从《数据安全法（草案）》解读我国数据安全保护体系建设*

马海群[1] 张涛[2]
（1. 黑龙江大学信息资源管理研究中心，哈尔滨 150080；2. 黑龙江大学信息管理学院，哈尔滨 150080）

摘要：数据是国家基础性战略资源，对数据掌控能力日益成为衡量国家竞争力的关键因素，但由数据所带来的安全问题也事关国家主权安全和发展利益。2020年7月发布的《数据安全法（草案）》（以下简称《数安法》）系统地反映当前国家整体数据安全与发展观，它对我国数据安全保护体系构建具有重要的战略意义。本文从定性和定量文本分析视角对《数安法》进行解读，并与《数据安全管理办法（征求意见稿）》《网络安全法》进行比较分析，最终从法律体系、保护制度、监管职责、风险评估4个方面为当前我国数据安全保护体系提出建设思路。

关键词：数据安全；政策解读；文本分析；数据安全法；数据安全保护体系
中图分类号：D63；TP309.2　　DOI：10.3772/j.issn.1673-2286.2020.10.007
引文格式：马海群，张涛. 从《数据安全法（草案）》解读我国数据安全保护体系建设[J]. 数字图书馆论坛，2020（10）：44-51.

在全球信息化进入引领发展的大背景下，数据所呈现出的爆发式增长正影响着人们的日常生活方式、工作习惯和思维模式，对数据的研究已逐渐成为当前学术界和产业界的热点。数据在助力经济社会发展的同时，也带来了前所未有的安全风险与挑战，尤其是新冠疫情期间，数据量急速增加使得数据安全与隐私保护问题尤为突出，由于数据过度采集所导致的隐私泄漏给用户带来严重困扰[1]。事实上，用户面临的威胁并不仅限于个人隐私泄漏，在数据存储、处理、传输等过程中还有很多安全风险，这些风险会对政府治理、社会稳定乃至国家安全产生深远影响。2013年美国“棱镜”事件曝光后，我国政府也越来越重视数据安全问题。2015年8月《促进大数据发展行动纲要》是国务院发布大数据产业布局的战略性政策，是目前促进大数据产业发展最权威的政策，政策中将强化数据安全保障作为主要任务之一[2]。此后我国在数据安全领域发布了一系列的政策法规，2017年6月1日《网络安全法》正式施行，它是保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益所制定的重要法规[3]。2017年11月公布的《中华人民共和国个人信息保护法（草案）》，主要目的是规范个人信息的收集、处理和利用，保护自然人个人信息权以及其他合法权益，促进个人信息的合理利用，规范个人信息跨境传输[4]。2018年10月全国人大开始组成专班针对数据安全法进行研讨，2019年5月国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》，对网络运营者在数据收集、处理使用、安全监管等方面提出了要求[5]。2020年4月在中共中央、国务院印发的《关于构建更加完善的要素市场化配置体制机制的意见》中将数据作为一种新型生产要素纳入其中，与土地、劳动力、资本、技术等一并成为市场化改革的重要组成部分[6]。2020年7月《数安法》在中国人大网公布并面向社会征求意见，这体现出国家对数据安全领域的高度关注。《数安法》的制定是继《中华人民共和国网络安全

*本研究得到国家社会科学基金重点项目“总体国家安全观下的国家情报工作制度创新研究”（编号：20ATQ004）资助。

法》之后，在数据保护领域重要的立法，它是我国数据安全保护体系构建的顶层设计，这部统筹数字经济时代“安全与发展”并重的法规不但是个人数据野蛮掘金时代的结束，还是数字经济加速发展的必要保证。2020年9月国务委员王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上提出《全球数据安全倡议》，体现我国政府在数据安全问题上兼具国际化视野与全局策略。

近年来，国内外学者从不同视角对数据安全的立法进行研究。在国内，如许可[7]从体系定位、立场选择与制度构造对数据安全法的出台提出建议。韩伟[8]提出在数据安全法立法过程中要安全与自由兼顾，在两者间取得平衡，进而实现数据安全的多元“共治”。徐漪等[9]以欧盟《通用数据保护条例》为借鉴从3个方向提出建议来推动数据安全法的立法进程。刘金瑞[10]从聚焦维护国家安全定位，健全数据安全管理制度角度对完善《数安法》提出若干建议。朱雪忠等[11]以总体国家安全观为理论指导，分析了数据安全法的价值定位和体系定位。在国外，2016年12月，普京总统颁布的《新版信息安全学说》是俄罗斯数据安全领域的重要战略规划。2017年8月，英国数字、文化媒体和体育部发布了一份《新的数据保护法案：我们的改革》的报告，将通过一部新的数据保护法案以更新和强化数字经济时代的个人数据保护。欧盟在2018年颁布的《通用数据保护条例》是保护欧盟用户个人数据的重要法律依据。美国国会研究服务局于2019年3月发布了《数据保护法：综述》，报告中系统介绍了美国数据保护立法现况及未来。其中对《通用数据保护条例》的研究成果最多，如Cornock[12]对《通用数据保护条例》进行解读，并且对该条例的实际意义进行讨论。Greene等[13]详细分析了《通用数据保护条例》对数据科学家和研究人员产生的影响。Hoofnagle等[14]详细介绍了规范个人数据的战略方法以及欧盟《通用数据保护条例》的规范基础。Sokolova[15]通过2018—2019年GDPR罚金情况，探讨了《通用数据保护条例》对于欧盟个人数据保护的重要作用。

基于以上综述，目前国内外对数据安全立法研究成果多以定性研究为主，因此本文基于定性和定量的方法对《数安法》进行全面解读[16]，并最终从法律体系、保护制度、监管职责、风险评估4个方面为当前我国数据安全保护体系提出建设思路。

1 定性解读

《数安法》共7章51条，分别为总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任及附则。总则部分提出制定《数安法》的主要目的，并对数据、数据活动、数据安全的概念进行了明确的定义。数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放是《数安法》的核心内容，而法律责任及附则是对前面章节所涉及的法律问题进行说明，以下对《数安法》的四部分核心内容进行解读。

1.1 数据安全与发展

该部分确立了国家坚持维护数据安全和促进数据开发利用并重的原则，具体内容框架如图1所示。在确保数据安全的前提下，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。《数安法》第13条进一步明确了国家发展数据驱动的数字经济决心，主要包括国家实施大数据战略、各省制定数字经济发展规划、国家将培育数据交易市场、大力推进电子政务建设和政务数据安全开放等举措，以数据开发利用和产业发展来促进数字经济发展。第14条和第15条提出推进数据开发利用技术和数据安全标准体系的建设是数据安全发展之本。第16条提出要依法开展数据安全监测、评估、认证等数据活动。第17条提出对数据交易的发展不但要建立健全数据交易管理制度，而且要规范数据交易行为和培育数据交易市场，这与第4章数据安全保护义务和第6章法律责任部分紧密关联。

1.2 数据安全制度

该部分凸显了数据安全制度建设的重要性，具体内容框架如图2所示。《数安法》第19条提出数据实行分级分类保护，国家要根据数据的重要程度以及危害程度确定重要数据保护目录，数据分级分类保护是数据安全制度建设的基础。本章内容与《网络安全法》相比，《网络安全法》主要侧重对技术安全的防护，突出了网络安全等级保护评估的重要作用[17]，但《网络安全法》中对网络安全内控制度的构建略显薄弱，这就导致一些网络安全事件在内部发生。而《数安法》将数据安

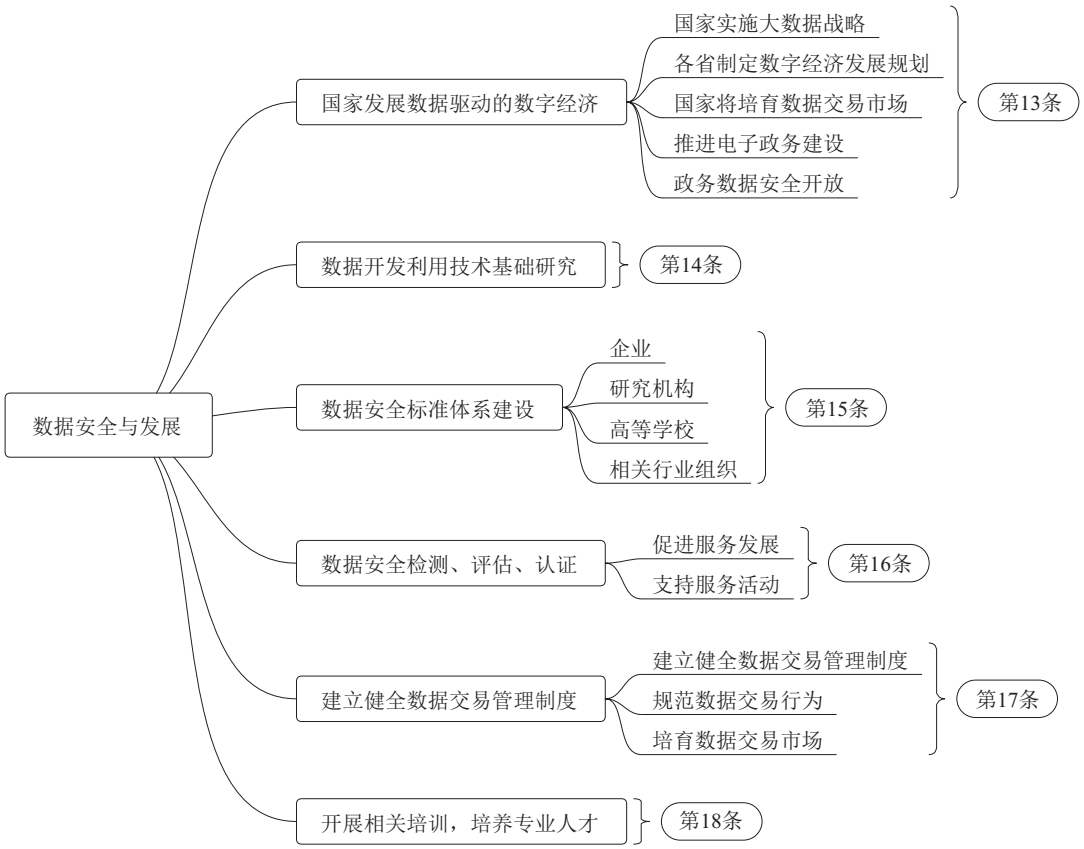

图1 数据安全与发展结构图

全制度单独作为一章进行规定，并且从数据分级分类保护、数据安全风险机制、数据安全应急处理机制、数据安全审查制度、数据实施出口管制、反制歧视性措施方面提出了规范与要求，弥补了当前重技术而轻内控制度建设的情况，进一步减少因内控制度缺失导致出现安全事件。

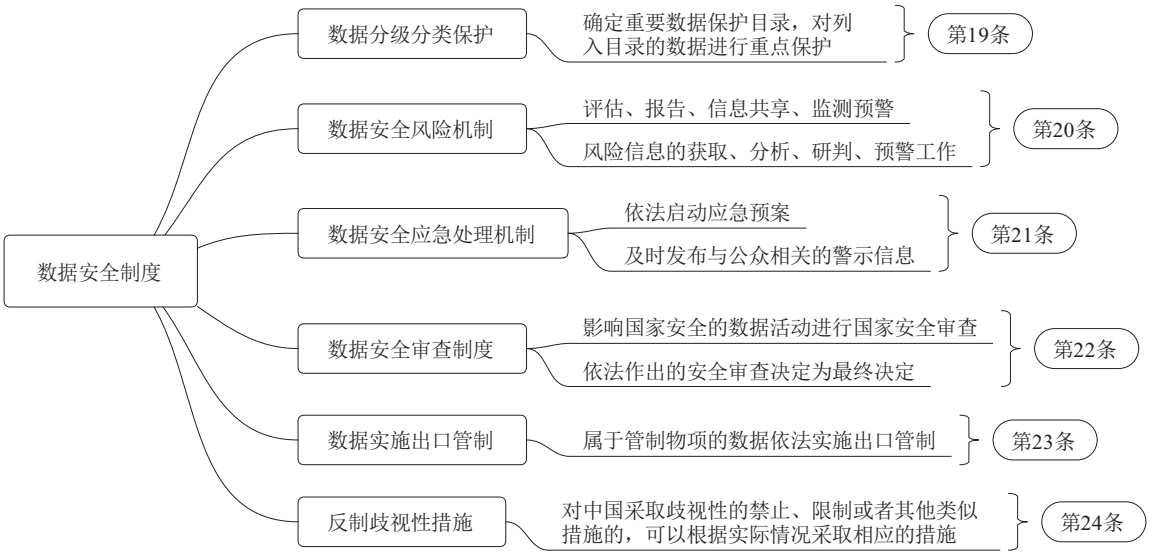

图2 数据安全制度结构图

1.3 数据安全保护义务

该部分确定了在开展数据活动中不同主体的数据安全保护义务，具体内容框架如图3所示，可以看出从第3章到第4章衔接较为紧密，呈现出递进关系。《数安法》第25条提出开展数据活动要依照法律法规和国家标准的要求，建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施，以及采取其他必要的措施确保数据安全，该条与第3章国家建立数据安全制度相关联，是对开展数据活动主体设置的安全保护义务。第30条提出在数据交易过程中，不但要说明数据来源，还要审核交易双方的身份，并留存审核交易记录。在法律责任部分是对本章的法律解释，针对不履行数据安全保护义务或未采取必要安全措施的组织或个人，将会面临组织最高罚款100万元，个人最高罚款10万元的行政处罚。

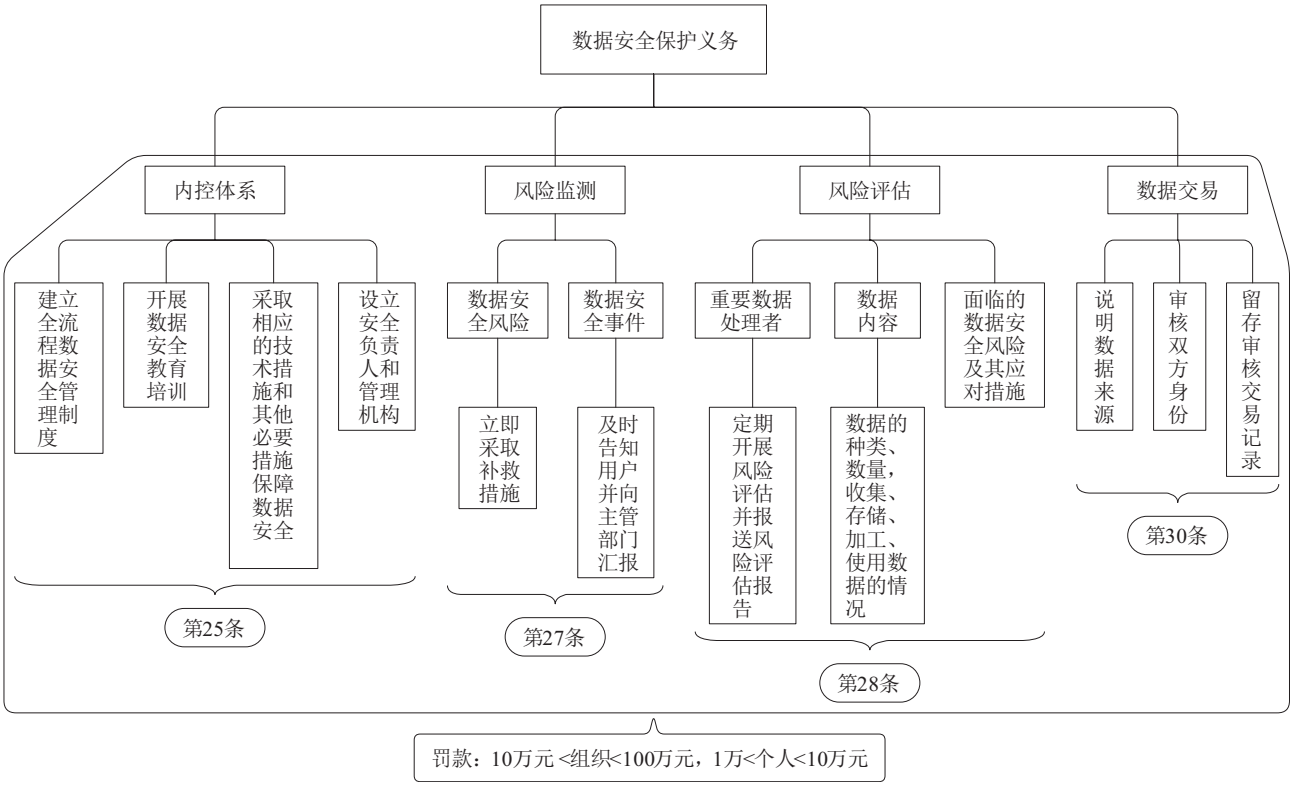

图3 数据安全保护义务结构图

1.4 政务数据安全与开放

《数安法》将政务数据的安全与开放单独作为一章充分说明了国家对政务数据安全与开放的重视程度，具体内容框架如图4所示。从数据的来源来看，目前大数据资源主要掌握在政府手中，因此政务数据的安全与开放是能否充分发挥大数据价值的关键[18]。本章从数据产生与流转的全过程切入，对数据的收集、使用、存储、加工、提供进行了明确的要求。第36条要求国家机关也应当建立健全数据安全管理制度，落实数据安全保护责任，实现国家机构与运营者的衔接。第39条是对我国政府数据开放制度的进一步细化，明确国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台。第40条将具有公共事务管理职能的组织，为履行公共事务管理职能开展的数据活动划定为本章的适用范围。

2 定量解读

本文利用NLPIR-ICTCLAS软件[19]对《数安法》进行新词提取，结合自建语料库[20]进行政策词表导入，利用python中jieba模块进行政策文本分词、去停用词等预处理操作，处理后全文共提取词语457个（去除重复词语），现对词频及共现强度进行分析。

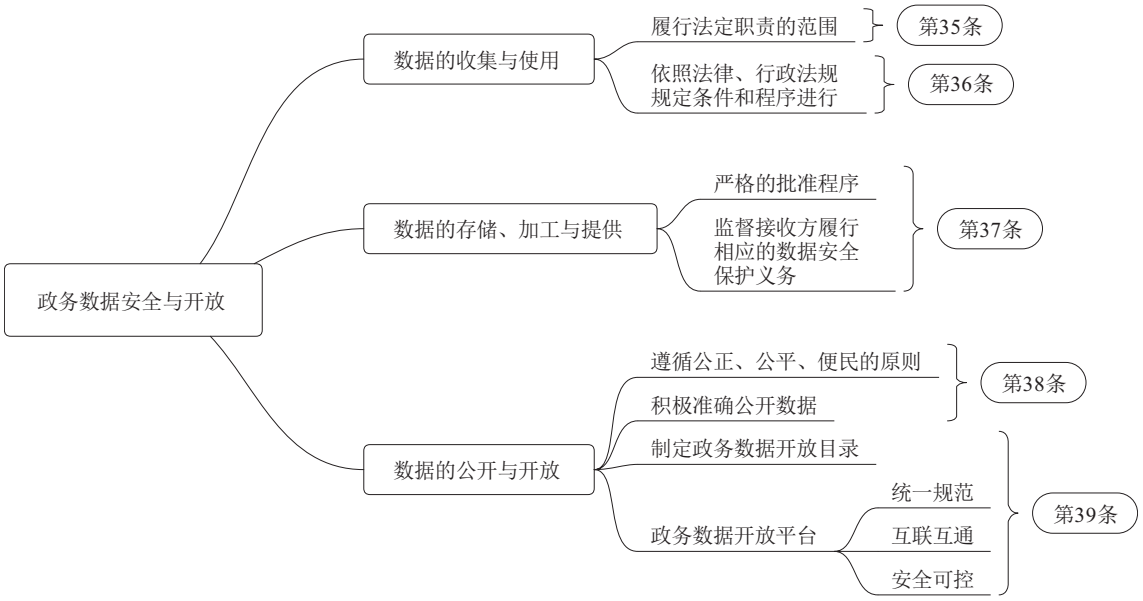

图4 政务数据安全与开放结构图

2.1 词频分析

通过python中wordcloud模块对《数安法》中的词语进行词频分析，剔除数据安全、国家、数据、应当、有关、促进等无实际意义词语，其中数据开发利用、开展数据活动、保障、保护是词频最高的词语，其次是数据交易、安全监管、合法权益、风险、评估等关键词。

《数安法》中“数据开发利用”出现12次，这体现国家对数据开发利用重视程度，第1条、第5条、第12条明确了数据安全保护与数据开发利用的关系，即国家坚持维护数据安全和促进数据开发利用并重的原则。加强数据开发利用可以促进数字经济的高质量发展，有助于提升国家治理水平，在确保数据安全的前提下，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。“开展数据活动”出现8次，《数安法》首次对数据活动进行了明确的定义，并且所有法律条款是在开展数据活动的前提下有效，确定了适用范围。“保障”和“保护”均出现7次，在《数安法》中将保障数据安全、保护公民和组织的合法权益作为主要目标。第3条中对数据安全的定义是保障数据得到有效保护和合法利用，并持续处于安全状态的能力，说明了国家对保障数据安全和数据安全保护的重要定位[21]。“数据交易”一词出现6次，数据交易是重要的数据活动场景，由于数据交易中出现数据安全问题风险较高[22]，因此在《数安法》中对建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场提出明确的要求，对一切非法来源数据交易的行为进行处罚。“安全监管”出现4次，数据安全监管职责是《数安法》的法律依据，第7条第2款明确了行业主管部门对本行业、领域的数据安全监管职责，此规定与《网络安全法》第8条相衔接，更加明确、突出了主管部门对行业数据的安全的监管职责。可以预见未来各行业、各领域会相继出台数据安全监管办法。

2.2 共现强度分析

本文利用共现分析法对《数安法》进行计算分析，通过计算词语间的共现强度来分析文本中的热点及主题内容[23]。共现强度如公式（1）所示，E_{ij}代表词共现强度，S_i和S_j分别表示词语在文本语句片段的数量，S_{ij}表示为两个词语共现在文本语句片段的数量。

$$E_{ij}=\frac{S_{ij}^2}{S_iS_j} \quad (1)$$

将《数安法》内容划分为73条语句片段，数据安全直接相关的语句34条，现对词频较高的词语与数据安全进行共现强度分析，如图5所示。通过数据分析发现，数据安全保护的共现强度数值最高为0.302 5，《数安法》中数据安全保护义务单独设置为一章，它强调重要数据的处理者应当设立数据安全负责人和管理机

构，落实数据安全保护责任；数据安全监管的数值为0.147 1，《数安法》中重点明确各行业、各领域数据安全监管职责，在出现履行数据安全监管责任问题时会依法给予相应处分；数据安全保障的数值为0.105 0，提高数据安全保障能力，坚持总体国家安全观，建立健全数据安全治理体系是《数安法》的总体原则和目标；数据安全风险的数值为0.094 1，它是影响数据安全的重要因素，建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制，加强数据安全风险信息的获取、分析、研判、预警工作是数据安全制度建设的首要任务；数据安全交易的数值为0，数据交易是数据活动的重要形式之一，在《数安法》中国家主要通过建立健全数据交易管理制度，来规范数据交易行为并培育数据交易市场，因此数据安全与交易在《数安法》中尚未体现出共现关系。

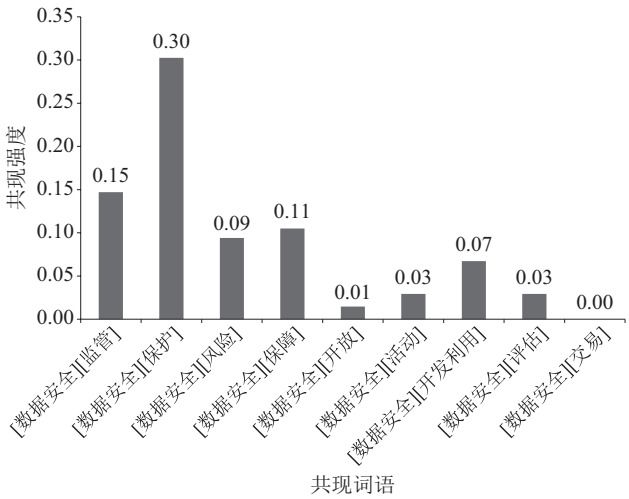

图5 《数安法》中词语共现强度分析

2.3 对比分析

对数据安全领域另外两部政策法规《数据安全管理办法（征求意见稿）》《网络安全法》中的词频进行分析，通过去除无实际意义的词语，在《数据安全管理办法（征求意见稿）》中显示个人信息、网络、运营者词频最高，数据安全、保护、保障、风险、评估、监督、合法权益等词频较高；而《网络安全法》中显示网络安全、网络词频最高，运营者、保护、保障、风险、评估、监督管理等词频较高。

对比发现，三部政策法规虽然在数据安全监管、数据保护力度，尤其是对重要数据保护和安全风险评估等方面具有较强的一致性，但整体关注的对象和重点差别较大。《数据安全管理办法（征求意见稿）》在继承《网络安全法》原则性规定的基础上，着重规范了网络运营者对于个人信息和重要数据的安全管理义务；而《数安法》是在《数据安全管理办法（征求意见稿）》基础上构建了数据安全保护管理制度，强化了国家数据安全保障能力，直面数据安全给国家安全带来的风险与挑战，切实维护国家主权、安全和发展利益。《数安法》紧紧抓住了国家安全保障和数据要素流通两个关键问题，较好地把握了安全与发展的平衡关系，《数安法》在《网络安全法》对网络数据安全保障的基础上，进一步覆盖了网络数据和非网络数据安全的管理，并在政府数据开放问题研究上有一定的突破。

3 数据安全保护体系建设思路

本文基于对《数安法》政策文本的分析结果，从法律体系、保护制度、监管职责、风险评估4个方面对我国数据安全保护体系提出建设思路[24]。

3.1 多法规共筑国家数据安全法律体系

《数安法》是国家数据安全立法的顶层设计，为全面维护国家数据安全奠定了重要法律基础。在比较《网络安全法》和《数据安全管理办法（征求意见稿）》中的词频后发现三部政策法规相互支撑、紧密联系，而《数据安全管理办法（征求意见稿）》中更多提到了关于个人信息的安全管理义务，其内容可以为《个人信息保护法》提供借鉴。未来随着《数安法》《个人信息保护法》的正式发布实施，它将与《网络安全法》形成从数据、网络数据、个人信息三个维度构建数据安全法律体系，数据安全法律体系的构建将对各行业数据合规工作提出更高、更细的要求[25]。这会使当前较分散的数据安全政策法规得到新的补充和完善，我国数据安全政策法规将紧紧围绕这三部法律来展开，全面实现以数据开发利用和产业发展促进数据安全法律体系建设的新局面。

3.2 完善数据分类分级保护制度

数据分类分级在保障数据安全过程中至关重要，它是数据安全保护的基础，数据分类的目的是要明确数据的业务范畴，数据分级要从满足监管要求的角度

出发，根据数据敏感制定不同的数据安全保护策略，它是组织内部管理体系编写的基础[26]。做好数据的分类分级是一个长期工程，在不同行业中数据特性不同，数据分类可以按数据行业进行划分，而对于数据分级应按照对国家安全和重大社会公共利益的危害程度进行划分：首先考虑重要数据，国家要通过建立重要数据目录保护制度来保障数据安全；其次考虑敏感数据和一般数据，而敏感数据是可能通过与一般数据进行关联形成重要数据，因此敏感数据应受到一定程度的保护。目前重要数据目录保护的确立权属于“本地区、本部门、本行业”，该划分缺乏审慎性和明确性，导致重要数据的划分存在随意、狭窄等问题，由于数据的类型和性质有所不同，国家要根据数据在经济社会发展中的重要程度有计划有针对性地建立分类分级保护制度。

3.3 进一步明确数据安全监管职责

通过构建数据安全监管体系来确立监管原则和目标，明确监管主体及其职责，形成不同区域、不同层级之间监管协调机制，运用监管和社会监督结合、全程监管、科技监管等方法全面保障数据安全。从数据生命周期涉及的全流程构建数据全监管体系，首先要明确行业主管部门对本行业、本领域的数据安全监管职责；其次要明确国家安全机关与公安机关在职权范围内承担的数据安全监管职责；再次要明确各地区、各部门的主体责任并重新划分监管职责，厘清相关部门监管职责不但能减少网安及公安部门的监管量，还能有效实现国家对数据安全统筹协调与监管作用，这也符合数据安全监管的需求和现状[27]；最后，尤其针对重要数据和跨境流动数据的安全问题要有单独的数据安全监管职责划分。在现存《数安法》中，虽然对数据安全监管提及较多，但针对不同分类分级数据的安全监管职责与范围尚需进一步细化和明确。

3.4 建立数据安全风险评估机制

数据安全风险预警要从源头建立数据安全风险评估机制。国家要建立集中统一的数据安全风险评估、报告、信息共享、检测预警机制，应重点关注以下内容：首先是建立数据安全风险预警机制，找出能够对经济社会发展产生影响的内外部潜在因素，分析潜在因素的风险，明确数据安全风险预警的标准，进而建立风险预警机制；其次是建立数据安全风险识别机制，数据安全风险评估必须要识别风险，最重要的是量化不确定性程度和风险可能造成损失的程度，国家要设立持续监察机制，实时关注数据安全风险的变化[28]；最后是建立数据安全风险处置机制，《数安法》中也明确提出建立数据安全应急处置机制，这是在数据安全风险识别的基础上，采取不同措施对已知安全风险进行应急处置。针对重要数据要特别重视，应由国家相关部门建立高效权威的数据安全风险评估专项机制，通过缩短评估周期，最大限度地降低数据安全风险。

4 结语

随着社会的进步，数据资源的价值已毋庸置疑，尤其是数据要素成为经济社会发展新动能后，数据产业已经形成一条完整的链路，它涉及数据收集、存储、加工、使用、交付、流通等诸多环节，国家为促进数字经济的快速发展，在政策上积极鼓励数据开发与利用，但数据安全保护的政策法规较为滞后。《数安法》的出台将填补此鸿沟，作为我国数据安全保护体系构建的顶层设计，它将使数据安全领域的政策和法规紧密结合，未来国家会围绕《数安法》不断出台配套政策为我国数据安全保护体系建设提供有力支撑。

参考文献

[1] 马海群，张涛，李钟隽. 新冠疫情下政府数据开放与安全的系统动力学研究 [J]. 现代情报，2020，37（7）：3-13.

[2] 张涛，马海群，易扬. 文本相似度视角下我国大数据政策比较研究 [J]. 图书情报工作，2020（12）：26-37.

[3] 王玫黎，曾磊. 中国网络安全立法的模式构建——以《网络安全法》为视角 [J]. 电子政务，2019（9）：128-133.

[4] 刘艳红. 侵犯公民个人信息罪法益：个人法益及新型权利之确证——以《个人信息保护法（草案）》为视角之分析 [J]. 中国刑事法杂志，2019（5）：19-33.

[5] 张旭，阮重骏. 人工智能非法应用的犯罪风险及其治理 [J]. 中国特色社会主义研究，2019（4）：78-86.

[6] 蒋洁. 培育发展数据要素市场的疑难问题与法律应对 [J]. 图书与情报，2020（3）：22-24.

[7] 许可. 数据安全法：定位、立场与制度构造 [J]. 经贸法律评论，2019（3）：52-66.

[8] 韩伟. 安全与自由的平衡——数据安全立法宗旨探析 [J]. 科技

与法律，2019（6）：41-48，67.

[9] 徐漪，沈建峰. 从GDPR看我国《数据安全法》的立法方向 [J]. 产业与科技论坛，2020（10）：33-35.

[10] 刘金瑞. 聚焦维护国家安全定位 健全数据安全管理制度——完善《数据安全法（草案）》的若干建议 [J]. 中国信息安全，2020（7）：60-63.

[11] 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.

[12] CORNOCK M. General Data Protection Regulation（GDPR）and implications for research [J]. MATURITAS，2018，111：1-2.

[13] GREENE T，SHMUELI G，RAY S，et al. Adjusting to the GDPR：the impact on data scientists and behavioral researchers [J]. BIG DATA，2019，7（3）：140-162.

[14] HOOFNAGLE C J，SLOOT V D B，BORGESIUS F Z. The European Union general data protection regulation：what it is and what it means [J]. Information & Communications Technology Law，2019，28（1）：65-98.

[15] SOKOLOVA M. First successes of the new pan-European general data protection regulation [J]. Contemporary Europe-Sovremennaya Evropa，2020（2）：56-66.

[16] 马海群. 从《俄罗斯联邦信息安全学说》解读俄罗斯信息安全体系 [J]. 现代情报，2020（5）：13-18.

[17] 何茜. 西方文化渗透下我国网络意识形态安全发展态势与对策研究 [J]. 中国社会科学院研究生院学报，2018（3）：55-63.

[18] 孟庆华. 基于消费者行为特征大数据平台信息安全与隐私保护模型研究 [J]. 上海商学院学报，2017（3）：30-36.

[19] 张华平. NLPIR-ICTCLAS汉语分词系统 [EB/OL]. [2020-07-24]. http://ictclas.nlpir.org/.

[20] 马海群，张涛. 文献信息视阈下面向智慧服务的语料库构建研究 [J]. 情报理论与实践，2019，42（6）：124-130.

[21] 齐爱民. 中华人民共和国个人信息保护法学者建议稿 [J]. 河北法学，2019（1）：33-45.

[22] 王卫，张梦君，王晶. 数据交易与数据保护的均衡问题研究 [J]. 图书馆，2020（2）：75-79.

[23] 张涛，蔡庆平，马海群. 一种基于政策文本计算的政策内容分析方法实证研究 [J]. 信息资源管理学报，2019，9（1）：66-76.

[24] 覃庆玲，彭志艺，李晓伟. 全球数字经济浪潮下数据安全保护体系 [J]. 信息安全与通信保密，2020（2）：67-81.

[25] 吕毅. 主动构建数据安全体系，稳步推进数据安全治理 [J]. 现代情报，2019（12）：54-55.

[26] 王欣亮，任弢，刘飞. 基于精准治理的大数据安全治理体系创新 [J]. 中国行政管理，2019（12）：121-126.

[27] 张永胜. 强化政府对个人数据安全监管问题研究 [D]. 天津：天津大学，2018.

[28] 冯登国，张敏，李昊. 大数据安全与隐私保护 [J]. 情报理论与实践，2014，37（1）：246-258.

作者简介

马海群，男，1964年生，博士，教授，研究方向：信息政策与法律。
张涛，男，1981年生，博士研究生，高级工程师，通信作者，研究方向：政策文本计算、数据政策研究，E-mail：zhangtao@hlju.edu.cn。

Interpretation of Data Security Protection System Construction in China from the Data Security Law (Draft)

MA HaiQun[1] ZHANG Tao[2]
(1. Research Center of Information Resource Management, Heilongjiang University, Harbin 150080, China; 2. School of Information Management, Heilongjiang University, Harbin 150080, China)

Abstract: Data is a country's basic strategic resource, and the ability to control data has increasingly become a key factor in measuring national competitiveness. However, the security issues brought about by data are also related to national sovereignty security and development interests. The Data Security Law (Draft) issued in July 2020 systematically reflects the current national overall data security and development concept, which has important strategic significance for the construction of China's data security protection system. The article interprets the Data Security Law (Draft) from the perspective of qualitative and quantitative text analysis, and compares and analyzes with the Data Security Management Measures (Draft for Comment) and the Cyber Security Law. Finally, from the legal system, The four aspects of supervisory responsibility, protection system, and risk assessment provide ideas for the construction of the current data security protection system in China.

Keywords: Data Security; Policy Interpretation; Text Analysis; Data Security Law; Data Security Protection System

（收稿日期：2020-08-19）