Цифровое право

数据安全与发展— 中国《数据安全法》草案述评
Обеспечение безопасности данных в электронном виде (о законопроекте КНР «О безопасности данных»)
Ensuring data security in electronic form (About the draft law of the People's Republic of China "On data security")

张建文杨欢[1]
pangdongmei71@163.com

Чжан Цзяньвэнь,
профессор Юго-Западного политико-юридического университета, КНР
pangdongmei71@163.com

Ян Хуань,
магистр Юго-Западного политико-юридического университета, КНР
pangdongmei71@163.com

Zhang Jianwen,
Professor of the Southwestern University of Politics and Law, China
pangdongmei71@163.com

Yang Huan,
Master's Degree from the Southwestern University of Politics and Law, China

DOI: 10.17803/2587-9723.2021.4.074-081

摘要：数据是信息时代中一种新的生产要素，在大数据、人工智能、云计算、区块链等新型科技领域和数字经济领域不断快速发展的大背景下，数据对于企业的发展、社会发展、国家安全至关重要，数据安全问题影响国家发展与安全，关系公众利益，也与公民个人权益密切相关，需要在法律层面对数据的安全保护作出规范。2020年7月2日，在中国人大网公布并征求意见《中华人民共和国数据安全法（草案）》，其系统地反映当前国家整体数据安全与发展观，标志着数据安全上升到国家安全层面，与《网络安全法》一样作为国家整体安全观的组成部分，同属上位法，是法律效力最高的法律，对我国数据安全保护体系构建具有重要的战略意义。数据安全法作为数据安全管理领域的基础性法律，对于数据内涵的界定有一定突破，数据安全法中的数据不限于网络数据，而是包含电子形式和其他方式记录的信息；在数据安全法草案中赋予了必要的域外效力，对保护我国国家主权和公民权利具有重要的意义；明确了数据安全保护与数据开发利用的关系，通过立法明确数据在数字经济发展中的地位，从而充分发挥数据的经济价值；确立了行业安全责任、监管与统筹协调主体，增加了各地区、各部门的主体责任，重新划分了监管职责，更加符合数据安全监管的需求和现状；确立数据分级分类制度，将数据分级分类的主体设定为国家，有利于数据安全监管机关开展相应工作；在数据安全风险评估、报告、信息共享、监测预警制度之中设定了设立国家层面的相应机制；确立了数据出口管制制度和数据安全对等保护制度，对我国数据跨境流动体系构建做出了规范；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据

[1] 张建文，男，西南政法大学教授，博士生导师，从事民法学、中俄比较私法研究。 杨欢，西南政法大学2019级法律硕士研究生。

安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施。数据安全法草案中构建了全面信息安全理念，即将出台的数据安全法将将为数据安全与发展提供指引与基本原则，各行各业均应关注数据安全与发展的综合治理体系与各项配套规制，逐渐构建数据高效利用与安全发展的良好环境，对蓬勃发展的信息化和数字化起到极大推动作用。数据安全法将所有类别的信息均纳入保护范畴，未来数据安全法应注意与《网络安全法》、《国家安全法》以及正在制定中的《个人信息保护法》做好衔接，将当前较分散的数据安全相关立法得到补充和完善，我国数据安全法律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。
关键词：数据安全；安全管理；开发利用；政务数据

Abstract. *Digital data is a new factor of production in the information age. In the context of the rapid development of the latest technologies, such as big data, artificial intelligence, cloud computing and blockchain, as well as the continuous development of the digital economy, digital data plays an important role in the development of enterprises. Data security issues affect the development of a country and its security, are related to public interests, and are also closely related to the personal rights of its citizens. It is necessary to regulate data protection at the legal level.*

July 2, 2020 the website of the National People's Congress published the Data Security Law of the People's Republic of China (draft), which systematically reflects the current national point of view on data security and development, noting the improvement of data security to the level of state security. Like the Cybersecurity Law, it is a component of the general concept of national security, belongs to the highest level of law and has the highest legal force. This law is of great strategic importance for building a data protection system in the PRC.

As the main law in the field of data security management ,the Data Security Law has made certain breakthroughs in the definition of the concept of data. The concept of data in the Data Security Law is not limited to network data, but includes information recorded in electronic form and in other ways; the necessary extraterritorial consequences are provided for in the draft Data Security Law, which is of great importance for the protection of national sovereignty and civil rights of the People's Republic of China; the relationship between data security protection, data development and use is clarified, and the status of data in the development of the digital economy is clarified through legislation in order to fully demonstrate the economic value of data; the main body responsible for security, supervision and overall coordination has been created, the main responsibilities of various regions and departments have been increased, supervision responsibilities have been redistributed, which is more in line with the needs and current situation in data security supervision; a data classification system has been established that promotes the relevant work of data security surveillance agencies; an appropriate mechanism has been created at the state level in the system of data security risk assessment, reporting, information exchange, monitoring and early warning; a data export control system and a mutual data protection system were created, as well as the construction of a cross-border data flow system of the PRC was standardized; data protection obligations in organizations and for individuals performing data operations and performing data protection duties were clarified; adhere to the principles of security and development and provide measures to support and promote data security and development; institutional measures have been taken to ensure the security of government data.

The draft law on data security contains a comprehensive concept of information security. The upcoming Law on Data Security will contain recommendations and basic principles for ensuring data security and development. All industries will have to pay attention to an integrated management system and various supporting provisions to ensure data security and development. Gradually, a favorable environment will be created for the effective use of data and safe development, which will significantly contribute to the rapid development of informatization and digitization.

The Data Security Law includes all types of information in the field of protection. In the future, the Law on Data Security should pay attention to the Law on Cybersecurity, Law on State Security and Law on the Protection of Personal Information, which are under development, supplement and improve today's relatively disparate legislation related to data security. The laws and regulations of the PRC on data security will be carefully developed on the basis of these three laws in order to fully implement the development, use of data and industrial development, thereby promoting new provisions in the creation of a legal data security system.

Keywords: *data security; security management; development and use; Government data.*

随着现代社会的网络化、数字化和智能化，物理世界的“人”逐渐走向网络空间。人们就在天然的生物属性之外，获得了数字属性，从“生物人类”迈向“数字人类”，塑造了数字时代中“生物—信息”的双重人性。[2]在此背景下，数据安全问题直接关系到“数字人类”的安全问题。

各类数据迅猛增长、海量聚集，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。数据蕴含着重要的价值，其安全问题正日益显出。一方面，数据安全影响着国家政治经济安全，如著名的剑桥分析案[3]；另一方面，数据安全亦影响个人生活的安宁，如生活中随处可见的信息泄露。数据风险日益增大的当下，数据安全已经成为各国亟须规范的问题。

各类数据的拥有主体多样，处理活动复杂，安全风险加大，必须通过立法建立健全各项制度措施，切实加强数据安全保护，维护公民、组织的合法权益。总体国家安全观“既强调安全，又强调发展”，[4]数据安全法作为数据安全管理领域的基础性法律，其坚持安全与发展并重，重点是确立数据安全保护管理各项基本制度，并与《网络安全法》、《国家安全法》以及正在制定中的《个人信息保护法》做好衔接。目前《数据安全法（草案）》全文共计七章《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》《附则》，共计五十一条。

一、数据安全法立法目的和适用范围

如何保障数据安全与发展作为立法总目标和指导思想，并且贯穿本法的始终。并且将“数据安全与发展”作为一章进行了规范。这充分体现了本法的立法目标是以“数据安全与发展”作为核心目标，促进数据的安全保护与开发利用。

《数据安全法》作为一部安全保障法，明确了数据安全保护与数据开发利用之间的关系，保障数据安全的同时，促进数据开发利用，体现国家坚持维护数据安全与数据发展并重的原则。在确保数据安全的前提下，鼓励数据依法有效利用，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。

在数据安全法草案中明确规定，数据是指任何以电子或者非电子形式对信息的记录（第三条第一款），[5]该信息的形式既可是电子形式，亦可是非电子形式，按照这一规定，纸质档案信息以及以其他书面形式对信息所进行的记录，也属于数据。随着信息技术及图像识别技术的发展，所有其他方式记录的信息都有可能被转化为电子数据，非电子形式的信息与电子形式的信息在本质上并无区别。数据安全法草案将规范的对象严格限制为“数据”及与数据有关的法律关系，明确将“数据”定义为“对信息的记录”，界定了法律规制的边界。

数据活动是指数据的收集、存储、加工、使用、提供、交易、公开等行为（第三条第二款）。[6]数据活动已成为中国境内组织或者个人开展业务、日常生活所必不可少的环节，由此可见，数据安全法的适用范围较广。数据安全是指通过采取必要措施，保障数据得到有效保护和合理利用，并持续处于安全状态的能力（第三条第二款）。[7]

数据安全法适用于公民、组织与数据有关的权益，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。在数据安全法草案中还赋予了必要的域外效力，境外的组织、个人开展数据活动，损害国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任（第二条），数据安全法草案基于必要性原则，在国家安全、公共利益或者公民、组织合法权益方面确立了域外适用效力，对保护我国国家主权和公民权利具有重要的意义。

二、数据的安全与发展

数据安全是数字经济能够持续健康发展的基础保证，随着互联网、大数据、区块链等为支撑的数字经济的发展，数据安全和隐私保护开始受到关注。坚持安全与发展并重，既要保护数据安全，又要促进数据的开发利用。构建科学合理的数据安全制度体系，为数据的开发利用提供相应的法治环境，促进以数据为关键要素的数字经济的发展。

（一）数据安全治理体系

构建以数据为主导，从数据的收集、存储、使用，共享、转让、公开披露乃至删除整个周期来构建全链条的数据安全治理体系。数据安全治理体系的构建是一个从中央到地方、涉及政府、各行各业及其行业主管部门、关键信息基础设施网络运营单位、互联网平台、第三方评估机构以及社会各界共同构建的一个系统性工程。

维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。[8]（第四条）数据安全法草案中对从中央到地方再到数据活动主体等不同角色在数据安全发展与保护方面提出了不同要求。中央国家安全领导机构负责数据安全工作的决策和统筹协调，研究制定、指导实施国家数据安全战略和有关重大方针政策。[9]（第六条）各地区、各部门对本地区、本部门工作中产生、汇总、加工的

---

2 马长山:数字时代的人权保护境遇及其应对［J］．求是学刊，2020(4):103—020.

3 英议会公布“证据”：剑桥分析公司或助力特朗普 URL: https://m.huanqiu.com/article/9CaKrnK7PQ1.

4 中央国家安全委员会第一次会议召开习近平发表重要讲话 URL: http://www.gov.cn/xinwen/2014-04/15/content_2659641.htm.

5 《中华人民共和国数据安全法（草案）》第三条。

6 《中华人民共和国数据安全法（草案）》第三条。

7 《中华人民共和国数据安全法（草案）》第三条。

8 《中华人民共和国数据安全法（草案）》第四条。

9 《中华人民共和国数据安全法（草案）》第六条。

数据及数据安全负主体责任。工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。[10]（第七条）数据主体在开展数据活动，必须遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害公民、组织的合法权益。[11]（第八条）国家建立健全数据安全协同治理体系，推动有关部门、行业组织、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。[12]（第九条）

在数据安全治理体系构建的过程中，首先应制定数据安全治理的目标、健全数据管理和开发利用机制；其次应将制定的数据安全治理目标、管理和开发利用机制落实到实践之中，落实责任，不得非法收集数据、不得滥用数据、不得泄露数据；然后应建立数据安全风险评估机制，由于数据安全治理体系涉及数据的收集、存储、使用，共享、转让、公开披露乃至删除，因此应建立涉及数据处理全程的安全风险评估机制；最后应在全社会树立数据安全保护意识，数据安全持续发展涉及多元社会主体，包括政府、企业和个人，因此应开展数据安全保护宣传，在广大人民群众之中树立数据安全保护意识。

（二）数据发展措施

坚持安全和发展并重，以数据开发利用和产业发展促进数据安全，以数据安全来保障数据开发利用和产业发展。

在数据安全法草案中主要从国家层面上对数据的发展进行规定，国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用，促进数字经济发展。[13]（第十二条）国家加强数据开发利用技术基础研究，支持数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品和产业体系。[14]（第十三条）国家推进数据开发利用技术和数据安全标准体系建设。[15]（第十四条）国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、研究机构、高等学校、相关行业组织等参与标准制定。[16]（第十五条）国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。国家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。[17]（第十七条）国家支持高等学校、中等职业学校和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。[18]（第十八条）

坚持维护数据安全和促进数据开发利用并重为原则，然后统筹规划、技术创新、相关标准制定、专业机构评估认证服务、数据交易制度及专业人才培养等方面对数据发展措施进行进一步规定，主要是由于我国数据安全发展体系尚处于初级阶段，因此数据安全法草案根据基本原则从各个方面对数据安全发展体系的构建进行规制，随着数据领域、安全领域等总体环境的发展，再逐渐完善、细化数据安全与发展的法律体系，出台一系列相应的配套规定。

（三）数据安全制度

1.数据的分级分类管理

数据的分级分类管理是数据安全管理的基础，其直接决定着数据的收集、存储、使用，共享、转让、公开披露乃至删除整个周期的管理，数据的分级分类管理是迈向数据安全精细化管理的重要一步。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。[19]

在数据安全法草案之前，我国现有的法律法规也有数据分级分类的规定，但进行数据的分级分类的主体绝大多数是规范对象自身，而非国家。规范对象本身开展的数据分类分级，与国家开展数据分级分类工作存在本质上的区别。目前的现有的法律法规所提出的数据分类分级路径，在规范对象自身可以适用，但是其面对众多组织的监管部门来说，不具备可操作性，各个规范对象的数据分类和数据分级存在差异，将会导致数据安全监管机关无法开展统一的管理和监督工作，更无法判断其所维护的国家和公共利益、个人合法权益是否得到充分的保护。因此，在数据安全法草案中将数据分级分类的主体设定为国家具有必要性。

---

10 《中华人民共和国数据安全法（草案）》第七条。
11 《中华人民共和国数据安全法（草案）》第八条。。
12 《中华人民共和国数据安全法（草案）》第九条。
13 《中华人民共和国数据安全法（草案）》第十二条。
14 《中华人民共和国数据安全法（草案）》第十三条。
15 《中华人民共和国数据安全法（草案）》第十四条。
16 《中华人民共和国数据安全法（草案）》第十五条。
17 《中华人民共和国数据安全法（草案）》第十七条。
18 《中华人民共和国数据安全法（草案）》第十八条。
19 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.

在数据安全法草案中确立数据分级分类管理，国家进行数据分级分类的标准和依据是数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分级分类保护。[20]（第十九条第一款）

2. 重要数据

在网络安全法中首次提出重要数据的概念，并在第三十七条规定了关键信息基础设施运营者掌握的重要数据境内存储及出境应进行安全评估。

在数据安全制度方面，数据安全法草案中采取“目录”的方式来对重要数据进行保护，各地区、各部门应当按照国家有关规定，确定本地区、本部门、本行业重要数据保护目录，对列入目录的数据进行重点保护。[21]（第十九条第二款）重要数据的确立权在地区、部门、行业具有一定的随意性，为了防止重要数据保护目录的不统一和不规范，应首先由国家确定全国范围内的重要数据保护目录，再赋予各地区、各部门一定的权利根据国家统一重要数据保护目录来确定本地区、本部门、本行业的重要数据保护目录。

对于重要数据的保护，除了制定重要数据保护目录，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。[22]（第二十五条第二款）重要数据的处理者还应当按照规定对其数据活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括本组织掌握的重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。[23]（第二十八条）

重要数据作为数据的一个分支，对其的保护工作贯穿各项重要制度之中，而且重要数据应当作为重点对象，实施重点保护，重要数据的处理者除履行设立管理机构、风险评估等特定义务外，也应当履行一般数据保护义务。

3. 数据的国际交流与合作

随着全球经济一体化和数字经济的快速发展，数据跨境流动的需求日益迫切，但与之相关的国家安全、个人数据保护等方面的问题和挑战也日益突出。数据安全法草案中对我国数据跨境流动体系构建做出了规范。

国家积极开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动，[24]（第十条）确立了我国在数据领域国际交流合作的大方向。

在数据安全法草案第二十三条中规定了数据出口管制制度，中国对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。[25]（第二十三条）其将出口管制法中的管制对象从“货物、技术、服务”扩大到“数据”，为重要数据、个人非敏感数据、政府和公共部门的一般数据、行业非限制性技术数据的数据出口管制提供分类依据。

在数据安全法草案第二十四条中规定了数据安全对等保护制度，任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区采取相应的措施。[26]（第二十四条）数据安全对等保护制度的构建将推动建立公平的数据流动国际环境，为我国的数据跨境流动中依法、合法采取反制措施赋权，增大我国在数据跨境流动过程中域外保护管辖权。

在数据安全法第三十三条中规定，境外执法机构要求调取存储于中华人民共和国境内的数据的，有关组织、个人应当向有关主管机关报告，获得批准后方可提供。中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的，依照其规定，符合一般的国际操作惯例，保障了国际数据执法合作的合理需求，有利于增强全球执法合作，让国内的国际犯罪受到相应惩处。[27]其与国际刑事司法协助法第4条，构成了应对外国长臂管辖的“封阻法令”。

4.数据的风险管理机制

在数据安全法草案第二十条中规定了风险评估、监测预警机制，国家建立集中统一、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。通过设立风险评估、监测预警机制，对关涉数据安全的重大问题做到尽早发现尽早处理。[28]企业作为数据活动的主体之一，故在数据安全法中也应规定企业依法设置风险预测与应急处置机制，以防外部入侵、盗取或破坏企业数据，威胁国家、社会、公共安全。

5.数据的安全应急处置机制

在数据安全法草案第二十一条中规定了数据的安全应急处置机制，国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。[29]

6.数据安全审查制度

---

20 《中华人民共和国数据安全法（草案）》第十九条。
21 《中华人民共和国数据安全法（草案）》第十九条。
22 《中华人民共和国数据安全法（草案）》第二十五条。
23 《中华人民共和国数据安全法（草案）》第二十八条。
24 《中华人民共和国数据安全法（草案）》第十条。
25 《中华人民共和国数据安全法（草案）》第二十三条。
26 《中华人民共和国数据安全法（草案）》第二十四条。
27 《中华人民共和国数据安全法（草案）》第三十三条。
28 《中华人民共和国数据安全法（草案）》第二十条。
29 《中华人民共和国数据安全法（草案）》第二十一条。

在数据安全法草案第二十二条中规定了数据安全审查制度，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活动进行国家安全审查。依法作出的安全审查决定为最终决定，[30]即该决定排除申诉、复审、司法审查等制度的可能性，在实践中应注意不受制约的审查权难以保证审查决定的公正性与合法性。

数据安全保护义务

在数据安全法草案第四章规定数据主体的一般数据活动义务以及重要数据处理的义务；中介机构、专门数据经营者等特殊主体的安全保护义务；公安机关、境外执法机关执法过程中对数据的安全保护义务。

任何组织、个人收集数据，必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据，不得超过必要的限度。[31]（第二十九条）

开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求，建立健全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和其他必要措施，保障数据安全。[32]（第二十五条）

开展数据活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当按照规定及时告知用户并向有关主管部门报告。[33]（第二十七条）

除了针对开展数据活动的一般主体应当遵循的准则，数据安全法草案还规定了从事数据交易中介服务的机构从事中介服务时应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录；[34]（第三十条）专门提供在线数据处理等服务的经营者，应当依法取得经营业务许可或者备案，具体办法由国务院电信主管部门会同有关部门制定；[35]（第三十一条）公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。[36]（第三十二条）

开展数据活动以及研究开发数据新技术，还应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。[37]（第二十六条）

数据安全法草案原来规范性法律文件的合规要求上升为法律，在法律层面，详细规定了企业、组织及个人等的数据安全合规义务，对开展企业的数据活动具有重要的规范意义。

三、政务数据

电子政务系统以数据运算为前提，利用信息化手段为社会治理赋能扩容、提质增效，而数据安全是实现这些功能的前提。政务数据作为数据要素市场化的重要主体，应当发挥其在数据安全和开放共享的先锋作用。数据安全法中政务数据的安全与开放独立成一章充分说明了国家对政务数据安全与开放的重视程度。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。[38]国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。[39]（第三十四条）

国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行。[40]（第三十五条）国家机关在履行法定职责范围内依照相关法律法规的条件和程序，应遵循目的并不是毫无节制和无目的的去收集、使用数据，既是原则性的说明，例如目的限制、合法收集使用等原则，同时该条文也赋予了国家机关在收集、使用数据方面的合法性。

国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。[41]（第三十六条）国家机关同样需要建立健全数据安全管理制度，国家机关并不享有在其单位范围内豁免建立数据安全管理制度，这对于国家整体的数据安全的角度是重要的保障措施，国家机关所掌握的数据和企业所掌握的数据都需要更需要保障安全。

国家机关委托他人存储、加工政务数据，或者向他人提供政务数据，应当经过严格的批准程序，并应当监督接收方履行相应的数据安全保护义务。[42]（第三十七条）

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，推动政务数据开放利用。[43]（第三十九条）政务数据应以开放为原则，不予公开为例外。为增强其可操作性，应制定不予

30 《中华人民共和国数据安全法（草案）》第二十二条。
31 《中华人民共和国数据安全法（草案）》第二十九条。
32 《中华人民共和国数据安全法（草案）》第二十五条。
33 《中华人民共和国数据安全法（草案）》第二十七条。
34 《中华人民共和国数据安全法（草案）》第三十条。
35 《中华人民共和国数据安全法（草案）》第三十一条。
36 《中华人民共和国数据安全法（草案）》第三十二条。
37 《中华人民共和国数据安全法（草案）》第二十六条。
36 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.
39 《中华人民共和国数据安全法（草案）》第三十四条。
40 《中华人民共和国数据安全法（草案）》第三十五条。
41 《中华人民共和国数据安全法（草案）》第三十六条。
42 《中华人民共和国数据安全法（草案）》第三十七条。
43 《中华人民共和国数据安全法（草案）》第三十九条。

公开的数据目录。国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。[44]（第三十八条）

除国家机关之外，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数据活动，适用关于政务数据的规定。[45]（第四十条）

四、法律责任

数据安全法草案第六章规定了各主体违反法律规定的相关义务或职责所需承担的法律责任。承担责任的方式有约谈、整改、警告、罚款、没收违法所得、处分及依法需承担的民事、行政、刑事责任。数据安全法草案对于违反数据安全法的主体及负责主管人员和直接责任人员实行双罚制。

有关主管部门在履行数据安全监管职责中，发现数据活动存在较大安全风险的，可以按照规定的权限和程序对有关组织和个人进行约谈。有关组织和个人应当按照要求采取措施，进行整改，消除隐患。[46]（第四十一条）明确了数据安全监管中的约谈制度。其与网络安全法中第五十六条规定的网络安全监管的约谈制度相类似，数据安全监管也将约谈制度法定化。二者的区别主要在于约谈的主体，网络安全法中所规定的约谈主体为“省级以上人民政府有关部门”，数据安全法草案中所规定的约谈主体的规定为“有关主管部门”，约谈主体的模糊胡规定有可能导致约谈制度的滥用。

开展数据活动的组织、个人未依法履行数据安全保护义务或者未采取必要的安全措施的，由有关主管部门责令改正，给予警告，可以并处一万元以上十万元以下罚款，对直接负责的主管人员可以处五千元以上五万元以下罚款；拒不改正或者造成大量数据泄漏等严重后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。[47]（第四十二条）

数据交易中介机构未履法律所规定的义务，导致非法来源数据交易的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得的，处十万元以上一百万元以下罚款，并可以由有关主管部门吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。[48]（第四十三条）

专门提供在线数据处理等服务的经营者，未依法取得经营业务许可或者备案，由有关主管部门责令改正或者予以取缔，没收违法所得，处违法所得一倍以上十倍以下罚款；没有违法所得的，处十万元以上一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。[49]（第四十四条）

在国家机关不履行数据安全保护义务和国家工作人员玩忽职守、滥用职权、徇私舞弊应承担相应的法律责任。国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。[50]（第四十五条）履行数据安全监管责任的国家工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。[51]（第四十六条）

通过数据活动危害国家安全、公共利益，或者损害公民、组织合法权益的，依照有关法律、行政法规的规定处罚。[52]（第四十七条）

违反数据安全法所规定，给他人造成损害的，依法承担民事责任；构成违反治安管理处罚行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。[53]（第四十八条）

五、结语

数据只有在交换和使用中才能产生价值。数据安全法草案坚持安全与发展并重，明确了发展是安全的目的。不存在绝对的数据安全，亦无法追求绝对安全，在构建科学合理的数据安全制度体系下，让信息网络助力各行各业转型和创新发展，促进以数据为关键要素的数字经济的发展。

数据安全法围绕着数据安全、数据流动和数据监管，构建数据安全基础上的数据流通和产业产品体系、数据安全标准体系、数据交易管理制度、数据安全培训和教育体系、重要数据保护目录制度、国家数据安全监测预警机制、国家数据安全应急处置机制、国家数据安全审查制度、国家数据出口管制制度、国家数据对等措施、企业数据安全管理制度、企业重要数据风险评估报告制度、数据中介交易审查制度、国家机关调取数据制度、配合境外执法机关的批准、政务数据安全与开放等制度，但数据安全法中大多为原则性规定，后续的实施需要大量的配套立法，在未来的实施过程中要注意与《网络安全法》、《国家安全法》以及正在制定中的《个人信息保护法》做好衔接工作。

---

44 《中华人民共和国数据安全法（草案）》第三十八条。
45 《中华人民共和国数据安全法（草案）》第四十条。
46 《中华人民共和国数据安全法（草案）》第四十一条。
47 《中华人民共和国数据安全法（草案）》第四十二条。
48 《中华人民共和国数据安全法（草案）》第四十三条。
49 《中华人民共和国数据安全法（草案）》第四十四条。
50 《中华人民共和国数据安全法（草案）》第四十五条。
51 《中华人民共和国数据安全法（草案）》第四十六条。
52 《中华人民共和国数据安全法（草案）》第四十七条。
53 《中华人民共和国数据安全法（草案）》第四十八条。

未来随着《数据安全法》《个人信息保护法》的正式发布实施，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。[54]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。

参考文献

1. 《中华人民共和国数据安全法（草案）》。
2. 马长山:数字时代的人权保护境遇及其应对［J］．求是学刊，2020 (4) : 103—111.
3. 英议会公布"证据"：剑桥分析公司或助力特朗普https://m.huanqiu.com/article/9CaKrnK7PQ1.
4. 中央国家安全委员会第一次会议召开习近平发表重要讲话http://www.gov.cn/xinwen/2014-04/15/content_2659641.htm.
5. 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.
6. 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.
7. 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.

[54] 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.