

数字时代公共安全领域电子数据证据效力问题探析

郭永亮

西北政法大学公安学院 陕西 西安 710061

【摘要】：数字技术全域渗透下，公共安全治理格局被重构，电子数据已经成为公共安全案件查办的主要证据载体。相比于传统的证据，电子数据具有虚拟性、易篡改性、技术性等特点，导致电子数据取证规范及证据效力认定体系存在适配性不足的问题。本文从数字时代的公共安全执法司法实践出发，对电子数据取证以及证据效力的核心概念进行界定，分析当下电子数据证据效力认定存在的现实困境，并梳理出证据效力认定的关键标准，以此来建立一套科学完整的证据效力保障体系，从而明晰公共安全领域的电子数据取证裁判逻辑，规制取证司法适用，助力公共安全法治治理现代化进程。

【关键词】：数字时代；公共安全；电子数据取证；证据效力；司法审查

DOI:10.12417/3041-0630.26.12.036

引言

数字化转型正在深刻地改变公共安全事件发生的形式以及查办的方式，网络违法案件、新型治安案件、数字领域公共安全隐患类案件层出不穷，电子数据是还原案件事实、认定法律责任的重要依据。公共安全领域的电子数据取证不同于一般民事取证，具有公共性、强制性和技术性三个特点，电子数据的证据效力直接影响到案件办理是否合法公正。目前我国有关电子数据的相关规制体系逐步建立起来，但是在实际的操作过程中，存在取证程序不规范、效力审查标准不明晰、技术和司法对接不通畅等问题。对此，深入分析公共安全领域电子数据取证效力问题，并提出相应的解决方案，这对规范执法司法行为、守住公共安全的法治底线有着重要的现实意义。

1 公共安全领域电子数据取证及效力核心界定

1.1 电子数据取证的核心内涵

公共安全领域的电子数据取证属于具有公权力性质的专门性司法取证行为，是由法定的执法、司法机关利用专业的数字取证技术和设备按照相关规程，在公共安全治理和案件调查过程中对所产生的各种形式的数字化信息进行发现、固定、提取、检验、分析及保全的工作过程。全面涵盖常态化的公共安全监管、突发的公共安全事件处理、网络上的公共安全违规查办以及治安与刑事类的公共安全案件侦查等多种工作情景。相比于民事纠纷、商事纠纷中的普通电子数据取证而言，公共安全领域的取证行为是为了维护社会公共秩序、保障公共利益、防范化解公共安全风险而采取的具有法定强制性、公共公益性和程序严苛性的特殊取证活动，不属于一般的市场化取证服务。当前数字社会业态持续更新换代，取证客体也处在不断发展变化中，除了传统的终端设备存储的数据、网络交互的日志、

即时通信的文本及音视频数据之外，云端分布的数据、物联网设备运转的数据、动态流媒体数据以及算法推送的轨迹数据等新的数字化信息逐渐变为关键的取证对象。

1.2 电子数据证据效力的核心属性

电子数据的证据效力，指经过法定取证过程后的数字化信息成为诉讼证据时所具有的证据资格及司法证明力，是电子数据得以被司法机关采纳，并且成为裁判依据的基本法律资格，它的效力系统一方面继承了传统的法定证据的主要判断逻辑，另一方面由于数字载体自身的特殊性而产生了不同的认定标准。合法性、真实性、关联性是电子数据作为证据时效力的三个主要条件，它们彼此依靠，互相牵制，无法被分开，一起塑造出公共安全领域电子数据在司法中被认可的全面考量体系，也是司法机关进行证据考察的主要准则。其中合法性是程序性效力要件，关注取证主体资格是否合法、取证实施过程是否合法、取证手段方式是否合法、证据保管移送等全流程是否合法，是电子数据具有证据效力的前提条件，侧重于保障公权力取证行为合法开展，防止程序侵权及权力滥用^[1]。真实性是实体性效力要件，主要针对电子数据内容本身是否客观、完整、可追溯，即电子数据从生成到提交给司法机关审查的过程中没有被篡改、删除、覆盖、失真等，是电子数据可以反映案件真实情况的重要保证。关联性是电子数据证据效力的核心要件，其指电子数据与待证案件事实存在客观联系，即电子数据可以对案件事实起到证明或证伪的作用，排除与案件无关或者仅具有间接、微弱关联的材料。在公共安全案件中，主要审查电子数据所记载的内容是否指向涉案行为、涉案人员或者案件的关键时间点，并非简单地考察数据载体本身，而是关注数据信息与案件争议事实是否存在逻辑上的关联。只有当电子数据能够对案件事实产生实际影响时，才具有关联性。

作者简介：郭永亮（1974.5）男，汉，山西长治人，副教授，研究方向：侦查学，司法鉴定学。

2 公共安全领域电子数据取证效力认定的现实困境

2.1 取证程序规范性缺失引发效力瑕疵

公共安全执法工作涉及社会治理的方方面面,具有场景突发性、处置时效性、范围广泛性的特点,一线取证工作常常要迅速反应、即刻处理,所以实务当中长久以来就存在着取证程序简化、操作标准不清、流程管控缺失等状况,从而致使许多电子数据存在程序上的效力缺陷,不能通过司法审查。在常态化执法办案中,一些执法主体具有重实体、轻程序的固有思维,只重视案件查办的效率以及事实查清的结果,而忽略了电子数据取证应有的法定程序规范。对原始存储介质实施查封扣押,在对相关设备开展封存保管处理时,针对数据执行了镜像备份,并且整个取证过程做到全程记录,对操作权限进行查验等等这些关键的核心环节,时常出现操作上的遗漏状况,存在流程缺失的现象,记录也出现空白的情况,无法营造出一个可以形成完全闭合回路的取证路径,从而不能证明所提取的数据过程具有客观性和规范性^[2]。对当下广泛使用的云端存储数据、远程交互数据、跨平台传输数据等新型取证客体,现有的执法操作规范存在适配度低的问题,对于远程调取、在线取证、云端数据固定等新型取证行为缺少前置审批、过程管控、结果留存等机制,数据跨设备、跨平台、跨区域传输转化过程的程序合法性难以被证明。

2.2 数据固有特质增加效力审查难度

电子数据依靠数字网络 and 智能设备产生、储存与流传,它那生来就有的虚幻性以及无迹可寻的状态,完全把传统的证据那种静态保存方式破掉,极大地增强了司法层面对其真实性和完整性的查验困难程度,成为影响证据效用判定的主要技术壁垒。传统实物证据被改动、损坏或者遗失时会有可以察觉到的外部迹象,司法审查可以通过直接核对来确定其效力,但电子数据的修改、删除、覆盖、拼接、还原等工作都可以在后台默默执行,并且不会留下明显的物理痕迹,普通的司法审查方法很难有效地识别出数据是否被人改动或者受到技术上的扭曲。在复杂网络公共安全、群体性公共安全风险、跨区域违法犯罪等重大案件中,涉案电子数据具有体量大、类型杂、来源广、碎片化的特点,核心案件数据散落在不同的终端设备、不同的网络平台、不同的云端服务器中,多源数据互相交织、互相覆盖、互相断裂,数据整合筛选、溯源核验、链条串联难上加难,很容易出现核心证据碎片化缺位、证据链条断链的问题。

3 公共安全领域电子数据证据效力的审查标准体系

3.1 合法性审查标准

合法性审查是电子数据取得证据资格、具有司法效力的第一道门槛,是程序正义在数字证据司法审查中的集中展现,主要从取证主体、取证程序、取证手段这三个方面展开全面的司

法检验,保证公权力的取证行为始终在法律范围内进行。主体合法性审查主要针对取证实体主体的资质及权限进行审查,要求参与电子数据取证、检验、保全工作的人员必须具有法定的执法司法资质或者专业技术资格,熟悉公共安全取证相关的规范和技术标准,在法定职权范围内开展取证活动,严禁无资质人员取证、越权取证、异地违规取证等违法情形发生,从而避免因主体问题导致证据效力受损。程序合法性审查覆盖电子数据从收集到提取、封存、保管、流转、移送、归档的全流程,必须保证每个取证步骤都严格遵循法律规定及操作规程,对原始存储介质实施查封封存,开展无损镜像数据提取,完成取证过程中的笔录记录,保存操作日志,执行多级审批程序,办理证据移交时的交接手续并做好详细记载。

3.2 真实性审查标准

真实性审查是电子数据证据效力的实质要件,它直接决定了数据内容是否能客观再现公共安全案件事实,是电子数据成为定案根据的基础性支持,审查工作贯穿于数据产生、存在、流动、取证等全部环节。电子数据的真实性审查,对数据生成源头是否可靠进行审查,主要对涉案的智能终端、网络系统、云端服务器、物联网设备等数据来源载体的运行情况进行审查,确保设备运行环境良好、系统无故障、无病毒、无后台篡改程序等,防止因设备故障、系统漏洞、网络攻击、人为干预等原因造成的数据失真、数据错乱、数据丢失等问题,从源头上保证原始数据的真实性^[3]。关注数据保全及流转过程的完整情况,对电子数据从产生到取证结束、移交归档整个过程的状态进行全方位检查,查看数据是否有数字签名、哈希校验值、设备独有标记、操作记录等法定的追溯证据,准确判断数据在提取、复制、存放、传送、移交时有没有出现新的添加、删减、改动或者更换等情况,保证取证前后的数据状态完全相同。

3.3 关联性审查标准

关联性审查是判断电子数据是否具有司法证明价值的“核心标尺”,直接影响着电子数据能否成为案件中的证据,并对案件裁判起到支撑作用。其本质是对电子数据与待证的公共安全类案件事实之间是否存在实质性的逻辑联系进行识别,区分出有效的证据与无效的冗余数据。公共安全案件涉案电子数据量大、内容庞杂、冗余信息多,关联性审查要联系案件查处的核心需求,对大量数据实施精确挑选、类别分析,仔细辨别核心关联数据、辅助关联数据以及无关数据,去除没有证实价值的无用信息,集中于可以佐证案件重要事实的有效数据。

4 公共安全领域电子数据取证证据效力的完善路径

4.1 规范全流程取证程序体系

建立起标准的、规范化的、全闭环式的取证程序体系,是防范电子数据效力瑕疵从源头上解决问题的根本途径,可以很

好地应对现实中取证过程混乱、操作标准不统一、程序存在瑕疵等实际问题。立足于公共安全执法的突发性、时效性和复杂性特点,需要对取证操作进行差异化、个性化的细化,打破传统的“一刀切”的取证标准,根据本地终端存储的数据、云端分布式的数据、远程网络交互的数据、物联网设备采集的数据、流媒体动态传输的数据等不同种类的数据,制定不同的、具体的、能够落实的取证流程规范、封存标准、留存要求及操作细则,做到不同场景、不同类别取证工作有标准可依^[4]。全面提升取证全流程留痕管理,形成包含取证审批、现场取证、数据提取、介质封存、校验核验、流转交接、归档保管在内的全流程文书体系,明确取证笔录、操作日志、封存清单、校验报告、流转记录等关键文书的制作要求,使每一步取证操作都有据可依、有迹可循,做到电子数据从产生取证到进入司法程序的全程可追溯。

4.2 构建技术司法协同审查机制

技术标准与司法裁判之间的衔接壁垒成为阻碍电子数据证据效力落实的关键障碍,只有形成技术支撑与司法裁判相互联动审查的机制,才能做到技术规范同法律规则的有效结合并且双向适应。首先要搭建起专业的、智能的技术审查支撑平台,利用大数据校验、区块链溯源、数据痕迹深度检测、系统环境模拟核验这些前沿的数字技术来创建适合于公共安全案件查

办的电子数据核验体系,精确地对电子数据是否完整、真实、原始进行技术上的判断,给司法审查工作赋予客观、准确、专门的技术依照,从而改善传统司法审查时技术能力缺乏的问题^[5]。其次,形成统一的技术操作规范与司法审查标准适配体系,界定技术合规与法律有效的边界关系,对新型取证技术、新型数据形态进行专门适配研究,确定各种新型电子数据的取证技术标准、司法采信条件及效力认定规则,消除技术操作与司法裁判的标准差异,做到技术成果与司法裁判的有机衔接。

5 结语

数字治理时代全速驶来,彻底改造着公共安全事件出现形式,流传途径及查处模式,电子数据已然成为公共安全法治治理体系中必不可少的核心证据载体,其取证是否规范,效力确认是否科学,直接影响到公共安全领域执法司法活动的公正性,权威性和公信力,是推动公共安全治理体系与治理能力现代化的重要举措。以后要一直加深数字技术和公共安全法治的融合深度,秉持问题导向和目标导向相结合的原则,不断改善电子数据取证规范以及司法适用系统,精准对接数字时代公共安全治理的新需求,最大限度发挥电子数据的证据价值和治理效果,用法治化,数字化的方法守住公共安全防护底线,守护好社会公共秩序,保障人民权益,推进新时代公共安全法治创建给予有力支撑。

参考文献:

- [1] 侯柔倩,刘梓涵.数字时代跨境电子取证的现实困境与治理对策[J].郑州轻工业大学学报(社会科学版),2026,27(4):76-85.
- [2] 李庆峰,戚佳璐.弥合与转型:数字时代跨境刑事电子取证制度的再思考[J].杭州电子科技大学学报(社会科学版),2026,22(2):68-78.
- [3] 欧顺芳,陈华.基层公安机关刑事电子数据取证的问题检视与完善进路[J].北京警察学院学报,2026,(1):52-61.
- [4] 王若冰,汤建华.我国刑事跨境电子数据取证路径及程序规范[J].山西警察学院学报,2026,34(1):69-76.
- [5] 韩希霖.跨境网络犯罪中电子数据取证的现实困境与调适路径[J].贵州警察学院学报,2025,37(5):44-55.