

# 第一章 网络信息安全基础

## 第四节 网络空间安全法律法规及标准 - 数据安全法

主讲人：李建华 张全海  
网络空间安全技术研究院

2024 年 9 月

饮水思源 · 爱国荣校



1

立法背景

2

立法意义

3

概览及特点

4

重要条款解读

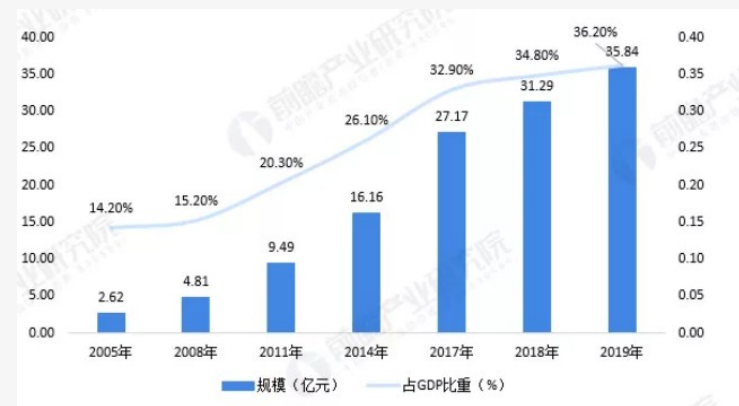
5

个人信息保护法



## 数据价值凸显

- 随着 5G、IoT、AI 等信息技术革命的推进，现实世界的各个角落变得越来越数字化、信息化。据 IDC 统计和研究，全球数据量已经进入了 ZB( $1\text{ZB}=10^{12}\text{GB}$ ) 级别，**IDC 的“大数据摩尔定律”表明，人类社会活动产生的数据一直在以每年 50% 的速度增长。**这些数据产生来源包括云、大数据平台以及各种各样的移动端、计算机、物联网设备与网络。2020 年，全球网络空间的数据量达到 64.2ZB 的规模，并且还将持续高速增长。
- 全球正式进入大数据时代，数据在社会发展、民众生活中扮演了越来越重要的角色。**数据是数字经济发展的新生产要素，甚至被认为是最核心生产要素，实现了可以构成生产资料的程度，被认为超过了石油的价值。**
- 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%。





## 数据泄露事件频发

- 2013 年曝光的美国棱镜事件更是使全球陷入数据安全恐慌，并引发了各国对于数据安全问题的警惕。在此背景下，欧盟等主要国家纷纷以立法形式规范数据安全问题，捍卫国家数据主权与安全。
- 2018 年 4 月，**Facebook 泄漏 8700 万人数据**，并将其用于美国总统大选，扎克伯格因此出席了美国参众两院听证会，被罚 50 亿美元；不久前欧盟隐私监管机构因**亚马逊违规收集和使用个人数据**，决定对亚马逊采取数额为 4.25 亿美元的处罚。







## 经济利益与数据安全发生冲突

- ① 数字化博弈的全球浪潮下，基于数据蕴含的极大价值，数字化转型的全球竞争日趋激烈，**世界各国对数据的争夺日益激烈**，且相关竞争已扩散到经济活动的方方面面，**覆盖范围从基础设施到生态应用**。
- ② 是围绕数据资源的国际争夺大幅延伸。数据跨境流动的隐蔽性会削弱一国对于本国数据的控制，**国家重要数据的流失也会危及该国的数据主权，对该国的数据安全产生威胁**。
- ③ 越来越多主权国家，开始用不同方式**构建并强化治理数据资源的整体框架**。各国数据治理体制机制遵循一个共同原则：即在国家安全、经济发展与社会繁荣之间，构建具有国别特色的均衡体系。



## 国内外相关法律法规

- ④巴西颁布了《通用数据保护法》，该法作为巴西首部有关个人数据保护的综合性立法显著增加了巴西个人数据保护的要求，进一步提升了巴西的数据保护能力。
- ④欧盟于2016年审议通过《通用数据保护条例》（**General Data Protection Regulation, GDPR**），并于**2018年5月正式实施的数据安全法律**，被认为是最严格的数据保护法令。《通用数据保护条例》，不仅加强了对相关企业的管控力度，还促进了对欧盟境内居民个人数据和隐私的保护。对于非个人数据的保护，欧盟委员会于2017年9月提出“促进非个人数据在欧盟境内自由流动”的立法建议。并于2018年10月4日，欧洲议会投票通过《非个人数据自由流动条例》。
- ④美国也在2018年出台《澄清域外合法使用数据法》。另外，美国于1996年颁布的《健康保险隐私及责任法案》（Health Insurance Portability and Accountability Act, HIPAA），确保健康信息的安全性和隐私性，并且保护个人的健康信息；2018年6月28日，美国加州**参考GDPR**通过《**2018加州消费者隐私法案**》（**California Consumer Privacy Act, CCPA**）该法案被称为美国“最严厉和最全面的个人隐私保护法案”，将于**2020年1月1日**生效。
- ④2016年11月，我国立法机构审议通过《**中华人民共和国网络安全法**》并于次年6月正式施行。2017年4月11日发布《个人信息和重要数据出境安全评估办法》征求意见稿。我国于2019年5月15日正式实施《中华人民共和国政府信息公开条例》，旨在保障人民群众依法获取政府信息。2019年5月28日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**）。2020年，我国先后发布了《**关于构建更加完善的要素市场化配置体制机制的意见**》《**关于新时代加快完善社会主义市场经济体制的意见**》等相关文件，明确将数据列为土地、劳动力、资本、技术之后的第五大生产要素。

**全球107个国家和地区已经制定了数据安全和隐私保护法律，亚洲、非洲只有不到40%的国家有相关法律**



1

立法背景

2

立法意义

3

概览及特点

4




重要条款解读

5

个人信息保护法



## 规范数据处理，保护合法权益


-  规范数据活动，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






## 对数据的有效监管实现有法可依、 填补数据安全保护立法的空白





近年来，数据泄露、勒索病毒、个人信息滥用等，都表明对数据保护的需求越发迫切

需要单独有一部针对数据安全保障领域的法律来加强对数据的监管，《数据安全法》的施行将提升数据安全保护的立法层级，在全国形成统一的数据安全保护体系，有效维护我国数据安全。

《数据安全法》构成了数字经济时代的法治基石，是构建国家安全法律制度体系的重要举措，有助于提高我国应对数据风险与挑战的能力。



## 提升国家数据安全保障能力

-  随着“云大物智移”等新技术的使用，全场景、大规模的数据应用对国家安全造成严重威胁
-  数据安全是国家安全的重要组成部分，通过法律的立法和实施，可以有效提升数据安全保障能力，如法律规定：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。
-  为我国数字化转型的健康发展提供法治保障，为构建智慧城市、数字政务、数字社会提供法律依据。
-  《数据安全法》进一步提升了国家数据安全保障体系和能力建设，推动形成安全有序、公正合理的数据治理新格局，切实全面维护国家主权、安全和发展利益。




## 激活数字经济创新，提升数据利用价值

- ① 数据作为在数字经济时代的关键生产要素，其自身具有很大的经济价值
- ② 安全是发展的前提，发展是安全的保障，数据安全是数字经济健康发展的基础。
- ③ 法律的发布，标志着国家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
- ④ 坚持维护数据安全性与促进数据开发利用并重，二者互相促进。《数据安全法》的正式实施将为我国在国际数字经济市场中提供坚实有力的保障。



## 扩大数据保护范围

 法律明确了：数据是指任何以电子或非电子形式对信息的记录，包括电子数据和非电子形式的数据，这对数据安全保障的范围提出了更广泛的要求，比《网络安全法》中的数据范围有所扩大。





1

立法背景

2

立法意义

3

概览及特点

4

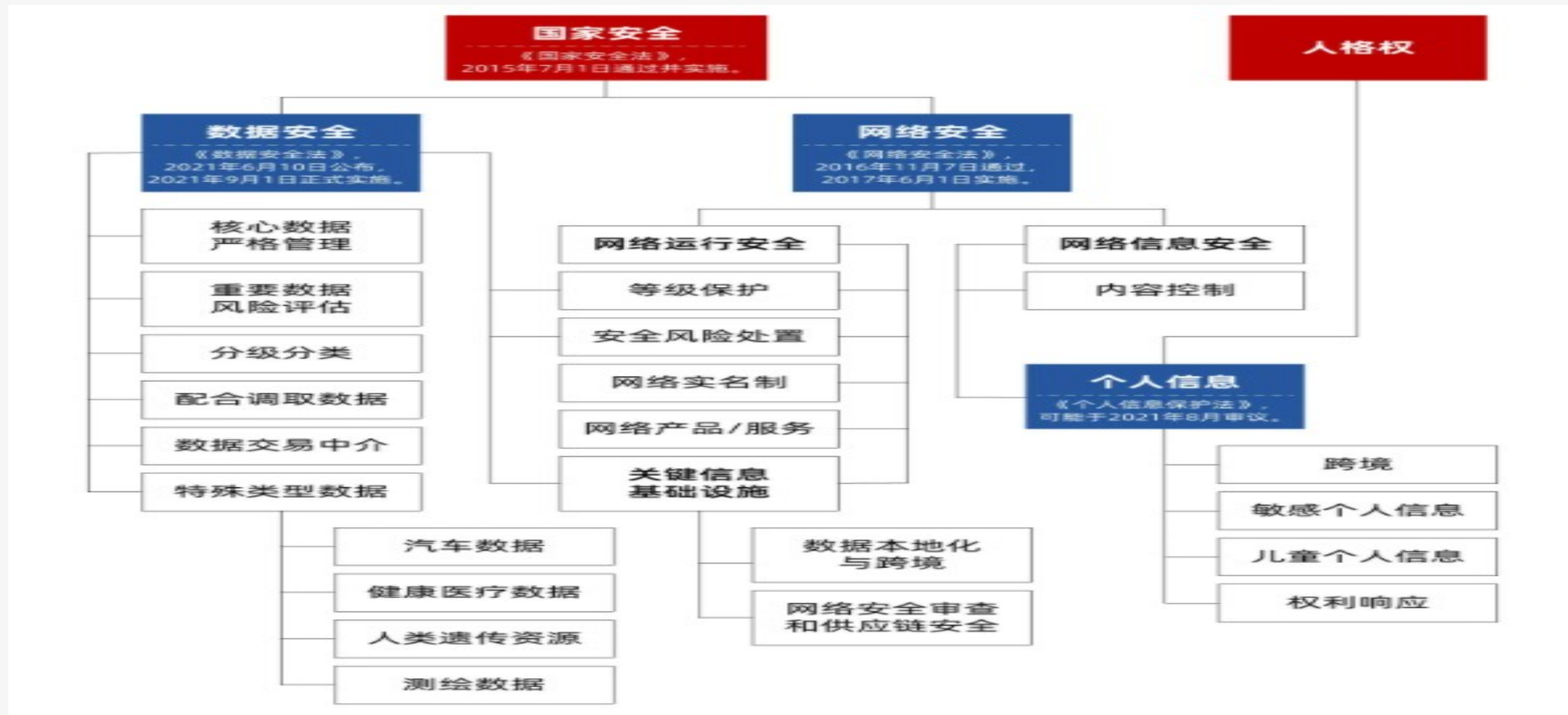
重要条款解读

5

个人信息保护法

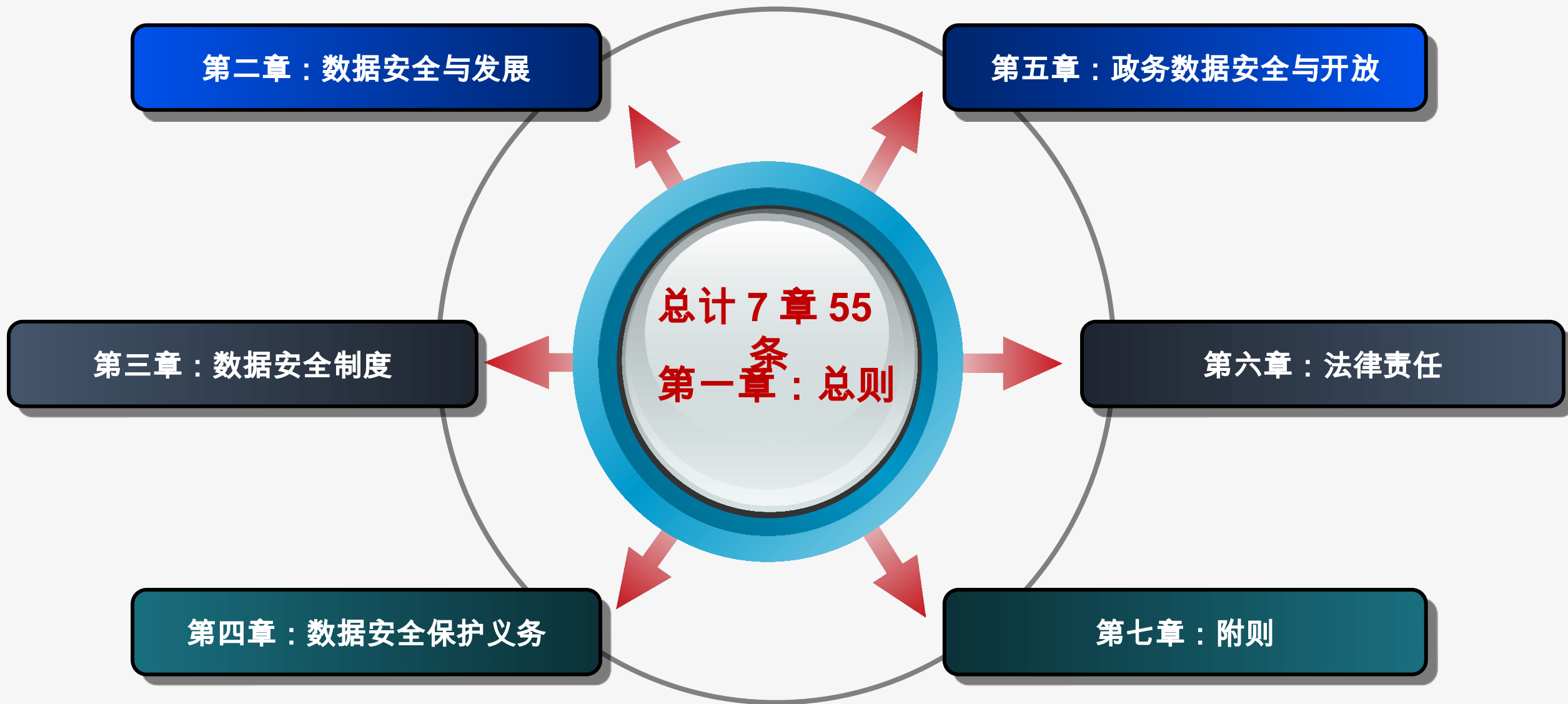


# 数据安全法概况





# 数据安全法概况





## 数据安全与数字经济发展的动态化平衡

- 提出了数据安全制度、数据安全保护义务等确保数据活动符合安全要求
- 推动政务数据开放利用，利用数据提升公共服务智能化水平
- 国家统筹发展和安全理念
- **数据交易制度的确立使得数据依法有序流动成为现实**



## 重视数据安全制度的建设

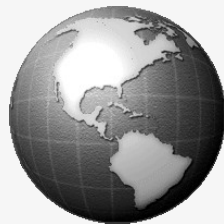
- 明确提出了**数据分类分级保护制度**，确定重要数据具体目录，并提出了核心数据的概念
- 明确了**数据安全风险评估、信息共享、监测预警机制、安全审查制度等**，强化内控制度建设，防控数据安全风险
- 《数据安全法》对**数据的出境管理**进行了补充和完善





## 加强国家对数据安全工作的统筹

- 明确了监管职责，确定给地区、各部门的主题责任，网信部门发挥统筹协调职能
- 通过明确国家层面的统筹协调职能，确保后续国家数据安全战略和重大方针政策的有效落地和执行。



## 增加对数据泄露危及国家安全的处罚力度

- 增加了对违反国家核心数据管理制度的处罚力度
- **对数据安全风险设置了基本“红线”**



1

立法背景

2

立法意义

3

概览及特点

4


**重要条款解读**

5

个人信息保护法



## 扩大数据保护范坚持总体国家安全 发展观

第一条确立该法的立法目确：“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。

规范数据处理活动的目的，是为了保障数据的安全，只有在确保数据安全的基础上，方能促进数据的有序开发和利用。



## 我国数据保护的域外法律效力

● 第二条第二款明确规定：“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。”。

- “境外开展数据处理数据活动”的主体既包括位于中国境外的数据处理者，也包括位于中国境内的数据处理者，但其数据处理行为在境外。
- 只要损害了我国国家安全、公共利益以及公民和组织的合法数据权益，均由我国法律管辖，并追究法律责任。






## 促进以数据为关键要素的数字经济 发展

● 第七条规定：“国家保护个人、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。”

- 数据作为生产要素由市场评价贡献、按贡献决定报酬，这是党的十九届四中全会首次提出的一项重大产权创新制度。
- 在个人和组织与数据有关的权益得到充分保护的基础上，依法推动数据合理有效利用和依法有序自由流动



## 数据可以合法交易


第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十九条 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。

- 并非一味就是强调“监管”或“制约”，在保护国家安全和数据安全的前提下，可以合法交易
- 数据的合法交易可以有效推动和促进数字经济和社会的发展



## 国家数据分类分级保护

第二十一条规定：“国家**建立数据分类分级保护制度**，根据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、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

- “数据分类”，采用了数据的“重要程度”+“危害程度”的立法手段，对数据实行分类分级保护。
- 从国家层面提出了数据分类分级，是确定数据保护和利用之间平衡点的一个重要依据



## 国家数据安全审查制度


第二十四条规定：“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。”

- 数据安全审查制度与网络安全审查是依法确立的国家安全审查制度中两项重要的安全审查制度。
- 数据安全审查制度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，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；





## 国家数据安全应急处置机制


第二十三条明确了“国家建立数据安全应急处置机制”，并要求“发生数据安全事故，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，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。”


- “有关单位”应当按照“谁主管谁负责、谁运行谁负责”的原则确定
- 采取最有效的应急处置措施，防止危害扩大，要消除安全隐患，同时要组织研判，保存证据，并做好信息通报工作
- 及时向社会发布与公众有关的警示信息
- 分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。





## 数据处理者的合规义务

第二十七条到第三十条明确了数据处理者履行数据安全的**四项重要合规义务**。

第二十七条规定：“开展数据处理活动应当依照法律、法规的规定，**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**。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。”

第二十八条提出了**数据处理活动以及研究开发数据新技术的三项合规义务**，一是数据处理者研究开发数据技术，一定要利于促进经济社会发展；二是数据处理者研究开发数据新技术，要以增进人民福祉为目的；三是数据处理者研究开发数据新技术应当符合**社会公德和伦理**。

第二十九条：“开展数据处理活动应当加强**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**立即采取处置措施**，按照规定**及时告知用户并向有关主管部门报告**。”

第三十条规定：“重要数据的处理者应当按照规定对其数据处理活动定期**开展风险评估**，并向有关主管部门报送风险评估报告。”



## 重要数据的出境安全管理制度




第三十一条规定：“关键信息基础设施的运营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，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。”

- 关键信息基础设施的运营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，适用《中华人民共和国网络安全法》。
- 除关键信息基础设施的运营者处理的重要数据外，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
- 数据出境，要求出境前必须经过“安全评估”。



## 提供数据处理服务的行政许可准入制度

第三十四条规定：“法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。”

- 许可 ( license ) 含有准许、允许或授权的意思，数据处理相关服务的行政许可，其基本性质是行政机关对特定的数据处理服务活动事前进行控制的一种管理行为。。



## 加大违法处罚力度



第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以**并处五万元以上五十万元以下罚款**，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**；拒不改正或者造成大量数据泄露等严重后果的，**处五十万元以上二百万元以下罚款，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**五万元以上二十万元以下罚款**。



对违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

- 对数据安全违法行为赋予了多项处罚说明第 44 条 ---52 条。





1

立法背景

2

立法意义

3

概览及特点

4

重要条款解读

5

个人信息保护法



- ④ 随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。**截至 2020 年 12 月，我国互联网用户已达 9.89 亿，互联网网站超过 443 万个、应用程序数量超过 345 万个，个人信息的收集、使用更为广泛。**
- ④ 虽然近年来我国个人信息保护力度不断加大，但在现实生活中，一些企业、机构甚至个人，从商业利益等出发，**随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全**等问题仍十分突出。
  - 2020 年中信银行泄露脱口秀演员池子个人信息案件以及各大平台的“大数据杀熟”
  - “3·15”爆出的各种个人隐私泄露事件，个人隐私已成为经营者手中用于交换利益的廉价或免费的筹码。



# 中华人民共和国个人信息保护法



• 2021.8.20 第十三届全国人民代表大会常务委员会第三十次会议通过，2021年11月1日施行（八章 74条）



第一章 总则（12条）



第二章 个人信息处理规则（25条）



第三章 个人信息**跨境提供**的规则（6条）



第四章 个人在个人信息处理活动中的**权利**（7条）



第五章 个人信息处理者的义务（9条）



第六章 履行个人信息保护职责的部门（6条）



第七章 法律责任（6条）



第八章 附则（3条）





## • 术语界定

- ① **个人信息**：是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
- ② **个人信息的处理**：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。
- ③ **敏感个人信息**：一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及**不满十四周岁**未成年人的个人信息。





## • 范围界定

🏠 **境内**：组织、个人在中华人民共和国境内处理自然人个人信息的活动。

🌐 **境外**：在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的：

- 以向境内自然人提供产品或者服务为目的
- **分析、评估境内自然人的行为**
- 法律、行政法规规定的其它情形



## • 处理规则（第五至第十二条）

- ④ 处理个人信息应当遵循**合法、正当、必要和诚信原则**，不得通过误导、欺诈、胁迫等方式处理个人信息。
- ④ 收集个人信息，应当限于**实现处理目的的最小范围**，不得**过度收集**个人信息。
- ④ 处理个人信息应当遵循**公开、透明原则**，公开个人信息处理规则，明示处理的目的、方式和范围。
- ④ 任何组织、个人不得**非法收集、使用、加工、传输他人个人信息**，不得**非法买卖、提供或者公开他人个人信息**；不得**从事危害国家安全、公共利益**的个人信息处理活动。
- ④ 国家建立健全个人信息保护制度，**预防和惩治侵害个人信息权益的行为**。
- ④ 国家积极推动与其他国家、地区、国际组织之间的**个人信息保护规则、标准等互认**。



## • 处理规则（第十三至第二十条）

- ④ 处理个人信息应当**取得个人的同意**。
- ④ 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。
- ④ 个人信息的处理目的、处理方式和处理的个人信息**种类发生变更的，应当重新取得个人同意**。
- ④ 基于个人同意处理个人信息的，**个人有权撤回其同意**。
- ④ 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。
- ④ 个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法**承担连带责任**。



## • 处理规则（第二十一至第三十七条）

- ④ 根据个人信息处理的不同环节、不同个人信息种类，对个人信息的共同处理、委托处理、向第三方提供、公开、用于自动化决策、处理已公开的个人信息等提出有针对性的要求。（第二十一条至第二十七条）
- ④ 设专节**对处理敏感个人信息作出更严格的限制**，只有在具有特定的目的和充分的必要性的情形下，方可处理敏感个人信息，并且应当取得个人的单独同意或者书面同意。（第二十八条至第三十二条）
- ④ 设专节规定国家机关处理个人信息的规则，在保障国家机关依法履行职责的同时，要求国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行。（第三十三条至第三十七条）



## 个人信息跨境提供规则（第三十八至第四十三条）

- ④ 明确关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的处理者，确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估；对于其他需要跨境提供个人信息的，规定了经专业机构认证等途径。（第三十八条、第四十条）
- ④ 对跨境提供个人信息的 **“告知 - 同意”**作出更严格的要求。（第三十九条，应告知接收方详细信息，并取得单独同意）
- ④ 未经中华人民共和国主管机关批准，**个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。**（第四十一条）
- ④ 对从事损害我国公民个人信息权益等活动的境外组织、个人，以及在个人信息保护方面对我国采取不合理措施的国家 and 地区，规定了可以采取的相应措施。（第四十二条、第四十三条，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。）





## 个人信息处理活动中个人的权利和处理者义务 (第四十四条至第五十九条)

- ④与民法典的有关规定相衔接，明确在个人信息处理活动中个人的各项权利，包括知情权、决定权、查询权、更正权、删除权等，并要求个人信息处理者建立个人行使权利的申请受理和处理机制。(第四十四条至第五十条)
- ④明确个人信息处理者的合规管理和保障个人信息安全等义务(第五十一条至第五十六条)
- ④明确提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的义务(第五十七条)



## 履行个人信息保护职责的部门（第六十条至第六十五条）

### ① 个人信息保护职责部门的定义。（第六十条）

- 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。
- 国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。
- 县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

### ② 明确个人信息保护部门的职责。（第六十一条、第六十二条）

### ③ 个人信息保护部门可以采用的措施，包括询问、查阅、复制资料、现场检查、检查设备及物品、查封或者扣押、约谈主要负责人、进行合规审计等。（第六十三条、第六十四条）

### ④ 对个人信息违法活动的投诉、举报及处置进行规定。（第六十五条）



## 法律责任（第六十六条至第七十一条）

### ❶ 违反规定。（第六十六条）

- 责令改正，给予警告，没收违法所得；
- 拒不改正的，并处一百万元以下罚款；
- 相关责任人：一万元以上十万元以下罚款；

### ❷ 情节严重。（第六十六条）

- 责令改正，没收违法所得；
- 五千万元以下或者上一年度营业额百分之五以下罚款；
- 责令暂停相关业务、停业整顿、吊销相关业务许可或者吊销营业执照；
- 相关责任人：十万元以上一百万元以下罚款；

### ❸ 存在违法行为的依照有关规定记入信用档案，并予以公示。（第六十七条）

### ❹ 国家机关不履行保护义务的处罚进行规定。（第六十八条）

### ❺ 个人信息侵权行为的归责原则为过错推定。（第六十九条）

### ❻ 个人信息主体可以对侵权行为发起集体诉讼。（第七十条）

### ❼ 与治安管理、刑法相衔接。（第七十一条）



上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

**Thank You**

飲水思源 愛國榮校