LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2592 1978
传真：+852 2868 0883

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

公司及并购法律评述
2019 年 6 月

数据安全立法的总结与创新
——详解《数据安全管理办法》(征求意见稿)

作者：潘永建 | 朱晓阳

中共中央网络安全和信息化办公室(国家互联网信息办公室)(以下简称“**网信办**”)在中国的网络安全立法及执法中均扮演着至关重要的角色。自 2017 年 6 月 1 日《网络安全法》生效以来，网信办共颁布了将近 30 部部门规章(包括征求意见稿)，其中不乏如《关键信息基础设施安全保护条例(征求意见稿)》《个人信息和重要数据出境安全评估办法(征求意见稿)》《区块链信息服务管理规定》等引起社会广泛关注的“重量级”法规。

在《网络安全法》生效将满两周年之际，网信办于 2019 年 5 月 28 日发布了《数据安全管理办法(征求意见稿)》(以下简称“**管理办法**”)。乍看之下，管理办法所规定的内容似乎只是对迄今为止网络安全领域立法的“划重点”及归纳、整理，但仔细研读可以发现，管理办法有其创新性和前瞻性，是对现行网络安全法体系的一次“补强”。

借此管理办法发布之际，通力网安数据团队结合管理办法，从管理办法与现行法律的关系、数据定义、数据活动等问题入手对网络安全法生效以来一直存在的若干重要问题做出解读。

For more Llinks publications, please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

如您需要了解我们的出版物，
请与下列人员联系:

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

1. 管理办法与现行法律的关系

管理办法中主要对 1)适用范围; 2)个人信息和重要数据保护; 3)网络运营者在数据活动中的义务; 4)违法数据活动的法律责任等主要方面做出了规定。上述内容在现行法律中均有规定。例如，个人信息的保护之规定散见于网络安全法及其他法律法规，《网络安全法》《个人信息和重要数据出境安全评估办法(征求意见稿)》《信息安全技术 数据出境安全评估指南(征求意见稿)》等对重要数据的保护作出规定，网络运营者在数据使用过程中的义务及相关违法责任也在现行网络安全法律中均有广泛规定。

管理办法并不仅仅是对现行法律的罗列和重复，而是在对现行法律进行梳理基础上的一次创新和补强。管理办法中新增了许多目前法律没有要求的网络运营者的义务；增强了网络安全法对于重要数据及个人信息的保护义务并扩大了义务主体的范围，同时顺应网络技术的发展，对网络爬虫及“洗稿”等现行法律尚未涉及的前沿问题作出了规定。

值得注意的是，目前管理办法及《个人信息和重要数据出境安全评估办法(征求意见稿)》等均尚属征求意见稿，在正式稿颁布之前仍存变数。管理办法的正式稿可能会受到其他尚未生效的法律法规征求意见稿的影响，反之亦然或相互影响。但无论如何，管理办法的创新和改进值得关注。

2. “数据”定义的反思与再解读

网络安全法律从业者对于“个人信息”及“重要数据”这两类数据已耳熟能详，但是似乎很少有人能够说清“数据”的内涵和外延，即现行法律下是否还存在除两类数据之外的其他类型“数据”?

管理办法将“网络数据”定义为“通过网络收集、存储、传输、处理和产生的各种电子数据”。该定义与网络安全法对网络数据的定义完全一致，但“数据”的内涵及外延究竟如何，现行法律付诸阙如，管理办法亦未做出明确界定。纵观现行法律法规，仅有“个人信息”及“重要数据”这两类数据被明确提及，那么这是否意味着“数据”仅包括个人信息及重要数据这两类呢?笔者认为，答案显然是否定的。首先，《信息安全技术 数据出境安全评估指南》(征求意见稿)中将“重要数据”定义为“相关组织、机构和个人在境内收集、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”，而管理办法也规定“涉及国家秘密信息……的数据活动，按照国家有关规定执行”。因此重要数据中显然不包括国家秘密。其次，管理办法中对于重要数据的定义将“企业生产经营和内部管理信息及个人信息”排除在重要数据的定义之外。综合上述分析，可以推断，目前中国法律体系下至少可以将数据分为以下几类: 国家秘密、个人信息、重要数据及“企业生产经营和内部管理信息”及其他尚不构成重要数据的数据(暂称为“非重要数据”)。

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

在现行法律体系下，国家秘密的监管主要受到《保守国家秘密法》等法律的规制。与网络安全法律直接相关的，也是直接受到网络安全法律规制的数据便是个人信息与重要数据这两类。探讨两类数据相关法律问题的前提是明确其定义。

2.1 个人信息的定义

管理办法沿用了《网络安全法》对“个人信息”作出的定义，即“以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息”。个人信息的定义散见于多部法律法规中，我们对现行主要法律法规对“个人信息”的定义做了总结，请见以下表 1。

数据安全管理办法(征求意见稿) (2019)	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息。
《网络安全法》(2017)	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息。
最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称“两高司法解释”) (2017)	刑法第二百五十三条之一规定的“公民个人信息”,是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者**反映特定自然人活动情况的各种信息**。
《个人信息和重要数据出境安全评估办法(征求意见稿)》(2017)	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息。
《信息安全技术 个人信息安全规范》 (以下简称“个人信息国标”) (2017)	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者**反映特定自然人活动情况的各种信息**。

表 1: “个人信息”的定义对比

从上表可以看出，在《网络安全法》生效之前的两高司法解释和《网络安全法》生效之后发布的个人信息国标均将“反映特定自然人活动情况的各种信息”纳入了“个人信息”的范畴。此处的“个人信息”包括两大类，一类个人信息是由信息本身的特殊性能够识别出特定自然人，另一类个人信息是由特定自然人在其活动中产生的信息，包括个人位置信息、个人通话记录、个人浏览记录等。而管理办法对“个人信息”的定义沿用了《网络安全法》的定义，并不包括“反映特定自然人活动情况的各种信息”，这在一定程度上限缩了个人信息的范围。

能够单独识别到自然人的个人信息很好理解，但问题在于上述所有法律法规均将“与其他信息

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

结合”而能够识别到特定自然人的信息也定义为个人信息。随之而来的问题是，此处的“与其他信息结合”为定性而非定量的规定，那么对于“个人信息”究竟要求结合其他信息到何种程度方可达到法定的“可识别”标准从而构成法律法规所规定的个人信息?换言之，如果一条信息结合其他5条信息可以识别到某个特定自然人，而另一条信息需结合50条其他信息才能识别到该特定自然人，那么这两条信息是否都属于个人信息?如果答案是肯定的，那么对这两条个人信息的保护是否因其各自所需结合其他信息而实现可识别的程度不同而有所不同?很显然，如果一条信息识别到特定自然人所需要结合的其他信息越多，那么其本身构成个人信息的可能性就越低，从而得到的法律保护也应该越弱。对于信息的结合程度，欧盟GDPR规定需要结合客观因素进行考量，例如结合其他信息识别个人所需的时间及处理数据时的可用技术等，但我国法律到目前为止尚未有类似的规定。我们期待管理办法的正式稿或其他法律能够对该问题有进一步的详细规定。

2.2 重要数据的定义

自《网络安全法》生效以来，可以说“重要数据”一直是一把悬在网络运营者头上的达摩克利斯之剑。《网络安全法》已经明确规定了关键信息基础设施运营者对重要数据的本地存储及跨境传输评估义务，而《个人信息和重要数据出境安全评估办法(征求意见稿)》将这一义务扩大至全部网络运营者，但该法规又迟迟未能出台。因此，虽然《网络安全法》已经生效两年，现行法律中对于究竟哪些数据属于重要数据仍然缺乏明确的指引。

管理办法将“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，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。”对比而言，2017年8月发布的《信息安全技术 数据出境安全评估指南(征求意见稿)》中将“重要数据”定义为“相关组织、机构和个人在境内收集、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”。

与《信息安全技术 数据出境安全评估指南(征求意见稿)》中的定义不同的是，管理办法中将“后果分析”这一要件直接加入了重要数据的定义中，明确了重要数据的认定主要是基于对于可能损害结果的判断，同时管理办法采用了“直接影响……”的表述，因而与《信息安全技术 数据出境安全评估指南》(征求意见稿)相比，管理办法限缩了重要数据的范围。同时，管理办法也明确将一般情况下的“企业生产经营和内部管理信息”和“个人信息”排除在重要数据的范畴之外。

值得注意的是，《信息安全技术 数据出境安全评估指南(征求意见稿)》中，附录A中详细列举了26个行业中的重要数据类型，但其中列举的重要数据包含了特定类型的个人信息，也包括可以构成管理办法下“企业生产经营和内部管理信息”的数据。因此，管理办法与《信息安全技术

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

数据出境安全评估指南(征求意见稿)》在重要数据的认定上存在差异。对此差异，我们认为在对重要数据的认定方式上，除了明确具体的数据类型外，还需要结合数据量及数据的组合/聚合方式进行综合判断。例如，我们理解管理办法中排除的“企业生产经营和内部管理信息”应当是针对企业的孤立的数据而言，如果某个企业的“生产经营和内部管理信息”数量巨大，或者其“生产经营和管理信息”通过聚合或其他形式的组合方式，使得该等信息的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，仍然有可能构成重要数据。管理办法中的“一般”二字应该也是为该等情形而做出的保留性规定。

我们认为，相较现行法律法规，管理办法对重要数据的认定更为科学、合理。相信管理办法与《信息安全技术 数据出境安全评估指南》经过协调并正式出台后，两者的结合将在重要数据保护方面对网络运营者提供具有更明确且较可操作的指引。

3. 数据活动

管理办法将数据活动界定为“在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动”，这同时也划定了管理办法的适用范围。数据的收集、存储、传输、处理、使用等环节相对比较容易理解；但是鉴于网络的无国界性，如何界定“在中华人民共和国境内利用网络”开展数据活动或成难题。例如，目前许多境外经营者通过设置中文页面、支持人民币支付方式、提供中文售前售后服务等方式，面向中国消费者开展经营活动(甚至明确招揽中国消费者)，但其网站/APP、服务器、其他网络设备、网络基础设施、公司实体地址均完全位于境外。在此情形下，中国境内消费者通过该网站或 APP 可以完成交易的全过程，境外经营者也通过网站或 APP 收集、存储、传输、处理及使用了中国消费者的个人信息，但这种情形是否属于“在中华人民共和国境内利用网络”开展数据活动?管理办法及其他现行法律法规均未对这一问题给出答案，我们期待管理办法的正式稿能对此类问题进行明确。

就具体的数据活动而言，管理办法第二章规制“数据收集”，第三章规制“数据处理使用”。下文中，我们结合现有法律法规对数据活动的相关规定，对管理办法的相关规定进行简要解读。

3.1 数据收集

管理办法的第二章为“数据收集”，主要规定了网络运营者收集个人信息过程中应尽的责任与义务。相较于目前已生效的关于个人信息保护的法律，管理办法对某些要求作出细化规定，从实际操作层面为网络运营者完善个人信息保护制度提出了指引；同时也根据时代的变化发展提出了一些全新的要求。具体变更内容我们以表格形式进行了总结对比(见表 2)。以下我们重点解析管理办法新提出的规则和要求:

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

3.1.1**网络运营者应区分渠道分别制定隐私政策。**网络经营者若通过网站、应用程序收集个人信息的，需分别制定并公开相应的隐私政策。网络运营者的网站、应用程序受众不同，功能不同，所收集的个人信息以及后续的处理方式亦有不同。这一要求意味着网络运营者需区分收集个人信息的不同渠道和情形，有针对性地起草隐私政策。管理办法正式生效后将不允许网络运营者采用一套适用于其全部渠道的"万金油"隐私政策。

3.1.2**网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为**，包括服务质量、价格差异等。该规定与我们通常理解中的"消费歧视"并不完全相同，因为该规定仍旨在于限制网络运营者收集个人信息的目的和方式，不得对授权范围不同的个人信息主体采取歧视待遇，如限制提供服务的范围、提高价格等。

3.1.3**网络运营者以间接方式收集个人信息者应承担同等义务**。管理办法第 14 条首次提出，"网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务"。这意味着即使非由网络运营者直接收集的个人信息，该网络运营者也需确保个人信息主体的权利受到保护，如审查直接收集者是否在收集时取得了信息主体的同意、个人信息的处理和使用应符合与信息主体之间的约定等。实践中，目前有企业认为从第三方获取个人信息，由于非由其直接收集个人信息，相关法律责任及义务是无需遵循关于"收集、使用个人信息"的相关规定的。这些企业应警醒管理办法第 14 条的规定，进一步改善从第三方获取的个人信息合规工作。

3.1.4**收集重要数据、个人敏感信息需备案并明确数据安全责任人。**管理办法第 15 条、第 17 条首次提出，网络运营者以"经营为目的"收集重要数据或个人敏感信息的，应(1)向所在地网信部门备案；(2)明确数据安全责任人。通常而言，法律意义上的"以经营为目的"指的是"直接产生利益"，与增值电信服务中的"经营性互联网信息服务"相类似。以此类推，我们认为"以经营为目的收集重要数据或个人敏感信息"应当指企业可以直接利用所收集的重要数据或个人敏感信息产生经济利益。符合该定义的经营者可能包括大数据分析公司、数据经纪人等商业化的数据收集、开发和挖掘者。但管理办法中"以经营为目的"的具体含义还有待于其正式稿或监管部门的进一步解释。

3.1.5**规范网络爬虫等新型数据安全问题**。管理办法第 16 条将爬虫手段严格限制在"不影响网站正常运行"的范围内。并且，当爬虫行为严重影响网站运行、网站要求停止自动化访问收集时，应当停止爬虫行为。该条款对于提供搜索服务、信息整合发布类平台的经营者提出了

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

更为严格具体的要求。该类经营者应考虑以适当频率发起内容请求，避免过高的请求频率引发网络安全事故。

数据收集环节		差异
收集个人信息应制定使用规则	《数据安全管理办法》 **第七条** 网络运营者通过网站、应用程序等产品收集使用个人信息，应当**分别制定**并公开收集使用规则。 《网络安全法》 **第四十一条** 网络运营者应公开收集、使用规则，明示收集、使用信息的目的、方式和范围。	更新已有规定
收集使用规则的制定要求	《数据安全管理办法》 ● **第九条** 收集使用规则在隐私政策中应集中、明显提示，方便阅读 ● **第十条** 网站、应用程序收集或使用个人信息的功能设计应同隐私政策保持一致，同步调整 ● **第八条** 收集使用规则明确具体、简单通俗、易于访问，突出以下内容: （一） 网络运营者基本信息; （二） 网络运营者主要负责人、数据安全责任人的姓名及联系方式; （三） 收集使用个人信息的目的、种类、数量、频度、方式、范围等; （四） 个人信息保存地点、期限及到期后的处理方式; （五） 向他人提供个人信息的规则，如果向他人提供的; （六） 个人信息安全保护策略等相关信息; （七） 个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法; （八） 投诉、举报渠道和方法等; （九） 法律、行政法规规定的其他内容。	重申已有规定
	《信息安全技术 个人信息安全规范》 ● **4 e)** 公开透明原则——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督; ● **5.6 c)** 隐私政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言，并在起始部分提供摘要，简述告知内容的重点; ● **5.6 a)** 个人信息控制者应制定隐私政策，内容应包括但不限于: 1) 个人信息控制者的基本情况，包括注册名称、注册地址、常用办公地点和相关负责人的联系方式等; 2) 收集、使用个人信息的目的，以及目的所涵盖的各个业务功能，例如将个人信息用于推送商业广告，将个人信息用于形成直接用户画像及其用途等; 3) 各业务功能分别收集的个人信息，以及收集方式和频率、存放地域、存储期限等个人信息处理规则和实际收集的个人信息范围; 4) 对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及所承担的相应法律责任; 5) 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施; 6) 个人信息主体的权利和实现机制，如访问方法、更正方法、删除方法、注销账户的方法、撤回同意的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等; 7) 提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响; 8) 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。	

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

不得误导个人信息主体给予同意	《数据安全管理办法》 **第十一条** 网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。	更新已有规定
	《信息安全技术 个人信息安全规范》 **5.1 a)** 不得欺诈、诱骗、强迫个人信息主体提供其个人信息; **b)** 不得隐瞒产品或服务所具有的收集个人信息的功能。	
区分核心业务功能	《数据安全管理办法》 **第十一条** 个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。	重申已有规定
	《信息安全技术 个人信息安全规范》 **5.2 a)** 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现。	
未成年人保护，明确年龄分界线	《数据安全管理办法》 **第十二条** 收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意。	重申已有规定的
	《信息安全技术 个人信息安全规范》 **5.5 c)** 收集年满 14 的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。	
不得歧视	《数据安全管理办法》 **第十三条** 网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。	新规定
对“二手”个人信息亦需负责	《数据安全管理办法》 **第十四条** 网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。	新规定
备案义务	《数据安全管理办法》 **第十五条** 网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。	新规定
爬取数据需当心	《数据安全管理办法》 **第十六条** 网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行。	新规定
数据安全负责人	《数据安全管理办法》 **第十七条**网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。	新规定
	《网络安全法》 **第二十一条** 网络运营者应确定网络安全负责人。	

表 2 管理办法与现行法律法规的对比 - 数据收集环节

3.2 数据处理使用

管理办法的第三章规制“数据处理使用”，主要规定了网络运营者使用、处理、个人信息；跨境传输数据及管理相关第三方过程中应尽的责任与义务。第三章对网络运营者提出了较多的新要求，且针对新兴数据应用场景如“定向推送”“洗稿”等首次作出了规定。具体变更内容我们以表格形式进行了总结对比(见表 3)。下文中，我们重点解析一些新提出的规则和要求:

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

3.2.1管理办法第 23 条首次对“定向推送”做出了规定。网络运营者利用用户数据和算法推送新闻信息、商业广告等，即可被认定为定向推送。值得注意的是，管理办法并不禁止网络运营者进行定向推送，但要求在推送信息上标明“定推”字样，且需为用户提供停止接受定向推送信息的功能。用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

此外，管理办法规定开展定向推送活动应遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。随着大数据时代的到来，算法系统所导致的歧视逐渐为公众所认知及重视。定向推送中的歧视行为可能会伤害用户个人的情感、导致用户财产受损、甚至可能严重影响用户个人的正常生活。管理办法首次涉及算法技术应用，对定向推送行为提出原则性要求固然具有“划时代意义”，但具体如何落实不仅需要法律法规的细化规定，也需要网络运营者在技术方面进行针对性的调整与革新。

值得注意的是，之前公安部等三部门联合发布的《互联网个人信息安全保护指南》中规定，“完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权”。这一要求虽然与管理办法并不矛盾，但两者如何进行结合与衔接还需网络运营者进一步考虑与规划。

3.2.2管理办法还首次从网络安全的角度对自动化洗稿进行了明确规制。2018 年，国家版权局等四部门联合启动“剑网 2018”专项行动，对媒体通过“洗稿”抄袭剽窃、篡改删减原创作品的侵权行为进行了重点打击。“洗稿”即指利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息。管理办法从监管角度限制了“洗稿”的展现方式和目的，要求网络运营者对此类合成的信息标明“合成”字样，且不得以谋取利益或损害他人利益为目的自动合成信息。

3.2.3管理办法强化了网络运营者对接入其平台的第三方应用需尽到的管理义务。管理办法第 30 条规定，若第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。该项规定对网络运营者提出了极为严苛的要求，相关平台的经营者应收紧第三方应用上线的条件与资质要求，并加强对平台内应用数

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

据安全方面的管理与监督。

3.2.4管理办法对重要数据的发布、共享、交易和境外传输提出了更高的要求。现行法律中仅涉及了重要数据的本地存储及跨境传输的安全评估，并未提及重要数据的“发布、共享、交易”等，而管理办法试图将这些涉及重要数据的环节也纳入法律的管理体系。对于重要数据境外传输，《网络安全法》规定关键信息基础设施运营者向境外传输重要数据的，应当进行安全评估；《个人信息和重要数据出境安全评估办法(征求意见稿)》将需要进行安全评估的主体从关键信息基础设施运营者扩大到了所有网络运营者。管理办法同样将涉及重要数据的相关义务扩大至全部网络运营者，同时在上述两个法规要求的安全评估的基础上，还要求应当报行业主管监管部门同意。除重要数据的境外传输之外，发布、共享、交易重要数据亦要求进行安全评估并报行业主管监管部门同意。就重要数据而言，管理办法无疑在深度和广度上均加重了网络运营者的相关义务。

值得探讨的是，管理办法对于重要数据需报行业主管监管部门同意的规定是否创设了一项新的行政许可?作为上位法的《网络安全法》对于关键信息基础设施运营者向境外提供重要数据这一事项作出了规定，但未就此事项设定行政许可或授权地方性法规或规章对其作出进一步规定。根据行政许可的设定规则，对于法律已经规定的事项，下位法不得增设行政许可。对关键信息基础设施运营者使用重要数据及关键信息基础设施运营者以外的其他网络运营者使用、向境外传输重要数据等事项，现行法律未予规定。在此情形下，管理办法创设的新许可如何符合《行政许可法》值得进一步思考。

3.2.5管理办法新增了一条此前《网络安全法》中从未出现过的规定。管理办法的第 29 条规定，境内用户访问境内互联网的流量不得被路由到境外。管理办法及网信办并未对该条的起草理由及具体含义做出解释。我们理解该条可能与第 28 条的重要数据有一定的关联，境内用户在访问境内互联网时会产生数据的传输与交换，这其中当然也可能包括重要数据。如果该等访问流量被路由到境外，则可能产生重要数据未经安全评估和主管部门同意即被传输到境外的风险。此外，流量路由到境外还可能会造成线路拥塞，导致流量被窃取、监听，禁止流量路由到境外可以防止路由泄露、流量误导和流量劫持。我们期待管理办法能在最终稿中对本条进行解释和完善。

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

数据处理使用环节		差异
数据保护措施参照国标	《数据安全管理办法》 **第十九条** 参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护。	重申已有规定
保存、使用个人信息应遵循收集使用规则	《数据安全管理办法》 ● **第二十条** 保存个人信息不应超出收集使用规则中的保存期限，用户注销账号后应当及时删除其个人信息，经过处理无法关联到特定个人且不能复原(以下称匿名化处理)的除外。 ● **第二十二条** 扩大个人信息使用范围应征得个人信息主体同意	重申已有规定
	《信息安全技术 个人信息安全规范》 ● **6.1** 对个人信息控制者的要求包括: a) 个人信息保存期限应为实现目的所必需的最短时间; b) 超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理。 c) 使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关 联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人 信息主体明示同意。 ● **7.3 c)** 使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。	
响应个人信息主体要求	《数据安全管理办法》 **第二十一条** 对个人信息查询、更正、删除及注销账号请求在合理时间和代价范围内响应	重申已有规定
	《网络安全法》 **第四十三条** 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。	
	《信息安全技术 个人信息安全规范》 **7.4 7.5 7.6 7.8 7.11** 个人信息的访问、更正、删除及个人信息主体注销账户	
定向推送行为限制	《数据安全管理办法》 **第二十三条** 定向推送行为限制，包括标明“定推”字样，为用户提供停止接受此类信息的功能等	更新已有规定
	《信息安全技术 个人信息安全规范》 **7.7 b)** 应保障个人信息主体拒绝接收基于其个人信息推送的商业广告的权利	
洗稿行为限制	《数据安全管理办法》 **第二十四条** 自动合成信息(俗称自动化“洗稿”)行为限制，包括标明“合成”字样等	新规定

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

需要个人信息主体同意的例外情形	《数据安全管理办法》 **第二十七条** 提出安全风险评估要求，并首次在部门规范性文件中提出个人信息主体同意的例外情形，包括: （一） 从合法公开渠道收集且不明显违背个人信息主体意愿; （二） 个人信息主体主动公开; （三） 经过匿名化处理; （四） 执法机关依法履行职责所必需; （五） 维护国家安全、社会公共利益、个人信息主体生命安全所必需。	重申已有规定
	《信息安全技术 个人信息安全规范》 **5.4** 以下情形中，个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意: a) 与国家安全、国防安全直接相关的; b) 与公共安全、公共卫生、重大公共利益直接相关的; c) 与犯罪侦查、起诉、审判和判决执行等直接相关的; d) 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的; e) 所收集的个人信息是个人信息主体自行向社会公众公开的; f) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道; g) 根据个人信息主体要求签订和履行合同所必需的; h) 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障; i) 个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的; j) 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的; k) 法律法规规定的其他情形。	
重要数据跨境传输风险评估	《数据安全管理办法》 **第二十八条** 重要数据发布、共享、交易或向境外提供前需进行安全风险评估，报行业主管监管部门同意。 向境外提供个人信息按有关规定执行。	更新已有规定
	《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。	
境内流量不得路由至境外	《数据安全管理办法》 **第二十九条** 境内用户访问境内互联网的流量不得被路由至境外。	新规定
对第三方的数据管理义务	《数据安全管理办法》 **第三十条** 对接入其平台第三方应用的数据安全管理义务。	新规定
数据承接方义务	《数据安全管理办法》 **第三十一条** 兼并、重组、破产场景下，数据承接方应承接数据安全责任和义务。	重申已有规定
	《信息安全技术 个人信息安全规范》 **8.3** 收购、兼并、重组时的个人信息转让 当个人信息控制者发生收购、兼并、重组等变更时，个人信息控制者应: a) 向个人信息主体告知有关情况; b) 变更后的个人信息控制者应继续履行原个人信息控制者的责任和义	

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

	务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意。	
数据处理的原则	《数据安全管理办法》 **第三十二条** 网络运营者分析利用所掌握的数据资源，发布市场预测、统计信息、个人和企业信用等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。	重申已有的原则性规定

表 3 管理办法与现行法律法规的对比 - 数据处理使用环节

4. 结语

如上所述，管理办法既是对现行网络安全重要问题的一次“阶段性总结”，也对网络安全监管作出创新尝试，其将对所有的网络运营者产生广泛而深远的影响。我们期待管理办法的正式稿对包括本文探讨的相关问题等作出进一步修改与完善，为网络运营者的合法合规运营提供更为明确且具可操作性的指引。

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

如需进一步信息，请联系:

作　者	
潘永建 电话: +86 21 3135 8701 david.pan@llinkslaw.com	

上　海	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**刘瓒春** 电话: +86 21 3135 8678 bernie.liu@llinkslaw.com
佘　铭 电话: +86 21 3135 8770 selena.she@llinkslaw.com	**娄斐弘** 电话: +86 21 3135 8783 nicholas.lou@llinkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@llinkslaw.com	**孔焕志** 电话: +86 21 3135 8777 kenneth.kong@llinkslaw.com
吴　炜 电话: +86 21 6043 3711 david.wu@llinkslaw.com	**潘永建** 电话: +86 21 3135 8701 david.pan@llinkslaw.com
姜　琳 电话: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
北　京	
俞卫锋 电话: +86 10 8519 2266 david.yu@llinkslaw.com	**刘瓒春** 电话: +86 10 8519 2266 bernie.liu@llinkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
香　港(与方緯谷律师事务所联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**吕　红** 电话: +86 21 3135 8776 sandra.lu@llinkslaw.com
伦　敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	

© 本篇文章独家授权威科先行法律信息库发布，未经许可，不得转载。

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。