数据安全审查实施困境与优化措施*

赵丽莉，刘晓瑞

（山东科技大学　文法学院，山东　青岛　266590）

摘　要：为防控数据安全风险，细化数据安全审查实施规范，实现维护国家安全的本质目的，提出应对数据安全审查实施困境的措施。基于数据安全审查实施的必要性，揭示现行数据安全审查实施在国家安全认定和影响难以衡量、数据安全审查主体和审查范围界定不清的困境，并对数据安全审查实施提出优化措施。研究针对数据安全审查实施中存在的挑战，实现“国家安全”审查因素具体化与抽象化的统一，以重要数据和核心数据的识别与管控为审查中心，实行常设与特设审查主体并行协调治理，推动数据安全审查的实施优化。

关键词：数据安全审查；国家安全；《数据安全法》；数据安全风险；数据处理活动

中图分类号：D912. 29　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 01. 019

引用格式：赵丽莉，刘晓瑞. 数据安全审查实施困境与优化措施［J］. 网络安全与数据治理，2025，44(1)：118 - 122.

Research on the implementation dilemma of data security review and countermeasures

Zhao Lili，Liu Xiaorui

(Institute of Intellectual Property，Shandong University of Science and Technology，Qingdao 266590，China)

Abstract：The study aims to prevent and control data security risks，refine the specifications for the implementation of the data security review. In order to achieve the essential purpose of the implementation of the data security review to safeguard national security，the study puts forward measures to address the dilemma of the implementation of the data security review. Based on the necessity of the implementation of data security review，the study reveals the dilemma of the current implementation of data security review in terms of the difficulty of measuring the national security identification and impact，the unclear definition of the subject and the scope of review. The study puts forward optimisation countermeasures for the implementation of data security review. In view of the challenges existing in the implementation of data security review，it is necessary to realize the unity of concretization and abstraction of national security review factors. Taking the identification and control of important data and core data as the center，the review implements parallel coordination and governance of permanent and specially established review subjects，so as to promote the implementation and optimization of data security review.

Key words：data security review；national security；Data Security Act；data security risks；data processing activities

0　引言

新时代的国家安全理念不断丰富和发展，不仅包括传统的军事、外交等领域，还涵盖了信息化带来的新兴领域安全问题，原本与国家安全关联不甚密切的网络安全和数据安全问题也逐渐纳入国家安全保障体系[1]。在此背景下，《数据安全法》提出对影响国家安全的数据处理活动进行数据安全审，数据安全与国家安全的关系进一步紧密[2]。

目前，学术界对于“数据安全监管”“数据安全调查”领域的探讨颇为丰富，针对“数据安全审查”议题的研究则相对较为匮乏。对审查的基本目的，现有的数据安全审查分别从国家、政府和企业三个层面进行剖析，数据安全审查的基本目的各有侧重，国家通过立法和政策引导，政府通过监管和执行，企业通过内部管理和技术防护，共同构建起一个全方位、多层次的数据安全防护体系；对于审查的实施主体，既有研究区分了由政府部门主导实施、企业独立实施或者二者联合实施的数据安全审查，并从技术和制度等不同视角提出应对策略，

*基金项目：山东省社会科学规划研究专项（23CSDJ41）；山东科技大学“智能科技安全治理创新团队”项目（2020RWB003）

这其中包括欧盟、美国等各自制定并贡献的独特的应对策略。然而，仍有少量学者未能对数据安全审查与网络安全审查进行充分区分，导致在理论探讨和实践应用中出现混淆现象，而且现有研究多倾向于研究数据安全审查的基本目的、功能定位、立法价值等宏观层面，对具体审查内容、审查主体、审查标准等实质性内容少有考察创新，基础理论框架构建存在空白，对于制度构建的逻辑探讨及实践层面深入的研究也稍显不足。这在一定程度上制约了数据安全审查的实施，数据安全审查规则的细化需求显得尤为迫切。

1 数据安全审查实施的必要性

1.1 数据安全风险防控的必由之路

数据主权和数据安全面临的重大风险主要源自于外部的潜在安全威胁。数据安全审查被视为风险防控的重要手段[3]。在国外逐步建立数据安全保障法律制度的背景下，我国同步推进并深化在数据安全领域的立法工作。2012 年，中国电信设备制造商华为和中兴公司在美国市场因“未通过安全审查”而遭到调查和封禁[4]，这一事件从客观上成为我国重视并加快完善安全审查机制的一个重要契机。2014 年 4 月，中央国家安全委员会第一次全体会议首次提出“总体国家安全观”理念，其中特别强调了网络安全在总体国家安全中的重要地位。在随后的十年间，我国又相继颁布了《国家安全法》《网络安全法》《数据安全法》等法律法规，逐步构建起以国家安全审查、数据安全审查和网络安全审查为核心内容的严密的法律监管框架。数据安全审查作为网络安全审查的延伸，两者皆可追溯至依据《国家安全法》构建的国家安全审查体系。网络安全审查着重于对关键信息基础设施运营商采购网络产品和服务的安全审查，更为强调产品和服务的安全性。数据安全审查的核心聚焦于任何可能威胁国家安全的数据处理活动，涵盖数据的收集、存储、使用、加工、传输、提供、公开等全链条环节，安全风险的存在倒逼数据安全治理体系的完善，而数据安全审查在数据安全治理体系中具有关键地位。

1.2 数据公共属性的必然要求

数据是数字经济的基础性战略资源，大数据时代的数据自身就天然带有公共属性。一般而言，依据数据所属主体、数据处理目的以及数据内容的不同可以将其划分为公共数据、企业数据和个人数据。对于公共数据，因其往往涉及公共利益，数据内容多指向公共服务，只有通过数据的广泛共享才能更好促进其价值的实现，因而具有鲜明的公共属性。企业数据和个人数据的公共属性尚存在争议。具体而言，大数据时代的个人数据不再单纯地被视为单一的财产权或人格权范畴[5]，展现出部分公共属性，但作为人格权益的个人信息权益以及隐私权与企业数据和公共数据的其他权益相比仍处于优先地位。企业在获取数据的过程中往往伴随经济投入或人力劳动，企业对企业数据的权益是财产性的。企业数据又可区分为公开、半公开和非公开三种类型。公开数据可视作公共领域内的公共资源，原则上具备公共属性，尽管其获取可能涉及商业成本。数据的公共属性既是数据安全得以保障的必要基础，同时也增加了数据安全保护的难度，催生了对数据安全进行必要审查的需求，使数据安全审查成为数据公共属性实现的必然要求。

2 现行数据安全审查实施面临的挑战

2.1 国家安全的认定和影响程度难以具体衡量

国家安全是一个国家得以生存和发展的基础，维护国家安全是任何国家都无法忽略的重要工作。虽然“国家安全”一词当前在我国法律框架中占据显著地位，已成为重要法律概念，但其内涵和外延在学术界持续引发广泛讨论和争议。在既有的立法实践中，2015 年是我国在法律制度中对于国家安全进行明确界定的重要转折点，《国家安全法》的出台，首次以法律的形式明确了国家安全的概念，即“国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。”学界认为，目前国家安全概念尚属于概括性界定，国家安全范畴处于全面拓展期，“安全的内涵和外延越来越丰富，时空领域越来越宽广，内外因素越来越复杂”[6]，从政治安全和军事安全领域向非传统安全领域扩展，条件组合和动态转换使得国家安全的定性模糊化，被学者们视为一种“弹性概念”。除此之外，有些研究者将其视为一种类概念，强调其本质上的动态演变形态[7]。在国家安全框架内，《数据安全法》进一步明确了对特定领域的国家安全的专门界定，专设章节对“数据安全审查”进行关注，以立法方式对国家安全中的数据安全领域进行界定体现出国家安全法治建设的不断发展。

在数据安全领域，传统的国家安全界定方法已不适应现代法治实践。数据安全审查不仅涉及技术层面，还需要综合法律、技术和社会影响进行评估。一方面需要判断是否存在危害国家安全隐患的数据处理活动，即便仅存在危及国家安全的可能性，仍然属于数据安全审查制度的审查内容；另一方面，需要判断审查对象是否符合数据安全的合规标准，如果不符合现有标准，需要进一步确定是否对国家安全的持续稳定造成潜在威胁。因此，数据安全审查的目标在于降低或者消除影响国家安全稳定性的任何潜

在风险，但如何判断数据处理活动中是否存在危害国家安全现实威胁或者隐患仍无认定和判断标准。

2.2 数据安全审查范围边界难以界定

数据安全的审查范围是该制度的核心内容，只有解决了“审什么”的关键内容，才能为后续数据安全审查工作的铺展做好准备，但是当前数据安全审查的审查范围仍存在不明晰的问题。

安全审查制度的构建需要关注审查内容和审查重点等内容，这是审查范围边界确立的重要问题，也是构建审查制度坚实框架的基础性实体问题[8]。《数据安全法》第二十四条明确设立了数据安全审查机制，从法律层面明确规定了数据处理的概念，涵盖数据的收集、存储、传输、公开等多个环节，但对于何种数据处理活动会对国家安全产生不利影响，并无进一步的说明解释。《数据安全法》第三条对于数据的概念进行了明确，即“任何以电子或者其他方式对信息的记录”，这种界定将任何在我国境内实施数据活动的组织和个人的行为都纳入了《数据安全法》的调整和规范之内[9]。虽然审查范围的拓宽对数据安全保护具有显著优势，但宽泛的界定使得被审查数据的范围产生不确定性，易引发对所有数据的数据处理活动的无差别审查或者肆意执法，可能导致个体和组织难以准确适应和遵循相关规范，使其在实践中无法适从[10]，使监管主体的权威性受到损害。

2.3 数据安全审查专门主体尚未明确规定

审查主体是拥有法定权限的审查机关，《数据安全法》未针对数据安全审查主体设有明确规定，只是在第六条规定了不同领域的主管部门承担本行业、本领域数据安全监管职责，“公安机关、国家安全机关等……在各自职责范围内承担数据安全监管职责”“国家网信部门……负责统筹协调网络数据安全和相关监管工作”等，使得在审查工作中各部门可能存在工作职责交叉混乱的情形。因此，进行数据安全审查工作的主体范围可以借鉴网络安全审查的相关做法，但是数据安全审查主体的权限范围仍需进一步规制和明晰。

3 优化数据安全审查实施的措施

3.1 审查标准：实现“国家安全”审查因素具体化与抽象化统一

国家安全具有动态性，其界定受国家利益、现实威胁和国际形势等多元因素的影响，从经济学角度审视，国家利益可被视为决定国家安全的唯一变量[11]。俄罗斯知名学者沙瓦耶夫强调，国家安全本质上是一个社会（国家）维持其稳定与功能的有效运行状态，在这种状态下，社会作为一个复杂的系统，具备自我保护、维护整体性、确保发展并防御内外部潜在威胁的能力，确保其生存与发展不受任何干扰或侵害[12]。我国学者认为“国家安全”是主权国家对于其内部事务的控制力[13]，强调国家安全的界定具有相对模糊性。还有学者坚持“国家安全由维护国家存续和基本权益的各类因素构成。”[14]国内外学者总体上均认同一个国家处于没有危险的客观状态构成国家安全的基本含义。

美国的国家安全法律法规体系涵盖了国家安全总体规定，包括外商投资安全、网络安全、科技安全等多维度多层面。在外商投资审查领域，美国 2007 年发布的《外国投资与国家安全法案》虽然没有对“国家安全”这一概念作出明确界定，但却为评估外商投资项目提供了重要的参考依据，涉及国防需求、关键技术、关键基础设施、关键能源和重要资源供给等。美国 2018 年发布的《外国投资风险审查现代化法案》（FIRRMA）对涉及外资投资风险的国家安全评估范围涉到关键技术和材料安全、关键基础设施安全、敏感数据安全、网络安全等各种类型安全。由此可见，美国外商投资安全审查制度将关键技术、基础设施、网络信息安全纳入“国家安全”审查因素，并将“国家安全”的解释具体化[15]。

我国对“国家安全”审查因素的考量应当以总体国家安全观为统领，协调《国家安全法》中“国家安全”的界定，具体应包括以下几个方面：首先，国防安全领域。数据处理活动是否触及并可能会对国防安全造成潜在影响；第二，经济安全领域，重点考察数据处理活动是否对重点产业、关键行业、关键基础设施和重要经济工程产生极大影响；第三，文化安全领域，深入审查数据处理活动是否对我国核心价值体系造成冲击性影响，是否对社会核心价值观、普遍的道德规范以及传统的公序良俗构成潜在威胁；第四，社会安全领域，主要审查数据处理活动是否对社会公共秩序的稳定性以及保障社会平稳运行产生潜在重大干扰；第五，金融安全领域，主要对数据处理活动是否产生金融风险，影响金融监管安全进行数据安全审查。当然，要通过法律的形式详尽无遗地列举出所有可能影响国家安全的考量因素是一项极其艰巨的任务[16]，新的安全威胁和挑战层出不穷。因此，为了应对这种复杂性和不确定性，可以采用兜底性条款的方式来处理，同时，赋予政府相关部门在必要时酌情处理的权限。

3.2 审查范围：以重要数据和核心数据的识别和管控为中心

《数据安全法》第二十四条将数据安全审查范围定为可能或实际威胁国家安全的数据处理活动，给予执法机构广泛的自由裁量权，可以将其理解为即便潜在威胁微小，执法机构也可启动审查，而无需确凿证据。同时避免将审查泛化至所有数据，可能导致过度审查，影响个

人和组织的数据处理自由，影响数据的正常使用和交换，这也是企业最为顾虑的一点[17]。因此，数据安全审查应以重要数据和核心数据的识别和管控为中心，对重要数据的识别作出更符合国家安全需求的界定[18]，在保障数据安全的前提下合理确定数据安全审查的范围。

我国《数据安全法》确立的数据分类分级保护制度中明确提出要加强对重要数据的保护。对高风险数据进行重点管控并非我国独创，而是很多国家的常见做法。例如，美国《外国投资风险审查现代化法案》通过明确高敏感数据分类标准和扩大审查范围，确保国家安全不受外国投资交易中高风险数据的威胁。该法案明确规定，可能对国家安全构成严重威胁的特定数据被称为“敏感个人数据”，在外资并购的安全审查中被视作评估潜在国家安全风险的关键因素之一。然而，重点并不在于强调保护数据主体的个人权益，而是着重于维护美国的国家安全利益。FIRRMA 从数据可识别性和“对国家安全的风险性”两方面界定了影响国家安全的敏感个人数据。无论域外还是国内，管控的主要理由均为关乎国家安全和公共利益。

《数据分类分级规则》根据数据在经济社会活动中的重要性及其泄露或篡改可能造成的危害，将数据分为一般、重要和核心三个等级。《数据出境安全评估办法》第19 条界定了“重要数据”，这类数据若遭受篡改、泄露或其他非法行为，将可能对国家安全、经济运作、社会秩序、公共健康以及公众安全构成威胁。《数据分类分级规则》进一步指出那些在特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能对国家安全、经济运行、社会稳定、公共健康和安全引发严重后果的数据，即为重要数据。重要数据的界定侧重于其非法处理的影响对象，但由于涉及行业和领域的广泛性，立法难以对其详尽列举。因此，建议从数据识别主体、认定标准和方式上识别和管控重要数据，以明确数据安全审查范围。

一是重要数据识别负责主体应由行业主管部门担任。不同行业、领域存在巨大差异，只有行业主管部门对本行业本领域的数据处理活动可能产生的风险最为熟悉，且需对产生的安全风险负主要责任。二是重要数据的认定标准应聚焦于国家安全风险。认定标准应强调数据对国家安全利益、社会稳定、经济发展造成的重大风险，仅对个人或者组织自身产生安全影响的数据，应不认定为重要数据。三是重要数据的认定方式，应当采取定性与定量相结合的方法进行认定。定性识别主要通过对数据价值的判定和数据毁损对国家安全、社会稳定的潜在影响，来判定其是否属于重要数据。定量识别则侧重于规模性数据集合的潜在风险分析，如美国的《外国投资风险审查现代化法案》就规定，当数据跨境传输或处理量达到特定阈值时，将触发审查程序。这个阈值可能因不同的法规和政策而异，但通常代表着跨境数据流动的规模已经达到了需要被特别关注和管理的程度，一旦触发审查程序，相关部门将对数据进行全面评估，包括对其内容、目的、来源和目的地等进行审查，以确保数据的流动符合所有适用的法律、法规和标准。采用定性与定量相结合的方法来识别重要数据，确保在保障数据保密性和完整性的同时，对数据流动性的潜在风险进行有效管控。

对于国家核心数据，《数据安全法》第 21 条明确规定，相较于重要数据和一般数据，核心数据级别更高，要求实施更为严谨的管控措施。从数据全生命周期的角度来看，数据安全审查应当涵盖重要数据和核心数据的数据处理活动全周期。数据处理者识别到其所收集存储的数据为重要数据或者国家核心数据后，应当向主管机关备案，为后续安全审查提供基础。审查机关可不定时进行抽样审查，或者由数据处理者进行自主申报审查，若抽样审查时审查机关认为数据处理活动可能产生对国家安全的影响，而数据处理者未进行自主申报审查，将依法追究数据处理者的责任。而一般数据因对社会影响较小，一般不作为审查重点。同时，需要建立一个动态更新的机制，以便在数据产生、存储、传输和处理的过程中，能够及时识别和应对可能出现的新风险和新挑战。

3.3 审查主体：常设与特设审查机构并行协调治理

审查主体是拥有法定权限的审查机关，数据安全审查机关在《数据安全法》及相关规范中并未进行明确规定，仅规定了实行由中央国家安全委员会统筹协调下的行业监管机制，规定了不同领域主管部门的监管职责，以及数据处理者所应尽到的数据安全审查义务，且未对各审查机关的审查权限进行明确规定。

面对日趋严峻的国家安全形势，依靠单个数据安全机构开展安全审查已经不能满足实际应用的需要，需要建立跨部门合作和协调机制，设立具有高度权威性的审查体系。以美国云计算服务安全审查框架为例，美国政府颁布的《联邦风险及授权管理计划》（FedRAMP）有效实施跨多个政府部门机构的紧密合作，同时专设网络安全审查机构[19]；德国通过《外国经济活动与国家安全法》设立专门机构，即联邦经济与出口管制局（BAFA），负责审查外国对德国企业的投资和收购。我国《网络安全审查办法》中对安全审查主体进行了较为细致具体的规定，网络安全审查的主要责任机构是隶属于国家互联网信息办公室的网络安全审查办公室。对于数据安全审查而言，由网络安全审查办公室下属的审查与技术认证中心来负责此项工作则面临着机构合法性不足、审查力

量有限、审查程序和质量难以保障的弊端。因此，本文主张设立独立的数据安全审查机构，特别提议在国家互联网信息办公室下设专门的数据安全审查办公室，以独立履行数据安全的审查与保障职责。设立独立机构进行审查，有利于明确具体权限和责任，提高数据安全审查专业性，同时有助于保持审查结果的稳定性和一致性。

具体而言，以审查主体的审查权限为标准，审查主体既可以是具有法定审查权限的常设审查机构，也可以是经授权具有临时审查权限的特设审查机构。由于数据安全审查事关国家安全、社会和个人利益，应设置相应的常设审查机构，即具有法定权限的行政主体，将常设审查机构分为领导和实施两类机构，领导机构由具有法定权限的网信部门和安全部门共同协作，实施机构是具有法定权限的行业主管部门或相关组织。数据安全审查可以借鉴网络安全审查的实践举措。譬如，中央网络安全和信息化委员会作为领导部门，由国家网信办会同发改委、工信部等13个部门建立协同审查机制。网络安全审查办公室设立在国家网信办，负责组织实施具体的安全审查措施。数据安全审查与网络安全审查情况相似，其领导机构都是中央网络安全和信息化委员会。而发改委等12个国家部委行署应当作为常设数据安全审查机构，发改委中行使主要数据安全审查职能的为国家数据局，上述常设机构在法定权限内行使审查权力，履行审查职责，开展审查工作。除此之外，应当建立“数据安全审查办公室”作为常设审查机构，下设在国家网信办，负责数据安全审查的具体制度设计，具体组织实施数据安全审查。

除设置常设审查机构之外，还应设置特设审查机构。特设审查机构是经授权而具有临时审查权限的主体，只有在遇到突发性或者重大的数据安全事件时才发挥审查机构职能。经授权具有临时审查权限的主管部门仍然由上述发改委、工信部等部门组成，增加中华人民共和国应急管理部门以及各级应急管理部门等机构。常设审查机构只能审查专有领域的数据处理活动，而具有临时审查权限的主体可以跨部门或跨领域审查相应的数据处理活动，具有更大的灵活性及应急性。特设审查机构不能超越授权范围行使职权，超过职权范围行使的数据安全审查活动无效，作出的决定相对具有独立性且更加专业，不受其他外部势力的影响，同时特设审查机构仍受基本的《行政诉讼法》《行政复议法》等法律规范的规制，只有将特设审查机构与常设审查机构一并装入“权力的笼子”[20]，方能将审查机构的权限限定在安全可控的范围内，并发挥应有作用。

参考文献

[1] 朱雪忠，代志在. 总体国家安全观视域下《数据安全法》的价值与体系定位［J］. 电子政务，2020（8）：82－92.

[2] 马其家，刘飞虎. 数据出境中的国家安全治理探讨［J］. 理论探索，2022（2）：105－113.

[3] 朱军. 数据安全治理背景下数据安全审查的定位、功能与实践［J］. 西部法学评论，2022（6）：12－22.

[4] 迟志培. 美国对华科技遏制战略的实施与制约［J］. 太平洋学报，2020，28（6）：27－42.

[5] 孙清白，王建文. 大数据时代个人信息“公共性”的法律逻辑与法律规制［J］. 行政法学研究，2018（3）：53－61.

[6] 编委会. 总体国家安全观干部读本［M］. 北京：人民出版社，2016.

[7] ［德］埃贝哈德·施密特－阿斯曼，等. 德国行政法读本［M］. 于安等，译. 北京：高等教育出版社，2006.

[8] 武长海. 我国国家金融安全的审查机构和范围［J］. 法学杂志，2020，41（3）：18－29.

[9] 谢杰. 大数据时代背景下数据安全法律问责制度研究［J］. 智库时代，2019（6）：248－250.

[10] 曾磊. 数据跨境流动法律规制的现状及其应对——以国际规则和我国《数据安全法（草案）》为视角［J］. 中国流通经济，2021，35（6）：94－104.

[11] 甘培忠，王丹. “国家安全”的审查标准研究：基于外国直接投资市场准入视角［J］. 法学杂志，2015，36（5）：11.

[12] ［俄］沙瓦耶夫. 国家安全新论［M］. 魏世举、石陆原，译. 北京：军事谊文出版社，2002.

[13] 黄仁伟，刘杰. 国家安全新论［M］. 北京：时事出版社，2004.

[14] 子杉. 国家的选择与安全［M］. 上海：三联出版社，2005.

[15] 董静然，顾泽平. 美欧外资安全审查法律制度新发展与中国之应对［J］. 国际商务研究，2020（5）：74－85.

[16] 肖海军，李茜. 外资安全审查标准：缺憾、价值取向与进路［J］. 湖南大学学报（社会科学版），2023，37（5）：134－143.

[17] 王新锐. 数据安全立法：难点于求解［J］. 网络信息法学研究，2020（2）：21－29.

[18] 许皖秀，左晓栋. 美国审查 TikTok 数据安全带来的启示与思考［J］. 数据安全研究，2022，41（2）：3－29.

[19] 张孟媛，袁钟怡. 美国网络安全审查制度发展、特定及启示［J］. 网络与信息安全学报，2019，5（6）：1－9.

[20] 任建明. 把权力关进制度笼子的逻辑与对策［J］. 理论探索，2015（6）：43－47.

（收稿日期：2024－10－22）

作者简介：

赵丽莉（1978－），女，博士，教授，主要研究方向：网络法学。

刘晓瑞（1999－），女，硕士，研究助理，主要研究方向：网络法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部