超级平台犯罪治理权的基本构造与行使规则

李　林

摘要：超级平台代行国家在网络空间中的犯罪治理权是技术便宜的重要体现。在网络空间犯罪治理中，超级平台既通过自主设定规则打击用户不良违法行为，又通过调取用户信息对政府提供技术支持与协助，呈现出“平台管用户”的现实形态。但平台本身往往存有“私心”，只有充分调动政府机能才能有效规制平台行为。应急式治理与常态式治理皆是“国家管平台”的直接体现，二者的行动依据是“分散”或“系统”的立法规范。为推动平台技术治理有序向前并防止技术被不当利用，国家应预先创设“法定允许”与“政府指令”两种权力行使的豁免范围。同时，国家应通过审查手段直接监督与管控权力，并适当下放权力承担引导者角色，形成“规范-规则-代码”的递进治理结构。

关键词：看门人；技术支持与协助；领域立法；技术便宜；网络生态治理

DOI：10.19836/j.cnki.37-1100/c.2026.04.018

网络空间犯罪治理是现代科技社会面临的重要议题。2025年11月，中共中央政治局就加强网络生态治理进行第二十三次集体学习。习近平总书记在主持学习时强调：“网络生态治理是网络强国建设的重要任务，事关国家发展和安全，事关人民群众切身利益。”①显然，网络空间犯罪治理是网络生态治理的重要一环，回应了数字社会总体层面犯罪形式的显著转变——“网络成为犯罪发生的主要空间”②。面对网络空间犯罪的复杂特性，“国家管平台、平台管用户”式的治理策略勃然而兴，即国家与政府监管部门按照法规政策指引规制平台行为，从而达成借助平台间接长期有效管控用户及防止网络空间犯罪发生的目的。在此之下，一部分原来由政府公权力控制的公共空间转化为“平台空间”③，平台在线控制犯罪成为主流，形塑出平台犯罪治理权这一新型“准公权”形态。然而，并非所有规模的平台都具有规范用户行为的能力，无标准的赋权只会增加治理网络空间秩序的烦扰。

按照2021年10月发布的《互联网平台分类分级指南（征求意见稿）》，应将拥有“超大用户规模、超广业务种类、超高经济体量及超强限制能力”的超级平台作为网络空间犯罪治理任务的主要承载主体。相较于大型和中小型平台（普通平台），超级平台的权力集中度高，聚合入驻审查、规则制定、用户处罚等多项权力于一体，并且其凭借自身提供的通信、支付、出行等基础性数字服务（公共承运人身份），让用户不得不同意平台内的诸多规则设定，以“服从”换取服务④。但“权力的生成”与“权力运行的风险”同在，缺乏规制的超级平台犯罪治理权可能将权力带入失序状态，甚至使平台本身转为网络空间中被治理的对象。如过度监测网络暴力信息、无端形成用户信息画像、因私调用接口传输数据信息等，都可被视为超级平台犯罪治理权失序的样态。因此，由超级平台完全掌控网络空间犯罪治理权并担任互联网安全的“看门人”（gatekeeper）尚存阻碍及隐忧。一方面，放宽犯罪技术治理范围会加剧

基金项目：教育部人文社科青年基金项目“金融数据治理的公私合作机制研究”（23YJC820026）；司法部法治建设与法学理论研究部级科研项目“数据资产化的法治保障研究”（24SFB3030）。

作者简介：李林，内蒙古大学法学院讲师，南京大学法学院博士后流动站研究员（呼和浩特 010021；lilyn1993@163.com）。

① 《习近平在中共中央政治局第二十三次集体学习时强调 健全网络生态治理长效机制 持续营造风清气正的网络空间》，《人民日报》2025年11月30日，第1版。

② 单勇：《数字看门人与超大平台的犯罪治理》，《法律科学（西北政法大学学报）》2022年第2期。

③ 马治国、占妮：《数字社会背景下超级平台私权力的法律规制》，《北京工业大学学报（社会科学版）》2023年第2期。

④ 解志勇：《超级平台重要规则制定权的规制》，《清华法学》2024年第2期。

用户的不安感;另一方面,“为数据行为设定过于严格的行动约束”[①]显然不利于平台经济的发展。于此境遇下,亟须系统探究超级平台犯罪治理权的基本构造,以此设定预防权力异变的回应方案,建立网络空间犯罪治理与技术发展秩序。

一、超级平台犯罪治理权的生成与正当性根基

网络空间技术能力的提升是超级平台犯罪治理权形成的基础。但掌握犯罪治理权的超级平台,本身并不如政府一般具有治理犯罪的权威。在网络空间中,政府作为主导治理者,天然享有介入与管理权威;非权威主体(超级平台)若要行使犯罪治理权,必须通过某种形式得到授权,以建立起权力行使的正当性根基。

(一)从普通到超级:平台演进下犯罪治理权的生成

按照时间发展的节点,自1994年中国全功能接入国际互联网后,平台这一概念进入大众视野并渐渐改变人们互动模式及社会经济模式。如今的BAT(百度、阿里巴巴、腾讯)均发轫于这一初创时期,正可谓互联网企业与平台的起步阶段。尤其是在2000年,三大门户网站(搜狐、新浪、网易)挂牌上市,各种社交、电商平台被乘势快速推出,极大地重塑了人们的生活方式。到2010年左右,移动互联网时代正式开启,用户开始习惯于从移动平台中时刻获取网络信息服务,形成了依赖式的“人机共存”社会,并逐步显现出向规模化(量)、超智化(质)迈进的发展趋势。在“量”与“质”的耦合交融下,平台的用户基础与技术能力不断攀升,其功能已由单纯的信息撮合扩展至规则设定。

在此基础上,超级平台除维护网络安全交易秩序外,循序承担起网络空间的犯罪治理任务。例如,平台按照法规要求对“审查程度极低却会暴露极端主义态度的评论区”[②]进行网络暴力监测(反网暴),依据工信部要求展开网络实名制登记以预防电信网络诈骗(反电诈),配合公安部门在网络空间巡查非法在线体彩赌博(反博彩)等。以上犯罪治理行为,从主动识别违法风险、配合执法机关取证,到依据政策指令开展技术干预,无一不体现出突破超级平台内部管理权能的公共治理职能。由此,一种在网络空间犯罪治理中的新兴概念得以衍生——平台犯罪治理权,即互联网平台在国家授权与公共利益要求下,为防范、发现、报告、遏制和协助处理平台内外相关犯罪行为所行使的一种治理性准公权。这种权力表面上虽由平台行使,但实质上是平台以网络技术能力助力国家实现其犯罪治理职能在技术领域的延伸。

(二)超级平台犯罪治理权形成的正当根基

探清犯罪治理权的权力来源是解析超级平台治理行为的前提。传统社会中,城市是吸引犯罪的主要场域,如给街道带来不安的危险驾驶、直接导致财产折损的盗窃、造成身体与心理双重损害的抢劫等。尤其是前两项犯罪,长期位于检察机关受理审查起诉案件排名的前列。当新业态走向前台,现有犯罪类型随之改变,以电信网络诈骗及其关联犯罪为代表的新型社会问题愈发凸显。最高人民检察院于2025年3月发布的《刑事检察工作白皮书(2024)》显示,全国检察机关共“起诉电信网络诈骗犯罪78203人,同比上升53.89%”[③]。面对网络空间犯罪的强势来袭,犯罪治理重点从“线下”转向“线上”。然而,超级平台“促使或强迫他人按自己的意志作为或不作为”[④]的权力本质上归“私”,这就意

① 吴沛泽:《数据犯罪规制路径的体系调适:基于双层法益观的确立》,《学术交流》2025年第5期。

② Hawdon J., Bernatzky C., Costello M., “Cyber-Routines, Political Attitudes, and Exposure to Violence-Advocating Online Extremism Crime and Deviance”, *Social Forces*, 2019, 98(1), p. 332.

③ 《刑事检察工作白皮书(2024)》,https://www.spp.gov.cn/xwfbh/wsfbh/202503/t20250309_688590.shtml,访问日期:2026年1月5日。

④ 刘权:《网络平台的公共性及其实现——以电商平台的法律规制为视角》,《法学研究》2020年第2期。

味着当其行使“公”属性权力时必然要获得最起码的初始性授权。那么,这种能够整治网络空间秩序的权力究竟源自何处?

第一,源自立法上的直接规定或宽泛授权。在我国,引导、约束超级平台有序治理犯罪的规范虽逐步出台,但由于技术发展远超规范制定者预计,平台操作可能在一定时间内处于“无具体根据”状态。超级平台不得不“双线并行”,形塑出两种规则制定及犯罪控制路径。一种是基于立法规范的直接规定,将比较明晰的法条转换成超级平台犯罪治理的具体代码指令。如2022年9月通过的《中华人民共和国反电信网络诈骗法》(以下简称反电诈法)第22条规定,互联网服务提供者可根据风险情况对涉诈账号“采取限期改正、限制功能、暂停使用、关闭账号、禁止重新注册等处置措施”。另一种是基于立法规范的宽泛授权,即面对原则性的留待平台细化的条文时,超级平台不得不利用技术权威在具体规范出台前形成犯罪治理规则(先行补位),以预防、阻止、惩治平台空间的不法行为。如2024年8月起施行的《网络暴力信息治理规定》(以下简称网暴规定)第7条规定,网络信息服务提供者应“建立完善网络暴力信息治理机制,健全用户注册、账号管理、个人信息保护、信息发布审核、监测预警、识别处置等制度”。不管是建立治理机制还是健全具体制度,都反映出网暴治理的防控落实将由平台承担。

第二,源自被动签订的用户服务协议。签订用户服务协议是超级平台获取数据的始端。当使用者点击“同意”时,标注用户权利与义务、隐私与数据管理、责任限制与免责声明等的格式化契约即刻生效。该协议由超级平台制定,尤其是赋予其犯罪治理权施展权限的隐私政策条款,用户方似乎只能被动接受。一般而言,平台隐私政策以“存于用户服务协议”(嵌入式规定)和“与用户服务协议并列”(单独式规定)两种形式出现[①],主要包含数据的收集、使用、共享与保护措施等内容。如2021年12月更新的《腾讯隐私政策》属于后者,在格式文本中详列了“我们收集哪些信息”“我们收集信息的用途”“您所享有的权利”这三大规则[②]。在现实中,用户面对隐私政策中晦涩的法律术语望而却步[③],导致条款签订大多非双方合意,形成“平台单方拟定、用户被动接受”的局面。除上述缘由外,这种被动签订情形更多可能是出于用户对超级平台服务内容的依赖,用户虽然明知但又无可奈何。

由上观之,时代造就了超级平台的犯罪治理能力,并逐渐替代政府接管部分网络空间秩序的维护任务。但平台权力毕竟本质为“私”,无法径直获得政府的公属性权威。进而,这种先天不足的“准公权”就须拥有权力来源,以佐证其行为的正当性。

二、超级平台犯罪治理权在网络空间中的二分形态

超级平台在网络空间中扮演着重要角色,其影响力不只体现在商业运营中,还体现在国家立法与用户服务协议双重交付下的犯罪治理层面。结合既有规范内容与“国家-平台-用户”三者间的关系,这种具有犯罪治理功效的新型权力,具体呈现出自主治理与协助治理两种现实形态。

(一)自主治理形态:超级平台对用户的规则设定

超级平台自主设定规则是其维护网络秩序、打击不良或违法行为和管控网暴信息的重要方式。从效力对象来看,该规则约束的是超级平台内的用户,意在为其提供使用平台服务的指引性准则。基于内容与结构,平台规则看似与国家出台的法律法规等“硬法”并无不同,但实际上,以互联网平台规则为代表的“软法”,一般不依赖国家强制力保证实施[④]。据此,超级平台的犯罪治理规则具有如下特征:

其一,特定主体范围内的有限效力。超级平台具备“技术先占”的领域控制特性,在打击犯罪方面形

① 李涛:《网络平台用户服务协议格式条款的类型化研究》,《北京理工大学学报(社会科学版)》2024年第5期。

② 《腾讯隐私政策》,https://privacy.qq.com/policy/tencent-privacypolicy,访问日期:2026年1月17日。

③ 高秦伟:《个人信息保护中的企业隐私政策及政府规制》,《法商研究》2019年第2期。

④ 沈岿:《自治、国家强制与软法——软法的形式和边界再探》,《法学家》2023年第4期。

成事实上的规则设定优势。比如，超级平台可凭借系统捕获海量用户行为信息，包括浏览事项、通信记录、转账情况等。以上数据，不但可以作为一种商业资源，还能够使平台准确、迅速地识别到用户的异常操作及潜在犯罪风险。由于信息技术正重塑着犯罪结构，电诈、网暴等犯罪的主要场域已非现实空间，转而迎来的是一种虚拟的“平台在场”。这将导致国家即使有意整治网络空间，也需借助平台提供的技术通道。最终，“关键服务的访问权限”①由平台直接掌控，特定环境下公权要依托私权才能有效运转。

其二，领域规范下的自主治理。信息技术的快速迭代加剧了社会问题的复杂程度，特别是在互联网平台普及的背景下，单一部门法已无力解决新型危机。并且，即使是多部门法合力，由于规范间的体系松散，也难以满足治理综合性犯罪的实际所需。回顾传统“因循部门”②的立法范式，强调特定调整范围的部门法容易造成规范间的沟坎。部门法间的分立让网络空间的法秩序维护表现为一种拼凑状态。为解决该缺陷，力图有效预防及打击某领域犯罪的立法模式勃然而兴，并主要适用于网络空间的犯罪治理场域。如2020年3月起施行的《网络信息内容生态治理规定》，主要以网络信息内容为治理对象，重在整治网络空间用户制造的违法及不良信息等。以领域规范为纲领，各互联网平台纷纷结合自身业务及常见犯罪情况制定治理规则。目前，国内最大的短视频平台抖音，总结出一系列样板型自主治理方案，将2022年9月生效的《抖音社区自律公约》作为社区总则，其中囊括“暴力与犯罪行为、时政有害及不实信息、侵犯人身权益”③等十项平台禁止内容，治理成效突出。

其三，犯罪惩罚上的权力交付。在互联网平台迈入大众视野并开辟网络空间前，现实社会中的“国家权力始终是唯一的支配力量”④。依随超级平台生成的网络空间无限延展，此种权力不得不逐渐地部分交付。值得注意的是，权力交付不等于权力替代，国家与平台的身份属性未产生改变。以2022年6月起施行的新浪《微博投诉操作细则》第13条为例，平台可视程度对涉诈信息账号予以禁言甚至关闭；若情节恶劣或造成严重后果，站方将会报送公安机关⑤。这说明，超级平台虽有犯罪治理权限，却无刑事法层面的惩罚能力。当网络空间内出现犯罪情形时，依旧要回归传统的以国家强制力为保障的司法程序。

（二）协助治理形态：超级平台对国家的技术支持

现行法体系下，国家作为治理网络空间犯罪的主体地位未曾改变，但由于用户信息的生成、存储和流通日益集中于平台之上，国家的犯罪治理职能不得不面临“技术依赖”的境况。尤其是在电诈等复杂的网络犯罪案件中，侦查机关的取证任务往往需要借助超级平台提供技术支持和协助才能完成。此刻，超级平台作为刑事侦查的协助方，承担起用户信息数据提供义务。如反电诈法第26条规定，“公安机关办理电信网络诈骗案件依法调取证据的，互联网服务提供者应当及时提供技术支持和协助”。这说明，协助治理模式下的超级平台扮演着刑事数据调取的“数据池”⑥角色。该模式的运转逻辑有效地将国家刑事侦查权力与平台技术资源进行结合，形成了有助于提升侦查效率和打击网络空间犯罪的合作机制。但这种合作在结构上并不对等，超级平台的作用更多是一种被动的响应。

与此同时，“规则便宜”是促成该协助式合作格局的重要推力，但常常饱受诟病。根据侦查行为是否限制、剥夺公民基本权利，可将侦查措施分为强制性与任意性两种。相应地，对于容易造成权力滥用的强制侦查，立法者对其规定了严格的启动程序及适用阶段。可是，这种绕开侦查对象向超级平台取证的方式，可能“规避强制性侦查措施的限制条件”⑦或脱离程序性规范的既定审查。并且，办案机

① 周尚君：《数字权力的理论谱系》，《求是学刊》2024年第1期。

② 周佑勇：《从部门立法到领域立法：数字时代国家立法新趋势》，《现代法学》2024年第5期。

③ 《抖音社区自律公约》，https://www.douyin.com/rule/policy？activeId=self_decipline，访问日期：2026年1月25日。

④ 孙笑侠：《数字权力如何塑造法治？——关于数字法治的逻辑与使命》，《法制与社会发展》2024年第2期。

⑤ 《微博投诉操作细则》，https://kefu.weibo.com/faqdetail？id=20543，访问日期：2026年1月26日。

⑥ 李延舜：《刑事数据调取中网络服务提供者的角色定位及关联义务》，《法学》2023年第1期。

⑦ 裴炜：《论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角》，《法律科学（西北政法大学学报）》2021年第3期。

关与平台本就在数据种类与体量、传输方式、后续处理等方面存在诸多争议,以至于实务操作中频频出现取证难、取证不及时、取证不全面等问题①。2019年2月起施行的《公安机关办理刑事案件电子数据取证规则》第41条,将"经办案部门负责人批准"与"开具注明需求的《调取证据通知书》"作为公安机关向平台调取电子证据的前置条件。这两项限制在一定程度上压缩了办案部门调取用户信息的权力范围,但与现实需求相比,依旧难以化解网络空间中犯罪侦查与数据提供间的不均衡冲突。

能够看出,二分形态的背后是超级平台作为国家助手管理用户的身份定位。在这一角色下,超级平台不仅协助国家开展网络空间犯罪治理,还凭借其对海量用户信息的掌握和强大的数据处理能力,成为维持网络空间秩序的重要支撑。在上述"平台管用户"关系中,国家是平台网络空间犯罪治理行为的根本权力来源,国家的角色定位是探明犯罪治理权失序的另一关键。

三、国家管控下超级平台犯罪治理权的治理模式与规范类型

国家作为管控超级平台的上位主体,决定了网络空间犯罪治理权的表现模式,其通过监管与立法两种手段,维持着网络空间的秩序和安全。当然,"国家管平台"机制虽未如互联网技术发展一般快速推进,但在紧跟其后的立法补救中也及时回应了诸多现实冲击。归根结底,超级平台犯罪治理行为是国家治理策略的践行,立法缺位是超级平台犯罪治理权无法有序行使的源头。

(一)超级平台与国家的互动及其治理模式

超级平台与国家的互动样态,通常取决于国家对平台的具体管控要求以及二者间的行为内容。一方面,国家根据其立法体系和犯罪打击目标,对超级平台设定网络空间治理准则。另一方面,超级平台凭借其技术和数据掌控优势,往往能对国家的犯罪治理策略产生反作用力。尤其是在技术性极强的场域,超级平台与其说是执行国家主导下的治理规范,不如说是根据技术规则生成治理规范。在上述管理与反作用的互动样态中,国家始终居于核心地位,并在事实上表现出两类不同的网络空间犯罪治理模式。

第一,以"事件为引"的应急式治理。当前,信息技术正日益成为犯罪的工具②,并在具体范围内形成如虚假信息传播、用户隐私泄露、网络极端言论攻击等具有规模的技术滥用。然而,对这些网络安全危机的觉察与重视,往往源自某个突发或造成严重后果的事件,即事件在网络空间犯罪治理中具有关键触发作用。当事件出现后,国家会发起并规定行动方式和议程③,集中力量依靠平台迅速开展以事件特征为名的专项行动,尽可能达到打击特定类型网络犯罪的目的。比如,针对侵犯公民个人信息、网络谣言、黑客犯罪、网络水军、网络黑灰产、网络暴力等突出网络违法犯罪④,公安部部署全国公安机关持续深入推进2025年"净网""护网"专项工作。这种非常规应急式治理的最大特点是聚焦事件特征形成短时的集中高压打击。换言之,国家会根据突发事件特征,锁定具有相似性的网络违法、犯罪行为,并通过密集执法行动来达到"雷霆式"治理效果。

第二,以"规范为据"的常态式治理。常态式治理有助于建立可持续的监管与惩罚机制,使得网络空间犯罪的整治不再依赖于突发事件的推动,转而迈向一种以规范为根据的长效之治。相比许多突发性事件由"吹哨人"披露而引起关注⑤,这种"国家主导、平台支持"的二元犯罪治理科层,能够尽可

① 王爱立、刘忠义、隋静等:《〈中华人民共和国反电信网络诈骗法〉释义与适用》,北京:中国民主法制出版社,2022年,第241页。

② Pandelică I. L., "The Phenomenon of Cyber Crime Section II: Studies and Analysis of Cybercrime Phenomenon", *International Journal of Information Security and Cybercrime*, 2020, 9(1), p. 30.

③ 谭荧:《运动式治理的长效问题与优化路径》,《理论视野》2024年第9期。

④ 《2025年"净网""护网"专项工作部署会召开》,https://www.mps.gov.cn/n2253534/n2253535/c10115671/content.html,访问日期:2026年2月10日。

⑤ 郑崇明:《松散关联、组织学习与结构化的灵活性——寻找常态治理与应急治理之间的平衡》,《政治学研究》2024年第4期。

能避免犯罪探查的不确定性并提高犯罪防控的主动性。依循此路径,超级平台一般先使用技术高效识别危险信号、快速定位恶意内容,然后借助关联分析算法在规范框架内整合用户数据,形成社交关系图谱。以此为基础,平台可对用户进行分级管理与精准监控,并觉察出潜藏的网络犯罪轨迹。上述过程实际形成了从“危险嗅探”到“数据画像”再到“风险评估”的全链条治理。

(二)“国家管平台”的规范类型

虽然应急式治理是一种临时的犯罪打击策略,但在危机过后,一些有益的经验会成为常态治理的重要组成部分。并且,即使其以事件为引也需要以一定的法律法规作为行动支撑,而形成长效机制的常态范式则呈现更强的规范性。由此,无论是何种网络空间犯罪治理形态,都要依托于体现国家意志的法律法规。具体而言,这种“国家管平台”的规范可分为两种类型:

1.分散规定式。在互联网形成早期,国内网络空间治理规范的出台相对于技术发展而言接近同步,显现出技术规范创立者的卓越预见能力。1994年2月,《中华人民共和国计算机信息系统安全保护条例》正式颁布,成为中国第一部关于互联网管理的专门行政法规①。规范的形成与前期互联网基础建设及接入国际互联网的时间相差无几。此后的二十余年间,国家规范及政府管控机制不断发布与调整,力图配合技术迭代并维护网络空间秩序。鉴于当时网络攻击的特点及传统立法的固有范式,我国针对网络空间犯罪治理采用了分散规定的方案,即国家层面不出台统一的领域型治理规范,而是将政府对平台的具体管控要求灵活放置于不同的部门法之中。可以肯定,在一段时间内这些分散规定起到了不可替代的治理作用,以较低的立法成本避免了因立法滞后带来的监管空白。

2.系统设定式。互联网技术的快速推进,让网络空间的犯罪类型日益集中和复杂化,渐渐出现了一些具有“高发生率”和“高危害性”的突出问题,如网络暴力、电信诈骗、信息系统入侵、数据库窃取等。这些犯罪形式不仅给用户带来实际损害,还打破了既有的网络生态秩序,让公众对互联网平台的安全性产生质疑。为解决上述问题,立法设计者渐渐开始探索领域立法范式以确保治理的有效性与系统性,即专注于系统设定“单一但全面”的规范体系来覆盖特定领域内的全部问题。

与依存于部门法的分散规定相比,系统设定式立法的特点在于:

其一,集中式规制。如今,网络空间犯罪手段越发复杂,传统的分散规定已无法满足犯罪治理的实际所需。从整体上制定更为全面的治理规范,从而弥补立法缺位并形成集中式规制,不仅能填补执法盲区,还能协调各部门力量提升治理效率。以2021年9月施行的《中华人民共和国数据安全法》为例,面对网络空间的数据处理活动,该法确立了国家网信部门的统筹协调与监管地位,实现了从“多头监管”到“统一协调监管”的重要转变。

其二,跨越法律部门。数据领域的权利(力)配置并不局限于某一部门法,而是具有跨法律部门的特征②。这种跨部门的配置方式,旨在全面回应网络空间中信息交互行为的复杂性,确保各部门在各自的职能范围内对平台及其用户行为进行不同侧重的监管。例如,具有显著跨法律部门属性的《中华人民共和国个人信息保护法》,其规制范围不仅限于民事隐私保护领域,还广泛涉及刑事诉讼中的数据和个人信息处理③。当然,这种立法模式“并不意味着消除部门法边界”④,而是强调跨部门间的协调和配合,即不同法律部门在规制内容和适用范围上仍具有独特属性,面向网络空间特定犯罪的系统式设定,只是从更高的视角进行统筹规制,以避免各部门出现执法推诿或执法冲突。

立法规范为国家在网络空间中的犯罪治理提供根本支撑,但当出现立法缺位时,超级平台的犯罪治理行动就会无据可循。特别是面对新出现的网络空间犯罪,规范滞后会进一步加剧超级平台陷入

① 方兴东、何可、钟祥铭等:《中国网络治理30年:“一体多元模式”的演进历程与规律启示》,《传媒观察》2023年第9期。

② 任颖:《数字立法基本范畴的分层逻辑与统合方式》,《政治与法律》2024年第9期。

③ 郑曦:《〈刑事诉讼法〉与〈数据安全法〉〈个人信息保护法〉衔接问题研究》,《中国刑事法杂志》2024年第2期。

④ 金梦:《数字时代科学立法的法理研究》,《中国法学》2024年第4期。

监管洼地的速度。因此,在“国家管平台、平台管用户”的治理策略中,除注重平台自我建设外,更应考虑既有的规范设定规则。

四、超级平台犯罪治理权的行使豁免及规制策略

国家对超级平台犯罪治理权无序行使的回应不能一概而论。根据“国家管平台”的监管机制与上位规范,平台行为应被视为一种国家规范指向或政府指令下的权力执行。然而,这不能排除作为私营主体的超级平台因不当动机而在网络空间犯罪治理过程中肆意突破规范框架内既定授权的可能。为更好地推动技术治理向前发展并避免权力滥用,应预先厘定超级平台犯罪治理行为的豁免范围,创建技术权力行使的“安全区”。与此同时,也应对平台权力进行规制,防止犯罪治理技术被用于权益侵害或违法犯罪,维持网络空间秩序。

(一)超级平台犯罪治理行为的豁免

超级平台代行国家在网络空间中的犯罪治理权能,已成为增强国家犯罪治理能力的重要方式。此时,平台即可借助大数据分析技术,协助国家机关与政府部门主动识别潜藏在网络空间中的隐蔽行为。显然,无论基于何种角度,超级平台的治理行为都俨然提高了对犯罪的响应速度。结合现有立法规范,超级平台的犯罪治理行为应在特定范围内得到豁免,如此才能确保犯罪治理技术的有效施展。

其一,法定允许行为。在现行规范框架内,超级平台的部分犯罪治理行为即使可能存有侵犯用户权益的嫌疑,但通常不会被视为违法。因为这些行为在法定允许范围之内,是国家网络犯罪治理职能的具体表现。例如,根据反电诈法第32条第1项的授权,互联网服务提供者可采用电信网络诈骗反制技术“监测识别、动态封堵和处置涉诈异常信息、活动”。此时,大到银行流水智能核查,小到生活支付结算,都时刻处于平台的监测之下①。尽管电诈监测行为会导致用户隐私被收集和解析,但为了更高效、精准地检测涉诈信息以阻断犯罪,该技术手段应被法律所允许。其法理基础在于,若干严格限定的监控技术措施(包括数据监测)在合乎法定授权、必要性与比例原则并配以监督机制的情形下,可被认为是符合宪法及相关部门法要求的。

其二,官方指令行为。国家机关与政府部门因办理刑事案件向超级平台调取用户个人信息,是数字社会政府指令行为的典型代表。回顾国内外相关事件,似乎只有预先免除平台责任才能最大限度换来信息数据的畅通调取。如在滴滴顺风车案中,平台以隐私泄露为由拒绝向警方及被害人亲友提供车牌等用户信息,导致解救行动延迟并造成难以弥补的后果②。此刻,我们不得不发出这样一种诘问:是何种缘由实质上左右了平台的最终判断?实际上,平台审核流程的繁杂及安全机制的疏漏都属于外部原因,而向有关单位披露用户信息影响平台信誉也只是由“未授权行为”衍生的一种担忧。委实而言,国家只有将平台提供用户信息的行为列入豁免范围,使其不属于隐私侵犯,才能有效打消网络服务提供者的疑虑,促使平台与国家达成合作并改进信息传输通道与事件反应机制。

对比来看,法定允许的行为给平台提供网络空间中的犯罪治理权限,让其能够在一定范围内推进技术治理的探索;官方指令则更容易由平台把握,平台只需在规范与技术的双重允许下尽可能遵循。当然,超级平台两类豁免行为并非没有限度,在进行网络空间犯罪治理时,应务必保持克制,始终围绕治理所需,避免因治理手段的泛化而侵犯用户的正当权益。

(二)国家对超级平台犯罪治理权的规制

在网络空间犯罪治理语境中,豁免范围的设定能够使平台拥有更多的自主性,加快技术治理的步

① 单勇、李林:《论互联网平台的反电诈协助执法义务》,《云南社会科学》2024年第5期。

② 高磊:《网络时代数据隐私的搜查干预——从滴滴顺风车司机抢劫、强奸、杀人案切入》,《安徽大学学报(哲学社会科学版)》2019年第3期。

调，或者说，能给网络服务提供者供应技术扎根的土壤。然而，正是出于这种技术便宜，让超级平台变相拥有“夹带私货”的机会，即那些本来用于犯罪侦查与预测的技术，可能成为超级平台调取用户个人信息的正当化工具。故此，不能放松对平台权力的管控与引导，应对超级平台的犯罪治理权进行规制。

1.审查式权力监督管控。审查式权力监督管控是指通过强制性手段，对超级平台的信息流动及技术使用行为等进行监督与限制，以确保犯罪治理技术符合既定的规范要求与政策目标。这种治理模式的最大特点在于有国家强制力作为保障，当平台瑕疵履行或拒不履行监管要求时，可能要面临警告、高额罚款、暂停相关业务，甚至直接关闭运营权限等处罚。立足于技术领域“国家管平台”的现状，审查模式的构建可分为两个步骤：

首先，需以算法备案的形式强制平台进行事前披露。超级平台将其使用的算法模型及相关信息进行报送与登记，是国家层面直接审查算法设计与运行是否符合立法期待的制度化方式。2021年9月，国家互联网信息办公室等九部门联合发布了《关于加强互联网信息服务算法综合治理的指导意见》，将有序推进算法备案工作视为构建算法安全监管体系的重要一环。其后，2022年3月起施行的《互联网信息服务算法推荐管理规定》初步搭建了算法备案的基本模式，指明了算法推荐服务提供者需填报的信息内容及具体步骤。该模式的出现，标志着以算法备案为核心的事前披露机制已初步落地。这在后续多次公布的《境内互联网信息服务算法备案清单》中能够得到证实。自此，除政府主体外，社会公众亦能通过备案清单了解算法名称、算法类别、主体名称、应用产品、主要用途和备案编号等信息，并可以在互联网信息服务算法备案系统中进一步查询公开的算法基本原理等各项信息[①]。当然，网络空间犯罪治理具有一定特殊之处，公众的知情在部分敏感区域仍需多加考量。但至少能够确定，国家当然拥有事前得知算法运作逻辑的权力，以避免算法负面影响的无节制扩张。

其次，要设置信息数据留存期，便于政府相关部门进行事后核查。通过留存关键数据，能够确保政府部门回溯性地分析超级平台犯罪治理权力的实际运行状况。例如，2016年通过的《中华人民共和国网络安全法》第6条第3项规定，网络运营者“按照规定留存相关的网络日志不少于六个月”。再如，2021年公布的《互联网信息服务算法推荐管理规定（征求意见稿）》第23条规定，算法推荐服务提供者应“对算法推荐服务日志等信息进行留存，留存期限不少于六个月”。当然，在此后正式出台的规范中，“不少于六个月”的表述被删除，转而形成了“具体留存期尚待进一步明确”的立法范式。尽管如此，“不少于六个月”似乎已成为网络空间信息数据留存的基本底线。令人难以抉择的是，虽然留存数据期越长则越利于面临争议时提供有效证明，但长期留存数据又可能增加“权力对个人隐私的窥探”[②]。因此，超级平台在践行数据留存义务时，不但要守住底线期限，还要根据政府的实际监管需求动态评估留存期限。

2.放权式间接技术引导。网络空间犯罪治理中的技术屏障，弱化了国家的直接管控能力。特别是在犯罪治理成本不断增长的情形下，政府部门渐渐开始有序放权，转而在技术性极强场域采取引导平台间接管控犯罪的方略。从平台本身来看，积极配合国家并承担治理责任并非单纯迫于外部监管压力，技术与资源的投入更多是为了达到构筑数字安全环境、吸引用户进驻使用的长期目标。虽然有些人可能会对公司承担责任持怀疑态度，但对社会责任的日益重视正在激励企业通过善行做得更好[③]。进而，国家将秩序维护权限下放给平台，是一种合作双赢的网络空间治理方式。但要注意，“放权”不等于“转权”，国家只是相对退居幕后担任引导者角色。这不失为一种“对规制者的规制”[④]的元规制（meta-regulation）路径。

① 张吉豫：《论算法备案制度》，《东方法学》2023年第2期。

② 姚建宗、龚志旺：《数字时代权力技术化及其法律风险应对》，《河南大学学报（社会科学版）》2024年第5期。

③ Boeken J., “From Compliance to Security, Responsibility beyond Law”, *Computer Law & Security Review*, 2024, 52, p. 2.

④ 罗伯特·鲍德温、马丁·凯夫、马丁·洛奇著：《牛津规制手册》，宋华琳、李鸽等译，上海：上海三联书店，2019年，第164页。

代码技术是网络规制的重要手段,而法律可以通过影响技术而实现间接规制①。站在国家立场,其引导方式主要是借助立法设定平台义务,并将更为具体的技术标准与犯罪防控方案留待平台完善。此刻,平台的功能在于将国家规范转化成代码,以技术执行者的姿态落实犯罪治理目标。同时,上述从规范到代码的过程中,平台规则处于枢纽位置,事实上形成了"规范—规则—代码"的递进转化结构。拥有超级用户体量的平台既是"规范解释器",又是"代码生成器",而两种功能的实现条件便是制定出用于犯罪治理的平台规则。由此可凝练出放权式间接技术引导的两大特征:一是规范框架设定义务,将犯罪治理的"方向盘"牢牢掌握在政府手中;二是平台规则驱动技术治理,让嵌入规则的代码执行具体的犯罪治理目标。这种治理模式既利用了平台的技术与数据优势,又降低了政府直接干预的成本,还赋予了平台结合自身实际自主制定规则与执行网络空间犯罪打击任务的权力。

五、结语

正如美国前卫科技领域权威思想家埃瑟·戴森(Esther Dyson)所言:"数字化世界是一片崭新的疆土,可以释放出难以形容的生产能量,但它也可能成为恐怖主义者和江湖巨骗的工具,或是弥天大谎和恶意中伤的大本营。"②现如今,这一经典论断伴随技术进步越发成谶。曾经推动社会进步与经济发展的网络空间,也会成为传播不良、违法信息的温床。更有甚者,一些不法之徒将其当作谋划暴力行动与制造虚假信息欺骗公众的工具,给部分用户乃至网络社会都造成了深远的负面影响。为恢复网络空间的正常秩序,国家借助超级平台在犯罪治理中的技术便宜,逐渐摸索出"国家管平台、平台管用户"式的双层治理策略。在发挥平台技术优势与节省治理成本的同时,有效实施了网络空间中的犯罪打击策略。当然,平台本身往往存有"私心",可能会借由犯罪治理肆意将用户信息用于他处。故而,在驱动双层治理策略时,既要将犯罪治理权力适度下放给平台,又要对平台可能造成的现实危害保持警惕。可以预见,随着信息技术的持续迭代,"国家-平台-用户"三者之间的权力结构势必进一步重塑,最终推动良性网络空间秩序的建立。

The Fundamental Structure and Rules for Exercising Governance Authority Over Super Platform Crimes

Li Lin[1,2]

(1. School of Law, Inner Mongolia University, Hohhot 010021, P. R. China;
2. School of Law, Nanjing University, Nanjing 210093, P. R. China)

Abstract: Against the backdrop of the profound evolution of the digital society, cyberspace is gradually replacing physical space as the primary arena for crime. Based on the technological control characteristics of super platforms, they, to a certain extent, replace relevant government departments in fulfilling crime governance tasks, giving rise to a new type of crime governance power. The emergence of this crime governance power is built upon the evolution of platforms from ordinary to super platforms; its essence is that platforms, through their technological capabilities, extend the state's crime governance functions. However, "shaping power" and "power risk"

① 毛海栋:《技术何以规制?——技术规制的概念证成与意义探究》,《浙江学刊》2024年第6期。

② 埃瑟·戴森:《2.0版数字化时代的生活设计》,胡泳译,海口:海南出版社,1998年,第17页。

coexist; the unregulated crime governance power of super platforms may lead to a state of disorder, even turning the platform itself into a subject of governance in cyberspace.

Combining existing normative content with the relationship between "state-platform-user," the crime governance power of super platforms can be divided into two basic forms: autonomous governance and assisted governance. The former is reflected in the rules set by the super platform for users, the effect of which only applies to internal users; the latter manifests as the super platform's technical support to the state, such as providing technical support and assistance to investigative agencies in complex criminal cases like telecommunications fraud. Both forms constitute the operational structure of "platform-managed users," but both are under the overarching constraint of "state-managed platforms," giving rise to two different models of cybercrime governance. One is an emergency-based governance model triggered by events, where the state intervenes swiftly through special operations and other means when a highly publicized emergency occurs in cyberspace, leveraging the technological capabilities of super-platforms to conduct concentrated rectification. The other is a routine governance model based on regulations, emphasizing close collaboration between the state and platforms, implementing tiered management and precise monitoring of users. Simultaneously, the "state-managed platform" governance must rely on national regulations reflecting the government's will. These regulations can be dispersed across different legal provisions or systematically established within domain-specific laws.

To promote the orderly advancement of platform technology governance and prevent its misuse, the state needs to pre-define the legitimate boundaries of the exercise of super-platform crime governance power at the institutional level, namely, constructing two categories of exemptions: "legally permitted" and "government mandated," creating a "safe zone" for the exercise of technological power. Then, power can be directly supervised and controlled through review mechanisms, such as mandating platforms to disclose information in advance through algorithm registration and setting information retention periods for post-event verification by relevant government departments. Meanwhile, in a highly technological environment, the state should not directly intervene in every matter, but rather use legislation to define platform obligations, taking a backseat and playing a guiding role, encouraging platforms to transform abstract legal norms into concrete platform rules, forming a structured governance system of "norms—rules—codes".

Keywords: Gatekeepers; Technical support and assistance; Domain legislation; Affordable technology; Network ecosystem governance

[责任编辑:苏　捷]