CAICT 中国信通院

集智 专题报告

数据治理研究报告

--网络数据安全管理法律制度体系研究

（2024 年）

中国信息通信研究院互联网法律研究中心

北京市金杜律师事务所

2025年1月

版权声明

前　言

近年来，随着信息技术和人们生产生活深度融合，数据处理活动更加频繁和复杂。以人工智能为代表的新兴技术发展日新月异，数据体量呈现爆发式增长，数据安全风险也与日俱增。与此同时，数据作为新兴生产要素，在推动数字经济发展、促进社会生产力变革、提升全要素生产率、发展新质生产力方面的重要性不断跃升。党中央、国务院高度重视数据安全工作，党的二十届三中全会通过的《中共中央关于进一步全面深化改革推进中国式现代化的决定》指出，要提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。2024年9月，国务院常务会议审议通过《网络数据安全管理条例》，标志着我国数据安全管理法律体系进一步完善，对明确网络数据安全管理要求、提升数据治理法治化水平具有重要意义，也为充分释放数据要素价值、护航数字经济高质量发展提供了有力法治保障。

本报告以我国数据安全管理制度框架为基础，重点结合《网络数据安全管理条例》（以下简称《条例》）相关规定，深入分析研究国内外网络数据安全管理法律制度体系，主要包含数据安全管理一般规定、个人信息保护、重要数据安全、网络数据跨境安全管理、网络平台服务提供者义务五方面内容。**数据安全管理一般规定方面，**建立健全数据处理全流程的安全管理制度，为网络数据安全管理工作的日常开展明确具体路径，对国家机关、关键信息基础设施等的网络数据安全管理作出要求，针对使用自动化工具收集、使用数据以及生成式人工智能等新技术场景设置数据安全管理专门条款。**个人信息保护方面，**我

国《个人信息保护法》《民法典》《网络安全法》和《数据安全法》共同构建个人信息保护的法治堤坝，结合实践中的新情况、新问题，持续完善“告知—同意”、个人信息权益实现等重点规则。**重要数据保护方面，**重要数据目录、相关组织和人员保障、安全保护义务等规则细化明确，为企业判断是否需履行相关义务要求方面提供稳定预期。**网络数据跨境安全管理方面，**《促进和规范数据跨境流动规定》简化优化相关监管规则，并通过《条例》将相关规定及实践中的成熟做法上升为行政法规。**网络平台服务提供者义务方面，**网络平台的网络数据安全管理责任进一步压实，区分不同类型网络平台明确网络数据安全管理义务。此外，本报告还对域外网络数据安全管理的相关立法进行了比较研究，为进一步完善我国数据安全立法提供了参考借鉴。

结合数据技术产业发展态势，本报告对未来数据治理领域法治建设进行了展望，并提出更新完善网络数据安全制度规范体系、加快构建数据基础法律制度、全面推进网络数据安全管理工作三方面建议。

目 录

图 目 录

一、以数据安全治理筑牢数字经济高质量发展底座

（一）数据安全是总体国家安全观的重要方面

数据安全是事关国家安全与经济社会发展的重大问题，没有数据安全就没有国家安全。近年来，随着信息技术和人们生产生活交汇融合，数据处理活动更加频繁，数据安全风险日益聚焦在网络数据领域，违法处理网络数据活动时有发生，给经济社会发展和国家安全带来严峻挑战。党中央、国务院高度重视数据安全工作，习近平总书记多次作出重要指示批示，强调要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。数据安全牵一发而动全身，完善数据安全管理不仅关乎数据本身作为重要生产要素的开发利用与安全问题，而且与国家主权、国家安全、社会秩序、公共利益休戚相关。

（二）数据安全是数据价值释放的前提和保障

安全是发展的前提，发展是安全的基础。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出，以维护国家数据安全、保护个人信息和商业秘密为前提，构建适应数据特征、符合数字经济发展规律、保障国家数据安全、彰显创新引领的数据基础制度。目前，我国推进数据要素市场建设，为充分发挥我国海量数据规模和丰富应用场景优势，激活数据要素潜能提供制度和政策牵引。数据大规模流通利用显著增加了数据触点和暴露面，数据泄露、滥用、垄断等风险问题日益凸显，对数据全生命周期安全保护提出更高要求。

数据安全事件频发，将导致企业不敢、不愿、不能共享数据。推动数据要素“活起来，动起来，用起来”，前提是保障数据安全。

（三）数据安全是国际社会重点关注治理议题

数据安全是全球性问题，没有哪个国家可独善其身。随着全球数据爆发增长、海量集聚，数据安全问题外延不断扩展，数据安全威胁日益严峻。大数据、云计算、人工智能、区块链等前沿技术加速发展，对数据安全带来全新挑战。世界主要国家和地区认识到数据安全问题的紧迫性和重要性，通过出台国家战略、立法等手段提升本国数据安全保护要求和防护水平。例如美国发布《澄清海外合法使用数据法》《关于加强国家网络安全的行政命令》《防止受关注国家访问美国人的大量敏感个人数据和美国政府相关数据行政令》等相关立法，强化本国数据安全举措和数据出境管理；欧盟《通用数据保护条例》（GDPR）对个人数据保护提出严格要求，《数据治理法》《数据法》《网络团结法》等强化数据安全管理和促进数据再用、流通。

（四）我国持续完善数据安全法律体系

近年来，我国加快推进网络数据安全管理相关立法，在发展和监管实践中不断探索完善网络数据安全管理基础制度。出台数据安全管理、促进数据要素市场建设相关政策文件，为保障国家数据安全、保护个人信息权益和企业商业秘密、激活数据要素潜能提供了重要的制度保障和规则指引。

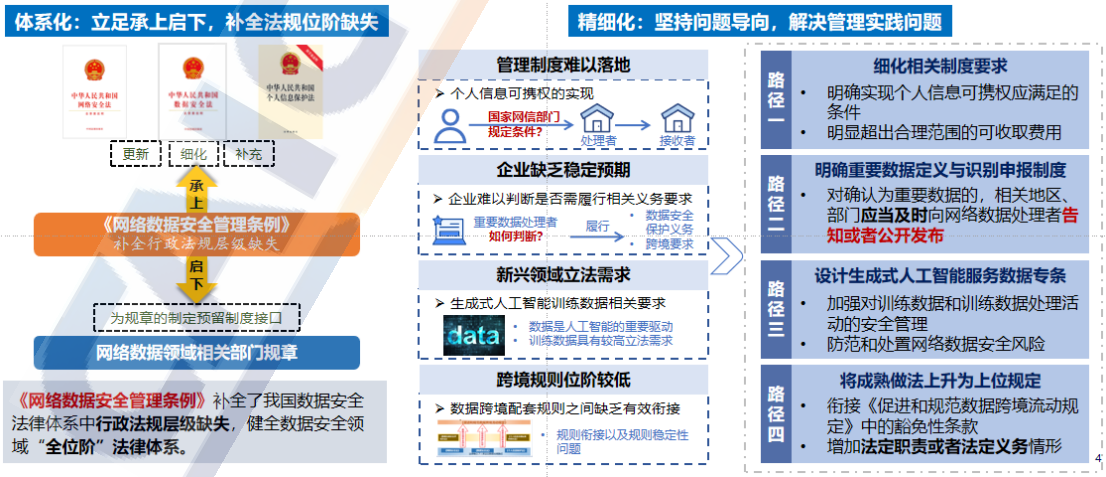
加快推进数据安全顶层立法。我国以“三法一条例”（《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护

条例》）为核心，基本构建起网络数据安全管理制度体系。2016 年出台的《网络安全法》明确了网络运营者需维护网络数据完整性、保密性和可用性的义务，采取数据分类、重要数据备份和加密等措施防止网络数据泄露或者被窃取、篡改，并对关键信息基础设施运营者的数据安全防护义务以及数据境内存储和出境管理进行明确规定。2021 年出台的《数据安全法》明确建立数据分类分级保护制度，对重要数据、国家核心数据等强化保护要求，确立了数据安全风险评估、应急处置以及数据安全审查等数据安全基础制度，明确开展数据处理活动的相关主体需履行的数据安全义务。《个人信息保护法》从个人信息保护视角出发，强调个人信息处理者处理个人信息需遵守的法律义务，保障个人信息权益。《关键信息基础设施安全保护条例》明确关键信息基础设施运营者应当强化数据安全保护，建立数据泄露报告机制等数据安全义务。

针对数据安全具体制度出台立法细化制度要求。为进一步落实上位法关于数据安全管理的重点制度，相关部门出台多部部门规章、规范性文件，明确数据安全管理具体要求。**为落实数据出境流动管理要求**，制定发布《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》等，细化数据出境安全评估、个人信息出境标准合同等数据出境制度的具体规则。**为细化网络安全审查制度**，制定《网络安全审查办法》明确网络安全审查中的数据安全保护具体要求。**为落实数据分类分级管理要求**，我国制定《工业数据分类分级指南（试行）》《证券期货业数据分类分级指引》等相关立

法和文件，细化具体领域数据分类分级要求。此外，重点行业领域结合本行业领域数据安全管理情况制定行业领域数据安全管理部门规章和规范性文件，例如《汽车数据安全管理若干规定（试行）》《会计师事务所数据安全管理暂行办法》《自然资源领域数据安全管理办法》《工业和信息化领域数据安全管理办法（试行）》《中国银保监会监管数据安全管理办法（试行）》等。

《网络数据安全管理条例》标志着我国数据安全法规体系的进一步完善。2024 年 8 月 30 日，国务院第 40 次常务会议通过了《网络数据安全管理条例》。《条例》针对网络数据安全管理的突出问题，在科学总结过往治理经验的同时，兼顾新技术新应用带来的新安全问题，明晰个人信息“告知—同意”规则、重要数据风险评估、个人信息跨境流动条件、网络平台服务提供者第三方安全管理等要求，对强化数据安全和个人信息保护、保障数据要素有序开发利用、促进数字经济健康有序发展具有重要意义。

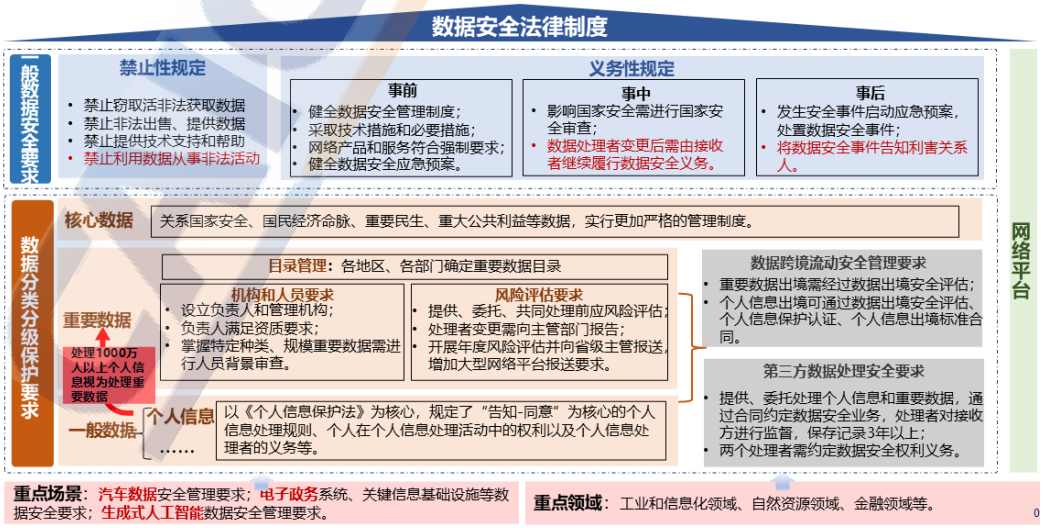


来源：中国信息通信研究院

图 1 《网络数据安全管理条例》基本定位

二、以体系化制度构建全面推进数据安全治理工作

我国《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等相关立法构建起数据安全管理的“四梁八柱”。从制度内容来看，我国数据安全管理制度重点分为四个方面。**一是**网络数据安全管理一般规定。明确禁止任何个人、组织利用网络数据从事非法活动及提供相应的帮助行为，针对网络数据处理的事前事中事后全流程提出一系列义务要求。**二是**数据分类分级安全管理制度。构建核心数据、重要数据、个人信息的保护制度。**三是**明确重要场景、重点领域网络数据管理要求。针对国家机关电子政务系统、关键信息基础设施运营者的场景作出专门规定。在工业和信息化、自然资源、金融等领域出台专门数据安全管理相关规定。**四是**明确网络平台服务提供者数据安全管理义务，规定其在网络数据安全管理、监督第三方服务等面的义务，强化全链条数据安全保护。



来源：中国信息通信研究院

图 2 网络数据安全管理制度全景图

（一）覆盖全类型网络数据明确安全管理要求

《条例》第二章明确了网络数据安全管理的一般义务，通过禁止性规定划定网络数据处理底线要求，细化网络数据处理事前事中事后的安全保护措施，并与时俱进地提出人工智能等新场景中的网络数据安全保护规则。

1.以一般禁止性规定划定数据安全红线

《条例》第八条明确针对所有主体的、危害网络数据安全的禁止性规定。一是不得利用网络数据从事非法活动，二是禁止窃取或以其他非法方式获取网络数据，三是禁止非法出售或非法向他人提供网络数据，四是禁止针对上述非法活动提供技术支持或其他帮助行为。

首次针对网络数据使用环节作出禁止性要求，同时对上位法中的禁止性规定进行细化补充。《条例》吸收了《刑法》中侵犯公民个人信息罪、帮助信息网络犯罪活动罪的相关表述，同时对《网络安全法》第二十七条、《数据安全法》第三十二条中所禁止的危害网络安全行为和从事非法网络数据处理活动进行了补充。《网络安全法》第二十七条禁止为危害网络安全的行为提供技术支持，但尚未明确此类帮助行为的类型，《条例》在此基础上将其明确为“提供互联网接入、服务器托管、网络存储、通讯传输等技术支持”行为，进一步提升了法律法规的可操作性和针对非法网络数据处理行为的打击精度。

与其他国家或地区相比，我国的禁止性规定多为一般性、原则性规定，如《条例》第八条是针对“任何个人、组织”提出的要求，是网络数据处理活动开展的基本安全底线。**美国**在数据领域的禁止性规定主要体现在对特定数据和特定交易活动的限制，如《保护美国人民数据免受外国对手侵害法》禁止“数据经纪人”(data broker)向包括中国、俄罗斯等在内的“受关注国家”提供敏感数据。**欧盟**维护网络数据安全的立法规定更多体现在命令性规定或授权性规定，而非禁止性规定，如《通用数据保护条例》（以下简称 GDPR）第 89 条规定，基于公共利益存档目的、科学或历史研究目的、统计目的而进行的个人数据处理行为应当采取适当的保护措施。

2.以全流程制度设计明确数据安全要求

在个人信息及重要数据的特殊保护要求之外，《条例》明确了网络数据处理事前事中事后全流程的安全管理要求，其中包含数据安全管理措施、产品和服务安全、应急处置及国家安全审查等内容。

（1）明确数据处理者需采取的数据安全管理措施

《条例》第九条要求网络数据处理者采取管理制度和技术措施相结合的方式，对所处理网络数据的安全负责。一方面，网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，建立健全网络数据安全管理制度；**另一方面，**网络数据处理者采取加密、备份、访问控制、安全认证等技术措施和其他必要措施。两类措施的共同目的是保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，进一步加强网络数据安全防护。

数据安全管理措施以网络安全等级保护为基础。《网络安全法》第二十一条明确，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护的要求，履行安全保护义务。《数据安全法》第二十七条也明确，利用互联网等信息网络开展数据处理活动，应在网络安全等级保护制度的基础上，履行数据安全保护义务。以此观之，网络安全等级保护是针对网络安全和数据安全领域的统一要求，不能脱离网络安全保护而谈数据安全，网络安全是基础。《条例》对《数据安全法》第二十七条作了进一步说明，解释了网络安全等级保护制度之上的“数据安全保护义务”的具体含义，这就包括建立健全网络数据安全管理制度、采取技术防护等具体措施。**此外，**《条例》还明确了国家标准在落实网络数据安全管理要求方面的重要性，并将网络安全等级保护所涉及的相关标准进一步纳入制度范围。

对数据处理规定强制性安全保护措施是域外立法中的通行做法。**欧盟**数据保护立法对相关义务主体采取事前保护措施进行了详细的规定，如《数据治理法》《数据法》《网络与信息系统安全指令》以及 GDPR 中都有对传输或处理数据采取保护措施的要求。**美国**联邦法律、州级立法、监管实践及标准认证等各层面均包含事前安全措施的相关规定，如《联邦信息安全管理法》（FISMA）要求所有直接与政府系统交换数据的政府机构、政府承包商和组织必须通过制定、记录和实施信息安全计划来保护其所有信息技术系统及存储数据，《加州消费者隐私法》（以下简称 CCPA）要求企业采取与其持有数据信息性质相称的合理安全措施。

（2）明确网络产品和服务安全要求

《条例》第十条明确网络产品和服务的风险处置要求。一是网络数据处理者提供的网络产品、服务应当符合相关国家标准的强制性要求；**二是**当发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；**三是**涉及危害国家安全、公共利益的，应当满足在 24 小时内向有关主管部门报告的要求。

安全报告义务是网络数据安全管理制度的重要组成部分。《条例》在《网络安全法》第二十二条的基础上，补充了“涉及危害国家安全、公共利益”的情形，明确网络数据处理者应当在更短的时间内履行向有关主管部门报告的义务。《网络安全事件报告管理办法》（征求意见稿）也作了类似规定，对于属于较大、重大或特别重大网络安全事件的，网络运营者须在更短的时间内向有关主管部门报告。2021 年 9 月，工业和信息化部等三部门颁布的《网络产品安全漏洞管理规定》，明确了一般情形下的时间要求，要求网络产品提供者在发现或者获知所提供网络产品存在安全漏洞后，应当在 2 日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。

网络产品及服务安全是欧美网络安全立法重点。欧盟《网络弹性法》（CRA）为欧盟市场内具有数字组件的产品制定了全面的网络安全标准，将带有数字组件的产品划分为“默认”、“重要”和“关键”产品三类，重要产品进一步划分为 I 类和 II 类产品，不同类别的产品适用严格程度不同的安全保护措施，如 I 类重要产品必须遵守欧洲网

络安全认证计划或相关标准，或者接受第三方评估。**美国**《确保信息通信技术服务供应链安全暂行规则》要求对美国国家或公民安全构成不可接受之风险的信息通信技术和服务（ICTS）开展安全审查，如认定具备相应风险，则可以采取措施降低交易风险或禁止该交易。

（3）明确数据安全事件应急处置要求

《条例》第十一条明确数据安全事件的应急处置要求。一是建立健全网络数据安全事件应急预案，当网络数据安全事件发生时，应立即启动预案，采取措施防止危害扩大，消除安全隐患并向主管部门报告。**二是**细化网络数据安全事件的通知措施，对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人；法律、行政法规规定可以不通知的，从其规定。**三是**建立违法犯罪线索举报机制，网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

吸收《个人信息保护法》相关规定明确发生网络数据安全事件时的告知义务要求。《个人信息保护法》第五十七条规定，个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人。换言之，只有在危害发生时，个人信息处理者才需要向个人履行告知义务。《条例》第十一条吸收了《个人信息保护法》相关要求，明确仅在对“个人、组织合法权益造成危害”

时，才需要通知受影响的个人和组织。《条例》还提出可采用电话、短信、即时通信工具、电子邮件或者公告等通知方式，其中公告告知具有广泛覆盖、持续性长、成本相对较低等优势。

应急处置要求也是域外数据立法重点。欧盟在 GDPR 的基础上，就数据安全事件及应急处置发布了相关指南及指令。GDPR 规定，发生数据安全事件导致数据泄露时应立即通知监管机构、数据控制者和受高风险影响的个人。《关于 GDPR 下的个人数据泄露通知的第 9/2022 号指南》规定，应急预案中应包括向主管部门报告及向个人数据主体通知的机制，且颗粒度要达到需要向哪一个具体主管部门通知的程度。《关于在整个欧盟全境实现高度统一网络安全措施的指令》（NIS 2 指令）对重大网络安全事件作出更为精细的规定，采用分层的方式规范通知流程，包括 24 小时内“预警”，72 小时内发出“事件通知”，1 个月内提交“最终报告”等要求。**美国**联邦层面制定了一系列网络安全事件披露的立法,如美国证券交易委员会要求上市公司为投资者的利益披露重大网络安全事件; 美国网络安全和基础设施安全局（CISA）发布相关拟议规则，要求相关实体在 72 小时内向 CISA 报告重大的网络安全事件，并在 24 小时内报告勒索软件情况。

（4）明确对相关数据处理活动国家安全审查要求

《条例》第十三条提出国家安全审查相关要求。针对网络数据处理活动提出要求，对于影响或者可能影响国家安全的，网络数据处理者应当按照国家有关规定进行国家安全审查。

国家安全审查制度体系进一步完善健全。我国《国家安全法》第

五十九条、《网络安全法》第三十五条、《数据安全法》第二十四条从法律层面对国家安全审查作出规定，其中《数据安全法》第二十四条提出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。2021 年 12 月，国家互联网信息办公室发布修订后的《网络安全审查办法》，明确关键信息基础设施运营者采购网络产品和服务，数据处理者开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险。《条例》的出台，进一步完善了国家安全审查制度在行政法规层面的要求。

美欧重视安全审查措施在数据安全领域中的作用。美国近年来频繁通过两类安全审查措施限制外国信息技术和服务，**一是**以《2019 安全和可信通信网络法》为代表实施的国家安全审查，防止威胁国家安全的通信设备或服务进入美国网络，移除正在使用的此类设备或服务；**二是**以《2018 年外国投资风险审查现代化法》（FIRRMA）为核心实施的美国外商投资委员会（CFIUS）审查，将敏感个人数据保护作为衡量国家安全的重要因素。**欧盟**《外商直接投资审查条例》从关键基础设施、关键技术、关键供应、敏感信息等方面，审查非欧盟投资对欧盟成员国国家安全和公共秩序的风险；其中，关键基础设施包括能源、交通、水资源、健康、通讯、媒体、数据处理和存储、航空、国防等，关键技术包括人工智能、芯片等，关键供应包括能源和原材料等。

3.以第三方数据安全义务区分主体责任

《条例》第十二条、第十四条明确了在发生主体变更情形时网络数据处理者的数据安全保护义务，第十二条涉及提供、委托处理个人信息和重要数据的情形，第十四条涉及因合并、分立、解散、破产等原因转移网络数据的情形。

（1）明确提供和委托处理数据情形下的数据安全要求

《条例》第十二条对个人信息及重要数据的流转作出规定。一方面，网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据时，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。网络数据处理者还需在 3 年内保存相关处理记录。另一方面，网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

在个人信息保护方面，《条例》第十二条主要延续了《个人信息保护法》第二十一条的规定，要求个人信息处理者应当与接受委托处理个人信息的受托人签署相关合同并且监督受托人。**在重要数据方面，**《条例》第十二条从行政法规层面确立了重要数据在一般情形下流转的基本框架，对重要数据安全有序自由流动具有至关重要的意义。

域外立法也对数据流转、委托过程中的相关主体数据安全责任进行制度设计。欧盟 GDPR 有关委托处理和提供处理的规定主要在序言部分。在委托处理方面，GDPR 序言（81）条明确，数据控制者应仅委托在专业知识、可靠性和资源方面有可靠保障的数据处理者，以

实施 GDPR 要求的技术及保障措施。数据处理者可通过行为守则或经批准认证机制的形式遵守数据控制者的相关义务，数据处理者应受合同或其他欧盟法及成员国法律的约束。在完成相关委托后，数据处理者应根据数据控制者的要求归还或删除数据。在提供处理方面，GDPR 序言第（61）条明确，当个人数据可以合法地披露给其他接收者时，应该在第一次披露时告知数据主体。当数据控制者意图基于数据收集初始目的以外的其他目的处理个人数据时，数据控制者应当在进一步处理之前向数据主体提供有关其他目的必要信息。**美国** CCPA 明确排除适用于提供数据服务的企业，即 CCPA 本身不对作为数据控制者的企业所委托的第三方数据处理者作出规定，企业与对其提供服务的数据处理者主要依靠合同或者服务协议约定相关数据保护义务。

（2）明确数据处理者发生主体变更时的数据安全要求

《条例》第十四条针对网络数据处理者发生合并、分立、解散、破产等原因需要转移网络数据的情形作出规定。该条主要吸收《个人信息保护法》第二十二条的规定，当网络数据处理者发生上述情形时，网络数据的接收方应当继续履行网络数据安全保护义务，避免数据因企业破产、分立、解散时而被非法获取或滥用。但与《条例》第十二条不同，这一条适用于所有网络数据，不限于个人信息和重要数据。

美欧立法对破产企业相关数据处理的限制较少。美国侧重于“商业利益优先”，《美国破产法》明确规定了破产企业的数据处理规则，其中第 363（b）（1）条规定，如果公司的隐私政策明确允许出售其客户的数据，则该公司可以出售其客户数据。但是，如果隐私政策未授

权出售客户数据，则必须任命消费者隐私监察员（CPO）审查出售实施和适用的非破产法，CPO 根据审查结果向法院提出是否批准拟议交易的建议。**欧盟**强调“个人信息保护”，GDPR 中的数据控制者和数据处理者范围可涵盖破产管理人，当债务人财产由管理人处置时，可以将管理人认定为数据控制者，由管理人承担相应责任。值得注意的是，在满足个人信息保护基本要求的前提下，GDPR 并未明令禁止出售数据。

4.以强化规定提升国家机关数据安全水平

《条例》第十五条至十七条明确涉及国家机关相关数据处理活动的特殊要求。一是委托情形需经过事前批准程序。《条例》第十五条规定，国家机关委托他人建设、运行、维护电子政务系统，存储、加工政务数据，应当按照国家有关规定经过严格的批准程序，明确受托方的网络数据处理权限、保护责任等，监督受托方履行网络数据安全保护义务。**二是网络数据处理者承担额外安全保护义务。**《条例》第十六条对向国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的网络数据处理者提出了额外的规定，要求其在按照法律法规以及合同约定履行网络数据安全保护义务的基础上，在未经委托方同意时，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。**三是自有系统提供服务参照电子政务系统管理要求。**《条例》第十七条明确，为国家机关提供服务的信息系统，应参照电子政务系统的管理要求加强网络数据安全管理，保障网络数据安全。《条例》

第十五至十七条有效地回应了实践中长期存在的乱象，厘清了公共领域中第三方服务提供者的权责边界。

美欧对公共部门信息系统建设中的数据安全进行了详细规定。欧盟《网络弹性法》（CRA）规定了关键信息基础设施中数字产品制造商、进货商和经销商等不同主体的义务。制造商对设计、开发和生产的数字产品需符合 CRA 规定的网络安全要求。经质量评估和网络安全评估后，制造商必须为产品张贴 CE 标志，并提供清晰、易懂、可理解和易读的产品随附信息和说明，以确保用户安全地安装、操作和使用。进口商需确认数字产品符合质量和网络安全要求，并在产品包装或随附文件中标明商家名称、注册商标、电子邮件等，并对产品的网络安全漏洞或事件承担报告义务。经销商则需要确保销售的数字产品带有 CE 标志，产品中包含制造商的随附信息和说明以及进口商的联系信息等。**美国**高度重视政务信息化项目建设中的数据安全保护。以国土安全领域为例，美国《国土安全采购规章》明确了相关项目承包商在访问受控非密信息时的安全流程和程序要求，并要求承包商具备相应的事件处置能力。

5.以专门条款确立新技术数据安全要求

《条例》第十八、十九条对涉及自动化工具、生成式人工智能等新兴技术的数据处理活动作出特殊规定。一是网络数据处理者使用自动化工具访问、收集网络数据，应评估对网络服务带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。**二是**提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理

活动的安全管理，采取有效措施防范和处置网络数据安全风险。

自动化工具方面，网络爬虫（Robotic Process Automation，RPA）的正当性及其边界问题一直广为讨论，此前我国主要从反不正当竞争的角度对自动化采集行为予以规制，如《网络反不正当竞争暂行规定》第十九条规定，经营者不得利用技术手段，非法获取、使用其他经营者合法持有的数据，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序。《条例》一定程度上吸收了实践经验，从网络运行安全的角度提出相应禁止性规定。**人工智能方面，**我国针对人工智能算法及算法治理领域已经发布了《生成式人工智能服务管理暂行办法》及其配套的《生成式人工智能服务安全基本要求》，并对训练数据活动提出一系列合规要求。《条例》对训练数据合规的规范进一步从行政法规的效力层级上完善了我国对人工智能训练数据合规监管的规范体系。

域外立法对人工智能训练数据的安全及质量要求作出规定。欧盟《人工智能法》第 10 条对高风险人工智能使用数据和数据治理的过程提出了规范性的要求，特别针对数据的训练、验证和数据库的测试等环节。**一是数据集的质量要求。**高风险 AI 系统和模型的训练、验证和测试所使用的数据集应与其预期用途相关、具有足够的代表性，并尽可能完整、免受误差的影响。数据应具备适当的统计特性，例如包括与系统预期适用人群有关的（个人或群体）相关的特性。这些数据集的特性要求可以在单个数据集层面或数据集组合层面得到满足。**二是数据集的选择应与高风险人工智能系统开发设计的目的相适应。**

根据系统的预期用途，数据集的选择和应用应考虑系统所适用的特定的地理、社会环境、行为或者功能要求背景，将相应的特征或要素涵盖其中。**三是个人信息数据使用的必要性和保护要求**。如人工智能系统提供者需要采取特别措施处理特定类型的个人信息，并采取适当的保障措施以保证自然人的基本权利和自由。**美国**《关于安全、可靠、值得信赖地开发和使用人工智能的行政命令》专门设置了“保护美国民众的隐私”章节，详细阐述了白宫应对人工智能数据安全问题的三条措施。**一是**针对人工智能技术在实际应用中对个人隐私的威胁，要支持并加快加密技术等隐私保护技术的研发和资金投入，保护用于人工智能的训练数据以及普通用户的个人信息的安全。**二是**推动开展机构评估工作，评估各机构如何收集和使用商业可用信息，包括从数据代理那里获得的信息，并加强对联邦机构的指导。**三是**制定实施指导方针，以评估人工智能技术中使用到的隐私保护技术的有效性。

（二）针对个人信息进一步细化重点规则

《条例》结合个人信息保护实践中的新情况、新问题，重点细化、完善了个人信息保护中的“告知—同意”规则、个人信息权益实现等规定。

1.细化处理个人信息“告知—同意”具体要求

《条例》细化网络数据处理者处理个人信息前的告知要求。**一是明确告知方式**。要求网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式进行告知。**二是明确告知的展示方式**。要求个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容

明确具体、清晰易懂。**三是细化告知内容要求**。要求个人信息处理规则必须包括:（1）网络数据处理者的名称或者姓名和联系方式;（2）处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响;（3）个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法;（4）个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。**四是明确以清单方式列明向第三方提供个人信息**。明确网络数据处理者向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。**五是强化收集未成年人个人信息的告知要求**。明确处理不满十四周岁未成年人个人信息应当制定专门的个人信息处理规则。

《条例》细化列举取得个人同意后处理个人信息的要求。**一是细化收集个人信息的“必要性”原则要求**。规定收集个人信息需为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意。**二是加重敏感个人信息、未成年人个人信息取得同意的要求**。规定处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意;处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。**三是细化取得同意后的个人信息处理要求**。规定不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息;个人信息的处理目的、方式、种类发生变更

的，应重新取得个人同意。**四是规范重复征求同意的情形。**规定不得在个人明确表示不同意处理其个人信息后频繁征求同意。

从上位法来看，针对处理个人信息的告知、同意规则，《个人信息保护法》重点规定五方面要求。**一是明确个人信息处理规则需公开的要求。**《个人信息保护法》第七条要求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。**二是明确告知的形式和内容。**第十七条规定，在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项:（1）个人信息处理者的名称或者姓名和联系方式;（2）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限;（3）个人行使本法规定权利的方式和程序;（4）法律、行政法规规定应当告知的其他事项。**三是明确个人同意的基本要求。**《个人信息保护法》第十四、十五条规定，同意应当由个人在充分知情的前提下自愿、明确作出；处理目的、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；个人有权撤回其同意；不得以撤回同意为由拒绝提供产品或者服务。**四是明确敏感个人信息的告知、同意要求。**《个人信息保护法》第二十九、三十一条规定，处理敏感个人信息应取得单独同意，告知处理必要性以及对个人权益的影响；处理不满十四周岁未成年人个人信息应取得未成年人的父母或者其他监护人的同意。**五是明确转移个人信息的告知、同意要求。**《个人信息保护法》第二十二、二十三条规定，个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当个人告知接收方信息；向其他网

络数据处理者提供个人信息的，应当向个人告知接收方信息并取得单独同意。

《条例》在《个人信息保护法》的基础上重点细化、补充告知、同意规则要求。**对告知规则的细化补充体现在四个方面：一是**细化对个人信息处理规则的展示、显示要求；**二是**增加了告知个人信息保存期限及到期后处理方式的规定；**三是**细化了需告知的个人信息权益类型及实现方法、途径；**四是**增加向其他网络数据处理者提供个人信息时应以清单方式列明告知事项规定。**对同意规则的细化、补充体现在三个方面：一是**补充“必要性”原则要求，即使获得个人同意也需满足“必要性”“最小化”要求。即为提供产品或服务必须处理个人信息，不得超范围收集，不得以误导、欺诈、胁迫等方式取得个人同意。**二是**补全了不得超范围处理个人信息的要求，即不得超出个人同意的处理目的、方式、种类、保存期限处理个人信息。**三是**增加禁止频繁征求同意的规定。

域外立法通过不同机制明确个人信息处理“告知-同意”规则。美国 CCPA 围绕“opt-out”机制明确“告知-同意”相关规则。告知规则方面，针对明确收集个人信息和出售个人信息两类场景规定了不同的告知内容要求。CCPA 区分了收集个人信息时和出售个人信息时不同的告知要求。在收集个人信息时，需重点告知信息的类别、信息是否会被出售或共享、存储期限等；在出售个人信息时，需告知出售信息的类别，并在收到消费者的核实请求后 45 日内提供相关信息。**同意规则方面，**CCPA 采用“选择退出”（opt-out）规则，默认个人同意

处理其个人信息但赋予个人拒绝的权利。CCPA 规定消费者可以要求企业不出售其个人信息，《加州隐私权法》（以下简称“CPRA”）对 CCPA 进行修改并扩展了这一权利，允许消费者选择退出不仅是出售，还包括共享个人信息。对于儿童个人信息的处理，CCPA 采用了“选择加入”（opt-in）规则，处理不满 13 岁儿童的个人信息，需要获得父母或监护人的同意；处理 13 至 16 岁儿童个人信息，企业在出售其个人信息前需要获得本人明确授权。CPRA 对儿童个人信息的处理提出了更严格的要求，要求企业在处理 16 岁以下儿童的个人信息时，必须获得父母的同意。

欧盟 GDPR 将“告知-同意”作为个人数据保护的基本规则。一是明确告知内容要求。GDPR 第 13 条规定，数据控制者必须告知数据主体有关同意的细节，以便数据主体以能够理解的语言和形式获得处理活动的所有必要细节，以便他们能够理解处理将如何对他们产生影响，包括处理个人数据的目的、收集个人数据的种类、向第三国转移的风险等。**二是明确告知的形式要求。**GDPR 第 12 条规定，数据控制者应以一种简洁明了、透明以及易获得的形式、使用清晰易懂的语言，将有关数据处理的信息提供给数据主体；尤其在涉及儿童时，更应遵守相关要求。另外，相关信息应当以书面或者其他方式提供，包括使用电子方式进行告知。**三是明确对同意的要求。**GDPR 第 4 条（11）款对数据主体的“同意”进行界定，即数据主体依照其意愿自由作出的、特定的、知情的、不含混的、表示同意对其相关个人数据进行处理的意愿。具体包括以下要求：（1）由数据主体自由作出，数

据主体在作出同意时，其选择是真实的，不存在受到胁迫或者欺诈的情况。如果数据主体受到数据控制者的影响（如数据控制者是数据主体的雇主），则考虑到此类关系的性质，同意并不当然被认为是自由作出的。（2）针对特定的数据处理目的和处理方式。同意应当清晰准确地指明数据处理的范围和结果，无明确目的的概括式同意是无效的。（3）基于对情况的充分了解。数据控制者必须向数据主体提供关于数据处理的最低限度的信息，提供的信息应足以保证数据主体作出充分知情的选择。（4）明确且充分地表达了数据主体的意愿。同意必须以声明或清晰肯定的行为作出，预先勾选的选择框并不构成同意。

2.创新性落实个人信息权益实现路径

《条例》明确网络数据处理者实现个人信息权益的义务。**一是要求网络数据处理者提供实现个人信息权益的方法和途径。**明确个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件。**二是补充实现个人信息“可携权”的条件。**明确网络数据处理者为其他网络数据处理者访问、获取相关个人信息提供途径应满足的条件，包括：（1）能够验证请求人的真实身份；（2）请求转移的是本人同意提供的或者基于合同收集的个人信息；（3）转移个人信息具备技术可行性；（4）转移个人信息不损害他人合法权益。**三是细化网络数据处理者删除个人信息或匿名化处理的要求。**明确网络处理者必须删除个人信息或进行匿名化处理的情形，包括因使用自动化采集技术等无法避免采集到

非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号。同时也规定例外情形，即在保存期限未届满或者在技术上难删除或匿名化的，网络数据处理者只能采取存储和安全保护措施，不得进行其他处理活动。

针对个人在个人信息处理活动中的权利，《个人信息保护法》重点规定了三方面内容。**一是明确个人信息权益类型**。《个人信息保护法》第四十四至四十七条规定，个人对其个人信息的处理享有知情权、决定权，有权向个人信息处理者查阅、复制其个人信息，有权请求个人信息处理者更正、补充、删除其个人信息。**二是规定了个人信息处理者实现个人信息权益的要求**。如个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供；个人请求将个人信息转移至其指定的个人信息处理者，个人信息处理者应当提供转移的途径；个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。**三是明确个人信息处理者应主动删除个人信息的情形**，包括（1）处理目的已实现、无法实现或者为实现处理目的不再必要；（2）个人信息处理者停止提供产品或者服务，或者保存期限已届满；（3）个人撤回同意；（4）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（5）法律、行政法规规定的其他情形。

《条例》在《个人信息保护法》基础上重点强调网络数据处理者为实现个人信息权益提供方法、路径。**一是**针对各项个人信息权益明确网络数据处理者的实现义务，网络数据处理者及时处理个人请求并提供便捷的行使权利的方法和途径。**二是**增加因自动化采集技术采集

非必要个人信息或未获得同意应当删除个人信息的要求。**三是**增加个人行使转移个人信息权利需满足的条件。

从域外立法来看，欧盟 GDPR 与美国 CCPA 都明确了知情权、访问权、删除权等一系列个人信息权。**欧盟 GDPR 重点规定了五类个人信息权利。一是个人享有对个人信息处理的知情权。**根据 GDPR 第 14 条的规定，数据控制者应向数据主体提供充足信息。具体而言，数据控制者在收集个人数据时，应当告知数据主体数据控制者的身份信息与联系方式、处理个人数据的目的与法律依据、被处理的个人数据的类型、个人数据储存的期限以及个人数据转移情况等。**二是个人享有对个人数据的访问权。**GDPR 第 15 条规定，数据主体有权访问已被数据控制者收集的个人数据，以便了解和验证有关数据处理行为的合法性，数据控制者应当在合理的时间内满足数据主体的这种访问请求。**三是个人享有撤回对个人信息处理同意的权利。**此项权利主要规定在 GDPR 第 7 条 3 款，明确数据主体有权随时撤回其同意，撤回同意不影响撤回之前基于同意的数据处理；在数据主体表达同意之前，数据主体应当被告知这点，且撤回同意应当和表达同意一样简单。**四是个人享有要求删除个人信息的权利。**GDPR 第 17 条规定了需删除个人信息的情形，包括个人数据对于实现收集或处理目的不再必需、数据主体撤回同意且无其他合法性基础、数据主体的个人数据被非法处理、履行法定义务等情形。**五是个人享有数据可携权。**GDPR 第 20 条规定，在数据控制者以自动化方式、基于合同条款或数据主体同意的情况下处理个人数据时，数据主体有权要求数据控制者提供其个人数据

集，这种数据文件应该是结构化、通用的、机器可读以及不同操作系统中都可以执行的格式，并且数据主体有权将这些个人数据传输给另一个数据控制者。

美国 CCPA 明确五类个人信息权益。一是个人对其个人信息的收集、售出的情况享有知情权。CCPA 规定，消费者有权要求收集其个人信息的公司披露收集的个人信息的类型和具体内容。**二是**个人享有访问个人信息的权利。CCPA 规定，企业从消费者处收到要求访问个人信息的请求后，应立即采取措施向消费者免费披露和提供规定要求的个人信息，个人信息的提供可通过信件或电子方式。**三是个人拥有撤回同意权。**对于向第三方出售或共享其个人信息的企业，消费者有权随时要求其不得出售或共享其个人信息。**四是个人拥有删除权。**在收到消费者的删除请求后，企业应及时删除数据，并确保已共享的第三方同时删除该数据。**五是个人拥有可携带权。**CCPA 中的可携权实际上是个人访问权及复制权的延伸，当数据控制者接收到个人查阅其个人数据的请求时，数据控制者应当采用便利的格式提供该法所规定的个人数据，使个人能够不受阻碍地将这些个人数据传输到另一数据控制者。

3.进一步补全数据处理者的个人信息保护要求

《条例》补全《个人信息保护法》对网络数据处理者的具体要求。**一是明确专门机构、指定代表进行信息报送的部门。**《条例》在《个人信息保护法》第五十三条的基础上，明确境外的个人信息处理者需将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市

级网信部门，由网信部门通报同级有关主管部门。**二是补充对合规审计方式的要求。**《条例》在《个人信息保护法》第五十四条的基础上，明确网络数据处理者通过自行或者委托专业机构的方式进行合规审计。**三是增加个人信息视为重要数据保护的情形。**《条例》在《个人信息保护法》第四十、五十二条的基础上，明确“国家网信部门规定数量”为处理 1000 万人以上个人信息，并对处理超过一定数量个人信息的网络数据处理者增加了网络数据安全管理要求。

欧盟 GDPR 规定了境内代表人信息公开的形式要求。欧盟 GDPR 第 27 条设立了境内代表人制度，当境外数据控制者或数据处理者适用 GDPR 第 3 条 2 款时，则应以书面形式在欧盟境内指定一名代理人，代表履行 GDPR 规定的义务。根据欧洲数据保护委员会（EDPB）发布的《关于 GDPR 第三条地域适用范围的解释指南》，境内代表人信息以两种形式公开：（1）向欧盟数据主体提供的，可以在收集数据时告知或在隐私通知中告知；（2）向数据保护机构提供的，仅达到使监管机构“容易获得”欧盟境内代表人的信息即可，如采用在公司网站上公布境内代表人的形式。

个人信息保护审计在多国个人信息保护立法均有体现。欧盟 GDPR 较早提出了数据保护审计的概念，并将数据保护审计作为核查、判断数据处理者以及数据控制者是否遵循 GDPR 处理个人信息的手段。根据 GDPR 第 28 条 3 款（h）项，数据保护审计是数据处理者向数据控制者证明自身履行 GDPR 项下个人信息保护合规义务的主要手段；GDPR 第 58 条 1 款（b）项则赋予了监管机构以数据保护审计

形式开展调查的权力。**美国** CPRA 在 CCPA 的基础上引入了网络年度审计规则，要求在个人信息处理活动中“对消费者隐私或安全构成重大风险”的企业应当进行年度网络安全审计，企业应当明确审计范围并通过审计程序确保审计的彻底性和独立性。

4.强化敏感个人信息保护要求

《条例》重申《个人信息保护法》对于敏感个人信息保护的相关要求。一是对敏感个人信息进行列举，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹以及不满十四周岁未成年个人信息等；**二是**明确处理敏感个人信息的特殊要求，处理不满十四周岁未成年个人信息，应当取得其父母或者监护人同意；处理其他敏感个人信息的，应当取得个人的单独同意。**三是**明确处理个人敏感信息，应向个人告知处理的必要性和对权益的影响。**四是**依规定需要取得书面同意的，应取得书面同意。

《个人信息保护法》第二十八条采用“定性+列举”的方式对敏感个人信息进行定义。敏感个人信息是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。《条例》吸收了《个人信息保护法》中对于敏感个人信息的列举内容。此外，第二十八条还进一步明确了个人敏感信息的处理要求，即只有在具有特定目的和充分必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

大多数国家和地区倾向采取“一般与特殊”的个人信息二分法，但对于特殊类型个人信息所用称谓并不一致，中美均采用“敏感个人信息”定义，欧盟则称“特殊类型的个人数据”。

欧盟 GDPR 第 9 条明确特殊类型个人数据定义，即显示民族或种族身份、政治观点、宗教或哲学信仰、工会身份的数据，或遗传数据、用于唯一识别自然人身份的生物特征数据、健康相关数据或有关自然人性生活或性取向的数据。**在特殊类型个人数据识别规则方面，欧盟法院在相关判决中提出应尽可能扩大解释。**针对“特殊类型个人数据”这一概念，应基于 GDPR 保护基本权利的目的进行广义解释。在这一框架下，即便无法准确判断，但只要有一定的概率能够追踪到数据主体，相关数据就应被视为健康数据等特殊类型个人数据。**GDPR 原则上禁止企业或组织处理敏感个人信息，除非满足特定条件。**处理敏感个人数据时有额外的规则，不仅必须存在第 6 条中的合法性基础，还必须遵守第 9 条的规定，主要包括获得数据主体明确同意、为了保护数据主体或其他自然人的重大利益、非盈利性数据处理等情形。

美国 CCPA 和 CPRA 列举了敏感个人信息类别，但对于敏感个人信息无概括性定义。CPRA 列举的敏感个人信息包括人种与民族信息、工会成员信息、宗教信仰、遗传数据、生物特征、健康信息、有关性生活或性取向的信息、财务账户信息等。根据 CPRA 的定义，公开获取的敏感个人信息不视为敏感个人信息，甚至也不视为个人信息。CCPA 和 CPRA 关于敏感个人信息没有特殊的处理要求，相关的处理规则仅在通知义务上存在差异。**此外，**《防止受关注国家访问美国人

的大量敏感个人数据和美国政府相关数据行政令》（第 14117 号行政令）也对特定敏感数据施加特殊保护，限制其向“受关注国家”流动。

（三）围绕重要数据系统强化数据安全管理

《条例》在《数据安全法》的框架下，补充了重要数据安全管理制度的基本内容。《条例》第六十二条明确地界定了重要数据的概念，即特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据，弥补了我国在法规层面对于重要数据界定的空白，并与国家标准《数据安全技术 数据分类分级规则》中的定义基本保持一致。

《条例》设立专章明确对于重要数据安全管理方面的要求，主要包含三个方面的内容：一是明确制定重要数据目录的要求，规定网络数据处理者识别、申报重要数据义务。**二是**规定网络数据安全负责人和网络数据安全管理机构责任。**三是**明确重要数据处理者比一般网络数据处理者更加严格的安全保护义务。

1.明确重要数据目录制定要求

从三个层面明确重要数据目录相关制定要求。一是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；**二是**各地区、各部门确定本地区、本部门以及相关行业、领域的重要数据目录，确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布；**三是**网络数据处理者按照国家有关规定识别、申报重要数据，履行网络数据安全保护责任。**此外，**第

二十九条第三款还提出国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全管理水平。

在《数据安全法》关于重要数据目录规定的基础上，进一步提出网络数据处理者主动申报、识别重要数据的相关要求。《数据安全法》第二十一条从国家和各地区、各部门两个维度出发，由国家数据安全工作协调机制统筹协调各部门重要数据识别工作，各地区、各部门负责重要数据的具体识别。《条例》进一步作出规定，一是确认为重要数据的，相关地区、部门应当及时向网络数据处理者履行告知义务，二是网络数据处理者应当按照国家有关规定识别、申报重要数据，履行网络数据安全保护责任。**《条例》在《数据安全法》第二十一条的基础上提出了更多要求，同时又为《促进和规范数据跨境流动规定》（以下简称《规定》）第二条提供了上位法依据。**《规定》第二条明确，数据处理者应当按照相关规定识别、申报重要数据，且未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

我国其他部门规定、国家标准中包含了对于重要数据的相关要求。《汽车数据安全管理若干规定（试行）》第三条明确了汽车领域的六类数据，包括军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据，车辆流量、物流等反映经济运行情况的数据，汽车充电网的运行数据等。GB/T 43697-2024《数据安全技术 数据分类分级规则》作为全国网络安全标准化技术委员会发布的首份数据安全技术标准，涵盖了数据分类分级、

重要数据和国家核心数据识别等重要内容，其中附录 G“重要数据识别指南（规范性）”对各地区、各部门开展重要数据识别工作具有重要的指导意义。此外，根据《规定》第六条的授权性规定，目前北京、上海、天津、福建等地自贸区已经发布了数据清单，对于重要数据目录的制定也具有重要的参考价值。

2.明确重要数据处理者组织和人员保障要求

要求重要数据处理者设立网络数据安全负责人和网络数据安全管理机构。针对网络数据安全负责人，一是要求其应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，并有权直接向有关主管部门报告网络数据安全情况；**二是**掌握特定种类、规模的重要数据处理者，应对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训，在审查时可以申请公安机关、国家安全机关的协助。**针对网络数据安全管理机构，《条例》明确其应当履行一定的网络数据安全保护责任，**如制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案，定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训，受理并处理网络数据安全投诉、举报等。

设立组织和人员保障是重要数据保护的关键步骤。《条例》在《网络安全法》《关键信息基础设施安全保护条例》基础上，将组织和人员保障的相关要求从关键信息基础设施运营者延伸至重要数据处理者。《网络安全法》第三十条要求关键信息基础设施的运营者设置专门安全管理机构和安全管理负责人，《关键信息基础设施安全保护条

例》第十四、十五条进一步细化《网络安全法》的规定，如对专门安全管理机构负责人和关键岗位人员进行安全背景审查，并明确了专门安全管理机构的特定安全保护职责。《条例》吸收了上述规定的部分要求，补充重要数据保护在组织和人员保障方面的特定要求，以此实现重要数据保护的组织化、常态化。

3.细化重要数据处理者的数据安全管理要求

重要数据处理者需履行比一般网络数据处理者更加严格的安全保护义务。一是重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，《条例》第三十一条明确了此类评估的主要内容，如网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要，网络数据可能被篡改、破坏、泄露的风险等。**二是**在重要数据处理者发生合并、分立、解散、破产情形时，需履行向省级以上有关主管部门的报告义务，主管部门不明确的，应当向省级以上数据安全工作协调机制报告。**三是**重要数据处理者应每年度对其网络数据处理活动开展风险评估，并向有关主管部门报送。《条例》第三十三条明确了年度风险评估报告的基本内容，其中处理重要数据的大型网络平台服务提供者还需额外说明关键业务和供应链网络数据安全等情况。

《条例》对上位法中重要数据处理者的安全保护义务作了重要补充。在涉及第三方时，重要数据处理除需满足《条例》第十二条和第十四条的一般规定外，还需要进一步满足事前风险评估和事后通报的义务。**在风险评估方面，**《数据安全法》第三十条明确，重要数据处

理者需履行定期开展风险评估，对评估内容进行了简单列举。《条例》进一步细化了风险评估报告的内容和程序要求，并为大型网络平台设立了额外的报告义务。

4.域外立法较少进行重要数据安全管理制度设计

欧盟并没有专门以“重要数据”命名的概念，但在相关法律中提出了“高价值数据集”“关键基础设施数据”等概念。欧盟《开放数据和公共部门信息复用的指令》（简称《开放数据指令》）提出了“高价值数据集”的概念，并规定了其开放和利用规则。《开放数据指令》明确，高价值数据是指再利用会对社会、环境和经济带来重大利益的数据。高价值数据能够创造增值服务、应用和高质量的工作岗位且潜在的受益者人数众多。《开放数据指令》在附件中列举了 6 类高价值数据主题类别，同时授权委员会通过制定实施条例的方式增加新类别。《网络和信息系统安全指令》（简称 NIS 指令）提出“关键基础设施数据”的概念，要求运营这些关键基础设施的组织实施严格的数据保护措施，防范网络攻击和数据泄露。关键基础设施运营者必须遵守更高标准的网络安全要求，确保数据的机密性、完整性和可用性。同时，这些数据的处理和保护需要符合欧盟的整体网络安全战略和相关法规。**美国没有统一的“重要数据”概念，但在金融、健康和教育领域等多个关键行业均有详细的立法和监管框架。**这些法规在保护敏感数据的隐私性和安全性方面提出了严格要求，类似于我国“重要数据”的保护思路。**在金融领域，**美国《金融服务现代化法》（GLBA）要求金融机构保护客户的个人金融信息，并制定隐私政策向客户公开其数

据的处理方式。金融机构必须实施强有力的技术措施来保护数据，并且在发生数据泄露时及时向相关监管机构报告。GLBA 还对金融数据的共享和传输做出了限制，防止未经授权的第三方访问。**在健康领域，**健康数据是美国受保护最严格的领域之一。《健康保险流通和责任法》（HIPPA）对健康数据的保护要求提出了详细的规定，HIPAA 要求医疗服务提供商、保险公司和相关第三方严格遵守数据保护标准，确保个人健康信息（PHI）的机密性、完整性和可用性。HIPAA 特别注重数据的传输安全，要求相关主体采取措施防止数据泄露、篡改和未经授权的访问。**在教育领域，**美国通过《家庭教育权利和隐私法》（FERPA）保护学生的教育记录。FERPA 赋予学生及其家长对学生教育记录的访问权和隐私保护权，要求教育机构未经许可不得向第三方披露学生的个人信息。FERPA 类似于我国对教育数据保护的要求，特别是在涉及学生隐私、成绩、学术记录等方面。

（四）优化完善网络数据跨境安全管理制度

1.我国持续推进数据跨境流动安全管理制度设计

《条例》第五章明确了网络数据跨境安全管理的相关要求。在我国有关数据跨境流动的法律体系上，《条例》和此前发布的《促进和规范数据跨境流动规定》《数据出境安全评估办法》《个人信息出境标准合同办法》等部门规章形成了有机衔接，尤其吸收了《促进和规范数据跨境流动规定》的相关规定，使其上升为行政法规下的数据出境机制。

《条例》对我国当前的数据出境路径进行了系统梳理。一是确立

“三主三辅”六大数据出境路径。三类主要数据出境路径是通过数据出境安全评估、个人信息出境标准合同以及个人信息保护认证制度，三类辅助出境路径是国际条约与协定，外国司法或执法数据调取，以及法律、行政法规规定的其他情形。除执法调取情形外，其他数据出境路径在《条例》第三十五、三十六条中均有体现。**二是衔接《促进和规范数据跨境流动规定》中的豁免性条款。**《规定》明确了六类豁免适用数据出境监管程序的情形，进一步优化了我国数据跨境流动制度体系。《条例》第三十五条在数据出境安全评估、个人信息出境标准合同以及个人信息保护认证制度之外，相应提出了“个人发起”、“员工数据出境”、“紧急情况”及“法定义务”其他四种出境情形。前三类在《规定》中均已有所体现，“为履行法定职责或者法定义务”则属于《条例》的新增情形。《条例》结合《规定》的豁免情形，对《个人信息保护法》第三十八条进行了补充。

《条例》第三十九条进一步强调数据跨境流动中的数据安全要求。一是重申重要数据的安全评估要求。《条例》明确重要数据出境需经过安全评估，通过安全评估后，网络数据处理者不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。同时，未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。**二是明确国家对于网络数据跨境的网络防护要求。**任何个人、组织不得提供专门用于破坏、避开国家所采取防护措施的程序、工具，明知他人从事破坏、避开技术措施等活动的，也不得为其提供技术支持或者帮助。

2.域外主要形成三类数据跨境流动管理模式

国际社会对数据跨境流动监管并未形成统一框架，各国综合考虑国家安全、隐私保护、产业能力等多元因素，构建符合本国利益的数据跨境流动监管制度，当前主要形成以美国、欧盟、新兴经济体为代表的三种类型管理模式。

美国针对特定“受关注国家”采取数据跨境流动限制措施。一方面，持续巩固盟友关系。美国通过 G7、G20、“四方安全对话”等不同机制，推动美欧、美日以及美英等双边规则体系相继成型和落地。另一方面，针对“受关注国家”限制数据跨境。2023 年 10 月，美国在 WTO 电子商务谈判撤回了数据跨境自由流动的主张；其后，美国通过法案、行政令、部门规则等形式丰富数据跨境流动政策工具，限制敏感数据向中国、俄罗斯、朝鲜等特定“受关注国家”流动。

欧盟区分个人数据和非个人数据进行数据跨境流动监管。一方面，欧盟将个人数据保护权利作为基本权利进行保障，在立法中明确规定欧盟公民的个人数据只能跨境流动到个人数据保护水平达到欧盟标准的国家或地区，引发了 GDPR 的“布鲁塞尔效应”。另一方面，欧盟一般不禁止非个人数据跨境流动，如《非个人数据自由流动条例》限制成员国制定非个人数据本地化立法，鼓励和促进非个人数据在欧盟境内自由流动。但近年来，欧盟在《数据法》《数据治理法》中原则性提出，非个人数据的跨境流动也应满足一定的安全保障水平。

新兴经济体注重实现产业发展和国家安全，在一定程度上实行数据本地化管理。如，印度规定物联网数据、支付数据等只能在本地进行存储，不允许跨境流动，同时规定中央政府可通知限制相应的个人

数据出境。印度尼西亚正在修订电子系统运营与交易规则，拟要求公共电子系统运营者拥有的战略性数据（政府、能源、交通、金融、医疗、IT 和通信、国防等）在境内进行存储。俄罗斯要求所有个人数据必须本地留存后，才能依据法律要求传输到境外。越南《个人数据保护法》规定个人数据在符合相关条件前提下可以出境，且需要在越南境内保存三年备份。

（五）明确网络平台服务提供者数据安全义务

1.我国逐步明确对网络平台的管理要求

《条例》进一步明晰网络平台服务提供者义务，对于压实网络数据安全管理责任具有重要意义。对于一般网络平台服务提供者，《条例》要求其在涉及第三方平台或提供应用程序分发时，履行对网络数据的安全保护义务，并在采用自动化决策的情形中，进一步保护网络用户的权益。**对于大型网络平台服务提供者，**《条例》明确其应当每年发布个人信息保护社会责任报告、履行国家数据跨境安全管理要求，并明确一系列禁止性规定。

对网络平台服务提供者提出若干安全监督管理义务要求。一是针对第三方产品和服务的监督义务。网络平台服务提供者应当通过平台规则或合同方式明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，并督促其加强网络数据安全管理。第三方产品和服务提供者对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者依法承担相应责任。预装应用程序的智能终端等设备生产者也适用此项规定。**二是应用程序分发服务的相关网络数据安全保护**

义务。提供应用程序分发服务的网络平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相关核验。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。**三是设置自动化决策关闭选项。**网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

细化“大型网络平台服务提供者”网络数据安全管理义务要求。我国目前仅在个人信息保护和未成年人网络保护两个领域的立法中涉及对大型网络平台的加重义务。《条例》对《个人信息保护法》第五十八条进行了细化完善。**一是明确“大型网络平台服务提供者”的定义。**根据《条例》第六十二条第（八）项规定，大型网络平台是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。对《个人信息保护法》第五十八条所规定的“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”作了具体解释。**二是明确发布个人信息保护社会责任报告相关要求。**大型网络平台服务提供者应每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等，细化《个人信息保护法》第五十八条中的时间要求。**三是遵**

守数据跨境安全管理要求。大型网络平台服务提供者跨境提供网络数据，应遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险。**四是针对大型网络平台服务提供者的禁止性规定。**如大型网络平台服务提供者不得通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据，不得无正当理由限制用户访问、使用其在平台上产生的网络数据等。

2.域外立法强化对大型网络平台管理

欧盟对网络平台的义务监管主要体现于《数字服务法》（DSA）和《数字市场法》（DMA）当中。DSA 侧重于内容、透明度等方面的平台义务，其可以分为所有平台均适用的一般义务和特定类型平台适用的特别义务，如尽职调查义务、与监管机构的合作义务等就适用于所有平台，年度风险评估、独立审计、任命合规官等额外的合规义务则适用于超大型平台和超大型在线搜索引擎（VLOP）。DMA **侧重公平竞争角度下的网络平台行为规制，**为大型平台制定明确的规则——“注意事项”和“注意事项”清单，防止它们对企业和消费者施加不公平的条件，比如不允许用户卸载任何预装软件或应用程序。DMA 将符合一定标准的核心平台服务提供者视为数字市场的守门人，并在反垄断法等竞争规则以外对守门人规定了加重义务。DMA 第 5 条中明确了守门人的 9 类具体义务，包括数据使用限制、禁止自我优待、广告透明度、互操作性等方面，以防止守门人对公平市场竞争的影响。违反这些义务的守门人可能会面临高达全球年营业额 10%的罚款，而对于屡次违规的情况，罚款可能高达 20%。

三、持续构建更加完备的数据安全法治体系

党的二十届三中全会通过的《中共中央关于进一步全面深化改革推进中国式现代化的决定》提出，要建设和运营国家数据基础设施，促进数据共享。加快建立数据产权归属认定、市场交易、权益分配、利益保护制度，提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。下一步，我们要准确把握我国网络数据安全管理面临的新形势新任务，以《网络数据安全管理条例》作为网络数据安全管理工作的新起点，全方位推进数据治理法治化进程，为促进数字经济高质量发展、推动数据依法有序自由流动提供制度规则保障。

（一）优化完善网络数据安全制度规范

在已有网络数据安全法律制度体系下，推动《条例》相关规定落地落实。结合行业特点，推动各地区、各部门重要数据目录出台，加快行业领域数据安全相关规章或规范性文件的制定实施，以及相关制度的试点工作，提升数据领域治理效能。

推动建立高效便利安全的数据跨境流动机制。一是加快推进数据清单制度建设，发挥北京、上海、天津等地自贸区数据清单示范作用，分步骤、分阶段推进其他地区数据清单出台，并在全国分类分级体系完善后，整合形成统一的国家级数据清单。**二是**探索便捷多样的数据出境路径，综合应用标准合同、备忘录等工具拓宽跨境数据范围及渠道，引入白名单、公司约束性规则（BCR）等更多数据出境便利化机制，进一步提高数据跨境流动规则的规范化、标准化和透明化。

制定应对新型风险的网络数据安全管理规则。一是系统构建人工

智能大模型的相关数据规则，明确模型开发者、部署者、使用者等相关主体义务，完善模型训练及应用的责任链条。**二是**重点解决未成年人智能终端应用安全风险，针对其安全性设置更加细化的准入标准，进一步明确相关软件开发商、设备制造商的特殊保护义务及责任，将未成年人智能终端的生产、销售、使用纳入常态化监管范围。**三是**加强终端直联卫星服务的数据安全保障，推动《终端设备直连卫星服务管理规定（征求意见稿）》适时出台，进一步明确其涉及的数据处理相关要求，以及应采取的数据安全保障措施。

（二）探索推进数据基础法律制度建设

新时代以来，我国充分发挥数据的基础资源作用和创新引擎作用，带动各类生产要素创新性配置，促进各类先进生产要素向发展新质生产力集聚，为发展新质生产力开辟新空间。同时，我国数据基础法律制度仍存在较多空白区，未来仍需在产权归属、市场交易、收益分配等环节发力，实现“供数”动力进一步释放，“用数”活力进一步迸发。

持续完善数据产权归属认定相关规则。抓紧解决数据产权归属认定存在的突出问题，强化数据产权功能，聚焦数据资源的合法持有，构建提高数据产权保护的精准度，构建各类经济主体在数据要素市场公平获取数据资源权利，激发市场主体合法开发利用数据资源的活力和创造力。

建立健全数据交易市场规则体系。依法构建全国统一的场内场外数据交易制度，推动数据交易场所管理办法出台，加快构建国家级数

据交易场所，制定完善数据交易、安全等标准体系，降低数据交易成本，进一步推动全国统一数据大市场建设。

构建公平高效的权益分配与利益保护制度。结合数据要素的特征，重点建立初次分配制度，根据相关主体在数据产品和服务价值形成过程中的实际作用得到合理回报，构建有利于数据要素价值收益向数据使用价值和价值创造者合理倾斜的分配制度。

（三）全面落地网络数据安全管理工作

充分发挥《条例》在网络数据安全管理中的枢纽作用，加强法规制度的宣传，强化法规制度的约束力，全面推动《条例》相关制度落地实施，有序推进网络数据安全管理相关工作开展。

构建完善“点面结合”的数据安全执法机制。在国家层面，加强数据安全监管执法统筹协调，围绕个人信息保护、重要数据保护、数据出境安全评估等重点问题建立专项督查、日常检查、企业自查的常态化、多层次监督检查工作体系；强化部门沟通协作，避免重复执法和执法空白。在行业管理层面，围绕具体行业领域数据全生命流程构建覆盖数据安全风险评估、风险报告、数据共享、检测预警、应急处置等各环节的动态监督机制;同时立足前期 App 专项治理工作基础，以典型数据安全事件为切入点开展协同监管执法专项活动。

支持鼓励数据安全保护技术开发应用。落实《数据安全法》《网络数据安全保护条例》关于建立数据安全监测预警机制要求，明确数据安全培训、测评、认证等公共服务的合法地位，提升数据安全风险监测、预警和处置的技术能力。在行业部门出台的相关规定中明确鼓

励开发、应用数据安全技术，开展数据安全技术应用试点示范和优秀项目评选，推动数据安全技术产品应用落地。

中国信息通信研究院 互联网法律研究中心

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62302581

传真：010-62304980

网址：www.caict.ac.cn