]“帮助行为可以在共同犯罪中起主要作用”等观点，[②]试图解决帮助犯的刑罚从属性和较轻的问题，不仅难以获得共同犯罪理论上的广泛认同，反而说明了下游犯罪对这类帮助性质的犯罪的依赖性，后者在犯罪链活动中起主要作用，是核心的犯罪行为，需要独立成罪和进行刑事责任的独立评价。

从罪刑单位的结构看，该罪设置了独立的法定刑，不可能是下游犯罪的帮助犯的量刑规则，但是，该罪法定刑较轻似乎意味着立法者将其定性为从属性的犯罪。对其他犯罪能起到帮助性质的作用，不等于就是帮助犯，也不应被评价为帮助犯的正犯化——仅承认犯罪的独立性而对其比照实行犯规定轻得多的法定刑，实际上我国刑法中具有帮助性质的犯罪较多，如洗钱罪、运输毒品罪等，这些犯罪的行为人都明知下游犯罪的犯罪性质，由于其自身在犯罪产业链条中的独立性，并被立法评价为具有严重危害性，被设定为独立的犯罪并规定了多层次的法定刑，且法定刑并非一律相对较轻。因此，符合帮助犯特征的犯罪并非都是帮助犯的正犯化，还要看该犯罪在犯罪生态中是否具有独立的地位。帮助利用信息网络犯罪活动罪与洗钱罪、运输毒品罪的特性相同，刑法将其设立为独立的犯罪是合理的，该罪与刑法第285条规定的“提供侵入、非法控制计算机信息系统的程序、工具罪”相似。为了使相关犯罪的罪刑均衡，应破除其帮助犯性质的认识，其法定刑设置上应当增设“具有特别严重情节的，处三年以上七年以下有期徒刑，并处罚金。”其罪名解释为“为他人利用信息网络实施犯罪提供技术支持和帮助罪”更为恰当。

（三）违反信息网络安全管理义务的不作为犯

前文分析到，国外立法如英国仅将拒不履行协助执法义务的行为入罪，我国法律和行政法规规定了较为宽泛的协助管理网络的义务，并在刑法中规定了拒不履行信息网络安全管理义务罪，该罪是法定犯、不作为犯和情节犯，其立法的适当性及其司法适用值得研究。

1.对立法适当性的思考

网络社会的良好治理不能缺少网络服务提供者协助管理，这只证明了网络服务提供者协助管理的必要性，而不是将拒不履行协助管理义务行为犯罪化的合理依据。我国刑法学通说认为，犯罪具有相当程度的社会危害性、刑法违法性和应受刑罚处罚性，[③]不具备其中任何一个特性，犯罪立法就缺乏必要性和合理性。

首先，该罪行为是否具有严重的社会危害性存疑。该罪被设定为情节犯，情

[①]参见李民、高凤立：《必要帮助犯之主犯化——以网络涉枪犯罪中提供“交易平台”和“技术信息”为例》，载《大连海事大学学报(社会科学版)》2015年第6期。
[②]参见谢彤：《帮助行为可以在共同犯罪中起主要作用》，载《华东政法学院学报》2002年第1期。
[③]参见高铭暄主编：《刑法专论（上）》，高等教育出版社2006年版，第124页。

节要件标准的模糊性降低了入罪门槛，部分不具有严重社会危害性的行为可能按该罪处罚，理由是：（1）难以区分行政违法行为和犯罪行为。《网络安全法》、《反恐怖主义法》和《互联网信息服务管理办法》都将“情节严重”规定为对网络服务提供者适用较重行政处罚的条件，其内容可以涵盖刑法第 286 条之一列举的 4 项情节。无论未来对拒不履行信息网络安全管理义务罪的“情节严重”作何种司法解释，其作为酌定情节的性质不会改变，致使司法实践中难以区分行政法意义上的“情节严重”与刑法意义上的“情节严重”，该罪与行政违法行为的边界不清晰。（2）该罪是法定犯和不作为犯，严重后果应当是构成条件。该罪的后果并非正常的网络服务引起，只是因为网络服务提供者的保证人地位，[①]被要求“对于危险源的监督，产生了保护他人法益不受来自于自己控制领域的危险威胁的义务。这种对于危险源的控制是不作为犯的义务。这种保证人义务的根据在于，复杂社会系统中的秩序必须依赖于（处分权人所管理的）特定空间和特定控制领域的安全。”[②]网络服务提供者违反信息网络安全管理义务，只有在应当履行、有能力且不超过合理的承受能力范围，而未防止他人违法行为或者系统危险导致严重后果，才具备了刑事追责的可能性和必要性。该罪可以类比于刑法第 139 条规定了消防责任事故罪，行为人违反消防管理法规且拒绝执行改正措施，造成严重后果的，才承担刑事责任，相比之下，拒不履行信息网络安全管理义务罪不是危害公共安全罪，犯罪性质不如消防责任事故罪严重，如果没有发生严重后果，仅具有“严重情节”，不足证明该罪行为具有严重的社会危害性及追究刑事责任的必要。（3）危害后果界定不明确。该罪法条规定的“违法信息大量传播”和“刑事案件证据灭失，情节严重”的界线不清晰，违法信息大量传播的标准难以合理划定，轻罪刑事案件的证据灭失不应被评价为情节严重和具有严重的社会危害。

其次，该罪行为是否应受刑罚处罚存疑。刑法是其他部门法的保障法，刑罚是一把“双刃剑”，只有其他法律手段不能有效规制时，才能发动刑罚，刑法立法和适用都应遵循谦抑原则。[③]该罪规定的信息网络安全管理义务由《网络安全法》、《反恐怖主义法》、《加强网络信息保护的决定》以及国务院《互联网信息服务管理办法》设定，并规定了相应的行政法律责任，[④]网络服务提供者拒不履行该义务的，最重可能被处以关闭网站、吊销经营许可证或者营业执照等处罚。如果其受到以上重处，要么已经丧失提供网络服务的能力而不可能实施该罪，要么其

[①]参见宫厚军：《“保证人说”之演变及其启示》，载《法商研究》2007 年第 1 期。
[②]【德】乌尔里希·齐白：《网络服务提供者的刑法责任—刑法总论中的核心问题》，王华伟译，载赵秉志主编：《刑法论丛》2016 年第 4 卷。
[③]参见张明楷：《论刑法的谦抑性》，载《法商研究》1995 年第 4 期。
[④]《网络安全法》规定的法律责任包括警告、没收违法所得、罚款、责令暂停相关业务、停业整顿、关闭网站、吊销相关义务许可证或营业执照，《反恐怖主义法》规定的法律责任是对直接责任人员的罚款、拘留，《关于加强网络信息保护的决定》规定的法律责任是警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务、记入社会信用档案并予以公布，以及依法给予治安管理处罚。国务院《互联网信息服务管理办法》规定的法律责任是责令改正、吊销经营许可证或责令关闭网站。

身份已经不是网络服务提供者，不应适用该罪。而且，拒不履行信息网络安全管理义务罪是轻罪，对单位犯罪只能处以罚金，法律责任反而比前述行政处罚轻，并没有剥夺其再犯能力。虽然能通过对直接责任人员处以刑罚来遏制犯罪，但是，受行政监管的网络服务提供者都是以单位形式存在，处罚单位比处罚个人效果更好，且能避免短期自由刑的流弊。当然，前述行政法律法规规定的行政处罚适用标准、处罚轻重、处罚措施不统一，行政执法可能遇到困难，解决之道应当是继续完善前述立法，而不是以刑代管。

无论从国内外立法比较还是从该罪的实际效果分析，该罪立法滥用刑法的威慑惩罚功能，欠缺立法的必要性和适当性，不能替代良好的行政监管，对我国信息社会的发展弊大于利。笔者认为，该罪不应设立，未来至少应提高该罪的入罪门槛，将其修改为结果犯。

2.司法适用的限制

基于前文分析，拒不履行信息网络安全管理义务罪存在过度犯罪化的缺陷，在立法没有修改前，对该罪的构成要件应当进行缩限解释，避免对网络服务提供者不当施刑。

（1）违反信息网络安全管理义务的认定

该罪是不作为犯，违反信息网络安全管理义务是成立该罪的前提，认定义务的范围应注意以下两点：第一，该义务的来源是国家法律和行政法规，当前仅有《网络安全法》、《反恐怖主义法》、《关于加强网络信息保护的决定》、《互联网信息服务管理办法》，其他部门规章和地方性法规不能成为义务的来源；[①]第二，义务的内容受限于刑法规定的范围。根据以上法律和行政法规，该罪的信息网络安全管理义务是网络用户身份的实名认证和服务限制、协助执法、关键信息基础设施中的个人信息和重要数据的境内留存、保护个人信息、监管所发现的违法信息以及针对恐怖主义、极端主义内容信息的监督义务，但是，违反前述 6 项义务，并非都要承担刑事责任，根据刑法第 286 条之一的规定，还必须能够造成“违法信息传播”、“用户信息泄露”、“刑事案件证据灭失”，并有其他严重情节。

其中，违反对网络用户身份实名验证和服务限制义务与发生上述 3 种结果之间的因果链条更长，本身不具有引起的性质，不可能引起严重后果，没有制造出法所不允许的风险，[②]违反该义务不应是该罪的危害行为，只可能是行政违法行为。此外，对于网络服务提供者未能完全履行恐怖主义、极端主义内容信息的监督义务，以致于该类信息大量传播的，也不应当追究刑事责任。《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、极端主义内容信息进行内

[①]有学者认为，只要是法律明文规定的义务都可以成为网络服务提供者不作为犯罪的义务来源，这种观点会进一步导致网络服务提供者刑事责任的扩大化。参见秦天宁、张铭训：《网络服务提供者不作为犯罪要素解构———基于“技术措施”的考察》，载《中国刑事法杂志》2009 年第 9 期。
[②]参见陈兴良：《从归因到归责：客观归责理论研究》，载《法学研究》2006 年第 2 期。

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，如果其已经尽到必要的努力，即使出现前述内容信息大量传播的，也不应追究其刑事责任。

（2）拒不履行义务的认定

本罪是特殊的不作为犯，除了满足不作为犯的基本特征，还必须被监管部门责令采取改正措施，因此，认定拒不履行义务时，应注意以下几点：

第一，监管部门责令其采取改正措施的认定。《网络安全法》第 8 条规定，互联网信息部门负责统筹协调网络安全工作和相关监督管理工作，电信主管部门、公安部门和其他有关机关依照相关法律和行政法规，在职责范围内负责网络安全的监督管理工作。其他部门如工商行政部门、广播电影电视部门依据部门规章责令网络服务提供者采取改正措施，不应被认为是符合该罪规定的监管部门。有权监管部门提出的改正措施应指向相对具体的违法行为和违法内容信息，而不能是一般性的责令履行信息网络安全管理义务。

第二，网络服务提供者履行义务能力的认定。该罪是不作为犯，成立该罪，网络服务提供者必须具有能力履行前述义务、执行监管部门责令的改正措施。网络服务提供者的管理能力不同于服务能力，其受限于互联网技术及其整体构架、信息系统的软硬件设备设施、网络服务平台管理的技术和条件、网络服务的经营成本等多方面。以网络信息服务提供者为例，面对海量的图片、音视频形式的色情、暴恐等违法信息，网络信息服务提供者目前只有特征信息的计算机自动搜索和人工审查两种措施，无法实时、无遗漏地发现全部违法信息，如果违法内容信息被使用了隐藏技术、非通用语言和密码技术等，则更难以做到有效发现和监管。因此，对网络服务提供者履行义务能力的认定，笔者认为，可以参考前述德国立法的规定，必须同时满足“在技术上有可能阻止”、“进行阻止不超过其承受能力”的条件，并采取兼顾业界一般能力水平和个体能力的判断标准，即，以当时多数网络服务单位履行义务能力的一般水平为基础，具体考察特定单位实际履行义务的可能性和承受能力。[①]如果改正措施超出了当时的一般能力水平，或者要求投入的管理成本太高，以致于严重影响被监管人的正常经营，不能认为其具有履行义务的能力。

第三，故意不执行改正措施的认定。该罪的“核心是拒不改正”，[②]主观上具有拒不履行协助管理义务、对抗法律的心态，客观上其拒不改正、未阻止法定后果的发生，分为两种情形，一种是完全不执行，另一种是表面应付、实际上不执行，前者容易判断，而后者则容易与执行不能、执行迟缓、执行困难等相混淆。笔者认为，应当综合考虑监管部门责令的改正措施的内容和网络服务提供者执行

[①]参见钱叶六：《不作为犯的实行行为及其着手之认定》，载《法学评论》2009 年第 1 期。
[②]赵秉志、刘志伟、袁彬：《关于<中华人民共和国刑法修正案（九）>新增及修改罪名的意见》，载《法学杂志》2015 年第 10 期。

改正措施的实际状况，如果内容比较明确、具体，执行难度不大，处于行为人有能力执行的范围内的，行为人不投入必要的人力物力、故意拖延和应付的，应当认定为拒不执行改正措施；如果是超出了行为人的管理能力，或者是改正工作量巨大导致过程长，或者其能力不足以完全改正，即使发生法定的后果，也不应认定为故意不执行改正措施。[①]

（3）严重情节

刑法第 286 条之一规定了 4 项“严重情节”，对违反用户信息保护义务的按照结果犯认定，对违反其他义务的按照情节犯认定。前文分析到，“严重情节”的界限模糊，对该要件“粗犷”适用不仅会使网络服务提供者承担个案的刑事责任，还会对大量网络服务提供者的日常经营以现实的刑事责任风险压力，迫使其强化对网络信息的筛查监控，危及公众的网络表达和言论自由权利。笔者认为，在该构成要件没有修改之前，对其的认定应当符合宪法原则，兼顾打击犯罪与保护人权。[②]由于该条对违反用户信息保护义务要求造成严重后果，对该罪的其他“严重情节”也应按“造成严重后果”来解释。可以考虑对“刑事案件证据灭失”解释为导致应判处三年以上的重罪的构成要件事实证据灭失，对“致使违法信息大量传播”规定高于故意传播违法信息的犯罪的数量标准，且违法信息的大量传播应与严重危害社会的事件有因果关系。由于违法信息的种类繁多，我国刑法没有对所有违法信息规定故意传播类犯罪，无法都采取参照的方法，法官在裁量时应当对比处最重的行政处罚的数量标准，避免轻易入刑。

结　论

网络服务提供者在网络社会中处于枢纽地位，网络社会的治理需要网络服务提供者协助管理，对网络服务提供者设立协助管理义务是各国立法的趋势，无论在法理还是立法上，网络服务提供者都不是具有“中立的义务”。国内外立法要求网络服务提供者承担的义务基本相同，主要是协助执法义务（协助通信监视和数据留存与提供）、内容信息监管、用户数据保护，我国相关立法在协助管理义务的类型化、区别化方面与国外立法差距较大。

国外立法较少专门对网络服务提供者规定犯罪立法。网络服务提供者对自己提供的内容信息，应当承担一般法律规定的责任；对他人提供的内容信息，在满足“知情”、“技术上有可能阻止”和“阻止不超过其承受能力”三项条件时，网络服务提供者有义务阻止，如果不阻止，将承担一般的法律规定的责任，包括刑事责任；网络服务提供者违反法律规定的管理义务，承担的法律责任主要是民事责任和行政责任。

[①]参见周光权：《网络服务商的刑事责任范围》，载《中国法律评论》2015 年第 2 期。
[②]参见张翔：《刑法体系的合宪性调控—以“李斯特鸿沟”为视角》，《法学研究》2016 年第 4 期。

我国网络服务提供者可能构成作为犯形式的单独犯、共同犯罪中的帮助犯、帮助他人利用信息网络犯罪活动罪和拒不履行信息网络安全管理义务罪，前二者与国外立法相似，拒不履行信息网络安全管理罪立法的必要性、适当性需要继续研究，当前应当对该罪进行限制性解释适用。

网络直播平台犯罪之治理

谢昊轩　郭泽强[①]

摘　要：网络直播内容的泛娱乐性、直播手段的技术依赖性、直播平台的逐利性等因素，造成直播平台野蛮生长而违法犯罪现象频出的现状。当下，主播可能涉及的犯罪类型主要是涉黄、涉赌、涉暴及侵犯知识产权类犯罪；直播平台则多涉嫌“拒不履行信息网络安全管理义务罪”、“非法利用信息网络罪”、“帮助信息网络犯罪活动罪”等。以犯罪学视角分析发现，网络直播平台犯罪的原因在于：平台和主播的“泛娱乐”标签化、平台布局存在诱罪因素、网络直播缺乏有效监管及网络直播的商业化本质。对此，可以通过弱化直播平台及主播的“泛娱乐”与“犯罪”标签、实现网络直播平台的科学布局、明确网络直播平台的监管地位和监管权力、推动网络直播价值目标高端化和警惕直播平台形成犯罪亚文化等手段进行治理。

一、问题的提出

“网络直播平台是基于互联网尤其是移动互联网技术产生的多向多渠道信息交互平台，其在社会信息交互、网络经济大众化、社会资源整合等方面发挥着重要作用。”[②]近年来，斗鱼、虎牙、火猫等网络直播平台迅速崛起，在丰富广大网民的网络生活的同时，也在一定程度上辐射了游戏、旅游、餐饮等行业，促进了社会的经济发展。据统计，截至 2018 年底，我国网络直播用户规模达 3.97 亿，用户使用率为 47.9%。[③]同时，中娱智库 2018 年发布的《2017 中国网络表演（直播）发展报告》显示，2017 年我国网络表演（直播）市场整体营收规模达到 304.5 亿元，比 2016 年的 218.5 亿元增长 39%。但是，由于网络直播内容的泛娱乐性、直播手段的技术依赖性、直播平台的逐利性等因素，造成目前直播平台野蛮生长而直播乱象频出的现状。例如某平台主播“莉哥”在直播中侮辱国歌

[①] 作者简介：谢昊轩，中南财经政法大学刑事司法学院 2017 级硕士研究生。
郭泽强，中南财经政法大学法治发展与司法改革研究中心教授。
[②] 参见刘雪斌，俎璐：《实现网络直播平台的法治化运营》，载《人民论坛》2018 年第 34 期。
[③] 参见《第 43 次中国互联网络发展状况统计报告》，
http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201902/t20190228_70645.htm

被行拘，主播”雪梨枪“在直播中进行色情表演成立制作、传播淫秽物品牟利罪被判处4年有期徒刑，2018年7月，浙江松阳警方捣毁4个涉黄涉赌直播平台。由此可见，在目前的网络直播中，违法犯罪现象并不少见，而且犯罪主体既有平台主播，也包括平台自身。因此，为规范网络直播行为，净化网络环境，促进我国网络直播平台的健康发展，需要对网络直播平台犯罪进行治理。

治理网络平台犯罪，“更多的是强调对网络违法犯罪行为的治理，因而可分解为两个层面，一是因网络平台而生成的网络犯罪，二是平台自身涉嫌的犯罪问题”[①]。故网络直播平台犯罪治理既要关注平台主播的犯罪行为，也要关注平台自身的犯罪现象。但基于平台与主播在社会生产和法律制度中的角色、属性不同，二者所可能涉及的犯罪类型和致罪原因必然存在一定区别。这就需要在分别分析网络直播平台与主播的犯罪类型和犯罪原因的基础上，实施有针对性的治理策略。

二、网络直播平台涉罪类型梳理

（一）平台主播可能涉罪类型

网络直播平台主播，”特指与直播平台签约，在直播平台专属直播间进行互联网直播活动的主播“[②]。在国家网信办发布的《互联网直播服务管理规定》中，平台主播是互联网直播的发布者，与用户一道作为互联网直播服务使用者。作为互联网直播的发布者，根据其经常发布的直播内容，平台主播主要可以分为游戏主播、真人秀主播和其他主播。游戏主播主要以自己的游戏操作画面为直播内容，并在直播过程中通过分享游戏体会、技巧等与观众进行实时沟通。此类主播以男性居多。真人秀主播则多为女性，他们的直播内容常以唱歌、跳舞、乐器演奏等才艺表演为主。而其他主播有的通过在直播中播放自己制作的视频、音频、图片等原创素材进行直播活动，有的则以非原创的网络资源作为直播内容。由于平台主播的准入门槛较低，并且直播的即时性较强，一些法律意识淡薄的主播就会为追求直播效果而做出逾越道德底线甚至法律红线的行为。结合已经发生的案例与主播的直播内容来看，主播的犯罪类型主要集中在涉黄、涉赌、涉暴及侵犯知识产权类犯罪。

① 姜瀛：《“以网管网”背景下网络平台的刑法境遇》，载《国家检察官学院学报》2017年第5期。
② 余杰：《反不正当竞争法视野下网络主播跳槽问题研究》，载《人民司法》（应用）2018年第10期。

1、涉黄犯罪

对于涉黄类犯罪，主播可能成立的罪名有”制作、复制、贩卖、传播淫秽物品牟利罪“、”传播淫秽物品罪“、“组织播放淫秽音像制品罪”、”组织淫秽表演罪“、”组织卖淫罪“、”协助组织卖淫罪“等。这些涉黄类犯罪多发生在网络直播平台的真人秀板块。易言之，在网络直播中，真人秀主播往往成为涉黄类犯罪的主体。由于目前网络直播的泛娱乐性特征突出，且观众观看网络直播主要出于休闲、释放压力甚至猎奇的心理，网络主播（尤其是女性真人秀主播）往往通过出卖色相来迎合这种心理，以博取关注度和经济利益。在直播过程中，一些女主播时常采用具有性暗示的挑逗性语言和肢体动作来鼓动直播间的观众给其刷“飞机”、“游艇”等礼物，更有甚者直接进行大尺度的色情表演。由于主播能够在其收到的礼物中抽取一定比例的数额，因此多数情况下可以肯定主播具有牟利的目的，成立”制作、复制、贩卖、传播淫秽物品牟利罪“。如果不能查明主播是否具有牟利目的，根据存疑有利于被告人的原则，则不能成立“制作、复制、贩卖、传播淫秽物品牟利罪”。但根据最高法、最高检《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》第3条的规定，当行为人不以牟利为目的，利用互联网等传播淫秽电子信息达到相应数量标准或造成严重后果时，可以成立“传播淫秽物品罪”。此外，一部分主播背后还有类似于经济人公司的主播公会。一个公会通常有若干主播，这些主播由公会对其包装、宣传、安排直播内容等。当公会安排主播进行色情表演时，则该主播公会可能成立”组织淫秽表演罪“。

2、涉赌犯罪

在涉赌犯罪中，“赌博罪”和“开设赌场罪”是两个非常重要的罪名。最高法、最高检《关于办理赌博刑事案件具体应用法律若干问题的解释》（以下简称“解释”）对“聚众赌博”做出了具体规定：在“以营利为目的”且满足“组织三人以上”的前提下，一旦抽头渔利数额、累计赌资数额、累计参赌人数达到相应标准，即可成立“赌博罪”。[①]在网络直播中，有的主播组织观众通过刷礼物

① 《关于办理赌博刑事案件具体应用法律若干问题的解释》： 第一条 以营利为目的，有下列情形之一的，属于刑法第三百零三条规定的“聚众赌博”：
（一）组织3人以上赌博，抽头渔利数额累计达到5000元以上的；
（二）组织3人以上赌博，赌资数额累计达到5万元以上的；
（三）组织3人以上赌博，参赌人数累计达到20人以上的；
（四）组织中华人民共和国公民10人以上赴境外赌博，从中收取回扣、介绍费的。

的方式参与其设置的竞猜活动。例如在斗鱼TV，一些游戏主播设置以游戏输赢为内容的竞猜活动，观众通过刷价值较低“水晶”参与竞猜，一旦猜中则有可能再次通过系统随机抽奖而获得数额较大的平台礼物、实物奖品甚至现金。这种竞猜首先符合赌博“以小博大”的本质属性。虽然观众是通过再抽奖的方式获得奖励，但这种抽奖的随机性本身也是竞猜的随机性，是整个“以小博大”的赌博过程的一部分。其次，虽然参与竞猜的“资金”是不可流通的平台礼物，但这并不影响赌博罪的成立。因为在有些赌场，参赌人员并非以现金赌博，而是通过兑换赌场不可流通的筹码参赌。竞猜中的平台礼物虽是观众购买的虚拟产品，但类似于筹码。此外，由于观众参与竞猜的礼物最终将按一定比例返给主播，作为主播的工资或绩效奖励。因此主播也有抽头渔利的嫌疑。最后，“又因网络空间是不特定人可以随意进入的公共空间，在参赌人数、抽头渔利数额、赌资数额符合上述《解释》时，主播涉嫌构成(聚众型)赌博罪”[①]。

在“开设赌场罪”方面，最高法、最高检《关于办理网络赌博犯罪案件适用法律若干问题的意见》规定，建立赌博网站接受投注或提供给他人赌博的，属于开设赌场。在这里”赌场“被限定为”赌博网站“。但是上述主播在直播间中开设竞猜活动，或者直接组织严格意义上的赌博，是否能成立”开设赌场罪“存疑。原因在于，”以门户网站及其互联网服务为代表的网络运营者虽可称之为网络中的服务平台，但由于其不具备’P2P’、’第三方’及’去中心化’的基本属性，应被列入传统的大型网站范畴，而不应被纳入到平台范畴”[②]。可见，由于直播平台的直播间与网站的区别，能否通过解释将前者纳入网站范畴，是主播成立“开设赌场罪”的关键。

3、涉暴犯罪

《互联网信息服务管理办法》规定，互联网信息服务提供者不得制作、复制、发布、传播暴力、凶杀、恐怖或者教唆犯罪的内容。但是，有的主播为了快速获取关注度和点击量，不惜在直播中对他人使用暴力。如2016年6月，云南省曲靖市陆良县两名男子在某直播平台直播暴打老人，涉案人员涉嫌寻衅滋事罪被刑拘。[③]此外，近年来快手主播“直播打人”、“直播约架”的事件也曾多次发生，

[①] 赵天水，刘欢：《网络直播主体涉罪性质分析》，载《重庆邮电大学学报》（社会科学版）2018年第6期。
[②] 姜瀛：《“以网管网”背景下网络平台的刑法境遇》，载《国家检察官学院学报》2017年第5期。
[③]参见凤凰网：“云南陆良警方：直播打人视频属实，4人被刑拘1人未归案 ”

在社会上造成了严重的不良影响。这些主播在对他人使用暴力时可能成立“寻衅滋事罪”、“聚众斗殴罪”。如果造成他人轻伤以上的结果，根据其主观意图，则可能成立“故意伤害罪”、“过失致人重伤罪”等。甚至一些别有居心的主播可能利用网络直播即时性强、受众范围广的特点，在直播过程中发表恐怖言论、宣扬恐怖主义。这时便涉嫌《刑法》第120条之三规定的“宣扬恐怖主义、极端主义、煽动实施恐怖活动罪”。

4、侵犯知识产权犯罪

前文提到，在其他主播中有一部分主播是通过播放非原创的网络资源进行直播活动的。例如一些主播在直播间提供付费电影点播，观众在给主播刷礼物后便可以向主播提出想观看的电影。如果主播没有电影著作权人的允许并支付报酬，则主播无疑侵犯了电影制片方的著作权。一些真人秀主播在直播中会演唱歌曲。虽然《著作权法》规定“免费表演已经发表的作品，该表演未向公众收取费用，也未向表演者支取报酬”的“可以不经著作权人许可，不向其支付报酬”。但是，当真人秀主播提出有偿点歌服务时，便意味着免费表演成了收费表演。此时应当经歌曲著作权人许可并支付报酬，否则就侵犯了作者的著作权。由于没有制作、复制、发行、出版、出售等行为，故不至于成立“侵犯著作权罪”，但也属违法行为。此外，有些主播会在直播中推销、售卖仿冒的服饰、食品等商品，这时主播的行为则可能构成”销售假冒注册商标的商品罪“。

（二）平台可能涉罪类型

“《网络安全法》、《互联网直播服务管理规定》、《网络表演经营活动管理办法》等法律法规规定，网络直播平台负有网络安全监督管理义务。网络直播平台违反网络安全监督管理义务时，基于共犯责任、不作为责任、正犯责任、重大管理或监督过失责任，可以成立拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助信息网络犯罪活动罪。”[①]

1、拒不履行信息网络安全管理义务罪

《刑法》第268条之一规定：“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，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致

http://news.ifeng.com/a/20160623/49225373_0.shtml?wratingModule=1_9_1
[①] 参见孙道萃：《网络直播刑事风险的制裁逻辑》，载《暨南学报》（哲学社会科学版）2017年第11期。

使违法信息大量传播的;(二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。”当网络直播平台接到监管部门责令改正的通知而拒绝或怠于整改时，平台的行为则违反了《刑法》第 268 条之一背后的禁止性规范。易言之，直播平台在本罪中违反的是刑法规定的“不得拒绝履行信息网络安全管理义务”，而非行政法规规定的“网络安全监督管理义务”。直播平台成立“拒不履行信息网络安全管理义务罪”的关键在于其“不履行”，而非“未履行”。因此，网络直播平台基于不作为责任而成立本罪。

2、非法利用信息网络罪

成立本罪的网络直播平台多是违法违规平台。目前，互联网中存在大量的色情直播平台。这些直播平台通过提供色情表演吸引用户注册、消费，以此攫取非法利益。此外，有的直播平台在其主页面发布带有暴力、淫秽内容的第三方广告，用户通过点击此类广告则会跳转到相应的不法网址。以上平台行为均有可能涉嫌“非法利用信息网络罪”。

3、帮助信息网络犯罪活动罪

此罪通常被视为帮助行为正犯化的结果。当下，“在网络发展到平台阶段之后，以网络在网络犯罪中的地位为标准，网络犯罪跃升到第三个阶段，即网络在网络犯罪中作为‘犯罪空间’的阶段”。[①]在这一阶段“网络空间中大量的帮助行为的社会危害性已经远远超过了实行行为的危害性，为犯罪行为提供网络技术帮助的行为越来越重要，已经逐渐占据了主导地位，开始突破帮助行为在犯罪中的从属地位，并主导犯罪和引领犯罪”。[②]正因如此，《刑法修正案（九）》增设了“帮助信息网络犯罪活动罪”。直播平台作为网络直播服务提供者，在明知主播利用直播平台进行违法犯罪活动并为其提供相应技术支持时，成立本罪。但是，由于技术的中立性，在认定本罪成立时，“要谨慎结合主客观方面，避免将提供网络技术支持和帮助的行为扩大化入罪”。[③]

三、网络直播平台犯罪原因

目前，很多对于网络直播平台犯罪原因的研究是通过分析监管部门、直播平

① 于志刚：《网络思维的演变与网络犯罪的制裁思路》，载《中外法学》2014 年第 4 期。
② 于志刚：《网络空间中犯罪帮助行为的制裁体系与完善思路》，载《中国法学》2016 年第 2 期。
③ 参见郭泽强，张曼：《网络服务提供者刑事责任初论——以中立帮助行为的处罚为中心》，载《预防青少年犯罪研究》2016 年第 2 期。

台、主播及观众等利益相关方进行的。最终得出的结论是：网络直播平台犯罪的原因在于“网络直播准入门槛低，主播素质良莠不齐”、“观众不良的使用心理催化相关犯罪”[①]、“网络直播平台盈利模式的推动”、“监管部门监管缺位”[②]等。以上结论更多的是在描述一种现象，并未深入剖析各种因素导致犯罪的运行机制。因此，利用相关犯罪学理论，能够一定程度地模拟网络直播平台犯罪现象的产生，并分析犯罪原因。但由于众多犯罪学理论存在内容交叉，故在分析时难免出现重复论证的现象。

（一）网络直播的商业化本质

“平台作为市场的参与者，与其他市场主体一样，首先是一家企业。根据经济学的定义，企业就是以盈利为目的，运用各种生产要素，向市场提供商品或服务，实行自主经营、自负盈亏、独立核算的法人。”[③]在平台经济下，“网络直播平台的获利模式主要表现为：平台专用摄像头自产自销、广告付费投放、观众打赏平台分成和其他有些平台转播版权收费。而主播收入主要来自平台或工会发放的底薪和打赏分成。”[④]直播平台的企业本质与平台和主播的获利模式反映出当下网络直播行业的主要价值目标，即赚取利润。在这一价值目标的指引下，直播平台和主播会通过各种可能的手段来使自己获得财富。但是，毕竟一定时期内的直播市场规模是相对稳定的。这意味着在每家直播平台或者每个主播都在尽力争取市场份额的过程中，必然有部分平台和主播由于存在劣势因素而难以实现盈利目标。这时，一些处于劣势的直播平台和主播为了获得收入，就会实施犯罪行为，这种现象就体现为犯罪学中的“社会失范”。

美国社会学家默顿提出的“社会失范理论”的基本内容是：在社会中，成员达到社会共同价值目标的机会（合法手段）因地位和阶层的不同而有差别。当下层成员难以通过公平竞争（合法手段)实现价值目标时，他们就会产生一种紧张情绪，并且该情绪可能会促使他们通过非法甚至犯罪手段以实现价值目标。[⑤]对于网络直播而言，由于其行业范围已经形成了“盈利”的价值目标，所以很多平

① 参见隗辉，严语，白玉洁：《网络直播泛娱乐化乱象解读与有序治理》，载《湖北社会科学》2018 年第 2 期。
② 参见梁国鹏：《网络直播治安监管浅析》，载《净月学刊》2018 年第 2 期。
③ 中国信息通信研究院：《互联网平台治理研究报告（2019）》，http://www.caict.ac.cn/kxyj/qwfb/bps/201903/t20190301_195339.htm
④ 参见 Jhony Choon Yeong Ng，于畅，谭清美：《网络直播运作模式和参与者动机研究》，载《西部学刊》2018 年第 6 期。
⑤ 参见张远煌，吴宗宪主编：《犯罪学通论》，北京师范大学出版社 2017 年版，第 115-118 页。

台和主播试图通过各种手段“赚钱”，而不考虑该手段是否被规则所允许。例如常见的“主播为高薪违约跳槽”、“平台为抢占市场不正当竞争”等。此外，由于网络直播的技术依赖性强，一些规模较小的直播平台因为在技术上处于劣势，所以很难通过提供高技术含量的直播来获得市场。但是，为了与大平台竞争，这些平台往往会利用含有色情、暴力等元素的直播吸引观众，并以此攫取利益。可见，网络直播平台的商业本质引发的以“盈利”为核心的一元化价值目标与其盈利模式之间的矛盾，成为网络直播平台犯罪的一个重要原因。

（二）平台和主播的“泛娱乐”标签化

所谓泛娱乐化，尼尔·波兹曼对其有精辟的描述：“‘一切公众话语都日渐以娱乐的方式出现，并成为一种文化精神。我们的政治、宗教、新闻、体育、教育和商业都心甘情愿地成为娱乐的附庸，毫无怨言，甚至无声无息，其结果是我们成了一个娱乐至死的物种”[①]在泛娱乐化的背景下，人们的社会活动方式逐渐丧失理性，癫狂的嬉笑怒骂成为常态，社会目的也从财富创造转向娱乐至上。最终，原本的社会价值瓦解，”价值功利化、价值碎片化、真实幻象化“引发众多道德失范、违法犯罪现象。[②]当前，网络直播正平台是资本与技术结合下泛娱乐化最为严重的互联网场域。网络直播平台设计各类娱乐版块吸引用户下载使用其平台软件。主播则通过丰富的娱乐表演获取关注度。无论是平台还是主播，他们都在尽力地将自己的娱乐属性发挥到极致。例如，有的直播平台将自己明确定位为”泛娱乐直播平台“并大力宣传。有的主播将直播间名称改为”娱乐直播间“。久而久之，直播平台和主播就被贴上了泛娱乐的标签。而这种标签则成为一些犯罪的部分原生力。

在犯罪学的标签理论中，“犯罪和各种违法行为都是社会创造的，是在社会的相互作用过程中被社会自身创制和规定的。”[③]根据标签理论，“‘标签’是犯罪最为重要的元素，‘贴标签’的行为是犯罪发生的肇始。”[④]因此，它所描述的犯罪机制应当是：贴标签-行为人对标签的认同-犯罪。虽然标签理论经常被用于解释犯罪人再次犯罪的原因，但是该理论的逻辑体系依然可以涵盖首次犯

① （美）尼尔·波兹曼著：《娱乐至死》，章艳译，中信出版社 2015 年版，第 4 页。
② 参见邢国忠：《泛娱乐主义对青年价值观的影响研究》，载《中国特色社会主义研究》2018 年第 6 期。
③ 李明琪主编：《西方犯罪学概论》，中国人民公安大学出版社 2010 年版，第 228 页
④ 李明琪，杨磐：《犯罪学标签理论的应然走向》，载《中国人民公安大学学报》（社会科学版）2012 年第 3 期。

罪。以网络直播平台犯罪为例，首先，在“贴标签”阶段，直播平台和主播的标签一方面来自社会及其自身设定的“泛娱乐”标签，另一方面来自司法活动给其贴上的涉黄、涉赌、涉暴等犯罪标签。在”泛娱乐“标签下，直播平台和主播瞄准自身定位，为了娱乐观众可能无所不用其极，甚至不惜违法犯罪。因此，平台及主播的”泛娱乐“标签可能成为他们初次犯罪的起点。其次，在“行为人对标签的认同”阶段，对于“泛娱乐”标签，平台及主播甚至自己给自己贴上此标签，可见对此标签的认同感极高。对于犯罪标签，则不同于“泛娱乐”标签。由于一旦被贴上犯罪标签则可能影响收入甚至被迫退出直播行业，因此，多数平台和主播并不认同此标签。这也可以说明网络直播平台犯罪的再犯率不高，以及平台、主播泛娱乐化下，犯罪仅是个别现象的原因。最后，在“犯罪”阶段，一旦平台和主播被贴上并认同“泛娱乐”或者犯罪标签，那么平台和主播则大概率会实施该标签下的犯罪。正因如此，网络直播平台犯罪的类型多是涉黄、涉暴、涉赌等与娱乐密切相关的犯罪。

（三）平台布局存在诱罪因素

目前，很多网络直播平台的布局为一些网络犯罪提供了条件。网络直播平台为了迎合用户的观看需求，设置了大量的娱乐版块，而且各个娱乐版块内部又根据直播内容细致划分为数个直播类型。同时，对于非娱乐直播，各直播平台或者不开设相关板块，或者开设相关板块但不再进一步划分直播类型。例如斗鱼 TV，该直播平台设置了“推荐分类”、“网游竞技”、“单机热游”、“手游休闲”、“娱乐天地”、“科技教育”、“语音直播”和“正能量”等共八大板块。其中，“推荐分类”中主要是比较热门的娱乐版块的子分类。“网游竞技”、“单机热游”、“手游休闲”、“娱乐天地”等板块之下又分为数量众多的子版块。与之相比，“科技教育”和“正能量”两个板块则简单不少。“科技教育”共有 7 个子版块，而“正能量”则没有子版块，这与其他板块动辄几十个子版块相比，难免显得“简陋”。此外，在斗鱼 TV 直播平台，“推荐分类”、“网游竞技”、“娱乐天地”等娱乐版块的排序靠前，其他非娱乐板块则被放置在末端。这样的布局就使大量的主播和观众集中在娱乐版块，而其它板块的使用人数则寥寥无几。由于网络直播平台形成了一种社交的网络空间，故可以以犯罪生态学的视角分析直播平台布局与平台犯罪之间的关系。

芝加哥学派的犯罪生态学，本质上是通过生态学的视角，分析不同社会空间中的人类关系，进而研究犯罪成因的理论体系。如芝加哥学派的城市生态学理论提出："人类社会也具有共生现象，人类社区的自然变动也经历一个'侵入、统治、接替'的过程。"[①]在芝加哥学派这里，基础的物理空间布局引起的社会成员间不同的相互关系是犯罪发生的重要原因。具体而言，不同的城市社区之间存在环境、资源、政策等方面的区别，基于这些区别，不同社区的居民就会形成各具特色的社会关系和生活方式。比如在贫民窟，因为基础设施较差，缺少政府管理，所以毒品犯罪、暴力犯罪、性犯罪多发。与物理空间类似，网络空间也存在这样的"社区"差异。如前文介绍的斗鱼 TV 的平台布局。在直播平台，娱乐版块本身就有相对非娱乐板块更高的犯罪可能性，加之平台布局使大量主播和用户集中在娱乐版块，这就进一步提高了网络直播犯罪的概率。此外，平台设置众多娱乐版块等于容纳了更多的娱乐主播。在用户人数不变的情况下，这意味着娱乐版块的观众资源相对减少。这时，主播之间的竞争则更加激烈。一些主播为了迎合观众的低俗趣味，便在直播中加入色情、暴力等元素。这些实施越轨行为的主播能够获得更多观众，而其他主播则因关注度降低则可能效仿越轨主播或者逐渐放弃直播，最终形成了越轨直播侵入、统治、接替娱乐板块的过程。总而言之，根据犯罪生态学的观点，直播平台"娱乐版块多且集中，非娱乐板块少且分散"的布局容易引发平台犯罪。

（四）网络直播缺乏有效监管

中国信息通信研究院发布的《互联网平台治理研究报告（2019）》指出："平台具备市场参与者与组织者的双重身份，扮演了信息壁垒打破者与重构者的双重角色。特别是那些规模很'大'的超大型平台企业，甚至已经成为具备准公共产品属性的基础设施。"可见，目前的互联网平台往往具备多种角色。同时，这也显示出当下互联网平台定位的模糊。因此，有观点指出："在现有网络平台监管模式下，网络直播平台作为私法主体行使行政法上的监管职责，在被课予第三方义务时没有获得监管权力，在平台运营阶段基于合同获得监管授权，这种混乱的定位和平台以获取流量为盈利的模式造成了网络直播平台监管机制的硬性缺陷。"[②]

[①] 参见李明琪主编：《西方犯罪学概论》，中国人民公安大学出版社 2010 年版，第 228 页 184-185 页。
[②] 此处引文出处为：李梦琳：《论网络直播平台的监管机制——以看门人理论的新发展为视角》，《行政法学研究》的网络首发论文。

当前，网络直播的监管由政府相关部门和网络直播平台承担。政府主要通过监管平台来实现对网络直播活动的间接监管。同时，政府还采取对违法直播行为科以行政处罚的方式进行事后监管。而直播平台则承担对直播活动的日常监管。如《互联网直播服务管理规定》赋予了直播平台对违法违规直播活动采取行警示、关停等措施的权力，同时也规定直播平台应当配备专业人员并健全信息审核、直播巡查、应急处理等制度。[①]但是，这种"政府+平台"的监管机制并不能有效的防止直播平台犯罪。原因除前述平台地位不清之外，还存在两方面的原因。一方面，目前有网信办、文化和旅游部门、市场监督管理部门等众多政府部门监管直播平台，难以厘清具体职责，多头执法最终影响监管效果。另一方面，虽然法律法规赋予了平台一定的监管权力，但平台更多是根据用户协议中规定的平台权利监管主播和用户。这就导致平台监管往往力度不足且处处掣肘。

以上多种原因造成的网络直播监管不力，在犯罪学的社会控制理论中就表现为社会控制的减弱，是犯罪产生的重要原因。"社会控制理论是指用社会控制的强弱来解释犯罪行为产生原因的一组理论。这种理论认为每个人都是潜在的犯罪人，而多数人不犯罪的原因在于施加在他们身上的社会控制较强"[②]对于网络直播来说，由于其具有即时性、用户流量大和泛娱乐性的特点，一旦对其监管不到位，造成对用户、主播、平台的社会控制减弱，那么这些主体犯罪的机率就会急剧上升。

四、网络直播平台犯罪的治理对策

（一）实现网络直播平台的科学布局

前文利用犯罪生态学的理论分析了网络直播平台的犯罪原因，最终得出直播平台"娱乐版块多且集中，非娱乐板块少且分散"的布局容易引发犯罪的结论。那么为了治理直播平台犯罪，从犯罪生态学的观点来看，可以通过改变平台布局的方式来降低犯罪发生的概率。仍以斗鱼 TV 直播平台为例，首先，斗鱼 TV 数量众多的娱乐版块吸引了大批主播和观众，造成了平台"娱乐人口"基数大的现状。

① 《互联网直播服务管理规定》：第七条 互联网直播服务提供者应当落实主体责任，配备与服务规模相适应的专业人员，健全信息审核、信息安全管理、值班巡查、应急处置、技术保障等制度。提供互联网新闻信息直播服务的，应当设立总编辑。

第十四条 互联网直播服务提供者应当对违反法律法规和服务协议的互联网直播服务使用者，视情采取警示、暂停发布、关闭账号等处置措施，及时消除违法违规直播信息内容，保存记录并向有关主管部门报告。

② 参见张旭，单勇著：《犯罪学基本理论研究》，高等教育出版社 2010 年版，第 98-99 页。

同时，这些娱乐版块的直播时间往往比较集中。根据中国互联网络信息中心发布的《第 43 次中国互联网络发展状况统计报告》显示：网络直播类 APP 在 12 点、20 点、23 点分别出现 3 次使用小高峰，其中在 20 点至 23 点这一时段，网络直播类 APP 的使用率明显高于其他类 APP。巨大的”娱乐人口“基数与集中的高度使用率造成平台监管捉襟见肘。对此，网络直播平台一方面可以相应地减少热度较低的娱乐版块。如对于”网游竞技”板块来说，一般是最近比较火的网络游戏直播热度较高，而一些过时的网络游戏直播则少有人问津。因此，直播平台可以取消那些关注度较低的游戏直播，或者将类似直播归纳在另设的“其他网游”中。另一方面，平台可以安排主播进行错峰直播，合理分配直播观众流量，减轻动态监管的压力。

其次，直播平台的非娱乐板块较少，而且相对娱乐版块而言比较难找到直播内容。对此，直播平台一方面可以多设置一些非娱乐板块。虽然非娱乐主播人数较少，但是平台可以先扩大非娱乐板块“筑巢引鸟”。在增设非娱乐板块的同时，平台可以通过与网络上一些比较知名的具有正能量的自媒体人进行合作，邀请他们定期或者长期在平台进行直播。另一方面，直播平台可以在其“推荐分类”中加入非娱乐板块的直播，或者将非娱乐板块放置在平台较为显眼的位置，提高非娱乐板块的使用度。

（二）明确网络直播平台的监管地位和监管权力

虽然“网络已全面介入社会生活。但世俗化的网络却尚未有与之匹配的安全保障机制。”[①]这种安全保障机制的缺乏就导致了网络直播的社会控制力减弱，并引发了众多犯罪。对于网络直播而言，完善安全保障机制就意味着明确相关监管主体并赋予主体相应的监管权力。

首先，明确监管主体。目前，政府无疑是最具权威的网络直播监管主体。政府通过设立相关部门、颁布行政法规、处罚违法人员和企业单位的方式主导着整个网络直播的监管。但是政府监管是一种运动式、事后性的监管模式。这种模式对于瞬息万变的网络空间而言是不适应的。此时就应该由网络平台承担常态化的监管职责。实际上，目前的网络直播平台通过行政授权和契约授权已经成为了网

[①] 岳平：《世俗化网络社会安全的现实风险及治理——论当前个体被害聚集性现象的生成》，黄河，高扬捷主编：《现代犯罪与社会治理：中国犯罪学学会年会论文集》（2018 年），中国检察出版社 2018 年版，第 465 页。

络直播的准监管人。这种准监管人的角色就像一个家庭中的“兄长”。在作为“家长”的政府之外，直播平台以“兄长”的身份对其“兄弟”（主播、观众等）进行监管。平台成为政府与主播、观众之间的桥梁。当平台监管尺度较严时，主播和观众受到的社会控制就强，反之则弱。可见，“在‘互联网+’时代，平台正逐步成为整个社会生产生活的组织者、协调者与管理者，且在网络空间中拥有特定的管理权(权力)，这正是平台的身份定位。”[①]

其次，赋予监管权力。虽然网络直播平台根据相关法规和合同规定具有了一定的监管权力。但是现有的监管权力并不足以支持平台对整个直播过程进行有效监管。例如对于运行阶段主播及观众个人信息的摘取、审核就缺乏依据。因此，未来可以通过更多的行政授权使直播平台有更充足的监管权。毕竟很多超大型网络平台已经具备了准基础资源的属性。

（三）弱化直播平台及主播的“泛娱乐”与“犯罪”标签

在“标签理论”看来，任何针对犯罪的社会反应，都会在不同程度上起到对犯罪的反作用。因此，对于犯罪的治理，就需要在保证犯罪得到惩治的基础上，将对犯罪的社会反应降到尽可能低的程度。“标签理论”的这种建议实际上是对犯罪的一种去标签化。这种思路对于标签化严重的网络直播平台而言，可以在网络直播平台犯罪治理中进行借鉴。

具体而言，由于网络直播平台及其主播的“泛娱乐化”和“犯罪”标签是形成网络平台犯罪的重要原因。故治理网络平台犯罪的关键就在于对平台、主播的去标签化。

首先，对于“泛娱乐”标签的去标签化。直播平台和主播的“泛娱乐”标签主要来自各类社会媒体及其自身，目的在于借助“泛娱乐”标签获取更大利益。同时，“泛娱乐”并不仅是一个词语，而是目前客观存在的社会现象。基于以上两点，直接生硬地取缔“泛娱乐”标签一方面难度较大，另一方面也不尊重客观事实。因此，以一个具有中性色彩的标签替代“泛娱乐”标签是一个可行的选择。考虑到网络直播平台的技术属性及其互联网信息交互的功能，可以以“信息交互”平台替代原本的“泛娱乐”平台。这既不会损害网络直播平台和主播的利益，也不会违背客观事实，更不会诱导犯罪。据此，媒体和直播平台在报道和宣传中要尽量使用“信息交互”平台，放弃“泛娱乐”平台的叫法。

[①] 姜瀛：《“以网管网”背景下网络平台的刑法境遇》，载《国家检察官学院学报》2017 年第 5 期。

其次，平台和主播的“犯罪”标签是通过立法和司法活动获得的。因此，平台和主播”犯罪”标签的去标签化主要从立法和司法两个方面开展。在立法方面，面对日益频发的网络违法犯罪，立法活动要保持足够的理性。尤其是刑事立法，更要谨慎权衡针对网络直播平台犯罪刑事立法的成本与收益，坚守刑法的谦抑性和人权保障功能。因为，立法的功能“并不在于创造或生产法律，而在于从规范中选择有拘束力的法律以及给予作为有约束力的法律规范以象征的尊严”。[①]因此，在目前网络直播平台犯罪并未给现有刑法体系带来颠覆性冲击，依然可以根据现有刑法规范对直播平台犯罪进行惩治的情况下，应当审慎立法。在司法方面，司法机关不能受网络直播“泛娱乐“标签的影响，要根据案件事实准确定罪量刑，避免“一见到主播犯罪，立刻想到传播淫秽物品，立刻想到寻衅滋事，立刻想到开设赌场”的主观入罪。

（四）推动网络直播价值目标高端化

在“社会失范理论”中，默顿构建的“价值目标-合法手段”的理论体系说明目标与手段之间的矛盾是犯罪产生的重要原因。因此，消灭犯罪产生的原因可以从“目标”与“手段”两个方面进行。但是，在市场经济条件下，网络直播平台作为企业具有盈利的本质属性，这种属性决定了其经营模式必须符合市场规律。就目前而言，网络直播平台的成功证明其经营模式是符合市场规律的。可见，通过改变直播平台的经营模式，在“手段”方面进行治理是行不通的。因此，根据“社会失范理论”，网络直播平台犯罪的治理可以通过改变网络直播价值目标来实现。

具体而言，改变网络直播的价值目标主价值目标的高端化。虽然目前网络直播以“盈利”为主要价值目标，但是网络直播属于文化产业，其目标体系也应当包含一定的文化目标。习近平总书记在中央文艺工作座谈会上指出：“文艺创作中低俗不是通俗，欲望不代表希望，单纯感官娱乐不等于精神快乐。”这就说明当下的文化应当具有高雅的本性，应当引导人积极向上。因此，治理网络直播平台犯罪，可以给网络直播设定更高的文化目标，推动网络直播内容提质升级。这一方面不会影响直播平台的创收，另一方面能够引导主播和观众培养高级趣味，摆脱低级趣味，最终实现网络直播的健康可持续发展。

（五）警惕直播平台形成犯罪亚文化

① 转引自王玉薇：《网络犯罪治理：从层级模式到功能分化》，载《河北法学》2018 年第 4 期。

在整个社会大的价值体系下，也存在不同的价值群体，其中与主流价值观激烈背反的则被认为是犯罪群体，这些群体的价值认同则形成犯罪亚文化。分析科恩的亚文化理论，犯罪亚文化的形成过程应是：社会接触-社会紧张（文化冲突）-犯罪亚文化。[①]古语云“不患寡而患不均”，社会成员在社交过程中会将自我与他人进行对比，当发现自己在金钱、地位、名声等方面逊于他人，并且没有获得相应事物的平等机会时， 基于相对剥夺心理产生的挫折、焦虑、愤怒等社会紧张情绪会促使他们做出一定行为。当那些基于社会紧张实施犯罪的人聚集起来，就形成了反主流的犯罪亚文化。在具有相同犯罪亚文化的群体中，犯罪行为得到承认，犯罪产生的主流社会的罪恶感则在犯罪亚文化中得到消解。判断犯罪亚文化的形成，可以把握三个要素：犯罪现象、犯罪现象与主流文化的关系、群体性。犯罪现象是判断犯罪亚文化形成的起点。犯罪社会学将犯罪视为客观的社会现象，如果缺乏犯罪现象这一客观要素，那么谈论犯罪亚文化也就失去了意义。犯罪现象与主流文化的关系是判断犯罪亚文化形成的第二大因素。存在犯罪现象不意味着形成了犯罪亚文化，比如不带有任何价值判断的激情犯罪，这类犯罪只是人在紧急情况下“应激”行为，并不足以形成亚文化。最后，犯罪亚文化作为一种文化现象，必然存在于群体中。因此，犯罪亚文化的形成也必然离不开众多同类型犯罪。

目前，虽然我国网络直播平台违法犯罪现象频发，且集中表现为几类罪名，但是出现的违法犯罪与主流文化背反之间的因果关系并不明显。比如多数平台和主播对于自己的违法犯罪行为在价值判断上仍是持否定态度的，只是出于经济等因素才实施违法犯罪行为。因此，当下我国网络直播平台的犯罪亚文化形成与否并不明晰。但是，所谓“近朱者赤，近墨者黑”，文化和价值的影响力是巨大而深远的。“亚文化一旦形成，它就稳定的持续下来，产生一种将这些价值、违法规范传导给新加入者的机制。它甚至通过人的学习，成为罪犯之间沟通联系的一种资源。”[②]对于网络直播平台的犯罪治理，一定要大力宣扬主流文化，警惕直播平台形成或者认可犯罪亚文化。

① 参见李明琪主编：《西方犯罪学概论》，中国人民公安大学出版社 2010 年版，第 177-178 页。
② 参见张杰，傅跃建编译：《萨瑟兰与犯罪学》，法律出版社 2010 年版，第 109 页。

网络服务平台的类型及其监管责任探讨*

叶良芳　应家赟**

一、问题的提出

随着网络技术的发展，一些涉及网络平台法律纠纷的案件频频出现，以下是三起较为典型的案例。

1、2010 年发生的 QQ 相约自杀案。自 2010 年 6 月初起，被告张涛多次在被告腾讯公司经营的不同的 QQ 群上向不特定的对象发出“浙江男找一起烧炭自杀”、“浙江男找一起自杀的联系我 15906423317”等内容的自杀邀请。2010 年 6 月 23 日，本案两原告之子范某（1990 年 4 月出生，原上海海事学院大学生）在 QQ 群上看到被告张涛留下的信息后，与被告张涛联系并约定到丽水自杀。6 月 23 日晚，范某从上海出发，于 6 月 24 日早上到达丽水，两人一起住进市区某酒店。当天，两人外出购买了脸盆、酒精、炭、密封胶带等自杀用具，回到酒店房间在卫生间里实施烧炭自杀。在自杀过程中，被告张涛用水浇灭了正在脸盆里燃烧的炭，终止自杀，并劝范某也放弃自杀。下午 5 时左右，被告张涛不理会范某“不要走，再来一次自杀”的要求，独自一人离开了宾馆。离开后直至晚上 8 时前，两人仍有手机通话和短信联系。晚上 11 时左右，被告张涛打电话给宾馆总台，告诉宾馆人员 502 房间可能有人自杀，宾馆工作人员撞开房门发现情况。[①]

2、2014 年发生的魏则西案。2014 年的 4 月，西安电子科技大学计算机专业大二学生魏则西被查出得了滑膜肉瘤。这是一种恶性软组织肿瘤，目前没有有效的治疗手段，生存率极低。与癌症斗争期间，他表现出坚强的一面，希望一次次燃起，又一次次破灭。他通过百度搜索找到排名领先的武警北京总队第二医院，曾 4 次前往这里进行生物免疫疗法，这个疗法曾像“救命稻草”一样被魏则西和父母紧紧握在手中。不过，这是百度医学信息竞价排名，这个号称“斯坦福”先进技术的生物疗法也不像百度搜索中说得那样好，甚至是被国外临床淘汰的技

* 本文系未完成稿，仅供会议交流，请勿引用，谢谢合作。

** 作者简介：叶良芳，浙江大学光华法学院教授、博士研究生导师；应家赟，浙江大学光华法学院博士研究生。

① 参见“门路、范黄河诉张涛、腾讯计算机系统有限公司生命权、健康权、身体权纠纷案二审判决书“，浙江省丽水市中级人民法院民事判决书([2011]浙丽民终字第 40 号)。

术。他的病情扩散很快。2016 年 4 月 12 日，魏则西去世。[①]

3、淘宝平台卖假货被诉案。2016 年 10 月 10 日，杜胜通过淘宝网上一家名叫“Robam 老板厨具”的店铺购物，以 3168 元的价格购买了一台该店铺销售的老板 CXW-200-8218 顶吸式大吸力抽油烟机一台，订单编号为：2513xxx368641，该店铺由许子建经营。在该店铺淘宝网销售页面上显示有“假一赔十”、“正品行货”、“送货入门”、“上门安装”等字样。后上述货物通过物流公司运至杜胜收货地。杜胜称在收到货物后，安装人员进行安装时发现挂板尺寸不对，无法完成安装。郑州天宫厨房电器销售有限公司出具的一份质量鉴定证明：“上门查看发现烟机止回阀颜色、伸拉管保护膜颜色和我们统一配置的白色不一致；公司电商平台也没有查到顾客订单信息，认定不是我们的产品。”杭州老板电器股份有限公司于 2017 年 8 月 22 日作出质量鉴定报告一份，认定送检产品从包装到材质均不是该公司生产，系假冒伪劣产品。杜胜后与淘宝公司的客服联系协商，淘宝公司将商家许子建个人身份信息向杜胜予以披露，杜胜涉案购物款 3168 元已退还。[②]

上述事案突显出一个法律问题：作为网络服务提供者的网络平台，对于事案所造成的危害结果，要不要承担相应的法律责任？如果需要，则其承担的法律责任是民事责任、行政责任抑或是刑事责任，其具体内容如何？如果不需要承担，则法理根据何在？本文不揣冒昧，拟对这些问题进行粗浅探讨。

二、网络平台的基本类型

（一）网络平台的立法分类

域外立法普遍以平台所提供的技术功能特征为标准，对网络平台进行分类。具体而言，美国 1998 年《数字千年版权法案》将网络服务提供商分为四类，即临时性数字网络传输服务的提供者、系统缓存服务的提供者、信息储存服务提供者和信息搜索、定位服务提供者。韩国 2011 年《著作权法》参照该法案，将网络服务提供者同样分为四类，即网络自动接入或自动传输服务提供者，系统缓存服务提供者，信息存储空间服务提供者和搜索、连接服务提供者。2000 年《欧盟电子商务指令》将网络服务提供者区分为三类，即作为纯粹的传输通道的服务

① 参见《青年魏则西之死》，载《新京报》2016 年 5 月 3 日第 A08 版。

② 参见“杜胜与许子建等产品责任纠纷案一审判决书”，河南省郑州市中原区人民法院民事判决书（[2017]豫 0102 民初 4873 号民事判决）。

提供者、缓存服务提供者和主机服务提供者。德国2007年《电信媒体法》明确区分四种类型的网络服务提供者，包括内容服务提供者，信息传输服务提供者或通道服务提供者，临时性、自动性缓存服务提供者和存储服务提供者。

相比之下，我国相关法律、行政法规对于网络平台的类型区分则不够明确统一。国务院2006年通过的《信息网络传播权保护条例》，对网络接入和传输服务提供者、自动存储服务提供者、存储服务提供者、搜索和链接服务提供者的免责条件进行了不同规定。2016年《网络安全法》规制的主体是“网络运营者”，具体又包含网络的所有者、管理者和网络服务提供者。从《网络安全法》的“法律责任”一章的相关规定看，又区分了“网络产品或服务的提供者”、“电子信息发送服务提供者”和“应用软件下载服务提供者”。《互联网信息服务管理办法》区分了互联网信息服务提供者与互联网接入服务提供者。《刑法》第287条之二则规定了“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，或者提供广告推广、支付结算等帮助”的不同犯罪主体。

（二）网络平台的学理分类

从理论界来看，网络服务平台主要存在以下分类：

（1）两分法：网络服务提供者（ISP），根据网络服务提供者提供服务内容的不同，可以分为网络信息内容提供者（ICP，自己组织信息通过网络向公众传播）与网络中介服务者（为传播网络信息提供 中介服务），后者有网络接入服务提供者（IAP）、网络平台提供者（IPP）等。

（2）三分法：网络服务商（ISP）包括网络连线服务商（IAP）、网络内容服务商 （ICP）和网络平台服务商（IPP），三者构成犯罪与承担的具体刑事责任不尽相同。此外，也有学者将网络服务提供者分为网络接入服务商、信息储存空间服务商与搜索引擎服务商。[①]

（3）四分法：以网络技术行为的主要功能为标准，将网络服务提供者分为内容提供者、网络接入服务提供者、缓存服务提供者、存储服务提供者四种类型，以确立层次性合合理、功能性鲜明的网络主体结构，并以此确定义务的核心内容与责任的边界。[②]

此外，还有学者从信息传播的角度将网络平台分为：纯粹的信息传输平台，

[①] 参见宋哲：《网络服务商注意义务研究》，:北京大学出版社2014年版，第4页。
[②] 参见王华伟：《网络服务提供者的刑法责任比较研究》，载《环球法律评论》2016年第4期。

信息自动缓存服务平台，信息存储平台，信息搜索、连接平台，以及去中心化的P2P平台。对于信息提供平台，可基于其开放程度不同，将其区分为开放类平台、非开放类平台和私密平台。开放类平台面向社会公众全体开放，例如，微博、论坛等。非开放类平台面向特定用户群体开放，如Facebook。私密平台则是为特定主体提供点对点网络信息通信交流服务，如微信、qq、Whatsapp。[①]

以上分类深受域外立法的影响，根据技术服务的内容作了不同类型的划分。总体是可取的，不足之处是标准和类型不够统一。笔者认为，划分网络平台的类型，是设定区别化的管理义务，因而应当根据网络服务的功能不同来进行分类。从本质上而言，网络平台是一种“网络中介”，扮演着为双方或多方用户提供信息传播、商事交易以及社会交往的媒介的角色。联合国经济合作组织2010年发布的《网络中介的经济与社会作用》，将网络中介定义为，“将网络上的双方或多方聚合在一起或为其交易提供便利服务的主体，其可以对第三方制作的内容、产品和服务提供接入、主机服务、传输和检索服务。”[②]这是以技术功能为切入点对网络平台类型的一种划分方法。在当前数字时代的社会背景下，更应当结合网络平台所承担的“中介者”的本质特征，以提供服务的内容为标准，对其进行分类。具体可以划分为以下几种类型：一是网络信息平台，包括视频聚合、新闻聚合平台；二是网络交易平台，例如eBay.de、Amazon、淘宝网、京东商城等；三是网络支付平台，如支付宝；四是网络搜索平台，如百度、Google；五是网络社交平台，如Facebook、Twitter、微信、微博、QQ和公共论坛等。这种对网络平台以提供服务内容和商业运营模式为标准的分类方式近年来也在我国各行政法规范中得到适用。

类型化划分的优势，在于明确不同性质、不同种类的网络服务提供者不同的法律责任。例如，《信息网络传播权保护法》针对的是“为服务对象提供搜索或链接服务的网络服务提供者”，《互联网信息搜索服务管理规定》重点规定“互联网信息搜索服务提供者”，《移动互联网应用程序信息服务管理规定》 重点规定“移动互联网应用程序提供者、互联网应用商店服务提供者”，《互联网广告管理暂行办法》重点规定“互联网广告主、广告经营者、广告发布者、广告需

[①] 参见周学峰、李平：《网络平台治理与法律责任》，中国法制出版社2018年版，第10-11页。
[②] Organization for Economic Cooperation and Development The Economic and Social Role of Internet Intermediaries （Paris：OECD，April 2010）.

求方平台经营者”，《互联网直播服务管理规定》针对的是“互联网直播服务提供者”，《网络表演经营活动管理办法》针对的是“网络表演经营单位”。这些具体规定有针对性地专门规制各种不同类型的网络平台。

三、域外关于网络平台监管义务的规定及其评析

（一）网络平台监管责任的传统立法模式

美国1996年《通信正派法》第230（c）（1）条规定：“互动式计算机服务提供者或者使用者不应被看作其他信息内容提供者所提供的信息的出版者或发布者。该条规定作为免责条款，豁免了网络服务提供者对第三方发布的违法信息的法律责任。而Roommates案[①]创设了对230条免责条款的适用条件，即网络服务提供者并没有对第三方发布的信息起到“实质性地促进”作用。

在网络平台的知识产权责任规制方面，美国《数字千年版权法》第512条创设了日后广为世界各国立法所借鉴的著名的“避风港”规则。根据其规定，该规则适用需要具备两个前提条件：首先，网络服务提供者必须已经采取并合理实施了有效的措施，并告知其会员和其他用户，在特定情况下，对实施重复侵权行为的会员或其他用户终止服务；其次，网络服务提供者必须采纳“标准技术措施”，且不与之抵触。此外，根据512条c款规定，第一，网络服务商并不知道侵权行为，包括其实际上不知道侵权，没有意识到侵权行为发生的事实或情况，或在得知或意识到的情况下，就立即撤下侵权材料，或封堵了侵权材料的访问入口。对于网络服务商“不知道侵权行为”的认定，采取红旗标准，即要求其没有意识到能够从中明显发现侵权行为的事实或情况。当有关他人实施侵权行为的事实已经像一面色彩鲜艳的红旗在网络服务者面前公然飘扬，以至于处于相同情况下的理性人都能发现时，如果网络服务者采取鸵鸟政策，故意装作看不见侵权事实，则同样能够认定其至少应当知道侵权行为的存在；第二，如果网络服务商有权利和能力对侵权行为进行控制，其必须没有直接从侵权行为种获得经济利益；第三，在收到合理的侵权通知以后，网络服务商必须迅速撤下侵权内容或阻止对侵权内容的访问。即“避风港规则“的适用具体采用”通知—删除”程序：网络平台在接到权利主张者的投诉通知后，应及时将被指控侵权的信息内容从网站上删除或屏蔽，并立刻通知发布该信息的用户，用户在接到通知后如果认为其发布的信息

① Fair House Council v. Roomates.com, LLC, Roommates. Com, LLC, 521 F.3d 1157 (9th Cir.2008).

不构成侵权，可向网络平台发出反通知。网络平台在收到反通知后应立刻将其转发给权利主张者，并告知其将在10天恢复被删除或屏蔽的信息。网络平台应当在收到反通知之日起不少于10日且不超过14日期间内恢复被删除或被屏蔽的信息，除非其在采取行动之前收到群里主张者已向法院提起诉讼请求用户停止实施侵权行为的通知。

欧盟的《电子商务指令》（以下简称《指令》）是适用于网络平台的重要法律文件之一。但是根据《指令》第15条的规定，法律不对信息社会服务提供者施加一般的信息监控义务和主动监控义务。德国1997年《电信服务法》（简称TDG）第5条规定：“（1）服务提供者根据一般的法律对自己提供的内容负责；（2）如果所提供的内容是他人的，那么只有在服务提供者知晓这些信息的内容并且在技术上有可能阻止且进行阻止不超过其承受能力的情况下，才承担责任……（4）如果服务提供者在不违反《电信法》第85条关于保守通信秘密规定的情况下知晓信息内容，有技术可能加以阻止，且阻止不超过其承受能力的，那么根据一般的法律产生的对于违法内容信息的封锁义务不受影响。”德国2007年《电信媒体法》（简称TMG）第7—10条规定：（1）服务提供者应当根据一般的法律对自己提供的信息承担责任。（2）在本法第8条至第10条的规定范围内，服务提供者对于传输或存储的信息不承担监管或查明违法信息并主动进行提示的义务。根据第8条至第10条的规定，虽然服务提供者对违法信息不承担责任，但应承担依据一般原则而要求其履行删除或对信息使用的屏蔽义务。由此可得，德国《电信媒体法》，TMG虽然规定了网络平台的法律责任，但其本质上却是对网络平台的免责条款，起到责任过滤机制的作用。

（二）网络平台监管责任的最新立法模式

基于网络平台提供的服务内容和商业模式进行分类，并针对特殊类型的网络平台进行专门和具体的立法，这是近年来域外国家网络平台监管责任的新型立法模式。

为强化社交网络平台法律责任，德国联邦议会于2017年6月正式通过《改进社交网络中法律执行的法案》（简称《网络执行法》），明确了社交网络平台的内容审查与监管义务。《网络执行法》对平台的范围和概念作出明确界定。该法的规制对象并非一切社交网络服务提供者，只有以营利为目的、以用户与其他

用户或向公众分享任意内容为取向、且在德国注册用户多于200万的社交网络平台才受该法约束，如Facebook、Twitter。相比欧美国家对于网络治理一贯采取的完全放任的“市场自治”模式，要求网络平台实施监管责任是一个全新的责任分担的方案。《网络执行法》建构了三项重要制度，一是社交网络平台的主体责任，二是社交网络平台的报告义务，三是违反义务的处罚机制和罚金数额。社交网络平台需要承担对平台信息的“托管责任”，具体包括及时删除、屏蔽责任，受理投诉的责任等，平台必须及时关注并清理暴力恐怖、极端、仇恨和谣言，如果被其他用户举报的明显而严重的非法内容则必须在2小时内删除或屏蔽。为此，网络平台应建立简单便民的投诉举报路径和受理处理制度。社交网络平台的报告义务要求互联网社交媒体平台必须每半年至少发布一次报告或者每季度报告，公示收到的用户投诉数量和平台的处理情况，且报告应在互联网上公布。在违反义务的处罚机制和罚金规定方面，根据《网络执行法》，联邦司法局可就违反该法的行为，对社交网络平台处以罚款，最高罚至5000万欧元。处罚前，法院有权监督司法局并就处罚做出裁定。《网络执行法》的立法目的乃是为更有效打击社交网络平台上的仇恨犯罪、构成犯罪的假新闻、恶意攻讦、恐怖主义宣传及其他刑事违法内容，即仇恨言论、煽动性言论和虚假新闻造谣三部分，包括违反德国《刑法典》以下各节的内容：第86条（宣传违宪组织宣传材料）；第86a节（使用违宪组织的标志）；第90条（诽谤联邦总统）；第111条（公开煽动犯罪）；第126条（威胁实施违反公共安宁）；第130条（煽动仇恨）；第140条（资助和批准犯罪）；第166条（诽谤宗教，宗教和意识形态协会）；第185至187条（侮辱、诽谤、故意诽谤）；第241条（威胁重罪）和第269条（伪造数据旨在提供证据）。

《网络执行法》因其加重社交类网络平台责任的鲜明立法模式而招致不少争议与批判。有论者提出，由于该法的规定，会导致的必然后果是，在对内容是否违法存疑时，平台为避免其法律责任而倾向于做出删除、屏蔽相关内容的选择，这势必会造成对于网络言论的“过度封锁”。然而支持者则认为言论自由并非毫无界限，刑法就划定了界限。社交网络平台并非只为用户提供中立的基础设施，而是通过其商业模式形塑网络交流空间。既然对内容的审查、删除或屏蔽是平台本来就行使的权力，也是其不可推卸的责任。

韩国《电子商务法》对电子商务网络平台予以特别规制。该法适用主体是为Cyber Mall（网络购物中心）提供服务的“通讯销售业者” 和“通讯销售中介人”。具体可划分为以下三种类型：网络购物中心使用许可人；提供信息型通讯销售中介人；参与交易型通讯销售中介人。网络中心使用许可人是指设立一个网络购物中心并允许网络卖家在此进行商业交易的第三方网络平台。提供信息型通讯销售中介人，是指以自己的名义为网络销售提供广告服务，或者以平台的名义发布广告并通过提供该网络销售信息的方式进行提供中介服务的第三方平台。通过搜索引擎提供商品实时信息的门户网站如shopping.naver.com，以及专门提供价格比较信息的价格比较网站如http://www.danawa.com/等网站都属于该类第三方平台。参与交易型通讯销售中介人，是指以自己的名义为网络销售提供广告服务或以自己的名义进行广告宣传并通过接受网络买卖要约等部分销售行为来为交易双方提供中介服务的第三方平台。如www.gmarket.co.kr。《电子商务法》规定了其保存交易记录、预防操作失误、通讯销售中介人告知及提供信息义务、通讯销售中介人对消费者的连带责任。

（三）域外关于网络平台监管义务立法的特点及评析

1.网络平台承担有限责任

针对网络平台的法律责任，域外国家在相关立法中普遍设立限制责任和甚至免责的专门规定。譬如美国《数字千年版权法》第512条对网络平台涉及著作权侵权责任设置了避风港规则，《通信正派法案》第230条则是针对知识产权之外的其他民事责任的免责条款。欧盟《电子商务指令》第12条、第13条和第14条规定了网络平台承担民事责任的免责条件。德国《电信媒体法》第8条、第9条和第10条，英国《电子商务条例》第17条案、第18条和第19条都几乎复制了欧盟的免责规定。日本《关于特定电信服务提供者的损害赔偿责任限制及向服务提供者请求提供发送者信息的法律》对网络平台的损害赔偿责任予以一般性的限制。

2.网络平台不承担一般性审查义务

美国《数字千年版权法》第512条规定，不得将有关网络服务提供者的法律责任或免责条款解释为网络服务提供者对于用户发布的网络信息负有监控或审查的义务。此外美国国会在制定《通信正派法》第230条时曾明确指出其立法目

的在于避免网络服务提供者承担对内容提供者所发布的信息的审查义务。欧盟《电子商务指令》第 15 条规定禁止欧盟成员国对网络服务提供者施加一般性义务，使其在提供服务的过程中对其传输或储存的信息进行监控，成员国亦不得对网络平台施加积极查找涉嫌违法活动的事实或情况的一般性义务。

虽然网络平台在法律上不负有积极进行审查或者屏蔽违法信息的一般性义务，但并不意味着在上述国家不存在任何的信息审查机制，事实上，在上述国家的网络平台的经营实践中都存在着各种各样的信息审查或屏蔽机制，只不过其在形式上并非政府依照法律强制网络平台实施的，而是采取互联网行业自律的方式，或者互联网企业与政府相关部分自愿合作的机制来实施的。

3. 鼓励平台对违法内容和行为采取自律措施

尽管欧美不主张对平台施加一般性的管理义务，但由于近年来过滤技术的发展，以及网络违法内容和假冒商品带来的负面影响不断扩大，欧美国家开始重视网络平台的作用。在欧盟，鼓励企业采取主动措施来履行违法内容管理的义务。2016 年，欧盟 IT 公司率先打击网上非法仇恨言论传播，与欧盟委员会达成了一项自律行为准则。欧盟委员会在 2016 年《欧盟在线平台和数字单一市场的挑战和机会》报告中强调，在线平台需要采取更加负责任的行动，加强欧盟范围内的自律措施，消除非法内容。据欧盟 2017 年 6 月的相关报告显示，6 个月内欧盟某些国家的通知的违法内容移除比例从 28%上升到 59%。违法内容移除的速度也有改进，这说明自律措施产生了作用。在美国，俄罗斯通过社交平台干预美国总统大选的事件引发美国互联网平台管理的改革，包括谷歌、Facebook、Twitter 等公司，都开始被要求对广告、新闻和相关信息进行监管。目前，Facebook 和 Twitter 已修改了企业规则，主动承担政治广告、伦理、种族等相关内容过滤的责任。

4. 区别化的管理义务立法。

网络服务提供者原则上应承担一般的法律规定的管理义务，但单纯技术服务类型的网络服务提供者在一定的条件下不承担民事责任，不同类型的服务提供者承担的管理义务不同，如协助执法机关进行通信监控、数据留存和保护用户数据是各类公共通信服务提供者的共同义务，网络服务提供者不承担审查用户上传信息的义务，如果没有同时满足“知晓内容”“技术上有可能阻止”“阻止不超过

其承受能力”等条件，那么提供纯粹传输、缓存、数据存储服务等所谓中间服务提供者不对用户提供的非法信息承担责任。

5. 鲜有追究刑事责任

在美国、德国的司法实务中，极少出现追究网络平台刑事责任的判例，权利人往往采取民事诉讼手段而非寻求刑事诉讼以进行维权。相比较而言，在日本和韩国对于网路平台的刑事责任则较为严苛。德国《电信媒体法》虽然规定了网络平台的法律责任，但其本质上却是对网络平台的免责条款。如果网络平台对此事并不存在直接故意或间接故意，以及无法从客观角度来证明平台对此存在直接故意或间接故意的情况下，网络平台只要做到了对于违法信息采取及时删除和封锁措施，即不应当追究其刑事责任。在探讨网络平台对用户行为承担刑事责任时，理论上可能会涉及“中立的帮助行为”问题，该理论也在很大程度上限缩了网络服务提供者的责任范围。如果网络平台对于他人所利用网络来实施犯罪行为，主观上存在直接故意或者间接故意的，可以根据帮助犯理论来解决其刑事责任问题。具体的罪名适用问题包括德国刑法分则中较为典型的违法犯罪行为。但从德国司法机关的判例实际来看，多数情况下并没有要求网络平台为他人利用该平台所实施的犯罪行为承担责任，因为在客观上很难有直接的证据证明网络平台和他人的犯罪行为之间有直接关联性。

由以上特点不难得出，域外对于网络平台的责任采取较为克制的立法态度。究其原因有三：首先，为保护信息网络的发展，故不对网络平台服务商施加较重的管理义务和责任。网络平台服务商施加严格控制信息意味着检查、阅览私人信息的过重负担。[①]其次，域外立法一贯坚持技术中立原则。技术中立原则指代美国知识产权法中的“实质性非侵权用途”规则。所谓的“实质性非侵权用途”规则，其实是一项责任抗辩事由。根据美国侵权法规定，明知或应知他人实施侵权行为而给予帮助的人也要承担侵权责任。但如果某类物品既可以被用于合法的用途，也可被用于侵权用途，那么，不能仅仅因为该类物品有可能被他人用于侵权用途而推定提供者“应当知道”他人侵权，更不能以此为由被要求承担帮助责任或替代责任。该项规则是美国联邦最高法院在 1984 年“索尼”案中提出来的，该案是一起涉及版权侵权的案件。“实质性非侵权用途”规则之目的在于将帮助

① 参见陈洪兵：《中立的帮助行为论》，载《中外法学》 2008 年第 6 期

侵权的责任限制在一个合理的范围内，在保护知识产权人的利益的同时，不妨碍技术的进步。国外对于中立帮助行为的司法态度则是逐渐沿着由主张入罪向主张限缩可罚的范围这一方向转变。德国和日本对于中立帮助行为所采取的态度不是大肆扩张而是极力限制其处罚范围。德日刑法对于传统的中立帮助行为的可罚性，祛除传统因果共犯论的局限，以客观归责论为基础，采取限缩处罚的态度，其出发点在于维护公民的安定感和日常交易的稳定性。当传统的中立帮助行为遭遇到信 息网络，德日刑法依旧秉持谨慎入罪的立场，让网络中立帮助行为的可罚性经受“全面性考察”的检验，以确保网络信息技术发展的通畅。第三，保护公民个人和言论自由和信息隐私安全。假如移动通讯企业对所有的信息予以甄别来判断是 否存在犯罪信息，这事实上必将造成移动通信用户个人信息的泄露，甚至可能侵犯言论自由。[①]

四、我国关于网络平台监管责任的规定

（一）网络平台的民事义务责任

我国关于网络平台民事责任的立法最早源于著作权领域，2006 年《信息网络传播权保护条例》明显受到美国的《数字千年版权法案》的影响。2009 年《侵权责任法》第 36 条为包括网络平台在内的网络服务提供者规定了侵权责任的一般规则：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。网络服务提供者知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。此后，最高人民法院又通过制定网络人身权益司法解释，确立了网络平台在侵犯人身权益领域的民事责任适用规则。2013 年修订的《消费者权益保护法》第 44 条亦为网络平台确定了其在消费者权益保护领域的民事责任规则：消费者通过网络交易平台购买商品或者接受服务，其合法权益受到损害的，可以向销售者或者服务者要求赔偿。网络交易平台提供者不能提供销售者或者服务者的真实名称、地址和有效联系方式的，消费者也可以向网络交易平台提供者要求赔偿；网络交易平台提供者作出更有利于消费者的承诺的，应当履行承诺。网络交易平台提供者赔偿后，有权向销售者或者服务者追偿。网络交易平

[①] 齐文远，杨柳：《网络平台提供者的刑法规制》，《法律科学(西北政法大学学报) 》2017 年第 3 期。

台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任。在 2016 年颁布的《网络安全法》对包括网络平台在内的网络运营者规定了多种法律义务，其大多数条款均为公法性质的管制性条款。但该法第 74 条作出了一条概括性规定，为创设网络平台的民事责任设定了一个入口，即“违反本法规定，给他人造成损害的，依法承担民事责任。”

（二）网络平台的行政义务与责任

近年来，随着与网络平台相关的法律、法规和行政规章的密集发布，我国已建立起规模日趋庞大的网络监管规则体系，其内容涵盖网络安全、数据安全、信息内容安全、电子商务、互联网广告、互联网金融、互联网医疗、互联网新闻出版、共享经济、个人信息保护、协助执法等多个领域。我国相关行政法规范对于网络平台承担的行政责任呈加重的立法趋势。2000 年颁布的《电信条例》和《互联网信息服务管理办法》对服务提供商规定的内容管理义务相对较轻。《电信条例》第 61 条规定：“在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十六条所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告。”《互联网信息服务管理办法》第 16 条规定：“互联网信息服务提；供者发现其网站传输的信息明显属于本办法第 15 条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。”前述两部立法仅要求网络服务提供商发现“明显”违法信息，停止传输和采取措施即可。而在随后颁布的《网络安全法》、《食品安全法》等法律中，对服务提供商则规定了较为严格的义务。例如，《网络安全法》第 47 条规定：“网络运营者应当加强对其用户发布的信息的管理，发现法律、行政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，防止信息扩散，保存有关记录，并向有关主管部门报告。”立法将原有的“明显”剔除，扩大了网络平台所承担的责任范围。此外，网络平台的监管责任从信息管理扩展到行为管理，审核平台上的经营者的身份和资质信息的真实性，对平台经营者的违法行为进行管理和及时处理也成为其监管义务的内容组成。《食品安全法》第 62 条规定：“网络食品交易第三方平台提供者应当对入网食品经营者进行实名登记，明确其食品安全管理责任；依法应当取得许可证的，还应当审查其许可证。网络食品交

易第三方平台提供者发现入网食品经营者有违反本法规定行为的，应当及时制止并立即报告所在地县级人民政府食品药品监督管理部门；发现严重违法行为的，应当立即停止提供网络交易平台服务。网络交易平台的审核经营者义务也较为严格。《网络交易管理办法》第 23 条规定："第三方交易平台经营者应当对申请进入平台销售商品或者提供服务的法人、其他经济组织或者个体工商户的经营主体身份进行审查和登记，建立登记档案并定期核实更新。"

（三）网络平台的刑事义务与责任

在我国当前规制体系中，网络平台的刑事责任大致可以归纳为三种基本类型：一是基于网络平台独立行为单独触发刑事责任；二是基于用户犯罪的帮助行为产生的刑事责任；三是基于协助执法义务触发刑事责任。就网络平台作为独立行为人单独触发刑事责任而言，其行为本质上并未超出传统刑法罪名的基本理论和犯罪构成。就网络平台因用户行为而产生的刑事责任而言，此时网络平台虽不是犯罪行为的直接实施者，但其作为或不作为对犯罪起到了辅助作用，亦有可能由此引发刑事责任。网络平台可能承担的第三类刑事责任源于协助行政执法义务，其启动以行政义务的不履行为前提。

我国司法解释对网络服务商刑事责任的规定如下：(1) 实质上对信息的传播。2004 年两高《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第 11 条规定："通过信息网络向公众传播他人文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的行为，应当视为刑法第 217 条规定的'复制发行'。"这适用于内容服务商。(2) 技术上提供了网络接入服务。2005 年两高《关于办理赌博刑事案件具体应用法律若干问题的解释》第 4 条规定："明知他人实施赌博犯罪活动，而为其提供资金、计算机网络、通讯、费用结算等直接帮助的，以赌博罪的共犯论处。"此处的"提供计算机网络"应当指的是网络接入服务。2004 年两高《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》第 7 条规定，明知他人实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算等帮助的，对直接负责的主管人员和其他直接责任人员，以共同犯罪论处。2010 年两高《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 6 条规定，电信业务经营者、互联网信息服务提供者明知是淫秽网站，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收费等服务，并收取服务费，以传播淫秽物品牟利罪定罪处罚。司法解释对于网络接入服务商、内容服务商和平台服务商等角色并没有细致区分。2010 年司法解释同之前相比，明确地将提供技术服务的一方以实行行为定罪处罚，明显有扩张网络服务商刑事责任的倾向。(3)为他人的信息负有管理责任。两高《淫秽信息解释（二）》第 3 条规定，利用互联网建立主要用于传播淫秽电子信息的群组，成员达 30 人以上或者造成严重后果的，对建立者、管理者和主要传播者，以传播淫秽物品罪定罪处罚；第 4 条规定，以牟利为目的，网站建立者、直接负责的管理者明知他人制作、复制、出版、贩卖、传 播的是淫秽电子信息，允许或者放任他人在自己所有、管理的网站或者网页上发布，以传播淫秽物品牟利罪定罪处罚。

《刑法修正案（九）》作出较大修改，并直接或间接涉及网络平台的刑事责任问题。主要包括以下方面：第一，新增第 286 条之一拒不履行信息网 络安全管理义务罪，犯罪主体是网络服务提供者，直接针对网络平台犯罪。第二，新增第 287 条之一非法利用信息网络罪，尽管并未明确规定网络平台是犯罪主体，但从设立网站与通讯群组以及发布信息等危害行为方式看，原则上可以延伸至网络平台。第三，新增第 287 条之二帮助信息网络犯罪活动罪。该条将网络技术中立帮助行为予以正犯化并独立成罪，客观上为追究网络信息服务者的刑事责任提供直接依据。

《刑法》只是概括地规定了网络服务提供者的管理义务，而《互联网信息管理办法》、《网络安全法》、《反恐怖主义法》、《关于加强网络信息保护的决定》、《电信条例》等前置法律中规定了各类网络服务提供者应承担各项义务，包括技术支持与协助、数据留存、保护个人信息、管理发现的违法信息、主动审查含有恐怖主义、极端主义内容信息、真实身份验证、对不提供实名认证者拒绝服务。

（二）我国关于网络平台监管责任的立法特点及其评析

一是偏向于维护网络平台的发展而不愿提高其民事责任。尽管近年来我国加重了对网络平台监管责任的立法规定，但在司法实践中对于网络平台的法律责任

仍然采取较为保守克制的传统态度，如在蔡振文诉淘宝公司网络服务合同纠纷案中，法院认为："淘宝平台虽拥有庞大的用户群体，但仍属提供一般服务性质，显然不属于公共服务企业或者准公共服务企业，不可仅据此而要求淘宝公司在平台规则的设立、执行等方面与公共服务企业具有同等或类似的高度注意义务。淘宝平台的规则合理与否，乃至其相应程度，应交由淘宝用户予以体验和评价，司法应对此给予足够的尊重和空间，而不应强行介入，否则，商事交易主体的私权利内容和处分意志将极大压缩，鼓励交易、尊重交易的司法导向亦将严重褪色。[①]

二是主要局限于民事责任的承担而鲜有追究刑事责任。虽然《刑法修正案（九）》对于网络平台增设相关罪名，然而在司法实践中却很少追究刑事责任。尤其是拒不履行网络安全管理义务罪，据不完全统计，自《刑法修正案（九）》增设该罪名至今，只有在一起案例中得到适用。[②] 究其原因，主要有以下两点：首先，当行政机关提出时要求网络平台履行网络安全管理义务后，网络服务提供商作为市场主体，基于成本与效益的考量，自然也大多会按令行事，以避免行政责任与刑事责任的承相关平台往往会接受行政机关指令，积极履行相关义务，"经管理部门责令改正而拒不改正"的情况极为少见。其次，该罪名得以成立的前提取决于行政机关的监管，而受到网络空间即时性、专业性、特殊性限制限制，行政机关往往很难发现网络平台未履行安全管理义务的情况。

三是基本立足于对网络服务者的综合性立法而没有类型化立法。前述欧美国家的最新立法的变化是，根据网络服务提供者的业务活动类型和义务承受能力，规定了类型化、区别化的管理义务，中间服务提供者的义务要明显轻于互联网信息服务提供者的义务。我国法律对网络服务提供者的类型化并不充分，仅前述行政法规和部门规章对网络服务提供者作了分类，且在管理义务几乎没有分类规定，而停留在概括式的综合规定。具体表现为对网络平台责任实行"一刀切"的立法模式，即不区分平台的运营模式、控制程度，均赋予相同的义务和责任。

五、类型化思维下网络平台的监管责任

（一）权责一致：网络平台的权限

网络平台出现早期，其往往扮演消极中立的第三方角色，为网络信息的传播

① 参见"蔡振文诉淘宝公司网络服务合同纠纷案二审判决书"，广东省佛山市中级人民法院民事判决书([2016]粤06民终3872号)。
② 参见"何某某、李某某开设赌场案一审判决书"，江西省南昌市东湖区人民法院刑事判决书([2018]赣0102刑初585号)。

提供通道、空间或技术支持，网络平台的商业模式也较为简单，然而，当前网络平台的商业模式日益复杂化，网络平台的自身信息提供行为与用户的信息发布行为难以区分，部分网络平台借助信息技术利用用户发布的信息内容进行盈利，或对用户发布的信息进行技术干预。由此导致的后果是，一些形态已经发生变化的网络平台可能无法满足立法者以网络平台的初始形态为样本设计的免责规则的适用条件。因此，应当根据网络平台的权力配置相应的义务，即坚持权责一致原则。一方面，由于网络技术的发展，一些网络平台本身具有的权力呈现扩张的样态；另一方面，网络技术的发展使企业越来越具有垄断性，从而分享了传统上行政机关的管理权限。由此，网络平台的权限整体上呈现扩张的态势，相应的，其应履行的责任也应相应增大。事实上，网络空间和物理空间一样，都是人类社会交往的场所，只是发生的场域不同而已，所以，网络空间中的行为主体至少要承担和物理空间相同的责任。并且，由于网络的集聚效应和增强效应，行为主体的权力比物理空间要大得多，根据权责一致的原则，其所应承担的义务也应相应增大。

（二）网络平台监管责任的具体设定

不同的平台类型，所涉法律关系主体关切的利益类型、考量因素均有所不同。譬如对于社交平台，注重的是对表达自由和个人隐私的维护，通信平台则会涉及对通信秘密的保护问题。不同种类网络平台在技术特征、商业模式和服务内容上均具有差异，这些差异对其法律责任具有显著影响。正是基于该规则，域外国家对于网络平台监管义务采取新型立法模式，即对特殊类型的网络平台进行专门化立法。"世界范围内各国立法存在一个普遍趋势，即以业务为标准，将网络中的行为主体做类型化区分，与之匹配相应的权利义务以及法律责任。"[①]与这一世界主流相比，我国当前的法律规定对于网络平台的类型划分尚不具有整体性和明确性，更遑论从类型化的角度形成网络平台法律责任"主体-行为-责任"的统一。因此，笔者认为，以提供的服务内容、商业模式为标准对于网络平台进行类型划分，并在考察不同种类网络平台功能特征的基础上对其设定具体化、专门化、特殊化法律责任乃是我国现行涉及网络平台立法规范的当务之急。

1. 去中心化的网络平台的监管责任

① 王华伟：《网络服务提供者的刑法责任比较研究》，载《环球法律评论》2016年第4期。

这类平台责任，美国的Napster案[①]可资参考。Napster是第一个被广泛应用的点对点P2P音乐共享服务，其开发的软件可以把音乐作品从CD转化成MP3的格式，同时它提供平台，供用户上传、检索和下载作品。在Napster案中，联邦地方法院认为尽管Napster的服务是免费的，但是通过进行侵权不断增加用户数量的行为将会给被告带来直接经济利益和潜在的商业利益，包括链接到特定商业网站的指定邮件、定点广告和委托。如果网络服务提供者仅对用户一次性的收取入门费用，或根据使用的时间长短或信息的传输量按照固定的费率进行收费，那么即使其用户实施了侵权行为，网络服务提供者也不承担替代责任。但是，如果网络服务提供者进行收费的行为与侵权内容相关，那么就应当承担侵权责任。[②]

2. 网络搜索平台的监管责任

搜索平台涉及的法律问题主要包括排名问题，关键词侵害他人商标权问题，使用搜索引擎搜索到的结果信息中含有涉嫌侵害他人名誉权、隐私权或知识产权问题。前述魏则西案即涉及到竞价排名问题。竞价排名，是指客户为自己的网站页面购买在搜索引擎中的关键字排名，而搜索引擎按点击（或时间段）对它们进行计费的一种服务。按照目前竞价排名的工作原理，任何个人和企业都可以在网上申请开户参与竞价排名，而且关键字的设置和排名费用完全由客户自主决定，网络平台只进行简单的审核。审核完毕缴纳开户费之后，企业就可以运用竞价排名来推广自己的产品。由于平台以收取费用的多少作为排名次序的依据，而非根据自然算法来排序，因此构成实质上的广告发布者，在享有广告发布者的权利的同时，也应承担广告发布者的义务。

3. 网络交易平台的监管责任

这类网络交易平台存在的主要问题是：平台的入驻商户销售假冒他人商标的商品、假冒伪劣商品、质量不合格商品，网络交易平台是否应当承担法律责任？对此，我国司法实务部门一般是持否定态度。例如，在相关案件中，法院认为："淘宝平台虽拥有庞大的用户群体，但仍属提供一般服务性质，显然不属于公共服务企业或者准公共服务企业，不可仅据此而要求淘宝公司在平台规则的设立、执行等方面与公共服务企业具有同等或类似的高度注意义务。淘宝平台的规则合理与否，乃至其相应程度，应交由淘宝用户予以体验和评价，司法应对此给予足

① A&M Records v. Napster,239F.3d 1004 (9th Cir,2001)
② Senate Report 105, at 44.

够的尊重和空间，而不应强行介入，否则，商事交易主体的私权利内容和处分意志将极大压缩，鼓励交易、尊重交易的司法导向亦将严重褪色。"[①]

本文则认为，对此问题，需要区别对待，具体问题具体分析。淘宝网并不是为所有的淘宝卖家提供广告位，与其有广告合作的卖家，可以视为淘宝平台从卖家的商品或者服务中获得收益或者说是变相获得收益，作为在其平台上要发布的广告，淘宝应当对产品和服务进行审查。同样，淘宝平台对一般的卖家，通过信用等级体系进行评价，但该体系基本依靠交易量和买家的评价来完成，淘宝平台并不对其进行过多的干预。而淘宝对其"金牌卖家"的认证与此不同，对信用等级、交易额、纠纷率、违规处罚、售假处罚等条件进行考核。因此，对于此类商家，平台应当承担相对于普通商家更多的管理义务，这是因为，一方面平台以自身的信用向消费者提供了认证和担保，另一方面淘宝确实在认证过程中有条件对商家行审核和管理。

总之，网络平台经营者虽然没有一般监管义务，但是在特殊案例中却有一定的注意义务。如果在平台上有违法侵权行为发生，网络平台经营者应当尽可能采取预防措施，阻止同类违法侵权案件再次发生。对此，国外的有关案例值得参考。例如，L' OREAL诉eBay案。该案的基本案情为：原告系化妆品和香水领域知名商标的权利人，其销售模式为封闭式的许可经营，被告eBay经营一家全球性的网购平台。原告发现，有商家在被告经营的网站上未经商标权人同意向欧盟国家销售带有原告商标的商品，其中部分商品仅在第三国家许可销售。此外，被告还使用了Google的关键词广告服务，当搜索服务的使用者输入与原告相关的关键词时，将被导向被告网站上从事商标侵权行为的上述商家。原告认为被告参与了其用户从事的商标权侵权行为，要求其承担相应的责任。对此，欧盟法院指出，网购平台提供的服务如果仅是便于其用户在其经营活动中展示自己带有商标的商品，则不能认为网络平台自己从事了使用商标的行为。但是，如果为用户的销售行为提供了帮助（此时用户必须从事的是商业活动），如果为其商品的展示进行优化设计及为商品的销售进行广告宣传（如使用Google的广告服务）等，则等于是在用户的商标侵权行为中充当了"积极"的角色，此时《电子商务指令》的免责规则无法适用。即使网购平台没有发挥积极的作用，如果其知道相关事实，

① "蔡振文诉淘宝公司网络服务合同纠纷案二审判决书"，广东省佛山市中级人民法院民事判决书([2016]粤06民终3872号)。

根据这些事实，一个理性的经济人可以推断违法行为的存在，并且在其知道相关事实后没有不延迟的删除或者屏蔽相关信息，则同样不能适用免责。此外，欧盟法院还指出，成员国法院应当要求网购平台采取措施以查明其作为卖家的用户的身份。即使存在对个人数据保护的必要，只要其用户并非以私人身份活动，则必须保证其身份是易于查明的。此外，成员国法院还应当要求网络平台采取措施阻止具体的侵权行为，且避免以后发生同一种类的侵权行为，这一措施不仅应当有效，且应符合比例原则，同时也不能给合法的商业行为造成阻碍。[①]

[①] EuGH，GRUR2011,1025-L'OREAL/eBay

网络平台犯罪的政策调适与刑法应对

魏东　悦洋*

（四川大学法学院）

内容摘要：网络平台商业模式在重塑全球商业格局的同时也催生出病毒式增长的平台犯罪，网络平台第三方责任犯罪的治理成为重要命题。域内外治理模式殊途同归，以政府的综合管制为主导力量，通过对平台的强力管控，挥舞起网络空间的权力之旗，同时寻求更为广泛的非法律解决模式。在我国的法律解决模式的最后一道屏障——刑法中，刑法理念的冲突亟待调适，网络风险刑法在立法模式、功能体系、规范构造等方面的教义化进程也跟进不足。网络平台犯罪未来的刑法应对应当能动、理性和多元，对于典型犯罪，传统的刑法观念依然有效；对于个性显著的新型风险，正确认识风险社会中“再造制度”的正当性和必要性；探索前置处罚、犯罪链条切断、非实行行为实行化、义务设置等关键问题的科学性，内在协调预防性刑法观与刑法的谦抑精神。以预防性刑法观为规制理念，我国刑法立法模式还必须做出重大调整，才能兼顾刑法的稳定性和适应性，回应社会发展要求。

关键词：网络平台犯罪　预防性刑法观　修正保证人义务

引言：网络空间中，和提供网络服务的个人相比，当平台服务者和犯罪行为结合时，平台服务者实施犯罪行为的能力和产生的危害性显然更大。随着网络代际3.0时代的到来，网络平台因其枢纽地位成为网络安全控制的重要节点。从发生学的角度观察平台经济的发展与网络平台犯罪的演化，可以得出哪些基本结论？我国的网络平台犯罪的综合治理措施在借鉴吸纳全球经验的基础上有哪些新发展？未来政策调适的重要内容有哪些？网络平台犯罪的刑法观念和法理阐释有哪些新变化？刑法应当如何应对？ 这些问题越来越突出地呈现在我们面前，亟需我们给出有理有据的答案和有效的解决方案。

根据唯物史观，经济关系在社会历史变迁中具有决定性作用，只有研究和把

* 作者简介：魏东（1966.01—），法学博士，四川大学法学院教授、博士生导师；悦洋（1978.11—），法学博士，四川大学法学院党委副书记。

握住这种关系才能揭示出社会历史发展的动力。在过去的十多年中，利用网络平台业务模式的企业在规模和领域上都有了显著的增长和扩展。网络平台商业模式已从社交、旅游、书籍或音乐进入运输，银行甚至医疗保健和能源领域；平台生态系统正在通过产品、服务和业务流程的数字化获得发展，并在此过程中重塑全球格局。与此同时，网络平台也具有破坏性。人们开始普遍关注网络平台的支配地位带来的高度的滥用可能性，以及由于处理私人数据的不太透明带来的社会风险。

一、网络平台犯罪的生成机理与发展趋势

网络平台的概念和法律责任在我国法律、行政法规和司法解释中尚无明确、统一的界定，在学理上也无定论。在电子商务领域，2019 年 1 月 1 日施行的《中华人民共和国电子商务法》第九条规定，电子商务平台经营者，是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。推而演之，网络平台是将两个或者更多有明显区别但又相互依赖的利益群体整合在一起，并为之提供共同的解决方案，以降低交易成本，提高网络价值的制度安排形式。[①]

（一）网络平台的特征与网络平台犯罪的生成机理

网络平台的特质在于：组建市场，具有明显的集聚和开放性；制定规则，但不参与核心价值的创造；搭建了一个相对独立的网络场域。同时，网络平台还是不断发展变化的，其蓬勃发展的根本动因在于网络效应的存在：随着越来越多的用户使用它们，平台变得更有价值，进而对潜在的新用户变得更具吸引力。网络平台的具体类型除了单纯以技术、产品或服务充当促进不同用户，买方或供应商之间交换或交易的管道或中介的交易平台，如美团、Uber；还有既提供交易管道也提供创新生态系统的集成平台，如 Apple 等公司，它不仅有 App Store 等交易平台，也有支持平台内容创建的大型第三方开发者生态系统；以及既提供技术也提供内容的混业经营模式平台，如淘宝和亚马逊商城。

与此同时，平台经济的暗面——网络平台犯罪同样在网络效应的催生下呈现病毒式增长。网络空间的隐蔽性、网络技术的先进性、网络传播的快捷性和网络

[①]崔晓明、姚凯、胡君辰：《交易成本、网络价值与平台创新——基于 38 个平台实践案例的质性分析》，载《研究与发展管理》2014 年 6 月，第 26 卷第 3 期。

平台的高度聚合性耦合在一起，给犯罪人提供了易于藏身之地和反侦查技术能力，且能够轻松地实施“一对多”“职业化”“持续性”的犯罪行为，实现社会危害性的聚拢和强化。平台越是高度聚合，越是裹挟着大量的法律风险。

从网络平台犯罪主体的角度看，网络平台犯罪可以分为三类。一类是以平台为名，专门实施犯罪行为的“伪”平台。如伪装成正规平台的钓鱼网站，是当前网络诈骗的主要工具，境外彩票、虚假购物、假冒银行是钓鱼网站主要的模仿类型。第二类是正规平台独立实施犯罪行为。如采取混业经营模式的交易平台，在提供交易场所的同时也作为卖售者成为交易的一方，在交易中发生的销售伪劣产品或者对商品、服务作虚假宣传的犯罪行为。“魏则西事件”暴露出的百度搜索的法律责任问题也应当纳入此类讨论之中。作为国内最大的信息搜索引擎平台，却隐瞒竞价排名、付费搜索的事实，导致信息网络的搜索者尤其是弱势群体陷入严重的信息不对称、误判或其他更严重的后果。这种人为干扰信息搜索的进程，深度介入了信息发布的过程，涉嫌虚假广告罪。“快播案”从判决结果看也属于网络平台独立实施犯罪的行为。法院认为，被告人以牟利为目的，在明知自己提供的网络服务被用户用于传播淫秽视频的情况下，仍然予以放任，导致大量淫秽视频在互联网传播，构成传播淫秽物品牟利罪。[①]不过，本文认为“快播案”的问题应当属于第三类：网络平台作为网络场域的搭建者，明知而帮助他人实施违法犯罪行为的犯罪行为，本文称为网络平台第三方责任犯罪。

（二）网络平台犯罪的发展趋势与未来模型

平台经济并非一蹴而就。在我国网络平台经济 1.0 阶段（2000 年前后开始），平台多体现为信息交流搭建的技术平台，以用户生成内容的 UGC 平台（User Generated Content）为主。在我国，门户网站以搜狐为典型代表，电商网站以淘宝为典型代表。以平台为主导的犯罪彼时并不突出。按照网络在犯罪中发挥的作用为标准，网络平台犯罪可分为以网络平台为犯罪工具的犯罪和以网络为犯罪空间的网络平台犯罪。[②]平台经济 1.0 阶段的网络平台犯罪主要表现为以网络平台为犯罪工具的犯罪，如传统的诈骗、盗窃、侵害知识产权类犯罪通过网络予以实施。

[①]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》，载《中外法学》2017 年第 1 期。
[②]参见于志刚、郭旨龙：《网络刑法的逻辑与经验》，中国法制出版社 2015 年版，第 1-27 页。作者分类还包括以网络为犯罪对象的网络犯罪。笔者认为，以网络为犯罪对象的犯罪严格说来并不是网络犯罪，而是计算机犯罪，故未纳入。

在网络平台经济 2.0 阶段（2008 年前至 2015 年前后），随着网络技术的不断发展，平台不仅提供技术，还提供一定的市场条件和交易规则。搜索引擎、电子商务、社交网络、网络游戏等领域的领先格局基本形成，平台的价值核心逐渐由搭建信息平台转向商业生态建设。以网络为工具实施的传统犯罪在这一阶段爆发式增长，网络因素几乎介入到所有传统犯罪当中。危害行为和技术的多维融合逐渐孕育出真正的、具体的、全新的法益种类(如数据等网络财产)和犯罪类型(信息战、网络恐怖主义、垃圾邮件)。同时网络空间本身承载着同样重要的各种社会管理秩序，这些法益在网络空间中就能够被“完结”，行为结果不需要“落地”就能达到传统现实空间类似行为的同等效果[①]，裂变出以平台为主导的犯罪，如专门的犯罪平台、利用平台实施的网络诈骗、非法集资、淫秽内容传播、网络造谣等。2016 年影响互联网第一案“快播案”标志着司法对平台经济 2.0 时代纯网络平台犯罪的清算与警示；立法上设立的新罪名“拒不履行信息网络安全管理义务罪”被认为是第一个以特殊主体建立网络服务提供商“平台责任”的立法。[②]

网络平台经济 3.0 阶段（2015 年至今），我国的网络平台经济已经完成从效仿到自主创新，从落后到领先的快速发展历程。网络平台与传统产业融合加速，平台不仅提供技术、提供市场条件而且还参与经营活动，出现大量的混业经营模式，在垂直领域出现平台独角兽企业。[③]由于“平台+组件”的模式足以横扫一切商业模式，以网络平台为犯罪工具的犯罪态势不减，网络空间内的纯网络犯罪逐渐增多。高危运行的网络平台社会风险主要包括：海量商事主体经营行为治理，如假冒伪劣、虚假宣传、非法集资、网络诈骗；自媒体时代的信息内容治理，如谣言、恐怖主义信息、低俗内容、网络赌博、网络传销；互联网平台企业滥用市场支配地位的平台垄断与竞争行为的治理；数据安全及合规利用的治理；自然人主体的税收征管治理；平台型就业的劳动关系治理六大类。[④]其中，在刑事领域，商事主体经营行为治理、信息内容治理、数据安全成为突出问题。在所有的网络犯罪中，与以上高危刑事风险交织发展的由网络平台主导的三种犯罪类型也同时存在：“伪”平台专门实施犯罪行为、正规平台独立实施犯罪行为、网络平台第

①参见魏东、金燚：《网络犯罪魔变中的刑法理性检讨》，载《刑法论丛》总第 50 卷，2017 年第 2 卷。
②参见于志刚：《网络空间中犯罪帮助行为的制裁体系与完善思路》，载《中国法学》2016 年第 2 期。
③参见杨乐：《揭开网络平台法律责任的面纱》载腾讯研究院著：《网络法论丛》（第二卷），中国政法大学出版社，2018 年 1 月版，第 21 页。
④参见《2017 年互联网治理白皮书》，中国信息通讯研究院 2017 年 12 月印制，第 13-17 页。

三方责任犯罪，其中，前两类犯罪行为仍是主要模态。

从发生学的角度观察平台经济的发展与网络平台犯罪的演化，可以得出的基本结论是：网络平台犯罪和平台经济的代际变化高度融合，相生相伴。尽管平台从本质上仍属于聚合信息的通道，但由于其设计程序、提供算法规则，拥有一定的技术能力去引导、塑造交易规则，从而对平台内的经济、社会活动具有一定的控制能力。[①]备受关注的人工智能伦理，数据治理，自动驾驶，网络中立，版权改革，区块链监管，算法歧视，假新闻，以及数字正义等无一不与平台发生紧密的关系。随着平台规模的进一步扩大和前沿科技的扩步前进，网络平台主导的犯罪也将进一步增长和魔变，可以预见的以网络平台为主导的犯罪中，“伪”平台专门实施犯罪行为和正规平台独立实施犯罪行为仍将继续存在；去中心化带来的大量分散、隐蔽的网络用户已经是政府很难控制的对象了，作为网络空间的重要枢纽——网络平台第三方责任犯罪的治理成为重要命题。

二、网络平台犯罪的综合治理与政策调适

“伪”平台专门实施犯罪行为和正规平台独立实施犯罪行为实质上属于传统犯罪的主体异态，是加害与被害二元结构的教义学阐释，刑事责任的认定与在现实空间并无特殊之处。真正导致传统刑法体系陷入一定失灵状态的情况是网络平台第三方责任犯罪。面对高发态势的网络犯罪，没有平台可以底气十足地声称互联网站只是纯粹的技术平台。不过，尽管平台拥有一定的控制能力，但这种控制能力并非体现在详尽审查某项具体交易上——对此，它们仍然是消极的、中立的；它所拥有的能力更多体现在程序设计和“算法”上。与平台本质不符的监管规则既无法解决问题，反而可能导致对互联网创新能力的压制。[②]这正是网络平台犯罪治理的最大难题。在网络平台犯罪综合治理模式的不断调整中，安全与发展始终交织博弈；如果没有相对完善的综合治理设计，法律政策的制定也将踯躅不定，裹挟难前。

（一）域内外网络平台犯罪的综合治理进程与基本模式

在线平台的产生在组织我们的生活、社会和经济等方面，扮演着越来越重大的角色；其繁荣发展，一方面得益于技术创新，另一方面有赖于互联网发展早期

①参见赵鹏：《论私人审查的界限——论网络交易平台对用户内容的行政责任》，载《清华法学》2016 年第 6 期。
②赵鹏：《论私人审查的界限——论网络交易平台对用户内容的行政责任》，载《清华法学》2016 年第 6 期。

制定的“避风港”规则。以美国和欧盟为代表的早期互联网立法，以保护国家创新能力为战略目标，紧紧围绕网络服务提供者责任的限制或豁免而展开，平台利益往往占据上风。[①]如今，随着网络平台的横向扩展和纵深发展，呈现高发态势的网络犯罪促使各国逐渐调整立法策略。仇恨言论、恐怖主义和极端主义言论成为平台治理的关注核心，不少国家在互联网管理和控制方面已初步达成共识，从国家发展战略高度加强顶层设计，制订各具特色的网络安全防护体系。对平台的规制正在从“避风港”向“平台治理”转变。

平台经济的发展同样驱动着我国的上层建筑。回顾我国互联网监管的历史进程，和美国、德国等国家从一开始以追究网络用户责任为重心、以网络用户为治理核心的制度模式不同的是，我国的监管路径是不仅管理网络用户的行为，也重视通过网络服务提供者来间接控制网络用户的行为，可归结为“网络用户+网络服务提供者并行管控模式”。这种模式的特点是在规范用户行为的同时，也将消减网络不法的希望寄于网络服务提供者，试图通过制度设计来促使网络服务提供者积极采取措施来应对网络中的不法现象。[②]可以说，在我国的互联网监管中，网络平台自发展起步时起就承担了网络治理的协助管理义务，并随着平台经济的发展不断得到强化。

时至今日，域内外针对网络平台犯罪的综合治理进程可以说是殊途同归。无论是从“萌芽期”的鼓励促进发展到“爆发成长期”的规范发展警惕风险，还是从成长之日起的一路并行监管，作为解决网络不法的关键主体，网络平台的责任不断走向严格化，最终走向“成熟期”的健全监管。从域内外实践来看，各国都在逐步调整治理格局，把市场、社会等多方的力量纳入治理体系，突出技术治理等柔性治理方式的重要性，寻求更为广泛的法律与非法律的解决模式。

在法律解决模式方面，包括平台在内的网络服务提供者的责任肇始于版权领域，经历了扩大到知识产权领域，再推广到整个民事侵权领域，最后及至行政、刑事领域的过程。其中，政府的综合规制是网络空间治理的主导力量。在网络服务提供者和用户的维度上，尤其是网络服务提供商因其独特的商业模式以及营造生态和发展市场的商业需求，对平台上的各类主体具有天然的管理优势，传统国

[①]Julie E. Cohen, *Law forthe Platform Economy*, 51 U.C.D. L. Rev. 133 (2017), Page171\172.
[②]参见徐伟：《网络服务提供者侵权责任理论基础研究》，吉林大学博士学位论文，2013 年，第 131-140 页。

家在网络空间的去中心化和平台在网络中的中心化互为表里，共同推动国家将规制权力向平台让渡。[①]在美国和欧盟，要求包括网络平台在内的不同主体“分担责任”成为网络治理的基本原则之一；网络平台必须承担相应的社会责任和法律义务[②]或要求平台提供商对其创建或推广的敌对环境负责[③]。欧盟 18 年以来的平台治理举措包括三个方面：一是建立有效打击在线违法内容的措施；二是在线平台交易的公平性和透明性规制；三是算法透明。[④]2017 年 5 月，Facebook 首席执行官马克·扎克伯格（Mark Elliot Zuckerberg）宣布在全球范围内招聘 3000 名员工，他们将加入 Facebook 现有的 4500 人内容审核团队，监测与暴力和犯罪行为有关的视频、帖子，以阻止悲剧的发生。Facebook 之所以一改“中立平台”的坚持，转而致力于使自己的网站成为“对恐怖分子来说非常敌对的环境”，正是与日益严峻的国家规制密切相关。[⑤]平台经济崛起的背景下，网络平台已经不能通过声称自己是信息渠道而非出版者来豁免责任了。

我国对网络安全的监管尽管起步晚于美国、德国等，但监管的步伐从未停止。随着网络安全威胁的加剧和网络技术的不断发展，在不断吸纳国际先进经验的基础上，行政规制措施也在不断升级和扩张。现有的法律、行政法规和部门规章对于平台服务提供者的主动监管，已经课以了相当数量、足以涵盖整个网络服务提供全过程的行政义务。其中，针对网络交易、食品外卖、网约车、信息服务、电子商务等与公民生活密切相关的网络领域还制定了专门的法律法规赋予网络平台行政义务，如《网络零售第三方平台交易规则制定程序规定（试行）》《网络食品安全违法行为查处办法》《网络预约出租汽车经营服务管理暂行办法》《互联网群组信息服务管理规定》《微博客信息服务管理规定》《电子商务法》。在行政监管的具体运用中，准行政行为——“约谈”成为最为频繁的监管手段之一。

在刑法的规制模式方面，对于网络平台刑事义务的建构，各国模式各有侧重。包括：（1）没有为网络平台设置法律义务的国家，多通过积极作为

[①]许可：《网络平台规制的双重逻辑及其反思》，腾讯研究院著：《网络法论丛》（第二卷），中国政法大学出版社，2018 年 1 月版，第 312 页。
[②]参见周汉华：《论互联网法》，载《中国法学》2015 年第 2 期。
[③]KrisAnn Norby-Jahner, *Minor Online Sexual Harassment and the CDA Sec. 230 Defense: New Directions for Internet Service Provider Liability*, 32 Hamline L. Rev. 207 (2009).
[④]曹建峰：《2018 年互联网法律政策趋势十大关键词》，腾讯研究院：https://mp.weixin.qq.com/s/NQo9157MMjMzcy52uSELlA，最后访问日期 2019 年 1 月 21 日。
[⑤]参见许可：《网络平台规制的双重逻辑及其反思》，腾讯研究院著：《网络法论丛》（第二卷），中国政法大学出版社，2018 年 1 月版，第 312、313 页。

产生的共犯责任和不作为产生的刑事责任的归责路径对网络平台予以规制。在法国，学说和判例是否定不纯正不作为犯的，对于有处罚必要性的网络服务提供者的不作为，是通过将提供基础设施服务、托管服务、存储服务等技术性行为本身解释为一种积极的作为行为来实现的。[①]（2）在特殊领域进行专门的立法规制。在西方国家中，德国是第一个对网络有害言论进行专门立法规制的国家，也是第一个规定可以对传播违法网络言论的网络服务提供商进行定罪的国家。德国2017年10月1日实施的《改进社交网络中的法律执行的法案》强化了政府对社交网络平台行业自律的监管，设定了社交网络平台的行政处罚机制，并与《刑法典》衔接流畅，直接转引《刑法典》的规定，调整违反刑法的仇恨言论、煽动性言论和虚假新闻造谣三个部分，避免了法律用语的不协调。[②]英国2017年生效的新《数字经济法案》，在线版权侵权的最长刑期从2年增加到了10年，还涉及网络监管的各方面。[③]（3）个别性条款和特殊义务的赋予。美国法在特定的法律领域存在大量的个别性条款。在刑事责任方面，根据相关案例，第230条的免疫力也是有限的，如果检察官提出的指控位于230（e）的例外——如促进卖淫，和儿童性剥削有关的服务，网络服务提供者的刑事责任仍然不会得到豁免。[④]美国法律中还能看见超越了责任条款的网络服务提供者的特殊义务，如《友好家庭互联网接入法》《互联网自由与儿童保护法》规定的提供过滤软件的义务；《性侵儿童保护法》规定的报告违法行为的义务；禁止罪犯使用互联网的义务等；对于这些特殊义务履行与否的抗辩，表现为网络服务提供者是否提前要求了使用信用卡或者提供未成年人的身份证号码。除此之外，对于出于商业目的，明知信息中含有对未成年人有害的内容，而将相关信息提供给未成年人的，网络服务提供者需要承担相应的责任。[⑤]（4）传统新闻出版领域责任的运用。欧洲个别国家在解决网络服务提供者为第三方行为承担的共同责任问题时，回归了传统的新闻出版领域，将新闻出版者和编辑的“级联责任”运用到网络服务提供者的责任判断

[①]参见【德】乌尔里希·齐白著，王华伟译：《网络服务提供者的刑法责任——刑法总论的核心问题》，载赵秉志主编《刑法论丛》2016年第4卷，总第48卷，第195-196页。
[②]参见贾茵：《德国<网络执行法>开启“监管风暴”》，载《网境纵横》2018年第2期。
[③]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》，载《法学评论》（双月刊）2016年第3期。
[④]Shahrzad T. Radbod, *Craigslist - A Case for Criminal Liability for Online Service Providers?*, Berkeley Technology Law Journal, Vol. 25, No. 1, ANNUAL REVIEW OF LAW AND TECHNOLOGY (2010), pp. 597-615.
[⑤]参见【德】乌尔里希·齐白著，王华伟、吴舟译：《比较法视野下网络服务提供者的责任》，载陈兴良主编：《刑事法评论·犯罪的阶层论》，北京大学出版社，2016年6月版，第211-213页。

之中。瑞典1998年关于“电子布告栏”的法案就存在比较严格的责任标准。除了通常的“通知+删除”义务外，电子布告栏的服务提供者需要监管服务的范围和目标，尤其是商业性的提供者。行为人如果故意或严重疏忽地违反义务处罚最重可达到2年有期徒刑。[①]

在我国，《刑法修正案（九）》第28条、第29条增设的拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助信息网络犯罪活动罪第一次对网络服务提供者的刑事责任进行了规定。有学者认为，拒不履行信息网络安全管理义务罪的设立，开创了政府和网络平台在网络犯罪领域的合作治理。[②]

在非法律的解决模式方面，行业协会的作用和网络服务提供者的自我规范在国外倍受重视；新技术的研发和运用不断发展，如过滤软件的安装、发展追踪罪犯的技术手段、犯罪预警手段尤其是恐怖犯罪、针对未成年人和儿童的违法犯罪行为以及建立年龄核实、过滤和评级系统等。我国的行业自律也在监管推动下萌芽发展。2018年5月实施的个人信息保护领域的推荐性国家标准《信息安全技术个人信息安全规范》，明确了个人信息的收集、保存、使用、共享的合规要求，为网络运营者制定隐私政策及完善内控提供了具体指引。同月，中国银保监会发布《银行业金融机构数据治理指引》，将《规范》同步纳入银行业金融机构的合规标准体系；以《规范》为基础，中央网信办、工信部、公安部、国家标准委四部委继续推进隐私政策评审工作，评审选取了与人们日常生活紧密相关、具有较大用户数量的网络产品，通过隐私政策评审来引导企业提高数据处理透明度。

（二）网络平台犯罪的未来政策调适

当代犯罪学观已经走上从“消灭犯罪”到“控制犯罪”的理性轨道。犯罪观理性转变也推动刑法目的、刑法功能的科学化，为刑法理性参与社会治理与犯罪治理奠定科学基础：不是完全寄希望于刑法的高压、威吓以及惩罚，而是倡导动用所有的社会资源共同有效控制犯罪。[③]行政监管、行业自律、技术支持和法律保障将在未来的网络平台犯罪综合治理中继续组合协同，共同发挥重要的作用。

不过，在我国的实然状况中，网络平台犯罪的综合治理模式还未达到较为理想的状态，未来的调适方向包括：

[①]参见【德】乌尔里希·齐白著，王华伟译：《网络服务提供者的刑法责任——刑法总论的核心问题》，载赵秉志主编《刑法论丛》2016年第4卷，总第48卷，第201页。
[②]李本灿：《拒不履行信息网络安全管理义务罪的两面性解读》，载《法学论坛》2017年第5期。
[③]高铭暄、孙道萃：《预防性刑法观及其教义学思考》，载《中国法学》2018年第1期。

1、行业自律的扶持

我国的行业自律尚处于萌芽状态，还未发挥出积极的主导作用，缺乏制度化、规范化的管理，未能在国家监管和平台企业之间形成良好的桥梁和纽带，进而对平台企业的指导也不足；反而是平台企业自身，在与传统经济迥然不同的富有效率的竞争中，会去努力去改善与网络社会中其他节点的关系，有动力和需要开展企业自律。新浪、百度、优酷、爱奇艺等知名平台企业，针对视频信息服务，有的建立数百人之多的专门人工审查部门，有的投入巨资研发技术筛查措施。[①]应当说，这些都是互联网企业合法经营的必然选择，但理应发挥更大作用的行业自律却相形见绌了。这种状况的形成和我国国家权威主导的网络监管体制有较大的关系。政府是网络治理的主导力量，无论从政策制定到具体监管实践，政府都是监管规则的主要设计者和执行者，作为体现产业自治的行业协会也是在政府的领导下开展工作，[②]鲜明的强力权威特征在一定程度上压制了行业自律的发展。

2、技术支持的发展

技术支持还未尚不足以抗衡刑事犯罪的发生。尽管《网络安全法》已经明确了国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力，但现实的情况是，不同的平台拥有不同的经济规模和技术能力，再加上行业自律能量未得到释放，平台企业同仇敌忾地研发高新技术抵御高发犯罪态势还长路漫漫。

3、行政监管的科学化

行政监管职权重复、多头管理，监管效率低下却又机能过载。随着网络的去中心化发展，对于政府来说，大量分散、隐蔽的网络用户已经是很难控制的对象了。监管历史中，国家和地方层面对网络服务提供者承担内容监管的一般性义务的强调从未缺失且不断加强。但是，根据媒体统计，自《网络安全法》实施半年内，监管部门公开的执法案例共计 30 例左右，然而在同一时间段，中国互联网违法和不良信息举报中心受理的网民有效举报数是 3466.1 万件，数量悬殊极大。相关学者认为，这是职权重复、多头管理导致的两极反差：效率低下的同时又有

[①]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》，载《中外法学》2017 年第 1 期。
[②]参见王融：《中国互联网监管 20 年》，载腾讯研究院著：《网络法论丛》（第一卷），中国政法大学出版社，2018 年 1 月版，第 12 页。

机能过载。[①]于是针对网络犯罪的多发态势，国家每隔一段时间都要由多个部门和单位联合开展如“净网”“剑网”“清源”“护苗”等互联网治理专项行动，形成打击治理的强大合力，使网络乱象得到有效整治。[②]在“剑网 2018”专项行动中，搜狐、百度、今日头条、凤凰网、网易等大型门户平台均位列整改名单之中。[③]通过集中优势人力、物力，采取有组织、有目的、规模较大的“运动式执法”，在短期内收效明显，但始终是一种临时性的短期行为，且存在程序瑕疵。

值得注意的是，我国的法律法规、各类政策办法已经对网络平台课以了相当数量、足以涵盖整个网络服务提供全过程的行政义务。但这些规定自颁布以来，真正要求网络平台，尤其是大型平台企业对其用户内容承担责任的案例并不多见，监管部门更多是以潜在的制裁能力为后盾，通过约谈等方式促使平台采取符合监管要求的内部控制策略。[④]究其原因，在于监管规范存在一个事实上的真空：一般性、积极性的监管义务强调过多，监管义务过于严苛，并不契合产业生态和网络技术机构，导致平台责任规范难以真正落实。

未来，政府应当充分尊重网络平台产业的生态结构，繁荣发展行业自律机制，激励平台开发自身的信誉机制，与平台探索合作治理的有效路径，将监管要求与网络生态发展契合、同步。

4、刑法应对的观念更新与范式调整

网络时代与网络犯罪形态共同导致传统刑法体系陷入一定的失灵状态，传统刑法体系的网络化知识转型已经悄然启动。《刑法修正案(九)》对网络犯罪的修改，已经初步形成了当代刑法的一个新兴领域——网络刑法。不过，《刑法修正案(九)》实施三年以来，网络平台明知而帮助他人实施违法犯罪行为的犯罪行为被课以帮助信息网络犯罪活动罪和拒不履行信息网络管理义务罪的却屈指可数，与高发的网络平台犯罪态势形成极大反差。是刑法应对不足还是另有原因？与此同时，“快播案”虽已尘埃落定，但争议仍在继续，焦点集中于网络平台对用户

[①]参见马荣春、王腾：《拒不履行信息网络安全管理义务罪的适用困境与解脱》，载《山东警察学院学报》2018 年第 3 期。
[②]参见《向着网络强国阔步前行——党的十八大以来网信事业发展述评》，新华网 http://www.xinhuanet.com/zgjx/2018-04/20/c_137124212.htm，最后访问日期 2018 年 4 月 30 日。
[③]“剑网 2018 专项行动启动”，中华人民共和国中央人民政府网，http://www.gov.cn/xinwen/2018-07/17/content_5306954.htm，最后访问日期 2019 年 2 月 1 日。“‘剑网 2018’专项行动：搜狐凤凰等多家 APP 被勒令整改”，环球网，http://smart.huanqiu.com/roll/2019-01/13977923.html?agt=92，最后访问日期 2019 年 2 月 1 日。
[④]赵鹏：《论私人审查的界限——论网络交易平台对用户内容的行政责任》，载《清华法学》2016 年第 6 期。

的行为到底应当承担什么样的刑事义务的问题。

三、网络平台犯罪的刑法应对与法理更新

网络犯罪已成为我国第一大犯罪类型，刑法的回应是积极且明确的：增设拒不履行信息网络安全管理义务罪以确定网络服务提供者的平台责任；增设非法利用信息网络罪将网络预备行为作为犯罪处理；增设帮助信息网络犯罪活动罪以确定网络技术帮助行为的正犯责任，凸显了刑法介入的早期化意图。学者将这种立法现象称之为继《刑法修正案（七）》预防化立法迹象的进一步发展。[①]

（一）网络平台犯罪刑法应对的理论阐释

紧随预防化刑法立法而来的是预防性刑法观的理论观察，包括风险刑法观、积极的刑法立法观、预防性刑法观、功能主义的刑法观等，均试图对这一趋势进行理论解读和评判，认为犯罪圈的扩大并不必然违背谦抑性原则；[②]批判性的见解则认为预防性刑法立法存在“抵牾刑法谦抑精神”“社会治理的过度刑法化”“刑法新工具主义”“象征性立法”等诸多问题。[③]不容质疑的是，《刑法修正案（九）》的确扩大了实然的犯罪圈，这种扩大是否理性则取决于应然的犯罪圈。

1、犯罪事实的增量与刑法规范的扩张

社会变迁导致着犯罪现象的蜕变，网络空间的出现也扩充了犯罪孵化的领域。过去发生在实体空间内的犯罪借助网络技术的翅膀在网络空间中异化出新的、难以通过刑法的扩大解释、实质解释去规制的犯罪类型，决定了刑法规范的扩张。

前述网络平台犯罪的三种类型中，对于前两种以网络为工具的犯罪类型，尚可通过对法律规范的理解与诠释，释放法律的意义和外延，将新型犯罪事实纳入法律评价能力之内，但对于第三种类型，《刑法修正案（九）》之前的刑法规范已经难以应对。域内外，网络服务提供者刑事责任承担的理论探索一开始是以共犯的判断为起点的；但面对网络犯罪的异化，即便是更新传统的共犯理论也难以承担有效控制网络平台犯罪的任务。修法针对帮助信息网络犯罪活动的行为以及拒不履行网络监管义务的行为“完成了信息网络服务者帮助犯正犯化的规范建

[①]参见高铭暄、孙道萃：《预防性刑法观及其教义学思考》，载《中国法学》2018 年第 1 期。
[②]焦旭鹏：《现代刑法的风险转向——兼评中国当下的刑法观》，载《西南民族大学学报（人文社科版）》2018 年第 12 期。
[③]高铭暄、孙道萃：《预防性刑法观及其教义学思考》，载《中国法学》2018 年第 1 期。

构，从而有效地超越了在传统共犯结构下分析业务行为刑事归责的局限性”[①]。社会生活领域从实体到空间扩张，犯罪现象也从实体社会向网络空间发展，承载着社会防卫使命的刑法规范的变革及立法的活跃化是正常的反映。犯罪事实的增量决定了刑法规范的扩张。

2、社会风险的变化与刑法规制技术的变革

社会风险从发生根源上是内生的，伴随着人类的决策与行为，是各种社会制度，尤其是工业制度、法律制度、技术和应用科学等正常运行的共同结果。当代的社会风险在后果上具有延展性，在空间上则超越了地理边界和社会文化边界的限制，在时间上具有持续性，一旦风险变为实害将导致严重的后果。对于恐怖活动、毒品泛滥、艾滋病扩散、社会性冲突等风险，需要告别的观念是，现有的风险计算能力或行政机构和专家能够准确地预测、了解并告知社会成员应该如何去消除风险；现有的社会保险、经济补偿等制度也难以弥补风险实害带来的巨大灾难。有学者指出，中国已经进入了德国学者贝克（Ulrich Beck）所言的“风险社会”，主要特征是日益增多的社会问题或社会矛盾，但同时没有个人或机构明确地为这些事负责。[②]于是，如何缓解伤害与分配责任成为核心问题。另一方面，在复杂化、多层次的社会系统中，风险逐渐高涨、积累、隐蔽，社会成员的风险意识也在风险环境的变化下不断提高，渴望安全和安心，关注风险消除和危机管理，出现了希望公权力尤其是刑事制裁承当消除风险、管理危险的需求。[③]

针对预防性刑法立法本身，与其说是刑法观念整体从消极谦抑更新为积极主动，毋宁说是基于社会风险使然，在特定的法定犯领域，通过诸如非实行行为独立罪名化、危险犯的设置、证明标准的改变、责任承担的多元化等方式调整刑法干预风险的措施。在这些领域，刑法前置、发挥预防的效用明显大于事后的规制。一个粗糙的比较即是，对于故意杀人的行为，刑法没有必要专门去规定一个“预备杀人罪”；而对于危害性可能巨大的新型风险，如网络平台犯罪，刑法的确有必要调整控制手段，“从传统的后卫地带走向前沿地带，通过惩治行为人行为所

[①]刘宪权：《论信息技术滥用行为的刑事责任——〈刑法修正案（九）〉相关条款的理解与适用》，载《政法论坛》2015 年第 6 期。
[②]徐立成、周立：《食品安全威胁下“有组织的不负责任”——消费者行为分析与“一家两制”调查》，载《中国农业大学学报（社会科学版）》2014 年第 6 期。
[③]参见【日】関哲夫著，王充译：《结果无价值论与行为无价值论的对立及其趋向》，载《刑事法学》2017 年第 1 期。

带来的风险来实现对法益更为前置的保护”[①]。近年来的预防性刑法立法主要表现在恐怖犯罪、网络犯罪、腐败犯罪、食药品犯罪、环境犯罪、公共秩序犯罪几大类，大多属于对抗社会风险的法定之罪。未来针对人工智能犯罪等新型风险，也应当在预防性观念的指导下，前置于人工智能的研发、投放和使用。否则，一旦不加控制的超级人工智能进入社会，发生人工智能操纵人类的灾难性后果已经不是法律能够威慑的了。

因此，在风险社会的变化中，刑法的规制技术也必然发生变革，再造制度以应对风险，不再固化于事后惩罚，而是前置于犯罪实害或直接割裂犯罪链条的生成。

3、犯罪结构的更迭与刑法观念的更新

在风险社会与网络社会的交织下，犯罪现象的结构变化集中表现为法定犯的增量态势，兴起中的法定犯时代正在成为当前各国刑法共同面临的挑战与机遇，也决定刑法规范的同步更新趋势。[②]

通过对网络犯罪治理客观事实的观察，“社会刑法”理论或许提供了一个好的思路。根据社会刑法理论，不同于以社会契约为基础、强调人人平等的市民刑法，社会刑法正视社会的复杂化和多层次化，承认事实上的人人并不平等，或者同一个人在不同的社会关系中也会有不同的权利义务承担，因此对于不同的社会主体不应当配置同样的罪刑规范，而是以实质正义为目的，重视刑法调整多元社会的功能，对不同的社会主体或不同的犯罪配置不同的罪刑规范。[③]对于网络犯罪防控，网络服务提供者显然比网络用户更具有技术优势、经济优势和控制力量。尽管我们会追问“口袋深深深几许”，但“深口袋”在一定程度上仍然体现了大企业的社会责任。在对用户行为进行管理和规范的过程中，有的义务也只有网络服务提供商才能承担，以保障弱者的社会权，在一定程度上限制强者的自由权。在网络高度发达的今天，社会对危险的管理、统制的影响力不断减弱是客观事实；以责任(刑罚）个别化为显著标志的刑法，绝非防御或者控制风险的最佳手段[④]，但却可以发挥其功能性的作用。对网络服务提供者在一定程度上设定刑法上的责

[①]姜敏：《法益保护前置：刑法对食品安全保护的路径选择》，载《北京师范大学学报（社会科学版）》2013年第5期。
[②]参见高铭暄、孙道萃：《预防性刑法观及其教义学思考》，载《中国法学》2018年第1期。
[③]参见姜涛：《中国刑法现代化的未来图景》，载《环球法律评论》2013年第3期。
[④]卢建平：《风险社会的刑事政策与刑法》，载《法学论坛》2011年第7期。

任，是社会发展、实质公平正义对刑法的功能导向提出的要求。

法定犯的兴起使得传统刑法观念面临转变的瓶颈。社会形态的变迁必然导致犯罪现象的多元化，所有的犯罪类型并不是铁板一块，刑法观念的更新同样应当契合这种变化。对于典型犯罪、自然犯罪，传统的刑法观念依然有效；对于个性显著的新型风险、法定犯罪，预防性立法未尝不可。刑法以存在论为根基，向着功能主义、目的理性的方向蜕变，关注刑法系统内部的运作图景以及系统和环境的互动关系，才能实现理论和实践的知行合一。[①]这与刑法的谦抑原则也并不矛盾。谦抑原则并不意味着罪名越少越好，而是刑法的必要与否，必要性的检验无论是在典型的自然犯罪还是法定犯罪的设定之中都必须得到贯彻。

（二）网络平台犯罪刑法应对的限度反思

《刑法修正案（九）》增设的三个纯网络犯罪中，与网络平台“第三方责任犯罪”密切相关的是拒不履行信息网络安全管理义务罪和帮助信息网络犯罪活动罪。[②]

拒不履行信息网络安全管理义务罪以网络服务提供者为特殊主体，明确课以了网络服务提供者刑事义务。网络服务是网络用户行为得以进行的必要条件，因此提供网络服务的行为本身就已经构成了帮助。因此，帮助信息网络犯罪活动罪的落脚点在于“明知”，责任排除要件是采取必要措施—— “不提供帮助和支持”，实际仍是课以了网络服务提供者法定的作为义务。新设之罪的义务型犯罪属性由此显露无疑。刑法在整体上属于禁止性规范，要求人们不得做什么，而刑事义务的设定是命令性规范，是要求人们要去做什么。作为最严厉的法律，“要去做什么”本身就是对个人自由的强干预。如果没有坚实的教义学基础，预防性立法观本身所裹挟的对个人自由的不当侵害风险的确有异化为“过度刑法化”“新工具主义”的危险，因此必须进行限度的反思。

1、防止将义务型犯罪和支配型犯罪相混淆

支配型犯罪和义务型犯罪是性质迥异的两种犯罪类型，源于归责原理的根本不同。义务型犯罪刑事责任的基础在于对来自于国家整体法秩序形塑的特别义务

[①]参见姜敏：《系统论视角下刑法修正案犯罪化限制及其根据》，载人大复印资料《刑事法学》2017年第9期。
[②]为了及时有效的控制严重犯罪行为的发生，立法者将一些预备行为的可类型化要素规定为实行行为，规定了具有危险犯内核的独立犯罪。对于构成非法利用信息网络罪的行为人，原本就是具有可罚性的其他犯罪的预备犯，只不过为了网络犯罪防控的需要提前处罚，切断犯罪的因果流程。因此，非法利用信息网络罪并不特别指向网络服务提供者的刑事责任。

的违背，其法益侵害性主要体现在破坏国家和法律所保障的社会生活秩序。义务型犯罪的形成有政治、经济、社会政策的原因，而不是天然的、道义的原罪。如果网络服务提供者拥有的是由一种自然权利推导出来的义务——一般义务，那么这种义务就有很大的延展空间。但是显然这种义务是基于对法秩序维护的需求，是法秩序的要求落实到刑法实在法的规范，其义务边界和责任范围应是有限和克制的。因此刑法自身也必须恪守国家整体法秩序形塑的义务界限。也正因为义务型犯罪不同于支配型犯罪，义务型犯罪的主体并不能像支配型犯罪的主体一样能够现实地、具体地对某个领域的社会生活内容形成事实支配或控制，其保证义务的负担仅仅存在于制度的要求。和考夫曼明显的形式法义务痕迹的功能二分说的旧保证人义务、许乃曼以支配为统摄的新保证人义务相区别，义务型犯罪的刑事义务为修正保证人义务。

当致力于矫治罪犯和预防犯罪的刑事政策刑法化后，在适用刑法规范和刑法体系的过程中，刑事政策的目的性思考就应严格控制在刑法规范和刑法体系所许可的范围内，坚决反对逾越刑法规范与刑法体系而作刑事政策的考量。[①]修正保证人的义务首先来自刑法的规定，只有刑法规定的义务才能成为修正保证人的义务来源。对于刑法而言，保证义务应当具有刑法的属性，不能直接等同于民法或行政法规定的义务；因此，当刑法对于义务的规定在文本上采用了和民法、行政法文本相同的表述时，保证义务也不能就是文本上的义务，而应当去实质地探究具有刑法属性的保证义务。[②]对修正保证人实质义务的考察则应当建立在刑法规定的法义务基础之上。当修正保证人进入支配型犯罪的领域时，应当按照犯罪支配的路径考虑刑事责任；在支配型犯罪中，修正保证人成为一般主体。

因此，对于网络平台提供者而言，一旦平台中出现了犯罪行为，并不都涉及刑事责任的负担，而是要具体考虑该平台提供者是否违反了刑法上的修正保证人义务。如果将义务型犯罪和支配型犯罪相混淆，认为义务犯是支配了犯罪的流程，对犯罪结果的发生有完全的原因力，只会导致义务型犯罪的范围被不当地扩张至支配型犯罪，窒息社会发展的活力。义务型犯罪的因果性仅仅限制在不履行义务与结果之间的合法则关系上，义务型犯罪的因果无法涵盖以行为对结果具有现实的作用力为前提的因果概念，负有义务的行为人并没有操纵因果的发展流程，只

[①]参见邹兵建：《跨越李斯特鸿沟：一场误会》，载《外国法译评》2014 年第 2 期。
[②]参见唐子艳：《论不纯正不作为保证人的实质义务来源》，载《湖北社会科学》2015 年第 8 期。

是对既有的因果发展历程不予干预，听任潜在的危险转变为现实的危害。导致结果发生的因果流程并非不履行义务所开启，而是由独立于被期待的义务履行之外的情状所引发。[①]“当其他人在其公务领域内捣乱时，他凭借这个保证人地位，对采取措施负有义务”，“但是，这个不作为的实行人也只是以特定的义务地位为基础，这个地位使他成为在其职务范围内事务的保证人”。[②]因此对于因仅仅违反了修正保证人义务而为别人的犯罪提供便利的人，不能径直运用支配型犯罪的归责原则，认为行为人也支配了相关的犯罪，动辄采取共犯思维，有罪重罚，以实现报应为目的，过于重视对危险防控的作用。

2、防止行政机构责任和修正保证人义务的错位

围绕形塑网络服务提供者修正保证人义务的抽象制度，是国家整体法秩序的一个重要环节，它的不同侧面决定它不仅首先会成为民事法的内容，行政法的内容，也构成刑法的内容。但是，民事法、行政法、刑法对网络服务提供者的义务因不同的部门法任务必然有不同的呈现。如果不对刑法上的修正保证人义务进行限定，容易导致网络服务提供者的私法义务被公法义务所替代的危险。

网络服务提供者承担修正保证人义务的实质是行政机关面对互联网带来的海量信息监管难题形成的监管思路和监管方法。传统线下社会形成了行政主体与相对人二元均衡的状态，而互联网的出现打破了这种均衡，作为网络犯罪治理行动中的主导者——政府，根本无法承受监控每一个人犯罪的成本。在互联网监管领域，从传统新闻媒体“守门人”理论出发，到“谁办网谁负责”原则确立，政府逐渐探索形成了“以网管网”的监管思路，以网络服务提供者为抓手，通过管网络服务提供者来实现最终监管目的。但是，如果具体监管方法不是以导致什么样的具体损害作为实施制裁的前提条件，而是以一种弹性极大的模糊性危险为制裁的前提，就会造成慌乱或不安。拒不履行网络安全管理义务罪就使用了弹性极大的模糊性用语，如“致使违法信息大量传播的”“造成严重后果的”“情节严重的”；当监管委之以刑法的结果责任却又是这种弹性极大的规定时，公权力的合法让渡容易导致对自由的不当侵害。

网络服务提供者的义务是来自于公权力的让渡，而行政机关的责任是自始即

[①]参见劳东燕：《事实因果与刑法中的结果归责》，载《中国法学》2015 年第 2 期。
[②]【德】克劳斯·罗克辛著，王世洲主译与校订，王钲、劳东燕、王莹、李婧、徐晓辉译：《德国刑法学总论》（第 2 卷），法律出版社，2013 年 5 月第 1 版，第 83 页。

有。从法学或者政治科学的角度定义责任应该遵循其最本质的属性，坚持公和私的区分。如果行政机关一味地将自身的政治职责强加给经济主体，把行政机关的惰性和社会管理能力的低下引发的冲突，交给刑法去解决，这种责任分工的错位，最终只会窒息整个互联网行业的发展。另外，责任的错位还会导致两个后果：网络服务提供者不能有效管理、政府不能被有效问责。网络服务提供者对于网络用户的管理是“依合同治理”，传统的行政法控制机制，如要求对相关违法行为的处理建立在事实清楚、证据确凿并遵守正当法律程序的基础上，难以发挥作用[①]，并且违背了任何人不得为自己法官的基本程序正义原则[②]，网络服务提供者并不是最佳的不法行为判断者。

3、防止忽视刑法的远程效应

大公司的社会功能和社会伤害是并存的。社会科学定性容易，定量却难。“允许的危险”“信赖原则”“社会相当性”在适用边界上都不可避免地存在模糊问题，对法安全造成危害。刑法的适用稍有不慎，可能影响过大，涉及的人员过广。对于大型的平台公司，刑法的运用尤其要考虑远程效应，而不是仅仅着眼于当下的社会控制。如果对大型平台公司动辄追求刑事责任，是否出现“赢了官司、丢了市场，案件办了、企业垮了、劳动者失业了”的风险？且诉讼程序也会很复杂[③]。并且，如前所述，每一个平台企业拥有的技术水平并不是一样的，内生治理能力和成效差异较大，如何判断是否已经履行了网络信息安全管理义务？以及如果履行了网络信息安全管理义务，仍然造成了危害后果的，如何出罪？同时，在高度网络外部性的经济环境中，安全、信誉等因素对企业的长远发展非常重要。即使政府不出手规制，网络服务提供商自身也必然承担相应义务消减经济的负外部性，达到恢复效率的目的。网络时代下，是否具有良好的信誉对资源配置的调节作用被进一步放大。平台企业基于发展的考虑不仅会自发约束自己的行为，也会主动管理用户的行为。[④]如果刑法动辄出手控制，不考虑犯罪追究的后果径直扼杀经济体的自身调节能力，在长远来看，并不利于经济的发展。

（三）网络平台犯罪刑法应对的未来调适

[①]参见《互联网平台的行政法律责任》，中国法律评论：
https://mp.weixin.qq.com/s/kT3MEIyjlIDQryxEn2dFYw，最后访问日期 2017 年 11 月 13 日。
[②]参见龙宗智：《司法的逻辑》，载《中国法律评论》2018 年第 3 期。
[③]参见姜涛：《经济新常态和经济刑法体系创新》，载《法学》2016 年第 7 期。
[④]戚聿东、李颖：《新经济与规制改革》，载《中国工业经济》2018 年第 3 期。

三年前，随着“快播案”的热议，学界针对《刑法修正案（九）》新增罪名的代表性观点呈对立状态。有学者认为刑法此举是将网络中立帮助行为入罪化。拒不履行信息网络安全管理义务罪和帮助信息网络犯罪活动罪的涵摄性太广，分别从不作为和作为犯罪两个方面堵死了网络中立帮助行为的出罪路径，与德日刑法理论和司法实践的探讨和做法完全相反。[①]然而，来自实践素材的反馈证明，新罪名的实施并未发生学界曾经担心的状况，刑法安全保障的积极效能并未充分释放，难以匹配高发的网络平台犯罪态势。截至 2018 年 5 月，利用 OpenLaw 裁判文书检索工具，得到帮助信息网络犯罪活动罪已决案件 33 个，其中涉及平台犯罪的仅 3 个，拒不履行信息网络安全管理义务罪 0 个。然而根据猎网平台《2018 年网络诈骗趋势研究报告》，仅 2018 年，猎网平台共收到有效诈骗举报 21703 例，举报者被骗总金额超过 3.9 亿元，人均损失 24476 元，创近五年新高，较 2017 年人均损失增幅 69.8%。网络平台是骗子最主要的“作案现场”，包括利用电子商务平台的“兼职刷单”；抖音、快手等短视频平台的刷赞、虚假抽奖、网络借贷；交友平台上的财物诈骗等。[②]两极化的反差一方面说明我国的司法机关对于义务型犯罪的司法适用保持了必要的审慎，另一方面也暴露出刑法规范的供给失衡。这里既有刑法理念的冲突亟待调适，也有风险刑法在立法模式、功能体系、规范构造等方面的教义化进程跟进不足。

1、预防性刑法观与刑法谦抑精神的协调

在功能主义刑法观念之下的未来刑事立法，应当是能动、理性和多元的。[③]针对法定犯，尤其是义务型犯罪的规制，应当建立起不同于传统的自然犯罪、典型犯罪的规制理念和模式。在理念上，以预防风险为指导，正确认识风险社会中“再造制度”的正当性和必要性，在模式上，探索前置处罚、犯罪链条切断、非实行行为实行化、义务设置等关键问题的科学性。对于多中心的互联网平台，拥有监管权力的政府实则无法实现对互联网用户的监管，而平台对于细分领域的运行机理、问题出现的深层次原因、治理问题的具体对策等，有着更为精准的理解，只有通过平台承载主动监管的义务，才能真正实现对网络的管理，也才能真正实现

[①]参见刘艳红：《网络中立行为可罚性的流变及批判——以德日的理论和实务为比较基准》，载《法学评论》（双月刊）2016 年第 5 期。
[②]参见《360：2018 年网络诈骗趋势研究报告》，中文互联网数据资讯中心
http://www.199it.com/archives/822927.html，最后访问日期 2019 年 1 月 31 日。
[③]周光权：《转型时期刑法立法的思路与方法》，载《中国社会科学》2016 年第 3 期。

保护法益的目的。平台的开发和集聚性决定了平台上的犯罪涉及多种法益、罪行多样化、罪种复杂，从诈骗到危害国家安全无所不可能。对于恐怖犯罪的预防、儿童色情信息的监管等，必须置于平台服务提供者义务的前端，如果不在到达可能被侵害的人之前阻止信息的显示和传递，事后的监管就失去了意义。

同时在整体的解决模式中，刑法仍然是最后的环节。根据国家整体法秩序的要求机能地发挥刑法调节社会的作用，是社会发展、实质公平正义对刑法的功能导向提出的要求；但是必须进行严格的限制，防止出现刑罚积极主义所隐藏的法治危险。没有充分依据就动辄入刑不能达到预防犯罪的目的，只会破坏企业的安全感。有时候，刑法需要允许一定程度的“混乱”，不轻易出手。“快播案”在社会上引起的强烈争议一方面源于判决理由本身的牵强之处，另一方面也说明了社会对色情视频的潜在需求。理论研究上，应当紧紧把握住义务型犯罪和支配型犯罪的不同归责原理，严守罪与非罪的边界，使预防性刑法观与刑法的谦抑精神内在协调。

2、现有罪名的科学解释与运用

（1）修正保证人义务的类型化。现有治理网络平台第三方责任的罪名中，刑事义务的设置是核心。出于刑法立法技术的考虑，可以在条文规定中对网络服务提供者的类型、刑事责任等采取统括的规定方式，但在学理研究中、未来的司法解释中，仍应以技术属性和信息网络安全控制可能性作为网络服务提供者类型划分的基点，根据网络服务提供者在网络中所处的位置、拥有的技术属性、可能的控制力和控制程度设定不同的刑法上的义务，才能较为准确、合理的判断该网络服务提供者的刑事责任。

和内容服务提供者、技术服务提供者相比，平台服务提供者的特点在于不仅提供内容、服务，还搭建了一个虚拟场域，在这个虚拟场域中，平台服务提供者是游戏规则的制定者，是虚拟市场的组织者。在平台的服务过程中，服务提供者不可避免地会接触到用户的个人信息，也可以合法收集用户的个人信息。根据我国《网络安全法》第 41 条的规定，网络服务提供者可以在合法、正当和必要的情况下，收集用户信息；在收集前应当向用户明示收集和使用信息的目的、方式和范围并得到用户的同意。通过各种算法实现的数据交易、精准营销等蓬勃发展的电子商务的背后，正是网络社交带来的海量用户以及与之相关的实时、完整数

据，平台电商通过挖掘数据进而了解用户，不仅能够了解用户的基本信息，甚至能够分析用户的偏好和情绪。平台的开放性也方便了第三方企业“共享”平台已有的用户信息。不过，信息的收集、使用和共享也带来了危险。尤其是可以采用“第三方登录”方式使用的 APP，尽管方便了用户，但也对用户的隐私形成了威胁。如微信“附近的人”的功能，该功能是默认打开的，除非用户手动设置关闭。尽管还不涉及用户信息泄露，但不怀好意的陌生人因此便能掌握到用户的动态，形成潜在的危险。用户信息、大数据，成为资本关注的重点。因此，对于拥有用户信息的平台服务提供者来说，采取技术措施和其他必要措施，确保收集的个人信息安全，妥善地保管好用户信息，防止信息泄露、毁损、丢失是必须履行的义务，一旦发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。因此，对于平台服务提供者来说，确保用户信息安全是首要的修正保证人义务，而且是主动、积极的义务。未来的平台监管应是针对基于控制的个人数据保护，也许最大的挑战是定义数据的元结构以实现服务之间的实时通信，以及数据可移植性需要一个既灵活又牢固的通用标准。[①]因此，平台服务提供者的修正保证人义务包括两类，一是主动确保用户信息安全的义务，二是被动排除侵害的义务。

（2）修正保证人义务的明确化。拒不履行信息网络安全管理义务罪设置了网络服务提供者的刑事义务——信息网络安全管理义务。该义务很明显是直接转引了行政义务，并不当然成为刑事义务。真正的刑事义务是“经监管部门责令采取改正措施而改正”。这就导致了三个奇怪的后果，一是刑事义务的内容是履行特别的行政义务——改正，刑法罪名的设置竟成为行政监管的保障执行条款，在司法解释未对定量情节做出进一步限定的情况下，空泛的“改正”可能导致犯罪的膨胀也可能罪不当罚而难以适用；二是一旦当监管部门做出了责令采取改正措施的通知，网络服务提供者一般也会为了自身业务的存续和发展进行改正，有沦为恐吓性的“象征性立法”条文的可能；三是对于具有二次违法性的犯罪，行政前置一般是起到限缩入罪范围的作用，但并不明确刑事义务；但拒不履行信息网络安全管理义务罪的行政前置暗含了刑事义务的认定，且认定主体是行政监管部门。信息网络安全监管部门实质上承担了确认“信息网络安全管理义务”的内容。

[①]Magnus Westerlund; Joachim Enkvist, Platform Privacy: *The Missing Piece of Data Protection Legislation*, 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. 2 (2016).

否则，法院如何判断经监管部门的责令指向的是本罪行为人的修正保证人义务呢？但是这样一来，刑法上负担的义务的判断竟然是由行政机关来确认的。[①]拒不履行信息网络安全管理义务罪确立的网络平台责任意义重大，但立法本身的欠科学性导致该罪名并不好用。帮助信息网络犯罪活动罪是隐含的义务型犯罪，网络服务提供者是本罪的修正保证人，至于网络服务提供者是以积极作为的方式提供帮助，还是在服务过程中得知了犯罪行为而继续不动声色地提供帮助，并不影响义务型犯罪的归责，义务的边界同样需要明确。

拒不履行信息网络安全管理义务罪的入罪情节聚焦于“信息”，包括违法信息、用户信息、特定信息。结合行政义务的规定，网络服务提供者的修正保证人义务是主动监控网络信息的行政义务的不履行的改正。对来自第三方企业的、用户的违法信息或泄露用户信息的情况等，平台服务提供者承担着相对更多的行政监管义务。但是，对于处于消极司法法地位的刑法来说，广泛而能动的社会“管理”职能与刑法在社会治理中应有的基本功能是相抵触的，因此要以刑法手段保障行政义务的落实需要“经监管部门责令采取改正措施而拒不改正”的闸门，同时也需要行政义务的明晰。通过顶层设计建立信息网络安全的国家标准、行业标准，明确平台服务商的行为规范；违反相应国家、行业标准的行为和监管部门的特别命令相结合，才能更加合理地确认网络服务提供者行政义务违反的内容。[②]同时，在行政义务的设置中，要求网络交易平台承担对交易内容的主动监控义务还必须满足两个基本条件：一是判断违法的标准清晰，即监管部门能够提供明确的负面清单；二是判断违法的标准简单，即现有技术手段可以将上述标准设定入平台的程序，进而自动过滤。如果没有判断平台是否具有过错的标准，监管部门更可能根据后果的严重程度而非平台本身的过错来问责，从而会产生大量的问题。[③]这同样适用于以不作为形式实施的帮助信息网络犯罪活动罪的认定。

（3）入罪标准的明确化。基于义务型犯罪的特征，义务违反直接带来可谴责性，因此，明确的入罪条件需要予以标识。这些条件表现为抗拒履行义务本身的严重性、义务违反带来的严重危害结果等，通过这些客观条件的设置，只有对

[①]参见马荣春、王腾：《拒不履行信息网络安全管理义务罪的适用困境与解脱》，载《山东警察学院学报》2018 年第 5 期。
[②]参见马荣春、王腾：《拒不履行信息网络安全管理义务罪的适用困境与解脱》，载《山东警察学院学报》2018 年第 5 期。
[③]赵鹏：《私人审查的界限——论网络交易平台对用户内容的行政责任》，载《清华法学》2016 年第 6 期。

严重违反了义务的行为人才给予刑罚的制裁。这从大多数义务型犯罪的刑罚设置也能发现，即便造成了严重的后果，刑罚的设置总体上都比支配型犯罪更加轻缓。[①]义务型犯罪的行为不是从行为人的行为自由中内在地产生的，而是从外部强加给行为人的，其可谴责性根本上来自于对制度的违反，而不是直接指向制度背后保护的法益。对于义务型犯罪的刑法责难，应当保持最谨慎的态度而不至于对公民的自由干预过多。

因此，针对拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪里的“大量”“严重后果”“情节严重”等模糊的罪量要素，应当通过司法解释设置更为明确的标准，否则这些不明确的话语会直接导致这些罪量要素的消解。“拒不改正”的标准也需要明确。“拒不改正”和“不改正”在语义上有不同的涵义。后者是对事实的客观描述，而前者含有对行为人主观态度的否定评价。因此，对于网络服务提供者有所行动但并未完整履行责令事项的，如果有证据证明该网络服务提供者表面上的行动只是为了逃避处罚，实际上怠于整改的，比如经调查确有技术措施可以整改却无正当理由不使用的情况，那么可以认为是“拒不改正”。如果确因客观条件的限制没有改正完善的，则不应当认为是“拒不改正”。对于在限期整改的期限还未到达时，危害后果已经出现的情况，网络服务提供者不承担刑事责任。

3、立法模式的未来调整

未来网络平台犯罪的新型风险类型和态势，还可能对刑法不断提出新的要求。以预防性刑法观为规制理念，我国刑法立法模式必须做出重大调整，才能兼顾刑法的稳定性和适应性，回应社会发展要求。

（1）适当借鉴吸纳附属刑法与分散式立法模式的有益经验，在刑法典分则中设置专节规定网络犯罪。我国有学者指出，德国、日本等大陆法系国家的分散立法模式实践值得我国借鉴，把网络犯罪等行为类型复杂多样、变化较快的犯罪根据行业特色或专业依赖程度以附属刑法的方式，直接转引刑法典的规定，由此适应不同行业或专业领域内的快速发展和特殊要求，保持和行政监管的衔接流畅。[②]我国的《网络安全法》是第一部全面规范网络空间安全管理方面问题的基

[①]法定不作为犯的死罪比例大大低于其他犯罪，就有期监禁刑的配置而言，法定不作为犯的刑期也普遍低于其他犯罪的刑期。参见白建军：《论不作为犯的法定性和相似性》，载《中国法学》2012 年第 2 期。
[②]参见焦旭鹏：《现代刑法的风险转向——兼评中国当下的刑法观》，载《西南民族大学学报（人文社科版）》2018 年第 12 期。

否则，法院如何判断经监管部门的责令指向的是本罪行为人的修正保证人义务呢？但是这样一来，刑法上负担的义务的判断竟然是由行政机关来确认的。[①]拒不履行信息网络安全管理义务罪确立的网络平台责任意义重大，但立法本身的欠科学性导致该罪名并不好用。帮助信息网络犯罪活动罪是隐含的义务型犯罪，网络服务提供者是本罪的修正保证人，至于网络服务提供者是以积极作为的方式提供帮助，还是在服务过程中得知了犯罪行为而继续不动声色地提供帮助，并不影响义务型犯罪的归责，义务的边界同样需要明确。

拒不履行信息网络安全管理义务罪的入罪情节聚焦于“信息”，包括违法信息、用户信息、特定信息。结合行政义务的规定，网络服务提供者的修正保证人义务是主动监控网络信息的行政义务的不履行的改正。对来自第三方企业的、用户的违法信息或泄露用户信息的情况等，平台服务提供者承担着相对更多的行政监管义务。但是，对于处于消极司法法地位的刑法来说，广泛而能动的社会“管理”职能与刑法在社会治理中应有的基本功能是相抵触的，因此要以刑法手段保障行政义务的落实需要“经监管部门责令采取改正措施而拒不改正”的闸门，同时也需要行政义务的明晰。通过顶层设计建立信息网络安全的国家标准、行业标准，明确平台服务商的行为规范；违反相应国家、行业标准的行为和监管部门的特别命令相结合，才能更加合理地确认网络服务提供者行政义务违反的内容。[②]同时，在行政义务的设置中，要求网络交易平台承担对交易内容的主动监控义务还必须满足两个基本条件：一是判断违法的标准清晰，即监管部门能够提供明确的负面清单；二是判断违法的标准简单，即现有技术手段可以将上述标准设定入平台的程序，进而自动过滤。如果没有判断平台是否具有过错的标准，监管部门更可能根据后果的严重程度而非平台本身的过错来问责，从而会产生大量的问题。[③]这同样适用于以不作为形式实施的帮助信息网络犯罪活动罪的认定。

（3）入罪标准的明确化。基于义务型犯罪的特征，义务违反直接带来可谴责性，因此，明确的入罪条件需要予以标识。这些条件表现为抗拒履行义务本身的严重性、义务违反带来的严重危害结果等，通过这些客观条件的设置，只有对

[①]参见马荣春、王腾：《拒不履行信息网络安全管理义务罪的适用困境与解脱》，载《山东警察学院学报》2018 年第 5 期。
[②]参见马荣春、王腾：《拒不履行信息网络安全管理义务罪的适用困境与解脱》，载《山东警察学院学报》2018 年第 5 期。
[③]赵鹏：《私人审查的界限——论网络交易平台对用户内容的行政责任》，载《清华法学》2016 年第 6 期。

严重违反了义务的行为人才给予刑罚的制裁。这从大多数义务型犯罪的刑罚设置也能发现，即便造成了严重的后果，刑罚的设置总体上都比支配型犯罪更加轻缓。[①]义务型犯罪的行为不是从行为人的行为自由中内在地产生的，而是从外部强加给行为人的，其可谴责性根本上来自于对制度的违反，而不是直接指向制度背后保护的法益。对于义务型犯罪的刑法责难，应当保持最谨慎的态度而不至于对公民的自由干预过多。

因此，针对拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪里的“大量”“严重后果”“情节严重”等模糊的罪量要素，应当通过司法解释设置更为明确的标准，否则这些不明确的话语会直接导致这些罪量要素的消解。“拒不改正”的标准也需要明确。“拒不改正”和“不改正”在语义上有不同的涵义。后者是对事实的客观描述，而前者含有对行为人主观态度的否定评价。因此，对于网络服务提供者有所行动但并未完整履行责令事项的，如果有证据证明该网络服务提供者表面上的行动只是为了逃避处罚，实际上怠于整改的，比如经调查确有技术措施可以整改却无正当理由不使用的情况，那么可以认为是“拒不改正”。如果确因客观条件的限制没有改正完善的，则不应当认为是“拒不改正”。对于在限期整改的期限还未到达时，危害后果已经出现的情况，网络服务提供者不承担刑事责任。

3、立法模式的未来调整

未来网络平台犯罪的新型风险类型和态势，还可能对刑法不断提出新的要求。以预防性刑法观为规制理念，我国刑法立法模式必须做出重大调整，才能兼顾刑法的稳定性和适应性，回应社会发展要求。

（1）适当借鉴吸纳附属刑法与分散式立法模式的有益经验，在刑法典分则中设置专节规定网络犯罪。我国有学者指出，德国、日本等大陆法系国家的分散立法模式实践值得我国借鉴，把网络犯罪等行为类型复杂多样、变化较快的犯罪根据行业特色或专业依赖程度以附属刑法的方式，直接转引刑法典的规定，由此适应不同行业或专业领域内的快速发展和特殊要求，保持和行政监管的衔接流畅。[②]我国的《网络安全法》是第一部全面规范网络空间安全管理方面问题的基

[①]法定不作为犯的死罪比例大大低于其他犯罪，就有期监禁刑的配置而言，法定不作为犯的刑期也普遍低于其他犯罪的刑期。参见白建军：《论不作为犯的法定性和相似性》，载《中国法学》2012 年第 2 期。
[②]参见焦旭鹏：《现代刑法的风险转向——兼评中国当下的刑法观》，载《西南民族大学学报（人文社科版）》2018 年第 12 期。

础性法律，将原来散见于各种法规、规章中的规定上升到人大法律层面，对网络运营者等主体的法律义务和责任做了全面规定，但遗憾的是，我国刑法与该法的衔接并不流畅，甚至在网络主体的称谓上也没有统一，刑法修正案对此问题予以关注不够。《网络安全法》第 74 条第 2 款规定的“构成犯罪的，依法追究刑事责任。”该规定的形式意义大于实质意义，对弥补网络刑法规范不足的作用有限。[①]行政监管和刑事义务的衔接不仅可以避免刑事义务的空泛、流于形式和判断主体异位，也能对网络平台提供者展示更加明晰的刑事负面清单，适应不同行业或专业领域内的快速发展和特殊要求。经过一个长期的发展后，在技术的发展和实践的累积基础上，立法上应当全面吸纳《网络安全法》和其他相关法律法规所涉对网络犯罪规定的重要规范内容并对刑法典进行补充或调整，采用刑法修正案形式解释网络犯罪新型术语、明确网络犯罪新型法益、规制新型网络犯罪，在条件成熟的时候对刑法典进行“大修”并在刑法典分则中设置专节规定网络犯罪。

（2）网络平台第三方责任的特别规制。网络平台第三方责任犯罪是网络空间犯罪治理的重要命题。和其他承担被动性刑事义务的网络服务提供者，如通道性质物理层服务提供者、针对特定用户的需求提供个性化解决方案的应用层服务提供者相比，网络平台除了被动性的修正保证人义务还有主动性的修正保证人义务，无差别地用同一条款规定所有类别网络服务提供者的刑事责任无法凸显网络平台的枢纽地位。当前，关于网络平台的行政规定已初具规模，行政上的标准还可以走得更远，在《网络安全法》的顶层设计下，进一步明确大型平台——尤其是一旦发生危害结果可能对关键信息基础设施产生重大危害的 IT 巨头运营的特定网络和系统——的定义、认定标准、技术行为规范、负面清单；刑法则在此基础上吸纳美国的立法经验，对于恐怖主义、促进卖淫、儿童性剥削、毒品泛滥等特殊的、重大的危险领域，比照义务型犯罪的设置规格，规定网络平台的义务犯罪模式，包括过失犯罪模式。

（3）刑事一体化的要求。基于刑事一体化的要求和风险社会、网络技术的不确定性，刑法需要不断地“瞻前顾后”。在刑法立法模式的调整过程中，立法机关应当保持谨慎的态度，充分调研和听取专业人员的意见；司法机构不轻易出台司法解释，不断完善案例指导制度，给予公民刑事政策效用的确定性和刑法的

[①]孙道萃：《网络平台犯罪的刑事制裁思维与路径》，载《东方法学》2017 年第 3 期。

安定性。在现有的刑罚体现上，需要通过适当的刑罚来达到对网络平台犯罪特殊预防的效果。《刑法》第 37 条之一规定了“因利用职业便利实施犯罪，或者实施违背职业要求的特定义务的犯罪被判处刑罚的，人民法院可以根据犯罪情况和预防再犯罪的需要，禁止其自刑罚执行完毕之日或者假释之日起从事相关职业，期限为三年至五年”。这一立法思路为网络平台处遇制度提供了契机。[①]在诉讼中，以专业的精神、技术与标准，遵循专业伦理，实现司法的公正和效率，发展司法的职业化与专业化，推动“司法专业主义”。[②]这不仅是网络空间治理精细化的要求，也体现了对网络空间本身的尊重。

四、结语

随着技术的不断演进，未来的中国信息网络还将呈现更多的颠覆性技术创新、创造更多新业态。在党的十九大报告中，我国互联网发展的宏观趋势被阐述为“推动互联网、大数据、人工智能和实体经济深度融合”。在万物联网的时代，随着数字化程度的不断加深，新型的网络安全威胁也将无处不在。新时代的主要特点之一是安全与发展并重并行。在网络去中心化的架构下，最大限度地依靠网络平台企业对用户行为进行管理既能克服政府专业知识不足、管控能力不及的问题，发挥技术治理的便捷性和高效性，又能促使网络服务提供者尤其是大型企业承担起社会责任；但是单凭法律的力量并不足以遏制网络风险，我国政府应当在社会共治理念、技术法律手段并重理念的指导下，规范行政监管，把市场、社会等多方的力量纳入治理体系、突出技术治理等柔性治理方式。在整体的解决模式中，刑法仍然是最后的环节。修正保证人义务的设置来自国家公权的赋予，是对公民自由的强干预，因此必须受到严格的限制。即使在一个强调危险控制的社会，个人自由的保障会在一定情况下让位于风险的预防，但罪责原则是现代刑法的基本原则，预防的观念必须以罪责边界为限度。

[①]魏东、金燚：《网络犯罪魔变中的刑法理性检讨》，载《刑法论丛》总第 50 卷，2017 年第 2 卷。
[②]参见龙宗智：《司法的逻辑》，载《中国法律评论》2018 年第 3 期。

政府数据开放的刑事风险及治理——基于刑法解释学的进路

柳洁*

（梧州学院 法学与公共管理学院，广西 梧州 543000）

摘 要：大数据时代下，政府数据开放具有巨大经济效益和社会价值，但同时也带来了不可估量的法益侵害风险。刑法是法益的最后保护手段，通过维克利S-C-R信息交流模式，从信源到信道再到信宿三个层面，梳理政府数据开放中的刑事风险，提出：借鉴刑法解释学三分法，对信源层面的职务犯罪进行伦理解释、信道层面的平台犯罪进行文义解释、信宿层面的数据犯罪进行刑事政策解释，以实现对政府数据开放平台刑事风险的刑法规制，保障政府数据开放的安全高效及法治化。

关键词：政府数据开放；刑事风险；刑法治理；刑法解释学

在当前大数据时代，数据成为与石油媲美的重要非物质资源。2016年，第十二届全国人大在《国民经济和社会发展第十三个五年规划纲要》中明确指出："建设国家政府数据统一开放平台；制定政府数据共享开放目录；研究制定数据开放、保护等法律法规。"①为实现数据资源的效益最大化、数据市场的规范治理，部分地方政府已通过"大数据+政务"模式，构建了统一的政府数据开放平台，将数据资源通过"脱敏脱密"处理后，向社会公众公开共享。这一举措无疑具有调停数据资源争夺战，引导公众合理使用政府数据，促进经济增长、社会发展的积极作用。然而，正如硬币有两面，政府数据开放在带来巨大利益的同时也不可避免的引发了一系列风险，特别是其中的刑事风险，如侵犯个人信息、危害公共安全、泄露国家秘密等，一旦爆发，危害后果不可估量。在目前地方政府数据开放非刑事立法缺位（仅部分地方政府颁行了数据开放共享条例和数据安全管理条例）、政府数据开放相关刑事风险研究缺失（主要研究均集中于平台构建、政策分析、数据治理等方面）的情形下，笔者坚持刑法立法谨慎原则，从刑法解

*作者简介：柳洁（1987—），女，汉，湖北黄冈人，梧州学院法学与公共管理学院讲师，主要研究方向：刑法学。联系方式：电话：13097886562；邮箱：364705401@qq.com。

①第十二届全国人大四次会议：中华人民共和国国民经济和社会发展第十三个五年规划纲要，2018-06-01. http://www.xinhuanet.com/politics/2061h/2016-03/17/c_1118366322_8.htm。

释学角度思考政府数据开放刑事风险的刑法治理策略。

一、政府数据开放的刑事风险考察

政府数据开放正如一把双刃剑，带来经济利益的同时，也不可避免的引发了一系列社会矛盾和风险，其中的刑事风险是我们首先需要思考和应对的。在此，笔者通过维克利的S-C-R信息交流模式，从信源到信道再到信宿三个层面，考察政府数据开放中的刑事风险。具体包括：

（一）信源层面的职务犯罪异化

信源这里指数据的来源，是政府数据开放的实现基础，主要是数据开放之前的政府职能部门收集、处理及内部交换共享数据，因此涉及的主要是传统的职务犯罪。然而，数据的指数增长和大数据技术的快速发展，导致信源层面的传统职务犯罪发生了"异化"，犯罪认定困难。具体表现在数据脱密脱敏和内部交换共享中。第一，数据采集中犯罪主体异化。政府数据采集一般是由有权的职能部门或者委托第三方进行，其职权来源主要是行政法规及部门规章等的规定，若其不履行或不认真履行数据采集职能，甚至故意超越职权采集涉及国家秘密的数据，这些渎职行为，不仅会造成公众经济利益损失，错误或虚假数据的快速传播和广泛使用，还会引发社会矛盾，危害公共安全。然而现行刑法，对于渎职犯罪的规制，多限于"国家机关工作人员"，而政府数据采集部门的犯罪主体身份难以认定，由此导致发生严重后果时，追责困难。第二，脱密脱敏中犯罪行为异化风险。数据脱密是指，政务部门及其工作人员采集完数据后，要对涉密数据，进行排除处理。对此，2016年，中共中央办公厅、国务院办公厅印发《关于全面推进政务公开工作的意见》，明确指出："各省（自治区、直辖市）政府和国务院各部门应将公开后危及国家安全、经济安全、公共安全、社会稳定等方面的事项纳入负面清单不予公开，并及时进行调整更新。"数据脱敏是指，政务部门及其工作人员收集到数据后，对某些敏感信息（如用户名、地址、身份证号、手机号、邮件登陆密码、病历卡等），通过脱敏规则进行改造、变形处理，实现敏感隐私数据的可靠保护。数据脱敏脱密的目的在于，保护开放的数据安全和高效使用。然而，对于这一阶段政务部门及其工作人员的数据脱密脱敏义务来源，主要是行政法规的规定，若其故意或过失不作脱密脱敏处理，造成严重后果的，是否能追究其行政不作为的刑事责任？在此，主要涉及不作为义务来源，根据现行刑法规定，

成立不作为犯罪，必须是负有法律明文规定的作为义务，能够作而不作，从而被刑法认定为是犯罪。而由于“脱密脱敏”义务是由行政法规所规定，因此难以适用传统不作为犯罪处理，导致发生严重后果时追责困难。

（二）信道层面的网络犯罪多元化风险

信道是指信号传输的媒介，政府数据开放中的信道就是政府数据开放平台，平台安全是政府数据开放安全的枢纽，平台通过网络来运营，因而网络安全又决定了平台安全。当前，网络所带来的最大挑战是“社会需要保证秩序：内部秩序与外部秩序”。[①] 就信道层面的网络犯罪而言，一方面，刑法对网络犯罪的很多规定，都突破了传统犯罪的立法模式，体现了“打早打小”的立法意图。但是，刑法大规模的犯罪化努力，并没有起到遏制犯罪的效果。[②]另一方面，数据本就蕴含巨大经济价值，数据越多经济价值越大，不法分子犯罪获利越多。因此，集中了海量数据的政府数据开放平台，无异于置于公共领域的未上锁“宝库”，不可避免的会遭受到一系列犯罪攻击。例如，不法分子非法侵入政府数据开放平台，或者通过木马植入、病毒感染等技术手段攻击政府数据开放网络平台，复制、更改或者删除平台数据、破坏数据开放信息网络系统，造成平台瘫痪、拥堵等。由于政府数据开放网络平台是数据安全的保障，因此牵涉法益众多，一旦网络平台被非法侵入或攻击，可能危及个人人身、财产安全，侵犯商业秘密，危害公共安全、甚至国家安全。然而，现行刑法对于此类犯罪的规制，更多的是从计算机信息系统出发，依照第 285 条，286 条规定的非法侵入计算机系统的犯罪和破坏计算机信息系统的犯罪追究刑事责任。就政府数据开放而言，司法实践中往往将“计算机信息系统”完全等同于“网络平台”。盲目的扩张解释，不但脱离了刑法本义，而且导致技术和网络平台不加区分，概念混淆滥用，难以实现对信道层面网络犯罪的规制。

（三）信宿层面的数据犯罪不可控风险

信宿指信号的接受者，即最终用户，政府数据开放中的信宿即数据使用者。信宿层面的数据犯罪风险，主要是由于数据使用者不当使用、滥用政府开放的数据而引发的。当前政府数据开放平台开放的数据涉及面广泛，涵盖了卫生健康、

①Brenne, Susan W.,Cybercrime and the Law. Challenges, Issues, and Outcomes. Northeastern University Press. Boston 2012. P.189。

②陈艳东：《网络犯罪定量证明标准的优化路径:从印证论到综合认定》，载《中国刑事法杂志》，2019 年第 1 期，第 127 页。

劳动人事、企业服务、交通运输、财税金融等公共生活的各个方面，并且随着技术的发展、平台的完善，开放数据的类型和数量等都在不断扩大。而政府开发数据的目的在于发动公众对数据的合理开发利用，从而促进经济增长和社会发展。因此，2016 年国务院印发的《政务信息资源共享管理暂行办法》中明确规定：“使用部门对从共享平台获取的信息，只能按照明确的使用用途用于本部门履行职责需要，不得直接或以改变数据形式等方式提供给第三方，也不得用于或变相用于其他目的。”然而，数据从政府开放平台公开后，被多方使用者使用、流转和后续利用，这一过程十分复杂、难以监控，也难以追责。由此导致，实践中信宿层面的数据滥用刑事风险易发高发难防控。具体表现为：第一，直接非法使用。例如对政府开放的数据进行监听、监控后，抓取遗漏的涉密或涉敏数据，进行非法获动。例如，东莞政府数据开放平台发布的“社会体育指导员资格信息”，将包括身份证号在内的数据全部公开；其中的“道路运输从业人员数据”将“从业资格证”字号相关信息完全公开，而一旦这些数据被不法分子监控到并进行非法活动，必将造成严重后果！第二，二次处理后非法使用。对政府开放的数据，进行技术分析或二次处理后，得到涉密涉敏信息再进行非法使用。一些数据从表面上看可能不包含关键的敏感信息，但是通过人工智能技术分析海量数据，以及对多个数据库进行综合分析，最终完全有可能通过推演得到关键的敏感信息，甚至包括一些威胁国家安全的重要信息。对此，现行刑法多是根据滥用数据行为侵害的具体法益来进行规制，例如“侵犯公民个人信息罪”、“侵犯商业秘密罪”、“故意泄露国家秘密罪”等。然而，由于数据牵涉的法益往往是多方面的，数据滥用行为的危害结果往往也十分复杂，难以把控，如个人信息的泄露，除了可能侵犯个人隐私权之外，还可能引发公共安全危机。而现行刑法，对于此类犯罪均要求“情节严重”才能定罪，但对于“情节严重”的标准却又缺乏具体解释，从而导致犯罪规制困难。

综上分析可知，大数据时代政府数据开放中的刑事风险呈现：“异化”、“多元化”、“不可控性”等特点。政府数据开放刑事风险的不确定性，无疑为刑法治理带来了挑战。但笔者认为，风险的不确定性不能成为刑法擅变的理由，坚持立法审慎原则，通过刑法解释方法，充分发挥刑法的社会保障功能，能够更好的实现政府数据开放刑事风险的治理目标。

二、信源层面职务犯罪的伦理解释之规制

在一个国家已经建立了比较完备的刑事法律体系时，解释乃是刑法的生命。[①]根据刑法解释的方法不同，可以分为文义解释、体系解释、历史解释、目的解释四种（经典四分法），但经典四分法自引入中国以来一直面临着争议和挑战，中国刑法学者现在越来越多地主张将刑法解释方法分为文义解释方法、论理解释方法、刑事政策解释方法（新三分法），这种新三分法逐渐成为有强大理论解释力的理论共识。[②]在此，笔者认为，刑法解释的过程其实也是一次利益博弈的过程，最好的刑法解释应当是能够在刑法文义范围内，实现社会效益最大化、保障最大多数法益的结果。笔者赞同应“坚持实践理性，选择对个案最为合适的解释方法”[③]，在此针对政府数据开放中的不同情况，借鉴刑法解释新三分法，思考不同阶段刑事风险的规制路径。

关于信源层面的职务犯罪，笔者认为可通过伦理解释方法予以规制。具体而言：

（一）信源层面职务犯罪中犯罪主体的当然解释

就政府数据开放信源层面职务犯罪的“犯罪主体”而言，主要涉及的是渎职罪中“国家机关工作人员”的认定问题。对此，全国人民代表大会常务委员会《关于<中华人民共和国刑法>第九章渎职罪主体适用问题的解释》（2002 年）对“国家机关工作人员”的外延进行了拓展：1. 在依照法律、法规规定行使国家行政管理职权的组织中从事公务的人员；2. 在受国家机关委托代表国家机关行使职权的组织中从事公务的人员；3. 虽未列入国家机关人员编制但在国家机关中从事公务，代表国家机关行使职权的人员。笔者认为，现行的司法解释，着重于对职务犯罪“从事公务”这一实质要件的的认定，而非完全要求“身份”，因此是能够满足规则当前信息技术发展中的新类型渎职犯罪新情况需要的。就地方政府数据开放而言，一般是由承担政府数据采集职能的政务部门工作人员负责数据采集工作，这一主体的“身份”属于“行政机关中从事公务的人员”，“行为”是“履行公职、从事公务”，因此当然符合渎职罪的犯罪主体范畴，属于职务犯罪中的

①冯军：《论刑法解释的边界和路径———以扩张解释与类推适用的区分为中心》，载《法学家》，2012 年第 1 期，第 64 页。
②魏东：《刑法解释学基石范畴的法理阐释—关于“刑法解释”的若干重要命题》，载《法治现代化研究》，2018 年第 6 期，第 111 页。
③周光权：《刑法解释方法位阶性的质疑》，载《法学研究》，2014 年第 5 期，第 159 页。

国家机关工作人员。此外，实践中还可能由政务部门以委托方式，委托非政务部门承担数据收集工作。此时，由于非政务部门非政务工作人员从事数据收集职能的“公务性”，符合职务犯罪的实质要件，因此，当然属于上述司法解释的第 2 项“在受国家机关委托代表国家机关行使职权的组织中从事公务的人员”，符合职务犯罪的主体要求，可能构成职务犯罪。

（二）信源层面职务犯罪中犯罪行为的扩张解释

解释者的智慧，表现在既遵守罪刑法定原则，不超出刑法用语可能具有的含义，又使解释结论实现正义理念，适合司法需求。[①]就信源层面职务犯罪中的“不作为”而言，现行刑法对于不作为犯罪，主要有两个限定要求：一是，违法法律明文规定的义务；二是，刑法认定为是犯罪。也即，若违反的不是法律规定的义务，而是其他行政法规、部门规章等规定的义务，则不构成不作为犯罪；若违反的是法律明文规定的义务，但刑法不认为是犯罪，也不当做犯罪论处。例如，欠债不还，违反了民法规定的义务，但刑法不认定为是不作为犯罪，因此不构成不作为犯罪。那么，本文信源层面职务犯罪中的“不作为”该如何理解呢？对此，笔者认为，在信源层面的职务犯罪中，可以将不作为义务来源中：“法律明文规定的义务”，其中的“法律”扩张解释为包含行政法规。首先，将“法律明文规定的义务” 扩张解释为包含行政法规，不违反立法精神。刑法中设立职务犯罪的目的是规制职权滥用或渎职等行为，保护的是国家对职务活动的管理职能。而职务犯罪主体的“职权”来源，除了法律明确规定之外，大多来自于行政法规的规定，特别是其中的“国家行政机关工作人员”。政府数据开放而言，其中的数据采集、脱密脱敏等工作，大多由大数据局、大数据处等行政部门工作人员承担，其行政职权主要来源于国务院发布的各项行政法规。因此，将职务犯罪中“法律明文规定的义务” 扩张解释为包含行政法规，能够对政府数据开放中的职务滥用或渎职等行为进行有力的规制，实现国家队政府数据开放活动的有序管理。其次，将职务犯罪“法律明文规定的义务” 扩张解释为包含行政法规，不违反罪刑法定原则。实现扩张解释方法与罪刑法定原则相协同，是这一解释方法合理适用的关键。笔者认为，罪刑法定原则强调的是“法无明文规定不为罪”，关于政府数据开放，其本质是由政府职能部门履行职责的政务服务行为，这一行为的主

①张明楷：《也论刑法教义学的立场 与冯军教授商榷》，载《中外法学》，2014 年第 2 期，第 360 页。

体为行政机关工作人员，行为性质为履行职责的行政行为。对此，刑法第 397 条明确规定了“玩忽职守罪”，因此，将职务犯罪“法律明文规定的义务” 扩张解释为包含行政法规，并不违反罪刑法定原则，仍然只是将法律明文规定的犯罪情形界定为犯罪处理。最后，其次，将职务犯罪“法律明文规定的义务” 扩张解释为包含行政法规，符合信息社会的发展需要。随着信息技术的发展，社会风险不断增大，而数据牵涉的法益众多，特别是涉密涉敏数据，一旦泄露，危害重大。因此，将职务犯罪“法律明文规定的义务” 扩张解释为包含行政法规，有利于增强数据管理机关的行政职责意识和渎职的刑事风险认识，有利于从信源上保障数据的安全性，减少后续刑事风险。

三、信道层面网络犯罪的文义解释之应对

信息技术的发展，愈发体现了现行立法的滞后性。然而，在现行立法滞后于信息技术的情况下，完全超脱刑法立法本意的解释，实质又是违反罪刑法定原则的。就政府数据开放而言，传统将计算机网络等同于计算机信息系统的解释方法，无疑太过宽泛，淡化了计算机信息系统的技术特征，同时混淆了网络与技术的涵义，不利于犯罪的规制。而“文义解释是一切解释的出发点”、“文义解释能保证解释的客观性与预测可能性，脱离刑法文本的解释必然损害刑法的安定性。”[①]因此，笔者建议，立足刑法本义对信道层面的网络犯罪通过文义解释方法进行合理规制。首先，区分“网络平台”与“计算机信息系统”。《刑法》第 285、286 条是对计算机信息系统功能的维护。计算机信息系统，是指在计算机中，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等功能[②]，属于人机系统。而政府数据开放网络平台，笔者结合前文政府数据开放的本质认为，其实质是政府通过网络系统实现政务服务的新模式，是通过技术设备将多个计算机系统连接起来，按照协议互相通信，达到信息交换、数据共享等功能的系统，属于机对机系统。可见，从字面上看，“网络平台”与“计算机信息系统”有明显区别，不可等同理解。其次，认识平台代表的法益。政府数据开放信道层面网络犯罪的目的，如果在于攻击平台，造成平台瘫痪等，该如何规制呢？对此，必须要正确理解平台代表的法益。根据上文分析可知，平台是政府政务服务的新模式，由政府职能部门负责平台的管理和维护。因此，笔者认为，按照文义解释，

①苏彩霞：《刑法解释方法的位阶与运用》，载《中国法学》，2008 年第 5 期，第 102 页。
②陈兴良：《规范刑法学》，中国人民大学出版社，2013 年第三版第 814 页。

平台代表的法益应当是行政机关正常的平台管理活动和管理秩序。以平台为目标进行攻击的犯罪行为，可能涉嫌的是“妨害公务罪”。最后，区分“平台”法益与“数据”法益。政府数据开放信道层面网络犯罪的目的，如果在于获取数据，并利用数据进行其他犯罪活动，是否属于此处的网络犯罪范畴呢？笔者认为，信道层面的网络犯罪，探讨的是攻击政府数据开放平台，并以此为目标的犯罪行为，侵犯的是“平台”法益。而攻击政府数据开放平台、获取数据，并利用数据进行其他犯罪活动的行为，侵害的是“数据”法益。这一犯罪行为，属于我们下文要讨论到的“数据犯罪”范畴。

四、信宿层面数据犯罪的刑事政策解释之思考

刑法解释本质上是利益衡量与价值选择的活动，必须将刑事政策的考虑融入刑法解释之中。[①]“法官可以有自己的价值判断标准，但是如果与已经明确的刑事政策相违背，则应当放弃自己的价值选择，而遵从贯彻一定的刑事政策所得出的解释结论。”[②]因此，笔者认为，基于数据的复杂性，信宿层面的数据犯罪，牵涉法益众多，危害后果严重而且不可控。有必要考虑通过刑事政策解释方法，从犯罪防治层面思考刑法应对策略。

关于数据法益的刑事政策理解。有学者看到了数据的财产性价值，因而将数据法益限定为财产权。笔者对此，持不同意见。理由如下：第一，从文义上看，“数据”本身没有意义，也没有固定的形状、姿态，它可以是连续的值，比如声音、图像，称为模拟数据。也可以是离散的，如符号、文字等。数据的价值也根本无法确定，而取决于它的使用者的需要和加工利用转化，才产生了价值。而且同一数据对于不同的使用者，价值也不同。例如，政府数据开放平台开放的地理数据，为高德地图导航公司节省了几十万的数据采集费用。但这些数据对于其他使用者，可能毫无价值。此外，数据价值的归属无法确定，通过政府数据开放平台开放的数据，其价值应当是由公众共享的，所有权属于公众。同时，大数据时代，数据的内涵不断扩大，数据所代表和牵涉的法益也愈发复杂，数据犯罪可能危及个人隐私、商业秘密、公共安全，甚至国家安全。因此，仅仅将数据法益限定为财产权，太过狭隘，无法满足时代需要。第二，从国外经验来看，欧盟和德

①劳东燕：《能动司法与功能主义的刑法解释论》，载《法学家》，2016 年第 6 期，第 14 页。
②时延安，阴建峰：《刑事政策在刑法有权解释中的功能》，载《南都学坛：南阳师范学院人文社会科学报》，2005 年第 2 期，第 80-83 页。

国采取了通过立法将数据法益独立直接保护的方法：欧洲理事会《网络犯罪公约》第4条规定了数据干扰行为，即故意实施无权限的对计算机数据毁损、删除、破坏、变更或者干扰的行为。这与公约第1条“非法存取”行为、第5条“系统干扰”行为是分别规定的，是以数据为犯罪对象的单独立法。《德国刑法典》第202 a条“数据窃探”行为，即未经授权非法为自己或他人窃探经特别保护的数据的行为，也是针对数据的立法。[①]国外的经验说明，数据法益可以作为独立的对象进行保护，但如何进行责任规制，实现罪责统一还需要进一步思考。第三，数据法益的刑事政策理解。笔者认为，由于数据法益实质上并不是单一法益，而牵涉多方权益，因此将数据法益单独作为财产权或者人身权或者其他单一法益，都不恰当，不能满足刑事政策下犯罪规制的需求。因此，笔者建议，可以借鉴欧洲、德国等国家的经验，通过立法将数据法益作为一项单独法益，进行保护。刑事政策主要的目的在于防止犯罪，而数据犯罪，基于其复杂性和不可控性，根据目前的刑法，无法实现对数据犯罪的有效规制。同数据犯罪作斗争的实际经验表明，此类犯罪危害重大，危及法益众多，因此必须予以严厉打击。所以可以说将数据法益单独予以保护，是符合刑事政策需要的。

关于数据犯罪的刑事政策规制。刑事政策对于复杂多变的数据犯罪，要求予以严厉打击，因此，主要涉及的是数据犯罪的罪名和刑罚设置问题。第一，关于数据犯罪的罪名设置。笔者建议，可以同过司法解释，新增一条“非法使用网络数据罪”。由于数据滥用的行为方式多元化，因此，可以直接规定“非法使用网络数据的，构成本罪”，本罪主观方面为故意。第二，关于数据犯罪的刑罚设置问题。笔者认为，基于数据滥用牵涉的法益众多，因此在刑罚方面，应当根据刑事政策的要求，予以较为严厉的刑罚配置。笔者建议，可以规定为“情节严重的，处三年以下有期徒刑；情节特别严重的，处三年以上十年以下有期徒刑”。关于“情节严重”的标准，笔者认为可以根据数据滥用行为侵害的具体法益的危害结果来认定。

五、结语

利益与风险是并存的，一方面，我们必须认识到政府数据开放的巨大经济价值和社会利益，另一方面，也必须具备危机意识，充分认识到其伴生风险，特别

①于志刚，李源粒：《大数据时代数据犯罪的制裁思路》，载《政治与法律》，2016年第9期，第23页。

是危害严重的刑事风险。被允许的危险理论启示我们，信息技术的发展不能因风险而被遏制。否则，社会将无法正常发展。因此，在政府数据开放过程中，我们既要杜绝“拿来主义”、“跟风行动”，又要避免“因噎废食”，因害怕风险而墨守成规、遏制发展。基于刑事风险性的严重性，如何治理和应对，成为首要问题。既然，刑事立法总是滞后于刑事风险。那么通过刑法解释方法，对当前政府数据开放的刑事风险予以治理就具有重要的现实意义。刑法解释的最终目的，是为了充分发挥刑法的社会保障功能，实现政府数据开放效益最大化，推动政府数据开放的法治化进程。

参考文献

[1]陈兴良.规范刑法学[M]．中国人民大学出版社，2013。

[2][美]史蒂夫•洛尔.大数据主义[M]．胡小锐，朱胜超，译．北京：中国出版集团，2015。

[3]迪莉娅.大数据环境下政府数据开放研究（第一版）[M].知识产权出版社，2014。

[3]李平.开放政府数据、推进应用创新的中外模式比较[J].中国科技论坛,2017，(12)。

[4]才世杰，夏义堃.试论政府数据开放风险的识别与防范[J].图书与情报,2017（08）。

[5]于志刚，李源粒.大数据时代数据犯罪的类型化与制裁思路[J].政治与法律，2016（9）。

[6]刘宪权.区分数据犯罪类型予以刑法应对.

[7]Bertot J C.大数据与开放数据的政策框架:问题、政策与建议[J]．郑磊，徐慧娜，包琳达，译.电子政务，2014(1).

[8]Kucera J， Chlapek P. Benefits and risks of open government data[J].Journal of Systems Integration,2014(1）。

[9] Brenne, Susan W.,Cybercrime and the Law. Challenges, Issues, and Outcomes[J]. Northeastern University Press. Boston 2012.

[10]何治乐，孔华锋. 机遇与挑战: 中国政府数据开放的法治化路径[J]．计算机应用与软件，2018（4）。

[11]陈志军.对大数据技术应用的合理刑法规制[J].中国人民公安大学学报（社会科学版），2018（6）。

[12]陈艳东.网络犯罪定量证明标准的优化路径:从印证论到综合认定[J].中国刑事法杂志,2019（1）.

[13]王燕玲.中国网络犯罪立法检讨与发展前瞻[J].华南师范大学学报（社会科学版），2018（4）。

[14]张明楷.也论刑法教义学的立场 与冯军教授商榷[J].中外法学，2014（2）。

[15]冯军.论刑法解释的边界和路径———以扩张解释与类推适用的区分为中心[J].法学家，2012（1）。

[16]魏东.刑法解释学基石范畴的法理阐释—关于“刑法解释”的若干重要命题[J].法治现代化研究，2018（6）。

[17]周光权.刑法解释方法位阶性的质疑[J].法学研究，2014（5）。

[18]徐岱. 刑法解释学的独立品格[J].法学研究，2009（3）。

网络直播平台犯罪风险的企业防控对策

齐守明 王若琪

摘　要：网络直播行业在经历了发展初期的内容乱象和资本狂热之后迅速“洗牌”，行业格局和直播内容生态得以真正建立，网络直播平台的经营行为也受到了强有力的监管，但由于主播和用户的自发行为、竞争对手或不法分子的有意为之使得直播平台深受网络犯罪之扰，只有主动履行安全管理义务、积极应对网络犯罪才能使网络直播行业得到长久健康发展。

关键词：网络直播；平台犯罪；传播淫秽物品罪；行业自律

一、网络直播行业背景

权威数据机构调查显示，2019 年在线直播用户规模有望达到 5.01 亿人，约占中国网民规模的 63%，直播行业市场规模预计超越 500 亿元，网络直播已经成为人们重要的娱乐社交手段之一，范围涵盖了秀场、游戏、体育、户外、电商等几十个细分领域。

网络直播受到资本力量的青睐和社会各界的广泛关注是从 2016 年开始的，从 16 年 3 月开始的几十家，仅数月时间激增至上千家直播平台涌入直播赛道，2016 也因被称作“直播元年”亦或是“千播大战”。新兴网络服务形式的出现、资本的狂欢以及司法和行政监管的滞后在一定程度上导致了行业野蛮生长阶段乱象频发，使得网络直播成为违法违规内容的“滋养区”甚至被不法分子利用进而实施网络犯罪行为。

随着监管力量的强势介入，司法实践的不断探索以及行业自律意识的增强，直播内容的规范化、多元化、纵深化显著提升，网络直播领域的行业格局已经得到清洗，只想“赚快钱”、“赚热钱”的投机者势必要离开，只有真正深耕直播内容生产、直播生态建设的直播平台才能留下，行业环境不断净化。

但是，由于网络直播自身具有的形式新、门槛低、高收益、用户多、传播快等特点，以及网络技术本身的时空跨度大、隐蔽性强、技术难度高等特征，使得网络直播平台容易被不法分子所利用进而实施犯罪行为。对此，网络直播平台必

须积极履行安全管理义务进行犯罪风险防控才能保障用户的合法权益、保证平台的正常运营、促进行业的健康发展。

二、网络直播平台涉罪性质及类型

网络直播行为主要涉及主播、用户和直播平台三方主体，主播和用户是网络直播服务的使用者，而平台则是网络直播服务提供者。主播提供直播表演，用户可以选择免费观看或通过充值打赏对主播进行肯定，直播平台负责提供平台服务和技术支持，并与主播或主播签约的公会按照约定比例进行礼物收入分成，这就构成了最基础的网络直播关系链条。在此基础上，任何一方的行为都会对其他各方甚至整个链条的稳定性造成影响。就涉罪风险而言，网络直播平台可能因为自身、主播或用户的行为而面临刑事风险，又因为犯罪行为的性质不同而承担不同的刑事责任。于此同时，网络直播平台作为互联网生态的一环，同样可能成为网络犯罪的受害者，需要援引法律武器进行救济。

（一）主要的刑事责任类型

1.独立的正犯责任

当直播平台直接实施犯罪行为时，应当独立承担刑事责任。如《刑法修正案（九）》将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，同时扩大了犯罪主体和侵犯个人信息行为的范围。《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》进一步明确了“公民个人信息”的范围以及该罪的定罪量刑标准。网络平台作为信息网络服务提供者对于公民个人信息的收集、处理和保护必须严格依照相关法律规定，否则将承担相应的刑事责任。

2.实施帮助或教唆行为的共犯责任

直播平台与主播或用户存在共同犯罪的意思联络，明知违反网络安全管理义务，仍积极提供直播平台技术服务或采取放任不管的态度，不采取删除屏蔽、“主播黑名单”、关闭直播间等必要的安全措施，放纵、帮助甚至教唆他人实施犯罪，以图从中获利的，直播平台应当承担共同犯罪的责任。《刑法》第二百八十七条之二将此类帮助行为正犯化规定明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的构成“帮助信息网络犯罪活动罪”，在此罪基础上同时构成其他

犯罪的，择一重罪定罪处罚。

尤其在网络直播发展不规范的初级阶段，存在着许多主播利用直播的手段传播涉黄、涉赌、涉暴等违法违规内容吸引用户关注、打赏，而有些直播平台为了眼前的短期收益，不仅不及时遏制，反而放纵甚至帮助此类低俗内容在平台上肆意传播进而牟利，大搞“眼球经济”，严重破坏行业生态和直播社区环境，应与主播构成共同犯罪，承担相应的法律责任。

3.因不作为而承担刑事责任

网络直播平台作为网络服务提供商，对其运营的网站应承担“谁运营、谁负责”的“主体责任”，负有法定的信息网络安全管理义务，应当具备相应的网络安全管理能力和应急条件。《网络安全法》第九条总括地规定了包括建立信息安全管理制度义务、用户身份信息审核义务、用户发布信息管理义务、保障个人信息安全义务、违法信息处置义务、信息记录义务、投诉处理义务、报告义务、配合监督检查的义务等十项信息网络安全法定义务。而根据《刑法》第二百八十六条之一的规定，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的构成“拒不履行信息网络安全管理义务罪”的不作为犯罪。

（二）主要涉罪类型

1.传播淫秽物品类型的犯罪

网络直播具备高收益、门槛低的显著特点，尤其在直播内容尚未得到规范化监管之前，不少主播缺少真材实料，为了吸引用户关注和打赏，不惜大打“擦边球”甚至公然提供色情表演，导致部分直播平台上低俗内容泛滥，严重危害广大网民的身心健康。但有些不良平台贪图流量红利或者分成收益，放纵甚至帮助平台上的淫秽内容肆意传播，更有甚者以招募、雇佣、引诱等手段故意组织主播提供淫秽表演，将直播打造成谋取不法利益的工具。

对于以招募、雇佣、强迫、引诱、容留等手段控制他人从事淫秽表演的直播平台则应当认定为“组织淫秽表演罪”依法追究其法律责任；对于利用网络直播工具提供淫秽色情表演的主播应认定为“制作、传播淫秽物品罪”或“传播淫秽物品牟利罪”，在网络直播平台明知却纵容主播实施犯罪行为或逃避监管审查的，则可以认定其以不作为的方式帮助网络主播共同实施违法犯罪活动，在主播的行为

成立犯罪的前提下，应当不作为的帮助犯认定网络直播平台与主播构成共同犯罪进而追究其法律责任。

在认定色情直播服务是否构成“淫秽物品”时，有部分观点认为“淫秽物品”必须具备“淫秽内容”和“载体固化”等两方面属性，而直播行为属于实时视频信号传输，不具有反复和继续传观的可能性，因而不适用该罪。但是通过法律以及法条目的解释的角度可以得出，判断是否属于本罪中的“淫秽物品”的必要因素在于是否传播了“淫秽内容”，载体只是在于“展示”淫秽内容而非提供反复传观，“反复传观性”并非判断“淫秽物品”的必要条件，在区别于传统媒体时代的网络空间中，对于“淫秽物品”的判断依据主要是“具体描绘性行为或者露骨宣扬色情的诲淫性”。

在我国同时追究直播平台和网络主播刑事责任第一案中，网络直播平台正是因为明知存在大量主播在该平台上进行淫秽色情表演，但却故意采取放纵的态度并以此牟利的原因而与主播一同被追究刑事责任。更有多家网络直播平台因此被要求依法整改、取缔或追究刑事责任。

2.赌博类型的犯罪

网络空间是物理空间的延续，网络赌博不仅危害社会秩序，更容易演变为其他犯罪的温床，必须严厉打击。对于利用直播形式开设网络赌场或者部分直播平台故意嵌入赌博游戏进行营利的，构成“聚众赌博”或“开设赌场”等赌博类型的犯罪，网络直播平台应当自发抵制涉赌内容在平台内部的传播，配合主管机关坚决打击此类犯罪行为，共同营造文明健康的直播环境。

然而平台虽然是互动玩法的提供者，希望通过互动玩法增强观看直播的趣味性，提高主播和用户的参与度并以此实现营收目的，但由于主播和用户的广泛参与或错误解读使得互动玩法的实际效果可能与平台的设计构想存在一定差异，甚至存在被不法分子利用的可能，进而导致平台虽无提供赌博游戏的故意却仍面临涉赌的风险。

近日宣告破产的熊猫直播，去年曾被举报平台涉赌，某主播通过一种名为“拉爆机”的道具组织用户开展赌博活动。“原理类似老虎机，摇到一定数字，会返回竹子，烤鱼等打赏直播的道具。”后可根据领到的道具打赏主播，主播在将打赏收益提现后也会通过其他方式向用户进行“返现”。此类玩法明显具有赌博性质，

宣扬赌博文化，在平台内部传播甚广，涉案金额较高，应依法追究平台责任。

3.扰乱公共场所秩序类型的犯罪

所谓“全民开播”、“草根直播”正是将麦克风和摄像头对准广泛的普通民众，只要有一技之长都可以成为主播，获得用户的关注并掌握话语权。用户更无需门槛即可免费观看，通过弹幕与主播进行实时沟通，甚至营造出“一对一”交流的感觉。直播平台为主播和用户创造了发表言论，传递观点的广阔空间的同时，也会受到平台上言论传播的制约，尤其是在有些主播和用户素质低下、言论粗俗、法律意识淡薄、情绪和处事手段过激，宣扬血腥暴力内容，参与或聚众“起哄闹事”，造成公众心理上的恐慌，扰乱网络空间的秩序可能涉嫌构成网络空间下的寻衅滋事罪；对他人实施侮辱、诽谤且情节严重的，可能涉嫌构成侮辱罪、诽谤罪。

直播平台虽没有直接实施扰乱公共秩序的行为，但放纵此类违法违规言论及内容在平台肆意传播，怠于承担主体责任，未能对直播内容和主播行为进行有效监管甚至乐见此类“爆点”、“炒作”、“吸睛”，危害网络空间秩序而不采取必要措施的，应视情节轻重而承担相应法律责任。

例如，某直播平台上有 90 后男主播为出位秀下限博眼球，被网友起哄、怂恿进行“恶作剧”，并按照网友提示拨打各地报警电话，自称家住“东海龙宫”，被“哆啦 A 梦”、“Pokemon”威胁，半年里多次用电话骚扰全国各城市的 110 报警平台，依法被追究刑事责任。

又如，某直播用户因主播发表不当言论，与其发生口角，通过在直播间内获得的手机号、微信、住址等信息，纠集众人殴打主播，该用户被认定为触犯寻衅滋事罪判处其拘役五个月。

然而“寻衅滋事罪”被过多的适用于网络空间中公民发表言论的行为，虽然为处理一些案情复杂、定性不准的案件时提供了极大便利，但容易导致该罪边界被随意延伸，违背罪刑法定的基本原则，落入“口袋罪”的范畴。要防止“寻衅滋事”成为“口袋罪”，对公民合法权益造成侵犯，必须严格界定“公共场所秩序严重混乱”等法律要件。只有当言论确实严重扰乱了现实或网络空间秩序，才可能构成“寻衅滋事”。

4.侵犯计算机系统安全类型的犯罪

信息技术是网络直播平台提供服务的基础也是其竞争能力的核心之一，计算

机信息系统安全是网络安全的重要基础。网络直播平台同样可能成为侵犯计算机信息系统安全类犯罪的受害者。不法分子采取侵入、控制、破坏计算机信息系统等手段，非法获取系统中存储、处理或者传输的数据或利用系统漏洞，开发外挂软件等方式对网络平台进行恶意攻击，针对或者利用网络平台实施犯罪行为，以牟取不法利益。

平台数据是各项知识产权、商业利益、玩法内容、商业秘密、用户个人信息、行为数据的集合，数据安全对于互联网企业而言是平台立身之本，也是"逆鳞"所在，绝不容许被肆意侵犯和不当利用，对于故意侵犯计算机信息系统安全类的犯罪行为，直播平台将坚决拿起法律武器予以反击，捍卫用户权益和自身正当权益。

在上海晟品网络科技有限公司抓取今日头条视频数据一案中，被告单位上海晟品网络科技有限公司及被告人张某、宋某、侯某，采用技术手段抓取被害单位服务器中存储的视频数据，并由侯某指使被告人郭某破解北京某网络技术有限公司的防抓取措施，使用"tt_spider"文件实施视频数据抓取行为。"tt_spider"文件中包含通过分类视频列表、相关视频及评论等接口对被害单位服务器进行数据抓取，并将结果存入到数据库中的逻辑。在数据抓取的过程中使用伪造 device_id 绕过服务器的身份校验，使用伪造 UA 及 IP 绕过服务器的访问频率限制。

法院经审理后认为，"爬虫"技术的有效使用有利于数据的共享和分析，但并不意味该技术的使用没有边界。从业人员必须在法律的框架之内合理使用该技术，违反法律规定利用该技术非法获取数据可能构成犯罪。本案的被告公司及被告人在数据抓取过程中，采取了规避或突破被害单位反"爬虫"安防措施的技术手段，未经许可进入了被害单位的计算机系统，属于非法获取计算机信息系统数据罪中"侵入"行为，从而构成了非法获取计算机信息系统数据罪[①]。

在付某利用系统漏洞修改抖音账号信息一案中，付某在浏览抖音相关信息时，发现通过某 e 语言程序编写软件的技术手段就可以修改成网上贩卖的靓号，甚至可以针对"买家"指定的靓号进行篡改，共计篡改近 3000 个抖音账号，致使出现账户充值错误等问题，严重影响抖音账户的管理和系统安全，付某行为构成对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能

① 参见：北京市海淀区人民法院（2017）京 0108 刑初 2384 号判决书

正常运行，目前因涉嫌破坏计算机信息系统罪已被检察机关批准逮捕。

5.诈骗类型的犯罪

网络直播受众广、付费率高、隐蔽性高、跨时空性强等特点不可避免地吸引了不法分子的关注。常见的包括兼职刷单、充值返现、虚假广告、冒充官方客服、提供虚假支付码或钓鱼链接等手段进行诈骗，严重侵犯用户的财产安全和平台运营秩序。直播平台通过关键字识别提醒、充值确认提示以及宣传教育等手段培养用户的防骗意识，对异常账号行为进行监控举报，积极配合公安机关侦查行动，致力于打击网络诈骗等不法行为。但是，网络诈骗属于智能型犯罪，诈骗行为具有隐蔽性、诈骗手段具有多样性、诈骗后果具有严重性，一直是网络犯罪的重灾区。近日还出现了利用平台规则漏洞对平台实施诈骗，非法占有虚拟货币进行充值打赏的恶性诈骗事件，进一步引发业界关注。

2019 年 1 月，一位 ID 为"HAC 无聊哥"的用户在斗鱼平台利用大客户系统漏洞，伪造转账记录，欺骗斗鱼官方人员获取大量鱼翅，进行充值打赏，涉及多位平台头部主播，涉案金额高达数千万元[①]。

三、企业风险防控对策

网络直播平台规模增长趋于稳定，行业发展回归理性，只有真正做到规范化、正规化运营，深挖内容创作，才能让直播行业得到长足的发展。对于网络直播平台犯罪风险的防控，一方面要完善刑法对于网络直播各方主体涉罪行为的评价，严格做到"罪刑法定"，依法对犯罪行为进行打击和惩处，通过国家强制力保障网络直播行业稳定有序发展；另一方面，要明确网络平台主体责任，加强自身监管力度，落实网络安全管理责任，从自身寻求企业突破的着力点。

1.内容审核前置，避免"被动挨打"

建立严格的内容审核机制，敏感内容屏蔽机制，对于涉黄、涉暴、涉赌、涉恐等违法违规内容实现"零容忍"，机器学习配合人工审核，算法过滤配合 AI 智能识别，在直播内容呈现的第一时间完成对内容的精细过滤，保障内容质量，让技术助力内容审核。

全面建立主播培育机制，帮助主播培养法治思维，规范主播言行。主播是平台内容的第一生产力，只有不断培育优质主播才能实现平台内容的规范化，提高

① 参见：斗鱼官方发布的《关于斗鱼账户（HAC 无聊哥）的欺诈声明》

平台竞争力。

打造文明和谐的网络社区文化氛围，规范用户参与行为，培养用户良好的观播习惯，将用户培育成直播文明生态中的重要一环。

深挖内容创造，“直播+”计划助力平台实现内容多样化及精细化布局，将直播延伸至教育、公益、电商等多细分领域，提供真正满足广大网络用户娱乐需求的优质内容，克服内容高度同质化带来的弊病，实现主播、用户和平台互利共赢。

2.严格遵守各项平台规则，保障监管效果

公平合理且行之有效的各项平台规则是保障平台监管效果的必要举措，建立与内容审核标准配套的分类分级违规处理办法，建立违规主播警示名单和黑名单制度，对于不同程度的违法违规行为进行约束，采取诸如屏蔽删除、封号、封 IP、投诉举报等必要举措，对于潜在的违法犯罪行为尽早打击，遏制可能发生的消极效果。

3.积极履行安全管理义务和运营主体责任

作为信息网络服务提供者，网络平台主动承担建立信息安全管理制度、用户身份信息审核、用户发布信息管理、保障个人信息、违法信息处置、信息记录、投诉处理、报告、配合监督检查等各项安全管理义务，明确运营主体责任，提升自身对于犯罪行为的应对能力。

4.发挥行业自律组织的有益作用

对于法律规制在直播领域存在的真空地带以及部分直播平台基于营利目的而可能采取的不正当行为，应发挥行业自律组织的有益作用，应从行业整体出发，不局限于个别企业的短期需求而是从行业长久发展角度出发探索行业发展的最优途径。

非典型网络开设赌场行为的刑法适用

王 刚*

摘要：传统犯罪在网络空间的兴起和发展，是信息化时代的一种犯罪常态。借助于发达的信息网络技术，当前我国网络赌博犯罪呈现出严峻态势，其中又以网络开设赌场犯罪较为常见。建立“赌博网站”或“赌博微信群”是典型的网络开设赌场行为，赌博游戏软件在运营中因违规操作而为他人赌博提供平台的，属于非典型的网络开设赌场行为。非典型网络开设赌场行为的刑法适用，要贯彻企业家保护政策、宽严相济刑事政策以及赌博违法犯罪治理政策。在非典型网络开设赌场行为的刑法定性中，开设、赌博、赌场、抽头渔利是核心要素。关于非典型网络开设赌场犯罪的量刑，要侧重从社会管理秩序、赌博游戏软件的属性以及行为人开发该软件的目的等方面对案件的不法程度和责任程度进行实质评价，不宜采用传统开设赌场罪的量刑思维和“赌博网站型”开设赌场罪的量刑标准。

关键词：非典型网络开设赌场；刑事政策；犯罪认定；量刑标准

一、非典型网络开设赌场行为的概念

（一）案例导入

甲系某网络公司负责人，长期从事网络游戏的开发和运营工作。自 2014 年起，国内的手机麻将 APP 业务开始兴起，吸引大量用户注册和参与。2015 年 6 月，经国家主管部门批准，该公司开发一款“全民麻将”APP，取得计算机软件著作权证书，并于 7 月份投放市场。“全民麻将”APP 是虚拟的麻将网游，玩家从软件后台购买“钻石”打麻将，每十颗“钻石”可以打八局麻将。每局结束后 APP 会显示四位玩家的分数，分数代表玩家的输赢情况。数月后，甲将乙、丙吸收进来，三人共同运营“全民麻将”APP，并由乙负责引入和推广代理的营销模式。乙发展若干名一级代理，一级代理再发展二级代理。代理的操作模式是：代理建立微信群并拉玩家入群打麻将，代理向软件后台购买钻石，群成员向代理购买钻石，代理的购入价格低于卖出价格，代理通过赚取差价而获利。在这些微信

* 王刚，江苏大学法学院副教授，硕士生导师，法学博士。

群里，有的成员纯粹打虚拟麻将，不涉及金钱；有的成员自行约定每分代表的金额，每局麻将结束后输家在群里发红包给赢家。赌资通常在几元至几十元之间，基本都在两百元以下。代理对微信群进行一定管理，如果输家不发红包就退群的，代理会将输家的钱垫付给赢家。“全民麻将”APP 运营半年，涉及“抽头渔利”近三百万元（玩家购买的钻石费用）。

关于本案的定性，主要存在无罪、赌博罪和开设赌场罪三种观点，司法机关倾向于开设赌场罪之说。作为一种新型的涉嫌网络赌博犯罪行为，本案是否构成开设赌场罪、与其他赌博犯罪有何关系、如何量刑等问题，都值得在理论层面进行深入探讨。鉴此，以实务观点为基础，本文拟以开设赌场罪为视角对非典型网络开设赌场行为的刑法适用展开讨论。

（二）概念梳理

我国刑法第 303 条规定了赌博罪和开设赌场罪，赌博罪分为聚众赌博和常业赌博两种类型。开设赌场罪的刑法规定极为简洁，从字面上无法把握其实行行为和犯罪构成，犯罪之认定主要应以赌场的物理特征、功能特征以及实践中赌场的常规运行模式为根据。一般认为，“开设赌场是指行为人以自己为主宰，提供固定场所、专业赌具设备，自己坐庄或招揽他人参加赌博游戏的行为。”[①]

随着信息网络技术的发展及其带来的网络赌博的便利性，网络开设赌场行为逐渐兴起，形成与传统开设赌场犯罪相对应的网络开设赌场犯罪。我国刑法没有规定网络开设赌场犯罪，根据刑事司法解释的规定和指导性案例确立的裁判规则，当前网络开设赌场犯罪主要有下述两种类型：其一，《关于办理赌博刑事案件具体应用法律若干问题的解释》（以下简称《解释》）和《关于办理网络赌博犯罪案件适用法律若干问题的意见》（以下简称《意见》）规定了以“建立赌博网站”为核心要素的开设赌场罪，这可称为“赌博网站型”开设赌场犯罪。其二，最高人民法院公布的第 105 号、106 号指导性案例明确，“以营利为目的，组建、控制微信群，设置赌博规则，以抢红包方式进行赌博的”构成开设赌场罪，这可称为“赌博微信群型”开设赌场犯罪。作为网络开设赌场犯罪载体的“赌博网站”和“赌博微信群”，由于行为人在建立之初即以营利为目的、以组织赌博为方式，并且设置了赌博规则，本质上与传统赌场并无二致。因此，建立“赌博网站”或

[①] 许晓娟、张龙：《对在住宅中开设赌场的认定分析》，载《法学杂志》2015 年第 11 期，第 108 页。

“赌博微信群”属于典型的网络开设赌场行为。

虽然我国刑法和司法解释没有规定赌场的含义及开设赌场的方式，相关司法解释也只是列举了部分形式的赌场，但这并不妨碍司法人员对刑法中的“开设赌场”进行实质理解并将有关涉案对象解释为赌场，从而将案件定性为开设赌场罪。例如，“两高”一部制定的《关于办理利用赌博机开设赌场案件适用法律若干问题的意见》（以下简称《赌博机意见》）规定：设置赌博机组织赌博活动的，应当认定为刑法规定的“开设赌场”行为。据此规定，可将“两高”一部关于“开设赌场”的观点归纳如下：未经国家主管部门许可，为他人赌博（赌资大小没有要求）提供场所、平台、设备的，是开设赌场行为。在“全民麻将”APP 案中，作为涉嫌犯罪之载体的 APP 本是合法游戏软件，而不是非法产品或赌博工具、场所，这是本案区别于典型网络开设赌场犯罪的根本特征。本案之所以涉嫌开设赌场罪，主要是因为采用了代理模式这种不当的营销方式。申言之，虽然“全民麻将”APP 并不天然地是赌博工具或赌博场所，但在采用代理的营销方式之后，代理组建微信群、拉人入群并加以管理、群成员在 APP 上赌博并用微信红包结算，此时这种微信群与赌场就具有相似的功能了。根据《赌博机意见》的精神，赌博游戏软件在运营中因违规操作而为他人赌博提供场所或平台的，可能涉嫌开设赌场罪，此即本文所界定的非典型网络开设赌场行为。

二、非典型网络开设赌场行为刑法适用的政策取向

非典型网络开设赌场行为是信息经济的产物，在工业经济向信息经济迈进的过程中，在信息经济蓬勃发展的历史进程中，由于网络立法的滞后性、司法认知的偏差性以及网络从业人员刑事合规意识不强等因素的影响，类似的非典型网络开设赌场行为必将日渐增多。从宏观上分析这类案件刑法适用的政策取向，有助于司法人员摆脱个案的局限，准确把握案件的危害程度和处罚尺度，为妥当适用刑法奠定基础。

（一）企业家保护政策

以“全民麻将”APP 案为例，与传统开设赌场犯罪和典型网络开设赌场犯罪相比，非典型网络开设赌场行为具有以下显著特征：在行为载体方面，赌博游戏软件是合法的网络服务产品，并且通常获得国家主管部门的确权和认证，而不是非法的赌具或赌场；在行为主体方面，行为人一般是从事信息产业方面的企业家，

而不是职业赌头；在运营主体方面，信息网络公司是合法企业，对科技创新、就业和国家税收等都有不同程度的贡献，而不是专门开设赌场的人或企业；在行为动机方面，行为人开发和运营赌博游戏软件是为了赚取合法经营收入，而不是通过组织他人赌博并抽头渔利来获利。由此可见，尽管非典型网络开设赌场行为涉及的罪名归属于妨害社会管理犯罪，但此类行为主要是因为行为人在信息经济活动中对网络空间法律风险的认知不足而引起的不法类型，从行为角度仍可归入经济犯罪范畴，从行为人角度则可归入企业家犯罪范畴。因此，网络开设赌场行为的刑法适用应当贯彻中央经济工作会议和习近平总书记在民营企业家座谈会中提出的有关保护企业家的规定和要求，将其与传统开设赌场犯罪和典型的网络开设赌场犯罪区别对待。正如习近平总书记所指出的：对一些民营企业历史上曾经有过的一些不规范行为，要以发展的眼光看问题，按照罪刑法定、疑罪从无的原则处理。

（二）宽严相济刑事政策

宽严相济刑事政策要求，根据犯罪的具体情况实行区别对待，做到该宽则宽，当严则严，宽严相济，罚当其罪。按照《关于贯彻宽严相济刑事政策的若干意见》的规定，即使非典型网络开设赌场行为构成犯罪，也属于应当从宽处罚的案件范围，原因有以下几点：一是犯罪性质轻微，属于非暴力的经济性犯罪；二是犯罪情节较轻，一般没有严重的犯罪情节；三是不法程度较低，对相关法益造成的损害极小；四是罪责程度较小，没有卑劣的犯罪动机，主观恶性不深。总体而言，除了涉及人数较多以外，非典型网络开设赌场犯罪的不法性和罪责性都无法与传统开设赌场犯罪和典型网络开设赌场犯罪相比。况且，此类案件之所以涉及人数众多，是由赌博游戏软件的便捷性决定的，但这一因素也不能用于评价行为的社会危害性。

（三）赌博违法犯罪治理政策

“全民麻将”APP 上的赌资很小，一般都在一两百元以下，玩家以消遣娱乐、消磨时间为目的。玩家都是普通百姓，以居家女性为主，一般不涉及起其他违法犯罪。因此，“全民麻将”APP 本质上是一种网络棋牌室，只是因为没有得到国家许可而涉嫌开设赌场罪。对于娱乐性赌博和棋牌室问题，我国历来采取宽缓的治理政策。2005 年“两高”一部制定的《关于开展集中打击赌博违法犯罪活动

专项行动有关工作的通知》（以下简称《通知》）规定：“要严格区分赌博违法犯罪活动与群众正常文娱活动的界限，对不以营利为目的，进行带有少量财物输赢的娱乐活动，以及提供棋牌室等娱乐场所并只收取固定的场所和服务费用的经营行为等，不得以赌博论处。”同年 11 月，《解释》第 9 条重申了这一要求。既然“全民麻将”APP 上的“赌博”基本属于国家政策允许的群众正常文娱活动，并且采用线下棋牌室的经营方式收取固定服务费，即使相关人员构成开设赌场罪，也应当从宽处理。

三、非典型网络开设赌场犯罪认定中的主要问题

非典型网络开设赌场行为在行为主体、行为方式和行为动机等方面与传统开设赌场犯罪、典型网络开设赌场犯罪都有较大区别，在罪与非罪的认定上存在较多疑难问题。非典型网络开设赌场犯罪与其他犯罪具有密切的关联性，在此罪与彼罪的界分上也有不少争议。

（一）罪与非罪认定中的疑难问题

1. 主体的确定

如前所述，在非典型网络开设赌场案件中，赌博游戏软件由合法的信息网络公司开发和运营，行为主体是单位而不是个人。根据我国《刑法》第 30 条和第 303 条的规定，这种情况因不构成单位犯罪而应作无罪处理。但是，2014 年全国人大常委会制定的《关于<中华人民共和国刑法>第三十条的解释》又为自然人构成非典型网络开设赌场罪提供了认定依据。尽管有学者对该立法解释提出过批判，认为其“变相地将单位犯罪扩大于所有犯罪”，[①]但是从司法者的角度来说，据此规定认定自然人构成开设赌场罪也是无可厚非之事。因此，即使行为主体是单位，也可以单独追究自然人开设赌场罪的刑事责任。

2. “开设”的含义

“开设”是开设赌场罪的实行行为，其字面含义是开创、设立的意思。此为一个无中生有的过程，即原本没有赌场，行为人开创、设立了赌场。由此可见，“开设”是刑法上的“作为”，不作为无法“开设”赌场，一般不是开设赌场罪的实行行为。“开设”的这一属性在传统开设赌场犯罪和典型网络开设赌场犯罪中没有疑问，但在非典型网络开设赌场犯罪的认定中却遭遇了诘问。

① 刘艳红：《“规范隐退论”与“反教义学化”——以法无明文规定的单位犯罪有罪论为例的批判》，载《法制与社会发展》2018 年第 6 期，第 109 页。

“开设”的对象是赌场，赌场是专门供人赌博的场所，人们在赌场中按其要求参与赌局的即是赌博。在非典型网络开设赌场犯罪中，赌博游戏软件仅仅提供了虚拟的赌博场景，其既不是真正的赌博平台，也不是天然的赌博工具，是玩家的自我选择决定了其是否具有赌博功能。这就如同扑克牌，既可以是单纯的游戏工具，也可以成为赌博工具。因此，信息网络公司开发和运营赌博游戏软件的行为显然不是“开设”赌场行为。

那么，代理组建微信群、拉人入群并对群成员进行一定管理，是否属于“开设”赌场行为呢？开设赌场罪的运行模式是，赌场是赌博的前提和场所，赌博依附于赌场，无赌场则无赌博。但在非典型网络开设赌场案件中，代理组建的微信群与群成员赌博之间并不存在这种赌博与赌场之间的依附关系：一方面，群成员可以自行组群并进行赌博，无须以代理组建的微信群为赌博前提和场所；另一方面，即使群成员加入代理组建的微信群，也可能只打虚拟麻将而不赌博。换言之，群成员想不想赌博、能不能赌博、赌大还是赌小均不受代理控制或者微信群影响，微信群不具有典型赌场的功能特征，至多是为群成员赌博提供了便利条件或营造了赌博氛围。在我国刑法规范没有明确规定“开设”和“赌场”含义的情况下，司法人员对“开设”和“赌场”的把握应以现实生活中开设赌场罪的行为样态为参照，而不能过于泛化地理解。基于此，将代理组建微信群、拉人入群并进行一定管理的行为解释为“开设赌场”行为，有类推解释之嫌。

3. “赌博”的界定

在开设赌场犯罪中，赌场为赌博提供场所或者平台，赌博在赌场中进行，赌场与赌博之间又存在一种反向依存关系。如何理解赌博和赌场，实务中有不同看法。有观点认为，赌资在两百元以下的“赌博”不是赌博，而是群众正常的文娱活动。[①]其理由是，《通知》和《解释》都规定，带有少量财物输赢的娱乐活动以及经营棋牌室的，不得以赌博论处。因此，为赌资在两百元以下的“赌博”提供场所或平台的，不是开设赌场行为，不构成开设赌场罪。

笔者认为，对于以上观点，应当一分为二地看待。一方面，从形式逻辑的角度分析，上述观点有其合理之处。赌场的设立目的和运营基础是为赌博提供场所

[①] 需要注意的是，部分地区已经提高了赌博违法的数额标准。例如，江苏省公安厅2019年3月13日发布的《赌博违法案件裁量指导意见》规定，参与其他赌博活动，个人独资或者人均赌资500元以上、不满2000元的才受处罚。

或平台，赌场依附于赌博存在，无赌博则无赌场。在“全面麻将”APP案中，微信群里的赌资基本都在两百元以下。根据《通知》和《解释》的规定，这类“赌博”不属于规范意义上的赌博，微信群不能被认定为赌场，从而决定本案不构成开设赌场罪。另一方面，从刑法教义学层面分析，上述观点也有不妥之处，因为赌资数额不是决定行为是否为事实赌博以及赌博场所是否为赌场的因素。理由是：其一，赌博是个事实概念，其本质是“就偶然的输赢以财物进行赌事或者博戏的行为”[①]，凡以偶然输赢为条件、以财物转移为代价的行为都可以说是赌博。事实意义上的赌博包含作为违法现象的规范意义上的赌博，处罚赌博的赌资标准只是国家为了控制处罚范围而设定的门槛，在此赌资标准之下和之上的两类赌博没有本质区别。相关法律规范主要基于社会政策方面的考量，没有对赌博采取完全禁绝的态度，而是采用分段处理的思路：将赌资在两百元以下的赌博视为群众娱乐，将赌资在两百元以上的一般赌博作为治安违法处理，将以营利为目的的聚众赌博和常业赌博作为犯罪处理。由于现行法律规范没有规定成立开设赌场罪的赌资标准，因此，赌资在两百元以下的“赌博”虽然不是规范意义上的赌博，但仍是事实意义上的赌博，并且可能构成赌博罪。其二，开设赌场罪主要侵犯社会公共秩序和国民健康的经济生活方式等公共法益，[②]其直接的不法性通常在于主动、积极地吸引、诱导、鼓动、欺骗多人、多次或长期赌博，从而对家庭生活、社会秩序、健康的社会风气造成消极影响。尽管赌资在两百元以下的赌博社会危害性较小，但如果是在赌场中进行，则其性质和危害性都将远甚于娱乐性赌博，会对开设赌场罪的保护法益造成侵害。其三，根据我国有关司法解释的规定，赌资数额大小不影响开设赌场罪的成立。如前所述，《赌博机意见》将设置赌博机、组织赌博活动的认定为开设赌场罪。常见的赌博机如“老虎机”，投币一元最多可以赌十次，即最小赌资是一元。实践中单人、单次玩“老虎机”的赌资往往都在几元至几十元之间，但放置老虎机者仍然构成开设赌场罪。

综上分析，由于我国刑事司法解释存在矛盾，导致赌资为两百元以下的“赌博”是否属于规范意义上的赌博以及能否成为开设赌场罪中的赌博，存在两种截然不同的观点和结论，从而决定非典型网络开设赌场行为的刑法定性有两种相反的结果：根据《解释》和《意见》的规定，不构成犯罪；根据《赌博机意见》的

[①] 张明楷：《刑法学》（第五版）（下），法律出版社2016年版，第1078页。
[②] 参见张明楷：《刑法学》（第五版）（下），法律出版社2016年版，第1078页。

精神，构成犯罪。

4. “抽头渔利”的地位

“抽头渔利”俗称“抽水”，是指赌场根据一定比例从赌客的赌资中提取费用。抽头渔利数额具有不确定性，其取决于赌资数额和抽头比例。在实践方面，传统赌场一般均以抽头渔利方式获利；在规范层面，《解释》和《意见》等司法解释对抽头渔利作了规定。但是，非典型网络开设赌场案件中不存在抽头渔利的情形，行为人是通过收取固定服务费来获利的，这与日常生活中棋牌室的营利方式一样。那么，抽头渔利是否是开设赌场罪的必备要素，从而也是决定非典型网络开设赌场罪成立的必要条件呢？笔者认为答案是否定的，理由主要有以下三点：其一，是否营利不是开设赌场罪的必备要素。《刑法修正案（六）》将开设赌场罪独立出来，并且取消了“以营利为目的”的主观构成要素。因此，是否营利不再是开设赌场罪的构成要素，作为营利方式的抽头渔利自然也不能决定网络开设赌场犯罪是否成立。其二，有关赌博犯罪司法解释没有规定抽头渔利问题。《赌博机意见》虽然规定放置赌博机的构成开设赌场罪，但没有规定抽头渔利，这说明“两高”一部也不认为抽头渔利是开设赌场罪的必备要素。其三，赌场形态随着时代发展而不断变化，营利方式也会有所改变，以抽头渔利这种营利方式来限定开设赌场罪的成立范围，不具有现实合理性。

综上分析，非抽头渔利的营利方式不应成为阻却非典型网络开设赌场罪成立的事由。但需要注意的是，我国赌博犯罪司法解释多以抽头渔利数额作为量刑标准之一，既然非典型网络开设赌场犯罪中没有抽头渔利情形，则不能以抽头渔利数额作为量刑标准。

（二）此罪与彼罪界分中的争议问题

开设赌场与聚众赌博之间具有交叉性，因此非典型网络开设赌场犯罪与赌博罪存在竞合的空间。在非典型网络开设赌场犯罪中，赌博游戏软件的运营者和代理之间存在微妙关系，双方关系的紧密程度也会影响案件的定性。

1. 非典型网络开设赌场行为与赌博罪的关系

开设赌场供他人赌博的构成开设赌场罪，以营利为目的聚众赌博的构成赌博罪。由于这两种犯罪在“存在赌博场所”和“聚集众人赌博”两方面是重合的，实践中如何区分二者较为困难。有观点认为，“开设赌场的行为人对赌博场所、

赌博的内部组织和赌场经营等整个赌博活动都具有明显的控制性、支配性；而聚众赌博则不具有这种控制性，通常只是表现为召集、组织、聚众等行为。”[①]该观点颇有道理，但仍有深化的空间。笔者认为，区分开设赌场罪与聚众型赌博罪应重点考虑以下几个方面。其一，在空间方面，是否以专门的赌场作为赌博场所。赌博一定需要场所，但赌博场所未必都是赌场。开设赌场罪以设立赌场为前提，聚众型赌博罪则无此要求，这是区分二者的关键因素。赌场一般具有人、财、物三方面的物理特征和专门用于赌博的功能特征：在“人”方面，赌场有出资人，有专人负责管理和维护事务，甚至还有人负责接送赌客，相关人员在赌场中领取劳务报酬；在“财”方面，赌场一般都会提供筹码，并向赌客出借赌资；在“物”方面，赌场有完备的赌博设施和工具，有的还提供烟酒和饮食。此外，赌场一般专门用于赌博，而不用于其他生产或生活。非赌场的赌博场所，不可能完全具备上述特征。其二，在人员方面，参赌人员是否较为固定、相互熟悉、有无流动性。在开设赌场罪中，赌场是公共场所，行为人希望通过招揽大量赌客来实现利益最大化，因此，参赌人员一般不固定、相互不熟悉、流动性大。相反，聚众赌博一般是熟人之间相邀赌博，人员较为固定、流动性小。其三，在犯意方面，行为人是否有通过收取参赌人员费用来获利的目的。开设赌场罪的行为人显然是以“抽头渔利”为犯罪动机，聚众型赌博罪的行为人是以赢钱或满足赌欲为犯罪动机，二者有明显区别。

综上分析，在非典型网络开设赌场案件中，赌博游戏软件不太符合赌场的空间特征，行为人比较符合赌场的犯意特征，参赌人员特征尚且难以准确评判。因此，将赌博游戏软件界定为赌场并非没有疑问。本着疑罪从轻和有利于被告人的原则，将非典型网络开设赌场行为定性为聚众型赌博罪也是可以考虑的方案。

2. 非典型网络开设赌场行为与帮助信息网络犯罪活动罪的关系

在非典型网络开设赌场案件中，赌博游戏软件运营者和代理的行为是相互分离的。代理的行为是正犯行为，涉嫌开设赌场罪或聚众型赌博罪，运营者行为的定性依附于代理的行为。根据运营者对代理的行为是否具有明知或控制，其行为定性分为三种情形：其一，运营者对代理组建的微信群中存在赌博缺乏认识的，不构成犯罪；其二，运营者仅明知代理组建的微信群中存在赌博的，如果代理的

[①] 宋君华、邢宏伟、陈启辉：《开设赌场罪与聚众赌博罪之区分应重点判断行为人对赌博活动的控制性》，载《中国检察官》2012年第12期，第63页。

行为构成开设赌场罪或聚众型赌博罪，则运营者涉嫌构成帮助信息网络犯罪活动罪；其三，运营者授意、指使、组织代理组建微信群并明知其中存在赌博的，如果代理的行为构成开设赌场罪或聚众型赌博罪，则运营者涉嫌构成共同犯罪。

四、非典型网络开设赌场犯罪量刑标准的反思

我国《刑法》、《解释》和《意见》都没有明确规定开设赌场罪的量刑标准，《意见》规定了“赌博网站型”开设赌场罪中“情节严重”的认定标准。因此，关于非典型网络开设赌场犯罪，目前尚无法定的量刑标准，而且也不能根据《意见》的规定来认定“情节严重”。

第一，非典型网络开设赌场行为的害恶性与传统开设赌场犯罪不具有可比性，不能以传统开设赌场罪的量刑思维来指导量刑。

罪行轻重决定刑罚配置，罪行轻重主要由行为的客观危害性和行为人的主观恶性决定。传统开设赌场犯罪的客观危害性和主观恶性极大：在客观方面，一方面涉及巨额赌资，动辄百万、千万甚至上亿，另一方面涉及职业赌徒、赌博利益链和赌博关联犯罪，如赌博犯罪团伙、高利贷、暴力犯罪、黑社会性组织犯罪、跨国性的赌博组织等。一般人在赌场赌钱必定会输钱，为了赢回赌资往往会输得更多，输光后往往会借高利贷，借贷后通常还不起，还不起后即会卖车卖房或四处躲债，这是传统开设赌场犯罪的基本逻辑。在主观方面，行为人通常会想法设法引诱好赌且有钱之人进入赌场，甚至对好赌、无钱但其亲属有一定财力的人也不放过，意图通过参赌者欠下赌债来间接地逼取其亲属的钱财。因此，传统开设赌场犯罪不仅会给参赌人造成重大财产损失，往往还会殃及其家人或亲属，并且掺杂着其他类型犯罪。立法者为开设赌场罪配置的刑罚，是建立在这种犯罪常态基础上的。由于非典型网络开设赌场行为完全不具备上述害恶性，故不能沿用传统开设赌场罪的量刑思维来指导量刑。

第二，非典型网络开设赌场行为不符合“赌博网站型”开设赌场犯罪的行为类型，不能参考《意见》规定的量刑事实进行量刑。

赌博网站一般有以下特征：一是设置赌博规则。参赌人员投注后必须按照赌博网站设置的规则赌博，赌博网站设置的赌博规则和参赌人员的投注金额决定输赢情况。二是接受投注。投注就是投入一定数额的金钱作为赌博筹码，参赌人员投入的金钱在赌博网站上转换为虚拟货币。在流程上，参赌人员先投注，再根据

赌博规则进行赌博。三是具有反向兑现功能。参赌人员在赌博网站上拥有的虚拟货币，可以从赌博网站上直接兑换为现金。但类似“全民麻将”APP 的软件完全不具备上述特征，显然不是赌场网站。根据罪刑法定原则，不能参考《意见》规定的量刑事实来裁量非典型网络开设赌场犯罪的刑罚。

第三，非典型网络开设赌场行为不具有“赌博网站型”开设赌场犯罪的常规社会危害性，不能以《意见》的规定来认定“情节严重”。

《意见》规定了抽头渔利数额、赌资数额、参赌人数等认定“赌博网站型”开设赌场罪“情节严重”的标准，但这些标准也不能用以认定非典型网络开设赌场犯罪是否达到“情节严重”。这是因为，“赌博网站型”开设赌场犯罪的害恶性，[①]也要显著大于非典型网络开设赌场犯罪。原最高人民检察院理论研究室主任陈国庆等人在《<关于办理网络赌博犯罪案件适用法律若干问题的意见>理解与适用》一文中指出：2010 年起全国范围内集中整治网络赌博违法犯罪专项活动，铲除了一批境外赌博集团在境内的据点，打击了大部分境外主要赌博网站在境内上层组织及为其提供相关帮助的利益链条；当前网络赌博的组织形式主要是由境外赌博集团通过逐层发展股东、总代理、代理、会员，形成庞大的金字塔形组织结构，一个赌博网站经常涉及全国数万人甚至数十万人。[②]实践中，“赌博网站型”开设赌场犯罪的危害性已经在“横向”扩散：一是开设冲击我国的经济秩序，二是通过与网络诈骗的结合来侵犯财产权，三是通过与电子交易支付平台的结合来破坏金融管理秩序，四是成为催生其他网络犯罪的平台。[③]类似“全民麻将”APP 的案件不具有上述危害性，根据罪责刑相适应原则，不能以《意见》规定的量刑标准来认定非典型网络开设赌场罪达到“情节严重”的程度。

此外，“情节严重”的开设赌场罪，是在基本犯罪形态的基础上具备更为严重事实的犯罪形态。一般来说，基本犯的成立条件是，通过对案件中各种主客观构成要素的综合评价，达到了应当进行刑罚处罚的严重程度，行为、结果、行为对象、主观恶性等都是影响犯罪成立的因素；加重犯的成立条件是，案件在具备基本犯成立条件的基础上出现了更加恶劣的情节或更加严重的事实。在决定基本

① 害恶性，泛指犯罪的客观危害与主观恶性。参见邱兴隆：《刑罚理性导论——刑罚的正当性原论》，中国政法大学出版社 1998 年版，第 13 页。

② 参见陈国庆、韩耀元、吴峤滨：《<关于办理网络赌博犯罪案件适用法律若干问题的意见>理解与适用》，载《人民检察》2010 年第 20 期，第 41 页。

③ 参见于志刚：《网络开设赌场犯罪的规律分析与制裁思路——基于 100 个随机案例的分析和思索》，载《法学》2015 年第 3 期，第 143 页。

犯或加重犯成立的构成要件要素中，某种要素的危害性指标高，其他要素的危害性指标要求就低；反之，其他要素的危害性指标要求就高。例如，盗窃、诈骗的入罪标准是数额较大，抢劫罪却无此要求。这是因为盗窃、诈骗在行为方面的危害指标低，故立法者在考虑入罪时设置了数额要求；抢劫由于在行为方面的危害指标高，立法者没有为其设置入罪的数额标准。实际上，在许多犯罪中，数额都不具有表征犯罪严重程度的主导地位，过于偏爱犯罪数额的司法实践也在被逐步纠正，《刑法修正案（九）》对贪污贿赂犯罪量刑标准的修改即是实例。

由上可见，不能仅仅根据《意见》规定的标准来判断非典型网络开设赌场犯罪是否属于“情节严重”，而是要对案件的客观危害性和主观恶性进行综合评估。即使案件在某些方面符合《意见》规定的“情节严重”标准，由于此类案件一般不具备开设赌场罪的常规害恶性，整体上也未必达到“情节严重”的程度。在客观方面，“全民麻将”APP 是合法的游戏软件，本质上就是网络棋牌室，并非违法产品。在主观方面，“全民麻将”APP 运营者的违法性认识低，主观恶性较小。APP 运营者长期从事网络服务产品的开发和运营工作，“技术中立”是这一群体根深蒂固的观念，这种深刻地影响着行为人的违法性认识。刑法是一种行为规范，但公民往往并非通过阅读刑法条文来规范自己行为，而是通过观察公权力部门对各种行为的处理来了解刑法禁止什么行为。当某种行为长期由国民公开实施，为一般人所认可，公权力不予制止时，国民就不可能预测到该行为是犯罪行为。[①]相应的，当某个行业中具有重大影响力的事件被公权力所认可时，这个圈内的人就很难预见到这种行为的违法性。2016 年 12 月 15 日，昆仑万维（13.780,0.38, 2.84%）发布公告称，作价 20 亿收购闲徕互娱 100%股权。其间，证监会对该模式是否涉赌问题进行了询问，并由律师团进行论证得出结论该模式并不违法。昆仑万维还附上了保荐机构中国国际金融股份有限公司和律师北京市天元律师事务所对于此事的意见，其中指出《闲来麻将》不构成赌博违法或犯罪。作为麻将软件行业领头羊的《闲来麻将》没有被证监会处罚，没有被司法机关追究刑事责任，显然容易使其他麻将软件的开发者和运营者们误以为，麻将 APP 不具有违法性。

综上所述，非典型网络开设赌场犯罪的法定量刑标准缺失，其实际的害恶性与传统开设赌场罪和“赌博网站型”开设赌场罪相去甚远，无论基于形式解释还

[①] 张明楷：《避免将行政违法认定为刑事犯罪：理念、方法与路径》，载《中国法学》2017 年第 4 期，第 39 页。

是实质解释，都不能沿用传统开设赌场罪的量刑思维来思考此类案件的量刑问题，也不能以《意见》规定的量刑标准作为此类案件的量刑依据。同时，结合前述刑事政策考量和人权保障原则，也不能轻易地将非典型网络开设赌场罪认定为“情节严重”。

我国彩票销售网络平台犯罪治理

宫步坦*、钟佳佳**

内容提要：以网络方式销售彩票有着明显优势，也引发了新的犯罪问题。依据《彩票管理条例》和《彩票管理条例实施细则》，从体系解释的角度来看，未经国务院特许，擅自发行、销售福利彩票、体育彩票之外的其他彩票的行为，或在中华人民共和国境内发行、销售境外彩票的行为，或互联网销售彩票平台自行增加福利彩票、体育彩票的品种和彩票游戏并加以销售的行为，可能构成非法经营罪。部分彩票销售网站存在的“吃票”行为，根据具体情况不同，可能涉嫌非法经营罪或诈骗罪。对销售彩票的网络平台可能构成犯罪的这四种情况，可以从立法、行政、行业协会、彩民四个角度予以治理。

关键词：彩票销售网络平台；非法彩票；非法经营罪；犯罪治理；

彩票是由人们自愿购买并能够证明购买人拥有按特定规则获取奖励的书面凭证，是一种建立在机会均等基础上的娱乐性游戏。我国现行的两大彩票系列即福利彩票和体育彩票，分别由国务院民政部门和体育行政部门负责管理工作。全国各地区依照公开、公平、公正的原则承销彩票，自二十世纪八十年代正式发行以来，彩票对我国的民政福利事业与体育事业的长足发展做出了突出贡献，根据2018年8月29日发布的《财政部公布2017年彩票公益金筹集分配使用情况》①，仅2017年一年，全国发行销售彩票总金额为42,666,909万元，其中福利彩票机构发行、销售彩票21,697,680万元，体育彩票机构发行、销售彩票20,969,229万元。

计算机的发明和普及使我们迈入信息时代，互联网的迅猛发展将我们生存的家园变成“地球村”，每一个人、每一种产业都是网络中的节点。从宏观角度，信息通信技术以及网络平台有助于优化和集成生产要素的配置，进而使传统行业

*宫步坦，湖北省律师协会网络信息法律专业委员会主任，武汉市法学会社会纠纷多元化解研究会会长，武汉市武昌区洪山侧路22号，430071
**钟佳佳，湖北金卫律师事务所律师，武汉市武昌区中北路126号德成中心裙楼3号门3楼，430071，13545347713
①数据来源：http://www.lottery.gov.cn/gyjzygg/20180829/68633.html，最后访问时间2019年3月8日。

焕发新的活力；从微观角度，互联网渗透居民生活的方方面面，包括我们购买彩票的方式。2005年我国互联网销售彩票兴起，互联网彩票销售总额从最初的1亿元增长到2014年的850亿元，而2014年全国彩票销售总额为3823.78亿元②，通过网络购买的彩票销售额超过全国彩票销售总额的五分之一。各大网络平台纷纷进入彩票行业，如中国竞彩网、淘宝彩票、百度旗下的乐彩网等。其中500彩票网作为我国首家在线销售彩票的网站，建立了网售彩票的完整商业模式①。

互联网与彩票的结合为我国彩票行业及公益事业带来新的发展机遇，也产生了新的问题。近年来，随着移动支付的跨越式发展，电子商务迈入新的发展阶段，在线购买彩票的市场需求渐涨，与之相反，互联网销售彩票的监管却日益严格。彩票销售网络平台的诸多违法行为引起多方关注，各地公安机关以涉嫌非法经营罪对众多互联网彩票从业者立案侦查，但仅有部分案件获得法院判决支持，彩票销售网站的违法行为是否都构成犯罪，值得我们认真研究②。另一方面，动辄以刑事手段处理互联网销售彩票问题能否达到预防犯罪之目的，也值得商榷。

笔者近年来承办全国各地的互联网销售彩票涉罪案件，频繁与办案单位、各彩票销售网络平台交流沟通，掌握了大量第一手资料，并在《检察日报》、《民主与法制时报》等刊物上发表《论互联网销售彩票定罪问题》、《未经委托在网上销售彩票不宜定罪》、《再论互联网销售福利彩票、体育彩票不宜定罪》等论文，以期厘清此类案件的定罪标准。本文拟从犯罪防控角度出发，梳理网络平台销售彩票的发展历程及现状，全面分析网络平台销售彩票各种违法行为的入罪标准，据此提出对治理此类犯罪的初步思考。

一、网络时代彩票销售的发展历程及现状

我国对彩票问题及网络彩票发行、销售的规制经历了一个变化的过程。

（一）限制发展时期

2005年5月11日“两高”《关于办理赌博刑事案件具体应用法律若干问题的解释》（以下简称《司法解释》）第6条规定：“未经国家批准擅自发行、销售彩票，构成犯罪的，依照刑法第二百二十五条第(四)项的规定，以非法经营罪

②数据来源：https://sports.qq.com/original/inside/sd316.html，《850亿！互联网彩票为何说停就停》，最后访问时间2019年3月9日。
①参见“360百科”词条“500彩票网”：https://baike.so.com/doc/6994618-7217492.html，最后访问时间2019年3月18日。
②宫步坦、刘斯凡：《互联网销售彩票数亿元 被追诉律师辩护获无罪》，载《律师世界》，2015年第2期。

定罪处罚。”2009年5月4日国务院发布《彩票管理条例》（同年7月1日起施行，以下简称《条例》），其中第3条规定：“国务院特许发行福利彩票、体育彩票。未经国务院特许，禁止发行其他彩票。禁止在中华人民共和国境内发行、销售境外彩票。”《条例》第15条规定，由国务院部门、体育行政部门依法设立的彩票发行机构和由省级人民政府民政部门、体育行政部门依法设立的彩票销售机构，都可以委托单位、个人代销彩票。《条例》的颁布进一步规范了彩票市场，彩票的发行、销售、开奖、兑奖以及资金管理等都有据可循。

基于当时互联网销售彩票平台确实为彩票行业及国家公益事业带来新的发展机遇，2010年9月26日财政部发布《互联网销售彩票管理暂行办法》（以下简称《暂行办法》），其中明确规定了受彩票发行机构委托或与彩票发行机构、彩票销售机构合作在互联网上销售彩票的准入条件，首次将受委托或合作在互联网上销售彩票确定为一种合法销售彩票的方式。此后，我国的彩票市场规模特别是互联网彩票销售总额持续走高，也伴生出新型的彩票销售违法行为。2012年1月18日财政部、民政部、体育总局联合发布《彩票管理实施细则》（同年3月1日起实施，以下简称《旧细则》），将《条例》内容进一步细化，明确规定了“非法彩票”的内涵。针对互联网彩票市场，财政部又于2012年9月29日发布《关于开展互联网销售体育彩票试点相关工作的通知》（财办综[2012]82号）[①]，同意国家体育总局体育彩票管理中心委托中体彩彩票运营管理有限公司、深圳市易讯天空网络技术有限公司试点开展互联网代理销售体育彩票业务。由此获得官方部门委托的试点彩票网站限定于上述两家公司分别经营的竞彩网、500彩票网。鉴于财政部2012年12月28日发布的《彩票发行销售管理办法》（以下简称《管理办法》）第5条明确规定彩票发行方式包括互联网销售，竞彩网和500彩票网迎来了发展黄金期，500彩票网更乘势于2013年11月22日在纽交所成功上市[②]。

（二）全面禁止时期

除上述两个“法定”试点网站之外，还有大量网站擅自经营在线销售彩票业务，关于彩票销售网站的新问题层出不穷。有些“地下彩庄”利用互联网将自己

①参见新浪博客：http://blog.sina.com.cn/s/blog_507de1780102f9xx.html，最后访问时间2019年3月18日。
②参见500彩票官方网站：http://www.500.com/about/，最后访问时间2019年3月18日。

包装成后，发行“私彩”牟利。有的彩票网站存在“吃票”行为，即彩票销售网站声称销售福利彩票、体育彩票并接受彩民在线投注，对中奖号码也完全按照福利彩票、体育彩票的返奖规则予以返奖，但为了牟取更多非法收益，并未将彩民投注的全部金额用于购买福利彩票、体育彩票[①]。对于没有用于购买彩票而被“吃”掉的彩民投注资金，如果网络平台完全按照福利彩票、体育彩票的返奖规则予以全部返奖，因涉及《旧细则》第7条第一种情形，涉嫌非法经营罪；如果网络平台在彩民中奖后，平台未完全按照福利彩票、体育彩票的返奖规则予以全额返奖则涉嫌诈骗罪。

2015年财政部、民政部、国家体育总局联合下发《关于开展擅自利用互联网销售彩票行为自查自纠工作有关问题的通知》，要求自2015年1月15日起，成立自查自纠工作协调小组对系统内彩票销售机构进行自查自纠，重点对行政区域内擅自利用互联网销售彩票行为实施交叉抽查。同年4月3日，财政部、公安部、国家工商行政管理总局、工业和信息化部、民政部、中国人民银行、国家体育总局、中国银行业监督管理委员会联合发布公告（以下简称：八部委《公告》），重申了现行互联网销售彩票的管理政策与相关制度，要求坚决制止擅自利用互联网销售彩票的行为，严厉查处非法彩票，并明确规定：“彩票发行机构申请开展互联网销售彩票，属于变更彩票发行方式，应当按规定经民政部或者国家体育总局审核同意，由彩票发行机构向财政部提出申请，财政部作出书面决定。未经财政部批准，任何单位不得开展互联网销售彩票业务。”[②]

2018年，针对擅自利用互联网销售彩票的行为不断出台更为严厉的政策，财政部、工信部、公安部等12个部委联合下达公告（财政部2018年第105号，以下简称《2018年公告》），要求“坚决禁止擅自利用互联网销售彩票行为”，并称“截至目前，财政部没有批准任何彩票机构开通利用互联网销售彩票业务”。数月来，各地基层公安机关以涉嫌非法经营罪侦办的互联网销售彩票案件，明显增多[③]，互联网销售彩票的众多从业人员以涉嫌非法经营罪被刑事立案及刑事羁

①宫步坦、刘斯凡：《再论互联网销售福利彩票、体育彩票不宜定罪》，载“智善”法律新媒体，2019年1月11日。
②参见中华人民共和国财政部官方网站：http://zhs.mof.gov.cn/zhuantilanmu/caipiaoguanli/201504/t20150403_1212979.html，最后访问时间2017年4月25日。
③宫步坦、刘斯凡：《论互联网销售彩票定罪问题》，载《民主与法制时报》，2019年1月10日理论版。

押，如腾讯彩票业务负责人、新浪彩通负责人等被警方带走接受调查[①]，各网站销售彩票的大量收入被控制或处置，众多网站纷纷关停彩票销售业务。

二、网络彩票销售平台涉非法经营罪的入罪分析

网络与彩票的深度融合既能推动我国彩票事业的蓬勃发展，也会滋生新型犯罪，扰乱市场秩序、破坏社会环境。要发挥彩票事业对我国经济发展的正向激励作用，需要根据上文列举的法律法规，结合《刑法》第二百二十五条的相关规定，厘清网络平台销售彩票行为在何种情况下构成非法经营罪，进而对网络销售彩票平台的不法行为甚至犯罪行为进行分类惩治。

（一）擅自发行、销售彩票行为的罪与非罪分析

根据《条例》和《旧细则》的规定，可能构成非法经营罪的擅自发行、销售彩票行为只有两类：一是未经国务院特许，擅自发行、销售福利彩票、体育彩票之外的其他彩票；二是在中华人民共和国境内发行、销售境外彩票。在互联网上发行、销售上述两类彩票的行为，无疑应当按照非法经营罪论处。[②]

（二）未经财政部批准，在互联网上擅自销售福利彩票、体育彩票品种或彩票游戏的罪与非罪界限

本文所称未经批准擅自销售福利彩票、体育彩票品种或彩票游戏，是指未经国务院财政部门批准擅自销售福利彩票、体育彩票品种或彩票游戏的行为。在互联网上违法发行、销售福利彩票、体育彩票品种和彩票游戏，具体包括两种情况：一种是彩票发行机构未经国务院财政部门批准擅自发行、在互联网上销售福利彩票、体育彩票品种和彩票游戏；另一种是彩票发行机构以外的其他主体擅自发行、在互联网上销售福利彩票、体育彩票品种和彩票游戏。

对于第一种情况，福利彩票、体育彩票的品种和彩票游戏由彩票发行机构擅自发行，互联网经营者只是负责销售。彩票发行机构擅自发行彩票的行为，是在其具有合法的发行权的基础上增加了福利彩票、体育彩票的品种或者彩票游戏，该行为的法益侵害程度明显小于擅自发行福利彩票、体育彩票之外的彩票乃至境外彩票的行为，不构成犯罪。

对于第二种情况，即彩票发行机构以外的其他主体自行增加福利彩票、体育

①少年维特：《互联网彩票大整顿腾讯新浪是最后一站么》，https://www.sohu.com/a/272867539_104421，最后访问时间2019年3月18日。
② 宫步坦、刘斯凡：《未经委托在网上销售彩票不宜定罪》，载《检察日报》，2013年8月28日理论版。

彩票的品种和彩票游戏并加以销售的行为。发行、销售此类彩票的合法性取决于是否获得“财政部批准”，而财政部批准的对象仅限于彩票发行机构。对于其他实体门店经营者或者网络经营者，因为他们不可能具备发行彩票的资质，其自行增加品种和彩票游戏的行为实际上是一种变相发行彩票的行为。该发行和销售行为与发行销售福利彩票、体育彩票之外彩票的行为性质没有实质差异，应当视为未经国务院特许，擅自发行、销售彩票的情形，按照非法经营罪定罪处罚。

综上所述，网络彩票销售平台未经国务院特许，擅自发行、销售福利彩票、体育彩票之外的其他彩票的行为，或在中华人民共和国境内发行、销售境外彩票的行为，或自行增加福利彩票、体育彩票的品种和彩票游戏并加以销售的行为，都可能构成非法经营罪。

三、网络彩票销售平台的犯罪原因分析

（一）网络平台销售彩票的特点

1. 技术实现简单。网络与彩票的结合有天然优势。经过正规渠道合法发行的彩票无论具体是什么品种都有其明确详细的购买和兑奖规则，其票面是采用高度标准化的格式打印的投注单，因而可以满足全国各地区统一发行的需求，也正是基于其公平性，彩票票面本身就是兑奖的唯一凭证。而互联网同样是面对全国的网民，其程序编写的规范化、格式化与彩票有天然的契合点，电子彩票完全可以代替纸质彩票实现其价值，甚至还具备纸质彩票所不具备的独特优势。

2. 购买方便快捷。在可以通过网络方式购买彩票之前，彩民购买彩票只能去各大彩票销售点。虽说销售点分布较广，但是彩民仍然要前往附近的销售点，并且彩票销售实体店有其固定的营业时间，超出该时间范围是无法投注的。若是居住在我国广大农村地区的彩民可能还要途经几十公里去乡、镇上的彩票实体店才能购买到彩票。但是互联网彩票平台兴起后，彩民足不出户可以在线购买彩票，大大节省了时间成本和交通支出，也突破了营业时间的限制，彩票购买变得灵活而快捷。

3. 领奖高效安全。根据众多互联网彩票平台的规则设置，中奖金额若是在一定标准之下，则奖金会直接进入该彩民的购买账户，若是中了大奖则会有专人联系该账号主人，协助进行领奖工作。而在实体店购买彩票即使中了最末等奖，也需要去店内兑奖，有时候彩民在购买彩票之后会发生遗忘，最终因为超过兑奖期

限而被动放弃奖金。同时奖金直接进入购买账户也是更大程度的保证中奖彩民的人身安全和财产安全。

4. 推动公益发展。福利彩票和体育彩票在发行之初都带有强烈的支持社会公益事业发展的目的。我国现行发布的福利彩票的前身是“中国社会福利有奖募捐券”，发行目的是发展以“安老、扶幼、助残、济困”为主要内容的社会福利事业。在新中国建成后第一次发行体育彩票是因为1984年福建省计划在省会福州市兴建体育中心，但是基建资金缺口较大因而发行体育彩票筹措资金[①]。国务院2001年10月30日发布《国务院关于进一步规范彩票管理的通知》(国发〔2001〕35号)，其中规定彩票发行资金构成比例调整为：返奖比例不得低于50%，发行费用比例不得高于15%，彩票公益金比例不得低于35%。财政部2015年11月13日又发布《关于进一步规范和加强彩票资金构成比例政策管理的通知》（财综[2015]94号）中，下调了大部分彩票游戏的发行费比例，且除去将中国福利彩票双色球游戏发行费下调的一个百分点转入该游戏调节基金用于返奖等外，其余的应当全部用于上调相应彩票游戏的公益金比例，可见政府在逐步强化彩票的公益性质。互联网与彩票销售的结合，使我国彩票销售总额开始质的飞跃，极大地支持了我国社会公益事业的发展。

（二）网络彩票销售平台的犯罪动因

1. 彩票收益诱惑巨大

网络销售彩票可以让平台获得比实体店销售更为丰厚的利益。彩票销售实体店即使店面大且位于人口稠密区也总是存在一定的辐射范围，它只能吸引附近的彩民购买彩票，但是网络平台可以突破空间的限制。经营者开设网络彩票销售平台可以吸引全国各地的彩民，相应的彩票销售金额会呈几何倍数的增长。正如马克思所说“一有适当的利润，资本就会非常胆壮起来。只要有10%的利润，它就会到处被人使用；有20%，就会活泼起来；有50%，就会引起积极的冒险；有100%，就会使人不顾一切法律；有300%，就会使人不怕犯罪，甚至不怕绞首的危险。如果动乱和纷争会带来利润，它就会鼓励它们。”[②]网络售彩的巨大销量会给销售平台带来巨大利益，令其不惜触犯刑法。

①参见百度百科“彩票”词条：https://baike.baidu.com/item/彩票/68808，最后访问时间2019年3月13日。
②马克思：《资本论》（第一卷），人民出版社1958年版，第839页。

以前文所述“吃票”现象为例，肇端于彩票网络销售平台出现之后，给平台带来更大的非法利益。在实体店购买彩票，彩民会得到与投注金额相应的纸质彩票，若出现彩票与投注金额不相符的情况彩民能够立即发现，实体店的彩票销售收入最终也都会进入管理部门的指定账户。但在网络售彩平台上，平台往往不向彩民提供纸质彩票，只有记载并不详尽的电子凭证。彩民下注之后，“吃票”的彩票销售平台只将彩民的部分投注资金用来购买福利彩票、体育彩票。在实践中，若彩民中小奖，由于“吃票”网站的利润丰厚，为持续经营的需要，网站会返还奖金；一旦彩民中巨奖，网络平台会迅速关闭以逃避兑奖，再开通新的网络平台重新销售彩票，继续“吃票”。

2. 缺乏合法的网络售彩平台

彩票作为一种游戏存在的基础，是满足参与者生理上和心理上的需要。与一般游戏相比彩票还有着极强的投机性，这与人们总是希望以最少的成本获得最大收益的美好愿望相契合。以福利彩票消费者的购买动机为研究对象，可以发现消费者的动机是多样的，但以物质性为主，以慈善、献爱心和消遣娱乐等精神性为辅共同构成福利彩票购买的综合性动机所占比例最大，多数彩民具有继续购买的意愿，在收入增加的情况下也愿意提高购彩金额，主要原因还是出于希望中奖[①]。彩票是彩民日常生活中的重要组成部分，网络平台购买彩票的诸多优点使彩民具有较强的通过网络购买彩票的意愿，但国内目前尚无合法的网络平台可以在线购买彩票。彩民的网络购彩需求无法通过合法途径得到满足，私设的网络售彩平台填补了彩民的需要。不少私设的彩票网络平台销售福利彩票、体育彩票之外的彩票，如“地下六合彩”或者平台自身发行的新的彩票游戏等。

3. 行政监管与执法力度不足

首先，彩票行业有发行销售机构，也有监管机构，但监管机构力量过于薄弱，无法对彩票市场进行全方位监管[②]。在未出台关于互联网销售彩票的法律规范之前，互联网彩票销售已经呈野蛮生长之势，彩票网站是否按照彩票本身的规则进行销售及兑奖，完全凭借平台运营者、实际控制人的守法意识。随着对彩票销售的规制越来越密集，互联网彩票发行、销售的程序都有章可循，但行政监管与执

①王素娟、赵静、夏恩君：《我国福利彩票消费者构成特征和消费系心理研究》，载《河北企业》，2008年第3期，第41页。
②《保障彩票回归公益亟需制定彩票法》，载《法制日报》，2018年11月20日，第005版。

法力度明显偏弱，导致网络彩票业务平台以身试法后，仍能逃脱制裁。低廉的违法成本无法起到震慑、预防犯罪的作用，更增加了违法者的侥幸心理。其次，对网络销售彩票的监管技术偏弱。例如打击上文所述的线上“私彩”，首先要发现线上销售“私彩”的线索，然后要运用技术手段对其进行调查、收集证据，待证据确凿、形成完整的证据链条后，再施以行政处罚甚至移交司法机关。最后，存在地方保护主义。省级彩票管理中心为扩大彩票销售金额，往往同意或默许与网络销售彩票平台实现数据对接。假如出现全国性的官方网络销售彩票平台，省级彩票管理中心负责的彩票销售金额将会大大降低，省级自留部分也会大大减少。

四、彩票销售网络平台犯罪的治理对策

购买股票与购买彩票相似，但股民的证券买卖操作早已实现了无纸化，都是在网上完成。网络彩票销售平台确实存在犯罪活动，但不应当因噎废食，完全禁止互联网形式的彩票销售活动。我们应该从彩票销售网络平台的犯罪特点、犯罪原因出发，对症下药予以治理。

（一）立法层面

《条例》第 3 条着重强调国家对福利彩票、体育彩票的特许发行权，以及禁止发行“其他彩票”，但并未在条文中直接禁止销售“其他彩票”，原因在于，我国特许经营的彩票品种只有福利彩票和体育彩票这两种，销售“其他彩票”以发行“其他彩票”为前提（注：境外彩票除外，因而单独规定，未放入“其他彩票”），因此，只要控制了“其他彩票”的发行，自然就控制了“其他彩票”的销售。换言之，在我国只可能存在“未经国家批准擅自发行（其他）彩票”的情形，不可能单独存在“未经国家批准擅自销售（其他）彩票”的情形，只要国家批准了某彩票品种的发行，自然就批准了该彩票品种的销售。

从社会危害性的角度来考量，发行和销售福利彩票、体育彩票以外的其他彩票的行为与违反规定销售福利彩票、体育彩票的行为存在明显差别，在立法和解释时应该区别对待。现行刑法普遍存在的空白罪状的表述方式，使得行为人的行为是否构成犯罪往往并不取决于刑法，而取决于行政法规，但行政法规常常滞后于刑法。2005 年《司法解释》中关于发行、销售彩票“以非法经营罪定罪处罚”的规定，本意是指“擅自发行、销售未经国家批准的彩票”，即以发行、销售彩票的种类来确定入罪标准，区分罪与非罪。但《司法解释》早在《条例》、《旧

细则》之前制定，当时不可能预判互联网时代特别是移动支付技术对彩票销售模式的深刻影响，《解释》采取的罪状描述“未经国家批准擅自发行、销售彩票”，并无不妥。但随着互联网销售彩票行为的兴起，本应作为定语、严格限定入罪彩票种类的“未经国家批准”会被错误解释为销售彩票行为的状语，从文义上大大扩张了被当作非法经营罪打击的彩票销售行为的范围，在司法实践中沦为降低非法经营罪入罪门槛的最好借口，错误扩大了打击面。

在立法层面，笔者建议尽快明确《司法解释》的罪状为“擅自发行未经国家批准的福利彩票、体育彩票之外的其他彩票”，以准确界定罪与非罪的界限，实现更加精准地打击彩票销售网络平台的犯罪行为。

（二）行政层面

彩票行业客观上具有巨大的经济效益，同时具有强国家属性与公益性，或者说，彩票的公益性是其获得国家大力支持的根基所在。国家相关部门不仅要对彩票的发行进行统筹安排，更要对其销售及售后的相关事项履行监管责任。只堵不疏的治理方式，无法杜绝开设私人作坊式的网络彩庄等犯罪行为的发生。针对互联网彩票销售平台乱象丛生甚至涉嫌犯罪的现象，政府各相关部门应该采取全面措施，兼顾预防与管控。

笔者建议彩票行业顺应信息化大趋势，允许各省存在一定数量的互联网销售平台。先制定严格的标准，再由省级主管部门负责审核申请材料，最终决定颁发经营牌照。对于之前因为实施相关违法行为被施以行政处罚甚至触犯刑法的申请者可以直接淘汰，在余下的信用良好、遵守法律、投诉率低的申请者中，选择有一定从业经验、运营技术过硬的企业。牌照的发放采取先批准试点、再进一步扩大的模式，给予彩民更多选择，培养彩民选择正规、合法的彩票销售网站购买彩票的健康消费习惯；促进销售平台健康竞争，共同维护网络销售彩票的良好秩序。或者借鉴火车票互联网销售平台 12306 的经验，由财政部牵头民政部、国家体育总局，建立全国统一的销售福利彩票、体育彩票的互联网平台，直接对接彩票发行及销售部门的运行系统，同步上线移动端应用程序，引导彩民简单便捷购买正规彩票。

另一方面，在网络平台获得经营互联网销售彩票业务的牌照后，主管部门要切实加强监管工作。例如，将各大互联网彩票销售平台进行联网并接入政府的监

管系统，对销售的彩票种类进行后台限制，只允许销售我国公开发行的福利彩票和体育彩票项下的彩票品种和游戏，从源头上进行管控。同时，在监管系统中设置动态流程监控功能，各大互联网彩票销售平台每售出一张彩票，系统的后台便立即开始数据追踪，包括彩票的编号、资金去向、是否中奖、奖金是否到位等信息，提高监管准确性和效率，作为加强行政执法的依据。

（三）行业协会

国际上的彩票组织有国家彩票组织国际协会（AILE）与国际足球和乐透型彩票组织协会（INTERTOTO），2000 年这两大协会合并为世界彩票协会，其主要活动为每两年举办一次的大会，在此期间世界各地彩票机构的官员及彩票运营商的代表将出席，共同探讨彩票行业的热门主题。2004 年 2 月 4 日成立的中国彩票工作委员会是世界彩票协会的合法会员，也是目前中国大陆唯一一个具有彩票行业协会性质的社团组织，自成立以来便动员社会各界力量，为彩票发行、从业人员、彩民服务。强化行业协会的作用可以使彩票更好的适应市场环境，实现行业“自净”。例如，中国彩票工作委员会可以对互联网销售彩票出台行业准则，建立综合考评机制，将考核指标细化，定期对各大彩票销售网络平台考核，不定期抽查销售情况，根据结果适用不同的反馈机制。

（四）广大彩民

相关部门应该向广大彩民主动提示法律风险，彩民自身也应当提升维权意识。彩票销售网络平台的违法犯罪行为，既侵犯了彩民可以获得奖金的机会利益，又有悖于国家设立彩票、推动公益事业的初衷。彩民在网络平台购买彩票后发现自己被侵犯权利时，一定要及时向行政管理机关或公安机关举报。

Governance of Crime of the Internet lottery Selling Platforms in China

Gong Bu-tan, Zhong Jia-jia

Abstract: Selling lottery tickets online has obvious advantages, but it also raises new criminal problems. As stipulated in *Lottery Ticket Management Regulation* and *Implementation Details of the Lottery Administration Regulations*, the acts in selling any other lotteries than welfare lotteries or sports lotteries constitute the crime of

illegal business operation, including foreign lotteries issued and sold within the territory of the People's Republic of China; the act of the Internet lottery sales platform increasing and selling the variety of welfare lottery, sports lottery and lottery games may also constitute the crime of illegal business operation. The behaviour of “eating ticket” of some lottery sales websites may be suspected of the crime of illegal business operation or crime of fraud depending on the specific situations. In four cases where online platforms that sell lottery tickets may constitute the crime above we can offer governing proposals from perspectives of legislation, administration, industry association and lottery players.

Keywords: Internet lottery selling platform; illegal lottery; Crime of illegal business operation; Crime governance

犯罪经济学视野下的网络平台数据泄露治理对策探究

王启欣*

摘　要：随着经济社会的发展，近年来网络平台数据泄露事件爆发。来自网络平台外部的“黑客”和来自内部的人员采取网络攻击和监守自盗的方式，非法获取网络平台中以平台用户个人信息为主的大量数据，严重侵害网络平台和用户的利益。造成这一现象的原因主要是网络平台数据泄露犯罪收益高、成本低。有必要控制网络平台数据的再利用价值，打击下游犯罪，以适当降低网络平台数据泄露犯罪收益，同时强化网络平台数据保护责任，打击上游犯罪，并增强网络平台数据泄露监测预警和有关部门的技术侦查能力，以增加犯罪的“投资性”成本和“惩罚性”成本，让违法者“犯不着”、“不能犯”、“不敢犯”、“不想犯”。

关键词：犯罪经济学；网络平台数据泄露；犯罪收益；犯罪成本

网络平台是信息技术应用于商业社会之后的产物，[①]其兴起被视为“数字革命”的三大标志性事件之一。[②]网络平台的崛起一方面“极大地改变了我们的生产和生活，它以空前的力量将人们连接在一起，为我们展示了一种更为有效的组织形式”，[③]另一方面也增大了“存储于计算机系统和全球数据网络中的数据面临着的安全风险”，[④]特别是近年来，与网络平台相关的大型数据泄露事件高发频发，引起社会广泛关注。[⑤]“我们生活在一个数据驱动的世界里，数据的价值无可限量，因此，数据泄露能够造成显著的影响。”[⑥]以网络平台数据泄露为主的“网络犯罪

* 王启欣，武汉大学法学博士。

① 在不同语境下“网络平台”有多种不同含义，即便是在互联网环境下也没有一个统一的概念界定和类型划分。参见周学锋、李平著：《网络平台的法律责任与治理研究》，中国法制出版社 2018 年版，第 3-12 页。本文所称“网络平台”，既包括采全国人大常委会法制工作委员会刑法室在对《刑法修正案（九）》第二十八条作出说明时提出的“网络服务提供者”的范畴，即“通过计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，向公众提供网络服务的机构和个人”，又涵盖通过互联网办公、经营，依托互联网建立、使用服务器等网络设备的机构。

② See Andrew Mcafee, Erik Brynjolfsson, Machie, Platform, Crowd: Harnessing Our Digital Future, W. W. Norton& Company, 2017, p.14.

③ 叶逸群：《互联网平台责任：从监管到治理》，载《财经法学》2018 年第 5 期。

④ See Kaite Hafner& John Markoff, Cyberpunk 251(1991).

⑤ See Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey 2018: Statistical Release.

⑥ [美]Aditya K Sood，Richard Enbody 著：《定向网络攻击 由漏洞利用与恶意软件驱动的多阶段攻击》，2016 年版，第 76 页。

的经济影响没有减缓”，[①]网络数据泄露的严峻态势必须加以遏制。本文尝试借鉴诺贝尔经济学奖获得者、著名经济学家加里•S•贝克尔提出的犯罪经济学理论，[②]探寻一种治理涉网络平台数据泄露犯罪的“最优”决策，使数据泄露“造成的社会损失降至最小”。[③]

一、网络平台数据泄露犯罪的现状与特征

网络平台数据泄露属于侵害计算机数据和计算机系统的保密性、完整性和可用性的犯罪范畴，是典型的网络犯罪。网络平台数据之所以会成为犯罪分子垂涎的重要目标，一方面与数据本身急剧膨胀的经济价值和社会价值密切相关，互联网中产生、流转的各类数据俨然成为信息时代最重要的生产要素，被视为“数据资产”、“新兴财富”；另一方面与互联网的体系架构以及网络平台在网络社会所处地位密不可分。“网络空间首先构造了一个信息环境。它包括了数据的创建、存储及更为重要的是分享。”“对计算机目前只有三件事情可以做：窃取数据，窃取凭证和劫持资源。不幸的是，我们对信息系统的依赖意味着，一个熟练的攻击者可以通过做这些中的任何一个而造成很大的伤害。”[④]网络平台是“网络社会运作的关键单元”，“是广大社会公众进入网络社会的入口和享受各种网络服务的平台”，[⑤]提供整体性的平台架构和服务，互联网上的数据都通过各类网络平台构建、聚合、存储、处理和传输，“数据的集中和数据量的增大给产业链中的数据安全保护带来新的威胁，数据开始成为主要的攻击对象”，[⑥]犯罪分子紧紧抓住这个绝佳的机会，通过各种非授权或者是非正常授权的手段获取网络平台数据，很轻易地挖掘到一笔又一笔“数据的金矿”。据统计，自 2013 年以来全球已有近 150 亿条数据泄露。2017 年是一个拐点，全球数据泄露事件数量开始呈现爆发式增长。2018 年上半年，每天有超过 2500 万条数据遭到入侵或泄露，也就是每秒 291 条。[⑦]金融行业、医疗保健行业、交通运输行业、教育行业、餐旅娱乐业、通信运营

① James Lewis, Economic Impact of Cybercrime—No Slowing Down.

② Becker G S. Crime and punishment: An economic approach[J]. Journal of Political Economy, 1968, 76 (2): 169-217.

③ [美]加里•S•贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等 2014 年版，第 71 页。

④ [美]P.W. Singer, Allan Friedman 著：《网络安全——输不起的互联网战争》，中国信息通信研究院译，电子工业出版社 2015 年版，第 89 页。

⑤ 陆旭：《网络服务提供者的刑事责任及展开——兼评<刑法修正案（九）>的相关规定》，载《法治研究》2015 年第 6 期。

⑥ 于志刚、李源粒：《大数据时代数据犯罪的制裁思路》，载《中国社会科学》2014 年第 10 期。

⑦ Varonis. 2018 Data Breach Investigations Report, https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

商网站、互联网企业都位居数据泄露榜前列。这些网络平台数据泄露给全球造成的经济损失惊人。根据 IBM Security 和 Ponemon Institute 发布的《2018 数据泄露损失研究》评估，2018 年全球数据泄露的平均成本为 386 万美元，百万条记录可致损失 4000 万美元，5000 万条记录可致损失 3.5 亿美元。[①]

本文收集了 2012 年—2018 年我国发生的 5 起网络平台数据泄露案件和 2017—2018 年境外发生的 8 起大规模网络平台数据泄露事件（其中"德国大型数据泄露事件"已被德国联邦刑警局 BKA 定性为犯罪），[②]经过分析概括出如下特征。

表 1 国内外大型网络平台数据泄露事件（案件）基本情况

案（事）件名	犯罪对象	犯罪主体	行为方式
CSDN 网站用户信息泄露案[③]	600 余万个明文注册邮箱账号和密码	犯罪嫌疑人曾某	非法侵入 CSDN 网站用户数据库服务器
12306 数据泄露案[④]	12306 官方网站用户登录账号、密码、信用卡信息、购买记录、常用联系人的电话及身份证号，不少于 131653 条	犯罪嫌疑人蒋某某、施某某	通过收集互联网某游戏网站以及其他多个网站泄露的用户名加密码信息，尝试登陆其他网站进行"撞库"，非法获取用户的其他信息
勾结前同事下载客户数据售卖换钱案[⑤]	北京某科技有限公司内部管理开发系统中储存的电子数据，涉及 600 余家客户、4000 余份数据报告	该公司女职员龚某、前职员卫某某及其商业合作伙伴薛某	卫某某利用龚某提供的账号、密码、Token 令牌，违反规定多次在异地登录该大型网络公司内部管理开发系统，查询、下载系统中储存的电子数据
华住数据泄露案[⑥]	1.23 亿条华住官网注册资料、1.3 亿酒店入住登记身份信息、2.4 亿条酒店开房记录	犯罪嫌疑人刘某某	利用黑客手段窃取华住集团旗下酒店数据
瑞智华胜数据窃取案[⑦]	30 亿条用户数据	新三板公司瑞智华胜	将自主编写的恶意程序放在运营商内部的服务器上，自动对用户流量进行清洗，采集并导出用户 cookie、访问记录等关键数据
德国大型数据泄露事件（案）[⑧]	包括默克尔在内的数百名政界人士、名人和记者的财务信息、电话号码、照片和通讯记录	一名 20 岁的德国男子	以不同方式攻击许多个人账号，并收集之前其他黑客攻破的数据，将其与自己捕获的信息进行整合而得（未确定）
Facebook 用户数据泄露事件	5000 万 Facebook 用户的个人资料数据	Cambridge Analytica	运用剑桥大学心理学教授 Aleksandr Kogan 开发的性格测试应用"thisismydigitallife"，在 Facebook 上获得 5000 万用户个人数据创建档案
Uber 大规模数据泄露事件	5000 万乘客的姓名、电子邮件和电话号码，以及约 60 万名美国司机的姓名和驾照号码	两名不知名黑客	通过外部代码托管网站 GitHub 获得了 Uber 工程师在 AWS 上的账号和密码，登录 AWS 盗取数据
美国信用机构 Equifax 用户数据泄露事件	大约 1.43 亿名用户数据，包括社保号码、生日、地址、信用卡信息等	不知名黑客	利用网站的应用漏洞来获取数据
南非 Dracore	包括南非总统祖玛在内的 3160 万份用户的	不知名黑客	访问该企业的 GoVault 平台发布用户数据的一台

① James Lewis, Economic Impact of Cybercrime—No Slowing Down

② 本文采用贝克尔犯罪经济学的观点，在分析研究时将"犯罪"进行泛化，并不局限于刑法规定的犯罪，而是包括所有的违法行为。参见[美]加里•S•贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等 2014 年版，第 42 页。

③ CSDN 网站数据泄露案告破 5 名犯罪嫌疑人被刑拘，https://news.qq.com/a/20120321/000091.htm，2019 年 2 月 12 日最后查看。

④ 12306 泄密犯罪嫌疑人已被抓 勿用第三方软件购票，http://www.dailyqd.com/2014-12/26/content_189992.htm，2019 年 2 月 12 日最后查看。

⑤ "内鬼"频频泄露客户信息，谁该为失控的数据负责，https://www.thepaper.cn/newsDetail_forward_1865360，2019 年 2 月 12 日最后查看。

⑥ 华住数据泄露案犯罪嫌疑人被抓 检察机关提前介入，http://www.chinanews.com/sh/2018/09-20/8632429.shtml，2019 年 2 月 12 日最后查看。

⑦ 30 亿条用户信息被盗 新三板公司瑞智华胜成背后源头，http://gd.ifeng.com/a/20180821/6821017_0.shtml，2019 年 2 月 12 日最后查看。

⑧ 德国大规模数据泄露事件疑为"带有政治倾向的攻击"，https://baijiahao.baidu.com/s?id=1622133598787753724&wfr=spider&for=pc，2019 年 2 月 12 日最后查看。

Data Sciences 数据泄露事件	个人资料		完全未经保护的 Web 服务器来获取数据
Ticketfly 数据泄露事件	2700 万个 Ticketfly 账户相关信息（如姓名、家庭住址、电子邮箱地址和电话号码等，涉及员工和用户）	黑客 IsHaKdZ	漏洞攻击
Under Armour 用户信息泄露事件	1.5 亿用户的数据，包含用户名、电子邮件地址和密码	不知名黑客	攻击该公司旗下存在数据漏洞的健身应用 MyFitnessPal
Saks 和 Lord &Taylor 数据泄露事件	500 万张被盗信用卡和借记卡的数据	JokerStash 黑客集团	系统入侵
万豪喜达屋客户信息泄露事件	大约 5 亿客户的用户信息，包括用户的姓名、住址、电话号码、电子邮件地址、护照号码、信用卡等所有核心的信息	不知名黑客	网络入侵喜达屋酒店预订系统

（一）犯罪对象：以网络平台用户个人信息为主，数据量极大且绝大多数未经加密

从上表所列 13 例网络平台数据泄露案件的犯罪对象属性来看，涉案的网络平台数据主要是与网络平台业务运营相关的用户个人信息。这些数据主要是用户在使用网络平台提供的各种服务时主动提供的个人信息，比如姓名、家庭住址、电子邮箱地址、电话号码、身份证号码和信用卡相关信息，当然，也有一部分信息是用户被动留下的，如"瑞智华胜数据窃取案"中恶意程序自动清洗用户流量而获取的用户 cookie、访问记录等。用户个人信息泄露在域外又被称为"用户身份盗窃"，自 2013 年金雅拓首次开始追踪数据泄露事件至今，有关用户身份盗窃的记录占所有被盗记录的 87%以上，比如 2018 年发生的 Facebook 和 Twitter 事件，泄露的个人数据条数分别超过 22 亿和 3.36 亿。除了用户个人信息外，网络平台的财务数据也是泄露的大头，仅 2018 年上半年泄露条数就高达 3.59 亿。[①]从安全性上来看，这些数据绝大多数未经过加密，或者仅是简单加密。国外有研究报告称，近年来网络平台泄露的数据只有不到百分之一的经过加密。Varonis 发布的《2018 年全球数据风险报告》分析发现，包括信用卡信息以及健康记录等在内的 62 亿份文件中，有高达 21%的文件是不受任何安全保护的开放文档，可供任何人访问。[②]

（二）犯罪主体：以匿名"黑客"为主，还包括一些网络平台内部工作人员

国外有关机构对网络平台数据泄露的犯罪主体组成情况进行了调查研究，得出的结论是：外部人员是数据泄露的罪魁祸首，占比 75%，另外 25%则是内部

① Varonis. 2018 Data Breach Investigations Report, https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

② Varonis. 2018 Data Breach Investigations Report, https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

人员。[①]上表所列 13 例网络平台数据泄露案件所反映的完成印证了这一结论。以“黑客”为犯罪主体的案件数量达到 11 起，其中匿名“黑客”作案 6 起，他们攻击网络平台获取数据都是出于恶意目的。另外 2 起案件则分别是由内部员工（“勾结前同事下载客户数据售卖换钱案”）或与公司有合作关系的“裙带机构”（“Facebook 用户数据泄露事件”）引发的，他们故意泄露网络平台数据的犯意也是恶意的。前述国外机构调研结果还显示，内部人员造成的数据泄露事件有五成以上（56%）是出于故意，比如报复，或者是非法利用，其它情况则是由于疏忽等过失原因导致的。[②]

（三）犯罪方式：因不同犯罪主体而异，“黑客”主要是通过互联网发起网络攻击，内部人员更多的是违规操作窃密

前述国外有关机构对网络平台数据泄露的犯罪方式进行了调查研究，发现“黑客”通常采取“恶意手段”，这些“恶意手段”几乎包括了所有常见的网络攻击方式，比如恶意软件、WEB 攻击、拒绝服务、钓鱼和社会工程、恶意代码、勒索软件、僵尸网络。[③]上表所列 11 起“黑客”作案的网络平台数据泄露案件，他们采取的手段正是一般“黑客”惯用的网络攻击方式，如“12306 数据泄露案”蒋某某、施某某使用的“撞库”攻击（属于典型的社会工程），“瑞智华胜数据窃取案”瑞智华胜使用的恶意程序攻击，“Uber 大规模数据泄露事件”两名不知名“黑客”使用的非授权登录、“美国信用机构 Equifax 用户数据泄露事件”等 6 起案件“黑客”使用的漏洞攻击。而内部人员往往以合法授权的方式非法窃取数据，这属于典型的监守自盗，或是将自身掌握的账号、密码、令牌等交由外部人员使用，非法登录授权访问网络平台的信息系统来获取数据。“勾结前同事下载客户数据售卖换钱案”龚某的犯罪方式就属于后一种，她把自己的账号、密码、Token 令牌提供给卫某某，以便卫某某非法登录公司后台系统盗取数据。

（四）犯罪结果：给网络平台和数据主体造成经济等方面的重大损失，违法者自身获取经济等方面的巨大利益

① Clare Ward, Nilesh Pritam. Cyber espionage and ransom ware attacks are on the increase warns the Verizon 2017 Data Breach Investigations Report, 04.27.2017.
② Varonis. 2018 Data Breach Investigations Report, https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.
③ Ponemon Institute. 2017 COST OF CYBER CRIME STUDY- INEIGHTS ON THE SECURITY INVESTMENTS. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.

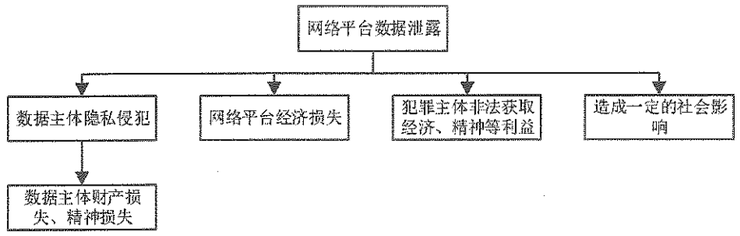


图 1　网络平台数据泄露造成的犯罪结果

如上图所示，网络平台数据泄露事件会引起四种不同结果。这四种结果既有可能是单独发生，也有可能是在同一犯罪链条上前后相继发生。

一是直接侵犯数据主体的隐私权，进而造成数据主体的财产损失或者精神损失。比如“万豪喜达屋客户信息泄露事件”中的违法人利用泄露的数据伪造、盗用客户的信用卡。

二是导致网络平台遭受重大经济损失。比如“Facebook 数据泄露事件”曝光第二天（2018 年 3 月 19 日），Facebook 股价就大跌 7%，市值缩水 360 多亿美元。“万豪喜达屋客户数据泄露事件”发生后，众多消费者向万豪提起诉讼，索赔金额高达 125 亿美元。“Uber 大规模数据泄露事件”令 Uber 不得不支付 1.48 亿美元给美国各州，以求事件和解。

三是违法主体自身获取经济利益、精神利益。第一种情况是犯罪主体直接销售牟利。上表案件中有 4 起案件的违法人在非法获取网络平台数据后直接销售以换取金钱，比如“勾结前同事下载客户数据售卖换钱案”中犯罪嫌疑人薛某通过 QQ 群寻找买家，将非法获取的客户数据出卖获利 3.7 万元；“华住数据泄露案”中犯罪嫌疑人刘某某在境外网站兜售泄露数据（未遂）；“Saks 和 Lord &Taylor 数据泄露事件”中黑客集团在暗网出售数据。第二种情况是犯罪主体向网络平台敲诈勒索。上表案件中有 3 起案件的违法人利用数据泄露事件向拥有数据的网络平台进行敲诈勒索，比如“Uber 大规模数据泄露事件”中 Uber 公司被迫向黑客支付 10 万美元以换取数据的安全；“Saks 和 Lord &Taylor 数据泄露事件”中黑客警告 Ticketfly 并要求其支付赎金。第三种情况是将泄露的数据作为犯罪工具继续从事其它犯罪。“瑞智华胜数据窃取案”中犯罪嫌疑人利用非法窃取的 30 亿条用户数据，操控用户账号进行微博、微信、QQ、抖音等社交平台的加粉、刷量、加群、违规推广，非法获利，旗下一家公司一年营收就超过 3000 万元。

四是造成一定的社会影响。上表案件中有 5 起案件的违法人利用泄露的数据制造各类不良影响，其中典型的是“德国大型数据泄露事件”和“Facebook 用户数据泄露事件”，前一案中违法者正是通过数据泄露发起“一次带有政治倾向的攻击，就是想让人名誉扫地”，后一案中违法者利用在 Facebook 上获得的 5000 万用户的个人资料数据，来创建档案、并在 2016 美国总统大选期间针对这些人进行定向宣传，直接影响了大选进程。

二、网络平台数据泄露的犯罪成因分析

犯罪经济学理论的首创者是贝克尔。作为一名经济学家，贝克尔将犯罪“看作是一种重要活动或‘产业’”，认为“犯罪行为只是更为一般的理论的一部分”，“当某人从事违法行为的预期效用超过将时间及另外的资源用于从事其他活动所带来的效用时，此人便会从事违法，由此，一些人成为‘罪犯’……在于他们的利益同成本之间存在差异”。[①]易言之，理性的违法者（犯罪人）在决定是否实施犯罪行为时，都会考虑并计算犯罪的收益和成本，权衡利弊得失，并最终决定是否犯罪以及采用何种方式来实施犯罪。[②]具体来说，违法者考虑的犯罪收益主要是因犯罪而获得的利益，包括经济收益、精神收益以及其它各种利益；考虑的犯罪成本则主要包括两个方面，一方面是为确保犯罪活动圆满完成而支付的“投资性”成本，包括为实施犯罪所做的物质准备、完成犯罪的难易程度，等；另一方面是由于实施犯罪行为而受到的“惩罚性”成本，比如逃避逮捕的机会、定罪可能性以及判定有罪后的惩罚，等。下面按照这三个大的方面对网络平台数据泄露的犯罪成因进行详细分析。

（一）网络平台数据泄露犯罪的收益：高

信息技术的发展和普及，使得网络数据逐渐成为极为重要的生产要素之一。由于信息技术革命所带来的生产生活方式的根本性转变，以能源、资本为核心的工业时代的经济发展模式，已经开始向着以网络大数据及其控制权为核心的经济发展模式转变。在这一变革过程中，形式各异的网络数据将逐步成为生产生活的重要组成内容，并逐渐被赋予更多的经济价值。[③]特别是网络平台中大量集中存

① [美]加里•S•贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等 2014 年版，第 42-47 页。
② [美]George B. Vold, Thomas J. Bernard, Jeffrey B. Snipes 著：《理论犯罪学》，方鹏译，中国政法出版社 2005 年版，第 57 页。
③ 于志刚、于冲著：《网络犯罪的罪名体系与发展思路》，中国法制出版社 2013 年版，第 42 页。

储的个人信息数据、企业财务数据，具有“含金量”非常高。正如法彦有云：有利益的地方就有犯罪人。贝卡里亚也认为，“个人之所以为自己的享乐而破坏社会契约，是因为支配其行为的是‘物质和精神世界所共有的涣散原则’。”[①]违法者选择实施网络平台数据泄露犯罪，也是出于非法获取利益的考虑。

从类型上看，这些利益至少包括：①经济利益。根据 Verizon 发布的《2018 年数据泄露调查报告》(DBIR, 2018 Data Breach Investigations Report)显示，2018 年发生的数据泄露事件，有 76%都是由于违法者为了获取经济利益而制造的，[②]这一比例较 2017 年上升约两成。通过出售或者非法利用泄露网络平台数据，违法者可以获取到巨额的经济利益。②政治利益。违法者可以利用泄露的网络平台数据制造某些政治影响，达到一定的政治目的。最典型的就是“Facebook 用户数据泄露事件”，据《纽约时报》、《卫报》等报道，从 2014 年起，由两位特朗普的支持者 Robert Mercer 和史蒂夫・班农（前白宫首席策略师）作为幕后人士的 Cambridge Analytica，利用 Facebook 的开放平台协议获取了超过 5000 万用户的资料（其中大部分是美国选民），从而帮助特朗普在 2016 年的大选中获胜。[③]作为一款知名网络社交平台，Facebook 的用户大数据能够快速关联更多用户的数据，进而被利用来分析用户们的行为模式、性格特征、价值观取向、成长经历，然后有针对性地推送信息和竞选广告，以影响美国选民在竞选中的投票。③精神需要。除了上述两种情况外，还有一部分违法者策划、实施网络平台数据泄露犯罪是为了情感的刺激和精神的满足，这和早期“黑客”犯罪的目的极为相似。早期的“黑客”更多的是出于技术挑战、戏谑取趣和捣乱破坏的目的而实施网络攻击行为。[④]由于网络平台数据涉及用户数量多，一旦公开影响面广，“黑客”才会利用这些数据作为威胁、泄愤的筹码。比如“CSDN 网站用户信息泄露案”的犯罪嫌疑人曾某曾在网站发帖自曝掌握 CSDN 数据库，要求与该公司合作未果，才将 600 余万个明文注册邮箱账号和密码在网上公开，引起网民的极大关注，正好也满足了自己从报复之心。

从难易程度上看，在全球化网络化环境下，违法者可以利用互联网等技术条

① [意]切萨雷•贝卡里亚著：《论犯罪与刑罚》，黄凤译，北京大学出版社 2008 年版，第 132-133 页。
② Verizon, 2018 Data Breach Investigations Report, 11th edition. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.
③ 参见《Facebook 数据泄漏事件始末，以及我们应该从中思考些什么？》，https://new.qq.com/omn/20180323/20180323A0BB0B.html，2019 年 3 月 10 日最后查看。
④ 皮勇著：《网络安全法原论》，中国人民公安大学出版社 2008 年版，第 149-151 页。

件“安全快捷”地获取利益。“安全”是指出售或者非法利用网络平台数据的途径安全，通过互联网等网络交易平台，违法者既可以在不露面的情况下与对方进行数据交易，又可以与网络平台有关人员联系，实施敲诈勒索。“快捷”是指非法交易或非法利用的速度快，收益转化快。以非法交易网络平台泄露数据为例，随着“暗网”的崛起，[①]违法者充分利用其匿名和虚拟货币交易不受监管的特质，搭建了一个更为安全、便利的销售网络平台数据的“市场”。近年来报道的“华住数据泄露案”、“800 万条 ACfun 网站用户数据泄露事件”、“1.27 亿条 Ixigo、Houzz 等 8 个网络平台数据泄露事件”中，违法者都是利用“暗网”发布买卖信息，进行非法交易的。这些交易使用的货币不再是现实社会流通的传统货币，而是比特币，。

从大小上看，违法者能够通过网络平台数据泄露犯罪获取的利益是十分巨大的。前述案例分析已有显示。再以通过暗网销售网络平台泄露数据事件为例，“华住数据泄露案”中的数据标价为 8 个比特币（约合 5.6 万美元），“800 万条 ACfun 网站用户数据泄露事件”中的数据售价为 1.2 万人民币，“1.27 亿条 Ixigo、Houzz 等 8 个网络平台数据泄露事件”中的数据售价是 2.909 比特币（约合 1.45 万美元）。至于违法者通过网络平台数据泄露获取的政治利益更是惊人，比如“Facebook 用户数据泄露事件”中，Cambridge Analytica 通过对非法获取的用户数据进行分析和利用，改变了美国大选的结果，帮助特朗普反败为胜，这种政治获利是无法用金钱估量的。

（二）网络平台数据泄露犯罪的“投资性”成本：低

犯罪经济学认为，在违法者考虑的犯罪成本中，有一部分是在准备和实施犯罪活动以及承担犯罪后果时，必须付出或可能付出的人力、物力、财力资源成本和时间机会成本，以及行为性成本、智能成本和心理感受成本。[②]试想，如果实施某一犯罪既容易上手又容易得手，那违法者还不趋之若鹜？从这一角度考察，违反者会毫不犹豫地选择实施网络平台数据泄露犯罪主要是以下两个方面的原因。

① 所谓“暗网”（Deep Web，又译“深层网络”），是与“明网”（Surface Web，又译“表层网络”）相对的互联网部分。“明网”指的是通过超链接可以被传统搜索引擎（如百度）搜索到的页面的集合；而“暗网”则是搜索引擎无法搜索到的部分，包括各种存储在数据库里的资料，还有需要注册才能浏览的论坛页面等，这个部分要比“明网”巨大得多。参见秉泽：《“暗网”：你所不了解的互联网》，载《保密工作》2016 年第 2 期。
② 吴闻、覃坚贞主编：《警察职务犯罪的预防》，中国人民公安大学出版社 2013 年版，第 176-179 页。

一方面容易上手。对于网络平台外部的“黑客”而言，实施网络平台数据泄露犯罪“易如反掌”。第一，攻击技能是“天生”的。“黑客”通常是指“对于计算机及计算机网络内部系统运作特别感兴趣并且有深入理解能力的一种人”，[①]他们往往热心于计算机技术、水平高超，能很容易地实施入侵网络平台数据库、流量分析等非法行为。第二，攻击工具和方法是现成的。比如“特洛伊木马”、邮件炸弹、网络嗅探器等黑客工具都能在互联网上免费下载或是付费购买到，还有一些专门的互联网站甚至是“黑客学校”为希望成为“黑客”的热衷者传授技术知识、提供技术支持。[②]第三，心理感受是轻松的。作为网络犯罪的一种，网络空间的虚拟性和匿名性本身也给涉案人员带来犯罪行为非常隐蔽的心理感受，[③]相比杀人、强奸、抢劫等传统暴力犯罪，心理承受的压力和罪恶感要轻很多。[④]对于网络平台内部的人员而言，实施网络平台数据泄露犯罪就是“监守自盗”。他们本是网络平台的合法授权者，按照工作职责理应掌握网络平台相关服务器的数据获取权限，但是出于报复泄愤或是图取私利的目的，他们既可以自己使用合法授权身份登录网络平台服务器，获取数据，如“Facebook 用户数据泄露事件”中的 Cambridge Analytica 利用“thisismydigitallife”应用获取 Facebook 数据库中的用户数据；也可以将自己的合法授权身份借予他人，“伪”授权后登录网络平台服务器，获取收据，如“勾结前同事下载客户数据售卖换钱案”中的龚某将自己在该网络公司内部管理开发系统的账号、密码、Token 令牌违规提供给卫某某。

另一方面容易得手。从网络攻击窃密的角度看，第一，相对“黑客”的网络攻击技术，网络平台安全技术防护往往显得十分薄弱，“道高一尺魔高一丈”。比如“瑞智华胜数据窃取案”中，瑞智华胜将自主编写的恶意程序放在运营商内部的服务器上，自动对用户流量进行清洗，相关运营商对此却毫不知情，也没有启动任何自动防御措施。第二，部分网络平台疏于安全管理，平台存在没有及时修补的漏洞，容易被“趁虚而入”。前文表 1 所列 13 个案例中，有 8 例都是因为网络平台存在漏洞而遭“黑客”攻击。更为严重的是，有些网络平台在明知自身存在安全漏洞的情况下，依然视而不见，不采取任何修复补救措施，造成更加严重的数据泄露结果。2018 年 4 月，美国面包连锁店 Panerabread 旗下网站

① RFC1392, the Internet Users' Glossary, usefully amplifies this as: A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.
② 于志刚著：《共同犯罪的网络异化研究》，中国方正出版社 2010 年版，第 38-44 页。
③ 李玫瑾主编：《犯罪心理学》，中国人民公安大学出版社 2009 年版，第 187 页。
④ 张保平、李世虎著：《犯罪心理学》，中国人民公安大学出版社 2015 年版，第 267-268 页。

panerabread.com 泄露了 3700 万用户信息。随后，安全机构 KrebsOnSecurity 表示，他们在早在 2017 年 8 月 2 日就曾发现了 Panerabread 网站的漏洞，告知对方后并没有进行及时修复，造成数据持续泄露超过 8 个月的严重结果。第三，网络平台中的数据都是集中存储，容易被“一网打尽”。在现有主流技术环境下，网络平台中包括许多数据库应用和应用服务器在内的应用都是直接连接到存储器上的，相关数据也是传输并集中存储在其中的。这就导致存储服务器一旦被非法入侵，里面存储和传输其中的数据就全部失去保护，可以被违法者尽收囊中。前文表 1 所列案例都是这种情况。第四，部分网络平台疏于内部管理，给了违法者泄露数据的可乘之机。比如前述“Uber 大规模数据泄露事件”，Uber 在一个外部代码托管网站存储工程师在 AWS 上的账号密码；“南非 Dracore Data Sciences 数据泄露事件”，该企业该的 GoVault 平台居然有一台完全未经保护的 Web 服务器。第五，绝大多数网络平台数据未加密，一旦泄露毫无秘密可言，对用户来说就容易被“一览无余”。基于信息安全考虑，数据加密技术通常用于增强数据库内部和外部的安全性，防止数据被破译。[①]前文表 1 所列案例所涉泄露的网络平台数据都没有经过加密，因此泄露即公开，违法者可以随意利用这些数据从事任何违法活动。

除了以上因素外，大量的非法地下交易市场和专业化的分工让违法者非法获取到泄露的网络平台数据后能够很快地“零成本”销赃套现。比如暗网销售交易、电信诈骗、信用卡诈骗等各成体系、大行其道，使得违法者没有“后顾之忧”，只要泄露数据在手，完全不用考虑也不用花时间费精力在如何用数据“换钱”“逐利”上面。

（三）网络平台数据泄露犯罪的“惩罚性”成本：低

贝克尔在其《犯罪与惩罚》一文中提出，违法同逃避逮捕的机会、定罪可能性以及判定有罪后的惩罚也是存在着某种关联。这种关联可以表述为：逃避逮捕的机会越大、定罪可能性越低、判定有罪后的惩罚越轻，违法者选择违法的可能性越大。[②]也就是说，实施犯罪的“惩罚性”成本越低，比如实施犯罪后如果很容易就逃脱法律惩罚，或是只需要承担较轻的刑罚，违法者就越容易甘冒风险去

① 唐坤剑等著：《新编大学计算机应用基础》，中国青年出版社 2016 年版，第 168 页。
② [美]加里•S•贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等 2014 年版，第 47-50 页。

实施犯罪。对比分析这三个因素不难发现，在现有刑事司法环境下，实施网络平台数据泄露犯罪的“惩罚性”成本是相对较低的。

第一，逃避逮捕的机会大。作为一种网络犯罪，网络数据泄露具有极强的隐蔽性，通常较难被发现。由于网络平台数据的易复制性，导致“盗窃”或者是“泄露”数据的行为中缺少“占有”要素，数据被盗了、泄露了，不像盗窃传统的钱包、钞票等可见有形物会发生转移，容易被发现，容易被监控。Ponemon《2018 年度数据泄露成本分析报告》显示，过去一年对于数据泄露事件的 MTTI（平均识别/发现时间）是 197 天，[①]也就是说，网络平台数据泄露事件往往需要半年甚至更长时间才能被发现，这种情况下违法者不仅能在这段很长时间里导致更多数据泄露，而且能够顺利完成后续的违法犯罪行为，最后“全身而退”。“时间是侦查计算机相关犯罪的一个重要因素”，必须采取足够迅速的侦查手段以获取网络犯罪的证据，否则就会因计算机数据“转瞬即逝”的本质特征影响案件侦查。[②]退一步说，即便网络数据泄露事件被网络平台或是有关监管机构发现了，但发动网络攻击的外部违法者是“黑客”，并且很多是故意匿名的“黑客”，他们利用计算机网络隐藏自己的身份，或者利用“跳板”技术、“僵尸网络”隐藏攻击源，用一般的侦查手段难以“追根溯源”，精准定位，违法者就可以在开放性、分散性极强的互联网络中“逃之夭夭”。前文表 1 所列案例中凡是“匿名黑客”作案的，都没有逮捕到犯罪嫌疑人，因此国外这类案件都只是定性为网络平台数据泄露事件，而没有以“犯罪”论。

第二，定罪可能性偏低。在网络攻击引起的网络平台数据泄露事件中，由于互联网数据传输速度极快，人们可以轻易删除、改变或移动数据的位置；“记录文件”（log files）即使存在，也只是保存在有限的时间内；显示交流链条（chain of communication）来源和路径的“往来数据”也只是短期保存。这种紧张关系给有效的侦查造成严重的后果。在刑事追诉中，必须确认犯罪行为人，并提供其犯罪行为的确凿证据。[③]因此，在司法实践中，司法机关会因为缺少足够的证据而影响对网络平台数据泄露事件的定罪。比如表 1 所列案例中的“德国大型数据

① Ponemon Institute. 2017 COST OF CYBER CRIME STUDY- INEIGHTS ON THE SECURITY INVESTMENTS. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.
② [德]乌尔里希·齐白著：《全球风险社会与信息社会中的刑法——二十一世纪刑法模式的转换》，周遵友、江溯等译，中国法制出版社 2012 年版，第 304-305 页。
③ [德]乌尔里希·齐白著：《全球风险社会与信息社会中的刑法——二十一世纪刑法模式的转换》，周遵友、江溯等译，中国法制出版社 2012 年版，第 305-306 页。

泄露事件”，尽管德国联邦刑警局 BKA 已将该事件定性为犯罪，多个部门已联合对该案展开调查，也抓获了一名犯罪嫌疑人，但是对于犯罪主体到底是“黑客团队”还是个人，作案目的到底是出于政治动机还是其它，犯罪方式到底是攻击某些大型数据库还是攻击个人账号并整合相关信息，都没有准确一致的定论。

第三，即便判定有罪，违法者所受的惩罚也不是很重。从我国刑法立法现状来看，网络平台数据泄露犯罪可适用的法条有：第 253 条之一“侵犯公民个人信息罪”、第 285 条第 1 款“非法侵入计算机信息系统罪”、第 2 款“非法获取计算机信息系统数据罪”。这三项罪名的量刑上限都不高，“侵犯公民个人信息罪”最高刑期为七年，“非法侵入计算机信息系统罪”最高刑期为三年，“非法获取计算机信息系统数据罪”最高刑期为七年。尽管这三款罪名都可以并处罚金，但是相对大规模网络平台数据泄露已经造成和可能造成的潜在社会危害来说，都显失衡。

三、网络平台数据泄露犯罪的防控对策

贝克尔的犯罪经济学，“研究的方法是建立违法造成的社会损失的公式，并找出使这一损失减至最低的资源支出与惩罚规模的公式”。[①]对于犯罪人来讲，犯罪是一种高风险投资，是成本分析的结果。犯罪人在实施犯罪行为以前是要充分评估其犯罪成本的，犯罪活动是犯罪人权衡犯罪的收益与犯罪的成本之后做出的选择。如果犯罪的收益大于犯罪的成本，潜在犯罪人就很有可能选择犯罪，成为现实的犯罪人。如果犯罪所付出的成本远远超过犯罪所获得的收益，潜在犯罪人就很有可能不会选择犯罪。所以，降低犯罪的收益，增加犯罪的成本，是减少潜在犯罪人成为现实犯罪人的最优之策。

对网络平台数据泄露犯罪而言，降低犯罪收益的难度较大。因为随着社会发展，网络平台数据的价值只会越来越大，数量只会越来越多。不能单纯寄希望于网络平台数据量减小、价值降低以达到预防和控制网络平台数据泄露犯罪的目的，因为这会在一定程度上影响网络平台正常运营。能争取做到的是在尽量控制网络平台存储、管理数据的数量和价值基础之上，切断网络平台数据泄露后的价值“兑现”之路，降低乃至彻底消减泄露的网络平台数据价值，而这一“兑现”之路实际上反映为违法者销赃的过程，在犯罪经济学理论中属于“投资性”成本

① [美]加里•S•贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等 2014 年版，第 42 页。

的范畴。而与降低犯罪收益较为困难相比，提高网络平台数据泄露犯罪的成本则相对容易。因为无论是“投资性”成本也好，还是“惩罚性”成本也罢，都与网络平台数据自身价值无关，控制这两类成本也不会对网络平台生存以及经济社会发展产生不良影响。综上所述，本文认为应当采取“适当降低犯罪收益、尽量增加犯罪成本”的原则来制定网络平台数据泄露犯罪的防控对策，具体建议如下。

（一）适当降低犯罪收益：控制网络平台数据的再利用价值，打击下游犯罪

从上文对犯罪结果的分析来看，利用网络平台数据的价值实施后续犯罪行为才是网络平台数据泄露真正造成社会危害的主要原因，真正体现违法者的主观恶性。因此，应当尽量切断网络平台数据泄露的后续延伸，防止数据价值“兑现”，从而降低违法者能够通过网络平台数据泄露犯罪获取的收益，让其即使非法获取到网络平台数据，也仅仅只是一堆含金量极地甚至根本无法再利用的数据而已，最终产生犯罪收益太低、“犯不着”去实施犯罪的认识，起到积极预防网络平台数据泄露犯罪的作用。基于上述考虑，本文建议从以下两个方面着手来适当降低网络平台数据泄露犯罪的收益。

一方面要控制网络平台数据的再利用价值。通过要求网络平台履行一定的数据保护义务，尽量减小网络平台获取并管理用户数据的数量，防止其无限度地获取用户数据。这样即便发生数据泄露事件，因为数据关联主体的数量和价值都不大，就尽可能地降低了数据泄露的影响范围和危害程度，犯罪收益自然也就随之降低。我国《网络安全法》第四章“网络信息安全”对网络运营者的用户个人信息的保密、收集、使用义务作出了较为明确的规定，应当严格遵守。除此之外，本文建议适当参考欧盟 General Data Protection Regulation(GDPR)，进一步强调网络平台个人数据的收集、处理规则，[①]增加通过设计以默认方式保护数据的义务（参考 GDPR 第 25 条）和通知受到实质性影响的用户的个人数据泄露的通知义务（参考 GDPR 第 34 条）。增加前一义务意在通过“假名化”等方式保护数据，确保个人信息不被归属到一个已被识别或者可被识别的自然人；增加后一义

① GDPR 第 6 条规定，只有符合以下条件之一，收集、处理个人数据的行为才是合法的：用户为了一个或者多个明确目的，同意处理其个人数据；为了履行用户与企业之间的合同必须处理其个人数据，或者为了基于用户请求而签订合同必须处理其个人数据；处理行为对于企业遵守其所负担的法律义务是必要的；处理个人数据是为了保护该用户或者其他自然人的重大利益；处理个人数据是为了公共利益；处理行为对于企业或者第三方所追求的合法利益目的是必要的，除非该利益屈从于需要保护其个人数据的自然人的利益或者基本权利和自由，尤其是当其是儿童时。此外，对于表征人种或者种族起源、政治意见、宗教或者哲学信仰、商会会员、基因、生物特征、健康状况、性生活等事项的特殊类别的个人数据（个人敏感数据），除非获得用户明确同意，或者具有其他正当理由，否则禁止收集、处理上述个人数据。

务意在及时通知相关用户已经发生数据泄露，可以提醒用户及时修改某些个人关键数据，比如银行卡密码。

另一方面要严厉打击下游犯罪。在难易程度上，打击冒头的下游犯罪远比打击隐藏深、发现难的网络平台数据泄露犯罪要容易得多，无论是违法者利用网络平台数据泄露敲诈勒索网络平台，还是进行非法传播、非法销售、信用卡诈骗、电信诈骗等，这些都是“面上”的犯罪，看得见、抓得着，易侦察、易追诉、易定罪、易处罚。建议司法机关加大对涉及网络平台数据相关犯罪的打击力度，这些犯罪主要包括：利用网络平台数据对网络平台实施的敲诈勒索罪；故意传播网络平台数据构成的侮辱罪；非法销售网络平台数据构成的侵犯公民个人信息罪；非法使用网络平台数据构成的盗窃罪、诈骗罪、信用卡诈骗罪。值得重点关注的是对暗网非法交易网络平台数据犯罪的打击。前文分析了暗网作为违法者进行网络平台泄露数据非法交易的原因及其危害，由于暗网服务器都在境外，涉及交易双方也在全球分布，建议采取国际合作的方式打击地下黑市、震慑暗网数据非法交易。[①]

（二）尽量提高犯罪的“投资性”成本：强化网络平台数据保护责任，打击上游犯罪

无论采用哪种行为方式，要使网络平台数据泄露，都必须突破网络平台技术或者管理方面的安全保护屏障，这就需要违法者为实施犯罪付出相应的“投资性”成本。如果让网络平台的安全保护屏障“加固”，同时不让违法者轻易得到攻破屏障的技术方法或者是授权，更不能如“探囊取物”般轻易导致数据泄露，在这种“彼长此消”的对比中，违法者无法利用自身掌握的或是能够获取的技能、手段成功实施犯罪，产生不了数据泄露的结果，徒劳无功“不能犯”，自然就不再策划实施犯罪“不想犯”。

首先要切实强化网络平台的数据保护责任。网络平台数据的实际控制和管理者是网络平台，理应承担数据保护的责任，做好具体工作，让违法者既无法通过外部网络攻击的方式制造网络平台数据泄露事件，又难以在内部实施违规操作使网络平台数据泄露。按照现有法律法规并借鉴域外有关立法规定，本文简要提出如下两点建议。

① 刘峣：《暗网已成非法交易温床 世界各国协力打击》，载《人民日报海外版》，2017 年 08 月 11 日第 08 版。

第一，要求网络平台落实数据保护措施。按照《网络安全法》和《信息安全等级保护管理办法》等现有法律法规并借鉴域外有关立法规定，建议网络平台从管理和技术两个维度加强对网络平台内存储、处理、传输的数据的保护。管理方面，基本原则是要落实信息安全等级保护制度，要制定网络平台内部安全管理制度和操作规程，落实网络安全保护责任，重点加强对网络平台所属各应用系统、数据库使用、管理人员的教育和管理，增强合规意识。技术方面，重点采取防火墙、病毒查杀等技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全的外部行为，以及身份鉴别、访问控制等技术措施，防范非授权获取登录、非授权访问数据等危害数据安全的内部行为；同时采取数据传输加密、数据存储加密、数据完整性鉴别和密钥管理技术，提高网络平台和数据的安全性和保密性，防止数据被外部非授权获取后破译；建议还要积极采用安全分析、UEBA、安全编排与自动化（SOA）、机器学习等新兴技术，最终实现低投入、高回报的安全技术投资效益。[①]

第二，加重网络平台数据泄露的法律责任。通过加重网络平台因数据泄露而承担的法律责任，威慑、警示、引导、教育网络平台遵守有关规定。对因拒不履行法律、行政法规规定的信息网络安全管理义务，致使用户数据泄露，构成犯罪的，应当依照刑法第 286 条之一“拒不履行网络安全管理义务罪”的规定对网络平台进行相应处罚。对因调查取证存在困难无法证明相关犯罪事实的，可以依照《网络安全法》第 59 条对出现数据泄露事件的网络平台进行行政处罚。但是鉴于当前网络平台在经济社会中的重要地位，建议借鉴 GDPR 的立法经验，提高网络平台违规的经济处罚标准，[②]以便更好起到威慑和警示力度，提高网络平台对履行网络安全保护义务必要性和紧迫性的认识。

同时要坚决打击网络平台数据泄露上游犯罪。网络平台数据泄露的上游犯罪是指为危害网络平台数据安全犯罪行为提供用于破坏计算机信息系统功能、入侵计算机信息系统的程序、工具或者技术帮助的行为。如前文分析的，这类行为极大降低了网络平台数据泄露的难度，因此，应当坚决打击这类犯罪行为。本文建

① Ponemon Institute. 2017 COST OF CYBER CRIME STUDY- INEIGHTS ON THE SECURITY INVESTMENTS. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.

② GDPR 第 83 条规定，对于违反 GDPR 的行为，严重违规者将被处以最高达 2000 万欧元或该企业全球年营业额的 4%（以两者较高者为准）的行政罚款；一般违规者将被处以最高达 1000 万欧元或该企业全球年营业额的 2%（以两者较高者为准）的行政罚款。

议，一是要充分利用刑法第285条第3款“提供侵入、非法控制计算机信息系统的程序、工具罪”和第287条之二“帮助网络犯罪活动罪”，严厉打击提供黑客工具、传授黑客技术、租借“僵尸网络”、出售网络漏洞信息等违法犯罪行为。二是要加强网络治理，及时清理黑客网站、论坛、群组以及发布的相关信息。

（三）尽量提高犯罪的“惩罚性”成本：增强网络平台数据泄露监测预警和有关部门的技术侦查能力

提高犯罪“惩罚性”成本的目的是为了让违法者不敢冒被逮捕和定罪的风险去实施违法行为。违法者一旦认识到其实施违法行为后越是容易被迅速逮捕，越是容易按照司法程序定罪处罚，那么他就不会冒这个风险，从而放弃实施犯罪。至于犯罪后所受刑罚的严厉程度对违法者违法行为的影响，贝克尔认为，在既有刑法立法前提下，“人们认为违法行为对定罪可能性变化的反应比对惩罚的反应更为敏感”，“定罪可能性比罪行惩罚更有威慑力”。[①]综上，建议从该事件能否被及时发现（逃避追捕）和犯罪证据能否被有效获取两方面入手来尽量提高网络平台数据泄露的犯罪“惩罚性”成本，让违法者不敢选择实施犯罪。具体提出如下两点建议。

第一，要提高网络平台的监测预警能力，及时发现网络平台数据泄露事件。网络平台对数据泄露的发生具有第一时间感知和发现的能力，从技术实现上考虑，主要是要增强网络平台的入侵检测能力。入侵检测是“对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程”，[②]通过从网络平台的若干关键点收集信息并进行分析，能够及时准确地中发现网络平台中的内部人员违规操作和针对平台的外部网络攻击。建议落实网络安全态势感知监测预警措施，建设网络安全防护管理平台，对网络运行状态、网络流量、用户行为、网络安全案事件等进行动态监测分析，并与同级公安机关对接，按照规定向同级公安机关报送网络安全监测预警信息，报告网络安全事件。[③]

第二，要提高公安等部门的技术侦查能力，及时锁定犯罪对象，有效获取犯罪证据，便于实施对违法者的逮捕、起诉。此外，基于网络平台的技术能力和协

① [美]加里·S·贝克尔著：《人类行为的经济学分析》，王业宇，陈琪译，格致出版社等2014年版，第48页。
② [美]Paul E.Proctor著：《入侵检测实用手册》，邓琦皓等译，中国电力出版社2002年版，第4页。
③ 2018年6月公安部公布的《网络安全等级保护条例（征求意见稿）》第24条、第30条对第三级以上网络运营者应当履行的网络安全态势感知监测预警义务提出了明确要求。

助公安部门侦破案件的需要，有必要强化网络平台的协助调查义务。建议要求网络平台在处置网络安全事件的同时应当保护好现场，记录并留存相关数据信息并对公安机关依法进行案件调查提供支持和协助。

数字经济培育与网络黑产治理

吴沈括

北京师范大学刑科院暨法学院副教授、硕导

进入新时期以降，伴随着诸多新一代信息技术的普及应用，数字经济得到了空前的蓬勃发展，无可否认的趋势是传统的服务与货物大生产模式正日益蝶变为以各类网络平台为中心场景的数字化生产方式。

与此同时，一方面，我们获得了更多的发展机遇，拥有了新的技术支持，例如大数据、人工智能等；也发展了新的业务样态，例如云计算、物联网等；还产生了新的应用内容，例如新型电子商务、数字金融、网络医疗以及在线文娱等。另一方面，我们蒙受了更多的安全风险，面对着新的技术要素风险，例如新式木马、病毒以及网络攻击威胁等；也面对着新的组织管理风险，例如新型网络黑产与电信网络诈骗等；还面对着新的在线内容风险，例如儿童色情、暴恐信息以及虚假消息等。

在这幅明暗错综的数字经济画卷中，继刷单、套现之后，当下颇具样本意义的突出场景莫过于针对网络平台的各类“薅羊毛”事件。其中值得特别注意的是，越来越多不法分子使用技术手段从事侵害平台利益、损害广大消费者权益的勾当，例如非法利用网络平台用户数据薅平台羊毛（包括为此专门蓄养大量虚拟号码并加以适用），或者将网络平台的技术漏洞广而告之并怂恿大量用户一起“收割”等等。而且短短数年间，散见的个体性“羊毛党”已经发展有组织的网络黑产团伙，他们对于健康市场秩序、良性产业运营以及合法用户权益构成了严重的威胁与侵害，却很少最终受到应有的法律惩处，个中原因着实需要全社会的共同反思，也能够为新型网络黑产的治理提供有益的思路。

从类型化的眼光来看，目前上述各种行为样态总体上存在两种主要的典型情形：第一，“羊毛党”黑产团伙主动搜索、挖掘网络平台的系统漏洞，通过抓包软件等技术手段恶意修改数据完成虚假充值、实现低价高套。对于此类严重侵害虚拟财产权益的行为而言，在涉案金额较大或者多次实施的情况下符合《刑法》第二百六十四条有关盗窃罪的犯罪构成，这一定性也得到了各地司法判例的有效

确证。

第二，恶意利用网络平台的技术漏洞“顺手牵羊”，常见为在网络平台生成优惠券后未公开、未推送、未发放的情形下，“羊毛党”黑产团伙在发现后借助制造大量虚假身份等技术方式高额套取，甚至时候出于进一步扩大侵害程度或者掩盖其不法行为等各种目的广为宣扬，诱使公众大面积参与其中。

客观而言，第二种情形因为往往与网络平台引入新技术应用和新经营模式相伴生，如何准确做出法律定性存在模糊地带，尚未产生相关司法判例，由此产生了一定的认识困惑。事实上，“羊毛党”黑产在此看似眼花缭乱的表现样态并不能改变其行为本质，也即通过欺诈手段使网络平台方基于错误认识做出财产处分进而非法获取财产，因此符合《刑法》第二百六十六条有关诈骗罪的犯罪构成。

需要指出的是，上述两类情形都有着复杂的组织构成，从上中下游黑产全链条的结构分析来看，往往还会触犯《刑法》规定的其他罪名，常见的包括侵犯公民个人信息罪、非法获取计算机信息系统数据罪、破坏计算机信息系统罪、非法利用信息网络罪以及帮助信息网络犯罪活动罪等等。为了更好地实现刑法一般预防和特殊预防功能以及贯彻“打早打小”的刑事政策，还有必要在满足法定构成要件时敢于、善于准确运用数罪并罚等刑罚裁量制度，严密刑事法网，依法提升刑事惩治水平。

然而，尽管法理层面不难得上述出合乎逻辑的判断结论，在司法实务中依然呈现刑事追诉比例较低的现状。究其原因，一方面，从客观的维度而言，现阶段“羊毛党”黑产刑事惩处工作普遍处于查处难、证明难、定罪难的“三难”处境，这种“三难”处境可以归究于新一代信息技术发展风险的不可预见性，尤其是人工智能新应用的不断创新引入，使威胁溯源、证据固定以及案件复盘等诉讼工作经常面对着工具不足、资源短缺的困境。

另一方面，从主观的维度而言，传统的公众意识与司法观念在一定程度上也加大了“羊毛党”黑产刑事惩处工作的难度。就公众意识来看，在实际案件中常常卷入了不少存在“有羊毛就要薅”、“法不责众”等观念的小金额“薅羊毛”普通个人用户。他们在单纯的“便宜就去占”的心理驱使下会忽视我国法律有关不当得利的制度规定，没有认识到在缺乏合法依据、有损他人而取得利益的场合中应当及时归还所得，如果拒绝归还则将触发进一步的特定法律责任。

就司法观念而言，当下我国正处于从农业工商业社会司法模式快速转变进入信息社会司法模式的过渡阶段，例如信息社会、数字经济语境下的数字化“财产”、“生产经营”、“计算机信息系统”等的事实理解与司法认定都需要深刻的理念更新与调适。而刑事司法运行同样存在一定的转型滞后性，对于若干传统范畴的革新理解需要更多的制度性建设，这也是国家高度重视司法机关信息化改造和司法工作队伍信息化能力建设的重要原因所在。

应当强调的是，不论“羊毛党”类网络黑产的表现形式如何，其本身带来的多重权益危害都是不容小觑的：其一，此类黑产的蔓延对于各类网络平台的正常生产经营造成了极大的伤害，除了特定案件中产生的巨大的直接经济损失和商誉等损失，还迫使网络平台在正常的安全管理投入之外进一步持续负担本不属于必要经营成本的特殊安防支出，成为平台发展壮大的不可承受之重。

其二，“羊毛党”黑产的扩散实质上必然用虚假交易、恶意交易挤占了广大普通民众在网络平台中的合法交易机会，大幅度降低他们获得数字经济红利的分享比例，而且黑产加害目标的无差别性频繁造成用户在被裹挟其中的同时受到黑产团伙二次伤害的情形，本身也是对人民群众人身财产安全和社会公共安全的严重威胁。

其三，作为更为深层次的问题，数字经济的长足可持续发展端赖健康的产业生态和良好的营商环境，如果任由“羊毛党”类网络黑产滋生扩散，将会在根本上动摇新经济形态培育所需的民众信任基础，甚至可能诱使更大范围的恶性效仿，形成“破窗效应”，普遍挫伤广大主体的创新创业热情，进而对内严重削弱数字经济培育的原生动力，对外严重伤害中国数字市场环境的国际口碑。

有鉴于此，为了更好地实现培育数字经济快速成长的国家战略，提升我国数字产业的发展水平，打造过硬的国际品牌形象，需要我们更为积极、更为全面地付诸“羊毛党”类网络黑产的新综合治理，特别地：

首先，作为治理的中心节点，网络平台应当依照《网络安全法》以及《电子商务法》等相关法律、法规的基本要求，采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障平台内交易安全，把牢综合治理的第一道关口。尤其需要制定网络安全事件应急预案，

在发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。

特别地，在操作层面，基于量大、高频的在线交易特点，网络平台有权采取的补救措施包括通过法定财产保全机制及时批量冻结存疑交易订单并展开溯源追踪，同时根据用户的合理证明或者司法机关的处理意见就正常订单及时解冻、恢复交易，以此实现此类案件中的动态权益平衡。

同时，作为治理的关键支撑，国家各级职能部门积极介入，实现监管以及司法环节的执法必严、违法必究将成为打击治理“羊毛党”类网络黑产的底线守护。时至今日，该类黑产的链条环环相扣、相互交织，具有高度的组织性和隐蔽性，严峻的态势既呼唤行政监管机关进一步改进执法方式，确保黑产上下游的无缝监管，最大限度消除其生存空间，为网络犯罪防治法规的制定颁布提供良好的机制基础，也呼唤各级司法机关在“两高”网络犯罪专项司法解释即将出台施行的大背景下，进一步严密刑事司法网，精准打击此类黑产，依法提高刑事追诉比例，有效震慑“羊毛党”类犯罪分子。

此外，作为治理的重要基础，应当承认，现实中部分网络平台用户的不良消费习惯和消费品位给“羊毛党”类网络黑产的形成提供了一定的便利条件，同时也削弱了有效打击治理此类黑产的群众基础，这一局面必须予以有效扭转。因此，通过具有审美吸引力的公众宣传教育，切实改进和提升网络平台广大用户的网络安全基础意识、在线消费习惯品味以及数字经济参与水平，造就积极活跃的数字经济社群生态，就属于黑产治理体系建设的题中应有之义。

论远程视频取证模式的构建*

张启飞　虞纯纯**

摘　要：远程视频取证符合刑事诉讼法的相关规定，已逐渐融入司法实践，对司法信息化建设具有典型的示范意义。远程视频取证作为“互联网+”在司法领域的具体运用，在观念层面，要符合刑事诉讼的基本规定并获得诉讼各参与方的认可。在技术层面，要提高网络专线的传输速度及审查音像证据的效率。在操作层面，应从固定的点对点模式、机动的远程模式、一体化的证据体系建立三方面加以规范。未来，远程视频取证具有广阔的应用前景。

关键词：刑事诉讼　远程视频取证　规范化　模式构建

2017年8月18日，杭州互联网法院正式揭牌。2018年4月2日，杭州互联网法院举行全球首个“异步审理模式”上线启动仪式，实现举证、质证、审判等全流程线上处理到异地错时线上审理，各地法院逐步开展远程视频审判工作。与此同时，各地检察机关逐步开展“互联网+”的工作模式，进行远程讯问，远程司法模式开始显现出强大的生命力。在“互联网+”背景下，如何构建远程视频取证模式，提高侦查效率，需要深入研究。

一、远程视频取证的实践与质疑

远程视频取证是“互联网+”融入司法实践，解决案多人少、降低异地取证经费、节约司法资源，提升司法效率的有效途径。当前，远程视频取证已取得显著的效果，但也存有质疑之声。

（一）远程视频取证的实践效果

在“互联网+”背景下，远程视频取证方式优势十分明显。其一，方便取证，节省司法成本。在网络犯罪案件中，被害人分布在全国各地，若通过传统方式取证，不仅效率低下，而且费用惊人，警力难以保障。通过远程视频取证，不仅可以免去舟车劳顿之苦，而且几乎没有差旅成本。其二，可有效解决犯罪嫌疑人在押解过程中的安保问题。异地押解的安全问题一直是困扰在司法人员头上的“达摩克利斯之剑”，押解过程中脱逃的案例不时见诸报端。远程视频取证可以避免

长途押解，有效解决押解过程中的脱逃问题。其三，方便证人作证，提高证人作证的出庭率。证人出庭率低下是我国刑事审判的不争事实，并成为制约控辩式刑事庭审方式改革的瓶颈之一。[①]通过远程视频作证，可以有效降低证人出庭成本，减少证人出庭的顾虑，提高证人出庭率。

（二）对远程视频取证的质疑

当前，对远程视频取证的办案方式的质疑主要体现在：一是刑事诉讼法并未明确规定该种取证方式，缺乏合法性依据；二是侦查活动是一项严肃的司法活动，远程视频取证缺乏传统面对面取证方式的严肃性，使严肃的执法活动“变味”；[②]三是言词证据的可信性问题。由于远程视频取证不与取证对象直接接触，取证对象容易掩盖事实，不易评价言词的可信性。[③]针对远程视频取证法律依据欠缺、司法权威不足、证据的安全性受到质疑等问题，需要我们认真探寻远程视频取证的价值意蕴与法律基础，构建合理的远程视频取证模式。

二、远程视频取证的规范化要求

远程视频取证作为“互联网+”在司法领域的具体应用，司法工作人员应当主动拥抱互联网技术，依托互联网技术进行工作方式的创新。在远程视频取证的规范化层面，需要从外在要求和内在要求两个层面进行考量，以全面提升远程视频取证的规范化水平。

（一）外在要求：远程协助取证要符合刑事诉讼的基本规定

对远程视频取证的质疑之一是法律上缺乏明确规定。我国2018年修订的《刑事诉讼法》并无对远程视频取证的具体规定，但2013年最高人民法院《关于适用〈中华人民共和国刑事诉讼法〉的解释》第206条规定，证人因身患严重疾病等客观原因无法出庭的，可以准其不出庭或者通过视频等方式作证。此处“视频作证”之语虽较含糊，但联系上下文表述，应理解为不出庭情况下的视听传输技

* 本文系2018年度最高人民检察院检察理论研究课题“网络犯罪证据的审查与运用”（项目编号：GJ2018D57）的研究成果。

** 作者简介：张启飞，浙江警察学院法律系讲师，法学博士，浙江省杭州市滨文路555号浙江警察学院，邮编310053，联系电话15990159101；虞纯纯，浙江省温州市瓯海区人民检察院政治部副主任科员，法学硕士，浙江省温州市瓯海区人民检察院，邮编325000，联系电话13867792026。

① 参见左卫民、马静华：《刑事证人出庭率：一种基于实证研究的理论阐述》，载《中国法学》2005年第6期。

② 参见范黎红：《远程审理的适用空间之展望》，载《法学》2010年第2期。

③ 参见郭欣阳、方莉：《科学技术在证人证言举证中的应用》，载《人民检察》2005年第4期。

术作证。因此，视听传输技术作证运用于刑事诉讼亦属合法。[①]需要注意的是，早在2001年，最高人民法院《关于民事诉讼证据的若干规定》第56条第2款就规定证人可以提交书面证言或者视听资料或者通过双向视听传输技术手段作证。2012年《民事诉讼法》修改时将上述规定纳入，在第73条明确规定："经人民法院许可，可以通过书面证言、视听传输技术或者视听资料等方式作证。"这是我国程序法上首次对远程视频作证作出规定，对民事诉讼远程取证提供了合法性保障。此后，2016年"两高一部"《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第9条对网络远程勘验作出规定。2019年1月2日公安部发布《公安机关办理刑事案件电子数据取证规则》，其中第四节共13个条文对网络在线提取电子数据作出详细规定。可以看出，网络远程取证法律依据充分。

（二）内在要求：远程协助取证要获得各诉讼参与方的认可

诉讼参与人平等的参与庭审活动，是提升司法公信力的重要保障，也是提升司法权威的重要途径。司法应有自己的威仪，司法威仪是通过法律活动或法律适用的程序化方式和过程，使司法活动、法官以及法律获得一种神圣、不可侵犯的权威。[②]远程协助取证若无法获得侦查人员、检察人员、审判人员及各诉讼参与人员的认可，其司法权威可想而知。

第一，对司法人员来讲，由于远程作证具有降低诉讼成本、便于证人出庭作证、适应网络时代侦查及庭审方式变革等诸多价值，互联网技术在司法实践中运用越来越广泛，侦查人员、检察人员、审判人员等司法工作人员应当顺应时代潮流，掌握最新的网络技术，不断提升司法实践中运用新技术的能力。

第二，对证人来讲，远程作证可以节省时间、降低出庭的费用、提升证人的出庭率。在我国司法实践中，证人出庭率低下是个历久弥新的话题。证人出庭率低下已成为控辩式刑事庭审方式改革的瓶颈之一。证人出庭率低下固然可以归因于检察官和法官的消极态度及书面裁判模式的承继，[③]证人因担心出庭作证而浪费自己的时间和精力，恐怕也是证人在面对与自己无任何关系的案件中不愿意出

① 参见李峰：《论视听传输技术作证的规范化——基于民事裁判文书的分析》，载《华东政法大学学报》2018年第5期。
② 参见季金华：《理性司法观的培养：司法权威的概念支持》，载《法律适用》2004年第1期。
③ 参见左卫民、马静华：《刑事证人出庭率：一种基于实证研究的理论阐述》，载《中国法学》2005年第6期。

庭作证的重要原因。采用远程作证可以解决证人出庭作证面临的现实困境，提高证人出庭的几率。

第三，对当事人来讲，分为犯罪嫌疑人、被告人和被害人三种情形。对于犯罪嫌疑人，若处于羁押状态，可以通过看守所的远程视频系统进行提审；若没有处于羁押状态，可通过定制的专用小程序进行讯问。对于被告人，根据我国2018年修订《刑事诉讼法》的规定，除缺席判决外，被告人要在庭审现场接受审判，较少存在远程庭审的情形。对于被害人来讲，是否到庭接受询问法律没有明确规定。司法实践中，侦查机关一般将被害人的询问笔录作为证据提交给法院，被害人很少出庭陈述受害事实。但从长远来看，被害人出庭陈述被害事实是大势所趋，采用远程取证，可以减少被害人的心理障碍，更容易获得被害人的认可。

第四，对于鉴定人、翻译人员等其他诉讼参与人来讲，这些诉讼参与人和案件没有利害关系，主要是辅助庭审的正常进行，由于鉴定人和翻译人员很少出庭，利用远程系统协助进行鉴定、翻译，不仅会达到同样的效果，还会提升鉴定人、翻译人员的出庭率。

三、远程视频取证模式的方案设计

在远程视频取证获得诉讼参与各方认可，现有技术已能有效支持远程视频取证的情况下，应建立一体化的远程视频证据体系，设计科学的远程视频取证模式，让侦查人员、检察人员、审判人员及社会公众逐渐接受远程视频取证。

（一）建立固定的远程取证模式

第一，点对点的远程取证模式。目前，网页端的视频录制软件及苹果、安卓系统的视频录APP随处可见，为防止侦查阶段视频证据被截取、窜改、盗用，不宜随意使用公用网络渠道进行录制，故在远程视频取证之初，宜采用加密网络通道建立固定的点对点的远程取证模式。即在同城同省一定范围内的公安机关、监所、检察院、法院之间建立远程视频系统，最终在全国各地的公安、司法机关之间建立远程视频取证系统，实现侦查人员、检察人员、审判人员在本单位就可对在同城或异地的当事人进行远程提审、讯（询）问。

第二，远程取证工作室模式。点对点的远程取证系统需合作单位建立各自的远程视频取证室，在不同的取证室之间连接专用网络线路，保证视频数据不被他人滥用、截取、盗用。目前，主要有使用VPN（虚拟专用网络）和有线专用光

纤两种网络宽带方式进行涉密工作网、涉密数据的处理。这两种方式均可实现对数据的加密传输，但在传输速度、覆盖范围、设置成本方面各有利弊，各单位之间的远程视频取证室的网络专线可按需进行设置。取证工作室的背景墙宜标明本单位名称及标志，让当事人最大程度地产生亲临现场感。在取证室里，应设置专用电脑、视频显示屏、打印机等相关录音录像设备，可参照《公安机关讯问犯罪嫌疑人录音录像工作规定》进行全面摄像。录制内容包括侦查人员、犯罪嫌疑人、其他在场人员、讯（询）问场景和计时装置、温度计显示等信息。图像正中应当显示犯罪嫌疑人正面中景，并通过画中画技术同步显示侦查人员正面画面，画面同步显示日期和 24 小时制时间信息。远程讯（询）问应当自讯（询）问开始时开始，至被讯（询）问人核对讯问笔录、签字捺指纹后结束。讯（询）问完成后，笔录可由协作单位邮寄送达至被协作单位，也可由被协作单位上门收取。若今后实现讯（询）问的电子化，摒弃传统的纸质笔录，直接采用音像记录作为证据，可由取证单位在远程讯（询）问时，同步录制视频。

（二）建立机动的远程取证模式

前述，远程取证系统主要针对在押与非在押两类犯罪嫌疑人、被告人及被害人、证人等。对在押的犯罪嫌疑人、被告人，可以通过看守所的远程视频讯问室进行远程视频提审，而对非在押的犯罪嫌疑人、被告人及被害人、证人可使用手机、电脑等通讯设备接受讯（询）问。故对这两类人员进行远程视频取证时，宜作区别对待。

第一，定制版侦查 APP 及侦查小程序。公安机关、检察院、法院可与互联网公司合作开发具备视频录制功能的专用讯（询）问 APP，实现随时随地取证。目前，微信、支付宝已支持购物娱乐、资金往来、教育公益等各类小程序，公安机关、检察院、法院可与腾讯、阿里巴巴合作开发具备视频录制功能的微信小程序、支付宝小程序，专门适用于讯（询）问。在当事人第一次到案或采取强制措施之时，告知当事人下载专用 APP 或添加小程序，并在专用 APP 及小程序中应嵌入人脸识别系统用于身份识别，以备远程讯（询）问。

第二，机动型远程视频取证程序。在进行远程视频取证时，应遵守我国刑事诉讼法的规定。在讯（询）问开始之前，侦查人员、司法人员应核实当事人是否已下载专用 APP 或小程序，并告知当事人通过绑定身份证、手机号码等方式进

行注册，填写姓名、出生年月、性别等相关信息，通过人脸识别系统自动识别身份，或当事人以手持身份证的方式，并通过点头、眨眼等方式进行身份的动态识别。侦查人员、检察人员、审判人员可通过摄像头在视频中出示询问通知书和工作证件，以向被取证人说明身份。为避免被害人、证人及在押的犯罪嫌疑人陈述、供述时受到干扰、影响或胁迫，上述人员应在封闭的空间内陈述、供述。在讯（询）问之初，当事人应手持摄像头环视作证环境，由讯（询）问人确定、核实作证环境的安全性。在讯（询）问开始时，讯（询）问人应再次口头核实在该环境下作证是否有受到影响、胁迫、干扰，并告知其虚假陈述应当承担的法律责任。在录制时，应参照《公安机关讯问犯罪嫌疑人录音录像工作规定》，全程无间断进行录制，并刻录成光盘予以保存、备份，在相关的文件名称上注明案件名称、被讯（询）问人、制作人、制作时间等相关信息。

第三，摒弃传统笔录，提高音像证据的审查效率。刑事案件取证用音像记录代替传统的笔录，可以解决远程视频取证时非面对面的模式下不能及时取得笔录的难题。传统笔录具有记录不完整的缺陷，办案人员不可能一字不落地记录下原话，也不能展现当事人的表情、动作。音像记录能完整的、全面的记录下取证、讯问过程，并可检验是否存在刑讯逼供、诱供的情况。当然，大量的音像视频资料将带来审查上的困难，传统的笔录可在较短的时间内全面阅读，而视频数据的播放时间是固定的，若全面审查视频数据，将占用司法办案人员大量的时间，且可能无法在审查逮捕、审查起诉的规定时间内全部审核完毕。为提高审查效率，可由侦查人员或司法辅助人员事先审查播放音像资料，对视频进行简要的文字说明，并对视频资料供述、陈述、证言的关键时间段等作文字说明，节约员额检察官、法官的审查时间。此外，可在办案系统或视频录制设备中嵌入语音识别系统，由语音识别系统自动抓取关键词，自动生成文字，记录关键词出现的相应时间点，以方便司法审查人员高效、有重点的播放、审查音像证据。

（三）建立一体化的证据体系

司法程序理论认为，证据应被视为一项过程而不是事物的集合。[①]采用远程视频取证模式，应当打通侦查机关与检察院、法院的办案系统，通过计算机操作，实现证据材料在使用终端的移送、共享。

① 参见[美]罗纳德·J.艾伦：《理性 认知 证据》，粟峥、王佳译，法律出版社 2013 年版，第 40 页。

第一，建立单位内部的数据交换通道。单位内部数据交换主要包括两种，一是普通电子设备与工作网的传输交换。利用计算机终端或移动设备端进行视频取证，相关视频数据存储在普通电子设备上。在录制完成后，先通过中间机器对视频资料进行杀毒，在检测安全后，对视频资料进行哈希值检测，检验视频资料是否完整，有无丢帧、被窜改情况。最后，将视频资料导入办案系统。二是工作网与涉密网之间的数据交互。目前，侦查机关已使用网闸解决公用互联网与工作网之间数据的导入导出，检察机关利用“光盘摆渡+光闸”模式实现涉密网与工作网间的数据交换，[①]单位内部网间的数据交换可由单位自行选择合适的模式进行。

第二，建立“数据交互共享”平台。数据交互平台可实现数据的跨域定向共享，在交互过程中根据处理算法进行数据格式的自动匹配，以便能够使用多种数据渠道实现数据资源的受控共享交换。[②]在视频取证模式下，建立数据交互共享平台，用网络传送方式代替人工移送卷宗材料模式，提高移送效率，减轻办案人员的工作量，节省办案资源。目前，公安机关的全国违法前科人员信息资源库已可以共享、查询犯罪嫌疑人的前科情况。在检察机关的统一业务应用系统中有“协同互联”的模块，可将数据传输至监所、法院、其他检察院等单位。法院的审判应用系统可进行高院与下级院的立案登记、文书制作，司法统计、查询等协同工作。换言之，在不同单位、系统之间实现数据交互、网络互联互通在技术上已无障碍，且已在一定范围内投入使用。侦查机关之间共享视频证据的关键在于制定、遵循相关规范。除非确因侦查涉及国家安全、涉黑、涉恐等有保密需要，可暂不共享外，原则上已侦查完结的案件，应实行证据共享。因此，侦查机关与检察院、法院之间对于同一案件的证据，宜采用智能共享功能。

第三，规范音像资料的存储。刑事证据承担着当事人有罪无罪的证明责任，在证据的保存、传输方面应设置严格的规范程序，避免证据错乱、混杂。在视频证据制作完成后，应及时在文档、文件夹上注明案件编号、案件名称、被讯（询）问人、制作时间等相关信息。同一个案件，应建立一个文件夹以存放所有的证据，在文件夹项下宜根据犯罪嫌疑人、被害人、证人等进行分类，并按需建立子文件夹，导入、传输音像资料的过程中，应检查文件名及相关信息是否与原数据名称

① 参见侯天子、王君：《检察机关建设大数据中心的研究与探讨》，载《检察技术与信息化》2018 年第 5 期。
② 参见马君毅、温睿：《基于大数据构建检察应用支撑平台的思考》，载《检察技术与信息化》2018 年第 5 期。

相一致。需要注意的是，视频格式种类较多，不同的格式对视频文件的压缩率不同，将导致视频的容量不同，进而影响到传输速度、存储空间的大小及播放器的选择。为避免视频证据在不同的单位间传输、播放时出现故障，侦查机关、法院、检察院之间应采用统一的视频格式及播放器。

四、结语

随着5G时代的到来及“互联网+”的不断发展壮大，远程视频取证存在巨大的潜力和广泛的发展空间。正如Lord Wolf所说，IT业发展所带来的，是彻底改变诉讼系统基础以及规则上诉讼现实的催化剂。这一发展趋势，对于诉讼程序和数字技术之间交互的吸引力、密切关联、一致性和兼容性而言，诉讼法领域还存在着更广阔的尚未开垦的领地。[①]目前，我国开展的远程视频取证实践，应当看到它的勃勃生机。随着科技与司法的融合，将来可实现取证、审查、审判全流程自动化，极大解放侦查人员、检察人员、审判人员等司法人员的双手，专注于疑难复杂案件的办理。远程视频取证模式的构建需要各部门、各地区协作完成、推进，随着远程取证实践经验的积累，在全国范围内推广远程视频取证，已触手可及。

①参见[德]Peter Gilles：《德国民事诉讼程序电子化及其合法化与“E—民事诉讼法”之特殊规则》，张陈果译，载《民事程序法研究（第三辑）》，厦门大学出版社 2007 年版，第 316 页。

智慧社会语境下的网络犯罪情势与治理对策

崔仕绣　崔文广*

（中南财经政法大学 刑事司法学院，湖北 武汉 430073）

（湖北省公安厅 科技信息处，湖北 武汉 430070）

摘　要：智慧社会语境下的万物互联、智能创新和多元融合，加速了网络犯罪由“计算机信息系统犯罪对象化”向“网络犯罪工具化”及“网络犯罪空间化”的历史演变。与现实社会并行的网络空间得以产生与发展，逐渐升级为相对独立的犯罪场域。结合我国网络发展的当代情势，理念滞后、立法保守、监管错位和技术落后等缺憾持续暴露，导致我国现阶段网络犯罪治理模式陈旧、实效不佳。为保障网络空间的有序和谐，促进网络治理智能化、社会化、专业化、法治化，应树立“预防本位”的网络犯罪治理面向，补充行政法规和刑事法律规范供给，协同行业内控与行政监管，重视技术创新，加速构建网络犯罪技术防控体系，妥善协调科技创新与网络安全的紧张关系，推进网络社会的法治化发展。

关键词：智慧社会；网络犯罪治理；网络空间；网络法治建设

The Situation of Cyber Crime and the Countermeasures under the Perspective of Smart Society

CUI Shi-xiu　CUI Wen-guang

(Zhongnan University of Economics and Law, Criminal Justice School, Wuhan 430073, China)

(Hubei Provincial Public Security Bureau, Science and Technology Information Department, Wuhan 430070, China)

Abstract: The interconnection, intelligent innovation and multiple fusion of all things in the context of smart society accelerate the historical evolution of cyber crime from "computerization of computer information system crime" to "instrumental of cyber crime" and "spatial of cybercrime". The cyberspace parallel to the real society has been produced and developed, and gradually escalated into a relatively independent crime field. Combining with the contemporary situation of network

* 作者简介：崔仕绣（1990-），女，满族，湖北武汉人，中南财经政法大学刑事司法学院 2016 级刑法学博士研究生、东盟刑事法中心研究员，国家公派美国 Oklahoma City University 联合培养博士。崔文广（1962-），男，满族，湖北黄冈人，湖北省公安厅信息科技处二级技术主任，高级工程师。

基金项目：教育部国家留学基金委资助项目：留金发[2017]3109；中南财经政法大学 2017 年博士科研创新课题：2017BX05。

development in China, the shortcomings of concept lag, legislative conservatism, regulatory dislocation and technical backwardness continue to be exposed, which leads to the outdated and ineffective governance model of cyber crime in China at present. In order to guarantee the orderly harmony of cyberspace and promote the intelligence, socialization, specialization and legalization of network governance, we should establish the network crime governance oriented of "prevention standard", supplement the supply of administrative regulations and criminal legal norms, cooperate with industry internal control and administrative supervision, attach importance to technological innovation, accelerate the construction of cyber crime technology prevention and control system, we should properly coordinate the tension between scientific and technological innovation and network security, and promote the legalization and development of the network society.

Keyword: Smart society; cyber-crime governance; cyberspace; network rule of law construction

近年来，党和国家逐步将“网络法治建设”提上法治国家、法治政府、法治社会一体化建设的日程，网络治理社会化、智能化、专业化与法治化水平取得显著提升。[①]习近平总书记在 2014 年 2 月的中央网络安全和信息化领导小组第一次会议上着力强调了网络安全和信息化的“双轨并进”，作出统一谋划、统一部署、统一推进、统一实施的全局性部署，强调妥善处理安全和发展之关系的重要性。[②]2015 年 12 月 15 日，习总书记在第二届世界互联网大会上提出坚持网络主权、维护和平安全、促进开放合作、构建良好秩序的“四项原则”和加快全球网络基础设施建设、打造网上文化交流共享平台、推动网络经济创新发展、保障网络安全、构建互联网治理体系的“五点主张”，为全球互联网治理贡献了卓具中国特色的智慧经验。[③]尔后的第三、四届互联网大会，习总书记再次提出携手共建网络空间命运共同体、深化互联网和数字经济交流合作的中国方案。由此可见，法治化治理逐渐成为全球互联网治理中国方案的重要构成要素，是法治思维在互联网全球治理问题上的征表，是捍卫国家网络主权、保障公民网络权利的重要体现。[④]然而，网络技术的高速发展，使得网络犯罪治理面临新的时代挑战，本文力图在概析智慧社会当代内涵和中国网络发展情势的前提下，对网络犯罪的演变进程进行梳理和解读，并针对网络犯罪治理不力的现状，探讨防控网络犯罪的方案和

① 徐汉明.我国网络法治的经验与启示[J].中国法学,2018(3):52.

② 中央网络安全和信息化领导小组第一次会议召开[EB/OL].[2019-024].中国政府网. http://www.gov.cn/xinwen/2014-02/27/content_2625112.htm.

③ 朱国贤,霍小光,杨依军.习近平出席第二届世界互联网大会开幕式并发表主旨演讲[N].光明日报,2015-12-17,第 001 版.

④ 支振锋.互联网国际治理的法治化[J].网络信息法学研究,2017(1):96-102.

出路。

一、智慧社会语境下的中国网络发展情势

（一）“智慧社会”的当代解读

立足时代背景，明晰“智慧社会”的当代内涵，有利于理解和把握我国网络发展情势、“网络空间”及“网络犯罪”的实质范畴。“智慧社会”（Smart City 或 Smart Society）一词的最早源于“未来的关键要素”这一概念。[①]随着互联网技术的普及和大数据、人工智能、云计算等技术的升级，以高度智能化、数字化和网络化为突出表现形式的“智慧社会”逐渐形成，并以数字化基础促进万物感知、网络化基础加快万物互联、智能化基础提升社会智慧水平为其突出特征。[②]以 Sotiris Zygiaris 教授为代表的外国学者认为，“智慧社会”应达到“融合了众多创新社会技术和经济发展理念”[③]的城市智能水平。随着城市技术性视角的确立，“智能社会”所包含的“硬场域”与“软场域”愈发凸显，前者指的是以信息交流技术为系统核心的建筑业、能源网、自然资源、水管理、废物处理、移动性与物流等产业；后者指的是教育文化传播、政策创新、社会融合、多元政府等非以信息交流技术为核心的行业或领域。[④]截止 2012 年，全球约有 143 个正在进行或已经完成的指定“智能社会”项目，包括 35 个北美城市，47 个欧洲城市，11 个南美城市，超过 40 个亚洲城市和共计 10 个中东及非洲城市。[⑤]由此可见，网络数据、智能技术和数据技术的高效运用不仅极大提升了个人及商业应用的准确性，还促进了新兴城市的规划、创建与管理，尤其是围绕“智慧社会”开展的产业设计与技术应用。[⑥]此外，作为城市发展内在动力的智慧治理模式，融合了传统城市发展模式的变迁与政府治理、公共服务方式的转变，不仅能够促进城市治理政策的持续优化，还能使城市在生产效率、效益和可持续发展能力上取得实质

① Vito Albino, Umberto Berardi, Rose Maria Dangelico. *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, 22 Journal of Urban Technology, 3 (2015).
② 汪玉凯.智慧社会与国家治理现代化[J].中共天津市委党校学报,2018(2):62.
③ Zygiaris 教授另从五个方面分述“智慧社会”的理念外延，分别包括：“绿色”，即指立足环境保护的城市基础设施建设和降低碳排放；“关联”，即指宽带经济革命；“智能”，即指城市实时信息的感测与催化进程中产生信息增值服务的容量；“创新”与“知识”，即指基于知识性、创新性人力资本的城市革新张力。Sotiris Zygiaris. *Smart City Reference Model: Assisting Planners to Conceptualize the Building of City Innovation Ecosystems*, Journal of Knowledge Economy, 218 (2013).
④ Vito Albino, Umberto Berardi, Rose Maria Dangelico. *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, 22 Journal of Urban Technology, 8 (2015).
⑤ Jung Hoon Lee, Marguerite Gong Hancock, Mei-Chih Hu. *Towards An Effective Framework for Building Smart Cities: Lessons From Seoul and San Francisco*, 89 Technological Forecasting and Social Change, 82 (2013).
⑥ Nathalie Vergoulias. *Smart Cities: Is Cutting-edge Technology The Method To Achieving Global Sustainable Goals?* 32 Journal of Environment Law & Litigation, 286 (2017).

性突破。

（二）中国网络发展的当代情势

随着网络空间的高速发展，有关网络平台治理模式的讨论成为理论界热议的话题，理性评价我国网络发展的当代情势，是理解“网络空间”和“网络犯罪”的前提语境，也是进行网络犯罪综合治理研究的基础背景。根据中国互联网信息中心（China Internet Network Information Center，以下简称 CNNIC）发布的第 42 次《中国互联网络发展状况统计报告》，截止 2018 年 6 月 30 日，我国网民规模达 8.02 亿，互联网普及率高达 57.7%，其中，手机网民规模达 7.88 亿，通过手机接入互联网的比例高达 98.3%。另外，由中国网络空间研究院编写的《世界互联网发展报告 2017》和《中国互联网发展报告 2017》，内容涵盖国内外信息基础设施、网络信息技术、网络安全、数字经济、电子政务、互联网媒体、网络空间国际治理等互联网发展重点领域，均显现出我国当前互联网发展情势的积极、高效与智能。

我国目前正处于初级智能社会发展阶段，现代科技推动互联网产业的变革，促进智能化、智慧化、便捷化的生产生活方式的更新与发展，创造巨大商业价值和技术福利的同时，也使得网络技术异化成为困扰人类社会的全球性痼疾。以大数据为代表的新一代信息技术与网络安全紧密关联，极大地增加了信息安全管理的复杂性、交织性、动态性和综合性，使得信息安全管理面临空前威胁。一方面，智慧社会下的网络技术给予人类社会、生产生活难以估计的智能福利。呈现喷井式增长的数据技术应用不仅能够有效监控能效措施的应用效能，还能快速定位亟待完善的发展领域或技术种类。另一方面，网络技术的异化和擅用极易与现行法治社会的制度规范形成对抗冲突。如网络犯罪类型更新迅猛，使得以计算机或网络平台为犯罪对象、犯罪工具的初始网络犯罪类型，正逐渐向犯罪空间层级渗透，该领域的刑事犯罪风险也随之提升，并显现出传统犯罪的“智慧型升级”特征，特别是犯罪运行过程向技术化、智慧化发展，利用智慧科技直接参与实施犯罪、

① 李云新,韩伊静.国外智慧治理研究述评[J].电子政务,2017(7):57-58.
② 《第 42 次中国互联网络发展状况统计报告》（The 42nd China Statistical Report on Internet Development）[EB/OL].[2019-02-16].中国互联网信息中心网站.http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201808/t20180820_70488.htm.
③ 孙道萃.网络犯罪治理的基本理念与逻辑展开[J].学术交流,2017(9):129.
④ 王世伟.论大数据时代信息安全的新特点与新要求[J].图书情报工作,2016,60(6):5-6.
⑤ Nathalie Vergoulias. *Smart Cities: Is Cutting-edge Technology The Method To Achieving Global Sustainable Goals?* 32 Journal of Environment Law & Litigation, 289 (2017).

分析犯罪治理的技术弱点等规避侦查和惩处的状况屡见不鲜。

二、网络犯罪的类型演变

随着互联网络的日益普及，网络犯罪的空间跨区域性、行为隐蔽虚拟化以及手段方式的智能化不断显现，如何准确定义网络犯罪的科学内涵，国内外学者对此众说纷纭、莫衷一是。如美国刑事法学界对“网络犯罪”（Cybercrime）一词所涵盖的具体犯罪行为意见不一，部分法学家主张狭义的犯罪类型，即对计算机和网络实施犯罪以及仅使用计算机作为工具实施犯罪。《美国法典》第 18 卷第 1030 节的规定，下列针对联邦政府、金融机构使用计算机，或针对州际或外国商贸和通讯的计算机实施下列行为的，构成网络犯罪：1、未经授权入侵政府信息系统并获取保密文件，非法向未经授权的他人披露或违法保留涉密文件的；2、非法入侵计算机并获得行为人无权访问的相关信息的；3、非法入侵计算机并实施欺诈行为的；4、因未经授权入侵计算机或将程序、代码或信息插入计算机而造成设备损害的；5、为向州际或外国商贸中的个人或其他实体法人勒索财物，威胁损害计算机的。

准确把握网络犯罪的发展规律，不仅是妥善协调网络科技创新与网络安全之间紧张关系的重要前提，更是立法、司法、监管等层面积极回应网络犯罪治理困境的必然要求。回归本国语境，随着网络代际演变，网络犯罪逐渐朝着“犯罪对象→犯罪工具→犯罪空间”的方向演进，具体表现形式如下：

（一）初级阶段：计算机信息系统“犯罪对象化”

上世纪九十年代起，计算机的低使用率折射出萌芽阶段网络空间的“弱连接性”，彼时的互联网的交互功能受限于经济社会发展水平和信息技术普及程度，较难实现网络使用者与网络平台的信息交流，个人冲突多发生于计算机信息系统使用过程中的违规侵入、删除、修改、增加、干扰等环节。因此，彼时的网络犯罪指的是将计算机信息系统作为犯罪对象的计算机犯罪，即仅能在计算机空间实施的，利用计算机操作所实施的危害计算机信息系统（包括内存数据及程序）安

[9] 此处针对传统犯罪的“智慧型升级”可从两方面加以理解：一方面是传统犯罪形式层面的技术升级，即通过行为人通过网络化、数据化及智能化科技实施犯罪，扩充传统犯罪的形式外延；另一方面是传统犯罪与智慧型犯罪相结合的升级模式，即，此类犯罪具有较强时效性，且多为涉及多个罪刑规范的“链式”犯罪模式。张旭,朱笑延.弱智慧社会语境下的犯罪治理：情势、困境与出路[J].吉林大学社会科学学报,2019(1):21-23.

[10] Thomas Fedorek. *Computer + Connectivity = New Opportunities for Criminals and Dilemmas*[J]. 76 New York State Bar Journal, 10 (2004).

[11] 18 U.S.C. § 1030 (1994).

全的犯罪行为，其犯罪对象主要为计算机信息系统，且犯罪行为主要通过非法操作计算机予以实现。彼时的网络犯罪通常被理解为危及计算机安全的犯罪，以 1997 年《中华人民共和国刑法》（以下简称 97 刑法）第二百八十五条和第二百八十六条为例，非法侵入计算机信息系统罪和破坏计算机信息系统罪的设立，分别旨在保护相关领域的计算机信息系统不被非法侵入和确保计算机信息系统正常运行。此外，根据国务院 1994 年 2 月 18 日发布的《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）第二条详述了计算机信息系统的内涵，即指有计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

简言之，计算机信息系统的“犯罪对象化”体现了网络犯罪类型演进初级阶段的整体特征，不仅体现了互联网发展初期的“弱交互性”特性，还是刑事法律、行政法规等对彼时计算机信息系统保护的体现。

（二）发展阶段：网络“犯罪工具化”

进入二十一世纪后，随着科技水平的逐步提升，网络使用者与网络平台的连接性随之增强，以“点对点”为主要特征的网络交互不断凸显，网络技术和网络连接的发展呈现出一派繁荣的盛况。2000 年 12 月 28 日，全国人大常委会审议通过了《关于维护互联网安全的决定》，对彼时的网络犯罪具体形态进行高度凝练，并其概括为以下五种类型：1、损害互联网运行安全的行为；2、利用互联网损害国家安全和社会稳定的行为；3、利用互联网损害社会主义市场经济秩序和社会管理秩序的行为；4、利用互联网损害个人、法人和其他组织的人身、财产等合法权利的行为；5、利用互联网实施的其他犯罪行为。不难看出，电子商务等网络平台迅速崛起，早前以计算机信息系统为犯罪对象的纯粹系统攻击型犯罪，逐渐被利用网络技术或网络平台为工具的传统犯罪所吸纳和发展。这种网络

[12] 赵秉志,于志刚.论计算机犯罪的定义[J].现代法学,1998(5):10.

[13] 97 刑法第二百八十五条规定：“违反国家规定，侵入国家事务、国防事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”第二百八十六条规定：“违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。”《中华人民共和国刑法（1997 年修订）》[EB/OL].[2019-02-16].最高人民检察院网. http://www.spp.gov.cn/spp/fl/201802/t20180206_364975.shtml.

[14] 《全国人民代表大会常务委员会关于维护互联网安全的决定》[EB/OL].[2019-03-05].中国人大网. http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content_5131101.htm.

[15] 于志刚.网络犯罪的代际演变与刑事立法、理论之回应[J].青海社会科学,2014(2):2.

“犯罪工具化”特征反映了网络发展阶段的犯罪共性，该时期的刑事法领域关于网络犯罪的理论探讨尤为热烈：如有学者主张将网络犯罪与计算机犯罪概念类型化；也有观点认为网络犯罪是利用计算机、网络技术等信息技术或者其特性，危害计算机、网络和数据安全，危害社会信息安全，社会危害性严重的行为；还有观点支持将网络犯罪理解为以计算机网络为犯罪工具或者犯罪对象而实施的严重危害网络空间安全的犯罪行为的观点；其他学者则认为应将网络犯罪定义为实施危害网络信息系统安全的犯罪行为。有学者将这种兼具网络技术参与和传统犯罪构成的表现形式成为“传统犯罪的网络异化”。如利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密等，或者利用网络传播淫秽物品等，均表现出利用计算机或网络技术作为犯罪工具的特征。

网络技术的蓬勃之势暴露出网络犯罪领域法律规范的匮乏和传统刑法理论的滞后。为缓解立法、司法领域的紧张矛盾，国家立法、司法机关前后出台多项法律修正案和司法解释以适应司法实践需求。如 2009 年 2 月 28 日全国人大常委会审议通过《中华人民共和国刑法修正案（七）》（以下简称《刑修（七）》），增设第二百八十五条第二、三款的非法获取计算机信息数据罪、非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系的程序、工具罪。尔后，最高人民法院、最高人民检察院（以下简称“两高”）于 2011 年 8 月 1 日发布了《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》（以下简称《计算机刑事案件解释》），具体列举了非法获取计算机信息系统数据、非法控制计算机信息系统的“情节严重”和“情节特别严重”的行为，并详细阐释了提供侵入、非法控制计算机信息系统的程序、工具行为中的“程序、工具”、“情节严重”和“情节特别严重”的具体事项。不难看出，网络发展阶段的立法转向，一方面为司法实践中突出问题提供了规范依据，另一方面，通过完善立法为高速发展的网络技术夯实法制基石，较好地发挥了承前启后的作用。

简言之，发展阶段的网络犯罪在吸纳了前一阶段的“犯罪对象化”的计算机犯罪基础上，还表现出网络“工具化”和“传统犯罪网络异化”等特征。刑事法

[89] 刘守芬,孙晓芳.论网络犯罪[J].北京大学学报,2001(3):115;皮勇,网络犯罪比较研究[M].北京:中国人民公安大学出版社.2004:11-12;赵秉志,卢建军.中国网络犯罪的现状及特点[J].法律学术,2005(5):67-68;杨正鸣.网络犯罪研究[M].上海:上海交通大学出版社.2004:11. 转引自:崔仕绣.网络犯罪的刑事管辖问题研究[J].金田,2014(4):364.

[90] 于志刚.传统犯罪的网络异化研究[M].北京:中国检察出版社,2010:1.

领域的有限扩张，虽一定程度上弥补了网络发展阶段的法治需求，但法律规范先天的滞后属性，使得网络技术发展与不断衍生的网络犯罪风险之间的断层加深，传统刑法理论、刑事法律规范和司法解释难以兼容网络犯罪逐渐繁杂的表现形式。

（三）成熟阶段：网络“犯罪空间化”

随着网络平台模式的升级，以移动智能手机为代表的即时通讯平台借助互联网迅速发展，包括社交平台、支付平台、搜索平台、信息平台在内的网络平台，通过个性化的定制服务、多元化的业务功能以及海量用户粘性，逐渐发展成为具有独立属性的网络生态系统，在平台思维和平台模式的共同作用下，“网络空间”与“现实社会”并行的“双层社会”局面逐渐形成。其中，作为“一个旨在促进信息融合的，运用技术实现个人与公共财产综合管理的，用于组织和传输且不断发展的人为领域”，“网络空间”（Cyberspace）逐渐升级成为一种相对独立的犯罪场域。在当前智慧社会语境和网络发展格局的耦合作用下，网络安全已经渗透到国家安全、社会安全、公共秩序以及公民个人信息、财产安全等各个层面，网络犯罪被赋予了新的时代特征。

首先，“逐层包容性”是现阶段网络犯罪最突出的特性之一。初级阶段和发展阶段的网络犯罪特征并未因时空、技术发展而泾渭分明地与现阶段的网络犯罪割裂，而是呈现出“逐层包容”的关系，即前一阶段犯罪类型通常被后一阶段的网络犯罪类型所吸收、包容和发展。

其次，“高度隐匿性、智能性”是网络犯罪相较于其他类型犯罪的重要特征。其中，高度隐匿性体现在犯罪手段的隐匿水平提升、犯罪行为人普遍匿名化、犯罪表征之隐蔽性等方面；高度智能化则依赖于智能技术、大数据、“互联网+”等科技的发展水平。当前网络犯罪分子多具备较为丰富的互联网技术和计算机知识，善于将智能科技运用与犯罪的各个环节，在缩短犯罪耗时的同时，通过加密或设置傀儡网站等操作以隐藏作案手段。此外，网络犯罪分子利用互联网高度开放性、虚拟性和时空跨越性等特点，运用技术屏障隐藏个人信息，加大犯罪侦破难度。结合了传统犯罪构成要素与信息网络技术的新型技术型犯罪，如盗取 QQ 号并欺骗被盗者好友汇款的、通过盗取银行账户密码盗取资金的，这些犯罪本质

[91] 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[J].政治与法律,2018(1):60-68.

[92] Gragam H. Todd. *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*[J]. 64 Air Force Law Review, 68 (2009).

上属于传统诈骗和盗窃的范畴，但其作案技术性特征更为显著。

最后，现阶段网络犯罪逐渐向“产业化、精细化”方向发展。随着智能技术和网络产业的蓬勃发展，网络犯罪逐渐表现出产业化和精细化趋势，即通过网络能将不同违法类型予以连接，形成上下游分工明确的产业链条，网络违法行为的分工日益精细。如上游网络诈骗犯罪肆意发展，与下游的非法获取个人信息、利用个人信息实施诈骗行为等不无关系，且逐渐形成以经营方式为分工的网络犯罪产业，这种共同犯罪意思联络不详、匿名化交易的犯罪协作格局也给当前刑事法律及司法解释带来了新的挑战。再如以互联网平台获取大众资金支持为主要特征的众筹融资(Crowd Funding)和通过网络平台实现借贷交互的 P2P 网络借贷(Peer to Peer Leading），网络技术的介入不仅降低了金融业务的投资门槛，还增加了金融活动受众的不确定性，使犯罪具备更高的隐蔽性、复杂性和广泛性，是当前网络犯罪典型的上下游犯罪。

随着大数据、智能科技和人工智能等网络技术新代际的发展和成熟，传统的法律制度和保守主义犯罪治理面向已难以应对技术爆炸局势下不断涌现的新型网络犯罪。为维护新型网络安全，规范惩处网络犯罪，立法、司法机构作出积极调整，其中，以 2015 年 8 月 29 日通过的《中华人民共和国刑法修正案（九）》（以下简称《刑修（九）》）最具代表性。《刑修（九）》不仅补充了第二百八十五条第四款和第二百八十六条第四款，即单位提供侵非法控制计算机信息系统的程序、工具罪和单位破坏计算机系统罪的情形，还增设了第二百八十六条之一拒不履行信息网络安全管理义务罪、第二百八十七条之一非法利用信息网络罪和第二百八十七条之二帮助信息网络犯罪活动罪。此外，根据最高人民法院、最高人民检察院、公安部于 2014 年 5 月 4 日（以下简称“两高一部”）出台的《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》（以下简称《网络犯罪意见》），网络犯罪案件的范围被明确为以下四类：一、危害计算机信息系统安全犯罪案件；二、通过危害计算机信息系统安全实施的盗窃、诈骗、敲诈勒索等犯罪案件；三、在网络上发布信息或者设立主要用于实施犯罪活动的网站、通讯群组，针对或者组织、教唆、帮助不特定多数人实施的犯罪案件；四、主要犯罪行为在网络上实施的其他案件。此外，《网络犯罪意见》进一步厘清了网络犯罪

[8] 吴孟栓.明晰诉讼程序 依法惩治网络犯罪[N].检察日报,2014-07-07,003.
[9] 崔仕绣.我国互联网金融领域的涉罪分析与刑法规制[J].广西大学学报(哲学社会科学版).2018(4):118.

的管辖争议，即以犯罪地公安机关立案侦查为原则，必要时可以由犯罪嫌疑人居住地公安机关立案侦查。此处的“犯罪地”包括用于实施犯罪行为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或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地，被害人被侵害时所在地，以及被害人财产遭受损失地等。

简言之，当前智慧社会语境加速互联网技术的飞速发展和广泛应用，网络平台的高度连接促进“双层社会”格局的形成。与此同时，现阶段网络犯罪在吸收和包容了计算机信息系统“犯罪对象化”和网络“犯罪工具化”特性的基础上，逐渐显现出产业化、精细化、高度隐匿性和智能性的网络“犯罪空间化”特性。

三、智慧社会语境下的网络刑事惩治困境

（一）“唯结果论”网络犯罪治理观念滞后

相较于传统刑事犯罪主要依据已经造成的危害后果及其程度作为惩处前提，网络犯罪治理若仍然沿袭这种“唯结果论”观念，势必会导致惩治时机的滞后，难以有效排除或控制妨害结果，不仅导致扩散于网络空间的危害行为的复制、传播风险加剧，还增加了司法实务部门认定犯罪的难度，特别是对损害后果严重程度和因果关系的确认。鉴于目前尚无特定归国际监管部门统一管理国际网络犯罪，有学者指出，随着网络安全风险的递增，设立国际网络安全监管机构的必要性也随之凸显。此外，国家社会治理与智慧科技发展的逻辑悖论还体现在控制本位的犯罪治理模式上，即长期盘踞的“压力维控型”传统犯罪治理模式强调国家管治和服从，主张对违法犯罪行为的常规防控和应急打击。

事实上，智慧社会驱动下的创新技术创新使得网络平台为代表的技术风险骤升。由技术安全衍生的刑事犯罪风险主要通过网络入侵的方式偷窥、复制、更改、或者删除计算机信息的行为和散步破坏性病毒、逻辑炸弹或者放置后门程序等。各类网络技术风险的骤现，导致“唯结果论”的网络犯罪治理观念的滞后性持续暴露。

（二）网络犯罪的法规范供给匮乏

[9] 时延安.网络规制与犯罪治理[J].中国刑事法杂志,2017(6):15.
[10] Susan Bagdasarova. *Brave New World: Challenges in International Cybersecurity and the Need for Centralized Governance*[J]. 119 Penn State Law Review, 1031 (2015).
[11] 周建达.转型期我国犯罪治理模式之转换——从“压力维控型”到“压力疏导型”[J].法商研究,2012(2):62.
[12] 上海市浦东新区人民检察院课题组.网络金融犯罪治理研究[J].山东警察学院学报,2016(1):77.

除了“唯结果论”的网络犯罪治理观念背离时代发展，各个网络发展阶段的法规范供给整体相当匮乏、被动。如前所述，尽管97刑法关于计算机犯罪的刑法规范基本迎合网络犯罪发展初级阶段的时代需求，但彼时以计算机技术为代表的科技水平还相当有限，顺势而生的法规范欠缺相关犯罪理论研究和实证调研，使得彼时网络犯罪规制呈现明显的“阶段性或应急性”特点，社会整体层面的计算机接纳程度低使得计算机犯罪形势基本可控，立法诉求并不突出。

随着计算机网络的全面普及，网络犯罪呈现愈演愈烈之势，保守的刑事法规范的滞后性、局限性日渐凸显。为此，《刑修（七）》增设部分网络犯罪类型，均围绕彼时司法实践之需求，但仍遗留较多问题，如故意制作、传播非病毒等破坏性程序，影响计算机系统正常运行并造成严重后果的，则不属刑法第二百八十六条第三款的范畴，实难定罪处罚。

直至当前，大数据时代和智能科技的广泛运用，加速了网络空间的发展，新型网络犯罪不断涌现。为有效打击网络犯罪，营造和谐共赢的网络环境，相关部门在规范层面贡献突出，其中以《刑修（九）》最为突出，有学者评价称其“客观上使中国网络犯罪的立法活动步入一个新的界定，凸显观念转型的时代气息”，刑事立法朝着积极回应的面向发展。但遗憾的是，新增罪名在立法格局上的被动性、离散性和低操作性仍不足以满足社会现实发展需求。此外，刑事立法的频繁修正也未与前置民事、行政法律法规以及其他部门法形成呼应，不乏担忧刑法“过度扩张”的学者转而思索法解释主义解决途径的适正性。鉴于刑事法领域针对网络犯罪普遍呈现的“唯结果论”惩治路径，仅依靠“专案解释”或“个案解释”的兜底策略，显然不能满足犯罪预防的需求，加之行政法规对网络违法犯罪行为的规范作用并不显著，使得发挥惩治作用的法规范供给匮乏。此外，随着人工智能科技的不断完善，以“智能人”为个体实施犯罪的可能性逐渐提高，不仅使传统刑法有关“人的主体性地位”的主张被撼动，还引发“智能人”刑事责任主体适格与否的广泛探讨。正视智慧社会狂潮下智能机器人刑事责任能力的变化，必然需要刑法规范作出适时、适度的扩张。

（三）“多层次”网络犯罪监管格局尚待完善

随着“双层社会”格局的确立与发展，有关“多层次”网络监管格局的构建

[9] 王燕玲.中国网络犯罪立法检讨与发展前瞻[J].华南师范大学学报(社会科学版),2018(4):130.
[10] 王燕玲.中国网络犯罪立法检讨与发展前瞻[J].华南师范大学学报(社会科学版),2018(4):129.

受到业界理论学者与实务人员的重视。“网络监管”指的是网络运营监管、网络内容监管、网络版权监管、网络经营监管、网络安全监管、网络经营许可监管等，通常由代表政府参与网络监管的主要职能部门发布行政命令，责令行为人改正违规行为，如通信管理部门、互联网新闻宣传管理部门、公安部门、文化部门、广播电影电视管理部门和新闻出版部门等。鉴于网络空间的形成，使得以计算机信息系统为犯罪对象和以网络为犯罪工具的传统型网络犯罪，逐渐向分工明确的网络空间上下游犯罪转移。监管部门层级繁杂、监管职责界限混乱、监管权限不清均导致不法网络违法犯罪行为游离于法律规范的灰色地带。智慧社会背景下的网络技术创新离不开适度弹性的“多层次”网络犯罪监管体系的支持，否则，不论是过于刚性还是柔性的的监管体制，都将导致网络空间发展被极度压缩或缺乏管束。

（四）网络犯罪技术防控体系亟需加强

技术防控体系的不成熟也暴露了网络犯罪综合治理的短板。如前所述，网络犯罪具有高度隐匿性、智能性的特征，行为人脱离传统犯罪的地域限制，匿名运用网络技术实施犯罪，未有任何身份信息备案的情况下，侦查部门需耗费大量精力追踪犯罪人线索，不仅增加了案件侦查难度，还会造成大量资源的浪费。我国网络犯罪技术防控体系尚处发展阶段，对于上下游犯罪结合的新型网络犯罪，网络见警率较低，常态化的网络巡查机制还有待健全，传统侦查手段易延误侦查时机，不利于网络犯罪的综合治理。此外，如何妥善运用大数据信息技术，实现公安业务系统与海量数据融合，辅助嫌疑人网络活动轨迹的确定，也是建立健全网络犯罪技术防控体系尤需关注的部分。

四、智慧社会语境下的网络犯罪治理对策

网络空间绝非“不法之地”，网络犯罪的时代特性预示着网络空间综合治理不能延续普通违法犯罪的治理旧途，结合智慧社会语境下的中国互联网发展情势，应从网络犯罪治理观的调整、法规范的适度补充、多层并行的监管体系的确立和智能防控体系的建构等方面展开讨论。

（一）树立“预防本位”的网络犯罪治理面向

针对智慧社会语境下网络犯罪所呈现的时代特性，纯粹的、绝对的报应主义

[11] 王利宾.网络运营商严重监管失职的犯罪化问题研究[J].湖南社会科学,2018(4):104.

犯罪治理观不仅不利于技术进步和社会发展，单纯的刑事惩治还会降低网络犯罪的一般预防功效，导致犯罪治理的极端僵化。此外，当前网络犯罪规制思路还存在着难以适应网络空间规律、规制主体责任不清、规制手段落后和因规制手段不当而过度干涉合法权利等不足。因而，网络犯罪的当代治理应注重战略、策略的协调与平衡，既要提高治理网络犯罪的意识和技术制衡能力，以科学的刑事政策引领与指导治理活动，又要兼顾校正和纠偏网络犯罪刑事治理的立法偏航与司法误区。如前所述，以犯罪协助为主要特征的上下游分工犯罪成为智慧社会语境下网络犯罪的重要特征。而树立“预防本位”的网络犯罪治理面向势必成为厘清这种“协作分工”的前提，如对于合法搜集和掌握公民、企业个人信息等相关数据的单位，应承担较为严格的信息保护责任，并对基于重大过失或未尽合理审查而造成严重后果的承担刑事责任。笔者较为赞同张旭教授关于预防本位的犯罪治理机制的建制思路，即宏观层面从社会结构、经济转型、技术革新、文化氛围、治理体系反思犯罪成因，并在此基础上确立预防主义犯罪防控体系；在中观和微观层面，加强对表象犯罪的深层次剖析，特别要注重对新型网络犯罪的上、中、下游违法行为的预防和惩治，加强在犯罪情景预防、成因分析及数据检测等环节的防控与惩治。这些外围违法行为通常游离于刑事法网而欠缺法规范制约，是助长智慧型网络犯罪的重要动因。除了强化网络犯罪的事后惩处和规制外，“预防本位”的网络犯罪治理面向还要求加强重点领域、重点人员和重点行业的事前防范和精准防控，要加强智慧型网络犯罪高发领域从业人员的岗前技术培训和普法教育。

（二）丰富网络犯罪的法律供给

内容适正的法律规范是治理网络犯罪的重要依据。以域外立法经验为例，美国代顿法学院 Susan W. Brenner 教授认为，加速联邦与州际层面针对“网络犯罪”的立法进程的动因可以概括为以下两个方面：一方面，科学技术的迅猛革新使得网络环境日益丰富，网络犯罪作为新兴犯罪类型，其犯罪特征不断丰富；另一方面，立法者对规制网络犯罪的“固有歧义”。其中，“固有歧义”表现为立法者对网络犯罪法律规制紧迫性认识上的分野：积极支持立法的学者认为，网络犯罪

[8] 时延安.网络规制与犯罪治理[J].中国刑事法杂志,2017(6):22.
[9] 孙道萃.网络犯罪治理的基本理念与逻辑展开[J].学术交流,2017(9):132.
[10] 张旭,朱笑延.弱智慧社会语境下的犯罪治理：情势、困境与出路[J].吉林大学社会科学学报,2019(1):27.

作为新兴犯罪类型，亟需具有时效性的实体法作为规范前提；反对者则坚持“老瓶装新酒”的刑法解释途径，认为足以通过司法判例和法官释法等途径，解释和丰富现行法律以匹配对网络犯罪的制约需求。习近平总书记在中央全面依法治国委员会第二次会议中强调，要坚持以人民为中心，坚持从实际出发，坚持尽力而为、量力而行，以规范的程序、科学的决策维护重大公共利益、维护人民合法权益，促进社会公平正义，不断增强人民群众获得感、幸福感、安全感。丰富当前网络犯罪的法律供给尤需注重立法过程的实事求是、科学规范。

首先，在行政法规领域，需要将行政处罚和行政法规介入应作为普通网络违法行为的前置规制条件。如网络运营商承担刑事责任的前提是行政违法和行政责任的确立，而具体行政违法内容和行政责任，须以明确的行政法规为前提。如前所述，不论是此前发布的《条例》、《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》、《关于维护互联网安全的决定》，还是2015年6月24日审议通过的《网络安全法》，均旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，对彼时计算机信息系统、发展阶段的网络犯罪具体类型进行了概括性总结。为了进一步强化行政法规与刑事法律规范之间的连接性，应不断加强前后规范之间的传递性、升阶性和发展性。如有关公民个人信息保护方面，应当建立完善的防范机制，尤其针对公民重要的个人信息，应当对具有个人信息采集需要的单位的收集、存储、使用、销毁等环节设立严格的法律规制，对于违反相关公民个人信息法规的单位及个人，应予以行政处罚。进而确保利用个人信息严重损害网络秩序的行为在行政处罚不足以规制的情形下，可以向刑事法惩治方向平稳过渡。此外，对具有个人信息采集需要的单位进行前期执业审批和定期巡查评估也具有其现实必要性，同样需要有关行政机关的合理监管和行政法规的规范。

其次，在刑事法律规范领域，有必要从加强司法解释和丰富立法两个层面提升网络犯罪综合治理能力。一方面，刑法作为保障公民人身财产安全的“最后屏

[11] Susan W. Brenner. *State Cybercrime Legislation in the United States of America: A Survey*[J]. 7 Richmond Journal of Law and Technology, 28 (2001).
[12] 习近平主持召开中央全面依法治国委员会第二次会议[EB/OL].[2019-02-25].新华网.http://www.xinhuanet.com/politics/leaders/2019-02/25/c_1124161654.htm.
[13] 王利宾.网络运营商严重监管失职的犯罪化问题研究[J].湖南社会科学,2018(4):103.
[14] 时延安.网络规制与犯罪治理[J].中国刑事法杂志,2017(6):19.

障”，对于严重侵害网络空间、违反网络管理法规的行为，应及时予以规制，特别在前置法律法规难以实现法益保护实效时，刑法有必要发挥“兜底”功能，以实现法益保护与人权保障相统一的旨趣。鉴于刑法内里的谦抑理念和《刑修（七）》、《刑修（九）》围绕日益丰富的网络犯罪类型而增设的数个罪名的现实，对于可以通过合理延展范围内的扩张解释，将相关犯罪行为类型纳入现有罪刑规范的约束范围内。如前所述，网络空间现已成为平行于现实社会的独立场域，对于恶意制造虚假社会热点，破坏网络正常舆论秩序，散布、转发谣言严重危害政府公信力、诋毁道德楷模等扰乱网络空间正常秩序的行为，可被解释为造成网络秩序严重混乱的行为，因而涵盖在涉及扰乱包括“公共场所”、“公共秩序”等构成要件的传统犯罪中。另一方面，当网络技术催生下的犯罪类型明显超出刑法解释的射程范围，且行为严重危害国家、社会秩序、公民的人身、财产等法益的，立法层面则须积极干预，将类型化犯罪行为涵盖在刑事法律规范的范畴之内，以体现法律灵活性与稳定性的动态平衡。尤其注意网络犯罪刑事立法的审慎克制，谨防过度膨胀的立法趋向对网络创新造成侵犯，这是因为刑法作为规范社会秩序的“最后一道防线”，应坚守其谦抑性和补充性，如果采用其他规范手段足以抑止并能充分保护法益时，就不宜轻易发动刑法。

最后，在程序保护层面，还需缜密设计网络治理法律程序。作为规制网络监管、行政执法、司法等公权力机关行使网络空间治理权所必要的限制方式及网民获得权益救济的程序规则，网络治理法律程序直接影响网络犯罪的治理效果，关系到公民、法人和其他组织的政治经济、文化社会、个人生活等权益在网络空间遭受侵犯时，能够迅速、有效地获得救济，涉及民事、行政和刑事法等多个领域。

（三）协同行业内控与行政监管

早在 20 世纪末，美国学者就围绕网络治理的监管模式进行了激烈讨论。1996 年，美国“电子前线基金会”（Electronic Frontier Foundation，以下简称 EFF）创始人之一的 John Perry Barlow 就已在其文《网络空间独立宣言》中提出，对互联网启用正式监管是“难以实现且不可取的”，因而主张私人自治本位的互联网监管格局。而以 Jack Goldsmith 教授为代表的学者则主张，传统的互联网正式监

[8] 于志刚.网络犯罪的代际演变与刑事立法、理论之回应[J].青海社会科学,2014(2):10.
[9] 徐汉明.我国网络法治的经验与启示[J].中国法学,2018(3):68.
[10] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, https://www.eff.org/cyberspace-independence, 2019-02-17.

管模式是“可能且不可避免的”。随后，美国网络行业各利益载体协调一致并联合出台《网络生成内容的服务商指导原则》（Principles for Users Generated Content Services，以下简称 PUGCS），旨在将现存版权法作为出发点和假设背景，提出了行业自治与传统监管协调并举的“中间道路”。一方面，“中间道路”对传统法律规则的依仗，折射出互联网监管亟需“清晰、合理且笼统的”法规范的实体支撑；另一方面，以灵活性、协同性和技术创新性著称的互联网行业的自治监管，对填补法律规范的空缺发挥着良好的兜底效用。

鉴于当前泛化的网络违法犯罪态势，我国网络监管机关与网络执法机构在网络治理法治化进程中发挥了重要的调节作用，监管效果明显。如国家网信监管、执法部门连续五年联合开展“剑网行动”、“护苗行动”；组织开展两轮重点地区的电信网络新型违法犯罪整治活动；针对党政机关、事业单位和国有企业的互联网网站组织开展专项整治活动；统筹开展打击电信网络新型违法犯罪和规范网络监管等专项行动；规范互联网群组信息服务提供者的信息安全管理责任等。这些监管举措对为了进一步提升网络安全防范能力，保障网络的安全运行，打击网络犯罪违法违规行为，在监管方面可从都起到了良好的促进作用，在给予肯定的同时，还需将成效显著的专项行动规律化、常态化。

然而，纯粹的行业自治或单一的行政监督均有其各局限性，因而需要立足智慧社会的现代化背景，结合行业自治和行政监管的有益成分，发挥政府主导功效的同时，建立网络犯罪长效治理机制，发挥行业自控和行政监督的双效合力。一方面，网络犯罪的综合治理应以行业内控为主导。提升各网络管理主体的自律能力，不仅是针对当前网络犯罪高度智能化、匿名化特征的综合考虑，更是鼓励网络技术创新、提升网络企业自我管理、自我监督、自我调节的表现。建立网络行业的自我管理机制，有助于充分调动网络服务提供商和广大网民的参与积极性，还能在确保政府宏观管控的前提下，节约网络犯罪治理成本、提供监管效率。具

[11] Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Indiana Journal of Global Legal Studies, 475 (1998).
[12] 《网络生成内容的服务商指导原则》（*Principles for Users Generated Content Services*），[EB/OL].[2019-02-26].http://ugcprinciples.com/.
[13] 这种“中间道路”要求在广义的法律框架内进行自治与私人监管，且法律框架须兼顾网络使用者的综合利益。其中，自治包含私人起草和私人协定两层含义。Harvard Law Review Association, *The Principles for Users Generated Content Services: A Middle-Ground Approach to Cyber-Governance*, 121 Harvard Law Review, 1387 (2008).
[14] Harvard Law Review Association, *The Principles for Users Generated Content Services: A Middle-Ground Approach to Cyber-Governance*, 121 Harvard Law Review, 1388 (2008).
[15] 徐汉明.我国网络法治的经验与启示[J].中国法学,2018(3):60.

体措施包括规范网络金融领域征信体系机制、加强网络业务的个人信息管理、强化网络参与者伦理道德教育等。另一方面，行政监管方面，要尽快厘清网络行业监管主体的责任边界，扭转“分业监管”所导致的重叠和真空区域。可考虑按照业务类别设立综合监督管理机构，如此，可加快纵向相关法律法规精神的传递，还能凸显政府保障网络空间和谐、有序的职责。

（四）重视技术创新和防控体系建设

大数据、人工智能等科技的进步带给网络犯罪综合治理新的启发和导向，其中，技术创新和防控体系的构建是网络犯罪综合治理的科技支撑。鉴于当前肆虐的网络犯罪形式，各地公安部门积极结合智慧社会的技术需求，在警务平台信息化建设、信息数据监管和网络犯罪侦查等方面，逐渐加大了科技创新力度，有力地回应了社会关切。以我省为例，根据湖北省公安厅发布的2016至2018年《湖北省公安工作情况统计》，全省公安机关在省委政法和公安部、省委政法委的领导下，创新推进信息化建设，将6大类48个项目纳入全省政法信息化建设工程总体规划，围绕“湖北公安云”核心，实现业务数据标准化，全面优化警综平台主体功能；围绕智慧公安、数据警务，兴建省公安厅大数据中心，整合数据资源4000类3万亿条，多策并举实现警务创新成果向现实战斗力的转化；先后出台《湖北省公安厅关于推进大数据条件下警务运行机制改革的指导意见》、《关于深入推行“情报勤舆”一体化警务机制建设的工作意见》等文件，确定了“一核四横三纵”的警务大数据战略总体框架，坚持“双轮驱动”，强化科技支撑，探索警务机制改革，推行“1+N”公安大数据服务模式，推动公安事业的转型升级。

为有效凝聚网络犯罪治理合力，提高社会网络安全防范意识，公安部门还应加大技术创新力度，不断提升犯罪防控体系建设的综合水平。首先，公安机关应充分发挥防控统领作用，有效整合政府部门、社会组织和公众力量，建立网络安全保障合作机制，构建网络安全防御体系，形成“统一领导、多方配合”的网络空间管理体系，营造和谐、共赢、富有活力的网络空间。其次应遵循国家网络技术研发战略，进一步加强网络技术自主创新，尤其重视对针对国家机关网站、公安内网等政府网站的系统漏洞排查，加大网络平台的监控力度，定期对网络安全

[6] 近几年，湖北省公安部分在电信网络诈骗犯罪侦破方面取得突破性进展，2016-2018年共侦破此类案件1662、8122、9675年起，挽回群众近7亿元损失。2016-2018年湖北公安工作情况统计[EB/OL].[2019-02-15].湖北省公安厅网. http://jwgk.hbgat.gov.cn/info/nIndex.jsp?node_id=GKhbgat.

威胁进行清理，通过更新技术设备，提升恶意代码和擅自利用信息数据等违法行为的定位精准度，提高金融、交通、通信等关乎民生的重要信息基础设施的防御水平，净化网络安全环境。再次，高素质信息化人才队伍是构建创新型网络犯罪综合治理平台的保障，应重视对科技信息人才的遴选和任用，培养业务素质过硬、信息技术突出的网络监管执法人才，可考虑将网络平台综合治理作为公安机关信息技术人才的定期考核内容，对取得显著成效的单位和个人给予奖励。最后，突出防控体系的“前端化”治理，监管部门应重视大众防范和教育宣传，通过多重传媒途径培养公民网络安全防范意识，增强民众维护网络安全的自觉性、主动性，建立健全网络服务提供方的安全风险评估、预警防范和信息共享机制。

综上所述，城市智慧治理妥善融合了网络技术、数据技术、信息通信等技术，不仅卓有成效地提升了政府全面、敏锐、准确地掌握社会实时信息的能力，还通过挖掘数据主动迎合社会需求，有力推进了智慧社会的创建升级。习总书记在十九大报告中明确提出，要构建现代社会治理新格局和深化供给侧结构性改革、加快建设社会主义文化强国的战略部署，强调互联网、大数据、人工智能和实体经济的深度融合，进一步强化互联网内容建设和网络综合治理体系的建立。面对大数据、智能科技高速发展的当今社会，网络犯罪表征出“犯罪对象→犯罪工具→犯罪空间”的演进格局，促使我们积极探索网络犯罪综合治理的智慧路径。开展多层次、多维度的网络犯罪治理，应基于“预防本位”的治理面向，在适当丰富行政法规和刑事规范的法律供给的同时，兼顾行业内控与行政监管，重视技术创新和防控体系总体建设，如此是为促进网络空间和谐法治、健康高效之根本。

[7] 白海将.中国网络安全形势及对策研究[J].云南警官学院学报,2015(1):84.
[8] 李云新,韩伊静.国外智慧治理研究述评[J].电子政务,2017(7):59.
[9] 习近平.决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告(2017年10月18日)[N].人民日报,2017-10-28,第001版.

电商法颁布背景下利用网络直播进行犯罪的现状及规制

陈奕屹

（武汉大学 法学院，湖北 武汉 430072）

摘 要：近年来，利用网络直播进行犯罪的数量激增，实证研究表明，利用网络直播进行的色情、赌博、诈骗类犯罪与直播平台的类型与规制方法有密切的联系，对网络直播平台进行分类规制对于减少利用网络直播进行犯罪有十分重要的意义。然而，2019 年 1 月 1 日开始实施的《中华人民共和国电子商务法》并未将网络直播平台及直播行为纳入其管辖范围内。在目前法律规范对网络直播行为的规范尚有缺陷的前提下，为减少利用其进行犯罪的数量，应当加强普通网民的防范意识、加大直播平台的自查与管理力度并加快落实电商法与刑事司法的介入与规制。

关键词：网络直播 互联网直播平台 网络犯罪

根据国家互联网信息办公室 2016 年 11 月 4 日颁布的《互联网直播服务管理规定》，网络直播是是指基于互联网，以视频、音频、图文等形式向公众持续发布实时信息的活动，网络直播服务提供者也就是直播平台，是指提供互联网直播平台服务的主体。截至 2018 年 6 月，我国网络直播用户规模达到 4.25 亿，用户使用率为 53.0%[①]。网络直播平台的迅猛发展和监管不够严格共同催生了利用网络直播进行犯罪的行为，给普通网民带来了严重危害。本文从 150 例利用网络直播进行犯罪的一审判决书入手，研究利用网络直播进行犯罪的基本现状、多发平台及其特征，分析此类犯罪猖獗的原因并提出治理建议。

一、利用网络直播进行犯罪的犯罪现状与多发平台

（一）犯罪的基本类型与现状

1. 犯罪的基本类型与多发地区

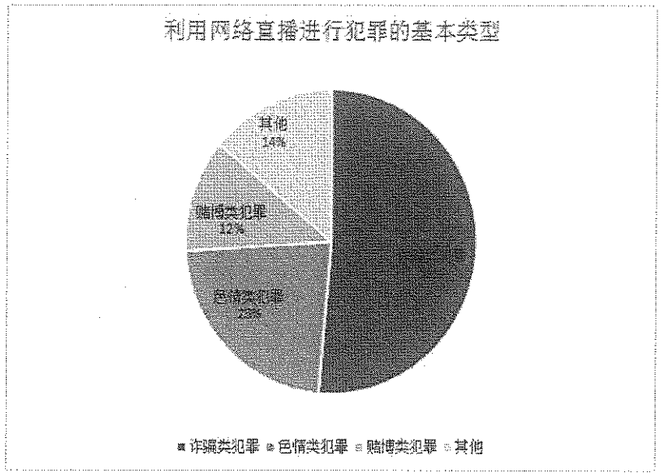
在被统计的 150 例利用网络直播进行犯罪的案件中，涉嫌诈骗类犯罪[②]的 77

作者简介：陈奕屹，武汉大学法学院博士研究生。

[1] 数据来源：《中国互联网络发展状况统计报告（2018 年 7 月）》

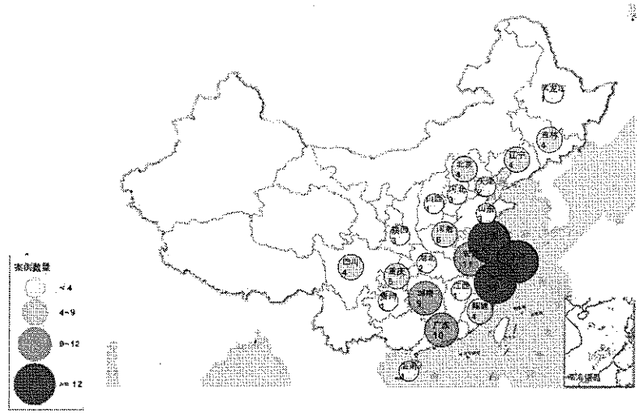
[2] 包括诈骗罪、集资诈骗罪等。

例（占总数 55%）；涉嫌色情类犯罪[③]的 34 例；涉嫌赌博类[④]犯罪的 18 例（图表一）。由此可见，与其他网络犯罪相似，诈骗类犯罪、色情类犯罪和赌博类犯罪也是利用网络直播进行犯罪的典型类型。



（图表一）

在被统计的 150 例案件中，浙江省、江苏省、上海市、广东省等经济发达、信息网络技术发展较为先进的地区为利用网络直播进行犯罪的高发地区，在某些北部、西北部欠发达地区暂无此类案件发生（图表二）。



（图表二）

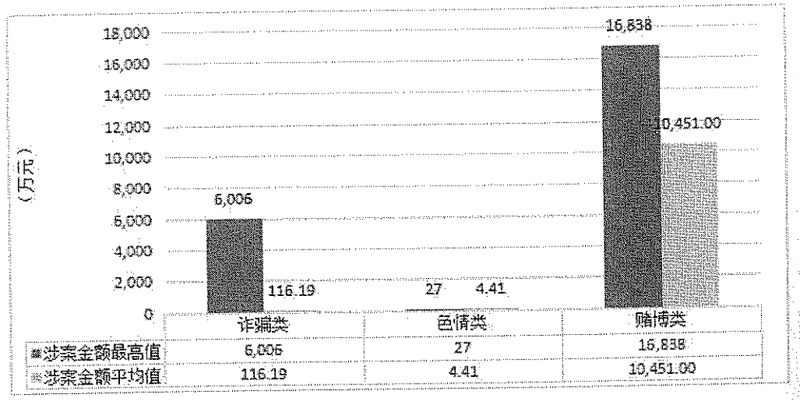
2. 各类犯罪的涉案金额与涉案人员

[3] 包括传播淫秽物品牟利罪、强奸罪等。

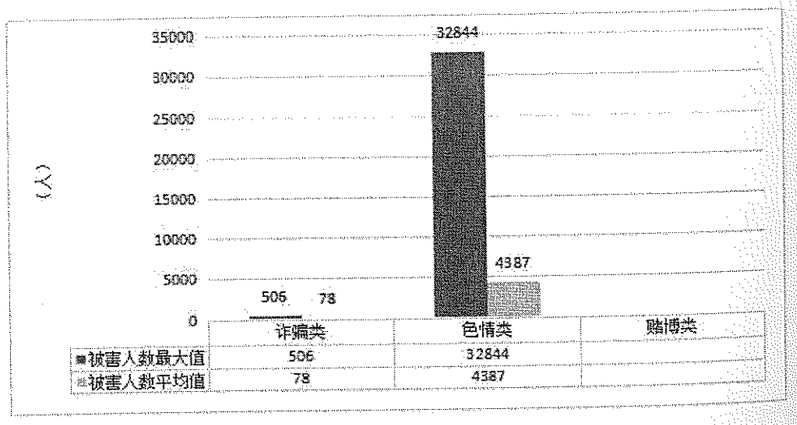
[4] 包括开设赌场罪、赌博罪等。

在利用网络直播进行诈骗类犯罪的 77 个案例中，涉案金额最高值为 6006,0000 元、平均值为 116,1947.75 元，被害人最大值为 506 人、平均值为 78 人；在利用网络直播进行色情类犯罪的 34 个案例中，涉案金额最高值为 27,1075 元、平均值为 4,4104.33 元，被害人（此处为观看色情直播的人员）最大值为 32844 人、平均值为 4387 人；在利用网络直播进行赌博类犯罪的 18 个案例中，涉案金额最高值为 16,8379,9262 元、平均值为 1,0450,9448.6 元，（因 18 例案例中没有任何一例判决书中提到参赌人员的具体人数，此处无法进行统计）。

由上述统计数据可知（图表三、四）：涉案金额方面，利用网络直播进行的赌博类犯罪涉案金额极高、诈骗类犯罪次之、色情类犯罪最少；被害人方面，利用网络直播进行的色情类犯罪被害人人数远高于诈骗类犯罪。



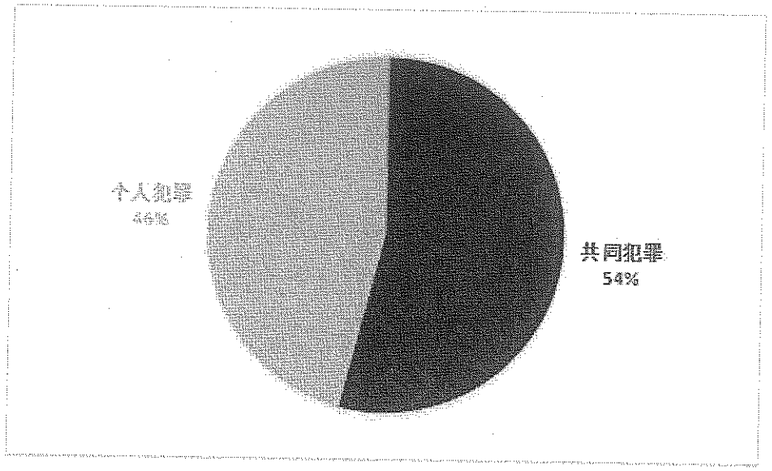
（图表三）



（图表四）

3. 犯罪行为人的基本情况

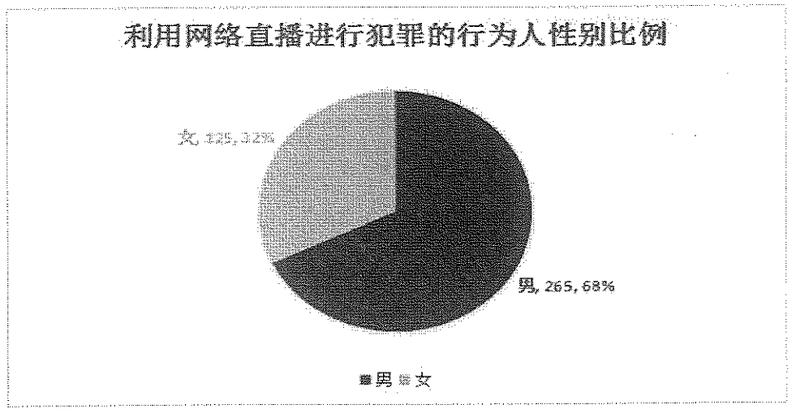
行为人方面，采用共同犯罪形式的行为人略多于个人犯罪（图表五），但从数量上没有显著差异。



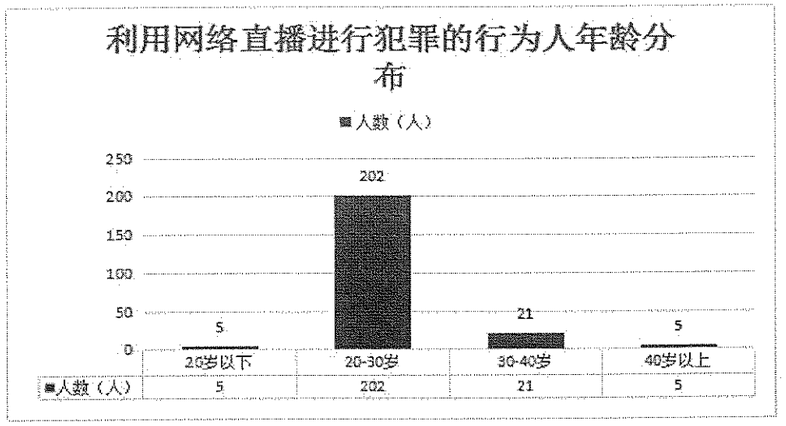
（图表五）

在被统计的的利用网络直播进行犯罪的 403 名行为人中，男性 265 人、女性 125 人[5]，虽然差异较为明显（图表六）但并不能说明性别与此类犯罪有直接、显著的联系。年龄方面（判决时年龄），20 岁以下的行为人有 5 人；20-30 岁的 202 人；30-40 岁的 21 人；40 岁以上的 5 人[6]，年龄分布较为集中（图表七），即此类案件的行为人年龄多在 30 岁以下，年龄较低。受教育程度方面，小学文化程度的行为人有 29 人；初中文化程度的 142 人；高中文化程度（包括中专）的 76 人；大学本科、专科文化程度的 85 人[7]，受教育程度的分布较为均衡（图表八），差异不明显从另一个侧面也可以说明利用网络直播进行的犯罪对行为人的文化程度没有过高的要求。

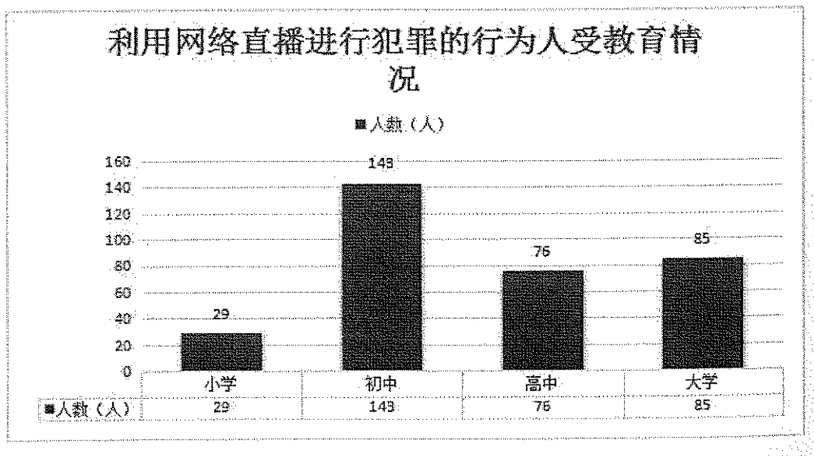
[5] 个别案例行为人性别未在判决书中明示。
[6] 个别案例行为人年龄未在判决书中明示。
[7] 个别案例行为人文化程度未在判决书中明示。



（图表六）



（图表七）



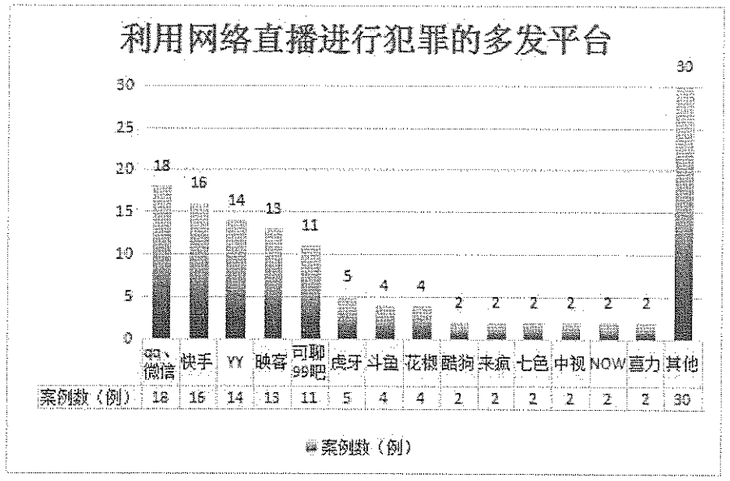
（图表八）

综上所述，利用网络直播进行的犯罪多发于浙江省、江苏省、上海市、广东省等经济发达、信息网络技术发展较为先进的地区，共同犯罪和个人犯罪的数量相近；行为人的年龄集中于 20-30 周岁，行为人的性别、文化程度差异并不明显。

（二）犯罪的多发平台及平台特征

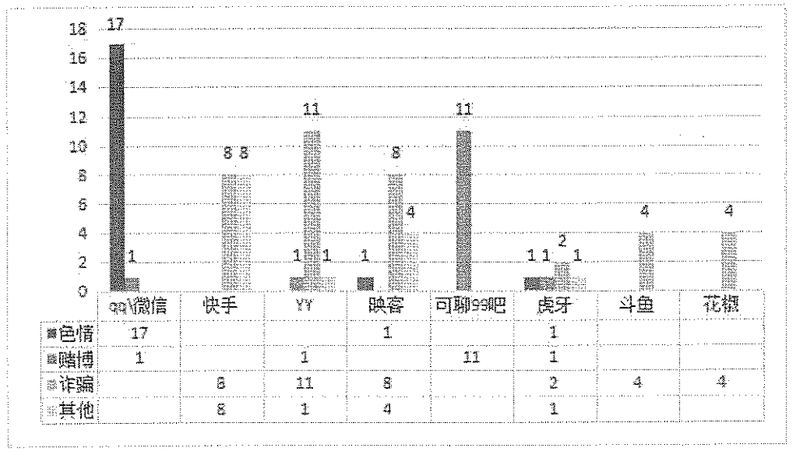
1. 犯罪的多发平台

在明确提到行为人所利用的平台的 127 例案件中，18 例利用了 qq、微信等社交软件附加的直播功能，利用快手平台的 16 例，利用 YY 平台的 14 例，利用映客平台的 13 例，利用可聊 99 吧的 11 例，利用虎牙平台的 5 例，利用斗鱼、花椒平台的各 4 例，利用酷狗、来疯、七色、中视、NOW、喜力平台的各 2 例，利用其他平台的共 30 例（图表七）。



（图表七）

其中，色情类案件多发于 qq、微信平台，赌博类案件多发于可聊 99 吧，诈骗类案件多发于快手、YY 及映客。（图表八）



（图表八）

各个平台案件类型的集中，说明不同类型平台的特征与高发案件类型有紧密的联系。例如，qq/微信平台是具有私密性以一对一社交功能为主要功能的社交类平台，具有较强的私密性，色情类直播在此类平台上不易被管理人员发现也因此盛行；快手、yy、映客是以直播为主要功能的合法、公共平台，由于其对主播的着装、行为有严格的要求并且实时监控不易发生色情类案件，但是，正因为此类平台的用户数量巨大、受众极广，诈骗类犯罪的行为人可以采用“广撒网”的方式获得大量受害人，获得巨额经济利益。

综上所述，将各直播平台进行分类研究，分析其特征和管理漏洞，对于减少犯罪数量有重要的意义。

1. 各类直播平台的特征和管理机制

根据平台搭建方式的不同，可以将上节中的平台分为三类：附加直播功能的社交平台（如：qq、微信等）；合规搭建、长期存续的直播平台（如：快手、YY、映客等）以及搭建不合规、存续时间短的直播平台（如蜜色、蜜桃、蜜汁等）。

（1）附加直播功能的社交平台[8]

顾名思义，附带直播功能的社交平台是指以社交功能为主要功能的网络平台同时拥有进行网络直播的功能，QQ 和微信即是此类社交平台的典型。

利用 QQ 和微信进行直播，也存在三种不同的方式：一对一直播、一对多直播和多对多直播。其中，一对一直播和一对多直播是利用社交平台的直播功能进

[8] 从广义上讲，直播平台自身具备社交功能，也是社交平台的一种。但是，由于直播平台和社交平台的侧重点不同，为了强调其与专业的社交平台的区别，此处笔者不认为其是社交平台的一种。

行犯罪的多发区域。

在 QQ 和微信进行一对一直播，是指一个行为人和一个被害人同时使用个人账号在一个私密的域内进行的具有排他性的直播，这类直播实际上利用的就是普通用户常用的远程视频功能。在一对一直播的过程中，被害人可以选择与行为人进行视频互动也可以选择不暴露自己的信息仅观看视频。一对多直播和一对一直播的模式相近，只不过一对多直播是一个行为人在“微信群”或“QQ 群”内对多个被害人进行直播，在私密性方面稍逊色于一对一直播。

无论是一对一直播还是一对多直播，利用社交平台的直播功能相较于利用专门的直播平台进行犯罪都拥有私密性的特征。

如前文所述，社交平台的直播功能实际上就是远程视频功能，这一功能本身就是一种用户用于特定群体间的、不公开的社交功能。因此，出于对用户隐私的保护，社交平台无法对所有的远程视频和直播进行监控，针对利用社交平台直播功能进行的犯罪只能依靠普通用户的举报才能发觉和处理。

针对在平台直播（远程视频）功能中可能发生的违法犯罪问题，腾讯公司在《腾讯服务协议》和《腾讯 110 服务协议中》分别对用户违规行为的内容及处理、用户的举报权限、腾讯针对违规内容的处理权限和警方介入时腾讯的配合义务等进行了规定。这些规定虽然详细，但仍存在以下问题：

第一，缺乏对直播（远程视频）功能的专门管理办法和规定；第二，过分依赖用户的举报，缺乏对自我管理、自我纠察的规定；第三，与警方的连接仅限于配合警方的调查、提供相关信息，缺乏对于违法犯罪问题的上报机制。

（2）合规搭建、长期存续的直播平台

合规搭建、长期存续的直播平台是指，平台搭建的目的和过程均符合法律法规并且长期稳定存在的，以网络直播为主要服务内容的网络平台，例如：快手、YY、映客、虎牙、花椒等平台。与附加直播功能的社交平台和搭建不合规、存续时间短的直播平台相比，这类平台的主要特征是：以网络直播为平台的主要功能，直播内容涵盖社会生活的各个领域，虽然可能存在一定的非法内容，但非法内容仅占所有直播内容的一小部分且平台自身对非法内容有一定的管理意识。

虽然与社交平台的直播（远程视频）功能相比，这类直播平台并不具有私密性，在管理过程中不存在为了保护隐私无法进行监控和管理的问题，但由于此类

平台直播范围广大、人数过多，在监管的过程中需要投入和消耗大量的人力和物力，给平台自身的运营成本带来了巨大的挑战。

通过对快手、YY、虎牙、映客、斗鱼、花椒等平台管理、服务条例的归纳和整理，笔者发现合规搭建、长期存续的直播平台对于直播中存在的违法问题的预防和处理主要是从以下几个方面进行展开的：

第一，对用户的注册进行实名制审查。在《YY 公约》、《虎牙用户服务协议》、《花椒用户注册协议》、《斗鱼用户注册协议》中，都明确规定了普通用户在该直播平台进行注册时需要提供其真实有效的身份信息进行实名制审查，快手和映客虽然在注册协议中没有关于实名制的严格规定，但在注册的过程中均需要将账户与手机号码进行绑定，实际上也对用户进行了实名制审查。

第二，对主播的行为和直播内容进行详尽的约束。在《快手直播规范》、《YY 主播违规管理办法》、《YY 主播违规管理办法补充条例》、《YY 娱乐主播违规管理办法》、《YY 未成年主播管理规定》、《金牌艺人直播行为管理规定》、《虎牙主播违规管理办法》、《斗鱼直播间违规管理办法》、《斗鱼用户阳光行为准则》、《花椒直播平台绿色文明直播公约》、《映客服务协议》等规定中，各平台均对主播的着装（如：男性不得赤裸上身、女性不得穿着过于暴露、不得露出纹身），主播的行为（如：严禁直播抽水烟、皮下注射等疑似吸食毒品的行为）以及直播的内容（如：用户不得使用直播功能发送或传播敏感信息和违反国家法律制度的信息）进行了明确、详细的禁止性规定，用以保障直播内容的合法、合规、合一般道德底线。

第三，对违规、违法内容及有违法、违规行为主播的处理办法。对于违规、违法内容的处理，各平台一般采取的做法都是删除有关内容，只有虎牙直播在其《主播违规管理办法》中提到了保留将违法内容移交司法机关的权力。针对有违法、违规行为的主播，各平台的处理方式也大致相同：均是根据违法、违规行为的严重程度对主播进行处罚金、暂时封号或永久封号的处理。

第四，普通用户举报机制。除了对于注册、主播行为、直播内容进行的规定外，各平台还针对直播的观众制定了投诉、举报的流程和具体实施细则。主要包括投诉和举报的基本流程以及平台对于投诉和举报的反应时间（如《YY 社区用户举报和投诉流程》规定的处理时限为三个工作日）等内

必须要肯定的是，与网络直播发展初期相比，目前合规搭建、长期存续的直播平台已经拥有了更加完善的管理体系，对预防利用网络直播进行的犯罪起到了不可忽视的积极作用。尽管如此，各平台与司法机关机关之间的连接仍然仅局限于“配合司法机关的调查”缺乏主动对违法、犯罪信息进行主动上报的意识。

（3）搭建不合规、存续时间短的直播平台

搭建不合规、存续时间短的直播平台是指，搭建目的、搭建程序涉嫌违法违规，同时存续时间较短的平台。这类平台搭建的目的本身并不是为了正常的合法经营而是为了给传播淫秽色情、赌博、诈骗信息的行为人提供桥梁。正因为其搭建目的、搭建程序的非法性，这类平台中的一部分在建成初期就会被网络监管部门发现并取缔，另一部分则为了防止被司法机关发现在上线后不久就会被开发者主动主动下线，导致其存续时间较短，不易统计。

由于此类平台自身的非法性，不能依靠平台自查对其直播内容进行管理和约束。因此，对搭建不合规、存续时间短的直播平台的只能在平台的搭建环节对其进行审查和管理，从根本上阻止其上线，从而达到预防利用其进行犯罪的目的。

目前，我国对于网络直播平台上线的管理机制主要包括：《互联网直播服务管理规定》、《网络表演经营活动管理办法》及《关于加强网络直播服务管理工作的通知》，其中《关于加强网络直播服务管理工作的通知》详细规定了网络直播服务提供者应依法向电信主管部门履行网站 ICP 备案手续，涉及经营电信业务及互联网新闻信息、网络表演、网络视听节目直播等业务的网络直播服务提供者应当分别向相关部门申请取得电信业务经营、互联网新闻信息服务、网络文化经营、信息网络传播视听节目等许可，并于直播服务上线 30 日内按照有关规定到属地公安机关履行公安备案手续。但是，由于管辖地不明确，监管不到位等多方面的原因，目前我国对于网络直播平台上线的管理仍然处在一个较不完善的阶段，使这类平台得以反复上线下线，逃避处罚。

三、利用网络直播犯罪猖獗的原因

（一）普通网民戒心不足

网络直播活动兴起于 2016 年底，各专门直播平台于 2017 年逐步上架、2018 年广泛应用、受众极速增长，对于普通网民来说仍是新兴事物。但是，正因为其尚属新兴事物，普通网民的好奇心过强并极易丧失应有的警惕性，导致利用网络

直播进行诈骗的犯罪活动屡屡得手、大量获益。

其次，普通网民对网络直播乃至互联网承载的信息拥有较强的猎奇心理，加之网络直播拥有的便捷性，直接导致导致了利用网络直播传播的色情信息拥有大量的受众，行为人也因此快速盈利。

最后，由于近年来消费主义的盛行，普通民众对于金钱的欲望提高，网络直播赌博应用而生。利用网络直播进行赌博活动给民众带来一个快速提高收益的市场，行为人也因此拥有了生存和盈利的空间

（二）直播平台管理不严

如前文所述，无论是拥有直播功能的社交平台，还是单纯的直播平台，都在与司法机关衔接的的环节存在缺乏主动性的问题。如果在平台主动发现或经用户举报发现犯罪行为时立即上报公安机，并提供 IP、身份信息等有关信息，行为人便会在极短时间内被公安机关发现并处理，从根本上打击犯罪行为。然而，目前各平台采取的措施均是封号、关停，除非受害人自己寻求公安机关的帮助，犯罪行为人便会逃脱法律的制裁，在另一平台继续进行犯罪行为。于此同时，除了诈骗类犯罪以外，色情类犯罪和赌博类犯罪实际上并没有明确的受害人，色情表演的观众、直播赌博的参与者大概率不会向公安机关举报行为人的犯罪的行为，此类犯罪便会逍遥法外甚至远愈烈。因此，直播平台仅仅通过关停、封号的方式处理行为人，并不能从根本上遏制犯罪。

（三）电商法与刑事司法介入不够

首先，2019 年 1 月 1 日《电商法》的实施，确实对各类网络平台起到了规制和震慑的作用，但其并没有囊括直播业务。换言之，立法机关虽然已经认识到了对网络平台进行系统规制的重要性，但是直播平台和其他平台的直播功能并没有真正的被纳入管辖，着显然是不合理的。

其次，刑事法律规范对于利用网络直播进行犯罪的介入不够。在刑事法律规范和司法实践中，解释者和实践者都仅仅把直播平台（包括拥有直播功能的社交平台）提供直播服务的行为当成了一个中立的帮助行为。但是，事实上除附带直播功能的社交平台外，其他各类直播平台对于平台上发生打赏行为都是从中抽成的，即直播平台会从主播的直播活动中直接获利，在这种情况下，如果主播的行为构成犯罪并有非法所得，直播平台在犯罪中起到的作用和地位是值得商榷的。

综上所述，《电商法》和刑事法律规范的介入不够，使这类犯罪缺失最后一道防线得以猖獗。

四、电商法颁布背景下针对利用网络直播进行犯罪的预防和治理

针对上一章中提到的三方面问题，可以从以下三个方面入手，对利用网络直播进行的犯罪进行预防、和规制，以达到减少犯罪数量、净化网络环境的目的。

（一）普通网民的警惕与预防

普通网民作为网络直播的受众，是预防利用网络直播进行犯罪的第一环也是最为重要的一环。提高普通网民的警惕性可以从政府的宣传和平台的提示两方面入手。例如，在进入直播间时平台可自动弹出对话框，提示网民谨慎对待主播输出的信息等。

（二）直播平台的自查与管理

直播平台的自查与自我管理，直接决定了公安机关对于直播平台内发生的违法犯罪问题的处理。

自查方面，直播平台务必须投入大量的人力与物力，对各个直播间进行自动和人工的监督和筛查，主动发现直播中有可能存在的违法犯罪问题，不能仅依靠用户举报获取违规信息。

管理方面，各平台应当承担起主动上报的义务。换言之，当发现平台内存在违法犯罪行为应当及时与当地公安机关联络并上报犯罪信息。对于违法犯罪问题应当主动协助公安机关进行规制，而非仅在平台内对其进行封号或罚款的处理。

（三）电商法与刑事司法的介入与规制

2019 年 1 月 1 日电商法已经生效并开始使用，这说明立法机关已经对各类网络平台产生足够的重视。网络直播平台，作为网络平台中的重要组成部分，理应拥有更为细化的规制方案。

笔者认为，对于网络直播平台的细化规制应当从两个方面入手：平台的准入机制和平台的法律责任及行政处罚。

首先，如前文所述，目前我国对于网络直播平台上线的控制主要依赖于《关于加强网络直播服务管理工作的通知》，但是这项规定内容繁琐、管辖不明，需对责任机构、上线标准进行进一步的规范和系统整理，才能更好的实习啊起运用价值。

其次，网络直播平台作为网络直播活动的重要载体，二者之间拥有密切的联系。因此，平台与主播之间不应仅有合作或者雇佣关系，平台自身还应负有管理的责任和义务。当其管理存在明显瑕疵时，应当承担一定的行政处罚。

在刑事司法方面，探究直播平台在犯罪中的地位同样有重要的意义。必须从刑法解释的层面明晰平台在行为人的犯罪中起何作用，根据其起到的作用不同，在犯罪中的地位不同，自然承担的责任也不尽相同。笔者认为，直播平台的地位可以分为一下几类：

第一，行为人虽利用直播平台进行犯罪，但犯罪行为与平台无关，平台不知情。这类情形，主要发生在利用网络直播进行的诈骗类犯罪中，因为平台无论如何进行监控也不能对主播言论的真伪进行鉴别，如无人举报，平台也无法知悉行为人的犯罪事实。在这种情况下，如果行为人利用平台进行诈骗，直播平台虽客观给行为人进行了变相的广告推广、促成了犯罪的发生或增加了犯罪的收益，但由于其主观并不知情，其行为不能构成犯罪。

第二，行为人利用直播平台进行犯罪，直播平台知情但并未制止或没有进行其他处理。这类情形可以分为两种情况：直播监控人员直接发现行为人的犯罪行为但未与制止或平台管理人员虽收到举报但未对主播及直播内容进行处理。直播平台的这种行为实际上是一种“通过在外形上看似中立的行为而从客观上促进正犯行为实施[①]”的行为。与此同时，平台已经认识到自己的正当业务行为与正在进行或发生的犯罪行为发生关联并清楚自己提供直播场所的行为对犯罪的意义依然选择放任[②]。这一行为正是一种可罚的中立帮助行为，应根据其具体行为及情形以犯罪处。。

第三，直播平台的设立以犯罪为目的。与其他两类相比，这类情形从鉴别和处理方面都更便捷。即，平台设立以犯罪为目的，事实上由促成、帮助了犯罪发生并从中获利，可直接以单位犯罪论处。

五、结语

网络直播及直播平台作为一个新兴实物近年来逐步进入人们的视野，其催生的各类犯罪及犯罪发生、猖獗的原因并非前文所能囊括。《电商法》的颁布实施，虽尚未将网络直播及平台纳入其管理范围，但已经宣告了国家对各类网络平台进

[9] 陈家林：《外国刑法通论》[M]，中国人民公安大学出版社 2009 年版，第 609 页。
[10] 马荣春：《中立帮助行为及其过当》[J]，《东方法学》2017 年第二期第 8 页。

行规制及治理的趋势。在对其进行管理的过程中，必须从行政管理和刑事规范两个层面入手，才能缓解利用其进行犯罪的行为、净化直播环境，使得网络直播业务可以平稳、有序的发展。

附　录：主题发言人讲稿

网络平台犯罪及其治理对策

皮　勇

在信息社会中，网络平台处于核心地位，信息社会活动高度依赖网络平台，网络平台是推动信息社会发展的核心力量，同时，网络平台相关犯罪随之迅速衍生，给信息社会的健康发展带来严峻挑战。从前面的相关犯罪学数据中，我们可以看到，多种网络平台相关犯罪与网络平台的运作模式紧密相关，有效治理网络平台犯罪，应以网络平台为抓手，落实网络平台的协助管理义务，强化国家管理机关的信息网络空间治权和用户个人信息的刑法保护，畅通网络平台与管理机关在违法犯罪数据上的联通，同打造有利于遏制网络平台犯罪的信息网络社会环境。

一、网络平台犯罪的基本类型

“网络平台是信息技术应用于商业社会之后的产物。新的信息技术的应用，新的商业模式的发明，新的应用领域的出现，都有可能造就与以往不同的新型网络平台。”网络平台在推动社会发展的同时，也存在自身的利益诉求，在新的网络社会生态中，产生来多种类型的网络平台相关犯罪。

（一）网络平台自身实施的犯罪

网络平台，作为提供网络空间服务的新型主体，自身实施犯罪同样严重，不仅可以实施网络化的传统犯罪，如曾经出现过的 QQ 平台中的以 Q 币为筹码的棋牌赌博，还可以实施新型的网络犯罪行为，如快播公司的共同传播淫秽信息。网络平台自身实施的犯罪有两种方式：一是由网络平台独自实施的犯罪，表现为作为犯形式的单独犯；二是由网络平台与其他犯罪主体共同实施的犯罪，或者由网络平台对他人的违法行为进行“升级”形成的犯罪行为，如快播视频网络平台对他人提供的违法内容信息进行深度编辑、整理，借助网络平台提供的网络空间广泛传播形成的犯罪。

（二）网络平台客观上起帮助作用的犯罪

具有网络技术和工具是网络犯罪的关键条件，除了国家以外，网络平台拥有最强的提供技术、程序等工具的能力，这种能力可能被网络平台使用者用于实施犯罪，网络平台客观上起了帮助作用。相比其他发挥帮助作用的犯罪主体，网络平台拥有技术、资金、用户群等不可比拟的优势，特别是借助计算机、网络技术应用的自动信息处理、低成本、高效便捷的特性，造就了“一人服务人人、人人服务于一人”的社会行为样态，使得网络平台环境下的犯罪具有了传统物态环境

下所不具有的作用广度和深度。网络平台的这种特殊帮助作用对其新犯罪能力的获得，无疑是关键的。一般而言，网络平台实施客观上起帮助作用的犯罪，涉及两类：一类是普通的帮助犯罪，即网络平台的帮助行为对犯罪实行者侵害法益仅起辅助性作用，实践中这种帮助行为易与正常的业务活动相混淆，网络平台的主观罪过乃是犯罪成立的关键要件；另一类则是起主要作用的帮助犯罪，网络空间中某些犯罪的帮助行为的社会危害性已经远远超过实行行为的危害性，如网络打码服务平台，这类犯罪性质上帮助行为性质，网络平台拥有强大的技术支持和帮助能力，是其他下游实行犯罪活动得以实施的关键，因此具有独立的社会危害性。

（三）不履行信息网络安全管理义务的犯罪

信息社会的良性治理离不开网络平台的协助，需要网络平台切实履行信息网络安全管理义务。网络平台，作为信息社会生态环境的主要创建者、网络活动规则的主要制定者，与包括违法犯罪在内的平台服务接受者呈现共生互利的关系，有责任履行信息网络安全管理义务。目前信息发达国家普遍对网络平台设立信息网络安全管理义务，我国包括《网络安全法》《反恐怖主义法》《关于加强网络信息保护的决定》《互联网信息服务管理办法》在内的法律规范也对网络平台规定了用户个人信息保护、违法犯罪监管以及协助执法等义务。在我国，网络平台不履行信息网络安全管理义务犯罪虽然没有司法判例，但客观上是不可能不存在的，如百度付费搜索竞价排名案、斗鱼直播平台乱象案等。

二、网络平台犯罪的治理模式及不足

网络平台犯罪需要进行有效治理，而当前的犯罪治理模式仍是传统的条块管理模式，以属地管理、管理物态对象和分行业管理为基础。首先，根据网络平台从事的行业确定具体的管理机关，特别是行政管理机关，如网络金融平台由央行、证监会、银保监会等金融部门监管，网络出行平台由交通部门监管，网络直播平台由文化部门监管等；然后，由具体负责管理的管理机关，以行政地域为界对网络平台相关违法犯罪进行管理或者执法。

在信息社会环境下，网络平台已不同于传统的管理对象，自身已形成封闭的生态系统，传统的条块管理模式不适应网络平台的运作方式，不利于社会管理机关掌握网络平台上的违法犯罪数据，实际上导致管理机关对信息网络空间治权的流失，而网络平台非法利用用户个人信息实施犯罪的可能性增大。

具体而言，网络平台利用信息网络技术的优势，累积了大量的用户和海量的用户个人信息、违法犯罪管理数据，将相互依赖的服务提供方和服务接受方聚集在一起，“网络平台的特点在于始终存在两方主体，一方提供各种不同的技术架构以提供信息服务；另一方在该架构内使用该种服务，”[①]但随着服务提供方技

① Volker Haug, Grundwissen Internetrecht, 3. Aufl., Stuttgart: Kohlhammer, 2016, S. 159.

术的不断进步，服务接受方群体的不断扩大，网络平台容易形成封闭的生态系统。在此情形下，以条块管理模式治理网络平台犯罪的不足越来越明显。

第一，国家的信息网络空间治权流失。在面对跨地域、全领域和信息态的网络平台经济活动时，条块管理模式遇到了低管理维度管不了高维度经营活动的困境。当前网络平台普遍处于封闭式运营和全领域扩张进程中，部分网络平台几乎成为信息网络空间中的封闭“藩国”，管理机关难以探知其经营活动，更不可能进行有效的监管，在我国社会全面信息化、网络化的发展趋势下，如果不提升国家对网络平台的管理维度，国家对信息网络空间的治权流失情况将更加严重。

第二，用户个人信息的法律保护不足，加剧了网络平台利用用户个人信息实施犯罪。网络平台自身实施的犯罪以及不履行信息网络安全管理义务犯罪，往往与利用用户个人信息有紧密关系。虽然《网络安全法》《关于加强网络信息保护的决定》《网络安全法》《消费者权益保护法》等法律规范对保护用户个人信息起积极作用，但刑法对用户个人信息的保护不足，《刑法》第 253 条之一规定的侵犯公民个人信息罪不能规制网络平台非法利用用户个人信息的行为，对于非法利用个人信息的行政处罚对网络平台而言只是增加了一些经营成本，根本起不到阻止违法犯罪的作用。

第三，网络平台与管理机关在违法犯罪管理数据联通不畅，不利于发现和防控网络平台中的违法犯罪。由于网络平台形成了封闭的生态系统，只有网络平台，才能第一时间掌握网络空间内他人实施网络活动的数据，实时发现违法犯罪活动并能采取有效控制措施。而网络平台与办案机关在违法犯罪管理数据上联通不畅，办案机关不能及时调取相关数据，调查网络平台上的不法行为，不能及时制止正在发生的犯罪，即使是案发后的调查取证都有一定的困难，如外地公安机关要调查淘宝网上销售假冒伪劣产品违法犯罪，去阿里巴巴公司调取涉案数据存在困难。没有强制性法律措施要求网络平台及时提供违法犯罪管理数据，在紧急事态下执法机关也无法强制网络平台实时提供司法协助，如滴滴出行平台网约车司机杀人案中出现的情形。网络平台不履行信息网络安全管理义务，导致违法犯罪发生不仅数量大，犯罪黑数也高。

三、网络平台犯罪的治理对策

治理网络平台犯罪，应以控制力理论为治理根据，从网络平台控制法益侵害事实的程度上落实网络平台的刑事责任，同时，强化管理机关的信息网络空间治权和用户个人信息的刑法保护，畅通网络平台与管理机关在违法犯罪管理数据上的联通，完善对网络平台犯罪的治理。

（一）消极的事后惩罚对策

对网络平台犯罪予以刑事处罚，是事后的对策，通过对网络平台犯罪活动的

消极评价，起到一般预防和公正惩罚的作用。控制力理论可以作为这一消极对策适用的理论依据。所谓控制力理论是侵权法学中的一种责任理论，是指包括网络平台在内的网络服务提供者承担侵权责任取决于对侵权事实的控制程度，借鉴到网络刑法中，可以根据网络平台对法益侵害事实的控制程度，来追究网络平台的刑事责任。

对于网络平台自身实施的犯罪，网络平台对法益侵害事实处于主导、支配地位，属于主导控制法益侵害事实的情形。此情形下网络平台完全基于自身意志实施犯罪，控制法益侵害事实的程度最强，应承担较重的刑事责任。

对于网络平台客观上其帮助作用的犯罪，网络平台不属于单独的犯罪主体，而是和其他主体共同参与控制法益侵害事实，其控制法益侵害事实的程度较前者弱，刑事责任程度较前者轻。但是，如果其起决定作用的，应以独立罪名追究刑事责任，只起辅助作用的，应按帮助犯处罚。

对于网络平台不履行信息网络安全管理义务的犯罪，网络平台负有管理义务、有管控能力，未采取有效改正措施有效履行义务，导致法益侵害事实发生的，依法对法益侵害事实负刑事责任。但是，如果履行义务超过其能力的，表明网络平台缺乏管控法益侵害事实的能力，阻却其刑事责任。

控制力理论不仅能反映网络平台不同犯罪行为控制法益侵害事实的程度，也能反映网络平台基于不同犯罪类型的刑事责任的有无及大小：

（1）有利于惩治网络平台犯罪。网络平台不仅是网络空间的提供者，更是网络空间的直接管理者，“网络服务提供者被视为连接上互联网的当然看门人，其毫无争议地处于过滤和制止互联网中非法和不良内容传播的最佳位置。”[①]网络平台“不再是纯粹的商业活动经营者。因而，在法律上都兼具网络服务提供者与网络安全管理者双重主体形象。”[②]以控制力理论作为网络平台承担刑事责任的根据，能及时反映网络平台对网络空间出现的不法行为的管控程度，确定应承担的刑事责任程度，实现罪责刑平衡。

（2）有利于预防网络平台犯罪。网络平台在网络空间不仅可以自身实施犯罪，他人也可以利用网络空间实施违法犯罪，依据控制力理论确定刑事责任，能提示网络平台管理好网络空间，将后者违法犯罪遏制在“萌芽状态”。正如有学者指出的那样，“为了预防损害的发生，应当由形成危险或风险的一方承担法律责任。因为这些人更加接近损害发生的源头，由他们来承担责任更有利于损害的预防。”[③]

---

① See Lilian Edwards and Charlotte Waelde, Online Intermediaries and Liability for Copyright Infringement. https://www.era.lib.ed.ac.uk/bitstream/handle/1842/2305/wipo-onlineintermediaries.pdf?sequence=1&isAllowed=y.

② 梁根林：《传统犯罪网络化：归责障碍、刑法应对与教义限缩》，载《法学》2017 年第 2 期，第 11 页。

③ 王利明：《侵权行为法研究》（上卷），中国人民大学出版社 2004 年版，第 251 页。

（3）有利于降低防控网络平台犯罪的管理成本。以网络平台为中心治理犯罪，不仅有利于规制网络平台自身的不法行为，也有利于降低管控其他各类相关违法犯罪的司法成本。

（二）积极的管控对策

除了依法追究网络平台犯罪的刑事责任，进行事后的一般预防，还应进行积极管控，打开网络平台构筑的封闭社会生态，实现对网络平台犯罪的有效治理。

一要强化管理机关的信息网络空间治权。关键是要提升对网络平台管理的维度，建议在国家网络与信息化办公室体系下成立实质性掌控社会管理各部门、各行各业数据的大数据局，打通信息社会空间中部门、行业之间的数据流通壁垒。通过大数据局管控好网络平台的数据，对于各地发生的网络平台相关违法犯罪活动，由当地管理机关依照法律程序向当地大数据局申请调取，各类数据分布式存储和集中调用。只有握住信息网络空间治权，才能更好地发挥管理机关治理犯罪的效能。

二要加强用户个人信息的刑法保护。用户个人信息是信息社会环境下的战略资产，对国家、社会和网络平台都具有关键价值，关于用户个人信息的利用和保护，应当平衡用户个人、网络平台和社会管理三方面的利益。应在确保用户个人的人身安全、重大财产安全等重要权益的基础上，在有利于社会信息化发展的前提下并经用户同意后，网络平台才能收集、提供和利用个人信息。对于网络平台违反国家有关规定非法利用、滥用用户个人信息开展业务的情形，除了从法律、行政法规方面完善用户个人信息保护规定外，网络平台违反国家有关规定利用用户个人信息情节严重的行为，应纳入《刑法》第 253 条之一侵犯公民个人信息罪的规制范围。

三要畅通网络平台与管理机关在违法犯罪管理数据上的联通。首先，要提高有关网络平台违法犯罪监管和协助执法等义务的规范效力层级。当前网络平台监管平台上的违法犯罪和协助执法的义务大多规定在部门规章和其他规范性文件中，有必要提升有关违法犯罪监管和协助执法等义务的规范效力层级。其次，要明确网络平台未履行违法犯罪监管和协助执法等义务的处置措施，规定强制性法律措施要求网络平台及时提供违法犯罪的涉案数据，在紧急事态下网络平台未实时向管理机关提供司法协助的，应及时依法处罚。

利用第三方支付平台犯罪及其治理

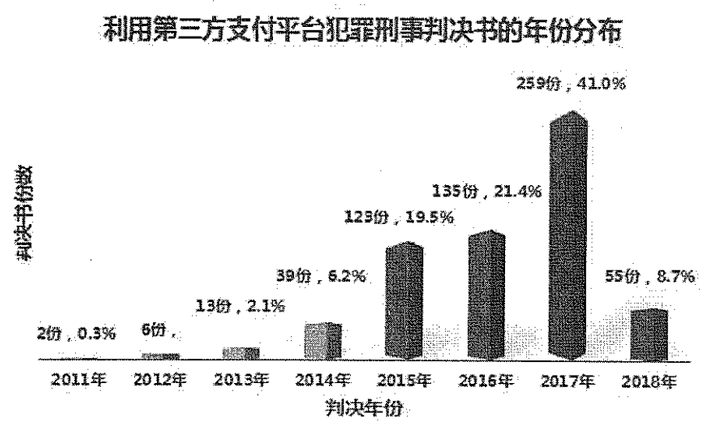
汪恭政

随着支付技术的进步和支付应用场景的丰富，利用第三方支付平台开展资金移转及其相关活动已十分普遍。然而，实践中行为人利用第三方支付平台实施各种犯罪的情形也经常出现，有必要以实际发生的犯罪案件为研究线索，厘清当前利用第三方支付平台犯罪的现状，为针对性治理提供准备。

一、利用第三方支付平台犯罪的现实状况

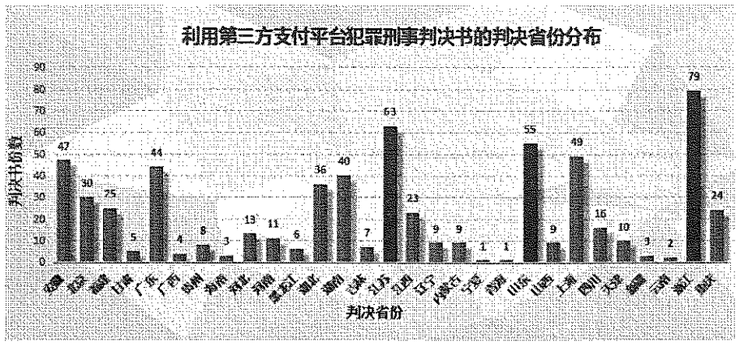
为了梳理第三方支付平台犯罪的现状，笔者在“OpenLaw”官网上，以“第三方支付平台”为关键词，共检索出 712 份刑事判决书。剔除重复的、并排除不是利用第三方支付平台犯罪的刑事判决书外，共得 632 份有效刑事判决书。分析有效判决书发现：

从判决年份上看，2011 年 2 件，占比 0.3%，2012 年 6 件，占比 0.9%，2013 年 13 件，占比 2.1%，2014 年 39 件，占比 6.2%，2015 年 123 件，占比 19.5%，2016 年 135 件，占比 21.4%，2017 年 259 件，占比 41.0%，2018 年 55 件，占比 8.7%。可见，随着网络支付应用的普及，利用第三方支付平台犯罪呈逐年递增的趋势。

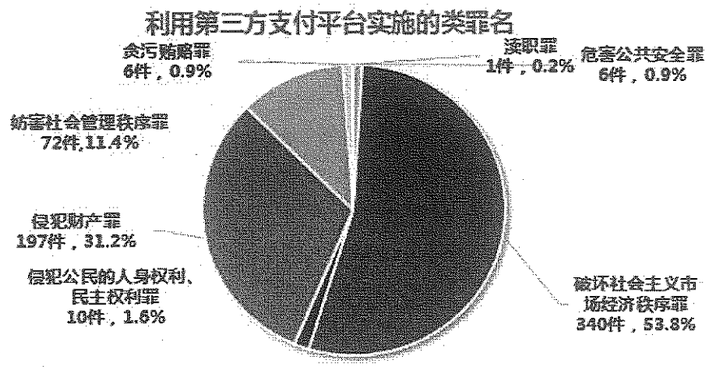


从判决省份上看，判决书数量从高到低依次为，浙江 79 件，占比 12.5%，

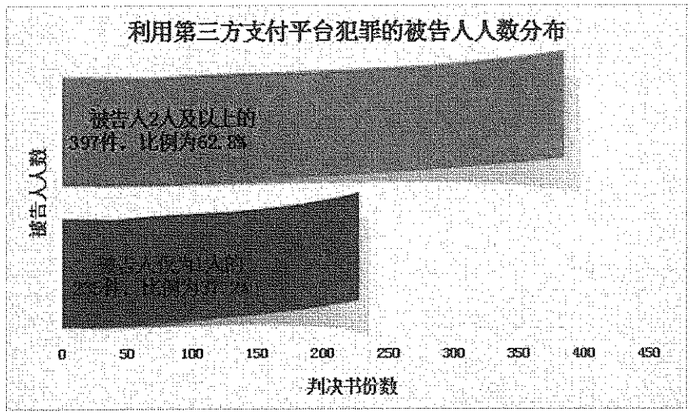
江苏 63 件，占比 10.0%，山东 55 件，比例为 8.7%，上海 49 件，占比 7.8%，安徽 47 件，比例为 7.4%，广东 44 件，占比 7.0%，湖南 40 件，占比 6.3%，湖北 36 件，占比 5.7%，北京 30 件，占比 4.7%，福建 25 件，占比 4.0%，重庆 24 件，占比 3.8%，江西 23 件，占比 3.6%，四川 16 件，占比 2.5%，河北 13 件，占比 2.1%，河南 11 件，占比 1.7%，天津 10 件，占比 1.6%，山西 9 件，占比 1.4%，辽宁 9 件，占比 1.4%，内蒙古 9 件，占比 1.4%，贵州 8 件，占比 1.3%，吉林 7 件，比例为 1.1%，黑龙江 6 件，占比 0.9%，甘肃 5 件，占比 0.8%，广西 4 件，占比 0.6%，海南 3 件，占比 0.5%，新疆 3 件，占比 0.5%，云南 2 件，占比 0.3%，宁夏和青海各 1 件，各占比 0.2%。由此，利用第三方支付平台犯罪主要集中在经济较为发达的地区，这与这些地区网络支付的广泛利用密不可分。



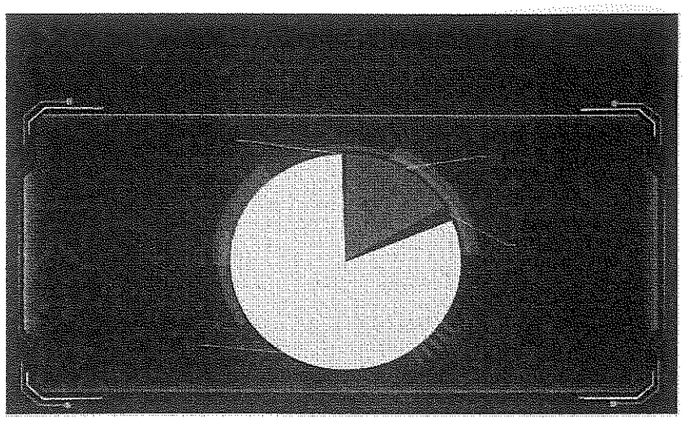
从利用第三方支付平台触犯的类罪名来看，利用第三方支付平台实施破坏社会主义市场经济秩序罪的案件数最多，多达 340 件，占比高达 53.8%，其次是侵犯财产罪，有 197 件，比例为 31.2%，再者是妨害社会管理秩序罪，涉案 72 件，占比 11.4%，而后依次是侵犯公民的人身权利、民主权利罪、危害公共安全罪、贪污贿赂罪和渎职罪，案件数分别为 10 件、6 件、6 件和 1 件，比例分别为 1.6%、0.9%、0.9%和 0.2%。可见，利用第三方支付平台侵犯秩序法益和侵犯财产法益的不法行为占据主体。



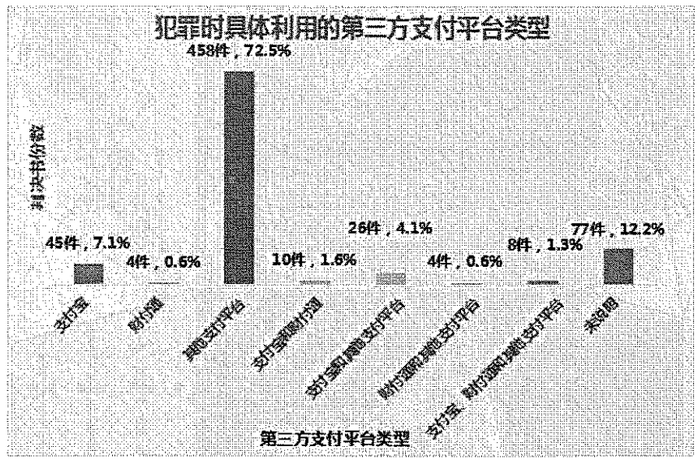
从被告人的人数分布上看，共同犯罪占据主体，共涉案 397 件，占比高达 62.8%，单独犯罪仅有 235 件，比例仅为 37.2%。这说明在利用第三方支付平台犯罪中，共同参与实行犯罪的情形较为普遍。



从利用第三方支付平台实施犯罪的类型来看，除 3 件未具体说明外。以第三方支付平台为犯罪工具占据绝大多数，案件数共有 511 件，比例高达 80.9%，其次是以第三方支付平台为犯罪主体，占比达 16.6%，案件最少的是以第三方支付平台为犯罪对象，仅有 13 件，占比仅为 2.1%。由此可知，第三方支付平台方便资金移转的同时，也为行为人犯罪提供了便捷的工具。



从利用第三方支付平台的具体类型来看，利用除支付宝、财付通（即微信）以外的第三方支付平台占绝大多数，涉案共有 458 件，比例高达 72.5%。利用支付宝这一支付平台犯罪的有 45 件，占比 7.1%，单独利用财付通支付平台犯罪的仅有 4 件，占比 0.6%。除了 77 件判决书对所利用的第三方支付平台类型未作具体说明的外，都是混合利用支付宝、财付通以及其他支付平台实施犯罪。其中，同时利用支付宝和其他支付平台的较多，涉案 26 件，占比 4.1%。据统计，从第三方支付平台的利用人数上看，支付宝和微信的利用人数分列前两位，然而实践中，行为人多是利用其它支付平台犯罪。



从利用第三方支付平台实施的具体犯罪来看，侵犯秩序法益的犯罪占据主体。其中，发案最多的是非法吸收公众存款罪，共有 158 件，比例高达 25.0%，其次是开设赌场罪，涉案 53 件，占比 8.4%，而后是信用卡诈骗罪，比例为 7.8%。

除了侵犯秩序法益的犯罪外，利用第三方支付平台实施的犯罪是侵犯财产法益的犯罪，其中，诈骗罪发案数最多，有 137 件，占比高达 21.7%，紧随其后的是盗窃罪，涉案 54 件，占比 8.5%。从如下表中分析得知，无论是实施侵犯秩序法益的犯罪，还是实施侵犯财产法益的犯罪，都是利用了第三方支付平台移转资金的便捷性、隐蔽性，转移非法资金或侵犯他人财产。

利用第三方支付平台实施的具体犯罪分布			
类罪名	具体罪名	案件数	百分比
危害公共安全罪	非法制造、买卖、运输、邮寄、储存枪支、弹药、爆炸物罪	5	0.8%
	破坏广播电视设施、公用电信设施罪	1	0.2%
破坏社会主义市场经济秩序罪	销售假药罪	1	0.2%
	走私普通货物罪	1	0.2%
	骗取贷款、票据承兑、金融票证罪	2	0.3%
	非法吸收公众存款罪	158	25.0%
	妨害信用卡管理罪	3	0.5%
	窃取、收买、非法提供信用卡信息罪	3	0.5%
	集资诈骗罪	26	4.1%
	信用卡诈骗罪	49	7.8%
	销售假冒注册商标的商品罪	4	0.6%
	侵犯著作权罪	12	1.9%
	销售侵权复制品罪	1	0.2%
	合同诈骗罪	4	0.6%
	组织、领导传销活动罪	35	5.5%
	非法经营罪	41	6.5%
侵犯公民人身权利、民主权利罪	侵犯公民个人信息罪	10	1.6%
侵犯财产罪	盗窃罪	54	8.5%
	诈骗罪	137	21.7%
	职务侵占罪	2	0.3%
	挪用资金罪	3	0.5%
	敲诈勒索罪	1	0.2%
妨害社会管理秩序罪	非法获取计算机信息系统数据、非法控制计算机信息系统罪	2	0.3%
	提供侵入、非法控制计算机信息系统程序、工具罪	2	0.3%
	赌博罪	3	0.5%
	开设赌场罪	53	8.4%
	掩饰、隐瞒犯罪所得、犯罪所得收益罪	10	1.6%
	贩卖毒品罪	2	0.3%
贪污贿赂罪	贪污罪	1	0.2%
	挪用公款罪	5	0.8%
渎职罪	滥用职权罪	1	0.2%

二、利用第三方支付平台犯罪的成因分析

利用第三方支付平台犯罪之所以频繁发生，与监管机关管控第三方支付平台的力度有限、第三方支付平台自身管控犯罪能力的不足以及与用户个人信息的保护力度不够密切相关。

（一）监管机关管控第三方支付平台的力度有限

无论是支付宝，还是财付通，抑或其他支付平台，实践中大量存在利用这些平台犯罪的情形，常与监管机关管控第三方支付平台的力度有限，具体表现在两方面：一是有关第三方支付平台的性质定位不明。在国内，有关第三方支付平台性质的规范定位，先后经历了《支付清算组织管理办法》的支付清算组织、《非金融机构支付服务管理办法》的支付机构，到《非银行支付机构网络支付业务管理办法》的非银行机构，再到《非银行支付机构风险专项整治工作实施方案》的非银行支付机构，以及《电子商务法》的电子支付服务提供者的诸多变化，但第三方支付平台在性质到底归属于哪里机构，仍未明确。定位不明，不利于国家，尤其是监管机关，从技术要求、规范履行上完善对第三方支付平台的管控。二是监管机关事前、事中监管第三方支付平台的力度不够。如前文所述，行为人利用其它支付平台犯罪高达 72.5%，占据案件数的主体。作为市场占有率遥遥领先的支付宝、财付通（微信），平台运营相对规范，因而发案率不高。然而，对于其他支付平台，由于市场占有率小，为抢占市场，很多在并获支付业务许可证或在运营不规范的情况下，便“铤而走险”实施犯罪为他人犯罪提供方便，而这与监管机关对第三方支付平台的市场准入把关不严或对已进入市场的平台未能强化事中监管有密切关系。

（二）第三方支付平台自身管控犯罪的能力不足

司法实践中之所以大量存在他人以第三方支付平台为犯罪工具实施犯罪，这与第三方支付平台自身管控犯罪的能力不足紧密相关，特别是表现在相关法律规定不完善。虽然我国法律规范规定了第三方支付平台负有违法犯罪活动的监管义务和协助执法机关执法的义务。例如，《非金融机构支付服务管理办法》规定，“支付机构明知或应知客户利用其支付业务实施违法犯罪活动的，应当停止为其办理支付业务”。[①]《非银行支付机构网络支付业务管理办法》要求支付机构“建

① 参见《非金融机构支付服务管理办法》第 31 条第 2 款。

立交易风险管理制度和交易监测系统，对疑似欺诈、套现、洗钱、非法融资、恐怖融资等交易，及时采取调查核实、延迟结算、终止服务等措施”。[①]《关于促进互联网金融健康发展的指导意见》旨在要求第三方支付平台在内的从业机构应坚持反洗钱和防范金融犯罪。[②]《非金融机构支付服务管理办法》指出，支付机构应配合央行及其分支机构定期或不定期的现场和非现场检查，如实提供有关资料，不得逃避检查。[③]《非金融机构支付服务管理办法实施细则》规定，司法部门调查可疑交易或违法犯罪活动涉及客户身份信息和支付业务信息时，支付机构应做好客户身份和支付业务信息的保存工作，以备司法部门查验。[④]《非银行支付机构网络支付业务管理办法》明确指出，支付机构发生重大风险事件的，应及时向机构所在地央行分支机构报告，发现涉嫌违法犯罪的，同时报告公安机关。[⑤]但是，上述有关管理义务的规定更多地源自部门规章和其他规范性文件，针对性的法律、行政法规缺乏，管理义务法律依据的效力层级普遍较低。

（三）用户个人信息缺乏有效的保护

随着支付技术的不断进步和国民支付需求的日益增加，第三方支付平台上累积了大量的用户个人信息。无论是利用第三方支付平台实施侵犯秩序法益的犯罪，还是实施侵犯财产法益的犯罪，行为人之所以成功，往往与行为人不当利用被害用户个人信息存在关系，由于现有规范保护用户个人信息的力度不足，加剧了行为人非法利用用户个人信息实施侵犯秩序法益犯罪、侵犯财产法益犯罪的可能性。虽然我国多部法律规范均涉及到对用户个人信息的保护，如《民法总则》从禁止侵害的角度保护用户个人信息，《网络安全法》对用户个人信息的收集和保管进行规制，但对用户个人信息的保护作用有限。迄今为止，专门保护用户个人信息的法律迟迟未出台。特别是从刑事规范角度分析，用户个人信息的保护力度明显不够。以《刑法》第 253 条之一为例，虽然该条规定了侵犯公民个人信息罪，将向他人出售、提供、窃取或者以其他方法非法获取用户信息的行为纳入此罪评价范围，但对于在第三方支付平台上非法利用用户个人信息的不法行为却缺乏及时的规制。

① 参见《非银行支付机构网络支付业务管理办法》第 17 条第 2 款。
② 参见《关于促进互联网金融健康发展的指导意见》第 18 点。
③ 参见《非金融机构支付服务管理办法》第 35 条。
④ 参见《非金融机构支付服务管理办法实施细则》第 39 条第 2 款。
⑤ 参见《非银行支付机构网络支付业务管理办法》第 31 条第 2 款。

三、利用第三方支付平台犯罪的治理建议

第三方支付平台，作为网络平台之一，治理利用第三方支付平台犯罪，应在增强监管机关对第三方支付平台的实际管控上，提高第三方支付平台自身管控犯罪的能力，并加大对用户个人信息的保护力度。

（一）增强监管机关对第三方支付平台的实际管控

增强监管机关对第三方支付平台的实际管控。建议从两方面着手：一是明确第三方支付平台的性质定位。在国内，规范上并未明确第三方支付平台是否属于金融机构的性质定位，而是将其定位为非银行机构、非银行支付机构或电子支付服务提供者。然而，事实上我国第三方支付平台不仅在发挥信用中介职能，也在逐步履行信用创造职能。为了进一步强化第三方支付平台对平台上资金和信息的监督和管控，有必要将其定位为金融机构，纳入金融机构的管理范畴。二是加强监管机关对第三方支付平台涉及违法犯罪活动的审查力度，对于未获支付业务许可证擅自从事支付业务的支付平台要依法取缔，对于已获支付业务许可证的支付平台参与违法活动或为这些活动提供方便的，应强化事中监管，构成犯罪的，及时移交司法机关。

（二）提高第三方支付平台自身管控犯罪的能力

提高第三方支付平台管控犯罪的治理能力，关键应在法律规范上作出完善。一是，提升调整第三方支付平台及其活动的基础规范的效力层级。建议将《非金融机构支付服务管理办法》升格为法律或行政法规，如由国务院出台制定《支付机构支付服务管理条例》。二是，进一步完善第三方支付平台管控违法犯罪活动、协助执法机关执法的管理义务。具体而言，管控违法犯罪活动方面，可从规范第三方支付平台上注册用户的资格审查、监管平台可疑资金流向等方面作出完善；协助执法机关执法方面，应完善第三方支付平台交易记录的保存机制，方便第三方支付平台向执法机关提供涉案证据。

（三）加大对用户个人信息的保护力度

第三方支付平台为资金移转提供了网络空间，资金的移转离不开用户个人信息，但用户个人信息利用的不当，易危及用户的财产安全。因此，在鼓励支付创新的同时，也应确保支付安全，特别是加大对用户个人信息的保护。建议出台专门保护用户个人信息的法律，如制定《个人信息保护法》，具体应在遵循合法、

正当、必要三原则的基础上，做到经用户同意后方可收集、提供和利用个人信息。对于实践中，行为人利用第三方支付平台违反国家有关规定利用用户个人信息的危害情形，除了从法律、行政法规方面完善用户个人信息保护规定外，应将针违反国家有关规定利用用户个人信息，达到情节严重的行为，直接纳入《刑法》第253条之一侵犯公民个人信息罪的治理范围。

利用网络直播平台进行犯罪的现状及成因分析

陈奕屹

尊敬的各位专家学者、各位老师、同学们：

下午好！

我是来自武汉大学法学院的博士研究生陈奕屹，非常荣幸能在这里向各位老师汇报我们的研究成果。今天我的报告主题是：《利用网络直播平台进行犯罪的现状及成因分析》。

根据国家互联网信息办公室 2016 年 11 月 4 日颁布的《互联网直播服务管理规定》，网络直播是指基于互联网，以视频、音频、图文等形式向公众持续发布实时信息的活动，网络直播服务提供者也就是直播平台，是指提供互联网直播平台服务的主体。

截至 2018 年 6 月，我国网络直播用户规模达到 4.25 亿，占我国总人口的 30%，用户使用率为 53.0%。网络直播平台的迅猛发展和监管不够严格共同催生了利用网络直播进行犯罪的行为，给普通网民带来了严重危害。基于此，我和我的同学们对裁判文书网上已经公布的全部 150 例，利用网络直播平台进行的犯罪进行了犯罪学的统计和分析，并希望可以通过这种方式对如何治理此类犯罪提出适当的建议。

我的报告主要分为利用网络直播进行犯罪的基本类型及现状和利用网络直播进行犯罪的多发平台及平台特征两个部分，分别从犯罪本身和依托的平台入手对其进行仔细的分析和研究。

首先，第一部分利用网络直播进行犯罪的基本类型及现状，这部分内容包括了犯罪的基本类型、多发地区、涉案金和和一些关于犯罪行为人的统计数据。

在被统计的 150 例利用网络直播进行犯罪的案件中，涉嫌诈骗类犯罪的 77 例；涉嫌色情类犯罪的 34 例；涉嫌赌博类犯罪的 18 例。由此可见，与其他网络犯罪相似，诈骗类犯罪、色情类犯罪和赌博类犯罪也是利用网络直播进行犯罪的典型类型。

地域方面，从 ppt 中我们可以看到，浙江省、江苏省、上海市、广东省等经济发达、信息网络技术发展较为先进的地区为利用网络直播进行犯罪的高发地

区，在某些北部、西北部欠发达地区暂无此类案件发生

涉案金额方面，在利用网络直播进行诈骗类犯罪的 77 个案例中，涉案金额最高值为六千零六万元、平均值为一百一十六万元，在利用网络直播进行色情类犯罪的 34 个案例中，涉案金额最高值为二十七万元、平均值为四万元，在利用网络直播进行赌博类犯罪的 18 个案例中，涉案金额最高值高达十六亿、就连平均值也有一亿零四百五十万元。

于此同时，在上述利用网络直播进行诈骗类犯罪的案例中被害人最大值为 506 人、平均值为 78 人；色情类犯罪的被害人（此处为观看色情直播的人员）最大值为 32844 人、平均值为 4387 人；因 18 例赌博类犯罪的案例中没有任何一例判决书中提到参赌人员的具体人数，此处无法进行统计。

由上述统计数据可知：涉案金额方面，利用网络直播进行的赌博类犯罪涉案金额极高、诈骗类犯罪次之、色情类犯罪最少；被害人数方面，利用网络直播进行的色情类犯罪被害人人数远高于诈骗类犯罪，接下来，我们研究了有关犯罪行为人的各项信息。

首先，利用网络直播进行的犯罪里，采用共同犯罪形式的行为人略多于个人犯罪 ，但在数量上没有显著差异

其次，在被统计的、403 名行为人中，男性 265 人、女性 125 人，虽然差异较为明显，但并不能说明性别与此类犯罪有直接、显著的联系。

再次，在年龄方面，判决时 20 岁以下的行为人有 5 人；20-30 岁的 202 人；30-40 岁的 21 人；40 岁以上的 5 人，年龄分布较为集中，也就是说，此类案件的行为人年龄多在 30 岁以下，年龄较低。

最后，受教育程度方面，小学文化程度的行为人有 29 人；初中文化程度的 142 人；高中文化程度（包括中专）的 76 人；大学本科、专科文化程度的 85 人，受教育程度的分布较为均衡，差异不明显，从另一个侧面也可以说明利用网络直播进行的犯罪对行为人的文化程度没有过高的要求。

综上所述，利用网络直播进行的犯罪多发于浙江省、江苏省、上海市、广东省等经济发达、信息网络技术发展较为先进的地区，共同犯罪和个人犯罪的数量相近；行为人的年龄集中于 20-30 周岁，行为人的性别、文化程度差异并不明显。

在对犯罪的基本情况有了基本的统计分析后，我们继续对利用网络直播进行

犯罪的多发平台进行了分析和研究，这部分的内容主要包括犯罪的多发平台、多发原因及各平台的特征与管理机制。

首先，在明确提到行为人所利用的平台的 127 例案件中，18 例利用了 qq、微信等社交软件附加的直播功能，利用快手平台的 16 例，利用 YY 平台的 14 例，利用映客平台的 13 例，利用可聊 99 吧的 11 例，利用虎牙平台的 5 例，利用斗鱼、花椒平台的各 4 例，利用酷狗、来疯、七色、中视、NOW、喜力平台的各 2 例，利用其他平台的共 30 例。

其中，色情类案件多发于 qq、微信平台，赌博类案件多发于可聊 99 吧，诈骗类案件多发于快手、YY 及映客。

各个平台案件类型的集中，说明不同类型平台的特征与高发案件类型有紧密的联系。例如，qq/微信平台是具有私密性以一对一社交功能为主要功能的社交类平台，具有较强的私密性，色情类直播在此类平台上不易被管理人员发现也因此盛行；快手、yy、映客是以直播为主要功能的合法、公共平台，由于其对主播的着装、行为有严格的要求并且实时监控不易发生色情类案件，但是，正因为此类平台的用户数量巨大、受众极广，诈骗类犯罪的行为人可以采用“广撒网”的方式获得大量受害人，获得巨额经济利益。

综上所述，将各直播平台进行分类研究，分析其特征和管理漏洞，对于减少犯罪数量有重要的意义。

基于此，我们将上面提到的平台分成了三类：附加直播功能的社交平台（如：qq、微信等）；合规搭建、长期存续的直播平台（如：快手、YnY、映客等）以及搭建不合规、存续时间短的直播平台（如蜜色、蜜桃、蜜汁等）。

第一类，附带直播功能的社交平台。这类平台是指以社交功能为主要功能的网络平台同时拥有进行网络直播的功能，QQ 和微信即是此类社交平台的典型。利用 QQ 和微信进行直播，也存在两种不同的方式：一对一直播和一对多直播。

在 QQ 和微信进行一对一直播，是指一个行为人和一个被害人同时使用个人账号在一个私密的域内进行的具有排他性的直播，这类直播实际上利用的就是普通用户常用的远程视频功能。一对多直播和一对一直播的模式相近，只不过一对多直播是一个行为人在“微信群”或“QQ 群”内对多个被害人进行直播。其实，根据之前说过的直播和直播平台的定义，我们对于这两类远程视频的活动能不能

算做直播也有疑问，但是由于裁判文书均将此类行为算做直播，所以放在这里一并讨论。

言归正传，无论是一对一直播还是一对多直播，利用社交平台的直播功能相较于利用专门的直播平台进行犯罪都拥有私密性的特征。正因为此，平台本身无法对所有的远程视频和直播进行监控，针对利用社交平台直播功能进行的犯罪只能依靠普通用户的举报才能发觉和处理。

因此，针对在平台直播功能中可能发生的违法犯罪问题，腾讯公司在《腾讯服务协议》和《腾讯 110 服务协议中》分别对用户违规行为的内容及处理、用户的举报权限、腾讯针对违规内容的处理权限和警方介入时腾讯的配合义务等进行了规定。

第二类直播平台是合规搭建、长期存续的直播平台。这类平台搭建是指搭建目的和过程均符合法律法规并且长期稳定存在的，以网络直播为主要服务内容的网络平台，例如：快手、YY、映客、虎牙、花椒等平台。与其他平台相比，这类平台的主要特征是：以网络直播为平台的主要功能，直播内容涵盖社会生活的各个领域，虽然可能存在一定的非法内容，但非法内容仅占所有直播内容的一小部分且平台自身对非法内容有一定的自我管理意识。

这类平台的自我管理主要体现在四个方面；第一，对用户的注册进行实名制审查。各平台的注册协议中，都明确规定了普通用户在该直播平台进行注册时需要提供其真实有效的身份信息进行实名制审查，快手和映客虽然在注册协议中没有关于实名制的严格规定，但在注册的过程中均需要将账户与手机号码进行绑定，实际上也对用户进行了实名制审查。

第二，对主播的行为和直播内容进行详尽的约束。各平台均对主播的着装、行为以及直播的内容进行了明确、详细的禁止性规定，用以保障直播内容的合法、合规、合一般道德底线。

第三，对违规、违法内容及有违法、违规行为主播的处理办法。对于违规、违法内容的处理，各平台一般采取的做法都是删除有关内容，针对有违法、违规行为的主播，各平台的处理方式也大致相同：均是处罚金、暂时封号或永久封号的处理。

第四，普通用户举报机制。除了对于注册、主播行为、直播内容进行的规定

外，各平台还针对直播的观众制定了投诉、举报的流程和具体实施细则。主要包括投诉和举报的基本流程以及平台对于投诉和举报的反应时间等。

第三类平台，是搭建不合规、存续时间短的直播平台。这类平台搭建的目的本身并不是为了正常的合法经营而是为了给传播淫秽色情、赌博、诈骗信息的行为人提供桥梁。正因为其搭建目的、搭建程序的非法性，这类平台中的一部分在建成初期就会被网络监管部门发现并取缔，另一部分则为了防止被司法机关发现在上线后不久就会被开发者主动主动下线，导致其存续时间较短，不易统计。

由于此类平台自身的非法性，不能依靠平台自查对其直播内容进行管理和约束。因此，对搭建不合规、存续时间短的直播平台的只能在平台的搭建环节对其进行审查和管理，从根本上阻止其上线，从而达到预防利用其进行犯罪的目的。

目前，我国对于网络直播平台上线的管理机制主要包括：《互联网直播服务管理规定》、《网络表演经营活动管理办法》及《关于加强网络直播服务管理工作的通知》，其中《关于加强网络直播服务管理工作的通知》详细规定了网络直播服务提供者应依法向电信主管部门履行网站 ICP 备案手续，涉及经营电信业务及互联网新闻信息、网络表演、网络视听节目直播等业务的网络直播服务提供者应当分别向相关部门申请取得电信业务经营、互联网新闻信息服务、网络文化经营、信息网络传播视听节目等许可，并于直播服务上线 30 日内按照有关规定到属地公安机关履行公安备案手续。但是，由于管辖地不明确，监管不到位等多方面的原因，目前我国对于网络直播平台上线的管理仍然处在一个较不完善的阶段，使这类平台得以反复上线下线，逃避处罚。

结合上面的数据研究和统计，我和我的同学们认为，利用网络直播进行犯罪的成因主要可以从三方面进行考虑：普通网民的警惕性不足、平台自身管理不完善、法律规范相对滞后，遏制此类犯罪也应该从这三方面入手。在我的会议论文中也针对治理和预防的建议提出了自己的观点和设想，此处就不赘述了。毕竟与我粗浅的观点相比，更期待各位老师的批评和指正。

我的报告到这里就全部结束了，感谢大家的聆听。

利用网约车服务平台犯罪基本情况及现状

吴 勃

（武汉大学 法学院，湖北 武汉 430072）

2018 年中国司法大数据研究院发布了《网络约车与传统出租车服务过程中犯罪情况司法大数据专题报告》，对比传统出租车司机和网约车司机犯罪案件数据，结论是：2017 年全国各级法院审理的被告人为网约车司机且在提供服务过程中实施犯罪的案件量不足 20 件，网约车司机每万人案发率为 4.8%；而审理的被告人为传统出租车司机且在提供服务过程中实施犯罪的案件量为 170 余件，传统出租车司机每万人案发率为 6.27%。传统出租车司机实施的犯罪案件数比网约车司机实施的近高出 8.5 倍。[①]但在 2018 年中国犯罪学学会年会上曾发布 2018 年典型案例，对 2017 年 9 月 1 日至 2018 年 8 月 31 日期间滴滴司机作为犯罪人的案件进行统计、分析，发现结论与中国司法大数据研究院发布的结论差异巨大。2018 年 9 月，交通部进驻滴滴的检查组报告了滴滴存在的 9 大问题，排在第一位的即是公共安全隐患巨大。因此，作为关乎公众出行安全的网约车平台治理值得研究，涉嫌行业垄断的滴滴更值得关注。于是报告人团队在 2018 典型案例发布基础上继续深入开展以下研究。

2018 年 12 月 31 日，报告人团队以“滴滴”为关键词，以“刑事案件”“判决书”为限定条件，在裁判文书网上共下载判决书 2589 份，经筛选，滴滴司机作为犯罪人的案件共 248 件，滴滴司机作为被害人的共 299 件，合计 547 件。

一、滴滴司机犯罪案件数据

滴滴司机作为犯罪人的案件共 248 件

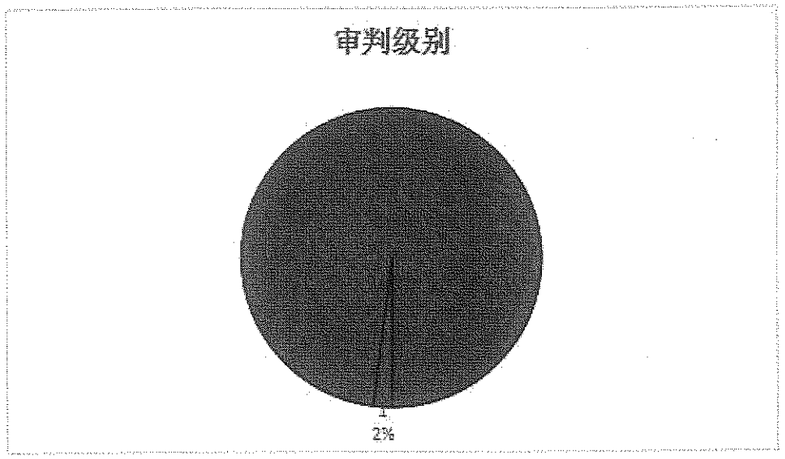
（一）案件特征

该部分主要涉及判决书审判级别、案发省份和案发年份。

1. 审判级别

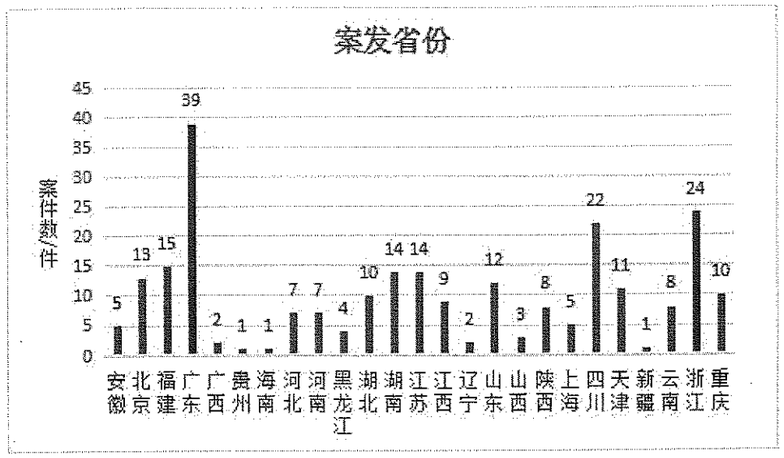
作者简介：吴勃，武汉大学法学院博士研究生。

① 参见中国司法大数据研究院：《网络约车与传统出租车服务过程中犯罪情况司法大数据专题报告》，2018 年 9 月，第 3 页。



在滴滴司机作为犯罪人的 248 份判决书中，一审案件共 243 份，占 98%，二审案件共 5 份，占 2%。

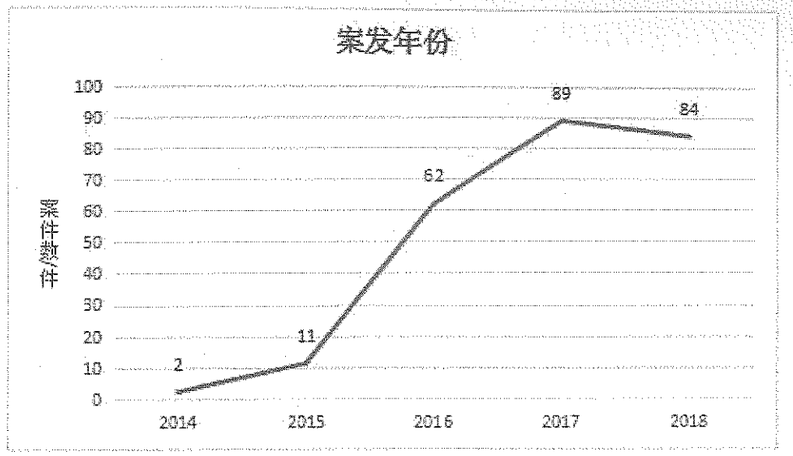
2. 案发省份



案发地分布广泛，广东省为发案最多省份，合计 39 件，占总案件数的 15.73%，浙江省发生 24 件，排名第二。其中 11 个省份案发件数超过 10 件。除四川省外，其余省份均为中东部 GDP 排名靠前省份。

表明滴滴司机犯罪与经济发达程度有关，因无法获取滴滴车总数量，无法得出案发比例结论。

3. 案发年份

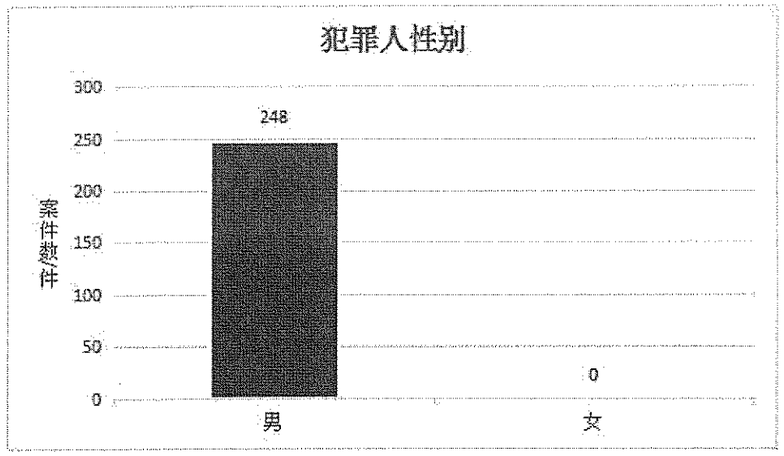


滴滴司机犯罪的案件最早案发于 2014 年 7 月，因裁判文书上网时间延后等原因，统计判决最晚案发时间为 2018 年 10 月。可以预见，2018 年案件数将超过 2017 年，案件数呈逐年上升趋势。其中 2017 年案发件数为 89 件，与中国司法大数据研究院公布的 20 件案件数差异较大。

（二）犯罪人特征

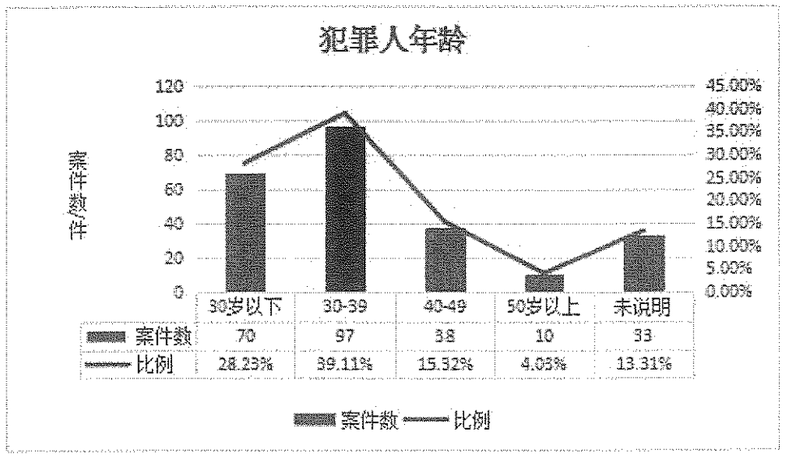
该部分主要合计犯罪人性别、年龄、学历、犯罪人是否有前科和司机类型。

4. 犯罪人性别



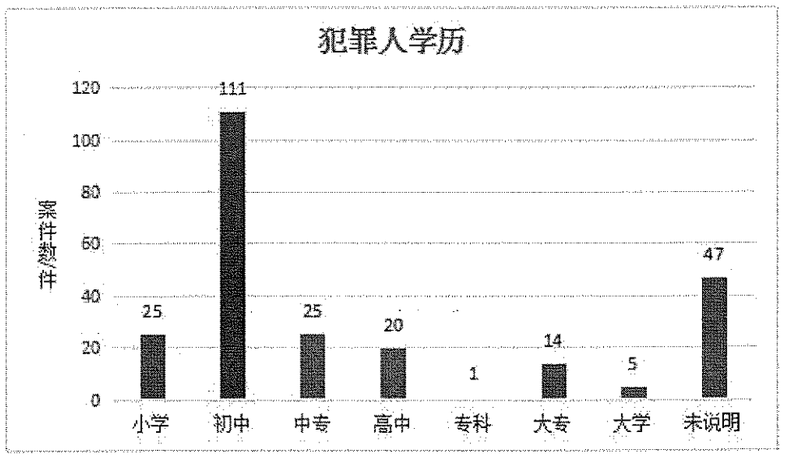
248 起事件，犯罪人全为男性，无女性司机犯罪判决书。与密闭空间中男性更易处于强势地位有关。

5. 犯罪人年龄



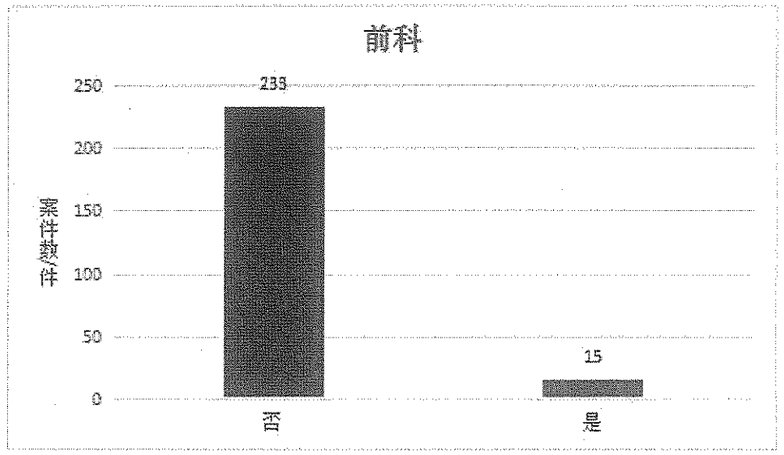
犯罪人人最小 20 岁，最大 60 岁，其中 30-39 岁年龄段人数最多，40 岁以下占到总犯罪人数的 2/3 以上。青年司机犯罪占比较重与犯罪所需体力有关，表明滴滴司机犯罪多为“体力型”犯罪。

6. 犯罪人学历



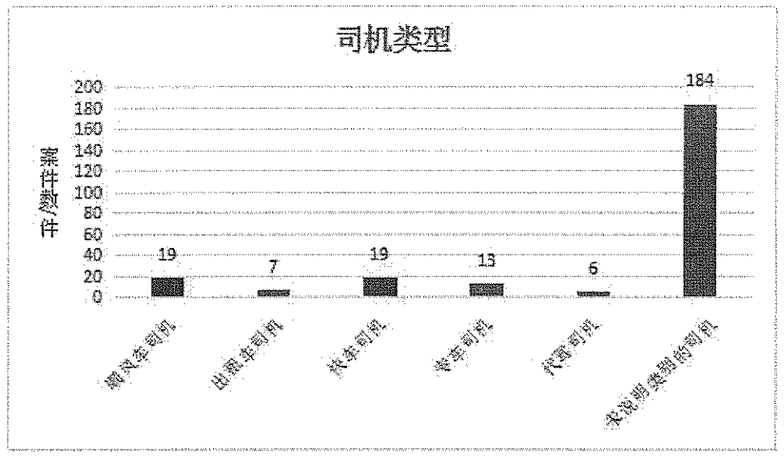
初中学历最多，达 111 件，初中及以下学历占总数 1/2 以上。表明低学历滴滴司机更易犯罪，不属于高学历犯罪。

7. 犯罪人是否有前科



其中 15 人具有犯罪前科，但其中 5 人有被行政拘留经历。其中未收到或任何刑事、行政处罚司机犯罪件数为 233 件，占总犯罪件数的 93.6%，表明是否具有犯罪前科对滴滴司机犯罪影响较小，滴滴公司要求的无犯罪记录是否合理值得商榷。

8. 司机类别

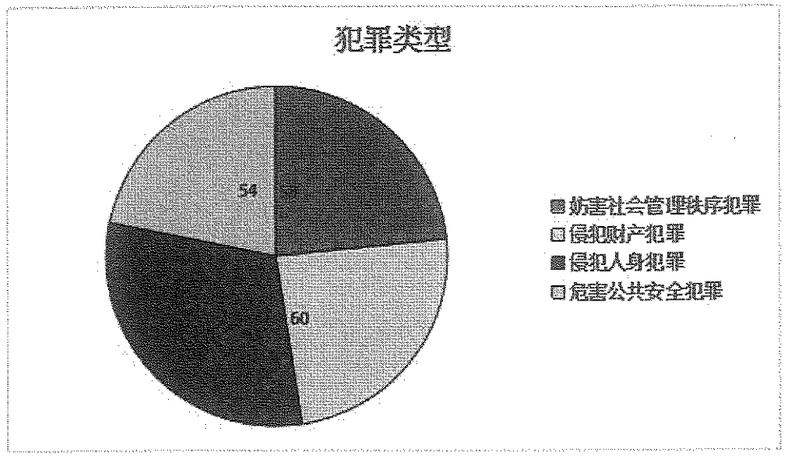


在已说明司机类别中，顺风车司机、快车司机占比最高。

（三） 犯罪特征

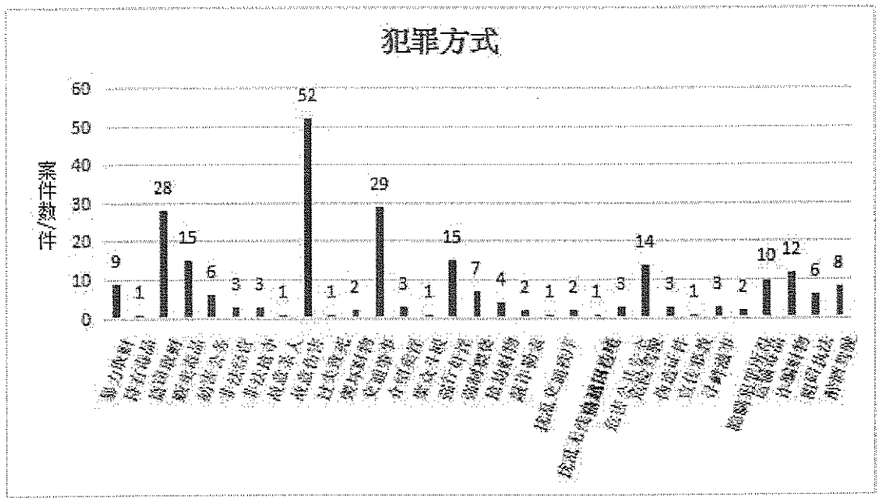
该部分涉及犯罪类型、犯罪方式和犯罪起因。

9. 犯罪类型



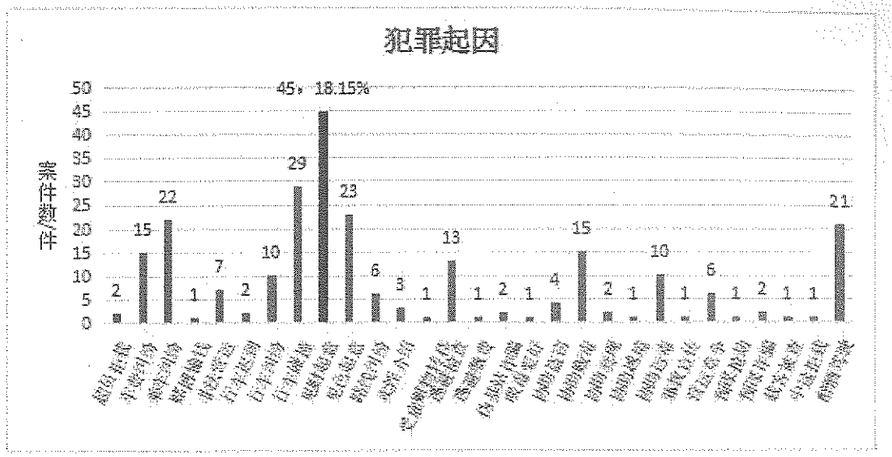
四中类型案件数量大致相当，四大类型犯罪中，侵犯人身犯罪案件数量最多，共 76 件，占比 30.65%，妨害社会管理秩序犯罪案件数量最少，共 58 件，占比 23.39%。

10. 犯罪方式



犯罪方式多样，共 31 种，其中故意伤害犯罪最多，达 52 件，占比 20.97%，其次是交通肇事犯罪，占比 11.69%。故意伤害犯罪与密闭空间、犯罪人性别、年龄有关，交通肇事是滴滴车长时间、大量在路的必然结果。

11. 犯罪起因



犯罪起因多样，共 29 种，以见财起意为最多，达 45 件，占总数的 18.15%

统计分析得出以下结论：滴滴司机犯罪案件中，犯罪人以 40 岁以下，初中学历以下的顺风车、快车司机占多数，且以暴力方式实施侵犯人身犯罪、侵犯财产犯罪为主。

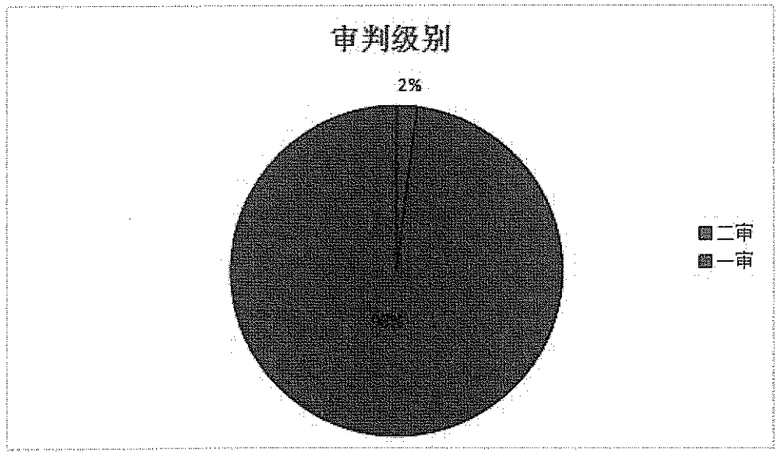
二、滴滴司机作为被害人案件

滴滴司机作为被害人的共 299 件，比滴滴司机作为犯罪人案件多 51 份，表明滴滴司机更易成为被害人，处于弱势地位，其权益保护势在必行。

（一）案件特征

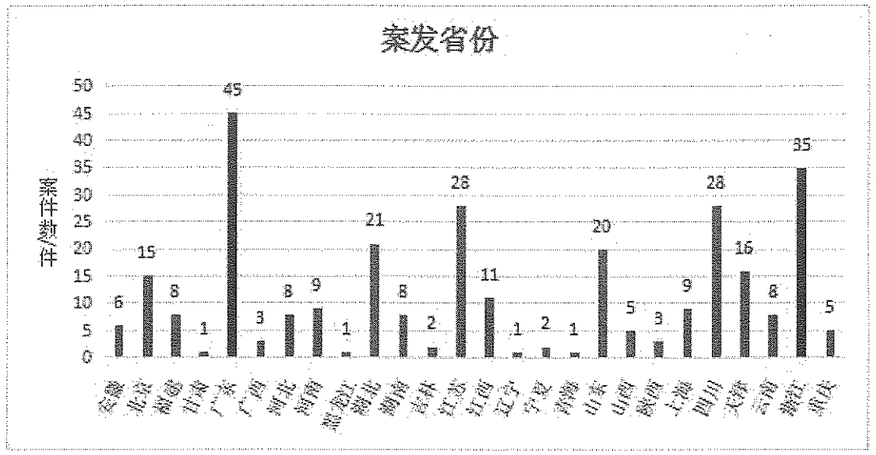
该部分主要涉及判决书审判级别、案发省份和案发年份。

1. 审判级别



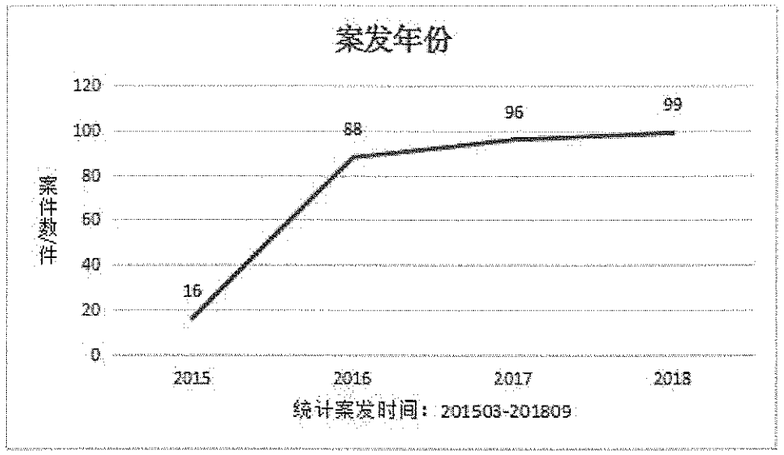
在以滴滴司机为被害人的 299 件案件中，一审案件 293 件，二审案件 6 件。

2. 案发省份



案发分布众多省份，以东部发达地区为主，其中广东省案件最多，达 45 件，占 15.05%。案发省份分布于滴滴司机作为被害人案发省份分布大体一致。

3. 案发年份

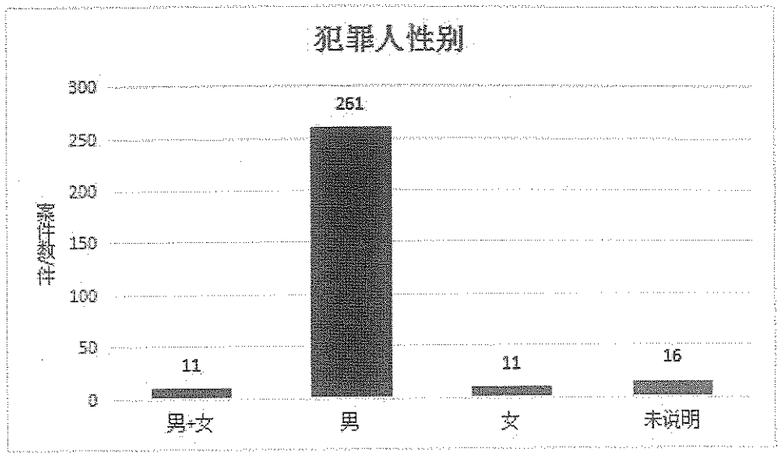


滴滴司机作为被害人的案件最早案发于 2015 年 3 月，统计最晚案发于 2018 年 9 月，案发数量呈逐年上升趋势。

（二）犯罪人特征

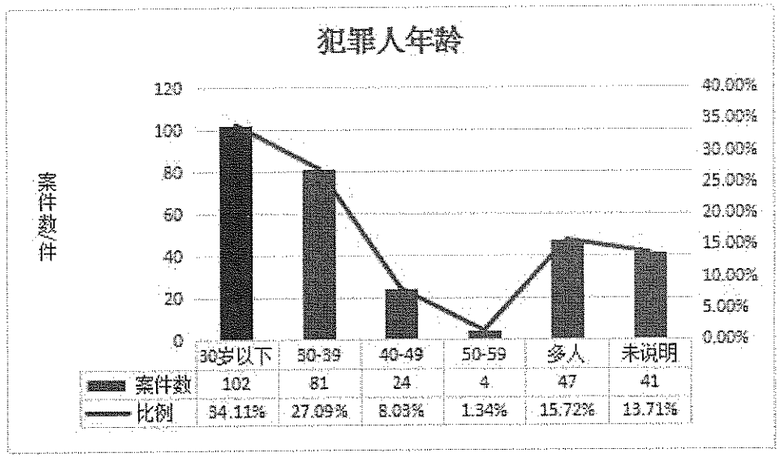
该部分主要合计犯罪人性别、年龄、学历、犯罪人是否有前科、犯罪人身份和被害司机类型。

4. 犯罪人性别



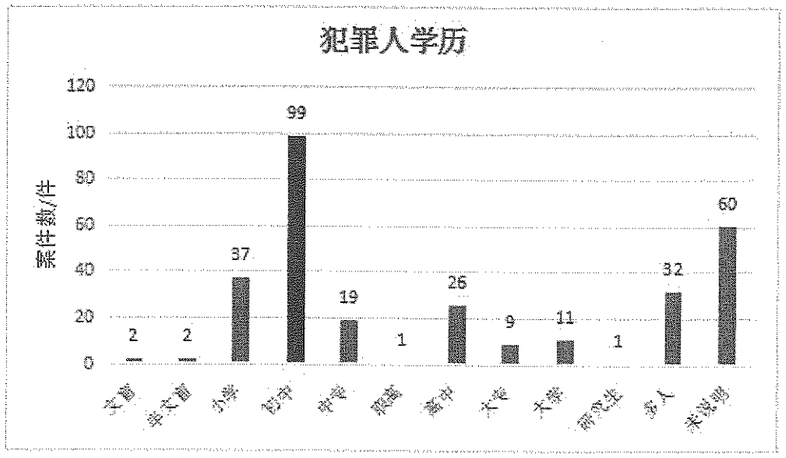
犯罪人以男性为主，但也存在 11 起男女共同犯罪和 11 起女性单独犯罪案件。

5. 犯罪人年龄



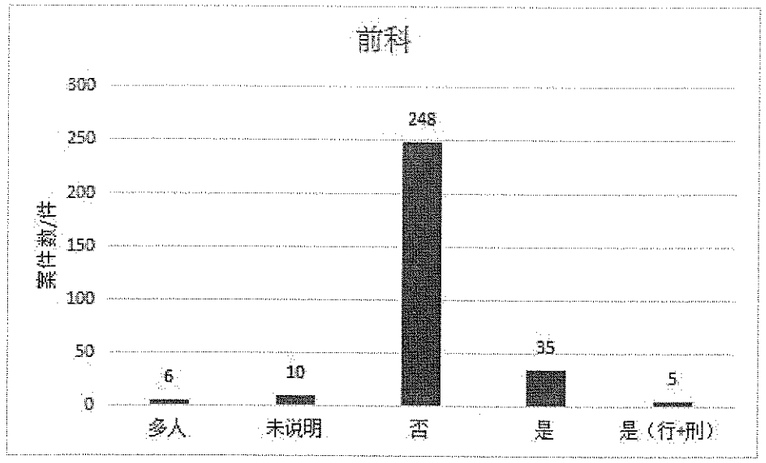
犯罪人年龄最小 17 岁，最大 59 岁，以 30 岁以下犯罪人最多，占比 34.11，40 岁以下犯罪人占比超过 60%。两人以上共同犯罪，犯罪人年龄未分别计入任一年龄区间。

6. 犯罪人学历



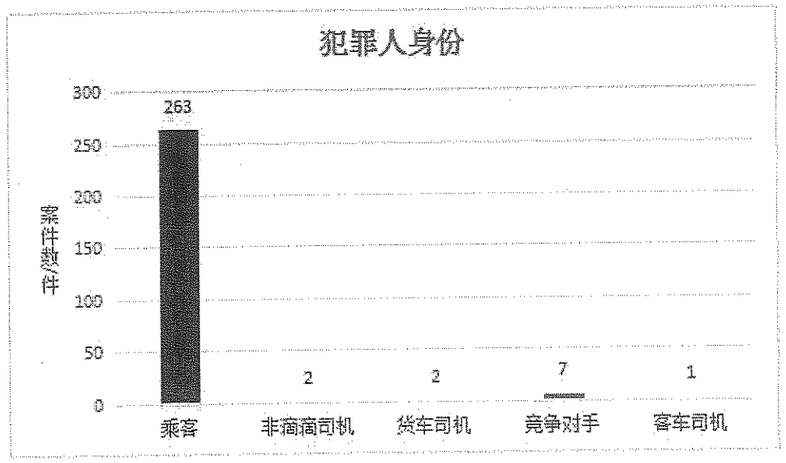
初中学历最多，达 99 件，以说明学历中，初中及以下学历占比超过总数的 1/2。

7. 是否有前科



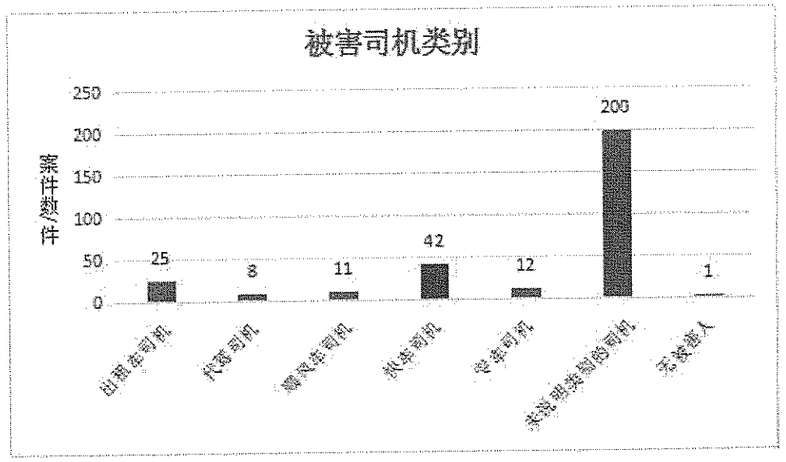
共 35 人有前科，占比 13%，其中 30 人有犯罪前科，5 人有被行政拘留经历。

8. 犯罪人身份



以乘客为主，但也存在竞争对手等第三人犯罪。

9. 被害司机类型

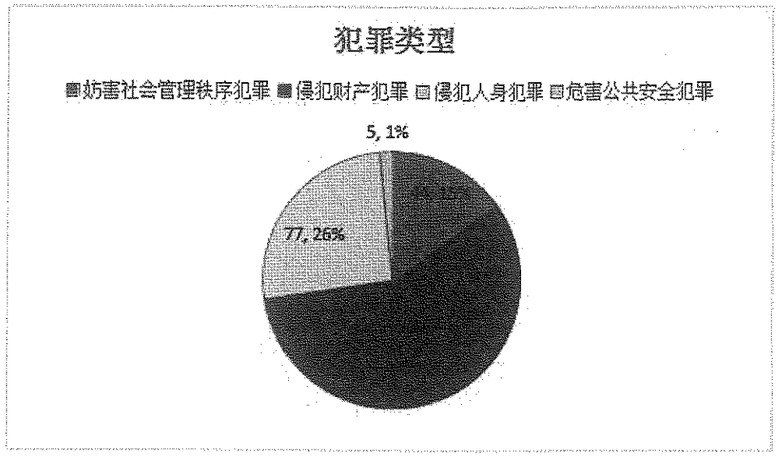


已说明类别中，快车司机最多，出租车司机次之。

（三）犯罪特征

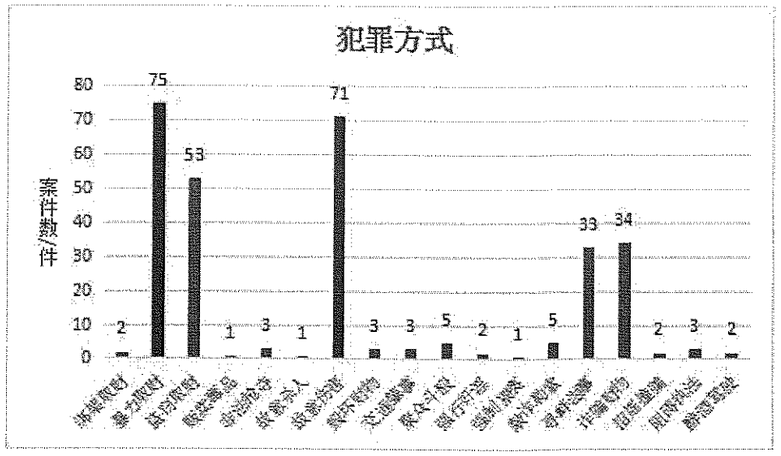
该部分涉及犯罪类型、犯罪方式和犯罪起因。

10. 犯罪类型



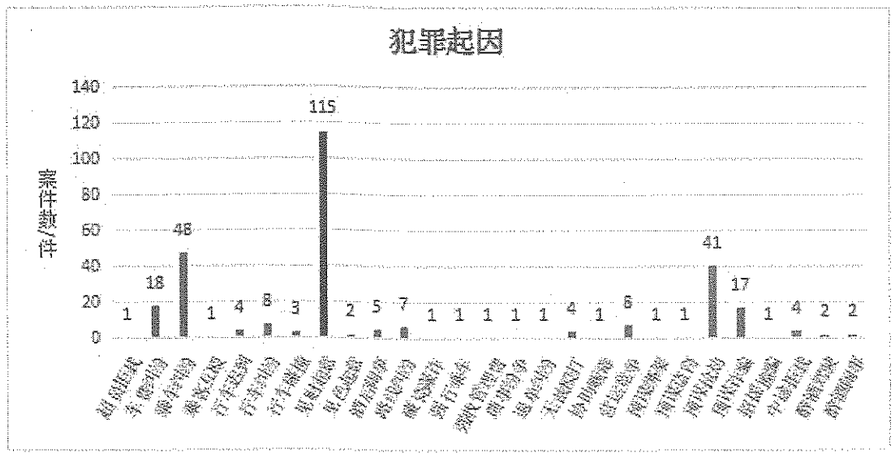
滴滴司机作为被害人案件中犯罪类型以侵犯财产犯罪最多，占比超过全部的1/2，侵犯财产犯罪和侵犯人身犯罪案件合计超过总数的80%。

11. 犯罪方式



以暴力取财和故意伤害为主要的犯罪方式，两种犯罪方式合计约总数的1/2。

12. 犯罪起因



犯罪起因中见财起意远超过其他原因，达115件，占总数的38.46%。

统计分析得出以下结论：滴滴司机作为被害人案件中，滴滴快车司机、出租车司机成为被害人占比最大，且多受到暴力型财产犯罪侵害，应采取有效措施保障滴滴司机人身、财产安全。

滴滴平台中，人人都可以成为内容生产者，平台借助算法，向用户推荐个性化信息匹配，平台具有市场参与者与组织者的双重身份。作为参与定价的平台，提供抢单、派单等匹配机制，对市场的“具化”程度高于一般平台，应受到更多的关注。自2016年9月，滴滴与Uber中国业务合并后，滴滴已在网约车领域处于“一家独大”的垄断地位，此时，它作为市场组织者及信息壁垒重构者，有成为具有准公共产品属性的新型经济社会基础设施可能。因此，应加强对以滴滴平台为代表的网约车平台的关注，规范企业责任。

以上，就是我报告的内容，不当之处，请各位老师指正。谢谢。