|  |  |
| --- | --- |
| ICS |  |
| CCS | 点击此处添加CCS号 |

|  |
| --- |
| 3209 |

盐城市地方标准

DB 3209/T XXXX—XXXX

移动电商监管规范

Specification for mobile e-commerce regulation

2024 - XX - XX发布

     - XX - XX实施

盐城市市场监督管理局  发布

目次

[前言 III](#_Toc160460009)

[1 范围 1](#_Toc160460010)

[2 规范性引用文件 1](#_Toc160460011)

[3 术语和定义 1](#_Toc160460012)

[4 数据预处理 2](#_Toc160460013)

[4.1 概述 2](#_Toc160460014)

[4.2 数据提取 2](#_Toc160460015)

[4.3 数据清洗 2](#_Toc160460016)

[4.4 数据比对 2](#_Toc160460017)

[4.5 数据关联 2](#_Toc160460018)

[4.6 数据标识 2](#_Toc160460019)

[4.7 数据推送 2](#_Toc160460020)

[5 主体管理 2](#_Toc160460021)

[5.1 概述 2](#_Toc160460022)

[5.2 更新管理 2](#_Toc160460023)

[5.3 归集管理 3](#_Toc160460024)

[5.4 标签管理 3](#_Toc160460025)

[6 监测流程 3](#_Toc160460026)

[6.1 概述 3](#_Toc160460027)

[6.2 任务发起 3](#_Toc160460028)

[6.3 组织实施 3](#_Toc160460029)

[6.4 结果处置 3](#_Toc160460030)

[6.5 分析应用 4](#_Toc160460031)

[7 证据要求 4](#_Toc160460032)

[7.1 概述 4](#_Toc160460033)

[7.2 基本要求 4](#_Toc160460034)

[7.3 证据获取 4](#_Toc160460035)

[7.4 证据存储 4](#_Toc160460036)

[8 监管系统要求 5](#_Toc160460037)

[8.1 政务云部署要求 5](#_Toc160460038)

[8.2 网络安全等级保护要求 5](#_Toc160460039)

[8.3 系统功能性要求 5](#_Toc160460040)

[8.4 取证物理节点部署要求 6](#_Toc160460041)

[8.5 取证终端安全性要求 6](#_Toc160460042)

[8.6 网络通信数据传输中的相关要求 6](#_Toc160460043)

[附录A（资料性） 网络交易监测任务单 7](#_Toc160460044)

[附录B（资料性） 互联网电子数据证据报告 8](#_Toc160460045)

[附录C（资料性） 自动取证实现路径 10](#_Toc160460046)

[附录D（资料性） 远程操作手机取证 11](#_Toc160460047)

1. 前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由盐城市市场监督管理局提出并归口。

本文件起草单位：

本文件主要起草人：

移动电商监管规范

* 1. 范围

本文件界定了移动电商监管相关的术语和定义，规定了数据预处理、主体管理、监测流程、证据和监管系统要求。

本文件适用于盐城市市场监督管理部门采用技术方式开展移动电商监管工作。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

SG 3 市场监管基础代码集

* 1. 术语和定义

下列术语和定义适用于本文件。

移动电商 mobile e-commerce

通过移动互联网销售商品或者提供服务的经营活动。

网络交易监测 network transaction monitoring

市场监督管理部门为履行网络交易监督管理职责，对网络交易主体、客体和行为等相关信息的合法性进行监督检查的技术辅助措施。

互联网电子数据证据 internet electronic data evidence

市场监督管理部门依法通过互联网信息系统或设备获取的，在互联网上公开传播的，能够证明待证事实的一系列数据信息。

主证信息 main certificate information

涉嫌或认定违反市场监督管理法律、行政法规、规章的相关网络经营信息，以及与此共同构成同一待证事实信息的关联信息。

主证附属信息 main certificate affiliated information

获取、存储、使用主证信息过程中，计算机信息系统与网络通信过程生成的计算环境信息、相关运行信息，以及相关人员在应用程序、工作记录中填写的内容等关联信息。

并行取证 parallel evidence collection

多节点针对同一个取证命令，同时或在较短的时间间隔内对同一个取证目标进行取证操作。

证据报告 evidence report

记录互联网电子数据证据获取、存储、使用等管理过程的文书。

* 1. 数据预处理
     1. 概述

按照SG 3的要求，对依据数据资源目录获取到的移动电商各类数据进行提取、清洗、比对、关联、标识，推送数据中心统一存储。

* + 1. 数据提取

根据预设规则获取数据信息，包括但不限于主体名称、统一社会信用代码、证照信息、行业分类、失信名单、市场监管关键词等。

* + 1. 数据清洗

根据清洗规则，去除不符合要求的垃圾数据和重复数据，按照SG 3进行归一化处理。

* + 1. 数据比对

支持主体名称/简称、注册号/统一社会信用代码、地址等预设规则，符合规则时触发智能推送。

* + 1. 数据关联

根据关联规则，将不同来源的数据信息建立关联关系，包括但不限于主体与投诉信息、案件信息、商标信息、广告信息、抽检信息等的关联。

* + 1. 数据标识

根据样例或用户需求，确定数据区域、数据敏感级别等标识。

* + 1. 数据推送

数据通过检索条件过滤、打包，由用户本地部署于政务云（符合政务云平台具体部署要求）的接收服务器接收数据，实时导入本地数据库中供使用、分析。

* 1. 主体管理
     1. 概述

主体管理是对APP、小程序、公众号、视频号等移动电商主体信息进行动态更新、归集，实施标签标注的过程。

* + 1. 更新管理

自动或手动对APP、小程序、公众号、视频号等移动电商主体进行新增、编辑、删除、查询、匹配监管单位等操作。

自动检测数据是否有效，检测发现无法访问、黄赌毒等异常数据即转入异常库。

数据自动更新周期一般为30日～45日，异常数据视数据量情况确定自动检测频次。

* + 1. 归集管理

将市场主体信息与其开设的APP、小程序、公众号、视频号等移动电商主体信息进行关联，在市场主体名下集中显示关联信息。

将市场主体信息按主营商品类别进行关联归集。

将市场监督管理部门依法依规掌握的投诉举报、监督检查、行政处罚、信用信息，与市场主体信息进行关联归集。

* + 1. 标签管理

建立标签库，支持对标签进行新增、分组、修改、删除等操作。

根据归集管理情况实施多维标注，即一个主体可同时标注多个标签。

根据监管工作需要，标注移动电商主体所关联的直播基地、电商园区、MCN机构等信息。

* 1. 监测流程
     1. 概述

监测流程包含对日常监测、专项监测和研究性监测进行任务发起、组织实施、结果处置、分析应用的过程。

* + 1. 任务发起

市场监督管理部门各业务机构以《网络交易监测任务单》的形式（示例见附录A），提出本监管领域日常或专项网络交易监测需求，确定涉嫌违法行为在网络交易信息中的具体表现形式，包括可能出现的文字（关键字词、行业用语、暗号暗语）、图形图像、音视频等内容，提供给市场监督管理部门网监机构组织实施监测。

市场监督管理部门可以根据移动电商新业态模式监管形势分析、监测技术研发、监测制度和标准制定需要，发起研究性监测任务。

* + 1. 组织实施

市场监督管理部门网监机构根据《网络交易监测任务单》，自主或委托第三方实施监测分析，形成监测结果信息并反馈提出监测需求的单位。

监测结果信息一般应包括涉嫌违法违规信息的链接或快照、经营主体、涉嫌违法违规表现、所属业务领域等信息。

监测结果信息附带互联网电子数据证据的，可通过监测智能触发取证进行证据固定。

* + 1. 结果处置

市场监督管理部门按照线上线下一体化监管原则，做好监测结果信息的后续处置，一般由提出监测需求的单位组织本条线做好研判确认、分派流转、调查核实、处理反馈等工作。

监测结果信息应通过市场监督管理部门自建网络监测技术系统进行分派、流转、处理、反馈，形成监测流程闭环，流转路径可通过操作日志进行追溯查看。

监测结果信息应自该信息分派之日起十五个工作日内处理结束。

研判确认构成违法线索的，依照有关规定运用行政指导、责令改正、行政处罚、信用惩戒等手段实施监管，反馈处理结果详情的同时应当附带相关文书证明材料，对涉及立案处理、实施信用惩戒以及需要检验检测鉴定、异地协查等情形，处理时限可以按照有关规定予以相应延长。研判确认不构成违法线索的，要说明理由和依据。

* + 1. 分析应用

分析监测任务运行过程、监测业务产生数据的基础上，持续更新标签标识、优化监测模型、完善监测流程、提升数据质量，对移动电商开展风险研判和分类监管施策评估。

* 1. 证据要求
     1. 概述

证据要求是对通过互联网公开传播的，涉嫌或认定违反市场监督管理法律、行政法规、规章的网络经营信息，实施获取、存储、使用过程中的具体要求。

* + 1. 基本要求

真实性：证据获取、存储、使用的每一步操作自动留痕，实时记录，全程可追溯，能够证明证据自获取之时保持完整、未经改变；

合法性：取证指令由市场监督管理部门执法人员发出或符合相关规定的市场监督管理部门自建技术系统发出，符合市场监督管理行政执法电子数据取证相关规范和流程；

完整性：主证信息与主证附属信息共同构成互联网电子数据证据的原则，二者缺一不可。

应用虚拟化技术及其他人工智能技术，应确保真实、合法的操作用户与技术系统物理节点。

* + 1. 证据获取

实施取证前，应对用来获取电子数据的计算机系统、设备的硬件、软件环境进行检测，确保完整、可靠，处于正常运行状态，连接在真实的移动互联网上。

基于移动电商电子数据存在可能无法重复获取或无法复现的情形，其证据获取应当采用全程录屏的方式，录屏过程中可对主证信息相关页面进行截屏。

主证信息获取中应含有移动电商主体证照公示信息、店铺首页、所在平台首页、主证内容相关页面信息。

主证附属信息获取中应含有技术系统名称、系统所属单位、取证单位、取证时间、取证指令发出者、取证指令内容、取证指令发出设备、执行设备、执行过程记录等足以证明主证信息真实性、合法性、完整性的相关信息。

对于移动电商中存在的基于算法推荐产生的“千群千面”“千址千面”等情形，可采取并行取证的方式获取一组证据进行相互印证。并行取证通过自动取证或远程操作手机取证来实现。

* + 1. 证据存储

市场监督管理部门采用技术方式下的证据存储，是对已获取的互联网电子数据证据自动进行固定、校验、存储等的过程。

存储内容：互联网电子数据证据的主证信息、主证附属信息，包括可校验的取证记录信息、可校验的取证要素信息。

存储过程：对截图、录屏等证据加盖时间戳，并对证据进行哈希值运算，将图片、音频、视频、文件等加密存储，实时固化互联网电子数据的内容、权属信息及存证时间，生成唯一的数据指纹。

存储方式：技术系统的存储具有防篡改、灾备等功能，在各物理节点上进行分布式冗余存储。对定义为案件使用的证据实行长期存储，存储时间支持三年以上。

* 1. 监管系统要求
     1. 政务云部署要求

配置参数不低于表1的要求。

1. 配置参数要求

| 序号 | 资源 | 用途 | 配置 |
| --- | --- | --- | --- |
| 1 | 弹性负载均衡 ELB | 负载均衡器，避免单点故障，提高系统可用性 | 80 443 两个端口 |
| 2 | Web前端——弹性云服务器 ECS | 部署Web前端代码 | CPU：4核  内存：8G  磁盘：100G |
| 3 | Web服务端——弹性云服务器 ECS | 部署Web服务端代码 | CPU：8核  内存：16G  磁盘：200G |
| 4 | 数据库——弹性云服务器 ECS | 部署MySQL数据库服务 | CPU：4核  内存：16G  磁盘：100G SSD |
| 5 | 全文检索服务——弹性云服务器 ECS | 部署全文检索数据存储服务 | CPU：16核  内存：64G  磁盘：100G |
| 6 | S3分布式文件存储服务 | 提供图片、视频等文件存储服务 | Bucket：2  总容量：1T |

* + 1. 网络安全等级保护要求

等保二级以上。

* + 1. 系统功能性要求

监测任务实施的技术路线主要涉及监测数据采集、数据处理、模型识别和数据整合。

1. 数据采集：以移动端APP采集技术模拟用户真实的浏览行为对数据进行采集，通过分布式流处理平台将数据实时收集并存储至分布式存储系统；
2. 数据处理：数据的传输与存储、分布式计算和OCR识别；
3. 模型识别：违法特征建模、违法数据识别；
4. 数据整合：数据清洗和数据结构化，将来自不同来源、不同格式的数据整合到统一的数据模型中，进行统一管理、分析和应用。

监测智能触发取证实施的技术路线涉及身份校验、自动取证、复核确认和证据存储。

1. 身份校验：通过用户登录管理，实现对执法人员的身份校验；
2. 自动取证：监测识别到违法数据时，第一时间将线索推送至取证模块，取证模块校验指令后，自动调度取证操作，自动取证数据至少保存30日；
3. 复核确认：自动取证的数据等待执法人员进行复核，确认其准确度及是否需要后续处理；
4. 证据存储：对后续采取立案处理的，自动转为长期存储，存储时间支持三年以上。

并行取证实施的技术路线要求如下：

1. 自动取证实现路径：对需要反复取证的可确认流程的取证场景做定制化脚本，配置基本属性信息（取证App、URL或其他约定标识），由取证系统自动完成取证（见附录A）；
2. 远程操作手机取证：执法人员登录系统后手动选择取证终端（手机），并在浏览器上远程操作手机浏览内容，发现需取证内容时在浏览器上发送“取证当前页面”的指令，完成所有取证动作后结束取证，系统自动记录取证数据。 远程操作手机取证可补充自动取证无法实现的场景，主要是未配置自动化流程的场景，如需要获取登录方可见的信息、冷门APP的页面等信息（见附录B）。
   * 1. 取证物理节点部署要求

取证物理节点部署要求如下：

1. 稳定的电源，24小时220V；
2. 稳定的网络，24小时100M；
3. 稳定的温度，低于35摄氏度。
   * 1. 取证终端安全性要求

取证终端安全性要求如下：

1. 物理安全：使用保险柜和受控访问区域来保护设备和存储介质；
2. 数据安全：使用写保护工具和方法来，防止在取证过程中对数据进行修改或破坏；
3. 加密和数据保护：敏感数据，加密存储和传输，保护在非授权访问下的保密性；
4. 访问控制：实施访问控制措施，只有授权人员能够访问取证数据；
5. 法规遵从性：遵守适用的法律、标准和最佳实践；
6. 连续性和灾难恢复：建立备份和灾难恢复计划，确保在硬件故障、软件故障或其他灾难性事件发生时取证数据的连续性。
   * 1. 网络通信数据传输中的相关要求

网络通信数据传输中的相关要求如下：

1. 加密传输：使用强加密算法保护网络通信数据在传输过程中不被截获或篡改；
2. 安全协议：使用安全的网络协议和标准来进行数据传输；
3. 端点验证：确保通信双方的身份通过数字证书和公钥基础设施（PKI）等机制进行验证，防止中间人攻击；
4. 网络隔离和安全区域：通过物理或逻辑手段将取证数据传输网络与公共网络或不安全网络隔离开来，创建安全的数据传输通道；
5. 访问控制和认证：确保只有授权的用户和系统能够访问或传输取证数据，通过实施强认证机制来加强安全性；
6. 日志记录和监控：对所有网络通信和数据传输活动进行日志记录和监控，以便于在需要时进行审计和调查；
7. 数据完整性验证：采用哈希算法等手段验证数据传输前后的完整性，确保数据在传输过程中未被篡改。
9. （资料性）  
   网络交易监测任务单

下面给出了网络交易监测任务单示例。

网络交易监测任务单

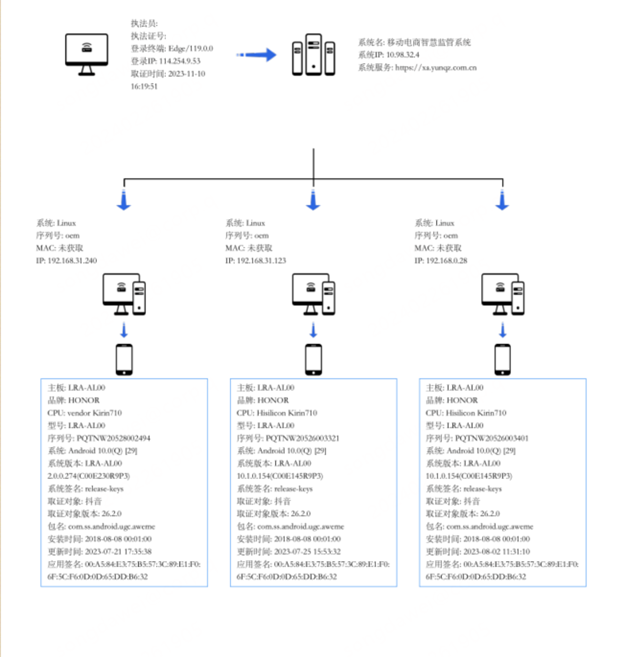
监测任务发起单位（盖章）： 编号：

|  |  |
| --- | --- |
| 监测任务名称 |  |
| 监测任务来源 |  |
| 监测类别 | □常规性监测（日常监测） □特定性监测（专项监测） □研究性监测 |
| 监测方式 | □自主监测 □委托第三方数据搜索 |
| 监测时间 | 年 月 日— 年 月 日 |
| 监测范围 |  |
| 监测对象类型 | □网站 □网店 □公众号 □小程序 □APP □视频号 □其他 |
| 监测内容 |  |
| 监测特征词 |  |
| 监测结果反馈 | □监测报告 □违法线索表 □网络经营主体清单 □监测电商平台（网站）个次 |

1. （资料性）  
   互联网电子数据证据报告

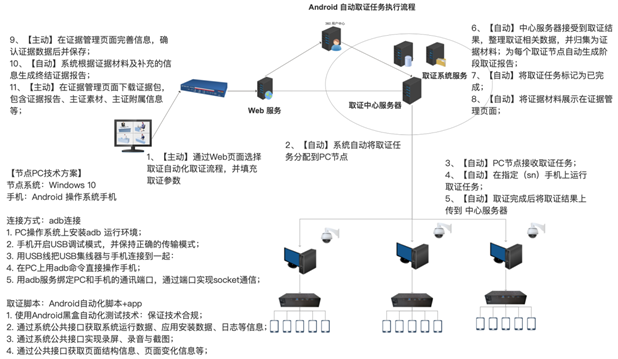
下面给出了互联网电子数据证据报告示例。

| 互联网电子数据证据报告  一 、序 言  本证据报告是执法人员对互联网电子数据证据获取、存储、使用等管理过程的记录，是证据的载体，通过盐城市市场监督管理局自主技术系统“盐城市移动电商智慧监管系统”自动生成，包括序言、主证信息、主证附属信息。  取证事由：  取证对象主体名称：  报告出具时间：  证据管理方式：  二、主证信息  （相关截图）  三、主证附属信息  1、系统设备信息  系统名称：  物理节点编号：  取证服务器：  存证服务器：  2、人员账户信息  取证人员：(执法证号： )  3、证据获取信息  取证方式：  取证类型：  取证指令内容：  指令发出设备：  指令发出时间：  指令执行过程：  文件 MD5值：  4、证据存储信息  存证方式：  存证时间：  5、证据使用信息 |
| --- |



1. （资料性）  
   自动取证实现路径

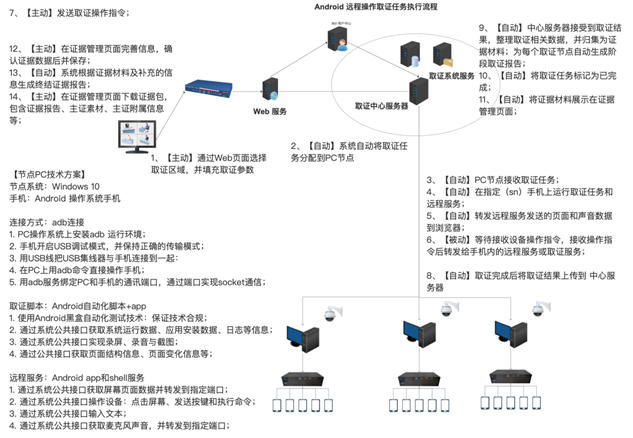
图C.1给出了自动取证路径。



* 1. 自动取证路径

1. （资料性）  
   远程操作手机取证

图D.1给出了远程手机取证路径。



* 1. 远程手机取证路径

