文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

大数据时代下的个人信息安全挑战与保护

时惠
DOI:10.12238/etd.v5i4.8579

[摘　要] 随着信息技术的飞速发展和互联网的广泛普及,大数据时代已经到来。大数据主要是指通过收集大量的公开信息,使用相关算法对收集到数据进行处理与分析,从而发现其中的价值。但人们沉浸于大数据所赋予的便捷与高效之中时,也面临数据泄露、网络攻击等安全威胁。本文深入分析了大数据时代下个人信息安全面临的挑战,并提出相应的应对策略,为个人信息保护提供了理论支持和实践指导,也为应对当今数字时代信息安全面临的复杂挑战提供深刻洞察。
[关键词] 大数据；个人信息保护；信息安全
中图分类号：TN911.2　文献标识码：A

Challenges and Protection of Personal Information Security in the Era of Big Data

Hui Shi

[Absrtact] With the rapid development of information technology and the widespread popularity of the Internet, the era of big data has arrived. Through collecting a large amount of public information, relevant algorithms are used to process and analyze the collected data, so as to discover its value. But when people immerse themselves in the convenience and efficiency provided by big data, they also face security threats such as data breaches and network attacks. This article deeply analyzes the challenges faced by personal information security in the era of big data, and proposes corresponding response strategies, providing theoretical support and practical guidance for personal information protection, as well as profound insights for addressing the complex challenges faced by information security in today's digital age.
[Key words] big data; Personal information protection; Information security

引言

随着云计算技术的蓬勃兴起与互联网技术的日新月异,我们正步入一个前所未有的技术繁荣时代。个人信息的采集、存储、处理和应用变得前所未有的便捷和高效,大数据深刻改变着我们的生活方式、工作模式乃至社会结构,在这个数据为王的时代,在享受从海量有价值信息中获取的社会生活便利时,人们也不得不面对一个严峻的现实:信息服务在提升生活质量的同时,也潜藏着个人信息被滥用、侵犯、泄露乃至不正当使用的风险。这种双刃剑效应要求我们在享受技术红利的同时,必须高度重视并加强个人信息的保护与管理,以确保技术的健康发展能够真正惠及每一个人。根据威胁猎人发布的《2024年上半年数据泄露风险态势报告》,2024年上半年全网范围内监测到的有效数据泄露事件达到了惊人的16011起,与2023年下半年相比激增了59.58%。个人信息安全面临着一系列的挑战。首先,数据采集手段多样化,智能设备、传感器等无时无刻不在记录着人们的个人信息,这些数据在采集、传输、存储和使用过程中均存在被泄露或滥用的风险。其次,大数据的潜在价值吸引了不法分子的关注,他们利用技术手段非法获取、贩卖个人信息,给个人财产和隐私安全带来严重威胁。此外,公众信息安全意识薄弱,对大数据信息安全的重要性认识不足、对大数据信息安全知识学习不够,法律法规不完善以及监管力度不足等问题也加剧了个人信息安全的风险。因此,如何有效应对大数据时代下的个人信息安全挑战,构建完善的保护策略体系,已成为亟待解决的重要课题。

1 大数据时代的特点

1.1大数据基本介绍

大数据即对数据进行存储、处理、分析、建模、AI等一系列的计算和应用,具有数据量非常大、数据处理需求量大、数据种类和来源多等特性。随着科技的不断发展,大数据与物联网、云计算等技术有机融合,为大量数据信息处理提供了可靠的技术支持。大数据的价值在于其能够通过对海量数据的分析和挖掘,通过深入剖析数据背后的深层信息与潜在规律,为企业的战略决策提供强有力的数据支撑,同时也为政府部门的科学管理提供精准的依据。为个人的生活带来便利。

1.2数据分析的特点

在大数据时代,数据分析不再依赖于随机采样,而是通过收集处理和某个特别现象相关的所有数据,这使得可以分析的数

据更多,数据误差更小,更具有权威性。随着数据规模的增大,不再需要过度的追求精准度,只需通过大数据掌握大概的目标方向进行研究,并且在大数据时代下,不再刻意追求事物之间的因果关系,而是去找寻事物之间的相关关系,通过寻找相关关系,即可判断哪件事情可能或者是正在发生。

1.3大数据与信息安全的关联

大数据与信息安全之间存在紧密的关联,这种关联涉及多个方面,包括大数据分析与信息泄露、风险评估与漏洞分析、威胁检测与安全监控以及隐私保护的技术手段。大数据分析是信息化中的重要工具,但它也带来了信息安全方面的挑战。可能导致信息泄露,通过对大数据集进行分析,可能会揭示出包括个人身份、财务信息和其他敏感数据在内的敏感信息;一旦这些信息被泄露,可能会导致严重的隐私侵犯和金融损失,因此,确保大数据分析过程中的数据隐私和安全变得至关重要。

2 个人信息安全面临的挑战

2.1个人隐私信息泄露严重

大数据时代,每个人都是数据生态中不可或缺的贡献者,我们的日常行为与信息交流不断为数据海洋注入新的能源。然而,随着个人信息的不断贡献,信息泄露与安全隐患也日益凸显,成为了一个不容忽视的严峻问题。智能手机、运动手表、智能手环等智能设备已经深深融入人们的日常生活,各类智能化应用程序(APP)如雨后春笋般涌现,极大地丰富了人们的生活体验,让科技触手可及,为日常生活带来了前所未有的便捷与乐趣,越来越多的人使用移动设备进行社交活动,这些APP存储了大量的个人信息和隐私数据,除此之外,众多手机APP在收集其正常运作所必需的基本数据之余,往往还会悄无声息地获取远超其服务范畴的大量个人隐私信息,包括但不限于用户的地理位置、通话详情、联系人列表,甚至通过麦克风监听与摄像头访问等方式收集敏感数据。在大数据的浪潮之下,个人隐私数据的掌控权已悄然从用户手中转移,如果第三方服务存在安全漏洞或不当行为,个人信息就可能面临泄露风险,一旦用户数据被窃取,不法分子通过对零散数据的深入分析,挖掘整理出有效的数据,并关联分析出更深层次的信息,这些信息可能被用于不正当目的。

2.2数据安全防护体系脆弱

大数据的处理和存储依赖于复杂的技术系统,这些系统往往存在未知的漏洞和缺陷,容易被攻击者利用,比如黑客使用各种手段对移动社交平台发起攻击,旨在窃取用户的个人敏感信息与隐私数据,给用户的网络安全构筑起一道难以逾越的阴影。更为严峻的是,随着数据类型的日益丰富和网络传播形式的多样化,特别是云计算与云服务技术的广泛普及,大量个人隐私数据被上传至云端存储。这一趋势使得黑客只需成功入侵一个云服务器,便能轻易获取到海量的个人数据,从而进一步加剧了个人隐私泄露的风险与危机。

2.3管理漏洞

信息安全的保障,除了依赖先进的技术手段外,更离不开个人信息安全意识的提升以及企业自身的安全防范与管理能力。制定并执行科学合理的安全操作流程、严格细致的权限管理机制以及定期的安全评审流程,对于构筑企业信息安全防线、防范潜在风险具有至关重要的作用。众多企业和机构追求经济效益,不重视用户个人信息的保护工作,忽视用户隐保护私的重要性,信息安全防护体系与管理制度的缺失或不完善,为外部攻击者打开了方便之门,使得用户数据面临严重的泄露与滥用风险。此外,部分移动社交平台在用户数据处理上,存在显著的尊重与保护意识缺失问题。它们倾向于将用户数据视为可随意支配的商业资源,进行不当利用。具体表现为,在未经用户明确同意的情况下,擅自将用户的个人信息转交给第三方,这种不负责任的行为直接导致了用户隐私的严重泄露。

2.4隐私保护难度加大

随着互联网信息技术的日新月异,个人信息的曝光度显著增强,成为了各类数据分析技术竞相争夺的宝贵资源。这一现象促使了数据分析技术的多样化与快速迭代,但同时也带来了一个不容忽视的副作用：IT技术架构正逐步向更加集成化、开放化的方向发展。这种转变意味着技术系统间的界限逐渐模糊,数据流通更加频繁,但同时也对系统的安全性、隐私保护以及数据治理能力提出了更高的要求。比如,人们在互联网上的搜索内容、言论等的捕捉越来越容易,攻击者通过多种手段收集个人在社交网络上的信息、电子邮件内容、微博动态、手机号码以及家庭住址等敏感资料,从而更加精确地锁定目标个体,网络欺诈也更有针对性和欺骗性,家与广告商会不遗余力地搜集与整合个人信息,旨在实现精准营销,网络暴力、人肉搜索也利用大数据的力量,恶意使个人的隐私数据暴露于网络之上,给受害人造成极大的伤害,这不仅对数据安全及个人隐私,甚至社会安全都会构成较大的安全隐患。

3 个人信息安全保护对策建议

3.1加强法律法规建设

政府应该加强对信息安全的监管,制定和完善相关法律法规,明确数据收集、处理、存储和传输的规范和要求,为数据安全提供法律保障。首要之务,法律法规应清晰界定信息保护的具体范畴与内容。这一范畴应广泛覆盖个人信息、商业机密以及国家安全等多个层面,其中,个人信息作为核心组成部分,其保护力度亟需加强。其次,鉴于现代社交媒体行业的迅猛发展态势,以及用户个人信息泄露途径的不断演变与复杂化,我们亟需紧跟时代步伐,对相关法律法规进行适时调整与优化。最后,法律法规应当详尽阐述信息保护的具体措施与手段,以构建坚实的信息安全防线。这包括但不限于设立专门的信息安全监管机构,以强化对信息安全领域的监督与管理,确保各项安全规范得以有效执行；同时,构建完善的信息安全技术体系,运用先进的技术手段提升信息安全防护能力,为个人信息、商业机密及国家安全等敏感信息提供全方位、多层次的保护。另外政府要加强对数据安全和隐私保护的执法力度,对于非法采集、滥用、泄露用户隐私信息的行为,出台严厉的惩戒措施,包括高额罚款、吊销经营许可、追究刑事责任等形成有效的法律震慑。

3.2提升个人信息安全保护意识

近年来,公民个人信息安全问题频发,其背后的重要原因之一是信息安全意识的普遍薄弱以及网络安全管理体系的不完善。鉴于智能手机APP频繁未经用户同意就肆意收集个人隐私信息的现状,用户在安装应用时需保持高度警惕。这些APP往往在用户不知情的情况下,以各种手段请求并获取包括通话记录、摄像头访问、录音权限及位置信息等在内的敏感隐私权限。为最大限度减少此类权限滥用,用户应养成定期检查并优化手机APP权限设置的习惯,确保每个应用仅获取执行其必要功能所需的权限,防止权限范围的不当扩张。此外,用户应坚决避免安装来源不明的软件,这类软件往往是黑客攻击和个人信息泄露的高风险源。在日常使用各类软件时,用户应时刻将隐私保护放在首位,定期运行手机杀毒软件以清除潜在威胁。同时,应坚决拒绝访问任何来历不明或非法网站,这些网站可能含有恶意软件、钓鱼链接等有害信息,对用户的个人信息安全构成严重威胁。总之,保持高度警觉,采取积极措施,是保护个人隐私信息不被泄露的关键。

3.3提升技术防护能力

在大数据时代背景下,海量的数据资源被存储于计算机网络中,这些数据资源成为网络黑客的恶意攻击或窃取的目标,个人信息泄露的严峻形势在很大程度上归咎于计算机信息安全技术的相对滞后。为了有效抵御个人信息被非法侵扰的风险,我们亟需提升大数据信息安全防护技术的整体水平,这意味着需要不断研发和创新更为先进、高效的信息安全技术,以应对日益复杂多变的安全威胁,企业更应建立多层次、全方位的安全防护体系,包括网络层、系统层、应用层和数据层等各个层面的安全防护措施,利用数据加密技术对信息进行加密,实现信息隐蔽；用防火墙、入侵检测、漏洞扫描等技术手段,及时发现和抵御网络攻击;通过定期的安全审计和风险评估,及时发现和纠正潜在的安全隐患。鼓励和支持数据安全技术的研发和创新,如人工智能、区块链等新技术在数据安全领域的应用。这些新技术可以提供更高效、更安全的数据处理和保护手段。

3.4建立健全管理制度

建立完善的个人信息保护内部管理制度,包括数据收集及使用、存储及传输、共享及销毁等各个环节的规范,切实提升企业社会责任感,提高用户数据保护水平。行业协会或相关机构应联合制定APP个人信息收集、使用、存储的行业标准,包括最小必要原则、数据加密标准、用户同意机制等,规范各种APP获取用户个人信息行为,明确信息收集范围、目的、方式及保护措施,确保合法合规。同时企业内部定期对员工进行个人信息保护法律法规、企业规章制度及道德准则的培训,提升行业从业人员的法律意识、隐私保护意识和职业道德水平,定期对个人信息保护工作进行定期审计与评估,及时发现和纠正存在的问题,鼓励主动发现并纠正个人信息处理中的违规行为。企业应制定数据安全应急响应计划,明确应急响应流程和措施。在发生数据泄露等安全事件时,能够迅速启动应急响应机制,采取有效措施减少损失和影响。

4 结语

大数据时代的到来,为社会的整体生产效率带来了质的飞跃。然而,这一进步是双刃剑,伴随而来的是日益严峻的信息安全问题,时刻威胁着每个人的个人隐私信息安全,让人们在享受科技便利的同时,也不得不面对这一不容忽视的挑战。提高大数据时代的信息安全需要从法律法规、技术防护、管理制度、个人信息保护和技术创新等多个方面入手,通过综合施策、协同推进,构建一个安全、可信、有序的大数据生态环境。

[参考文献]

[1]周敏,郅慧.感知信息过载对社交媒体用户隐私披露意愿影响的实验研究[J].新闻大学,2023(5):12-28,118-119.

[2]帅斌.新媒体环境下移动社交领域个人信息保护现状与对策研究[J].新闻研究导刊,2023,14(22):76-79.

[3]张芳菲.新媒体环境下个人信息保护探究[J].文化学刊,2023(3):129-132.

[4]彭丽徽,蒋欣.风险认知视域下社交媒体用户健康信息规避行为生成机理研究[J].图书情报工作,2022,66(22):55-65.

作者简介：

时惠(1995--),女,汉族,山东省德州市齐河县人,硕士,研究方向：信息通信。