比利时数据安全审查制度评鉴*

赵丽莉[1]，劳鑫鑫[2]

（1. 山东科技大学　数字法治研究院，山东　青岛　266590；2. 山东科技大学　知识产权学院，山东　青岛　266590）

摘　要：为降低数据安全风险和提高数据流通效率，数据安全审查制度应运而生。基于欧盟数据保护规则基础，比利时确立了相应的数据安全审查制度，特别是优先监管特定行业、实施严格的应急处理机制、要求数据保护官的本地化、加强对关键基础设施数据的保护等内容，但其依然面临数据保护资源和数据审查执行实践不足、部门协同性有限、数据安全风险评估标准和监督缺失、中小企业合规负担增加等实施困境。有鉴于此，我国在推进数据安全审查制度建设方面，应重视完善数据安全审查规则、提升数据安全审查机构的独立性、创新企业监管方式等建议，促进我国数据安全治理和数字经济高质量发展。

关键词：比利时；数据安全审查；《通用数据保护条例》；《比利时数据安全法》

中图分类号：D912. 1　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097-1788. 2025. 05. 007

引用格式：赵丽莉，劳鑫鑫. 比利时数据安全审查制度评鉴［J］. 网络安全与数据治理，2025，44(5)：42-48.

Review of the data security review system in Belgium

Zhao Lili[1], Lao Xinxin[2]

(1. Digital Rule of Law Research Institute, Shandong University of Science and Technology, Qingdao 266590, China;
2. Intellectual Property College, Shandong University of Science and Technology, Qingdao 266590, China)

Abstract: In order to reduce the data security risks and improve the efficiency of data circulation, the data security review system came into being. Based on the European Union data protection rules, Belgium has established the corresponding data security review system, especially in terms of prioritizing the supervision of specific industries, implementing strict emergency handling mechanism, requiring the localization of data protection officers, strengthening the protection of key infrastructure data, but it still faces implementation dilemmas that data protection resources and data review implementation practices are insufficient, collaboration is limited, data security risk assessment standards and supervision are lacking, compliance burden of small and medium-sized enterprises has increased. In view of this, in promoting the construction of data security review system in China, we should pay attention to suggestions such as improving the data security review rules, improving the independence of data security review institutions, and innovating enterprise supervision methods, to promote the high-quality development of China's data security governance and the digital economy.

Key words: Belgium; data security review; General Data Protection Regulation; Belgian Data Security Act

0　引言

在大数据时代，从数据的概念来看，数据自身就天然带有公共属性，有学者直言“数据作为天然的公共品服从固有的互惠分享的原理”[1]，这里的数据并不区分掌握在何种主体手里。就个人数据而言，在大数据时代也不再只作为一种绝对的财产权或人格权对象而出现[2]，而是具有了“公共性”。由此可见，数据的公共性和流动性决定了数据保护的必要性[3]。然而，当数据安全影响着国家安全和个人信息安全，数据安全审查应运而生。

1　比利时数据安全审查制度的确立背景

比利时的法律和政策框架在很大程度上受到欧盟数据保护法规的影响，但比利时同时也有自己的历史积淀。比利时的《隐私法》早在1992年就规定了数据保护的基本框架，体现了比利时在个人数据保护方面的立法先行性，所以比利时的数据安全审查制度并非完全依赖欧盟的规定。欧盟关于数据安全和有序流动的监管规则体系

*基金项目：山东省社会科学规划研究专项（23CSDJ41）

建设在全球具有标杆性地位，欧盟2016年4月27日通过了全面的数据保护法规《通用数据保护条例》（General Data Protection Regulation，GDPR），旨在加强和统一所有欧盟成员国的个人数据保护标准。目前GDPR被一百多个国家当作参照，深刻影响着全球数字治理规则的方向[4]。比利时作为欧盟成员国，受到GDPR制定的数据安全审查框架约束[5]。在GDPR的基础上，比利时修改和更新了其国内的数据保护法律框架，如表1所示。比利时还根据GDPR的规定成立了数据保护局（Data Protection Authority，DPA），负责监督数据保护法规的执行，并处理与个人数据保护相关的事务。在特定领域、跨境数据流动以及国际合作等有关数据安全审查和保护方面，比利时的法律法规也做出了相应的规定，以促进数据的自由流动和技术创新。

表1　与比利时数据安全审查制度有关的法律法规

名称	颁布时间	生效时间	内容概括
《通用数据保护条例》（GDPR）	2016年4月27日	2018年5月25日	规定了数据处理的合法基础、数据主体的权利、数据泄露的通报要求等
《比利时数据保护法》	2018年7月30日	2018年8月5日	细化了GDPR在比利时的实施，设立了数据保护管理局，赋予其广泛的调查和监督权力
《信息安全委员会法》	2018年9月5日	2018年9月20日	建立了信息安全委员会，负责监督和协调国家层面的信息安全工作，并修改了若干法律以落实GDPR的要求
《关键基础设施安全和保护法》	2011年7月1日	2011年7月15日	规定了对关键基础设施的安全保护措施，旨在提高其抵御网络威胁的能力
《网络和信息系统安全法》（《NIS法案》）	2019年4月7日	2019年5月1日	建立了网络和信息系统的安全框架，适用于公共安全的通用利益

作为欧盟的成员国，比利时的数据安全审查制度包括对数据主权、数据隐私以及数据贸易等方面影响国家安全的高风险数据的审查[6]，同时比利时在此基础上进行了细化。根据比利时现行法律法规可知，比利时的数据安全审查主体主要包括比利时网络安全中心（BCC）、联邦计算机应急响应小组、行业机构、国家危机中心（NCCN）、比利时邮政和电信局（BIPT）、国家安全委员会；威胁分析协调单位（CUTA）；数据保护局（DPA）、信息安全委员会（ISC）等。根据GDPR第4条、2018年7月30日比利时颁布的《关于个人数据处理的自然人保护法》、比利时《NIS法案》和《关键基础设施安全与保护法》的规定，比利时数据安全审查的客体包括个人数据、企业数据、政府数据以及关键基础设施数据等多个方面。

2　比利时数据安全审查制度的内容和特点

2.1　比利时数据安全审查制度的内容

比利时的数据保护立法具有显著的先行性，早在1992年12月8日比利时就颁布了《隐私法》。该法律奠定了比利时数据保护的基本框架，包括明确数据处理的合法性、规定个人数据监督主体的权利、设立机构等，例如比利时隐私保护委员会，后改为数据保护局（DPA）。欧盟的《数据保护指令》（Directive 95/46/EC）直到1995年才通过，而比利时在此之前便已经确立了完善的数据保护框架，这体现了其在隐私保护领域的洞察。先行性使比利时成为欧洲较早实施数据保护法律的国家之一，为后续适应欧盟框架奠定了基础。比利时的数据安全审查制度有悠久的历史背景，在欧盟法律制度框架的规制下，有其独特之处，值得借鉴。

2.1.1　明确数据保护官的数据安全监督和审查职能

欧盟成立之前，欧洲委员会和欧洲人权委员会等机构发挥着数据安全和隐私保护的重要作用。欧盟成立以后，《95指令》和GDPR均对数据保护机构设置和权力配置等做出了相应的安排，欧盟逐渐形成覆盖全域和各成员国两个层面的数据保护机构体系，规定了各成员国需设有独立的数据保护机构，负责本国范围内数据安全。

比利时数据保护官是指在比利时境内负责监督和推动数据保护法规的官员或机构。在比利时，数据保护官（DPO）的角色由比利时DPA承担。DPA是独立的监管机构，负责保护个人数据的隐私和安全。其主要职责包括：（1）监督和确保比利时的组织和个人遵守欧盟GDPR以及国内的数据保护法规。（2）负责处理关于数据保护违规行为的投诉，可以是来自个人数据主体或其他机构的投诉。（3）向组织和个人提供关于数据保护最佳实践、合规性和处理个人数据的建议和指导。（4）负责注册和监督数据保护官的行为，特别是在需要指定DPO

的情况下。（5）致力于提高公众对数据保护问题的认识，通过教育和宣传活动推动数据保护意识的提高[7]。数据保护官应在独立和自主的地位下履行其职责，根据国家法律和规定、国际数据保护标准和实践进行培训，监督数据控制者和数据处理者的数据保护行为，保护数据安全。

2.1.2 将数据保护影响评估制度纳入数据安全审查制度

数据保护影响评估制度（Data Protection Impact Assessment，DPIA）体现在 GDPR 第 35 条，其规定了对数据保护影响评估的要求，当特定的数据处理可能导致高风险时，特别是对个体的权利和自由方面的风险，数据控制者应进行数据保护影响评估。数据保护影响评估应至少包括：（1）评估数据处理的性质、范围、上下文和目的；（2）评估潜在的风险对个人的权利和自由的可能性；（3）采取的措施和方法以及措施的有效性，以确保数据处理符合本条例[8]。通过对数据处理风险的评估，能够在事前采取有效措施，减少数据泄露、丢失或滥用等安全问题，从而增强数据的机密性、完整性和可用性。在数据安全审查过程中实施 DPIA，可以有效识别潜在的法律风险和不合规行为，帮助数据控制者在早期阶段做出调整，避免因不合规处理而面临罚款或法律诉讼。数据安全保护影响评估机制是比利时数据安全审查的一部分，以保护数据的机密性、完整性和可用性。当数据处理可能对数据主体的权利和自由带来高风险时，数据控制者必须进行数据保护影响评估，以识别和减轻潜在风险。

2.1.3 数据泄露通知作为数据安全审查制度的补救措施

GDPR 第 33 条规定了在个人数据违规发生时，数据控制者在无不当延迟的情况下，应在不超过 72 小时的时间内向监管机构通知该违规行为，除非个人数据违规不可能对自然人的权利和自由产生风险。GDPR 第 34 条规定当个人数据违规事件可能会对自然人的权利和自由产生高风险时，数据控制者应在违规事件发生后立即通知数据主体，除非适用于第 33 条的例外情况[9]。由此可见，GDPR 第 33 和 34 条规定了数据安全违规通知的要求。图 1 描述了 GDPR 数据泄露通知制度的内容，包括向监管机构和受影响的个人及时通知数据安全违规事件，详细描述数据泄露后的措施等。数据泄露通知是数据安全审查的重要组成部分，体现了数据安全审查的事后监管。由此可知，将数据泄露通知制度作为比利时数据安全审查制度的补救措施是很有必要的。

2.2 比利时数据安全审查制度特点

2.2.1 明确优先监管特定行业

2020 年 1 月，比利时 DPA 公布了 2020－2025 年战略规划，表达了引领公民、企业、协会和政府走向人人享有隐私的数字世界的雄心。与此同时，比利时 DPA 还设定了三类优先监管事项，其中第一类即是指针对特定行业开展优先监管，涵盖电信和媒体、政府、直销、教育与中小企业 5 类。电信和媒体行业处理大量的数据信息；政府部门掌握着公民的敏感信息；直销行业常依赖于大规模的个人数据进行精准营销；教育机构处理大量的个人信息；中小企业单独处理数据的数量众多。由此可见，这些行业多数为数据处理规模较大或者涉及数据敏感性较强，故成为优先监管对象，这也成为比利时相较欧盟其他国家而言的一个特点。

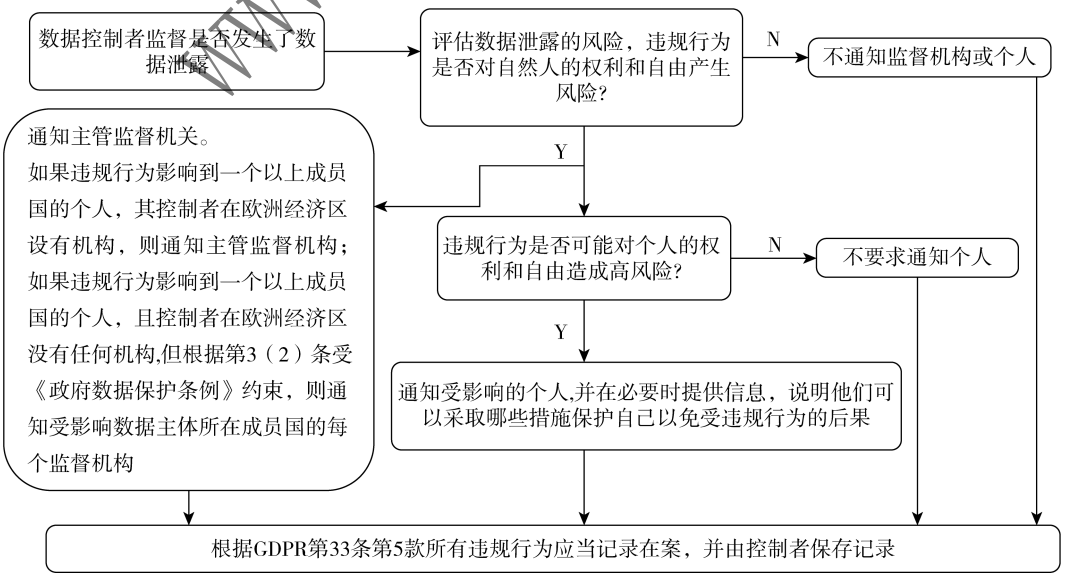

图 1 GDPR 数据泄露通知制度示意图

2.2.2 实施严格的应急处理机制

虽然 GDPR 要求数据控制者在发生数据泄露事件后 72 小时内向监管机构通知，但比利时有更严格的执行规范。DPA 不仅规定了在 72 小时内通知监管机构，还提供了详细的指南和工具，以确保数据控制者能够准确和全面地报告数据泄露事件。DPA 要求在报告数据泄露事件时，必须提供详细的事件描述，包括但不限于泄露数据的种类和数量、受影响的个人、泄露原因、已采取的补救措施等。

2.2.3 要求 DPO 法律和语言本土化

比利时数据安全审查制度对 DPO 有本地化的要求。比利时的数据安全审查制度要求 DPO 必须具备一定的本地化知识，熟悉比利时的法律和语言，以确保其能够有效履行职责。因为 DPO 在执行任务时，需要与本地居民和组织进行交流，这要求他们精通本地语言。荷兰语、法语和德语是比利时的官方语言，DPO 必须全部掌握。语言的精通确保了在处理投诉、进行调查和提供咨询时的沟通顺畅，避免因语言障碍导致的误解或错误。根据 GDPR 的规定，当企业在处理大量个人数据或高风险数据时，必须指定 DPO。DPO 的任命、职能和任务见表 2。

2.2.4 加强对关键基础设施数据的保护

比利时的《NIS 法案》在 GDPR 的基础上，进一步加强了对关键基础设施的数据保护，防止发生数据泄露危害国家安全和公共利益。根据《NIS 法案》的规定，关键基础设施运营商在可能对网络安全造成重大影响的事件发生时，必须迅速向计算机安全事件应急响应小组（CSIRT）或主管当局报告“重大事件”及引发原因、严重影响等详细情况。比利时扩展了事件报告的范围，对风险管理和安全措施、网络安全事件报告、国家级协调和监督等几个方面进行了加强，确保关键基础设施数据的更高安全性。

表 2 有关 DPO 的任命、职能和任务的相关判例和概述

任命条件	职能	任务
专业素养（GDPR 第 37 条）： 具备数据保护法律与实践专业知识； 通过认证培训或同等资质	监督与合规： 监督数据控制者/处理者遵守 GDPR 及《比利时数据安全法》； 审查数据处理活动的合法性、透明性	风险管理： 执行 DPIA，识别高风险数据处理活动； 制定并实施数据泄露应急预案
独立性（GDPR 第 38 条）： 独立于企业运营部门； 直接向最高管理层汇报	指导与支持： 向数据控制者/处理者提供合规建议与最佳实践指导； 协助制定数据保护政策与流程	事件响应： 72 小时内向监管机构报告重大数据泄露事件； 高风险事件中向数据主体发出通知
本地化要求： 精通比利时官方语言（荷/法/德语）； 熟悉比利时法律与文化背景	教育与协调： 推动企业内部数据保护培训与意识提升； 协调跨部门数据保护措施，确保与业务融合	合规报告： 推动企业内部数据保护培训与意识提升； 配合监管机构开展调查与审计
无利益冲突： 不得兼任 IT 或法务部门负责人； 避免参与利益相关决策	监督与问责： 注册并监督企业内部 DPO 行为； 对违规行为提出整改建议并追踪执行	持续改进： 根据技术发展与法规更新调整数据保护策略； 推动数据保护技术工具与流程优化

3 比利时数据安全审查制度的不足性审视

3.1 数据安全审查的人员和预算有限

DPA 负责监督和执行 GDPR 及有关数据安全保护和审查的法律，确保所有数据处理活动符合 GDPR 和比利时数据保护法的要求；审查数据主体投诉的认为其权利受到侵犯的行为，接收和处理数据主体关于其数据保护权利的投诉；评估发生数据泄露时的严重性并指导控制者采取适当的补救措施等。

鉴于 DPA 的职责，其人员配备、资金和专业知识会影响数据安全审查制度的实施效果。比利时网络安全市场报告指出，许多公司缺乏熟练的网络安全专业人员，与金融机构、政府组织和私营部门/工业公司的网络安全专家需求相比，熟练的网络安全专业人员数量很少。专业人员的缺乏将会影响比利时数据安全审查工作的效果和效率。例如，若数据安全审查的专业人员缺乏，DPA 可能难以开展工作，导致延迟处理数据泄露事件和日常

审查工作，从而限制 DPA 对数据泄露事件的快速响应能力和有效监管。数据安全保护本就是一个快速发展的领域，比利时面临不断增加专业人员的数量，并持续加强对专业人员的专业技能进行培训和教育的诉求和困境。

根据欧盟委员会 2020 年 1 月从境内所有 DPA 处回收的问卷，在 GDPR 出台的 2016 年至生效一年后的 2019 年期间，大多数 DPA 的雇员和预算有所增加，但其中很多都表示对资源配置不满，而且成员国之间的情况并不平衡。尽管与 2016 年相比，DPA 的雇员总人数增长 42%，预算增长 49%，但自 2019 年以来，各国 DPA 的雇员和预算大多陷入了停滞状态。资源配置的不足会直接影响比利时数据安全审查工作的进展。

3.2 数据安全风险评估标准和监督的缺失

目前比利时设立 DPA，负责监督个人数据保护原则的遵守情况。在此范围内，DPA 被授予向司法当局通报侵权行为的权力，并在适当情况下，自主启动法律程序以执行数据保护原则。但是对于数据安全风险的评估标准和具体程序，比利时没有具体的规定。

在当今数字化时代，技术进步正在改变人们生活、工作和相互交流的方式。从人工智能（AI）到物联网（IoT）设备和区块链技术，新技术正在重塑社会的方方面面，包括数据的收集、处理和存储方式[10]。尽管这些创新带来了许多好处和机遇，但也带来了新的挑战和风险，尤其是涉及数据安全和隐私方面。一方面，监管机构制定和实施新规则和指导方针的能力可能难以跟上数据处理实践和新兴技术不断发展的步伐，再加上新兴技术可能在监管的灰色地带运作，其使用和实施受到不明确或过时的规定管辖，这就会导致一些合法的权益受到不法侵害或者一些不法的行为不受管制。另一方面，因为许多新技术是复杂和跨学科的，所以有效监管这些技术的专业知识会有所缺乏，导致监管新兴技术存在挑战。因此，比利时数据安全审查制度中新技术监管不足对数据安全和隐私产生了重大挑战。

3.3 数据安全审查的部门间协调和信息共享的难度大

比利时负责数据安全审查的机构众多，包括联邦公共服务经济部（FPS Economy）、联邦公共服务内政部（FPS Interior）、比利时数据保护局（DPA）以及国家安全委员会（National Security Council）等，这些机构各自拥有不同的职责和权限，尽管比利时设有国家安全委员会，凡是仍缺乏一个统一的领导机构来统筹各部门的工作，导致在数据安全审查过程中各部门往往各自为政，难以形成统一的行动。这将会导致在执行和实施数据安全审查时出现冲突，从而增加了协调和信息共享的难度。再者，比利时的数据保护法律相对比较分散，在数据安全审查方面更是如此，这将会导致在实施过程中出现重叠。通过分析可知，各部门之间的信息共享和协调的有限性是一个突出问题，由于各部门信息的不互通和法律的限制，各个部门之间无法及时有效地交换信息，将会影响数据安全审查工作的有序进行。

3.4 中小企业的合规负担增加

欧盟《数据法案》为了促进数据的自由流动，要求企业提高技术互操作性确保数据可以被传输和使用，还要求在特定的情况下企业有能力迅速响应紧急情况确保公共机构可以访问企业所持有的数据，这些将会增加中小型企业的投入成本。有跨境数据传输需求的企业需要在本地化的计算机设备与人员配置上持续增加投入，从而导致企业的数据使用、管理与合规成本不断增加[11]。由此可见，资源有限的中小企业在遵守数据保护法规方面有着较大的合规负担。数据应用合乎法律规定和数据应用不得侵犯他人的正当合法权益是企业数据合规最关键的两点，这同时也是数据合规审查的两条红线。正是由于合规要求复杂且繁重，中小型企业很难做到上述两点，因为上述数据合规的成本十分高昂。比利时的数据安全审查一方面增加了企业的运营成本，因为履行这些合规义务需要相应的人力、财力等资源；另一方面还会影响到其日常业务运营。例如，一些中小企业因为缺乏足够的资源和专业知识，无法全面理解和遵守复杂的数据保护法规，从而面临合规风险和潜在的法律责任。

4 比利时数据安全审查制度对我国的启示

4.1 我国已初步确立以《数据安全法》为核心的数据安全审查制度

根据《数据安全法》第 5、6 条可知，中央国家安全领导机构，各地区、各部门，行业主管部门，公安机关、国家安全机关，国家网信部门等是我国法律规定的数据安全审查的主体，从而确定了在现有的法律框架下我国数据安全审查的主体。《数据安全法》第 24 条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行安全审查。由此条可知我国数据安全审查确保数据处理活动的安全，保护国家安全、公共利益以及公民、法人和其他组织的合法权益。《数据安全法》明确提出建立数据安全风险评估机制的要求。我国数据安全评估制度正在加紧建设形成中，呈现出国家顶层设计与行业探索同步推进的现状。国家标准层面，《网络安全标准实践指南——网络数据安全风险评估实施指引》发布，同时《信息安全技术数据安全风险评估方法》国家标准也处于报批阶段。根据《网络安全法》第 21 条规定，网络运营者应当按照网络安全等级保护制度

的要求，履行网络安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。上述规定了对数据安全管理的基本要求，数据处理者应当采取措施保障其收集和处理的个人信息安全，防止数据泄露、篡改和丢失。由《网络安全法》第37条、第44条，《数据安全法》第4条、第9条、第21条，《个人信息保护法》第4条、第51条，《关键信息基础设施安全保护条例》第11条的规定可知，我国数据安全审查的客体主要包括个人数据、企业数据、政府数据等。我国信息安全标准化技术委员会已经在数据安全方面建立了较为全面的标准体系。这些标准涵盖了各类常见情境，为数据安全提供了较为完善的技术支持。综上所述，我国数据安全审查的概念可以界定为：数据安全审查机构依据国家相关法律法规，对数据处理活动进行系统性评估，确保数据处理过程中的安全性和合规性，保护数据免受未经授权的访问、泄露、篡改和丢失。

4.2 区别网络安全审查与数据安全审查

由我国《国家安全法》第59条可知，国家安全审查包括网络安全审查和数据安全审查，两者在审查对象、目的、范围等方面有所不同。根据《网络安全审查办法》第2条，关键信息基础设施运营者采购网络产品和服务，网络运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查；《数据安全法》第24条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。前者的审查对象主要是针对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的情形；后者的审查对象主要针对影响或者可能影响国家安全的数据处理活动，包括数据的收集、存储、使用、加工、传输、提供、公开等。但是我国对于网络安全审查和数据安全审查的审查范围区分及其具体的审查标准还不明晰，正确区别数据安全审查制度和网络安全审查制度，有助于我国数据安全审查规则的建立，促进我国数据安全审查制度的完善。

4.3 我国数据安全审查制度的完善建议

4.3.1 完善数据安全审查规则，将风险评估机制纳入安全审查制度

我国关于数据安全审查的立法薄弱且分散，顶层设计之间的衔接不够流畅，而底层配套的法律规范文件也不够明确。为解决上述问题，我国应当完善数据安全审查的具体规则，明确数据安全审查的范围。

数据安全审查制度所依赖的重要数据识别制度、数据分类分级制度以及数据出境安全评估的具体实施制度尚未正式出台。在国际竞争日趋白热化的背景下，我国迫切需要完成各类标准的建设。在制定这些标准的过程中，应当积极汇集各技术专家的力量，广泛征求意见，预判各种风险并制定相应的应对措施。在数据安全审查标准制定的过程中，不仅应当聚焦于当前的问题，还应当以动态的眼光看待数据技术的发展[12]。标准的制定需要设置基本的安全防线，兼顾可操作性与灵活性，并坚持持续安全评估，将数据风险评估审查贯穿于数据的全生命周期中，这样可以确保数据安全审查制度在实践中发挥作用，为我国的数据安全提供更加坚实的保障。

4.3.2 提升数据安全审查机构的独立性，增加其资源配置

我国数据安全审查的主体包括中央国家安全领导机构，各地区、各部门，行业主管部门，公安机关、国家安全机关，国家网信部门等。相较于比利时，我国应当完善监管机构在监督和执行数据安全审查方面作用的具体配置，提升数据安全审查机构的独立性，以保证其决策的公正性和权威性，避免受到政治和经济因素的影响，确保数据安全审查工作的有效开展。我国还应为数据保护机构提供必要的人力、技术和财政资源，保障我国数据安全审查制度能够有效实施，避免数据泄露或者其他威胁数据安全的事件发生。在数据安全审查机构方面，应当建立透明的运作和决策机制，确保其活动受到公众和利益相关者的监督。

通过分析比利时数据保护资源和数据审查执行实践不足的问题，我国应该按照财政事权和支出责任相适应原则，统筹利用现有资金渠道，统筹运用财政、金融、土地、科技、人才等多方面政策工具，加大对数据资产开发与利用、数据资产管理运营基础设施建设以及试点试验区构建等的扶持力度，鼓励产学研协作，引导金融机构和社会资本投向数据资产领域[13]。

4.3.3 创新监管方式与跨部门协作，减轻中小企业数据合规负担

国务院办公厅发布的《关于深入推进跨部门综合监管的指导意见》强调了跨部门综合监管责任分工的重要性。在数据安全审查制度的实践中，各部门之间的协调合作同样至关重要。首先，我国应建立跨部门协调机制，确保在处理数据泄露事件时相关部门能够迅速合作并共享信息。再者，我国应建立一个协同高效的跨部门综合监管工作机制，监督数据安全审查工作的执行。最后，我国可以成立专门的数据保护工作组，负责跨部门的协调和沟通，确保信息和措施的及时传达和执行。

我国的立法机构应制定统一的执行标准和指南，对数据安全审查制度的相关内容进行详细解释，并定期对地方政府和相关部门的工作人员进行培训。此外，定期评估和检查各地区和部门的执行情况，以提高执法人员

的水平和执法措施的一致性，不断完善数据安全审查的实施体系。为了强化跨部门的协作机制并创新监管方式，中小企业在遵守数据保护法规时面临的合规负担尤其沉重。由于合规要求的复杂性和繁重性，再加上合规成本高昂，导致了他们在数据应用上频繁出现违规行为。为解决这一问题，政府可以实施具体政策，根据企业规模或者企业数据体量进行细分，并要求不同规模的企业遵守相应的数据合规标准。这样既照顾到中小型企业的发展，也明确了企业必须遵循的合规要求。

随着新兴技术的快速发展，我国现有的监管框架可能无法及时应对由此带来的数据安全挑战。通过成立专门的监管机构和及时更新相关法律法规，评估新兴技术的发展，可以避免一些数据安全风险的发生。随着数据交易行为的多元化，数据流通交易的方式也将变得更加多样。针对这种情况，需要采取更加有效的监管措施，不断创新数据监管方式。

5 结论

伴随全球数字经济的持续发展，数据流通安全成为国家安全的重要部分，数据安全审查制度是促进和保障数据安全流通的重要环节。比利时数据安全审查制度的特殊性在于其能够在欧盟统一框架内，结合自身独特的历史背景、法律传统和政治结构，形成一种既遵循欧盟规范又具备比利时特色的审查机制。我国数据安全审查制度在促进和保障数据跨境流通方面依然面临诸多问题，故此，应秉持综合安全观理念，立足国情，优化制度设计，进而提升数据安全审查的效能和效率。

参考文献

[1] 梅夏英. 在分享和控制之间 数据保护的私法局限和公共秩序构建 [J]. 中外法学，2019，31（4）：845 - 870.

[2] 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.

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

[4] 张丽丽. 数据安全监管的欧盟经验及对中国的启示 [J]. 北京经济管理职业学院学报，2024，39（1）：3 - 9.

[5] WALSH C，RUSSELL L. European data protection：a review of the new regulatory framework [J]. International In-House Counsel Journal，2016，10（37）：1 - 9.

[6] 冯洁菡，周濛. 跨境数据流动规制：核心议题、国际方案及中国因应 [J]. 深圳大学学报（人文社会科学版），2021，38（4）：88 - 97.

[7] DUBUISSON T. Data protection authority provides new policies on GDPR infringements and litigation proceedings aspects [J]. European Data Protection Law Review（EDPL），2021，7（3）：435 - 449.

[8] 赵景欣，岳星辉，冯崇朋，等. 基于通用数据保护条例的数据隐私安全综述 [J]. 计算机研究与发展，2022，59（10）：2130 - 2163.

[9] 盛小平，杨绍彬. GDPR对科学数据开放共享个人数据保护的适用性与作用分析 [J]. 图书情报工作，2020，64（22）：48 - 57.

[10] COLONNA L. Artificial Intelligence in the Internet of Heal the Things：is the solution to AI privacy more AI? [J]. Boston University Journal of Science and Technology Law，2021，27（2）：312 - 344.

[11] 人民法院报. 欧盟《数据法案》概览 [EB/OL]. [2014 - 05 - 12]. https：//www. chinacourt. org/article/detail/2024/03/id/7873539. shtml.

[12] 崔静. 欧美数据跨境流动监管的经验做法及我国的策略选择 [J]. 经济体制改革，2021（2）：173 - 179.

[13] 关于印发《关于加强数据资产管理的指导意见》的通知 [EB/OL]. [2014 - 03 - 12]. https：//www. gov. cn/zhengce/zhengceku/202401/content_6925470. htm.

（收稿日期：2025 - 02 - 18）

作者简介：

赵丽莉（1978 - ），女，博士，教授，主要研究方向：网络法学。

劳鑫鑫（1998 - ），女，硕士研究生，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