基于数据分类分级的数据流转与共享安全研究

陈　彬

闪捷信息科技有限公司　浙江杭州　310000

摘　要：数据分类与分级是现代信息安全研究的重要内容之一，其目的在于对数据进行合理的分类与分级，保证不同层次的数据能够得到妥善地保护与管理。在数据分类分级的背景下，数据流转和共享的安全性是一个非常重要的问题。数据在不同系统、部门及机构间的传输与共享，需要对其进行严格的控制与权限认证，以防范数据泄露、滥用、篡改等潜在的安全风险。本文从数据分类分级的角度出发，对数据流转和共享安全问题进行研究，并提出相应的策略，希望能够促进数据安全性的有效提升。

关键词：数据分类分级；数据流转；共享安全

随着大数据、物联网、人工智能及云计算等技术不断发展，我国数字经济站上世界经济发展的主舞台，并步入高速增长的轨道。当下，我国从全球数字经济跟跑者变为领跑者，新产业、新业态、新模式迅猛发展，正在为中国经济注入新动能。数据的重要意义和价值被重新认识和定义。国家十四五规划和 2035 年远景目标纲要提出要迎接数字时代，加快建设数字经济，以数字化转型整体驱动生产方式的发展道路。

数据资产作为新型生产要素，其在流通和使用过程中不断产生新的价值，而受到数据价值的提升、流动性的加剧、防护边界模糊以及数据自身海量无序、类型繁杂、场景多样等诸多内外复杂因素的影响，数据安全风险异常突出，数据在云平台海量汇聚集中存储，成为网络攻击的靶子，大规模数据泄露风险剧增；另机器学习、人工智能等技术的运用，需要大量数据做支撑，数据在汇聚、使用、加工过程中可挖掘和泄露敏感信息。

在以上背景下，数据的流通和共享安全问题变得更加突出。由于数据在不同层次上的敏感性与重要性不同，因此需要对其进行分类分级，并建立相应的流通与共享策略。而且数据在传输与共享过程中，往往要跨越多个网络环境、多个系统平台，因此，必须构建安全可靠的数据传输通道与协议，才能保证数据在传输过程中不会被窃取或攻击。另外，在数据共享过程中，还应考虑数据的可追溯性与审计功能，以便及时发现数据的异常与违规行为。只有社会各界通力合作，不断探索，才有可能建立起更加安全、可靠的数据流通共享机制，推动数据安全与信息安全事业的进一步发展。

1. 数据分类分级对数据流转和共享安全的重要性

1.1 有利于限制数据流转的范围

对数据进行分类分级能够有效地限制数据流转范围，防止未经授权的数据泄露和滥用 [1]。在企业内部，数据经常在不同的部门、不同的人员之间流动、共享，这就带来了安全风险。通过对数据的分类分级，企业可以设置不同层次的数据访问权限，并在此基础上制定相应的数据流转规则，以保证特定层次的数据只有授权的人可以访问并处理。这样即使数据在流通过程中出现意外泄漏、滥用等情况，也能将损失与影响范围降到最低，保证数据的安全性与完整性。

1.2 有利于促进数据敏感度的提升

对数据进行分类分级，有助于企业和组织了解数据的价值与敏感性，并据此制定针对性的保护措施。藉由将数据分类，组织和企业能够清楚地知道哪些数据最重要、最敏感，以及哪些数据可以公开分享。这样组织和企业就能针对不同层次的数据建立不同的安全策略与控制方法，以保证不同类型的数据受到恰当的保护。例如，对高度机密的业务数据，可采取严格的存取控制及加密措施，防止非法存取与泄露；对于一般公共数据，可采用较为宽松的共享策略，以促进信息的流动与使用。

2. 数据分类分级在组织机构中的体系构建与流转应用实施难点

2.1 组织机构无法有效摸清数据资产

构建数据安全治理体系，首先需对数据资产进行梳理和

分类分级，以摸清数据防护对象。但目前大量组织机构对数据资产的规模、存放位置、敏感数据构成与使用情况等信息都无法有效掌握，或者掌握的可用数据分类分级信息滞后，这些信息不能反映数据资产的真实情况。从而无法根据数据的重要程度制定安全保护策略，直接影响了后续的数据安全体系化建设。

2.2 内容识别技术准确度低

当前大量单位机构虽然构建了数据管理平台或者工具，但是在内容识别技术这方面需要大量的人工干预，且无法将人为经验进行机器智能化学习。另一方面内容识别过程中会产生错误的数据分类分级结果。这会导致后续制定的数据安全保护策略不合理，从而对数据安全产生危害。

2.3 缺乏基于资产分类分级的数据安全风险监测能力

单位组织对环境中较高级别数据，或者涉敏涉密数据的泄露、违规访问、漏洞缺陷等情况无法做出针对性的风险监测与异常分析，往往会按照部门理解或者个人认知进行一刀切的策略部署，从而导致数据安全工作的针对性不强。

3. 基于数据分类分级的数据流转和共享安全措施

3.1 构建完善的权限把控机制

在数据分类分级条件下，数据流转和共享安全问题尤为重要。为保证数据在不同层次上的流动与共享不被非法访问或泄露，必须建立严格的权限控制机制。在此机制下，权限的分配要严格和精确，保证每个用户只有自己需要的权限，而不能访问其它数据 [2]。在构建权限控制规则中，可以根据用户的身份、角色、要求等，对数据进行不同层次的权限控制。例如，对机构内部人员，可根据其职位及工作需求，设置相应的存取权限；如果是外部合作伙伴或者第三方服务供应商，需要根据协议设置临时的数据访问权限。在此基础上，设计严格的权限控制规则，保证数据仅由适当的人员进行访问与处理，从而有效地避免了数据泄漏与滥用的风险。另外，为了保证数据的安全性，采用多级认证方法也是一种行之有效的方法。采用多层认证方法，如密码认证，生物识别认证，硬件令牌认证等等，能够有效地提高数据访问的安全可靠性。例如，在存取敏感数据时，可要求使用者输入密码，并采用生物测定技术，以确保只有合法使用者能存取数据。采用多层身份验证方法，可有效地防止非授权数据存取，并能保证数据的安全与完整性。由此可见通过制定详细的访问权限规则，建立多层认证机制，对数据进行细致的分类分级，实现数据的有效保护与管理。只有授权用户才能访问并处理数据，有效防止数据泄漏与滥用，提高数据安全与隐私保护水平。在信息时代，数据安全已成为企业与组织不可缺少的一环，因此建立严格的权限控制机制是保证数据安全的前提与保证。

3.2 构建严格的数据审计机制

在信息时代，数据分类分级管理下，数据的流转和共享安全问题一直是一个亟待解决的问题。随着数据规模的增长、应用范围的扩大，对数据流动与共享的要求越来越高。然而，数据在流通与共享过程中存在安全隐患，一旦数据泄露或被篡改，将严重影响个人隐私、企业利益乃至国家安全。因此，建立健全的数据审核机制是保证数据安全的重要措施。为了保证数据的安全性、完整性和可追溯性，必须对数据的流转与共享过程进行监控、记录与分析。在建立数据审核机制时，必须对数据进行分类，并对其进行分级。不同级别的数据具有不同的敏感性和安全性需求，针对不同级别的数据采取相应的审计措施，有针对性地加强对高风险数据的监测与防护。例如，在建立健全数据审核机制时，应明确审计范围与对象。审核范围应涵盖所有涉及敏感数据的系统与应用，并确保所有数据的流动与分享均可审核纪录与监察。审计对象包括系统管理员、数据处理员和用户，需要对其实施全面的审计监督。同时，也需要建立健全的审计记录制度。审计日志作为审计机制的核心，记录着审计过程中数据的流动与共享情况，是审计工作的重要基础。审计日志系统应能实时记录数据的运行状态，并能及时地检索、分析数据。此外，还要制定严格的审计制度与标准。审核规则与标准应清楚地界定数据处理之权限与流程，以确保数据之流动与分享符合规定，并可由审计追踪。对异常操作及违规行为应能及时发现，并采取相应措施加以处理。最后还可以通过构建专业化的审计队伍与机制，以保证数据的安全性。审核团队应具备专业知识及经验，能对数据审核工作负全责，及时发现并解决数据安全性问题。此外，还应建立健全的内部监督与外部评价机制，以保证审计独立、客观。

3.3 注重员工安全意识的培训

加强员工安全意识与培训，是数据分级数据流通与共享安全的重要内容。随着信息化进程的加快，数据对企业及组织的重要作用越来越突出，而数据的流动和共享也成为了企业生产经营的需要 [3]。但是，数据的流动和共享也带来

了安全风险，如果员工对数据安全的认识不够，就很容易造成数据泄露或者被恶意篡改，给公司造成重大损失。例如，数据安全培训应当成为一个组织的常规活动。定期进行数据安全培训，不但可使员工了解数据安全制度及相关规定，更可加深员工对数据分类等级制度的了解。在培训过程中，员工能够清晰地了解不同层次数据的处理方法以及共享权限，从而避免因不理解而导致数据泄露。此外，还可针对不同岗位的人员，设计有针对性的培训课程，以提高其对数据安全的认识与运用能力。而且在培训内容上，还应包括提高数据安全意识与实际操作能力。在培训过程中，除了要对员工进行数据安全方面的培训，还要加强员工对数据安全的认识。员工要认识到数据安全是大家共同的责任，只有大家时刻保持警觉，才能共同保卫企业的数据安全。另外，应加强实际操作演练，使员工掌握正确的数据处理与共享技术，增强其日常数据安全意识与操作技能。除此之外，企业也可以制定相应的奖惩制度，鼓励员工积极参与到数据安全的培训中来。或者还可以建立数据安全监管机制，定期检查、评价员工数据处理行为，及时发现并纠正违规操作。这样既能提高员工对数据安全性的关注，又能提高企业整体数据安全性。

4. 结束语

综上所述，数据分类分级过程中数据流转与共享安全问题，是信息时代面临的重大课题与挑战。随着信息技术的发展与应用，数据的重要性与价值与日俱增，数据安全问题日益突出。数据是信息社会中最基本、最核心的资源，其安全与隐私保护事关国家安全、社会稳定与个人利益。只有建立一个完善的数据安全管理制度，强化数据安全意识与培训，完善数据安全审计，才能保证数据在流转与共享过程中不受任何风险与威胁，提高数据的安全性。

参考文献

[1] 赵思宇 , 唐晋 , 刘晓毅 , 尚旭 , 林琦力 . 基于数据安全网关的数据安全防护体系研究 [J]. 信息安全与通信保密 ,2023,(04):105-112.

[2] 周成祖 , 吴文 , 蔡晓强 . 基于分类分级的数据安全防控策略研究 [J]. 数据与计算发展前沿 ,2023,5(01):128-135.

[3] 张峰 , 于乐 , 马禹昇 , 张弘扬 , 江为强 . 数据安全分类分级研究与实践 [J]. 信息通信技术与政策 ,2021,47(08):45-50.