大数据环境下的电子取证研究

黄少荣，陈丹
（广东司法警官职业学院，广东广州 510520）

摘 要：随着互联网技术的飞速发展，网络犯罪案件急剧上升，电子取证已经成为一个严峻的问题。近来年，在大数据环境下，电子取证面临着新的挑战，因此在大数据环境下的电子取证问题，具有重要的科学研究和实际应用价值。文章在介绍电子数据和电子取证的基础上，讨论了电子取证在大数据环境下面临的挑战，指出了大数据取证发展趋势，并提出了相应改进措施，对大数据环境下的电子取证研究做出了有益的探索。

关键词：电子数据；电子取证；大数据；云计算
中图分类号：TP393.098 **文献标识码：**A

Study of electronic forensic under big data environment

Huang Shaorong , Chen Dan
(*Guangdong Justice Police Vocational College, Guangdong Guangzhou 510520*)

Abstract: With the rapid development of internet technology, network crime is on the rise, electronic forensics issue has become very austere, especially in recent years, with the advent of the era of big data, the traditional electronic forensic faces new challenges. Therefore, the issue of electronic forensics under the environment of big data has important scientific research and practical application value. Based on introducing electronic data and electronic forensics, this paper discusses the forensic challenges under the environment of big data, put forwards the development trend of big data forensics, and some valuable suggestions is provides. It makes a beneficial exploration of electronic forensics under the environment of big data.

Key words: electronic data; electronic forensics; big data; cloud computing

1 引言

随着5G时代到来以及“互联网+行业”的数字化推进，传统行业掀起了一场数字化改革的浪潮，开启了万物互联的大数据网络新时代。近年来，我国网络大面积普及，网民急剧增加，数字经济在飞跃式上升。根据中国互联网络信息中心统计，截止到2019年6月，我国网民规模达8.54亿人。《中国数字经济发展与就业白皮书（2019年）》指出，2018年我国数字经济总量达31.3万亿元，占GDP的比重超过三分之一。网络技术促进了社会的进步，同时也给犯罪分子提供了一定的机会，黑客攻击、在线赌博、网络诈骗、网上贩卖公民个人信息、利用网络煽动暴力恐怖活动等网络犯罪日益猖獗，网络犯罪规模呈越来越大趋势，危害程度越来越高，已经严重地影响到了国家安全、社会稳定和经济发展[1]。公安部门为了侦破网络犯罪案件，必须搜集相关电子数据进行技术分析，为案件提供证据，因此电子取证成为破案的关键。

2 电子数据及其法律资格

电子数据是指电子化的客观资料，主要包括存储在计算机中的文件、手机通话记录、短信记录、通信聊天记录、电子交易记录、平台发布信息、网页浏览记录、电子邮件、注册认证信息、登录日志等。

电子数据已渗入到人们生活的各个方面，成为一种无处不在的“痕迹”，因此相关的证据问题也涉及到民事、刑事等领域。2012 年《中华人民共和国刑事诉讼法》第48条和2014年《行政诉讼法》第33条，将电子数据列为一种新的独立证据类型，在立法上明确了电子数据的资格问题。2016 年，最高人民法院、最高人民检察院和公安部三个部门联合制定了《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》。该规定是针对电子数据取证所出台的规范性文件，明确了电子数据的概念和法律地位，并规范了电子取证收集提取和审查判断流程。

3 大数据环境下的电子取证

电子取证即识别、恢复、提取和保存电子数据形成报告并使之成为法律证据的过程，包括数据收集、数据分析和报告撰写等步骤。

大数据为社会发展带来了颠覆性的变化，上至国家治理下至个人生活，都受到了巨大的影响，其作用堪称又一次工业革命[2]。大数据环境下的电子取证就是从海量数据中提取证据的过程，包括数据采集、过滤、清洗、存储、处理和查看过程，由于数据数量大、类型多、存取速度快，取证工作非常复杂[3]。与传统的电子取证相比，大数据环境下的电子取证具有三个特点[4]。

（1）取证对象不同。随着电子商务、电子政务、网络交易和各类网络服务被大量应用，数据越来越多地从终端设备向云端迁移，与此相应的网络犯罪也向云端迁移，很多关键数据会存储在云端，所以电子取证的对象，必须从独立设备转移到云端。

（2）取证技术不同。随着“智慧城市”中城市安全、智能交通等的迅速发展，非结构化的数据量越来越大，单机技术已经无法处理，必须依托云计算、区块链等最新技术才能完成。

（3）取证流程不同。传统电子取证主要是静态取证，大数据电子取证更多的是动态取证，取证流程更加复杂，取证云平台将向动态信息采集、信息安全和云计算的混合模式发展[5]。

4 取证工作面临的挑战

4.1技术上取证难度越来越高

大数据的载体广泛性，导致复杂性证据难以发现，一些易失性、动态性的证据很难获取，数据的多样性让相关分析难度加大，数据的大体量对分析效率提出了更高要求，数据之间的相互融合和共享不容易实现。

作为电子证据的主要存储平台，云平台大多是分布式存储系统，数据的存储经过多个虚拟层，虚拟化环境增加了取证的复杂性[6]。另外，海量数据需要人工智能进行筛选和分析，以提高分布式和整理相关数据的效率，电子取证同时也面临着高速计算的要求。

4.2 法律上取证规范越来越严

到目前为止，我国的电子取证立法还没有全面落实，没有形成一定的规范体系。电子取证的法律规定和条款比较零散，相关司法解释、规范性文件仅有原则性规定，操作性不强，对电子取证的工具、技术和方法也没有做明确规定[7]。

如果没有按照合法的程序和技术进行取证，就会使得电子证据受到一定的“污染”，不能保证其合法性和真实性，取证结果也不能作为合法证据使用在刑事和民事诉讼中[8]。

5 发展方向及改进措施

5.1 规范取证程序，实现司法公正

在大数据时代，新的技术手段和与之相伴的网络犯罪活动不断出现，电子取证要求有更加

精细和规范的取证程序与之相匹配。现有的电子数据取证程序理论，面临着快速被淘汰的命运，对原来规范的修订，已不足以抑制大数据发展带来的风险[9]。为了更好地在海量数据中收集、提取和运用电子证据，需要全新的制度，规范侦查取证程序，做到取证过程合法，兼顾隐私安全，实现技术与法律的深度融合与和谐平衡[10,11]。

5.2改进取证技术，提高取证效率

紧跟大数据技术发展，改进传统的取证技术。全面收集数据，特别是对存储大量数据的云端和无处不在的物联网传感器进行数据收集[2]；建立大数据平台智能取证检索系统，开发智能检索引擎，进行快速、精确查询和检索；优化数据挖掘算法，提高数据清洗和分析速度；改进结果可视化方法，把抽象的数据以更加直观的方式展示。

5.3 培养专业取证人员，提高取证认知

大数据环境下的电子取证涉及多方面的知识和技能的应用，要求有较高的信息技术、网络技术以及相关工具和软件的有效支持，还需要有一定的侦查思维，这就需要对取证人员进行全面系统的专业培训。明确大数据环境下的电子取证需要哪些知识和技能，这些知识和技能需要达到一定水平，然后根据实际需求有针对性地进行培训。此外，还必须将其他行业、领域的新思路、新技术、新方法，运用结合到电子取证中，助力电子取证技术发展。

5.4 建设大数据电子取证平台、专业取证机构和取证实验室

大数据环境下的电子取证面对的是TB甚至PB级别的数据量，传统取证平台已经无法高效完成。必须建设大数据电子取证平台，对海量数据进行快速收集和处理，提取关键证据，为侦查破案和情报分析等工作提供充分证据，满足大数据环境下打击犯罪的需要。由于电子取证需要特定设备和专业技术，很多取证工作只有专业取证机构才能完成。目前，我国该类机构较少，满足不了实际需求，而且对电子取证的研究主要依靠各大高校和科研机构，但是高校和科研机构中电子取证实验室建设投入比较少，实验条件存在着不足[8]。电子证据已经成了一种主要的证据类型，必须加大财政投入，重视电子数据专业取证机构的建设，满足日益增加的取证需要，并在高校和科研机构中增设电子取证实验室，提高取证人员的取证能力。

5.5 多方协作取证

在取证工作中，经常出现取证人员由于授权不够无法采集到足够数据，或是由于取证技术不同导致结果产生偏差，这就需要多方协作取证。特别是在大数据环境下的复杂案件，取证工作必须争取相关部门间的多方协作，尽量使取证调查工作更全面更详细，以使取证结果更可信。

6 结束语

近年来，大数据技术快速发展，大数据的应用已全面开展，电子证据已经成为主要的证据类型。大数据环境下的电子取证对取证设备的储存能力、数据分析能力以及计算能力提出了更高的要求。电子取证必须紧跟大数据技术发展，最大限度地发挥出电子取证的实效，打击网络犯罪，为国家安全和社会进步做出贡献。

基金项目：

广东司法警官职业学院第三届院级课题（项目编号：2017ZD004）。

参考文献

[1] 王学光.计算机犯罪取证法律问题研究[M].北京:法律出版社,2016.

[2] 张其前,尤俊生,高云飞.大数据取证技术综述[J].信息安全研究,2017,3(9):795-802.

[3] 王宝章.浅谈大数据环境下电子数据取证平台的若干关键

问题[J].内蒙古科技与经济,2016(9):62-65.
[4] 姜凤燕,姜瑾,姜吉婷.基于大数据环境的电子取证研究[J].信息网络安全,2016(9):60-63.
[5] 潘金昌.基于“区块链+电子认证”的可信电子存证固证服务平台[J].网络空间安全,2019(3):85-88.
[6] 郭婧.论电子证据的时代新特征[J].法制博览,2018(12):93-95.
[7] 岑冬玲,陈儒敏.完善大数据时代的电子取证工作[J].人民法治,2018(22).100-101.
[8] 刘申时.论电子证据收集中存在的问题及对策[J].法制与社会,2015(10):130-131.
[9] 维克多·迈尔·舍恩伯格,肯尼思·库克耶;盛杨燕,周涛,译.大数据时代:生活、工作与思维的大变革[M].杭州:浙江人民出版社,2013.
[10] 郑令晗.大数据时代云取证的法律困境及其治理[D].海口:海南大学,2016.
[11] 尹鹤晓.电子数据侦查取证程序研究[D].北京:中国人民公安大学,2019.
[12] 李均涛,唐郑熠,张金磊.基于行为时序逻辑的多方协作取证研究[J].网络空间安全,2018(11):82-86.

作者简介:

黄少荣（1976-），女，汉族，广东饶平人，中山大学，硕士，教授；主要研究方向和关注领域：计算智能、计算机应用。

陈丹（1978-），女，汉族，海南海口人，中山大学，硕士，讲师；主要研究方向和关注领域：网络技术、数据库技术。

（上接第78页）

[10] Praveen S. Challagidad, Ambika S. Dalawai, Mahantesh N. Birje. Efficient and Reliable Data Recovery Technique in Cloud Computing[J]. Internet of Things and Cloud Computing, 2017, 5(1): 13-18.
[11] Wei Chen, Yu Tingshang. Disaster Recovery of Online System Based on Cloud Computing[J]. Applied Mechanics and Materials. 2017, (865): 636-641.
[12] Li T, Huang Y, Chen S C, etal. Data-Driven Techniques in Disaster Information Management[J]. ACM Computing Surveys, 2017, 50(1): 1-45.
[13] Yu Jun, Yang Lihong. The Cloud Technology Double Live Date Center Information System Research and Design based on Disaster Recovery Platform[J]. Procedia Engineering, 2017, (174): 1356-1370.
[14] Kokkinos P, Kalogeras D, Levin A, et al. Survey: Live Migration and Disaster Recovery over Long-Distance Networks[J]. ACM Computing Surveys, 2016, 49(2): 1-36.
[15] Andrade E, Nogueira B, Matos R, etal. Availability Modeling and Analysis of a Disaster-Recovery-as-aService Solution[J]. Computing, 2017, 23(6): 34-40.
[16] Anderson J, Meling H, Rasmussen A, etal. Local Recovery for High Availability in Strongly Consistent Cloud Services[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 99(2): 1-2.

作者简介:

孔春伟（1991-），男，汉族，甘肃永靖人，兰州理工大学，硕士，中国人民银行西宁中心支行，工程师；主要研究方向和关注领域：网络与信息安全、企业信息化系统与工程、金融科技。

柳秀秀（1989-），女，汉族，河北衡水人，青海师范大学，硕士，青海师范大学，讲师；主要研究方向和关注领域：网络与信息安全、新一代无线传感技术。