

Decoding “Important Data”: Through the Lens of National Security and Global Competitiveness

Author: YANG, Jianyuan WU, Dan WEI, Yiwen ZHAO, Yaze

一、我国正在迎来重要数据的监管落地

“重要数据”这一概念早在2016年《网络安全法》中首次提出，并在2021年《数据安全法》中结合数据分类分级保护制度予以进一步规定，但“重要数据”的范围和界定经历了较长时间的不确定和探索期。**近年尤其今年以来，随着各领域的立法及实践纷纷推进，我国正在迎来重要数据的监管落地。**

我国以数据出境监管为先锋，并逐渐完善重要数据立法。2022年《数据出境安全评估办法》对重要数据作出定义，而2024年《促进和规范数据跨境流动规定》健全了重要数据的出境规则。2021年《网络数据安全条例（征求意见稿）》细化了重要数据的认定标准，并规定了重要数据的特殊保护要求；而2024年8月底国务院审议通过该条例草案，即将从行政法规层面明确重要数据的监管要求。

多个部门逐步推进重要数据的识别与行业监管，自由贸易试验区亦开始推进重要数据的识别与出境监管，为监管落地做实质准备。目前，工信、汽车、医疗、金融、能源、航空、教育等重点行业均已开展重要数据识别工作，并逐步形成成果。此外，汽车、工信、自然资源、金融等多个行业的监管机构已公开发布专门针对数据安全管理的部门规章或其征求意见稿，其中包括重要数据的特殊保护要求。此外，《促进和规范数据跨境流动规定》允许自由贸易试验区（简称“自贸区”）自行制定需要纳入监管的数据清单，包括重要数据清单。天津自贸区、北京自贸区均于今年发布了重要数据的识别规则及数据清单，逐渐明确了需要申报出境安全评估的数据范围。

中外经济往来需求成为尽快界定重要数据范围、明确监管方向的催化剂。一方面，我国已意识到重要数据范围模糊可能影响我国对外开放、引进外资，例如，国务院办公厅2024年《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》中提出，“健全数据跨境流动规则。科学界定重要数据范围”。**另一方面，重要数据概念不清已在国际上引起讨论。**在2024年8月27日的中欧数据跨境流动交流机制第一次会议上，欧盟对中国重要数据概念的模糊性、适用的广泛性、及跨境流通的困难提出担忧，并表示这可能导致欧洲投资者对中国的信心下降。在中美博弈的基本格局之下，保持与欧盟的良好合作对我国意义重大，而欧盟的态度或将助推我国加快界定重要数据。

二、如何理解重要数据的监管逻辑：国家安全与国际竞争力

相较于在全球范围内普遍受到保护的“个人信息”，我国的“重要数据”似乎有些特立独行。对于重要数据监管，直接受监管的中国企业可能感到困惑，而间接受影响的外国企业也在提出疑问。

要真正理解重要数据，不能囿于数据保护的视角，而要站在更宏观的立场，看到其背后的国家安全与国际竞争力的考量。基于此，我们既能更好地理解我国对重要数据的监管逻辑，也会发现其他国家的监管工具同样意在**守护国家安全、维护竞争优势**。即，在本国企业出海、外企外资入境的双向流动中，一国势必必要保障本国的国家安全和核心优势，并维持本国企业在国内市场及海外市场的竞争力。

新型汽车产业正是一个典型例证。以新能源汽车、智能网联汽车为代表的新型汽车产业，是近年来经济发展的新赛道、大国竞争的角力场，而中国在新型汽车领域的领先优势可能颠覆西方在传统汽车领域的优势。对此，各国均从自己的“监管工具箱”中选出趁手的工具，以加强对新型汽车及其相关技术与数据的进出口监管，从而守护国家安全、维护竞争优势。例如：

1. 中国--重要数据出境安全评估：重要数据出境应提交监管机构进行安全评估，2021年《汽车数据安全管理若干规定（试行）》率先列举了重要数据清单、并确立了年度监管报送机制，而最新的《中国（北京）自由贸易试验区数据出境管理清单

（负面清单）（2024版）》（简称“《北京自贸区负面清单》”）进一步明确并扩大了汽车行业的重要数据清单。我国以重要数据及其出境为抓手，加强了对汽车行业尤其是涉外业务的监管。

2. 美国--ICTS国家安全调查：美国商务部今年发布拟议规则制定预先通知，计划对嵌入“外国对手”的信息通信技术或服务（如嵌入中国软件）的网联汽车交易进行ICTS国家安全审查，以应对其中的美国国家安全风险。有消息称，美国商务部拟禁止在美国境内的自动驾驶及网联汽车中使用中国软件，并限制中国公司在美国道路上测试自动驾驶汽车。

3. 欧盟--反补贴调查：欧盟委员会去年发起了针对中国电动汽车的反补贴调查，认为原产中国的电动汽车因政府补贴，能够以低价在欧盟快速扩大市场份额，伤害了欧盟的汽车产业。对此，欧盟委员会拟对中国电动汽车征收17.4%~37.6%的临时反补贴税。为克服反补贴税可能带来的价格劣势，中国企业可能需要在欧盟境内投资建厂、直接制造电动汽车。

由此可见，重要数据是中国保护国家安全、增强国际竞争力的方式选择，而美欧采用的供应链管理、反补贴亦能实现类似的监管目的。在全球化与国际竞争局势下，各国对新型汽车、人工智能等重点产业领域的监管措施可能不断演化升级，并随着各国角力而动态发展。例如，当外国针对我国特定行业频繁采取限制性措施时，我国可能通过自有的监管措施予以回应及牵制。但万变不离其宗，各国都希望在参与国际合作的同时，守护本国的国家安全，并保留具有核心竞争力和国家安全影响力的技术及数据。

三、预判重要数据保护的特征和趋势

我国的重要数据监管，不止于数据保护，也不止于国内监管。只有从国家安全与国际竞争的宏观视角，才能看清重要数据的本质与底层逻辑。在策略上，我国的重要数据监管将进一步强化风险路径——围绕国家安全与国际竞争层面的风险，对高风险领域进行强监管，对低风险领域进行弱监管，以免给经济发展、企业合规造成过高成本。

（一）不同行业的差异性监管

从行业维度，不同行业之间的差异性监管逐渐显现，究其根源是各行业对国家安全、产业竞争的影响力不同。对于汽车、人工智能等新时代引擎行业，中美欧等主要国家正在这些领域加强竞争与发展，因此，这些行业领域的重要数据范围将扩张，甚至整个行业呈现出重要数据的特征。

1. 汽车：2021年《汽车数据安全若干规定（试行）》首先在我国部门规章层面提出了具体、明确的重要数据清单，而最新的《北京自贸区负面清单》在此基础上进一步明确并扩大了汽车行业的重要数据清单，覆盖范围非常广泛（详见下表）。

《汽车数据安全若干规定（试行）》	《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》	
	数据子类	数据基本特征与描述
（一）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；	1. 涉及军事管理区、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；在向政府机关、军工企业及其他敏感重要机构提供车联网信息服务过程中产生的不宜公开信息。	包括但不限于：车辆研发、车辆测试、车联网信息服务场景。包括重要敏感区域的车辆位置信息精确坐标、行踪轨迹、地址等；军工企业较长一段时间内的联网汽车相关的信息等数据。
（二）车辆流量、物流等反映经济运行情况的数据；	2. 车辆流量、物流等反映经济运行情况的数据。	包括但不限于：车辆研发、车辆测试、车联网信息服务场景。包括路面交通流量数据、物品流转精确路径信息等。
（三）汽车充电网的运行数据；	3. 能够反映一定区域内汽车充电网运行情况的数据。	包括但不限于：充电站服务场景。包括充电桩站位置信息、使用状态、计费 and 支付信息、充换电车辆统计信息、站点统计、分布信息等数据。
（四）包含人脸信息、车牌信息等的车外视频、图像数据；	4. 包含人脸信息、车牌信息、路牌信息等的车外视频、图像数据。	包括但不限于：车辆研发、车辆测试、车联网信息服务场景。包括通过摄像头、雷达等传感器从车外环境采集的未达到国家有关规定处理要求的人脸、车牌、路牌等车外视频和图像数据。

/	5. 包含车辆远程操控、车辆工况等的关键车联网信息服务数据。	包括但不限于：车联网信息服务场景。包括身份鉴权信息、车辆远程操控类信息（远程启动、远程开关空调、远程车窗、远程车门解闭锁、远程充电）、车辆工况类数据（电控单元的运行状态、系统工作参数等相关信息、电控单元诊断数据）、涉车服务类数据（应用程序使用数据）、车联网服务平台基础属性数据（车辆日志数据）、车辆外部环境感知数据（车辆、电信运营商、云平台、行人之间的通信数据和连接数据，依法偏转后的车辆位置信息）等。
/	6. 包含车辆控制等在线升级数据；包含电控单元等售后数据。	包括但不限于：OTA 在线升级、售后场景。其中 OTA 在线升级场景包括 OTA 类型、OTA 主控模块、联网终端、可远程升级系统、升级涉及的系统零部件、加密方式、下载更新状态、设备信息、协议版本、软件版本、固件版本、固件配置信息、服务请求和处理系统信息、车端物联网卡号相关数据、升级中与安全节能环保防盗等有关的技术参数；售后场景包括电控单元信息、固件配置信息、重编程相关数据、诊断仪数据、车辆钥匙（含 APP）相关数据等。已在工信部备案，并通过相关安全技术措施处理，可确保升级包数据不被篡改的情形除外。
/	7. 可能被利用实施对车联网关键设备、系统组件供应链的破坏，以发起高持续威胁等网络攻击相关的数据；可一定程度反映交通、运输等行业性关键信息基础设施网络安全保护情况，可被利用从而对车联网关键信息基础设施实施网络攻击的数据；涉及车联网信息服务的关键信息基础设施相关数据。	包括车联网领域重要客户清单、未公开的车联网关键信息基础设施运营者采购产品和服务情况、未公开的汽车及车联网产品的重大漏洞等；反映交通、运输等行业性关键信息基础设施以及车联网关键信息基础设施网络安全方案、系统配置信息、核心软硬件设计信息、系统拓扑、应急预案等；与车联网信息服务有关的关键信息基础设施规划建设、运行维护、安全保障、流量监测等数据，以及其他关键信息基础设施供应链、关键业务链相关的数据等。
(五) 涉及个人信息主体超过 10 万人的个人信息；	/	/
(六) 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。	/	/

2. 人工智能：在人工智能训练数据方面，《北京自贸区负面清单》直接将“**与行业竞争力相关**的高价值敏感数据”作为界定重要数据的一项标准，其辐射范围非常广泛，“包括但不限于：模型训练、算法开发、产品测试场景。包括人工智能的算法源代码、关键组件数据、控制程序、基础模型数据、数据挖掘分析数据、测试数据等”。

3. 零售：作为对比，对于零售与现代服务业，《北京自贸区负面清单》并未界定任何重要数据。

（二）个人信息的分层监管

个人信息也不止于个人权益保护的微观视角，而呈现出分层监管、宏观把握的趋势。从国家安全与国际竞争力的视角，需要侧重监管的个人信息的数量级进一步提高，且在不同的细分领域和业务场景中呈现出不同的权重。

1. 个人信息如何构成重要数据

我国正在逐渐明确个人信息构成重要数据的判断标准，主要取决于个人信息的敏感度与数量级。此前，我国数项规定提及“100万个人信息”的概念，而业内猜测这是否构成重要数据。今年陆续发布的《中国（天津）自由贸易试验区企业数据分

类分级标准规范》《中国（北京）自由贸易试验区数据分类分级参考规则》，均提出了个人信息如何构成重要数据的统一识别规则：

- » **一般个人信息**：**1000万人**以上个人信息（不含敏感个人信息）；
- » **敏感个人信息**：**100万人**以上敏感个人信息；
- » **特殊敏感个人信息**：**10万人**以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的敏感个人信息。

2. 个人信息出境的数量门槛

在数据出境方面，作为出境个人信息的合规机制，相较于标准合同及认证，安全评估具有更强的监管属性与国家安全考量。**我国已数次更新适用数据出境安全评估的个人信息数量级，整体趋势是数量门槛逐渐提高、数量规则逐渐精细化。**这一方面降低了中外企业跨境运营的合规成本，促进了我国参与全球化经济；另一方面，这也将监管资源倾斜至真正有风险的领域及场景。

具体而言，2022年《数据出境安全评估办法》项下，需要安全评估的个人信息数量门槛约为“个人信息**10万人/2年**、敏感个人信息**1万人/2年**”，而今年《促进和规范数据跨境流动规定》提高至约“个人信息**100万人/1年**、敏感个人信息**1万人/1年**”。最新的《北京自贸区负面清单》则在医药、民航、零售与现代服务业、人工智能等行业领域，进一步细化业务场景及数据类型，并分门别类地提高了数量门槛，其中最高的是零售与现代服务业中会员管理场景的个人消费者会员信息，约为“个人信息**500万人/1年**、敏感个人信息**100万人/1年**”。

这与美国的监管思路有共通之处。美国在《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》及其《拟议规则制定预先通知》中，为不同类别的敏感个人信息设置相应的数量门槛（如下表所示），并基于对国家安全重大风险的考量，加强对批量敏感个人信息的监管。（解读文章详见[《海问·观察 | 以“国家安全”之名：美国政府如何限制敏感数据流向中国？》](#)）

范围	人类基因组数据	生物识别标识符	精确地理位置数据	个人健康数据	个人财务数据	受覆盖的个人识别符
低	100	100	100	1,000	1,000	10,000
高	1,000	10,000	10,000	1,000,000	1,000,000	1,000,000

（三）监管合规中的国家博弈

国家安全与国际竞争力已成为大国立法及监管行动中的核心考量。各国的监管工具虽然外观不同、模式相异，却往往有着守卫国家安全、在科技竞争中突围的共同底色。例如，美国外国投资委员会（CIFUS）的外国投资交易审查聚焦关键技术、关键基础设施、敏感个人信息，无不关切国家安全。美国议员请求商务部对中国WiFi路由器制造商TP-Link发起ICTS国家安全调查，则是为应对美国被发动网络攻击的安全风险。而前文中针对新型汽车产业的强力监管，则是中美欧开展科技竞争的典例，毕竟“**不发展就是最大的不安全**”。

于企业而言，在理解、落实新法新规时，不能囿于单一的“法律领域”或“合规领域”，例如，就数据合规论数据合规。**无论面对本国监管、还是应对外国监管，企业均应建立起贯通的视角，并意识到各国对于国家安全与国际竞争力的关切，**

从而作出妥善的合规决策。

“重要数据”的目录清单或许永远无法穷尽，各国的监管工具或许一直都在迭代交锋，但根植于国家安全与国际竞争力的本质诉求，将超越时间与空间，为企业在混沌未明的全球大环境中点一盏引路灯。

2024-09-04