深度
《数据安全法》全面解读

2021年6月10日，新华社报道，十三届全国人大常委会第二十九次会议通过了数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于2021年9月1日起施行。

数字化改革推动我国生产模式的变革，随着经济数字化、政府数字化、企业数字化的建设，数据已经成为我国政府和企业最核心资产。合资企业、跨境贸易、多厂商全球合作的模式变迁，数据开始在企业与企业之间、政府与企业之间以及国与国之间流转、融合、使用。

根据公开报道，2020年全球数据泄露的平均损失成本为1145万美元，2019年数据泄露事件达到7098起，涉及151亿条数据记录，比2018年增幅284%，数据泄漏事件影响大、损失重。

有专家提出，对数据掌控、利用以及保护能力，已成为衡量国家之间竞争力的核心要素。

外力驱动和内部需求促使数安法落地

外力驱动

2018年3月23日，时任美国总统特朗普正式签署《澄清域外合法使用数据法》，法案要求对危害美国国家安全的犯罪、严重刑事犯罪等重大案件，无论服务提供者的通信、记录或其他信息是否存储在美国境内，要求服务商根据该法案进行调取并提供相关证据。

2018年5月25日，欧盟《通用数据保护条例》（GDPR）正式实施。GDPR法案要求不论数据控制者、处理者及其处理行为在欧盟境内还是境外，只要处理的是欧盟境内居民的数据，均适用此法案，对数据实施长臂管理。

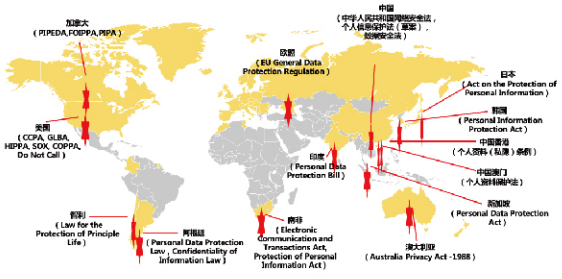


图1 全球数据安全保护立法情况（部分）

目前全球已有近100个国家和地区制定了数据安全保护的法律，数据安全保护专项立法已成为国际惯例。

面对欧美国家将数据主权从物理边界转向技术边界，将会直接影响到第三方国家的主权，在数据跨境流动愈加频繁的今天，必须尽快完善我国相关法律法规，保护我国国家利益、跨国公司以及公民个人利益。

内部需求

当前全球传统经济增长缓慢，尤其是2020年全球"新冠疫情"给经济带来了沉重的打击。迫切需要通过新的经济增长点拉动内需，增加就业，而数字经济正是切入点和发动机，将发展数字经济提升到国家战略高度则水到渠成。

近年来数字经济增速也证明了数字经济发展空间的巨大，中国信息通信研究院发布的《中国数字经济发展白皮书》数据显示，我国数字经济的总体规模已从2005年的2.62万亿元增长至2019年的35.84万亿元;数字经济总体规模占GDP的比重也从2005年的14.2%提升至2019年36.2%。中国信息通信研究院最新发布的数据显示，2020年中国数字经济规模达39.2万亿元，占GDP比重上升至38.6%。

可见，数字经济已成为我国国民经济增长要素的重要一员。从2015年，国务院发布的《促进大数据发展行动纲要》开始，2018年国务院发布《科学数据管理办法》，2020年国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，2021年3月12日，新华社公布了《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，数据安全政策导向明确，国家数据战略清晰。因此，亟需一部国家的基本法，为中国数字经济的安全发展保驾护航。

上述背景下数安法诞生，恰逢其时，旨在维护我国的数据主权，保障国家的安全、促进经济健康发展。

数据来源：中国信息通信研究院

数安法要点解读和提炼

数安法的发布标志着我国将数据安全保护的政策要求，通过法律文本的形式进行了明确和强化。

本法一共七章五十五条，其中 “总则”、“法律责任”及“附则”三章属于常规章节，另外四个章节围绕着“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”展开。

数据安全法

第一章	总则
第二章	数据安全与发展
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
第六章	法律责任
第七章	附则

我们对数安法进行深入解读后，为大家提炼出39个要点。

总则的要点

1	适用范围	在中国境内开展数据活动的组织和个人。
2	定义数据	是指任何以电子或者其他方式对信息的记录。
3	保护要求	采取必要措施，对数据进行有效保护和合法利用，并持续保持其安全能力。
4	责任任务	工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主要行业会落地数据保护行业规范，并且落地本部门的数据安全规范。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。网信部门负责统筹协调和监管。
5	特别强调	特别的对行业组织提出了制定安全行为规范，加强行业自律，指导会员加强数据安全保护的要求。这项法规有效地消灭了灰色地带，对各行业都形成了法律约束，杜绝了数据的随意共享和流转。

数据安全与发展要点

6	发展原则	国家统筹发展和安全，坚持保障数据安全与促进数据开发利用并重。
7	战略要求	省级以上人民政府应制定数字经济发展规划。进一步细化了国家数据战略的执行主体。
8	标准体系	国家主管部门负责相关标准和体系的制定。
9	评估认证	国家促进数据安全检测评估、认证等服务的发展，支持专业机构依法开展服务。
10	人才培养	要采取率多种方式培养数据开发利用技术和数据安全专业人才。
11	特别强调	特别地，加强了公共服务的要求，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

数据安全制度要点

12	分类分级	国家建立数据分类分级保护制度，对数据实行分类分级保护，并确定重要数据目录，加强对重要数据的保护。
13	风险评估	要建立集中统一、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。
14	应急处置	要建立数据安全应急处置机制。
15	安全审查	要建立数据安全审查制度。
16	出口管制	对属于管制物项的数据依法实施出口管制，可以根据实际情况对该国家或者地区对等采取措施。这项法规进一步明确了国家对中国数据的主权，即我国数据是否在境内，并受到中国法律的保护。

数据安全保护义务要点

17	管理制度	在网络安全等级保护制度的基础上，建立健全全流程数据安全管理制度，组织开展教育培训。重要数据的处理者应当明确数据安全负责人和管理机构，进一步落实数据安全保护责任主体。
18	风险监测	对出现缺陷、漏洞等风险，要采取补救措施；发生数据安全事件，应当立即采取处置措施，并按规定上报。
19	风险评估	定期开展风险评估并上报风评报告。

20	数据收集	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。
21	数据交易	数据服务商或交易机构，要提供并说明数据来源证据，要审核相关人员身份并留存记录。
22	经营备案	数据服务经营者应当取得行政许可，服务提供者应当依法取得许可。
23	配合调查	要求依法配合公安、安全等部门进行犯罪调查。境外执法机构要调取存储在中国的数据，未经批准，不得提供。
24	特别强调	特别的，对关基信息基础设施的运营在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定;其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

政务数据安全与开放要点

25	管理制度	建立健全全流程数据安全管理制度，落实数据安全保护责任。
26	存储加工	委托他人存储、加工或提供政务数据，应当经过严格审批，并做好监督。受托方不得擅自留存、使用、泄露或向他人提供政务数据。
27	数据开放	构建统一政务数据开放平台，发布数据开放目录，推动政务数据开放利用。
28	适用主体	法律、法规授权的具有管理公共事务职能的组织。

法律责任要点

29 **不履行规定保护义务**

责令改正和警告，给予单位5万至50万元罚款，给予负责人1万至10万元罚款；拒不改正或造成大量数据泄漏等严重后果的，给予单位50万至200万元罚款，最高责令吊销相关业务许可证或者吊销营业执照，给予负责人5万至20万元罚款。

30 **危害国家安全和损害合法权益的**

给予200万至1000万元罚款，责令停业整顿、吊销相关业务许可证或者吊销营业执照，构成犯罪的，追究刑事责任。

31 未经审批向境外提供重要数据的

违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并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可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、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十万元以上一百万元以下罚款。

32 交易来源不明的数据

没收违法所得，对违法所得一至十倍罚款。没有违法所得或违法所得不足10万元的给予10万至100万元罚款，最高责令吊销营业执照；对主管和直接责任人1万至10万元罚款。

33 拒不配合数据调取的

由有关主管部门责令改正，给予警告，可以并处5万元至50万元罚款，对直接负责的主管人员和其他直接责任人员可以处1万至10万元罚款。

34 国家机关不履行安全保护义务

对负责人和直接责任人员依法处分。

35 国家工作人员违法

因玩忽职守、滥用职权、徇私舞弊，依法给予处分。

36 窃取或非法获取数据的

依照有关法律、行政法规的规定处罚。

37 给他人造成损害

依法承担民事责任，构成犯罪的，依法追究刑事责任。

附则要点

38 涉及国家秘密的数据

依据《中华人民共和国保守国家秘密法》以及相关法律法规执行。

39 涉及军事秘密的数据

由中央军事委员会依据本法另行制定。

数安法是继《 网络安全法 》提出数据的概念后，国家在数据安全立法层面的一个重大里程碑，是中国数字经济高速发展的压舱石和定海神针。

数据安全建设的几点建议

数安法作为数据安全管理的基本大法，给我们指明了方向并提供法律保障。有关单位和个人收集、存储、使用、加工、传输、提供、公开数据资源，都应当依法建立健全数据安全管理制度，采取相应技术措施保障数据安全。

未来如何做好数据安全建设?

政企在进行数据安全能力建设时，考虑数据安全、访问控制以及数据保护三个层面。形象地说，数据安全的首要目标是需要找数据在哪里？数据的主体是谁？访问控制是目前主流的数据安全能力之一，首要目标是数据使用者如何证明具备相应的数据权限？数据保护是更高层面的建设框架，首要目标是组织或个人如何确保数据已经被保护好了？

对于IT和信息安全从业人员来说，数据安全能力建设是最艰巨的任务之一。

关于数据安全能力的建设，安恒信息首席科学家刘博认为：

在业务层面，应当考虑建设包含预防、发现、消除泄密隐患为主的数据安全体系；

在技术层面，应当考虑建设数据风险核查能力、数据梳理能力、数据保护能力以及数据威胁监控预警能力4大核心数据能力；

最终建立"数据安全运营"的全过程自适应安全支撑能力，直至达到整体智治的安全目标。

1、建立健全管理组织体系和组织架构

企业数据安全管理的成败，主要取决主要领导是否重视？意识是否提升？全员是否参与？是否建立了一套完善数据安全管理组织？这是数据安全的重要保障。要形成"管理层重视、一把手负责、全员参与"的管理模式。

数据安全的六大基础

1. 意识到信息安全不仅是首席信息官的工作。
2. 将数据和信息视为业务资产般保护。
3. 保护可移动媒体和移动设备上的重要数据。
4. 知道您组织的重要数字资产的位置。
5. 意识到并非所有数据泄露都是由于外部攻击而发生的。员工也可能有意或无意地导致数据泄露。
6. 认识到满足立法和法规标准只是信息安全战略的起点。

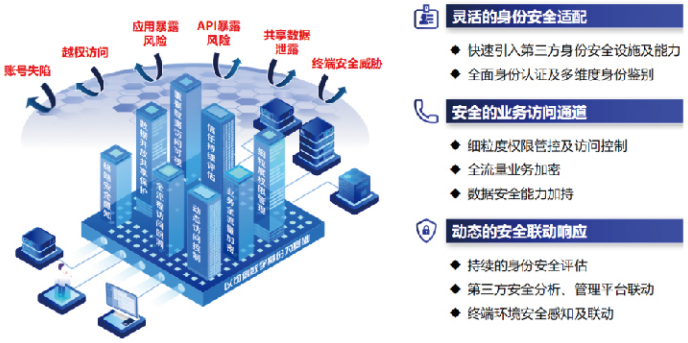
2、建立完善的数据安全技术体系并落地

传统方式已经无法适应新时代数据安全的需要，面临安全的新态势、新要求，在继续做好业务安全的基础之上，通过智能化管理平台，在技术层面实现对风险核查（Check）能力、数据梳理（Assort）能力、数据保护（Protect）能力以及数据威胁监控预警（Examine）能力4大核心能力的建设，在业务层面，实现对数据采集、传输、存储、处理、交换、销毁全生命周期的管理。

3、引进下一代技术，实现流程自动化

人工智能和机器学习将是未来数据安全工作的关键，目前，多数大型企业正在寻求使某些法规遵从流程自动化，包括数据定位和提取，自动化是大型企业保持对大量存储在数据中心和云中的结构化和非结构化数据兼容的唯一方式。

对于数据安全能力建设较为薄弱的企业，建议考虑零信任模式作为一种安全策略，有了“零信任”，企业将着眼于数据管理的整个生命周期，并将关注点从数据安全本身扩展到企业整体信息安全框架。



4、政府需落实数据安全保护责任，推动政务数据开放利用

政务数据安全与开发作为数安法的独立章节，要求我国政府在落实数据安全保护责任的同时，推动政务数据开放利用。如何实现数据要素安全、高效的共享开放？个人隐私保护、敏感数据使用、数据确权等难题都成了数据要素市场化的“拦路虎”，我们可以通过引入“数据安全岛”模式，利用安全计算沙箱、安全多方计算、区块链等技术，实现原始数据不出本地，只交换计算结果，做到数据共享的“可用不可见”，解决数据信任和隐私保护、溯源等难题，让流动的数据成为驱动数字经济发展的新动能。