

# 网络平台犯意的算法证明

何家弘 谢君泽

**[摘要]** 在网络平台犯罪中，主体的犯意往往是司法证明的难题，而通过算法去进行证明则是可行路径。算法是一种特定化的行为工具，能够在一定程度上反映行为人的意志。算法鉴定可以通过“白盒”等功能评价方法对行为人的意志进行判断。算法推定则是依据算法所包含的时间、范围、主体、数据、事件等特定技术规则与行为人意志的伴生关系或常态联系而设立的司法证明规则。

**[关键词]** 网络平台；犯意；算法；推定

在网络信息环境下，行为主体具有网络用户与网络平台的二元化特征。<sup>①</sup>“网络用户是访问并使用网络资源的需求方，网络平台是为网络用户提供资源交换、承担组织调度角色的纽带性组织。”<sup>②</sup>“网络平台是网络信息传播的中枢，因为其实现了信息的搜集、储存、分析和发布等工作的一体化。”<sup>③</sup>从行为方式来看，网络用户主要是以网页“点击”方式<sup>④</sup>来达到生活需求目的，而网络平台往往是以信息系统的“算法”运行来达到服务或生产目的。网络平台要与网络用户实施数据交换行为，首先要设计数据交换的技术规则并以算法形式表达在相关的软件、程序或代码之中，其次要将包含算法及技术规则的软件、程序或代码部署到服务器等电子设备之中，最后通过算法及技术规则对数据交换的自动处理来实施服务或生产行为。就网络平台而言，服务器等电子设备仅是形式意义上的行为工具，而以算法为核心的软件、程序、代码才是实质意义上的行为工具。简言之，算法是网络信息行为工具的核心。

网络平台在开展服务或生产过程中可能涉嫌犯罪，成为犯罪的主体。这属于法人犯罪的范畴，或者如我国刑法所称的“单位犯罪”。网络平台对其实施的犯罪行为也要承担刑事责任，譬如2016年被判传播淫秽物品牟利罪的快播公司。正如陈兴良教授所言：“法人作为一个独立实体，具有其

---

作者：何家弘，中国人民大学法学院教授，hjihong@126.com；谢君泽，中国人民大学法学院博士研究生，junzexie@188.com。

\* 本文系河北省重点研发计划“‘廉洁雄安’智能监督关键技术研究及应用”示范项目（20310106D）阶段性成果。

① 在21世纪，“公司+雇员”这一基本结构的空空间已逐渐受到“平台+个人”这一结构的挤压。换言之，“互联网平台+海量个人”正在成为全新且显著的商业组织形式。参见宋斐：《未来商业组织不再是“公司+雇员”，而是“平台+个人”》，参见<http://www.iwshang.com/Post/Default/Index/pid/242534.html>。

② 谢君泽：《网络平台的法律责任界定——兼评“快播”案与百度贴吧事件》，载《中国信息安全》，2016（2）。

③ 王利明：《论互联网立法的重点问题》，载《法律科学（西北政法大学学报）》，2016（5）。

④ 一般情况下，网络用户不会直接涉及算法问题，除非他采取网络入侵等非正当方式访问网络平台，此时才有可能涉及恶意程序、恶意代码或相关软件中所蕴含的算法问题。

利益追求与行动目的，法人成员在这一范围内的活动应视为法人行为，因而对法人犯罪追究刑事责任是理所当然的，符合刑法原理。”<sup>①</sup>

在此类案件的审判中，网络平台的犯意往往是证明的难题。所谓犯意，就是犯罪的意图，主要包括犯罪的故意、明知等主观心理状态。犯意是英美刑法中的犯罪要件之一，近似于我国传统刑法理论中的犯罪主观要件或主观方面，但是一般认为其不包括疏忽大意的过失。<sup>②</sup>我们在讨论网络平台犯罪时使用犯意一词可能比主观要件更为合适，因为网络平台犯罪的主观状态一般不包括过失。顺便说明一下，我们赞成法人犯罪的主观方面不包括过失的观点。<sup>③</sup>

从理论上讲，网络平台的犯意可以通过行为、行为人、行为工具这三条路径进行证明。第一条路径是从网络平台所实施的具体行为本身去认定其主观状态，例如，通过侦查实验获得的证据或网络用户的证言认定网络平台的具体非法行为，据此推断出其主观状态。由于侦查实验受网络环境的限制可能取证不能，证人数量太多太广也会导致取证难，所以这条路径往往不太顺畅。第二条路径属于传统的证明方法，主要通过言词证据来证明网络平台的设计人员、管理人员、经营人员等自然人的主观状态。然而，网络平台一般由公司企业或单位运营，其决策往往是集体意志的体现，司法人员不能简单地把某个人的主观意愿作为平台的集体意志来定罪处罚，因此这条路径可能也很曲折。第三条路径是通过网络平台所使用的软件、程序或代码所包含的算法及技术规则来证明其犯意。与普通工具不同，算法是一种特定化的行为工具，是一系列技术规则的集合与表达。当行为人通过设计并使用特定化的算法去实施具体行为时，这种算法就在一定程度上隐含了行为人（自然人或法人）的主观目的和意志。诚然，通过算法去证明网络平台的犯意并非易事，但这正是我们在本文中所要讨论的主题。

## 一、网络平台犯意的证明难题

2016年，快播公司及其管理人员涉嫌传播淫秽物品牟利罪一案（以下简称快播案）在社会上产生了广泛影响，也引起了法学界的极大关注。该案的审判过程揭示了网络平台犯意的证明难题。作为一种网络平台，快播案的特殊性在于缓存算法在业务行为中的介入。陈兴良教授指出，“利用缓存技术为传播淫秽物品提供缓存服务，这部分行为无疑与快播公司的缓存技术存在较大的关联性，对于这种行为性质的理解困难，会存在一定的分歧。”<sup>④</sup>周光权教授也认为，“缓存是本案的核心行为。”<sup>⑤</sup>作为一种技术方案，缓存是以算法的形式将各种技术规则部署在调度服务器以实现网络传输的加速响应。<sup>⑥</sup>因而，缓存算法又可以称为调度算法或缓存调度算法。对淫秽视频传播而言，快播公司就是通过缓存调度服务器所部署的算法而自动实施的行为<sup>⑦</sup>，即以算法为工具的行为，简称为算法行为。

①③ 陈兴良：《本体刑法学》，569-570、574-575页，北京，商务印书馆，2001。

② 高铭暄、王作富、曹子丹主编：《中华法学大辞典·刑法学卷》，125-126页，北京，中国检察出版社，1996。

④ 陈兴良：《快播案一审判决的刑法教义学评判》，载《中外法学》，2017（1）。

⑤ 周光权：《犯罪支配还是义务违反》，载《中外法学》2017（1）。

⑥ 刘永卫、唐新春、刘戊开、陈谦：《基于缓存区段的P2P流媒体调度算法》，载《计算机工程与科学》，2008（6）；郑凯：《一种P2P VOD系统的缓存部署及调度机制》，载《华南师范大学学报》（自然科学版），2009（2）；曾文烽、许胤龙：《采用分区缓存调度策略的P2P点播系统》，载《计算机工程》，2010（9）。

⑦ 快播公司通过免费提供QSI（QVOD Server Install，即QVOD资源服务器程序）和QVOD Player（即快播播放器程序或客户端程序）的方式，为网络用户提供网络视频服务。为提高热点视频下载速度，快播公司搭建了以缓存调度服务器为核心的平台，通过自有或与运营商合作的方式，在全国各地不同运营商处设置缓存服务器1000余台。在视频文件点播次数达到一定标准后，缓存调度服务器即指令处于适当位置的缓存服务器抓取、存储该视频文件。当用户再次点播该视频时，若下载速度慢，缓存调度服务器就会提供最佳路径，供用户建立链接，向缓存服务器调取该视频，提高用户下载速度。缓存服务器方便、加速了淫秽视频的下載和传播。

由于缓存算法的介入，法律界对快播公司的犯罪定性产生了较大的争议，其中就包括犯罪故意的证明与认定。就快播公司被诉的传播淫秽物品牟利罪而言，其典型的犯意形态一般是直接故意而非间接故意。从逻辑上讲，法院应该首先讨论快播公司对淫秽视频的传播是否具有直接故意，即快播公司是否“明知”自己行为的危害结果而且还持追求或希望态度。

关于是否“明知”的问题，法院认为：“本案并不要求各被告人对于快播公司缓存服务器在调度服务器的支配下传播淫秽视频的具体方法、技术具有认知，只要求各被告人对于快播公司传播淫秽视频这一基本事实具有明知即可。”<sup>①</sup>显然，法院在该案中所认定的“明知”是一种概括性认识。概括性认识是一种“可能知道”，“可能知道”不等于“明确知道”。概括性认识这一概念最初使用在毒品犯罪案件中，它的具体含义是：“在运输毒品案件中，只要能够证明嫌疑人、被告人对运输物品的非法性具有概括性认识，不需证明行为人明确认识行为对象为毒品，即可认定成立犯罪。”<sup>②</sup>作为一种“抽象”的明知而非“具体”的明知，概括性认识在一定程度上降低了明知的证明标准。

诚然，且不论概括性认识的正当性如何，这一认定方式缓解了“明知”的证明困难，但它并没有解决快播公司对于淫秽视频的传播是否持主观上的追求或希望态度这一问题。<sup>③</sup>笔者注意到，在该案中，司法人员曾试图运用两种方法来解决这个问题，即行为类比和技术鉴定，但最终都没有成功。

北京市海淀区人民法院副院长范君认为，快播公司的行为属于针对“不法”视频资源的“有意识的主动行为”。理由如下：一是快播的缓存服务器偏好“不法”的视频资源，除了淫秽视频和侵权视频，其他视频屈指可数。二是快播公司的中心调度服务器一旦发现用户下载速度不能满足观看需要，就会通过缓存调度服务器指令最便利（同一运营商或距离最近）的缓存服务器直接向用户提供视频文件。<sup>④</sup>如果范君法官的观点是可以成立的，那么“有意识的主动行为”之“主动”应该倾向于是一种直接追求的希望态度，即直接故意。

然而，范君法官的论证存在着司法人员对技术事实的误解。一方面，调度服务器是一种算法行为，算法行为应当理解为通过技术自动实现的通常性业务行为。调度服务器根据缓存调度算法自动化运算处理，它只能根据技术规则的设置决定哪些视频资源需要缓存技术的介入而加速响应，并不会区分这些视频资源哪些是非法的、哪些是合法的。快播公司的主观意愿并不能直接参与具体数据的处理，而只能影响缓存调度算法的设计。“这不能等同于快播公司从主观上直接参与了具体非法视频的处置，更不能简单认定快播公司对‘所有’非法视频具有主观故意。”<sup>⑤</sup>如果把缓存算法行为看作是专门针对“不法”视频资源的“有意识的主动行为”，那么其实是将缓存算法调度服务器与汽车客运调度中心<sup>⑥</sup>等传统事物进行了行为效果上的类比思考。另一方面，以缓存服务器中留存“不法”视频资源的数量特征来反推行为意图，这对于网络缓存而言不具有合理性。从某种意义上讲，这是以行为效果反推行为性质，容易走入客观归罪的误区。网络缓存是为了解决突发大量访问而提出的技术方案，淫秽视频等最可能触发缓存算法的运行，正常视频反而不容易触发缓存算法的运行。也就是说，淫秽视频等大量留存在缓存服务器而正常视频反而少留存，这在技术上是完全正

① 北京市海淀区人民法院刑事判决书（2015）海刑初字第512号。

② 褚福民：《证明困难解决体系视野下的刑事推定》，载《政法论坛》，2011（6）。

③ 网络平台上非法内容的用户投诉或监管部门警告，也可以在一定程度上反映网络平台的主观犯意。但是，用户投诉或监管部门警告往往只是针对某个或某些特定的非法内容而做出，并不能反映网络平台的整体算法意志，因此只能用于证明网络平台部分特定行为的犯意，或者作为证明网络平台整体算法意志的佐证。

④ 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（1）。

⑤ 吴沈括、何露婷：《网络缓存的法律认定及其规制——以快播案为分析视角》，载《财经法学》，2019（5）。

⑥ 汽车客运调度中心是通过自然人的操作对车辆和乘客进行调度，操作人员的主观意志与意识都能参与其中。

常的。快播公司的缓存服务器就犹如公司记账，假设一个公司主要经营合法业务并存在少量非法业务，该公司对合法业务不记账对非法业务记账，最终不能因为查扣的账本中全是非法业务记录而武断声称该公司主要是为了经营非法业务，并将其认定为单位犯罪。这是因为，查扣的非法业务记录不能有效反映整个业务状态，更遑论完整的目的意图。同理，缓存服务器所留存的“不法”视频资源也不能有效反映快播公司的行为性质。

以行为效果反推行为性质是一种常见的法律思维。由于认知的局限性，相较于通过技术原理或本质的演绎来理解事物，法律界人士更擅于通过法律现象或效果的归纳来认识事物。然而，在新兴科学技术面前，这种思维惯性不仅不能有效解决证明问题，而且还潜伏着认知偏离的风险。

在快播案中，法院曾试图借助于司法鉴定机构的技术力量来解决网络缓存的行为定性问题。法院在委托司法鉴定机构对4台服务器进行鉴定时，其中第三项请求为：“结合在案证据及4台服务器的存储内容，从技术角度分析快播软件对于淫秽视频的抓取、转换、存储、搜索、下载等行为的作用及效果。”鉴定机构的意见为：“四台送检服务器不是完整的快播系统平台，根据现有存储数据内容不足以从技术角度分析快播软件对于视频的抓取、转换、存储、搜索、下载等行为的作用及效果。”<sup>①</sup>这种鉴定犹如司法人员通过侦查实验的方式对服务器在扣押之前的行为效果进行取证与证明。且不论该案中服务器并非完整而无法鉴定，即使可以鉴定也不能得出相应的判断。法院委托的鉴定请求与范君法官的思维方式是一样的，即：希望通过行为效果来判断网络缓存的行为性质及背后意图。但是，如前所述，通过行为效果并不能有效反映快播公司的行为性质。

法院最终没有认定直接故意，转而认定“可能知道”的间接故意，即：快播公司是对他人传播行为及传播后果的放任。<sup>②</sup>然而，笔者认为，如果快播案的鉴定请求得当、技术方法正确，快播公司的犯罪意图是可以查清的。算法是解题方案的准确而完整的描述，以及用系统的方法描述解决问题的策略机制，它是一系列解决问题的清晰指令。算法在任何地方的设计都有它特定的目的与功能，任何细节的错误几乎都是不可容忍的。因而，算法是一种特定性非常强的行为工具，其中所表达的技术规则处处隐含着设计者的目的与意图。在网络环境与业务场景足够明确的情况下，司法人员完全可能并可以通过分析算法及其所蕴含的技术规则直接做出行为意图的判断。这便是算法证明所要研究的问题。

## 二、网络平台犯意的算法鉴定

算法是一种信息技术，算法行为则是信息技术与人的行为相结合的产物。根据事物的对称性，算法及算法行为的认识也必定要借助于信息技术。在我国现行司法体制下，信息技术对司法认识的帮助主要表现为司法鉴定形式。以下主要讨论如何从技术鉴定<sup>③</sup>的视角展开算法证明。

在过去，涉及算法的技术鉴定主要发生在网络用户即个人所实施的网络入侵或恶意程序犯罪案件之中。比如，在温州“八·一”广电案中，温州有线电视网络系统机顶盒遭黑客攻击，出现一些反动宣传内容。在该案的侦查鉴定过程中，技术人员就需要对42段涉案程序代码进行技术解读，

<sup>①</sup> 国家信息中心电子数据司法鉴定中心电子数据司法鉴定意见书（2016）电鉴字第2号。

<sup>②</sup> 快播案判决书指出，缓存服务器介入视频传播中，快播公司在主观上并没有对视频内容进行选择，而只是根据视频热度提供加速服务。也就是说，缓存服务器介入传播何种内容的视频，不是快播公司主观意志选择的结果，而是对他人传播行为的放任，对他人利用自己技术服务传播淫秽视频的放任，对自己的缓存服务器介入到淫秽视频传播行为之中的放任，对自己的行为造成淫秽视频在网络上大量传播的放任。参见北京市海淀区人民法院刑事判决书（2015）海刑初字第512号。

<sup>③</sup> 这里的技术鉴定可以做广义理解，即：如果在专家辅助人、勘验检查笔录甚至证人证言等证据形式中涉及算法的技术分析与鉴别，也可按此处理。

从而推断出技术入侵的行为过程。<sup>①</sup>再如，在DDos攻击案件中，技术人员往往要对相关的恶意程序代码进行技术分析，从而判断恶意程序代码的功能。就司法实务而言，虽然这类案件也涉及程序代码所内含算法的技术鉴定，但它们往往更关注算法整体（即程序代码）的功能及作用，而对算法本身的内部结构并无特别要求。因而，在这类案件的技术鉴定中，既可以仅仅对算法整体（即程序代码）的外部功能及效果进行分析，也可以进一步对算法的内部结构进行深入解读。

其实，这种技术鉴定也可以运用到网络平台的算法鉴定之中。算法鉴定在技术方法上有“黑盒”法与“白盒”法之分。“黑盒”与“白盒”都是软件测试的技术术语，“黑盒”法与“白盒”法是软件测试方法在技术鉴定领域的援引。二者在技术原理及证明作用上均有所不同。

“黑盒”法，又称黑盒测试法，它是在不知道算法的内部结构与实现逻辑的情况下对算法的行为效果进行功能测试。在软件测试领域，黑盒测试又称功能测试、数据驱动测试或基于规格说明书的测试，它是一种从用户观点出发的测试。“测试人员把被测程序当作一个黑盒子。它是已知产品所应具有的功能，通过测试来检测每个功能是否都能够正常使用。在测试时，在完全不考虑程序内部结构与内部特性的情况下，测试者在程序接口进行测试。”<sup>②</sup>在技术鉴定中，黑盒测试一般只关心算法的输入与输出效果，不关心算法本身的内部结构与实现逻辑。当人们将算法作为一种行为工具时，算法的输入输出效果即算法行为的效果。

“白盒”法，即白盒测试法，则是通过对算法在内部结构与实现逻辑上的技术解读来达到功能评价的目的。在软件测试领域，白盒测试也称结构测试或逻辑驱动测试。“它是知道产品内部工作过程，可通过测试来检测产品内部动作是否按照规格说明书的规定去正常进行，按照程序内部的结构测试程序，来检验程序中的每条通路是否都能按预定要求正确工作，而不管它的功能是怎样的。”<sup>③</sup>在技术鉴定中，白盒测试一般无需展示软件的具体功能效果，而是由技术人员通过算法的技术解读去理解和认识它的设计目的与实现功能。当理解了算法设计的目的与功能时，自然就能够理解算法行为的目的与意图。

从技术原理来看，“黑盒”法与“白盒”法都可以实现算法的功能鉴定，但是，对于目的意图的证明而言，这两种鉴定方法的作用则有所不同。具体而言，由于“黑盒”法没有对算法的内部结构与实现逻辑进行分析，因而是无法通过算法本身推断目的意图的，“白盒”法则可以。在严格意义上讲，在个人所实施的网路入侵或恶意程序犯罪案件中，通过算法整体（即程序代码）的功能来判断行为的过程及意图，这并不是真正的算法鉴定，而只是程序鉴定。

当然，司法领域的算法鉴定毕竟不同于技术领域的软件测试。算法鉴定不仅要像软件测试那样对算法本身的内部结构与实现逻辑进行分析，还要对算法的形成过程进行全面分析。算法的形成过程分析，不仅包括算法在各个版本升级过程中的变化，还包括算法在生成过程中设计者、管理者、运营者的知情及决策情况。前者往往反映算法意志的变化过程，后者往往反映算法意志的合意过程。作为网络平台的行爲工具，算法一般是由集体组织合意形成，但是，在某些特殊情况下，算法也可能是个别算法设计师或开发工程师的个人意志行为。例如，某互联网企业的开发工程师在其负责设计的软件产品算法中私自嵌入“后门”，就属于其个人的犯意行为。

回到快播案来看，该案的犯意证明可以通过算法证明来解决，而且应当采用“白盒”法而非“黑盒”法。快播案希望鉴定机构通过服务器的检验判断快播平台的行为作用及效果，这是关注算法的输入输出效果，而不是要真正搞清楚算法的内部结构与实现逻辑。也就是说，快播案在技术鉴定时选择了“黑盒”法的思路，这是错误的。

<sup>①</sup> 中国人民大学物证技术鉴定中心司法鉴定检验报告书（2014）技鉴字第36号。

<sup>②③</sup> 胡静：《浅析黑盒测试与白盒测试》，载《衡水学院学报》，2008（1）。

值得说明的是,快播案的技术鉴定不应仅限于视频的缓存算法,还应当对相关的内容推荐、用户管理乃至广告策略等算法进行分析或鉴定。换言之,上述各种算法之中都采取了哪些技术规则以及它们有何功能与目的,这些都能从一定程度上反映快播公司的犯意。比如,视频缓存算法中是否存在处理淫秽视频的专门技术规则,从而使淫秽视频更广泛地传播?内容推荐算法是否针对白天与夜间的时间不同而采取差异化的技术规则,从而使夜间脱离监管的淫秽视频更易传播?快播公司是否给特定类型的用户(如男性成年人)设置了特别的技术管理规则,使之更易访问淫秽视频?等等。从算法的技术实践来看,根据数据类型、行为时间、用户特征等相关条件来设置特殊的技术规则,这在淫秽视频或非法广告类案件中广泛存在。也就是说,如果算法中存在这些特殊技术规则的设置,那么它们就能够用于认定网络平台的非法目的与行为意图。

诚然,算法规则的认定有赖于技术鉴定,但是算法规则能否证明网络平台的犯意往往还需要一个推理的过程。在推理过程中,有些算法规则与平台犯意之间的联系是偶然的,有些联系则是常态的。如前所述,淫秽视频或非法广告类案件中就经常会有一些针对数据类型、行为时间、用户特征等相关条件的算法规则设计,而这种常态联系或伴生关系就可以作为推定的逻辑基础。

### 三、网络平台犯意的算法推定

作为一个法律术语,推定是由法律规定并由司法人员做出的具有推断性质的事实认定。这包括三层含义:第一,推定是对未知案件事实或争议事实的认定;第二,推定是以推理为桥梁的对未知事实的间接认定;第三,推定是关于这种事实认定的法律规则。推定规则的基本功能是要规范司法人员在认定案件事实中的推断行为,以保证司法裁判的正确、公正和效率。<sup>①</sup>

推定规则的表现形式是以一定的事实为基础,然后根据客观事物之间联系的规律推导出另一事实的存在。在此,前一个事实称为“基础事实”或“前提事实”(A);后一个事实称为“推定事实”或“结果事实”(B);而推理就是连接这两个事实(A和B)的认识桥梁。推定的依据一般是基础事实(A)与推定事实(B)之间的伴生关系或常态联系。一般来说,这种关系或联系并不具有必然性,并不是有A就一定有B,而只具有一定的盖然性,即有A就可能有B。作为设立推定规则的标准,我们应该要求这种关系或联系具有较高的盖然性,即有A就很可能有B。

由于推定都是以法律规定为依据的,因此在司法活动中运用推定方法认定案件事实就表现为对“推定规则”的适用。设立推定规则有两种基本模式:其一是由立法者在有关法律中明确规定的推定规则;其二是由司法者通过解释法律和创设判例等方式确立的推定规则。前者可以简称为“立法推定”;后者可以简称为“司法推定”。<sup>②</sup>推定规则的制定既需要理论研究的引领,也需要实践经验的支撑。在此,我们建议最高人民法院和最高人民检察院通过司法解释或指导性案例的形式,制定网络平台犯意的算法推定规则如下。

#### (一) 目的推定规则

所谓目的推定,是指在刑事诉讼被告人是否具有“犯罪目的”的情况不够明确的时候,根据一定的基础事实来确认其具有犯罪目的的推定。我们建议制定网络平台犯罪目的的算法推定规则如下:

算法的技术规则具有以下情形时,可以推定网络平台具有实施犯罪行为的目的:(1)按照特定数据改变技术规则,使该特定数据更大可能成为非法行为的中介,如对淫秽视频、盗版视频等加速缓存或加速传播;(2)按照特定时间改变技术规则,使该特定时间内非法网络信息行为大量增加,

<sup>①</sup> 何家弘:《论推定概念的界定标准》,载《法学》,2008(10)。

<sup>②</sup> 何家弘:《从自然推定到人造推定——关于推定范畴的反思》,载《法学研究》,2008(4)。

如通过白天和黑夜的算法设置不同，使夜间可以访问淫秽视频或非法广告等；（3）按照特定主体改变技术规则，使该特定主体具有开展非法网络信息行为的便利，如对收费客户或高等级客户提供更大范围的盗版图书等；（4）按照特定范围改变技术规则，使该特定范围内非法网络信息行为大量增加，如通过境外 IP 地址与境内 IP 地址的算法设置不同，使服务器差异性提供网络赌博或网络色情等服务；（5）按照特定主题内容、关键词等改变技术规则，使特定事件所造成的影响更为恶劣，如对造谣传谣内容进行推荐或转发。

不同网络平台的业务模式有所不同，不同业务模式背后的技术方案有所不同，因此推定规则的适用也有所不同。例如，在快播案中就可以根据上述第（1）（2）（3）条规定的情形推定快播公司具有犯罪故意。

## （二）明知推定规则

所谓明知推定，是指在刑事诉讼被告人对某些犯罪构成要件的主观认知状态不够明确的情况下，根据一定的基础事实来确认其明知的推定。如前所述，当算法包含对某些非法行为进行回应的技术规则时，它可以反映行为人的意识状态。据此，我们建议制定网络平台明知的算法推定规则如下：

算法的技术规则具有以下情形时，可以推定网络平台对相应的具体犯罪行为是明知的：（1）针对某类非法数据进行技术规则回应，如通过设立不良信息过滤系统等进行管控；（2）针对某类非法数据进行过多次技术处置，如通过指令日志发现曾对非法数据进行专门分析。

在上述情况下，网络平台应该具有犯意，因为只有主观明知的情况下才会针对非法行为做出相应的技术回应或处理。例如，前述快播公司之所以采用不良信息过滤系统的技术规则，就是因为其明知存在相应的非法行为。当网络平台存在上述情形时，这种推定的“明知”就是具体的明知，而不是抽象的概括性明知。

据央视报道，2020年6月23日，国家网信办会同相关部门对31家网络直播平台的内容和生态进行了全面巡查，其中有10家网络直播平台因为存在传播低俗内容等问题被约谈。在这些平台的直播网站中，某些主播进行色情直播，有的是直接裸露身体敏感部位，有的则是通过语音和肢体动作引诱网友打赏，还有的是白天以播放唱歌、聊天为主，但晚上10点以后直播内容就变了味。<sup>①</sup>毫无疑问，网络平台有责任对直播内容进行监管。如果平台明知甚至放纵淫秽物品的传播和销售，就要受到治安处罚，甚至要承担刑事责任。在此类案件的司法审判中，算法对网络平台的犯意证明具有重要意义。

如前所述，网络平台的犯意还可以通过行为人的陈述和行为的具体内容进行证明。显而易见，行为人的供述是证明犯意的有力证据。此外，行为人在网络上的表达记录也可以证明犯意。在网络信息行为方式下，不论个人愿意与否，其表达总会被机器及数据所记录，如对话记录和聊天记录等。如果这些记录中包含了表达主观意愿的内容，那么就为证明犯意提供了直接证据。

一般来说，行为都是人的主观意志的外在表现，因此行为本身的记录也可以反映行为人的主观状态。由于这种反映是间接的，因而它的证明效果取决于行为记录的具体性和丰富性。在网络信息环境下，通过电子设备实施的行为往往具有丰富且翔实的数据记录。电子设备由硬件系统（计算设备、网络设备、存储介质等）和软件系统（操作系统、应用程序、代码指令等）组成。网络信息行为要借助电子数据经由电子设备的操作系统、应用程序及代码指令依时序逐层运算才能完成。在这一过程中，电子设备中的静态数据和动态数据都记录了行为的内容。前者如操作系统、应用程序、

<sup>①</sup> 央视《新闻直播间》：“晚10点以后内容就变了味，直播网站仍藏色情角落”，参见 <http://news.ynet.com/2020/07/04/2706061t70.html>。

代码指令等软件数据,记录软件运行过程中所产生的日志数据,以及人所意欲传播或记录的信息数据。后者如正在内存中执行的程序指令数据、正在传输的网络中继数据,以及正在计算的实体信息数据。此外,电子设备中还存在一些时静时动的特殊数据,如账户密码、证书密钥等电子签名数据。在网络犯罪案件中,这些电子数据就是作案人遗留的“电子痕迹”,而根据这些痕迹来追溯并证明犯罪行为的方法就称为“电子痕迹溯源法”<sup>①</sup>。司法人员依据丰富的电子痕迹所还原的具体行为内容,就可以为推断网络平台犯意提供依据。

综上所述,司法人员可以在网络犯罪案件中通过行为、行为人、行为工具来证明网络平台的犯意。随着大数据和人工智能等新型科学技术的迅速发展,我们正在快步进入人类社会的智能时代。在这一历史背景下,“算法经商”正在成为现代化企业的主流生产经营方式,而借助于传统劳动力作业的生产经营方式正在被智能机器、信息系统、机器人等算法性生产经营方式所替代。许多互联网企业借助网络平台在算法智能化方面的先天优势来开展各式各样的信息服务。一些传统企业也在不断探索利用智能机器、智能系统、智能算法等方式来完成生产经营的智能化升级。无论是生产性企业还是服务性企业,当其制造的产品或提供的服务可能存在违法犯罪问题时,执法人员和司法人员在查明案件事实时就需要研究其涉及的算法规则并进行证明。例如,在无人驾驶汽车出现“失灵”致人死亡的事件中,查办案件的人员就需要对无人驾驶的算法规则进行“解剖”并证明其主观上有无犯意;在网络平台提供“非法”信息服务时,查办案件的人员则需要对网络平台的算法规则进行“解释”并进行主观犯意的认定。总之,在社会智能化和行为算法化的发展趋势下,以算法这种行为工具为视角来研究网络平台犯意的证明,具有特别重要的理论意义和实践价值。

## On Algorithm Proof for Criminal Intentions on Network Platforms

HE Jiahong, XIE Junze

(School of Law, Renmin University of China)

**Abstract:** While criminal intentions are often difficult to locate in network criminal cases, algorithm proves to be a viable way to solve this problem. Algorithm, as a specific tool, can in a certain degree calculate human will of behavior, for example, to employ the method of “white box” to measure one’s intentions. The working assumption of algorithm in identifying criminal intentions refers to a set of legal, technical rules determined by the correlations between human will of behavior and the variants of time, scope, subject, datum, event, and so forth, required by the aforementioned algorithm method.

**Key words:** Platform; Criminal intention; Algorithm; Presumption

(责任编辑 李 理)

<sup>①</sup> 电子痕迹溯源法,也称为溯源性分析或形成过程分析,它是基于电子痕迹和时序重组的分析方法。参见徐立根主编:《物证技术学》,第四版,313、319页,北京,中国人民大学出版社,2011。