

网络个人信息安全与保护

李 赫

首都航天机械有限公司 北京 100076

摘 要: 数字化时代下, 网络服务深度融入生产生活, 个人信息数据的披露与流转频次持续提升, 信息安全隐患逐步凸显。数据采集不规范、存储传输防护薄弱、非法数据流转利用等问题, 持续侵扰网络用户隐私权益, 扰乱网络空间正常秩序。本文结合网络信息安全运行的实际现状, 梳理个人信息防护工作中的各类突出隐患, 剖析平台管控、技术防护、行业监管等层面的深层成因, 确立科学规范的防护原则, 从平台管理、技术升级、行业治理等多个维度搭建完善的保护体系, 全方位提升网络个人信息安全防护水平。

关键词: 网络空间; 个人信息; 信息安全; 隐私保护; 网络治理

引言: 互联网技术的快速普及, 推动各类线上服务场景不断丰富, 个人信息数据成为网络运行与数字服务开展的重要基础。日常网络交互、线上服务使用、社会化网络活动开展的过程中, 大量隐私信息持续产生、流转与留存。网络生态的快速迭代伴随多样新型安全风险, 数据泄露、隐私滥用、网络侵权等问题频繁发生。信息防护体系与动态网络环境适配不足, 防护短板逐步凸显。强化个人信息安全治理, 补齐网络防护漏洞, 能够有效维护网络用户合法权益, 维系稳定有序的网络运行生态。

1 网络个人信息安全现存隐患

1.1 个人信息采集存在随意性

网络平台与线上服务持续扩张数据获取边界, 个人信息采集的界定标准逐步模糊。服务运行所需的基础数据相对有限, 平台却不断延伸采集维度, 大量收录与核心功能无关的隐私内容。敏感个人数据无节制搜集、长期超额留存, 用户难以自主把控信息提交范围, 私人生活动对应的隐私空间持续收缩。线上产品信息采集环节普遍缺少标准化约束, 授权页面提示内容模糊隐晦^[1]。后台存在静默抓取、隐性收录等不规范操作, 用户常在不知情状态下完成隐私授权, 让数据采集过程彻底脱离人为可控范围。

1.2 信息存储传输存在安全漏洞

中小型网络平台普遍采用单一数据防护手段, 存储安全架构设计不够完善, 防护等级难以匹配海量数据的存储需求。系统留存大量未修复程序缺陷, 容易诱发数据外泄、内容篡改等安全问题。个人信息通过网络链路完成跨节点流转时, 防护覆盖存在盲区, 部分传输节点缺失加密设计。外部风险程序能够利用系统漏洞侵入传输链路, 窃取、拦截用户私密数据。平台对存储设备日

常运维较为松懈, 设备老化、系统更新滞后、后台权限松散等问题长期存在, 持续放大数据存储与传输阶段的安全隐患。

1.3 非法信息利用行为频发

分散留存于网络端口的用户数据, 容易被不法主体批量抓取、整合汇总, 逐步形成隐蔽封闭的地下信息流转通道。大量隐私数据在灰色渠道私自流转、违规交易, 脱离正规网络治理体系的约束。不法人员依托完整用户数据, 推送商业骚扰内容、开展精准网络诈骗、传播不实营销信息, 滋生多样侵权行为。个人数据脱离本人掌控后, 衍生多重侵害私人权益的网络乱象, 扰乱正常网络使用节奏, 破坏网络空间整体运行秩序。

1.4 用户自主防护意识存在短板

用户使用线上应用与网络服务时, 普遍存在隐私授权随意、权限开放过度的问题, 开放范围与时长缺少合理把控。用户对隐私权限管控缺乏严谨态度, 容易忽视权限过度开放带来的信息暴露风险。普通网民缺少稳定的风险辨识能力, 难以精准识别虚假链接、内嵌病毒程序、非合规授权场景。网络浏览、软件操作、线上交互的日常行为存在诸多不规范细节。不良上网习惯持续提升信息暴露概率, 让隐私数据长期处于不稳定的安全状态。

2 网络个人信息安全风险成因

2.1 网络平台管控体系不完善

互联网服务平台搭建的内部信息管控机制存在明显漏洞, 信息采集、储存、流转等操作环节, 缺少精细化管理规范与刚性约束流程。平台内部数据访问权限划分混乱, 岗位权责界定不清, 在岗人员能够随意调取、查阅后台留存的私密数据。人为操作失误或恶意泄密问题时有发生, 为内部信息泄露提供可乘空间^[2]。多数平台尚未建立常态化安全排查模式, 无法主动梳理日常数据管

理的疏漏,难以第一时间排查并修补内部管控缺陷。

2.2 网络技术防护能力存在短板

网络攻击与数据窃取手段持续迭代升级,主流防护技术的更新节奏滞后于风险演变速度,无法有效抵御新型窃取方式。信息加密、隐私脱敏、风险隔离等基础安全技术,尚未在行业内全面普及。多数中小型平台压缩安全防护投入,未部署成熟的数据防护系统,用户数据长期处于低防护存储状态。传统风险预警模式灵敏性不足,难以捕捉隐蔽化、碎片化的非法窃取行为,无法在风险萌芽阶段完成拦截与处置。

2.3 网络信息监管体系存在疏漏

现有网络安全监管覆盖范围存在局限,监管重心集中于主流大型平台,对小众服务端口、新兴社交场景的约束力度相对薄弱。个人信息流转链条冗长复杂,跨平台、多渠道的数据传输与交易行为,很难实现全程追踪与闭环约束。监管方式偏向传统固化模式,依赖人工排查与定期核查,适配新型信息泄露风险的能力不足,难以灵活应对持续变化的网络安全态势。

2.4 网络行业自律约束力度不足

网络行业尚未形成成熟稳定的安全自律氛围,部分市场主体片面追逐流量红利与经济收益,主动放宽信息安全管控标准。行业内部缺少统一通用的隐私安全管控准则,平台依据自身运营需求制定管理规则,造成行业防护水平参差不齐。针对违规采集、私自流转、非法使用个人数据的行为,行业内部缺少刚性约束手段,无法对违规经营主体形成有效震慑,难以规范整体数据运营生态。

3 网络个人信息安全保护原则

3.1 最小必要使用原则

网络服务运营全程需要严格把控信息采集尺度与使用边界,仅收录保障基础服务稳定运行、支撑核心功能落地的必要数据。彻底杜绝冗余、无关的隐私搜集行为,整治行业普遍存在的过度采集、盲目收录乱象。对信息采集品类、操作频次、覆盖范围实施精细化约束,从源头缩减隐私数据收录体量。规范个人数据二次利用渠道,禁止未经授权的重复调用与跨领域流转。精准锁定数据传播与扩散边界,依托源头管控筑牢隐私保护第一道防线^[1]。平台需要根据业务功能划分数据采集清单,精准区分必填信息与选填信息,杜绝捆绑式采集与强制性授权行为。严格限制已采集数据的复用场景,杜绝跨业务、跨板块的无授权数据流转与资源调用。

3.2 全程可控防护原则

个人信息生命周期涵盖采集录入、静态存储、网络

传输、场景应用与最终销毁多个阶段,需要对全部流程落实常态化防护与动态管控。系统梳理信息流转链条中容易出现泄露、篡改、窃取的风险节点,结合各阶段运行特征匹配对应防护手段。逐一对标清除流程潜藏的安全盲区,补齐碎片化管控造成的防护短板。维持全程管控节奏连贯统一,规避阶段性管控松弛引发的安全隐患。通过全流程跟踪模式,实现个人数据流转轨迹可溯源、管控可落地。

3.3 动态适配防护原则

网络场景保持持续迭代状态,信息安全风险不断衍生全新形态,传统固化的防护模式难以适配复杂多变的网络生态。贴合网络环境演变规律,阶段性优化现有防护方式与管控机制。针对全新风险形态与新兴服务模式,及时补齐防护短板,细化不同场景的管控执行细则。根据网络生态动态特征持续升级防护架构,完善分层分类的安全防护体系,灵活应对各类新型网络安全威胁。紧跟网络服务模式与网络攻击手段的迭代节奏,定期复盘现有防护体系的适配短板。针对新兴短视频、即时社交、云端共享等新型场景,定制差异化防护方案,消除新增场景下的安全管控空白。

3.4 多方共治联动原则

信息安全防护工作无法依靠单一主体完成,需要整合平台运营方、网络用户、监管部门等多元主体协同参与。搭建互联互通、联动协作的共治格局,打破单一主体独立防控的局限。清晰划分不同主体在隐私保护、风险排查、隐患治理中的工作内容与责任边界。打通主体间协作壁垒,建立顺畅的工作对接与风险处置链路。聚合多方防控力量与资源优势,层层夯实网络个人信息安全防护根基。

4 网络个人信息安全保护优化路径

4.1 规范平台信息管理机制

平台作为个人信息归集与处理的核心载体,需要持续优化内部数据管理体系。围绕信息采集、静态存储、跨场景流转等关键环节,制定严谨细化的管控规范与操作标准,约束平台日常数据处理行为。整治超额收录、过度采集、无节制索取隐私数据等问题,从业务源头规范数据获取逻辑。系统梳理内部岗位的数据操作权限,明确信息查阅、后台调取、业务复用的边界标准,规避权限无序开放带来的安全风险。精准排查封堵内部操作漏洞,切断数据违规流出的传播渠道。搭建长效安全自查机制,定期筛查数据管理、权限分配、流程运行的隐性隐患,实现隐患问题常态化排查与闭环整改。对内部岗位权限实行分级授权、按需赋权模式,清理冗余账号

与无效权限,杜绝超范围数据操作^[4]。建立数据操作全程留痕与异常预警机制,针对高频调取、批量导出等风险行为及时拦截核查,压实内部数据管理责任。

4.2 升级网络安全防护技术

全面落地数据加密、信息脱敏、内容匿名化等基础防护技术,让安全手段覆盖数据存储与网络传输全流程,夯实平台基础防护能力。依托专业技术弱化原始隐私数据的可识别特征,降低数据泄露引发的权益损害风险。持续优化风险识别、主动拦截、提前预警的技术体系,升级风险甄别逻辑与处置机制,高效应对隐蔽化、碎片化的数据窃取与网络攻击行为。紧跟网络风险迭代节奏,持续推进防护技术更新升级,弥补传统防控模式的固有短板。适配新型风险演变特征优化技术防控架构,搭建稳定性强、适配范围广的智能防控体系。引入智能风控算法对数据流转行为进行实时研判,精准识别异常访问、批量抓取、跨域传输等风险行为。对存量数据开展定期脱敏优化,对增量数据落实加密存储,全方位提升数据抗窃取、抗破解能力。

4.3 完善全域网络监管模式

拓宽网络信息安全监管辐射范围,突破传统场景局限,将新兴网络服务、小众运营端口、新型交互模式纳入常态化监管范畴。结合个人信息跨平台传播、多渠道流转的复杂特征,出台针对性管控细则与治理举措,搭建完整的数据流转追踪体系。完整记录信息采集收录、流转共享、落地应用的全链条轨迹,实现动态溯源、全程可控。突破传统固化监管思维,引入智能动态监管工具,优化风险筛查方式。提升风险识别精准度,缩短隐患处置响应周期,全面强化网络空间个人信息监管质效。依托数字化监管平台实现全网数据动态监测,对小众平台、新兴服务场景开展常态化抽查核验。打通跨平台数据溯源通道,精准定位违规采集、私自流转的数据源头,实现隐患快速处置、违规快速追责。

4.4 强化用户自主防护能力

推进常态化网络安全科普宣讲,面向全网用户普及隐私保护、权限管控、安全上网的实操知识。引导用户正视隐私数据的价值,规范应用授权行为,理性把控权限开放尺度。逐步提升用户对恶意程序、虚假链接、伪造场景的分辨能力,精准识别潜藏的网络风险。规范日常浏览、线上交互、软件操作的行为细节,规避不当操

作引发的信息泄露问题。引导用户养成严谨规范的上网习惯,主动排查日常场景中的隐私隐患,持续提升自主防护水平。针对不同年龄段、不同网络使用群体开展分层科普,细化隐私授权、权限关闭、风险甄别等实操教学内容。引导用户定期清理闲置应用、关闭无效授权,从个人操作层面减少隐私暴露的各类风险隐患。

4.5 压实行业自律约束效能

搭建统一通用的行业信息安全管理标准,规整不同规模、不同类型平台的数据防护规范,统一行业安全管理尺度。激活行业内部监督动能,构建自我约束、互相监督的良性治理格局,整治违规采集、私自流转、滥用数据等不良业态。深耕行业诚信体系建设,将信息安全合规情况纳入日常运营考核。细化市场主体经营约束规则,规范线上服务的数据处理流程,推动行业培育合规有序、安全稳定的经营生态。搭建行业信息安全互评机制,定期开展平台合规性核验与安全评级公示^[5]。对存在违规数据操作的经营主体开展行业通报,限制其运营权限与流量资源,以行业约束推动平台规范数据运营行为。

结束语

网络个人信息安全治理是一项长期性、系统性的工程,贯穿数据生成、流转、应用的完整生命周期。信息采集不规范、技术防护薄弱、监管体系不完善等现存问题,共同构成隐私安全的主要风险来源。依托科学的防护原则优化治理模式,持续规范平台数据管理机制,升级网络安全防护技术,完善全域监管体系与行业自律机制。多维度补齐信息安全防护短板,能够有效化解各类隐私泄露风险,持续净化网络空间环境,为数字网络生态的良性发展筑牢安全根基。

参考文献

- [1]平亚鸽.基于网络空间安全的个人信息保护研究[J].网络空间安全,2024,15(4):47-51.
- [2]姚锐.网络安全等级保护在信息安全建设中的应用[J].无线互联科技,2023,20(20):152-154.
- [3]杨新涛,李文朋,常津铭.信息安全、网络安全与隐私保护的研究[J].信息系统工程,2023(9):138-141.
- [4]王辰宇.网络信息安全对个人隐私权保护的影响研究[J].警戒线,2025(5):29-32.
- [5]李远海,翟岩,李小波.数字平台个人信息安全风险的发生逻辑与应对策略[J].信息安全研究,2026,12(5):445-451.