

走向“看门人规制”的网络犯罪治理

单 勇

在改革开放的前三十年，受城镇化进程负效应的影响，以盗窃为代表的流动人口犯罪是彼时第一大犯罪类型。

近十年来，随着我国步入数字化时代，网络诈骗、网络赌博、帮助信息网络犯罪活动罪（以下简称“帮信罪”）等违法犯罪的立案数大幅增加。2020年，诈骗立案数首次超过盗窃，成为公安机关刑事立案阶段的第一大罪。传统犯罪与网络犯罪此消彼长的犯罪分层愈发凸显，从“城市吸引犯罪”到“网络吸引犯罪”的变迁已然形成。

传统刑事规制模式的局限反思

应对新型网络犯罪的传统模式可归结为刑事规制。刑事规制是在刑事法框架下以政法部门统揽为组织形式、以事件性治理（个案处遇）为规制方式、以事后回应为导向的犯罪治理模式。相对前端防范导向的“反电诈法”等预防性法律制度，刑法主要是在犯罪发生后为惩治犯罪提供依据，故而“事后法”色彩和“回应型法”属性鲜明，故而刑事规制虽卓有成效，但在治理中也暴露出明显的局限。

第一，刑事规制所能规制的案件数量相对犯罪总量甚为有限。司法漏斗效应表明，受犯罪黑数影响，真实犯罪数量远高于公安立案数；受破案能力制约，公安侦查的立案数远高于移送检察院的案件数；在刑事诉讼分流下，检察机关办案量高于移送法院审理的案件数。2021年，公安机关刑事立案诈骗案件195万件，而检察机关当年起诉诈骗案件人数仅为11万人。海量的犯罪黑数和较低的破案率意味着刑事规制仅能将有限的案件纳入司法流程，对更多的网络犯罪力有未逮。

第二，刑事规制的预防效果不显。从实践看，无论如何强调预防，以个案处遇为基础的刑事规制具有明显的事后性和被动性，易陷入治标不治本的窘境。网络犯罪依附于庞大的网络黑灰产业。完整的网络黑灰产业包括上游的提供信息类物料和工具类物料环节、中游的网络诈骗及网络赌博等犯罪实施环节、下游的转移赃款及掩饰隐瞒犯罪所得等洗钱环节。2021年检察机关起诉“帮信罪”129297人，起诉人数在全部案件中排名第三。从立法目的看，帮信罪系堵截性罪名，该罪名的大幅适用，对网络黑灰产业的全链路治理与源头治理的效果并不理想。

第三，刑事规制的治理主体单一。事后回应为主的刑事规制依赖政法部门统揽的组织安排、执法和司法的程序安排而运行。以往，公安机关以数字技术实现对现实空间中接触性犯罪的“在场控制”，但该策略无法复制到网络空间。从事网络犯罪的不法分子依附于各大平台生态系统，形

- 相对前端防范导向的“反电诈法”等预防性法律制度，刑法主要是在犯罪发生后为惩治犯罪提供依据，故而刑事规制所能规制的案件数量相对犯罪总量甚为有限，预防效果不显，治理主体单一。
- 平台兼具市场属性与公共属性，成为重塑社会结构的新型规制者和控制网络空间、约束用户守法的“看门人”。“看门人规则”并非明确现于某部法律的条文字面，而是对一揽子看门人义务规范之制度内核的法理凝练。
- 看门人义务在本质上是一种阻却用户在线违规违法的风险控制义务，其义务的实现高度依赖于看门人社会权力的行使。合理地组织对网络犯罪的反应包括刑事规制和看门人规制两种并行不悖、互补互促的治理模式。

成了庞大人员基数的黑灰产犯罪圈层。黑产犯罪是一种在线犯罪，故而须臾离不开“在线控制”；擅长“在场控制”的政法部门缺乏“在线控制”网络空间的有效途径。这一困局迫切呼唤国家和社会开展分工、合作，引入新型社会力量开展“在线控制”，以形成全新的数字社会治理架构和全社会反诈新格局。

数字看门人的崛起与看门人规则的立法创设

面对前述治理困局，我国的犯罪治理模式发生重大转型。数字时代，以互联网平台为代表的网络服务提供者进化为整个社会须臾不可替代的数字基础设施，以数字在场方式吸纳最广泛的人群成为其用户，渗透至社会的核心，重塑着国民生活的社会结构。平台兼具市场属性与公共属性，成为重塑社会结构的新型规制者和控制网络空间、约束用户守法的“看门人”（gatekeeper），构成科层国家必须整合以及联合的新兴社会力量。由此，“国家管平台，平台管用户”的策略勃兴，以互联网平台为代表的相关市场主体开始承担监管用户违法犯罪的治理责任，数字看门人作为新型治理主体登上历史舞台。

从规范视角看，平台对用户的在线控制是基于看门人规则的法律规制。从法律渊源看，看门人规则既散见于网络法的丰富规范之中，还被《反电诈法》系统化设定。从法律性质看，看门人规则以义务性规范为主，国家通过看门人规则为平台设定愈发丰富的看门人义务（平台义务），义务履行的实质在于平台对用户的在线控制。“看门人规则”并非明确现于某部法律的条文字面，而是对一揽子看门人义务规范之制度内核的法理凝练，是对义务规范所孕育的全新在线控制架构的制度表达。从规范文本的创设看，看门人规则的法律渊源主要包括如下两个方面：

1. 看门人规则根植于网络法规范的分散性规定

看门人规则根植于网络法的土壤，初见于2000年制定、2009年修正的《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》，该决定第七项要求，从事互联网业务的单位要依法开展活动，发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告。“从事互联网业务的单位”系初代看门人，该决定可视为看门人规则的制度源头。2012年通过的《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》以第四至第六项为“网络服务提供者”设定保障个人信息安全、加强对用户发布信息的管理和用户实名认证的看门人义务。

2017年施行的《网络安全法》为网络运营者设定网络安全保护义务、对侦查犯罪的技术支持和协助执法义务、对用户发布信息的管理义务。2020年3月施行的《网络信息内容生态治理规定》第十条规定，“网络信息内容服务平台不得传播本规定第六条规定的信息，应当防范和抵制传播本规定第七条规定的信息。”该条款要求平台加强内容治理，防范违法信息和不良信息传播。2022年3月施行的《互联网信息服务算法推荐管理规定》为算法推荐服务提供者设定建立用于识别违法和不良信息的黑样本库、处置违法信息、对老年人的反诈被害预防、对未成年人的网络保护等义务要求。2023年1月施行的《互联网信息服务深度合成管理规定》对深度合成服务提供者设定了一系列的信息安全主体责任和深度合成内容审核义务。

2. 看门人规则依托于以“反电诈法”为代表的社会治理法

“反电诈法”是针对电信网络诈骗的犯罪治理法。与刑事规制的事后回应不同，该法案发展出一套针对犯罪信息链、资金链、人员链、技术链等关键环节的预防性法律制度，确立了预防导向的看门人规制模式，将电信业务经营者、银行业金融机构和非银行支付机构、互联网服务提供者设定为在线控制的看门人，分电信治理、金融治理、互联网治理三个领域为之设置详细的反诈义务。该法案明确了国务院及地方政府组织领导、公安部门牵头负责、行业主管部门开展行业监管、互联网服务提供者等市场主体承担具体的风险防控责任的治理分工，形塑出的“国家管看门人，看门人管用户”的双层治理体系，

即政府监管部门支持、引导、监督看门人履行反诈控制义务，看门人在线控制用户。

“反电诈法”对看门人规则进行了体系性设定。第一，通过市场主体的引入，将基于刑事规制的外部治理转化为基于看门人规制的内部治理。因不法分子实施违法活动须借助特定产业或平台的用户身份。引入电信、金融及互联网产业的市场主体，依靠市场主体对其服务用户的内部风控，将电信诈骗治理从外部治理转换为内部治理，从而大大缩短了电信诈骗的治理距离。第二，看门人的在线控制聚焦于电诈的信息链、资金链、技术链、人员链，由此构筑起前端防范的制度基础。第三，看门人的在线控制以反制技术措施为基本手段，发展出大数据反诈的技术治理体系。

看门人规制的法治实现路径

在“国家管看门人，看门人管用户”的双层结构下，“国家管看门人”表现为国家主导的看门人规则的制定，即国家通过看门人规则为平台等主体设定在线控制用户的一揽子义务；“看门人管用户”表现为市场主体主导的看门人规则的适用，即各类看门人在义务履行过程中对其用户违规违法的影响、干预、控制。看门人义务的履行同时意味着看门人对用户的实质性影响和控制，这种影响和控制既非公权力，也非私权利，而是一种社会权力。

看门人义务在本质上是一种阻却用户在线违规违法的风险控制义务，其义务的实现高度依赖于看门人社会权力的行使。看门人义务既是一种积极保护义务，要求看门人在自身的平台生态系统内积极作为，主动控制和积极响应监管部门的控制指令，以保障用户的权利和平台秩序不受违法犯罪侵害；同时也是一种强制性义务，要求看门人依循特定规则开展治理，如若违反强制性义务则要承担法律责任，“反电诈法”为此提供详细的追责依据；更是一种综合性义务，全面涵盖各类义务类型。看门人义务的履行和实现表现为看门人以在线控制用户的方式行使社会权力的过程。

值得注意的是，合理地组织对网络犯罪的反应包括刑事规制和看门人规制两种并行不悖、互补互促的治理模式。看门人规制有效弥补了刑事规制的诸多局限，依据刑事法之外的看门人规则，为相关市场主体设定了愈发丰富的看门人义务，将其作为犯罪治理的第一道防线，搭建起前端防范导向的“国家管看门人，看门人管用户”的双层治理体系，成为改善犯罪治理之国家能力的关键所在。

（作者系南京大学法学院教授、博导）



扫描左侧二维码关注