个人信息保护法
企业合规启示报告

下篇
企业合规风险研判

SFC 南方财经全媒体集团
Southern Finance Omnimedia Corp.
21世纪经济报道 21st CENTURY BUSINESS HERALD | 21财经 掌握全球财经脉搏
南方财经全媒体集团合规科技研究院

前言

近年来，伴随着数字经济发展，对个人信息的采集和利用成为一种“刚需”。个人信息保护不断涌现出新问题，随意收集、违法获取、过度使用、非法买卖个人信息等情况“野火烧不尽”。信息数据的挖掘利用与个人保护之间张力扩大，急需专门法律对个人信息处理活动提供规范样本。

放眼全球，个人信息保护立法在如火如荼地展开，目前已经有128个国家通过立法保护个人信息和隐私。欧盟《通用数据保护条例》、美国加利福尼亚州隐私保护法的出台，在国际上颇具影响力。

《个人信息保护法》在此背景下被纳入立法进程，并在各方推动下不断提速，千呼万唤始出来。2021年8月20日，《个人信息保护法》由第十三届全国人民代表大会常务委员会第三十次会议通过，自2021年11月1日起施行。

《个人信息保护法》共8章74条。在有关法律的基础上，该法进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。该法成为我国迈入数字化社会，彰显“以人为本”的法律制度里程碑，也是我国为全球数字治理贡献的中国方案。

南方财经全媒体集团合规科技研究院长期关注个人信息保护议题，持续跟踪报道立法进程、监管动态、公众呼

声。借《个人信息保护法》落地之际推出解读报告，分析当前“大数据杀熟”、强制同意、人脸识别、超大型平台义务等多项热点。

报告分为上下两篇，上篇《个人信息处理新变局》梳理立法路径与模式，聚焦个人信息处理逻辑的转变，下篇《企业合规风险研判》则将目光放到企业合规的重点与难点，以及新的信息处理机制在数字经济发展中面临的新挑战。

本篇展现企业在个人信息权带来的冲击下，存在的八大合规风险。对企业成本压力的提升、敏感个人信息的处理、超大型平台的责任、个人信息跨境流动进行分析；梳理受《个人信息保护法》的影响，竞争执法产生的不确定性，公益诉讼将开启的新局面；解读个人信息保护与反垄断的竞合以及与经济发展的平衡。

目录

一、企业合规成本上升

一直以来，企业作为个人信息采集主体，在权利天平中占据绝对高地。《个人信息保护法》明确了在个人信息处理活动中个人的各项权利，包括知悉个人信息处理规则和处理事项、同意和撤回同意，以及个人信息的查询、复制、更正、删除等总结提升为知情权、决定权。

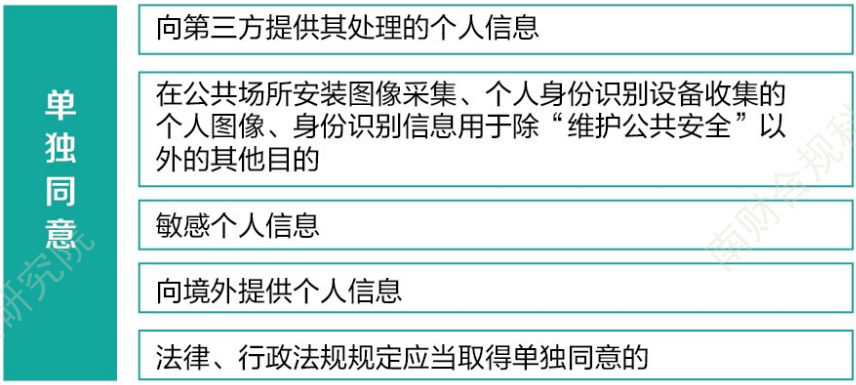
这意味着，用户的权利地位得到很大的转变，一改企业强势、用户弱势的局面，企业处理个人信息的逻辑需进行调整，面临巨大的合规压力。

1. 个人信息自主权带来冲击

《个人信息保护法》明确了用户享有的一系列个人信息权利，企业负有协同配合用户权利行使的义务。只要进行个人信息收集的企业都必须知道他们拥有哪些个人信息、存储在何处、如何处理这些信息以及与谁共享这些信息等，需要根据用户需求，灵活和准确地响应数据主体访问查询、同意、更正、删除、数据迁移等要求。

“单独同意”也增加了企业信息转移时的合规负担。《个人信息保护法》第二十三条要求：如果企业向第三方提供其处理的个人信息，应向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

《个人信息保护法》三审过程中，不少委员提到这一规定不利于数据流动。对于企业而言，转移个人信息必须通知个人并取得单独同意，法律的合规成本较高，操作层面实现难度大。



可以预见，《个人信息保护法》和《数据安全法》落地后，为响应法律，企业合规成本必然增加，部分业务需要进行较大的调整。人员、管理制度与流程构建以及由此产生的效率下降、业务重构、管理系统的构建以及运维成本等将成为企业无可回避的支出。

从更广泛的视域审视，欧盟《通用数据保护条例》（简称GDPR）落地后给企业带来的合规成本的增加，可以作为参考。根据《福布斯》报告，GDPR让美国财富500强企业多花费了78亿美元合规成本，普华永道给出更明确的合规成本估计：68%的公司预计将花费100万到1000万美元。

2. 个人信息全生命周期管理

数字经济下，新技术、新应用、新模式层出不穷，极大地增加了企业风险，并产生了更复杂的合规义务。

法律规定原则性框架，企业需思考落实到每个业务环节，从数据安全生命周期角度制定了一系列数据安全管理制度，以保证收集、存储、使用、处理/加工、交换/提供、删除的合规和安全性。

个人信息全生命周期管理

事前评估

评估情形	● 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
评估内容	● 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

收集

- 限于实现处理目的的最小范围，不得过度收集个人信息
- 遵循“告知-同意”原则

处理

共同处理	● 应当约定各自的权利和义务 ● 侵害个人信息权益造成损害的，应当依法承担连带责任

委托处理	个人信息处理者	受托人
	与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等 对受托人的个人信息处理活动进行监督	按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息 委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留 未经个人信息处理者同意，受托人不得转委托他人处理个人信息

（续上表）

个人信息全生命周期管理

转移个人信息（因合并、分立、解散、被宣告破产等）	 **转移方** 向个人告知接收方的名称或者姓名和联系方式	 **接收方** 继续履行个人信息处理者的义务 变更原先的处理目的、处理方式的，应重新取得个人同意。
向第三方提供	● 向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类 ● 取得个人的单独同意 ● 接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息 ● 接收方变更原先的处理目的、处理方式的，重新取得个人同意	
自动化决策	● 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 ● 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	
公共采集	● 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需 ● 遵守国家有关规定，并设置显著的提示标识 ● 收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外	

（续上表）

个人信息全生命周期管理

公开	● 不得公开其处理的个人信息，取得个人单独同意的除外 ● 在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外 ● 处理已公开的个人信息，对个人权益有重大影响的，应当取得个人同意
删除	● 处理目的已实现、无法实现或者为实现处理目的不再必要 ● 个人信息处理者停止提供产品或者服务，或者保存期限已届满 ● 个人撤回同意 ● 个人信息处理者违反法律、行政法规或者违反约定处理个人信息 ● 法律、行政法规规定的其他情形
存储	● 以显著方式、清晰易懂的语言真实、准确、完整地向个人告知保存期限 ● 除另有规定外，保存期限为实现处理目的所必要的最短时间 ● 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，应将境内收集和产生的个人信息存储在境内 ● 非经主管机关批准，不得向外国司法或者执法机构提供存储于境内的个人信息

二、敏感个人信息处理风险

敏感个人信息处理规则

定义

- 一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息
- 生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息
- 不满十四周岁未成年人的个人信息

处理前提

- 具有特定的目的和充分的必要性
- 采取严格保护措施
- 取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定
- 告知处理的必要性以及对个人权益的影响，规定可以不向个人告知的除外
- 处理不满十四周岁未成年人个人信息的，应取得其父母或者其他监护人的同意
- 事前影响评估
  - 处理目的、方式等是否合法、正当、必要
  - 对个人权益的影响及安全风险
  - 保护措施是否合法、有效并与风险程度相适应

监管要求

- 为不满十四周岁未成年人制定专门的个人信息处理规则
- 影响评估报告和处理情况记录至少保存三年

《个人信息保护法》设专节对处理敏感个人信息作出更严格的限制，第二十八条至第三十条在定义、处理规则上作出要求。其他章节中，第五十五条对事前影响评估进行规定，第六十二条提出监管将制定专门的个人信息保护规则、标准。

1. 人脸信息

人脸信息作为生物识别信息属于敏感个人信息，除敏感个人信息专节规制之外，第二十六条进一步强调在公共场所安装图像采集、个人身份识别设备的要求，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。只能用于维护公共安全的目的，取得个人单独同意的除外。

人脸识别正在迎来强监管时代。4月，信安标委就国家标准《信息安全技术 人脸识别数据安全要求》征求意见；7月，最高人民法院发布《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，提出7种处理人脸信息构成侵害人格权益的情形，为相关民事案件的审判提供裁判指引。

人脸信息的采集目的、范围、场所、处理方式、个人同意原则等具体内容正逐步完善，对人脸信息控制者提出了明确且严格的要求。

国家对人脸信息的重视程度不仅从个人信息保护出发，还在于人脸信息属于数据信息，是优化公共服务的数据支撑，具有公共资源属性。保护人脸识别信息，一定程度上是保护网络安全以及国家整体安全。

2. 医疗健康信息

医疗健康个人信息，主要指与个人生命健康、医疗诊断和治疗有关的个人信息。具有以下特征：第一，人身依附性，与特定个人主体

紧密相连；第二，敏感性，一旦泄露、非法提供或滥用，可能危害人身和财产安全，个人名誉、身心健康受到损害或歧视性待遇；第三，大数据属性，如果将某一群体的医疗信息整合，将产生社会和商业价值[①]。

近年来，医疗个人信息和隐私保护的法律规范，见于《侵权责任法》《精神卫生法》《传染病防治法》《网络安全法》《国家健康医疗大数据标准、安全和服务管理办法（试行）》《人口健康信息管理办法（试行）》《人类遗传资源管理条例》等法律法规中，特别对医疗健康信息的跨境传输进行了更严格的规制。国家标准层面，2020 年 12 月，信安标委发布《信息安全技术健康医疗信息安全指南》，针对常见医疗健康应用场景提出安全措施建议。

《个人信息保护法》聚焦个人信息，将医疗健康信息作为敏感个人信息实行更严格的保护。同时，鉴于此类信息的特性，突破了将“个人同意”作为处理医疗健康信息的唯一依据。第十三条将应对突发公共卫生事件，或者紧急情况下保护自然人的生命健康和财产安全，作为处理个人信息的合法情形之一。这对于疫情时期公民出行必须填写“健康码”等特殊情况给出了法律许可。

对于医疗健康行业，在已有法律法规上，更注重健康医疗企业的信息化建设，保障网络安全及数据保护，例如国家健康医疗主管部门制定明确的等保工作意见。立法趋势更关注互联网医疗的合规管理，以及与电子商务、广告营销、商保医保等不同渗透场景的规范化管理[②]。

3. 不满 14 周岁未成年人信息

我国未成年人的互联网普及率已达 99.2%，显著高于总体互联网普及率 64.5%。此外，未成年人首次触网年龄不断降低，10 岁及以下开始

接触互联网的人数比例达到78%[③]。

未成年人的个人信息保护一直是全球个人信息保护的重点之一。2019年10月出台《儿童个人信息网络保护规定》，2020年10月二次修订后的《未成年人保护法》新增了“网络保护”章节和个人信息保护条款，凸显我国的高度重视。

《个人信息保护法》第三十一条将不满14周岁未成年人的个人信息作为敏感个人信息，要求个人信息处理者对此制定专门的个人信息处理规则。

这一规定同样见于2021年7月出台的《深圳经济特区数据条例》及2020年10月施行的《信息安全技术个人信息安全规范》中。这也符合GDPR第三十八条中关于儿童因为不了解个人数据相关风险、后果、权利和保障措施，因而需要特殊保护的规定。

对于未成年人的同意，《个人信息保护法》第三十四条规定，应获得未成年人的父母或者其他监护人同意，与《未成年人保护法》第七十二条表述一致。

4. 合规要点

4.1人脸信息

4.1.1密切关注行业立法与监管态势

当前，人脸信息受到多部法律法规及监管部门的规制，国家层面后续也将出台针对人脸识别、人工智能等新技术、新应用而制定专门的个人信息保护规则、标准。企业需积极应对相关主管部门对人脸识别技术应用有关的规范出台情况，及时调整自身处理人脸识别信息的制度规范。

例如在小区物业的人脸识别上，杭州、四川等地方相继修订发布

物业管理条例草案，拟将“不得强制业主通过指纹、人脸识别等生物信息方式使用共用设施设备”纳入条例。此类立法动向值得智慧安防、智慧社区业务的企业重点关注[④]。

相较于地方性立法，最高人民法院2021年7月出台的《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》已经直接规定物业不得将人脸识别作为进出小区的唯一方式，需要特别关注。

4.1.2 改变一揽子告知同意的方式

浙江宁波20家房企被罚203万释放监管讯号——即便设置了采集人脸信息的提示标识，但未经消费者同意仍不能免罚。

特别注意针对APP处理人脸信息时，需取得用户的单独同意。APP可能需要依据使用功能设置多个用户同意界面，在使用人脸信息页面由用户逐一勾选同意。这一规定将倒逼企业更注重APP产品功能设计，合规管理海量用户的同意范围。如何精细化管理收集的信息，对企业也是较大挑战。

4.1.3 合规的关键是赋予个人选择权

从多起人脸识别的案例来看，对企业在信息收集场景下的合规设计提出了更高的要求，强制索取及捆绑索权问题也需高度重视并完善改进。企业不得要求用户同意处理其人脸信息才提供产品或者服务，除非处理人脸信息属于提供产品或者服务所必需；不得以授权捆绑、强迫或变相强迫等方式要求用户同意处理其人脸信息。

人脸信息处理

处理流程	合规建议
 收集	• 风险评估，遵循“合法、正当、必要”的原则 • 明确告知人脸信息处理者身份、联系方式、目的、方式和种类等，告知必要性及对个人影响 • 取得个人的单独同意 • 建立非人脸识别身份识别方式以供选择使用 • 企业符合免责的事由依据留痕
 处理	• 完善对外业务及内部规范制度，不得泄露、出售或者非法向他人提供 • 将信息提供给他人处理应取得单独同意，告知处理相关信息 • 变更处理目的和方式的，应重新取得个人同意
 存储	• 采取加密保护、隔离存储、脱敏使用等措施确保安全 • 不具备处理使用的必要性后及时且彻底的销毁 • 信息发生或可能发生泄露、损毁、丢失时，及时履行通知和补救义务

4.2 医疗健康

4.2.1 注重数据类型的监管体系

当前，从医疗行业看来，不同法律法规界定差异显著，部分采取囊括式的界定方式，涵盖医疗行业经营过程中可能涉及的相关数据，如“健康医疗大数据”与“人口健康信息”，体现国家对医疗行业数据整体的监管态势。从信息安全监管出发，与个人信息、网络安全、信息安全等相关的法律法规中，医疗健康信息或数据同样保护严格。

4.2.2 明确数据来源的合规性

开展医疗数据的商业合作中，涉及医疗健康信息的流转，应确认数据提供方收集、共享相关个人信息的合法合规性，或是否已进行充分的脱敏处理。企业利用患者个人信息进行人工智能算法训练时，同样应注意是否已获得充分的患者知情同意或已进行充分的脱敏处理。

4.3 未成年人

4.3.1 建立儿童专门的个人信息保护规则及专岗

企业应建立儿童或未成年个人信息专门的个人信息处理规则，设置专门的儿童个人信息保护负责人。明确应用主要面向儿童的年龄段以及所属的常规应用类别，并且发出准确声明。特别说明监护人应履行的监护职责，对征得监护人的同意后收集和使用儿童个人信息制定规范；在收集信息的评估风险阶段，必须考虑对儿童产生任何影响的可能性和严重程度；在信息存储时，将相应儿童个人信息分割独立存储。

4.3.2 以儿童的最大利益原则设计产品功能

由于年龄的特殊性，对于面向全年龄段用户的产品及服务建议设置儿童模式，在儿童身心健康发展及权益保障上有更多考量。

英国的《适龄设计法规》（Age Appropriate Design Code，AADC）提到限制使用“轻推技术”。“轻推技术”指刻意引导或鼓励用户在决策时遵循设计者首选路径而采用的策略，例如设计者希望获得用户授权的场合，其通常把同意授权的选项做得更为显眼。这可能导致儿童被鼓励允许平台获取比他们自愿提供更多的个人数据，或引导儿童在个性化隐私设置时选择较少的隐私增强选项。

4.3.3 广告符合面向儿童的标准

如果应用中投放广告，必须对广告产品及服务、营销手段及呈现方式上进行重点评估，可以在儿童模式下提供一键关闭广告的选择。

三、超大型平台责任加重

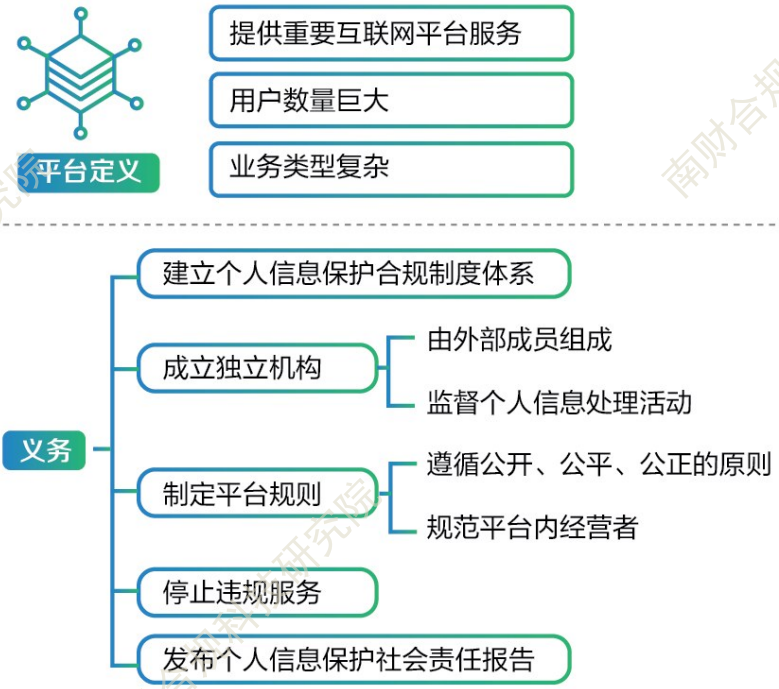
《个人信息保护法》首次从法律层面明确提出加强超大型互联网平台个人信息保护义务的要求。

第五十八条规定，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，应当履行下列义务：建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构进行监督；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；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；定期发布个人信息保护社会责任报告，接受社会监督。

这一法条强调数据治理要多方参与，增加独立第三方的制约，同时要有更高的透明度，以强化对平台的监督。

第五十二条的要求一定情况下同样适用于超大型互联网平台。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。应当公开个人信息保护负责人的联系方式，并将其姓名、联系方式等上报。

超大型互联网平台个人信息保护



1. 重要互联网平台服务

在《个人信息保护法》二审稿时，“重要互联网平台服务”被表述为“基础性互联网平台服务”。当时，学界引入“守门人”概念，作为理解“基础性互联网平台服务”的参考。

中国人民大学法学院教授张新宝将“守门人”界定为“控制关键环节，有资源赋予其他个人信息处理者处理个人信息能力的互联网运营者”，主要包括应用程序的分发平台，比如苹果、谷歌、华为、腾讯、百度等；提供系统权限供APP调度的操作系统，比如苹果的iOS、谷歌的安卓、华为鸿蒙系统等；以及搭载小程序的大型APP，省略用户下载、安装、注册、卸载APP的过程，实现即点即用[5]。

2021年8月，国务院公布《关键信息基础设施安全保护条例》，作为《网络安全法》的重要配套法规，对关键信息基础设施范围认定、运营者责任义务等进行规定。

由于关键信息基础设施，包括公共通信和信息服务等重要行业和领域的网络设施、信息系统，而大型互联网平台用户规模普遍在亿级以上，掌握海量个人信息和重要数据，一旦遭到破坏或者丧失功能、发生数据泄露，危害程度不亚于传统行业，有可能被纳入关键信息基础设施的范围[6]。

8月24日，《关键信息基础设施安全保护条例》国务院政策例行吹风会上，国家互联网信息办公室网络安全协调局局长孙蔚敏表示，前述《条例》9月1日实施后，将重点抓的工作之一，即是要求经营者全面落实安全保护的主体责任。主要从五个方面开展：一是建立健全网络安全保护制度和责任制，实行一把手负责制，保障人力、财力、物力的投入。二是要设置专门的安全管理机构参与网络安全和信息化的决策，履行《条例》规定的8项工作职责。三是开展网络安全检测和风险评估，并及时整改。四是建立并落实网络安全事件和网络安全威胁的报告制度。五是要优先采购安全可信的网络产品和服务，按照规定申报网络安全审查。

2. 增加独立第三方的制约

成立主要由外部成员组成的独立机构，对个人信息处理活动进行监督，是为了应对大型互联网平台拥有的海量数据，以及民众在使用产品和服务、维权过程中所面对的数据壁垒和业务不透明情况。

外部人员组成的独立机构，突出外部性和独立性，更能保证客观公正。有助于提高企业在产品和服务的设计过程中对于各方利益诉

求的事先考虑及平衡。对于消费者而言，外部监督的存在对用户权益的维护，尤其是在维权渠道的畅通性有更好助力。

如何保持外部机构的独立性，还待进一步明确。政府后续或颁布相应规定，对参与该独立机构外部成员的任职资格、义务规范和法律责任等作出要求，通过定期发布报告对外披露信息，提高中立性和透明度，使平台及机构均接受更广泛的外部社会监督，避免个人信息在平台算法的“黑匣子”中存在被不当采集和不当利用的可能性。

3. 公平合理对待平台内经营者

当前，数据和流量成为网络市场竞争的关键要素，大型互联网平台及平台内普通经营者都可能通过滥用个人信息不当获利。从实践情况来看，平台实施的限制行为隐蔽性强，给监管执法增加了难度。

基于这些现状，相较《个人信息保护法》草案二审稿，《个人信息保护法》增加了大型互联网企业制定有关个人信息保护的平台规则时，应当遵循公开、公平、公正的原则对待平台内经营者。

为进一步压实平台的主体责任，还增加了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。

4. 个人信息保护社会责任报告

个人信息保护社会责任报告，同样是法律层面首次明确提出的要求。对于报告内容，还需要后续相关的立法解释、配套规定的明确和实践探索。

与之相类似的企业探索，为部分企业如腾讯、蚂蚁金服、中兴、华为云等发布过的《隐私保护白皮书》。国外也有谷歌、苹果等科技公

司发布《透明度报告》。

5. 合规要点

5.1转变经营理念，业务发展伴随合规驱动

2020年《网络安全审查办法》通过后，“滴滴出行”APP2021年7月因网络安全审查被下架，此后出台的《网络安全审查办法（修订草案征求意见稿）》将数据处理活动纳入网络安全审查范围。

尽管个人数据的取得、加工、分析已经成为互联网驱动企业获得竞争优势的关键，但作为超大型平台，其网络、数据安全已经涉及到了国家安全领域，将直接关系到业务发展乃至企业生存，不能忽视存在的网络安全隐患和管理漏洞而去片面重视追求经济效益，未来通过违规收集用户个人信息以此进行“大数据分析”“千人千面”等间接牟利行为不可取。

5.2 在顶层设计上构建有效的合规体系

设置专门安全管理机构。重新审查企业内部治理结构、规章制度、人员管理等方面存在的问题，制定可行的合规管理规范，健全合规风险检测、防范、报告、整改机制。超大型平台除须履行《个人信息保护法》的合规义务外，还应注意《关键信息基础设施安全保护条例》等法规项下的合规义务。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，以此确立问责制度合规框架。实践中，曾有不少企业因未确定网络安全负责人而被工信部和公安机关处罚。

设置个人信息保护负责人。如首席数据官、隐私官等专有岗位，建立公开的联系方式，并将其姓名、联系方式等上报监管部门。当

前，已有头部企业搭建个人信息保护合规体系。中兴通讯已建立合规管理委员会并设置专职数据保护官，蚂蚁金服设立首席隐私官并成立隐私保护办公室，小米成立信息安全与隐私委员会统筹集团的信息安全与隐私保护工作。

定期发布个人信息保护社会责任报告。报告内容可以包括公司在个人信息保护顶层设计上的安全战略、合规体系、安全措施、处理安全事件情况等；在合规共建层面，可以聚焦客户、供应商、合作伙伴，同时提升用户参与度，如对用户的普法教育、用户权益主张的响应情况等；在社会实践助力层面，介绍相关安全研究应用、参与立法讨论、举办个人信息保护活动等。

5.3 强化业务链条风险控制

超大型平台大部分可被纳入关键信息基础设施，其供应链曾被网信办重点关注。由于涉及网络产品和服务从无到有再到废弃的整个生命周期，不仅包含传统的生产、仓储、销售、交付等供应链环节，还延伸到产品的设计、开发、集成等生命周期，以及交付后的安装、运维等过程。特别是在供应链全球化和市场全球化的背景下，供应商和客户分布于世界不同的国家，平台还将注意落实国外相关法律法规的要求，优先采购安全可信的网络产品和服务，按照规定申报网络安全审查。

5.4 发挥平台资源优势，助力行业规范

由于超大型平台控制个人信息处理的关键环节，为其他企业提供个人信息的处理通道、空间、技术等资源。平台应发挥资源优势，对平台内制定个人信息保护标准的准入规范，拒绝不达标的企业使用其

服务，同时利用必要的技术手段进行监督，建立相关的投诉机制和投诉受理处置机制。在净化行业信息安全的同时，促进企业自身的良性发展。

四、个人信息跨境流动

我国头部互联网企业已经建成了具有国际领先水平的大数据存储与处理平台，在跨境网络支付、跨境电子商务、信息网络服务等应用领域的发展，必然涉及数据的跨境双向流动。

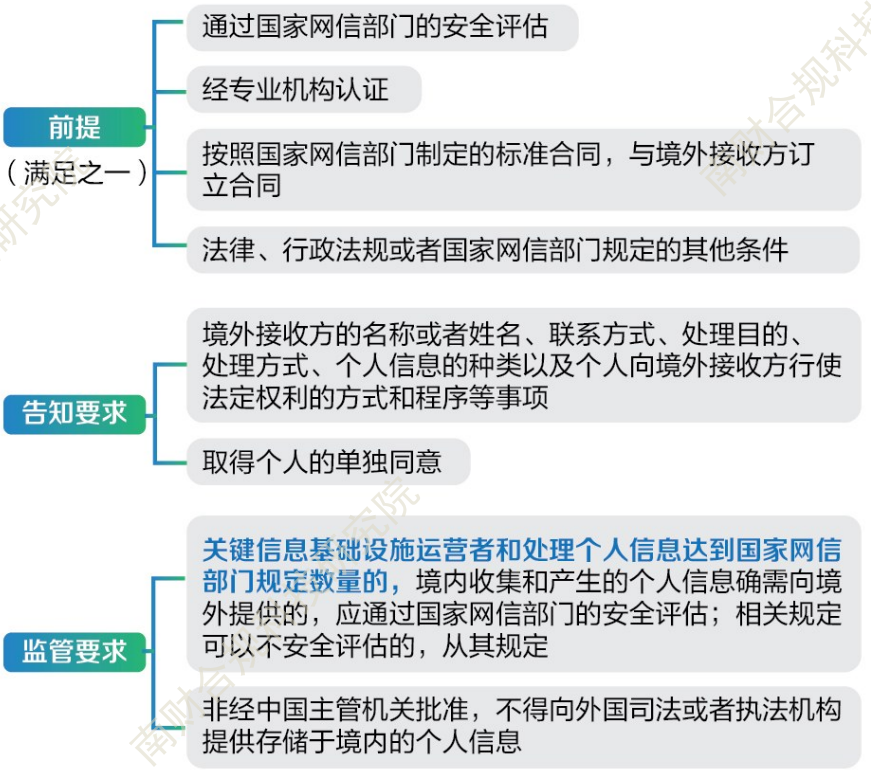
《个人信息保护法》对个人信息跨境流动需要满足的必要前提进行了整合，并将向个人主体的告知和获取个人主体的单独同意作为另一必要前提条件。

1. 完善个人信息跨境提供规则

对于跨境数据的要求，我国多部法律法规以及国家标准进行规制。

2016 年，我国《网络安全法》要求关键信息基础设施的运营者在中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，确需向境外提供的应安全评估。2019 年，网信办出台的《个人信息和重要数据出境安全评估办法》（征求意见稿）则将《网络安全法》中的“关键信息技术设施运营者”扩大到所有“网络运营者”，同时规定“自行评估”和“行业监管部门评估”两种评估形式以及数据出境评估必须每年开展一次。2020 年，信安标委发布的《信息安全技术 数据出境安全评估指南》（征求意见稿），明确“网络运营者”“境内运营”“重

个人信息跨境流动监管规则



要数据”“数据出境”等概念，规定评估总体流程及要点，主要对“出境目的”和“安全风险”进行评估且达到“合理正当”和“安全可控”，同时对数据接收方安全保护能力作出规定，包括接收方主体背景、管理制度、技术手段以及政治法律环境等指标。

根据不同行业的特殊性，监管部门严控数据出境，在金融、征信行业、网络车行业、网络出版和网络地图行业、医疗卫生等特殊领域，必须首先本地化存储，要求服务器设置在境内，或者是某类数据禁止跨

境进行传输。例如医疗数据、人口健康信息相关的服务器要求设置在境内，金融机构要求如果数据传输，只能传递至其子公司、母公司等关联公司，征信数据只能在中国境内处理等。

《个人信息保护法》进一步完善个人信息跨境提供规则。

第四十条明确，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处理者，确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估，与《网络安全法》基本保持一致；对于其他需要跨境提供个人信息的，规定了经专业机构认证等途径。第五十五条与第五十六条同样对向境外提供个人信息作出事前影响评估并对处理情况记录的要求，并提出评估的具体内容。

对跨境提供个人信息的“告知—同意”作出更严格的要求，第三十九条提出，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该法规定权利的方式和程序等事项，并取得个人的单独同意。

对因在境外参与司法程序或面临行政调查，需要向境外提供个人信息的，要求依法申请有关主管部门批准。

2. 个人信息管制和反制条款

出于在全球数据治理博弈中对中国个人数据主体和数据主权的保护，也出于在国际关系中取得微妙的平衡，《个人信息保护法》首次创制对个人数据的管制和反制条款，为将管制和反制对象列入限制或禁止个人信息提供的清单，对于反制对象可以根据实际情况对该国家或者地区对等采取措施。《数据安全法》也提出了应当对属于管制物

项的数据依法实施出口管制。

管制和反制的适用条件在第四十二条及第四十三条进行了严格限制。其中管制的对象为：从事损害了中国数据主体权益或危害中国国家安全、公共利益的个人信息处理活动的境外组织和个人。而反制的对象则是对中国采取歧视性的禁止、限制或者其他类似措施的国家和地区。

3. 建立境外机构在境内的监管

对于境外的个人信息处理者，《个人信息保护法》要求设立境内专门机构或指定境内代表，并要求履行沟通渠道的报送义务，弥补了一直以来针对境外机构监管的敞口，与欧盟GDPR等域外个人信息保护法的机制保持一致性的对等要求。

《个人信息保护法》第五十三条规定，中国境外的个人信息处理者，应在境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送监管部门。

4. 合规要点

4.1 系统部署国内外的合规体系

各行业应基于《个人信息保护法》及《网络安全法》等基本法及所在行业的相关法律法规，确立个人数据出境及信息安全的保障义务。

数据跨境流动已经跨越公司的边界、跨越了国界，企业需要对其位于不同国家的合作伙伴的安全承担同样的责任，并面临更多的监管。当前，各国越来越意识到互联网主权的重要性，对于跨境数据保护标准不统一，法律法规在历史根源、立法模式、规制方式以及司法

确认方面都各不相同，加之国际政治经济局势多变，如企业一旦违法将面临高额罚款。对于“走出去”的企业，应拥有全球化视野，提前做好各国跨境数据法律风险预案。

4.2 完善事先控制，注重数据来源与流向

现阶段，任命个人信息保护负责人，成立相关部门，建立内部合规管理制度和相关措施成为重点与难点。数据跨境流动企业在创建合规和数据治理规定时，对于风险的控制不应仅限于事后补救，而需实现事先控制。

例如，企业需确认自身储存个人数据的内容、地点、方式、来源、流向，储存这些数据的原因以及获取数据的方式，尤其针对存在数据跨境、产品/服务跨境、业务主体跨境等情况的业务场景，了解数据的访问设置、服务器的调用等所涉及的数据是否跨境。

对于具体操作过程中涉及的软件设计，应根据数据在不同法域的风险，设计不同的模块的启动和调用，或者设计不同的版本，以及运用各种必要的技术措施管理数据访问权限，实现数据的分离和对数据访问的控制。对合作的第三方进行管理时，对供应商、分包商、或其他商业合作伙伴，均应在合同关系建立前进行调查和数据风险评估。

五、执法竞争带来的不确定性

对于个人信息保护职责的部门，《个人信息保护法》从中央和地方层面进行了规定，同时兼顾到行业监管差异。对履职部门的职责、可采取的措施及用户投诉举报机制作出要求。

1. 中央与地方共同监管

《个人信息保护法》第六十条规定，在中央层面，由国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。这也意味着，由网信部门集中统一监管体系，工业和信息化部、公安部、中国人民银行等则兼顾各部门和各行业的差异性进行监管。

在地方层面，第六十条明确了由县级以上地方人民政府有关部门履行个人信息保护和监督管理职责。

2. 多部门参与APP执法监管

当前我国APP数量达302万款，成为个人信息保护规范的重要内容。《个人信息保护法》第六十一条对履行个人信息保护职责的部门职责中规定，组织对应用程序等个人信息保护情况进行测评，并公布测评结果。

从监管执法部门对APP的治理过程来看，经历了从内容生态整治到监管个人信息违法违规收集的发展，并呈现多部门参与的执法态势。

工业和信息化部2019年起开展“APP侵害用户权益行为专项整治行动”，规制APP服务提供者、APP分发服务提供者，重点整治违规收集使用用户个人信息等8类问题行为，该项行动仍在有条不紊进行。

公安部则展开“净网”专项行动，集中整治APP违法违规收集使用个人信息行为，2021年3月深化行动，开展侵犯公民个人信息、黑客攻击破坏等十大会战。

国家市场监管总局开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动，《APP违法违规收集使用个人信息专项治理

报告（2019）》显示，共立案1474件，查获涉案信息369万余条，罚没款1946万余元；组织执法联动4225次，行政约谈3536次。

网信办对APP的治理整顿已进入常态化阶段并逐渐细化。2021年网信办对APP治理工作主要聚焦在常见39类APP，一定原因是《常见类型移动互联网应用程序必要个人信息范围规定》刚实施，细化了“必要原则”，明确常见39类APP收集必要信息的界限。

对于企业而言，面临个人信息保护执法“九龙治水”的局面，各部门专项行动各有侧重，执法标准透明度不高，《个人信息保护法》从顶层设计上对APP进行评测，将一定程度上统一标准和流程。

3. 合规要点

3.1 APP企业注重多头监管的具体要求

未来APP的个人信息保护测评将成常态化监管，企业应从管理机制、技术手段、自纠自查等多方面保障用户安全，对于超范围收集、频繁索权、隐瞒第三方SDK收集行为等违规收集个人信息的行为进行日常检测更改。如被监管部门通报，应立即开展问题整改、问题复盘及责任处罚工作。

3.2 加大投入个人信息管理与数据安全技术

工信部网络安全管理局调研员张洪7月曾透露，工信部接下来将立足行业监管职责，重点开展制定出台行业数据安全管理制度，建立数据安全认证体系，开展数据安全监督检查等工作。企业应加大投入，不断优化完善数据脱敏、防泄露、加密等基础性通用性的数据安全技术，加强安全多方计算、联邦学习、可信计算等技术的研究攻关和部署应用。

六、公益诉讼

《个人信息保护法》第七十条规定，个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。在法律层面明确了个人信息保护公益诉讼制度。

个人信息保护公益诉讼

法律法规	起诉主体	内容
《个人信息保护法》	人民检察院、法律规定的消费者组织和由国家网信部门确定的组织	个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的
两高修订《关于检察公益诉讼案件适用法律若干问题的解释》	人民检察院	损害社会公共利益的行为，可提诉讼
最高检《关于积极稳妥拓展公益诉讼案件范围的指导意见》	人民检察院	将个人信息保护作为网络侵害领域的办案重点
最高法《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》	法律规定的机关和有关组织	对处理人脸信息符合民事诉讼法、消费者权益保护法等关于民事公益诉讼规定的，可提诉讼
最高检《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》	人民检察院	履职时重点把握敏感个人信息、特殊群体、重点领域、100万人以上的大规模个人信息、特定对象的个人信息等保护

相较二审稿，此法条对提起诉讼的主体新增“法律规定的消费者组织”，与《消费者权益保护法》相衔接，增强了社会参与力量。对个人信息公益诉讼的形式予以确认，扩大个人信息公益诉讼的适用范围，更好保护公民的个人信息权益。

1. 个人信息保护成为公益诉讼新领域

公益诉讼制度见于我国《民事诉讼法》第五十五条，其规定“对污染环境、侵害众多消费者合法权益等损害社会公共利益的行为，法律规定的机关和有关组织可以向人民法院提起诉讼”。

在个人信息维权案件中，由于案件的专业性、举证能力等限制，用户维权难度很高。通过将个人信息保护纳入检察公益诉讼范围，能够让用户摆脱维权中的弱势地位，对保护个人信息具有重要意义。

最高检第八检察厅厅长胡卫列曾介绍，最高人民检察院2020年9月出台《关于积极稳妥拓展公益诉讼案件范围的指导意见》，明确将个人信息保护作为网络侵害领域的办案重点。检察机关通过办理行政公益诉讼案件，督促协同相关行政机关严格执行监管措施；通过办理民事公益诉讼包括刑事附带民事公益诉讼案件，增加侵权责任主体的违法成本。

近年来各省市已开展个人信息保护案在公益诉讼中的运用。浙江省杭州市下城区人民检察院2021年1月对一起个人信息保护案提起了公益诉讼。该案是《民法典》实施后，全国首例个人信息保护公益诉讼案件。4月，最高人民检察院发布检察机关个人信息保护公益诉讼典型案例，透露将突出办理全国性、有影响力的个人信息保护公益诉讼案件。截至5月，有19个省份明确要求检方积极稳妥开展个人信息保护领域公益诉讼。7月，广东省人民检察院公布了4件关于

个人信息保护检察公益诉讼的典型案例[7]。

检察公益诉讼外，多方力量也参加其中。针对人脸识别相关案件，最高人民法院于2021年7月颁布《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，从民事公益诉讼的角度规定了信息处理者处理人脸信息的行为符合《民事诉讼法》《消费者权益保护法》等关于民事公益诉讼的相关规定时，法律规定的机关和有关组织可以提起民事公益诉讼。

金融账户被《个人信息保护法》纳入为敏感个人信息进行严格保护，基于公益诉讼的规定，考虑到金融领域个人处理具有高度的复杂性、专业性，且涉及主体众多，因此个人信息中涉及金融数据收集、存储、确权、使用、转让、处置、清算产生的纠纷，可由金融法院这类专门法院集中管辖。

8月21日，最高人民检察院下发的《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》明确，根据《个人信息保护法》有关规定，各级检察机关在履行公益诉讼检察职责时应当突出重点、从严把握以下方面：生物识别、宗教信仰、特殊身份、医疗健康、金融账号、行踪轨迹等敏感个人信息应当严格保护；儿童、妇女、残疾人、老年人、军人等特殊群体的个人信息需要特别保护；教育、医疗、就业、养老、消费等重点领域处理的个人信息，以及处理100万人以上的大规模个人信息应当重点保护；对因时间、空间等联结形成的特定对象的个人信息加强精准保护。

2. 合规要点

2.1加强内控工作

企业应提高对自身经营活动中涉及到的与个人信息保护相关法

律法规合规性的关注程度，除了《个人信息保护法》之外，还有《民事诉讼法》《民法典》《消费者权益保护法》《合同法》等。

2.2 建立良好的用户沟通机制

企业面对公益诉讼的压力比个人发起的诉讼更大，几乎很难胜诉，最好的结果是和解。因此，企业应及时排查用户可能面临的各项风险，注意到可能或已有不法分子利用企业产品或服务企图侵害用户权益的情况下，对用户进行明确的风险提示，提供投诉与举报机制，完善客服体系，健全反馈机制。

2.3 梳理明确举证责任

《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》对举证责任的明确，也为企业开展合规工作时需要固定的证据提供了目录。在前期的合规工作中就应当考量相关措施能否作为证据在法庭上进行使用。

七、与反垄断竞合风险

个人信息保护与垄断行为规制看似两个独立的问题，在数字时代发生了关联。个人信息具有丰富的附加价值，效能凸显，涉及相关利益者的复杂性问题，比如数据垄断。尤其是握有大量用户数据的平台企业，个人信息保护与反垄断两条线缠绕在一起，成为不容忽视的合规方向。

从各地数据立法与政策来看，打击数据垄断、数据不正当竞争行为，建立数据分类分级和隐私保护制度也成为高频词汇。

1. 审视数据垄断与个人信息保护关系

数据是信息的表达或承载形式，信息则是数据的实质内涵。个人信息成为构成数据源的基础。

个人信息对企业越来越具有重要的意义。企业之所以能够提供大量的“零价服务”并得以生存，个人信息是重要保障，数字经济下“零价服务”的利润来源主要是个人信息，其对企业的意义为：个人信息能够服务于个性化广告，直接为企业创造利润。第二，个人信息能够帮助企业改善服务，间接为企业创造利润；个人信息积累能够助推企业平台化，夯实企业生存基础[8]。

关于个人信息保护与反垄断的关系需辩证看待：第一，是否会基于个人信息保护为由，做出诸如链接封禁等新型垄断行为；第二，需考虑个人权益的保护。有学者提出，企业间的个人信息保护合谋与支配地位企业的个人信息剥削应被视为新型垄断行为；数据驱动型集中的竞争损害分析应更多关注个人信息的损害。

2. 信息保护与平台垄断的权衡

伴随着个人信息保护法的出台，信息处理行为将更为谨慎，在这种情况下，需警惕平台垄断的新态势。

2021 年，京东、抖音、淘宝纷纷更新订单信息加密通知及系统升级改造方案，对生态链路的消费者敏感个人信息采取脱敏、加密措施，不再向商家、服务商提供明文的消费者敏感个人信息。

平台对订单中的消费者敏感信息脱敏处理，可以降低用户信息泄露风险。这一背景下，平台垄断的可能性同样需要纳入考量范围。由于各平台系统升级后，不同平台加密算法不同，下游只能调整接口以

适配不同电商平台。每一个上游的平台或形成自己体系的话语模式，下游只能被动接受。

在高压的监管态势下，本身就占据资源与技术优势的平台，在保护数据安全的大势下，或进一步巩固自己的数据优势。此时，数据的开放也应一并去研究和尝试，营造更良好的数据生态。

3. 数据可携带权带来的新变化

《个人信息保护法》新增了个人信息的“可携带权”，即个人将个人信息转移至其指定的处理者的权利。

该项权利早在欧盟的 GDPR 中被确立，但自提出便争议不断，落实情况不尽如人意。欧盟将可携带权的客体定为机器可读的个人数据，面临各企业数据不兼容的阻碍。

《个人信息保护法》对于数据可携带权的规定还比较笼统。关于数据可携带权适用的数据范围尚不明确；数据可携带权下传输的数据形式不明确。将“符合国家网信部门规定条件”作为数据可携带权的前置许可，需要网信部门出台具体细化的标准规范。

引入可携带权，初衷是打破信息垄断、不充分竞争的格局，促进信息共享流动，其与反垄断有着千丝万缕的联动效应。

现实中，数据安全保护的技术高低让作为数据主体的消费者用脚投票。在风险较大，且对接收数据企业的技术和安全保障能力缺乏认知的情况下，数据主体转移个人信息的意愿会被明显地抑制，可能更愿意将自己的个人信息储存在那些比较知名、自己相对信得过的大公司系统里，极有可能使得数据自由流动成为一种美好的幻想。

数据可携带权是乌托邦还是中小企业的救命稻草，仍待后续考证。

八、个人信息保护与经济发展的平衡

个人信息权益的保护与数字经济发展两者的兼顾与平衡，是必须要面对的命题。

大数据经济与个人信息保护形成巨大张力，个人信息保护严格，或促使数字经济发展面临多一些压力。故此，必须首先建立个人信息的底线，在此框架内促进数字经济发展。

1. 数据权属与授权明确

要讨论数据要素市场发展、数字产业进步，首先需厘清基于个人信息生成的数据的性质以及权属分配的问题，对个人信息的保护也需要放置到不同场景中考量。

数据的所有权、使用权、管理权、交易权、享有权目前尚无相关的法律充分认同和明确界定。不过，地方立法中已有探索，《深圳经济特区数据条例》第四条、第五十八条、第六十七条对于数据产品和服务的财产权益明确赋权，并明确合法处理形成的数据产品和服务可以依法交易。

根据司法实践可以按以下思路理解：

第一、来源于用户个人信息的单一数据，分散化、碎片化，商业价值有限，无独立的财产权或财产性权益可言；

第二、网络运行者若只是对用户信息进行数字化记录的转换，虽付出了一定劳动，但原始数据仍未脱离原用户信息范围，故网络运营者对于原始网络数据仍应受制于网络用户对于其所提供的用户信息的控制，不能享有独立的权利，网络运营者只能依其与网络用户的约

定享有对原始网络数据的使用权；

第三、对用户个人信息经算法或技术加工处理后的数据，进行大量的智力劳动成果投入，经过深度开发与系统整合，产生大数据产品，独立于网络用户信息、原始网络数据之外，该产品作为经营者的劳动成果，其所带来的权益应当归经营者所享有；

第四、经营者征得用户个人明示同意，在用户同意的范围内对用户个人信息进行分析处理，用户个人信息属于自然人人格权的一部分，其性质不可转让，因此电商平台只可能获取、存储个人信息，但不可能“拥有”。

2.探索新型数据治理之道

守住个人信息安全底线需要严格把控个人信息处理链条的风险，扎紧制度的笼子，利用技术与法律规范相协调，筑牢个人信息安全防线。

中国社会科学院法学研究所副所长、研究员周汉华曾提出探索激励相容的个人数据治理之道。

他认为，在大数据时代，信息控制者（作者注，根据《个人信息保护法》可理解为信息处理者）对于个人信息有很强的利用激励而缺乏同等程度的保护激励。如果法律规则只是简单施加各种禁止性或者强制性规定，势必因为激励不相容影响有效实施。

因此，应以培育信息控制者内部治理机制为目标，将个人信息保护要求嵌入整体信息安全防范体系中，明确各个环节的相关法律义务和组织要求，完善多元参与与互动机制，实现法律规范的外在要求与信息控制者的内在需要激励相容，达到既保护个人信息安全又强化信息控制者的安全防范能力的双赢结果。

相关技术也在不断发展。联邦学习、同态加密、安全多方计算等，均试图在实现有效的数据共享和信息连接的前提下，保证数据安全和隐私。其中，隐私计算技术正成为风口。国内市场规模将快速发展，三年后技术服务营收有望触达100-200亿人民币的空间，甚至将撬动千亿级的数据平台运营收入空间[9]。

隐私计算抛弃直接抹除个人数据中身份信息内容的技术逻辑，而是在数据流动和共享过程中记录所有数据处理流程，预防和遏制相关隐私信息的泄露[10]。不过隐私计算的算力是否能支撑复杂场景，仍需观察。

技术固然是实现合规的关键手段，但是合理、科学的制度也是数据保护过程中必不可少的一环。此外，解决数据流动的问题，也可以通过管理手段实现数据的可知、可控，实现数据合规流动。

个人信息保护需多方共同守住个人信息保护的底线，尊重个人信息权益，共筑数字经济良好生态。

参考资料

①于润东等.“互联网+行业”个人信息保护研究报告(2020 年)[R]. 北京:中国信息通信研究院,2020

②陈际红等. 健康医疗企业 IPO 数据合规重点问题与应对(下)[EB/OL]. 2021[2021-08-23]. http://www.zhonglun.com/Content/2021/03-23/1050543264.html

③季为民等. 青少年蓝皮书:中国未成年人互联网运用报告[R]. 北京:中国社会科学院新闻与传播研究所,中国社会科学院大学新闻传播学院与社会科学文献出版社, 2020.

④杨锦文等. 人脸识别知多少——从“人脸识别第一案”说起[EB/OL]. 2021[2021-08-23]. www.junhe.com/legal-updates/1466

⑤王俊. 个人信息保护法提速 人大教授张新宝建议头部平台承担“守门人”责任[EB/OL]. 2021[2021-08-23]. https://m.21jingji.com/article/20210323/herald/757241fdafb1411933f128079fcb1235.html

⑥张雅婷等.《关键信息基础设施安全保护条例》出台,大型互联网平台或被纳入[EB/OL]. 2021[2021-08-23]. https://m.21jingji.com/article/20210817/herald/30f6c4a51459eaf9fcd167572fb88d0e.html.

⑦张雅婷等. 广东公布 2 起“人脸识别”公益诉讼典型案例,多地个人信息保护公益诉讼进行时[EB/OL]. 2021[2021-08-23]. https://m.21jingji.com/article/20210803/herald/ea82e4bc1696ba3bfcbb5734cdda0bff.html.

⑧焦海涛. 焦海涛:反垄断法应实现“关注个人信息保护”的制度转型[EB/OL]. 2021[2021- 08- 23]. http://www.jcrb.com/xueshupd/cs/202105/t20210525_2282393.html

⑨徐磊等. 隐私计算行业研究报告[R]. 微众银行,毕马威, 2021.

⑩赵精武,周瑞珏.隐私计算技术:数据流动与数据安全的协同保护规则构建[J]. 信息通信技术与政策,2021,47(07):53-58.

学术指导

周辉 中国社会科学院法学研究所副研究员，
中国法学会网络与信息法学研究会副秘书长

致谢

本报告筹备与撰写过程中得到了不少专家、学者支持，在此特别表示感谢。

王新锐 世辉律师事务所合伙人

邓志松 大成律师事务所高级合伙人

张仁卓 北京尚隐科技有限公司CEO

何延哲 中国电子技术标准化研究院网安中心测评实验室副主任

夏海龙 上海申伦律师事务所律师

商希雪 中国政法大学网络法学研究所副所长

何兴驰 上海市锦天城（南京）律师事务所合伙人

监制：虞伟 曹金良
统筹：王俊 张雅婷
研究员/撰写：张雅婷 王俊 郭美婷
设计：林潢 徐晖 默默 邓居轩

2021年8月

南方财经全媒体集团合规科技研究院

关于个人信息保护的问题，您还关注哪些方面？
对我们的报告有什么意见与建议？欢迎沟通。

南方财经全媒体集团合规科技研究院研究员 张雅婷（zhangyt@21jingji.com）
南方财经全媒体集团合规科技研究院研究员 王俊（wangjun@21jingji.com）
南方财经全媒体集团合规科技研究院研究员 郭美婷（guomt@21jingji.com）