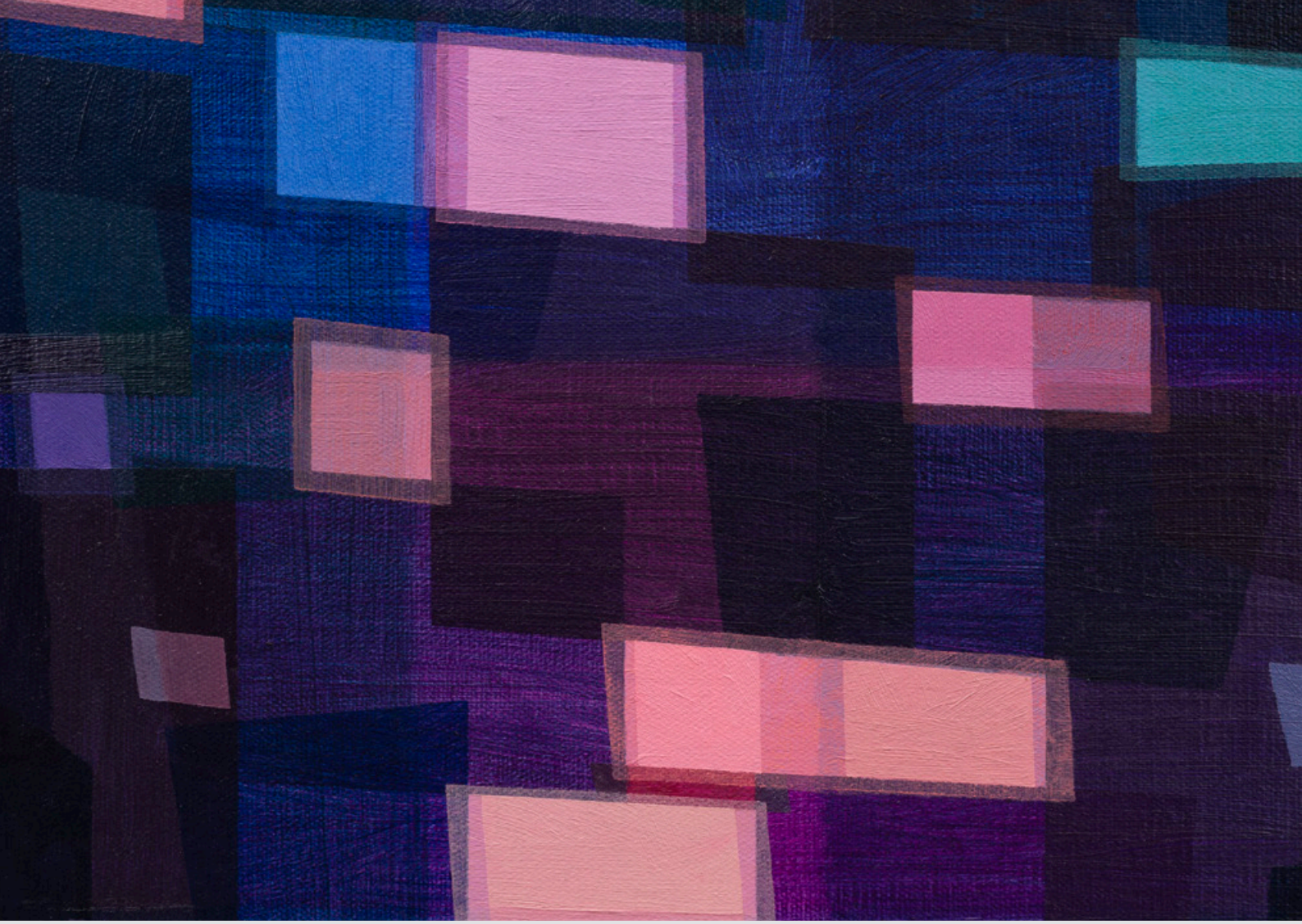


数字社会网络安全、数据合规及治理 II

金杜律师事务所
KING&WOOD MALLESONS

数字社会网络安全、数据合规及治理 II

画作：林子豪

有关本资料的咨询及意见和建议，请联系：
publication@cn.kwm.com

序 言

党的十八大以来，党中央高度重视发展数字经济，实施网络强国战略和国家大数据战略，拓展网络经济空间，支持基于互联网的各类创新，推动互联网、大数据、人工智能和实体经济深度融合。在此背景之下，互联网、大数据、云计算、人工智能、区块链等技术加速创新，日益融入经济社会发展各领域全过程，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有。《中国互联网发展报告 2021》指出，2020 年中国数字经济规模达到 39.2 万亿元，占 GDP 比重达 38.6%，保持 9.7% 的高位增长速度，成为稳定经济增长的关键动力。

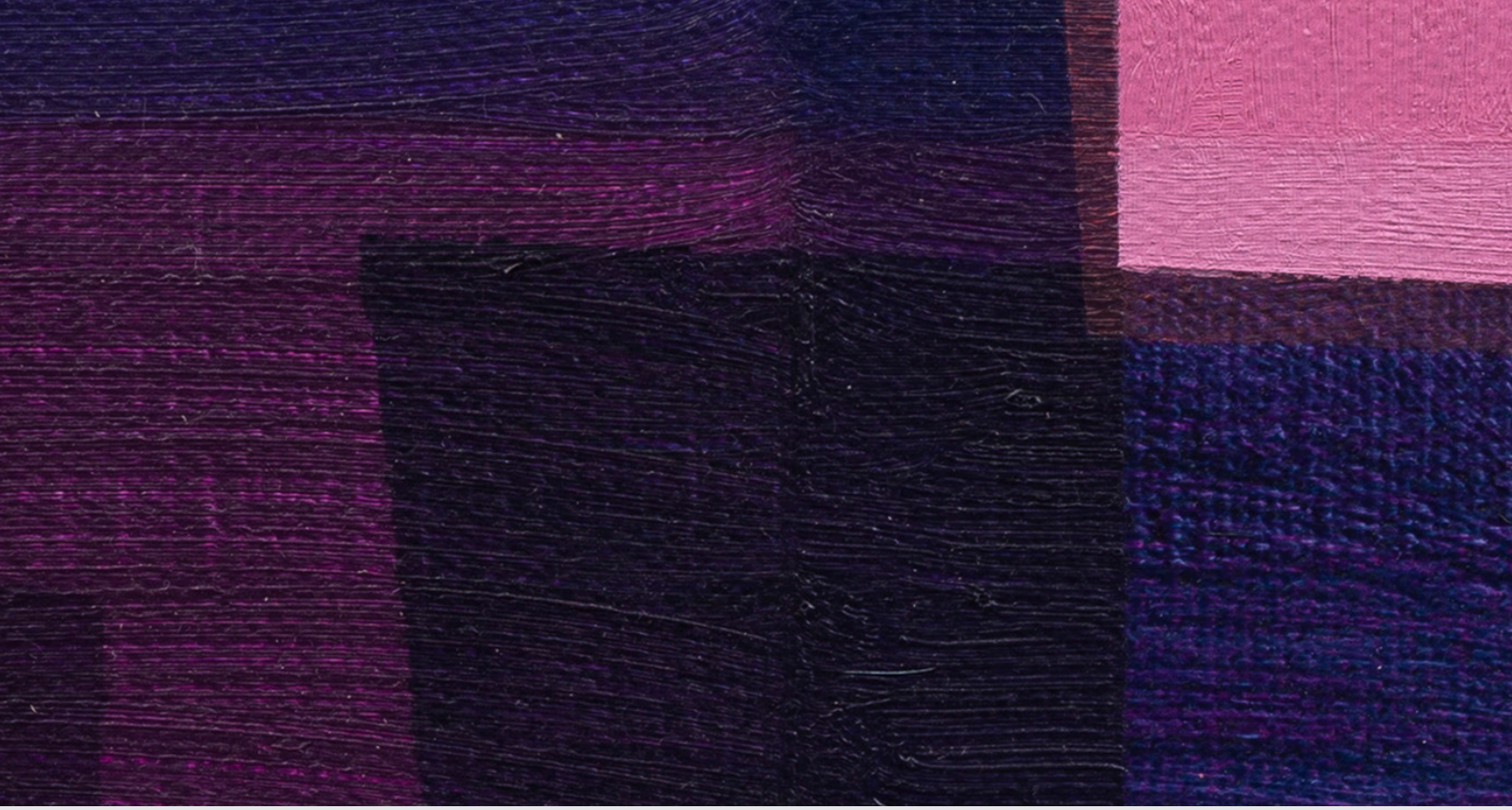
另一方面，随着《网络安全法》《数据安全法》《个人信息保护法》等法律的相继生效，以及《数据出境安全评估办法》等一系列配套法律法规和规范性文件的颁布，我国也将迎来网络空间治理规范集中完善、更新的一轮浪潮，这也显示出我国从规范监管层面顺应信息时代的系统设计，为世界提供充满借鉴意义的中国方案。同时，这也促使企业在数据驱动的经营理念中树立起合规价值的根本性认知。

作为国内首家专注数字经济领域法律研究和法律服务的国际化创新型综合法律服务平台，金杜数字经济国际法律服务中心（简称“数字经济中心”）自成立以来，积极跟踪市场变化与发展、参与规则制定，为企业客户提供具有行业前瞻的跨行业、跨学科综合顾问服务，也为数字经济的发展保驾护航。

本次呈现给大家的这本《数字社会网络安全、数据合规及治理 II》，是数字经济中心专业研究团队聚焦数字经济高速发展中全新的法律问题及立法空白，通过深度的行业调研及国内外立法研究，基于多年来服务客户的经验而形成的法律成果，也是理论与实践相结合的成果。其中，包含了人工智能、数据确权、数据资产、个人信息保护、网络安全等领域的前沿法律问题的探讨及实践。希望能够帮助企业客户成功应对数字经济浪潮的新挑战。

宁宣凤

合规业务部
高级合伙人



金杜数字经济国际法律服务中心

作为引领未来的新经济形态，数字经济已成为推动我国经济高质量发展的重要引擎。“十四五”期间，中央推出新的政策和举措，扶植数字经济的发展，明确将数据作为新型生产要素，在国家层面正式确认数据的基础资源地位，正式开启数字经济社会新阶段。在数字经济社会发展的同时，社会各界亟需从理论和实践角度研究和分析数字经济社会产生的法律关系，例如分享经济中的灵活用工劳动关系、个人信息处理者与个人信息主体的委托关系、智慧城市构建中多主体的法律责任和权益等。

作为国内首家专注数字经济领域法律研究和法律服务的国际化创新型综合法律服务平台，金杜数字经济国际法律服务中心（以下称“数字中心”）整合行业头部资源，组成跨学科、跨法域的研究战队，致力于内容、产品和业务模式的创新。数字中心运用智慧和经验，为数字经济立法和规则制定提供极具价值的专业研究成果，同时将前沿研究转化为具有商业价值的法律服务和产品，帮助企业客户成功应对数字经济浪潮新挑战。

数字中心依托金杜律师事务所在法律实践和平台资源的领跑优势，结合数字经济的无疆界特点拓展全新服务平台和产品，将“法律 + 数字经济”的构想付诸实践。

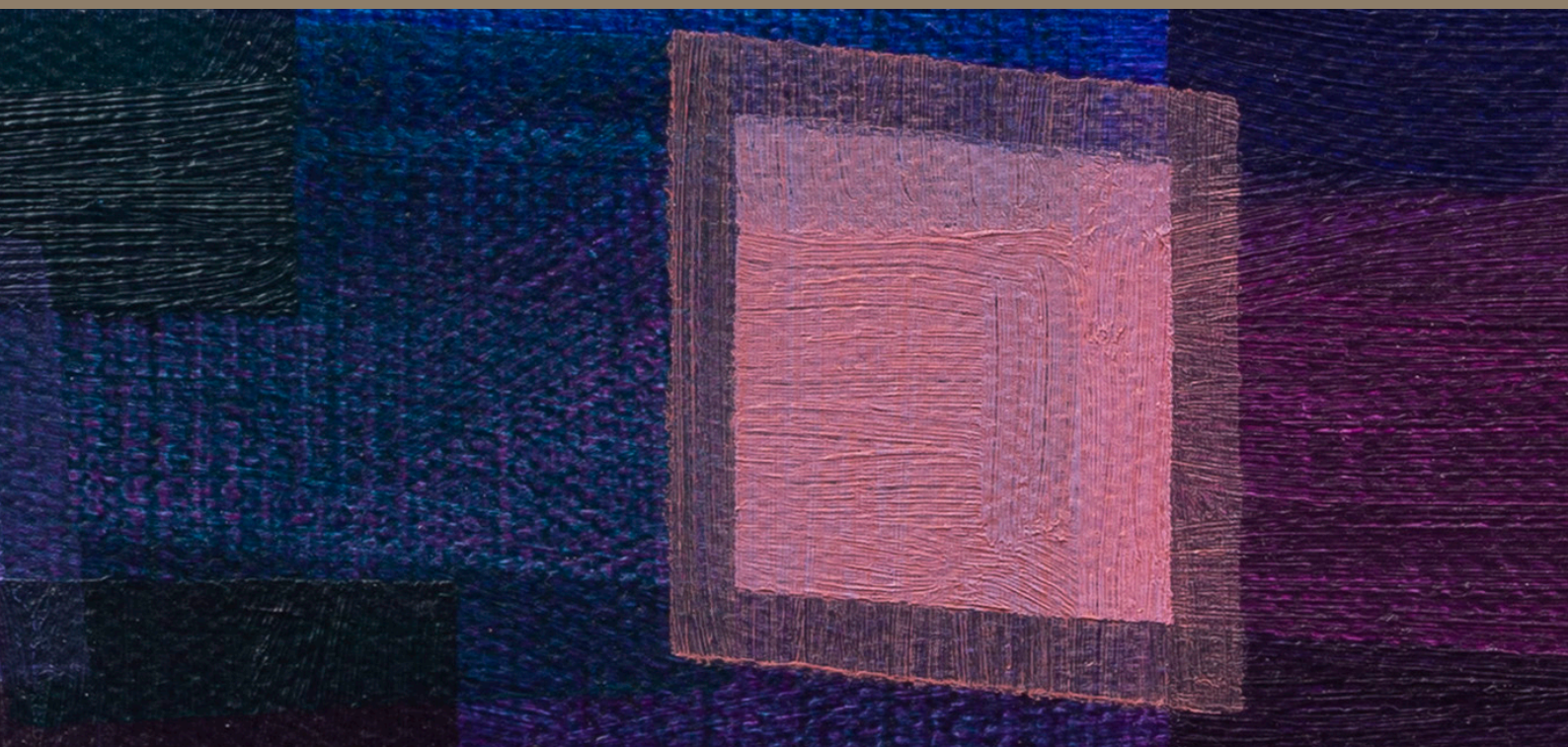
目录

人工智能

数据合规

网络安全

人 工 智 能



积跬步，至千里
——算法治理之互联网信息服务算法推荐管理

宁宣凤　吴涵　陈胜男　屈尘

继《数据安全法》及《个人信息保护法》等法律法规从一般规则层面概括性地对数据新技术的开发应用、自动化决策等的公平公正性进行总体性规范[1]后，国家网信办于2021年8月27日发布了针对互联网信息服务算法推荐的专门管理规范——《互联网信息服务算法推荐管理规定（征求意见稿）》（以下简称“**《规定》**”）。相比于此前法律法规层面对于算法监管的总体、概括性要求，《规定》以互联网信息服务为基础，从算法的公平公正及信息内容角度对算法推荐服务提出了各项具体细化的要求，反映了有关部门对于数字产业监管愈发深入，已从对于**算法问题所凸显的法律价值层面的监管渗透到对于算法应用过程的技术性监管**。

同时，《规定》还尝试在监管策略上对算法推荐服务建立起一套流程监管体系，在进行实体规范的同时，以程序化的方式保障算法推荐服务应用的向善性。相比于国外在算法治理统一规则方面的尝试，《规定》充分考虑了国内当下对于算法监管治理的理论与实践现状，采取了“专题性”的规则设定思路，在监管要求上将更具针对性和灵活性。

一、《规定》的适用范围及规制对象

根据《规定》第二条，《规定》主要适用于在中华人民共和国境内应用算法推荐技术提供互联网信息服务。

首先，对于“算法推荐技术”的范围，《规定》从算法适用的功能场景及所应用的技术类型出发，明确了其包含应用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术：

[1] 例如，《数据安全法》第二十八条规定，开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

- **生成合成类算法**：我们理解，该类算法基于深度学习技术拟合一种概率分布，从而合成或生成文本、语音、图像等文件，如利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息。该类算法技术同样可能适用于 AI 换脸 APP 涉及的“深度伪造”与“深度合成”等场景。

- **个性化推送类算法**：我们理解，该类算法通过人工智能分析和过滤机制对海量数据进行深度分析，可以实现信息内容与用户的精准匹配，例如线上购物软件通常可应用该算法，基于用户喜好为其推荐可能喜欢、感兴趣的商品。

- **排序精选类算法**：该类算法可以将一串资料依照特定方式排序，例如搜索引擎对搜索结果进行排序展示。

- **检索过滤类算法**：该类算法可以基于用户需求或法律要求，从可行的决策（推荐）方案中过滤出合适的推荐结果，例如可用于自动识别敏感字词。

- **调度决策类算法**：该类算法可以在资源有限但有多个进程同时发出请求的情况下，决定合适资源使用者，如作业调度算法、进程调度算法等。典型场景如网约车平台调度算法向乘客附近的网约车司机派单，并为司机与乘客提供信息撮合服务。

其次，《规定》对于算法推荐技术的类型在定义中采用了非穷尽列举的方式。从内容上看，《规定》实质规制的算法类型并不局限于上述算法类别。例如，《规定》第十八条强调，算法推荐服务提供者向消费者销售商品或者提供服务的，不得利用算法在交易价格等交易条件上实行不合理的差别待遇等违法行为。该规定剑指当下平台经济中的“大数据杀熟”热门问题，虽然《规定》指出价格歧视行为是算法基于消费者的偏好、交易习惯等因素进行的决策，但“大数据杀熟”除推荐算法外，不排除还会应用到定价类算法，因此《规定》实际适用范围可能会被扩大。

此外，《规定》将算法推荐技术的监管场景限定于“互联网信息服务”范畴，而根据《互联网信息服务管理办法》：互联网信息服务是指通过互联网向上网用户提供信息的服务活动，包括经营性互联网信息服务与非经营性互联网信息服务。可见，互联网信息服务仍可能涵盖较大范围的线上服务场景，无论是网站还是 App、是提供电子商务服务还是社交娱乐服务，只要涉及以互联网为媒介向用户提供信息，则会落入互联网信息服务的范围内。

二、算法推荐服务的监管原则与规则

《规定》在第四条与第六条中提出算法监管的主要原则——公正公平、公开透明、科学合理、诚实信用以及内容向善原则，并以此为基础在后续条文中进一步明确具体的监管规则。纵观《规定》全文，其对于算法监管细则可主要分为两类，一类是对算法推荐服务提供者**提出的新增要求**，另一类是**在既有法律法规规章基础之上对涉及算法场景的细化要求**，因此前者对应的罚则为《规定》所直接规定的法律责任，而后者的法律责任则是需要按照既有的法律、行政法规和部门规章的规定进行处理。本章节将对上述算法监管原则及相应的细化规则进行梳理和总结，以为公司提供指引和参考。

（一）公正公平、科学合理、诚实信用

上述原则要求算法推荐服务提供者在为用户提供服务时一方面应当保证对不同用户所提供的服务的平等性和合理性，避免歧视对待；另一方面也应确保服务本身符合商业道德要求，防止造假、欺诈、利用信息不对称实施欺骗等现象。

根据《规定》，算法推荐服务提供者应当从以下方面落实上述原则：

要求	罚则
• **定期审核算法模型的公德伦理性** 应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等，确保未设置诱导用户沉迷或者高额消费等违背公序良俗的算法模型。 • **加强用户模型和用户标签管理** 不得利用违法和不良信息关键词生成用户标签或将其记入用户兴趣点，并据以推送信息内容；不得设置歧视性或者偏见性用户标签。 • **禁止流量造假、流量劫持** 不得利用算法虚假注册账号、非法交易账号、操纵用户账号，或者虚假点赞、评论、转发、网页导航等，实施流量造假、流量劫持。 • **禁止网络操控** 不得利用算法屏蔽信息、过度推荐、操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现，实施自我优待、不正当竞争、影响网络舆论或者规避监管。	• 警告、通报批评，责令限期改正。 • 拒不改正或者情节严重的，责令暂停信息更新，并处五千元以上三万元以下罚款。 • 构成违反治安管理行为的，依法给予治安管理处罚。 • 构成犯罪的，依法追究刑事责任。
• **劳动者工作调度算法，应保障劳动者合法权益** 算法推荐服务提供者向劳动者提供工作调度服务的，应当建立完善以下算法，保障劳动者权益： （1）平台订单分配 （2）报酬构成及支付 （3）工作时间 （4）奖惩等 • **定价或其他交易条件算法，应保障消费者合法权益** 不得根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实行不合理的差别待遇等。	按照有关法律、行政法规和部门规章的规定予以处理。

（二）公开透明

算法的透明度原则是国际社会在进行算法监管时所普遍要求的原则之一。算法的公开透明、可解释性一方面可以保障作为用户或者消费者的算法使用者的知情权，另一方面有助于算法服务提供者自证算法合规，例如算法服务提供者为证明其算法并未设置诱导用户沉迷或者高额消费等违背公序良俗的模型，或者并未根据消费者的偏好、交易习惯等特征在交易价格上实行不合理的差别待遇，其需要对其的算法逻辑、基本原理和机制进行解释。除此之外，算法的公开透明原则也有助于对算法进行监测和审核，以确保其运行状态和输出结果在预期范围内且相对可控。

《规定》中为落实算法的公开透明原则提出细化要求，企业可从以下方面加强算法的公开透明程度：

要求	罚则
建立健全相关制度和规则 （1） 落实算法安全主体责任，建立健全以下制度： • 用户注册制度； • 信息发布审核制度； • 算法机制机理审核制度； • 安全评估监测制度； • 安全事件应急处置制度； • 数据安全保护和个人信息保护等管理制度。 （2） 制定并公开算法推荐相关服务规则。 （3） 配备与算法推荐服务规模相适应的专业人员和技术支撑。 • **加强服务规则的可解释性和透明性** 综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响、引发争议纠纷。 • **公示算法相关情况** 以显著方式告知用户其提供算法推荐服务的情况，并以**适当方式公示算法推荐服务的基本原理、目的意图、运行机制等**。	• 警告、通报批评，责令限期改正； • 拒不改正或者情节严重的，责令暂停信息更新，并处五千元以上三万元以下罚款。 • 构成违反治安管理行为的，依法给予治安管理处罚； • 构成犯罪的，依法追究刑事责任。

（三）内容向善

根据《规定》第六条，算法推荐服务提供者应当坚持主流价值导向，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善，同时不得利用算法推荐服务传播法律、行政法规禁止的信息。《规定》对此从多方面进行了细化规定，企业可以参考以下要求完善算法内容合规体系：

要求	罚则
• **建立违法和不良信息识别机制** 加强信息内容管理，**建立健全用于识别违法和不良信息的特征库**，完善入库标准、规则和程序。 • **对合成信息作显著标识** 发现未做显著标识的算法生成合成信息的，**应当作出显著标识后，方可继续传输**。 • **建立人工干预与用户自主选择机制** 加强算法推荐服务版面页面生态管理，建立完善**人工干预和用户自主选择机制**，在首页首屏、热搜、精选、榜单类、弹窗等重点环节积极呈现符合主流价值导向的信息内容。其中用户选择机制可以包括： （1） **向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项**。用户**选择关闭**算法推荐服务的，算法推荐服务提供者应当**立即停止提供相关服务**；	• 警告、通报批评，责令限期改正； • 拒不改正或者情节严重的，责令暂停信息更新，并处五千元以上三万元以下罚款。 • 构成违反治安管理行为的，依法给予治安管理处罚； • 构成犯罪的，依法追究刑事责任。 注： 3（1）与 3（2）的罚则为：按照有关法律、行政法规和部门规章的规定予以处理。

要求	罚则
（2） 用户认为算法推荐服务提供者应用算法**对其权益造成重大影响**的，有权**要求算法推荐服务提供者予以说明并采取相应改进或者补救措施**； （3） **向用户提供选择、修改或者删除**用于算法推荐服务的用户标签的功能； （4） **设置便捷的投诉举报入口**，及时受理和处理公众投诉举报；建立用户申诉渠道和制度，规范处理用户申诉并及时反馈。	
• **违法和不良信息处置机制** （1） 发现违法信息的，**应当立即停止传输，采取消除等处置措施**，防止信息扩散，保存有关记录，并向网信部门报告； （2） 发现**不良信息的，应当按照网络信息内容生态治理有关规定予以处置**。 • **未成年算法推荐服务的特殊保护要求** （1） 通过**开发适合未成年人使用的模式、提供适合未成年人特点的服务**等方式，便利未成年人获取有益身心健康的信息内容； （2） 不得向未成年人用户推送可能**引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息内容**； （3） 不得利用算法推荐服务**诱导未成年人沉迷网络**。	按照有关法律、行政法规和部门规章的规定予以处理。

三、《规定》提出的具体监管手段

在《算法治理系列之——智能时代的算法治理》一文中我们提到，国际社会的算法规制的方式较为多样化，大致可以分为事前、事中与事后三个阶段的监管模式。其中，事前的监管方式主要包括禁止算法使用、备案、影响评估、对 AI 算法（系统）设计提出要求等；事中的监管机制主要包括要求算法供应商主动持续上报和赋予主管机构对 AI 算法系统检查和监视权力两种模式；事后的监管机制主要指赋予用户私人诉权或赋予国家权力机关代为行使诉权的救济模式。本次《规定》从监管方式上看似与上述监管思路有所交叉，具体而言包括分级分类、备案、安全评估、配合检查等。

（一）分级分类

根据《规定》第十九条，网信部门将对算法建立分类分级管理制度。企业可以根据下列因素对既有算法进行梳理并进行初步分类分级，以识别出敏感程度较高的算法，并加强对其的审核、监测以满足上述算法推荐服务监管规则的要求：

（1）舆论属性
（2）算法的社会动员能力
（3）内容类别
（4）用户规模
（5）算法推荐技术处理的数据敏感程度
（6）对用户行为的干预程度

（二）备案

在上述分级分类制度的基础之上，根据《规定》第二十条和第二十二条，对于满足特定条件的算法推荐服务提供者，还须履行一定的备案手续，保障执法部门对于企业算法推荐技术应用的干预监管：

要求	罚则
• **需要进行备案的主体** 具有舆论属性或者社会动员能力的算法推荐服务提供者； • **备案时间** 应当在提供服务之日起十个工作日内； • **备案内容** 服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息； • **备案方式** 通过互联网信息服务算法备案系统填报； • **备案变更** 算法推荐服务提供者的备案信息发生变更时，应当在变更之日起五个工作日内办理变更手续。	未按照要求备案或者在报送备案时隐瞒有关情况、提供虚假材料或者通过欺骗、贿赂等不正当手段取得备案的，由国家和省、自治区、直辖市网信部门依法撤销备案，并给予警告、通报批评，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，并处五千元以上三万元以下罚款。
• **备案注销** 算法推荐服务提供者终止服务的，应当在终止服务三十个工作日前办理注销备案手续，并作出妥善安排。	未按照要求及时办理注销备案手续，或者发生严重违法情形受到吊销互联网信息服务许可、关闭网站、终止服务等行政处罚的，由国家和省、自治区、直辖市网信部门予以注销备案。
• **备案公示** 完成备案的算法推荐服务提供者应当在其对外提供服务的网站、应用程序等显著位置标明其备案编号并提供公示信息链接。	警告、通报批评，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，并处五千元以上三万元以下罚款。构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

（三）安全评估

在上述分级分类制度的基础之上，根据《规定》第二十三条，具有舆论属性或者社会动员能力的算法推荐服务提供者应当按照国家有关规定开展安全评估。算法推荐服务提供者应当完善算法推荐服务管理机制，对算法推荐服务日志等信息进行留存，留存期限不少于六个月，并在相关执法部门依法查询时予以提供。若相关算法推荐服务提供者未按上述要求完成安全评估或日志留存等义务，则按照有关法律、行政法规和部门规章的规定予以处理。

（四）配合检查

根据《规定》第二十四条第二款，算法推荐服务提供者应当配合有关主管部门依法实施的安全评估和监督检查工作，并提供必要的技术、数据等支持和协助。对于违反者按照有关法律、行政法规和部门规章的规定予以处理。这意味着主管机构在进行安全评估和检查工作时，算法推荐服务提供者可能需要向其提供数据、算法模型等，以供其查验。

结语

《规定》是我国首次专门针对算法推荐建立监管规则，对于算法推荐服务的深层技术性要求反映了执法部门对于网络信息安全治理已经逐渐从统一规则的普适性监管到特定领域和场景的纵深性监管，这也进一步提示企业，未来企业内部的业务合规工作将不再仅聚焦于整体层面的合规内控框架，对于诸如算法应用等具体场景下的技术合规工作也将愈发必要。

如前所述，在《规定》发布之前，已有多部部门法律法规或规范草案对算法及自动化决策等类似技术在不同场景下的应用提出了规范要求，例如《个人信息保护法》第二十四条要求个人信息处理者利用个人信息进行自动化决策时应当保证决策的透明度和结果的公平公正，不得实行不合理的差别待遇；《数据安全管理办法（征求意见稿）》也曾就基于信息收集采取的服务质量与价格歧视行为、采取自动化手段访问收集网站数据、利用用户数据和算法进行的定向推送，以及利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等行为进行规制。在电子商务领域，《电子商务法》第十八条也规定了类似的“大数据杀熟”条款，而《网络交易监督管理办法》涉及的多个条款，包括搜索降权、下架商品、限制经营、屏蔽店铺等干涉平台经营者自主经营的行为等，以及向消费者发送商业信息等行为，都可能使用算法完成。此外，《国务院反垄断委员会关于平台经济领域的反垄断指南》对平台领域内可能涉及的算法共谋，以及利用算法进行的拒绝交易、限定交易、差别待遇等行为进行规制。在具体的罚则方面，《价格违法行为行政处罚规定（征求意见稿）》还专门规定了“新业态中的价格违法行为”，对就基于算法实施价格歧视的行政处罚进行规定。司法实践中，近期浙江省绍兴市柯桥区人民法院还就某用户与在线旅行平台的“大数据杀熟”纠纷中明确平台作为中介对标的实际价值有如实报告义务，如未践行承诺则可能存在虚假宣传、价格欺诈和欺骗行为[2]。该案例被视为“大数据杀熟”领域法院判决消费者方胜利的第一案。

这些以往的立法规则、司法实践进一步说明，算法的治理与监管具有较高的多维度价值取向性，一项算法技术的应用将不仅涉及某一部门法领域的监管规则，甚至且往往牵扯多部门、多领域监管规则的“竞合”。在这一背景下，企业更应审慎对待自身算法技术的内部监管与合规，现阶段在进行算法技术开发与应用的内部审查时，在关注《规定》的监管走向和趋势的同时，更应综合考虑其他部门领域的法律法规和监管要求，保障内部审查内容与审查流程的全面性和完整性。

总之，《规定》是我国对算法监管迈出的重要一步，首次系统地从实体与流程监管方面对互联网信息服务场景下的算法伦理与合规提出要求。**我们可以期待，未来算法的纵深式监管将愈发趋向于专业化和技术化，在回应监管需求的同时为技术可行性留下操作空间。**

[2]https://new.qq.com/omn/20210716/20210716A0ESYA00.html，最后访问：2021 年 8 月 29 日。

算法治理系列之
——智能时代的算法治理

宁宣凤　吴涵

根据大英百科全书的定义，算法是在有限的步骤中生成问题答案或者解决方案的系统程序。算法在大数据时代之前就已经被广泛应用，理论上包括机械原理、逻辑思维和社会规则等都能纳入算法的范畴。但随着大数据时代和智能时代的交叠，AI 算法得到普遍应用。

人类使用 AI 算法的初衷在于辅助或部分代替人类决策，使生活变得更加便捷和智能。AI 算法作为人工智能、区块链、大数据分析等技术的核心要素，确实地推动人类生产生活的变革。但同时，AI 算法作用过程和决策机制较为隐蔽甚至不便于人类思维理解，有时类似密不透风的“黑匣子”——这导致其被滥用的风险骤然提升，最终可能与使用初衷背道而驰。信息茧房、大数据杀熟、算法歧视等事件的层出不穷也让人们对看似理性、中立的算法进行反思。在此背景下，各国政府开始尝试对算法进行监管。包括但不限于在整体层面上，设立 AI 的伦理原则，将算法的发展方向框定在“对人类有益”的范围之内，而在各类应用场景中，提出算法透明、公正、保证算法的“可信度”等细致要求。

本文将从作为底层逻辑的 AI 算法开始，从技术特征和适用场景两个维度探讨国际社会所监管的 AI 算法类型，对各国算法规制的重点进行介绍。之后，本文将从各国采用的 AI 算法监管方式入手，以事前、事中、事后三个角度进行剖析，分析各类方法的优劣。

一、AI 算法的治理范围

虽然 AI 算法治理已经逐渐成为各国监管探索的焦点问题，但从国际社会目前的实践来看，并非所有的算法都被列为监管对象或重点。各国对“应被监管的算法类型”进行范围界定时主要有两个考查维度，其一是 AI 算法本身的技术性质，其二是 AI 算法的应用场景。

（一）AI 算法本身的技术性质

根据欧盟今年四月发布的《制定关于人工智能的统一规则（人工智能法案）并修订某些欧盟立法》(Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts) 提案（以下简称“《人工智能提案》”）第三条第 1 款中的定义，人工智能系统是指“使用附件 I 中所列的一种或多种技术和方法开发的软件”[1]，具体而言包括：

（a）机器学习算法，包括使用深度学习等各种方法的监督学习、无监督学习和强化学习算法；
（b）基于逻辑和经验的算法，包括知识表示、归纳（逻辑）编程、知识图谱、推理和演绎、（符号）推理和专家系统；
（c）统计方法，贝叶斯估计以及搜索和优化方法[2]。

由此可知，《人工智能提案》中对算法的监管并非仅限于近期的热点黑箱 AI 算法，也包括一些传统的逻辑推理以及统计方法。与此类似，英国信息专员办公室（Information Commission's Office）发布的《解释 AI 决策的指南》（Explaining decisions made with AI）中也针对多种算法进行规制，其中既包括神经网络等人工智能时代的热点算法，也包括逻辑推理、线性回归、逻辑回归等传统算法。这一方面是由于传统算法的“可理解性”不代表其在实践过程中可以确实的“被理解”，简单算法的叠加和复杂逻辑也可以使得其不易被公众理解。另一方面算法最终的输出结果也在很大程度上与算法所处理的数据相关，因此传统算法在大数据的作用下也可能输出难以预料的结果。

虽然国际社会对算法的监管较为广泛，不仅限于人工智能时代的热点算法，但针对不同类型算法的监管思路与程度大相径庭。例如《解释 AI 决策的指南》中以算法本身是否为黑箱算法而对其进行分类，并且鉴于黑箱算法的不可解释和隐匿性，规定在有其他非黑箱算法可以实现类似目的并且不需要带来巨大或难以承受的额外成本时，优先选择非黑箱算法[3]。

[1] 参照欧盟《制定关于人工智能的统一规则（人工智能法案）并修订某些欧盟立法》(Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts) 提案第三条第 1 款。
[2] 参照欧盟《制定关于人工智能的统一规则（人工智能法案）并修订某些欧盟立法》(Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts) 附件一：人工智能技术和方法。
[3] 参考上注。

（二）AI 算法的适用场景

AI 算法适用场景的敏感程度是国际社会对 AI 算法进行监管时重点考虑的因素之一。即使使用的 AI 算法本身并不复杂和敏感，但若被应用于敏感程度较高的场景中，依然可能会因为处理数据的敏感程度、处理数据本身的偏差、可能影响的公众范围之广以及应用场景本身所处领域的法律规定等因素而被重点监管。

1. 执法机构使用的算法

2019 年 2 月 5 日，加拿大出台的《自动化决策指令》（Directive on Automated Decision-making）对政府部门使用算法决策进行规制，指出若政府部门在作出行政行为过程中使用自动化决策系统，则应当进行算法影响评估，通过事前通知、事后解释、公布源代码等方式提高决策的透明度，通过监测结果、保障数据质量、为员工提供培训、提供人工干预等方式保证算法决策质量等。

而在美国，时任总统特朗普于 2020 年 12 月 3 日签署行政命令，为联邦机构使用人工智能制定指导方针，旨在促进对人工智能的创新和使用，以促进公众信任，建立对人工智能的信心。该行政命令提出，联邦机构在使用 AI 技术时应当合法并尊重国家价值观、目的明确、准确可靠且有效、安全且灵活、可理解、可问责且可追溯、透明等原则 [4]。

与上述规定不同的是，欧盟委员会发布《人工智能提案》中则是针对不同场景下公共机构使用的具体人工智能技术提出监管规定。例如对于公共机构或代表公共机构对自然人的可信赖性进行评估或分类的社会评分人工智能系统 [5] 和以执法为目的在公共场所使用的远程生物特征识别系统均进行重点规制，要求原则上不得投放和使用，明文规定的特殊情形除外。

2. 搜索排名算法

在交易场景之下，作为网络服务提供方的交易平台要承担保护平台上商家的竞争公平性及保护消费者权益等义务，改善交易场景下的透明性和公平性。因此平台对商家或商品的搜索排名算法自然成为各国监管的重点，例如美国参议员于 2019 年 10 月 31 日提出的《过滤泡沫透明度法案》（Filter Bubble Transparency Act）中要求，大型互联网平台在使用内容筛选或排名的算法时，原则上不得运营使用不透明算法。

此外，日本《改善特定数字平台上的交易透明度和公平性法》法案从今年春季开始实施，该法案规定了特定数据平台供应商的信息披露义务，披露重点就在于平台使用的排序、分类的方法，从而避免出现优惠或歧视性待遇的情况，例如平台使用优先自身的排序系统等；但要求商家披露的内容不包括排序的具体算法，以免侵犯其商业秘密。

类似的还有韩国于 2020 年颁布的《在线平台公平交易法》，为了提高平台与在线商店之间交易的透明度和公平性，其要求通过透明公开的合同条款和条件来防止事前纠纷，平台运营商必须草拟书面合同并将其交付到在线商店，并在合同中指定重要项目，其中包括用于确定诸如商品等信息的展示方式以及在线平台上顺序的标准，包括费用对信息呈现方法和顺序产生的影响等。

3. 劳动雇佣算法

鉴于劳动雇佣场景直接关系到个人的劳动就业权与平等就业权，对个人利益和公共利益具有较高影响，同

[4] 参见《特朗普签署行政令：在联邦政府推行“可信赖人工智能”》，可于以下网址访问：https://www.secrss.com/articles/27595，最后访问时间：2021 年 6 月 3 日。
[5] 详见《提案》第 5 条第 1 款 c 项。

时 AI 算法越来越多地被应用在招聘、晋升场景之中，由 AI 来分析面试者是否具有某种特质、是否符合工作岗位的要求，从而辅助人力资源部门来进行决策。因此，各国对劳动雇佣场景下的 AI 算法提出了一系列监管要求。

目前美国平等就业机会委员会（EEOC）也对招聘算法中可能存在的歧视和偏见展开了调查。具体到美国的立法层面，2019 年 5 月，伊利诺伊州通过了《人工智能视频面试法》(Artificial Intelligence Video Interview Act)，对 AI 参与招聘流程进行了限制。该法案要求雇主在使用 AI 进行招聘的时候需要向面试者解释 AI 的工作方式及技术检测的特征，并需要获得面试者的同意，并且雇主还需要在 30 天内删除所有的视频内容。[6]

欧盟则将应用于公民就业场景的 AI 认定为八个高风险级别的场景之一，概括地对高风险级别的 AI 工具作出了几点强制性规定，包括训练数据、数据和记录、须披露的信息、稳健性和准确性、人工监管等要求，力图控制风险，使其对公民权利的影响在可控范围之内。

二、 AI 算法的治理方式

虽然算法治理已逐渐成为国际社会共同关注的焦点之一，并且以美国、欧盟为代表的多个国家已经开始积极探索算法可能的监管思路与治理框架，但目前各国算法规制的方式较为多样化，大致可以分为事前、事中与事后三个阶段的监管模式。

（一）事前

目前国际社会对 AI 算法在投放市场或使用之前的治理方式较为多样，主要可以分为以下两种：

1. 事前禁止、备案、影响评估等要求

2021 年 4 月欧盟委员会发布的《人工智能提案》中对 AI 算法采用基于风险等级区分规制方法的监管路径。具体而言，AI 算法系统在投入使用或投放市场之前应当确定其所属的风险等级。对于四类导致或者可能导致自然人身体或心理伤害的 AI 算法系统，《人工智能提案》认为其风险不可接受（Unacceptable risk）因而禁止该等系统的使用和投放。**此外，对于使用或投放于关键基础设施、公民教育、公民就业、公共服务、执法等领域可能存在危害健康和安全或对基本权利造成不利影响风险的 AI 算法系统，《人工智能提案》将其归类为高风险系统并规定了注册义务，即在将高风险 AI 系统投入市场或投入使用之前，其供应商或授权代理人（如适用）应将该系统注册到欧盟针对独立高风险 AI 系统建立的欧盟数据库中。**供应商注册时应提供以下信息，且欧盟数据库中包含的信息应向公众开放：

- 供应商的名称，地址和联系方式；
- 由他人代表提供者提交信息的，该人的姓名，地址和联系方式；
- 授权代表的姓名，地址和联系方式（如适用）；
- AI 系统的商品名称和任何其他可以识别和追溯 AI 系统的参考；
- 描述 AI 系统的预期目的；
- AI 系统的状态（在市场或服务中；不再放置在市场 / 服务中，已召回）；
- 指定机构签发的证书的类型，编号和有效期，以及该指定机构的名称或标识号，以及证书扫描件（如适用）；
- AI 系统已经或已经投放市场，已投入服务或已在联盟中提供的成员国；

[6]《美国人工智能相关立法概述》，可于以下地址访问：https://www.worldip.cn/index.php?m=content&c=index&a=show&catid=66&id=261，载《GDPR 观察手册》2021 年版，最后访问时间：2021 年 6 月 1 日。

- 欧盟合规声明的副本；
- 电子版使用说明；
- 其他信息的网址（可选）。

由上述列举信息可知，注册时需要提供的信息基本限于 AI 系统及其供应商的基本信息，而不涉及 AI 系统的逻辑与算法、体系与结构等更加深入和详细的信息。根据《人工智能提案》第 11 条以及 50 条，该等更详细的信息应**在 AI 系统使用或投入市场之前被记录在技术文档之中，用于进行事前影响评估，同时该技术文档应在 AI 系统被投入市场或投入使用后的十年内，保持国家主管部门对该技术文档的处置（keep at the disposal of the national competent authorities）**，但根据该法案目前的表述，无法判断该技术文档是否需要交由国家主管部门保存或备案。

类似地，2019 年 4 月美国两位民主党参议员 Cory Booker 和 Ron Wyden 联合提出的《算法问责法案》（Algorithmic Accountability Act）中也指出美国联邦贸易委员会应颁布法规要求拥有或控制高风险自动化决策系统的实体在部署或实施该系统之前进行自动化决策影响评估和数据保护影响评估。

2. AI 算法（系统）设计相关要求

鉴于增强 AI 算法的透明度在一定程度上有助于降低 AI 系统可能导致的风险并增强公众对 AI 算法的信任感，许多国家对 AI 算法（系统）的设计提出要求，以提高其在投放市场或投入使用时的透明度。例如美国《过滤泡沫透明度法案》要求，大型互联网平台在使用根据特定用户的数据对互联网平台上的内容进行筛选或排名的算法时，原则上不得运营使用不透明算法，除非其在用户第一次与不透明算法进行交互时以清晰、明显的方式向用户发送可以拒绝的一次性通知，以告知用户平台使用不透明算法，并且向用户同时提供使用透明算法的平台版本，使用户可以轻松地在使用不透明算法的平台版本和透明算法的平台版本之间切换选择，以此提高大型互联网平台面向消费者的透明度。

韩国最大的搜索引擎公司 Naver 被韩国公平贸易委员会（Korea Fair Trade Commission，“KFTC”）指控其将自己的服务放在搜索结果顶部，同时降低竞争对手出售的产品的排名，以操纵有利于其的搜索算法的设计方式违反《垄断法规和公平贸易法》，因此对其下达了纠正令（corrective orders）。欧盟《人工智能提案》中则是更明确地规定供应商应确保以与自然人互动的方式设计和开发 AI 系统，以使自然人被告知他们正在与 AI 系统互动，除非从情况和使用语境中显而易见 [7]。

（二）事中监管式

事前审查、备案等方式并不能排除 AI 算法系统在投放于市场后或在市场中使用时所可能产生的多方面风险，例如市场环境中的真实数据可能使得 AI 算法的输出结果超出预期并给个人甚至公共利益带来危害。鉴于此，一些国家在 AI 算法系统的整个运行过程中对其进行监管，以动态检测 AI 算法的实际运行情况。

日本《改善特定数字平台上的交易的透明度和公平性法》规定了对特定数字交易平台供应商在 AI 算法系统使用过程中的**持续上报义务**，即特定数字平台供应商向日本经济产业省部（METI minister）提交年度报告，说明其合规状况，并就其在该法案下的义务的履行情况进行自我评估。METI 将对该报告进行审查，以确保交易的透明度和公平性，并将审查结果与每个供应商的报告大纲一并公布。

除供应商主动上报外，一些国家还规定了主管机构对 AI 算法系统进行检查和监视的权力。例如欧盟《数

[7] 参见《KFTC imposes corrective measures on Naver for favoring its own real-estate search, shopping, and video services over competitors》，可于以下地址访问： https://www.ftc.go.kr/solution/skin/doc.html?fn=508d97db636c2f7f0961bf6361cfd44f09977d1a7a06f4dd5603f17c11d61013&rs=/fileupload/data/result/BBSMSTR_000000002402/，最后访问时间：2021 年 6 月 3 日。

字服务法》规定，在现场检查过程中，欧盟委员会及其指定的审计人员或专家可要求有关的超大型在线平台就其组织、运行、信息技术系统、算法、数据处理和业务行为作出解释。《数字市场法》同样规定，欧盟委员会可以通过简单请求或通过决定要求企业和企业协会提供信息，要求提供所有为了持续监测、实施和执行本法规所规定的规则所必要的信息。委员会可以要求访问企业的数据库和算法，并可以简单地请求或决定要求提供解释。此外，欧盟《人工智能提案》在第 63 条中规定了主管机构对欧盟市场中 AI 系统的市场监视和控制，例如国家监管机构应定期向委员会报告有关市场监督活动的结果。同时其第 64 条要求 AI 算法系统应当对“向监管机构透明”，其赋予市场监督机构在其活动范围内通过 API、远程访问工具等方式访问供应商 AI 算法系统的数据（包括训练集、验证集和测试集）的权力，以及为评估高风险 AI 系统是否符合《人工智能提案》相关规定而访问源代码的权力，并且公共机构可以要求市场监督机构通过技术手段对高风险的 AI 系统进行分析测试。

（三）事后救济式

除事前审查、事中监督之外，若 AI 算法的使用给利益相关方带来威胁或损害，有些国家规定了相应的救济措施，**但在不涉及既有法律领域规则所规定的私人诉权的情况下，目前基于 AI 算法监管而产生的救济措施大多由国家权力机构行使或代为行使**，而并非由利益受损相关方直接行使。例如美国《算法问责法案》中规定，若一州的司法部部长（attorney general of State）有理由相信该州的居民因为违反该法案规定的实践而受到威胁或者不利影响，则该州的总检察长可以代表该州的居民向美国地区法院提起民事诉讼以获得适当的救济。

类似地，日本《改善特定数字平台上的交易的透明度和公平性法》中规定，如果数字交易平台的用户（包括第三方卖方和消费者）认为特定数字平台供应商未采取必要的措施，则可以向 METI 报告，并可以要求实施适当的措施。平台用户可能会利用此报告系统帮助 METI 收集有关违规的信息。该法案还禁止特定数字平台供应商拒绝交易或以其他方式对平台用户进行报复，以掩盖向 METI 的此类报告和请求。

三、算法治理方式的利弊分析

前述事前、事中、事后的算法监管方式可以在算法设计、运行与实施的各个阶段对算法进行监管并为利益相关者提供保障，但同时该等算法治理方式也可能根据算法本身的性质、应用场景、监管权力分配等因素存在一定的局限性。

（一）事前禁止、备案、影响评估以及介入算法设计等监管方式

根据算法本身的性质对算法进行事前规制可以在一定程度上为算法设立市场准入的门槛，事先对一些以损害他人、公共甚至国家利益为目的的 AI 算法或者 AI 算法设计进行禁止，防止部分个人、团体甚至国家公权力机关将非法目的或行为包装成 AI 算法并实施。这种防止技术“本身违法”（“per se illegal”）的事前监管方式在其他法律领域也有所涉及，但在算法领域可能存在部分局限性。

对于事前禁止 AI 算法的规制方式而言，一方面，如何在事前定义 AI 算法“本身违法”是一个亟待解决的难题。欧盟《人工智能提案》第 5 条中采用了“导致或可能导致该人或他人的身体或心理伤害”“以导致或可能造成该人或他人的身体或心理伤害的方式”“导致对某些自然人或整个群体的有害或不利待遇”等结果导向的定义形式，但在事前预估其可能造成的后果在事实上可能具有一定的实践难度，并且伤害程度如何衡量也需要进一步的探讨。尤其在算法决策过程存在不透明以及不可解释性时，排除或确定可能的危害和危害程度更是难上加难。另一方面，这种监管方式的有效性可能受限于 AI 算法结果的不可预测性。AI 算法输出的结果不仅依赖于算法本身的性质和设计思路，也在很大程度上依赖于输入算法的数据（包括训练集、验证集和测试集等），AI 算法在被投放于市场或投入使用之后，其所处理的数据可能较为庞杂并且本身存在一定的偏差，因而造成输出结果不符合预期的情况。

对于**事前备案**的方式而言，需要解决的核心问题之一是对 AI 算法的哪些信息进行备案。尽管目前采取这种监管方式的国家较少，并且欧盟《人工智能提案》中仅要求供应商将 AI 系统在欧盟数据库中进行注册时提供 AI 算法的基本信息，这种备案的优势在于可以对现有的 AI 算法进行梳理和分析，并且在 AI 算法系统发生损害或不利影响时快速追溯到具体系统以及供应商并采取相应措施。此外还能归纳总结历史上发生损害的具有共性的应用场景或者算法技术，在事前备案中予以设定预防纠正措施等。但目前在实践中其并未对算法准入门槛和标准进行更加详细和细致的规定，例如在确定哪些 AI 算法需要履行备案手续时是否需要考虑其本身的技术性质（如是否为黑箱算法）、应用场景、处理数据的敏感程度以及体量等。

就目前国际社会的实践情况而言，事前对算法进行影响评估的监管方式正逐渐成为各国探索的方向之一。影响评估可以提高 AI 算法供应商以及使用者的注意义务，同时对该等影响评估的公开也可以敦促 AI 算法供应商或使用者接受社会审查，并提高公众对算法的信任度。但目前而言，国际社会更倾向于由 AI 算法供应商或使用者自己而非监管机构完成影响评估。考虑到影响评估的客观性，主管机构可能需要出台配套措施以保证对该影响评估结果进行严格的审查和验证，以及细致具体的影响评估细则或指南要求 AI 算法供应商、使用者或者第三方机构在进行算法影响评估时必须客观考量和评估的指标和方面，从而保证算法影响评估的真实有效。

此外，**对 AI 算法的设计方式提出要求从而保障算法透明度**的方式是大多国家采用的监管方式。透明度不仅可以提高 AI 算法供应商或使用者在设计、开发、使用算法时的注意义务，还有助于保障和落实消费者的知情权，减少信息不对称，从而增强公众对 AI 算法的信任度。但是具体的设计要求与 AI 算法的适用场景息息相关，例如对于在线购物系统，提供退出选项可能是较为有效的方式，而对于视频监控系统而言，提供退出选项可能在事实操作层面存在一定困难，需要采取其他更为有效的方式。因此对透明度的监管规定需要根据场景进行具体划分并细化落实。

（二）事中监管式

在 AI 算法进行测试、运行以及投放市场后对其进行持续监测的事中监管机制有助于及时发现算法存在的问题和风险，从而采取措施加以应对和解决，避免威胁的发生或损害的扩大，同时可以提高相关 AI 算法供应商或使用者对其开发、使用 AI 算法的持续注意义务，在一定程度上降低 AI 算法出现预期之外结果的风险。

根据目前各国的探索和实践，事中监管机制可以分为 AI 算法供应商持续主动上报以及主管机关持续监测和调查这两种方式。对于前者而言，需进一步明确具体上报的信息类型以保证风险可以被主管部门有效监测，同时，如何保障 AI 算法供应商上报信息的准确性、真实性、有效性也需要配套措施加以完善；而对于后者，核心问题是如何界定主管机构的权力范围。一方面，若允许主管机构在 AI 算法暂未出现较大或不利影响时查阅所有的数据、源代码以及文件，可能有违行政领域的比例原则，过度扩张主管机构的权力边界，并给企业带来不必要的负担；另一方面，监管机关行使权力的条件存在较大不确定性，例如“为了持续监测、实施和执行本法规所规定的规则所必要的信息”范围如何界定，何为“在其活动范围内”等，并可能因此导致权力寻租。

（三）事后救济式

与其他法律领域事后救济的规定类似，算法领域的事后救济规则可以防止危害的进一步扩大并弥补利益相关方一定的损失。但是根据目前国际社会的规定来看，其倾向于采取在不涉及既有法律领域规则所规定的私人诉权的情况下，由国家权力机构行使或代为行使基于 AI 算法监管而产生的诉权而并非由利益受损相关方直接行使的救济方式，这可能由算法领域本身的性质所决定，如私人主体在行使请求权时需要面对严重信息不对称的现状等。

但是公权力机构行使或代为行使的方式也需要配套措施的完善以保障救济方式的有效性，例如公共机构代

为请求赔偿是否意味着该等算法的损害要达到一定的额度或造成公共利益损害时才可以起诉？如何分配举证责任？此外，这种事后救济机制能在多大的程度上对利益相关方起到有效救济的功能也需要进一步论证。

尽管目前的治理方式有利有弊，我们发现国际社会对 AI 算法进行事前、事中、事后的治理**依然沿用了物质社会传统法律领域的监管模式**，尚未创设在智能时代虚拟现实社会中新的监管方式。我们仍需要进一步思考，当面对如智能合约等新技术的出现，这种传统的法律监管模式是否可能存在一定的局限性，或者未来对算法的监管是否可能跳出现有思维，针对 AI 算法本身的性质和特点设计新型治理模式，例如是否可能采用算法监管算法的治理模式等。此外，针对上述事前、事中、事后每个具体阶段中的监管方式是否依然有必要采取传统法律模式，例如对算法的事后监管是否仍需局限于现行有关事后救济的法律法规等，都是在算法长期治理过程中亟待解决的问题，有待法律与技术等各界人员进一步探讨。

四、算法治理初衷与企业的应对措施

虽然 AI 算法治理已经成为国际社会研究和探索的焦点问题，但治理 AI 算法的根本原因和初衷仍然并不明确。AI 算法已被应用于社会生产生活的各个领域，而因其导致的损害很大程度上可以通过法律在各个领域既有的规定解决如 AI 算法在劳动雇佣领域的应用应当受制于劳动法的相关规定，因此若雇主通过 AI 算法对雇员进行歧视性待遇，同样构成对劳动法相关条款的违反并应对此承担责任。因此，对算法进行单独规制的原因以及必要性基础仍需要进一步论证。

但有一点是可以明确的，那就是政府对算法的监管已经成为不可逆的潮流，中国也必须顺应趋势，对算法在社会生活中引发的种种问题作出回应。而面对目前实践中的 AI 算法在设计和实施时可能面临的输出结果不确定等诸多问题，目前考虑的监管思路是对现有算法类型以及基础信息等进行初步了解，因此，采取算法备案的监管方式可能有助于达到这一目的。

而对于被规制方企业而言，一方面要认识到算法监管的大趋势，及时自治；另一方面也要向监管部门自证算法合规。具体而言，可以采取如下措施，以降低算法被监管的风险：

1. 梳理现有的算法，尤其是可能被规制的算法；
2. 就核心算法等起草、准备算法可解释性说明；
3. 建立算法内部管理机构；
4. 就 AI 道德伦理测试等建立制度。
5. 针对可能存在的算法歧视、大数据杀熟等现象核查并提供影响报告等。

感谢实习生张子谦、万慧对本文做出的贡献。

数 据 合 规

迎接个人信息保护法的正式生效：《数据出境安全评估办法（征求意见稿）》规则解读

宁宣凤　吴涵　姚敏侣　陈虹吕

引言

根据国家互联网信息办公室（以下简称“国家网信办”）官方网站发布的消息，自 10 月 29 日起的一个月内，《数据出境安全评估办法（征求意见稿）》（“**《办法》**”）正式向社会公开征求意见。《办法》在第一条中开宗明义，明确表示了其出台的目的与价值，即“为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动。”

数据出境的安全管理与评估，自《网络安全法》以来一直成为数据合规领域中的关键性话题。此次《办法》制定的上位法依据，也十分鲜明地将《中华人民共和国网络安全法》（“**《网安法》**”）、《中华人民共和国数据安全法》（“**《数安法》**”）和《中华人民共和国个人信息保护法》（“**《个人信息保护法》**”）这三部当下构成我国网络空间治理框架性规则的基础法律，作为了自身的立规授权来源和上位法依据。尤其是，**作为三部基础法律中与个人信息权益最为密切相关的法律，《个人信息保护法》于 2021 年 11 月 1 日正式生效施行，**

这意味着，在我国迎来网络空间治理规范集中完善、更新浪潮，形成顺应信息时代的系统法律设计的时代节点上，《办法》将成为网络空间治理框架性法律正式成型后，在数据出境安全管理系列规范中具有关键意义和地位的配套规则。

本文下述将对《办法》的规则理解和适用，以及相应的合规理念和价值进行初步解读，以期数据处理者在面临数据出境安全评估与管理问题时，对《办法》的规则适用的框架和原理初步树立基本的出境数据安全意识与合规理念。

一、理解《办法》的适用对象和范围

根据《办法》第二条：“数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和依法应当进行安全评估的个人信息，应当按照本办法的规定进行安全评估；法律、行政法规另有规定的，依照其规定。”对该条的解读，应该至少从《办法》的“适用对象”和“适用范围”等层面进行对应解读。

（一）谁是应当依据《办法》进行评估的行为主体？

在对需要履行数据出境安全评估的行为或业务主体的规定上，《办法》要求“数据处理者”将境内所涉数据向境外提供的场景中，应当进行安全评估。使用“数据处理者”来进行规则约束主体的描述，在此前国家网信办出台的《汽车数据安全管理若干规定（试行）》中已经存在类似做法。但从法律规则的沿革上来看，需要进行出境安全评估的主体，随着对数据出境安全客观风险的认识不断加深，存在一个外延扩展的过程。

一般认为，《网安法》第三十七条首次明确向关键信息基础设施的运营者提出了个人信息和重要数据出境安全评估的法定要求，即“在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”可见，数据出境安全评估制度最初的适用主体一般仅限于关键信息基础设施的运营者。这是因为《网安法》所规制的对象范围是在境内建设、运营、维护和使用网络的运营者，从网络安全的重要性角度出发，《网安法》要求关键信息基础设施的运营者这一特殊类型的“网络运营者”履行数据出境安全评估义务。但考虑到目前大量的数据跨境传输活动可能并非由关键信息基础设施的运营者执行，而且大量的非关键信息基础设施的运营者的数据跨境传输同样可能面临着潜在或者现实的安全风险，因此，原本限定于关键信息基础设施的运营者的评估义务适用对象客观上需要扩张。而自《数安法》以来，随着数据安全义务履行主体的延展，《办法》将“数据处理者”作为适用的主体对象便有了相应的法律基础。不过，由于《数安法》本身未对“数据处理者”这一概念进行法律界定，其是否可以沿用或者借鉴《个人信息保护法》下的“个人信息处理者”的定义还有待进一步探讨。

总体上，《数安法》在立法规范设计的思路上系针对“数据处理”的行为约束法，虽未专门定义“数据处理者”，但在第三十一条中承接了《网安法》第三十七条规定中关键信息基础设施的运营者的出境安全评估要求；同时也进一步通过相关规定，扩充了负有数据出境安全评估的法律义务主体，即“其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。”而《个人信息保护法》第三十八条和第四十条紧接着规定了“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”应该在向境外提供个人信息时的通过国家网信部门组织的安全评估的法定义务。**至此，通过《网安法》《数安法》和《个人信息保护法》在法律条文规则上的相互支撑与补充，为《办法》中要求“数据处理者”履行数据出境安全评估义务提供了全面而完整的上位法基础。**

（二）如何理解“向境外提供”所涵盖的地域范围？

依据国内法律法规（典型如《中华人民共和国出境入境管理法》）和规范性文件对于“境外”的通常用法，除做特殊说明外，一般理解“境外”应当同时包含国外（地区）以及我国的港澳台地区。因此，向国外国家或者地区、我国的港澳台地区提供重要数据和个人信息的数据处理者，如果满足《办法》规定的相应条件，应当主动向主管部门申请开展数据出境安全评估。

上述问题延伸出的进一步思考可能主要在于：今年 7 月由国家网信办公开向社会征求意见的《网络安全审查办法（修订草案征求意见稿）》中规定：“掌握超过 100 万用户个人信息的**运营者**赴国外上市，必须向网络安全审查办公室申报网络安全审查。”而《办法》同样对处理个人信息达到 100 万人的**个人信息处理者**向境外提供个人信息时，提出了申报和开展数据出境安全评估的法定义务。在制度运行上，虽然两条规定的约束对象分别是“运营者”和“个人信息处理者”，两者不完全等同，但在实践中也有可能存在身份的重合。例如，某掌握了超过 100 万用户并处理其个人信息的互联网科技公司，在赴海外上市的过程中，由于上市活动需要，将不可避免地存在向境外中介机构、监管部门提供诸如董事、高管的个人信息，以及公司在接受尽职调查中将对客营业的业务数据中可能包含客户信息等情况。而根据上述规定，这种数据的跨境提供行为，也将分别纳入网络安全审查和出境安全评估的制度监管体系之下。由此，在**可能同时涉及数据出境的场景下，网络安全审查制度与数据出境安全评估制度如何得以衔接或者协调适用？**

我们原则上认同这样的观点：在《网络安全审查办法（征求意见稿）》的前提下，其所规定的“网络安全审查制度”与此次《办法》中规定的“数据出境安全评估制度”在“维护国家安全”这一规范价值点上存在交叉重叠，但在制度构建的原理和规范目的上并不完全相同，**所以应当认为两者属于并行和独立的制度关系**。但我们同时也认可，在前述“处理个人信息超过 100 万人的运营者赴国外上市”的特殊场景中，必不可免地将同时启动运行两个制度。此时，在“维护国家安全”这一规范价值点的共同指引下，网络安全审查制度中所主要考虑的因素之一“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”，可能与数据出境安全评估制度中所需要的各项重点评估事项，呈现出法定要求相似乃至一致的密切关系。在目前未有官方解释或者声明的前提下，虽然不排除需要同时进行两次申报的可能，但就两个制度的理念内核和运行价值均是高度一致的，至于在具体情形下如何做好两个申报制度之间的协调、衔接，以实现监管效率最大化，需要数据处理者接受有关主管部门的进一步指导。

二、领会《办法》的评估原则与价值

《办法》第三条规定的是数据出境安全评估的原则与价值。

首先，“坚持事前评估和持续监督相结合、风险自评估与安全评估相结合”。事前评估与持续监督相结合的原则，事实上贯穿的是数据出境全生命周期管理和风险全链条控制的理念。事前监督可以体现为《办法》中设立或者细化的“风险自评估”和特定情形下的“安全评估”制度；而持续监督，集中体现在《办法》第二十条，即“**数据出境评估结果两年有效期**”的规定。类似规定最早可见于 2019 年《个人信息出境安全评估办法（征求意见稿）》。此外，根据《办法》，如在有效期内出现特定变化，则数据处理者需要重新申报评估。

《办法》中也体现了在确保安全的前提下，保障数据流动自由的规范价值。此前，在《个人信息保护法（草案一次审议稿）》就曾使用“保障个人信息依法有序自由流动”相关表述作为总则第一条。而此次《办法》中将“促进数据跨境安全、自由流动”作为立规目标，彰显了在涉及数据出境安全管理的监管取向，即调动一切以安全为前提和保障下的数据有序、自由流通的价值。

三、申报数据出境安全评估的条件与流程

作为《办法》的主要规定事项以及影响《网安法》《数安法》和《个人信息保护法》中关于数据出境安全管理的关键环节，**如何申报和开展数据出境安全评估，成为数据处理者应当重点关注的内容**。

事实上，在此次《办法》出台之前，有关国家部门分别在 2017 年和 2019 年分别就个人信息和重要数据、个人信息的出境安全评估办法起草相应条款并征求意见。此外，2017 年全国信息安全标准化技术委员会也曾发布《信息安全技术 数据出境安全评估指南（征求意见稿）》，以期对相关方开展数据出境安全的评估工作提供内容和流程上的指引。正如本文开篇言及，相关的规范性文件草拟和征求意见，体现出了人们对于数据出境安全风险本身和管理方法认识的逐步深化。

（一）如何认定申报数据出境安全评估的触发情形？

首先，可以在《办法》解读中得到明确的一点是，**并非所有的数据处理者向境外提供数据都需要通过国家网信部门组织的安全评估**。这一点在《个人信息保护法》中体现得比较明确，根据《个人信息保护法》第三十八条，“通过国家网信部门组织的安全评估”仅是不涉及《个人信息保护法》第四十条规定的情形时，个人信息处理者因业务需要确需向境外提供个人信息应当具备的三个主要条件之任一。

其次，此前分散规定在《网安法》《数安法》和《个人信息保护法》下必须通过有关主管部门的出境安全评估的情形，在此次《办法》的第四条规定中得到了集中体现。从立法法的角度，《办法》作为上述三部上位法的配套性规范，发挥着对数据处理者可能触发申报数据出境安全评估的情形进行梳理、整合规定的重要作用。

总体而言，触发数据出境安全评估申报的条件，判断的关键因素在于数据处理者是否属于“特定身份”和出境数据是否存在“敏感性和规模”的特定情形，以及是否属于国家网信部门规定的其他情形。绘制表格以更为清晰地示意：

判断的关键因素	对应的触发条件
1. 基于数据处理者的“特定身份”	1） 被认定为“关键信息基础设施的运营者”
	2） 个人信息处理者且处理个人信息达到一百万人及以上
2. 基于出境数据的“敏感程度与规模”	3） 出境数据中包含重要数据
	4） 累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息
3. 其他根据规定需要申报的情形	5） 国家网信部门规定的其他情形

具体而言：

◆ 情形 1：“关键信息基础设施的运营者收集和产生的个人信息和重要数据”

该触发情形直接来源于《网安法》第三十七条，也即“数据出境安全评估制度”来源的情形。《数安法》第三十一条中再次强调，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《网安法》的规定。但我们同时注意到，相比于《网安法》第三十七条，该款对个人信息和重要数据的描述中省略了**“在中华人民共和国境内运营中收集和产生的”**这一用作限定范围的定语短句。

对这一变化的理解，至少在文义解释上存在两个维度：其一是，条款在此处仅是作表述省略，并无实

质差异。理由是上位法《网安法》和《数安法》，以及《办法》本身在第二条中均明确要求了“在境内运营中收集和产生的”这一限定性条件，《办法》作为配套性规范，如果将这一限定性条件删除，将可能带来解释上的不当扩张；其二是，条款在此处删除“在境内收集和产生的”这一限定性条件，考虑到部分关键信息基础设施的运营者在向境外提供产品和服务过程中同样可能收集到（至少是）个人信息，而《办法》将此部分收集的个人信息再重新向境外提供的过程纳入数据出境安全评估的监管范畴之内。**基于谨慎合规的立场，我们建议已经被相关主管部门认定为“关键信息基础设施的运营者”的数据处理者，在向境外提供个人信息和重要数据前，将申报安全评估作为数据出境的前提为宜。**

◆ 情形 2：出境数据中包含重要数据

该情形下的触发条件，主要基于出境数据的敏感程度，即包含重要数据。根据《数安法》，一般从“数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度”等角度来对数据进行分类分级。在前述基础上，各地区、各部门将确定本地区、本部门以及相关行业、领域的重要数据具体目录。**而对于列入目录的重要数据，依据此次《办法》，应当严格落实数据出行安全评估申报义务。**

此外，值得数据处理者注意的是，虽然此触发情形中仅说明了“重要数据”，但根据《数安法》相关规定，如果在出境数据中包含了关系国家安全、国民经济命脉、重要民生、重大公共利益等的“国家核心数据”，则根据“举轻以明重”的基本法律逻辑，自然更需要申报并通过安全评估，并不可避免地将面临极为严格的审查。而**如工信部在不久前发布的《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》中更是明确规定“核心数据不得出境”。**

◆ 情形 3：处理个人信息达到一百万人的个人信息处理者向境外提供个人信息 & 情形 4：累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息

这两个情形主要规定的是个人信息（包括敏感个人信息）的出境安全评估申报触发条件。根据《个人信息保护法》第四十条，**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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

显然，《办法》中规定的个人信息出境安全评估申报规则来源于《个人信息保护法》第四十条。由此，**理解这两项触发条件的关键在于如何理解该条中的“处理个人信息达到国家网信部门规定数量”**。从《办法》的规定来看，其应该包含两层不同的含义：其一是，在向境外提供个人信息前需申报出境安全评估的个人信息处理者，其本身即掌握、存储、拥有，或者对多达一百万人的个人信息的处理握有事实上的控制权。如前所述，这是基于个人信息处理者身份的特殊性，其从事的个人信息跨境传输活动即意味着事实推定上的高风险；其二是，在个人信息处理者向境外提供的个人信息达到了涉及十万人以上的程度，或者对外提供的敏感个人信息达到了影响一万人以上的规模。相对而言，这是基于个人信息跨境提供活动带来的客观风险而要求的评估情形。顺带而言，理解其中的“以上”一般包含了“十万人”和“一万人”本数，即分别达到了十万人和一万人规模的个人信息和敏感个人信息出境，便意味着需申报安全评估。

理解上述条件中的两层含义其实并不困难，《个人信息保护法》也将个人信息的“存储”和“向境外提供”作为个人信息的处理进行定义，从文义解释而言，情形 3 和情形 4 均应作为个人信息、敏感个人信息出境安全评估申报的触发条件。**但联系企业的一般实践，我们理解囿于个人信息处理者本身掌握用户基础和跨境传输活动的业务需求，上述触发条件可能会比较常见，因而对于这部分企业而言，意味着进行安全评估申报将属于“规定动作”，而考虑到评估本身的流程性要求，也因此不可避免地将带来更高的合规成本，数据本地化可能将成为长远来看缓解合规压力的替代性方案。**

（二）如何理解数据出境安全评估重点评估事项及内容？

《办法》中的相关条款进一步细化说明和补充了进行数据出境安全评估的重点评估事项和审查要

点，从而提升了数据出境安全评估制度的落地执行力，加强了相关规范的实践指导意义。

首先，从风险预防的立规思路出发，《办法》第八条表明：“数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险。”并且具体从以下事项展开：

1. 数据出境的目的、范围、方式等的合法性、正当性、必要性；
2. 境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规规定和强制性国家标准的要求；
3. 出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险；
4. 数据安全和个人信息权益是否能够得到充分有效保障；
5. 数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务；
6. 遵守中国法律、行政法规、部门规章情况；
7. 国家网信部门认为需要评估的其他事项。

不难发现，综合上述事项中，为了达成客观全面的评估结果，**需要数据处理者就数据出境的全生命周期流程进行尽可能完整的披露**。对于数据出境的合法、正当和必要要求，如评估是否属于法律法规明令禁止的，是否符合我国政府与其他国家、地区签署的关于数据出境条约、协议；基于个人信息主体同意跨境传输时是否已经获得其单独同意，以及还需评估的关键事项，即“是否为从事正常业务活动所必需”（即是否为确需向境外提供数据的情况）。

与此同时，数据出境安全评估不仅需要关注数据传输方的出境动因、传输方式以及数据范围，还需要关注境外的数据接收方所在国家或地区的政治法律环境，以及在境外数据接收方环境中发生数据安全事件、导致数据泄露等不良后果的可能性。此外，一些管理性要求（如数据跨境传输协议）也成为了评估跨境风险的必需事项。

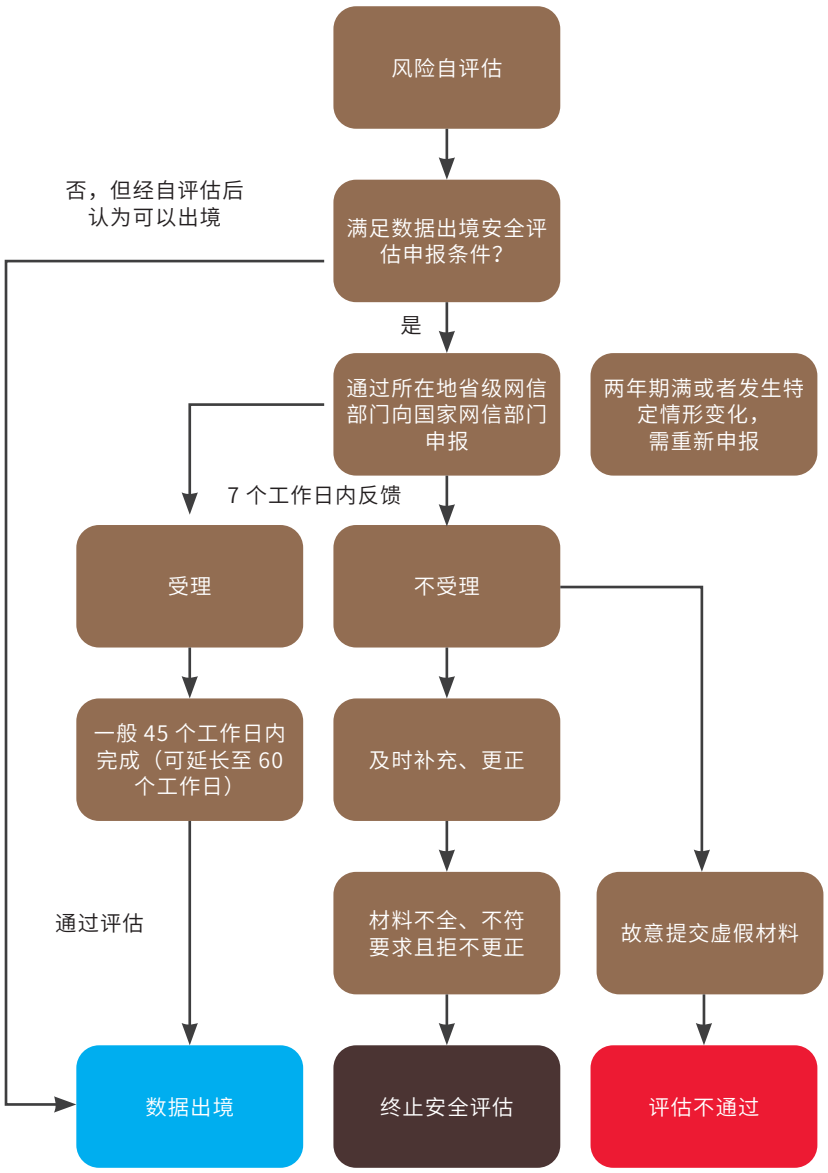
其次，《办法》进一步细化了如何评估上述重点事项中的第五项：“数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务”。具体而言，应当包括但不限于以下内容：

1. 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；
2. 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施；
3. 限制境外接收方将出境数据再转移给其他组织、个人的约束条款；
4. 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导致难以保障数据安全时，应当采取的安全措施；
5. 违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款；
6. 发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。

上述六项应当成为数据跨境传输协议中的必需条款和约定内容。其中，除目前可能已经为数据处理者之间普遍认识并采纳的常规条款之外，需要注意的是，《办法》对限制境外接收方将出境数据进行再次转移提出了特定要求，以及可能需要约定实现前述约束的具体方式。而对于此前常常提及的应当在协议中明确约定双方数据安全保护权利义务关系，也进一步细化于“特殊情况下（接收方变更经营性质或者范围、所在司法辖区发生法律环境变化）采取的数据安全措施”“数据安全违约追责与争端解决条款的可执行性”和“保障个人信息权益响应方式和渠道”以及其他更多方面。

（三）如何认识数据出境安全评估的基本流程和可能结果？

《办法》在相关条款中明确了申报数据出境安全评估的基本流程，同时也在程序性规定的基础上，对于数据处理者申报可能产生的结果（包括程序性结果和实体性结果）做到了可执行落地的细致规定。本文对相关流程性规范和评估可能结果进行绘图示意，以更为清晰地展现。



图：数据安全出境安全评估基本流程与可能结果示意

四、数据出境风险自评估

与在触发特定条件下向有关主管部门申报数据出境安全评估不同，根据《办法》第五条，数据处理者在向境外提供数据前，事先开展数据出境风险自评估成为一项法定义务。

首先，就重要数据出境而言，根据《数安法》第三十一条，数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。由此，**作为该条款中“出境安全管理办法”规范的一部分，风险自评估成为网信办规定下来的一项管理性的强制要求**。

其次，就个人信息出境而言，根据《个人信息保护法》第五十五条规定，个人信息处理者在向境外提供个人信息时，应当事前进行个人信息保护影响评估。我们理解，此处的个人信息出境前的风险自评估制度，与法律中规定应当事先开展的“个人信息保护影响评估”存在同时触发、交叠执行的现实情况。但与上述同时触发监管部门的安全审查或者评估情况不同，考虑到个人信息出境前的风险自评估和个人信息保护影响评估均为企业“自律”行为，因此，从提升数据合规效率一并节约合规成本的角度考虑，企业在进行专

门针对出境业务场景下的个人信息保护影响评估制度设计时，可以将《办法》中规定的个人信息出境前风险自评估视作特殊场景下的个人信息保护影响评估，并考虑将《办法》中着重规定的下述评估要求，与个人信息保护影响评估的要求进行糅合，交由负责个人信息保护合规的部门和同事负责执行。

最后，《办法》明确要求，数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，重点评估以下事项：

1. 数据出境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；
2. 出境数据的数量、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
3. 数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险；
4. 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
5. 数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等;
6. 与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。

与由有关主管部门执行的数据出境安全评估相比，所关注的重点事项和风险基本保持了一致。由此我们认为，数据处理者内部的数据出境风险自评估并没有降低评估的要求、水准，也没有过多地减少必要的评估事项，或是减轻自评估的义务与责任。对于日常业务中涉及数据跨境传输的企业而言，严格遵循相关法律法规要求，建立内部数据出境安全管理制度，成为一个不容忽视的关键合规任务。

五、违反《办法》的相关法律责任

《办法》第十七条以指示性规定条款，强调了数据处理违反数据出境安全评估制度时的法律责任。具体条文为：“违反本办法规定的，依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。”

我们理解，《网安法》《数安法》和《个人信息保护法》中关于违反数据出境安全和不履行网络安全、数据安全和个人信息保护义务的相关罚则条款将得到适用。具体梳理如下：

法律条文	具体内容
《网安法》第六十六条	关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
《数安法》第四十六条	违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

法律条文	具体内容
《个人信息保护法》第六十六条	违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

除上述外，不容忽视的是，关于法律责任的条款还不仅局限于上述三部主要法律，在特定的场景下，还可能包含《消费者权益保护法》《治安管理处罚法》乃至《刑法》的适用；此外，由于上述法律责任所指示的范围还包括“法规”，因此这意味着将来随着我国网络安全与数据合规相关法律法规体系的逐步完善，一系列专门规范（如《关键信息基础设施保护条例》）和特定部门、行业的法规要求也将得到更好地适用。

结语

无疑，这是个特殊的节点。自 2017 年 6 月 1 日，《网络安全法》正式施行已逾三年有余；自 2021 年 9 月 1 日，《数据安全法》正式生效并展现出执行力；2021 年 11 月 1 日，后天，《个人信息保护法》将作为影响力巨大的新法，开始生效实施。我们正在亲历并见证我国网络安全、数据安全与个人信息保护的这座大厦，正在从最初的夯实地基，到如今搭建起房梁支柱，再到如今日之所见与将来之预期，诸如《数据出境安全评估办法》等一系列配套法律法规和规范性文件，将成为一步步落实国家总体安全观下的网络空间治理的智慧。

总体而言，作为数据出境安全管理制度的重要一环，安全评估制度的建立和严格落实，将更好地把控其中的潜在风险，不过，如何更好地设置制度运行的触发机制，以平衡安全和发展的两大主题价值，依然是往后值得社会各方碰撞观点、建言献策的不变话题。

在愈发紧锣密鼓的规范出台之际，数据处理者在积极准备相关合规举措落地，迎接全面的网络数据安全与个人信息保护新时期时，还需要关注数据全生命周期管理中每一个环节、每一处细节的合规风险管控，实时关注着来自技术发展与监管趋势所带来的新矛盾和新要求，在数据驱动的经营理念中树立起合规价值的根本性认知。所谓，我们之所为与所在，即为我们的时代。

责无旁贷
——探讨《个人信息保护法》下互联网平台处理者的特殊责任

宁宣凤　吴涵　林云汉　屈尘

引言

大型互联网平台企业借助网络效应精确匹配供需，极大缩短生产与消费的周期，为社会和商业机构创造了巨大的价值，也为产业结构的优化作出巨大贡献。与此同时，大型互联网平台由于积累了大量包括个人信息在内的产业资源，使得其一举一动都可能对产业市场造成深远影响，直接或间接关联到数字经济的市场经营健康。能力越大，责任越大，大型互联网平台实践中需要承担产业健康发展、数据安全等公共属性的社会责任。因此各国从国家经济安全和数据安全等多个角度都在尝试加强对大型互联网平台企业的监管措施。《中华人民共和国个人信息保护法》（以下简称“《**个信法**》”）第五十八条首次明确规定大型互联网平台的个人信息保护义务，从数据保护的角度回应了国家对大型互联网平台的监管需求。《**个信法**》的出台为大型互联网平台企业数据合规指明了基本原则与合规任务，势必为今后数字经济下互联网企业的发展带来深远影响。

本文将以《个信法》第五十八条为核心，在阐明立法背景的基础上，为企业详细解读平台责任的内涵，以期协助企业在《个信法》正式实施前做好相应的准备，更好地以平台主体的身份参与市场交易。

一、立法背景：“守门人”规则与敏捷治理

（一）设置平台处理者责任的必要性——“守门人”规则的目的

在迅速发展的现代社会中，愈来愈多的商业活动与公共利益以及国家经济安全息息相关，逐步成为监管的重点。这些商业活动呈现出以下特点：第一，从经济角度看，管制对象缺乏竞争对手、无法被排除，具有进入壁垒高、规模报酬递增等特性。对于大型互联网平台而言，其独特叠加的规模经济、网络经济效应和生态竞争范式，不仅加速平台市场走向集中化，而且易导致用户产生路径依赖，被主导平台锁定，从而使得平台市场的集中度呈现出较强的稳定性和持久性，[1] 最终从侧面反映大型互联网平台的市场进入壁垒不低。第二，从影响力度看，用户的经济和社会活动很大程度上依赖其产品或服务的提供，使得用户利益极易受到影响。在实践中，大型互联网平台企业作为服务提供商能够轻松地以单方和有害的方式，为商业用户和最终用户设置商业条件和条款。[2] 基于上述两点，大型互联网平台无疑容易对市场造成重大冲击，从国家经济安全与公共利益出发，往往成为国家监管的中心。近年来，我国已在反垄断法的传统领域迈出了重要的一步，2021 年 2 月 7 日发布的《国务院反垄断委员会关于平台经济领域的反垄断指南》（以下简称“《**反垄断指南**》”）针对国内互联网平台反垄断诉讼频发的现状，在平台经济的相关市场界定、垄断协议、滥用市场支配地位和经营者集中等传统竞争法问题上作出明确规制。

但在互联网产业迅速发展的当下，互联网平台的影响力早已不仅局限于传统竞争法领域，而延展到数字经济的各方各面，其中数据安全保护问题尤为突出——平台势必将发挥其规模经济和网络经济效应的优势，利用其算法优势、巨量用户和完备的生态体系，将用户的个人信息进行高度集中处理，并广泛应用于数据挖掘、用户标签制定、自动化决策、个性化推荐等领域，使得个人用户难以充分理解和掌控其个人信息处理情况。可以想见，面对高度集中产业优势资源、具备完整生态及高度竞争优势的大型平台，个人用户授权平台收集、使用其个人信息的选择权往往是在受限制的条件下作出的。

为此，近年来针对大型互联网平台的合规审查逐渐成为国家个人信息保护监管的重点。2017 年，工信部、国家网信办等四部门开展 APP 隐私政策条款评审工作；2019 年上述部门继续联合开展 APP 违法违规收集使用个人信息专项治理行动；2020 年监管主体与监管行动持续增加，公安部“净网行动”，工信部“APP 侵犯用户权益专项整治行动”均与互联网平台的个人信息保护问题相关。根据工信部官方网站信息，2021 年以来，我国已累计完成 29 万款 APP 技术检测，对其中 1862 款违规 APP 提出整改要求，并下架了 107 款拒不整改的 APP。[3] 由此可见，在《个信法》第五十八条生效之前，大型互联网平台企业的个人信息保护义务已通过各项监管行动初步显现。

然而，监管行动的迅速增加一方面显示出国家对于网络安全与个人信息保护的重视，另外一方面也表明互联网平台侵犯用户权益的现象普遍存在，并且仅靠执法监管治理成效有限，仍需立法进一步完善。具体来看，大型互联网平台借助网络效应吸引、聚集大量用户，其用户个人信息体量之大使得目前的监管治理难以做到全面覆盖。与此同时，广大用户也对部分互联网平台违法违规收集、使用个人信息的问题反映强烈。因此，主要依靠政府对互联网平台实行“单独评估与整改”的模式无法适应目前的客观情况，有必要重新调整监管责任在政府与企业之间的分配。与政府相比，大型互联网平台企业作为网络服务提供者，掌握着用户接入互联网处理个人信息的重要渠道，同时为用户提供必要的技术支持。若由其参与个人信息监管工作，势必可以更有针对性地规范个人信息处理活动，从而达到有效保护个人信息的目的。

综上所述，《个信法》第五十八条对大型互联网平台企业提出特殊的、更高的个人信息保护要求，是维护国家经济安全和公共利益、在数字经济发展的新格局下保障个人信息权益的必然要求。

（二）平台处理者责任是可行的敏捷治理手段

在新一代科技浪潮中，平台成为新经济引擎，不断驱动着技术和商业模式层面的创新。而新兴产业的发展与监管需要寻求治理模式上的突破。因此，

[1] 王磊：《加快推进互联网平台竞争监管现代化》，载《现代研究》2020 年第 11 期。
[2] 高薇：《平台监管的新公用事业理论》，载《法学研究》，2021 年第 3 期。
[3]《我国已完成 29 万款 APP 技术检测对 1862 款违规 APP 提出整改要求》，网址：http://www.gov.cn/xinwen/2021-04/22/content_5601266.htm，最后访问日期：2021 年 9 月 21 日。

各个国家都在寻求具有柔韧性、流动性、灵活性和适应性的敏捷治理方法[4]，而《个信法》第五十八条就是我国在互联网平台敏捷治理层面的大胆尝试。首先，相较于传统的政府监管模式，第五十八条赋予了群众、第三方机构等一定程度的监督权，广泛的参与度有助于提升监管的有效性。同时，考虑到平台自身基于技术垄断而获取的专业性，第五十八条第三款还赋予了平台在审核层面的监管权限，能够有效弥补监管机构的信息盲点。

在法律层面，《个信法》第五十八条并非“开创性”规定，《民法典》第一千一百九十八条规定经营场所的经营者、公共场所的管理者以及群众性活动的组织者具有安全保障义务。大型互联网平台虽非传统意义上的经营场所，但其仍以营利为目的提供各种类型的网络服务，从而将原本分散、潜在的市场交易对象组织起来，形成更大规模的交易群落。[5]这一观点同样被制定《数字服务法（草案）》(the Digital Service Act，以下简称“**《数字服务法案》**”）的欧盟委员会所认可。因此，大型互联网平台企业应对自己控制的网络空间应负有相应的安全保障责任，个人信息保护自是应有之义。

其次，在经济层面，由大型互联网平台企业保护用户个人信息，比政府机关在各个分散的环节投入监管资源更具有经济合理性。事实上，部分关注个人信息保护的互联网企业已自发采取措施，如美国的苹果公司和国内的小米公司。同时，考虑到由法律给所有大型互联网平台设置必要的个人信息保护责任，虽然可能增加少量经营成本，但是同时也会将全行业置于相同的合规标准中，因此我们理解平台责任不会影响企业之间的公平竞争，[6]增加的成本亦可通过定价机制进行分配和转移。故而，无论是从监管方还是平台方的角度出发，设置平台责任具备经济层面的可行性。

最后，在技术层面，大型互联网平台提供了网络服务运行所需的技术环境和运营环境。相关平台企业借助技术上的强大控制力，有能力实现对用户个人信息处理活动的监管。大型互联网平台企业有能力发挥自身资源优势，优化交互流程，规范个人信息处理活动，提出对平台经济的特殊个人信息保护要求，有利于实现监管部门多元共治、敏捷治理，从而在数字经济发展的大背景下实现充分保障公共利益和个人信息权益的目的。

（三）“守门人”规则符合全球的立法监管趋势

对于大型互联网平台处理者的个人信息合规保护要求，在全球已有不少国家有先例可以参考。以欧盟为例，2020年12月15日，欧盟委员会提出《数字市场法（草案）》（the Digital Markets Act，以下简称“**《数字市场法案》**”）和《数字服务法案》。这是欧盟近20年来在数字领域的首次重大立法，旨在明确数字服务提供者的责任，加强对社交媒体、电商平台和其他大型互联网平台的监管。欧盟《数字市场法案》明确设立“守门人”制度，弥补反垄断事后监管应对数字平台垄断问题时的不足，丰富完善了其竞争规制体系，是对欧盟反垄断法的重构。

值得注意的是，欧盟委员会认为：随着大型互联网平台的规模及其在日常生活中越来越多存在，它们有时可以被比作表达和经济交易的公共空间，是促进互联网上信息交流和行使言论自由的关键行为者，也带来了最高的社会和经济风险。[7]因此，《数字服务法案》针对大型互联网平台规定了一系列具体责任，包括：打击网上非法商品或服务，采取科学算法增强内部数据运营透明度以及对其风险管理系统进行独立审查等。可以说，欧盟的《数字服务法案》建立了网络平台问责框架，使平台方明确了“必须做”或“不得做”的业务界限，在强化在线平台内部运营透明度的同时，通过责任平衡机制进一步协调平台方与用户之间的关系[8]。

与此相应，美国《终止平台垄断法案》（Ending Platform Monopolies Act）对大型互联网平台的界定采取了同欧盟相一致的立场。此外，美国联邦贸易委员会（FTC）也在《移动手机隐私披露——通过透明度建立信任》的报告中明确指出，诸如微软、谷歌等大型互联网平台企业，在改善移动设备隐私披露方面拥有极大影响力，建议平台通过及时披露、隐私控制面板等方式实现对用户的充分告知，

[4] 参见薛澜，赵静：《走向敏捷治理：新兴产业发展与监管模式探究》，载《中国行政管理》2019年第8期。
[5] 参见 张守文：《数字经济与经济法的理论拓展》，载《地方立法研究》2021年第1期。
[6] 参见 张新宝：《互联网生态“守门人”个人信息保护特别义务设置研究》，载《比较法研究》2021年第3期。
[7] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
[8] 吴沈括、胡然：《数字平台监管的欧盟新方案与中国镜鉴——围绕<数字服务法案>、<数字市场法案>提案的探析》，载《电子政务》2021年第2期。

向用户传达关键术语和概念，并呼吁利益相关方开发适用于移动设备的禁止追踪机制。[9] 我们理解，未来全球主要互联网空间的治理规范都将逐步落实大型互联网平台企业的监管责任，尤其是在个人信息保护领域的特殊义务。

二、首要难题：如何界定“平台”？

第五十八条规定的义务主体是“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”（即本文所称的“平台处理者”），但目前在法律法规层面并未对上述平台处理者的范围作具体界定。我们结合境外立法、学界讨论与近期行业实践，探讨第五十八条规定的“平台”“重要服务”“巨大数量”和“复杂业务”概念：

（一）“平台”概念的提出

《个信法》虽然没有对“平台”这一概念进行明确解读，但根据《反垄断指南》，我们理解，此处的“互联网平台”是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。《反垄断指南》对平台的定义是从市场竞争的角度归纳总结平台特质。类似地，美国众议院发布的《终止平台垄断法案》对其规制的平台范围作出了明确界定，即：（1）市值超过 6000 亿美元；（2）在美国境内月活跃达到特定规模（五千万 / 在线平台；10 万 / 传统平台）；（3）被视为“关键贸易伙伴”（critical trading partner）的企业。与《反垄断指南》中的定义类似，美国立法者在划定“平台”的范围时，主要考察互联网平台对市场的支配程度、扭曲市场的能力，因此其考量因素包括平台企业的市值、用户规模，以及业务的重要性等。然而，在数据保护领域，对平台的定义可能更加强调其在通讯管道支撑服务与数据应用服务层面的作用。

基于欧盟在数字服务领域的立法实践，我们或许可以管窥我国《个信法》“平台”的范围。前文提到的欧盟《数字服务法案》第三章第三节专门规定了适用于在线平台（Online platforms）的附加条款。在线平台是指信息托管服务的提供者，此类在线平台应用户的要求，存储并向公众传播信息。但上述“在线平台”存在一种例外：如果某平台满足（1）提供纯粹的辅助活动，即其他产品或服务失去其提供的技术支持就无法使用；且（2）将该服务纳入平台功能并不是为了逃避监管，则该平台就不是《数字服务法案》所规制的“在线平台”。此外，《数字服务法案》还强调第三章第三节之规定不适用于小微企业。考虑到《数字服务法案》的立法思路与第五十八条具有一定的相似性，我们理解“在线平台”与第五十八条的“平台”在性质上可能具有一定的相似性，但其范围应该更大。我们理解，《数字服务法案》第三章第四节规定的“超大型在线平台”（Very large online platforms）可能与《个信法》中的“平台”概念更为相似，但欧盟认定“超大型在线平台”的主要考量因素是用户数量（我们将在“用户数量”部分详述具体的认定逻辑与认定思路），而我国还将从平台提供服务的重要性、业务的复杂程度进行综合性考察认定。

（二）“重要服务”：维护国家与公共安全的本意？

《个信法》二审稿中使用了“提供基础性互联网平台服务”来定义平台处理者，而在《个信法》正式稿中，该术语变为“提供重要互联网平台服务”。此前曾有学者提出，平台处理者主要指三类平台，即应用程序的分发平台、移动终端操作系统、搭载小程序的“超级 App 平台”。上述三类平台的共同特征是能够提供第三方移动 App 的接入（包括分发、下载、更新等），或向第三方移动 App 运营提供技术资源和信息收集渠道，以及提供市场和用户触达的中介服务。[10] 换言之，此处的“基础性”主要指为第三方移动互联网服务提供基础性或支持性服务，起到一个“通道”的作用，该等平台往往坐拥大量用户与流量，接入或合作的第三方也多种多样。

从“基础”到“重要”的转向，也便于与《数据安全法》中的“重要数据”相衔接。《数据安全管理办法》（征求意见稿）将“重要数据”定义为“一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据”。因此，此处的“重要服务”也不排除与国家安全、经济安全、社会稳定、公共健康和安全等因素有关。因此，我们理解，“重要服务”的范围可能较之于二审稿提出的“基础服

[9] Mobile Privacy Disclosures Building Trust through Transparency, https://www.ftc.gov/reports/mobile-privacy-disclosures-buildingtrust-through-transparency-federal-trade-commission, 转引自同注释 6。
[10] 同注释 6。

务”更加注重业务自身的重要性。如果某平台提供的服务并不属于基础性或支持性服务，但其收集、处理的个人信息具有较高重要性和敏感性（如收集大量个人敏感信息或个人生物识别信息），则其依然可能被认定为提供“重要互联网平台服务”。

（三）“用户数量”：需要动态关注的门槛

《个信法》下的平台需满足“用户数量巨大”这一要求，但暂未说明具体需达到何种量级。《信息安全技术 个人信息安全规范》第 11.1 条要求处理超过 100 万人的个人信息或超过 10 万个人敏感信息的企业设置专门的个人信息保护负责人和个人信息保护工作机构。我们理解，个人信息保护负责人义务主要针对处理数据达到国家网信部门规定数量的个人信息处理者，具有一定普遍性；而第五十八条规定的义务主要针对国内大型互联网平台，因此二者并不相同。此外，无论用户数量的认定标准如何，广泛适用第五十八条都可能不符合比例原则，高昂的合规成本甚至可能在一定程度上扼杀创新。学者研究显示，我国国内常用的应用分发平台不超过 10 个，移动终端操作系统不超过 10 种，搭载小程序的“超级 App”平台目前不超过 8 个。[11]

美国和欧盟在与平台竞争相关的法律草案中对大型平台的用户数量标准进行了明确的界定。欧盟《数字市场法案》认定守门人的标准包括该平台是否“控制了经营者和终端用户之间的重要通道”。具体而言，在 To C 端层面，该法案下使用核心平台服务的月活跃终端用户数应当超过 4500 万，此处的用户既包括本土用户，也包括暂居于欧盟境内的用户；在 To B 端层面，该法案将上一财政年度内拥有注册于欧盟境内的商业用户超过 10000 家的平台视为守门人。而美国《终止平台垄断法案》同样要求平台在美国境内月活跃达到特定规模，即 5000 万 / 在线平台或 10 万 / 传统平台。由此可见，无论是《数字市场法案》还是《终止平台垄断法案》，其用户数量标准都是从市场竞争的角度出发，基于平台对平台内经营者或用户的支配程度制定的。

然而，《个信法》在用户数量层面可能更加关注平台掌握大量个人信息后，因系统入侵、数据保护不周，或数据滥用等原因导致个人信息主体权益受到侵害的风险。在这一方面，《个信法》的逻辑与《数字服务法案》更类似。欧盟立法者认为，大型在线平台可能造成的社会风险在范围和影响程度方面都远超小平台，一旦某平台的用户数量达到一定程度，其造成的系统性风险就可能对欧盟产生不成比例的负面影响。欧盟立法者将这一平台用户数量门槛定位欧盟总人口的 10%，即 4500 万。同时，鉴于上网人数并非一成不变，因此在 10% 的标准上，欧盟将不定期基于人口数量对用户数量门槛进行调整。然而，考虑到我国的人口基数、经济水平、信息产业发展程度等均与欧盟存在较大差异，因此在用户数量标准问题上，《个信法》可能与《数字服务法案》有所不同，随着人口和数据经济水平的发展，用户数量标准也建议设立动态的检验标准。

（四）“业务类型”：结合多方面现实因素综合考量

除服务内容、用户数量外，《个信法》还要求平台具有复杂的业务类型。考虑到平台数据来源的多样性、数据处理的透明度、可解释性等多方面因素，将业务类型纳入界定平台范围的考量因素具有合理性。从当前业务实践来看，我们理解，有以下几类业务模式可能被认定为“业务类型复杂”：

（1）“超级 App+ 小程序”：在该场景下，超级 App 作为内容分发平台可能对接各种第三方小程序，可能存在大量个人信息收集、共享、处理活动 [12]。

（2）内嵌多种业务功能的单一 App：例如，在某生活点评类 App 中，可能同时提供外卖服务、在线旅行社、移动出行、社区团购，以及金融服务等多种业务功能。

（3）通过多种渠道提供在线服务：考虑到互联网平台出于差异化打法、开展新业务等需求，可能同时通过不同的渠道提供多种在线服务，而不同服务之间可能出现交互，从而构成一种体系性的复杂业务网络。

此外，美国《终止平台垄断法案》提到的“关键贸易伙伴”这一概念也对业务类型作出了一定要

[11] 同注释 6。
[12] 同注释 6。

求。“关键贸易伙伴”是指有能力限制或阻碍业务用户访问其用户或客户的实体，或限制或阻碍业务用户访问其有效为用户或客户服务所需的工具或服务的实体。我们理解，关键贸易伙伴的认定主要旨在强调平台对用户的支配力，即是否可能限制或阻碍用户实现其自由访问的权利，而《个信法》的要求则重点关注业务类型的复杂程度，因此二者存在一定差别。我们理解，判断业务类型的复杂程度可能需要结合平台运营主体及其关联公司开展的业务、平台对接的第三方业务、平台内部的数据交互程度等多方面因素进行综合考量。

三、平台处理者的四大义务

第五十八条对平台个人信息处理者提出了四大个人信息保护的特殊义务，其中不乏在个人信息保护领域具有开创意义的保护要求。

（一）健全个人信息保护合规制度体系，建立外部独立监督机构

《个信法》第五十八条首先要求企业建立健全个人信息合规制度体系，并成立主要由外部成员组成的独立机构对平台进行规制。“个人信息合规制度体系”是《个信法》相对于此前《个信法》二审稿新增的内容，首次从个人信息保护角度在法律层面对平台处理者提出了明确的制度体系要求。此前，《网络安全法》第二十一条仅对网络运营者从网络安全等级保护角度提出了“制定内部安全管理制度和操作规程”的一般性要求，这导致了从法律层面《网络安全法》可能仅被理解为要求企业建立信息安全属性的制度文本，如信息安全管理总则、信息安全组织机构制度、信息安全人员管理制度、系统建设管理制度、系统运维管理制度等，而未能将制度要求细化到个人信息保护层面。《个人信息安全规范》第 11.1 条虽然也要求个人信息控制者组织制定、落实和更新个人信息保护工作计划、政策、内部制度和相关规程，但《个人信息安全规范》仅属于推荐性国家标准，不具有强制执行力。

但更值得关注的，是成立个人信息保护独立监督机构的要求。这是《个信法》独创的个人信息保护领域的独立监督机构机制。目前，第五十八条没有规定独立机构的任免程序、成员门槛、报酬、负责机制等，但反垄断领域经营者集中的监督受托人机制对理解该制度有较大的参考价值。

监督受托人机制在欧盟与美国实施已久，在中国近年来也已成为经营者集中的一大监管利器。根据 2020 年 12 月 1 日施行的《经营者集中审查暂行规定》的第四章，对于附加限制性条件批准的经营者集中，市场监管总局可以通过监督受托人对义务人履行限制性条件的行为进行监督检查。经营者集中监督受托人由义务人委托并支付报酬，对义务人进行督查，但该监督受托人的指派需经市场监管总局评估确定，且受托人对市场监管总局负责。根据第四章要求，受托人应当独立于义务人和剥离业务的买方、具有具备所需专业知识技能的专业团队、具有可行的工作方案、能符合市场监管总局提出的其他要求等，而实践中往往由律师事务所、会计师事务所等外部专业机构承担。从外部成员、机构独立性等构成要件来看，《个信法》第五十八条规定的个人信息独立监督机构与经营者集中的监督受托人有较大的相似性，我国在经营者集中领域已积累的成熟的监督受托人制度应用经验[13]势必将为《个信法》第五十八条第（一）款的实施提供宝贵的实践支持。不过，该制度如何具体落地执行仍有较多地方待后续的配套制度文件进行展开，例如：“主要由外部成员组成”，则非外部成员可以占比多少，可以多大程度参与监督？外部成员的准入资质如何确定，如何参考《经营者集中审查暂行规定》的监督受托人资质要求？如何确保平台处理者承担成本的同时，保证独立机构向网信部门等监管机构负责，特别是确保机构人员履行监督责任？如何具体开展监督，机构具体有哪些监督权限？等等。

（二）制定公开、公平、公正的平台规则

《个信法》出台前，个人信息处理者的规则公开义务主要限于对个人信息处理规则的披露，如隐私政策。但考虑到大型平台运营机制以及个人信息处理情况的复杂性，仅公开隐私政策可能难以使用户及监管部门完整了解个人信息的处理情况与目的。例如，用户标签是大型互联网平台最重要且用途最广泛的个人信息，其处理往往与平台复杂的功能与机制挂钩，仅通过隐私政策中的自动化决策等条款披露标签数据的处理方式和目的，可能存在披露内容流于形式的问题，使得用户无法全面了解自

[13] 例如，《关于附加限制性条件批准丸红公司收购高鸿公司 100% 股权经营者集中反垄断审查决定的公告》，商务部公告 2013 年第 22 号。

身标签的实际应用场景和算法机制对用户造成的影响。为此，第五十八条第（二）款要求平台处理者“遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务”。考虑到平台运行机制的复杂性，该条显然并不意在重申第五十一条制定对内的管理制度与操作规程要求；另一方面，该要求也可能并不是简单重复第七条关于公开隐私政策等个人信息处理规则的要求，而可能进一步指向包括了披露个人信息运作相关的平台运作机制，例如平台介绍、网络安全保护机制、SDK 具体应用机制、标签应用场景、自动化决策的算法、常见问题等。考虑当前对第五十八条具体适用仍有待细化，“平台规则”的外延和内涵有待后续补充，但当前不少头部互联网平台都设有法律规则汇总页面以及开发者平台的规则中心，这些实践可以在当下为平台处理者制定《个信法》下的公开规则提供一定的参考价值；此外，平台处理者还可以参考电子商务平台根据《电子商务法》第三十二条制定公开平台交易规则的具体实践，来落实在《个信法》下的平台规则公开方式方法。

（三）对严重违法违规的平台内产品或服务停止提供服务

大型互联网平台自身即是生态圈，其中的产品和服务不仅由平台运营者自身提供，还可能由进驻的第三方商家以及用户提供。对于大型平台而言，第三方产品和服务可能良莠不齐，若管理不善则可能广泛存在对个人信息的侵权行为。在《个信法》生效前，《网络安全法》《民法典》仅笼统地规定了个人信息处理者保护个人信息的义务，停止违法违规处理个人信息行为的义务往往仅限于个人信息主体提出权利请求，或处理者发现违法违规事项后，但并没有明确采取积极制止措施的义务。而《网络信息内容生态治理规定》虽然规定了网络信息内容服务平台的管理主体责任，要求平台方建立完善的账号管理、信息审核、实时巡查等积极的生态治理机制，但该主动审查义务仅限于对色情、暴力、恐怖等违法违规的信息内容，并未延伸到违法违规处理个人信息。

为此，第五十八条第（三）款要求平台处理者“对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务”，对平台施加了个人信息保护的监督义务。然而，该条款仅规定了停止提供服务的要求，但并没有就平台是否以及如何采取措施发现严重违反法律法规的处理行为进行细化，也未明确平台处理者是否以及如何建立相应的主动监管机制。该条在后续的实施中，平台将被多大程度施加积极的个人信息处理管理责任与审核义务，有待后续观察。当前情况下，平台可以参照《网络信息内容生态治理规定》的平台方内容监管实践以及《电子商务法》下电子商务经营者对产品质量、消费者权益、知识产权、网络安全与个人信息保护等方面的保障与监督实践，制定相应的平台个人信息主动管理机制。

（四）个人信息保护社会责任报告

发布企业社会责任（CSR）报告是平台自律的重要表现形式之一。传统的企业社会责任主要包括经济责任、文化责任、教育责任、环境责任等，其关注点也往往聚焦在可持续发展、公益活动、劳工权益等方面。而信息技术和互联网的发展为企业社会责任议程增加了新的课题，如网络安全、数据管理、个人信息保护和网络平台责任等。互联网具有“技术工具”和“信息平台”的双重属性，在其边界不断扩大的同时，大规模的市场将影响成千上万的个人信息主体，有必要将个人信息纳入企业社会责任的考量范围。因此，许多企业都逐渐开始在其企业社会责任报告中披露个人信息保护的具体情况。例如，腾讯提出了“科技向善，数据有度”的隐私保护理念，并强调“把个人信息和数据安全放在优先地位”[14]。

然而，互联网平台往往只在其集团年度社会责任报告中设置某一小节披露个人信息保护情况，篇幅较短，内容也不甚充分，且部分互联网平台甚至未在其企业社会责任报告中披露与个人信息保护有关的内容；此外，考虑到此前并无强制的法律法规要求，部分互联网平台并非每年发布都会发布企业社会责任报告。《个信法》将定期发布个人信息保护社会责任报告作为互联网平台的法定义务，能够有效提升企业合规意识，促进平台自律。

当前互联网平台在其企业社会责任报告中披露的个人信息保护相关内容包括但不限于隐私保护方

[14]《2019 腾讯社会责任报告：向善力》，网址：https://static.www.tencent.com/uploads/2020/11/20/080fa12557087ba52b7ac4bef6504359.pdf，最后访问日期：2021 年 9 月 22 日。

法、合规管理体系、数据保障措施等。例如，在数据安全保障方面，部分互联网平台会在其企业社会责任报告中声明其已实施网络安全等级保护评级与备案，且获得 ISO 等隐私信息管理体系认证；在用户权利实现方面，某些平台还会在报告中披露其响应数据主体请求的次数。然而，鉴于《个信法》并未详细说明个人信息保护社会责任报告应当包含的内容、发布报告的频率、社会监督的方式等问题，具体的实施方式仍需法律法规进一步释明。

四、企业宜如何应对平台处理者特殊监管要求?

在《个信法》体系下的法规、指南、标准均未出台的情况下，互联网平台应当如何履行《个信法》第五十八条规定的平台义务?

在平台主体认定层面，企业首先应当基于《个信法》第五十八条之规定，从服务的重要程度、用户数量、业务类型等方面综合评判自身是否落入“平台”的范围内。在法规未进行细化的情况下，企业可适当参考境外立法以及其他领域立法。同时，企业应当自行或通过行业协会与监管部门积极沟通，明确“平台”的认定标准等问题。比如在《数据安全法》生效前，工信部就曾委托中国互联网协会召开头部平台座谈会，召集 12 家互联网企业参加，并就强化平台数据管理责任，明确数据安全责任人，加强重要数据安全评估和出境管理等问题作出指示。[15]

在合规义务层面，在考虑到信息的第三方审计、隐私保护社会责任报告等行业最佳实践于企业而言同时也是十分有效的宣传媒介，因此如企业认为自身可能被认定为“平台”，应当尽可能贯彻落实第五十八条之义务，一方面能规避合规风险，另一方面可提升正面形象。考虑到当前监管尚未出台第五十八条的实施细则，企业在贯彻落实平台特殊义务时，可以如本文第三章所述，比照参考此前其他领域的法律法规相关制度，从严解释第五十八条以推动合规方案的落地，如参考《经营者集中审查暂行规定》设置独立监督机构、参考《电子商务法》和产业实践制定公开的平台规则、参考《网络信息内容生态治理规定》与《电子商务法》建立积极的个人信息审查与治理机制等。

结语

《个信法》第五十八条的平台处理者特殊义务，不仅体现了数字经济时代下对用户个人以及其他市场参与者的特殊保护，更是从国家安全与公共利益出发，面对平台经济为市场带来的巨大机遇与冲击而充实监管工具库、实现敏捷监管治理的必然要求。将大型互联网平台的“守门人”规则从竞争法延伸至个人信息保护领域，体现了我国对互联网经济的敏锐观察与强化数据保护的决心，也揭示了我国平台企业的数据合规之路任重而道远。我们将持续关注平台处理者义务后续实施细则的出台与行业实践动态，与大家共同探讨我国平台经济繁荣发展大背景下平台数据治理与保护新路径。

感谢实习生王璐瑶对本文的贡献。

[15]《工信部召集 12 家互联网平台开会 要求落实＜数据安全法＞》，载自财新网，网址：https://www.caixin.com/2021-07-30/101748909.html，最后访问日期：2021 年 9 月 22 日。

知我者，当谓我心忧：个人信息自动化决策的法律规制与合规要求

宁宣凤　吴涵　潘驰　姚敏侣

引言

不知你是否感同身受，我们已经身处在这样的一个虚拟但又无比真实的“熟人社会”：虽仍然渺小，但作为数字时代巨幕中的每一个“像素点”，无限扩张的互联网空间将每一件点滴的过往，都像刺青一样刻画在我们的“数字皮肤”[1]上。人们彼此不相知、不相识，但有人却比你更了解你的喜好、你的过往，乃至于你未来的可能。与此同时，你的标签取代了你的名字，描述一个人远比识别一个人更重要。与此同时，正如已经被人无数次提及的“啤酒和纸尿裤”故事，大数据分析和自动化决策作为有效的可以显著提升平台创造用户价值和市场需求的手段或者工具，被公认成为互联网竞争的制胜秘籍[2]。在此基础上，个人信息和海量的数据成为推动互联网乃至整个社会生产力机器运转的原油与动力。

显然，大数据的预言家们早就料想到了这样的社会结构与场景，但原先可能他们憧憬和向往的全新时代遭遇了一系列令人措手不及的现实问题，“大数据杀熟”无疑是其中的一个典型。本文将以“大数据杀熟”为切口，对其背后的自动化算法运行机制和《个人信息保护法》第二十四条的法律规范要义进行探究与考察，最后为互联网市场竞争主体如何合法合规运用自动化决策机制提供些许启发。

一、个人信息自动化决策的法律意义与规制框架

（一）通过规制自动化决策以规避“大数据杀熟”的理论逻辑

“大数据杀熟”背后引人愤怒的道理其实很简单：当我们事后发现达成的交易、采纳的行为是提供方通过研究我们的喜好、过往，而基于全部关于

[1] VIKTOR MAYER-SCHÖNBERGER: “Delete: The Virtue of Forgetting in the Digital Age”, *Princeton University Press, 2009*.
[2] Geoffrey G. Parker & Marshall W. Van Alstyne & Sangeet Paul Choudary:《平台革命: 改变世界的商业模式》，志鹏译，机械工业出版社，2019 年。

我们的历史信息形成的洞察甚至偏见，对于时下的消费或者未来的行为进行自主预判，并施加不合理的影响而形成的结果，我们会不满于这种类似于原先时常发生在熟人社会中的“差别待遇”，或者说，我们因为自己的某种特征为相对方所熟悉后而受到了“歧视”。

但与以往最主要的不同点在于，这种所谓的“差别待遇”或者“歧视”的产生，或许仅来自于一种自动化程序的结果，至少在这种结果产生的时点缺少人为干预的因素。**这成为判断企业运用自动化决策而可能带来差别待遇时，其合法性、合理性备受争议的问题焦点。**

从简要的经济学观点来看，“大数据杀熟”实则产生于一方利用自动化决策所产生的信息差。典型的大数据杀熟是交易中的一方利用其充分掌握的交易相对方的信息，来进行个别化的、差异化的定价。这种差异化定价策略，在此前之所以不普遍，主要是因为相关方难以掌握交易相对人的足够信息以及处理相关信息时存在很大难度。但随着互联网信息技术的发展，消费者数据被大量收集以及商家数据处理、运用能力的飞跃，使得差异化定价不再是困难的事情。因此从理论和逻辑上看，在未来的商业实践中，商家采取差异化定价的策略会越来越普遍。[3] 不可否认的是差异化定价策略具有一定经济意义上的合理性，比如基于不同交易主体的特点达成不同的交易条件，定制化地提供服务。

但与此同时，上述基于“定制化服务”而形成的差异化定价策略的前提在于交易双方对于交易条件的合理性和公正性至少不具备显著的信息壁垒。即使交易方就交易条件形成合意，在大数据分析工具、自动化决策这样高效率的算法机制介入的情形，我们无法期待交易中的消费者作为个体，可以对其所达成的全部交易条件的合理性、公正性作出完全准确的预判。

因此，如何在进行互联网营销、广告推荐以及达成交易的过程中合法设计、使用自动化决策的算法程序，成为法律可以介入的关键节点。我国《个人信息保护法》在定义条款中明确表示，“自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。”上述“大数据杀熟”的产生过程，便是自动化决策的自然结果，而《个人信息保护法》第二十四条便通过规制“自动化决策”作为一种生产工具的使用方式，要求自动化决策机制的透明度、公正性，以及在展示自动化决策结果的多样性、保障个人对自动化决策的解释说明权和拒绝权等一系列组合拳的方式，以尽可能规避“大数据杀熟”的消极后果。

（二）通过规范个人信息处理以治理“大数据杀熟”的规则要义

那么，**“大数据杀熟”可能带来何种消极后果**？为何法律需要通过规制个人信息处理的方式，以实现对“大数据杀熟”的治理？这又是另一个有趣且深刻的话题。

从最为直观的感受上来看，当个人因自动化决策结果而遭受“大数据杀熟”时，第一反应是直觉上的“不公平”。在法律上来看，这种公平感的缺失，可以理解为个人作为消费者在未充分知情的前提下，未被公平、公正地对待。因此，平台经济下的“大数据杀熟”行为，的确有可能构成《消费者权益保护法》下的侵害消费者知情权、公平交易权的违法行为。但对于此性质的定性分析，需要慎之又慎，原因在于商业实践中完全相同的交易环境和交易条件非常少见，衡量公平交易权的介入因素还应当包括时间、地域乃至消费动机。换句话说，并非接受了不同的交易价格，消费者便可以径直认为自身受到了“价格歧视”。当然，这也成为现行法律规则中通过界定何为“交易条件”和“合理差别”等约束自动化决策实现平衡的规则设计时的难点，本文将在后文详细介绍分析。此外，为了与《消费者权益保护法》相衔接，《电子商务法》第十八条第一款通过约束自动化决策的展示选项，即搜索结果的呈现方式上，以保障消费者的公平交易等基本权益。但无论如何，上述规则均适用于消费领域，而互联网空间中使用自动化决策分析的场景其实更为广泛。

其次，“大数据杀熟”作为一种间接的消极结果，还有可能成为不正当市场竞争行为，乃至市场

[3] 薛军:《大数据杀熟的是与非》，载“法治日报”，http://views.ce.cn/view/ent/202010/21/t20201021_35915415.shtml 最后访问日期: 2021 年 9 月 12 日。

主体利用算法技术而滥用支配地位、实施垄断的具体表现。就目前所受关注的典型案件而言，不难发现，由于平台效应愈发加剧的赢者通吃局面，大型或者超大型互联网企业凭着优势的算法与数据竞争地位，在技术规则的隐蔽之下实施不合理的差异化推荐和交易实则更为普遍和典型，而如果法律放弃对此类行为的规制，无疑是对其滥用技术优势条件而扭曲合理的市场竞争秩序、损害其他市场竞争者，最终导致社会整体福利受损等可能结局的纵容。但客观地说，《反不正当竞争法》和《反垄断法》的保护法益主要着眼于市场主体的竞争利益和社会层面的竞争秩序，且适用于各自的条件和范围，因此，对于因不合理地利用自动化决策机制带来的消极后果，仍有待于更为直接的新规建制。

从根本上说，算法等自动化决策机制是互联网平台提供服务的一种工具和具体手段，而“大数据杀熟”作为一种外在的消极表现结果，**来源于对其用户个人信息和海量数据的滥用**。因此，对于“大数据杀熟”孰是孰非的讨论，如果说可能存在某些法律层面上的问题，那就在于平台或者商家收集用户个人信息，并且利用这些信息对用户进行数据画像的行为是否合法合规。采用大数据技术来分析特定用户的消费习惯，从而进行差异化定价，**应该被限制于用户知情同意以及法律允许的范围之内**。[4] 因此，综合以上分析，“大数据杀熟”的本质是未能在合法性和合理性的法律框架内处理个人信息，从而产生的对消费者个人合法权益的“侵害”和对市场竞争的“乱序”。**有效地规制“大数据杀熟”，根源上需要着眼于约束个人信息处理者处理个人信息的合法性、合理性要求**。

（三）规制利用数据和算法技术，实现利益平衡的法律框架

时下，对于利用大数据分析技术实现个性化内容推荐的算法而言，已经受到了日渐严格的监管。而经我们的归纳整理，如果聚焦于“大数据杀熟”背后的数据与算法技术规制，结合不同的规范领域和层次，已然形成了一整套利益平衡的法律规则框架。

在这个框架体系内，以《电子商务法》《个人信息保护法》等近些年的互联网时代立法，以及《在线旅游经营服务管理暂行规定》《深圳经济特区数据条例》等为代表的部门规章或者地方性法规等，通过具体条文的方式体现出了相近的价值理念。以下是我们梳理的法规总结表。

法律法规	具体条款
《个人信息保护法》	**第二十四条** 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。 通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。
《反垄断法》	**第十七条** 禁止具有市场支配地位的经营者从事下列滥用市场支配地位的行为： （六）没有正当理由，对条件相同的交易相对人在交易价格等交易条件上实行差别待遇。

[4] 同上注 [3]。

法律法规	具体条款
《消费者权益保护法》	**第十条** 消费者享有公平交易的权利。 消费者在购买商品或者接受服务时，有权获得质量保障、价格合理、计量正确等公平交易条件，有权拒绝经营者的强制交易行为。
《价格法》	**第十四条** 经营者不得有下列不正当价格行为： （五）提供相同商品或者服务，对具有同等交易条件的其他经营者实行价格歧视。
《电子商务法》	**第十八条** 电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。
《在线旅游经营服务管理暂行规定》	**第十五条** 在线旅游经营者不得滥用大数据分析等技术手段，基于旅游者消费记录、旅游偏好等设置不公平的交易条件，侵犯旅游者合法权益。
《互联网信息服务算法推荐管理规定（征求意见稿）》	**第十八条** 算法推荐服务提供者向消费者销售商品或者提供服务的，应当保护消费者合法权益，不得根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实行不合理的差别待遇等违法行为。
《禁止网络不正当竞争行为规定（公开征求意见稿）》	**第二十一条** 经营者不得利用数据、算法等技术手段，通过收集、分析交易相对方的交易信息、浏览内容及次数、交易时使用的终端设备的品牌及价值等方式，对交易条件相同的交易相对方不合理地提供不同的交易信息，侵害交易相对方的知情权、选择权、公平交易权等，扰乱市场公平交易秩序。 交易信息包括交易历史、支付意愿、消费习惯、个体偏好、支付能力、依赖程度、信用状况等。
《价格违法行为行政处罚规定》（修订征求意见稿）	**第十三条【新业态中的价格违法行为】** 违反价格法第十四条规定，有下列情形之一的，给予警告，可以并处上一年度销售总额1‰以上，5‰以下的罚款，有违法所得的，没收违法所得；情节严重的，责令停业整顿，或者吊销营业执照： （一）电子商务平台经营者利用大数据分析、算法等技术手段，根据消费者或者其他经营者的偏好、交易习惯等特征，基于成本或正当营销策略之外的因素，对同一商品或服务在同等交易条件下设置不同价格的。

法律法规	具体条款
《国务院反垄断委员会关于平台经济领域的反垄断指南》	**第十七条 差别待遇** 具有市场支配地位的平台经济领域经营者，可能滥用市场支配地位，无正当理由对交易条件相同的交易相对人实施差别待遇，排除、限制市场竞争。分析是否构成差别待遇，可以考虑以下因素： （一）基于大数据和算法，根据交易相对人的支付能力、消费偏好、使用习惯等，实行差异性交易价格或者其他交易条件； （二）实行差异性标准、规则、算法； （三）实行差异性付款条件和交易方式。 条件相同是指交易相对人之间在交易安全、交易成本、信用状况、所处交易环节、交易持续时间等方面不存在实质性影响交易的差别。平台在交易中获取的交易相对人的隐私信息、交易历史、个体偏好、消费习惯等方面存在的差异不影响认定交易相对人条件相同。 平台经济领域经营者实施差别待遇行为可能具有以下正当理由： （一）根据交易相对人实际需求且符合正当的交易习惯和行业惯例，实行不同交易条件； （二）针对新用户在合理期限内开展的优惠活动； （三）基于平台公平、合理、无歧视的规则实施的随机性交易； （四）能够证明行为具有正当性的其他理由。
《深圳经济特区数据条例》	**第六十九条** 市场主体不得利用数据分析，对交易条件相同的交易相对人实施差别待遇，但是有下列情形之一的除外： （一）根据交易相对人的实际需求，且符合正当的交易习惯和行业惯例，实行不同交易条件的； （二）针对新用户在合理期限内开展优惠活动的； （三）基于公平、合理、非歧视规则实施随机性交易的； （四）法律、法规规定的其他情形。 前款所称交易条件相同，是指交易相对人在交易安全、交易成本、信用状况、交易环节、交易持续时间等方面不存在实质性差别。

二、自动化决策约束下个人信息处理规则重点研讨

（一）第二十四条第一款解读

“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。”

1. 如何理解“保障决策的透明度”

显然，《个人信息保护法》第二十四条第一款对于自动化决策的过程透明性和结果的公平性提出了法律上的要求，即“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正”。

一般理解来看，对于过程的透明性要求，一方面与个人信息处理者使用了自动化决策的算法机制的可解释性以及解释的程度相关，另一方面，也向个人信息处理者提出了向个人信息主体告知其所可能用于自

动化决策、用户画像分析以及基于此所进行的一系列大数据处理活动规则的必要性。实践中常见的提升个人信息处理自动化决策机制透明性的方法，如在隐私政策中明确告知使用自动化决策或者画像分析技术的业务场景，并且在具体的业务模块或者前端界面中使用通知横幅、弹窗或者页面标签等形式向用户明示自动化决策机制的使用。此外，还可以专门形成对自动化决策机制所使用的个人信息类型、目的和方式等基本要素的单独描述文件，以满足相应的法律要求。

2. 如何理解“在交易价格等交易条件上实行不合理的差别待遇”

与“决策过程透明度”要求一起被规定在此次《个人信息保护法》条款中的，还有“决策结果的公平公正性”要求。如前所述，自动化决策作为一类算法机制，其使用在法律上并不必然具有被责难的属性，但之所以需要对自动化决策机制进行一定的法律规则限制，原因在于对于这类算法机制的使用不当，便有可能形成结果上的失衡，从而导致个人信息主体权益受到侵害，而最为典型的表现就是当个人信息主体为消费者时的公平交易权受损。

从法律规定的解释上看，**把握自动化决策机制结果公正性要求的关键，在于确保在交易价格等交易条件上的“差别待遇”被控制在“合理”的范围之内**。事实上，该条款其实从侧面认可了个人信息处理者通过大数据分析和自动化决策机制，为个人信息主体提供个性化和定制化的服务，这种合理范围内的个性化服务的差异待遇，也可以体现在包括对个人在交易价格等交易条件上。我们看到由于个性化推荐、定制化服务对于互联网经济效率和整体福利提升的好处，因此，首先需要明确的是，《个人信息保护法》以及相关法律并未一刀切地完全禁止或者严格限制使用自动化决策以提供个性化服务。

但此时的法律理解难题在于，“合理”作为一个法律术语中可解释空间较为宽泛的描述性概念，事实上具有较大的不确定性。从理论上看，“合理的范围”至少需要符合法律以及社会一般价值观念对于“公平公正”的预期。我们理解，如借鉴合同法领域中“显失公平”的相关理解思路，或可从结果向度更好地理解“公平”。此前我国学者对显失公平的定义多根据最高法的司法解释（《最高人民法院关于贯彻执行 < 中华人民共和国民法通则 > 若干问题的意见》第 72 条）：一方当事人利用优势或者对方没有经验，致使双方的权利义务明显违反公平、等价有偿原则的，可以认定为显失公平[5]。《民法典》第一百五十一条规定，一方利用对方处于危困状态、缺乏判断能力等情形，致使民事法律行为成立时显失公平的，受损害方有权请求人民法院或者仲裁机构予以撤销。有学者认为，在消费者合同中，消费者只要能够举证证明合同关系失衡，自己处于不利境地，即可主张合同显失公平[6]。可见，**因所处窘迫或者缺乏信息判断能力而将自己处于合同关系中的不利境地，或可成为“公平”原则被破坏与否的一个标准**。同理，如因自动化决策而达成的交易条件使得消费者一方因缺乏信息对等地位而订立了消费合同，产生了消费者个人合法权益的损害结果，这一定意义上便意味着可以认定自动化决策带来的差异化结果超出了合理范围。

从现有的配套或者相关法规解释来看，《国务院反垄断委员会关于平台经济领域的反垄断指南》规定，分析是否构成差别待遇可以考虑的因素包括：（1）基于大数据和算法，根据交易相对人的支付能力、消费偏好、使用习惯等，实行差异性交易价格或者其他交易条件；（2）实行差异性标准、规则、算法；（3）实行差异性付款条件和交易方式。而《深圳经济特区数据条例》中将交易条件细化为交易安全、交易成本、信用状况、交易环节、交易持续时间等方面，并以例外条款的形式规定了不被认为属于“对交易条件相同的交易相对人实施差别待遇”的情形，具体包括：

（一）根据交易相对人的实际需求，且符合正当的交易习惯和行业惯例，实行不同交易条件的；

（二）针对新用户在合理期限内开展优惠活动的；（如常见的“拉新促活”）

（三）基于公平、合理、非歧视规则实施随机性交易的；

（四）法律、法规规定的其他情形。

由上可见，对于该款的“交易条件”“合理范围”等均需要进一步的立法与司法的互动过程，进

[5] 王政红，严洁：《合同法中显失公平制度探析》，载“中国法院网”，https://www.chinacourt.org/article/detail/2013/11/id/1149128.shtml，最后访问日期：2021 年 9 月 13 日。
[6] 崔建远：《合同法总论》（上卷），北京：中国人民大学出版社，2011 年版。

行更为立体、全面和生动的解释，以更好地廓清自动化决策机制下的公平公正的法律含义。

（二）第二十四条第二款解读

“通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。”

《个人信息保护法》第二十四条第二款赋予个人充分的选择权。如企业涉及通过自动化决策方式向个人进行信息推送、商业营销，则需要考虑至少向用户以下一项合规路径，即：

- 路径一：向用户提供不针对个人特征的选项；
- 路径二：向用户提供便捷的拒绝方式。

1. 如何理解“信息推送”所指代的服务范围

相较于“商业营销”一般指代广告投放，对于“信息推送”内涵的理解可能存在一定争议。从技术角度出发，狭义的“信息推送”往往指代通过自身产品或第三方工具对于用户移动设备、信箱进行的主动信息推送，从而使得用户能够在移动设备通知栏、信箱中接收到 产品主动推送的信息。但参考此前 App 执法文件 中的监管要求以及包括《信息安全技术[7] 个人信息安全规范》（以下简称“**《个人信息安全规范》**”）、《信息安全技术 网络音视频服务数据安全指南（征求意见稿）》在内的一系列标准对于个性化展示的规制范围与要求，我们理解将本条所提“信息推送”局限于上述狭义的信息推送可能大大限缩了立法预期的规制范围，如今社区、电商、短视频等各类产品应用中常见的根据用户基本资料、使用偏好以及标签信息所进行的“信息流推送”可能同样应作为本条要求规制的重点对象，例如根据用户画像向用户推送用户感兴趣视频的短视频服务提供商、在首页根据用户偏好展示其感兴趣商品的电商平台。

2. 如何从实操层面赋予用户选择或拒绝的权利

就路径一而言：如何理解向用户提供不针对其个人特征的选项成为相关企业重点关注的问题，而就这一问题，《个人信息安全规范》7.5 b）的注释中曾给出较为明确的解答，“基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。”因此，如产品提供方在提供基于自动化决策推荐服务外，还提供了仅根据用户选定地理位置进行信息推送或商业推广的选项，则可视为满足路径一的要求，例如电商平台在商品搜索环节，除向用户提供基于用户画像的结果展示，还向用户提供基于地理位置、销量、评价等维度排序的商品检索功能，则可以认为电商平台向用户提供了不针对个人特征的选项。

但此时，可能又有些企业会提出疑问，如果基于选定的地理位置信息进行信息推送可以被认定为提供了不针对个人特征的选项，那么仅基于用户填写的性别、爱好等信息进行信息推送或商业营销是否又可能被认为向用户提供了不针对个人特征的选项？就这一问题，如果仅从字面解读的角度出发，性别、爱好都能够具体反映用户的个人特征，那么基于这类个人特征所推送的信息可能仍无法被认定向用户提供了不针对个人特征的选项。而回溯立法目的，我们理解要求企业提供不针对个人特征的选项的目的，是为了赋予用户自由选择的权利，避免用户仅能访问企业基于用户画像所推荐的其希望用户看到的内容，使得用户陷入“信息茧房”，进而造成认知面狭隘等问题。那么如果企业从产品设计层面出发，能够确保用户自主选择并切换所希望看到的内容（如可在界面内自主切换性别或所希望看到的频道内容），那么基于用户自主选定的性别或爱好进行信息推送与商业营销是否能够被认定满足提供可不针对个人特征选项的要求。基于以上，我们理解关于“提供不针对个人特征的选项”的定义与实现方式可能仍存在一些模糊地带，有待进一步解释与澄清。

就路径二而言：我们理解实践中已有不少企业在产品中加入开关，在用户关闭按键后，即停止向用户提供个性化推荐内容。例如，部分 App 已在“设置 - 隐私”中加入“是否允许向用户展示程序化广告”的开关，并在用户点击关闭后提醒用户未来提供广告内容的相关度会降低，但所看到广告数量将不会受到影响，从而满足“向用户提供便捷的拒绝方式”的合规要求。

[7]《App 违法违规收集使用个人信息行为认定方法》：三、以下行为可被认定为“未经用户同意收集使用个人信息”：…6. 利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项…。

当然值得注意的是，目前部分企业出于业务转化率角度出发会对于开关关闭期限进行限制，并在用户关闭一定期限后重新开启个性化推荐选项。我们理解仅提供一定期限的拒绝选项在一定程度上对用户对其个人信息处理的决定权与拒绝权造成了一定程度的削弱，而在新法生效后，此等设计的合法合规性无疑将受到进一步考验。

（三）第二十四条第三款解读

“通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。”

近年来，各国立法者开始关注自动化决策机制不透明性带来的风险。《通用数据保护条例》（以下简称“**GDPR**”）不仅在第十五条中规定了数据主体有权要求解释一般性自动化决策规则以保障其自身的知情权，同时还在第二十二条明确规定了“对数据主体产生重大影响的纯自动化决策”的适用限制以及数据控制者所需采取的安全保障措施。《个人信息保护法》第二十四条第三款充分借鉴域外立法经验，在保证自动化决策透明度和公正性的一般性要求的基础上，针对结果会对个人权益有重大影响的自动化决策提出了更为严格的限制条件，个人有权要求个人信息处理者对于该等自动化决策进行说明，同时也有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。然而，实践中，该条款的适用面临了诸多质疑，仍需要进一步明确“对个人权益有重大影响的决定”的定义并厘清解释说明权与拒绝权的行使机制，否则该条款难免将沦为具文而被束之高阁。

1. 如何理解“对个人权益有重大影响的决定”

“对个人权益有重大影响的决定”的定义在《个人信息保护法》中暂付阙如，该等立法空白可能增加侵害个人信息主体合法权益的风险，同时也在一定程度上可能加重企业的合规负担。对此，我们注意到，域外立法经验、现行部委规章以及国家标准为立法者审慎而清晰地界定何为“对个人权益有重大影响的决定”提供了重要的借鉴，同时也为企业采取相应的合规措施提供了一定的指引。

从比较法的角度来看，GDPR 第二十二条明确规定，数据主体有权不受到对其产生法律效力或对其造成类似的重大影响的自动化决策的限制。在此基础上，欧盟第二十九条数据保护工作组制定的《关于自动化个人决策目的和识别分析目的准则》（Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679）（以下简称“**《自动化决策准则》**”），进一步厘清了“对个人权益有重大影响的决定”的定义。在 GDPR 语境下，对个人权益有重大影响的决定是指“具备对个人的境况、行为或选择的产生重大影响的潜在可能，在最极端的情况下，可能导致对个人的排除或歧视”的决定，以下决定均属于“对个人权益有重大影响的决定”：影响某人的财务状况的决定，如在线申请信用卡以及向经济困难的人展示在线赌博广告，以及影响某人的就业机会的决定，如在线招聘。

就国内的现行规范而言，GDPR 第二十二条的类似表述亦见于《互联网个人信息安全保护指南》6.3c）以及《个人信息安全规范》第 7.7 条，前述规范将自动决定个人征信及贷款额度、用于面试人员的自动化筛选以及行政司法决策纳入了“对个人权益有重大影响的决定”的范畴之中。此外，《个人信息安全影响评估指南》（GB/T 39335-2020）则要求从“限制个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“人身财产受损”四个维度对个人权益影响的重大性进行评估。

可见，国内现有规范均在不同程度上借鉴了 GDPR 及其配套指南的规定，但对于何为“对个人权益有重大影响的决定”仍缺乏统一的界定标准，具体监管规则的边界有待相关主管部门出台进一步的规章和指南予以明确。在自动化决策监管日渐趋严但缺乏明确监管规则的当下，企业或可先行参考前述境内外立法规定，结合自动化决策机制的可替代性以及适用自动化决策的具体场景，在日常经营中尽可能识别和判断自动化决策是否对于个人信息主体产生重大影响，并采取必要的合规措施。

2. 对自动化决策的解释说明权与拒绝权的实践困局

伴随着自动化决策的广泛应用，自动化决策结果对于个人的影响不再限于单个具体场景，还可能

通过数据流通共享对个人产生跨越公私领域的深远影响。例如，第三方征信机构根据个人的支付软件使用行为形成的信用评分，不仅影响到了个人对于该支付软件的使用，而且业已成为在银行风控、租车租房、预订酒店乃至办理签证等场景中对个人进行信用评估的重要依据。同时，自动化决策规则的不透明性进一步加剧了个人对于自动化决策广泛影响的顾虑，各国立法者逐渐就个人信息主体对于自动化决策的解释说明权以及拒绝权达成共识。为了平衡个人主体权益以及自动化决策应用所产生的经济效益，《个人信息保护法》对于如何约束对个人权益产生重大影响的自动化决策机制进行了一定立法尝试，然而，目前《个人信息保护法》第二十四条第三款的实操性仍有待考验。

（1）对自动化决策的解释说明权

《个人信息保护法》虽规定个人可以要求个人信息处理者对于自动化决策予以说明，但是个人信息处理者对于自动化决策机制的解释说明范围与个人信息主体的具体行权机制均悬而未决。

首先，不乏有人主张个人信息处理者需对于自动化决策机制的源代码进行完全的公开，对此，有人就源代码的可理解性以及可能损害商业秘密提出反对意见。实践中，网信办的监管调查以及司法裁判中均未要求相关企业公开算法的源代码，而是要求相关企业就算法的设计理念以及算法决策结果的可验证性与可追溯性进行解释和说明。对此，回溯立法目的，我们理解设置个人信息主体对自动化决策要求解释说明权的制度目的之一在于保障个人信息主体的合法权益，矫正自动化决策中双方严重信息不对称的地位，为保障个人知情权以及对自动化决策进行必要干预提供有力的抓手[8]。而公开源代码显然无助于个人信息主体理解和评估自动化决策的可验证性与公平，相反可能使得个人信息处理者对自动化决策机制的解释囿于形式，有违设置自动化决策解释说明权以保护个人信息主体权益的立法初衷。

其次，个人信息处理者对于自动化决策机制的说明是否限于个人信息处理者对于个人信息处理规则所需的解释说明亦亟待进一步厘清。该问题不仅仅关乎《个人信息保护法》第二十四条与第四十八条之间的适用关系，而且也关系到了自动化决策应用的合理性与正当性的判断标准。尽管判断自动化决策合理正当性的标准有待结合多种因素进行深入研讨，但是至少可以明确的是，自动化决策技术本身其实无涉合理性与正当性的判断，立法者增设对于自动化决策的特别规制，是为了防范与救济个人信息主体无法有效干预自动化决策而对其合法权益产生的侵害，而此处的合法权益并不限于对个人信息主体的知情权的保障。若自动化决策的解释权完全等同于对个人信息主体知情权的保障，那么个人信息主体所面临的选择只能是接受或者退出自动化决策，并无法发挥自动化决策解释权应有的救济功能。同时，若个人信息处理者对于自动化决策机制的说明仅限于个人信息处理规则的说明，那么立法者对于自动化决策机制解释权适用范围的有限性与个人信息处理者解释说明义务的普遍性之间将产生冲突。因此，个人信息处理者对于自动化决策进行说明的范围不限于对个人信息处理规则的解释，还可能包括公平性解释（如决策机制公平性以及结果公平性）、影响性解释（包括决策如何影响个人以及广泛社会群体、为减轻其所可能带来的负面影响而采取的纠正机制等），甚至包括可修正自动化决策的路径等。因此，法律赋予个人对自动化决策的解释说明权，是为个人提供知情权与必要干预路径的双重权利构造。

最后，目前个人信息主体对自动化决策要求解释说明权的触发条件尚不明确，更遑论个人主张自动化决策解释权行权机制的合理性。我们理解，自动化决策可解释权的适用机制需综合考虑企业商业效率与个人权益救济的衡平，未来进一步细化相关行权机制时可能需要进一步讨论个人信息主体是否应当承担一定的举证责任，个人信息处理者是否有义务停止相应自动化决策机制的使用，以及个人信息处理者向个人信息主体提供解释说明的期限以及可验证性要求等。

（2）拒绝自动化决策权

《个人信息保护法》第二十四条第三款通过法律确定了个人信息主体的**拒绝自动化决策权**，具体而言，个人有权拒绝个人信息处理者仅通过自动化决策的方式作出决定，但该条款的落地性与实操性亦有待进一步商榷。

[8] 张凌寒：《商业自动化决策算法解释权的功能定位与实现路径》，载《苏州大学学报（哲学社会科学版）》，2020 年第 2 期。

一方面，无论是基于数据库编码的计算机自动化，还是基于机器学习的算法自动化，现有自动化决策机制可能无法彻底避免人工的介入，而目前立法规定个人仅有权拒绝“仅通过自动化决策的方式作出决定”，那么个人信息主体对于自动化决策的拒绝权可能面临着被架空的风险，而难以为个人信息主体权益提供切实有效的保障和救济。另一方面，拒绝自动化决策权的行权条件亦具有讨论的现实意义。如前所述，如何界定“对个人权益有重大影响的决定”仍有待商榷，但至少可以明确的是，“重大影响”的认定不应完全采取主观标准进行事前判断，相反个人信息主体在不公正的决策结果产生外部性后，方可行使拒绝自动化决策权，可能更为符合立法者为个人信息主体提供不再因自动化决策而遭受合法权益侵害的退出路径的立法目的。此外，拒绝自动化决策权、拒绝他人处理个人信息的权利以及个人信息可携权之间的适用关系可能也是未来自动化决策监管机制可能的细化方向。

三、给企业的建议

可以预见在《个人信息保护法》生效后，监管部门对于自动化决策算法的监管进一步有法可依，产品用户维护个体权益亦将持有法律的武器，而对于企业而言无疑将面临更严峻的合规考验。因此为降低相关合规风险，我们建议涉及自动化决策算法应用的企业关注以下合规要点问题：

（一）确保数据来源合法合规

在自动化决策算法研发与应用过程中，往往涉及大量数据的收集与使用，企业为了提升算法的准确性与有效性，往往需要通过产品直接收集大量个人资料信息、设备信息以及使用行为信息，或通过第三方间接获取大量标签信息。而数据作为算法演练与后续应用的基础，如相关数据来源合规性存在瑕疵，将不可避免地使得整体业务模式的合规性存在较高风险。因此，为确保整体业务模式的合规性，企业应首先确保数据来源合法合规。具体而言：

- 针对直接从用户侧收集使用的数据：如无法基于《个人信息保护法》第十三条（一）之外的条款建立个人信息处理的合法性基础，则企业需要通过隐私政策披露等方式就个人信息的收集及后续使用获取用户同意，以构建收集相关信息用于自动化决策的合法性基础；
- 针对间接从第三方获取数据：建议企业在开展合作前，对于第三方数据供应商进行全面评估，就供应商资质、数据安全能力、是否存在任何不良记录进行尽调，要求对方提供数据来源合法合规的相关证明，并签署关于数据来源合法合规的相关承诺，从而尽可能规避因数据来源瑕疵而引发的合规风险。

（二）评估将数据用于自动化决策的必要性

根据《网络安全法》第四十一条所确立的个人信息收集使用“合法、正当、必要”的原则，企业在算法研发应用过程中，除满足上述合法性要求外，还应满足数据收集使用的必要性要求。尽管我们理解企业为提升算法推荐的精准度实现“千人千面”，往往需要收集海量个人信息用于算法研发、精准画像，而从业务角度出发，各类信息的收集使用均具有其必要性。但从目前监管实践来看，如收集个人信息的类型与实现产品服务的业务功能缺乏直接关联、频次过高或数量过多均可能被认定超出收集个人信息的必要范围，从而引发合规风险。因此从合规角度出发，企业仍应建立针对信息收集使用的必要性评估机制，从用户侧角度评估将信息用于算法研发、精准画像的必要性，并重点关注监管目前可能重点关注的字段类型，如应用列表信息、设备标识符信息（包括但不限于 IMEI、Android ID、IDFA）等。

（三）事前进行个人信息安全影响评估并留存相关记录

参照《个人信息保护法》第五十五条的要求，个人信息处理者如涉及利用个人信息进行自动化决策应当事前进行个人信息保护影响评估并对处理情况进行记录。因此，企业在产品规划设计阶段或首次使用前即应参照《个人信息保护法》第五十六条以及《个人信息安全影响评估指南》（GB/T 39335-2020）的要求开展相关评估并留存相关记录，评估点应至少包括但不限于以下内容：

- 是否向用户说明了自动化决策的基本原理或运行机制；
- 是否定期对自动化决策的效果进行评价；
- 是否对自动化决策使用的数据源、算法等持

续优化；

- 是否向用户提供针对自动化决策结果的投诉渠道；
- 是否支持对自动化决策结果的人工复核。

（四）将合规要求纳入产品设计环节（Privacy by Design）

鉴于《个人信息保护法》以及相关国家标准、指南为进一步保护用户权益，均要求产品服务提供者向用户提供不针对个人特征的选项，为避免产品研发后为满足合规要求重新对产品功能模式进行调整从而造成不必要的资源浪费与时间拖延，我们建议企业在产品功能设计环节即对于相关服务类型或算法类型涉及的个人信息保护、消费者权益保护要求进行全面梳理，并参考相关要求进行产品功能设计。例如参照《信息安全技术 个人信息安全规范》的要求，企业产品如在推送新闻信息服务的过程中使用个性化展示的，则应在功能设计时，即考虑为用户提供简单直观的退出或关闭个性化展示模式的功能，而当用户选择退出或关闭个性化展示模式时，应在界面内为用户提供删除或匿名化定向推送活动所基于的个人信息的选项。

（五）建立畅通权利响应渠道，并确保能够响应权利请求

为确保满足用户对于个人信息处理以及产品服务自动化决策机制的相关权利请求，企业宜建立畅通的权利响应渠道，及时响应用户各类权利请求。同时考虑到用户可能要求公司就产品相关自动化决策的公平性、合理性等问题进行解释说明，我们建议企业提前准备相关算的法可解释性文档或应答话术，确保相关客服人员能够准确应答用户请求，保障相关用户的知情权。

（六）积极关注算法监管领域相关立法动态

伴随《数据安全法》《个人信息保护法》相继发布，针对算法相关立法工作也在有条不紊地开展，2021 年 8 月 27 日，《互联网信息服务算法推荐管理规定（征求意见稿）》正式发布。尽管相关规定仍处于征求意见阶段，但可以预见未来对于算法的监管将从对于算法问题所凸显的法律价值层面的监管渗透到对于算法应用过程的技术性监管。因此，企业在自动化决策算法的研发使用过程中，除需满足个人信息保护领域相关合规要求外，还应进一步关注算法监管领域的合规要求。具体而言，企业一方面应确保相关算法满足“公正公平、公开透明、科学合理、诚实信用以及内容向善”的基本原则，同时对于特定类型算法还应确保满足相关具体规制要求；另一方面，企业还应关注并及时响应网信部门对于算法的分级分类、备案、安全评估、配合检查等各类监管要求。

结语

维真德在《数据为民》一书的开篇提出，“时间已经认识到，隐私和自主不过是一种错觉。”[9] 回看近年来自动化决策技术的滥用现象，不料竟一言成谶。《个人信息保护法》对于自动化决策的滥用现象予以积极的回应，并对于互联网市场竞争主体如何合法合规运用自动化决策机制提供了重要指引。值得注意的是，自动化决策的法律规制并不是为了阻碍大数据技术的发展，相反，合法正当和必要范围内的自动化决策机制的使用始终可以为商业与法律制度所接纳。尽管数字市场发展未必尽善尽美，但合理应用自动化决策技术始终是企业应对算法监管所必需遵守的底线，勿让被滥用的自动化决策技术成为智能时代的弗兰肯斯坦。

未来，我们将继续关注自动化决策机制可能的法律监管思路与实现路径，与大家共同探讨自动化决策规制如何与个人信息保护的整体监管机制进行有机联动，秉承着科技向善的愿景和使命共同构建向上向善的网络“熟人社会”，让知我者，知我所求，也谓我心忧。

感谢实习生蒋雨琦对本文的贡献。

[9]Andreas Weigend, Data for the People, How to Make Our Post-Privacy Economy Work for You, Basic Books, 2017.

斯人已逝，生者如斯
——浅析死者个人信息权利

宁宣凤　吴涵　陈胜男　张凯勋

伊莱恩·卡斯凯特在《网上遗产》里写道：“我们曾用技术手段抓住死者，但现在，技术已经不仅仅是一种帮助我们和逝者取得联系的媒介，死者就存在于技术之中。”[1] 随着数字经济的发展，越来越多的人在数字空间中活跃，而我们对某个人的印象、回忆也在很大程度上取决于其留存于数字空间中的信息。随着生者逝去，留存于数字空间中的信息在某种程度上即提醒着思念者斯人已去，但同时也留下了追思的碑石。

对于死者的个人信息保护，《个人信息保护法（草案二审稿）》（以下简称“**二审稿**”）参照《民法典》中的规定，增加了保护死者个人信息的条款；2021 年 8 月 20 日正式通过的《个人信息保护法》（以下简称“《**个信法**》”）进一步完善了这一规则，对个人信息处理者保留的“数字遗产”应当如何处置进行了一定回应，有助于解决随着数字经济快速发展而日益增多的因自然人死亡引发的个人信息纠纷。[2] 本文尝试回顾从死者相关权益保护的过去、现状，结合域外有关死者个人信息保护的规定，探讨《个信法》死者个人信息权益保护规则的适用性。

[1] 刺猬公社，《打开一个逝者账号，进行一次赛博时代的扫墓》。
[2] 法制日报，死者个人信息保护是否应设保护期，http://www.npc.gov.cn/npc/c30834/202108/4a68209f74e842f681807f55dc261838.shtml.

一、《个人信息保护法》死者个人信息权益保障条款

根据二审稿第四十九条，自然人死亡后，其对于个人信息处理活动中的权利由近亲属行使。这一新增规定一度引发了理论界较为激烈的讨论，特别是在如何有效保障个人信息的处理符合死者生前意志的问题上，争议尤为突出。对此，《个信法》第四十九条充分考虑了对死者生前意志的尊重和保障，要求死者的近亲属行使相关权利时应有自身合法、正当的权益保障基础，且在死者生前如另有安排，则近亲属维护自身利益而行使权利的行为将需要让渡于死者生前意志。

二审稿	《个信法》
第四十九条 自然人死亡的，本章规定的个人在个人信息处理活动中的权利，由其近亲属行使。	第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

另一方面也应看到，相比于二审稿第四十九条直接说明死者享有在个人信息处理活动中的权利，近亲属只是代为行使，修订后的条款变更为近亲属可以对死者的相关个人信息行使权利。从文义解释上看，《个信法》在保护死者个人信息的同时，似乎也有意对个人信息权益的主体更多向生者倾斜，将死者个人信息的查阅、复制、更正、删除等权利建立于生者自身合法正当利益保护的基础之上。这一立法思路的转变呼应了此前对于死者个人利益保障的理论基础之争议，也反映了立法层面在防止个人信息权利主体不当扩大和有效保障死者意愿之间的抉择与平衡。

二、死者人格权益保护的国内法渊源

在我国民法体系下，对于死者权利的保护讨论较多且司法实践已有触及的首先见于死者人格权的保护。虽然普遍承认应当保护死者的人格利益，但是我国学者对其制度架构的理论选择一直争论不休。有部分学者主张“死者权利保护说”，认为人格权不依附于人的生命而消失，自然人在死后仍然可以拥有某些权利。但是这与目前的民事权利体系相矛盾，作为重要的民事权利的一种，人格权也应当同民事权利一样“从出生起到死亡时止”。[3] 而大部分学者都主张“近亲属权利保护说”，认为死者其实已经丧失了民事权利能力，也不再是民事权利主体，只有生存着的死者的近亲属能够以权利主体的地位获得法律的保护。并且，死者与近亲属的人格利益上存在一定的关联性，一方面，名誉是社会对主体的综合性评价，一方的人格权破坏在很大程度上也很可能影响其近亲属的名誉，另一方面，基于死者和近亲属的特殊关系，对于死者的人格利益侵犯往往也是对于其近亲属的情感和精神的巨大伤害。[4]

如前所述，相对于二审稿对于死者享有个人信息主体权利的规定，《个信法》第四十九条规定除死者生前另有安排的，近亲属可以为了自身的合法、正当利益对死者的相关个人信息进行查阅、复制、更正、删除等操作，可见其最终采取了“近亲属权利保护说”的观点，这也与此前国内对于死者人格权益保障的司法实践相呼应。

早在 2001 年颁布的《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》曾规定，自然人死亡后，以侮辱、诽谤、贬损、丑化或者违反社会公共利益、社会公德的其他方式，侵害死者姓名、

[3] 参见刘召成，《死者人格保护的比较与选择：直接保护理论的确立》，载《河北法学》2013 年第 10 期。
[4] 参见陈林林、 陈杰，《< 民法典 > 保护死者人格利益的法理基础——兼论近亲属权益保护说的理论困境及其解释论分析》，载《广西社会科学》2021 年第 2 期。

肖像、名誉、荣誉或非法披露、利用、非法侵害死者隐私的，其近亲属因遭受精神痛苦，可以向人民法院起诉请求赔偿精神损害；自然人因侵权行为致死，或者自然人死亡后其人格或者遗体遭受侵害，死者的配偶、父母和子女或其他近亲属可以向人民法院起诉请求赔偿精神损害。在 2020 年修订司法解释中也同样规定，死者的姓名、肖像、名誉、荣誉、隐私、遗体、遗骨等受到侵害，其近亲属向人民法院提起诉讼请求精神损害赔偿的，人民法院应当依法予以支持。可见，司法解释赋予死者的近亲属提起精神损害赔偿诉讼的资格，通过保护死者近亲属的情感需要和利益，来间接保障死者人格利益免遭不法侵害。

除了司法解释对死者近亲属因死者权益受到侵害而主张精神损害赔偿的请求权基础予以确认和支持外，现有司法案例中也不乏为保障近亲属合法利益而一定程度让渡死者个人隐私或权益的现实案例。在 2015 年“陈森豪诉某市房产局案”[5]中，死者陈林的法定继承人陈森豪（一审原告）在父亲去世后申请房产局（一审被告）告知其名下房产信息，而房产局以“房屋作为所有权人的私有财产，其登记信息往往涉及到所有权人的个人隐私或商业秘密”以及房屋权属相关的信息查询规定查询机构及其工作人员应当对房屋权属登记信息的内容保密为由，拒绝了原告的请求。对此法院认为，原告基于《继承法》《物权法》对死者的合法财产享有继承权，应当受到尊重和保护。原告作为死者第一顺序法定继承人，知悉死者名下的房产信息是实现其继承权的前提，查询死者名下房产信息是其继承权的权利延伸，我国《物权法》第十八条[6]的规定即体现了该项权利。基于此，法院最终支持了原告的诉讼请求。

这一案例可谓构成《个信法》第四十九条的典型适用场景，在当时尚缺乏明确法律规定的情况下，法院援引了《继承法》《物权法》等对近亲属继承权利的确认和保障规则，为维护和实现近亲属法定的继承权利，明确了近亲属查询死者房产信息具备合理的基础，虽然在裁判说理上使用了“权利延伸”的论证思路，但“殊途同归”，起到了保障近亲属合法权利的效果。实际上，因向公权力机关查询死者个人信息 / 隐私信息而引发纠纷的案件不在少数，虽然因事实情况的千差万别和法律规则的缺位导致法院裁判思路不尽相同，但多数法院仍旧肯定了近亲属具备查询、要求政府公开死者生前信息的权利。例如在 2012 年另一起“曹某等诉某市社会保险基金管理中心案”中，原告作为死者近亲属申请要求被告公开死者工伤赔偿保险核定表，而被告以核定表属于个人信息不应该公开为由拒绝了原告要求，法院最终支持原告的请求。该案后来入选《人民司法》刊。同样是在没有法律明确规定的情况下，主审法院在“死亡公民的近亲属能否申请公开涉及该死亡公民的个人信息”这一焦点问题上类推适用了《行政诉讼法》中有权提起诉讼的公民死亡，其近亲属可以提起诉讼的规定，认定原告具备申请公开个人信息的资格。值得注意的是，该案法院在评析中肯定了近亲属构成死者个人信息权利人。在《个信法》生效后，如相类似的情况再出现，是否需要重新变换论证思路，重点考虑近亲属在案件中的合法利益基础，将有待实践的进一步检验。

三、死者个人信息权益保障的域外经验

随着数字经济的发展以及对“隐私”这一概念的不断诠释，全球各司法辖区也对应当如何保护死者的个人信息提出了不同的见解。

其中，欧盟《通用数据保护条例》（以下简称“GDPR”）在序言第 27 段中规定，GDPR 并不适用于死者的个人信息，但成员国可以对处理死者个人信息的方式制定规则。我们理解，如何处理死者的个人信息本身存在较大争议，且与各国文化高度相关，可能无法以“通用”或“公认”的数据保护规则予以规制。目前，就欧洲地区而言，奥地利、比利时、克罗地亚、塞浦路斯、芬兰、德国、希腊、立陶宛、卢森堡、马耳他、荷兰、挪威、波兰、罗马尼亚以及英国尚未对死者个人信息进行额外的规定，即数据保护法律不适用于死者个人信息。对于其他国家而言，以法国为例，个人信息处理者可以处理死者个人信息，但死者生前可以对其个人信息在去世后如何留存、删除或者披露制定通用或者特别的指示。[7]对所有个人信息处理活动相关的通用指示可以向经过法国国家信息自由委员会（CNIL）认证的可信第三方登记，而对个人信

[5] 南京市中级人民法院 (2015) 宁行终字第 403 号行政判决书。
[6]《物权法》第十八条规定，权利人、利害关系人可以申请查询、复制登记资料，登记机构应当提供。
[7] LOI no. 2016-1321 du 7 October 2016 pour une République numérique (Digital Republic Act).

息处理行为的特别安排则必须向数据控制者提交。当数据控制者收到个人的特别指示后，必须基于该人同意，才能在其死亡后继续处理相关的个人数据，且数据控制者不能在使用条款中免除该同意要求[8]。虽然西班牙数据保护法明确规定不适用于死者个人信息，但却认可，死者的继承人、利益相关人或委托人可以访问死者在社交网络和数字平台上的个人信息，并可以要求相应数据控制者对个人信息进行修改和删除等操作（除另有遗嘱外）。[9] 死者若为未成年人，则由其法定代理人或者公诉人依职权或者依申请行使上述权利；死者若为残疾，在扶养范围内，由承担扶养职责的人行使上述权利。[10] 除此之外，丹麦、冰岛等成员国则直接规定死者个人信息可以适用 GDPR 的相关规定，但对保护期限进行了限制，例如丹麦规定对死者个人信息的保护自去世之日起十年内有效[11]。

美国加利福尼亚州的《加州消费者隐私保护法》（CCPA）以及《加州隐私权法》（CPRA）均未对死者个人信息的保护进行任何规定，但美国统一州法委员会发布的示范法《受托人访问数字资产统一法》（RUFADDA）则从继承法的角度提出了一些规则，对如何保护死者个人信息具有一定的借鉴意义。RUFADDA 将数字资产定义为“个人拥有权利或利益的数字记录”，具体可以包括 (1) 电子文件，如电子邮件、微软办公系统各类形式文件等；(2) 社交媒体账号，如脸书、领英等媒体账号；(3) 金融资产，如 PayPal、Amazon 钱包账户；(4) 商业资产，如数字化客户信息、数据库、专利、域名、网页等；(5) 其他形式资产，如博客账户内容、线上音乐及视频、线上游戏等。根据《存储通讯法案》（Stored Communication Act）的要求，RUFADDA 区分了数字通讯类和非数字通讯类数字资产的访问权限及要求。[12] 任何人（包括遗嘱执行人在内的受托人）均无权访问对于数字通讯类资产，除非获得了死者明确的授权同意，而授权同意可以通过遗嘱、信托、授权书或者在线工具提供。[13] 通过设置数字通讯类数字资产默认不可访问的方式，RUFADDA 可以相对比较好的保护死者及其交往者的隐私。

在授权层级上，RUFADDA 设立了在线工具＞遗嘱＞服务协议的“三层优先访问体系”。如死者生前已利用在线工具制定数字资产披露指示，则该指示的效力大于遗嘱。如果死者没有通过在线工具做出任何有关数字资产的指示，则遗嘱中的相关规定适用。但若死者没有通过在线工具或者遗嘱做出任何指示，则数据资产将按照死者生前和服务提供商签署的服务协议处理。[14]

除数据保护法律之外，医疗行业的监管也对如何处理死者个人信息作出了一定限制。例如，虽然英国的《数据保护法案》（UK Data Protection Act）没有对死者个人信息做出明确的规定，但根据《病历访问法案》（Access to Health Records Act 1990），仅限死者的代理人（包括遗嘱执行人和遗产管理人）以及因死者去世而有请求权的个人（无论是死者的近亲属还是其他人）访问病历。[15] 美国《健康保险携带和责任法案》（HIPPA）也要求相关机构在个人去世 50 年内给予死者的个人信息与其在世时相同程度的保护。[16]

这些域外规则的设定大多数考虑了死者生前遗嘱对于其个人信息的处理要求，虽然不同国家对于遗嘱效力的具体要求上不尽相同，但总体体现了对于死者生前意志的尊重和保障，这与我国《个信法》的规定不谋而合。而另一方面也可以看到，也有国家同步关注到了死者个人信息过度保护问题，从而在信息类型、保护期限上设置一定的限定条件，防止死者个人信息保护的无限制扩张。

四、延伸思考

（一）《个信法》的生效规定是否意味着死者合法权益保障的回退？

《民法典》将自然人个人信息相关权益保护纳入人格权编，可以视为立法层面对于个人就其个人

[8] *Id*.
[9] Art. 3, Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.
[10] *Id*.
[11] *See*, Art. 4, Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (Act No. 90/2018 on Data Protection and the Processing of Personal Data). *See also*, Art. 5, Databeskyttelsesloven (Data Protection Act).
[12] Michael D. Walker, THE NEW UNIFORM DIGITAL ASSETS LAW: ESTATE PLANNING AND ADMINISTRATION IN THE INFORMATION AGE, https://www.siouxfallsepc.org/assets/Councils/SiouxFalls-SD/library/Viren%20-%20Digital%20Assets%20-%20Michael%20Walker%20Article%2012-18.pdf.
[13] *Id*.
[14] *Id*.
[15] *See generally*, British Medical Association, Access to Health Records-Updated to reflect the General Data Protection Regulation and Data Protection Act of 2018, https://www.bma.org.uk/media/1868/bma-access-to-health-records-nov-19.pdf.
[16] Department of Health & Human Services, Health Information of Deceased Individuals, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html.

信息享有的权利具备人格权属性予以肯定和保护。基于此，从人格权益保障的视角，《个信法》第四十九条中的“死者生前另有安排的除外”规定，可以视为一定程度上对死者生前在个人信息层面享有的人格利益及其处理意愿予以尊重和保障。而另一方面，这也同步说明了立法对于死者享有个人信息权利的某种“否定”。无论是“死者**生前**另有安排”，还是近亲属基于自身合法权益保障方可对死者的个人信息行使查阅、复制、更正、删除等权利，均表明对于死者而言，其已不再具备《个信法》所规定的个人信息主体的资格，除非在其生前作为个人信息主体时有明确的个人信息处理意愿外，死后将丧失行使或间接由其近亲属行使个人信息权利的能力。这一规则不禁引发我们进一步思考：**当我们因二审稿对于死者个人信息权利的承认而引发个人信息权利过度保护的担忧时，《个信法》修订后的条款是否会将问题带向另一极端，即在缺乏论证近亲属需要保护的合法正当利益而死者也没有生前做出安排时，死者的合法权益是否可能丧失被保护的渠道**？

从人格利益角度出发，《民法典》第九百九十四条规定，死者的姓名、肖像、名誉、荣誉、隐私、遗体等受到侵害的，其配偶、子女、父母有权依法请求行为人承担民事责任。相较于此前司法解释着重对于近亲属精神损害赔偿的支持态度，这一规定从某种程度上肯定了死者对于姓名、肖像、隐私等所享有的人格权利，近亲属可直接基于死者的上述权益受到侵害而请求行为人承担民事责任，而无须以提起精神损害赔偿为由实现死者权益的间接保护。我们理解，当死者的个人信息相关权益受到侵害的，考虑到个人信息权益的人格属性，理论上死者近亲属也应有权基于《民法典》的上述条款请求行为人承担民事责任。同样的，在《个信法》的语境下，如为了保障死者合法权益，而需要对其个人信息进行查阅、复制、更正、删除的，是否也应当给予相应的实现途径？实际上，我们在前面提到的“曹某等诉某市社会保险基金管理中心案”就已经凸显这一问题。当有权行使申请政府信息公开、享有知情权利的行政相对人死亡时，其近亲属代为申请信息公开的行为显然是为实现死者的上述合法权益保护，而很难被直接解释为是为了保障近亲属自身的合法正当权益。在上述场景下，死者的近亲属是否只能参照《民法典》《行政诉讼法》的有关规定，以提起诉讼、追究责任的方式才能有效解决现实的争议问题？

（二）《个信法》可否作为个人信息继承规则的法律基础？

另一方面，随着个人信息商业价值的不断挖掘，个人信息的财产属性已经引发了从理论到实践层面的多方讨论。对于死者个人信息保护，同样需要长远考虑个人信息财产价值的认可所带来的未来立法规则上的发展变化。从上述民法体系的基本规则来看，不同于人格权具有较强的人身属性，财产权利具有更强的流通性，通常可以继承，故死者的财产权利由继承人获得并行使可以有效保障相关权益免受他人侵害。长远来看，如个人信息的财产权益在未来的立法中得到认可，则对于死者的该等财产权益是否也可适用继承规则，即相关财产权益归属于继承人，也应同样审慎考虑。结合我们前面提到的司法案例，**《个信法》的现有条款似乎给予了财产属性语境下个人信息权利行使的合理逻辑：当死者的个人信息可以有效地转由近亲属继承时，是否意味着近亲属可以对死者的个人信息主张享有合法权益，而基于这一合法权益来行使对死者个人信息的查阅、复制、更正、删除等权利？而当死者生前另有安排时，例如通过遗嘱对其个人信息进行了一定的处分，则是否也可以类比继承法下的既有规则，遵从死者遗嘱对其个人信息进行保护和处置**？当然，这一问题的根源仍旧需要回溯到法律对于个人信息之上所载财产权利的态度，而实际上这一问题离我们已经不远，关于个人在网络上的账号信息（例如淘宝店铺账号、游戏账号）、游戏装备、虚拟货币、视听资源等在继承案件、婚姻家庭案件中如何确权、如何判定归属早已引发诸多讨论，实践中也有不少平台企业遭遇类似诉求。[17] 因此，《个信法》第四十九条在个人信息继承规则上的合理适用，仍有赖于未来个人信息财产权益方面的立法发展。

（三）如何实现《个信法》死者个人信息保护条款的落地？

在分析与展望《个信法》死者个人信息保护条款的可能影响和未来趋势的同时，我们同样需要回

[17]《过户已逝亲属手机号需亡者到场？回应：营业员解释不清》，见中国新闻网，http://www.chinanews.com/sh/2019/07-24/8904843.shtml，最后访问日期：2021 年 9 月 5 日。

归到条款本身考察其实践应用。《个信法》对死者个人信息的保护思路与方式值得肯定，但实践中应当如何落地还有待进一步明确。

例如，对于死者生前的“另有安排”，这一安排所应具备的条件和效力为何，才能够有效验证死者生前意志，就有待进一步讨论。从个人信息的财产属性出发，对个人信息权利的安排是否需要按照遗嘱的形式进行，即仅能通过《民法典》继承编的要求以公证遗嘱、自书遗嘱、代书遗嘱、打印遗嘱、口头遗嘱或录音录像遗嘱的形式安排如何处理个人信息？如参考域外的一些立法经验，死者生前是否可以通过第三方提供的网络服务进行安排？而在这一情形下，应当如何确定此类第三方服务的可靠性？此外，若死者生前就个人信息的处理进行了多种形式的安排，而不同安排下的个人信息处理意愿又存在不一致时，是否还需要进一步评估不同形式安排之间的效力顺位？除此之外，未来随着数据信托等商业模式的兴起发展，对于个人信息的处置安排可能还存在由第三方参与的情形，此时法律是否可允许相关的第三方全权参与和安排处理死者生前的个人信息？

另一个有待实践落地的问题在于，由于《个信法》没有规定近亲属的权利行使顺序，如死者近亲属基于各自的合法权益主张，对如何处理死者个人信息意见不一致时，个人信息处理者应当如何响应近亲属提出的请求？此时是否需要参照《民法典》第九百九十四条以及有关继承顺位的规定，来依次确定权力行使的顺位和效力？

写在最后的话

总而言之，从二审稿提出对死者个人信息权益的保护，到《个信法》第四十九条对死者个人信息权益保障进行条件限缩，反映了当下立法者在个人信息主体权利乃至数据权益问题上的审慎态度。一方面，这一规定有效弥补了当下对于死者个人信息保护的空白，体现了个人信息乃至数据权益保护范围的扩张趋势；另一方面，为防止这一范围的无限扩张，立法通过设定前提条件的方式对行使个人信息 / 数据权利的场景和主体进行限定，以尽可能确保死者个人信息落入法律所认可的必要保护范围。这一做法与域外的死者个人信息保护的规则也具有一致性。

诚然，在全球视野下，死者权利保障目前还是主要集中在与经济权益相关的知识产权、继承等传统领域，对死者隐私权和个人信息保护仍处于探索阶段。我国《个信法》第四十九条对死者个人信息的保护无疑在全球隐私和个人信息保护领域添上了浓墨重彩的一笔，但长路漫漫，无论是个人信息的理论属性还是第四十九条应当如何在实践中落实，均需要立法者和个人信息处理者的共同推进，进一步探索可行、可靠的死者个人信息保护方案。未来随着互联网的不断渗透及时间的推移，对于死者个人信息的处置问题将更加凸显，我们也期待着《个信法》的这一规定能够有效指引此后的个人信息处理实践，结合个人信息保护理论和立法的深入发展，为个人信息及数据权益的保障问题起到“定分止争”的作用。

感谢实习生徐晓妍对本文做出的贡献。

“不畏浮云遮望眼，风物长宜放眼量”——全球视域下的中国数据跨境流动规则探析

宁宣凤　吴涵

前言

伴随互联网和全球贸易的飞速发展，数字经济时代已然到来，数据作为第五大生产要素在当今的企业跨境合作中具有重要地位，跨境流动的数据在促进全球经济协同发展的同时，也伴随着个人隐私、社会公共利益、经济发展以及国家安全的风险，防范数据跨境过程中产生的风险成为全球数据治理重点。与此同时，随着数据主权理论的兴起，各国对于数据跨境的规则讨论从安全风险上升到国家竞争的新高度。近年来，在欧盟通用数据保护条例（General Data Protection Regulation，“GDPR”）就个人数据跨境设置不同的安全要求和前提条件后，各国出于不同目的纷纷加强了数据跨境治理。有鉴于此，本文以我国现实需求为导向，通过总结欧盟、美国、俄罗斯、印度的数据跨境治理模式及核心要点，进而梳理和分析全球视域下我国数据跨境流动治理模式的必要性和长远影响。

一、全球数据跨境流动治理模式及规制体系

近年来，随着新型信息基础设施建设逐步铺开，信息化水平不断提高，数据跨境流动治理已成为世界各国高度关注的全球性问题。各国政府和企业对数据资源的价值与意义已经形成共识，如何对快速发展的数字技术和数字贸易进行有效监管，并在有效实施数据跨境流动治理的同时，寻找到一种可与其他主要贸易伙伴进行有效协调的模式已成为各主要经济体面临的共同挑战。除美国、欧盟等主要发达经济体在积极探索之外，俄罗斯、印度作为主要的发展中国家，也在不断加强其数字经济和数字贸易的治理机制的建设，其中，数据跨境流动治理问题逐渐得到各国重视，总体来看：

- 欧盟作为世界范围内最早对数据跨境流动进行规制的区域性组织之一，建立了较为完善的数据跨境流动规制，欧盟提出要打破数字经济壁垒，建设内部单一的数字市场。其中《关于个人数据自动化处理的个人保护公约》是欧洲首个针对数据跨境流动进行规制的法律文件，此后相继通过了《108 号公约关于监管机构及跨境数据流动的附加议定书》《数据保护指令》，《通用数据保护条例》在 1995 年颁布的《数据保护指令》的基础上进一步完善了跨境数据治理举措，最终确立了欧盟数据跨境流动的治理方案。
- 美国法律传统奉行“法不禁止即自由”原则，受贸易利益驱动，其鼓励并推行宽松的数

据跨境流动政策，主张在确保国家安全利益的前提下最大限度地促进数据自由流动。在数据跨境流动治理上，美国主要采事后监管模式，发生侵权事件后再通过争端解决机制进行追责，但其在宣扬数据自由流动的同时，对联邦政府的重要数据采取了较为严格的管理措施，在投资、采购等方面及环节予以限制，提出数据本地化要求。在国际上，美国对外积极拓展长臂管辖，在全球宣扬数据跨境自由流动理念，以防止其他国家对数据的严格控制。

- 俄罗斯、印度作为严格限制流动模式的代表，尤其注重对数据安全的保护，并强调对核心数据和敏感数据的控制力。俄罗斯于 2019 年 11 月完成“主权互联网”立法，在该国关键行业和领域陆续替换国外产品和数据服务，以及对俄罗斯国家顶级域名进行内循环控制，要求实现信息数据的强制本地化；印度数据治理则以民族主义为基调，随着印度将数据治理逐步上升至国家层面，印度各类政府机构和监管部门均深度参与至数据治理中，其数据治理框架以《个人数据保护法草案》和《非个人数据框架》最具代表性。在数据跨境流动治理上，为应对西方国家及企业的“数据殖民主义”，印度将数据视为关键国家资源，严格限制关键个人数据的跨境转移，但在敏感数据上，印度试图实现流转与安全的折中处理，在开放数据跨境流通的同时要求必须事先在本地完成数据备份操作。

下表针对欧盟、美国、俄罗斯、印度的数据跨境治理相关的法律和政策进行分析和梳理，总结其治理模式与核心要点，把握数据跨境流动治理的国际动向，进而立足维护我国数据主权的基本立场，思考总体国家安全观指导下，我国数据跨境流动治理的内在逻辑与外在规范。

治理模式	主要国家和地区	相关法律法规	核心要点
有条件开放	欧盟	《通用数据保护条例》 《个人数据和电子通信指南》 《非个人数据在欧盟境内自由流动框架条例》	欧盟是世界范围内较早对数据跨境流动进行治理的区域性组织之一，欧盟尚无明确的数据本地化存储规定，但对于欧盟区域外的数据跨境传输具有条件限制（例如充分性认定、约束性公司规则、合适的安全保障等），具体而言： • 对于欧盟区域外，《通用数据保护条例》第 3 条设置了长臂管辖原则，并在第 5 条提出了个人数据处理的合法、公正、透明等原则，个人数据跨境同样需要遵守个人数据处理的一般原则。在数据跨境的具体规制上，欧盟在“充分性保护”流通准则的基础上，构建了其独特的“事前保护”模式。当前，欧盟对数据跨境传输规定以充分性认定为基础评估标准，需经充分认定才可跨境流通，以有约束力的公司规则 BCR、标准合同条款、临时合同条款和国际协议为充分性认定之外的法定保障工具，以数据主体明示同意、履行主体间的合同、为达成公共利益等合法利益场景作为在必须进行个人数据跨境传输时的减损规定，从而形成在个人数据传输实施之前的事前保护实施模式。且事前保护模式中的各项评估标准、法定保障工具在信息环境下动态更新与拓展，欧盟在个人数据跨境治理的数据类型、数据主体保护、业务数据流及事后风险管理等方面做出了持续的合规路径探索。欧盟主要通过《通用数据保护条例》及《非个人数据在欧盟境内自由流动框架条例》对数据跨境传输进行规制，旨在兼顾个人信息权益保护与欧盟数字经济发展。

治理模式	主要国家和地区	相关法律法规	核心要点
			• 对于欧盟区域内，欧盟建立单一数字市场战略（digital single market strategy）最核心的内容之一即为推动数据（包括个人数据和非个人数据）在欧盟境内的自由流动。《通用数据保护条例》已经规定了个人数据自由流动的原则，并废除了第 95/46/EC 指令；《非个人数据在欧盟境内自由流动框架条例》则为消除各成员国的数据本地化要求、确保成员国有权机关能够及时获取数据、保障专业用户能够自由地迁移数据提供了法律确定性。 • 严格的数据跨境流动限制在保护欧盟居民的数据安全的同时，也提高了欧盟法律在域外的效力，使得欧盟在全球数据流动规则制定中掌握了一定的话语权。
原则上开放（实际以安全为由限制，例如“清洁网络计划”）	美国	《公平信用报告法》 《澄清境外数据的合法使用法》 《美国出口管制改革法案》 《外国投资风险审查现代化法》 《信息时代关键基础设施保护》 《全球电子商务政策框架》 《健康保险携带和责任法案》 《儿童在线隐私保护法》 《网络安全信息共享法案》 《加利福尼亚州消费者隐私保护法案》 《华盛顿隐私法》等系列法案	• 美国推行宽松的数据跨境流动政策，在确保国家安全利益的前提下最大限度地促进数据自由流动。同时，美国建立了个案式的事后监管机制，对联邦政府的重要数据采取较为严格的管理措施，在投资、采购等方面及环节予以限制，提出数据本地化要求。此外，美国通过安全审查等方式满足特定情形下的本地化需求。例如，在外国投资安全审查中，美国通过与外国投资者签订协议的方式控制数据流动。 • 基于美国形成的联邦与各州分散立法、公共部门与私营部门分别立法、私营部门分业立法的分散立法模式，在数据跨境流动治理领域，同样呈现出分部门、分行业监管的治理路径。如美国《公平信用报告法》《健康保险携带和责任法》《金融服务现代化法》等法案对关键行业和领域的个人数据本地存储与跨境流动进行了明确的规定，从而能够及时有效地解决个人数据跨境流动过程中出现的问题。 • 在国际上，美国积极宣扬数据自由流动理念，倡导反数据本地化政策，不断拓展其数据领域的长臂管辖以延伸治理效力范畴，2018 年通过《澄清境外数据的合法使用法》确立数据控制者原则，该法以国家安全为由，赋予了美国政府调取存储于其他国家主权域内数据的权利。

治理模式	主要国家和地区	相关法律法规	核心要点
严格限制	俄罗斯	《俄罗斯联邦个人数据法》 《信息、信息技术和信息保护法》 《俄罗斯劳动法》 《俄罗斯航空法》 《俄罗斯行政犯罪法》等	• 国家安全是俄罗斯数据跨境治理的核心诉求。俄罗斯采取严格限制数据本地存储的严格限制模式，以期实现对于数据跨境的安全保障，并维护国家主权安全。 • 在个人数据跨境流动方面，只要是在俄罗斯开展业务的外国公司，在涉及个人数据处理时，均应遵守俄罗斯现行法律规定的个人数据本地化原则。值得注意的是，外国公司包括那些未在俄罗斯设立代表处或其他法人实体的公司。在没有特殊条件和限制的情况下，可以将个人数据跨境传输到加入欧盟《个人数据自动化处理的个人保护公约》的国家，以及在俄罗斯“确保充分保护个人数据主体权利”白名单中的国家。如将个人数据转移至上述国家以外的其他国家，则必须另征得个人数据主体对个人数据跨境转移的同意。 • 出于数据主权、国家安全以及数据泄露危机频繁化等因素，俄罗斯数据跨境规则日趋严格化。
	印度	《个人数据保护法草案》 《非个人数据框架》 《电子药房规则草案》 《印度电子商务国家政策框架草案》等	• 印度主张数据跨境传输不得影响印度的主权和领土完整，此外，印度数据本地化的另一核心驱动力为发展印度本土数据产业，推动印度数字基础设施的建设。 • 印度的数据本地化与跨境流动立法规制对象包括个人数据及非个人数据，在监管路径上，区分数据类型，多种监管机制并行，实施数据分级分类管控，并设有豁免规则。 • 针对支付数据、IOT 设备收集的数据、社交数据以及搜索记录，印度实施了高度严格的数据本地化要求，禁止该类数据的离境。 • 在个人数据方面，印度《个人数据保护法草案》将个人数据划分为一般个人数据、敏感个人数据和关键个人数据，并对敏感个人数据、关键个人数据的本地化和跨境设置了更严格的要求。具体而言，印度《个人数据保护法草案》体系下个人数据跨境传输的情形包括：对于一般个人数据没有作出限制，可自由传输至境外；对于敏感个人数据，在满足该法第 34 条第（1）款条件时，可以传输至境外；对于关键个人数据，原则上禁止传输至境外。例外情况如满足该法第 34 条第（2）款列举的医疗急救事由或获得印度中央政府允许时，可以传输至境外。

如上表所示，欧盟、美国、俄罗斯、印度在实践中各形成了不同的数据跨境流动治理模式，在不同治理模式下，蕴含着不同的立法考量与核心诉求，从俄罗斯、印度以数据主权、国家安全为要义的数据本地化路径，欧盟的附条件数据跨境自由流动规则，到美国开放的数据跨境原则，可以窥见，各国因具体国情及互联网发展阶段不同，在数据跨境安全管理规则制定上对数据主权、自由贸易这两大重要课题的侧重点选择上有所差异。

二、我国数据跨境流动规则分析

在全球经济协同发展的背景下，随着我国数字经济蓬勃发展、“一带一路”以及网络空间命运共同体的构建，数据作为第五大生产要素在当今的企业跨境合作中逐渐凸显出其重要地位。我国在国家安全主视角下，数据跨境流动规则体系日渐完善，监管力度逐步加强，**目前我国主要从个人信息、重要数据、国家秘密、行业数据以及出口管制、境外调取进行多维度的跨境活动监管**。

回溯我国数据跨境流动的法律体系构建过程，从最初的《网络安全法》中对个人信息和重要数据的跨境行为规范，到立法活动更多落脚于个人信息方向。随着数字经济发展，数据作为生产要素不仅关涉到个人隐私安全，部分重要数据可能会对于国家安全造成影响，我国随即出台《数据安全法》等相关法律法规对重要数据的跨境活动进行规制。各个行业监管部门也在相关法律指引下，针对各自领域的敏感数据、重要数据进行跨境流动行为规范。

整体而言，**我国对于数据跨境主要从两个维度进行规制，一是本地化限制**，按照目前中国相关法律法规，本地化要求更多适用于关键信息基础设施运营者（“CIIO”），要求其在境内运营过程中收集和产生的个人信息和重要数据都应当在境内进行存储。**同时部分行业敏感数据也存在分散的本地化要求**，包括但不限于征信业、银行业、汽车制造业等接触敏感数据、重要数据较为频繁的领域。**二是限制性数据跨境**，我国目前对于数据跨境活动主要采取限制性规范，要求数据控制主体在数据跨境活动前需符合法律规定条件或按照规定完成安全评估、保护认证等条件。**我国对于跨境活动监管规则从多角度多层级进发**，具体要求请见下表：

监管目标	法规名称	法规内容
个人信息	《网络安全法》	第三十七条 **关键信息基础设施的运营者**在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
	《个人信息保护法》	第三十八条 **个人信息处理者**因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一： （一）依照本法第四十条的规定**通过国家网信部门组织的安全评估**； （二）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**； （三）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； （四）法律、行政法规或者国家网信部门规定的其他条件。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。 个人信息处理者应当**采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准**。

监管目标	法规名称	法规内容
个人信息	《个人信息保护法》	第三十九条 **个人信息处理者**向中华人民共和国境外提供**个人信息**的，应当向个人**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**。
		第四十条 **关键信息基础设施运营者**和**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，应当将在中华人民共和国境内收集和产生的个人信息**存储在境内**。确需向境外提供的，应当通过国家网信部门组织的**安全评估**；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。
		第五十五条 有下列情形之一的，个人信息处理者应当**事前进行个人信息保护影响评估**，并对**处理情况进行记录**： … （四）向境外提供个人信息； …
	《个人信息出境安全评估办法（征求意见稿）》	第二条 **网络运营者**向境外提供在中华人民共和国境内运营中收集的个人信息（以下称个人信息出境），应当**按照本办法进行安全评估**。经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。 国家关于个人信息出境另有规定的，从其规定。
		第三条 个人信息出境前，网络运营者应当向**所在地省级网信部门**申报**个人信息出境安全评估**。 向不同的接收者提供个人信息应当**分别**申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估。 每 2 年或者个人信息出境目的、类型和境外保存时间发生变化时应当重新评估。
		第八条 网络运营者应当建立**个人信息出境记录**并且**至少保存 5 年**，记录包括： （一）向境外提供个人信息的日期时间。 （二）接收者的身份，包括但不限于接收者的名称、地址、联系方式等。 （三）向境外提供的个人信息的类型及数量、敏感程度。 （四）国家网信部门规定的其他内容。
		第九条 网络运营者应当**每年 12 月 31 日前**将本年度个人信息出境情况、合同履行情况等报**所在地省级网信部门**。 发生较大数据安全事件时，应及时报所在地省级网信部门。

监管目标	法规名称	法规内容
个人信息	《信息安全技术 - 数据出境安全评估指南（征求意见稿）》	本标准规定了**数据出境安全评估流程、评估要点、评估方法等**内容， 国家网信部门、行业主管部门以及网络运营者按照本指南对其向境外提供的个人信息和重要数据进行主管部门评估和安全自评估，发现存在的安全问题和风险，及时采取措施， 确保个人信息和重要数据合法流动的同时，避免其对国家安全、经济发展、社会公共利益和个人信息主体权益造成不利影响。
	《个人信息和重要数据出境安全评估办法（征求意见稿）》	第二条 网络运营者在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**，应当**在境内存储**。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。
		第四条 个人信息出境，应向个人信息主体**说明**数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，**并经其同意。未成年人**个人信息出境须经其**监护人同意**。
		第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估： （一）含有或累计含有 **50 万人以上的个人信息**； （二）数据量超过 **1000GB**； … （六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。 行业主管或监管部门不明确的，由国家网信部门组织评估。
		第十一条 存在以下情况之一的，**数据不得出境**： （一）个人信息出境未经个人信息主体同意，或可能侵害个人利益； （二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益； （三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。
		第十二条 网络运营者应根据业务发展和网络运营情况，**每年对数据出境至少进行一次安全评估**，及时将评估情况报行业主管或监管部门。 当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时**重新进行安全评估**。
	《数据安全管理办法（征求意见稿）》	第二十九条 境内用户访问境内互联网的，其**流量不得被路由到境外**。

监管目标	法规名称	法规内容
重要数据	《网络安全法》	第三十七条 **关键信息基础设施的运营者**在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
	《数据安全法》	第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。
	《个人信息和重要数据出境安全评估办法（征求意见稿）》	第二条 网络运营者在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**，应当**在境内存储**。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。
		第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估： … （三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等； （四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息； （五）关键信息基础设施运营者向境外提供个人信息和重要数据； （六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。 行业主管或监管部门不明确的，由国家网信部门组织评估。
		第十一条 存在以下情况之一的，**数据不得出境**： … （二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益； （三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。
	《数据安全管理办法（征求意见稿）》	第二十八条 网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经**行业主管监管部门**同意；行业主管监管部门不明确的，应经**省级网信部门**批准。 向境外提供个人信息按有关规定执行。
	《个人信息保护法》	第四十条 **关键信息基础设施运营者**和**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，应当将在中华人民共和国境内收集和产生的个人信息**存储在境内**。确需向境外提供的，应当通过国家网信部门组织的**安全评估**；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

监管目标	法规名称	法规内容
数据出口管制 / 境外调取限制	《数据安全法》	第二十五条　国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。
		第三十六条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。
	《国际刑事司法协助法》	第四条　非经中华人民共和国主管机关同意，外国机构、组织和个人不得在中华人民共和国境内进行本法规定的刑事诉讼活动，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助。
	《证券法》	第一百七十七条　境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。
	《个人信息保护法》	第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。
		第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。
国家秘密	《保守国家秘密法》	第二十八条 互联网及其他公共信息网络运营商、服务商**应当配合**公安机关、国家安全机关、检察机关对泄密案件进行调查；发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，**应当立即停止传输，保存有关记录**，向公安机关、国家安全机关或者保密行政管理部门报告；应当根据公安机关、国家安全机关或者保密行政管理部门的要求，删除涉及泄露国家秘密的信息。
		第二十四条　机关、单位应当加强对涉密信息系统的管理，任何组织和个人不得有下列行为： （一）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络； （二）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换；

监管目标	法规名称	法规内容
特定行业（示例）	《人口健康信息管理办法（试行）》	第十条 责任单位应当结合服务和管理工作需要，及时更新与维护人口健康信息，确保信息处于最新、连续、有效状态。 **不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。**
	《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》	六、 在中国境内收集的个人金融信息的储存、处理和分析**应当在中国境内进行**。除法律法规及中国人民银行另有规定外，银行业金融机构**不得向境外提供境内个人金融信息**。
	《征信业管理条例》	第二十四条 征信机构在中国境内采集的信息的整理、保存和加工，应当**在中国境内进行**。 征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和**国务院征信业监督管理部门**的有关规定。
	《网络预约出租汽车经营服务管理暂行办法》	第二十七条 网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在**中国内地存储和使用**，保存期限**不少于 2 年**，除法律法规另有规定外，上述信息和数据不得外流。
	《汽车数据安全管理若干规定（试行）》	第三条 本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。
		第十一条 **重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估**。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。 我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。 第十二条 汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。 **国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示**。
		第十三条 汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门**报送**以下年度汽车数据安全管理情况：
	《地图管理条例》	第三十四条 互联网地图服务单位应当将存放地图数据的**服务器设在中华人民共和国境内**，并制定互联网地图数据安全**管理制度和保障措施**。 县级以上人民政府测绘地理信息行政主管部门应当会同有关部门加强对互联网地图数据安全的监督管理。

（一）个人信息跨境流动规制

从个人信息的角度，企业在满足相关通用条件的基础之上，应当首先判定其是否有可能落入关键信息基础设施运营者范畴，进而确定适用跨境规则，即本地化前提下的安全评估或其他跨境条件。

具体而言，企业可采取与境外接收方签订跨境合同、进行审计评估、技术监测等措施以基本满足《个人信息保护法》（“《个保法》”）中强调的企业需满足的各项跨境前提要求。但《个保法》下针对个人信息跨境之“单独同意”的要求具体如何实现，仍有待监管部门进一步地指引。此外，对于数据跨境主体事先进行个人信息保护影响评估，我们理解企业在评估时可参考《信息安全技术 个人信息安全影响评估指南》中的方法论及流程，对是否满足个人信息处理基本原则、对个人权益的影响及安全风险以及安全保护措施有效性等进行评估，并将评估报告及处理情况至少保存三年。

除满足上述通用要求以外，个人信息处理者在进行个人信息跨境传输时，还需要根据自身的性质适用相应的个人信息跨境传输规则。构成关键信息基础设施运营者或所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主体，第一步，需进行数据本地化，企业应当将在中国境内收集和产生的个人信息存储在境内；第二步，需通过国家网信部门组织的安全评估，应当在通过国家网信部门组织的安全评估后再进行数据跨境传输。参考网信办于2019 年发布的《个人信息出境安全评估办法（征求意见稿）》，安全评估的重点在于评估个人信息跨境传输是否符合法律法规及政策规定，传输方与接收方所签署的合同是否能够保障个人信息主体合法权益、是否都得到有效执行，传输方与接收方是否发生过个人信息泄露等不良事件。但目前对于安全评估的具体流程及要求，仍有待立法机关进一步明确。

而需要满足数据本地化义务的处理者所处理个人信息量级仍暂未公开。同时，如何正确理解在“中国境内收集和产生的个人信息”，是否涵盖处理者于境外获取产生于境内的个人信息的场景，也有待立法和监管部门的进一步澄清。

对于其他个人信息的处理者，则可以选择满足数据跨境条件，包括但不限于安全评估、个人信息保护认证、标准合同等。但值得注意的是，在现阶段，企业如何进行相关认证、哪些专业机构有权认证仍有待立法者进一步澄清。此外，虽然网信部门尚未发布标准合同，但为了合规准备，实践中已有部分企业参考《个人信息出境安全评估办法（征求意见稿）》、GDPR 下的 SCCs、东盟发布的 MCCs 等跨境传输条款对传输范围、方式、频率等事实的明确以及不同数据处理关系下双方权利义务进行约定。

（二）重要数据跨境流动规制

对于重要数据而言，关键信息基础设施运营者应在满足本地化要求的基础上，经安全评估后出境；而其他数据处理者的出境活动，则有待相关管理办法的出台与规范。此外，对于关键信息基础设施运营者的认定而言，根据近日已生效的《关键信息基础设施安全保护条例》，重要行业和领域的主管部门、监督管理部门（简称“保护工作部门”）根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。[1]

（三）数据出口管制或境外调取限制

除个人信息与重要数据之外，如果企业掌握的数据有可能属于管制物项相关数据或企业因特殊情形触发境外监管机构数据调取的，则还应当适用特殊的数据安全保护规则进行数据本地化，或经国内主管机关批准，否则向外国司法或者执法机构提供存储于中华人民共和国境内的数据将会受到严格限制。

（四）特定行业数据跨境流动规制

当企业掌握的数据落入特定行业时，还应遵守相应的行业规范和要求，目前对数据跨境进行特殊规制的主要包括医疗业、银行业、征信业及汽车业，企业在跨境数据中含有人口健康信息、个人金融信息、征信业相关信息、网约车平台采集的个人信息和生成业务数据、汽车全流程中涉及数据及地图数据时，应当遵守相应的本地化要求或审批申报流程，保障数据流动的合规性。

[1]《关键信息基础设施安全保护条例》第十条。

三、总体国家安全观视域下数据跨境流动治理的价值与定位

如前所述，数据作为社会进步和国家发展的重要战略资源，在内容上既可以表现为个人信息，也可以表现为商业利益，甚至涉及国家安全和公共利益。

首先，我国通过《网络安全法》《数据安全法》《个人信息保护法》等法律法规及配套措施，不断提升数据跨境治理重要性并提供数据跨境治理的“中国方案”，力图保障数据的保密性、完整性、可用性。

其次，数据跨境流动治理不仅关切个人的权利保障，海量的数据跨境流动甚至可能影响到一国的经济安全、社会安全，乃至国家安全。一方面，数据作为新型战略资源对全球经济增长、社会发展的贡献愈发凸显，世界主要国家和地区都在致力于研究如何在数据跨境治理中平衡数据自由流动与有效监管的矛盾。网络空间成为国际政治、经济、外交、安全博弈的新空间和新战场，将国家间的博弈纬度从海、陆、空、太空进一步扩展到第五维度。[2] 另一方面，数据的跨境流动不仅会削弱数据主体对自身数据的控制权，国家关键数据资源的流失还会危及一国数据主权[3]，潜藏了巨大的国家安全风险隐患。完善数据跨境流动治理体系不仅是保障数据主体权利的基本要求，也是维护国家安全和网络主权的重要保障。

总体而言，全球各国数字产业发展面临严重失衡的情况下，数据由发展中国家不断流动积聚到发达国家，可能助长数据霸权的形成，并进一步演化为单边主义的又一重要武器，加剧全球经济发展的失衡状态，深化发展中国家对发达国家的经济依附。[4] 数据跨境流动所引发的国家安全威胁的担忧并非无的放矢。对于包括我国在内的发展中国家而言，国家安全挑战成为数据跨境流动治理体系构建的重要考量因素。但同时，数据的价值在于流动，数据驱动的趋势愈发明显，确保数据安全前提下的自由流动是世界经济的普遍需求。尽管各国对数据跨境流动限制普遍存在，我国立法中也存在数据自由流动的机制安排，以协调数据主权和数据流动的需求。[5]

结论

通观我国和全球主要国家和地区数据跨境流动治理模式与规制规则，跨境数据流动治理已经成为经济发展和时代发展的必然要求，全球数据跨境治理正处于高速发展阶段，数据跨境流动背后不仅为数据安全风险，更是逐步涉及国家竞争问题。我国紧随国际数据流动治理热潮，在总体国家安全观视角下结合国家现实需求搭建了较为完善的中国特色的数据治理体系。诚然，我国数据跨境规则的落地仍存有诸多尚待澄清的内容，为确保企业跨境活动的合法合规，我们也期待后续国家立法部门及相关部门就落地方案予以明确指引与澄清，进一步完善我国数据跨境流动治理体系，促进公民权益、经济发展、国家安全等目标的有机协同，在飞速发展与安全保障中找到可实现数据价值最大化的平衡点。

感谢实习生甘雨丰、刘婉蓉对本文做出的贡献。

[2] 梁亚滨．网络空间：大数据时代国家博弈的新领域 [N]．学习时报，2014-10-20（2）.
[3] 齐爱民．论大数据时代数据安全法律综合保护的完善———以《网络安全法》为视角［J］．东北师大学报 (哲学社会科学版)，2017(4) : 108 — 114.
[4] 参见竺彩华：《市场、国家与国际经贸规则体系重构》，载《外交评论（外交学院学报）》2019 年第 5 期。
[5] 刘云 . 中美欧数据跨境流动政策比较分析与国际趋势 . 中国信息安全 .2021-01-28.

道路千万条，数说十九条：《汽车数据安全管理若干规定（试行）》重点解读

宁宣凤　吴涵　张凯勋　姚敏侣

引言

2021年8月20日，国家互联网信息办公室（以下简称“**国家网信办**”）、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《**规定**》）。《规定》全文共计十九条，自2021年10月1日起施行。在此前的5月份，《汽车数据安全管理若干规定（征求意见稿）》（以下简称“**征求意见稿**”）全文在国家网信办官方网站上公布，已经向社会传达出了将严格管理和保护汽车行业数据安全的明确监管态势，《规定》的颁布正式拉开了行业数据监管的序幕。

但相比于征求意见稿，《规定》在**汽车数据相关概念的基本定义、汽车数据处理者的法律义务、重要数据的识别与认定，以及个人信息主体授权的获取方式等**具体规则上存在较为突出的变化。本文将结合汽车行业不同市场主体的数据安全保护实践，探讨汽车数据合规中的普遍性义务与重点问题，并为汽车企业做好数据合规和监管配合提出可行意见。

一、《规定》出台的背景及其关键概念

（一）法律与事实背景

《规定》出台具有较强的现实与法律背景。在全球数据主权竞争和个人信息保护合规浪潮下，近期我国的网络与数据安全立法立规举措不断。继《网络安全法》之后，《数据安全法》已于2021年6月表决通过，成为我国数据安全领域的基础性法律，也成为国家安全法律体系下的一部重要法律。最终出台的《规定》亦将《数据安全法》作为上位法依据。在个人信息保护领域，在与《规定》发布的同日，我国个人信息保护首部专门立法《个人信息保护法》经历了三审后正式由全国人大常委会通过，2021年11月1日生效后成为保护个人信息的“安全锁”[1]。根据相关部门负责人的说法，此次《规定》“定位于若干规范要求，聚焦汽车领域个人信息和重要数据的安全风险，就若干重点问题作出规定。”[2]由此可见，《规定》基于数据安全和个人信息保护相关法律、行政法规的基本原则，以期进一步实现对汽车行业领域内数据处理活动中的重要安全风险

[1] 北京青年报：《依法打造个人信息保护“安全锁”》，载“光明网”https://m.gmw.cn/2021-08/21/content_35097911.htm 最后访问日期：2021年8月21日。
[2] 国家网信办：国家互联网信息办公室有关负责人就《汽车数据安全管理若干规定（试行）》答记者问，http://www.cac.gov.cn/2021-08/20/c_1631049985019087.htm 最后访问日期：2021年8月20日。

予以事前预防、事中监管和事后处罚，规范和促进汽车数据的合理开发利用。

（二）相关重要概念定义

1. 首次对“汽车数据”进行规章层面上的定义

《规定》第一条第一款对“汽车数据”作出了明确的概念阐释，即**包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据**。从定义上看，相比于征求意见稿，《规定》进一步明确了汽车数据既包括了个人信息数据，也包括重要数据。其中，以《民法典》和《个人信息保护法》中的个人信息定义为参照，《规定》使用“个人信息数据”的概念，从文意解释上可能既包括个人信息的内容（如车主姓名、姓名和联系方式等），也包括对个人信息的记录的各种结构化或者非结构化的相关数据。尽管在理论上对“信息”和“数据”的概念还存在进一步讨论的空间，但根据《数据安全法》对“数据”的定义（任何以电子或者其他方式对信息的记录），由此，对个人信息收集、存储以及使用加工等处理活动的记录本身也成为一类数据，且该类型数据与个人信息主体密切相关，两者是互为表里、相辅相成的关系。《规定》将上述数据看作为整体并以一种独立的数据类型归纳为“个人信息数据”，体现了概念定义上的延展性与全面性。

2. 澄清重要数据与个人信息的内涵关系

《规定》中关于“汽车数据”的定义问题，也引发**数据、重要数据与个人信息之间的关系问题**讨论。首先可以明确的是，《数据安全法》等上位法相关规定没有将个人信息排除出数据或者重要数据的范畴；而《规定》则通过“汽车数据”的概念定义中更加明确地认为，个人信息属于一种特殊类型的数据。此外，根据《规定》第三条条第六款，**超过一定体量（10 万个人信息主体）的个人信息还将构成重要数据**。

基于上述认识，**本文认为相关主管部门通过《规定》进一步澄清了由来已久的“重要数据不包含个人信息”的争议或者误解**。为澄清前述误解，还需联系国家网信办于 2019 年公布的《数据安全管理办法（征求意见稿）》第三十八条第五项[3]中对“重要数据”的定义，其中规定了“重要数据一般不包括企业生产经营和内部管理信息、个人信息等。”但联系该条规定的具体语义环境，对照此次《规定》中对于“个人信息数据”的提法不难发现，所谓的“不包括个人信息”应当解释为不包含企业生产经营和内部的个人信息。换言之，**如果汽车企业在开展生产和经营活动过程中处理达到一定量级的客户或者消费者的个人信息，将不排除被认定为重要数据的处理行为**。对这一关键概念与法律关系的厘清，也体现了此次《规定》出台的重要价值和意义。

3. 与上位法依据做好规则层面上的衔接

如上所述，作为《网络安全法》《数据安全法》以相关上位法在汽车数据安全管理规范中的配套部门规章，最终出台的《规定》多处体现了在规则层面上的接榫和自洽。就本文的观察而言，主要存在以下几个关键方面：

- 首先，在立法思路上，**《规定》呼应了《数据安全法》以行为规范而非主体规范的适用逻辑与立法定位，将适用对象规定为汽车数据处理活动**，即凡是在境内开展汽车数据处理活动，均需满足《规定》的相关要求，由此，适用《规定》的关键在于判断是否涉及“汽车数据的收集、存储、使用、加工、传输、提供、公开等”处理行为，而非局限于狭隘地认定汽车行业相关运营主体的资格范围问题。
- 其次，在适用主体的认定上，《规定》与《数据安全法》保持一致，以“汽车数据处理者”囊括了汽车相关行业及产业上下游的市场主体，尤其是涵盖了利用互联网等信息通讯技术开展汽车服务的市场主体等，**所达成的实质立规目标是实现对汽车行业全生态的数据安全风险管理**。而事实上，考虑到数据作为流动资源的特殊性质，APP 数据安全治理等不同监管专题中已经体现了**“生态圈”监管的思路**，对于各垂直行业内的数据安全管理和立法立规活动，必然将引发全行业、多主体和复杂产业生态的数据合规义务。
- 最后，在汽车行业的个人信息和重要数据的识别和分类上，《规定》遵循《个人信息保护法》中根据信息敏感程度区分保护的法律规则，将汽车数据处理过程中可能涉及的敏

[3] 第三十八条 本办法下列用语的含义：……（五）重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

感个人信息设计了更为严格的安全保护要求。在重要数据各部门落实分类分级保护制度的过程中，《规定》中率先对汽车行业的重要数据以列举的形式作出规定，旨在实现汽车重要数据处理的加强型保护。

二、《规定》下汽车数据处理者的义务责任梳理

对于汽车行业的相关市场主体而言，**严格落实和遵循《规定》中对处理个人信息、敏感个人信息和重要数据的安全管理义务，成为合规经营不可或缺的组成部分**。下文将对其中重点需要关注和履行的汽车数据处理者义务与责任进行表格形式的梳理，帮助企业更好地理解与适用《规定》中的具体合规要求。

（一）个人信息保护

合规义务	具体条文	简要解释
告知义务	第七条 汽车数据处理者处理个人信息应当通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式，告知个人以下事项： （一）处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等； （二）收集各类个人信息的具体情境以及停止收集的方式和途径； （三）处理各类个人信息的目的、用途、方式； （四）个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则； （五）查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径； （六）用户权益事务联系人的姓名和联系方式； （七）法律、行政法规规定的应当告知的其他事项。	汽车数据处理者处理个人信息应当告知处理个人信息种类、收集情境、停止收集方式途径等相关信息。
征得同意义务与匿名化要求	第八条 汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。 因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。	汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。因保证行车安全需要，无法征得个人同意采集到个人信息且向车外提供的，应当进行匿名化处理。
敏感个人信息强化保护要求	第九条　汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法律、行政法规和强制性国家标准等其他要求： （一）具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等； （二）通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响； （三）应当取得个人单独同意，个人可以自主设定同意期限； （四）在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利； （五）个人要求删除的，汽车数据处理者应当在十个工作日内删除。 汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。	在履行告知、征得个人单独同意等义务基础上，汽车数据处理者处理敏感个人信息还应当满足限定处理目的、提示收集状态、为个人终止收集提供便利等具体要求。针对个人生物识别特征信息，明确汽车数据处理者具有增强行车安全的目的和充分的必要性方可收集。

（二）重要数据处理安全

合规义务	具体条文	简要解释
开展风险自评估并向主管部门报送报告	第十条　汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。 风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。	汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。
通过主管部门出境安全评估	第十一条　重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。 我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。	重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。
配合主管部门抽查核验与数据安全评估	第十二条　汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。 国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示。 第十五条第一款　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依据职责，根据处理数据情况对汽车数据处理者进行数据安全评估，汽车数据处理者应当予以配合。	国家网信部门会同国务院有关部门以抽查等方式核验汽车数据出境评估有关事项，或者根据处理数据情况开展数据安全评估，汽车数据处理者应当予以配合。
年度报告	第十三条　汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况： （一）汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式； （二）处理汽车数据的种类、规模、目的和必要性； （三）汽车数据的安全防护和管理措施，包括保存地点、期限等； （四）向境内第三方提供汽车数据情况； （五）汽车数据安全事件和处置情况； （六）汽车数据相关的用户投诉和处理情况； （七）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。 第十四条　向境外提供重要数据的汽车数据处理者应当在本规定第十三条要求的基础上，补充报告以下情况： （一）接收者的基本情况； （二）出境汽车数据的种类、规模、目的和必要性； （三）汽车数据在境外的保存地点、期限、范围和方式； （四）涉及向境外提供汽车数据的用户投诉和处理情况； （五）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确地向境外提供汽车数据需要报告的其他情况。	汽车数据处理者应当在每年十二月十五日前向省、自治区、直辖市网信和有关部门报送年度汽车数据安全管理情况；如涉及向境外提供重要数据的汽车数据处理者，还应当补充报告相关情况。

（三）法律责任

《规定》明确汽车数据处理者违反本规定的，由省级以上网信、工业和信息化、公安、交通运输等有关部门依照《网络安全法》《数据安全法》等法律、行政法规的规定进行处罚；构成犯罪的，依法追究刑事责任。例如，根据《网络安全法》六十六条，关键信息基础设施运营者未按照要求在本地存储数据或数据出境时未进行安全评估的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。而在《数据安全法》下，违反上述规定向境外提供重要数据的，可能被处以最高一千万元的罚款。

三、《规定》中的亮点解读与重要法律问题分析

（一）汽车数据中重要数据处理安全相关问题

1. 重要数据的认定

如前所述，对比《数据安全管理办法（征求意见稿）》，《规定》在规章层面澄清了“重要数据”的外延也可能涵盖个人信息，即**个人信息也可能属于重要数据的范畴，尤其是超过一定体量的个人信息**。《规定》第三条明确了涉及个人信息主体超过 10 万人的个人信息，属于汽车数据处理者处理的重要数据。这就意味着，处理超过 10 万人个人信息主体的个人信息的汽车数据处理者，需要在满足个人信息保护要求的基础上，遵从于重要数据安全处理规范。值得注意的是，**《规定》在定义上也是首次在生效规章层面将“可能危害个人和组织的合法权益”纳入重要数据认定或者识别的概念性描述和考量因素之一**，并且在汽车行业率先对重要数据的范畴以列举形式进行了明确。这对于指导汽车行业的各市场参与主体内部梳理和确认是否涉及重要数据、是否需要遵循重要数据处理安全一系列法律义务，具有较强的现实指导意义。

上述重要数据外延的扩展，与《数据安全法》第二十一条对“核心数据”与“重要数据”的概念区分或许也有一定联系。在此前的规范性文本中，对重要数据的识别基准主要关注的可能还仅是关系国家安全、经济发展和公共利益这一侧面，但《数据安全法》在此基础上加以细化，即“关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。”而与此同时，**考虑大体量个人信息的处理风险也可能涉及对个人、组织合法权益遭到减损或者危害结果，因此《规定》将其也纳入了重要数据的保护范围**。在数字化生产时代，这更贴合了产业发展实际规律，因为大量个人信息的非法处理也可能对于个人或者有关组织产生严重的事实影响或者后果，体现出了立法立规工作对于重要数据的认识在不断深化。除《规定》外，下表将对以往关于重要数据识别认定的相关规范性依据予以简要归纳。

规范名称	公布时间与机构	所涉条款	简要概括
《网络安全法》	2017·全国人大常委会	第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和**重要数据**应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行**安全评估**；法律、行政法规另有规定的，依照其规定。	**首次提出**重要数据的概念，同时规定了重要数据本地化存储和出境安全评估要求。

规范名称	公布时间与机构	所涉条款	简要概括
《个人信息和重要数据出境安全评估办法（征求意见稿）》	2017·国家网信办	第十七条 本办法下列用语的含义：重要数据，是指**与国家安全、经济发展，以及社会公共利益密切相关**的数据，具体范围参照国家有关标准和重要数据识别指南。	赋予对《网络安全法》中的“重要数据”**描述式**的法律定义。
《信息安全技术数据出境安全评估（草案）》	2017·信安标委	《附录 A：重要数据识别指南》 重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据 (包括原始数据和衍生数据), 一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：……	首次提出了**重要数据的完整定义**，并列举了 27 个行业的重要数据类型、范围。
《数据安全管理办法（征求意见稿）》	2019·国家网信办	第三十八条 本办法下列用语的含义：（五）重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。	对重要数据做出法律概念解释，但通过反面列举，将“企业生产经营和内部管理信息、个人信息”排除在重要数据的范围之外。
《数据安全法》	2021·全国人大常委会	第二十一条 ……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。 关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。 各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。	强调对国家核心数据、重要数据的区分以及严格管理、强化保护要求，再次明确各部分、各地区依照数据分类分级保护制度，确定本地区、本部门及相关行业、领域的重要数据目录。

2. 重要数据处理情况的报送义务

国家加强对重要数据保护的一个重要体现，即通过备案或者要求重要数据处理者报送情况的形式，以强化对重要数据处理风险的防范。早在 2019 年《数据安全管理办法（征求意见稿）》中，即规定（第十五条）处理重要数据和敏感个人信息应当向所在地网信部门备案。《规定》中进一步明确和细化重要数据处理情况的报送义务，第十条规定汽车数据处理者开展重要数据处理活动时的风险评估与报送义务，并且明确要求需要向主管部门告知所处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。此外，《规定》第十三条和第十四条规定了每年定期的情况报告义务，进一步强化了主管部门的备案要求。

综合上述，**向网信等主管部门通过自评估报告、管理情况说明等形式，汇报汽车企业所涉及的重要数据处理情况，以达成强化备案和事中监管的效果，**将成为汽车企业接下去合规调整期间的一项必须面对的、较为重要且必须落实的法定义务。

3. 重要数据的本地化存储问题探析

从《规定》的具体条文中不难看出，国家对于重要数据的保护，将愈发强调与重申本地化存储，以及确有业务需要时应当通过出境安全评估的基本监管原则。出境安全评估由国家网信部门会同国务院有关部门组织。通过安全评估后，汽车数据处理者还需要确保在向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。

《规定》第十一条所使用的具体表述为“**应当依法在境内存储**”。由此可见，对于汽车数据处理过程中的重要数据本地化存储原则，应当与《网络安全法》、《数据安全法》及相应的法律、行政法规相衔接。目前，《网络安全法》第三十七条和《数据安全法》第三十一条第一款均规定了关键信息基础设施运营者对于重要数据原则上本地化存储的强制性义务。但与此同时，《数据安全法》第三十一条第二款规定，其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

结合《数据安全管理办法（征求意见稿）》第二十八条规定，网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准；以及《个人信息和重要数据出境管理办法（征求意见稿）》第二条规定，网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。虽然上述相关数据出境安全管理的规定均未实际生效，且条款所用主语均仅限于“网络运营者”，但我们可以预见的是，在《数据安全法》出台后，各行业的数据处理者将成为主要的规制对象，而一系列数据安全配套法规将进入研究、制定和颁布的序列，届时将为汽车数据出境安全评估等要求提供更为坚实的法律基础。

此外，《规定》第十一条第二款要求：“未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。”我们认为，《个人信息保护法》第三章中的第三十八至四十三条，共计六个条款将成为汽车数据处理活动中个人信息跨境提供规则的基础法律依据。

总之，尽管本地化存储义务适用范围尚有不确定性，但**值得注意的是，第一、对于非关键信息基础设施运营在境内收集和产生的重要数据尚未有明确法律法规要求其必须在境内存储；第二、结合出境安全评估义务来看，本地化存储和处理重要数据无疑是国家和企业推荐的实践做法，有利于重要数据的安全防护和行政监管。**

（二）汽车数据中个人信息主体授权相关问题

1. 由个人自主设定同意的具体方式与效力期限

告知同意原则是个人信息保护的基础与主要的合法性来源。与征求意见稿相比，此次最终通过的《规定》对于个人信息主体的授权获取方式和时效问题做出了更符合个人信息主体利益需求和汽车企业实践的规定。征求意见稿第六条第五项中规定的“默认不收集原则”要求：除非确有必要，每次驾驶时默认为不收集状态，驾驶人的同意授权只对本次驾驶有效；此外，征求意见稿第八条第四项中关于敏感个人信息的授权法定要求为：每次都应当征得驾驶人同意授权，驾驶结束（驾驶人离开驾驶席）后本次授权自动失效。总结上述要求来看，对于汽车企业收集个人信息的要求基本可以概括为“每次 opt-in 授权 + 驾驶人离开驾驶席自动失效”。

但上述规则或许在实施落地环节存在一定的困难，此外，考虑到汽车驾驶通常的事实情况，在最终通过的《规定》中，上述要求经过了灵活调整，将个人信息主体的同意具体方式以及授权有效性判断，交由个人信息主体自主决定，具体表现为：

- 处理一般个人信息，需遵循《规定》第六条第二项：默认不收集原则，**除非驾驶人自主设定**，每次驾驶时默认设定为不收集状态；（除非驾驶人自主设定为“opt-out”授权，否则应当单独 opt-in 授权）；
- 处理敏感个人信息，还需额外遵循《规定》

第九条: 汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法律、行政法规和强制性国家标准等其他要求：……（三）应当取得个人**单独同意**，个人可以**自主设定同意期限**；（单独 opt-in 授权 + 个人自主设置有效同意期限）。

2. 无法获得个人授权时应当匿名化处理

《规定》第八条在规定汽车数据处理者处理个人信息原则上应当遵循知情同意或者其他合法性依据的基础上，在第二款中明确：因行车安全需要但无法征得同意时，采集车外个人信息并对外提供的情形下，应当进行匿名化处理。实践中该款规定最为典型的适用场景如在汽车自动驾驶道路测试环境下，为了完成道路场景模拟和算法训练，为设计和完善自动驾驶系统模型而提供车外图像采集信息服务的技术供应商或合作商，除了必须具备开展业务所必需的资质条件下，还需要满足《规定》中的匿名化的个人信息保护要求，具体为：其一，删除含有能够识别自然人的画面；其二，对画面中可能包含的人脸信息等进行轮廓化处理等。该要求实际上是个人信息处理和对外提供的最小够用原则在汽车数据处理中的具体化。

此外，最终通过的《规定》区分了脱敏、匿名化和去标识化处理。征求意见稿中在该款对应的条文中保留了“脱敏处理”作为匿名化处理的替代选项，但在《规定》中，脱敏已经作为一种原则性要求，其实践做法包括匿名化和去标识化不同的方式。这一变化符合了《个人信息保护法》对“匿名化”的定义以及敏感个人信息的处理要求。

（三）汽车数据中特殊类型的数据管理和保护问题

1. 汽车事件数据

汽车事件数据记录器（Event Data Recorder）是基于多个车载电子模块（Electronic Control Units）构成，具有监测、采集并记录碰撞事件发生前、发生时和发生后短时间内车辆和乘员保护系统的数据的设备。汽车事件数据通常会包含车辆速度、车辆制动系统（ABS 等）、车辆识别代码（VIN）等数据[4]，但不包含车辆行程轨迹。汽车事件数据通常以二进制方式存储，需要汽车事件数据提取工具对原始数据进行鉴别、转译，才能形成可读报告。通过记录上述数据，在处理交通事故时，可以全面并客观地分析车辆相关系统的介入程度、人员操作等多重因素，或者结合其他信息，用于司法鉴定目的等。

通常而言，因为可以通过汽车事件数据与第三方数据结合识别特定自然人，包括车主、驾驶人、乘车人，汽车事件数据很可能被视为个人信息，但对于其是否属于敏感个人信息这一问题，《规定》并未专门对此作出明确说明。此前，鉴于汽车事件数据可以“用于判断违法违规驾驶”的特征，征求意见稿曾将汽车事件数据参照敏感个人信息的标准给予保护。如根据征求意见稿第八条规定，运营者收集和向车外提供敏感个人信息，包括车辆位置、驾驶人或乘车人音视频等，以及可以用于判断违法违规驾驶的数据等，应当符合……。此外，征求意见稿还明确要求，科研和商业合作伙伴查询和利用汽车事件数据应当受到严格的限制。

理论上说，不论汽车事件数据是否属于敏感个人信息，在读取、转译汽车事件数据并形成汽车事件记录报告时，均应当获得个人信息主体（一般是“车主”）的同意，或者根据法律法规的要求向执法部门提供。此外，如果跨国汽车企业的汽车事件数据转译能力部署在境外，在形成汽车事件报告时涉及向境外传输汽车事件数据原始数据的，应当向车主告知境外接收方名称或者姓名、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，并取得车主的单独同意。[5]

但实践中，产生汽车事件数据的主体并不一定都是车主，多人使用同一车辆的情况在生活中较为常见，如近亲朋友、代驾司机等。因此，在获得处理汽车事件数据的同意时，可能存在授权主体和个人信息主体不一致的情况。就此问题，美国联邦《司机隐私保护法案（2015）》（Driver Privacy Act of 2015）规定了任何从汽车事件数据记录器中读取的数据，均属于车主或者车辆承租人，并且除特定情形外，读取汽车事件数据必须经过车主或者车

[4] 汽车事件数据的定义可以参见强制性国家标准 GB 39732 – 2020《汽车事件数据记录系统》。
[5] 法律依据为 《个人信息保护法》第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当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。

辆承租人同意，以立法的形式对上述问题作出了明确回应。而目前《规定》还未对此问题进行明确规定，有待后续立法、司法和执法的进一步澄清。但出于审慎合规之目的，汽车企业应当在处理汽车事件数据时获得车主的同意。

此外，汽车事件数据一旦遭到篡改，会影响到当事人事故鉴定的结果，从而对当事人的合法权益产生直接影响。因此，根据《规定》对重要数据的定义，目前并不能完全排除汽车事件数据作为重要数据的可能性，汽车企业亦有可能需要满足重要数据处理义务。如同《规定》将涉及个人信息主体超过 10 万人的个人信息新增列为重要数据，个人信息和重要数据的范围可能有一定的重合，汽车企业应当根据数据泄露或者毁坏可能造成的后果开展数据分级分类工作。

2. 车辆流量、物流等反映经济运行情况的数据

相较于征求意见稿，《规定》将车辆流量、物流等能够反映经运行情况的数据纳入了重要数据的范畴，通过分析大量此类数据，可以形成直接反映国家战略储备、工业生产等重要领域运行状况的数据，或者间接体现各个省市整体经济发展水平的数据。例如，通过分析车辆流量可以直接反映各省市高速中客车和货车的百分比，以及去年同期的变化值，侧面印证各省市的经济发展状况；通过分析物流数据也可以获得反映产业发展和运行的数据；基于互联网信息技术提供网约汽车或者货车等出行服务企业，在提供服务中可能涉及用作上述用途的车辆流量和物流数据。

鉴于汽车产业供应链长而复杂，尤其在“十三五”期间，我国整车和零部件产业体系日渐完善[6]，物流数据在实践中涉及的主体可能较多，包括各级供应商、整车制造商、第三方汽车物流企业和平台等。一级供应商的采购订单、整车制造商生产时的生产计划和零部件采购订单、物流配送企业的生产经营统计数据，均有可能属于物流数据。出于供应链精益、准时（just in time）管理之必要，整车制造商和与供应链伙伴之间需要达成高度协同，而正是基于对零部件供应商进行密集管控，大量数据交互的需求应运而生，而此类数据交互也均可能涉及物流信息。

尽管《规定》并未做穷尽列举，但是对此类重要数据限定了“反映经济运行情况”的前提。**由此可见，并非所有的车流、物流数据均落入重要数据的范畴**，但可以肯定的是，上述数据经过统计分析后形成的统计级的车辆流量、生产经营计划、各类电子信息设备（如芯片）的销售情况，以及根据上述信息发布的报告等，由于与特定行业发展状态联系紧密，而很可能构成《规定》界定下的重要数据。客观说来，这对于跨国汽车企业和供应商全球统一订单或销售管理的模式构成了一定的风险与挑战，因此需要企业在内部自评估的基础上，满足《规定》中对处理重要数据的相关义务，并且开始认真对待乃至考虑本地化部署相关订单和销售系统的必要性问题。

3. 智能网联汽车数据

根据工业和信息化部联合公安部和交通运输部于 2021 年 7 月 27 日发布了《智能网联汽车道路测试与示范应用管理规范（试行）》，智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与 X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现安全、高效、舒适、节能行驶，并最终可实现替代人来操作的新一代汽车。

因为智能网联汽车涉及各类数据交互能力以及决策能力，相较于传统汽车，智能网联汽车产生的数据更加多样化，且车辆安全相关基本特征、技术参数仍在不断变化，对汽车数据处理者的网络安全和数据安全管理也提出了更高的要求。

(1) 智能网联汽车数据安全

作为《规定》中的新增条款，《规定》第十六条强调了国家推动智能网联汽车网络平台的建设，开展智能网联汽车运行和安全保证服务等，并协同汽车数据处理者加强智能网联汽车网络和数据安全防护。此外，国家工业和信息化部（以下简称“工信部”）近期发布的《关于加强智能网联汽车生产

[6] 中国汽车工业协会，《2020 年中国汽车工业经济运行报告》，http://lwzb.stats.gov.cn/pub/lwzb/tzgg/202107/W020210723348607396983.pdf 最后访问日期：2021 年 8 月 20 日。

企业及产品准入管理的意见》(以下简称“**《意见》**”),再次强调了对智能网联汽车生产企业的网络安全和数据安全要求,与此前发布的《智能网联汽车生产企业及产品准入管理指南(试行)》(征求意见稿)保持基本一致,智能网联汽车生产企业应当建立数据资产管理台账,实施数据分类分级管理,加强个人信息与重要数据保护,并且应当落实网络安全等级保护制度和车联网卡实名登记管理要求,建立汽车网络安全管理制度,依法落实网络安全等级保护制度和车联网卡实名登记管理要求,明确网络安全责任部门和负责人。此外,《意见》对在线升级(OTA 升级)场景下的汽车数据处理者也提出了一定的告知义务,即向车辆用户告知在线升级的目的、内容、所需时长、注意事项、升级结果等信息。

为了确认配备自动驾驶功能的智能网联汽车的安全性能,《意见》提出此类汽车应当具有事件数据记录系统和自动驾驶数据记录系统,满足相关功能、性能和安全性要求,用于事故重建、责任判定及原因分析等。其中,自动驾驶数据记录系统记录的数据应包括车辆及系统基本信息、车辆状态及动态信息、自动驾驶系统运行信息、行车环境信息、驾乘人员操作及状态信息、故障信息等。虽然《意见》没有对事件数据记录系统应当记录的数据进行规定,但工信部在 2020 年就发布了强制性国家标准 GB 39732—2020《汽车事件数据记录系统》,对 M1 类车辆的汽车事件数据记录系统应当采集的数据类别、数据格式等进行了详细的规定。

综合以上,智能网联汽车生产企业应当根据相关法律法规的要求,加强数据和网络安全管理能力、规范软件在线升级、加强产品管理,落实完善保障措施,在开展新兴科技业务的同时,坚守数据安全的法律底线。

(2) 自动驾驶相关数据处理要求

自动驾驶发展浪潮已经经过了 12 个年头的发展,无论是传统整车制造厂商还是新兴的互联网科技公司,都已经投入了这场颠覆性的技术革命中。作为前沿科技和传统汽车的结合,发展自动驾驶已经上升到国家战略层面,以期抢占技术和产业的高点。

自动驾驶以实现完全代替人类司机为目标,因此需要不断感知车辆周边环境并实时进行决策。在自动驾驶技术研发过程中,车辆需要配备各类传感器(比如 LiDAR、毫米波雷达和摄像头),并通过传感器融合的方式感知并收集大量的真实场景数据,以不断的训练自动驾驶算法,提高识别和决策能力。此外,自动驾驶技术还需要依赖于高精地图,即相较于传统 GPS 地图,具有厘米级精度以及更多数据维度的地图。自动驾驶算法需要通过传感器捕捉的各类信息将与高精地图融合后重建三维场景,并根据融合后的数据进行决策。[7]

因此,无论是在研发自动驾驶技术的过程中还是最终实现自动驾驶的目标,均涉及将传感器捕捉的信息传输至终端进行计算、验证并且反馈决策结果至车辆的过程,而这一过程可能被认定为测绘行为,并且此过程处理的数据可能属于测绘成果,从而可能涉及国家秘密。对于跨国汽车企业而言,出于统一管理自动驾驶算法技术优化之目的,可能会涉及将境内采集的相关数据向境外传输。在此过程中,应当注意国家对外提供测绘成果的相关要求,比如《测绘成果管理条例》第十八条规定,对外提供属于国家秘密的测绘成果,应当按照国务院和中央军事委员会规定的审批程序,报国务院测绘行政主管部门或者省、自治区、直辖市人民政府测绘行政主管部门审批。

我们注意到,最终通过的《规定》在界定重要数据时,删去了征求意见稿中将“高于国家公开发布地图精度的测绘数据”作为重要数据的规定,但我们理解,如上所述,可能是由于该类型的数据精度较高,反而可能构成原本就受到强监管和保护的地图和测绘成果及相关保密信息,而又考虑到我国测绘相关的法律法规已相较完善,对该种类型数据的保护或许也更高于对重要数据的处理安全性要求,为了使得《规定》更具针对性和聚焦性,从而略去了征求意见稿的上述规定。因此,我们一方面不能理所当然地从中解读出“测绘数据不是重要数据”的观点;另一方面,鉴于兜底条款,基于自动驾驶所需的各类传感器捕捉的数据亦有可能属于重要数据。

此外,自动驾驶汽车在行驶过程中,传感器会捕捉周围行人的个人信息,并可能需要对此类数据进行分析以进行行为分析和意图预测,但出于现实原因限制,此过程无法获取行人的授权同意。针对此情况,《规定》第八条第二款也做出了一定回应:因保证行

[7] 除预先录入高精地图外,某些汽车企业的自动驾驶技术还可以通过传感器,获取各类交通信息并实时构建地图。

车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面或者对画面中的人脸信息等进行局部轮廓化处理。本款结合第六条的脱敏处理原则，对汽车企业保护个人信息指出了方向。但对涉及行人的画面或者人脸信息进行删除或者模糊化处理，首先需要识别具体某一帧画面包含行人或人脸信息，而自动驾驶车辆通过多个高速摄像头采集数据，每秒可能产生几百帧画面，这意味着将需要付出大量的数据处理活动和时间，也对汽车企业和地图服务商提出了技术难度上的更高要求。

鉴于以上，汽车企业在开展自动驾驶业务时，应当注重数据合规要求，在系统研发和部署时通过设计保护隐私（Privacy by Design），并且与地图服务提供商深入讨论具体的业务开展方案，在合作协议中明确约定技术细节和双方的数据安全责任，以确保地图服务商和汽车企业双方均具备足够的数据处理安全能力，满足相关法律法规要求。

写在最后的话——纵深监管下的汽车行业数据合规与企业应对

汽车行业数据安全与行业发展息息相关，自2020 年以来，国家密集部署“新基建”政策，智能网联汽车迎来发展黄金期，但在大力发展新兴科技的同时，汽车企业也需要认真考虑《网络安全法》《数据安全法》《个人信息保护法》以及《规定》下的数据安全与个人信息保护的要求，在满足强制性规定的同时寻求优化数据资产管理的空间。随着智能网联汽车行业的快速发展，我们可以预见相关的立法和监管将日趋完善，进一步加强智能网联车技术的实际应用能力，在技术发展和法律要求的不断迭代发展中，推动着工业时代的汽车被电动化、网联化、智能化等全新概念重塑。

而《规定》作为《网络安全法》与《数据安全法》的重要配套规章，明确了汽车数据安全的基本原则与具体要求，作为行业垂直监管的典型，体现了网络安全和数据安全正在从一般性法律规则向具体和细分行业纵深发展的趋势。正如我们在此前数据安全法评析文章中指出，重要数据的识别是数据安全工作的重中之重，各行业主管部门会根据行业发展变化，结合考虑诸多因素，确定各行业涉及的重要数据以及相应的重要数据管理要求。随着我国数据安全制度的逐步完善，此类行业垂直监管的趋势必将向其他行业产生辐射效果，最终形成以《数据安全法》为框架，各行业数据安全管理规定为内容的数据安全合规体系。而在激烈的市场合规经营竞争中，企业自应当打起十二分精神，准备迎接数据安全治理与保护的新纪元。

横看成岭侧成峰——从《个信法》和《数安法》等看网络空间治理的中国方案

宁宣凤　吴涵

前言

2021 年 8 月 20 日《中华人民共和国个人信息保护法》经人大常务会议表决通过，并于 2021 年 11 月 1 日开始实施。与此同时《数据安全法》也于 2021 年 9 月 1 日施行。可以欣喜地看到，国内将迎来网络空间治理规范集中完善、更新的一轮浪潮，显示出我国从规范监管层面顺应信息时代的系统设计，为世界提供充满借鉴意义的中国方案。

本文将分析中国网络空间治理“四位一体”的监管思路与多维互联的监管体系。在此基础上，通过梳理欧盟、美国在网络层、软件层与数据层的监管规范，阐明中国网络空间治理的特点。最后，本文将对国内网络空间治理三大核心法律（《网络安全法》《数据安全法》《个人信息保护法》）的框架、规制对象以及重点内容进行概述与比较，为企业由表及里、由浅至深地呈现我国网络空间治理全貌。

一、中国网络空间治理体系概述

（一）新信号：信息技术的发展催发数据价值，数据成为新的监管重点

从用户端的网络购物、在线结算，到企业端的云计算服务、信息化管理，再到国家层面的贸易政策、安全战略——不同主体的关注焦点都与信息技术息息相关。同样，电子商务、生物制药、互联网金融等行业热点也全部围绕信息技术展开。毫无疑问，步入 21 世纪，信息技术正以前所未有的速度

更新迭代，并在市场经营、社会治理等方面迅速铺开，由此成为国家监管的核心。然而，与金融、资源、粮食、生态和核等具体领域的安全不同，信息安全的特殊性在于：它自成一个领域，同时也是信息时代所有领域的基础。对此，有学者明确指出：信息安全中“安全”对应的是事关一国生死存亡的“security”，而不仅仅是“safety”，信息安全不应只被视为网络领域或信息系统的安全，而应是信息时代的国家安全。[1]

数据作为记录信息的主要载体之一，随着信息技术的发展，其商业和社会价值被广泛认可，但同时，由信息安全延伸的数据安全问题上升到新的高度。中共中央 国务院在 2020 年 5 月发布的《关于新时代加快完善社会主义市场经济体制的意见》中明确指出，要加快培育发展数据要素市场，完善数据权益界定、开放共享、交易流通等标准和措施。而在 2021 年 7 月 14 日举办的中国互联网大会数据安全论坛上，中国信息通信研究院安全所信息安全部主任魏薇表示，展望未来，2023 年中国数据安全行业市场规模有望达到 97.5 亿元；回顾过去，2020 年全球数据泄露超过去 15 年总和。其中政务、医疗及生物识别信息等高价值特殊敏感数据泄露风险加剧，云、端等数据安全威胁居高不下，数据交易黑色地下产业链活动猖獗。各国纷纷将信息与数据安全上升至国家安全高度，优化相关安全政策，加快设立统一的安全保护机构，加强对重点主体、重要数据类型、重要数据处理活动的安全监管 。[2]

（二）新框架：安全监管思路纵深发展

基于现有立法文本与政策文件，我们理解目前中国网络空间治理的监管思路呈现出纵深发展、逐层细化的特点。

具体来看，网络安全成为信息时代国家安全的重点内容已自不待言。而在网络安全中，信息是最核心的部分，对于信息的操纵、破坏和应用已是当代政治经济和文化统治的重要领域，也是引起国际安全格局发生重大变化的重要因素之一[3]。同时，尽管信息的存在形式多种多样，但其能够在网络空间中高效传播，离不开数据这一重要载体。由此，数据一跃成为国家的基础性战略资源，对于数据安全的重视也使得“数据主权”成为相关立法的基本立场[4]。综上，我国目前网络空间的治理思路可以概括为“**四位一体**”，即“**国家安全——网络安全——信息安全——数据安全**”。

上述“四位一体”的监管思路体现在不同时期的立法活动中，比如中共中央政治局于 2015 年 1 月 23 日审议通过了以“总体国家安全观”为指导的《国家安全战略纲要》，就国家安全各领域做出宏观协调部署。2015 年 7 月 1 日，全国人大常委会高票通过了《国家安全法》，通过基本法律形式确立了“总体国家安全观”的指导地位。2016 年 11 月 7 日《网络安全法》（以下简称《网安法》）在全国人大常委会通过，成为网络空间安全治理的重要法律依据。而在 2021 年 9 月 1 日实施的《数据安全法》（以下简称《数安法》）则进一步明确数据处理活动中的监管规范。

值得特别注意的是，此次表决通过的《个人信息保护法》（以下简称《个信法》）表明个人信息已成为信息安全中的重要内容。《个人信息保护法》第一条开宗明义：“为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。”，表明我国将个人信息受保护的权利提升至更高的高度。与此相应，《民法典 - 人格权编》《刑法》《电子商务法》和《消费者权益保护法》也都补充个人信息保护条款[5]。

在2021年年底《数安法》《个信法》相继实施后，将以《网安法》《数安法》、《个信法》为核心，各领域法律法规相互衔接补充，形成覆盖各行各业的网络空间安全保护网。

（三）新体系： 多维互联，网络、软件、数据多层发力

除去《网安法》《数安法》和《个信法》，在上述监管思路的指导下，我国政府相继出台《网络安全审查办法》《关键信息基础设施安全保护条例》

[1] 左亦鲁：《国家安全视域下的网络安全——从攻守平衡的角度切入》，载《华东政法大学学报》2018 年第 1 期。
[2] 参见 澎湃新闻 李文姬：《中国信通院专家魏薇：去年全球数据泄露数量超过去 15 年总和》，https://www.thepaper.cn/newsDetail_forward_13591270，最后访问日期：2021 年 8 月 22 日。
[3] 参见张新华：《信息安全：威胁与战略》，上海人民出版社 2003 年版，第 110 页。
[4] 参见 黄志雄：《网络主权论》，社会科学文献出版社 2017 年版，第 27 页。许可：《数据安全法：定位、立场与制度构造》，载《经贸法律评论》2019 年第 3 期。
[5] 参见 腾讯研究院 王融：《< 个人信息保护法 >——五个划时代意义》，https://mp.weixin.qq.com/s/A1qlwxIbtU0UT-bZt2K0Kg，最后访问日期：2021 年 8 月 22 日。

等一系列法律法规，多维度、全方位治理网络空间。

从实务的角度分析，我国网络空间治理的法律法规可划分为：网络层、软件层、数据层[6]。具体来看，“网络层”多指基础物理设备，即众多提供关键服务的服务器、路由器、交换机、终端接入设备以及将这些设备连接起来的有形或者无形的线缆。于 2021 年 9 月 1 日实施的《关键信息基础设施安全保护条例》即为此层级的典型规范；“软件层”可理解为运行于网络层之上的软件，这些软件构成并限定了用户使用网络的方式和限度。除非具备特定的能力，否则最终用户只能在软件层限定的权限内，接入网络并使用相关的资源；最后则是由众多互联网用户所创造的“数据层”，即通过网络层与软件层传播的具体内容，比如《数安法》明确将保护对象划分为一般数据、重要数据、核心数据[7]。面对这种多层发力、多维互联的立法体系，企业合规应当注重理解不同法律规范的基础定位及相互联系，从而在运营全过程中甄别风险，及时调整。

二、域外网络空间治理比较研究

根据国际电联定义，网络空间可以描述为“由计算机及其系统、网络及其软件、各种数据以及用户在内的所有要素或部分要素组成的物理和非物理领域”[8]。作为全球新兴安全领域及治理领域，国际上在网络空间治理领域已有诸多尝试及努力，例如，联合国等国际组织寻求在全球网络安全规范制定中发挥作用，中国和美国等大国积极寻求发展关于网络安全的双边对话和合作，欧盟区域性网络安全治理不断走向规范化发展。

基于上文分析，我们认为，网络基础设施安全是网络安全的物质基础，保障网络层及软件层的安全，是确保通过网络层及软件层传播的数据安全的必由之路。有鉴于此，下文将以网络层、软件层、数据层三个维度为出发点，梳理域外主要国家和地区的网络空间治理体系，综观全球视野下的中国网络空间治理架构。

（一）美国网络空间治理概述

美国是现代计算机技术和互联网的诞生地，美国在利用法律和政策工具治理网络空间方面拥有丰富的经验。目前，美国已形成包括立法、司法和行政三大领域以及联邦与州两个层次在内的网络空间治理体系。美国的互联网法规涉及面较为宽广，虽尚无联邦层面普遍适用的网络安全法，但已有诸多针对互联网的宏观整体规范以及微观的具体规制，其中囊括了行业准入规则、电话通信规则、数据保护规则、消费者保护规则、版权保护规则、反欺诈与误传法规等诸多方面。美国网络空间的治理，也主要通过执行关于互联网领域的各项法律来实现的。早在 1977 年，美国便颁布了《联邦计算机系统保护法》，开创了网络空间法制治理的先河；美国《1987 年计算机安全法》将计算机自身的安全以及计算机系统内数据的安全上升到国家高度。伴随互联网发展的每一步前进，美国的相关立法都会紧随其后，据统计，相关法律法规多达 130 多部，涵盖联邦立法及各州立法，囊括网络空间治理的方方面面，美国也因此成为世界上拥有互联网法律最多的国家。

在治理理念层面，美国前国务卿希拉里·克林顿曾对美国《网络空间国际战略》的评价中明确指出，美国网络空间治理的目标为“确保互联网的开放、安全和自由”。美国在保障基本安全和公民权利的前提下，采取了更为积极主动的治理理念。网络空间安全实质上已成为国家安全的核心范畴之一，美国政府认识到掌控网络空间的重要性，从战略层面做出规划，不断加大规制力度，主动肩负保障国家网络空间安全的责任。

在网络层方面，通过法律途径保护一国关键信息基础设施的安全，已成为各国网络空间治理的重点。美国最先开启关键网络基础设施领域的相关信息立法，先后制定了《国家信息基础设施保护法》《关键基础设施信息保护法》和《增强联邦政府网络与关键性基础设施网络安全》等多部法律政令，美国国家标准与技术研究院（NIST）于 2018 年 4 月发布了改善关键基础设施网络安全的框架文件。美国的网络安全政策战略始终以网络空间内关键基础设施的保护为中心，着力于与其有关的三个重点方面，即政府部门和私营部门之间的公私合作、网络安全信息的共享以及个人隐私和公民自由的保护，并构建了以国土安全部为领导的信息监管体系，相关部

[6] 相关分类初步形成学界共识，参见 YochaiBenkler，“From Consumers to Users: Shifting the Deeper Structures of R egulation towards Sustainable Commons and User Access”，Federal Communications Law Journal，Vol. 52，No. 3，2000.
[7]《数据安全法》第二十一条。
[8] 劳伦斯·莱斯格 . 代码 2.0：网络空间中的法律 [M]. 北京：清华大学出版社，2009 版，p.36

门各司其职，共同维护美国关键信息基础设施领域的安全。此外，美国联邦法律《计算机欺诈和滥用法案》（CFAA）禁止未经授权访问或使用受保护的计算机，违反该法的处罚相当严格，部分违法行为最高可被判处 20 年监禁。除此之外，该法同样将黑客行为定义为犯罪。美国《电子通讯隐私法》（ECPA）规定，未经授权（或超出授权）故意访问提供电子通信服务（ECS）设施的行为是一种刑事违法行为，个人计算机则不被视为提供 ECS 的设施。此外，美国总统拜登于近日签署了一份国家安全备忘录，要求联邦机构制定关键基础设施的网络安全性能目标。

同时，美国高度重视信息系统安全防护及保障工作，2002 年出台的《联邦信息安全管理法案》（FISMA）[9] 定义了全面的框架以保护政府信息、操作和财产免于自然及人为威胁。FISMA 把责任分配到各个机构，以确保联邦政府的数据安全。该法案要求程序员和每个机构的负责人对信息安全计划执行年度评审，目的是为了以一种低开销、及时和有效的方式来把风险控制在可接受的范围之内。NIST 概括了遵守 FISMA 的九个步骤：（1）保护信息分类；（2）底线控制；（3）采用风险评估程序以重新修改控制；（4）在系统安全计划中记录控制；（5）在合适的信息系统中实施安全控制；（6）一旦安全控制付诸实施，评估安全控制的有效性；（7）决定任务和商业案例的风险等级；（8）赋予信息系统处理权；（9）持续监视安全控制。此外，为提升信息系统安全，配合 FISMA 法案的实施，FISMA 给联邦机构、美国国家标准技术研究院（NIST）和预算与管理办公室（OMB）指派了特定的职责。明确 NIST 的职责是研制信息安全标准（联邦信息处理标准）和非国家安全信息系统指南（特别出版物 800 系列）[10]。为有效实现 FISMA 下的各项目标，NIST 通过一整套涵盖信息系统规划、风险管理、安全意识培训和教育以及安全控制措施的信息安全标准体系，为确保信息安全提供了有效的框架和机制，特别出版物 SP 800 系列是其中的重要组成部分。迄今为止，美国大部分网络安全框架都是由行业最佳实践指南推动形成的，美国 NIST 此前制定的诸多信息安全框架更多针对联邦机构，但其他机构特别是行业组织，也可自愿采用其发布的信息系统指南。

在软件层方面，美国已针对移动恶意软件、间谍软件等破坏性应用程序出台相关规定，相关政府部门及标准组织已就互联网应用程序开发及安全审查出台了相关标准及规定，其中，针对软件层的个人信息保护方面，美国采取补充既有法律体系和行业自律模式，多强调企业与政府合作。该层面主要立法包括《间谍软件控制法》、CFAA 等法案中针对间谍软件等应用程序的相关规制。该层面指南如近期由 NIST 发布的《开发者软件验证最低标准指南》，2021 年 5 月 12 日，美国总统签发第 14028 号行政令，要求 NIST 在 60 天内推荐针对软件验证的最低标准，在此背景下发布的《开发者软件验证最低标准指南》推荐可广泛应用的构成最低标准的技术，包括“建立查找设计层安全问题的威胁建模”“采用静态代码扫描查找重要漏洞”“模糊测试”等十一条技术建议；早先于 2016 年美国国土安全部发布的《移动安全研发项目指南》则从移动设备安全、基于移动可信根的软件、移动恶意软件分析、移动应用安全等方面提供了实现移动安全的研发技术指南。除在立法及标准层面出台相关法律及指南之外，美国网络安全和基础设施安全局（CISA）和 NIST 于 2021 年上半年联合发布《防御软件供应链攻击》报告，其中提供了与软件供应链攻击相关的信息、关联风险以及缓解措施。

在数据层方面，美国国会颁布了一系列旨在为个人信息提供法定保护的联邦法律，与中国和欧盟采用的统一立法模式不同，美国的联邦法律则是“拼凑”起来规范组织机构的数据保护实践，而非单一的综合性法律。美国联邦层面的数据保护立法诸如《儿童在线隐私保护法》，其针对在线运营商收集的儿童信息提出了相关数据保护要求；《电子通信隐私法》，其中包括禁止未经授权访问或拦截储存或运输中的电子通信信息；《公平信用报告法》涵盖了与消费者信誉相关的信息的收集和使用的相关规定；《联邦证券法》规定了针对数据安全控制以及数据泄露报告责任；《健康保险可携带性和责任法案》包括了医疗保健提供者收集和披露受保护健康信息的相关规定；《联邦贸易委员会法》则通过禁止“不公平或欺骗性的行为或做法”以有效填补其他法案未涉及的立法空白；《格雷姆 - 里奇 - 比利雷法案》（GLBA）中存在金融机构使用、披露和保护客户个人信息的相关规定；《电话消费者权

[9] 全国信息安全标准化技术委员会：国外信息安全政策法规《美国联邦信息安全管理法案》（Federal Information Security Management Act，FISMA），https：//www.tc260.org.cn/front/postDetail.html?id=20141211111207。
[10] 美国国家标准和技术研究院信息安全标准化系列研究 （ 七 ） 联邦信息安全管理法案实施项目进展研究 [J]. 信息技术与标准化 ，2011（10）：35~39.

益保护法》（TCPA）限制电话和短信招揽顾客;《存储通信法》保护电子通信中所涉及的个人隐私信息;《家庭教育权利和隐私法》中存在有关学生记录保护的规定；2018 年 3 月，美国国会通过《澄清海外合法使用数据法》（“CLOUD 法案”），为美国数据领域的“长臂管辖”规则提供了基础。《国家数据销毁法》《国家社会保障号码保护法》《国家保险信息和隐私保护法》《反垃圾邮件法》中同样存在个人信息保护的相关规定。此外，美国 51 个司法辖区要求向消费者和 / 或监管机构报告自身违反个人信息保护规范的行为。

除联邦层面的法律之外，美国各州层面也出台了相关数据隐私法案。如 2020 年 1 月 1 日起正式实施的《加利福尼亚州消费者隐私保护法案》（CCPA），该法案建立了全面的数据保护制度。CCPA 适用范围为在美国加利福尼亚州开展业务的任何公司，该法案为消费者提供了三项主要权利：首先，消费者有权知悉企业收集或出售的消费者信息，即要求企业将收集的个人信息告知消费者；其次，CCPA 为消费者提供了“opt-out”的权利; 再次，CCPA 在某些情况下赋予消费者权利以要求企业删除所收集的消费者的任何信息（即“删除权”）。此外，CCPA 要求网站进行隐私披露；《伊利诺伊州生物特征信息隐私法》（BIPA）也存在个人信息保护的相关规定。

（二）欧盟网络空间治理概述

欧盟在网络空间治理体系建设方面成效显著，已形成包括立法、战略、实践三大部分的网络空间治理。立法体系包含决议、指令、建议、条例等，欧盟有关网络安全的重要立法有三：网络与信息安全（Network and Information Security，NIS）指令、一般数据保护条例（General Data Protection Regulation，GDPR）和欧盟网络安全法案（EU Cybersecurity Act）；战略体系包含长期战略与短期战略，如欧盟于 2013 年发布的《欧盟网络安全战略：开放、安全和可靠的网络空间》，提出有效减少网络犯罪、制订欧盟网络防御政策、发展网络安全产业和技术以及建立欧盟统一的网络空间国际政策等战略要点，力图在欧盟建成世界上最安全的网络环境。实践体系则包含机构建设、培训、合作演练等多项内容，如欧盟委员会于 2013 年 1 月在荷兰正式成立的欧洲网络犯罪中心，该中心连通所有欧盟警务部门的网络，整合欧盟各国的资源和信息，支持犯罪调查，旨在保护欧盟范围内企业和民众不受网络犯罪威胁。

在治理理念层面，欧盟范围内，任何可能导致公民权利遭到侵犯的政府职能扩张都会遭到质疑，其行为合法性亦会遭到削弱。虽然近年来欧盟不断加大网络空间监管力度，但同时政府对于信息审查和监控权利也被加以严格限制，防止网络审查损害公众利益和网民利益。欧盟“不要求为网络问题建立新的国际法律文书”，相反，它建议把重点放在如何促进和执行现有的法规，以及如何制定新的行为规范。

在网络层方面，作为欧盟数字单一市场（Digital Single Market，DSM）一系列举措的重要组成部分，NIS 指令是欧盟层面第一部综合性网络安全立法，NIS 指令于 2016 年 7 月 6 日在欧盟议会二读程序中通过，其目的在于在欧盟范围内实现统一的、较高水平的网络与信息系统安全，它还为基础服务的运营者制定了强制性的安全和通知要求，并涵盖了许多其他与网络安全相关的主题，该指令建立的网络层法治框架包括以下内容：

1. 欧盟成员国须提高网络安全能力，制定网络与信息系统安全的国家战略

NIS 指令要求欧盟成员国制定网络与信息系统安全的国家战略以明确战略目标、合理政策以及相应监管措施，具体应囊括：一是 NIS 国家战略的目标和优先工作，以及与之相应的治理框架，其中应涵盖政府机构以及相关参与者各自的角色与责任；二是网络与信息系统安全相关的防范、应对以及恢复措施，包括政府机构与私营部门之间的合作；三是与 NIS 国家战略有关的教育以及培养项目；四是研究与发展计划；五是相关风险评估计划。此外，欧盟成员国应确定至少一个计算机安全事故响应小组（Computer Security Incident Response Team，CSIRT），负责欧盟成员国国家层面的网络安全事故监测，就网络安全风险和事故相关利益方提供预警、警报、通知、信息传递等，应对网络安全事件，提供动态网络安全风险和事故分析。

2. 增强欧盟层面各成员国之间的网络安全战略合作与信息共享

为增强欧盟层面各成员国之间的网络安全战略

合作与信息共享，NIS 指令要求建立一个合作团体和一个国家 CSIRT 网络，合作团体由成员国代表、欧盟委员会、欧盟网络与信息安全局（ENISA）组成。合作团体主要作用包括制定工作计划，指导网络安全相关工作开展，分享网络安全风险信息等。

除此之外，2016 年通过的 NIS 指令还适用于基础服务运营者以及部分数据服务提供商的信息系统。首先，NIS 指令适用于基础服务运营者（Operators of Essential Services），基础服务包括交通、能源、银行业、金融市场基础设施、饮用水供给、数字基础设施（包括 IXP、DNS 服务提供者、顶级域名注册）。根据 NIS 指令第 14 条的规定，基础服务运营者需要履行三项义务：第一，应采取适当的技术和组织措施管理网络安全风险，这些措施应确保一定程度的网络安全；第二，应采取恰当措施防止和削弱网络安全事件的影响；第三，应将具有重大影响的网络安全事件通知主管机构。在确定网络安全事件影响的程度时，应考虑以下因素：一是受影响的用户数量；二是事故持续时间；三是事故影响的区域范围。此外，为督促基础服务运营者履行义务，主管机构可以要求基础服务运营者提供网络安全评估信息，并提供相关证据证明其已采取有效安全措施。其次，NIS 指令还适用于部分数据服务提供者（Digital Service Providers）的信息系统，包括网络搜索引擎、云计算、网络交易市场，且 NIS 指令不适用于小微企业和前述三类数字服务提供者之外的企业。数字服务提供者同样需要履行 NIS 指令第 14 条规定的三项义务。综上，对于数字服务提供者，NIS 指令遵循“轻监管”的思路，欧盟成员国不得对数字服务提供者施加其他更为严格的安全和通知义务，也仅在有证据证明数字服务提供者未履行义务时才展开相关监管活动。

在软件层方面，1995 年，欧洲理事会出台了“计算机软件法律保护”指令和“数据库法律保护”指令。其后，2019 年 6 月生效的《欧盟网络安全法》主要制度创新即指定 ENISA 作为欧盟网络安全的常设机构。该法规定了 ENISA 的任务目标：即采用欧洲网络安全认证体系框架，确保欧盟 ICT 产品、ICT 服务或 ICT 流程的网络安全达到足够的水平。《欧盟网络安全法》的特色制度设计包括网络安全认证制度以及界定合格评定机构的资格标准，其中，《欧盟网络安全法》最终确定网络安全认证框架需要的两项基本要素：其一，必须是国家级评估机构，以确保该机构具备评估产品的技术能力；其二，必须由明确定义的评估标准和准则，以监控产品是否符合要求，再授予和更新网络安全认证。网络认证框架还要求能够报告和处理以前未检测出的漏洞。《欧盟网络安全法》还界定了合格评定机构的性质：合格评定机构是根据国家法律设立、具有法人资格、独立于其评估的组织或 ICT 产品、ICT 服务或 ICT 流程之外的第三方机构。

聚焦欧盟近期网络空间治理动态，软件层相关动态包括欧盟委员会于 2021 年 3 月 2 日在其官网公布《2021 年管理计划：通信网络、内容和技术》（以下简称《计划》），《计划》包括数据、人工智能、网络信息安全和网络内容管理四部分，其中，围绕网络和信息安全，《计划》将修订 NIS 指令，实施网络安全认证计划，加强对个人隐私和通信机密的保护。

在数据层方面，GDPR 在《1995 年个人数据保护指令》的基础上增设了一系列的数据主体权利，同时也大幅度强化了数据控制者的义务。GDPR 具有在欧盟成员国直接适用的法律效力，且高于成员国的国内法，促进了欧盟范围内个人数据保护立法的统一；GDPR 还将适用范围扩展至了“未在欧盟境内设立营业地，但向欧盟提供商品或服务”的机构。其构建了个人信息跨境提供制度框架，规定了允许个人数据转移的两种场景和八种例外情况。GDPR 的目标是统一和协调欧盟范围内所有数据隐私法，为数据保护设定高标准，并对不遵守规定的人处以高额罚款。一方面，GDPR 强化了用户的个人数据权利，要求数据主体在知情的情况下自愿做出授权，同时明确了用户被遗忘权、删除权等权利的具体含义；另一方面，GDPR 明确了相关主体的责任机制，首次设立数据保护专员制度，明确了数据泄密事件发生时，相关主体应尽快通知数据主体并上报监管机构，监管机构可对违法者处以最高达总营业额的 4% 的罚款。概言之，GDPR 从个人信息权利、数据收集和处理原则、监管机制和责任处罚等方面对个人数据提供了全面保护机制。

（三）全球视野下的中国网络空间治理

中国网络空间治理体系是由网络安全及数据安全相关的法律、行政法规和部门规章等多层次规范所构筑的治理架构，涵盖网络主权维护、关键信息基础设施保护、网络运行安全、网络监测预警与应急处置、网络安全审查、网络数据安全以及网络空

间各行为主体权益保护等制度。

第一，在法律体系构成方面，中国网络空间治理法律体系分为法律、行政法规、部门规章三层次，与欧盟相类似，中国网络空间治理架构也包括战略和多层次立法体系，但有别于欧盟的是，中国网络空间治理体系架构中，立法构成了相对于战略更为主要的部分。此前中国网络空间治理领域的规范文件大都集中在规章和行政文件上，法律层面的立法较少，整体而言，立法主体多元和立法层级较低。美国网络空间治理体系则分为法律和法规两个层次。美国对网络空间治理的具体政策指令来自美国历届总统颁布的总统令，管理实践中坚持以国家安全战略报告为指导思想。从宏观层面看，中国网络空间治理法律体系具有与其他国家所不同的法律层次，以美国为例，美国关于网络安全的规范主要由具有较高效力等级的法律构成，而我国则以专项立法和行业立法为基础，相关规范指引为补充，但随着《网安法》《数安法》《个信法》和《电子签名法》等法律的颁布及执行，我国的法律体系基础将更为扎实。

第二，在治理理念方面，中国网络空间治理以保护人格权益为基本价值，注重政府治理。美国宣称信息自由为网络空间治理的首要原则，强调信息公开的优先性；其次，中国既往的网络空间治理侧重事后纠正，针对既有问题制定规章，美国则强调事前预防，随着网络空间治理的法律体系逐步搭建完成，中国网络空间的治理将有望建立事前、事中和事后的治理框架。从平衡网络安全与经济发展的角度来看，欧盟注重在切实保护并提高网络安全的同时，避免给互联网企业发展带来过分负担，例如NIS 指令明确了适用主体以及豁免主体，如前所述，NIS 指令明确规定只针对基础服务运营者和部分数字服务提供者（包括网络交易市场、搜索引擎以及云计算）提出相关义务性要求，而豁免小微企业以及前述类型之外的数字服务提供者，中国网络空间治理体系中则暂未明确提出此类豁免。

其三，在中央治理机构方面，之前中国网络空间治理的职能较为分散，未采用统一的协调机构进行网络空间治理，但随着中央网络安全和信息化委员会的成立，中国将建立网络空间治理的中央统一协调机制，在中央网络安全和信息化委员会领导下，国家网信部门发挥统筹协调职能，不断强化网络空间治理工作的顶层设计、总体布局、统筹协调、整体推进、督促落实。国务院公安部门加强对网络安全保护工作的指导监督，国务院电信主管部门和其他有关部门根据法律法规各司其职。对于政府各个部门而言，美国于 1996 年通过的《信息技术管理改革法修正案》中确立了首席信息官制度（CIO），联邦政府的各部门都设有 CIO，CIO 的核心职能是为本部门开发、维护一个稳妥的、整体的信息化架构。值得注意的是，近年来，中国许多省市相继成立或组建政府大数据局或政府大数据发展管理局等类似机构，显示出中国网络空间治理方式与相应组织运行体系的变化，其中蕴含的是中国政府数据管理从单一化行业管理迈向整体化功能管理，并通过配套工作机制加以落实，具有鲜明的制度价值。此外，根据近日各地相继发布的《广州市推行首席数据官制度试点实施方案》《深圳市推行首席数据官制度试点实施方案》《佛山市首席数据官制度试点工作实施方案》等首席数据官制度方案，其中，广州首席数据官职责主要侧重于数据要素配置流通和数据资源共享开放、开发利用等数据治理工作；深圳首席数据官职责为推进智慧城市和数字政府建设、完善数据标准化管理、推进数据融合创新应用等。通过首席数据官制度，将助力政府“数据孤岛”问题的解决，最大程度发挥数据价值。

第四，在治理模式方面，中国在网络空间治理中主要采取政府主导和行业自律相结合的方式。首先，政府主导强调政府的作用贯穿网络监管的全过程，具体包括事前资质审查及监管，事中依法依规监管，事后整改或取缔。对于互联网服务平台在运营过程中的违法行为，相关执法部门将视乎情节轻重程度予以限期整改或依法取缔。其次，行业自律则基于网络空间治理相关立法有时滞后于网络技术及实践发展。由于网络社会的快速发展，网络空间的技术革新速度使得政府难以及时预测和规范网络社会的未来发展。因此，中国政府鼓励互联网行业自律，以此避免国家对网络领域的过度管控。美国采用的则是由联邦通信委员会（FCC）专门管理，法律、技术、道德三方面共同推进的治理模式。

第五，在治理程度方面，以数据层面为例，中国新出台的《个信法》的严厉程度实际已基本与欧盟 GDPR 相当，美国最具代表性的隐私法案 CCPA 相较则更为宽松。在适用地域范围上，《个信法》相对欧盟和美国的类似立法显现出了克制的立场。

具体来看，欧盟 GDPR 采取机构成立地标准（境内）与目标指向标准（境外）；中国《个信法》采取信息处理活动发生地标准（境内）和目标指向标准（境外）；美国加州 CCPA&《加州隐私权与执法法案》（CPRA）最有限，仅针对在加州进行的商业活动。在排除适用的范围上，CCPA&CPRA 排除范围最广，GDPR 次之，《个信法》最有限。具体来看，CCPA&CPRA 的排除适用范围为：所有要素都完全发生在加州以外的商业活动；履行法定义务的数据处理；医疗、征信、驾驶、金融、政府公开信息、雇员信息、车辆信息以及财产所有权信息；GDPR 的排除适用范围为：欧盟管辖之外的数据处理活动；欧盟成员国因为履行《欧盟基本条约》第二章第五款所规定的活动而进行的个人数据处理；自然人在纯粹个人或家庭活动中所进行的个人数据处理；刑事犯罪和公共安全相关的个人数据处理；而《个信法》的排除范围仅包括：自然人因个人或者家庭事务处理个人信息；法律对各级人民政府及其有关部门组织实施的统计、档案活动中的个人信息处理另有规定的。此外，在规制的数据活动方面，《个信法》和 GDPR 调整范围更宽泛，CCPA&CPRA 更为限缩。而在受规制的对象类型、信息主体的反对权、删除权、发生数据安全事件时的通知义务等方面，GDPR 最严格，《个信法》次之，CCPA&CPRA 最宽松。[11]

当然，在某些重点问题上，中国仍存在立法尚待完善之处。例如在数据跨境流动方面，现行法律中虽已确立关键信息基础设施中个人信息和重要数据境内存储的相关要求，但有关数据跨境流动的法律体系尚未健全，现有规定仍较为简单，《网安法》中的相关要求还需要配套规定进一步细化，韩国在此方面建立的相关制度可作为立法经验进行参考，如区分不同数据类型，并在此之上明确相应数据跨境流动要求以及例外规定。

总体而言，中国网络空间治理在治理思路、规制主体、责任机制等方面与上文分析的主要国家和地区具有相似之处，但治理机构、治理模式、治理程度、具体规制等仍存在差异，中国网络空间治理尚有许多领域有待具体规范出台。伴随整体制度框架纵深化发展，中国网络空间治理将承接《网安法》《数安法》《个信法》等法律规范继续向前迈进。

三、我国网络空间治理领域核心立法概览及企业合规启示

基于以上，我们在下附表格内简要总结目前我国网络空间治理三大核心法律《网安法》《数安法》以及《个信法》的重点内容并为企业在我国网络空间治理领域下的合规义务进行提示与说明。

	《网络安全法》	《数据安全法》	《个人信息保护法》
规制对象	网络运营者（及关键信息基础设施运营者）	开展数据处理活动的组织、个人	个人信息处理者和接受委托处理个人信息的受托人 个人信息处理者：在个人信息处理活动中自主决定处理目的、处理方式的组织、个人

[11] 相关对比研究详见 腾讯研究院 王融、易泓清：《中美欧个人信息保护法比较》，https://mp.weixin.qq.com/s/UhFcT1W9O9LKU2JJofToZw，最后访问日期：2021 年 8 月 22 日。

	《网络安全法》	《数据安全法》	《个人信息保护法》
适用范围	在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理	1）在中华人民共和国境内开展数据处理活动及其安全监管； 2）在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的	1）在中华人民共和国境内处理自然人个人信息的活动； 2）在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法： （一）以向境内自然人提供产品或者服务为目的； （二）分析、评估境内自然人的行为； （三）法律、行政法规规定的其他情形
重点内容概述	**（一）概览**		
	网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置等	数据安全治理与数据开发利用：数据安全标准体系建设、数据安全检测评估和认证服务、数据交易管理、数据分类分级保护、重要数据目录清单和管理、数据安全风险预警机制及应急处置机制、数据国家安全审查等	个人信息的保护，包括个人信息范围的界定、个人信息处理基本原则、个人信息跨境流动规则、个人信息主体权利及保护等
	（二）网络层		
	1） 网络运行安全： 网络安全等级保护； 网络关键设备和安全专用产品认证检测； 网络安全事件应急预案 **2）关键信息基础设施运行安全：** 建设安全、运营者安全保护义务、采购安全（国家安全审查与安全保密义务）、数据存储与对外提供、安全检测评估	1）利用互联网等信息网络开展数据处理活动，应当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； 2）关键信息基础设施运营者重要数据出境安全管理； 3）电子政务系统建设维护批准制度	关键信息基础设施运营者个人信息出境安全管理

	《网络安全法》	《数据安全法》	《个人信息保护法》
重点内容概述	（三）软件 / 应用层		
	网络安全产品与服务安全； 网络用户身份管理	数据交易管理； 数据处理相关服务之行政许可	1）应用程序等个人信息保护情况测评； 2）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用之专门的个人信息保护规则、标准； 3）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的个人信息保护义务； 4）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设； 5）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务
	（四）数据层		
	个人信息保护：从网络信息安全的角度出发	重要数据保护：分级分类管理、定期开展风险评估并报送评估报告； 国家核心数据保护； 数据安全应急处置； 国家数据安全审查； 数据出口管制	个人信息（包括敏感个人信息）保护

由此，在三法下，企业往往具备网络运营者、数据处理者以及个人信息处理者的多重身份，在数据处理活动过程中，企业应当根据其数据处理身份识别、厘清并履行所适用的法律义务，建立完善业务开展以及内部数据管理过程中所涉及的网络安全、数据安全以及个人信息保护三大方面的合规举措，包括但不限于：网络系统等级保护测评与认证、数据及网络安全事件响应、数据全生命周期管理、个人信息与重要数据出境安全评估机制等。

在我国日益完善的网络空间治理的法律框架下，如何有效平衡正当商业需求与新法带来的合规要求，提前进行有关合规工作，进行必要的业务调整，将成为企业无法回避的一个问题。

感谢实习生刘婉蓉、王璐瑶对本文的贡献。

数中有术、术中有数——数据权益理论与司法实践探析

宁宣凤　刘迎　吴涵　姚敏侣

前言

数据在当前时代的重要性无须赘述，其不仅是数字经济时代的生产要素，也关系到国家安全，甚至是人类迈向智能时代的基础。但由于数据本身可复制性、创造速度、历史性等不同的特征，对比传统资产而言，数据基于怎样的前提能被定义为数据资产，以及是否应当创设新的社会和法律规制来定义和保护数据资产一直是学术界和实务界试图解开的难题。**定义数据资产首要的任务是明确不同主体对于数据的权益边界，具体而言如何区分和界定“个人、企业及社会组织、国家、全人类”群体对于数据的权益将关系到公民权利、企业竞争、国家竞争和全人类福祉等多个方面。**

中共中央国务院在2020年5月发布的《关于新时代加快完善社会主义市场经济体制的意见》中明确指出，要加快培育发展数据要素市场，完善数据权益界定、开放共享、交易流通等标准和措施，是站在时代新高度上对于数据/数据权益重要性的总结。其他国家尽管没有明确指明数据权益的基础作用，但都不约而同地部署数据战略，可以预见国家之间对于数据权益的竞争无疑也将愈演愈烈。比如美国发布《联邦数据战略与2020年行动计划》[1]，聚焦于联邦层面的数据管理、共享治理以及战略愿景；欧盟发布了包括《欧洲数据战略》在内的一系列关于“塑造欧洲数字化未来”的战略规划，涵盖了数据利用、人工智能、平台治理等领域的发展和立法框架，始终努力向“单一数字市场”稳步迈进[2]。

与各国数据战略保持齐头并进、一路迅猛发展的是基于数据驱动的新兴科技产业。据国际数据公司（IDC）数据预测，预计到2025年，全球数据量将比2016年的16.1ZB增加十倍，达到163ZB。然而，成熟的行业市场有赖于清晰、明确和稳定的权益架构和交易规则，但纵观国内外现有法律规范，总体而言在数据权益问题上还少见有明确规定，理论界关于数据权益主张的边界与利益平衡关系处在充分的观点表达与论证阶段。

在前述背景下，本文拟通过对国内外数据权益理论和判例实践进行梳理，尝试对“个人-

[1]Office of Management and Budget (OMB):federal data strategy 2020 action plan, https://strategy.data.gov/action-plan/ 最后访问日期: 2021年7月28日。
[2]腾讯研究院 朱开鑫:《<欧洲数据战略>解读：距离单一数据市场还有多远？》，https://www.tisi.org/14048，最后访问日期：2021年7月28日。

企业”以及“企业 - 企业”两类常见的数据争议关系探析，以期指引企业数据资产管理实践。

一、数据权益的现有法律规则

（一）国际立法规则整理

从目前范围内的数据法律来看，在各国纷纷推进展开数据立法进程，在已有接近 1/3 个国家通过数据保护专门法律的现实情况下，对于数据确权、数据的财产属性和归属，在法律条文上体现得可能并不充分。归总而言，在现有的数据立法框架内，存在以下几种立法规则的特征：

首先，各国个人数据立法保护趋势加强，但实则尚未确立个人数据主体的所有权规则。从素有全球个人信息保护立法样板之称的欧盟《通用数据保护条例》（General Data Protection Regulation, GDPR）来说，法律规则朝着强化数据主体权利、确保对个人数据使用控制的方向发展。GDPR 在进一步确认和完善个人的既有权利的基础上，通过第 17 条增加了清除权（被遗忘权），通过第 20 条增加了持续控制权（可携带权）等，以实现数据主体对其个人数据的更有效控制。但即便如此，条文本身未见对于其个人数据的所有权和财产权益分配在法律规则上的安排。换句话说，即便对个人数据的控制权不断强化，但这不等同于对个人数据的所有权，GDPR 也没有赋予数据主体对数据的完全的所有权 [3]。

其次，就鼓励企业数据流通和数据产业发展的立法规则而言，各国立法仍然在不断探索个人和企业之间就个人数据的权益分配和主张的可能空间。以美国为例，一旦涉及数据权益纠纷，通常采用的做法是，援引现有判例法中关于隐私侵权的规定来处理互联网上用户个人信息的规范定位和法律问题，借此保护用户个人信息和规范数据经营者的行为界限，同时也会根据市场对数据流动与实际需要进行一定变通，更加务实地调整用户与数据经营者之间基于个人信息产生的利益关系，从容在数据保护与利用之间达到再平衡 [4]。日本《个人信息保护法》对个人数据的保护并不是通过为个人数据增设“所有权”等法定权利赋予个人对数据的拥有权或控制权，而是新设“匿名加工信息”制度，兼顾保护与开发利用、投资激励之间的平衡关系 [5]。

（二）国内立法脉络梳理

1. 《民法典》定义的个人信息性质

相较于欧洲、美国等国家地区将个人数据保护作为基本人权的内容，或通过隐私体制对个人信息主体的权益予以保障，《民法典》并未明确个人信息的定位。虽然个人信息保护条款本身并未对“个人信息”是否构成法律意义下的民事权利进行明确，但从条款编排来看，无论是此前的《民法总则》还是当下的《民法典》，均将其置于“民事权利”章节之下，这一编排一定程度上反映了立法者从民事权利视角对个人信息保护进行法律定位的意图。

此外将个人信息保护纳入《民法典》人格权编，尽管尚未具化为独立权利的“人格权益”受到保护，但已经为产业释放了重大信号，即个人信息的人格权属性得到立法肯定。

2. 数据安全法明确原则

新颁布的《数据安全法》作为数据领域的基本法，对数据权益问题进行了原则性规定：“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。”

3. 地方政策及立法摸索前行

在国家培育数据要素市场的方针指引下，各地对数据立法的探索不断深入，地方性数据立法接踵而至。依托贵阳大数据交易所，贵州率先于 2016 年推出了全国首部关于数据开发应用的地方性法规《贵州省大数据发展应用促进条例》，受限于地方立法权及条例制定时的数据经济发展阶段，该条例仅规定“采集数据不得损害被采集人的合法权益”，

[3] Nestor Duch-Brown, Bertin Martens, Frank Mueller-Langer, The Economics of Ownership, Access and Trade in Digital Data, p.17 (European Comm'n JRC Digital Economy Working Paper 2017-01)，https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf，最后访问时间：2021 年 7 月 28 日。
[4] 刘新宇：《大数据时代数据权属分析及其体系构建》，载《上海大学学报（社会科学版）》，2019 年第 6 期。
[5] 李慧敏，王忠，《日本对个人数据权属的处理方式及其启示》，载《科技与法律》2019 年底 4 期。

并未直接触及数据权益问题。天津市在 2020 年发布的《天津市数据交易管理暂行办法（征求意见稿）》中已经意识到数据确权对数据交易的重要性，并明确规定“数据供方应确保交易数据获取渠道合法、权利清晰无争议，能够向数据交易服务机构提供拥有交易数据完整相关权益的承诺声明及交易数据采集渠道、个人信息保护政策、用户授权等证明材料。”但是该征求意见稿也未能触及数据确权的核心问题。

深圳走得更远，也获得了中央的强有力支持。中共中央办公厅、国务院办公厅印发了《深圳建设中国特色社会主义先行示范区综合改革试点实施方案（2020 — 2025 年）》，支持深圳率先“完善数据产权制度，探索数据产权保护和利用新机制，建立数据隐私保护制度。试点推进政府数据开放共享。支持建设粤港澳大湾区数据平台，研究论证设立数据交易市场或依托现有交易场所开展数据交易。开展数据生产要素统计核算试点。”

深圳曾在《深圳经济特区数据条例》征求意见稿中尝试定义数据权，并以此分类，即“自然人对个人数据依法享有数据权；公共数据属于新型国有资产，其数据权归国家所有；要素市场主体也有数据权，任何组织和个人不得侵犯。”尽管该分类和权益归属最终未被确立，但 2021 年 7 月 6 日正式通过的《深圳经济特区数据条例》中依然明确了“自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益。”

4. 行业规范百花齐放

除法律法规外，我国还存在众多数据交易的行业自律性规范，例如贵州大数据交易所推出的《贵阳大数据交易所 702 公约》、中国信息通信研究院等联合发布的《数据流通行业自律公约（2.0）版本》、上海数据交易中心发布的《数据互联规则》等等，也对数据交易、数据权益等问题或有涉及，但是这些行业自律性规范并不具有法律效力，缺乏可执行性。

由于数据具有无形性和非排他性的特征，区别于传统民法意义上的“物”，且数据流转过程中会涉及多方主体，数据权益不明晰将会影响数据交易规则的确定，导致数据纠纷频发，有碍数据要素市场高效、健康发展。数据权益是当前亟待研究和立法解决的问题，其规则构建应当审慎。

二、数据权益的主要理念和理论

（一）国外数据确权与数据权益观点概览

对自始以来秉持开放互联网倾向的美国来说，实现数据确权无疑存在客观阻碍。如美国教授奥林·科尔 (Orin Kerr) 认为：“互联网的一般原则是开放性，这种开放性允许世界上任何人发布信息或数据。”[6] 简单来说，数据权益纷争和阻碍来源于数据共享流通的经济价值。此外，美国还有将“数据视作言论”的理论观点，以宪法保护和自由流通的价值。在欧洲大陆，个人数据一贯被视作数据主体的人格权的一部分而作为数据主体的基本人权来加以保护，但劳伦斯·莱斯格 (Lawrence Lessig) 教授也尝试提出“数据财产化理论”，主张应该认识到数据的财产属性，通过赋予数据以财产权的方式，来强化数据本身经济驱动功能，以打破传统法律思维之下依据单纯隐私或信息绝对化过度保护用户而限制、阻碍数据收集、流通等活动的僵化格局[7]。与此相类似，著名隐私学者波斯纳认为，隐私权应被视为财产权法的分支，信息主体对他们的信息拥有产权[8]。

但诚如 Richard Hill 教授所言，数据可以自由流动并不能逻辑地推出数据是商品。“数据本身不是财产价值之源，而是依赖一个庞大的工具和行为系统才能产生经济价值。”[9] 从本质上来看，可以借鉴法经济学上经典的“卡·梅框架”来理解数据权益理论之争的根本矛盾：如果简单通过财产规则确定数据归属主体，便带来了交易成本的无限扩大，这与数据经济发展规律是背道而驰的；而如果采取责任规则，即“只要付出相应的补偿，即使没有信息主体的同意，平台也可以占有信息和数据”[10] 的

[6] 丁晓东，《数据到底属于谁？——从网络爬虫看平台数据权属与数据保护》，载《华东政法大学学报》2019 年第 5 期。
[7] 龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年 7 月第 4 期。
[8] 杨立新，陶盈：《公民个人电子信息保护的法理基础》，载《法律适用》2013 年第 8 期。
[9] 梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期。
[10] 帕特里克·博尔顿：“同意”按钮真的能保护个人隐私吗？ https://www.luohanacademy.com/cn/insights/38a8466eb62c844a，最后访问日期：2021 年 7 月 28 日。

规则，对于隐私、人格等权益的保护自然是无法周全顾及的。两难的境地导致数据权益理论的发展，向数据权益主张边界的探讨方向发展。

（二）国内数据权益理论发展与共识

随着《数据安全法》的正式出台与《个人信息保护法（草案）》的多次修订，为了呼应数据产学研各界的切实需求，数据权益的多种保护路径与主张观点实则在理论上获得了深入和长足的研讨。虽然仍存在许多开放性讨论的空间，但其中不少合理观点经反复商榷后已被提炼并逐渐成为可以被人们接纳的“共识”。我们充分理解，“数据的多重属性和复杂权利义务关系使得难以笼统地对数据作出权属上的单一安排”“数据权益问题的界定并不排斥对个人数据保护的合规遵从”[11]，但毋庸置疑的是，此前多种解释路径下构建企业数据权益保护框架的理论尝试，将起到多维度保护企业数据资产和发展利益的积极效应。

1. 基础的数据分类方法

数据依其不同属性、特征可以划分不同种类，讨论数据权益不能对数据一概而论。廓清数据类别将有助于我们对数据权益问题的认识和理解。根据不同维度，从公权力与私权利划分的角度来看，关于数据权存在国家层面的“数据主权”与“数据权利”的划分；从数据持有主体的分类来看，可以将数据划分为个人数据、企业数据及公共数据；从数据来源分类角度来看，还可以将数据分为“原始数据”和“衍生数据”[12]。从“个人 - 企业”二元论角度来说，这是一对讨论数据权益问题时所无法规避的矛盾，也即需要各界付出努力寻找和论证“权益边界”所在的地方。用户对原始数据享有权利，企业因对衍生数据的形成投入了物力、财力因而可以对衍生数据享有财产性权益。

2. 可能的数据权益主张路径

从数据生命周期来看，由于数据生产使用存在诸多参与者，特别是在作为数据原发者的用户和数据处理者的企业之间，如何设定不同的权益，并依据何种逻辑在这些数据形成的参与者之间分配权益，成为当下数据权益体系构建的焦点和难点。结合众多的学界理论和商业实践，一般认为数据权益的财产属性方面，在目前的法律框架下可能至少包括以下三种可能路径：数据用益权、数据竞争性权益和数据知识产权。

（1）数据用益物权

国内有学者为了解决数据流动与共享需求，同时应对物权法定的固有困境，借助上述数据基础分类的方法，提出了“数据用益权”的解释思路，即根据不同主体对数据形成的贡献来源和程度的不同，应当设定数据原发者拥有数据所有权与数据处理者拥有数据用益权的二元权利结构，以实现数据财产权益分配的均衡。数据用益权既可以基于数据所有权人授权和数据采集、加工等事实行为取得，也可以通过共享、交易等方式继受取得。数据需要依托具有公信力的公共数据平台、数据中间商进行交易与共享[13]。引入数据用益权概念，有助于实现用户和企业之间的权限分配、调和不同数据企业之间的利益冲突，从而为数字经济的发展搭建清晰的利益分配框架。更重要的是，目前国内外均已出现数据交易市场和共享平台，为促进数据权益的通畅流转，并确保各方的交易安全，构建数据用益权以及相关的配套制度就变得更为必要。

（2）数据竞争性财产权益

从交易成本理论、劳动财产权理论以及激励理论的角度，数据收集企业对于收集的数据集，数据增值企业对于增值数据，应该享有一定的财产性权益。在业界和司法实践认定中，该观点可以说得到了较大范围内的认同（以下详述）。一般认为，企业可以通过对原始数据进行整合、算法过滤、匿名化处理等一系列加工、处理行为，可以主张其对增值数据具有《反不正当竞争法》下的、对第三方的排他竞争性权益。

（3）满足特定条件下的数据知识产权

由于竞争法特有的事后救济属性或者说固有特

[11] 腾讯研究院 王融，易泓清：《数据权属大讨论中的共识凝聚》，https://www.tisi.org/18958，最后访问日期：2021 年 7 月 28 日。
[12] 参见王渊、黄道丽、杨松儒：《数据权的权利性质及其归属研究》，载《科学管理研究》，2017 年 10 月第 35 卷第 5 期；高完成：《数据确权与交易规则研究》，载《西安交通大学学报（社会科学版）》，2018 年第 3 期。
[13] 申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期。

点，无法满足人们构建实现事前保护的数据权益主张框架需求。因为我国《反不正当竞争法》适用的局限性，知识产权保护制度仍是目前企业建立数据产权的主要途径。实践中，企业通常利用多项知识产权对数据进行保护。例如，对于数据的编排和选择，企业可以主张著作权下的权益；对于数据本身，企业可以主张商业秘密下的权益。但不可避免的是，因为既有的知识产权制度并不完全匹配、贴合企业保护数据的需求，使用知识产权的法律体系保护企业数据仍然存在着一定的局限性。

三、数据权益的司法实践反映

（一）国内外数据权益相关案例梳理

早在 2011 年北京市第一中级人民法院审理的（2011）一中民终字第 7512 号中，因被告网站长期大量复制原告平台的用户评论，法院在判决中认为原告通过商业运作吸引用户在原告网站上注册、点击、评论，并有效地收集和整理信息，进而获得更大的商业利润，该合法权益应受法律保护。但是该判决仅仅点到为止的表示企业对平台上用户信息享有的合法权益应受法律保护，没有进一步明确企业对此享有何种权益。

随着大数据交易产业的发展，2016 年后企业间因数据引发的纠纷高涨。我们对 2016 年后涉及数据权益判断的典型法院裁决和观点进行了以下梳理：

案号	管辖法院、裁决时间	判决主文中法院关于企业数据权益的认定逻辑	法院观点小结
（2016）京 73 民终 588 号	北京知识产权法院 2016 年 12 月 30 日	原告在多年经营活动中，已经积累了数以亿计的用户……这些用户信息不仅是支撑原告作为庞大社交媒体平台开展经营活动的基础，也是其向不同第三方应用软件提供平台资源的重要内容。规范、有序、安全地使用这些用户信息，是原告维持并提升用户活跃度、开展正常经营活动、保持竞争优势的必要条件。本案中，被告的行为……损害了原告的合法竞争利益。	原告的用户信息是其多年积累的结果，是其开展正常经营活动等的必要条件，原告对其用户信息享有合法竞争利益。
（2016）沪 73 民终 242 号	上海知识产权法院 2017 年 8 月 30 日	原告用户评论信息是原告付出大量资源所获取的，且具有很高的经济价值，这些信息是原告的劳动成果。被告未经原告的许可，在其产品中进行大量使用，这种行为本质上属于未经许可使用他人劳动成果……原告对涉案信息的获取付出了巨大的劳动，具有可获得法律保护的权益。	因原告付出大量资源获取平台用户评论信息，这些信息属于原告的劳动成果，虽然不属于法定权利，但原告对此享有可获得法律保护的权益。
（2018）浙 01 民终 7312 号	浙江省杭州市中级人民法院 2018 年 12 月 18 日	随着网络大数据产品市场价值的日益凸显，网络大数据产品自身已成为市场交易的对象，已实质性具备了商品的交换价值。对于网络运营者而言，网络大数据产品已成为其拥有的一项重要的财产权益。……本案中，原告数据产品中的数据内容系原告付出了人力、物力、财力，经过长期经营积累而形成，……该数据产品系原告的劳动成果，其所带来的权益，应当归原告所享有。	因原告对数据产品付出了人力、物力、财力，经过长期经营积累而形成，故原告对数据产品享有竞争性财产权益，但基于“物权法定”原则，原告对数据产品不享有财产所有权。

案号	管辖法院、裁决时间	判决主文中法院关于企业数据权益的认定逻辑	法院观点小结
（2018）苏 0684 民初 5030 号	江苏省海门市人民法院 2019 年 1 月 17 日	三被告的行为是否构成侵权主要在于原告有否民事权利受到实际损害。……本案中，原告平台上的销量、评价等数据经过长期交易积累而形成，信用评价体系系原告核心竞争利益。……三被告以敲诈为目的对商家进行恶意差评，客观造成原告平台上相关数据的不真实，直接影响并破坏了其构建的信用评价体系，亦即损害了原告合法的民事权益。	原告对其平台上经过长期交易积累而形成的评价性数据享有民事权益。
（2018）浙 8601 民初 956 号	杭州铁路运输法院 2019 年 10 月 31 日	涉案经销商数据库不仅是原告的竞争力，也是生产力。…会员账号及密码使用权虽然归属用户，但账号对应的经销商数据库的财产性权益应当属于平台，且涉案经销商数据库中数据内容虽然来源于意向加盟商，但经过原告的深度开发已不同于普通的客户信息…凝结了原告人力和劳力付出…原告诉称其对涉案经销商数据库共同享有竞争性财产权益的诉讼主张，本院予以支持。	涉案数据库为原告核心竞争力，且经过原告深度开发，原告对涉案数据库享有竞争性财产权益。
（2019）浙 8601 民初 1987 号	杭州铁路运输法院 2020 年 6 月 2 日	原告产品数据资源的积累已成为两原告获取市场收益的基本商业模式及核心竞争力。原告产品数据资源系两原告投入了大量人力、物力、经过合法经营而形成的，该数据资源能够给两原告带来商业利益与竞争优势，两原告对于产品数据资源应当享有竞争权益。	原公司因对产品数据资源投入了大量人力、物力等，因而对此数据资源享有竞争权益。
（2017）京 0108 民初 24512 号	北京市海淀区人民法院 2020 年 7 月 20 日	结合涉案数据系原告产品的重要基础，原告为运营平台，维护涉案数据安全付出了相应成本，原告对涉案数据进行衍生性利用或开发，以及服务使用协议中关于涉案数据归属的约定等因素，原告可基于其对涉案数据享有的经营利益，依据反不正当竞争法对被告擅自抓取并使用涉案数据的行为提出相应主张。	因原告对产品数据付出了相应成本，原告对这些数据享有经营利益，可受到反不正当竞争法的保护。
（2020）湘 0104 民初 10602 号	湖南省长沙市岳麓区人民法院 2020 年 10 月 29 日	被告辩称原告的数据信息属于公开的市场价格信息，取得方式和发布形式没有独创性，也不具有权威性，原告对其数据信息不享有法定权利。因原告通过人力物力对全国多个城市相关钢材价格信息进行汇编，其成果具有一定的独创性，且在互联网上以数字表格的形式固定，以会员方式对相关人员进行发布，故原告享有汇编作品所有权，应依法予以保护。	原告付出人力、物力对公开的钢材价格信息进行汇编，具有独创性，构成汇编作品，受到知识产权法保护。

案号	管辖法院、裁决时间	判决主文中法院关于企业数据权益的认定逻辑	法院观点小结
（2019）京 73 民终 1270 号	北京知识产权法院 2020 年 12 月 3 日	被告未经许可使用原告的涉案导航电子地图，必然会使用该导航电子地图中的地理信息数据。由于该地理信息数据系原告耗费巨大的人力、物力、财力，经过复杂的情报收集、数据采集、数据制作、数据质检等过程形成，且导航电子地图的编制活动，只能由依法取得导航电子地图测绘资质的单位实施，故涉案导航电子地图数据，具有较高的经济价值，成为原告的无形资产和核心竞争力，原告通过合法途径获取的数据应当受到法律保护，通过该数据获取的利益属于合法权益，任何自然人、法人和非法人组织无权通过不正当手段攫取。	原告耗费巨大的人力、物力等资源收集、采集的地理信息数据属于受法律保护的合法权益。但该案中相关数据信息已经被认定构成地图作品受到著作权法保护，因此法院未再予以不正当竞争法保护。

与此同时，我们摘取了美欧法院就企业间数据权益纠纷中部分具有代表性的判例和说理，具体如下：

判例索引编号	判例简要情况	主要裁判观点
100 F. Supp. 2d 1058 (N.D. Cal., May 24, 2000)	被告对原告网站利用爬虫进行了数据爬取，原告因此向加利福尼亚北区法院提起诉讼，理由包括：该爬虫行为违反了 robot 协议，具有非法侵入（trespass）、计算机欺诈和滥用、不公平竞争等违法行为。	在这一案件中，法院回避了数据权利归属的问题。主要以服务器私有这一理由认定了被告的行为属于非法入侵动产，间接承认了爬取公开数据需要平台授权的竞争性原则。
938 F.3d 985 (9th Cir. 2019)	被告是知名在线职场社交平台，原告是一家数据分析公司，收集被告平台上公开信息，在进行数据分析后销售给其他公司。被告曾作为合作伙伴多次派员工参加原告内部会议，知晓原告抓取平台信息也十分了解原告的商业模式。当被告决定利用自身平台优势开发与原告类似的数据分析产品之后，向原告发送律师函并屏蔽了原告的访问。原告向法院提出临时禁令，要求被告收回律师函、移除屏蔽原告访问的技术措施。	法院认为数据并不仅仅是平台所有，同时还需要考虑公共利益，若被抓取的数据具有公共开放性，属于网络空间的公共产品，那就无须数据控制者的授权。第三方网络平台对公开数据的抓取下载可以被视为经过了默示授权。 *但根据该案的最新进展，根据公开消息，该案被美国最高法院发回重审*[14]*，这意味着此前发出的禁止被告禁止原告爬取数据的禁令将受到司法挑战，该案的最终走向仍存在不确定性。*

[14]https://www.supremecourt.gov/orders/courtorders/061421zor_6j36.pdf 最后访问日期：2021 年 7 月 28 日。

判例索引编号	判例简要情况	主要裁判观点
C 08-5780 JF (RS), October 22, 2009	被告运营 power.com 网站，是一家账户聚合类平台。被告以现金鼓励方式邀请注册用户参与网站推广计划，对参与推广的用户，在用户知晓的情况下，被告操作用户账户，向该用户好友同时以站内信、站外信的方式发送邀请，信件落款会写上“Thanks, The Facebook Team”。原告注意到被告的推广行为之后，向被告发送了律师函，要求其加入原告官方的开发者计划，遭到拒绝。原告随后屏蔽了被告的 IP 地址，被告却在更换 IP 地址后继续进行推广计划，继续抓取、复制和使用平台数据。	法院认为，被告仅有用户授权是不够的，还应当获得原告的授权才可以抓取用户好友数据和其他平台数据，法院最终认定被告在收到原告律师函后（视为对其抓取行为的明确拒绝）的数据抓取行为违反了美国《计算机欺诈和滥用法》（Computer Fraud and Abuse Act，CFAA）。简言之，法院倾向于认为，以账号密码方式保护的用户数据被明确认定为不属于公开数据，而非公开数据需遵守“用户 + 平台”双重授权规则。
C-30/14，(15 January 2015)	被告作为机票比价服务提供者，使用自动系统直接从原告航空网站和可公开访问数据库来撷取航班信息，然后由收费用户支付佣金从其网站上进行预定。不过，原告网站的访问者都必须通过勾选来接受原告的一般条款和条件。除非第三方直接与原告签署了书面许可协议，网站信息均只能用于私人和非商业目的，且禁止使用自动化系统或软件从网站提取数据用于商业目的。原告声称，被告侵犯了著作权法和数据库的特殊权利，并且违反了被告所接受的网站使用条款和条件。	欧盟法院认为，原告公司网站提供的航班数据，尚不能受到著作权法或数据库权的保护，并进一步肯定当网站经营者就其本身数据内容，无法透过著作权排除他人未经授权使用时，仍得以服务条款限制其他企业以撷取方式自动抓取、收取网站资料的行为。2015 年 1 月，法院最终裁定原告公司有权禁止被告以自动化系统抓取网站数据后转为商业使用。

（二）典型案例所映射的数据权益理论观点

首先，**由于在立法上缺乏数据权益归属认定的法律规定，司法实践尽量避免就财产归属作出直接认定。**上述案例中，（2018）浙 01 民终 7312 号被称为国内第一起数据产品权益纠纷，对于原告主张其对“生意参谋”数据产品享有财产所有权的诉讼主张，一审法院认为财产所有权作为一项绝对权利，如果赋予网络运营者享有网络大数据产品财产所有权，则意味不特定多数人将因此承担相应的义务。是否赋予网络运营者享有网络大数据产品财产所有权，事关民事法律制度的确定，限于我国法律目前对于数据产品的权利保护尚未作出具体规定，基于“物权法定”原则，故对原告该项诉讼主张，一审法院不予确认。相类似地，美国法院在 100 F. Supp. 2d 1058(N.D. Cal., May 24, 2000) 一案裁判说理中，也避开了对数据财产权归属的直接认定，并且同样以认定行为侵犯原告竞争性的合法利益作为主要的裁判理由论述。

其次，**对于数据是否受到知识产权法的保护，国内外法院将进行一轮法律适用性审查，审查范围与标准将依据当地的知识产权法传统与主流裁判规则确定。**例如，在上述（2020）湘 0104 民初 10602 号案和（2019）京 73 民终 1270 号案件中，均对原告提出的数据知识产权保护诉求进行了适用条件审查，即对作为诉争标的的数据是否构成著作权法下的作品或者其他知识产权部门法的客体进行说理和判断。由于

知识产权保护的地域性，对于其客体范围的认定，各地法院可能存在差异。在上述欧盟法院作出的C-30/14 ,(15 January 2015) 一案中，就原告是否享有数据库权，欧盟法院认为数据库权应当以对数据的获取、核实或输出进行实质性的投入为前提，且根据“副产品原则”，数据库和数据内容、获得数据库而进行投入和为生成数据内容而进行的投入均被严格区分。显然，倘若获得数据的行为与该数据的生成过程无法分离，那么制作者就难以证明其为数据库进行了实质投入，从而不能享有数据库权的保护。当然，欧盟法院亦指出，如果数据内容的创造未经事前计划，且其收集、核实、编排、呈现需要额外的实质性支出，那么制作者同样可以取得数据库权。基于上述理解，法院认为原告的数据库不过是其经营的副产品，且未就相关数据的收集进行额外投入，因此构成典型的“单一数据源数据库”，并非《数据库指令》的保护对象。

最后，**作为事后救济的主要方式，竞争法和数据财产性利益的关联得到了国内外法院的普遍支持**。例如，在（2017）京 0108 民初 24512 号案件中，海淀法院对企业数据权利的观点与（2018）浙 01 民终 7312 号案一致，并对企业数据权利非法定权利但仍可受到法律保护进行了更细致的阐述。海淀法院认为，根据民法总则第 123 条的规定，知识产权是权利人依法就特定权利客体享有的专有权利；该条第八项关于“法律规定的其他客体”对知识产权权利客体保护做了兜底规定；第 127 条规定，法律对数据、网络虚拟财产的保护有规定的，依照其规定。即便有前述规定，因我国立法尚未就数据进行单独立法，故数据是否能作为前述规定的知识产权权利客体而受民法或其他知识产权部门法保护仍有争议。海淀法院进一步指出，在当前的市场环境下，数据已经逐渐成为经营者，尤其是互联网经营者之间相互竞争的基础性资源，获得数据意味着可据此进行分析并改进、完善产品功能，从而获得更多的经营利益。因此，司法不能以数据尚未成为一种法定权利为由而拒绝裁判。海淀法院结论性提出，当经营者为收集、整理数据，以及维护其互联网产品中的数据运行和安全而付出成本，且该种数据整体上可为经营者进行衍生性利用或开发从而获得进一步的经营利益时，其他经营者未经许可擅自抓取且使用平台数据的行为，当然可以落入反不正当竞争法调整的范围。而在C 08-5780 JF (RS), October 22, 2009 案件中，对于用户账号类数据的未经授权爬取行为，认定其落入了 CFAA 的管辖和保护范畴，因此原告基于数据产生的相关合法权益受到保护。

关于企业可以对何种数据享有何种权益这一问题，通过上述对案例的梳理考察，我们可以发现目前国内司法实践对此问题的分析逻辑和态度如下：

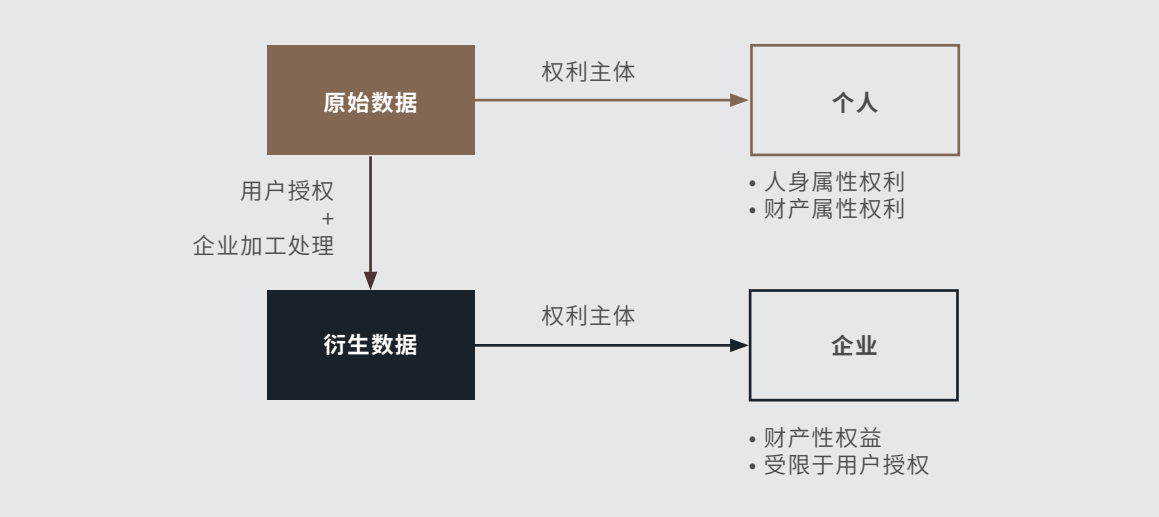
- 首先应当考察企业掌握的数据产品或数据服务是否可以落入知识产权法保护范畴，比如相关数据产品是否具有独创性可以构成作品进而受到著作权法保护。在（2019）京 73 民终 1270 号案件中，因原告的地理信息数据具有独创性，构成地图作品，所以法院认定原告对其数据享有著作权，可以受到著作权法和侵权责任法的保护。在（2020）湘 0104 民初 10602 号案中，法院认为原告付出人力、物力对公开的钢材价格信息进行汇编，具有独创性，构成汇编作品，对其数据享有汇编作品所有权。
- 其次，在企业的数据产品或数据服务无法被认定为受知识产权法保护的作品时，法院会考察企业是否对数据投入了人力、物力等资源，是否对数据进行过加工处理，进而判断企业是否对相关数据享有权益。
- 相关数据是否构成企业的核心竞争力，是否为企业开展经营活动的基础，也会影响法院对企业是否享有数据权益的判断。
- 至于企业对数据享有何种权益，法院会因数据尚未成为一种法定权利而否认企业主张的数据所有权，但是认可企业对其投入资源、加工处理后形成的数据享有财产性权益或者竞争性权益，企业对数据的此种合法权益可以受到法律保护。

（三）企业数据与个人数据的权利边界

1. 依托原始数据与衍生数据划分权利边界

从前述数据分类和数据用益权理论角度来说，企业通常基于用户授权获取到大量的用户个人数据，在用户个人数据的基础上进行一定的加工处理从而形成企业数据。用户作为原始数据的提供者或创造主体，自然对其基于自身所产生的数据享有权利，包括人身权利和财产权利。企业基于用户提供

的这些原始数据进行整理、加工，获得衍生数据，因企业投入了人力、物力等成本，企业对衍生数据可以享有财产性权益。但是企业的衍生数据因基于用户原始数据产生，企业与用户之间存在授权协议，因此企业对基于用户数据产生的衍生数据享有的权益还受到用户授权范围的限制。



例如在（2018）浙 01 民终 7312 号中，一审法院认为网络大数据产品不同于原始网络数据，其提供的数据内容虽然同样源于网络用户信息，但经过网络运营者大量的智力劳动成果投入，经过深度开发与系统整合，最终呈现给消费者的数据内容，已独立于网络用户信息、原始网络数据之外，是与网络用户信息、原始网络数据无直接对应关系的衍生数据。网络运营者对于其开发的大数据产品，应当享有自己独立的财产性权益。

在（2019）浙 8601 民初 1987 号案中，法院特别指出，网络平台中的数据，以数据资源整体与单一数据个体划分，网络平台方所享有的是不同的数据权益。就原告平台数据资源整体概念而言，原告依法享有竞争性权益，但对于某个特定的单一用户数据，原告并不享有专有权，仅享有受限于用户授权的有限使用权。

2. 企业与其他企业、用户个人的三方数据权益划分

在爬虫技术的广泛应用下，企业平台上的公开数据可以被其他企业爬取，在业务合作或产业链中不同企业也会发生数据交互，例如输入法软件对社交软件中聊天记录数据的获取，而这些数据又由用户个人初始提供。在不同数据主体出现权利交叉的情况下，需要明确企业与其他企业、用户个人等多主体之间的数据权益划分规则。

从国外判例的情形来看，爬虫工具的使用所引发的企业间竞争纠纷可以作为影响数据权益边界认定规则的观察角度。在 938 F.3d 985 (9th Cir. 2019) 案件中，法院对于使用爬虫爬取公开数据显然保持相对开放的态度，以鼓励数据的开放和自由流通。辅之以参考 C 08-5780 JF (RS), October 22, 2009 进行两案的对比，我们发现，用户数据是否受“账号密码”的保护（即数据是否为公开）可能是法院认定爬虫使用行为的重点考量因素，但不得不注意的是，如前述提及，目前美国最高法院将此案件发回重审，意味着数据抓取行为的定性仍具有不确定性。最关键的问题仍然在于：如若属于用户的公开个人数据，是否有必要考虑用户的授权原则？此外，对于被抓取的数据生产方而言，是否需要兼顾其合法权益？这些问题都有待于 938 F.3d 985 (9th Cir. 2019) 案件发回后重审法院来面对和解答。

就国内司法实践而言，早在（2016）京 73 民终 588 号案中，北京知识产权法院就多主体之间数据权益关系进行了详细的探讨。针对平台上用户公开发布的信息，其他企业是否有权利用技术手段抓取问题，北京知识产权法院提出了“用户授权”+“平台授权”+“用户授权”的三重授权原则。根据这一原则，对于企业平台上的用户数据，即便该数据是由用户公开发布的，其他企业通过该平台抓取数据不仅应获得用户授权，还应获得平台方授权。

在（2018）浙 01 民初 3166 号中，法院认为，原告研发的基于 Android 系统的“智能收银一体机”因系统功能和特性是可以安装其他应用的，被告的收款应用在安装过程中，已经向用户获取了读取交易金额数据的授权，因此被告读取交易金额数据的行为不构成非法获取数据。

在（2017）京 0108 民初 24512 号中，海淀法院将企业平台数据分为公开数据和非公开数据，并分类讨论了其他企业抓取和使用平台数据的正当性。海淀法院提出，对于平台中的公开数据，基于网络环境中数据的可集成、可交互之特点，平台经营者应当在一定程度上容忍他人合法收集或利用其平台中已公开的数据，否则有违互联网网络互通之精神。但是如果他人抓取网络平台中的公开数据行为手段不正当，则数据抓取行为及后续使用行为亦难谓正当。对于平台中设置了访问权限的非公开数据，其他企业在未获得授权的情况下获取这些非公开数据，仅能利用技术手段破坏或绕开平台设定的访问权限，这种行为显然具有不正当性。

可见，在企业平台、其他企业及用户等多方主体的数据关系中，用户授权依然为数据合法性的基石，而爬取他人平台数据的技术手段是否正当、是否遵守被爬取平台的有关技术协议等因素，是判断企业爬取、使用数据行为合法性、正当性的重要标准。

四、构筑企业数据资产价值与安全防护墙

由上可见，即便目前无论是立法进程还是理论探讨，都尚未明确界定数据的权益规范，但在数据要素市场的竞争局势中，**数据作为企业的特殊竞争力及其愈发显著的经济价值，使得企业需要正视并尽早布局内部数据资产管理体系，并形成与之相配套成熟的数据资产识别、固定和保护的法律工具或者解决方案，做到“数中有术”**。

结合我们在数据合规以及数据竞争市场的法律服务经验，概括来说，这套方案至少需要重视以下几个方面的内容：

（一）数据安全与合规确保数据质量与资产有效性

“数据资产的收益取决于数据资产的质量和数据资产的应用价值。数据资产质量价值的影响因素包含真实性、完整性、准确性、数据成本、安全性。”[15] 通常意义上说，企业数据资产得以固定和价值体现的前提和基础是数据本身的合法合规及其质量保证。目前，《民法典》高屋建瓴，《网络安全法》《数据安全法》相辅相成，《个人信息保护法》呼之欲出，数据安全与个人信息全生命周期流程性合规已经成为企业日常经营不容忽视的重要事项。

正如前述司法案例中所涉及的具体场景，如果主管部门或者司法机关不认可企业数据来源和数据处理活动的合法合规性，则该企业对于基于该数据处理活动而形成的数据集合主张的财产性权益受保护的价值和可能性都大打折扣。因此，企业一方面必须严格按照法律规定及与自然人约定的目的、范围和方式，在得到个人信息主体事前同意的前提下，收集、存储、处理个人信息；另一方面，通过全面履行企业既有的网络安全保障义务，落实数据安全制度安排，以确保数据本身没有合法性的质量缺陷，从而铺垫好数据资产价值管理体系的牢固基石。

（二）数据分类分级管理识别资产边界与价值挖掘

企业数据资产的要素识别和体系构建，有赖于对其所收集和“掌握”数据的情况、可开发利用的价值以及基于此而进一步探讨的数据商业化方案或者策略。“数据分级分类最初是网络运营者对数据资产进行一致性、标准化管理的方法，随后成为网

[15] 德勤、阿里研究院：《数据资产化之路——数据资产的估值与行业实践》，https://www2.deloitte.com/cn/zh/pages/finance/articles/data-asset-report.html 最后访问日期：2021 年 7 月 29 日。

络数据安全风险管理的技术方案。”[16] 就现行《数据安全法》以及配套法规来看，企业完善内部的数据分类分级制度实则是一举两得的高收益管理策略，即在满足从网络安全向数据安全的企业法律要求的同时，也能够帮助企业主动梳理、识别与确定得以进一步实现价值挖掘的数据类型与范围。从上述国内的多个司法裁判案例可以看出，目前各地法院对于企业就其收集的数据集，或者说数据驱动企业对于增值数据享有一定的“财产性权益”持较为认可的倾向态度。因此，建立在数据分类分级基础上的数据挖掘，包括数据清洗、加工、提取、交换、共享以及算法训练等，有助于形成企业独特的数据资产竞争力。

（三）形成数据权益手册以及信息化管理系统以支撑商业合作磋商策略

数据权益理论的探讨最终服务于业务实践操作，形成对企业固定和保护数据资产的方法论。基于前述数据合规、数据分级分类和价值挖掘环节后，为了便于企业在实际工作中更好地主张数据权益，企业可以根据数据处理实际情形制定内部数据权益手册。权益手册相当于一本工具字典，帮助企业对不同类型的数据进行分类和标签化，明确了企业作为数据控制者或者委托处理者可主张的数据权益可能空间，为企业提出更为有利的权益主张思路和立场建议，以在实践中快速和准确判断某数据资产的权益主张边界，并且指导与第三方之间涉及数据合作的商业谈判。

同时企业应当根据权益手册内容利用信息化技术开展数据资产的自动化识别、存储、流转及交易等工作，利用数字科技来管理数据资产，做到“术中有数”。

（四）积极主张数据权益以凝聚数据行业价值共识

作为司法救济的最后一道防线，企业应当注重准备多种诉讼策略，以更为积极地主张企业数据权益的可能空间。在缺乏明确立法规则的前提下，通过争议解决的路径设计和诉求主张，也有助于通过个案的方式探索行业数据价值有序的分配规则。正如我们在这篇文章中所提及的既往案例，对于数据行业而言，通过司法裁判的说理、判决，有助于我们加深对数据行业资产管理与保护的需求，并且对于推进个人与企业数据权益边界的认定，以及凝聚企业间数据竞争与合作的价值共识都或有裨益，从而在积极的诉讼策略中形成尊重与保护数据生产、流动与共享价值的积极行业生态。

结语

数据确权是数据流转、数据交易等基于数据开展的各种活动的前提。明确、合理的数据权益规则为数据主体开展数据处理活动提供行为边界，不仅能预防数据纠纷，也为数据权利人提供保护和救济。虽然国内外目前立法层面并未有明晰的数据权益规定，但是在长期的司法实践中形成和积累的数据权益分配规则，对数据活动起到一定的指导、规范作用。本文通过对于数据权益理论的梳理，以及对当前国内外数据权益纠纷相关案例的考察，希望能够为当下的数据实践活动略有助力。

感谢甘雨丰、徐晓妍对本文的贡献。

[16] 刘云：《健全数据分级分类规则，完善网络数据安全立法》，http://www.cac.gov.cn/2020-09/28/c_1602854536494247.htm 最后访问日期：2021 年 7 月 29 日。

利刃出鞘：《数据安全法》下中国数据保护路径解读

宁宣凤　吴涵　张凯勋

引言

事实证明，数据安全是当前国家间实力博弈的重要战场。据华盛顿当地时间 6 月 9 日消息，美国白宫签署行政令，宣布撤销此前于 2020 年由美国前任总统颁出的对 T 公司、W 公司等多款母公司在中国的移动应用程序禁令。纵观行政令全文[1]，有媒体指出此举并不意味着美国已经放弃了对中国应用“以安全为由”的审查、阻拦乃至封锁。[2]新签署的行政令还要求美国商务部等相关部门对可能影响美国国家安全和敏感数据（包括身份信息、健康和基因信息等）安全构成风险的“外国敌手（foreign adversary）”的应用程序开展评估，并视情况采取必要措施。该行政令被部分西方媒体解读为“美方对华政策的最新风向”[3]。

与此同时，据全国人大北京时间 2021 年 6 月 10 日消息，《中华人民共和国数据安全法》（“**《数据安全法》**”）经历三轮审议，已由十三届全国人大常委会第二十九次会议表决通过。正逢其时、掷地有声，作为我国数据安全领域内的“基础性法律”和我国国家安全领域内的“重要法律”[4]，**《数据安全法》积极回应了时下国内外数据竞争和保护的关键问题，给企业数据经营合规，以及进一步的数据资产化治理与发展提供指引。**

一、《数据安全法》对全面数字时代的主动回应

（一）当“数据安全”成为一项全球冲突与合作议题

1. 应对全球数字主权化浪潮

近些年来，从网络主权延伸至数据主权的发展趋势日渐明显，数据安全成为国际间竞争与合作的全新议题。围绕数据控制权和管辖权，全球各个国家和地区正在兴起新一轮的“数字主权化”浪潮，对抗与防御在数据竞争领域里表现得日益显著。

当人们意识到“数据关乎国家主权”[5]后，除开篇所提及的 T 公司事件所依赖的时局背景（即美方针对性发起的“清洁网络”计划），美国自

[1] Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/ 最后访问日期：2021 年 6 月 14 日。
[2] 参见王是业（贝果财经）：《解禁 TikTok 等中国 APP 是拜登的拨乱反正？》，https://finance.sina.com.cn/china/2021-06-12/doc-ikqciyzi9299849.shtml 最后访问日期：2021 年 6 月 15 日。
[3] *See* Trump's TikTok, WeChat Actions Targeting China Revoked by Biden, https://www.wsj.com/articles/biden-revokes-trump-actions-targeting-tiktok-wechat-11623247225 最后访问日期：2021 年 6 月 15 日。
[4] 《数据安全法：护航数据安全 助力数字经济发展》，载“中国人大网”，http://www.npc.gov.cn/npc/c30834/202106/b7b68bf8aca84f50a5bdef7f01acb6fe.shtml 最后访问日期：2021 年 6 月 14 日。
[5] 许可：《数据安全法：来路与前途》，载“数字经济与社会”，https://mp.weixin.qq.com/s/LpKvYpdTm9vZSTB0YtFsJQ 最后访问日期：2021 年 6 月 14 日。

CLOUD 法案以来以“域外长臂管辖”争夺网络空间数据控制权，试图建构国际数据市场竞争规则的新秩序；而印度通过其数据本地化策略加以应对的同时，也以“国家安全”为由对我国出海互联网企业实施了“大面积封锁”。在对抗日益加剧的同时，遗憾的是，数据领域的国际合作努力频频受挫。2019 年 G20 大阪峰会上，印度就因秉持数据本地化立场而拒绝会谈，印度尼西亚和南非则拒绝签字，并且表达了对跨境数据流动持反对意见，认同数据本地化价值，[6] 客观上呈现出世界主权国家就数据合作的割裂趋势。

不难理解，在数据已经成为一种全新的国际竞争领域的前提下，凭借综合国力和科技影响力，确认数据要素地位并优先立法的国家，能够占据国际数据竞争市场高地，从而成为数据领域的游戏规则制定者。2020 年，我国向国际社会公开呼吁全面客观看待数据安全问题，维护全球信息技术产品和服务的供应链开放、安全、稳定，并发出《全球数据安全倡议》[7]；而**眼下出台《数据安全法》，正是基于此种国际社会历史的背景而诞生，且被寄予了提升数据主权竞争优势、改变并重塑数据国际规则的厚望**。

2. 确保“国家总体安全观”下的数据安全

国际数据竞争的另一目标维度，是通过确保数据安全的路径以维护国家核心利益。在全面数字化时代，数据安全已经成为国家战略层面的重要考量。2020 年，欧盟发布《欧洲数据保护监管局战略计划（2020—2024）》，旨在从前瞻性、行动性和协调性三个方面继续加强数据安全保护；美国发布《联邦数据战略与 2020 年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则；德国成立国家网络安全机构，负责发起网络安全创新项目、研究打击网络威胁，以加强德国的“数据主权”[8]。

根据《数据安全法》第 4 条规定，维护数据安全，应当坚持总体国家安全观。基于国家总体安全观，网络与数据安全属于政治、领土和军事威胁之外的非传统安全，但在国家安全战略体系中的地位仍然十分关键。这是因为，数字化时代多源信息融合技术的发展模糊了国家秘密与非秘密之间的界限，而部分影响国家安全的数据并不在传统国家安全部门的统领之下，不少可能影响国家经济命脉、社会稳定和整体福利水平的重要数据可能由企业掌握 [9]。**加强国家总体安全观指引和定位下的企业数据安全治理，成为是维护国家安全的必然要求、促进数字经济健康发展的重要举措** [10]。

（二）当“数据安全”成为我国的一项专门立法

我国《数据安全法》最终文本在中国人大网上全文公布，并且于 2021 年 9 月 1 日产生法律效力。在接近正式生效的三个月过渡期内，企业需要准确认识、深入研究和仔细解读其中的法律适用具体问题，以避免不必要的合规风险乃至违法成本。

1. 适用范围

最终通过的《数据安全法》延续了此前一审、二审稿的做法，为执法者的数据安全监管保留了必要的域外适用空间。**总结来看，《数据安全法》从规制对象、适用地域和管辖内容与法律体系衔接三个侧面，划定了其规范约束的基本边界**。

首先，《数据安全法》着眼于“数据处理活动与安全监管”，将其作为一部行为约束法的法律特征凸显出来。换句话说，《数据安全法》跳脱出此前“限定约束主体”的立法思维，转而定义“数据处理”和“数据安全”并作为其规制对象，凡是符合数据处理活动的主体均需要满足或者履行数据安全义务，使得人们在解释和适用规则时不必拘泥于适用主体范围的划定，而专注于数据处理活动本身的安全、可靠性。

其次，《数据安全法》将“损害国家安全、公共利益或者公民、组织合法权益”作为监管域外数据处理活动的触发条件，以实际影响或者后果为导向，进一步明确了维护国家数据安全的决心；而从企业合规角度来看，凡是以中国公民为数据处理对

[6] 何傲翾：《数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析》，载《北京航空航天大学学报（社会科学版）》2021 年 5 月第 3 期，第 19-20 页。
[7] 外交部：《全球数据安全倡议》，https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml 最后访问日期：2021 年 6 月 14 日。
[8] 王伟洁，周千荷：《国外数据安全保护的最新进展、特点及启示》，载《中国计算机报》2021 年 5 月 17 日第 013 版。
[9] 朱雪忠，代志在：《总体国家安全观视域下 < 数据安全法 > 的价值与体系定位》，载《电子政务》2020 年第 8 期，第 82-92 页。
[10] 同上注 2。

象，或者数据处理活动对中国可能产生实际影响的境外主体，亦需履行中国法下的数据安全义务，这为跨国企业面向中国提供服务、在境外开展数据处理活动提供了管辖连接点。

最后，**我们认为《数据安全法》仍然包含了对“个人数据”安全的原则性适用，其与《个人信息保护法》可能不是非此即彼的适用关系，而应当理解为，在数据安全的一般性原则之上，个人数据处理仍需遵循《个人信息保护法》中的特殊规则**。虽从欧盟的立法经验来看，《通用数据保护条例》（General Data Protection Regulation, GDPR）和《非个人数据流动条例》（Regulation on the Free Flow of Non-personal Data）在明确区分数据性质属于“个人”或者“非个人”的基础上进行了法规适用，但从《数据安全法》第 53 条的文义解释角度来看，“开展涉及个人信息的数据处理活动，**还应当**遵守有关法律、行政法规的规定”，显然是为即将出台的《个人信息保护法》留出了立法接口与体系空间。相似地，《统计法》《档案法》也均存在类似的体系规范接口，在涉及数据处理活动时，除需满足《数据安全法》规定的数据安全监管责任规范外，也适用其特殊规则。

2. 价值体系

自《数据安全法》草案面世以来，“坚持安全与发展并重”一直是官方所明确秉持的立法原则。法律中多处体现了“**促进以数据为关键要素的数字经济发展**”的价值取向，包括国家实施大数据战略，制定数字经济发展规划；支持数据相关技术研发和商业创新；推进数据相关标准体系建设，促进数据安全检测评估、认证等服务的发展；培育数据交易市场；支持采取多种方式培养专业人才等 [11]。

具体而言，关于数据的保护价值与发展价值事实上已有不少讨论。而如今《数据安全法》站在立法价值体系的高度上，所需要融合或者强调的，应当是以“数据风险管控”为核心的安全价值这一统一概念，其既包括数据本身的保密性、完整性与可用性，也包括数据处理活动（即数据要素增值过程）的可控性和正当性 [12]。换句话说，数据保护本身作为一种手段而非目的，最终所应当达成的目标是在合理有效控制数据处理活动的客观风险的前提下，不断实现数据要素的增值、经济财富积累以及社会总福利的提升。因此，数字时代的《数据安全法》，在准确认知数据保护与数字经济发展两大基本价值体系的基础上，不断地引领数据安全立法的前进方向。

《数据安全法》给依法依规经营的境内外数字化企业带来的应是信心而非阻力。可以预见的是，数据产业与数字经济发展将在《数据安全法》的护航下走向下一个红利期，尽管必不可免地将带来一定的数据合规成本，但法律明朗的游戏规则还会将成本转换为一定的竞争门槛与安全优势，从而有效地防止“劣币驱除良币”效应，使得合法合规的数据驱动型企业更为精准、有力地把握市场机遇。

3. 立法定位

结合立法背景和价值考量，不难理解数字经济时代下的《数据安全法》理应包含两个层面的定位：其一，《数据安全法》是关乎国家安全与数据主权的基本“宣言”，顺应了国际数据竞争的客观趋势，同时积极回应规则挑战与域外影响，以立法这一国际社会通行的现代文明方式服务于维护国家利益、公民合法权益这一最高价值目标；其二，《数据安全法》亦是数据领域里的上位法与基础性法律，除特定类型数据处理活动（涉国家秘密和军事数据）外，进行数据处理活动的企业均需以《数据安全法》为蓝本和依据，进行深层次的数据安全合规。

二、《数据安全法》的法规范重点制度图景

（一）以“重要数据”为核心搭建的安全监管制度

1. 重要数据的识别

作为数据安全层面的上位法和基础性法律，《数据安全法》搭建了以“重要数据”为核心的安全监管制度，而重要数据的识别则是数据安全工作的重中之重，同时也体现了数据治理的分类分级管理和保护原则。

《数据安全法》第 21 条在笼统定义重要数据并要求国家数据安全工作协调机制统筹协调各部门

[11] 刘俊臣（全国人大常委会法制工作委员会副主任）：《关于 < 中华人民共和国数据安全法（草案）> 的说明——2020 年 6 月 28 日在第十三届全国人民代表大会常务委员会第二十次会议上》，载“中国人大网”，http://www.npc.gov.cn/npc/c30834/202106/2ecfc806d9f1419ebb03921ae72f217a.shtml 最后访问日期：2021 年 6 月 14 日。
[12] 刘金瑞：《数据安全范式革新及其立法展开》，载《环球法律评论》2021 年第 1 期，第 10-11 页。

重要数据识别工作的基础上，将重要数据的具体识别工作下放至各地区、部门，以地区、部门以及相关行业、领域为维度制定重要数据目录，充分平衡了法律规定的普适性和灵活性。同时，相较于此前的二审稿，《数据安全法》加强了国家层面对重要数据目录制定的统筹工作，可以有效避免因各部门管理标准的差异而导致的数据安全规则碎片化，无形增加不必要的合规成本。

而早在《数据安全法》正式发布前，各部门与行业也不乏根据行业特性进行重要数据识别的尝试。例如，2017 年全国信息安全标准化技术委员会发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》附录 A“重要数据识别指南”中对 27 个重点行业的重要数据做了概括性的描述，如石油、电力、金融等。

近期，国家互联网信息办公室发布的《汽车数据安全管理若干规定（征求意见稿）》（“**《汽车数据规定》**”）首次明确界定了汽车行业重要数据的范围，具体包括：

- 军事管理区、国防科工等涉及国家秘密的单位、县级以上党政机关等重要敏感区域的人流车流数据；
- 高于国家公开发布地图精度的测绘数据；
- 汽车充电网的运行数据；
- 道路上车辆类型、车辆流量等数据；
- 包含人脸、声音、车牌等的车外音视频数据；以及
- 国家网信部门和国务院有关部门明确的其他可能影响国家安全、公共利益的数据。

从上述重要数据范围可以看出，《汽车数据规定》对重要数据的框定偏于严格，车辆外装的摄像头等传感器记录的数据，以及车辆 GPS 定位数据均有可能落入重要数据的范畴。根据行业实践，相关车联流量数据、高精测绘数据是自动驾驶、智能汽车行业常用数据类别，参考《汽车数据规定》下的重要数据处理原则，如车内处理，非必要不向车外提供，以及数据本地化要求，相关企业更需要在进行重要数据识别与分类的基础之上审慎合规。

诚然，重要数据的识别需要考虑诸多因素，并且重要数据的识别并不是一成不变的，如何确定重要数据将取决于各地区、各部门制定的重要数据目录以及诠释，而各行业主管部门也会根据行业发展变化，对本行业重要数据的定义和范围进行调整，并对重要数据目录进行适当的替换 [13]。

2. 重要数据的安全保护义务主体

《数据安全法》延续《网络安全法》的规定，以重要数据为锚点，对重要数据的处理活动提出了若干延展数据安全保护义务，主要包括：

- 重要数据的处理者应当明确数据安全负责人和管理机构（第 27 条）；
- 重要数据相关活动定期开展包括重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等在内的风险评估，并向有关主管部门发送风险评估报告（第 30 条）；
- 如果重要数据的处理活动影响或者可能影响国家安全的，应当接受国家安全审查（第 24 条）；
- 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。（第 31 条）。

虽然《数据安全法》明确了定期评估并发送报告的方式，但评估主体、报告报送对象、以及评估频率还有待配套规章制度的进一步明确。同时，风险评估更多意味着事中监管。而从防范数据安全事件的角度出发，各地区、行业重要数据目录可能会提出更为细致的监管要求，以进一步落实数据安全保护义务。例如，《汽车数据规定》明确要求的运营者事前报告义务；运营者处理重要数据，应提前当向省级网信部门和有关部门报告数据类型、规模、范围、保存地点与实现、使用方式，以及是否向第三方提供等。除事前报告外，运营者还需将年度数据安全管理报告报送省级网信部门和有关部门。

此外，关键信息基础设施运营者重要数据跨境

[13] 中国信息通信研究院娇娇：《< 数据安全法 > 亮点解读：立法沿革和重点条款》。

传输规则应适用《网络安全法》相关规定的指示性规定，揭示了《数据安全法》和《网络安全法》的体系地位，即两者均为以《宪法》为上位法的基本法律，二者为同一阶层平行的法律[14]。

最后，对于可能涉及重要数据处理活动的企业而言，其应当明确的数据安全负责人和管理机构是否需区别于《网络安全法》下有关网络安全负责人、《个人信息保护法》个人信息保护负责人的设置，以及是否需将相关负责人员以及管理机构于主管部门报备仍有待立法者在后续实施细则与配套措施中予以澄清。

（二）以“数据交易”为机制的数据权益主张共识

1. 数据交易制度延续了一审稿中的规定

《数据安全法》中关于数据交易的制度延续了一审稿中的规定，明确建立健全数据交易管理制度，确定数据交易行为的合法性，培育数据交易市场，则是数据作为一种生产要素的必要发展。在《数据安全法》的出台之前，国务院及各部委出台了多项综合性或专业性与数据市场发展相关的政策，但缺乏上位法依据和顶层制度方面的统筹，而《数据安全法》对数据交易制度完善，可以有效弥补这一缺陷，增强数据交易市场的可操作性。[15]

除上述原则性规定外，《数据安全法》还对从事数据交易中介服务的市场参与者提出了额外的安全保护要求，比如从风险控制的角度出发，规定从事数据交易中介服务的机构应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录，但关于审核的具体模式、数据提供方的合规风险是否会传导至中介服务提供者等细化规则还有待相关配套制度进一步明确[16]。同时，为加强事前监管，提高安全保护意识，《数据安全法》于正式稿内加强了处罚力度，未履行上述要求的数据交易中级机构，将可能被处以没收违法所得以及最高十倍的罚款，并可能被责令停止相关业务、停业整顿、吊销相关业务许可证或营业执照。

同时，根据《数据安全法》第 34 条，法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可，本条对从事数据交易的准入资格提供了上位法依据，后续可能会在市场准入环节加强监管[17]。

建立数据交易管理制度的基础是明确数据产权或权属问题，即需要明确个人数据、公共数据、国家数据、数据要素市场主体的数据权等基础法律问题，否则数据的流通和交易将面临制度障碍。目前我国关于数产权的规定仍为原则性规定，数据产权规则不清晰，可能会导致多方数据主体之间的利益冲突，因此，数据交易市场的健全还有待后续配套规则对数据产权的细化[18]。

除此之外，数据市场的反垄断制度尚需改善。虽然 2020 年公布的《< 反垄断法 > 修订草案（公开征求意见稿）》第一次将互联网行业的垄断界定及其处置写入法律，今年年初发布的《平台经济领域反垄断指南》更细化了各类互联网平台的反垄断规则，也为数据市场反垄断提供了重要的制度性依据。但是，对于数据市场特有的垄断行为，现有反垄断相关法律法规难以覆盖。比如，对于经营者集中的垄断行为，现行《反垄断法》以及《平台经济领域反垄断指南》主要以经营者的营业额作为基准，然而对于数据公司而言，虽然营业额不高，其仍然可能对市场产生非常大的影响[19]。

2. 借助卡梅框架的解释方法：数据财产规则

自 2017 年《民法总则》对数据采取引制性规定，数据出现在权益兜底性条款之后，数据权益客体认定以及数据赋权一直是社会热议话题。我国理论界形成了数据人权说、数据知识产权说、数据新型财产权说等不同观点，而各地方政府也争相尝试创设相关权益[20]。以深圳为例，深圳市司法局于 2020 年发布的《深圳经济特区数据条例（征求意见稿）》明确提出了数据权这一概念，将其规定为权利人依法对特定数据的自主决定、控制、处理、收益、利益损害受偿的权利，并根据不同数据内容

[14] 翟志勇：《数据安全法的体系地位》，载《苏州大学学报 - 哲学社会科学版》2021 年第 1 期，第 76-77 页。
[15] 曾铮、王磊：《数据要素市场基础性制度：突出问题与构建思路》，载《宏观经济研究》2021 年第三期，第 88 页。
[16] 同上注 11。
[17] 同上注。
[18] 同上注 13，第 86-87 页。
[19] 同上注。
[20] 崔淑洁：《数据权属界定及“卡—梅框架”下数据保护利用规则体系构建》，载《广东财经大学学报 - 法和经济学》2020 年第 6 期，第 79-80 页。

区分为个人数据权、公共数据权和数据要素市场主体的数据权[21]。针对该征求意见稿，理论和实务界普遍认为，由于目前还存在公众对于数据权属问题认知不统一、数据权划分边界不清，权利客体交织重合，以及划分过为绝对等问题，故直接在经济特区法规中创设“数据权”可能还为时尚早。有鉴于此，2021 年新发布的《深圳经济特区数据条例（征求意见稿）》在充分考虑社会共识与司法实践的基础上，将数据权这一宽泛的概念进一步细化为对自然人对其个人数据的人格权益以及企业对其投入大量智力劳动成果形成的数据产品和服务的财产性权益的保护[22]。

从比较法的角度，虽然美国和欧盟对数据保护和利用模式不尽相同，但二者均将数上权益进行多层次区分并适用不同的保护标准，以实现数据保护与数据利用的平衡。如美国将数据分为个人数据与经过匿名处理后产生的衍生数据，对个人数据适用以隐私权为中心的保护标准，而对衍生数据适用市场自治和竞争法相结合的模式以确保对衍生数据的开发和利用[23]。

因此，基于我国的数据分类分级制度要求，并参考借鉴域外数据权属界定经验，我国日后对数据权属的划分，可考虑从数据全生命周期出发，结合数字经济发展阶段和数据应用场景，对不同类别数据的数上权益进行区分，以适用不同的保护规则，进而实现数据权利化。例如，根据处理方式，可以区分为原始数据和衍生数据；根据数据主体，可以分为个人数据、业务数据，以及公共数据[24]。

（三）以“分业管理”“自上而下”为特征的数据安全体系

1. 数据分类分级制度

承《网络安全法》为保障网络运行安全而采纳的网络安全等级保护思路，《数据安全法》确立的数据分类分级保护制度作为数据安全管理工作的前提与基础将直接决定企业对于不同等级与类别数据全生命周期管理应承担的保护义务。

在制度范围方面，虽然《数据安全法》仅针对重要数据和国家核心数据（“关系国家安全、国民经济命脉、重要民生、重大公共利益”的数据）明确提出“重点保护”与“更加严格管理”的安全要求，但对于重要数据和国家核心数据之外的其他数据，仍然需要以《数据安全法》下有关数据在经济社会发展中的重要程度与可能的数据事件危害程度为基准进行相应的分类分级划分与差异化保护设置。

在制度制定方面，一方面《数据安全法》将国家界定为数据分类分级制度建立的主体，为国家开展“自上而下”监管提供依据，另一方面，在《数据安全法》正式颁布之前，各行业已进行行业数据分类分级标准制定的尝试，包括但不限于《金融数据安全 数据安全分级指南》《证券期货业数据分类分级指引》《工业数据分类分级指南（试行）》《电信和互联网服务用户个人信息保护定义及分类》《电信和互联网服务 用户个人信息保护分级指南》等。其中，中国人民银行印发的行业标准《金融数据安全数据安全分级指南》明确了金融数据安全分级的要素、规则，以及定级过程，并给出了金融业机构典型数据定级规则供实践参考，同样由中国人民银行印发的行业标准《金融数据安全数据生命周期安全规范》则根据金融数据的安全等级，对不同级别金融数据的采集、传输、使用、删除、销毁做出了详细的要求。但值得注意的是，“分业管理”下形成的数据分类分级的科学性、合理性以及可验证性仍有待进一步探讨。

2. 数据安全标准体系建设

《数据安全法》通过统一立法的形式加强数据安全标准体系的建设，而依托于行业组织依法制定的数据安全行为规范和团体标准也将构成安全标准体系的重要部分。根据《数据安全法》第 17 条，国务院标准化行政主管部门和国务院有关部门牵头数据安全相关标准的制定，国家支持企业、社会团体和教育、科研机构等参与标准制定工作。在数据使用技术高速发展的情况下，立法往往滞后于行业发展，而本条则旨在加强市场参与者踊跃参与行业标准的讨论，积极分享在数据安全合规建设中探索

[21] 参见《深圳经济特区数据条例（征求意见稿）》。
[22] 见关于《深圳经济特区数据条例（征求意见稿）》的说明，载互联网金融法律研究，http://ifls.cupl.edu.cn/info/1066/1630.htm 最后访问日期 2021 年 6 月 14 日。
[23] 同上注 18，第 81 页。
[24] 同上注，第 82 页。

出的实践经验，并以行业最佳实践为基础推动完善技术发展和合规建设[25]。

目前，工业和信息化部已经开始布局数据安全标准体系的建设。2020 年 12 月工业和信息化部发布的《电信和互联网行业数据安全标准体系建设指南》对电信和互联网行业的数据安全标准提出了原则性要求，并列出数据安全体系建设的短期目标：于 2021 年研制数据安全行业标准 20 项以上，初步建立电信和互联网行业数据安全标准体系，有效落实数据安全管理要求，基本满足行业数据安全保护需要，推动标准在重点领域中的应用。到 2023 年，研制数据安全行业标准 50 项以上，健全完善电信和互联网行业数据安全标准体系，标准的技术水平、应用效果和国际化程度显著提高，有力支撑行业数据安全保护能力提升。

（四）以“出口管制”“对等措施”为抓手的必要反制措施

1. 属于管制物项的数据出口管制

与《出口管制法》第 2 条规定的“管制物项，包括物项相关的技术资料等数据”相衔接，《数据安全法》第 25 条规定，国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。虽然“维护国家安全和利益、履行国际义务”可作为禁止相关数据出口的合法依据，但在具体适用上，还存在和《出口管制法》的衔接问题[26]。根据《出口管制法》，我国对出口管制物项实行清单管理，包括由国家出口管制管理部门出台的管制清单及根据需要对管制清单外的物项实施临时管制，因此有关数据是否属于管制物项需要依据《出口管制法》所确立的清单目录和标准来判断。值得注意的是，商务部、科技部在 2020 年修订了《中国禁止出口限制出口技术目录》，将包括人工智能交互界面技术以及语音合成技术等多项信息处理技术纳入限制出口部分，对经济活动中的技术出口行为进行限制，而未来国家出口管制管理部门是否会将相关技术以及数据直接纳入出口管制范畴仍有待观察确认。

2. 投资、贸易歧视性措施的对等措施

为更好地应对国外立法和执法，依据“对等原则”，《数据安全法》第 26 条规定了数据领域下的反制裁措施，即任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施，为我国依法反制外国歧视性限制措施进一步提供了有力的支撑，并充分体现了我国在网络数据空间主张数据主权的立法思想。

值得注意的是，除《数据安全法》下的对等反制措施外，根据《反外国制裁法》，我国还可以对外国制裁采取阻断措施，并可以对被列入反制清单的个人、组织采取反制措施[27]。

（五）以“安全开放”为目标的政务数据体系建设

数据作为关键生产要素，不仅个人信息和企业数据受到广泛关注，在后疫情时代，政务数据的价值同样不言而喻。政务数据公开既可以促进政府科学决策，提高公共管理效能，又可以增加数据要素市场的数据资源供给，盘活数据资源交易[28]。

基于此，《数据安全法》在提出对政务数据来源合法性、管理安全性以及电子政务系统安全性要求的基础上，进一步对政务数据公开进行原则性规定。具体而言，《数据安全法》明确了政务数据以公开为原则，不公开为例外的基本理念，要求在国家层面制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据的开发利用，以消除实践中普遍存在的“数据烟囱”“数据孤岛”[29]。但同时，政务数据的开放与利用条件仍有待后续配套措施的进一步明晰。

三、《数据安全法》的法规范关键合规要领

《数据安全法》为涉及数据处理活动的企业设定了包含消极义务和积极义务在内的多层次、全方位的数据安全义务群，期以规范数据处理活动，进

[25] 同上注 11。
[26] 同上注。
[27] 参见《反外国制裁法》。
[28] 刘权：政府数据开放的立法路径，载《暨南学报（哲学社会科学版）》2021 年 1 月，第 92-93 页。
[29] 同上注。

一步促进数据市场发展。经我们简要概括分析，企业需要在《数据安全法》下遵从以下几点“有所为有所不为”的基本法律要求，以在实质上降低企业的数据安全合规风险。本部分将主要针对《数据安全法》向企业提出的合法合规要求进行提纲挈领式地介绍。

（一）有所不为：法律为企业设定严守的消极义务

一方面，**企业应当坚持底线思维，在法律划定的数据安全红线以内从事数据处理活动**。简要概括来看，以下几个合规要点需要在法律过渡期和《数据安全法》正式实施后由企业保证严格遵守，否则容易对经营活动的正常开展造成较大麻烦：

1. 确保数据来源合法合规

合法合规处理数据是《数据安全法》提出的基本要求。《数据安全法》第 27 条明确规定，“开展数据处理活动应当依照法律、法规的规定”；进一步地，第 32 条第 1 款明确指出，“任何组织、个人收集数据，**应当采取合法、正当的方式**，不得窃取或者以其他非法方式获取数据。”可以理解为，该条在“合法合规”要求的基础上，向数据处理活动的源头，及数据来源的方式提出了“合法、正当”的约束性条件。

在解释上，一方面，“合法”要求说明，如特定法律法规对于数据收集和数据来源合法性进行了特别说明，即意味着需要满足该种合法性要求，最典型如个人信息收集的“告知 - 同意”原则；另一方面，“正当”同时意味着数据采集手段、方式的恰当、不过度，或者说需以合理的理性人判断可被接受的程度以进行数据处理。这种“可被预期、可被接受”不意味着对手段、方式创新的限制，而是更加侧重于保护数据源对可能被采集、处理后果与潜在影响可预期的安全价值。近期频发的企业或者个人利用爬虫、在未经多重授权的情况下进行数据爬取的案例[30]，轻则违反竞争法律受罚、重则入刑，也提醒着我们重视数据来源合法要求的严肃性与必要性。

通常情况下，数据来源的合法合规是企业固定与构筑自身数据资产的第一步，同时也是关键一步。企业数据资产的稳固与否、价值高低，均与数据来源的合法合规性密切相关。我们建议，企业可以区分数据来源进行内部审查，并采取必要的技术、组织管理或是协议措施，从数据来源这一最初环节做好数据隔离与风险排除，为后续的数据处理、数据治理体系以及资产化管理打下牢固根基。

2. 履行前置性的行政许可义务

《数据安全法》第 34 条规定，“法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。”此规定意味着，相应行业或者不同经济部门的法律、行政法规设定事前许可事项的，应当严格遵照其规定，在取得相应资质或者许可牌照的前提下开展合规的数据处理服务与经营活动。

虽然在 TMT 领域内要求经营实体进行事前的资质证照的申请可能并非是新鲜事，但值得企业注意的是，随着个别强监管的行业领域（如金融、健康医疗和智能汽车等）数据服务样态与形式的日趋丰富，经营实体所涉及数据处理服务逐渐深入，对数据处理（尤其是个人信息处理）风险的把控也渐趋困难，**不排除可能将传统经营领域内专门针对数据处理服务模块纳入监管范畴并新设许可事项**。最典型如个人征信领域内提供相关数据服务可能需通过获取牌照或者与具有牌照的实体通过协议合作的方式展开。

由此，我们建议可能涉及相关强监管行业服务的数据服务提供商紧密跟踪相关立法立规动态，在具体开展数据处理和提供数据服务前了解强制性许可要求以及潜在的审批要求，充分评估相关业务开展的数据合规风险，提前避免可能采纳的违法经营方案。

3. 谨慎处理域外冲突管辖与证据调取问题

《数据安全法》第 36 条针对可能的域外法律适用所导致的冲突管辖及其所涉及的跨境证据调取问题，提出了数据安全层面的法律要求，即“**经主管机关批准**”。

[30] 参见：（2021）豫 1403 刑初 78 号、（2020）浙 0106 刑初 437 号。

从根本上说，该条款属于回应域外“长臂管辖”所作出的防御性规定。该条所约束的对象为“境内的组织、个人”，相比于“数据处理者”显然拥有更加广泛的范围；但与此同时，我们认为“境内的组织、个人”并不等同于“依据境内法律设立的组织、拥有境内国籍的个人”，而应当与《数据安全法》规范的对象范围保持体系一致性，即在境内进行数据处理活动、且数据存储于境内的组织和个人均需受该条约束。虽然目前暂未有相应的主管部门审批程序或者成文规则一并公示，但我们认为相应的配套措施将在《数据安全法》实施后紧锣密鼓地出台，以尽快落实其维护境内数据安全的立法目标。

对于企业而言，在做好数据跨境合规意识准备的同时，也需要充分注意此后境内外因冲突管辖而造成的数据合规要求截然相反的实践困境和法律风险。事实上，受 2020 年美国《外国公司问责法案》（Holding Foreign Companies Accountable Act，HFCA）相关条款影响，此前在赴海外上市的企业证券经营活动中的冲突管辖风险已然显现，由于监管政策的不稳定性而出现了中概股退市与赴港上市的小浪潮。不过，在未有更好的解决方案出现之前，**面对客观存在的冲突监管风险，我们仍然建议在境内或者面向境内开展数据处理服务的企业仍严格遵照《数据安全法》的相关要求应对境外的跨境提交数据请求**，必要时咨询主管部门意见，保持必要沟通，否则依据罚则条款将可能面临封顶五百万元以下罚款，并被主管机关责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照的严重处罚。

（二）有所作为：搭建全面的数据处理安全与管理体系

另一方面，相较于上述相关消极性的义务规范，企业在迎接《数据安全法》生效实施的过渡期间，还可以发挥主观能动性，积极履行日常性和应急性的数据安全保护与治理义务，搭建企业内部数据处理合规体系，将数据安全与合规打造为企业经营管理、产品或服务上市的突出优势，以形成独特的数据竞争优势。

1. 常态化、全流程的数据安全保护义务

由于企业日常经营涉及大量数据收集、处理活动，因此从节约成本、提高效率的角度而言，**搭建企业内部常态化和贯穿数据全生命周期的数据安全保护体系，无疑是最经济有效的解决方案**。结合此前数据安全合规相关法律服务经验，我们提出在该体系中以下几个最为关键的合规要点：

合规要点	具体建议
建立可操作的数据分级分类办法或实践指南	数据治理的基础是数据分级分类操作，结构化数据治理框架依赖于前期基于安全与风险模型考量的数据分级分类办法。如前所述，目前在金融、通信与互联网等行业内数据分级分类管理办法已初见成型，我们建议企业在接受专业法律服务的指引下，结合行业重要数据监管规范要求，形成企业内部可落地实施的数据分级分类治理方案。
创建企业内部数据处理风险评估模型，落实安全影响评估要求	作为企业进行内外部数据保护影响评估（DPIA）的参考性规范，在前述数据分级分类标准的架构基础上，将数据处理风险囊括至数据全生命周期考虑，并严格落实数据处理记录法律要求，控制可能因数据处理这一增值过程而导致的额外风险与不利因素。此外，根据《数据安全法》第 30 条规定，重要数据的处理者还应当将风险评估报告报送主管部门。

合规要点	具体建议
采纳行业通行的数据安全技术和组织措施，履行安全等级保护义务	《数据安全法》向企业明确了采取必要技术或其他必要措施的数据安全合规义务。我们理解，对于涉及数据处理的企业而言，基于节约成本和经济性角度可考虑采购并组建相应的技术与组织安全解决方案；但对于提供数据处理服务的企业而言，由于涉及大量的数据接收与处理，应建立在此前国家网络安全等级保护制度体系的基础上，应当严格落实国家相关技术标准和组织管理标准，提高数据安全管理能力和水平。
定期或者不定期开展数据安全教育、演练或者培训	我们建议涉及数据处理活动的企业通过内部定期或者不定期的数据安全培训、数据安全事件模拟演练以及多样化的数据安全教育，以巩固和落实企业内部员工的数据安全意识与能力。

2. 数据安全事件的应急响应规范

《数据安全法》第 29 条规定，开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。该条事实上与此前《网络安全法》、网信办《国家网络安全事件应急预案》和相应法律法规和标准规范形成了衔接和过渡。一方面，在已有的常见网络安全事件（包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件）管理规范基础上，应形成企业内部数据安全事件的应对策略以及应急预案；另一方面，《数据安全法》强调从网络系统安全发展到数据及数据处理安全，亦体现了经济发展与法律规制同步，从网络层到数据层，此后将发展到算法安全的智能层治理趋势。我们建议企业尽快构建区分网络信息系统与内容、数据处理与安全、算法伦理与合规等不同维度和层次的应急管理体系。

写在最后的话

理想照进现实，《数据安全法》经历这一年多的起草、初审、公开征询意见，以及二审和三审等立法历程，成为 2020 年立法计划中进展最为快速的部门立法之一，并且将于 2021 年中正式生效实施。不可否认，限于篇幅与体系，《数据安全法》仍然为一些问题留出了空间，有待实践经验的积累、丰富、提炼和总结。但作为我国数据领域内的“基础性法律”，给予尊重、保护以及依此不断提升数据安全合规质量，才是我们对待全新的数据安全立法的端正姿态。

此外，作为对国际数据竞争和数据主权化浪潮的及时回应，《数据安全法》已然建立起了一道屏障。靴子落地、利剑出鞘，这部数字时代的法律为我们锻造和提供了更好保护企业数据安全与资产利益、国家稳定与长足发展的武器，接下来摆在人们面前最为关键的问题，便是学会如何在纷繁复杂的数据市场竞争中游刃有余地“亮剑”。

感谢实习生姚敏侣对本文所做的贡献。

个人信息保护立法效果、理念及价值平衡——欧盟GDPR生效实施三周年比较与前瞻

宁宣凤　吴涵

引言

当格林尼治的时针指向2021年5月25日，欧盟《通用数据保护条例》（General Data Protection Regulation，“GDPR”）生效实施就已正式届满三周年。回顾这三年，在欧洲数据保护委员会（European Data Protection Board，“EDPB”）以及各成员国数据保护机构的共同努力下，欧盟司法辖区内的个人数据保护法律框架已渐趋成熟，并以一个统一体的姿态更加自信地向“数字主权”和“数字单一市场”的重要立法目标迈进。[1] 三年来多个国家参考借鉴GDPR的立法技术，但更值得重视的是GDPR背后蕴含的个人信息保护理念和价值倾向可能将更为深刻地影响全球数字时代的发展与监管方向。

在地球的另一端，我国个人信息保护立法顶层设计步稳蹄疾，在不久后尘埃落定[2]。北京时间2021年4月28日，《中华人民共和国个人信息保护法（草案二次审议稿）》（以下简称“《个人信息保护法》二审稿”）在中国人大网全文发布并公开向社会征询意见[3]。在历史与现实的交汇点上，我们不禁思考：应当如何站在全球数字经济发展的视角看待个人信息保护立法与执法的走向？在数字化尚未完全落地，智能化提前进场的复杂经济和社会变革阶段，个人信息中蕴含的人格权益与商业价值应当如何在法律规范的下取得精妙的平衡？企业又该如何自如地应对其中潜在的挑战，化风险为动力、趁势而上挖掘数据价值把握竞争优势？

本文试从GDPR三周年来出现的现实问题以及立法理念出发，对比观察我国包括《个人信息保护法》在内的立法动向，与大家一同探讨个人信息保护的核心价值与监管技术。

[1] Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889，最后访问日期：2021年5月22日。
[2] 申佳平：《增强顶层设计 我国个人信息保护立法步稳蹄疾》，转引自“人民网” http://it.people.com.cn/n1/2020/1223/c1009-31976314.html 最后访问日期：2021年5月22日。
[3] 个人信息保护法（草案二次审议稿）征求意见，http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b35d78b4eb4 最后访问日期：2021年5月22日。

一、个人数据保护法律的目标效果与现实回应

欧盟 GDPR 立法者一样十分关心这部个人数据保护统一立法在实际运行中的效果与问题，注重来自行业上下和欧盟内外如何看待这部法律的声音与意见。

（一）高度认同个人数据保护法律的基本价值

GDPR 生效两周年时即经历了首次内部评估。2020 年 6 月欧盟委员会正式发布了官方报告（中文译名大致为《保护数据作为增强公民权利以及实现欧盟数字化转型的基础——GDPR 生效实施两年》）[4]。而就在三个月前，欧洲议会又高票通过了《欧盟委员会关于 GDPR 实施两年后执行情况的评价报告》。在该份报告“一般性意见（General Observations）”章节中，欧洲议会认为 GDPR 总体上是成功的，并且同意欧盟委员会的观点，认为现阶段尚无更新或再度审查 GDPR 的必要[5]。由此可见，GDPR 在个人数据保护领域内所发挥的作用和价值，获得了以考察人权状况为主的欧盟唯一直选议会机构的认可。**在 GDPR 生效实施三周年之际，官方的立场已经鲜明地高度赞同了 GDPR 在个人数据权利保护的法律价值与实际影响力**。

可以预见的是，个人数据得到更高层级保护时，其几乎必然会影响当前数据经济产业的发展。GDPR 自诞生以来一直备受产业争议，尤其是批评 **GDPR 的强监管态势和严格的惩罚性举措可能极大地阻碍世界互联网的进步与发展等**[6]。相关意见尤见于原先采取另一种个人数据保护模式的美国产业研究机构或者专家观点。美国国家经济研究局 2018 年公开发表《GDPR 对科技创业投资的短期影响》一文，从经济学视角对 GDPR 给欧洲科技行业带来的负面影响进行了实证分析[7]；而在 GDPR 实施一周年之际，美国智库——信息技术和创新基金会（Information Technology and Innovation Foundation, ITIF）发布了《GDPR 实施一年以来的影响》报告，并在报告中通过调研数据指出 GDPR 立法“损害了欧洲科技创业公司，降低了数字广告行业的竞争力”[8]。

然而，考虑到美国相关产业秉持数据自由流通价值至上倾向，我们需要更为客观和历史的眼光来看待 GDPR 的实施效果。不可否认个人数据保护立法对于依赖于数据生产要素的数据经济发展造成阻碍。但同时我们需要思考基于个人数据“滥用”发展的数据经济是不是“空中楼阁”。一旦个人数据滥用造成的社会影响超过数据经济发展的价值，理论上将不得不对已经发展到一定阶段的商业模式“拨乱反正”，纠正成本将大大增加。此外，GDPR 的立法思路已经被多国借鉴，必将影响全球企业的数据保护以及数据利用的方式，其意义之一在于输出相对通用的标准。在全球数据保护基本规则和监管工具趋同的前提下，欧洲企业关于个人数据保护的“先行先试”至少将使得欧洲企业在未来“绿色”数字经济发展中占据“道德高地”以及“先发优势”。

因此我们不排除当前欧洲数据经济发展的滞塞仅仅是**数字化与智能化产业合规发展成熟必经的“阵痛期”**，我们仍然相信只有在法律框架约束下有序、自由的数字服务市场，才能够在尊重数据主体基本权益的前提下，更好地创造社会财富，形成真实、稳定与可持续的产业竞争力，我们也期待《个人信息保护法》正式生效后，国内企业的合规努力不仅将进一步推动中国数字经济的发展，也会增加企业和国家的国际竞争力。

（二）充分重视数据保护执法能力的客观限制

GDPR 执法状况成为目前欧盟数据保护领域内的主要关切。**归总来看，执法工作质量参差不齐、行政处罚案件与投诉的跟进不力、采取措施的反应时限与执法周期过长，以及执法机构的能力建设相较落后等问题，成为困扰欧盟 GDPR 实施效果的关键矛盾**。

[4]Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 最后访问日期：2021 年 5 月 22 日。
[5]Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html 最后访问日期：2021 年 5 月 22 日。
[6] 沈建光：《“惩罚性”监管有碍创新与增长——从欧洲 GDPR 谈起》，https://www.iyiou.com/news/20191017115624 最后访问日期：2021 年 5 月 23 日。
[7]THE SHORT-RUN EFFECTS OF GDPR ON TECHNOLOGY VENTURE INVESTMENT, 原文链接可见：https://www.nber.org/system/files/working_papers/w25248/w25248.pdf 最后访问日期：2021 年 5 月 23 日。
[8]What the Evidence Shows About the Impact of the GDPR After One Year, https://datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/ 转引自“CAICT 互联网法律研究中心”公众号，最后访问日期：2021 年 5 月 23 日。

此前，部分欧盟成员国家（如奥地利、保加利亚）提出 GDPR 设置的过低投诉门槛和大量重复投诉严重妨碍了监管部门的正常运作，强大的数据主体权利也给执法带来了巨大现实压力[9]。而根据上述提及的官方报告，目前有至少 21 个欧盟成员国的数据保护监管部门明确表示缺乏充足的人力、技术和财政支持以完全实现 GDPR 的各项监管权力与职责。一系列数据与摆在欧盟面前的实际问题，均体现出了个人数据保护执法能力保障的必要性和重要性。

相对应地，我国在个人信息保护过程中也高度重视执法落实的问题。《个人信息保护法》二审稿针对第 61 条进行了部分修订，明确了网信部门在部分规则与标准领域的制定工作中的统筹地位、工作职责。在 GDPR 的经验引鉴之下，明确个人信息保护机构及其职责，专门从事个人信息保护的日常监督、管理、执法、评估等工作，并定期对我国个人信息保护状况进行汇总并向公众通告[10]，有助于提升个人信息保护的法律贯彻执行力度，已成为实践中我国秉持的一项常态化工作内容。

此外，随着大数据、神经网络、机器学习等技术的飞速发展，如何穿透数据及新型技术的迷雾，有效地监管新型业态，将成为所有监管机构亟须解决的难题。因此我们理解，重视执法专业团队组建与技术能力建设的同时，可能需要在必要时引入外部独立机构的能力支持，动员社会力量，一方面避免因资源保障不到位而可能导致被动局面，另一方面也防止僵化执法以实质性阻碍新型业态的发展。

（三）有效执行对大型数字平台和综合性公司、数字服务的数据合规监管

欧盟在对 GDPR 进行内部评估的过程中，充分关注到了综合性大型数字服务平台的个人数据监管问题，**尤其是针对在线广告、精准定位、算法自动化决策与用户画像、内容推荐等互联网技术与商业营销手段的使用方式问题上。**就 GDPR 条文本身而言，其分别在第 21 条和第 22 条以赋予数据主体拒绝权的方式，应对可能因直接营销（direct marketing）以及自动化识别分析（profiling）等带来的潜在不利影响与危害。但在评估中欧盟认为仍需要通过更为有效地执行相关制度和规则，以进一步落实对大型数字平台、综合性公司以及采纳相关技术提供数字服务的市场主体的监管。

此外，2020 年底，欧盟委员会发布《数字服务法》（Digital Services Act）和《数字市场法》（Digital Markets Act），两部法律分别从互联网服务和市场竞争两个维度，对欧盟境内或者向欧盟提供的互联网服务进行了重点规制。“社会和经济的加速数字化创造了这样的现实，即一些大型平台控制着数字经济中的重要生态系统。他们成为了数字市场中的守门员，并具备了担任私主体规则制定者的能力。”[11] 因此，《数字服务法》中定义了月活用户超过 4500 万的“超大型平台”的更高法律义务，如内容审查、报告审计和透明度等；《数字市场法》中还要求满足“守门人”（Gatekeeper）条件的大型平台企业向用户开放数据的权限等额外责任[12]。

在法律层面强化大型平台数据保护法律义务也成为了我国《个人信息保护法》二审稿中的一大备受关注的亮点。二审稿中新增的第 57 条为“提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”增加了如“独立审计”和“发布社会责任报告”等强制性义务。虽然目前尚无相关配套法规与规范性文件说明该条所约束的具体适用主体和对象，**但可以预见的是，为了防范平台型企业利用其双边市场地位下传导效应可能形成的垄断倾向[13]，并滥用这种由数据和技术竞争力和供需市场关系中的信息对称差产生的优势地位，法律从个人信息保护的立场出发，进一步作出数据处理、共享的限制，强调数据主体的合法权益乃是未来趋势。**而对于掌握数据资源和市场优势地位的平台型企业而言，提前做好数据合规准备、不断提高数据处理的透明度和算法合规性，才是正视数据合规与执法挑战的明智之举。

在《个人信息保护法》二审稿中，还有一点值得数据保护领域人士关注，即新增**由超大型平台成立由外部成员组成的独立机构对个人信息处理活动**

[9] 王融，朱军彪：《GDPR 两周年：来自欧盟内部的反思与启示》，转引自“腾讯研究院”，https://www.tisi.org/14590 最后访问日期：2021 年 5 月 22 日。
[10] 刘玉琢：《欧盟个人信息保护对我国的启示》，载《网络空间安全》2018 年第 7 期，第 42 页。
[11] EU Commission: The Digital Services Act package，https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package 最后访问日期：2021 年 5 月 23 日。
[12] The Digital Markets Act: ensuring fair and open digital markets, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en 最后访问日期：2021 年 5 月 23 日。
[13] 冯源：《互联网领域优势传导效应与反垄断规制——以双边市场为视角》，载《网络法律评论》2015 年第 2 期，第 177 页。

监督的相关规定。尽管目前对于如何组建外部成员组成的独立机构还尚未有任何的指引文件，但利用独立机构监督管理在其他法域并不少见，比如反垄断执法领域中存在多年的“监督受托人”机制，就是平衡监管者、监管对象和独立监督机构关系的成功先例。

（四）宽严相济：关注中小企业豁免与市场竞争利益失衡问题

GDPR 并不是一部仅仅保护个人数据的法律，且与市场竞争有着不可分割的关系。已有研究揭示，随着 GDPR 的出台，在许多网络技术市场上占主导地位的公司——谷歌公司的市场份额增加了，而所有其他提供网络技术的公司要么没有被观察到市场份额的变化，要么遭受了损失。“监管隐私会对市场结构和竞争产生意想不到的后果——网络技术市场集度的提高，可能是 GDPR 后果中一种意料之外但有不可避免的现象。”[14] 此外，以免费互联网模式最主要的创收来源——广告投放行业的调查结果为例：GDPR 实行后，谷歌及 Facebook 等大平台的竞争力增强。谷歌及 Facebook 控制着 3/4 的数字广告开支，拥有大量资金和研发能力，于是很早就开始着手应对 GDPR 和提前采取合规措施，广告主们倾向于相信其能力而乐意在其平台上投放广告，以确保互联网广告投放的合规性与安全性 [15]。

在数字市场领域内的客观竞争现状，也可能带来对众多中小平台的打击效应。由此，**这一点也理所当然地联系到了 GDPR 实施效果中的另一个关键问题——对中小企业的特殊豁免政策尚未得到完全落实。**例如，荷兰监管机构在执法实践发现：即使最小规模的企业，也普遍采用了软件的方式来收集处理相关数据。德国指出，对于其核心业务并不是数据处理活动的中小企业、协会等机构，应简化 GDPR 中规定的数据处理记录、设立数据保护官（DPO）等义务。这一建议的基本考虑是这么一种事实，即在欧洲 99% 以上的企业是中小型企业（员工少于 250 人的企业）[16]。

由上可见，GDPR 在实施过程中显露出对中小企业的合规责任过分苛责，导致影响市场创新活力的现实问题。在市场经济自由配置市场资源，尤其是配置互联网生产力资源的同时，大力支持中小企业发展，将更有利于体现市场竞争的公平性，促进数字服务市场健康持续发展，警惕一项立法可能在客观上人为制造的“马太效应”。

因此，**在基本的个人信息保护法律原则和规则框架内，适度考虑对不同份额和技术特征的数字服务市场主体进行差异化监管**，或许是我们能从 GDPR 生效三周年获得的启发。从个人数据安全所可能导致的实质威胁角度而言，区分非数据驱动型企业的数据保护义务和以大数据、自动化算法技术等为核心竞争力的市场主体的数据合规监管重点或是处罚门槛，或许可以进一步符合个人信息保护立法的价值取向。此外，对于同在数字服务市场范围内的数据处理者而言，根据数据保护影响评估的客观结果，尽可能避免一刀切的隐私监管政策而可能形成的非公平的数字服务市场竞争秩序。

二、个人数据保护法律的域外效力与风险应对

（一）国家层面积极立法，回应监管工具输出与“长臂管辖”效应

在全球个人数据保护法律框架体系内，由于 GDPR 被认为是全球性隐私监管的最高标准与准则，故而成为了欧盟向其他国家或者地区输出的数据合规监管工具。在这个由 GDPR 提供的监管工具箱内，包括数据处理合法性（第 6 条）、数据处理协议 DPA（第 28 条）、数据保护影响评估 DPIA（第 35 条）、数据保护官制度（第 37-39 条）以及数据跨境传输机制（第 5 章）等均成为监管机构的具体执法手段。

上述执法工具箱加之 GDPR 的域外适用效力，对全球范围内的个人和企业都形成了实实在在的“长臂管辖”效应。GDPR 第 3 条以及 EDPB 相对应发布的《域外适用指南》[17] 都对其域外适用的对象与范围进行了相应的解释与界定。归总而言，满足“设立商业实体”（establishment）或者“针

[14]Christian Peukert, Stefan Bechtold, Michail Batikas, Tobias Kretschmer: Regulatory export and spillovers: How GDPR affects global markets for data, https://voxeu.org/article/how-gdpr-affects-global-markets-data , 转引自“数字经济与社会”公众号，《前沿译文 | 欧盟 GDPR 如何影响全球数字经济？》，https://mp.weixin.qq.com/s/WJlRrX2uG2sy05PPg1hD8w 最后访问日期：2021 年 5 月 23 日。
[15]Adtime：《面对越来越严格的隐私法律，数字营销该何去何从？》，转引自“新浪财经头条”，https://t.cj.sina.com.cn/articles/view/3212340783/bf786e2f027009u1a?cre=tianyi&mod=pcpager_fintoutiao&loc=2&r=9&doct=0&rfunc=100&tj=none&tr=9& 最后访问日期：2021 年 5 月 22 日。
[16] 王融，朱军彪：同上注 [10]。
[17]Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en 最后访问日期：2021 年 5 月 23 日。

对性提供服务”（targeting）等相关要求，欧盟境内外从事个人数据处理活动的相应主体均有可能成为其管制的具体对象。在“数据隐私作为一项基本人权不受时空地域限制”的法理念支撑下，凭借GDPR强大的域外管辖法律效力，欧盟数据保护主管机构天然地被授予了一项可以实际行使“长臂管辖”的权力，但毋庸置疑对全球数字服务市场内的隐私监管、商业战略设计与执行产生了本质影响。

就本文观察来看，已有的相关研究[18]以网站的Cookie设置为主要观察对象，GDPR的生效实施影响了全球范围内设立于欧盟境内外网站引入第三方技术服务商提供数据合作的数量和意愿，在为境内外客户提供日常数据合规服务的过程中，我们也存在一个非常直观和鲜明的感受：以全球化经营为长期战略愿景的公司一般会倾向于选择提前将GDPR规则作为前置性合规要求，无论其业务是否已经实质或者潜在地落入了GDPR的管辖。尽管由此造成了合规资源的浪费和合规成本的不合理增加，但简言之，欧盟通过单方面的数据隐私监管法规和执法动作，充分发挥了其在全世界范围内针对个人数据处理企业和个人法律监管的外部性。

因此，在个人数据保护法律中，目前国际通行的法律规则似乎始终在宣示“效果原则应当成为属地原则的补充、扩大法律域外效力”成为普遍共识[19]。回观近期公布的《个人信息保护法》二审稿，在适用范围条款上保持了此前草案一审稿的做法，以约束境内个人信息处理活动为主，但保留了必要的域外适用管辖接口和空间。我国《个人信息保护法》二审稿第3条规定了三种发生在境外处理个人信息的活动也接受本法管辖的具体情况，分别为“以向境内自然人提供产品或者服务为目的”“分析、评估境内自然人的行为”以及“法律、行政法规规定的其他情形”。相比于GDPR广泛的域外适用和难以清晰界定的现状来看，我国法律更为清楚明确地以“主观意图”和“行为效果”作为主要判断标准，在考虑实际执行可能性的基础上相应扩大了域外适用范围。尤其是“主观意图”的标准，正好切中了此前GDPR评估中“针对性”标准过于广泛所带来的执法难以落地的实际问题，即只要向欧盟境内提供服务的客观性满足，忽视了提供服务的主观性要求，使得一些偶发性的个人数据处理活动也被纳入了不合理的监管范畴，影响了执法的落地执行力。

总体而言，为了防范个人数据域外监管可能带来的不利影响，主动保护境内自然人或者企业在参与全球化数据竞争合作中的合法利益，我国个人信息保护立法以更为主动的姿态，在GDPR的基础上进一步完善个人信息保护的域外适用规则，是在国家总体安全观战略定位下兼顾数据安全与流动、强化数据主权与执法效力的积极回应。

（二）企业层面提升合规，注重全球化数字经营战略部署

可以预见，当GDPR成为具有国际示范乃至通行效力的监管工具输出至其他国家和地区，以及凭借其广泛的域外适用效力，致力于出海提供互联网信息服务的全球化公司不仅需要适应和满足基本的数据合规要求，还应当在GDPR规则下积极探索有利于展开全球化合规经营的市场战略模式。

对于这一点而言，由于欧盟GDPR生效实施三周年过程中，欧盟境内各国数据保护机构曾作出了不少处罚案例，其中对于谷歌、Facebook等巨头互联网企业的关注和处罚事实，也引发了不少对个人数据保护规则有效运用和风险应对的积极启示。其中较为具有代表性的就是谷歌公司就“一站式机制”的管辖异议诉法国数据保护机构（CNIL）案件[20]。该案中谷歌公司因涉嫌缺乏数据处理透明度而受到CNIL的行政处罚。但该案被人们关心的重点问题是，谷歌公司以其欧洲主要实体（main establishment）设置在爱尔兰，而要求上诉法院（法国最高行政法院，the Council of State）审查CNIL是否具有管辖权。该案涉及了GDPR下对各国数据保护机构监管一致性机制——“一站式机制”[21]（one stop shop mechanism）的解释问题。最终法院经审查认为，由于谷歌公司爱尔兰欧洲总部事实上并无对其他子公司的控制和决定权，因此导致谷歌公司不被认为在欧盟境内设立了主要实体，CNIL不受限于“一站式机制”反而基于域

[18]Christian Peukert, Stefan Bechtold, Michail Batikas, Tobias Kretschmer: Regulatory export and spillovers: 同前注 [11]。
[19] 张建文，张哲：《个人信息保护法域外效力研究——以欧盟 < 一般数据保护条例 > 为视角》，载“大数据和人工智能法律研究院” https://mp.weixin.qq.com/s/acvmzME-74OHUD-2_xjpjw 最后访问日期：2021 年 5 月 23 日。
[20]EU: How CNIL fined Google - insights on the One Stop Shop mechanism, https://www.dataguidance.com/opinion/eu-how-cnil-fined-google-insights-one-stop-shop 最后访问日期：2021 年 5 月 23 日。
[21]GDPR 由于需要协调各国执法的一致性，因此设立“一站式机制”，简言之即当某监管对象在欧盟司法辖区内任意成员国设有主要实体（main establishment），则该成员国境内的监管机构将获得监管执法的主导权。

外管辖效力享有对谷歌公司的行政处罚权。

上述案件一锤落音后，**我们理解欧盟数据保护机构对于 GDPR 的域外适用以及何为境内设立主要实体的认定遵从于实质且动态的过程**。从事后角度来看，给予出海企业涉及欧盟地区的全球化运营思路的启发至少有两点：其一，明确欧盟境内主要实体并赋予其符合 GDPR 下认定主要实体的商业决策权，主要是个人数据的处理决定和对欧盟境内其他关联主体的控制权；其二，注重 GDPR 域外管辖的兜底效力，尤其是在企业不被认定为在欧盟境内设立主要实体的情形之下，广泛的“针对性提供服务”（targeting）标准就将成为口袋执法工具“粉墨登场”，成为企业全球化运营数据合规的主要风险。而这对于此前出海企业习惯性的离岸远程运营开展全球化数字服务的商业模式而言，显然已经不足以规避 GDPR 所必然可以实现长臂管辖的具体情形。为了避免由于长臂管辖带来的境内外法义务冲突问题，企业进行必要的数据隔离与架构独立，一定意义上或将成为应对与化解风险的可行路径。

三、个人数据保护的挑战与国际协作

（一）多样化提供个人信息处理合法性依据，灵活满足现实需要

在 GDPR 生效实施的第二个年头，便遇到了来自 COVID-19 的严峻挑战。这一场突发性公共卫生事件中，GDPR 所内含的个人数据保护与基于公共利益需要而产生的数据处理目的产生了极为激烈的价值碰撞，也因此不断考验着欧盟个人数据保护法律的韧性和灵活度。

归结起来，现实的困难主要来源于 GDPR 个人数据处理的合法性依据规定过窄，即 GDPR 以“数据主体同意”为主要的合法性依据而建构，个别例外规定都难以作为在疫情中强制获取个人数据的合法性依据。2020 年 4 月 8 日，欧盟委员会发布《关于新冠疫情中利用移动数据和应用官方建议》[22]，并于 4 月 17 日进一步发布配套的《支持抗击新冠疫情的 APP 的数据保护指引》[23]，准备和使用统一的移动应用程序、政府主动介入参与以解决个人数据处理的安全性忧虑；此外，EDPB 主席也通过发布官方声明[24]，表示 GDPR 已经为 COVID-19 下官方机构处理个人数据提供了依据，并不妨碍个人数据保护规则的执行。但事实上，各国公民对公共卫生事件带来的隐私保护冲击敏感性不同，尤其是在公共利益与个人隐私之间的平衡度把握上存在较大差异，导致欧盟内部数据保护的执法步调、举措等都难以协调一致。

鉴于 GDPR 存在的客观反映，这一场全球性的突发公共卫生事件，一定程度上也对国内个人信息保护立法产生了实际影响。《个人信息保护法》二审稿延续了此前草案一审稿的规定，更新了《网络安全法》下仅将“个人信息主体同意”作为合法性基础的做法，在第 13 条中新增了新的合法性依据，尤其是“为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需”明确作为其中的一项情形。此外，草案二审稿为了与此前《民法典》相关规定保持一致，此次修改补充了“依照本法规定在合理的范围内处理已公开的个人信息”这一合法性依据。我们认为，不再拘泥于“告知 - 同意”这一过于单纯或理想化的框架设计隐私监管规则，而是更加服从于个人信息保护立法落地的实际需要，并且参考“风险控制路径”[25]、强调评估个人信息保护风险的方式，也是从这场对于全人类而言的灾难中所可能参透的一点教训。

（二）主动应对数据主权浪潮，完善跨境提供规则，寻求国际协作

2020 年内，影响 GDPR 在全球范围内的规则运行的第二个重要事件便是欧盟法院对欧盟 - 美国“隐私盾协议”无效的宣告。这是继 2015 年以来法院第二次推翻欧美之间数据传输及使用协议。[26] 但在无效宣告中，欧盟法院仍然维持并确认了 GDPR 规则下标准合同条款（Standard Contractual Clauses, SCCs）的有效性。“隐私

[22]Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps, https://mp.weixin.qq.com/s/rQJ-IRLX19c-ScYweb41zg 最后访问日期：2021 年 5 月 23 日。
[23]Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29 最后访问日期：2021 年 5 月 23 日。
[24]Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak, https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en 最后访问日期：2021 年 5 月 23 日。
[25] 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期。
[26] 商务部：《欧盟法院裁定欧美“隐私盾”协议无效》，http://eu.mofcom.gov.cn/article/jmxw/202008/20200802993103.shtml 最后访问日期：2021 年 5 月 23 日。

盾协议”被宣告无效，再度触碰了欧盟和美国两个司法辖区下不同的个人数据保护立法价值观念。但尽管如此，正因为此前由于白名单国家范围过小、数据跨境传输成本过高而导致全球性数据交换成本居高问题，招致了包括德国、比利时等在内的成员国的批评[27]。欧盟仍在积极认定数据跨境传输与流动的白名单国家，最近的消息表明，韩国或将成为欧盟认定下的“充分性保护水平”国家[28]。

事实上，在经济全球化、网络化的时代，个人数据的跨境流通不可避免。GDPR 严格限定充分性保护水平国家以及跨境传输规则的使用，一定意义上意味着对未来国际经济树立了一道无形的法律屏障，成为今后国际贸易摩擦和谈判的重要内容。[29] 面对愈发明显的数据主权全球化浪潮，**对于境内的个人信息保护而言，在确保数据主权的前提下，通过降低企业数据跨境可能的规则执行成本，使得个人数据在合适、必要和充分安全的环境中得到流动成为今后立法与执法的主要目标**。《个人信息保护法》二审稿第 38 条：通过新增国家网信部制定标准合同，一方面降低企业在数据跨境时支出的额外合规成本，另一方面以保持相对安全的数据跨境传输协议控制水平，体现着立法者达成上述目标的努力。

此外，我们认为不能想当然地将《个人信息保护法》二审稿中第 1 条中删去“保障个人信息依法有序自由流动”的条文改变，解读为立法已经持有否定数据跨境传输的基本态度。相反，我们同时也要注意到，草案二审稿对一审稿的第 12 条进行了沿用和保留，将“国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认”作为总则章节下的一项原则加以规定，以体现出个人信息跨境安全流动的法律价值取向。

四、个人数据保护法律的价值平衡与立法艺术

GDPR 生效实施的三年来，欧盟进一步加强个人数据权利作为一项基本人权的保护。我们也逐步认识到，**在本文谈及的诸多个人信息保护规则上与 GDPR 存在的客观差距，究其根本都来源于其背后的立法价值理念的根本差异**。由于人类正在依赖高速发展的互联网和人工智能技术，加速向下一个智能化的人类纪元迈进，这种根源于立法价值取向的不同，形成了如今基于个人数据而生长、丰富和成熟的产业模式的巨变与割裂。而如何继续维持互联网设计之初的“全球互联互通”愿景，成为各国在个人数据保护立法和隐私监管政策的出台制定时所必须严肃正视的问题。

欧盟向来将个人数据受法律保护作为一项基本人权加以规定，由此才有了 GDPR 作为全球最高个人数据合规最高要求和标准的法理基础。[30] 根据《欧盟基本权利宪章》（EU Chapter of Fundamental Rights）第 8 条，以及作为《里斯本条约》（Lisbon Treaty）一部分的《欧盟运行条约》（Treaty on the Functioning of the European Union）第 16 条，个人信息保护权是欧盟公民的一项宪法性权利。[31] 基于此，我们才不难以理解 GDPR 项下为个人数据控制者和处理者所附加的严格义务。

但客观上而言，个人数据主体过度和无限制的绝对权和控制权，对于法律天平另一端的依赖个人数据分析挖掘的产业利益，就将形成更为现实的打击。**不断强化的个人数据主体基于其个人数据所掌握或享有的权利，必然将导致数字服务市场主体基于生存压力而主动寻求商业模式的转变**。而最先体现出这种改变的消极效应，应该是全球的互联网广告行业。举例而言，近期某国际终端设备制造商操作系统已经开始实行“隐私新规”，其赋予所有用户以事前主动选择开启或者关闭跟踪工具以获取设备广告标识符（在 GDPR 下符合“识别 + 关联”的个人数据的定义）的自主权利。这种理想化的隐私设计完全符合 GDPR 的合规要求，但几乎必然会损害赖于设备广告标识符而形成的互联网广告行业的经营利益。近期，该操作系统开发公司向两家境内应用开发者发出邮件警告，要求限期 14 天内完成版本更新以符合其隐私新规。[32] 而被要求限期整改的内容，正是此前互联网广告协会联合多家单

[27] 王融，朱军彪：同前注 [10]。
[28] European Commission: Adequacy decisions-How the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en 最后访问日期：2021 年 5 月 23 日。
[29] 高富平：《个人数据保护和利用国际规则》，法律出版社 2016 年 9 月第 1 版，第 135 页。
[30] EDPB: Data Protection, https://edps.europa.eu/data-protection/data-protection_en 最后访问日期：2021 年 5 月 23 日。
[31] 参见刘泽刚：《欧盟个人数据保护的“后隐私权”变革》，载《华东政法大学学报》2018 年第 4 期。
[32] 凤凰网：《A 公司警告中国开发者：不要尝试绕过新隐私功能》，https://tech.ifeng.com/c/84jSB4UCAlF 最后访问日期：2021 年 5 月 23 日。

位共同制定的基于 CAID（一种可变广告标识符）的替代性底层技术方案。而该种替代性方案，已经通过多种技术手段和管理要求，一定程度上降低用户的个人信息风险。尽管对于 CAID 方案是否符合法律法规要求尚不明确，但如果基于该操作系统开发公司全部推行落地隐私新规，将尤其对未能掌握大数据用户画像库的中小型互联网广告市场主体带来毁灭性的打击。基于“免费服务”+“个性化推送”的经营模式也将面临近乎颠覆性的变革，此前长期的市场流量与获客战略，不计其数的技术研发投入与市场投放成本，已经使得原本采取免费互联网创收模式的竞争玩家难以轻松地实现盈利模式的转型。

基于个人数据保护领域的立法空白与实践混乱，我们目前仍需要不断强调与突出个人信息保护的积极意义与法律价值，也不断地在各个角度寻求其基本的法理基础与权利来源[33]。但与此同时，我们还需要对这样一种事实保持清醒的认知，即评价包括个人信息保护在内的任何一项法律制度良善与否的重要标准，就在于其是否精妙地平衡了各种值得追求与需要权衡的多样价值。我们也应当完全理解，个人信息保护是立法追求的重要目标，但绝非是唯一目标。如果脱离社会生活实际，在个人信息保护问题上一味追求“理想化”和“高标准”，对社会整体福祉和个人信息主体所可能接受因互联网产业发展带来的福利而言，也未必会产生积极效果[34]。我们期待即将迎来全面的个人信息法律保护时代，我们的立法立规、合法合规活动，都将更好地在我们迈向智能化时代的过程中，在值得追求的社会价值保护上展现法律衡平的最佳艺术。

结语

回顾、反思欧盟 GDPR 制定、颁布与执行的三周年历程，其对于提高全球个人数据保护水平、保障个人数据主体享有合法权益同时促进规范数字服务产业的竞争秩序与行业规则，都具有国际社会公认的积极和正面的示范效应。不难预见，未来的 GDPR 仍将在较长的一段时间内继续发挥其个人数据保护的法律功能，并且在大型平台数字服务的算法透明度与市场竞争规制、新技术应用下个人数据处理的风险识别、个人数据主体权利的可落地性以及个人数据跨境规则的全球性图谱探索等方面，引领着国际互联网和数字服务企业进一步注重个人数据的合法合规处理与商业化运营。

更值得期待的是，我们也即将迎来全面的个人信息保护全新时代，我们建议企业密切关注其中的立法动态以及规则演变，也寄希望于向同仁们传达个人信息保护立法立规背后的理念与价值。我们心怀人类社会智能的远大宏景，也执着于脚底每一步迈出的数据合规要领，以更为坚实地理解、贡献和拥抱互联互通的美好数字图景。

感谢实习生姚敏侣对本文做出的贡献。

[33] 参见王锡锌，彭錞：《个人信息保护法律体系的宪法基础》，载《清华法学》2021 年第 3 期。
[34] 参见薛军：《苹果隐私新政背后的利益衡量需引起关注》，载“法治日报”http://views.ce.cn/view/ent/202104/14/t20210414_36470908.shtml 最后访问日期：2021 年 5 月 23 日。

数字征信时代的重要信号
——征信业务新规草案解读

宁宣凤　吴涵　陈胜男　颜婷婷

2021 年 1 月 11 日，中国人民银行发布了《征信业务管理办法（征求意见稿）》（下称“新规草案”）。这是继《征信业管理条例》及《征信机构管理办法》颁布生效后，征信行业在快速发展的数字征信时代，即将迎来的一项重要新规，有望对不断涌现的征信新业态在规范层面做出澄清和回应。纵观规则全文，本次新规草案凸显了征信业务监管思路的重要变化，一方面从适用和管辖角度有意扩宽征信行业的规制范围，另一方面着重强调信用信息收集与应用、流转方面的合规要求，从而促进征信行业发展和信息主体合法权益保护层面实现平衡。此外，随着数字征信行业时代的到来，不断有新的业态参与到整体的征信业务生态，新规草案也对征信行业的新技术应用、征信业务相关参与主体提出原则性要求。

总的来说，新规草案不但对征信机构及征信生态提出更具体的要求，同时对于“类征信”行业也会有肃清和规范的效果。具体而言，有以下问题值得业内关注。

一、境外征信业务主体也可能受到管辖？

新规草案第二条规定了适用本办法的两种情形：

- 在中华人民共和国境内，对个人和企业、事业单位等组织（以下统称企业）开展征信业务及其相关活动的，适用本办法。
- 在中华人民共和国境外，对中华人民共和国居民（自然人和法人）开展征信业务及其相关活动的，也适用本办法。

《< 征信业务管理办法（征求意见稿）> 起草说明》（下称“起草说明”）制定原则部分明确表明新规草案“充分吸收《民法典》《网络安全法》《消费者权益保护法》等现行法律法规有关个人信息保护的内容，充分考虑与《个人信息保护法（草案）》的衔接工作，吸收相关立法原则和精神，细化个人信息保护力度”。新规草案该条规定相比之前《征信业管理条例》（下称“《条例》”）第二条[1]明确了其域外适用的效力，与《个人信息保护法（草案）》的管辖规则思路相类似。[2]一定程度上体现了新规草案与现行法律法规相衔接的制定原则。

如何理解“对中华人民共和国居民（自然人和法人）开展征信业务及其相关活动”，可能需要基于征信业务及相关活动的核心内容来做具体分析。一方面，征信业务涉及信用信息的收集和处理，而另一方面涉及基于该等信用信息对外提供征信服务。新规草案将位于中国境外面向境内主体开展上述征信业务相关活动纳入监管，条款中使用“居民”而非“公民”这一概念也在明确新规草案域外效力所涉及的对象范围。新规草案这一适用范围上的延伸与发展，均或多或少向拟在中国境内从事征信业务的境外主体释放了明确的信号：一旦新规草案生效，执法部门对于该等境外机构将具备更加明确的监管抓手，而一旦境外主体被认定为构成从事征信业务，则将不可避免面临我国征信行业监管设定的一系列准入条件和合规要求，例如向国内有关监管部门办理备案、许可审批，同时还需要考虑根据新规草案第三十五条等的要求，进行数据本地化的业务部署等等。

二、征信与类征信业态的界限更加清晰？

在新规草案发布之前，对于“征信业务”的理解往往停留于《条例》第二条所述“对企业、事业单位等组织（以下统称企业）的信用信息和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动”，而对于“信用信息”并未清晰界定。因此在实践中，出现多种比如反欺诈、智能风控决策、信用咨询等类征信业务生态。此次新规草案尝试从“信息类型”和“服务类型”两个角度对“信用信息”和“征信业务”这两项对于征信活动而言最为关键的“识别要素”的边界予以进一步的澄清。

（一）信用信息

根据新规草案第三条的规定，信用信息是指“为金融经济活动提供服务，用于判断个人和企业信用状况的各类信息。包括但不限于：个人和企业的身份、地址、交通、通信、债务、财产、支付、消费、生产经营、履行法定义务等信息，以及基于前述信息对个人和企业信用状况形成的分析、评价类信息。”这一定义弥补了《条例》在信用信息定义上的空白，但另一方面也一定程度上对于普遍信用信息的范围进行了拓展。具体而言，信用信息的这一定义不仅可能将个人、企业在各类金融、经济活动过程中的各项信息均纳入信用信息的范畴，也进一步将对个人或企业作出的分析、评价、画像类信息一并纳入。

（二）征信服务

新规草案在不同条款中对监管部门意欲纳入征信业务的服务业态予以“点名”规制，包括第二十五条提到的“**画像、评分、评级等评价类产品服务**”“**个人信用评价服务**”“**企业主体或债项信用评级服务**”，以及第二十七条所述“**信用信息查询、信用评价、反欺诈服务**”，第四十四条进一步将以“**信用信息服务、信用服务、信用评分、信用**

[1]《条例》第二条第一款规定，在中国境内从事征信业务及相关活动，适用本条例。
[2]《个人信息保护法（草案）》第三条第二款规定，在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）为分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。

评级、信用修复”等名义对外提供征信功能服务纳入监管范畴。相关立场也在起草说明中得到了印证:“当前实践中，利用该信息对个人或企业作出的**画像、评价**等业务界定为征信业务，属于新规草案的约束范围”。

实际上，关于征信监管范围拓展的讨论由来已久，此前，央行曾在公开会议上强调将“替代数据”纳入征信监管，认为利用替代数据为金融和经济活动提供信用管理服务，在本质上属于征信活动。新规草案在信用信息和征信业务上的规定，进一步反映了央行对于征信活动拓展监管的表态。

新规草案的上述规定以及央行的公开表态，反映了监管当局在数字经济时代背景下对征信业务范畴的监管思路转变。大数据产业的发展使得征信、信用服务边界愈发模糊，一些借贷信息范畴外的其他数据愈来愈发挥着与个人、企业信用信息相类似的评估价值，也由此产生了大量的使用“替代数据”进行类似于个人、企业信用评级、个人 / 企业分析画像的大数据风控新兴业态。这些企业往往扮演着与征信机构类似的角色，构成“现代化征信体系”的重要组成部分，被认为是借贷信息的有益补充。[3] 然而纵观过去一段时间，因数据来源非法等诸多问题，反欺诈、智能风控等行业曾多次面临着监管、司法当局的质疑和调查。此次新规草案将信用画像、信用评价等服务纳入征信业务监管，也充分释放了相关信号，此后对于大数据风控行业的监管将逐步构成征信业务监管的重要组成部分。

与此同时，大数据风控等类征信企业也未必只有申请征信业务审批“华山”一条路。值得注意的是，新规草案第四十三条对于征信机构以外与征信机构合作，为金融经济活动提供个人或企业信用信息的“**其他信息处理者**”，以“**签署合作协议**”+“**监管报备**”方式予以规制。我们理解，这一规定可帮助有关当局了解征信机构获取个人、企业信用信息的具体来源，间接实现对与征信机构合作的大数据风控等类征信企业监管把控。

三、如何定义信用信息采集的“最小必要”？

整体而言，新规草案对信用信息的采集规范体现出趋严的监管趋势。值得注意的是，与《民法典》《网络安全法》《条例》等规定相一致，新规草案第五条依然秉持“最小必要”的信息采集原则。但实践中基于目前的大数据技术，对于个人及企业的风险或信用判断的准确性可能与获得相关信息的数量和种类成正比。考虑到征信活动的目的是对信用信息进行分析，以全面判断个人及企业信用状况、控制信用风险、进行信用管理等，例如《商业银行互联网贷款管理暂行办法》第二十条规定：“商业银行应当在获得授权后查询借款人的征信信息……全面了解借款人信用状况”。

如秉持最大限度了解个人信用情况的原则，如何判断信用信息收集的“最小必要”，如何实现征信活动实际目的与个人信息主体权益保障之间的平衡，将可能成为未来实践操作中有待进一步探讨和商榷的问题点。同时，新规草案第九条要求经营个人征信业务的征信机构制定采集个人信用信息方案，并就采集的数据项、与信用的相关度、信息主体权益保护等事项向中国人民银行报备，这一规定可能使得征信机构就信用信息收集范围和必要限度的合规判断交由监管部门来协助处理，有利于增强透明性和确定性。

四、董监高履职相关信用信息不作为个人信用信息？

新规草案第十三条沿袭了《条例》的规定，将“征信机构采集企业董事、监事、高管人员与履行职务有关的信用信息，不作为个人信用信息”，结合上下文关于个人信用信息的采集，可以推知在新规草案语境下，董监高与履职有关的信用信息的采集将可能无须经过信息主体本人同意。

我国一般个人信息保护领域对于个人信息的收集、处理仍以信息主体同意为基本原则，但往往存在“法律、行政法规另有规定”的除外适用空间；《个人信息保护法（草案）》试图将个人信息处理的合法基础予以扩张，这也同样为特定行业领域、特定场景情境下的个人信息收集提供了信息主体同意之外的其他合理理由。我们理解，新规草案沿袭《条例》的上述规定，体现了征信行业对于特殊群体信用信息收集在实现企业信用评估的现实需求与特定群体个体权益保障之间的评估考量，在未来个人信息保护立法日益完善的趋势下，我们也期待着

[3] 央行首度明确：“替代数据”本质属于征信活动 需要纳入征信监管，https://finance.sina.cn/2020-12-15/detail-iiznezxs7080322.d.html。

不同行业领域的法规之间能够有效保障信息收集规则的逻辑自洽。而就同一规则内的逻辑自洽而言，有必要注意的是，董监高履职相关信息不作为个人信用信息，不排除其可能作为企业信用信息的组成部分，在该等信息处于非公开状态时，结合新规草案的要求，不排除仍可能需要获得企业的同意。

五、非公开企业信用信息采集需要获取同意？

值得注意的是，新规草案第十二条规定征信机构采集非公开的企业信用信息，应当采取适当的方式取得企业的同意。此前，《条例》第二十一条对征信机构获取企业信用信息的渠道进行说明外，并未明确标识该等企业信用信息是否需要经过企业的同意，而近年来对于数据保护的讨论以及立法、执法发展往往以自然人个体信息相关权益保护展开。新规草案的上述规定，表明了征信行业在企业信用信息采集规则上的新态度，而相关的规则如何理解适用，例如何种信息构成“非公开”，如何取得企业的同意以及何为“适当的方式”，仍有待进一步明确。

六、征信业务的算法透明？

新规草案第二十五条要求提供画像、评分、评级等评价类产品的征信机构建立评价标准并且对评价服务所使用到的数据、评分方法与模型进行披露。这一规定，意味着算法合规开始进入监管机构的关注视野。

我们理解，信用画像、信用评价等与个人和企业的经济活动息息相关，从确保公平客观的角度，从事该等业务的相关企业应至少保证信用评价的准确性与非歧视性。而信用评价结果的准确性与非歧视性都会受到模型设计与训练数据的影响，新规草案第二十五条要求披露评分方法和模型，以及评价使用的所有数据，可以有效确保征信机构所应用的信用评价算法模型与数据偏差的审查。但恰如我们此前所探讨的，考虑到数据偏差本身的隐蔽性与复杂性，这可能无法在事实上完全避免准确性偏差与非歧视性，仍可能需要一定的事后救济制度设计来保证对个人和企业合法权益的最大保障。

七、征信机构与合作方的权利义务？

根据合作主体的角色不同，新规草案将征信机构、第三方之间在不同合作情境下的合规义务进行了原则性规定。总体而言，对于信息提供者、信息使用者，新规草案对征信机构的审查要求予以了原则性的明确，并对征信机构、信息提供者、信息使用者在信用信息主体的权益保障上提出了某些相对具体的要求，例如要求信息提供者告知征信机构的身份、要求信息使用者不得超出约定使用个人信用信息等。具体如下表：

信息提供者	• 第七条 征信机构采集信用信息的，应当对信息提供者的**业务合法性、信息来源、信息质量、信息安全、信息主体授权等进行审核**，保障采集信用信息的合法、准确和可持续。 • 第八条 征信机构应当与信息提供者明确各自在数据更正、异议处理、信息安全等方面的权利义务。 • 第十一条 征信机构通过信息提供者取得个人同意的，**信息提供者应当明确告知信息主体征信机构的名称**。 • 第十五条 征信机构在整理、保存、加工信用信息过程中发现信息错误的，如属于信息提供者报送错误的，**应当及时通知信息提供者更正**；如属于内部处理错误的，应当及时更正，并完善内部处理流程。

信息使用者	• **第十八条** 征信机构应当采取适当的措施，**对信息使用者的身份、业务资质、使用目的等进行必要的审查**。 征信机构应当对通过网络形式接入征信系统的信息使用者的网络和系统安全、合规性管理措施进行必要的审查，对查询行为进行监测，发现违规行为，及时停止服务。 • **第十九条** 征信机构应当对信息使用者进行必要**的审查，保障信息使用者查询个人信息时获取信息主体同意、按照约定用途使用**。 • **第二十条** 信息使用者使用征信机构提供的信用信息，应当**用于合法、正当的目的，不得滥用**。 信息使用者使用个人信用信息应当有明确、具体的目的，按照与信息主体约定的用途使用，**超出约定用途的，应当另行取得同意**。 • **第三十六条第二、三款** 征信机构向境外提供企业信用信息查询服务，应当**审查信息使用者的身份、用途，确保信用信息用于跨境贸易、融资等合理的用途**，并采取单笔查询的方式提供。 征信机构不得将某一区域、某一行业批量企业的信用信息传输至境外同一信息使用者。
被委托机构	• **第二十二条第一、二款** 征信机构应当通过互联网、营业场所、委托其他机构等多种方式为个人信息主体提供每年两次免费信用报告查询服务。 征信机构委托其他机构向信息主体提供免费信用报告查询服务的，**应当对被委托机构资质、服务能力、安全保障设施、合规性要求进行审核，并对被委托机构的查询行为、泄露行为承担连带责任**。
合作机构	• **第四十三条** 与征信机构合作，为金融经济活动提供个人或企业信用信息的其他信息处理者，应当在**签署合作协议**后向**中国人民银行或其副省级城市中心支行以上分支机构报备**。

八、信用信息数据库的本地化部署与出境限制?

个人信息和重要数据跨境一直是我国数据保护立法当下广为探讨的热门话题。此次新规草案结合征信行业的信息属性和特点，同样对行业领域内的数据跨境规则作出了明确要求。

《条例》对于征信信息跨境作出概括性的规定，要求征信机构对在中国境内采集的征信数据在中国境内整理、保存和加工；如需向境外提供的，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。新规草案延续了这一原则性规定，并明确要求将“生产数据库、备份数据库应设在中国境内”。这一规定此前曾出现于央行颁布的推荐性行业标准《征信机构信息安全规范》（JR/T 0117-2014）第 9.9 条，新规草案的这一增补，反映监管部门对征信业务数据库本地化部署要求的进一步强化。

除此之外，在向境外传输征信信息的具体执行层面，新规草案第三十六条作出了更明确、严格的安排，要求区分个人信息用信息、企业信用信息分别遵循国家相关法律法规进行落实：

- 个人信用信息：征信机构向境外提供个人信用信息，应当符合国家法律法规的规定。
- 企业信用信息：征信机构向境外提供企业信用信息查询服务，应当审查信息使用者的身份、用途，确保信用信息用于跨境贸易、融资等合理的用途，并采取单笔查询的方式提供。征信机构不得将某一区域、某一行业批量企业的信用信息传输至境外同一信息使用者。征信机构向境外提供企业信用信息的，应当向中国人民银行备案。

从我国《网络安全法》《数据安全法（草案）》《个人信息保护法（草案）》等对数据出境问题的一般立法思路来看，主要针对关键信息基础设施及一般网络运营者的个人信息、重要数据这两类数据的出境问题进行规制。我们理解，征信机构掌握大量的个人及企业信用信息，本身具有较高的敏感性，且规模化的信用信息甚至可能对整体金融行业及国家经济、社会安全等产生实质影响。因此，从征信机构自身定位及所持信息属性的角度，不排除可能会被视为《网络安全法》下的关键信息基础设施运营者，从而需要落实个人信息、重要数据的本地化部署要求。新规草案的上述规定，一方面反映了监管部门意图实现数据出境与其他数据保护法律法规的相互衔接，另一方面对于企业信用信息的出境要求（特别是禁止批量传输、央行备案规定），或多或少反映了监管部门对于“重要数据”的保护思路。

结语

新规草案的颁布，很大程度上预示着征信行业“强监管”时代的到来。无论是征信业务监管范畴的扩张，还是对于征信机构在信息收集、使用方面的细化要求，均体现了监管当局肃清征信行业乱象、保障信息主体权益的决心。这一监管思路的转变对于无论是已持牌主体，还是对于游走在“边缘”的类征信企业而言，均是一个明确且强烈的信号。

Tips：

- 对于持牌主体，宜尽早结合新规草案的内容展开自身业务的合规审查，对存量信用信息合规风险予以识别并尽早应对，对信息的收集、加工、留存、使用、对外提供等进行流程管控，对与不同角色的第三方主体之间数据交互及业务合作模式的合规性进行回顾审查。
- 对于从事类征信业务的企业，也宜审慎判断自身业务模式的潜在问题和风险，结合新规草案的相关规则尽早论证和探寻业务发展的可行路径。当然，如我们在前面探讨的，新规草案中的部分规则仍有进一步解释和发展的空间，未来如何具体走向，有待在未来的立法和执法中进一步明确。

感谢实习生张子谦、刘婧姝对本文的贡献！

网络安全

新起点、新征程：《数据安全法》时代下的数据安全与发展

宁宣凤　吴涵　陈胜男　赵天琦　姚敏侣

前言

自 2021 年 9 月 1 日起，《中华人民共和国数据安全法》（以下简称“**《数据安全法》**”）正式生效施行。作为国家安全领域的重要立法，也作为数据安全领域的基础性法律，《数据安全法》为国家有关部门行使数据治理权力、开展数据安全监管，为企业合法处理数据、保障数据处理安全等，均提供了充分的上位法依据。可以说，《数据安全法》的正式生效，为我国数字经济和社会进步拉开了以“数据安全与发展”为主题的时代序幕。

本文中，**我们将进一步提炼企业在进行《数据安全法》合规工作中，应当熟稔于心的若干法律合规要点、厘清关键概念与制度之间的关系**，以期在服务企业合规实务工作的同时，和大家共同见证数据合规新时代的到来。

一、理解《数据安全法》的立法目标和规则体系

准确理解和适用《数据安全法》，**需要从立法的基本目标、必要性及其与《国家安全法》《网络安全法》以及《个人信息保护法》等法律之间的衔接关系为起点，建立起企业适用《数据安全法》的体系基准和坐标认知。**

总体而言，在《国家安全法》以及“总体国家安全观”指引之下，依赖于《网络安全法》《数据安全法》和《个人信息保护法》，在网络、数据和算法等事物发展的客观维度，在个人 / 企业、组织 / 社会和国家安全三个基本权益保障层次上，实现全面的维护稳定与促进发展的规则协调体系、综合提升网络与数据安全现代化治理能力。

（一）基本认知：坚持“以发展促安全、以安全保发展”

《数据安全法》开宗明义，在第一条中明确描述了立法目标，在第七条中明确促进以数据为关键要素的数字经济发展，并且在第十三条中重点阐述了数据发展与安全的辩证关系，即“**国家统筹发展和安全，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。**”与此同时，《数据安全法》第二章的相关规定也不容忽视。透过相关条文规定不难发现，国家将在今后鼓励和扶持合法合规的数据创新利用，尤其是**在公共智能化服务、数据安全技术产品与认证服务、**

数据交易市场、教育和科研等具体领域中创造新的机遇与突破。

可见，《数据安全法》充分彰显了其作为数字经济时代特色的部门立法。而与此同时，企业亦应当明确树立这样一个基本感知或者信心，即《数据安全法》除了给企业带来了一定的数据安全合规成本之外，**不应该忽视产业数据有序利用和流动下的广泛利益**。从《数据安全法》诸多条文中均可以看出，这部法律对于促进企业数据合法利益的保护、开发和利用所体现出的立法保护决心，以及促进数字产业和数据产品的创新和利用所建立起的行业发展信念。

不难理解，安全和稳定是实现长足发展的前提，数据安全亦是如此。企业的数据安全、合规与资产化治理，将成为企业今后发展的关键命题。对于企业来说，以更为积极的姿态做好《数据安全法》下的数据安全合规，既是在应对法律规则变化的挑战，更是在积极利用规则开拓的发展机遇，积累与培育新的行业竞争力与市场品牌价值。

（二）立法目标：遵循“总体国家安全观”下的数据竞争、合作与治理

作为新时代维护我国国家安全的行动指南，总体国家安全观认为：“没有网络安全就没有国家安全”[1]、“数据安全关乎国家安全”[2]。近年来，总体国家安全观在数字经济时代的外延不断拓展，如网络安全观，倡导尊重网络主权、推进全球互联网治理体系变革、构建网络命运共同体等均为其表现形式[3]。虽然网络安全与数据安全同属于非传统安全领域，但与网络安全不同，数据安全的核心在于保障数据的安全与合法有序流动[4]。由此，**《数据安全法》以“数据处理活动及其安全监管”这一动态过程与安全作为法律的适用对象，这体现了“总体国家安全观”主导和指引着《数据安全法》规则的具体制定与体系搭建**。

首先，数据安全工作需要积极应对国际数据主权竞争，有效防范和抵御境外数据处理的安全风险。一方面，《数据安全法》通过第二条赋予了对境外企业处理数据可能损害国家安全、公共利益或者公民、组织合法权益时的域外适用效力，这意味着面向境内提供产品和服务的跨国企业，即便在境内不涉及数据处理活动，亦将受到《数据安全法》的管辖；另一方面，为了提供有效应对域外长臂管辖的法律武器，第三十六条规定处理境外主管机关调取境内存储数据时应当遵循的依据有关国际条约、协定和平等互惠的原则，同时明确需要境内主管机关的批准。此外，针对我国企业近年来频繁遭受的在数据和数据开发利用技术有关的投资、贸易领域受到的歧视性禁止、限制或者其他类似措施的行为，第二十六条提供了我国可以采取对应反制措施的法律依据。对于境内企业而言，在遇及境外调取数据的过程中遵循《数据安全法》要求，并积极利用《数据安全法》提供的法律规则，在国际市场竞争中维护自身经营的数据安全与合法权益，既是一种法定义务，也成为了一种现实可能的选择权。

其次，竞争并不排斥合作，《数据安全法》为深度参与全球数字经济市场的数据开发、利用和分工协作的企业，提供在确保安全前提下数据跨境流动的机制保障。客观上说，《数据安全法》为企业依照国际社会数据跨境流动合规水准和要求开展经营提供了衔接的良好契机。《数据安全法》中规定的数据安全制度、数据安全保护义务等，有助于提高企业在数据处理过程中的合规水平，更好地融入全球数字市场。此外，《数据安全法》第十一条表明了国家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的开放态度，在“总体国家安全观”下，《数据安全法》贡献了全球数据安全治理的中国智慧和中国方案[5]，也为企业参与国际合作打了一剂强心针。

最后，企业内部数据处理安全风险不容小觑。《数据安全法》的基本价值仍在于规范企业的数据处理活动，帮助企业建立数据安全管理体系。从个人和组织的合法权益角度来看，数字化时代下“数据”往往构成了一种社会身份的象征，深刻影响着个人尊严或者组织声誉与利益。**因此，强调企业数**

[1] 国家网信办：《习近平：没有网络安全就没有国家安全》，载“国家网信办官网”，http://www.cac.gov.cn/2018-12/27/c_1123907720.htm 最后访问日期：2021 年 8 月 30 日。
[2] 中央纪委国家建委网站 李云舒：《数据安全关乎国家安全》，载“中国人大网”，http://www.npc.gov.cn/npc/c30834/202107/39abeb5d40744aeaa65e17794714c559.shtml 最后访问日期：2021 年 8 月 30 日。
[3] 高祖贵：《深刻理解和把握总体国家安全观》，载《人民日报》2020 年 4 月 15 日 09 版，http://theory.people.com.cn/n1/2020/0415/c40531-31673757.html 最后访问日期：2021 年 8 月 30 日。
[4] 安静：《审视数据安全在国家层面的重要意义》，载《中国社会科学报》2021 年 2 月 23 日 008 版。
[5] 国家网信办：《专家解读丨＜数据安全法＞为全球数据安全治理贡献中国智慧和中国方案》，在“中国网信网”，http://www.cac.gov.cn/2021-06/15/c_1625341228851523.htm 最后访问日期：2021 年 8 月 30 日。

据安全义务，也体现了《数据安全法》对于数据处理活动中所涉基本民事权益的保护。此外，对数据安全的保护也不局限于数据本身，还需要进一步考虑到数据对于人工智能的影响。近来的一系列执法和立规动作（如《互联网信息服务算法推荐管理规定》，折射出相关法律制度对于数据的规制，也就从数据安全进一步推进到算法安全[6]。

（三）法律体系：与相关法律的规则接洽关系

1. 与《国家安全法》的关系

《国家安全法》以法律的形式确立了中央国家安全领导体制和总体国家安全观的指导地位，明确了维护国家安全的各项任务，建立了维护国家安全的各项制度，对当前和今后一个时期维护国家安全的主要任务和措施保障作出了综合性、全局性、基础性安排[7]。《数据安全法》同样明确以维护国家主权、安全为根本立法目标和宗旨，聚焦数据处理过程中所形成或者可能面临的安全风险及其监管。由此可见，在总体国家安全的法律规则体系下，《数据安全法》与《国家安全法》可能存在特殊与一般的规则适用关系。

从《数据安全法》第五条规定亦可以发现，中央国家安全领导机构（“中央国安委”或者“国安委”）作为国家数据安全工作的决策和议事协调机构，既负担有国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策的宏观职权，也存在统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制的具体职责。关于国安委作为《数据安全法》的主管机关的具体职权与职能，本文将在第三部分进行重点介绍。简言之，国安委作为《数据安全法》的法定执法机关，具有依《数据安全法》行使职权和管理职能的法律基础，将在自身的职责范围内，对可能影响国家安全、利益的数据处理活动开展执法和监管。

2. 与《网络安全法》和《个人信息保护法》的关系

不难看出，在《数据安全法》立法起草和征求意见过程中，其与《网络安全法》《个人信息保护法》这两部法律之间的衔接关系最为密切，考虑也最为周到全面。最为典型的如在对“数据”和“个人信息”的定义上，均对其载体形式统一表述为“以电子或者其他方式”。因此，有不少人认为，《数据安全法》与《网络安全法》《个人信息保护法》共同构成了网络安全与数据合规领域的基本法律规则框架。本文将从制度衔接与规则接洽的层面上，进一步梳理《数据安全法》中不少规定所体现出与《网络安全法》《个人信息保护法》之间的适用关系。

- 就《数据安全法》与《网络安全法》之间的制度衔接方面：
  首先，从适用范围上，《网络安全法》规范网络运营者（网络的所有者、管理者和网络服务提供者）在境内建设、运营、维护和使用网络的行为。相对而言，《数据安全法》所规制的数据处理行为更为广泛，主体也更为多样，对于非通过网络方式处理数据的行为亦提出了相应的确保安全的法律要求。
  其次，在具体规则上，《数据安全法》第二十七条规定，利用互联网等信息网络开展数据处理活动，需在《网络安全法》所规定的网络安全等级保护制度基础之上，履行数据安全保护义务。该条款是《数据安全法》依据二读阶段立法意见所采纳而新增的，梳理与明确了与《网络安全法》的规则适用关系。相类似地，《数据安全法》第二十九条所规定的数据安全漏洞风险监测、第三十一条规定的关键信息基础设施运营者的重要数据出境安全管理要求等，均体现了两部法律在具体规则层面上的接榫。

- 就《数据安全法》与《个人信息保护法》之间的适用关系而言：
  毋庸置疑，个人信息属于数据的一种特殊类型，其上承载的人格尊严属性和财产归属的特殊性，使得我们国家专门对个人信息保护进行专门立法。**我们认为《数据安全法》仍然包含了对“个人信息”安全与保护的规则适用**。这是因为，从《数据安全法》第五十三条的文义解释角度来看，

[6] 杨蓉：《从信息安全、数据安全到算法安全》，载《法学评论》2021 年第 1 期，第 131 页。
[7] 全国人大常委会：《关于 < 中华人民共和国国家安全法（草案）> 的说明》，在“中国人大网”，http://www.npc.gov.cn/wxzl/gongbao/2015-08/27/content_1945964.htm 最后访问日期：2021 年 8 月 30 日。

“开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定”，该条应当被理解为：在数据安全的一般性原则之上，个人信息的处理需同时遵循《个人信息保护法》中的规则。换句话说，当企业处理个人信息时，应当同时遵循《数据安全法》与《个人信息保护法》的合规要求。

3. 与《保守国家秘密法》《统计法》《档案法》以及军事数据安全保护办法等相关规定的关系

区分数据的开放性与秘密性，《数据安全法》第五十三条规定，开展涉及国家秘密的数据处理活动，适用《保守国家秘密法》等法律、行政法规的规定。关于国家秘密与国家核心数据、重要数据的概念关系，将在下文第二部分进行厘清。而如属于国家秘密领域内的数据处理，需要满足强制性要求更高的《保守国家秘密法》等法律和行政法规规定。

区分数据处理的具体领域，如在统计、档案等工作涉及数据处理，企业应当在遵循《数据安全法》的基本规定之上，按照《统计法》和《档案法》规定开展工作。此外，如涉及军事数据安全的特殊领域，《数据安全法》第五十四条规定，军事数据安全保护的办法，由中央军事委员会依照本法另行制定。

二、厘清《数据安全法》的关键定义与重点概念

在《网络安全法》的基础上，《数据安全法》进一步建立了专门针对数据的安全保护制度体系，结合此前刚颁布不久的《个人信息保护法》对特定类型的数据——个人信息的专门规定，使得在数据相关的概念及规范要求层面，不免出现三部法律重叠与交叉的情况。对于企业而言，在理解并落实《数据安全法》的各项规则制度时，有必要从法律概念和规范设计层面对三部法律的法律概念及规定之间的关系予以厘清。以下我们尝试从《数据安全法》的重点概念或规则出发，对三部法律所规定具有相似属性的概念或规则制度进行澄清说明。

（一）数据、重要数据与个人信息

继《网络安全法》对网络数据[8]的定义予以明确，《数据安全法》在法律层面首次对数据的概念进行了界定，是指任何以电子或者其他方式对信息的记录。这一定义同步对数据与信息之间的关系进行了澄清，表明信息指向事物所传递的内容或属性，而数据构成这一内容或属性的记录形式。《数据安全法》对于数据的定义也传达了该法对于各类数据处理活动的总括适用性。在数据概念之下，基于数据本身属性或所保障的法律价值不同，又囊括了个人信息和重要数据两类法律重点关注的数据。

直观来看，个人信息和重要数据在定义上存在比较显著的差异，值得注意的是，二者定义的出发点存在一定不同。个人信息的定义[9]强调其与个人的关联属性，从信息的客观属性出发进行外延和内涵的划定；与此不同的是，重要数据[10]是从法律所关注或期望保护的价值与利益（例如国家安全、公共利益或者个人、组织的合法权益）出发，将可能影响或与该等价值或利益实现具有关联的数据拟制性地纳入保护范围。**上述差异意味着个人信息和重要数据在范围上并非绝对的互斥关系，如果个人信息所反映的法律价值或利益落入重要数据的范畴，将同样可能作为重要数据来保护**。国家网信办发布的《汽车数据安全管理若干规定（试行）》对重要数据的定义有所印证，对于涉及个人信息主体超过10万人的个人信息，将被该规定视为重要数据予以保护。因此，对于企业而言，在进行内部的个人信息和重要数据安全保障工作时，宜同步考虑两者之间的关联，避免过分割裂两类数据而引发相关数据安全保护的切割和断层。

（二）个人信息出境和重要数据出境

自《网络安全法》颁布生效之日起，数据出境制度一直是立法、执法以及从业者层面广为讨论和关注的问题。从《网络安全法》设置了关键信息基础设施运营者在个人信息和重要数据出境上的限制条件，到此后关于个人信息、重要数据出境要求各

[8]《网络安全法》第七十六条规定，网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。
[9]根据《个人信息保护法》第四条规定，个人信息是指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。
[10]《数据安全法》尚未对重要数据进行明确定义，国家网信办颁布的《汽车数据安全管理若干规定（试行）》首次对汽车领域的重要数据进行了定义，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，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。

项征求意见稿的出台，直至目前《数据安全法》《个人信息保护法》的颁布，有关个人信息、重要数据出境的规则（包括适用主体、数据范围、出境限制条件等）渐渐浮出水面，且仍在不断发展。值《数据安全法》生效之际，对现阶段个人信息和重要数据出境的有关规则进行厘清和明确，对于企业业务的全球布局具有重要的前瞻意义。以下我们从数据出境主体属性出发，尝试将《网络安全法》《数据安全法》《个人信息保护法》等近期颁布的正式法律法规中涉及个人信息和重要数据出境的规则进行梳理说明：

	重要数据	个人信息
关键信息基础设施运营者	• 在中国境内运营中收集和产生的重要数据应在境内存储，因业务需要，确需向境外提供的，应当按照有关规定进行安全评估；法律、行政法规另有规定的依照其规定。（《网络安全法》第三十七条，《数据安全法》第三十一条）	• 在中国境内运营中收集和产生的个人信息应在境内存储，因业务需要，确需向境外提供的，应当按照有关规定进行安全评估；法律、行政法规（和国家网信部门规定）另有规定的依照其规定。（《网络安全法》第三十七条，《个人信息保护法》第四十条）
一般网络运营者 / 数据处理者	• 其他数据处理者在中境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。（《数据安全法》第三十一条） • 重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。（《汽车数据安全管理若干规定》第十一条） • 汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。（《汽车数据安全管理若干规定》第十二条） • 向境外提供重要数据的汽车数据处理者应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送有关情况。（《汽车数据安全管理若干规定》第十三条、第十四条）	• 因业务等需要，确需向中国境外提供个人信息，应具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）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；（三）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；（四）法律、行政法规或者国家网信部门规定的其他条件。中国缔结或者参加的国际条约、协定对向中国境外提供个人信息的条件等有规定的可按其规定执行。（《个人信息保护法》第三十八条） • 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，取得个人的单独同意。（《个人信息保护法》第三十八条） • 处理个人信息达到国家网信部门规定数量，应将在中国境内收集和产生的个人信息存储在境内，确需向境外提供的，应通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的从其规定。（《个人信息保护法》第四十条）
	• 中国主管机关根据有关法律和中国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据 / 个人信息的请求。非经中国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中国境内的数据 / 个人信息。（《数据安全法》第三十六条，《个人信息保护法》第四十一条）	

值得注意的是，考虑到个人信息和重要数据可能存在范围上的重合，因此当出境的个人信息同样落入重要数据的范畴时，从法律解释角度看也将需要同步遵循重要数据出境的各项要求。而对于向境外执法、司法机关提供境内存储的数据，多部法律采取了一致性的规则手段，企业未来面临类似场景时，无论是个人信息还是重要数据的对外提供均不得违背上述原则。

（三）网络安全负责人、数据安全负责人、个人信息保护负责人

《网络安全法》《数据安全法》《个人信息保护法》基于履行网络安全义务、数据安全保护义务、个人信息处理者义务等对企业设置相应安全保护负责人分别作出规定：

网络安全法	数据安全法	个人信息保护法
• 第二十一条 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制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，**确定网络安全负责人**，落实网络安全保护责任……	• 第二十七条第二款 **重要数据的处理者应当明确数据安全负责人和管理机构**，落实数据安全保护责任。	• 第五十二条 **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应当指定个人信息保护负责人**，负责对个人信息处理活动以及采取的保护措施等进行监督。

上述规定是基于不同法律保护的客体出发对安全管理人员组织上的各自要求，故在具体的职责职能上也会有所侧重，网络安全负责人主要关注网络环境下的安全保护责任，数据安全负责人和个人信息保护负责人则分别侧重数据安全和个人信息安全维度的安全保障职能。恰如前述对于各法之间的关系以及个人信息和重要数据之间关系的讨论，上述负责人的管理责任也将不可避免存在一定的重叠交叉，例如网络安全负责人的职责范围也可能涉及对网络环境下数据的安全保护。因此，企业在进行相关的组织架构设计时除了明确各自职责的侧重，也要关注各负责人之间在职能上的关联关系。同时，考虑到法律上并未禁止不同类型的安全保护负责人重复任职，在明确相关负责人在网络安全、重要数据、个人信息保护方面分别、专门的职责的情况下，不排除上述职责可设计由同一人员或管理机构同时承担。

（四）重要数据处理活动风险评估、个人信息保护影响评估、网络安全审查

除数据出境可能涉及一系列安全评估事项外，《数据安全法》等法律法规还对其他满足特定条件的数据处理活动提出了风险评估的要求，而基于不同法律法规的规定，不同类型数据、不同场景数据处理活动风险评估的触发条件不尽相同，在此我们也尝试对不同法律中规定的主要评估义务进行分门别类：

	重要数据处理活动风险评估	个人信息保护影响评估	网络安全审查 / 国家安全审查
评估义务主体	• 重要数据处理者	• 个人信息处理者	• 关键信息基础设施运营者 • 数据处理者

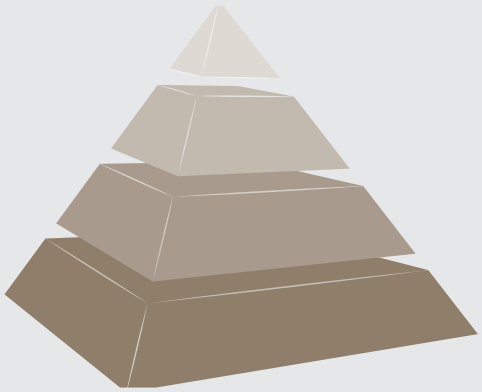
	重要数据处理活动风险评估	个人信息保护影响评估	网络安全审查 / 国家安全审查
触发条件	• 对数据处理活动定期开展风险评估	• 处理敏感个人信息 • 利用个人信息进行自动化决策 • 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息 • 向境外提供个人信息 • 其他对个人权益有重大影响的个人信息处理活动	• 关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的 • 数据处理者开展数据处理活动，影响或可能影响国家安全的 • 掌握超过 100 万用户个人信息的运营者赴国外上市（*《网络安全审查办法》草案要求） • 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务、数据处理活动以及国外上市行为，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照规定进行审查（*《网络安全审查办法》草案要求）
评估内容	• 风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等	• 个人信息的处理目的、处理方式等是否合法、正当、必要 • 对个人权益的影响及安全风险 • 所采取的保护措施是否合法、有效并与风险程度相适应	• 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险 • 产品和服务供应中断对关键信息基础设施业务连续性的危害 • 产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险 • 产品和服务提供者遵守中国法律、行政法规、部门规章情况 • 核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险 • 国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险 • 其他可能危害关键信息基础设施安全和国家数据安全的因素（*《网络安全审查办法》草案要求）
报送要求	• 向有关主管部门报送风险评估报告 • 汽车数据处理者开展重要数据处理活动还应在每年十二月十五日签向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全管理情况	• 暂无明确规定，但个人信息保护影响评估报告和处理情况记录应当至少保存三年	• 向网络安全审查办公室申报网络安全审查（*《网络安全审查办法》草案要求） • 提交材料：申报书、关于影响或可能影响国家安全的分析报告、采购文件、协议、拟签订的合同或拟提交的 IPO 材料等、网络安全审查工作需要的其他材料（*《网络安全审查办法》草案要求）

具体实践中，企业有必要根据自身数据处理活动所可能触发的场景，适时讨论上述风险评估工作的必要性，并据此开展相对应的评估工作。

三、明确《数据安全法》的监管机构与执法机制

作为一项系统性工程，数据安全总体目标的达成与具体工作的落实，关系到国家和社会经济各部门、各行业和各地区的行政执法体系的构建。如上所述，《数据安全法》与《国家安全法》《网络安全法》《个人信息保护法》以及其他相关法律、行政法规等相辅相成；相对应地，为了共同构筑国家数据安全的保护屏障，《数据安全法》按照区分经济部门以及地域的方式，明确了有权执法机关和监管单位。

根据我们对《数据安全法》第五条、第六条的初步理解，《数据安全法》下的监管机构及其对应职责，大致如下图所示。



中央国家安全领导机构：

决策和议事协调、战略方针、统筹协调、建立机制

各行业（工业、电信、交通、金融等）主管部门：

承担本行业、本领域数据安全监管职责

公安机关、国家安全机关：

在各自职责范围内承担数据安全监管职责

国家网信部门：

统筹协调网络数据安全和相关监管工作

尤其值得注意的是，“中央国家安全领导机构负责统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制”是《数据安全法》在三读阶段所新增的关于执法机制的新表述。根据全国人大网上公布的审议结果报告，考虑到“数据安全工作涉及面广，应当建立国家数据安全工作协调机制，同时明确其在制定重要数据目录、加强数据安全风险分析预警等方面的统筹协调职能。”[11]这即意味着，在“数据安全工作协调机制”的统一指挥下，各部门、各地区负责各项具体的数据安全工作的主管机关或者单位，将形成相互协调、协助和配合的执法体系，连同《数据安全法》第五章规定的政务数据安全与开放工作一道，实现基于数据安全基本目标和价值的监管数据共享和执法体系联动。

下表中，我们将《数据安全法》下所提及的各行政主体及其对应职能进行归纳总结，以便于企业了解和熟悉相关主管部门依职权进行的立规、指引与监管活动。

[11] 全国人大常委会：《全国人民代表大会宪法和法律委员会关于＜中华人民共和国数据安全法（草案）＞审议结果的报告》，载“中国人大网” http://www.npc.gov.cn/npc/c30834/202106/a2292e20dfa743febe23b01fa6aa330b.shtml，最后访问日期：2021 年 8 月 31 日。

执法机关	职权范围	具体职能及对应法律依据
中央国家安全领导机构（“中央国安委”或者“国安委”）	国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策	实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用；（第十四条第一款）
		建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场；（第十九条）
	统筹协调国家数据安全的重大事项和重要工作，建立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；（第二十一条）
		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、预警工作。（第二十二条）
中央网络安全和信息化委员会、国家互联网信息办公室（“中央网信办”或者“国家网信办”）	扎实推进数据安全应急处置机制	发生数据安全事件时，依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息；（第二十三条）
	执行落实网络与数据安全审查制度	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，依法作出的安全审查决定为最终决定；（第二十四条）
	执行落实数据安全风险评估制度	接受重要数据处理者对其数据处理活动定期开展的风险评估报告；（第三十条）
	执行落实数据出境安全管理规范	依照《网络安全法》有关规定对关键信息基础设施运营者的重要数据出境开展出境安全评估，制定其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法；（第三十一条）
公安部、各级公安机关，以及国家安全机关	贯彻执行网络安全等级保护制度	在网络安全等级保护制度的基础上，监管督促数据安全保护义务的履行；（第二十七条）
	依法维护国家安全、侦查犯罪	按照国家有关规定、经过严格批准程序调取数据，有关组织、个人应当予以配合；（第三十五条）

执法机关	职权范围	具体职能及对应法律依据
工业和信息化部、各级通信管理部门	执行落实互联网通信安全制度，如网络安全漏洞监测等	加强对开展数据处理活动的风险监测，当发现数据安全缺陷、漏洞等风险时，应当接受报告并督促采取补救措施，给予必要行政指导；（第二十九条）
国务院标准化行政主管部门	积极推进数据开发利用技术和数据安全标准体系建设	组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准；（第十七条）
省级以上人民政府	贯彻落实国家数据安全战略和有关重大方针政策，将数字经济发展纳入本级国民经济和社会发展规划	根据需要制定数字经济发展规划；（第十四条第二款）
各地区、各部门	贯彻落实和监督执行数据分类分级保护制度	确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护；（第二十一条第三款）

为简洁起见，上表中将部分通常由跨部门联合执法或者建立联席监管机制的监管职能，进行了一定的合并与划归，如国家网信部门在督促执行网络与数据安全事件应急处置的过程中，其往往作为牵头部门，联合其他相关执法机关进行联合监管。如根据《国家网络安全事件应急预案》要求建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作；再如，《网络安全审查办法（修订草案征求意见稿）》中明确，在中央网络安全和信息化委员会领导下，国家网信办会同国家发改委、工信部、公安部、国家安全部、财政部、商务部、央行、国家市场监管总局、国家广电总局、证监会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。

此外，为了进一步在全社会范围内形成提高数据安全意识、形成数据安全社会共建的良好氛围，《数据安全法》规定任何个人、组织都有权对违反规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

四、落实《数据安全法》下的企业数据合规路径

《数据安全法》针对企业的数据处理活动提出了一系列合规要求，为企业设定了积极义务与消极义务在内的多层次数据安全义务群，以通过整体规范数据处理活动，实现对数据安全的全面保障。《数据安全法》生效伊始，我们建议企业重点从以下几方面出发，结合企业内部实践情况，积极探寻合规路径。

（一）合规重点 1：梳理企业运营过程中可能涉及的数据类型并初步判断是否可能包含重要数据

在法律法规及国家标准整体层面，重要数据的概念首次被《网络安全法》第三十七条[12]提出，而后《信息安全技术 数据出境安全评估指南（征求意见稿）》附录 A“重要数据识别指南”中对 27 个重点行业的重要数据做了概括性的描述，如石油、电力、金融等，再后《数据安全管理办法（征求意见稿）》第

[12]《网络安全法》第三十七条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

三十八条第（五）项对重要数据的概念从较高层面进行了阐释，即一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据。重要数据的概念虽然很早就已经被提出，但是对于重要数据的认定方法及认定标准确至今尚未明确。

《数据安全法》第二十一条在笼统定义重要数据并要求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的基础上，将重要数据的具体识别工作下放至各地区、部门，以地区、部门以及相关行业、领域为维度制定重要数据目录。鉴于此，我们理解未来各地区、行业均可能会陆续制定重要数据识别目录，重要数据类型及认定标准也会得到进一步明晰。

在细分行业规范层面，部分行业对于重要数据的认定作出了更为清晰的规定。以汽车行业为例，于 2021 年 10 月 1 日正式生效的《汽车数据安全管理若干规定（试行）》，其在第三条中首次提出汽车行业重要数据包括“5+n”类数据[13]；再以金融行业为例，中国人民银行于 2020 年 9 月发布的《金融数据安全 数据安全分级指南》明确金融业机构在开展数据安全分级工作时，对于重要数据的安全级别不宜低于指南中确定的 5 级保护标准，且在附录 A 梳理了典型金融数据定级规则参考表，但是并未列出安全级别为 5 级以上的金融数据类型，虽然稍有遗憾的是，该指南并未以列举形式明确金融行业重要数据类型， 但是主管机关也逐渐释放出未来将由行业内部制定重要数据识别目录的信号，我们也相信未来重要数据的认定方法及识别机制也会越来越清晰。

在现阶段，建议企业应尽可能地：

- 梳理企业日常业务运营过程中可能涉及的所有数据类型及具体的信息字段，以作为初步识别工作的基础；
- 确定企业所在行业是否已存在成文的识别标准或识别方法，若无，企业需从现行有效的法律法规所提出的重要数据的概念出发，判断各类数据落入重要数据范围可能性的高低，对于较高可能会构成重要数据的数据，企业应积极履行《数据安全法》提出的数据安全保护义务；
- 与主管部门保持密切联系，并积极跟进后续配套性指引文件及细则的出台，届时采取更全面、更有针对性的合规对策。

（二）合规重点 2：明确企业内部数据安全组织架构

《数据安全法》第二十七条提出，重要数据的处理者应当明确数据安全负责人和管理机构，并落实相应的数据安全保护责任。正如上文所述，目前国内对于重要数据的定义较为宽泛，企业应当充分结合实践谨慎评估自身落入“重要数据的处理者”范围的可能。我们建议企业应尽可能地按照《数据安全法》的要求，明确内部数据安全负责人及数据安全管理机构，以避免引发不必要的合规风险。

参考欧盟 GDPR 对于数据保护官（Data Protection Officer, DPO）的相关规定，DPO 既可以是企业内部的部门或员工，也可以是与企业签署协议的外聘第三方机构或个人。而《数据安全法》并未明确外聘的第三方是否可以作为企业的数据安全负责人和管理机构，但是由于《数据安全法》明确提出了“直接负责的主管人员和其他直接责任人员”所需承担的行政责任，而外聘的第三方能够代表公司承担相应行政责任在实践中还存在一定的不确定性。

另外，与“数据安全负责人和管理机构”规则类似的是，《网络安全法》第二十一条确立了“网络安全负责人”制度、《个人信息保护法》第五十二条还确立了“个人信息保护负责人”制度，三类负责人或机构的职责在某些方面具有一定的共同性，但其各自岗位职责仍存在一定的区别。通常而言，网络安全负责人、数据安全负责人更侧重技术背景，但同时兼具一定的法律背景，负责企业内部整体网络安全及数据保护相关工作，但个人信息保护负责人则更侧重法律背景，熟悉国内个人信息保护立法规则，同时兼具一定的技术背景，落实企业个人信息保护义务。

由于上述三部法律采用的表述为“明确”“指定”

[13]《汽车数据安全管理若干规定（试行）》第三条：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，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，包括：（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；（二）车辆流量、物流等反映经济运行情况的数据；（三）汽车充电网的运行数据；（四）包含人脸信息、车牌信息等的车外视频、图像数据；（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。

负责人，而并未提出指定“单独”或“专门”负责人的要求，因此实践中企业可以根据企业自身组织架构情况，并结合相关岗位人员的知识及管理背景，综合考虑选择“分立式”岗位设置，抑或是“兼任式”岗位设置方式。

（三）合规重点 3：建立企业内部数据安全合规制度体系

综合《数据安全法》第四章对处理者提出的数据安全保护义务，为满足相关要求，建议企业在内部建立如下数据安全合规制度：

- 全流程数据安全管理制度（第二十七条）：从字面含义理解，企业需要基于《数据安全法》及相关法律法规的规定，并结合自身业务实践从全生命周期（包括收集、处理、存储、共享、跨境传输）对所涉数据的安全管理机制提出内部管理要求，充分保障数据安全；
- 风险监测与安全事件应对制度（第二十九条）：从加强风险监测、应对数据安全缺陷角度，以及明确发生数据安全事件时，内部需要采取的对策及报告流程，建议企业依照法律法规及相关国家标准的要求，将处置措施及流程纳入在内部制度文本中，落实相关合规义务；
- 重要数据风险评估报告制度（第三十条）：虽然《数据安全法》明确了定期评估并发送报告的方式，但评估主体、报告报送对象、以及评估频率还有待配套规章制度的进一步明确。建议企业积极跟进立法动态，届时建立内部定期风险评估的报告机制，落实内部责任人；
- 从事数据交易中介服务的机构还应建立数据提供方数据来源审核制度（第三十三条）：除上述一般性要求外，《数据安全法》还从风险控制的角度出发，对从事数据交易中介服务的市场参与者提出了额外的安全保护要求，其规定从事数据交易中介服务的机构应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。就此，我们建议相关交易中介服务企业建立数据来源合法合规审核制度，审核交易平台内数据提供方的数据来源合法性及授权完整性问题，以避免相关合规风险传导至企业自身。

由于《网络安全法》《个人信息保护法》与《数据安全法》所关注的角度并不完全相同，对于内部已经按照其他法律法规建立上述合规制度的企业，我们建议相关企业依照生效的《数据安全法》及相关规定，对内部已存在的合规制度进行补充及优化，以确保充分落实相关义务要求。

（四）合规重点 4：确立企业内部数据跨境传输机制

数据跨境传输一直以来都是全球化企业最关注的问题之一，而《数据安全法》也从 “企业基于业务目的向境外传输数据”及“境外执法机构调取境内数据”两方面作出了积极回应。

1. 企业基于业务目的向境外传输数据

对于属于关键信息基础设施运营者的企业而言，根据《数据安全法》第三十一条规定，企业在境内运营中收集和产生的重要数据的出境安全管理，应参照并适用《网络安全法》的规定。依照《网络安全法》第三十七条的规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

对于不构成关键信息基础设施运营者的企业而言，根据《数据安全法》的规定，其在境内运营中收集和产生的重要数据的出境安全管理要求，将由国家网信部门会同国务院有关部门制定。而参考网信办 2019 年发布的《数据安全管理办法（征求意见稿）》第二十八条，非关键信息基础设施运营者在向境外提供重要数据前，也应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。

考虑到国内目前对于重要数据及关键信息基础设施运营者的认定尚未完全清晰，建议企业首先应通过梳理相关规则、与行业主管部门沟通等方式确定企业自身是否可能落入关键信息基础设施范围

内。同时，梳理在日常业务运营过程中可能涉及的数据跨境传输场景，即便某些企业被认定为关键信息基础设施运营者的可能性较小，但是对于有可能涉及重要数据跨境传输的业务场景，在开展数据传输行为前，同样建议在现阶段积极开展内部自评估工作，并与监管部门保持密切沟通。

2. 境外执法机构调取境内数据

除了企业基于其业务自身需要主动向境外提供数据之外，《数据安全法》第三十六条同样针对可能的域外法律适用所导致的冲突管辖及其所涉及的跨境证据调取问题，进而导致数据跨境发起的业务场景进行了明确，并提出了数据安全层面的法律要求，即“经主管机关批准”。其实现行生效的法律法规已针对特定场景下的“域外数据调取”提出了类似规定，如《国际刑事司法协助法》第四条规定：“非经中华人民共和国主管机关同意，……，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助”，《证券法》第一百七十七条规定：“境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料”。

《数据安全法》第三十六条相较于上述仅适用于相较于特定场景下的“域外数据调取”的相关条款，其所能够适用的场景更为宽泛，具有一定的普遍适用性。同时，第三十六条相较于《数据安全法》内其他大多条文的适用范围亦有所扩大，即从适用主体来看，其适用于“境内的组织、个人”，而非仅限于“数据处理者”“重要数据的处理者”等；从适用对象来看，其适用于“存储于中华人民共和国境内的数据”，而非仅限于“重要数据”“国家核心数据”等。《数据安全法》现有宽泛的表述是否意味着任何存储与境内的数据被境外司法或执法机关调取时，均需要获得国内主管机关的审批？

举例而言，国内某全球化公司 A，在其境内服务器中存储了海外子公司 B 的财务及税务数据，海外监管机关出于审查目的需要调取 B 公司的财务及税务数据。A 公司是否需要就提供该财务及税务数据行为获得国内监管机关审批？如果此前财务及税务数据曾经存储在 A 公司服务器内，但由于公司管理模式调整，相关数据目前存在 B 公司所在境内，那么海外监管机关调取该等财务数据是否仍需要获得国内监管机关审批？此外，对于所调取“财务及税务数据”如果其既不构成个人信息，也未被认定为重要数据，是否会导致前述结论有所不同？

我们理解，上述问题在现行法律法规框架下并不存在唯一确定的答案，如果所有域外调取数据的行为均需要获得国内监管机关的审批，那么无疑也会为监管机关增加大量的审查成本，一定程度上可能还会造成行政资源浪费。因此，在相关问题仍有待进一步立法明确的情况下，我们仍建议企业建立内部关于域外数据调取的内部流程，积极探寻在冲突管辖场景中可能存在的合规出路。

结语

身处数字经济发展时代当下，具有标志性意义的《数据安全法》生效，昭示着我国数据安全与治理已经站在了新的起点，开启了新的阶段。数据作为生产要素的战略性地位得到确认，企业在积极探寻数据资产管理方案与价值挖掘的同时，同样意味着应当自觉担负起数据安全保护义务和治理责任。我们不难预见，数字与智能化技术的发展，将遇及越来越多的法律合规问题；而在用数字化的思维解决一个又一个具体的合规问题之外，势必将推动数据与法律领域的深度融合。不负所望、如期而至，以安全和发展为主题的数字化法律时代正在踏浪而来。

国之重器
——《关键信息基础设施安全保护条例》解读

宁宣凤　吴涵　陈胜男　屈尘

自2017年7月10日国家互联网信息办公室（以下简称“网信办”）发布《关键信息基础设施安全保护条例（征求意见稿）》（以下简称《征求意见稿》）并向全社会征求意见已四年有余（见此前的解读文章“必将婴城固守，皆为金城汤池——看《关键信息基础设施安全保护条例（征求意见稿）》”）。2021年8月17日，《关键信息基础设施保护条例》（以下简称《CII条例》）终于千呼万唤始出来，并于9月1日正式实施。作为我国在关键信息基础设施安全方面的首部行政法规，《CII条例》在推进关键信息基础设施保障、完善我国网络安全体系、保障国家安全、国计民生与公共利益等诸多方面都有着十分重要的作用。

《CII条例》从关键信息基础设施的认定、完善监督管理体系、运营者责任义务、保障和促进措施与法律责任等多个方面提出总体监管要求，在关键信息基础设施保护法律体系建设中起到提纲挈领的作用。本文将从《网络安全法》（以下简称《网安法》）体系构建的角度出发，对《CII条例》规定的重点内容进行梳理和解读。

一、关键信息基础设施的认定与识别

（一）CII的定义

《CII条例》第二条与《网安法》第三十一条采取了类似定义，强调相关网络设备与信息系统被破坏、丧失功能或者数据泄露后的严重危害性。较之于《征求意见稿》围绕行业和领域分别进行细化说明的定义方式，《CII条例》沿用了《网安法》对于CII所涉行业的开放式列举方式，并在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务基础上增加了“国防科技工业”这一类别。实际上，通过行业列举方式明确CII涉及的关键行业已成为国内外认定关键（信息）基础设施的重要且首要方法，例如英国明确了“关键国家基础设施”（Critical National Infrastructure, CNI）涉及化

工、民用核能、通信、国防、应急服务、能源、金融、食品、政府、医疗、航天、交通运输和水务等十三个行业；[1] 美国则于 2013 年以第 21 号总统令形式，对关键基础设施进行调整并按联邦部门进行划分，确定了十六类关键基础设施部门，包括化学、商业设施、通信、关键制造、水利、国防工业基地、应急服务、能源、金融服务、食品和农业、政府设施、医疗保健和公共卫生、信息技术、核反应堆、材料和废弃物、交通运输系统、水务及污水处理系统[2]。

（二）CII 认定过程

相较于《征求意见稿》中将关键信息基础设施识别的组织工作交由国家行业主管或监管部门来进行，《CII 条例》则进一步明确了相关监管部门在认定、识别 CII 工作上的主动权——基于《CII 条例》第九条、第十条的规定，重要行业和领域的主管部门、监督管理部门（即保护工作部门）需要在制定本行业、本领域关键信息基础设施认定规则的基础上，组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

另一方面，实践中可能出现网络设施或信息系统因业务调整、技术迭代或其他情况，导致其数据范围、数据重要性、数据量发生重大变化，从而不再被认定为 CII 或可能被认定为 CII 的情况。根据《CII 条例》第十一条，在 CII 发生较大变化可能影响其认定结果时，运营者应及时将相关情况报告保护工作部门，保护工作部门进而进行重新认定。

上述规定使得 CII 认定工作的职权分工更加明确，也向可能处于关键领域和重点行业的企业主体释放了明确的信号，在未来自身 CII 认定与保护工作中，有必要紧跟主管、监管部门步伐，密切跟踪所述行业、领域 CII 认定与保护规则的最新动向，并适时根据与主管、监管部门的沟通情况审慎把控自身网络设施、信息系统落入 CII 的可能性。

（三）CII 边界识别

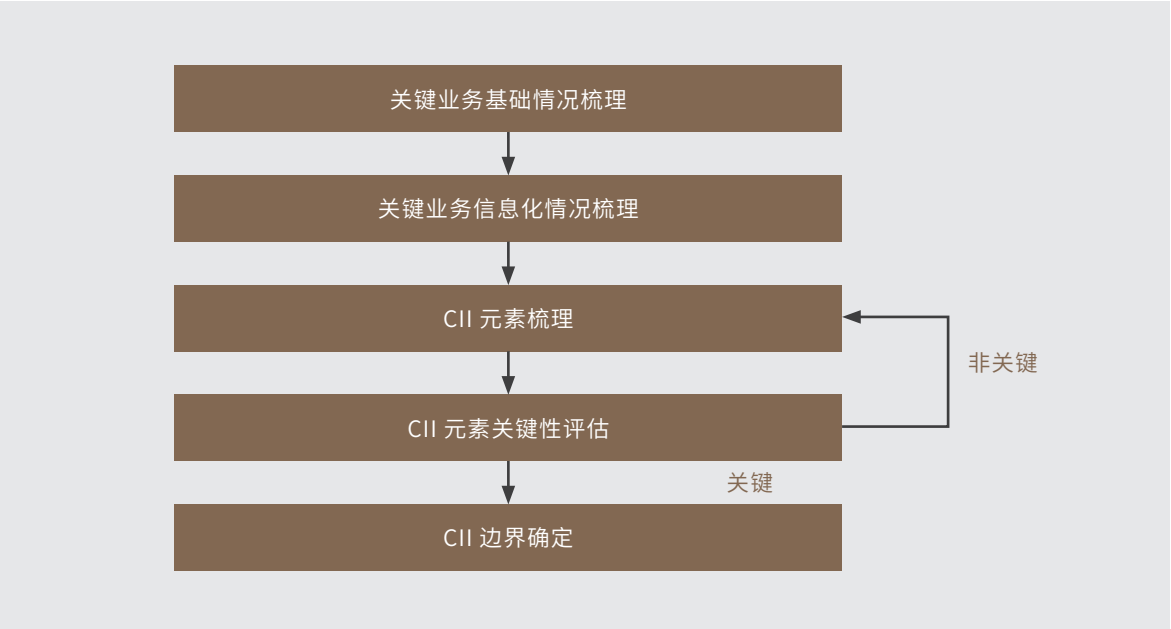
诚然，仅凭对于 CII 所涉行业及对象的规定，实践中可能仍较难准确界定处于“模糊地带”的网络设施与信息系统是否落入 CII 的范畴。这一问题自《网安法》生效及《征求意见稿》颁布以来，就始终是全国各地有关部门广为研究和探索的话题。例如，云南省互联网信息办公室曾发布研究报告，认为 CII 的最大可能边界为关键业务正常运行所需的信息流从初始到终止所流经的网络设施、信息系统；如果上述网络设施、信息系统对保障关键业务正常运行至关重要，就应当纳入 CII 保护范围。[3] 可见，报告认为在识别 CII 边界时，首先应当明晰企业关键业务类型及其对应的信息流，再依据该信息流即可确定有关的网络设施与信息系统，从而一一判断其是否落入 CII 保护范围。该文件同时为识别者设置了 CII 边界识别流程，从业务分析到 CII 元素识别、关键性评估，最后进行 CII 边界确定，如属于 CII 则按照规定进行信息备案。

除地方相关工作部门对于 CII 边界识别进行研究确认外，2020 年 8 月，全国信息安全标准化技术委员会（以下简称“信安标委”）发布了《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》（以下简称《CII 边界确定方法（草案）》），明确提出一种基于信息流的 CII 边界确定方法。《CII 边界确定方法（草案）》提出了 CII 边界识别模型所涵盖的六个方面，包括关键业务、网络设施、信息系统、CBI（关键业务信息）、CBIF（关键业务信息流），以及基础运行环境。其中关键业务为核心要求，由行业主管部门进行认定，是开展 CII 边界识别的基础，其他要素都围绕关键业务产生。

对比分析可以看出，《CII 边界确定方法（草案）》所提出的 CII 边界识别方法与上述云南网信办研究确定方法理念相似，可见确认 CII 边界的关键要素仍在于关键业务及其相关信息流。网络设施及信息系统运营者可针对行业主管部门认定的关键业务进一步梳理分析，从而明确关键业务信息种类和作用等关键业务基础情况信息，方可辅助各行业各领域保护工作部门对 CII 的识别与认定。

此外，根据《CII 边界确定方法（草案）》，CII 边界具体的识别流程如下图所示[4]：

[1] 见英国国家网络安全中心网站，https://www.ncsc.gov.uk/section/private-sector-cni/cni#section_4，最后访问日期：2021 年 8 月 22 日。
[2] 见美国网络安全与基础设施安全局网站，https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19，最后访问日期：2021 年 8 月 22 日。
[3] 云南省互联网信息办公室，《关键信息基础设施边界识别 研究报告 1.0 版》，相关新闻报道见 http://www.cac.gov.cn/2019-07/08/c_1124724585.htm，最后访问日期：2021 年 8 月 22 日。
[4] 见《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》第八节：关键信息基础设施边界识别流程。



具体而言，当行业主管部门认定关键业务后，在关键业务基础情况梳理阶段，需要对基本信息、业务特征、业务架构、业务范围进行梳理，并基于此输出关键业务基础情况描述文件；随后，在关键业务信息化情况梳理阶段，则需要就信息化范围、CBI 等进行细致梳理；在 CII 元素梳理阶段，需要根据关键业务信息化情况描述文件，识别并分析关键业务信息（CBI）在整个生存周期内的流动轨迹，即 CBIF，并对其中的网络设施、信息系统进行去重处理，得到 CII 候选元素清单；而后，在 CII 元素关键性评估阶段，需要考察 CII 候选元素对关键业务持续、稳定运行的重要性，如评估结果为“关键”，则列入 CII 元素清单；最终，通过对上述关键业务基础情况梳理、信息化情况梳理、CII 元素梳理、CII 元素关键性评估的结果进行整合，即可形成 CII 边界信息文件，作为保护、审查、应急处置等工作的参考依据。

虽然《CII 条例》将关键信息基础设施的认定规则交由各行业、各领域的保护工作部门来具体制定，考虑到《CII 条例》适才颁布，各行业、各领域的配套规则仍有待未来一段时间成熟定型。因此对于企业而言，现阶段上述地方及标准层面对于 CII 边界识别的探索研究仍具有重要的参考价值，特别是在国家大力推动 CII 安全标准体系建设的背景下，关于 CII 边界识别的各类标准指导文件仍具有十分重要的实践意义。

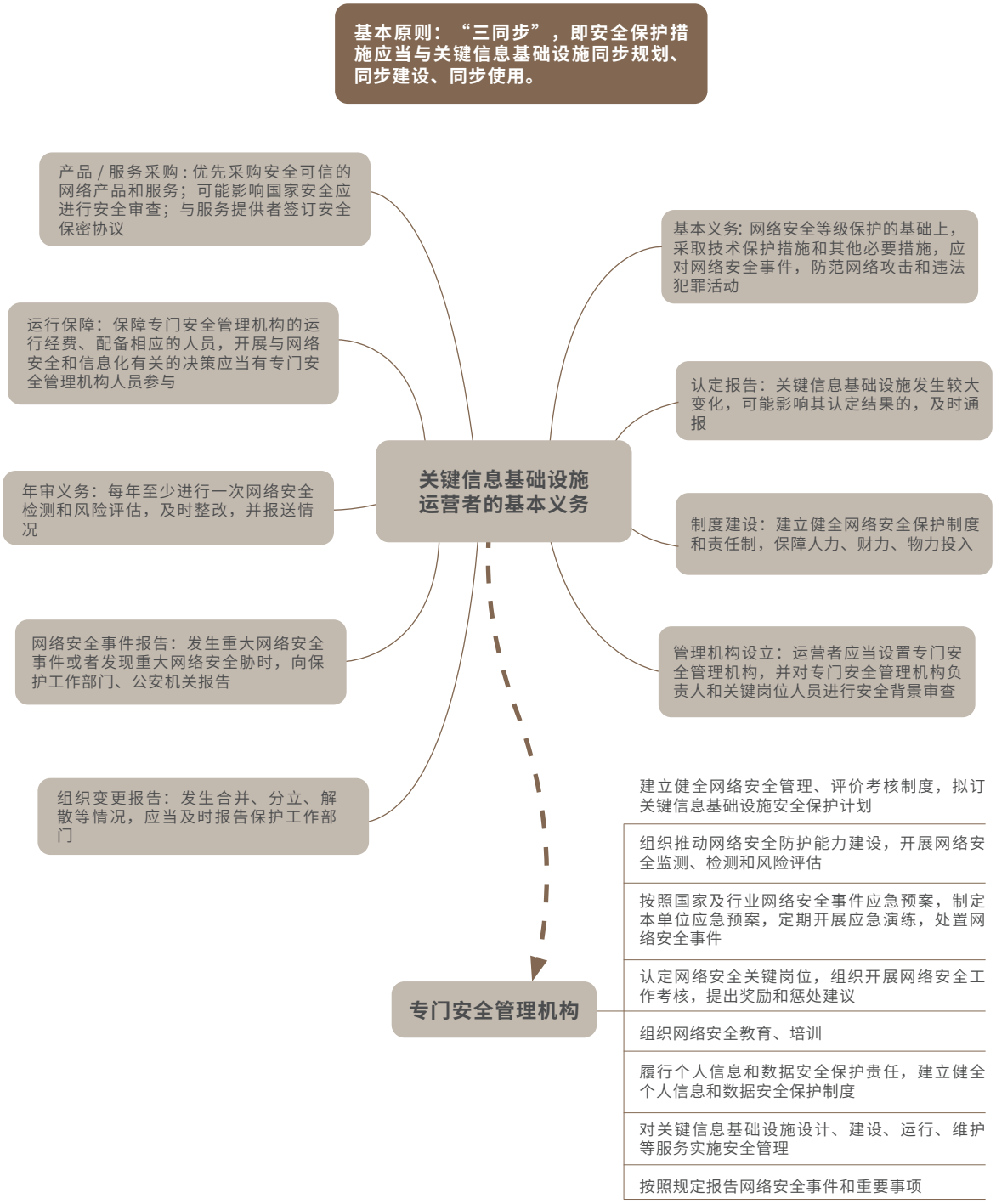
二、关键信息基础设施运营者的基本义务

（一）CII 运营者义务概述

《CII 条例》第四条规定：关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（“**运营者**”）主体责任。为此，《CII 条例》第三章专章规定了运营者的具体义务，并在《网安法》的基础上，进行了更为具体、全面且深入的规定。据报道，《CII 条例》带来的安全投入规模预计将达到百亿元级。[5] 因此，运营者应当严格依照《CII 条例》以及其他法律法规的要求，严格落实针对 CII 的网络安全保护义务。

我们总结了《CII 条例》中规定的运营者的九大基本义务，以及其下设的专门安全管理机构的八大义务，如下图所示：

[5] 张蕊 . 《关键信息基础设施安全保护条例》出炉 预计将带来百亿级安全投入规模 [N]. 每日经济新闻 ,2021-08-19(002).



（二）与《网安法》的衔接

四部门在就《CII 条例》答记者问时曾强调，《CII 条例》的一个重要的总体思路就是做好与相关法律、行政法规的衔接，即在《网安法》确立的制度框架下，细化相关制度措施，同时处理好与相关法律、行政法规的关系[6]。《网安法》第三章第二节对 CII 的运行安全作出了明确规定，相关要求在《CII 条例》中进一步得到重申与细化。例如，《网安法》第三十三条规定了 CII 安全保障的“三同步”原则，即“保证安全技术措施同步规划、同步建设、同步使用”，而《CII 条例》在第三章开篇便再次强调了该基础原则。此外，《网安法》规定的运营者设置安全管理机构和负责人和进行安全背景审查，以及在采购网络产品和服务时

[6] 耀文 . 四部门负责人就《关键信息基础设施安全保护条例》答记者问 [N]. 中国电子报 ,2021-08-20(003).

进行国家安全审查和保密协议签订等义务，也分别在《CII 条例》第十四条、十九条和第二十条得到重申。

值得注意的是，《CII 条例》对《网安法》第三十四条第一款规定的“设置专门安全管理机构”作出进一步规定，并明确了其具体义务。具体而言，专门安全管理机构是运营者的内设机构，具体负责本单位的 CII 的安全保护工作，其运行经费、配备相应的人员等均有运营者保障。同时，《CII 条例》要求运营者在开展与网络安全和信息化有关的决策时，应当有专门安全管理机构人员参与。此外，《网安法》第三十四条明确的运营者的部分安全保护义务，包括定期进行教育培训与考核、制定应急预案与应急演练等，也由专门安全管理机构一并承接。《网安法》第三十四条第三款规定的“对重要系统和数据库进行容灾备份”虽并未在《CII 条例》中具体规定，但信息系统的容灾备份既是个人信息和数据安全保护的考察重点，理论上也是 CII 运维安全管理的重要组成部分，从上位法规定角度，这一要求同样构成 CII 运营者应当同步落实的安全保障措施。

（三）与《网络安全审查办法》的衔接

《CII 条例》第十九条要求运营者优先采购安全可信的网络产品和服务，如该等产品和服务可能影响国家安全，还应当按照国家网络安全规定通过安全审查；该义务是对《网安法》第三十五条的重申。我们理解，此处“国家网络安全规定”主要指《网络安全审查办法》（以下简称**《审查办法》**）。近期，有关部门也在尝试就《审查办法》根据国内网络安全相关的立法与实践进行修订与更新，引起业界不小的关注。

此处所指的“网络产品和服务”，结合《审查办法》的规定，主要包括核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对 CII 安全有重要影响的网络产品和服务。根据《审查办法》，运营者在采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。如影响或者可能影响国家安全，则应当向网信办下属的网络安全审查办公室申报，提交申报书、报告、采购文件等材料。同时，运营者就已申报的采购活动，还应通过采购文件、协议等要求该等产品和服务提供者配合执法者进行网络安全审查，并督促其履行其在网络安全审查中作出的承诺。

三、CII 的监管落地

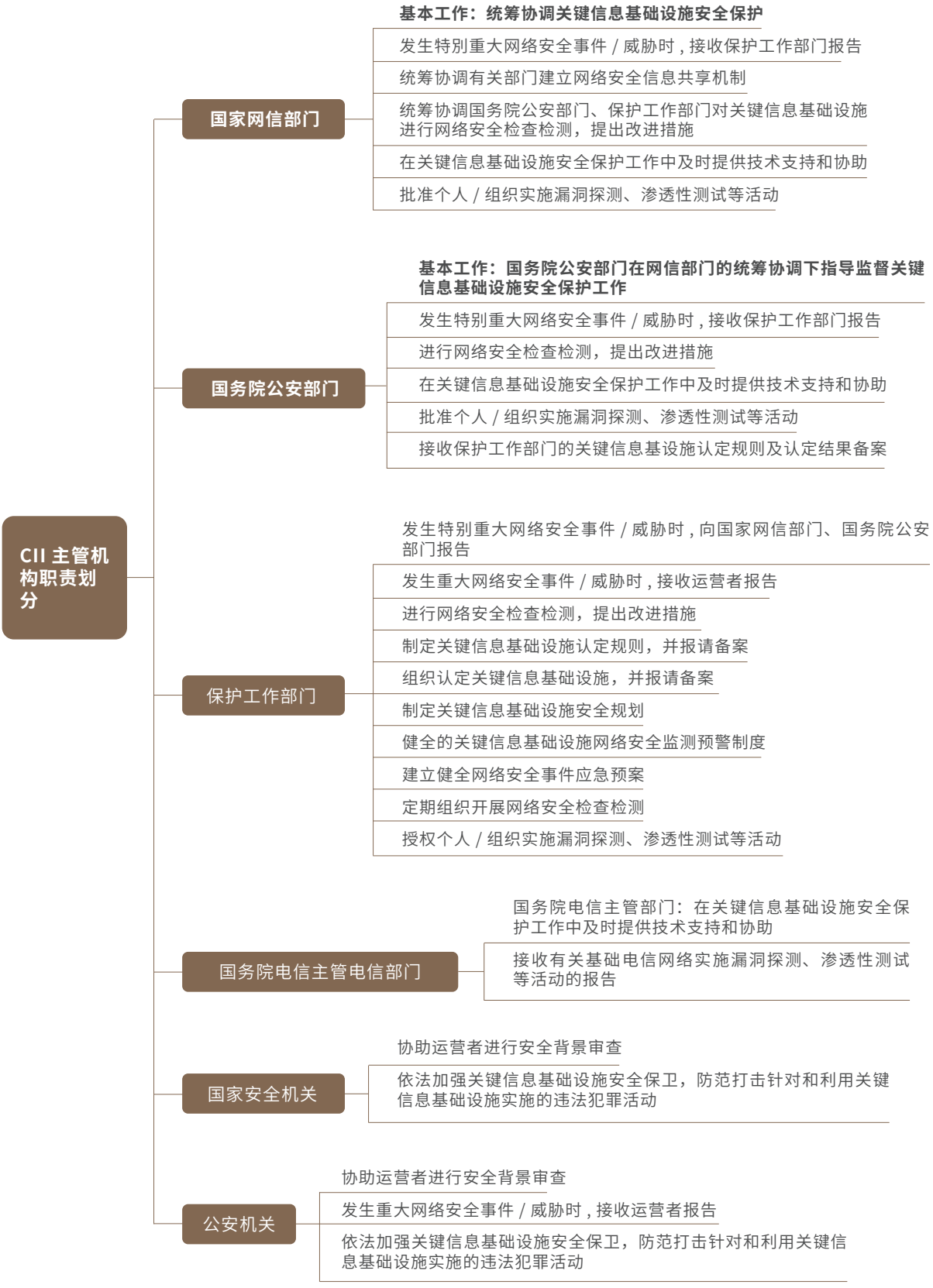
（一）CII 监管保护“各司其职”

在 CII 的监督管理体制方面，《CII 条例》第三条明确了各个监管机构的职责分工。具体而言，国家网信部门负责 CII 安全保护的统筹协调，而国务院公安部门则负责具体指导监督 CII 的安全保护工作。国务院电信主管部门和其他有关部门依照《CII 条例》及其他相关法律、行政法规的规定，在各自职责范围内负责 CII 安全保护和监督管理工作，而省级人民政府有关部门依据各自职责对 CII 实施安全保护和监督管理。

较之于此前的《征求意见稿》第四条，《CII 条例》有明显的变更：首先，《CII 条例》再次强调了网信部门在 CII 的安全保护工作中“统筹协调”的地位，但删除了“相关监督管理工作”的表述。其次，《CII 条例》明确了公安部门对 CII 指导监督的基本职能，该规定进一步明确了监管机构的职权划分，能够有效预防不同机构之间职权交叉与冲突的情况。再次，《CII 条例》将此前《征求意见稿》中“国家安全、国家保密行政管理、国家密码管理等部门”这一列举式表述改为了“国务院电信主管部门和其他有关部门”的定性式表述，这一改动强调了国务院电信主管部门在 CII 保护和监管中的作用，有效防止定义过宽或是过窄，同时还规避了“泄露关键信息基础设施清单”的情况。[7] 最后，地方层面的管理机构由县级以上提升至省级，从监管级别层面进一步提升了 CII 安全保护和监督管理的重要程度。

具体到上述机构的职权方面，《CII 条例》着重规定了网信部门、公安机关、电信部门、负责关键信息基础设施安全保护工作的部门（“保护工作部门”）等机构的职权。具体而言，上述机构的职权如下图所示：

[7] 南方都市报 APP • 隐私护卫队课题组，《关键信息基础设施保护条例：由行业监管部门负责制定认定规则》，https://m.mp.oeeee.com/a/BAAFRD000020210817579889.html，最后访问日期：2021 年 8 月 21 日。



不难看出，《CII 条例》强调了本行业、本领域的保护工作部门在 CII 的认定与保护工作中的重要性。我们理解，考虑到行业主管部门在各自领域、行业长期的执法实践，在准确识别、认定、保护和管理 CII 上拥有更多经验。当出现网络安全问题时，行业主管部门也可以结合行业实践，寻求更符合行业特征的解决方式。但是，考虑到网络安全作为一种不断变化、不断演进的非传统风险，行业主管部门在统筹传统安

全和非传统安全的过程中也可能出现无法及时应对新型安全威胁因素、不同行业安全保障措施标准不一等问题。因此，《CII 条例》着重强调了国家网信办在 CII 保护与监督执法中的统筹地位，以及公安部的指导监督作用。通过网信办与公安部的统一指导监督，能够有效统筹各个行业、各个领域在 CII 安全保障层面的基本要求，保障《CII 条例》在各个行业的适用性。

（二）CII 保护细则形成“纵横体系”

《CII 条例》作为我国 CII 安全保障方面的首部行政法规，为保障 CII 的各项监督管理制度能够有效实施，通过一个更为完备、全面、精细的法规体系支持其进一步落地，从行业、地方、标准化等多个方面对 CII 的安全保障实现多方位、立体化的规则设定，同样构成《CII 条例》发挥其提纲挈领地位的重要内容。

首先，在行业层面，《CII 条例》对保护工作部门提出了制定本行业、本领域 CII 安全规划，建立网络安全监测预警制度，健全网络安全事件预案等要求。基于此，建立、健全本行业、本领域 CII 配套安全管理体系将成为相关重要行业和领域的主管、监管部门的重要职责。这将为《CII 条例》及运营者的 CII 安全保障义务在具体行业的横向落地提供便利与保障。

其次，在地方层面，《CII 条例》第三条规定省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理，使得 CII 在横向的行业保护的基础上，能够有效地通过地方政府有关部门的安全保障和监管措施得以纵向践行。

再次，在标准化建设层面，《CII 条例》第三十四条同步要求国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作，表明国家在推动 CII 安全保护标准化体系方面的决心。与网络安全、个人信息保护类似，标准化工作也将为 CII 领域在行业和地方安全保护细则的基础上提供有益补充，为包括主管、监管部门和企业在内的各类主体在 CII 的认定与保护工作中提供更具有实践意义的深化指引。此前，信安标委制定了《信息安全技术 网络安全等级保护基本要求》等多部网络安全等级保护相关的行业标准，对包括 CII 运营者在内的所有网络运营者均具有重要的参考意义，涉及的维度包括但不限于基本保护要求、安全保护要求、安全控制措施、防护能力评价要求、供应链安全要求。当前，针对 CII 安全保障体系建设，信安标委也在积极推动 9 项相关标准的研制工作，围绕安全保障体系建设各维度，从边界识别、保护要求、控制措施、保障指标、应急体系、检查评估以及供应链安全、数据安全、信息共享、监测预警等方面系统开展标准研制与标准试点工作。信安标委还选取金融、能源、交通等多个行业的运营者展开标准试点，验证标准的可行性、合理性与完备性[8]。通过地方与行业规则的纵横部署，辅之以标准化体系建设，将能够有效保障《CII 条例》全局性、概括性、总体性规定得以进一步细化和落地。

结语

从国家战略高度，关键信息基础设施的保护工作历来是国家网络安全战略部署的核心要素之一。早在 2016 年 7 月，中共中央办公厅、国务院办公厅印发的《国家信息化发展战略纲要》就明确提出要“加快构建关键信息基础设施安全保障体系，加强党政机关以及重点领域网站的安全防护，建立政府、行业与企业网络安全信息有序共享机制”[9]。特别是在近期因某些企业赴境外上市而引发国内监管部门发动网络安全审查之际，作为网络安全审查核心角色的关键信息基础设施，其具体识别和边界认定更加成为行业内争相讨论却悬而不决的热门话题。因此，对于特别是处于重要行业领域或扮演行业领域内基础设施角色的企业而言，在看待《CII 条例》规则时不可忽视与之相互呼应和配套的网络安全保护规则，严格把握和评估自身业务的安全风险，审时度势，谋求业务的稳健发展：

- 密切关注行业主管部门在 CII 识别认定方面的最新动向，与主管、监管部门及地方政府部门保持持续沟通。
- 结合 CII 识别现有规则趋势，必要情况下对自身网络信息系统构成 CII 的可能性展开内部评

[8] 杨建军，《标准助力关键信息基础设施安全保障体系建设》，http://www.moj.gov.cn/pub/sfbgw/zcjd/202108/t20210817_435024.html，最后访问日期：2021 年 8 月 21 日。
[9] 中共中央办公厅 国务院办公厅印发《国家信息化发展战略纲要》，http://www.gov.cn/xinwen/2016-07/27/content_5095336.htm，最后访问日期：2021 年 8 月 22 日。

估，形成事先预期，为未来可能的 CII 保护工作做好提前预备。

- 关注与 CII 保护相配套的具体规则制定和落地情况，特别是对于 CII 涉及的网络产品和服务采购引发的网络安全审查、CII 个人信息和重要数据跨境等专门的制度规范，提前形成风险防范意识。

附：《CII 条例》与《征求意见稿》条文对比

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
目录	第一章　总则 第二章　支持与保障 第三章　关键信息基础设施范围 第四章　运营者安全保护 第五章　产品和服务安全 第六章　监测预警、应急处置和检测评估 第七章　法律责任 第八章　附则	第一章　总则 第二章　关键信息基础设施认定 第三章　运营者责任义务 第四章　保障和促进 第五章　法律责任 第六章　附则
意见稿对应章节	**意见稿对应条文内容**	**第一章 总则**
第一章 总则	第一条 为了保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，制定本条例。	第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。
第三章 关键信息基础设施范围	第十八条 下列单位运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围： （一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位； （二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位； （三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位； （四）广播电台、电视台、通讯社等新闻单位； （五）其他重点单位	第二条 本条例所称关键信息基础设施，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。
第一章 总则	第四条 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。 国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。 县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。	第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。 省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第一章 总则	第三条 关键信息基础设施安全保护坚持顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。	第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。
	第六条 关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。	第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。 任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。
第二章 支持与 保障	第八条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动。	
	第十六条 任何个人和组织不得从事下列危害关键信息基础设施的活动和行为： （一）攻击、侵入、干扰、破坏关键信息基础设施； （二）非法获取、出售或者未经授权向他人提供可能被专门用于危害关键信息基础设施安全的技术资料等信息； （三）未经授权对关键信息基础设施开展渗透性、攻击性扫描探测； （四）明知他人从事危害关键信息基础设施安全的活动，仍然为其提供互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等帮助； （五）其他危害关键信息基础设施的活动和行为。	
第四章 运营者 安全保护	第二十三条 运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改： （一）制定内部安全管理制度和操作规程，严格身份认证和权限管理； （二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为； （三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月； （四）采取数据分类、重要数据备份和加密认证等措施。	第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
		第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。
意见稿对应章节	**意见稿对应条文内容**	**第二章 关键信息基础设施认定**
第一章 总则	第四条第一款 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。	第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。
第三章 关键信息基础设施范围	第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。 国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。 关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。	第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。 制定认定规则应当主要考虑下列因素： （一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度； （二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度； （三）对其他行业和领域的关联性影响。
		第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。
	第二十条 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。 国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。	第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。
意见稿对应章节	**意见稿对应条文内容**	**第三章 运营者责任义务**
第四章 运营者安全保护	第二十一条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。	第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第四章 运营者安全保护	第二十二条 运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。	第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。
	第二十四条 除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务： （一）设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查； （二）定期对从业人员进行网络安全教育、技术培训和技能考核； （三）对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施； （四）制定网络安全事件应急预案并定期进行演练； （五）法律、行政法规规定的其他义务。	第十四条 运营者应当设置专门安全管理机构，并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。审查时，公安机关、国家安全机关应当予以协助。
	第二十三条 运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改： （一） 制定内部安全管理制度和操作规程，严格身份认证和权限管理； ……	第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责： （一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划； （二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估； （三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件； （四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议； （五）组织网络安全教育、培训； （六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度； （七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理； （八）按照规定报告网络安全事件和重要事项。
	第二十四条 除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务： …… （四）制定网络安全事件应急预案并定期进行演练； ……	
	第二十五条 运营者网络安全管理负责人履行下列职责： （一）组织制定网络安全规章制度、操作规程并监督执行； （二）组织对关键岗位人员的技能考核； （三）组织制定并实施本单位网络安全教育和培训计划； （四）组织开展网络安全检查和应急演练，应对处置网络安全事件； （五）按规定向国家有关部门报告网络安全重要事项、事件。	

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第四章 运营者安全保护	第二十七条 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于 1 个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于 3 个工作日。	
	第二十八条第一款 运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。	
		第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。
第四章 运营者安全保护	第二十八条第二款 运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时进行整改，并将有关情况报国家行业主管或监管部门。	第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。
		第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。 发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。
第五章 产品和服务安全	第三十一条 运营者采购网络产品和服务，可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。	第十九条 运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。
		第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。
		第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
意见稿 对应章节	意见稿对应条文内容	第四章 保障和促进
第二章 支持与保障	第十三条 国家行业主管或监管部门应当设立或明确专门负责本行业、本领域关键信息基础设施安全保护工作的机构和人员，编制并组织实施本行业、本领域的网络安全规划，建立健全工作经费保障机制并督促落实。	第二十二条 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。
第六章 监测预警、 应急处置和 检测评估	第三十六条 国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息。	第二十三条　国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。
	第三十八条 国家网信部门统筹协调有关部门、运营者以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享。	
	第三十七条 国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息。 国家行业主管或监管部门应当组织对安全监测信息进行研判，认为需要立即采取防范应对措施的，应当及时向有关运营者发布预警信息和应急防范措施建议，并按照国家网络安全事件应急预案的要求向有关部门报告。	第二十四条　保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。
	第三十九条 国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。 国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况。	第二十五条　保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第六章 监测预警、应急处置和检测评估	第四十条 国家行业主管或监管部门应当定期组织对本行业、本领域关键信息基础设施的安全风险以及运营者履行安全保护义务的情况进行抽查检测，提出改进措施，指导、督促运营者及时整改检测评估中发现的问题。 国家网信部门统筹协调有关部门开展的抽查检测工作，避免交叉重复检测评估。 第四十四条 有关部门组织开展关键信息基础设施安全检测评估，不得向被检测评估单位收取费用，不得要求被检测评估单位购买指定品牌或者指定生产、销售单位的产品和服务。	第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。 第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。 有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。
	第四十一条　有关部门组织开展关键信息基础设施安全检测评估，应坚持客观公正、高效透明的原则，采取科学的检测评估方法，规范检测评估流程，控制检测评估风险。 运营者应当对有关部门依法实施的检测评估予以配合，对检测评估发现的问题及时进行整改。	第二十八条　运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。
		第二十九条　在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。
	第四十三条　有关部门以及网络安全服务机构在关键信息基础设施安全检测评估中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。	第三十条　网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。
第二章 支持与保障	第十六条　任何个人和组织不得从事下列危害关键信息基础设施的活动和行为： …… （三）未经授权对关键信息基础设施开展渗透性、攻击性扫描探测； …… （五）其他危害关键信息基础设施的活动和行为。	第三十一条　未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第二章 支持与保障	第十四条　能源、电信、交通等行业应当为关键信息基础设施网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持。	第三十二条　国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。 能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。
	第十五条　公安机关等部门依法侦查打击针对和利用关键信息基础设施实施的违法犯罪活动。	第三十三条 公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。
	第十条　国家建立和完善网络安全标准体系，利用标准指导、规范关键信息基础设施安全保护工作。	第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。
	第九条　国家制定产业、财税、金融、人才等政策，支持关键信息基础设施安全相关的技术、产品、服务创新，推广安全可信的网络产品和服务，培养和选拔网络安全人才，提高关键信息基础设施的安全水平。	第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。
		第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。
		第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。
第八章 附则	第五十四条　军事关键信息基础设施的安全保护，由中央军事委员会另行规定。	第三十八条　国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。
意见稿 对应章节	**意见稿对应条文内容**	**第五章 法律责任**
第七章 法律责任	第四十五条　运营者不履行本条例第二十条第一款、第二十一条、第二十三条、第二十四条、第二十六条、第二十七条、第二十八条、第三十条、第三十二条、第三十三条、第三十四条规定的网络安全保护义务的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款： （一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第七章 法律责任		（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的； （三）未建立健全网络安全保护制度和责任制的； （四）未设置专门安全管理机构的； （五）未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的； （六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的； （七）专门安全管理机构未履行本条例第十五条规定的职责的； （八）未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的； （九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的； （十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。
		第四十条　运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。
	第四十七条　运营者违反本条例第三十一条规定，使用未经安全审查或安全审查未通过的网络产品或者服务的，由国家有关主管部门依据职责责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	第四十一条　运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 倍以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。
		第四十二条　运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第七章 法律责任	第四十八条　个人违反本条例第十六条规定，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款；构成犯罪的，依法追究刑事责任。 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本条例第十六条规定，受到刑事处罚的人员，终身不得从事关键信息基础设施安全管理和网络运营关键岗位的工作。	第四十三条　实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处 5 日以下拘留，可以并处 5 万元以上 50 万元以下罚款；情节较重的，处 5 日以上 15 日以下拘留，可以并处 10 万元以上 100 万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处 10 万元以上 100 万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。
	第五十条　有关部门及其工作人员有下列行为之一的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任： （一）在工作中利用职权索取、收受贿赂； （二）玩忽职守、滥用职权； （三）擅自泄露关键信息基础设施有关信息、资料及数据文件； （四）其他违反法定职责的行为。	第四十四条　网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。
		第四十五条　公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。
		第四十六条　网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。
	第五十一条　关键信息基础设施发生重大网络安全事件，经调查确定为责任事故的，除应当查明运营单位责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。	第四十七条　关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
		第四十八条　电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。
		第四十九条　违反本条例规定，给他人造成损害的，依法承担民事责任。 违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。
意见稿对应章节	**意见稿对应条文内容**	**第六章 附则**
第八章 附则	第五十三条　存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。 关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。	第五十条　存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。 关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。
	第五十五条　本条例自 **** 年 ** 月 ** 日起施行。	第五十一条　本条例自 2021 年 9 月 1 日起施行。
意见稿对应章节	**意见稿被删减条文内容**	
第一章 总则	第二条　在中华人民共和国境内规划、建设、运营、维护、使用关键信息基础设施，以及开展关键信息基础设施的安全保护，适用本条例。	
	第五条　关键信息基础设施的运营者（以下称运营者）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。 国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。	
	第七条　任何个人和组织发现危害关键信息基础设施安全的行为，有权向网信、电信、公安等部门以及行业主管或监管部门举报。 收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。 有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。	

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第二章 支持与保障	第十一条 地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。	
	第十二条 国家鼓励政府部门、运营者、科研机构、网络安全服务机构、行业组织、网络产品和服务提供者开展关键信息基础设施安全合作。	
	第十七条 国家立足开放环境维护网络安全，积极开展关键信息基础设施安全领域的国际交流与合作。	
第四章 运营者安全保护	第二十六条 运营者网络安全关键岗位专业技术人员实行执证上岗制度。 执证上岗具体规定由国务院人力资源社会保障部门会同国家网信部门等部门制定。	
	第二十九条 运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。	
第五章 产品和服务安全	第三十条 运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。	
	第三十二条 运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测。	
	第三十三条 运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告。	
	第三十四条 关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。	

	关键信息基础设施保护条例（征求意见稿）	关键信息基础设施保护条例（最终稿）
第五章 产品和服务安全	第三十五条　面向关键信息基础设施开展安全检测评估，发布系统漏洞、计算机病毒、网络攻击等安全威胁信息，提供云计算、信息技术外包等服务的机构，应当符合有关要求。 具体要求由国家网信部门会同国务院有关部门制定。	
第六章 监测预警、应急处置和检测评估	第四十二条　有关部门组织开展关键信息基础设施安全检测评估，可采取下列措施： （一）要求运营者相关人员就检测评估事项作出说明； （二）查阅、调取、复制与安全保护有关的文档、记录； （三）查看网络安全管理制度制订、落实情况以及网络安全技术措施规划、建设、运行情况； （四）利用检测工具或委托网络安全服务机构进行技术检测； （五）经运营者同意的其他必要方式。	
第七章 法律责任	第四十六条　运营者违反本条例第二十九条规定，在境外存储网络数据，或者向境外提供网络数据的，由国家有关主管部门依据职责责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	
	第四十九条　国家机关关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接负责人员依法给予处分。	
	第五十二条　境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门、国家安全机关和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。	

感谢实习生甘雨丰对本文做出的贡献。

八问八答——《网络安全审查办法（修订草案征求意见稿）》重点解读

宁宣凤　吴涵

引言

国家互联网信息办公室于 2021 年 7 月 10 日上午 12 点发布通知，公开征求《网络安全审查办法（修订草案征求意见稿）》（下称“**意见稿**”）意见。考虑到近期国家互联网信息办公室及网络安全审查办公室等监管机构对多家企业采取的监管措施，我们对意见稿部分重点内容进行分析解读，以供大家参考。

一、重点内容解读

本解读主要关注意见稿中的两方面重点内容，其一是本次重点新增问题，其二是基础问题。我们将从这两方面进行逐一介绍。

（一）重点新增问题（文末请见意见稿与现行生效版本之对比表格）

1. 意见稿的适用对象？

意见稿适用对象包括关键信息基础设施运营者以及数据处理者。鉴于其中的数据处理者为新增主体，**因此我们理解，即使企业不落入或者不确定是否落入关键信息基础设施运营者范围，若开展数据处理行为且达到影响或可能影响国家安全的标准，也有较高概率落入意见稿的监管范围。**

2. 主体适用的情况下，满足什么条件需要申报网络安全审查？

如果企业为关键信息基础设施运营者或者数据处理者，则满足以下条件之一即需要申报或通过网络安全审查：

自行申请

- 关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的；
- 掌握超过 100 万用户个人信息的运营者（关键信息基础设施运营者及数据处理者）赴国外上市的。

主动审查

网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务、数据处理活动以及国外上市行为的。

3. 拟在港股上市，是否需要申请网络安全审查？是否也要符合数据出境等合规要求？

意见稿中所使用的表述为“国外上市”而非“境外上市”，我们理解，二者之间可能存在部分差别。

根据《中华人民共和国出境入境管理法》第八十九条，出境是指由中国内地前往其他国家或者地区，由中国内地前往香港特别行政区、澳门特别行政区，由中国大陆前往台湾地区；入境是指由其他国家或者地区进入中国内地，由香港特别行政区、澳门特别行政区进入中国内地，由台湾地区进入中国大陆。由此我们理解，“境外”实际上包含港澳台地区。

而对于“国内”“国外”的区分，我们理解从文义解释，“国内”通常而言应当包含港澳台地区，而“国外”指“中华人民共和国以外的国家和地区”。

在上述理解的前提下，我们理解**港股上市被认定为“国外上市”的可能性相对较低**。但是鉴于我们上述对“境外”和“国外”的解读源于对其他领域法律的研究和参考，且本意见稿中并未对相关术语进行明确，我们仍无法排除相关概念有其他含义的可能性，建议对相关法律动态保持跟踪和关注。

对于港股上市过程及上市后数据传输至香港而言，参照《信息安全技术 数据出境安全评估指南》内“数据出境”的定义，其主要指“网络运营者通过网络等方式，将其在中华人民共和国**境内运营中收集和产生的个人信息和重要数据**，通过直接提供或开展业务、提供服务、产品等方式**提供给境外的机构、组织或个人**的一次性活动或连续性活动”，因而从“境内”“境外”划分的角度并结合上述对概念的解读，我们理解，**数据传输至香港仍应属于数据跨境，因此企业需要满足我国《网络安全法》《数据安全法》及配套措施内有关数据跨境的规定**。

4. 100 万用户个人信息是指 100 万条个人信息还是 100 万人的个人信息？

与此要求类似的规定可见于《国家网络安全检查操作指南》中“认定关键信息基础设施”部分。在认定关键信息基础设施时所考查的因素包括“注册用户数超过 1000 万”“日均访问量超过 100 万人次”“造成超过 100 万人个人信息泄露”等，均从个人信息主体数量而非个人信息数量的角度进行规定。

鉴于《国家网络安全检查操作指南》与意见稿具有类似的立法目的，即对可能影响个人数量较多的实体或者活动（包括但不限于赴国外上市）进行严格监管，以保障经济和民生利益，我们理解，意见稿中的“100 万用户个人信息”指 100 万自然人个人信息的可能性较高。

5. 如何理解“掌握”个人信息，如仅提供存储或传输服务，或委托云服务商等其他第三方处理，是否落入监管范围？

我们理解，“掌握”个人信息这一表述与“控制者”的概念存在相似之处，因此对其的解读可以参考对控制者的定义。但鉴于我国目前在法律层面尚未进行控制者和处理者的明确区分，从监管趋严的角度而言，我们建议企业将物理上的数据的控制以及法律上对数据的处置均纳入此范畴并申请网络安全审查。

6. 申报网络安全审查需要提交什么材料，IPO 材料需要提供多少？

申报材料应当包括：

（一）申报书；

（二）关于影响或可能影响国家安全的分析报告；

（三）采购文件、协议、拟签订的合同或拟提交的 IPO 材料等；

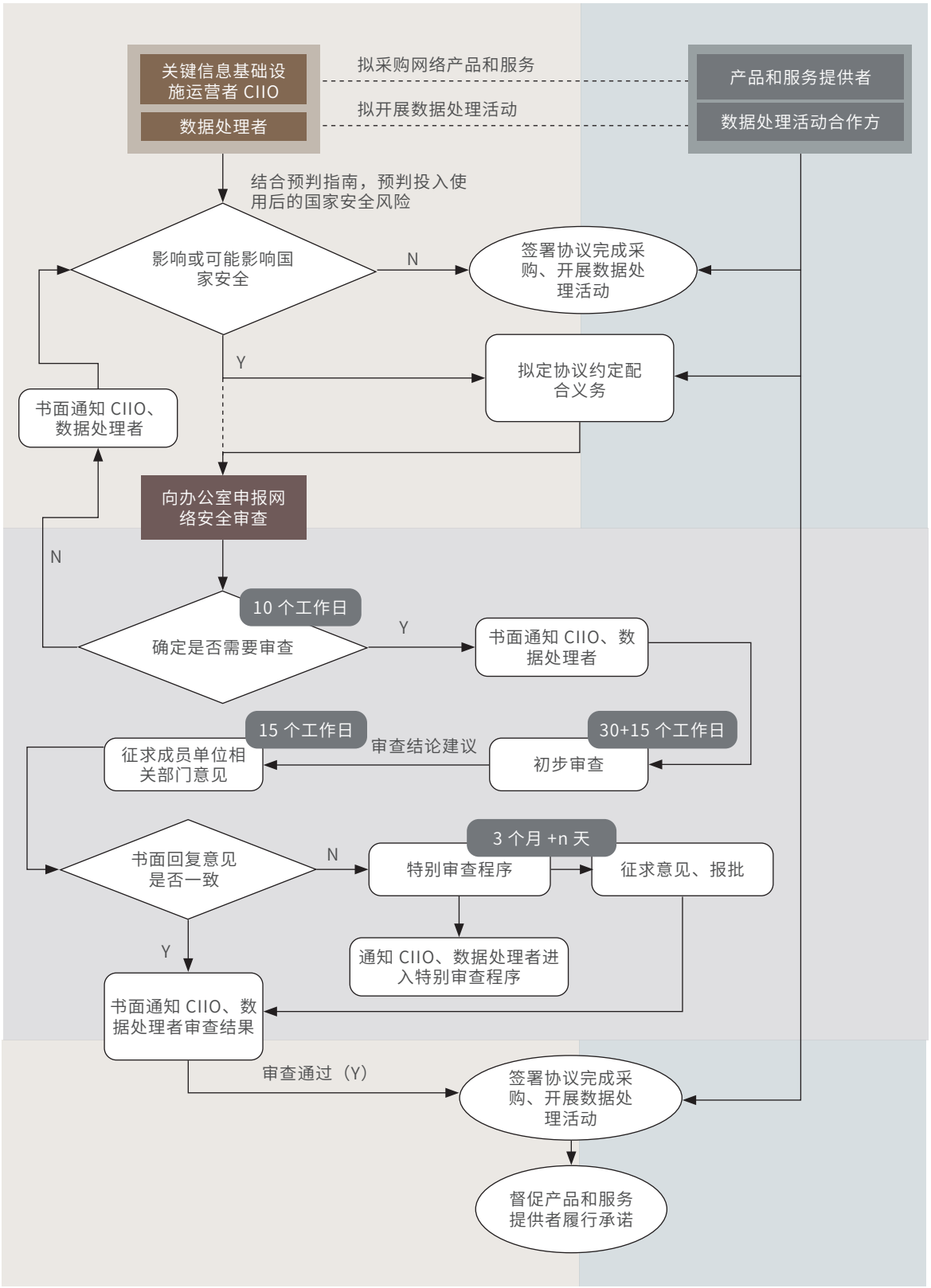
（四）网络安全审查工作需要的其他材料。

具体而言，参考数据安全等相关立法，我们理解分析报告可能包含供应链安全、数据安全及合规、数据出境、司法管辖冲突解决机制等多项内容。出于审查目的考虑，我们理解 IPO 材料可能包括招股书等，但是否包括工作底稿还有待确定。

7. 网络安全审查需要多长时间，是否会影响上市进程？

根据意见稿的规定，网络安全审查办公室应当自收到审查申报材料起，10 个工作日内确定是否需要审查并书面通知运营者。如果认为需要开展网络安全审查的，自向运营者发出书面通知之日起 30 个工作日内完成初步审查，情况复杂的可以延长 15 个工作日。网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门自收到审查结论建议之日起 15 个工作日内向运营者书面回复意见。网络安全审查工作机制成员单位意见不一致的，按照特别审查程序处理，特别审查程序一般应当在 3 个月内完成，情况复杂的可以延长。

总的来说，一般程序所需时间，自申报开始，最长需要 10+30+15+15=70 个工作日。而对于特别审查程序，最长为：70 个工作日 +3 个月 +n ≈ 135+n 个工作日，即实际所需自然日可能达到 180 日（6 个月）以上。



8．意见稿生效时间

鉴于近期较为活跃的网络安全审查执法趋势以及意见稿对赴国外上市等活动的重点监管，我们不排除

意见稿较快生效的可能性。但即使还未生效或者推迟生效，考虑到当前已经有企业被查处，我们理解，企业提前准备应对措施而非以未生效为由对抗可以在一定程度上降低风险。

（二）基本问题

1. 什么是关键信息基础设施运营者？

关键信息基础设施包括公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等**重要行业和领域**，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，但其具体范围和安全保护办法暂未正式出台。

在 2020 年公安部发布的《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》中，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主管、监管部门应制定**本行业、本领域关键信息基础设施认定规则**并报公安部备案。同时应将符合认定条件的**基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象**纳入关键信息基础设施。

2. 网络安全审查的主管机构有哪些？

主要包括**国家网络安全审查工作机制**和**网络安全审查办公室**。

其中，网络安全审查工作机制由国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局组建。同时，本次意见稿还将中国证券监督管理委员会纳入工作机制范畴。

网络安全审查办法（对比版）

原版	修订草案征求意见稿
第一条 为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，制定本办法。	第一条 为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》，制定本办法。
第二条 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。	第二条 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，数据处理者（以下称运营者）开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。
第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。	第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。

原版	修订草案征求意见稿
第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家网络安全审查工作机制。 网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。	第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。 网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。
第五条 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。	第五条 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。
	第六条 掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
第六条 对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。	第七条 对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。
第七条 运营者申报网络安全审查，应当提交以下材料： （一）申报书； （二）关于影响或可能影响国家安全的分析报告； （三）采购文件、协议、拟签订的合同等； （四）网络安全审查工作需要的其他材料。	第八条 运营者申报网络安全审查，应当提交以下材料： （一）申报书； （二）关于影响或可能影响国家安全的分析报告； （三）采购文件、协议、拟签订的合同或拟提交的 IPO 材料等； （四）网络安全审查工作需要的其他材料。
第八条 网络安全审查办公室应当自收到审查申报材料起，10 个工作日内确定是否需要审查并书面通知运营者。	第九条 网络安全审查办公室应当自收到审查申报材料起，10 个工作日内确定是否需要审查并书面通知运营者。

原版	修订草案征求意见稿
第九条 网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，主要考虑以下因素： （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险； （二）产品和服务供应中断对关键信息基础设施业务连续性的危害； （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险； （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况； （五）其他可能危害关键信息基础设施安全和国家安全的因素。	第十条 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，主要考虑以下因素： （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险； （二）产品和服务供应中断对关键信息基础设施业务连续性的危害； （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险； （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况； （五）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险； （六）国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险； （七）其他可能危害关键信息基础设施安全和国家数据安全的因素。
第十条 网络安全审查办公室认为需要开展网络安全审查的，应当自向运营者发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；情况复杂的，可以延长 15 个工作日。	第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向运营者发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；情况复杂的，可以延长 15 个工作日。
第十一条 网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。 网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见一致的，网络安全审查办公室以书面形式将审查结论通知运营者；意见不一致的，按照特别审查程序处理，并通知运营者。	第十二条 网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。 网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见一致的，网络安全审查办公室以书面形式将审查结论通知运营者；意见不一致的，按照特别审查程序处理，并通知运营者。
第十二条 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关~~关键信息基础设施保护工作~~部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知运营者。	第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知运营者。
第十三条 特别审查程序一般应当在~~45 个工作日内~~完成，情况复杂的可以适当延长。	第十四条 特别审查程序一般应当在 3 个月内完成，情况复杂的可以延长。

原版	修订草案征求意见稿
第十四条 网络安全审查办公室要求提供补充材料的，运营者、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。	第十五条 网络安全审查办公室要求提供补充材料的，运营者、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。
第十五条 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务、数据处理活动以及国外上市行为，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。	第十六条 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务、数据处理活动以及国外上市行为，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。
第十六条 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。	第十七条 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。
第十七条 运营者或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。	第十八条 运营者或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。
第十八条 运营者应当督促产品和服务提供者履行网络安全审查中作出的承诺。 网络安全审查办公室通过接受举报等形式加强事前事中事后监督。	第十九条 运营者应当督促产品和服务提供者履行网络安全审查中作出的承诺。 网络安全审查办公室通过接受举报等形式加强事前事中事后监督。
第十九条 运营者违反本办法规定的，依照《中华人民共和国网络安全法》~~第六十五条~~的规定处理。	第二十条 运营者违反本办法规定的，依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》的规定处理。
第二十条 本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。 本办法所称网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。	第二十一条 本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。
第二十一条 涉及国家秘密信息的，依照国家有关保密规定执行。	第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。
~~第二十二条 本办法自 2020 年 6 月 1 日起实施，《网络产品和服务安全审查办法（试行）》同时废止。~~	

感谢实习生张子谦对本文的贡献！

主 要 作 者

宁宣凤

susan.ning@cn.kwm.com

吴　涵

wuhan@cn.kwm.com

刘　迎

liuying3@cn.kwm.com

陈胜男

chenshengnan@cn.kwm.com

颜婷婷

yantingting@cn.kwm.com

潘　驰

panchi@cn.kwm.com

赵天琦

zhaotianqi@cn.kwm.com

姚敏侣

yaominlv@cn.kwm.com

张凯勋

zhangkaixun@cn.kwm.com

林云汉

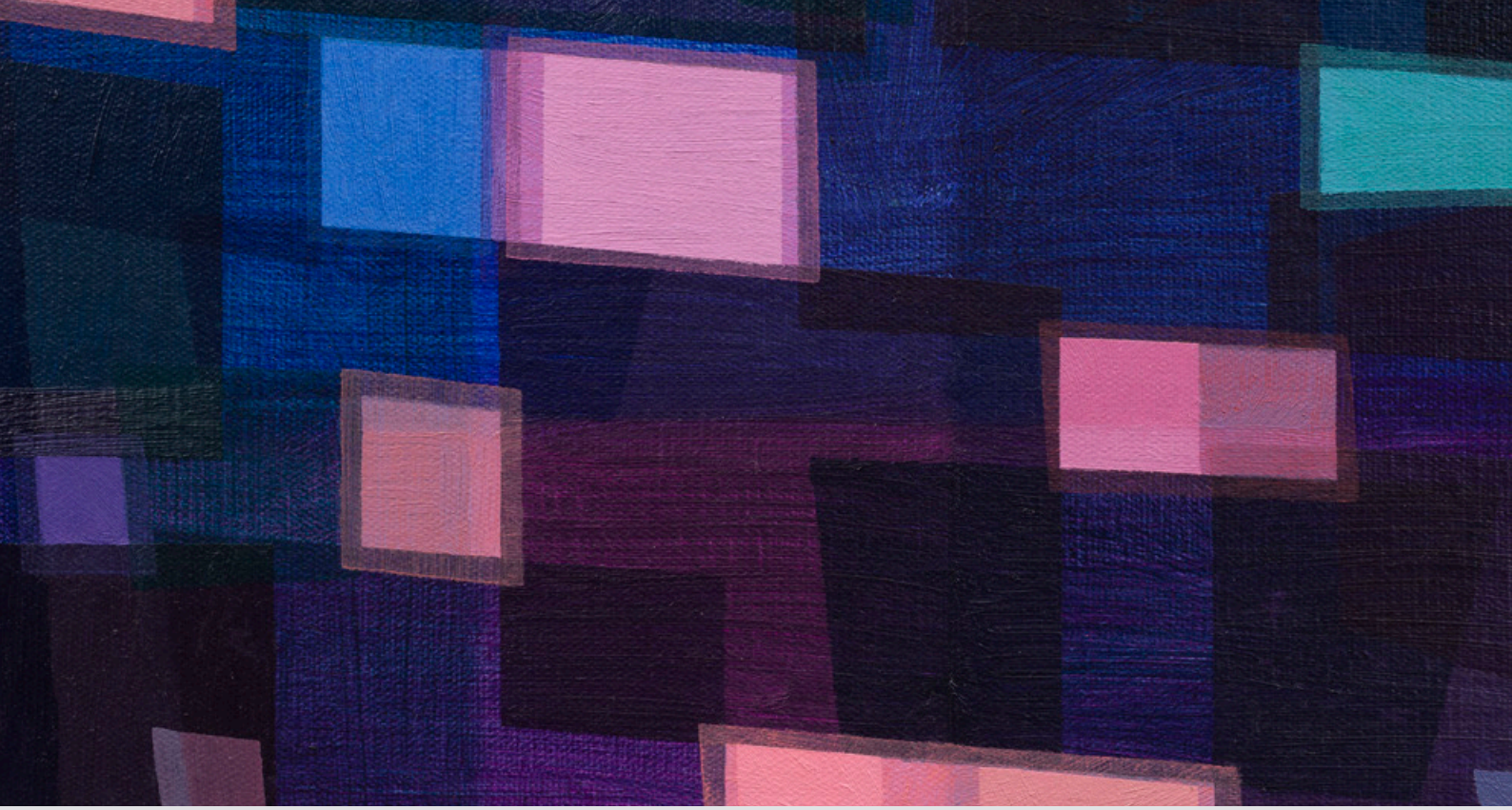
linyunhan@cn.kwm.com

屈尘

quchen1@cn.kwm.com

陈虹吕

chenhonglv@cn.kwm.com



金杜律师事务所

金杜律师事务所被广泛认为是全球最具创新力的律所之一，能够提供与众不同的商业化思维和客户体验。金杜拥有近 3000 多名律师，分布于全球 30 个城市，借助统一的全球平台，协助客户了解当地的挑战，应对地域性复杂形势，提供具有竞争优势的商业解决方案。

作为总部位于亚洲的国际领先律师事务所， 我们为客户发掘和开启机遇，协助客户在亚洲市场释放全部潜能。凭借卓越的专业知识和在核心市场的广泛网络，我们致力于让亚洲走向世界，让世界联通亚洲。

我们始终以伙伴的合作模式为客户提供服务，不止步于满足客户所需， 更关注实现客户目标的方式。我们不断突破已取得的成就，在重塑法律市场的同时，打造超越客户预期的律师事务所。

金杜法律研究院是由金杜律师事务所和金杜公益基金会联合发起成立的非营利性研究机构。自设立以来，一直致力于打造具有国际影响力的中国特色新型智库，依托于金杜律师事务所过往二十多年来服务国家经济建设和法治建设过程中所积累的丰富执业经验和专业洞见，对企业“走出去”战略中面临的重要问题进行分析研究，以提供具有建设性和实操性的政策建议和咨询意见。

金杜研究院
KWM_CHINA

如需了解更多信息，请访问 kwm.com。