数智时代手机个人数据安全风险与防护策略研究

万雪勇
江西警察学院，江西 南昌 330100

DOI: 10.61369/TACS.2026090038

摘　　要： 数智时代飞速发展使智能手机成为人们生活生产的重要工具，海量的个人身份信息、社交数据、金融数据等都储存在手机终端里，数据交互、共享、传输的频率明显提高。与此同时，数据被盗取、恶意删除、泄露、非法恢复等安全问题不断出现，手机个人数据安全面临新的挑战。本文聚焦数智时代手机个人数据安全风险，从数据盗取、数据损毁删除、非法数据恢复三个维度分析隐患问题，提出防护策略，以规避个人数据安全风险，保护个人数据。

关 键 词： 数智时代；智能手机；个人数据；安全风险；防护策略

Research on Security Risks and Protection Strategies of Mobile Phone Personal Data in the Digital Intelligence Era

Wan Xueyong
Jiangxi Police College, Nanchang, Jiangxi 330100

Abstract: The rapid development of the digital intelligence era has made smart phones an essential tool for people's life and work. A massive amount of personal identity information, social data, financial data and other private information is stored in mobile terminals, with the frequency of data interaction, sharing and transmission increasing significantly. Meanwhile, security problems such as data theft, malicious deletion, leakage and illegal recovery have emerged continuously, posing new challenges to the security of personal mobile data. Focusing on personal data security risks of smart phones in the digital intelligence era, this paper analyzes potential hidden dangers from three dimensions: data theft, data damage and deletion, and illegal data recovery, and proposes targeted protection strategies to avoid personal data security risks and effectively protect personal private data.

Keywords: digital intelligence era; smart phone; personal data; security risks; protection strategies

一、数智时代手机个人数据安全风险分析

（一）手机个人数据非法盗取风险突出

数智时代智能手机装有各种智能应用、物联网交互模块，数据采集和传输全程智能化、自动化，大大降低了不法分子窃取手机个人数据的技术门槛，数据非法盗取是手机安全最大的隐患。目前，手机数据盗取方式多样化、隐蔽化，不法分子利用恶意软件、钓鱼链接、伪基站、公共陌生 WiFi 等手段对手机终端进行入侵，悄悄地获取用户的通讯录、短信、位置信息、支付密码、浏览记录等重要个人信息[1]。大多数用户没有基本的安全识别能力，随意下载非正规渠道的 APP、点击陌生链接、连接公共网络，给数据被盗取创造了条件。同时数智场景下数据爬虫、智能破解技术被广泛应用，不法分子可以利用自动化工具大批量获取手机交互过程中产生的碎片化数据，再整合成完整的用户信息画像。一些第三方 APP 存在违规收集、后台偷传数据的情况，未经用户同意私自抓取个人信息并出售，形成黑色数据产业链，严重侵犯了用户的个人数据权益，盗取行为常常全过程隐蔽，用户很难发现，事后追责难度大。

（二）手机个人数据恶意删除与损毁风险频发

在手机日常使用以及网络交互的过程中，个人数据被恶意删除、意外损毁、批量丢失的安全风险一直居高不下，给用户个人数据的完整性造成了严重的破坏。一方面，网络不法分子利用病毒程序、木马插件远程操控用户的手机，有目的的删除用户的影像资料、文档文件、聊天记录等重要数据，部分恶意程序具有批量损毁数据的功能，可以对手机存储的数据进行篡改、格式化处理，造成用户数据永久性丢失。另一方面，数智设备兼容性问题、系统漏洞、APP 程序冲突会造成手机数据自发性删除和损毁，系统更新失败、智能程序运行故障会导致本地存储的数据莫名其妙地丢失[2-3]。除了人为误操作，手机设备丢失被盗后他人恶意操作，会造成个人数据被恶意删除。相比传统数据丢失而言，数智时代数据删除损毁具有突发性、不可逆性的特点，大多数普通用户没有养成常态化的备份习惯，数据丢失之后不能自主挽回，不但会造成个人隐私泄露，部分工作、证件类重要数据损毁还会给用户的生活、工作造成直接损失。

（三）废弃手机数据非法恢复带来隐私泄露风险

数智时代手机数据恢复技术越来越成熟，门槛也越来越低，

基金项目：江西省教育厅科学技术研究项目“基于 SQLite 数据库的手机删除数据的恢复与取证研究”（GJJ2202303）。

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

用户删除或者清空的手机数据可以通过专业的恢复工具或者技术手段恢复出来，因此，废弃手机隐私泄露被用户忽略的风险越来越大。大多数用户存在着认知误区，认为手机里的照片、聊天记录、文件数据删除、清空之后就彻底清除了，随意转让、变卖、丢弃废旧手机，没有做深度数据销毁处理。目前市场上各种免费和付费的手机数据恢复软件操作简单，不需要专业的技术就可以恢复出手机格式化或者手动删除过的大部分数据，包含私密影像、聊天记录、金融流水、身份信息等。不法分子可以回收废旧手机、破解二手设备的存储分区，用数据恢复技术获取用户的遗留数据，然后出售给其他人[4]。同时部分手机维修机构、第三方数据处理平台存在违规操作，维修、拆解手机时私自恢复用户删除的数据，并非法留存、传播，形成隐私泄露途径，该类风险具有很强的隐蔽性，用户很难察觉到，长期存在隐私泄露隐患。

二、数智时代手机个人数据安全防护策略

（一）强化手机终端安全防护，阻断数据盗取渠道

终端安全是手机个人数据安全的第一道防线，根据数智时代数据盗取渠道多、手段智能的特征，需要从各个方面提升手机终端的安全防护能力，从源头上阻止非法的数据窃取行为。首先，用户需要规范手机软件的安装和使用行为，拒绝非正规应用市场上的 APP 下载安装，不随便点击陌生的短信、社交平台链接、弹窗广告，授权给未知来源的 APP 获取通讯录、位置、相册、麦克风等敏感权限，从源头上防止恶意软件、钓鱼程序的入侵。其次，要对手机系统的安全进行常态化的维护，及时更新手机的官方系统补丁以及安全组件，修复系统漏洞，关闭手机后台运行的不安全设备连接、陌生人发送的文件下载等危险的功能，经常使用手机自带的安全软件来检查病毒、检测风险，删除后台的恶意插件和缓存风险程序。同时，谨慎使用公共网络环境，商场、地铁、酒店等公共场所的免费 Wi-Fi 存在着极大的数据泄露风险，日常使用手机进行支付、登录账号、传输私密数据的时候，应该切换到专属移动网络，不在公共网络上进行隐私数据的交互[5-7]。另外，根据实际需要选择正规的第三方安全防护软件进行安装，并开启实时防护、网络监控、权限管理等功能，智能拦截爬虫抓取、后台偷传数据等违规行为，全方位加强手机终端的安全防线，有效的避免出现数据被盗取的风险。

（二）规范日常操作行为，规避数据删除损毁风险

针对手机数据恶意删除、意外损毁、丢失等情形，要从规范用户操作、健全数据备份、规避设备故障风险三个方面入手，创建起常态化的数据防护体系，从而尽可能地保证手机个人数据的完整和安全。用户应该养成规范的手机操作习惯，不能随意删除系统文件、格式化存储分区、强制结束系统程序等危险操作，在清理手机缓存、垃圾文件的时候要仔细辨别文件属性，防止误删重要的私密数据、工作文档和核心资料。同时，对于手机系统的更新、APP 的升级等操作要从官方正规途径进行，防止在升级时造成程序冲突、系统崩溃而使数据遭到破坏，升级前对设备的存储情况进行提前检测，留有足够大的运行空间，减少由于程序运行故障造成的数据丢失。再者，创建起多重数据备份体系，采取“云端备份 + 本地备份 + 外接设备备份”的三重备份形式，定时把手机相册，聊天内容，文档，身份证明等关键数据存入正规云端平台，电脑硬盘，U 盘等设备当中，防止单一备份途径出现故障造成数据全部丢失的情况发生。另外还要做好手机设备防护工作，防止手机磕碰、进水、中毒等造成的系统故障和数据损毁，手机丢失、转借他人使用时，及时锁定设备、关闭数据权限，防止他人恶意删除、篡改个人数据，全方位规避各种数据删除损毁的安全风险[8]。

（三）落实废旧手机数据深度销毁，杜绝非法数据恢复泄露

为了解决废弃手机数据被非法恢复而引起的隐私泄露问题，应该对手机设备的淘汰、转让、报废全过程进行深入的数据销毁，从根本上消除数据恢复的风险。首先，用户要抛弃“简单删除就彻底清除”的错误认识，明白普通删除、清空只是把数据的存储轨迹隐藏起来，并不是真正删除了数据，数据依然可以通过专业技术手段恢复，废旧手机处置前不能只用手动删除、基础格式化的方式处理数据。其次，使用专业的深度数据销毁方法，对于自用淘汰、转让的手机可以使用手机自带的恢复出厂设置和覆盖存储两个步骤来达到数据清除的目的，即恢复出厂设置之后，用视频、垃圾文件填充手机存储空间，覆盖掉原有的数据存储分区，彻底消除原始数据的痕迹，使数据不能被技术恢复。对报废、不再使用的手机，可以到正规的线下数据销毁机构，使用专业的设备对手机进行物理销毁或者数据粉碎处理，破坏存储芯片，防止数据恢复[9-10]。规范二手手机交易流程，交易前自己对数据进行深度销毁，不委托给陌生平台或者个人处理数据，交易后及时解除手机账号绑定、关闭云端同步、注销设备信息，从各个方面阻止不法分子通过云端关联恢复本地数据，保护用户隐私安全。

（四）提升用户数据安全意识，构建常态化防护体系

用户安全意识薄弱、防护认知欠缺是手机个人数据安全风险频频出现的主要主观因素，在数智时代应当全方位提高用户个人数据安全防护意识，规范日常行为，创建起常态化的、持久的数据安全防护体系。首先，用户要主动学习数智时代手机数据安全知识，掌握数据盗取、恶意删除、非法恢复的常见手段和隐蔽形式，认清过度授权、随意联网、简易数据清除等行为的安全隐患，打破传统数据防护认知误区，树立全程防护、全面防护的安全理念。其次，对个人数据的权限进行严格的控制，并且设置合理的隐私保护措施，对手机上的所有应用程序权限进行整理，关闭不必要的敏感权限，及时删除过期或者不再使用的应用程序，防止第三方软件私自采集和传输个人数据。养成常态化的安全自查习惯，定时查看手机后台运行记录、数据传输日志、设备登录记录，及时发现异常操作、陌生设备接入等问题，第一时间予以处理，防止风险扩散。另外，社会和平台要一起开展安全科普活动，用短视频、科普文章、公益讲座等形式来普及手机数据备份、深度销毁、风险识别等实操方法，全方位提高全民手机数据安全防护能力，从主观上杜绝各种人为操作造成的数据安全风险，筑牢个人数据安全防护的思想防线。

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

三、结论

总而言之，手机个人数据安全防护并非单一技术防护工作，需要结合技术防控、行为规范、认知提升、流程管控多方协同发力。未来，随着数智技术的持续升级，手机数据安全风险将呈现全新形态，用户需持续更新防护理念，优化防护手段，常态化落实数据安全防护措施，同时依托技术革新与行业规范，持续完善个人数据安全防护体系，全方位守护数智时代个人数据安全与隐私权益。

参考文献

[1] 刘恩稷，李想，谭卓，等 . 人工智能手机产业发展现状、趋势及对策建议 [J]. 机器人产业，2025,(6):18-35.

[2] 王阳，曾亚博 . 智能手机与农村家庭负债——基于中国农户调查数据的实证 [J]. 宜宾学院学报，2025,25(11):21-32.

[3] 温德成，李秀琳，陈晓 . 产品创新扩散中社会化问答内容特征对用户购买意愿的影响机制研究 [J]. 管理学报，2025,22(2):336-344.

[4] 彭轲，韩奎斌，王团伟 . 健康素养和手机依赖的交互作用与在校大学生亚健康状况的关联研究 [J]. 现代预防医学，2024,51(24):4536-4541.

[5] 何庆，何榕健，李晓，等 . 居民空气污染暴露健康风险实时动态评价的研究进展 [J]. 复旦学报 (自然科学版),2023,62(4):496-506.

[6] 赵欣，赵凯旭，黄晓军 . 基于 ECOSTRESS 地表温度和手机信令数据的城市人口热环境暴露风险评价——以西安市为例 [J]. 地理科学进展，2022,41(11):2061-2072.

[7] 周文娟 . 浅谈金融科技对手机银行发展的影响 [J]. 财经界，2021,(14):5-6.

[8] 林萍 . 大数据背景下租赁公司风险控制研究 [J]. 中国市场，2020,(35):189-190.

[9] 王仲羊 . 大数据时代手机定位侦查的制度挑战与法律规制 [J]. 中国人民公安大学学报 (社会科学版),2020,36(6):55-63.

[10] 叶脉，张佳琳，张路路，等 . 手机信令数据在粤港澳大湾区大气环境风险管理中的应用研究——以江门市为例 [J]. 生态学报，2020,40(23):8494-8503.

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License