中国联通
China unicom

企业数据跨境合规与技术应用白皮书（2023）

中国联通研究院

中国联通网络安全研究院

下一代互联网宽带业务应用国家工程研究中心

2023 年 11 月

版权声明

目录

表目录

图目录

前 言

在数字经济背景下，数据已经成为国家战略资源和关键生产要素，也是企业的核心竞争资产。伴随着经济全球化，数据跨境活动日益频繁，数据出境场景越来越多，防范数据出境安全风险，保障数据依法有序自由流动成为我国关注的重要方面。目前，我国数据出境安全管理体系已经初步构建形成。《网络安全法》《数据安全法》《个人信息保护法》确立了数据出境的基本原则和主要路径，《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》等进一步明确了不同数据出境路径的具体要求。

企业作为数据跨境活动最活跃的主体之一，无可避免的成为履行数据跨境合规义务的重要主体，但在具体实践中，如何采取相应的措施、采取哪些措施仍面临许多问题，比如：如何判断是否需要申报数据出境安全评估，或订立并备案个人信息出境标准合同，或通过个人信息保护认证？三条路径具体应如何实施？能够采取哪些方法和手段防范数据出境安全风险？……

本白皮书力图从分析政策、剖析概念、归纳方法、总结举措等方面，尽可能全面、系统地整理当前我国数据跨境的有关法律法规和实施举措，希望为提高有关企业或个人对数据跨境制度的认识和理解，增强经营管理和业务开展过程中对数据出境合规风险的防范意识，强化数据出境合规管理贡献力量。

本白皮书由中国联通研究院主笔，中国联通集团网络与信息安全部、联通数字科技有限公司数据智能事业部、中国联通国际有限公司、中兴通讯股份有限公司、北京市环球律师事务所联合编写。

编写组成员（排名不分先后）：

总策划：苗守野、李浩宇、叶晓煜

编委会：徐雷、杨锦洲、吴钢、马瑞涛、林海、张航、陶冶、曹咪、孙艺、吴连勇、李佳杭、康旗、刘亚琪、孟洁、王程、刘洋、李冰、陈靖、杨晓蔚、韩莹莹、薛竞、黄一申、李佳敏、孙进芳、杨开敏、赵灿、刘宇健、张钦华

一、全球数据跨境流动背景

当前，以 5G、云计算、大数据、人工智能等为代表的新一代信息通信技术快速发展并逐渐跨界融合，加速推进全球数字化转型和国际数字贸易发展。数据作为新型生产要素，数据跨境流动在当今数字经济中扮演着重要角色，因其机遇与风险并存，已经成为各个国家和地区重点关注的议题之一。

1.1 数据跨境驱动全球数字经济加速增长

数据跨境安全有序流动是数据要素高效运转流动的关键环节，自 2008 年以来，跨境数据流动对全球经济增长的贡献已经超过传统的跨国贸易和投资，支撑了包括商品、服务、资本、人才等其他几乎所有类型资源的全球化活动，已经成为驱动数字经济增长的主要力量。数据跨境流动是经济全球化的必然结果，也是当下和未来经济发展的常态。数据跨境流动对于促进数字创新、提高经济增长效率和增进社会福祉具有重要意义。

一是促进国际贸易高质量发展。跨境数据流动已成为推动经济全球化与国际贸易发展的重要力量。作为国际贸易发展的最新趋势，数字贸易在提升贸易效率、拓展贸易对象、降低贸易成本、丰富贸易业态等方面发挥着重要作用。

二是加速企业发展国际化进程。企业作为市场主体，其业务模式和经营模式引发高频化、规模化且常态化的跨境数据流动，在全球产业分工日趋细化的背景下，企业的海外业务布局通常涉及多个国家，数据的集中协同处理是企业经营的客观需求。企业跨境数据流动可促进各类资源要素畅通流动以及各行业市场主体加速融合，帮助企业持续推动自身运营方式改善、供应链优化与商业模式创新，助力企业实现资源的高效配置。跨境数据流通是推动人才流、物流、资金流和信息流跨域自由流转的基础，在推动企业全球化等方面发挥着积极作用。

三是驱动数字经济加速增长。全球数据流动对经济增长有明显的拉动效应，据麦肯锡估算，数据流动量每增加 10%，将带动 GDP 增长 0.2%。预计到 2025 年，全球数据流动对经济增长的贡献将达到 11 万亿美元。据经济合作与发展组织（OECD）测算，数据流动对各行业利润增长的平均促进率在 10%，在数字平台、金融业等行业中可达到 32%。依托数字技术和信息网络推动数据跨境流动，可带动各类资源要素高效流动、各类市场主体加速融合，促进数字经济做强做优做大。

1.2 各国加快构建自身数据跨境流动规则

数据跨境流动给数字经济发展带来了强大的推动作用，但是数据跨境后也隐藏着不受控的安全风险。当前，国际上广泛认为，数据跨境流动不仅包括物理意义上的跨越国界，还包含第三国主体对数据的

跨境访问和使用。随着经济全球化的发展，国际交流合作愈加频繁，数据跨境传输、存储、访问、使用的频次大幅上升，所带来的安全风险渗透至数据全生命周期，且随着数据跨境流动的范围不断扩大，产生的风险从个人隐私保护、商业利益保护升级跃迁至国家数据主权甚至国家安全。随着各国对数据跨境流动意义和影响的认识日益深入，数据跨境流动逐步成为国家和地区间博弈的重要问题。基于国家安全、经济发展、隐私保护、技术能力等多方面的考量，各国确立了不同的数据跨境流动策略，并基于此加快构建自身的数据跨境流动规则体系。

分国家层面来看，当前，数据跨境流动规则还处在探索阶段，各国对于数据跨境流动规则尚未形成共识，整体呈现多元性与差异化的特点。比如，**美国**采取的策略是理念上主张全球数据自由流动，实践中构建数据“单向”流动格局。**欧盟**“两手都要抓，两手都要硬”，双边场合推动数据互认标准，多边场合提倡数据自由流动，在强化个人隐私数据保护的同时，提升数据竞争优势。**日本**对数据跨境流动的限制性条件较少，但强调对涉及国家安全的敏感或关键数据进行监管。**俄罗斯**要求俄公民个人数据收集必须使用位于俄境内的数据库。**印度**将个人数据分为一般个人数据、敏感个人数据和关键个人数据，一般个人数据和敏感个人数据在境内存储副本的条件下可跨境流动，关键个人数据仅能存储在印度境内的服务器或数据中心，绝对禁止离境。**澳大利亚、加拿大、韩国、巴西**等国支持数据自由流动，但主张将保

护个人隐私和国家安全写入例外条款，包括实现公共政策目标、保护个人隐私安全、保护国家安全等。截至目前，全球已有 70 多个国家或地区对数据跨境流动进行了不同程度的限制。

从当前国际数字贸易相关协定来看，数据跨境流动规则正在成为高水平贸易协定的重要标志，无论是发达国家成员主导的《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《数字经济伙伴关系协定》（DEPA），还是发展中国家成员签署的《区域全面经济伙伴关系协定》（RCEP），保障数据合理数据跨境流动都是其中的核心条款。

各国限制数据跨境流动的规章制度存在显著差异，而且具有明显的冲突性，给数据跨境流动带来了很大难度。但是国际主流的跨境管理思想较为统一：基于数据的重要程度，分类分级的开展数据跨境管理工作，并在既有的国际合作框架下探索数据跨境合作，在经济发展、数据安全、国际环境三者约束条件下，形成数据跨境流动规则。

1.3 我国数据跨境流动监管面临较大挑战

我国明确将数据作为新型生产要素，据《数字中国发展报告（2022 年）》数据显示，2022 年我国数据产量达 8.1ZB，同比增长 22.7%，占全球数据总产量的 10.5%，位居全球第二；我国数字经济规模达 50.2 万亿元，占国内生产总值比重提升至 41.5%。我国已经发展成为全球第二大数字经济体，数据跨境流动在数字经济中的作用愈发重要。但是如何在维护好国家数据安全、保护好个人信息权

益的前提下促进数据有序流动成为当前面临的难题，我国数据跨境流动监管也面临较大挑战。

一是数据跨境流动隐蔽性强，难以有效监管。数据跨境流动深植于国际贸易、交往互动中，处理过程涉及多方参与协商，数据流动隐蔽性高，增加了数据跨境流动监管的复杂度。隐蔽的方式包括通过恶意软件采集、网络爬虫抓取或其他非法方式获取他人未授权的数据并流转使用。全球经济一体化背景下，数据是否以隐蔽且未授权的方式流动出境，成为数据出境安全治理亟需重点关注的问题，准确识别数据的不合法出境是数据跨境安全治理的基础。

二是数据跨境量级指数递增，分类监管难度较大。随着互联网的快速普及，海量数据不断汇聚积累，呈现出“数据海量化、种类多样化、处理快速化”等特点，这些数据遍布通信、金融、能源、交通等各个行业领域，数据格式混杂多样，数据价值各有不同，在数据跨境流动过程中，如何对海量的数据进行全面梳理分类和有效监管仍是挑战。数据规模庞大、数据流转实时变化、数据持续聚合拆分，增加了数据分类分级的难度。数据级别评估基准不统一，对重复加工生成的衍生数据状态判断不明，使得数据跨境流动风险难以有效判定。

三是数据跨境攻击不断升级，数据安全态势严峻。随着数据价值不断提升，以数据为目标的跨境攻击愈加频繁，数据跨境攻击技术持续升级，攻击者的组织形式趋于集中化、专业化；攻击对象日益渗透

至管、网、云、端等各环节以及各类网络设备、软硬件、关键信息基础设施等；攻击方式走向智能化、多样化，以人工智能等新技术为载体的攻击方式不断演变升级，难以防范。

近年来，**我国积极构建实施数据保护相关的法律法规，秉持“统筹安全和发展”的理念**，关注国家利益、公共安全与国际合作，探寻合规高效的跨境数据流动规则。我国立法明确提出“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”“积极开展数据安全治理、数据开发利用等领域的国际交流与合作，促进数据跨境安全、自由流动”的政策目标。同时，我国遵循多元共治的理念，在数据出境国际规则构建中，兼顾发达国家关注数字贸易利益以及发展中国家关注数据安全与产业发展利益的情况，支持基于公共政策目标或者国家安全利益而采取的数据本地化策略，与各国在独立自主基础上的开展合作与治理。一直以来，我国积极参与国际交流合作，逐步构建完善国内数据要素治理的顶层法律法规，推进具体落地实施，目前基本形成了符合我国数字经济发展要求的数据跨境流动规则。

二、我国数据跨境政策环境与重点内容解读

我国的数据跨境流动规则已基本建立，本章将进行归纳分析，剖析重要数据、个人信息、关键信息基础设施等基本概念，总结数据出

境合规路径的判断方法与实施流程，并以举例形式详细阐述数据出境的典型场景。

2.1 我国数据跨境监管制度

近年来，我国相继出台**《网络安全法》《数据安全法》和《个人信息保护法》**，对网络安全、数据安全、个人信息保护进行了制度要求，也为数据跨境流动构建了基础框架。虽然理论上数据跨境分为数据出境和数据入境，但我国主要规制数据出境活动，故本次报告主要从数据出境的角度进行切入探讨。总体来看，前述三部法律主要从重要数据和个人信息保护两个维度监管数据出境活动，建立了“数据出境安全评估”、“个人信息保护认证”和“标准合同条款”三大合规路径，具体要求如表 2-1 所示。

其中，《数据安全法》和《个人信息保护法》还明确，向外国司法或者执法机构提供数据，应经主管机关批准。个人信息处理者向境外提供个人信息前应履行相应的义务，包括：基于个人同意向境外提供个人信息的，应当取得个人信息主体同意；数据出境前应当开展个人信息保护影响评估等。

表 2-1 我国法律规制的数据出境合规路径

法律名称	生效日期	规制数据	规制主体	合规路径
《网络安全法》	2017 年 6 月 1 日	**重要数据 个人信息**	**关键信息基础设施运营者**	向境外提供，应当进行**安全评估**
《数据安全法》	2021 年 9 月 1 日	**重要数据**	**关键信息基础设施运营者**	向境外提供，应当进行**安全评估**
			其他数据处理者	遵照国家网信部门会同国务院有关部门制定的办法
《个人信息保护法》	2021 年 11 月 1 日	**个人信息**	国家机关	向境外提供，应当进行**安全评估**
			关键信息基础设施运营者	
			处理个人信息达到国家网信部门规定数量的个人信息处理者	
			其他个人信息处理者	向境外提供，应当具备下列条件之一： （1）通过国家网信部门组织的**安全评估**； （2）按照国家网信部门的规定经专业机构进行**个人信息保护认证**； （3）按照国家网信部门制定的标准合同与境外接收方**订立合同**，约定双方的权利和义务； （4）法律、行政法规或者国家网信部门规定的**其他条件**。

随后，国家互联网信息办公室（以下简称“国家网信办”）陆续发布**《数据出境安全评估办法》《个人信息保护认证实施规则》《个人信息出境标准合同办法》**（以下分别简称《评估办法》《认证实施规则》《合同办法》）等，进一步明确了“数据出境安全评估”、“个人信息保护认证”和“标准合同条款”的实施细则，我国数据出境监管制度已基本建立。三大合规路径的适用情形如表 2-2 所示。

表 2-2 数据出境合规路径适用情形

部门规章	生效日期	适用情形	配套文件
《数据出境安全评估办法》	2022 年 9 月 1 日	数据出境安全评估适用于以下四种情形： （1）数据处理者向境外提供**重要数据**； （2）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供**个人信息**； （3）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人**敏感个人信息**的数据处理者向境外提供**个人信息**； （4）国家网信部门规定的**其他**需要申报数据出境安全评估的情形。	《数据出境安全评估申报指南（第一版）》（以下简称《评估申报指南》）
《个人信息保护认证实施规则》	2022 年 11 月 4 日	对个人信息处理者开展个人信息跨境等处理活动进行认证	《信息安全技术 个人信息安全规范》 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》
《个人信息出境标准合同办法》	2023 年 6 月 1 日	通过标准合同方式向境外提供个人信息应**同时符合**下列情形： （1）非关键信息基础设施运营者； （2）处理个人信息不满 100 万人的； （3）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的； （4）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。 法律、行政法规或者国家网信部门另有规定的，从其规定。	《个人信息出境标准合同备案指南（第一版）》

2023 年 9 月 28 日，国家网信办发布**《规范和促进数据跨境流动规定（征求意见稿）》**（以下简称《规定（征求意见稿）》），向社会公开征求意见，拟对申报数据出境安全评估、订立个人信息出境标准合同等的适用门槛进行调整，这一变化预计将在很大程度上减轻企业的数据出境合规负担，降低数据出境成本，进一步规范和促进数据依法有序自由流动。《规定（征求意见稿）》明确，“《数据出境安全评估办法》、《个人信息出境标准合同办法》等相关规定与本规定不一致的，按照本规定执行”。根据《规定（征求意见稿）》，“数据出境安全评估”、“个人信息保护认证”和“标准合同条款”的适

用情形将发生变化，总结如表 2-3 所示。

表 2-3 《规定（征求意见稿）》出台后合规路径的适用情形

合规路径	《规定（征求意见稿）》出台后的适用情形
申报数据出境安全评估	（1）向境外提供重要数据； （2）国家机关和关键信息基础设施运营者向境外提供个人信息； （3）预计一年内向境外提供 100 万人以上个人信息。
订立个人信息出境标准合同或通过个人信息保护认证	（1）预计一年内向境外提供 1 万人以上、不满 100 万人个人信息。
豁免	（1）预计一年内向境外提供不满 1 万人个人信息； （2）国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据； （3）不是在境内收集产生的个人信息向境外提供； （4）为订立、履行个人作为一方当事人的合同所必需，如跨境购物、跨境汇款、机票酒店预订、签证办理等，必须向境外提供个人信息的； （5）按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，必须向境外提供内部员工个人信息的； （6）紧急情况下为保护自然人的生命健康和财产安全等，必须向境外提供个人信息的； （7）自由贸易试验区负面清单外的数据出境。

建议企业对《规定（征求意见稿）》的正式出台保持关注，以便根据《规定（征求意见稿）》的正式发布版本及时调整、确认自身适用的数据出境合规路径。我国现有数据出境相关的法律法规和国家标准情况详见附录。

2.2 数据出境合规路径判断方法

根据我国现行法律法规政策要求，企业在数据出境时应结合自身的主体类型、出境数据类型和数量等因素，综合判断是否需要申报并通过数据出境安全评估；订立并备案个人信息出境标准合同；或通过个人信息保护认证。具体应当适用何种路径，可参考如下判断方法。

1. 判断出境数据类型

- 重要数据出境，应当申报数据出境安全评估。
- 个人信息出境，则需进一步判断数据出境主体的性质、涉及个人信息主体数量。
- 向境外提供涉及党政军和涉密单位敏感信息、敏感个人信息的，依照有关法律、行政法规、部门规章规定执行。

2. 判断数据出境主体

个人信息出境，如果出境主体属于关键信息基础设施运营者，确因业务需要向境外提供，应当申报数据出境安全评估。如果不属于，则需进一步判断出境所涉及的个人信息主体数量。

3. 判断出境数据数量

若《规定（征求意见稿）》正式出台的版本与本次征求意见稿内容保持一致，那么数据出境数量对应的合规路径的判断方法如下：

- 预计一年内向境外提供 100 万人以上个人信息的，应当申报数据出境安全评估。
- 预计一年内向境外提供 1 万人以上、不满 100 万人个人信息的，需要进行个人信息出境标准合同备案或个人信息保护认证，但可以不申报数据出境安全评估。
- 预计一年内向境外提供不满 1 万人个人信息的，属于豁免情形，即不需要申报数据出境安全评估、订立个人信息出境标准合同、

通过个人信息保护认证。

需要说明的是，企业在实际工作中，**应以当时的生效规定为准**。

4. 判断是否属于豁免情形

《规定（征求意见稿）》列明了不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形，以下情况属于豁免情形。

- **不包含个人信息或者重要数据：**国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据的。
- **个人信息过境：**不是在境内收集产生的个人信息向境外提供。
- **履行合同所必需：**为订立、履行个人作为一方当事人的合同所必需，如跨境购物、跨境汇款、机票酒店预订、签证办理等，必须向境外提供个人信息的。
- **人力资源管理所必须：**按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，必须向境外提供内部员工个人信息的。
- **紧急情况所必须：**紧急情况下为保护自然人的生命健康和财产安全等，必须向境外提供个人信息的。
- **未列入自贸区负面清单的数据：**自贸区可自行制定数据出境“负面清单”，报经省级网络安全和信息化委员会批准后，报

国家网信部门备案后生效。自贸区企业向境外传输“负面清单”之外的数据，无需适用三大数据出境合规路径。

上述豁免场景中提及的部分定义仍需被进一步阐释说明，涉及的数据类型和范围也需要被进一步明确。此外，虽然《规定（征求意见稿）》阐述了多类出境豁免情形，但这并不意味着由此豁免了企业数据出境活动的事前数据安全保护义务、管理义务和安全事件发生后的报告义务。因此，企业应关注《规定（征求意见稿）》正式稿的发布情况，对企业自身数据出境涉及的豁免情形进行识别认定，以满足数据出境合规义务要求。

另外，还须注意的是，数据出境安全评估是法律的强制要求。企业一旦达到触发条件，则必须开展安全评估，不存在所谓选择数据出境路径的问题。

2.3 数据出境合规路径实施流程

2.3.1 数据出境安全评估

若企业适用数据出境安全评估路径，则需要遵守《评估办法》《评估申报指南》中明确的数据出境安全评估的申报方式及相关流程。

其中，企业应按要求提交申报材料，包括统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、数据出境安全评估申报书、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件、数据出境风险自评估

报告以及安全评估工作需要的其他材料。提交材料形式包括书面材料和电子版材料。此外，因《评估申报指南》要求提交的材料的语言必须是中文，如果企业准备的材料只有非中文版本，则必须同时提交准确的中文译本。企业还应严格按照《评估申报指南》准备和提交上述各项材料，如提交的材料不够完整，申请可能被退回。

根据《评估办法》的要求，数据出境安全评估整体流程期间为57+N 天（5+7+45+N，N 代表补充材料审核时间）；如涉及复评的，则为 72+N（57+N+15）天。具体流程如图 2-1 所示。

图 2-1 数据出境安全评估流程

2.3.2 个人信息出境标准合同

若企业适用个人信息出境标准合同路径，则需要明确个人信息出境标准合同的签署及备案流程。其中，企业需要重点关注以下义务：

首先，根据《个人信息保护法》第五十五条、第五十六条以及《合同办法》第五条规定，企业应当事前针对个人信息出境活动进行个人信息保护影响评估，并对处理情况进行记录，形成个人信息保护影响

评估报告并至少保存三年。

其次，企业在签署标准合同后，应遵守《合同办法》第三、六、七条的规定，履行标准合同备案要求，即在标准合同生效后方可开展个人信息出境活动，在标准合同生效之日起 10 个工作日内，向所在地省级网信部门提交标准合同和个人信息保护影响评估报告等材料进行备案。省级网信部门在收到材料后，会在 15 个工作日内完成材料完备性查验，并通知个人信息处理者备案结果。具体流程如图 2-2 所示。

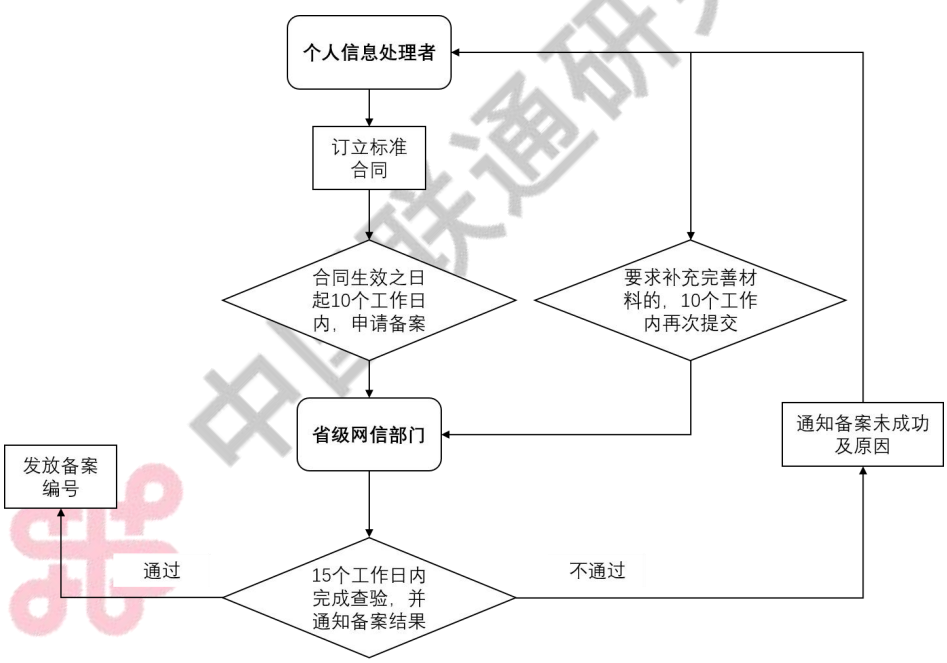


图 2-2 个人信息出境标准合同备案流程

2.3.3 个人信息保护认证

若企业适用个人信息保护认证路径，则需要遵守《关于开展个人信息保护认证工作的公告》及《认证实施规则》中关于个人信息保护

认证流程的相关规定。对于跨境数据处理活动的个人信息保护认证的依据则为《信息安全技术 个人信息安全规范》以及《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》。

具体的认证模式为“技术验证+现场审核+获证后监督”。其中，技术验证是指由专门技术验证机构按照认证方案实施技术验证，并出具技术验证报告。现场审核是指由认证机构实施现场审核，并出具现场审核报告。认证机构会根据技术验证报告、现场审核报告和其他相关资料信息进行综合评价，并作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求限期整改，整改后仍不符合的，以书面形式通知终止认证。此外，认证机构会在认证有效期内采取适当的方式实施获证后监督，确保获得认证的个人信息处理者持续符合认证要求。

需要注意的是，除上述数据出境合规路径之外，企业的数据跨境传输活动还可能同时会触发其他的审批程序。例如，根据《网络安全审查办法》第二条，企业的数据出境活动影响或者可能影响国家安全的，应按照该办法进行网络安全审查等。

2.4 数据出境所涉基本概念

数据出境场景复杂，尤其是数据类别、数据处理者身份等因素的不同，也会导致所适用的数据出境合规路径大有不同。因此，准确把握相关基本概念对有效识别数据出境合规路径及相应风险意义重大。

本部分以相关法律法规和规范性文件为基础，对数据出境所涉及的几项基本概念展开介绍。

2.4.1 重要数据

根据《评估办法》，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

2.4.2 个人信息

《个人信息保护法》明确了个人信息与敏感个人信息的概念，即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。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。

判断处理的信息是否为个人信息时，应重点关注其是否“已识别”或“可识别”自然人个人身份，只要有可能识别到特定个人，则应按个人信息的标准对待和处理。只有被真正匿名化处理过的信息，才不属于个人信息。判断处理的信息是否涉及敏感个人信息，可以结合该信息对数据主体权益的影响程度、是否属于特殊类型数据、以及结合《信息安全技术 个人信息安全规范》的附录举例表等进行综合判断。

2.4.3 关键信息基础设施

《关键信息基础设施安全保护条例》明确了关键信息基础设施的定义，即关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

2.5 数据出境典型场景

综合《个人信息保护法》《评估申报指南》等相关法律规章及国家标准的规定，在判断数据处理行为是否涉及构成数据出境时，可以结合业务场景分别从“被传输数据是否在‘境内运营中’收集和产生”以及“是否属于数据出境活动”两方面来判断。

2.5.1 被传输数据是否属于在“境内运营中”收集和产生

对于“境内运营”的概念，现行生效的政策文件尚未明确定义，但实务中一般认定为是网络运营者在中国境内开展业务，或向中国境内提供产品或服务的活动。判断网络运营者是否在境内运营不以其是否在境内注册实体，而是关注企业是否面向境内开展业务，或提供产品或服务，包括但不限于以下参考因素：

- ❖ 是否以为中国境内居民提供服务为目的；
- ❖ 提供产品和服务的过程中是否使用了中文；
- ❖ 是否提供了可以用人民币作为结算货币的选项；

❖是否向中国境内配送物流等。

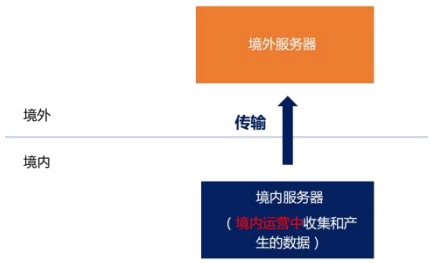
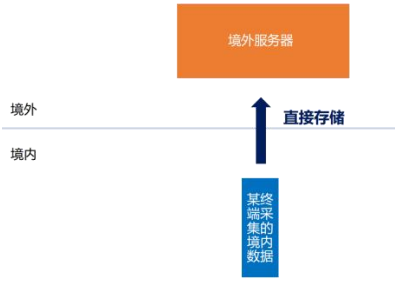
在实践中，如果境内外的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，均不视为境内运营。

2.5.2 是否属于数据出境活动

《评估申报指南》明确数据出境活动主要包括两种行为模式。一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外；二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问、查询、调取、下载、导出。在上述两种行为模式下，实践中企业常见的几类数据出境场景分别如表 2-4 和表 2-5 所示。

表 2-4 数据出境行为模式一：

数据处理者将在境内运营中收集和产生的数据传输、存储至境外

序号	场景示例	图示
①	境内主体将在境内运营中收集和产生的数据从境内服务器传输至境外的服务器。 ***例**：某公司将收集的境内业务数据上传至境内服务器，随后传输至境外母公司服务器。*	
②	境内运营的终端（如 App 等应用）采集的数据“直接存储”至境外服务器。 ***例**：某款服务器位于新加坡的 App 将在境内收集的用户数据直接存储于新加坡。*	

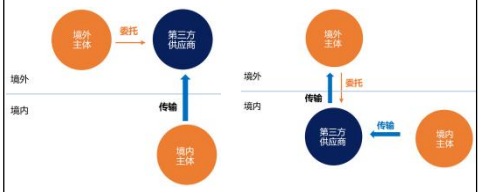
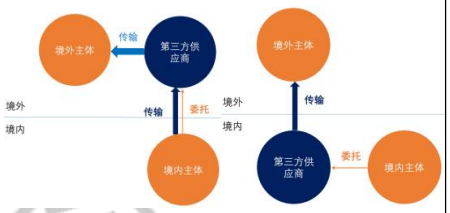
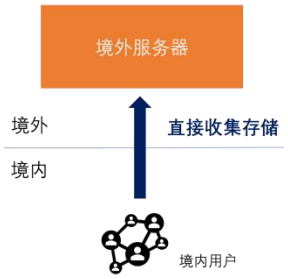
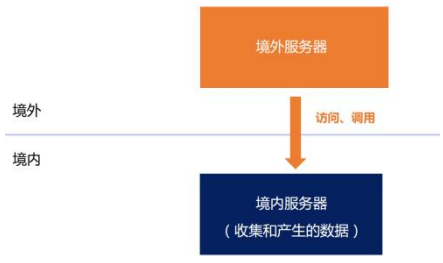
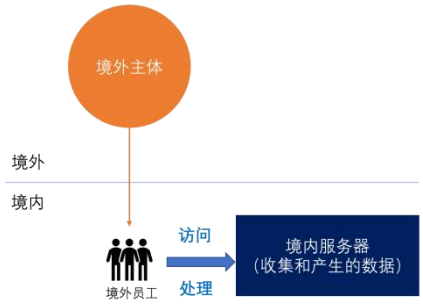
③	境外主体委托境内或境外第三方供应商代为收集境内主体在境内运营中产生的数据。 ***例：****公司聘请第三方机构代为招聘员工，由第三方机构将收集的拟聘请员工数据传输至境外，供境外母公司进一步评估考核。*	
④	境内主体委托境内或境外第三方供应商处理其在境内运营中产生的数据，并传输给境外主体。 ***例：****境内子公司委托境外数据分析供应商处理境内运营数据，供应商按照子公司委托将数据进一步传输至境外母公司。*	
⑤	境外公司直接向中国境内个人或用户提供产品或服务，且于境外直接收集境内产生的用户数据。 ***例 1：****在公司招聘的过程中，由应聘人员直接访问境外企业网站填写相关个人信息。* ***例 2：****境外母公司通过部署在境外的全球人力资源管理系统直接收集境内子公司的员工数据。*	

表 2-5 数据出境行为模式二：数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用（公开信息、网页访问除外）

序号	场景示例	图示
①	跨国公司或者同一经济、事业实体下属子公司或关联公司访问或调用境内主体存储于境内的数据。 ***例：****企业将境内员工个人信息上传至境内服务器，*	

	境外母公司可以通过登录系统直接访问、调取境内服务器上的员工数据。	
②	境外员工或人员到境内出差，访问境内系统或在境内接收数据。 ***例：****企业将境内业务运营信息上传至境内服务器，境外母公司来华视察的高管直接访问并拷贝境内服务器上的运营信息。*	

此外，一般而言，“数据过境”的情况不属于数据出境，即并非是在我国境内产生和收集的个人信息和重要数据，即使经由我国境内中转出境或是在我国进行了存储、加工处理后出境的，也均不属于数据出境。但需要注意的是，如果该等在境外产生和收集数据与境内产生收集的数据“混存”在同一境内服务器上（尽管进行了逻辑隔离），或在该服务器上对境内外数据进行融合加工分析，那么当境外主体或应用可访问、调用该境内服务器上的数据时，此类场景也可能会被认定为数据出境。

三、企业数据跨境合规治理体系建设

企业是开展数据跨境活动最活跃的主体之一，在推动数据跨境业务发展的同时，也需履行好数据跨境合规义务，维护数据安全。我国《数据安全法》第四、七条明确“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”，“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”。数据跨境流动作为数据处理活动的其中一环，需要采取多项措施健全数据跨境治理体系，提高数据安全保障能力，确保数据跨境业务的有序进行。根据国家法律规章要求，结合我们在实务中的具体实践，制定了企业数据跨境合规理框架，如图3-1 所示。下面将对框架图展开介绍。

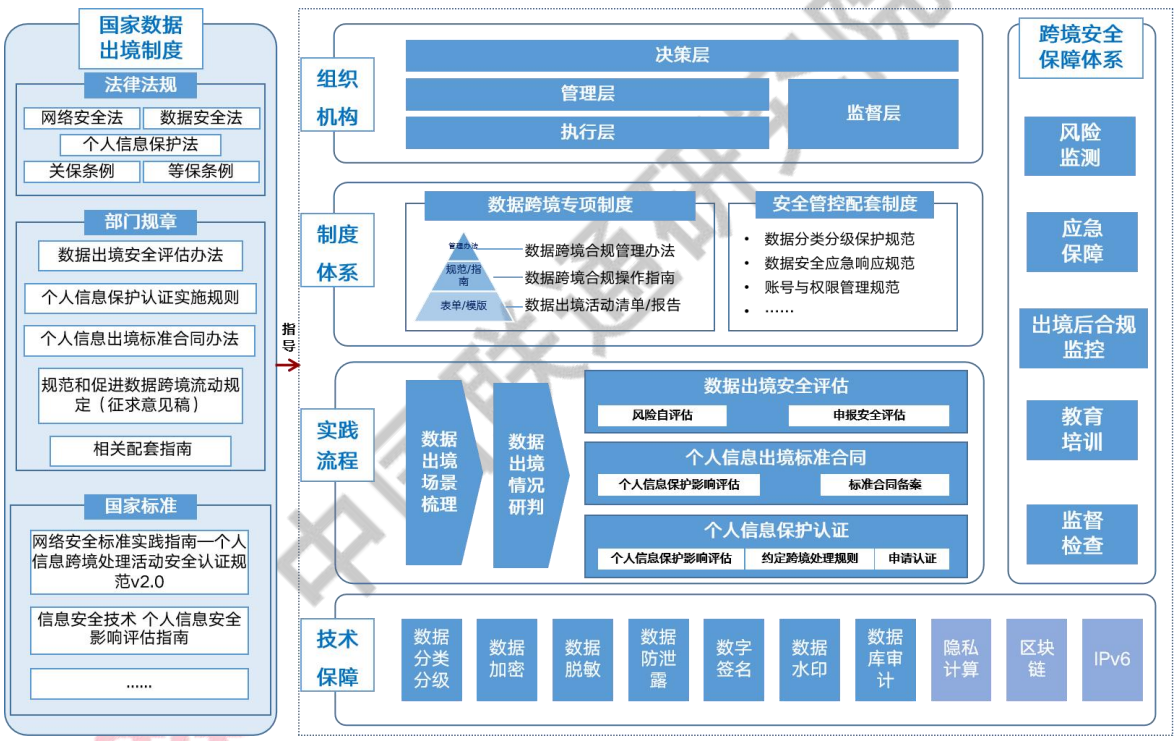


图 3-1 数据跨境合规治理框架

3.1 组织机构建设

数据跨境合规治理需要企业在内部建立相应的组织机构，以便推进数据跨境合规工作。可以在现有数据安全组织架构的基础上，明确各岗位的数据跨境安全管理职责，也可以参照决策层、管理层、执行

层、监督层的结构单独设立数据跨境合规机构，并明确岗位职责体系。例如：

- **决策层：**负责统筹决策数据跨境重大事项和重要部署，协调人力、物力资源推进数据跨境合规治理；
- **管理层：**负责制定数据跨境管理规划和制度，对数据跨境合法性、必要性、安全性等开展审核审查；
- **执行层：**负责落实数据跨境管控策略和要求，实施数据跨境活动，在开展数据跨境业务时保证操作安全合规；
- **监督层：**负责监督检查数据跨境活动的执行情况，及时发现潜在的安全风险和问题。

另外，根据有关法律和标准要求，还需重点明确关键岗位角色：

- **数据安全负责人：**需由具备数据安全专业知识和相关管理工作经历的数据处理者决策层成员承担，并负责向网信部门和主管、监管部门反映数据安全情况。
- **个人信息保护负责人：**对个人信息处理活动以及采取的保护措施等进行监督，对个人信息处理活动的合规性负责，建议由决策层成员承担。同时，应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

3.2 制度体系建设

管理制度是规范数据跨境处理活动的基础和依据，企业可建立数据跨境专项管理制度，并结合数据分类分级等其他支撑制度，规范开展数据跨境工作，规避合规风险。

3.2.1 数据跨境专项制度

围绕数据跨境安全主体责任、安全保障及运行管理的实际需求，可结合企业自身制度体系，开展数据跨境管理专项制度体系建设。例如，在数据安全和个人信息保护方针下，建立数据跨境管理办法、操作指南、清单与报告等制度体系，为数据跨境安全管理工作提供指导和依据，促进数据跨境管理工作标准化、流程化、规范化开展：

❖ **数据跨境管理办法**

数据跨境管理办法作为数据跨境管理的顶层制度，明确数据跨境管控目标、原则、各相关方职责和具体要求，规范各相关方数据跨境活动。

❖ **数据跨境合规操作指南/规范**

数据跨境合规操作指南/规范为数据跨境管理提供操作规程和实施指引。

❖ **配套表单/报告/模板**

针对数据跨境管理的具体工作事项，设计与操作流程配套的流程表单、记录、报告模板等文件。相关表单/模板可以包括数据出境活

动清单、数据出境安全评估报告、个人信息出境标准合同及其相应的模版等。

3.2.2 安全管控配套制度

数据跨境流动作为数据处理活动的一种场景，需要依靠数据安全管理制度，配套辅助数据跨境流动过程中的安全管理。

根据数据安全法律法规和标准，结合企业实际情况，建立覆盖数据分类分级、数据全生命周期安全防护、权限管理、日志留存、风险监测预警、应急响应、安全评估、教育培训、监督检查等方面的数据安全制度体系，是数据跨境安全管理工作开展的基础。例如，在数据出境前需要依据数据分类分级制度判断出境数据的类别和级别，在数据出境中和出境后需要依据有关要求采取相应的防护举措并做好风险监测等数据安全保障工作。

3.3 合规路径操作实践

3.3.1 数据出境场景梳理

企业需要对自身的数据出境场景进行全面盘点，以掌握实际的数据出境情况。可以制定数据出境情况调研表，面向各部门进行发放，对已开展的和计划开展的数据出境的详细情况进行梳理，形成数据出境情况清单。调研内容包括数据出境业务场景、信息系统、出境时间、出境方式、数据类型、数据量、出境原因、境外接收方情况等。

3.3.2 数据出境合规路径实施

完成数据出境情况调研后，需要逐个判断数据出境业务以及境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性，在满足合法性、正当性、必要性的情况下，还需要进一步判断该数据情况应采取的数据出境合规路径。判断方法可以参照本文第 2.2 节所述的方法。如果需要通过申报数据出境安全评估，或订立并备案个人信息出境标准合同，或通过个人信息保护认证的方式出境的，则应在满足有关法律法规的要求下合法开展数据出境活动，本文 2.3 节介绍了三种数据出境路径的实施流程。

需要注意的是，如果涉及个人信息出境，按照《个人信息保护法》，在数据出境前，企业还应向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。同时企业应进行个人信息保护影响评估，对处理情况进行记录。数据出境过程中，应当采取必要措施，保障境外接收方处理个人信息的活动达到我国《个人信息保护法》规定的个人信息保护标准。

3.4 保障体系建设

3.4.1 风险监测

数据出境中和出境后，企业均应加强对数据出境活动的风险监测，宜根据数据跨境情况建立针对性的数据安全风险监测预警方案，对数

据跨境远程访问、使用以及数据跨境传输等实施监测巡查，对异常流动等行为进行预警和处置，形成处置记录。

涉及境外远程访问、使用数据的，需做好权限管理，按照业务需求、安全策略、权责明确原则和最小授权原则，合理界定境外接收方的数据访问和处理权限。建议保留数据出境处理活动的全过程操作行为记录，做好日志留存，并定期开展日志审计，形成审计报告，对发现的问题及时整改处置。

3.4.2 应急保障

企业宜根据数据出境业务情况建立针对性的数据安全事件应急预案，明确数据安全事件级别、应急响应流程、责任体系等，并定期开展应急演练，以便在紧急事件发生后，能够立即采取补救措施，并按照规定及时告知用户并向有关主管部门报告。根据演练结果，不断优化数据出境安全保护措施，并形成演练总结报告。

3.4.3 出境后合规监控

企业可以根据数据出境情况，绘制数据跨境流转图，用可视化方式呈现各业务场景下的数据跨境流转情况，包括境外接收方信息、数据出境方式、数据在境外存储位置、数据处理情况等，便于厘清数据出境情况，从而更有针对性地识别不同跨境业务场景下的合规问题及安全风险。

企业还需要持续关注数据接收方所在国家或地区的数据跨境相关法律动态，对发生变化的情况进行评估，及时调整数据跨境策略，如触发重新申报数据出境安全评估的情况，还应当重新申报。

3.4.4 安全意识培养

企业宜在内部加强对数据跨境政策、数据跨境流动安全保障技术、案例应用等方面的教育培训，强化员工对数据跨境政策的认识，提高业务人员对数据跨境场景下的合规意识，加强安全措施的实施以及对风险的发现和防范能力，规范数据跨境安全治理工作开展。

3.4.5 监督检查

企业宜定期对数据出境安全管理情况和落实效果进行监督检查，并及时督促问题整改，防范不合规的数据出境情形。例如，定期查验数据出境调研是否全面、是否覆盖最新政策要求，数据出境活动清单是否完整、更新是否及时；针对公网出境场景，监测核查实际出境数据是否与申报内容一致；是否采取加密等技术措施保障数据出境安全等。

3.5 技术防护措施

开展数据跨境合规治理，除了管理体系的建设之外，也需要相应的技术手段对数据跨境过程提供安全防护。基础的数据安全防护策略和技术，包括数据资产识别、数据脱敏、传输加密、审计等，是数据跨境安全的必要防护手段。除此之外，近年来飞速发展的隐私计算技

术，能够在原始数据不出本地的前提下，完成多方任务的安全计算，此外使用区块链技术进行辅助，可以同时保障高敏感数据的机密性和不可篡改性。

3.5.1 数据安全通用技术应用

1. 数据资产梳理

在数据跨境流通前，首先需要理清数据资产家底，通过数据资产梳理技术，对各类数据进行清查盘点，并以资产目录及资产索引的方式，绘制数据源、数据表、文件、类型、大小等多维度数据资产地图，直观、形象地描绘数据资产的分布、数量、归属等信息。数据资产地图通过树状结构图、数据关系图等可视化图表能够清晰、准确地揭示数据源、数据库、数据表、字段、文件之间的关系和脉络。

2. 数据存储加密

依据数据分级分类的标准，对于敏感数据、内部数据等在存储时进行加密处理。加密后的数据以密文的形式存储，保证存储介质丢失或数据库文件被非法复制情况下数据的安全。采用数据存储加密技术，能有效防止数据库高权限账号泄漏、黑客攻击等风险事件而造成的数据泄密。

3. 数据脱敏

数据静态脱敏技术，通过数据脱敏机制对敏感信息通过脱敏规则进行数据的变形，实现敏感数据的可靠保护。在不影响数据跨境需求

方，对数据要求的条件下，对真实的生产数据进行改造并提供使用。在数据跨境流通之前，可以通过数据静态脱敏技术，对原始数据进行处理，提升即将跨境数据的机密性。

数据动态脱敏技术，使用屏蔽、随机、仿真等类型的脱敏算法，基于数据分级分类标准和用户访问数据的权限，在敏感数据跨境传输的过程中，根据相关的权限及授权要求，对实时的 SQL 查询语句进行修改和模糊化处理，防止敏感数据的跨境泄露。

4. 数据防泄漏

对于非结构化数据，特别是设计、代码、技术方案等数据的保护，是各国、各行业、企业数据中的弱点，也是重点和难点。在数据跨境流动的应用场景下，针对不同的数据传输方向，通过在境内传输边界节点应用数据防泄漏技术，部署在终端和网络出口处，可有效监管非授权外设传输、拷贝、跨境外发等高风险操作。

5. 数字签名

在数据跨境传输过程中的完整性保护，可以通过数字签名技术来实现。在电子公文流转、敏感数据交换等流程中，采用数字证书的数字签名对数据传输过程中的文件信息进行签名，杜绝数据伪造、滥用，全面保障信息的完整性、严肃性和权威性。

6. 数据水印

通过数据水印技术，可确保敏感数据的完整性和真实以及可追责性。数据水印通常是不可见的或不可察的，它与原始数据紧密结合并隐藏其中，成为源数据不可分离的一部分，并可经历一些不破坏源数据使用价值或商用价值的操作而保存下来。在数据跨境流通的流程中，一旦信息泄露，可第一时间将水印标识解封，通过读取水印标识编码，追溯数据泄露的全流程，精准定位泄露单位及责任人，实现精准追责定责。

7. 数据库审计

在数据跨境流通之前，对所有数据库系统、数据操作日志进行统一收集、记录、全局审计。按照数据安全管理规范中的规定，通过数据审计监控、行为分析、溯源追踪、权限管控等技术手段，在安全事件发生后，迅速准确的定位责任人，提供有效证据，按照相关法律法规进行处置。

3.5.2 数据安全创新技术应用

1. 隐私计算

在隐私计算的框架下，各计算参与方的数据不出本地，能够在不泄露各自数据的前提下通过协同计算实现多源数据的跨域合作。针对有出境需求的数据，通过采用隐私计算方案，在数据本身不出境的情况下，跨境进行模型训练、安全统计等多中心联合分析，可替代传统

的数据复制跨境流动方式，以数据可利用实现安全合规的数据出境。通过采用隐私计算的方式，跨国组织或企业，可以实现多方数据之间的虚拟融合，而无须再采用像传统的数据物理传输和统一汇集的方式，最大程度的实现了出境数据的最小化。隐私计算是“数据可用不可见”技术集合的统称，包括多方安全计算、联邦学习、可信执行环境等多项技术。

（1）多方安全计算

多方安全计算能够同时确保输入的隐私性和计算的正确性，在没有可信第三方的前提下通过数学理论保证参与计算的各方输入信息不暴露，而且同时能够获得准确的运算结果。多方安全计算通常借助多种底层密码框架完成，主要包括不经意传输，混淆电路，秘密共享等。多方安全计算逐渐发展为现代密码学的一个重要分支。

不经意传输是指数据传输方发出多条信息，而接收方只获取其中一个，由于传输方不确定最终到达的信息是哪一条，接收方也无法得知未获取的其他信息，从而双方的数据都处于隐私状态；混淆电路是多方参与者利用计算机编程将输入的计算任务转化为布尔值，对输入的具体数值加密，因此多方在互相不掌握对方私人信息时，可共同完成计算。秘密共享是对加密信息的随机切分过程，将信息的片段分散至多个参与方保管，因此除非超过一定数量的多方协同合作，否则无法还原完整的数据并进行解密。

（2）安全联邦学习

安全联邦学习被认为是兼具隐私保护和跨机构数据共享的技术解决方案，它能连接多个数据源，但在数据共享过程中只交换加密的经过处理的中间计算结果，因而不会泄露明文的个体数据，从而同时达到数据共享和隐私保护的双重目标。在没有加密计算的情况下，在联邦学习阶段，每次迭代时需要交换数据源方的中间统计信息，这些信息可用于推断来自数据源的敏感私有输入数据。另一方面，联邦学习本身无法支持许多数据预处理步骤，而这些对于后续步骤中的数据分析至关重要，例如重复数据消除、样本对齐、参数对齐、数据筛选等。

简单地说，联邦学习是一种可以减少机器学习阶段交换的个体信息的有效参考技术框架，但是如果只单纯依赖联邦学习技术是无法确保在整个数据分析阶段最终保护敏感的私有数据。

针对普通联邦学习的缺陷，业界对联邦学习进行多层次改进，形成安全联邦学习的技术能力，在普通联邦学习技术基础上基于隐私保护计算技术做出大量的改进，克服原有的弊端和风险，既能够消除信息泄露的问题，还同时具有较高的执行效率和处理能力。安全联邦学习技术主要解决隐私机密数据多数据源的联合分析需求。

通过使用安全联邦学习技术，使得隐私保护计算平台能够作为大数据平台的数据底座，打破数据孤岛，建立跨行业、跨部门，跨主体，

可以实现多行业、多部门、多中心的数据联合计算。可实现在符合我国的网络安全法以及 GDPR、HIPAA 等严格隐私保护法律法规情况下的多中心多维度实时大数据分析计算。传统联邦学习和安全联邦学习的比较如表 3-1 所示。

表 3-1 传统联邦学习和安全联邦学习的比较

技术	成熟度	性能	算法能力	安全性	依赖可信方	概要
普通联邦学习	高	高	中	中	部分需要	普通联邦学习，存在风险需要结合其它技术改进，才能合规。
安全联邦学习	高	高	高	高	可不需要	综合运用 TEE、密码学等隐私保护计算方法，适用于各种业务场景，容易合规。

（3）可信执行环境

可信执行环境作为易开发、高性能的隐私计算技术，与硬件提供方存在强依赖关系。其实践路径表现为：在 CPU 内划分出独立于操作系统的、可信的、隔离的机密空间。由于数据处理在可信空间内进行，数据的隐私性依赖可信硬件的实现。其核心思想是以可信硬件为载体，提供硬件级强安全隔离和通用计算环境，在完善的密码服务加持下形成“密室”，数据仅在“密室”内才进行解密并计算，除此之外任何其他方法都无法接触到数据明文内容。

2. 区块链

区块链技术具备数据可抽象、不可篡改、防伪溯源等特点，可以较好地满足目前数据跨境场景下对原始数据隐私保护、数据实时查询、历史数据可追溯、跨境备案数据防篡改、日志记录多重备份以及自动化审计等需求，从而增强数据跨境行为的透明性与安全性。

对于数据跨境流动，可以开展境内外开放网络环境下区块链系统的研究，基于区块链网络的跨境数据流动示意图如 3-2 所示。境内外开放网络采用授权管理模式，参与方在可控条件下读取、发送和确认交易，及其它共识过程。境内外开放网络环境下，区块链系统通过部署高性能硬件保障底层性能，并采用安全弹性的网络拓扑结构和高效的数据分发技术提升系统响应处理效率，实现境内外全球化部署网络环境下，高安全、高吞吐率、低数据冗余度的区块链网络服务。

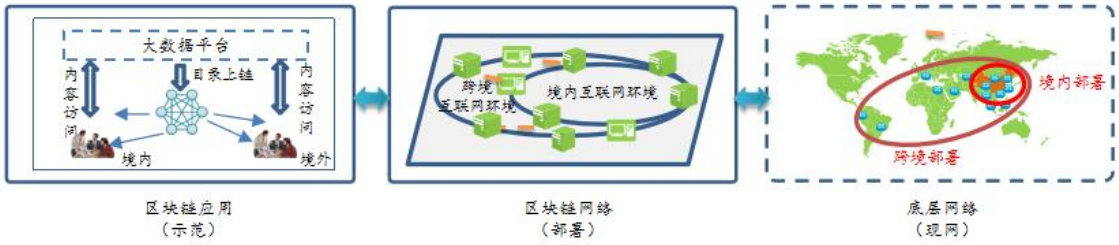


图 3-2 基于区块链网络的跨境数据流动示意图

可以依托开放网络的区块链系统，研究数据跨境流动服务示范应用，搭建由区块链作为底层技术的平台系统，形成覆盖数据采集、数据分析、数据交互、数据跨境监管的一整套系统和解决方案，并由一

系列的法律法规和标准规范作为有效支撑，最终形成完整可行的数据跨境流动管理解决方案。

3. IPv6

IPv6 具有充足的地址空间、层次化的地址结构、灵活的扩展头和强大的邻居发现机制，在数据跨境流动场景中，具有巨大的应用潜力。在数据跨境流动的过程中，可以应用各类IPv6+的核心能力，例如，SRv6（基于IPv6 转发平面的段路由）技术在IPv6 报文中插入一个显式的IPv6 地址栈，该地址栈储存一条有序排列的转发路径，这种方式有能力在数据跨境流动过程中控制数据的传输路径。APN6（应用感知型IPv6 网络）技术则是将应用信息携带在IPv6 数据报文中传递进入网络，使用该技术可以在数据跨境流动的过程中明确数据的类型和级别，并进一步为不同类型和级别的数据提供不同的服务。IFIT（随流检测）技术是在真实业务报文中插入IFIT报文头以进行特征标记，这种方式有能力实现数据跨境传输的路径溯源跟踪。

可以说，IPv6 为感知数据、管理并优化数据跨境传输提供了一个潜在的解决方案。企业可以积极探索并推进IPv6 在数据跨境场景中的应用落地，保证数据安全流动的前提下，最大程度的促进数据自由跨境流通，促进数字经济的高质量发展。

四、数据跨境安全管理发展建议

4.1 健全数据出境制度体系与保护机制

一是细化完善数据跨境安全管理制度。建立一套可执行和可操作的数据跨境流动安全管理制度，涵盖数据出境全流程，细化数据出境安全评估的事项和标准，明确跨境数据安全审批、监管的要求，由各行业各领域建立符合本行业、领域特点的数据出境安全管理措施，强化对数据出境的全流程安全管控。

二是健全数据分类分级保护制度。数据分类分级保护制度是开展数据出境安全评估、数据出境分级保护的基础，建议加快制定数据分类分级国家标准、行业标准等，指导数据处理者在实践层面加强数据出境分级管控。针对重要数据出境，建议行业或地方主管部门进一步细化行业或地方重要数据目录，强化对重要数据的识别和对重要数据的出境管控，保障重要数据安全。

三是强化数据出境事中事后监管机制。数据出境监管是数据出境活动前、中、后阶段保障数据出境安全的重要手段，数据出境后可以从监管主体、监管流程与实施机制方面制定不同的监管策略，提升数据跨境安全风险防范能力。例如，可以制定跨境数据安全事件定级与响应处置的判定标准，建立数据出境跟踪监督与报告机制，当数据出境后出现威胁国家安全的问题时，国家有关部门及时通知相关企业，

或者企业主动通知有关部门，协同开展应急处置机制，针对性地解决数据出境活动所带来的安全威胁，降低安全风险。

4.2 强化数据跨境技术创新研究与应用

除了顶层设计以及规则制定的完善之外，针对数据跨境场景，还需要通过数字技术手段保障跨境数据的安全流动。

一是加强数据跨境场景下安全技术的创新应用。需加强数据资产梳理、数据加密、数据脱敏等数据安全通用技术在数据跨境环节的安全保障，提高数据访问、流向控制、溯源等关键环节的管控能力，同时，积极推进隐私计算、区块链、IPv6 等新技术在数据跨境场景下的创新应用，通过“数据不跨境、算法模型跨境”“数据可用不可见”的新型数据传输模式，在敏感数据不出境的情况下，推动数据要素价值发挥。

二是加强数据跨境流动安全风险监测。可以探索建立国家层面的数据跨境风险监测、预警、安全信息共享调度平台，统筹协调有关部门加强数据安全风险信息的获取、分析、研判与预警工作，通过技术手段对数据出口节点开展持续流量监测，对涉及重要数据的出境流动进行严格审查，对发现的数据出境安全风险及时开展应急处置，规范数据出境行为，保障数据安全。另外，可以全面排查开源软件和数据系统存在的潜在数据出境风险与安全隐患，避免数据违规泄露。

三是布局数据跨境基础设施建设，夯实安全底座。试点可信数据空间建设，开发数据空间通用规则，通过技术、语义、组织和法律互操作性实现不同组织间的信任，通过数据空间促进可信的数据跨境流动。推动跨境数据基础设施建设，加大国际海底光缆、国际互联网数据交互点等数据基础设施建设，提升跨境数据基础设施安全保障能力。

4.3 推动数据跨境协同治理与国际交流合作

一是探索建立政企协同的数据跨境治理体系。企业作为跨境规则的实践者和数据跨境业务的直接参与者，能够为数据跨境规则制定和数据安全风险监测提供实践经验，政府和企业协同开展数据跨境规则制定和安全风险监测，对于推动数据出境国家安全治理意义重大。数据跨境治理中，政府与企业合作已成为各国常态。可以探索建立“以政府为主导，以企业为辅助”的数据跨境协同治理体系，政企联动共同推动数据跨境安全有序流动。

二是探索建立跨境数据“白名单”制度。可参考 GDPR，认定一批允许数据直接出境的国家“白名单”，加快建立互信互任的双多边协定。可以充分研判各个国家的数据管理法规及法律环境，并将与我国签订双边、多边合作协议的国家纳入考量范围，以今年 6 月 29 日国家网信办与香港特区政府创新科技及工业局签署的《关于促进粤港澳大湾区数据跨境流动的合作备忘录》为始，利用各地自贸区优势，

增设数据出境“白名单”，逐步带动数据自由流动的多边效应，加快区域间协定的谈判与建立，深化与其他国家的数据合作。

三是探索建立国际数据自由港。我国作为全球数字经济第二大市场，天然具备成立中立数据中心的条件。可以结合自贸区负面清单，通过打造国际数据自由港，一部分数据可以在国际上自由流动，推动更大范围的国际合作，有助于参与国际社会数据跨境流动规则的制定，建立发展与安全相协调的跨境数据流动规则体系。

附录：数据出境相关法律法规和国家标准

序号	文件名称	发布机构	施行时间
一、法律			
1	《中华人民共和国网络安全法》	全国人大常委会	2017 年 6 月 1 日
2	《中华人民共和国数据安全法》	全国人大常委会	2021 年 9 月 1 日
3	《中华人民共和国个人信息保护法》	全国人大常委会	2021 年 11 月 1 日
二、法规			
4	《关键信息基础设施安全保护条例》	国务院	2021 年 9 月 1 日
三、部门规章			
5	《网络安全审查办法》	国家网信办等 13 部门	2022 年 2 月 15 日
6	《数据出境安全评估办法》	国家网信办	2022 年 9 月 1 日
7	《数据出境安全评估申报指南（第一版）》	国家网信办	2022 年 8 月 31 日
8	《个人信息保护认证实施规则》	国家市场监管总局、国家网信办	2022 年 11 月 4 日
9	《个人信息出境标准合同办法》	国家网信办	2023 年 6 月 1 日
10	《个人信息出境标准合同备案指南（第一版）》	国家网信办	2023 年 5 月 30 日
11	《规范和促进数据跨境流动规定（征求意见稿）》	国家网信办	征求意见稿
四、国家标准			

12	GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》	TC260	2020 年 3 月 1 日
13	GB/T 35273-2020《信息安全技术 个人信息安全规范》	TC260	2020 年 10 月 1 日
14	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	TC260	2021 年 6 月 1 日
15	TC260-PG-20222A《网络安全标准实践指南-个人信息跨境处理活动安全认证规范 V2.0》	TC260	2022 年 12 日 16 日
16	GB/T 41817-2022《信息安全技术 个人信息安全工程指南》	TC260	2023 年 5 月 1 日
17	GB/T 42574-2023《信息安全技术 个人信息处理中告知和同意的实施指南》	TC260	2023 年 12 月 1 日
18	20230255-T-469《信息安全技术 个人信息跨境传输认证要求》	TC260	征求意见稿

参考文献

[1] 张茉楠．数据跨境流动新规的风向标意义．[EB/OL] https://mp.weixin.qq.com/s/ValKum9gK-u07ZMbuf8xJw,2023-10-20

[2] 余宗良,张璐.我国数据跨境流动规则探析——基于粤港澳大湾区先行先试[J].开放导报,2023(02):86-93.

[3] 世界银行，World Development Report2021_Data for Better Lives[R],2020.

[4] 刘如,周京艳.我国数字经济外循环面临的跨境数据流动政策问题与对策[J].科技中国,2021,(04):53-56.

[5] 斑马数据合规研究中心.数据跨境现状调查与分析报告[R],2023.

[6] 德勤,中兴. 数据跨境合规治理实践白皮书[R],2021.

[7] 郭春镇,候天赐.个人信息跨境流动的界定困境及其判定框架[J].中国法律评论,2022,(06):86-106.

[8] 吴丹君,周天一.《网络安全法》系列解读之（二） 数据跨境转移合规.[EB/OL] http://ggzyjy.dl.gov.cn/TPFront/infodetail/?infoid=15e745a4-d812-48e5-a0e0-937cd8019334

[9] 丁伟,倪诗颖. 数字贸易视野下我国跨境数据监管的发展困境及合作治理[J].北京邮电大学学报(社会科学版),2023,25(01):67-76.

[10] 王伟玲．数据跨境流动系统性风险:成因、发展与监管[J].国际贸易,2022,(07):72-77.

[11] 肖雄. 国际贸易体制下数据跨境流动监管之困境[J].上海法学研究,2020,3(01):294-310.

[12] 许力先，盛佳宇. 国家安全视角下数据跨境流动管制面临的困境及其应对策略.[EB/OL] http://www.zjbar.com/info/2d5d84d5dc62438dbe20878dd83d120f

[13] 孟凡新. 双循环视角下提升数字平台治理水平的机制研究[J].商业经济研究,2023,(06):105-109.

[14] 马其家,刘飞虎. 数据出境中的国家安全治理探讨[J].理论探索,2022(02):105-113.

[15] 孙珵珵. 数据跨境流动监管与安全比较研究[J].中国电子科学研究院学报,2023,18(01):91-96+102.

[16] 陈思琦. 智能网联汽车数据跨境流动的法律问题研究[J].网络安全技术与应用,2023,(04):146-148.

[17] 华为. NE5000E V800R022C00SPC500 特性描述.[EB/OL] https://support.huawei.com/enterprise/zh/doc/EDOC1100278759/d169625f

[18] 何林,况鹏,王士诚等. 基于“IPv6+”的应用感知网络（APN6）[J].电信科学,2020,36(08):36-42.

[19] 熊光清,张素敏. 总体国家安全观视角下我国数据出境安全管理制度的完善[J].哈尔滨工业大学学报(社会科学版), 2023,25(05):32-40.

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院致力于提高核心竞争力和增强核心功能，紧密围绕联网通信、算网数智两大类主业，按照 4+2+X 研发布局，开展面向 C3 网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国建设，大力发展战略性新兴产业，加快形成新质生产力。联通研究院现有员工 700 余人，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话：010-87926100
邮编：100176

中国联通研究院　　中国联通泛终端技术