

Reflection on the User Data Security and Privacy Protection Strategy in the Biomedical Cyberspace Governance System

Gaoshan Zhu¹ Mengqi Sun^{2*} Chunhui Ma¹

1. Shanghai Fuhong Hanlin Biotechnology Co., Ltd., Shanghai, 200233, China

2. Shanghai Fosun Pharmaceutical (Group) Co., Ltd., Shanghai, 200010, China

Abstract

Under the background of the development of modern Internet technology, the data security and privacy protection of users in cyberspace have been more seriously challenged. Once the data security is threatened, it will cause a crisis of social trust and harm the harmonious and stable development of society. Based on this, it is necessary to further improve relevant laws, regulations and policies, continuously improve the cyberspace governance system, and realize the normative development of data protection and use. At the same time, a perfect data security technology system should be built on the basis of data leakage prevention technology, so as to protect sensitive data, and to have a detailed understanding of the use of the data in the organization, so as to ensure that the security personnel fully understand the data, and promote the improvement of data classification and management ability. In addition, it is also necessary to strengthen the technical prevention ability, improve citizens' MIL literacy, improve the multi-party cooperation mechanism, and ensure the orderly progress of user data security and privacy protection strategies. This paper mainly analyzes the user data security and privacy protection strategies in the cyberspace governance system, so as to effectively improve the user data security, avoid data leakage, and realize the continuous optimization and development of the cyberspace governance system.

Keywords

network space governance system; user data security; privacy protection strategy

生物医药网络空间治理体系中用户数据安全及隐私保护策略思考

竹高山¹ 孙梦琪^{2*} 马春辉¹

1. 上海复宏汉霖生物技术股份有限公司, 中国·上海 200233

2. 上海复星集团, 中国·上海 200010

摘要

现代化互联网技术发展背景下,网络空间中用户数据安全、隐私保护受到了更加严重的挑战,一旦数据安全受到威胁,会引发社会信任危机,危害社会和谐稳定发展。基于此,要进一步完善相关法律法规政策,持续性完善网络空间治理体系,实现数据保护和使用工作的规范性开展。同时,要在数据防泄漏技术基础上构建完善的数据安全技术体系,从而保护敏感数据,且能够对组织内数据使用情况进行详细了解,确保安全人员充分理解数据,促进数据分类、管理能力的提升。此外,还需要强化技术防范能力,提升公民的MIL素养,完善多方协作机制,保障用户数据安全、隐私保护策略的有序进行。论文主要对网络空间治理体系中用户数据安全及隐私保护策略进行分析,从而有效提升用户数据安全,避免数据泄露,实现网络空间治理体系的持续性优化发展。

关键词

网络空间治理体系; 用户数据安全; 隐私保护策略

1 引言

近年来,互联网技术高速发展,对用户数据安全、隐

私保护工作带来了极大的挑战和威胁,如网络攻击、网络诈骗等,严重侵犯用户的合法权益,危害网络空间的正常秩序,需要迫切保护网络空间个人数据安全和隐私。因此,要加大用户数据安全及隐私保护研发和实践力度,强化用户的网络安全意识,营造安全、有序的网络环境,实现网络空间的可持续发展。在数据安全技术体系建设中,需要对数据防泄漏技术进行优化应用,确保数据管理措施与《网络数据安全管理条例》的相关要求保持契合性;需要对敏感数据进行精准识别,实现网络数据的安全保护,进而保护企业数据资产;

【作者简介】竹高山(1984-),男,中国浙江嵊县人,博士,从事网络空间治理体系中用户数据安全及隐私保护策略思考研究。

【通讯作者】孙梦琪(1985-),女,中国上海人,硕士,从事数字经济安全技术研究。

能够对敏感数据截图外发互联网的逃逸行为进行精准识别，管控员工访问行为，真正保障数据安全。

2 网络空间治理体系中用户数据安全及隐私保护问题

2.1 先进技术使用不当

当前，网络技术持续升级更新，同时对网络空间治理体系带来了新的风险问题。尤其是人工智能技术的普及发展，对用户数据安全、隐私保护带来极大挑战，尤其是人工智能的滥用，对个人隐私、国家安全带来极大威胁^[1]。生物医药领域尤需保护患者等敏感信息，防止滥用风险。ChatGPT 持续采集数据，易引发未授权、超授权及非法获取风险，加剧生物医药营销中的数据泄露概率。AI 模型执行环节中，会以文字形式在线用户敏感信息，引起数据泄露，严重侵害用户的切身利益。

2.2 资本诱发数据泄露

信息时代，数据成为企业决策的关键要素之一，然而大数据技术的普及应用，往往会出现非法采集用户数据的现象，甚至部分企业利用 AI 过度采集用户数据谋取非法利益，进而在利益驱使下无节制的采集用户的个人信息，向第三方销售，致使用户隐私数据泄露。企业在处理内部资料时，往往存在信息误用、二次利用等隐患，再加上对海量私人信息非法违规管理，加大了个人信息被泄露概率^[2]。此外，在使用大数据技术对部分信息进行处理时，需要对特定个体进行追踪，也加大了隐私泄露风险。

2.3 生物医药研发与 APP 运营中的数据安全策略

在生物医药研发与 APP 运营中，数据安全管理至关重要。第一，建立严格的数据访问权限控制机制，确保只有授权人员能访问敏感数据，并实施数据加密技术保护数据安全。第二，识别并记录所有涉及敏感数据的接口，分析其功能和用途，确定重要性和敏感性级别，并进行分类管理。评估每个接口可能面临的风险，如未授权访问、数据篡改等，制定相应的安全防护措施，并定期更新风险评估。针对已识别的风险，利用最新的 IT 技术，如人工智能、大数据分析等，提升数据安全能力并制定具体的整改措施，如加强身份验证、限制访问范围等，设计并实施加固方案，提高系统的整体安全性。引入先进的安全工具和平台，增强防御能力。第三，对所有对外提供的接口进行严格监控，防止未经授权的访问和使用，实时访问日志记录，跟踪接口的使用情况。第四，部署数据流动监控工具，实时检测数据流向和传输过程，当发现异常数据流动时，立即发出预警并采取措施阻止进一步的数据泄露。建立实时监控系统，监测数据使用情况，及时发现违规行为，设置预警机制，当检测到异常活动时，自动触发警报并通知相关人员。第五，采用用户实体行为分析（UEBA）技术，识别用户的异常行为模式，结合机器学习算法，提高异常行为的检测准确率和响应速度^[3]。

3 网络空间治理体系中用户数据安全及隐私保护策略

3.1 强化技术防护能力

在网络技术高速发展背景下，网络空间治理难度逐渐呈现增长趋势，用户数据安全和隐私受到严重威胁，针对这种情况，需要对现代化技术进行优化应用，进一步提高技术防护能力^[4]。在具体实施中，需要加大网络安全技术研发力度，尤其要对防火墙、入侵检测系统、加密技术等网络安全技术进行融合应用，从而进一步强化恶意攻击防范能力，避免数据泄露，保障数据安全。此外还需要对大数据技术、物联网技术、云计算等技术优化应用，进而优化数据安全防范方案；需要加大企业的用户隐私保护意识，并对用户处理进行科学性收集、存储和处理，严格按照相关法律法规要求，对数据使用界限进行明确规定，防止数据挪用、泄露。要进一步健全数据安全管理制度、技术防范体系，尤其要完善数据安全管理制度，对不同部门的具体责任、义务进行明确划分和落实，才能保障数据齐全性和精准性。要实现技术防范体系的持续性维护，安排专业人员定期检查数据安全，及时修补系统漏洞，以便对持续变化的网络安全威胁进行良好适应。

3.2 企业数据安全与高效管理策略

为了确保生物医药的企业数据安全和高效管理，通常会采取以下措施：所有研发数据不落地，即在研发过程中，所有数据都存储在云或集中式存储中，防止数据泄露或丢失。从技术和制度两个层面控制文件外泄，通过设置文件权限、加密等技术手段，以及制定严格的文件管理制度来保护文件安全。对于桌面系统，采用终端零管理和维护策略，只需远程维护虚拟机，并统一下发和管理策略，降低 IT 运维成本和复杂度。对安全通道进行严格控制，如磁盘、剪贴板的映射行为和 USB 外设的连接，通过 PID/VDI 设置黑白名单来限制非法设备接入。此外，采用水印防拍照技术，在终端设备屏幕上显示包含客户端 IP、连接时间、用户名等内容的水印，并在服务器端也设置水印，以防止屏幕信息被非法拍摄和服务器被非法访问。企业应定期开展数据安全、隐私保护等培训，组织开展网络教育宣传活动，协助保障数据安全；员工应强化个人自我保护意识，掌握隐私权限设置方法，严禁轻信不知来源链接^[5]；这些措施能协同构建起一个全面的数据安全和管理体系。通过构建协同治理架构，强化信息共享，实现联动合作，及时对网络空间数据安全问题进行处理。

3.3 精准识别企业协同办公数据安全管控

企业协同办公系统的数据安全至关重要，签署专属安全协议确保员工知情同意，合法合规。严格管理系统登录，防止非组织成员访问专属 APP，并限制部分员工加其他组织或个人好友。限制文件操作权限，移动端无法下载、编辑或复制协同工具的内容文件，禁止在线文档导出到本地或上

传本地附件。严格管理员工群，防止数据通过下载附件图片或转发给外部人员。可选全局明暗水印和防录防截功能增强安全性。账号与工作设备 MAC 地址绑定，防止非工作设备登录。精确设置沟通权限，根据个人、角色或部门间关系放行、审批或禁止。定义不同密级间的数据流转规范。授权或禁止具体 IP 地址段的特定动作^[6]。集成第三方 DLP 类系统，智能识读文件内容后自动打标分级并配置流转管控策略，全面保障企业数据安全。

3.4 完善数据安全管理体系建设

构建具有决策层、管理层、执行层、监督层的管理组织，明确具体的职责内容，同时要对各个岗位的权限进行合理规划，构建和谐的协作关系，构建更加系统完善的数据安全治理的责任体系。结合数据全生命周期特点和要求，对数据安全管理工作流程、方法、指南进行优化布控和实施，从而确保数据安全工作的持续性开展，强化安全管理有效性。《网络数据安全管理条例》要求构建完善的网络数据安全管理制度，且重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。此外，还需要完善网络数据安全管理工作流程，首先要完善账号权限申请流程，其次要完善数据处理场景各流程，最后要完善应急处理流程、安全事件处置流程、合规审计流程等^[7]。通过数据安全管理体系的建设，能够确保监管机构能够对数据安全进行有效检查，减少法律风险，防范网络数据安全事件。

3.5 提升企业研发数据的防泄密能力

为了提升企业研发数据的防泄密能力，整合一套全面的解决方案。首先，文件加密能力是关键，通过强制加密文档并对使用者进行透明解密，确保外发的文件无法直接使用，同时保持操作简单、应用方便且现场无痕。其次，文件审计能力对于流程解密、EOD 外发和特权解密等操作均能进行附件下载审计，确保文件流转的透明度。最后，外发控制能力能够对外发文件的打开方式、次数、阅读时长和使用权限进行严格控制，防止信息泄露。审计报表能力则实现了对身份和操作行为的完整记录、报表分析与查询，便于审计

追踪。风险预警能力针对文档解密等风险操作进行预警管理，基于日、周、月三个不同维度进行配置，提前防范潜在风险。最后，应用灵活能力根据业务实际情况进行结合，使文档管理更加灵活，达到“多方适应，技管结合，兼顾现状”的系统应用机制^[8]。这套解决方案将全面提升企业的研发数据防泄密能力，保障企业信息安全。

4 结语

综上所述，新时期，为了保障用户数据安全，避免隐私数据泄露，需要进一步优化建设网络空间治理体系建设，完善相关法律法规，强化安全防护技术，并提升公众的媒介信息素养教育，完善多方参与机制，促进网络空间治理体系的可持续发展。

参考文献

- [1] 叶小源,王维先.网络空间治理体系中用户数据安全及隐私保护研究[J].中国高校社会科学,2024(5):147-155+159.
- [2] 祝新宇.新时代网络空间治理能力研究的回溯与展望[J].科技传播,2024,16(12):30-33+39.
- [3] 徐素萍.我国网络空间治理立法的困境与对策[J].韶关学院学报,2024,45(4):41-48.
- [4] 董浩然,姜子云.网络治理视域下提升青年数字素养的路径[J].全媒体探索,2024(3):127-128.
- [5] 徐龙第.全球网络空间治理:核心问题、中国方案与未来方向[J].欧洲研究,2023,41(6):58-79+6.
- [6] 王宗强.新媒体时代的网络意识形态探究——评《网络空间意识形态安全治理体系研究》[J].中国教育学刊,2023(11):118.
- [7] 上海市长宁区人民法院课题组.网络空间治理体系和治理能力现代化目标导向下的互联网审判工作展望[C]//《上海法学研究》集刊——上海市法学会互联网司法研究小组论文集.[出版者不详],2019:10.
- [8] 张影强,宋煜,潘斐斐.全球网络空间治理现状及发展趋势[C]//国际经济分析与展望(2016—2017).中国国际经济交流中心信息部;中国社会科学院社会学研究所;互联网实验室,2017:15.