ZHONG HUA REN MIN GONG HE GUO
SHUJUANQUANFA SHIYI

中华人民共和国
数据安全法
释义

新法解读　逐条释义　实务指导

龙卫球 ◎ 主编

高品质专家释义　立法专家组织编写，满足学习研究、实务应用多层次需要

特色释义体例　针对法条从规范对象、规范基础、条文理解、典型案例、关联规定等多方面展开深入分析

实务操作指引　为新法的准确适用提供专业解读和适用指引

中国法制出版社

主 编

龙卫球

副主编

周学峰　赵精武

撰稿人

崔馨元　程　喆　何傲翾　韩富鹏　林洹民　刘　建
李　游　雷震文　裴　炜　徐　实　魏露露　赵计义
张建悦　周瑞珏　赵　鑫　周子琪

ZHONG HUA REN MIN GONG HE GUO
SHUJU ANQUANFA SHIYI

中华人民共和国
数据安全法
释义

新法解读 逐条释义 实务指导

龙卫球 ◎ 主编

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

前 言

2020年4月9日，中共中央、国务院首次出台关于要素市场化配置的文件《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》，指出土地、劳动力、资本、技术、数据五大生产要素的改革方向和相关体制机制的建设要求。数据由此成为最新一种广泛应用于社会生产经营活动的生产要素，这充分说明数字技术和数据已经从助力经济发展的工具转变为引领经济发展的关键要素。在数字经济的时代浪潮之下，数据产业从计算领域发端，陆续延伸到科学、商业和政务领域，极大地变革了人类社会的产业结构和生活方式，但随着大数据时代的迭代更新，各类数据处理活动逐渐展现出“野蛮生长”的态势，政务数据、企业商业秘密和个人数据泄露时有发生，无序的数据跨境流动为国家主权安全埋下隐忧，部分企业、平台甚至利用数据侵害公民合法权益，为我国数据产业的可持续健康发展提出了现实挑战。

数据发展与数据安全相伴相成，不可偏废。全球范围内，数据应用的发展正逐渐从技术向治理迁移，数据治理将提供更具共识、更可操作性、更加安全的制度方案和政策框架，以释放数据新动能，推动数字经济发展。但总的来看，目前在数据处理的分级分类管理、数据安全制度和安全义务、政务数据制度、法律责任等各方面，我国还尚未形成系统的社会治理规则，法律指引并不充分，制度建设还有待进一步细化，迫切需要在总体国家安全观的指导下，出台一部数据安全领域的基本法提供明确指引。

2021年6月10日，第十三届全国人大常委会第二十九次会议通过了《中华人民共和国数据安全法》（以下简称《数据安全法》），我国首部聚焦于数据安全的法律应运而生。《数据安全法》作为我国在数据领域的基

础性法律和国家安全领域的重要法律，为其他国家探索如何开展有效的数据治理、维护本国数据安全提供了中国方案，具有极强的实践意义和示范价值：

第一，《数据安全法》填补了数据安全立法的空白，完善了数据安全治理和保障国家安全的法律体系。在《数据安全法》之前，我国已经颁行了《中华人民共和国国家安全法》《中华人民共和国网络安全法》等促进国家安全治理能力提升与现代化的立法成果，其中虽然也规定了涉及网络安全与数据安全的条文，但无法充分应对我国数字产业化和产业数字化带来的显著问题。《数据安全法》旗帜鲜明地以“规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益”作为立法目的，重在维护数据处理活动中的国家主权、安全和发展利益，是在数据安全领域对总体国家安全观的深入贯彻，有效整合了分散的数据安全规定和政策标准，实现了数据安全的法制化，有利于不断发展和提升我国的数据安全治理能力。在《数据安全法》中，数据分类分级管理、数据安全审查、风险评估、监测预警和应急处置等基本制度得以确立，相关法律责任得以明确，从“规则之治”的层面强化数据安全领域制度建设。

第二，《数据安全法》主动回应实践中显现的新趋势、新问题、新挑战，兼具立法的完整性与开放性，兼采原则治理与规则治理的双重手段。从立法框架上看，《数据安全法》主要包括总则、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、法律责任和附则七大部分，从总体来看，数据安全法律规范的框架已基本完备，并与民法、刑法、行政法等部门法高度关联，体系上呈现高度的开放性。此外，《数据安全法》也关注到了数据产业的创新性要求，一方面有原则性规定，引导市场竞争有序开展、行业主动积极自律，不过多干涉相应主体的自发行动，另一方面也有较为具体和细致的制度性规定，明确了数据管理者、运营者乃至于国家机关应当遵守的义务和责任，在形成制约机制的基础上为其建立健全数据安全治理体系、提升数据安全保障能力指明了合规方向。

第三，《数据安全法》贯彻了发展与安全并重的基本原则，统筹考虑了数据安全与发展的两大需求。《数据安全法》虽以“安全”为名，但在制度构建上坚持数据安全保障与数据开发利用相辅相成、互相促进，相应地提出了促进数据开发利用、弥合数字鸿沟、推进政务数据开放、培育数据交易市场等要求，在促进数据创新应用、激发数据要素价值上进一步加强了顶层设计，也能让广大人民群众在数字化发展中获得更多幸福感、安全感。

总的来看，伴随《数据安全法》的落地实施，我国数据安全法律体系将进一步完善，数据处理活动也将进一步规范，国家主权、安全和发展利益将得到有效维护。未来，我国还将进一步制定相应配套法律法规和细分领域的更多单行立法，以应对全球数字化和一体化经济发展背景下的数据安全风险与挑战，促进《数据安全法》的有效性和可操作性不断提升，更充分地发挥数据要素的关键作用。

目 录

Contents

第三章 数据安全制度

第四章 数据安全保护义务

第五章 政务数据安全与开放

第一章 总 则

第一条 【立法目的】为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

【释义】

本条旨在阐明本法的立法目的。立法者阐明立法目的有助于人们理解立法宗旨，为执法机关和司法机关适用法律和进行法律解释提供指引和参考，以确保法律的正确贯彻实施。

随着以互联网、大数据、人工智能为代表的现代信息技术的广泛应用，当今社会正在加速进入信息化、数字化时代，特别是随着5G技术和工业互联网、物联网的发展，各类智能传感器遍布在人类生产、生活的各个角落，万物互联的时代即将到来，无论是人的生理状态、自然环境监测指标，还是社会生活的方方面面，几乎均可实现“数据化”。借助现代信息通信网络，数据可以在世界范围内进行实时传输和共享，其一方面可以促进全球范围内的经济往来和人与人之间的交往，另一方面数据安全的问题日益凸显，其不仅事关个人、组织的切身权益，亦事关国家主权、安全和发展利益。数据安全立法，旨在通过规范数据处理活动，保障数据安全和促进数据开发利用，从而实现保护个人、组织的合法权益与维护国家主权、安全和发展利益的目的。

数据安全法的规范对象是数据的处理活动。所谓数据处理活动，是指

数据的收集、存储、加工、使用、提供、交易、公开等行为。数据安全法所规范的数据类型既包括个人数据、商业数据，亦包括政务数据，特别是，数据安全法还以专章的形式规定了政务数据的安全与开放制度。数据处理活动，不仅是数据安全法的规范对象，亦是其他法律所规范的对象。例如，《民法典》中的有关条款亦涉及数据处理活动，但是，《民法典》侧重的是从私法的角度对民事主体的数据权益进行确认和保护，特别是对个人信息主体的民事权益进行保护。相比较之下，《数据安全法》从公法角度对数据活动进行规范，侧重维护数据处理活动中的公共秩序和国家安全。《数据安全法》与《个人信息保护法》亦有所不同。《个人信息保护法》主要是针对个人数据，而《数据安全法》则是针对一般性的数据，其注重的并不是个人数据和非个人数据的分类，而是基于安全目的对数据进行分级分类，区分重要数据和非重要数据，并对重要数据，特别是国家核心数据，进行重点规制。

坚持保障数据安全与促进数据开发利用并重是数据安全法在立法时坚持的一项基本原则。虽然从立法名称来看，《数据安全法》侧重“安全”属性，但是，立法者并非一味地强调安全，而是秉持安全与发展并重的指导思想，坚持保障数据安全与促进数据开发利用并重的原则。如果将本条款与《数据安全法》第13条结合起来看，更容易理解《数据安全法》的立法宗旨。数据安全法所维护的数据安全，并不限于以数据存储安全为代表的静态的数据安全，或以限制数据收集为目的的消极的数据安全，而是更加强调数据的动态安全和积极安全，强调维护数据在开发利用过程中的安全。维护数据安全的目的并不是要限制数据的开放利用，而是为了更好地保障数据开发利用的健康发展和可持续性发展。党的十九届四中全会明确提出数据系一种新的生产要素，[①] 从长远来看，数据的开发利用将会越来越广、越来越深，通过数据安全法律制度为数据开放利用和数字经济的

① 《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》，2019年10月31日中国共产党第十九届中央委员会第四次全体会议通过。

发展提供法治保障是立法的一项重要任务。

保护个人、组织的合法权益是制定数据安全法的重要目的。在当今数字社会时代，个人和组织的行为是数据持续产生的重要来源，亦是与数据处理活动关系最直接、最密切的群体，数据安全关系着每一个个人和组织的切身利益。近些年，发生了一些不良企业和犯罪分子实施窃取、泄露、非法交易和滥用数据，以及利用数据实施电信诈骗等违法犯罪活动的事件，导致许多公民和企业的合法权益遭受了严重损害，因此，制定《数据安全法》的一个重要目的就在于通过建立数据安全风险评估、报告、信息共享、监测预警和应急处置机制等数据安全制度，对数据处理者施加安全保障的法律义务，对违反数据安全法律制度的数据处理行为进行惩治，切实维护个人、组织的合法权益。另外，个人、组织的安全与国家安全之间亦具有密切的关联性。当发生数据安全事件，导致大规模的个人、组织的数据泄露或被滥用时，不仅会损害个人、组织的数据权益，亦有可能危及公共安全和国家安全。

维护国家主权、安全和发展利益，是制定数据安全法的根本目的。所谓“国家主权、安全和发展利益”，其含义并不是静止的、一成不变的，而是动态的、与时俱进的。在当今信息化时代背景之下，数据已成为一种重要的国家基础性战略资源，对数据和数据处理活动的管辖和规范是一个国家行使主权的表现形式之一，数据主权是国家主权的重要组成部分。从国家安全的角度来看，数据安全亦是国家安全的重要组成部分，在信息化时代，没有数据安全就没有国家安全。党的十八届四中全会指出，贯彻落实总体国家安全观，加快国家安全法治建设，抓紧出台反恐怖等一批急需法律，推进公共安全法治化，构建国家安全法律制度体系。[①] 2015 年 7 月，第十二届全国人民代表大会常务委员会第十五次会议通过新的《国家安全法》，该法第 25 条明确规定：“国家建设网络与信息安全保障体系，提升

① 《中共中央关于全面推进依法治国若干重大问题的决定》，2014 年 10 月 23 日中国共产党第十八届中央委员会第四次全体会议通过。

网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”因此，制定《数据安全法》的目的之一在于落实《国家安全法》的相关要求，通过建立数据分级分类管理、数据安全审查、数据处理规范等法律制度，建立健全数据安全治理体系，充分保障数据的安全可控，确保数据领域的国家安全。在当前世界范围内，数字经济已成为引领经济发展的新引擎，而数据系数字经济的重要要素，亦是数字社会的基础，数据资源已成为国际竞争的重要资源，因此，数据安全不仅事关国家安全，亦关乎中国的发展利益。

【关联规定】

《中华人民共和国国家安全法》第2条、第25条

（撰稿人：周学峰）

第二条 **【适用范围】**在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

【释义】

本条是关于本法调整范围的规定。

第一，数据处理者实施的数据处理活动和监管机构对数据处理活动的

安全监管行为，都应当受本法调整。数据安全法所规范的数据，不仅包括电子数据，亦包括以除电子外的其他形式存在的数据。所谓数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。所谓数据处理者，是指从事数据处理的个人和组织。只要数据处理者实施了上述数据处理活动中的一种，就要受数据安全法的约束。数据安全监管机构在对数据处理活动实施监管时，应当遵循依法监管的原则，严格按照数据安全法所规定的权限分工和执法程序履行监管职责。

第二，《数据安全法》是数据安全领域的基本法，其确立了数据安全的一般性法律制度。在数据安全法律领域，除了数据安全法以外，还存在其他相关法律。如果其他法律对特定类型的数据安全做出了特别规定，应遵循该特别法的具体规定，而对于特别法没有规定的事项，则应适用数据安全法。为了准确地理解数据安全法的适用范围，应当将该法的第 2 条与第 53 条、第 54 条结合起来进行分析。例如，对于涉及国家秘密的数据处理活动，因为该类数据具有特殊性，并且《保守国家秘密法》等法律、行政法规已对此作出了特别的具体规定，因此，应当适用该特别规定。

第三，从空间效力来看，在确定一部法律的管辖权范围时，不同国家、不同法律所采取的原则并不相同，主要有属地原则、属人原则、保护原则。所谓属地原则，是以地域作为界定管辖权的标准，凡是在本国领域内发生的行为，均应适用本国法律；所谓属人原则，是指以人的国籍为标准，凡是本国的公民、法人从事的行为，不论其行为发生在本国领域内还是本国领域外，均应适用本国法律；所谓保护原则，是指以保护本国利益为标准，凡是侵害本国国家、公民、法人或其他组织的利益的，无论行为人的国籍为本国人还是外国人，也无论行为发生在本国领域内还是本国领域外，均应适用本国法律。从总体上来看，我国的数据安全法在确定管辖范围时采取了以属地管辖为原则、以保护管辖为补充的方式，其以行为人的行为地，即数据处理活动发生地，而非行为主体的身份，作为确定管辖权的基准，同时辅之以保护原则，以全面维护国家利益、公共利益、公民

和组织的合法权益。

第四，依照属地管辖原则，在中华人民共和国境内开展数据处理活动，应受到本法的调整。《数据安全法》所规范的数据，既包括电子形式的数据，亦包括以其他形式存在的数据。对数据的处理，有可能通过互联网进行，也有可能采取网络以外的方式。因此，在判断数据处理活动是否是发生在中华人民共和国境内，需要基于数据类型、数据处理方式和具体情形来进行判断。

第五，依照保护管辖原则，在中华人民共和国境外实施的数据处理活动，如果其损害了中华人民共和国国家安全、公共利益或者公民、组织合法权益的，中国有关主管机关有权依照数据安全法和相关法律追究行为人的违法责任。基于该规定，对于发生在中华人民共和国境外的数据处理活动，是否适用中国的数据安全法，是依照其行为效果来确定的，只有当其损害了中国的国家安全、公共利益或者公民、组织的合法权益时，才适用中国的数据安全法，中国的有关行政机关和司法机关可基于此行使执法管辖权和司法管辖权。赋予数据安全法以一定的域外效力是十分有必要的，因为，实践中大量的数据都是以电子形式存在的，而且对数据的收集、存储、使用、加工、传输、提供、公开等数据处理活动都是通过互联网进行的，许多违法犯罪分子往往使用设置在中国境外的服务器对中国境内的公民、组织的网络设施进行攻击、侵入，并将非法获取的数据传输到境外进行处理，如果对此仅适用属地原则，将难以对违法者追究法律责任。通过立法所确认的保护管辖原则，中国的执法机关和司法机关可以对发生在中国境外的违法行为进行管辖并追究违法者的法律责任。

【关联规定】

《中华人民共和国网络安全法》第2条、第5条

（撰稿人：周学峰）

第三条 【数据、数据处理和数据安全的定义】本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

【释义】

本条的规范对象是《数据安全法》的具体适用范围和调整对象，明确界定“数据”“数据处理”和“数据安全”三个关键概念，这也是区分《民法典》个人信息保护条款、《个人信息保护法》和《数据安全法》三部重要法律体系定位的重要依据。

首先，该条明确将“数据”界定为“信息”的表现形式，即是以电子或其他方式记录的信息，在第 2 条的基础上进一步细化本法的适用范围。在该法制定过程中，“数据”和“信息”之间的概念区分存有争议，主要包括三种观点：一是“信息”属于“数据”的子概念，“信息”是从采集的“数据”中提取的有用内容；二是“信息”与“数据”相互混用，概念区分没有实质意义；三是“数据”属于“信息”的子概念，仅表示“信息”在电子通信环境下的表现形式。但从第 3 条内容来看，“数据”和“信息”的关系是载体与内容的关系，所有的“数据”都是信息，但不是所有的“信息”都是“数据”，因为现实生活中“信息”的表现形态除了电子数据之外，还包括日常对话、横幅标语等。此外，据第 2 条第 1 款之规定，“数据”的实际表现形态除了常见的二进制、电信号、计算机代码等电子方式之外，还包括其他信息记录方式。这里的兜底性规定实际上为未来信息技术迭代产生的新生客体预留了足够的解释空间，及时填补了相对稳定的法律规定与技术创新实践之间可能产生的立法空白。