大数据时代个人信息安全防护

洪斌
金华市金东大数据技术有限公司

摘　要：随着科技的不断进步，大数据已逐渐成为现代社会中一个不可忽视的重要资源。然而，随之而来的是个人信息安全问题面临着诸多的挑战。本文将概述大数据的内涵，探讨大数据时代个人信息安全风险及其成因，并提出相应的安全防护措施，以确保个人信息在这一信息爆炸的时代得到充分的保护。期望本文能够为相关工作者带来一定的参考作用。

关键词：大数据时代；个人信息；安全；防护
【DOI】10.12252/j.issn.2096-6261.2022.03.121

一、大数据概述

随着信息技术的飞速发展，社会已经步入了一个数字化、信息化的时代。在这一时代背景下，大数据逐渐成为一个炙手可热的概念。所谓的“大数据”并非单纯指数量的数据，而是指数据的规模大、种类多，在不同领域中起着重要的影响力。这些数据大多来源于社交媒体、传感器、交易记录、日志文件等多种渠道，能够以惊人的速度增长，影响人们生活的方方面面。

大数据的核心特征可被总结为“3V”：Volume（数据量大）、Velocity（数据生成速度快）和Variety（数据多样性）：首先，大数据的规模十分庞大，这意味着以往的数据存储、处理方式已无法胜任大数据时代的要求；其次，数据生成的速度十分迅猛，计算机需要对数据进行实时处理，以方便人们利用这些数据；

最后，数据的多样性指的是数据的类型和结构多种多样，既包括结构化数据如数据库记录，也包括半结构化和非结构化数据如文本、图像、音频等。

大数据的应用价值十分显著。通过对大数据实施分析，可揭示出隐藏在其中的模式、趋势和规律，从而为个人及企业的决策提供有力支持。在商业领域，大数据可帮助企业了解消费者行为，预测市场趋势，优化供应链管理，提高经营效率[1]；在科研领域，大数据有助于揭示科学规律，推动医药研发，应对气候变化等全球性问题；在社会管理层面中，大数据可用于进行城市规划、交通管理，使人们的社会生活变得更为有序。

然而，目前对大数据的应用也面临着一系列挑战，其中之一就是个人信息安全问题。在大数据时代中，个人的各类信息正在被不断采集、传输、存储和分析。社会中数据泄漏事件屡见不鲜，为个人隐私造成了极大的威胁。因此，有必要加强对大数据时代个人信息安全防护的研究，从而更好地发挥大数据的潜力，适应信息爆炸时代的要求。

二、大数据时代个人信息安全风险及原因

（一）网络安全风险

在这信息时代，网络时刻影响着人们生活、工作的方方面面。然而，随着网络的普及，网络安全问题也日益凸显，在大数据时代，这种问题变得更为严重，对个人信息安全构成了严重的威胁。其中，网络非法入侵、木马程序和病毒等威胁，逐渐成为主要的个人信息安全风险。

其中，网络非法入侵主要是指未经授权的人或程序进入系统、网络或手机应用的行为。黑客可通过各种手段突破网络的防线，获取敏感信息，窃取个人信息，这可能会导致身份盗用、金融欺诈等严重的后果；木马程序是一种潜藏在正常程序中的恶意代码，一旦计算机被植入这种程序，黑客就可在背后控制受感染的计算机，获取用户的隐私信息；计算机病毒则是一种能够自我复制并传播的恶意软件，它可损坏计算机系统、盗取信息，对个人信息安全构成威胁。

（二）网络安全风险成因

网络安全风险成因极其复杂，涉及技术、人员、管理等多个方面：

①网络先天存在缺陷：网络系统的构建与设计本身就是一项具有高度复杂性的工作，如若网络设计本身存在漏洞，攻击者可利用这些漏洞入侵网络，获取用户信息。实践中，虽然网络安全专家会不断修补这些漏洞，但新的漏洞也会不断形成，对个人信息安全构成威胁[2]；②计算机软硬件问题：计算机系统的软硬件存在问题，也可能导致系统出现漏洞。如，操作系统、应用程序等软件存在错误，会为黑客的侵入提供契机，同时，不及时更新软件和系统也会增加安全风险；③木马病毒：木马病毒是恶意软件的一种，可潜藏在正常的程

序中，不易被发现。黑客可通过木马病毒获取用户的敏感信息，控制计算机；④缺少网络维护：一些企业和个人在网络维护方面缺乏投入，未能及时发现、修补已知漏洞，这为攻击者提供了机会；⑤缺乏安全意识：个人和企业缺乏足够的网络安全意识，容易在浏览网页、下载附件的过程中暴露个人信息。同时，密码设计过于简单、随意共享信息等也是网络安全意识不足的表现，这也容易导致网络被入侵。

三、大数据时代个人信息安全防护措施

（一）加强网络环境管理

在当今大数据时代，加强网络环境管理，逐渐成为保护个人信息安全的必要之举。有效的网络安全管理不仅有助于降低风险，防止信息泄漏，还能够提升数据的机密性和完整性，使人们得以更好地享受大数据带来的便利。基于此，需要采取一系列切实可行的措施，构建更加安全可靠的网络环境。

首先，可建立更为完善的网络安全制度。举例而言，在企业内部，针对不同的管理层级和各个部门，应制定相应的网络安全规定，明确各部门的责任和义务。在这些制度中，应涵盖各种安全管理内容，如访问控制、数据加密、安全审计等。通过建立规范和明确的制度，可有效地规避安全漏洞和风险。

其次，也应构建完善的信息安全规章制度。在企业和组织内部，针对网络设备采购、使用、维护，以及数据的存储、处理、传输，有必要建立全面的信息安全管理机制，规范相关人员的操作流程，从而减少潜在的漏洞和隐患，为网络安全提供更加牢固的保障。

再次，坚持从严管理是确保信息安全的关键。针对企业内部的信息安全管理，需要建立起一套严格的流程和标准。对于那些违反安全政策的行为，必须采取相应的惩罚措施，以保持制度的严肃性和有效性。只有管理得当，员工才会更加认真地遵守安全规定，从而确保网络环境的安全。

最后，在社会层面，应当建立完善的信息安全法律。政府应当积极出台相关的法律法规，明确网络安全的法律责任，并建立相应的追究机制。这些法律在实际实施中，不仅能够为网络安全保护提供明确的法律依据，还促使企业和个人更加重视网络安全维护。总之，信息安全法律的存在，将为个人信息的保护提供有力支持，有助于构建更加安全的网络环境。

（二）针对信息人员加强管理

在大数据时代，信息人员往往会成为大数据技术的直接使用者，因此加强对他们的管理和培训有着重要的意义。具体而言，所谓的“信息人员”主要包括企业员工、系统管理员、开发人员等，他们的安全意识和操作水平，直接影响着网络的安全性。如下列举针对信息人员的管理策略：

①信息安全培训：企业应定期为员工提供信息安全培训，增强他们对网络风险和安全措施的认识。具体的培训内容可包括网络威胁的类型、识别恶意链接和附件的方法、密码管理等。在培训过程中，应当培养员工的安全意识，使他们能够警惕社会工程学攻击、钓鱼邮件等欺诈行为。应强调个人信息的重要性，增强他们对信息保护的责任感[3]；②访问控制和身份认证：对于有权限访问大数据的人员，需要实行严格的访问控制和身份认证机制，通过多重因素认证、访问审计等手段，限制未经授权的访问，维护网络信息安全；③保护用户隐私：员工在使用大数据分析工具时，要有意识地保护用户隐私，不应滥用数据，也不应窥探用户的个人信息；④持续监测和评估：应建立定期的安全评估和监测机制，及时发现、解决员工在信息安全方面遇到的问题，确保信息人员的操作始终符合安全标准。

（三）应用与推广新技术

在大数据时代，为了更好地应对个人信息安全风险，必须不断应用和推广新技术，有效地提升网络安全防护水平，减少信息泄漏的风险。如下列举具体的对策：

①防火墙技术：防火墙是一种位于网络之间的安全设备，可监控和控制网络流量，阻止未授权访问。它可设置规则，限制来自外部网络的访问，从而隔离内外网络，防止攻击者入侵。不论是企业还是个人，都应在网络中部署防火墙，加强网络边界防护；②入侵检测系统：入侵检测系统（IDS）能够实时监测网络流量，识别异常行为和攻击。一旦发现可疑活动，IDS会发出警报，帮助管理员及时采取措施，这可大大缩短攻击者的滞留时间，减少风险；③防病毒技术：利用防病毒技术，可检测和清除计算机系统中的恶意软件和病毒，及时发现并处理潜在的威胁，保护系统免受病毒侵害。企业和个人应当定期更新防病毒软件，确保其数据库中包含最新的病毒定义；④加密技术：加密技术在使用中，可将敏感数据转化为密文，在传输和存储过程中保护数据的安全性。此种情况下，即使攻击者获取了加密数

据，由于没有密钥，也无法解读其中的内容。因此，通过使用加密技术，可有效地防止数据泄漏；⑤多因素认证：传统的用户名和密码认证容易受到黑客的攻击。多因素认证（MFA）引入了多个验证要素，如密码、指纹、手机验证码等，这样，即使攻击者获取了某个因素，仍然需要其他因素的认证才能够进入网络，如此便提高了系统的安全性；⑥人工智能和机器学习：人工智能和机器学习技术可对大量的网络数据进行分析，识别出不寻常的模式和行为。它们可自动学习网络的正常状态，并在检测到异常时发出警报。通过使用这种技术，网络使用者可在更早的阶段发现威胁，提高网络安全性；⑦漏洞扫描和修复：利用漏洞扫描工具，可自动检测系统中存在的安全漏洞，并提供修复建议。企业可定期运行这些工具，及时修补系统中的漏洞，减少被攻击的风险。

（四）实施智能化的信息安全保护

随着科技的不断进步，人工智能（AI）和大数据分析技术日益成熟，智能化的信息安全保护逐渐成为一个全新的研究课题。通过将人工智能和大数据应用于信息安全领域，可更加高效地识别和应对各种网络威胁，保护个人信息安全。下面将探讨如何实施智能化的信息安全保护：

①智能分析网络行为：人工智能可对网络流量进行实时分析，识别出正常和异常的网络行为。通过建立模型，AI能够学习和了解正常的网络活动模式，一旦检测到异常行为，如大规模数据传输、频繁登录失败等，系统可自动发出警报，提醒管理员采取措施[4]；②异常检测和预测：基于大数据分析，智能系统可识别出潜在的威胁和漏洞。通过分析历史数据，AI可以预测未来可能出现的安全问题，并采取相应的预防措施，从而在安全威胁发生之前就进行干预；③智能风险评估：利用智能化系统，可对系统和网络进行全面评估，识别出可能存在的安全风险。具体而言，这种系统可分析网络拓扑、设备配置、软件漏洞等因素，并给出风险评分和建议，帮助管理员及时改善安全管理措施；④自动化响应：在检测到异常威胁时，智能化系统可自动采取响应措施，如封锁恶意IP地址、隔离受感染的设备等。通过这种自动化响应，可显著减少攻击者的影响范围，降低损失；⑤智能日志分析：借助大数据分析技术，可对系统日志进行深入分析，发现异常的活动。使用智能系统，可自动对大量的日志数据进行处理，快速识别出与安全有关的事件，帮助管理员及时发现和解决问题[5]；⑥自学习和适应：实际应用中，AI系统可不断学习和适应新的网络威胁和攻击手法，从而不断提升其识别和应对能力。随着时间的推移，智能系统会变得越来越准确和高效；⑦智能安全意识培训：通过人工智能，可为员工提供个性化的安全意识培训。系统可分析员工的网络行为，根据其特点提供相应的安全提示和培训，帮助员工更好地识别威胁、采取防护措施。

然而，现阶段看来，实施智能化的信息安全保护也需要企业或个人解决一些问题：首先，对智能系统的训练需要用到大量的数据信息，由此而来的隐私与合规问题需要被考虑；其次，实际应用中，智能系统可能会出现误报或漏报的情况，需要不断进行调优和改进；最后，黑客也可能利用智能技术进行攻击。基于此，有必要在大数据时代下，不断探索智能化的个人信息安全防护策略，推动这一领域的持续发展。

结语

总而言之，在大数据时代，个人信息安全问题日益凸显。网络安全风险的存在使得企业与个人必须采取一系列的防护措施。通过加强网络环境管理、针对信息人员加强管理、应用新技术以及实施智能化的信息安全保护，可确保个人信息安全，更好地发掘、发挥大数据技术的潜力，享受大数据带来的便利。通过政府部门、企业及个人的共同努力，相信大众可在大数据时代，更加安全地使用和管理数据信息。

参考文献

[1]李鹏举.大数据背景下计算机信息安全体系研究[J].数字技术与应用，2021，39（06）：183-185.

[2]郭森芳.计算机信息安全管理存在的问题及对策[J].信息与电脑（理论版），2020，32（11）：229-230.

[3]诸世华.探讨通信计算机信息安全问题及解决方案[J].智能城市，2020，6（10）：244-245.

[4]薛俊海，李晋泰，张承，栗志新.大数据技术在计算机信息安全中的应用研究[J].网络安全技术与应用，2021（02）：70-71.

[5]魏忠，李光明，郭盛刚，李群，姜向宏.大数据时代下的计算机网络安全及防范对策探讨[J].电脑知识与技术，2020，17（30）：68-69.