聚焦数字经济监管：如何保护个人信息？

东方证券 ORIENT SECURITIES

研究结论

- 出台数据监管政策有助于为数字经济打造良性的发展环境。2020 年 12 月中央经济工作会议指出，要完善平台企业垄断认定、数据收集使用管理、消费者权益保护等方面的法律规范。要加强规制，提升监管能力，坚决反对垄断和不正当竞争行为。在这个问题上，**海外发达国家（尤其是欧盟）监管措施已经趋于成熟，近年来推出了一系列法律法规规范互联网平台在数据收集、使用和保留等方面的行为，有望成为中国完善数据监管的参考。**
- **欧盟在个人信息保护和数字经济的立法上走在前列，一方面是由于欧盟一贯重视隐私保护，将其视为基本人权，但更重要的原因在于欧盟本土的数字经济平台稀缺，谷歌、脸书和推特等美国科技巨头垄断了欧洲的数字市场，欧盟希望能够通过立法的方式增强中小平台在数字市场的竞争力。**在此背景下，欧盟在 2016 年通过了《通用数据保护条例》，之后又先后出台《数字服务法案》和《数字市场法案》：（1）《通用数据保护条例》扩大了数据主体的各项权力（包括数据访问、纠正、删除和限制），也限定了企业收集、处理数据时的行为，此外，全球关于数据监管的法规几乎都涉及了“数据主权”，在这一条例中体现为对数据的长臂管辖；（2）《数字市场法案》具有反托拉斯法的性质，大型平台应允许其商业用户在这些平台以外的平台进行推广和签订合同、禁止限制消费者前往第三方平台、禁止将自身产品排在第三方平台之前，达到为中小平台打造更为公平的数字经济竞争环境的目的；（3）《数字服务法案》聚焦于用户、平台和公共机构职责的再平衡，将中间服务、托管服务、在线平台和超大型在线平台区分开来，不同规模的企业承担与其能力相匹配的义务。
- **以 FAANG（Facebook，苹果，亚马逊，奈飞和谷歌）为代表的美国科技公司在全球范围内获取利润，因此出于产业利益的考量，美国对数据监管颇为宽松，以行业自律为主，辅之以政府监管**，其中政府监管部门包括联邦贸易委员会、联邦通信委员会和州监管机构等。
- **中国已总体建立了个人信息保护机制和数据监管机制，但还不足以适应高速发展的数字经济**，个人信息泄露、平台违规收集和处理信息，利用海量数据形成垄断等现象多有出现。**此外，数据安全正成为国家安全的一部分，无论是欧盟的《通用数据保护条例》还是美国的《国家安全与个人数据保护法》提案，都对“数据主权”做出定义，这也要求我国采取对应的措施。**2020 年 10 月，十三届全国人大常委委员长会议提请了审议《个人信息保护法（草案）》的提案，这将成为中国个人信息保护领域的“基本法”。具体来看这一草案：（1）惩罚力度与欧盟《通用数据保护条例》不相上下，彰显了中国对于数据监管的决心；（2）与世界各国、各地区的主流规定一致，该草案采取了地域和公民管辖相结合的适用范围，能够更好地保护我国“数据主权”；（3）展望未来，预计在一些细分领域我国还将进一步完善个人信息的针对性保护措施，例如未成年人的个人信息收集、以及金融领域的征信数据等。

风险提示

- 跨国公司的数据监管涉及国家之间的博弈，具体政策落地存在难度；
- 平台数据监管的执行力度不及预期。

报告发布日期 2021 年 01 月 04 日

证券分析师 陈至奕
021-63325888*6044
chenzhiyi@orientsec.com.cn
执业证书编号：S0860519090001

证券分析师 孙金霞
021-63325888*7590
sunjinxia@orientsec.com.cn
执业证书编号：S0860515070001

证券分析师 王仲尧
021-63325888*3267
wangzhongyao1@orientsec.com.cn
执业证书编号：S0860518050001

联系人 陈玮
chenwei3@orientsec.com.cn

相关报告

聚焦数字经济监管：数字税会来吗？	2021-01-03
“十四五”的细节之三：迈向数字乡村 2.0，困难与增量何在？	2020-11-18
“十四五”的细节系列之二：什么是产业基础再造工程？	2020-11-10
“十四五”的细节系列之一：从新型举国体制到揭榜挂帅	2020-11-09

动态跟踪

【宏观经济·证券研究报告】

2020 年 3 月《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》正式出台，数据要素与传统的生产要素——土地、劳动力、资本和技术要素一同列出，原表述为“加强数据资源整合和安全保护。探索建立统一规范的数据管理制度，提高数据质量和规范性，丰富数据产品。研究根据数据性质完善产权性质。制定数据隐私保护制度和安全审查制度。**推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护**。”

出台数据监管政策有助于为数字经济打造良性的发展环境。互联网已经成为全球性的商业和交流平台，且不断向个人生活的方方面面延伸。2020 年 12 月中央经济工作会议指出，**要完善平台企业垄断认定、数据收集使用管理、消费者权益保护等方面的法律规范。要加强规制，提升监管能力，坚决反对垄断和不正当竞争行为。金融创新必须在审慎监管的前提下进行。**

海外发达国家（尤其是欧盟）在数字平台监管和个人数据保护方面走在前列，近年来推出了一系列法律法规规范互联网平台在数据收集、使用和保留等方面的行为，有望成为中国完善数据监管的参考。

海外如何监管数据?

数字平台的发展历程仅有短短几十载，多数国家的监管框架尚未完善，但立法是实施监管的第一步。20 世纪 70 年代以来，许多国家相继制定了个人信息和数据保护方面的法律，其中欧盟采用了“综合立法”的模式，美国则采用“分散立法”和“行业自律”相结合的模式。

欧盟：以个人数据保护对抗美国公司垄断

欧盟在个人信息保护和数字经济的立法上走在前列，一方面是由于欧盟一贯重视隐私保护，将其视为基本人权，但更重要的原因在于欧盟本土的数字经济平台稀缺，谷歌、脸书和推特等美国科技巨头垄断了欧洲的数字市场，欧盟希望能够通过立法的方式增强中小平台在数字市场的竞争力。

在此背景下，欧盟在 2016 年通过了《通用数据保护条例》（General Data Protection Regulation，简称 GDPR），该条例被视作数字时代用户个人数据保护的里程碑，或将为其他国家的数字时代个人数据保护提供借鉴。之后的 2020 年 12 月，欧盟出台《数字服务法案》（Digital Services Act，简称 DSA）和《数字市场法案》（Digital Market Act，简称 DMA）两项法案，明确了数字平台监管的法律框架，目标有二，一是创建一个更安全的数字空间，保护所有数字服务用户的基本权利，二是建立一个公平的竞争环境，以促进欧洲市场和全球市场的创新。

通用数据保护条例

GDPR 于 2018 年 5 月生效，取代了欧盟在 1995 年出台的《数据保护指令》。该法案对个人数据和隐私作出了规范，取回了个人对于自身数据的控制，以及限制欧盟个人资料向境外的传输。**与 1995 年的《数据保护指令》相比，GDPR 扩大了数据主体的各项权力（包括数据访问、纠正、删除和限制），也限定了企业收集、处理数据时的行为。**如果发生数据泄露，数据控制者需要在泄露后的 72 个小时内通知主管监管机构。

全球关于数据监管的法规几乎都涉及了“数据主权”，在 GDPR 中体现为对数据的长臂管辖。GDPR 的管辖权非常宽泛，凡是欧盟公民的个人资料都涵盖在内（无论数据在哪里处理）。

表 1:《数据保护指令》与《通用数据保护条例》的对比

个人权利	数据保护指令	通用数据保护条例
访问请求	个人有权了解其个人数据是否被处理以及怎么被处理	数据主体应该有权访问其个人数据、数据地来源、所涉数据地类别等
拒绝权	个人可以在拥有令人信服的合法理由的情况下以及直接营销的情况下拒绝处理个人数据	在以下情景下个体有要求删除其个人数据的权力: ● 有关数据对于收集或者处理数据的目的而言已经不是必要的; ● 数据主体撤回了处理其数据所依据的同意; ● 数据主体依法反对有关处理; ● 数据被非法处理; ● 为遵循欧盟或成员国规定的法定义务必须对数据进行删除; ● 数据收集与向儿童提供信息社会服务相关。
修正或删除权（“被遗忘权”）	个人可以完善和修正不完整和不准确的数据	数据主体有权纠正与其相关的个人数据，或者有权要求将其不完整的数据补充完整
限制权	无限制处理的权力	数据主体在对数据的准确性提出质疑、数据处理不合法、基于处理目的已不再需要有关数据或者数据主体反对有关处理的情况下有权限制对个人数据的处理
删除权	如果符合数据保护原则，个人有权要求删除其个人数据，但是该权力十分有限	GDPR 扩大了删除权的使用范围，比如个人撤回处理许可且无相关法律规定支持后续处理时，可以行使删除权
数据可携权	没有明确将数据可携权作为数据主体的权力	个人可以要求将数据控制者所掌握的个人数据提供给自己或其他控制者

数据来源:《数据保护指令》,《通用数据保护条例》，东方证券研究所

数字市场法案

《数字市场法案》（DMA）具有反托拉斯法的性质，针对具有市场影响力的大型数字平台（谷歌、脸书、亚马逊、TikTok 等），通过规定这些大型平台**应允许其商业用户在这些平台以外的平台进行推广和签订合同、禁止限制消费者前往第三方平台、禁止自身产品比第三方平台排名更靠前**等，达到为中小平台打造更为公平的数字经济竞争环境的目的，从而促进数字经济的创新和长期繁荣发展。该法案对未遵守规定的企业制定了严格的惩罚措施，包括最高可达公司全球年营业

额 10%的罚款，最高可达日均营业额 5%的定期罚款，甚至是出售和剥离（部分）业务等非罚款性质的惩罚措施。

表 2:《数字市场法案》的具体内容

	规定	具体内容
适用对象	在数字市场中扮演“守门人”（gatekeeper）角色的大型在线平台	具有强大的经济地位：公司过去三个财政年度在欧洲经济区（EEA）实现的年营业额大于等于 65 亿欧元；或者在过去一个财政年度其平均市值或等值的公平市值至少达到 650 亿欧元，并在至少三个成员国提供核心平台服务（谷歌等公司满足该条件）
		具有强大的中介地位，控制着商业用户通往最终消费者的重要通道：公司在最近一个财年，核心平台服务在欧盟的月活跃终端用户超过 4500 万，并且在欧盟建立的年活跃商业用户超过 1 万（Facebook，YouTube，Twitter 和 TikTok 等均满足条件）
		在市场上拥有(或预期拥有)根深蒂固和持久的地位：公司在过去三个财政年度中的每个年度都符合其他两个标准
被认定为“看门人”的企业需要遵守的规则	需要做到的行为	在某些特定情况下，允许第三方与“守门人”自身的服务进行互动
		允许其商业用户访问其在使用“守门人”平台时生成的数据
		为在其平台上投放广告的公司提供必要的工具和信息，以使广告商和发布者能够对“守门人”托管的广告进行自己的独立验证
		允许其商业用户在“守门人”之外的平台推广并与客户签订合同
	禁止的行为	**将自身提供的服务和产品排在第三方提供的相似服务或产品之前**
		限制消费者链接到“守门人”平台外获得服务
		组织用户卸载任何预装软件或应用程序
未遵守规定的惩罚	罚款额最高可达公司全球年营业额的 10%	
	定期罚款最高可达日均营业额的 5%	
	针对“守门人”系统性的违规行为，可能会在调查后对施加其他补救措施，这些补救措施必须与所犯的违法行为相称。如果有必要且作为最后的选择，可以施加非财务的额外措施。**这些措施可以包括行为和结构上的补救措施，例如剥离（或部分剥离）企业**	

资料来源：ec.europa.eu，东方证券研究所

数字服务法案

《数字服务法案》（DSA）则聚焦于用户、平台和公共机构职责的再平衡，将公民置于中心位置，目的是更好地保护消费者，为在线平台建立高度透明和明确的责任框架，以及促进创新、增长和竞争力。DSA 将提供网络基础结构的中间服务（互联网访问提供商、域名注册商）、托管服务商（云和网络托管服务提供商）、在线平台（应用程序商店、社交媒体平台等）和超大型在线平台（覆盖欧洲 1.5 亿消费者中的 10%以上的平台）区分开来，不同规模的企业承担与其能力相匹配的义务。其中超大型平台在传播非法内容和社会危害方面有特殊的风险，同时也具备承担更多义务的能力，因此其义务要超过其他三类。**欧盟希望通过 DSA 打击线上非法产品、服务或内容，为用户提供有效保障，增强在线平台各种维度上的透明度（包括提供建议的算法），等等。**

表 3:《数字服务法案》下不同类型的平台需要承担的义务

	中间服务	托管服务	在线平台	超大型在线平台
报告透明度	√	√	√	√
适当考虑基本权利的服务条款要求	√	√	√	√
联络点以及必要时的法定代表人	√	√	√	√
配合政府当局的要求	√	√	√	√
向用户提供信息的通知，行动和义务		√	√	√
投诉和补救机制以及庭外争端解决			√	√
值得信赖的举报人			√	√
反对滥用通知和反通知的措施			√	√
审核第三方供应商（“KYBC”）的凭据			√	√
在线广告面向用户的透明度			√	√
报告刑事罪行			√	√
风险管理义务和合规官			√	√
外部风险审计和公共责任				√
推荐系统的透明度和用户选择信息的方式				√
与当局和研究人员共享数据				√
行为守则				√
危机应对合作				√

数据来源：ec.europa.eu，东方证券研究所

美国：行业自律为主，相对宽松

美国在数字信息领域的发展位居世界前列，以 FAANG（Facebook，苹果，亚马逊，奈飞和谷歌）为代表的科技公司在全球范围内获取利润，因此**出于产业利益的考量，美国对数据监管颇为宽松。**

在此背景下，美国在全国层面上尚未有完善的数据监管法律体系，主要是《联邦贸易委员会法》和《儿童在线隐私权保护法》等，前者限制了不公平竞争和欺诈行为，后者禁止收集 13 岁以下儿童的个人信息，立法时间均较为久远。

从监管体系来看，美国数据监管以行业自律为主，辅之以政府监管，其中政府监管部门包括联邦贸易委员会、联邦通信委员会和州监管机构等。

图 1：美国与信息保护相关的法律法规

数据来源：中国信通院互联网法律研究中心，东方证券研究所

近来由于数据泄露事件频发，且美国加大了对于大型科技公司的反垄断调查（包括利用数据进行不公平竞争），数据监管的立法工作也在逐步推进，但全国层面上迟迟没有进展。

加州消费者隐私法

2018 年 6 月，美国加州通过了《加州消费者隐私法案》（The California Consumer Privacy Act，简称 CCPA），该法案于 2020 年 1 月 1 日起正式实施。CCPA 旨在提高加州居民对“企业对个人信息的收集以及个人信息如何成为企业财产”的关注，要求各机构更加透明地收集、处理和利用用户数据，并赋予加州居民对企业收集、处理、分享数据的知情权。

CCPA 主要赋予了数据主体以下几方面的权利：

- 要求企业公开其个人数据收集及出售情况；
- 要求企业提供过去 12 个月内收集的个人可识别信息的副本；
- 要求企业删除所收集的所有个人身份信息；
- 要求企业不得出售其个人数据。

《国家安全与个人数据保护法》提案

2019 年 11 月，共和党参议员 Josh Hawley 向参议院提交了《国家安全与个人数据保护法》（National Security and Personal Data Protection Act of 2019），目前该法案提交至商业、科学和运输委员会，其正式生效还需要参众两院通过和总统签署。**该提案除了对企业提出了数据安全的要求外，还着重强调了“数据主权”，值得注意的是中国和俄罗斯在提案中被单列为特别关注国家**：

- 特别关注企业（在州际贸易和涉外贸易中提供基于数据的在线服务（如网站、互联网应用）或提供基于数据的在线服务并可能影响州际贸易或涉外贸易的）在数据收集方面实行“最小化原则”，即仅能收集为运营网站、服务或应用所必需的最小限度的用户数据；

- 禁止特别关注企业将收集的用户数据用于次要用途，含定向广告、不必要的共享、以及发展人脸面部识别技术；
- 赋予用户访问权和删除权；
- 禁止向特别关注国家（中国、俄罗斯）直接或间接传输任何用户数据或可能被用于破译该数据的信息；
- 禁止在特别关注国家境内的服务器或存储设备上存储在美国境内收集的个人用户数据或可能用于破译该数据的信息；禁止在位于美国境外的服务器或存储设备上存储任何美国公民或居民的用户数据或用于破译该数据的信息；
- 违法将可能处以不超过 5 年的监禁和罚款。

中国实行数据监管的路径：从个人信息保护法到其他细分领域

中国已总体建立了个人信息保护机制和数据监管机制，但还不足以适应高速发展的数字经济，个人信息泄露、平台违规收集、处理信息，利用海量数据形成垄断等现象频发。作为信息时代的生产要素，数据需要被妥善地纳入监管，包括合理地保护个人信息，以及监管科技企业的数据收集、处理行为。此外，数据安全正成为国家安全的一部分，无论是欧盟的 GDPR 法案还是美国的《国家安全与个人数据保护法》提案，都对“数据主权”做出定义，这也要求我国采取对应的措施。

欧盟的 GDPR 推出后遭到诸多的匹配和质疑，这些声音在我国加强数据监管的过程中也会出现。首先，企业满足 GDPR 的要求势必将提高企业成本，而这些成本将转嫁给消费者，其次，对数字收集和处理的限制将阻碍企业和数字行业的快速发展。美国著名科技创新智库美国信息技术与创新基金会（Information Technology and Innovation Foundation，简称 ITIF）发文指出，GDPR 的严格标准将大幅提高公司的合规成本，提高消费者的花费，减少在创新上的投资，最终将损害美国数字生态系统和消费者的利益，进一步的，其认为合理的数据保护水平可以促进消费者对数字行业的信任并加快行业发展，但没有证据表明进一步加强监管能够增强额外的信任或鼓励更多的应用。

中国关于信息的法律建设已历经 10 余年，在信息保护方面初步构建了相关法律体系，但改善空间仍然巨大。现行法律法规包括 2017 年 6 月正式实施的《网络安全法》、2018 年 5 月正式实施的