# 数据经济学

# 第十一章：数据经济的对外开放

陈希路

暨南大学经济学院

2026 年春

# 章节目录

# 章首导言

## 理论背景

经济学中，为简化分析常假设**封闭经济**，但现实世界的主流是**开放经济体系**。

——N. 格里高利 曼昆《经济学原理》

**数据经济在开放条件下的基本表现：**

- **规模地位**：全球数据流动规模不断扩大，数据贸易在数字贸易中地位凸显
- **价值增长**：数据经济的价值在开放网络中呈现倍增趋势
- **核心挑战**：数据流动引发的安全性问题愈发引起关注
- **治理演变**：跨境数据流动的治理成为新领域，国际规则日益重要

# 第一节

# 开放条件下的数据经济

# 开放条件下数据流动的特点

## 1. 扩大资源配置的范围

在理论上，商品、资本、技术乃至其他要素的自由流动可以实现全球范围内的资源最优配置，**数据作为新生产要素同样符合此规律**

- 马克思在《1857-1858 年经济学手稿》中指出：“生产力……的普遍发展成了基础，同样，交往的普遍性，从而世界市场成了基础”
- **开放经济的本质**：
  - 把一国市场与世界市场连接起来
  - 鼓励尽可能充分地参加全球分工
  - 在国际分工中发挥出本国经济的比较优势

# 开放条件下数据流动的特点

## 2. 独特的交易方式与流动视角

数据流动并不直接发生在生产者和消费者之间，理解它需要三个视角：

- **视角一：商业交易相关数据**
  - 如账单、银行数据、地址等，通常*自愿提供*，政策争议较少
- **视角二：原始数据**
  - 从个人活动、产品、事件中收集，*本身没有价值*，汇总处理后才产生价值
- **视角三：数据产品**
  - 原始数据处理成数字智能，跨境销售时被视为贸易统计中的服务项

# 现实案例：从原始数据到数据产品的跨国贸易

## 案例：运动社交平台 Strava 的数据变现

Strava 是一款全球流行的跑步与骑行记录 App，其数据流转完美体现了交易视角的转化。

- **商业/用户自愿提供**：全球数亿用户免费上传个人的 GPS 运动轨迹
- **原始数据（无直接商业价值）**：单条轨迹除了记录个人生活，在国际市场上无法直接标价出售
- **数据产品化（高价值服务贸易）**：
  - Strava 将大量跨国原始数据进行**脱敏、汇总与算法分析**
  - 推出 *Strava Metro* 数据产品，将其出售给全球各地的城市规划部门（用于优化自行车道、分析交通拥堵）
  - **启示**：数据的跨境流转实现了从免费足迹到高昂市政数据资产的价值跃迁

# 开放条件下数据流动的特点

## 3. 数据跨境贸易与要素流动的特征

- **进出口的重定义**:
  - *出口*: 国内产生而流入国外的数据
  - *进口*: 国外产生而流动到国内的数据
- **自由流动 vs 市场交易**:
  - 当前很多数据在国际市场中未产生明显交易，而是自由流动的
  - 仅少部分数字企业实现了在世界数据市场上买卖数据
- **开放度的制约因素**:
  - 一般规律: 经济发展水平越高，越接近开放型经济
  - 现实反差: 因安全性问题，数据经济的开放性受政策限制极大

# 开放条件下数据流动的特点

**核心悖论：效率——安全——公平**

复杂利益使数据经济极难在“效率—安全—公平”三维达到完美均衡。

## 4. 效率与安全的妥协

- **理论支撑**：某问题一旦被定义为安全事务，将获得绝对优先地位
- **数据经济的效率—安全悖论**：
  - *效率来源*：数据要素市场的自由竞争
  - *安全焦虑*：竞争使个人、公司、国家处于一定程度的不安全状态
  - *现实结果*：对效率的追求经常让位于对安全的追求

# 现实案例：效率—安全悖论的商业代价

## 案例：TikTok 的得州项目与云端计划

为了应对欧美国家对跨境数据流动的安全焦虑，跨国企业往往需要付出极高的效率代价。

- **纯市场逻辑（追求效率）**：
  - 全球统一算法，数据集中回传至单一数据中心处理，成本最低、技术迭代最快
- **国家安全逻辑（安全焦虑）**：
  - 美欧担忧公民数据回流引发国家安全隐患，强制要求数据本地化
- **妥协与代价**：
  - *得州项目*：TikTok 耗资 **15 亿美元**将美国用户数据交由甲骨文在本土托管
  - *云端计划*：每年花费 **12 亿欧元**在欧洲建立三个本地数据中心
  - **结论**：跨国数据企业为获得安全准入，被迫放弃部分技术架构的效率

# 开放条件下数据流动的特点

**5. 数据收益在跨国间的公平分配难题**

在开放条件下，数据要素的收益很难在不同经济体间公平分配。

- **发达国家的优势地位**:
  - 基于科技先发优势，建立了对自己有利的跨境数据流动规则
- **发展中国家的防御处境**:
  - 技术上处于追赶阶段，在规则制定上更多处于防御地位

# 开放条件下数据流动的主要趋势

**1. 全球数据流动规模不断扩大**

驱动力：物联网、云计算和数据分析；2005 年以来，全球数据流增长了**数百倍**

## 中国的超大规模数据优势（2022 年数据）

- **数据产量**：8.1 ZB，同比增长 22.7%，全球占比 10.5%
- **数据存储量**：724.5 EB，同比增长 21.1%，全球占比 14.4%
- **未来预测**：预计 2025 年将达 48.6 ZB，成为全球最大的数据区域

# 开放条件下数据流动的主要趋势

## 2. 全球数据流动范围趋于集中

2004–2020 年，全球数据流动主要集中在**北美、欧洲和亚洲**之间

- **价值获取的不平衡**：
  - **发达国家**：垄断主要平台与人才，处于生态网络中心
  - **发展中国家**：
    - 流出：低价值原始数据；流入：高额付费服务
    - 从属困境：沦为少数全球性数字平台的**原始数据提供方**

# 现实案例：AI 时代的数据掠夺与分工不平等

## 案例：生成式大模型背后的全球数据链

全球数字化发展集中于欧美大平台，发展中国家正面临新形态的数据殖民。

- **原始数据的单向抽取**：
  - 欧美头部 AI 企业通过爬虫技术，无偿获取全球（包括广大发展中国家）的互联网公开数据用于模型训练
- **低端数据劳动的外包**：
  - 将数据清洗、有害内容标注等密集型工作外包给肯尼亚、菲律宾等国的廉价劳动力，时薪往往不足 2 美元
- **高附加值服务的高价倾销**：
  - 发展中国家提供了语料和人工，但最终需向欧美平台支付高昂的 API 调用费，印证了沦为原始数据提供方的理论

# 开放条件下数据流动的主要趋势

### 3. 数据贸易在数字贸易中的地位凸显

数据是数字贸易发展的**基础和重要载体**

- **应用场景扩展**：跨境电商、社交媒体视频、工业互联网等
- **形态演变**：目前内嵌于服务贸易，未来或成为独立的贸易形态
- **中国地位**：2021 年数据产生量 6.6 ZB，数据贸易枢纽地位初显

# 开放条件下数据流动的主要趋势

**4. 开放使得数据经济价值倍增**

全球数据流动对经济增长有明显的拉动效应

- **经济增长拉动**：
  - 流动量每增加 10%，带动 GDP 增长 **0.2%**
  - 行业利润促进率平均为 10%（金融行业高达 32%）
- **网络效应（梅特卡夫定律）**：
  - 网络价值与用户数的平方成正比 ($V \propto n^2$)
  - 开放条件下节点增加，价值指数级倍增

# 第二节

# 开放条件下数据流动的安全性考量

# 开放条件下数据流动的安全性考量

## 核心观点

越是开放，越要重视安全。

**相较于封闭条件，安全性考量的特殊性：**

- **个人层面**：主要涉及隐私保护问题
- **国家层面**：主要涉及经济安全问题，也不可避免会牵扯政治议题等

# 跨境数据流动在国家层面的影响

## 1. 经济安全是国家安全的基础

- **2005 年《国家经济安全》**:
  - 将经济安全视为国家安全的基础
  - 经济发展与经济安全休戚相关，因为发展是一国经济安全的关键，弱国无安全
- **2014 年总体国家安全观**:
  - 强调以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托

# 跨境数据流动在国家层面的影响

## 2. 经济安全的相对性

- 著名国际安全学者**巴里 布赞**认为：
  - 经济安全代表了一种可广泛应用的绝对价值，是一个虚幻的观点、一个妄想
  - 真的经济安全是由各种矛盾、妥协、交易拼凑起来的奇怪而又模糊的东西，是一个相对概念

## 3. 核心安全隐患

- 数字平台企业在跨国服务中获取的数据量达到一定量级时，便能对国家安全事务进行分析，进而给被服务国带来安全隐患
- 这一问题需要从全球、区域等更大的视角加以关注

# 跨境数据流动在国家层面的影响

## 潜在的逻辑冲突：国家安全 vs. 经济规律

从国家角度考察跨境数据流动容易局限于国家安全需求的满足，从而忽视经济及经济安全本身的运行特征和规律。

- **国家安全的逻辑**：通常遵循零和博弈逻辑
- **市场经济的逻辑**：基于市场的跨国经济关系往往是非零和关系
- **风险后果**：国家安全的逻辑有可能诱导经济安全的极端化
  - 这在数据流动领域已经略有体现

# 现实案例：智能网联汽车的数据主权与本地化

## 案例：特斯拉在华数据中心建设

跨国科技企业在面对国家安全逻辑时，往往需要调整其市场经济部署。

- **安全隐患的具象化**：
  - 智能汽车不仅是交通工具，更是数据的移动收集器（高清摄像头、GPS 轨迹、车主声纹等）
  - 若这些数据不受限制地跨境流出，将直接威胁所在国的地理与社会安全
- **企业的合规妥协**：
  - 2021 年，特斯拉宣布在中国建立数据中心
  - 实现数据本地化存储，将在中国大陆市场销售车辆产生的所有数据留在境内
  - 企业为了保住市场份额，必须在商业效率与东道国国家安全之间做出让步

# 跨境数据流动在个人层面的影响

## 1. 个人隐私安全问题的复杂性

相比于一般数据流动，跨境数据流动在个人层面造成的安全问题更加复杂，体现在不同国家或地区对于隐私的态度有所差异

**被广泛关注的敏感个人隐私数据包含：**

- 性别、年龄、经济状况、健康水平
- 性生活或性取向
- 种族或民族起源、政治观点
- 宗教或哲学信仰、工会成员身份
- 遗传或生物特征数据等

# 跨境数据流动在个人层面的影响

## 2. 欧盟：极其严格的数据保护

欧洲国家历来重视个人隐私安全，实行了极其严格的保护条例。

- **《通用数据保护条例》，2018**：
  - 对个人数据流出欧盟进行了严格限制，以此保护个人数据
- **充分性认定**：
  - 数据如需跨境流动，必须通过欧盟的此项认定
  - 核心要求：只有当第三国对于个人数据的保护水平达到欧盟的要求，欧盟成员国的个人数据才能进行跨境流动

# 现实案例：跨国巨头在欧盟的“隐私合规代价”

## 案例：Meta（Facebook 母公司）遭天价重罚

欧盟对个人数据流出境外的保护不仅标准极高，且执法力度空前。

- **事件背景**：
  - 2023 年 5 月，爱尔兰数据保护委员会（DPC）向 Meta 开出高达 12 亿欧元（约合 91 亿人民币）的罚单，创下《通用数据保护条例》实施以来的最高纪录
- **违规核心点（跨境数据流动）**：
  - Meta 将欧洲用户的个人数据系统性地传输并存储至美国服务器
  - 欧盟监管机构认为，美国的情报监控法律无法为欧洲用户提供与《通用数据保护条例》同等水平的隐私保护，未通过充分性认定测试
  - 在开放条件下，无视区域性隐私保护差异的跨境数据流动，将面临毁灭性的财务与声誉风险

# 跨境数据流动在个人层面的影响

**3. 英国：对特殊类别数据的高标准要求**

- **《特殊类别数据的处理指南》，2019**：
  - 为了避免可能存在的风险，要求控制者采取一切必要的预防措施来保护特殊类别个人数据（种族、信仰、生物特征等）
- **英国–欧盟《自由贸易协定》，2020**：
  - *DIGIT.3*：明确规定了隐私和数据保护的条
  - *DIGIT.7*：强调每一方承认个人有权保护隐私，并且这方面的高标准有助于增加人们对数字经济和贸易发展的信任

# 跨境数据流动在个人层面的影响

## 4. 俄罗斯：极力强调隐私安全的发展中国家代表

俄罗斯对跨境数据流动带来的隐私安全问题重视程度极高

- **强制数据本地化，2006 年法案**：
  - 公民个人数据及相关数据库必须存储在俄境内（必须设置本地服务器）
  - 公民个人数据的处理活动必须在俄境内进行
- **严厉的执法与重罚机制**：
  - *2021 年*：谷歌因违反此法案相关条款被罚款
  - *2020 年*：《俄罗斯联邦行政违法法典》修正案出台，将泄露个人数据的罚款额提高十倍

# 跨境数据流动在个人层面的影响

## 现实威胁：隐私泄露问题仍然令人担忧

尽管有法规约束，个人数据频繁成为国际黑客的窃取目标，因其包含极高价值的隐私和安全信息，泄露后危害极大。

**典型案例：Neopets 数据库泄露**

- **背景资料**：据 Termly 于 2022 年 11 月更新的《98 个最大的数据泄露、黑客和曝光事件》资料显示，单次泄露影响用户数从几十万到上千万不等
- **2022 年最大泄露事件**：
  - *时间*：2022 年 1 月至 7 月。
  - *对象*：Neopets（尼奥宠物）数据库
  - *损失*：黑客窃取了潜在的6900 万用户个人数据和 460MB 的源代码

# 跨境数据流动在个人层面的影响

**5. 中国：系统化构建数据治理的制度基础**

中国正积极细化完善相关法律法规，全面规范数据跨境传输活动

- **《数据安全法》(2021 年 6 月出台)**：
  - 首次较为系统地明确对数据处理、使用、流动的规制要求
  - 旨在加强数据安全保护和监管
- **《个人信息保护法》(2021 年 8 月出台)**：
  - 细化完善个人信息保护制度规则
  - 对个人信息处理、数据收集和使用、数据跨境传输相关活动进行全面规范

# 现实案例：统筹发展与安全的中国监管实践

## 案例：滴滴出行网络安全审查案

是中国全面适用数据合规三驾马车（网安法、数安法、个保法）的标志性案件。

- **事件回溯**：
  - 2021 年赴美上市引发数据外泄担忧，国家网信办对其启动网络安全审查
  - 2022 年 7 月，对其处以80.26 亿元人民币罚款
- **违法事实的两个层面**：
  - **个人层面（隐私）**：违法收集用户相册、过度索取权限、未准确清晰说明个性化推荐等，严重违反《个保法》
  - **国家层面（安全）**：存在严重影响国家安全的数据处理活动，规避监管
  - **结论**：数字平台在参与全球化（如赴境外上市）时，绝不能以牺牲国家数据安全和公民个人隐私为代价

# 第三节

# 跨境数据流动的全球治理

# 跨境数据流动的全球治理现状

## 当前全球治理的两大特点

1. **寻求动态平衡**：在数据安全和自由流动中寻求合理取舍
2. **国际规则未统一**：各框架尚未达成一致，缺乏全球统一标准

**全球数据治理的发展格局：**

- 总体呈现多极化和俱乐部化发展格局
- 欧美发达国家争抢全球数字经济规则的**领导权**
- 对广大发展中国家客观上形成了排挤之势

# 全球数据治理的主要原则与阵营

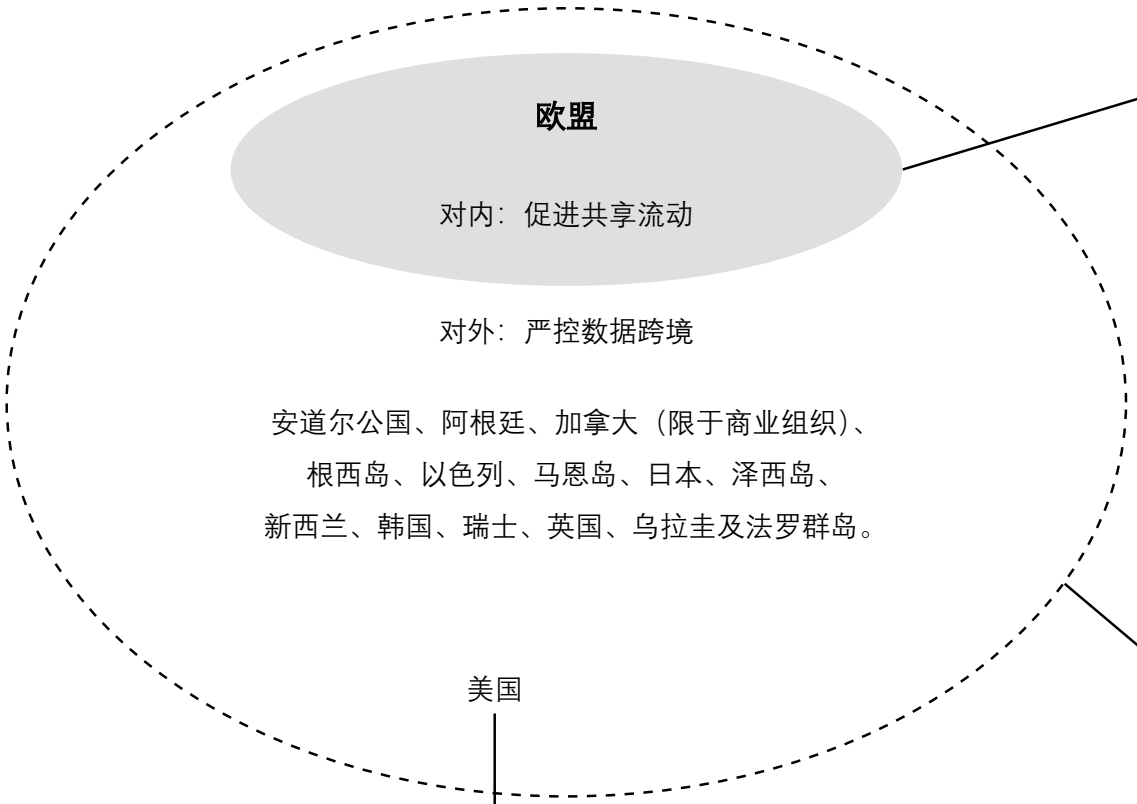
**各经济体基于自身利益，秉持不同的治理逻辑：**

- **欧盟**：倡导数据保护主义，构建高标准规则壁垒
- **美国**：倡导数据自由主义，旨在扩大数字平台优势
- **新加坡、日本等**：倡导数据发展主义，兼顾保护与流动
- **新兴国家（中、俄、印等）**：
  - *积极探索者*（如中国）：寻求安全与发展的双赢模式
  - *主权强调者*（如俄罗斯）：强调数据本地化与自主权

# 国际规则：欧盟的数据保护主义

- 核心战略：
  - 建立单一数字市场
  - 对内促进共享，对外严格管控
- 关键法案：
  - 《通用数据保护条例》，2018
  - 《数据法案》，2022
- 朋友圈机制：
  - **充分性认定**：与日、韩等国构建高标准传输协议
  - **对美态度**：2022 年达成《跨大西洋数据隐私框架》原则协议
  - **对华态度**：尚未通过充分性认定，传输需依赖替代性路径

# 欧盟主导的数据保护主义朋友圈




- 2018 年，《通用数据保护条例》
- 2018 年，《非个人数据自由流动条例》
- 2019 年，《开放数据指令》（修订）
- 2020 年，《欧洲数据战略》
- 2022 年，《数据法案》（侧重于私人部门释放数据）
- 2022 年，《数据治理法案》（侧重于公共部门释放数据）
- 2022 年，《数字市场法》《数字服务法》

2023 年之前通过 GDPR 个人数据跨境传输“充分性认定”的 14 个国家和地区

美国

- 2022 年 3 月 25 日，美欧就《跨大西洋数据隐私框架》重新达成原则性协议
- 2023 年 7 月，美国通过 GDPR 的“充分性认定”

尚未与中国建立伙伴关系

# 现实案例：欧盟充分性认定的杀伤力

## 案例：施雷姆斯二案与隐私盾失效

欧盟的数据保护主义绝非纸上谈兵，其高标准甚至曾让欧美之间的数据通道直接瘫痪。

- **事件背景**：
  - 奥地利隐私活动家 Max Schrems 起诉 Facebook，指控其将欧洲用户数据传输至美国服务器后，会被美国情报机构（如棱镜计划）监听
- **世纪判决（2020 年）**：
  - 欧盟最高法院裁定，美国国内的监控法律未能为欧盟公民提供等同于《通用数据保护条例》的保护
  - 直接废除了欧美之间赖以生存的隐私盾数据传输协议
- **商业震动与启示**：
  - 导致数千家依赖跨大西洋数据流动的跨国企业（从科技巨头到中小企业）瞬间陷入非法传输的合规危机，这充分证明了欧盟规则壁垒的**强制力与排他性**

# 国际规则：美国的数据自由主义

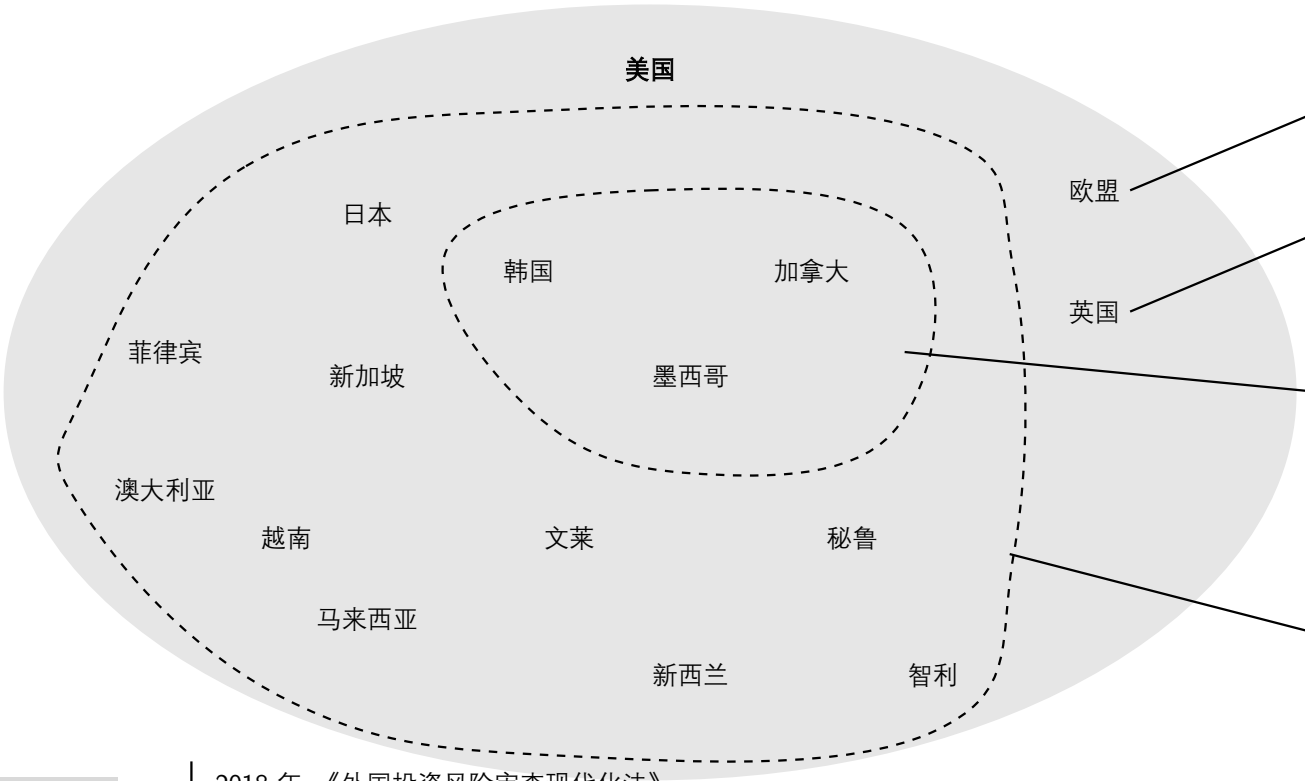
**核心主张**：减少数据流动障碍，维护美国数字产业的全球霸权

## 主导的多边开放与区域合作路径

通过贸易协定将数据自由流动条款植入国际规则：

- APEC 跨境隐私规则体系
- 《美墨加协定》
- 《韩美自由贸易协定》
- CPTPP 相关数字贸易条款

# 美国主导的数据自由主义朋友圈




2022 年，《跨大西洋数据隐私框架》

2018 年，《澄清境外合法使用数据法》

自由贸易协定伙伴关系

- 2012 年，《韩美自由贸易协定》
- 2020 年，《美国-墨西哥-加拿大协定》

国际组织多边开放关系

- 2011 年，APEC 实施跨境隐私规则
- 2016 年，《跨太平洋伙伴关系协定》
- 2022 年，全球跨境隐私规则体系宣言

美国为排除中国颁布的法案

- 2018 年，《外国投资风险审查现代化法》
- 2018 年，《加利福尼亚州消费者隐私法案》
- 2020 年，《外国投资审查法案最终规则》
- 2022 年，《出口管理条例》增加“网络安全物项”
- 2022 年，全球跨境隐私规则体系宣言

# 国际规则：美国针对中国的遏制措施

- **路径一：国内法案长臂管辖**
  - 更新《出口管理条例》等，将华为、TikTok等列为重点观察对象
- **路径二：操纵国际规则设置壁垒**
  - 2022 年修改为全球跨境隐私规则体系宣言，使其独立于 APEC
  - **借口与行动**：以信息管控为由拒绝中国审核，意图建立排华数据圈

# 国际规则：数据发展主义与中国实践

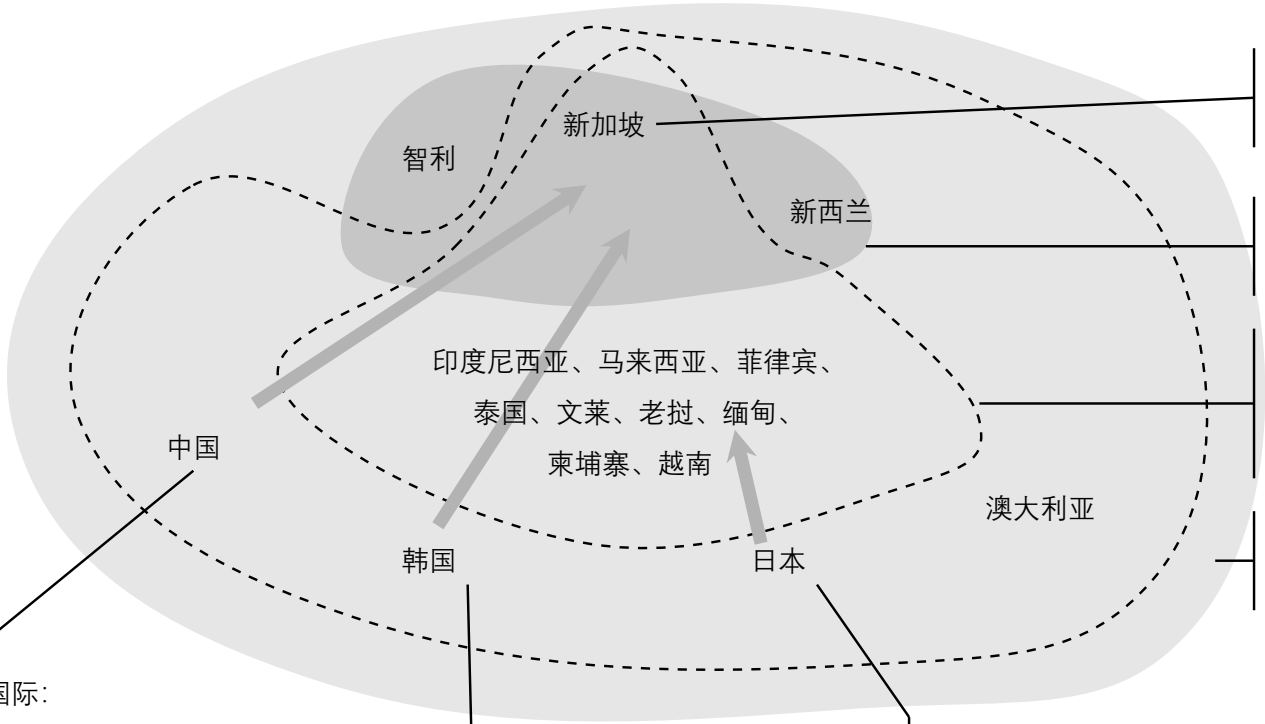
## 核心特征

以新加坡、日本为代表，强调在高水平保护下实现自由流动（如 DEPA 协定）

**中国的积极作为：**

- **法治基础**：形成以《数据安全法》为核心的自评估 + 国家评估体系
- **国际贡献**：
  - 2020 年提出《全球数据安全倡议》
  - 2021 年申请加入 DEPA（数字经济伙伴关系协定）
  - 2023 年承办第四届联合国世界数据论坛

# 以新加坡、日本等国为代表的数据发展主义朋友圈




2012 年，《新加坡个人数据保护法》（PDPA）

2020 年，《数字经济伙伴关系协定》（DEPA）

2021 年，《东盟数据管理框架》（DMF）和《东盟跨境数据流动示范合同条款》（MCCs）

2020 年，《区域全面经济伙伴关系协定》（RCEP）

国际：

2021 年，申请加入 DEPA

2021 年，申请加入 CPTPP

国内：

《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》

2020 年，《个人信息保护法》、《信用信息法》（修订案）、《信息通信网法》（修订案）

2018 年，《全面与进步跨太平洋伙伴关系协定》（CPTPP）

2019 年，日本-欧盟《个人数据跨境传输充分性框架》

# 国际规则：部分新兴国家的保留与担忧

- **俄罗斯：强硬本地化**
  - 要求数据必须在境内存储，实行白名单式流出政策
- **印度的主权抗议**：
  - 2019 年 G20 峰会：反对基于信任的数据自由流动方案
  - 观点：数据是国家主权的一部分，发展中国家应保留监管权
  - 行动：拒绝签署《大阪数字经济宣言》

# 现实案例：新兴国家的数据主权武器化

## 案例：印度封禁数百款中国 App 事件

发展中国家在面对外部数字平台扩张时，常以国家安全与数据主权为由进行反制。

- **行动过程**：
  - 自 2020 年起，印度政府以损害印度主权、国防及国家安全为由，分批次封禁了包括 TikTok、微信、UC 浏览器在内的 300 余款中国背景的应用程序
- **背后的治理逻辑**：
  - **政治考量**：防范本国公民的地理位置、消费偏好、社交网络等核心数据流向被其视为竞争对手的国家
  - **经济考量**：通过切断外来巨头的数据获取渠道，为印度本土数字企业（及部分受其扶持的美国企业）腾出市场空间
- 在缺乏统一全球规则的当下，数据主权极易被泛化为贸易保护主义的新手段

# 跨境数据流动治理存在的问题

1. **传统贸易规则失灵**：
   - WTO 现有框架难以覆盖复杂的实体产业数据，缺乏专项规制
2. **治理方案缺乏国际共识**：
   - 治理呈现碎片化态势，规则由少数大国主导
   - 广大发展中国家的数字发展权面临被剥夺的风险

# 跨境数据流动治理存在的问题

3. **个别国家的双重标准**：
   - 对己方要求绝对自由（长臂管辖），对他国要求强制本地化（针对 TikTok）

4. **大型平台的负面安全事件**：
   - **谷歌**：因透明性问题被罚 4 亿元
   - **Meta**：2023 年因非法数据传输被重罚 91 亿元人民币

# 现实案例：数据治理中的双重标准现场

## 对比案例：美国的《云法案》vs. 围剿 TikTok

在数据流动的全球博弈中，部分大国的核心诉求并非规则公平，而是我的绝对控制。

- **对己方：极度扩张的长臂管辖**
  - 2018 年出台《云法案》：规定只要受美国管辖的企业（如微软、苹果），无论其数据存储在世界上哪个国家的服务器上，美国政府均有权依法调取
  - *逻辑*：我的企业在全球的数据，我都要看
- **对他国：极度保守的数据本地化**
  - 2023 年–2024 年：以数据被外国政府获取为由，在国会听证会上对 TikTok 轮番施压，最终通过法案要求其强制出售否则封禁
  - *逻辑*：外国企业在美国收集的数据，绝对不能出境

# 结语：中国在跨境数据治理中的主张

**核心理念：拥抱数据，共赢未来**

中国愿同世界各国一道，在全球发展倡议框架下深化国际数据合作。

- 以数据之治助力落实联合国 2030 年可持续发展议程
- 构建开放、公平、非歧视的国际合作格局
- 维护全球数据供应链安全，促进共同进步

# 本章总结：逻辑架构与核心特征

## 核心逻辑：从要素流动到全球治理

本章通过开放—安全—治理三位一体的逻辑，探讨了数据要素在全球化背景下的运行规律。

- **开放特征**：数据流动突破了封闭经济的资源约束，通过网络效应（梅特卡夫定律）实现价值倍增
- **多维属性**：区分了商业数据、原始数据与数据产品，明确了数据作为服务贸易新增长极的地位
- **主要趋势**：全球数据流规模激增，2005 年来增长数百倍，但地理分布呈现高度的极化与中心—外围特征
- **安全性考量**：个人层面的隐私权保障与国家层面的经济安全构成了开放的边界

# 本章总结：核心悖论与中国方案

- **核心悖论：效率—安全—公平**
  - 数据经济在开放条件下难以达到完美均衡，效率追求往往让位于安全诉求
  - 发达国家凭借先发优势垄断规则，发展中国家面临数字发展权被挤压的风险
- **治理格局：碎片化与俱乐部化**
  - 全球治理尚未形成统一共识，呈现出保护主义（欧）、自由主义（美）与发展主义（新、日）并存的碎片化格局
- **中国战略位势：从规模优势走向治理引领**
  - **位势**：中国已是全球第二大数据产出国，2025 年有望成为全球最大数据区域
  - **主张**：坚持数据发展主义，完善国内合规三法，积极参与国际规则谈判
  - **愿景**：以数据之治助力可持续发展，构建开放共赢的国际合作格局

# 谢谢大家！