

# 数字经济背景下的数据安全治理

巫 健

武昌职业学院 湖北武汉 430200

**摘要：**数字经济的迅猛发展已经改变了商业和社会的格局，然而，随之而来的是日益增多的数据安全威胁和隐患，本文旨在探讨数字经济背景下的数据安全治理，分析数字经济对数据安全的影响，并提出相应的应对策略。通过对数字经济时代的数据安全挑战的深入剖析，本文旨在为组织和决策者提供有关如何保护和管理数据安全的见解，以期促进数据安全治理行业的进步。

**关键词：**数字经济背景；数据安全治理；策略

## 引言：

随着信息技术的不断进步和数字化转型的推进，数字经济已成为当今世界的主要驱动力之一，数字经济的核心是数据，企业和政府机构日益依赖于数据来推动创新、提高效率和满足客户需求。然而，随着数据的普及，数据安全威胁也呈指数级增长，数据泄露、网络攻击、恶意软件和隐私侵犯等问题已成为数字经济时代的现实挑战。数据安全治理在这一背景下变得至关重要，数据安全治理不仅关系到组织的声誉和财务稳定，还关系到个人的隐私和权益，因此，本文将深入研究数字经济背景下的数据安全治理，并提出有效的应对策略。

## 一、数据安全治理的含义

数据安全治理是一种组织内部和外部的管理框架，旨在确保数据的保密性、完整性、可用性和合规性，这个概念涵盖了一系列策略、政策、流程和技术措施，以管理和保护数据，以降低数据泄露、滥用和其他潜在威胁的风险。

### 1. 数据安全治理的主要目标

(1) 数据保密性：确保只有授权的用户能够访问敏感数据，防止未经授权的访问或泄露。(2) 数据完整性：防止数据被篡改、损坏或意外修改，以确保数据的准确性和可信度。(3) 数据可用性：确保数据在需要时可用，防止数据丢失或不可访问，以维护业务连续性。(4) 合规性：遵守适用的法律、法规和行业标准，以确保数据的合法性和合规性，特别是与隐私法规相关的合规性。

### 2. 数据安全治理包括的关键元素

(1) 政策和规程：制定明确的数据安全政策和规程，明确定义数据的分类、存储、传输和处理规则，这些政策应该适应组织的需求和风险。(2) 数据分类：对数据进行分类，根据其敏感性和价值，确定适当的保护措施，

例如，将敏感客户数据与一般信息数据区分对待。(3) 访问控制：设定访问权限，确保只有授权人员可以访问特定数据，这包括身份验证、授权和监控访问。(4) 数据加密：对敏感数据进行加密，以保护数据在传输和存储过程中的安全。(5) 风险管理：进行风险评估和管理，识别潜在的数据安全风险并采取措加以降低，数据安全治理不仅仅是技术问题，它还涉及组织的文化、管理和战略层面。它需要全面的方法，确保数据安全与组织的目标和价值观保持一致，并能够适应不断演变的威胁和技术，数据安全治理对于保护组织的声誉、客户信任和合法合规性至关重要。

## 二、数字经济背景下数据安全治理所面临的问题

在数字经济背景下，数据安全治理面临一系列新的和复杂的问题和挑战，以下是一些主要问题：一是大数据和数据爆炸：数字经济时代，数据量呈指数级增长，组织需要有效地管理、存储和保护大规模的数据，以避免混乱和泄露。二是数据隐私和合规性：随着隐私法规（如GDPR和CCPA）的出台，数据隐私和合规性成为了数据安全治理的重要问题，组织需要确保数据的合法性、透明性和用户权益，以避免罚款和声誉损失。三是多样化的数据来源：数字经济产生了多样化的数据来源，包括社交媒体、物联网设备、移动应用程序等，这些数据来源可能不受传统安全措施的保护，增加了数据泄露的风险。四是云计算和第三方服务提供商：许多组织将数据存储于云中或使用第三方服务提供商来处理数据，这引入了额外的安全风险，因为组织需要依赖外部实体来保护其数据。总之，在数字经济时代，数据安全治理需要不断演进，以适应新的威胁和技术，组织需要采取综合性的方法，包括技术、政策、文化和教育，以有效地管理和保护数据，同时，合作和信息共享也是应对数字

经济背景下数据安全挑战的关键。

### 三、数字经济背景下数据安全治理的必要性

数字经济背景下数据安全治理的必要性是显而易见的，因为数字经济的快速发展带来了大量的数据交换、存储和处理，同时也带来了一系列新的数据安全威胁和挑战。以下是数字经济背景下数据安全治理的必要性：

1. 保护敏感信息：数字经济时代，企业和政府机构积累了大量的敏感信息，包括客户数据、财务信息和知识产权，数据安全治理是确保这些信息不被未经授权的访问或泄露的关键。2. 遵守法规和合规性：随着数据隐私法规（如GDPR、CCPA等）的普及，组织需要遵守严格的合规性要求，不符合合规性可能导致高额罚款和声誉损失。3. 预防数据泄露：数据泄露可能对组织的声誉和财务造成严重损害，数据安全治理可以帮助预防和识别数据泄露事件，从而减轻潜在的风险。4. 支持数字化业务：数字经济的核心是数据，有效的数据安全治理为数字化业务提供了支持，它使组织能够充分利用数据来推动创新和增加竞争力。5. 防止网络攻击：攻击者越来越多地瞄准数字经济中的数据，数据安全治理可以帮助组织减少网络攻击的成功率，并降低恶意软件的风险。总之，数字经济时代的数据安全治理是确保组织的可持续发展和竞争力的关键，它不仅是一种反应性的措施，还是一种积极的战略，有助于提高数据价值、降低风险并维护组织的声誉，数据安全治理不仅仅是一项技术任务，还需要全面的管理和文化变革<sup>[1]</sup>。

### 四、数字经济背景下的数据安全治理策略

#### 1. 全面风险评估

全面风险评估在数字经济背景下的数据安全治理中起着至关重要的作用，因此，全面风险评估的首要任务是明确其目的，组织需要明确为何进行风险评估，是为了满足合规性要求、保护客户数据、防范网络攻击还是其他目的。同时，在风险评估的初期，组织应该对其数据进行分类，将数据分为不同的类别，根据敏感性和重要性进行区分，这有助于确定哪些数据最需要保护。此外，对数据的流动和处理过程要进行详细分析，这包括数据的收集、存储、传输和处理，组织需要了解数据在整个生命周期中的流动路径。在此过程中，企业还需要识别和评估与数据相关的潜在风险，这些风险可能包括未经授权的访问、数据泄露、网络攻击、恶意软件感染、员工失误等。总之，全面风险评估是数据安全治理的基础，它帮助组织了解其数据生态系统中的潜在威胁和风险，并制定适当的控制和防护策略，这个过程应该与组

织的整体风险管理流程相结合，以确保数据安全与组织的战略目标一致<sup>[2]</sup>。

#### 2. 数据分类和标记

数据分类是将数据分为不同类别的过程，通常根据数据的敏感性和重要性来分类，数据分类的目的是确保适当的保护措施针对不同类型的数据，以降低潜在的风险。同时，数据分类可以根据组织的需求和法规采用不同的标准，通常，数据可以根据以下标准进行分类：（1）敏感性：将数据分为敏感数据（如客户信息、财务数据）和一般信息数据。（2）重要性：根据数据对组织运营的重要性进行分类。（3）合规性：根据适用的合规性要求对数据进行分类。（4）业务用途：根据数据的具体业务用途进行分类。此外，一旦数据被分类，就可以使用标签或标记来标识数据的类别，标签可以包括敏感、机密、个人隐私等，以帮助员工识别数据的敏感性。不仅如此，数据分类也可以与数据生命周期管理相结合，确保数据在其整个生命周期内受到适当的保护和处理。总之，数据分类和标记是确保数据安全治理的关键步骤之一，它有助于组织识别、保护和管理敏感数据，降低数据泄露和滥用的风险，同时也有助于遵守合规性要求，组织应该根据其特定的需求和环境制定适当的数据分类和标记策略<sup>[3]</sup>。

#### 3. 强化访问控制

设定严格的访问控制措施，确保只有授权人员可以访问敏感数据，使用多因素身份验证（MFA）和单一登录（SSO）等技术来加强访问安全性。因此，强化访问控制是数字经济背景下数据安全治理的重要策略之一，以下是相关内容：（1）身份验证和授权：强化访问控制的第一步是确保只有经过身份验证的用户才能访问系统和数据，这可以通过用户名和密码、多因素身份验证（MFA）、生物识别等方式来实现，一旦用户身份验证成功，系统会根据其权限授权其访问特定数据和资源。（2）最小权限原则：实施最小权限原则，即确保用户只获得完成其工作所需的最低权限级别，这有助于降低不必要的风险，因为用户只能访问和修改与其工作相关的数据。（3）角色和组：创建角色和组，将用户分组并分配权限，这样可以更轻松地管理访问控制，特别是对于大型组织。当员工加入或离开组织时，只需更改其角色或组的权限，而不必单独处理每个用户。（4）单一登录（SSO）：使用SSO解决方案，使用户可以使用一组凭据登录多个应用程序和系统，而无需多次输入密码，这有助于简化访问控制并提高用户体验。（5）网络隔离：将

网络划分为不同的区域, 根据需要进行网络隔离, 这有助于阻止横向移动攻击, 即攻击者从一个系统跳到另一个系统。综上所述, 强化访问控制有助于降低未经授权的访问和数据泄露的风险, 组织应该根据其特定的需求和风险评估来制定和实施适当的访问控制策略, 同时, 访问控制策略需要定期审查和更新, 以适应不断变化的威胁和需求<sup>[4]</sup>。

#### 4. 数据加密

对敏感数据进行加密, 包括在传输和存储过程中的加密, 加密可以有效保护数据免受未经授权的访问, 其主要体现在以下几个方面: 一是加密基础知识: 数据加密是将数据转换为不可读的形式, 以保护数据的机密性, 它使用加密算法将明文数据转换为密文数据, 并需要一个密钥来解密数据。二是加密算法: 有多种加密算法可供选择, 包括对称加密和非对称加密, 对称加密使用相同的密钥来加密和解密数据, 而非对称加密使用一对公钥和私钥来进行加密和解密。三是传输加密: 在数据传输过程中, 使用传输层安全性协议(TLS)或安全套接字层(SSL)来加密数据, 这确保了数据在传输过程中的机密性, 防止中间人攻击。四是存储加密: 对于存储在磁盘或云中的数据, 可以使用磁盘加密或文件加密来保

护数据, 这使得即使物理设备被盗或云提供商受到攻击, 数据也不会泄露。总之, 数据加密是保护数据机密性的关键措施之一, 可以降低数据泄露和未经授权的访问风险, 然而, 加密应该作为整体数据安全策略的一部分, 并与其他措施相结合, 以实现综合的数据安全管理。

#### 五、结论

总之, 数字经济时代的数据安全治理是一项复杂而紧迫的任务, 在这个快速发展的领域, 数据安全问题需要全球范围内的合作和创新解决方案。在数字经济时代, 数据安全治理是企业 and 政府不容忽视的重要议题。只有通过综合性的方法和全球合作, 我们才能有效应对数据安全挑战, 确保数字经济的持续发展和繁荣。

#### 参考文献:

- [1]秦晓鹏.基于大数据背景下的数字经济发展分析[J].现代商业, 2023(07): 47-50.
- [2]彭长根.数字经济背景下的数据安全治理[J].信息安全研究, 2022, 8(04): 316-317.
- [3]魏国富, 石英村.人工智能数据安全治理与技术发展概述[J].信息安全研究, 2021, 7(02): 110-119.
- [4]陈鹏东.大数据时代数据安全治理的网络安全研究[J].数字通信世界, 2021(02): 167-169.

