漢坤律師事務所
HAN KUN LAW OFFICES

汉坤专递

2019 年第 6 期（总第 146 期）

新法评述

1、 使命与界限：近期个人信息和数据安全新规的一些思考

2、 《个人信息出境安全评估办法》公开征求意见

新法评述

1、使命与界限：近期个人信息和数据安全新规的一些思考

作者：朱敏丨蔡克蒙

近期个人信息和数据安全规范密集出台，包括《网络安全审查办法（征求意见稿）》、《数据安全管理办法（征求意见稿）》（“**《管理办法》**”）、《儿童个人信息网络保护规定（征求意见稿）》（“**《儿童个人信息保护规定》**”）以及《移动互联网应用基本业务功能必要信息规范》等，后续也还有不少关键性的法规文件亟待落地。

监管机构衔枚疾进，不排除有多重考量因素的作用，尤其是在特定时期需要加快相应领域立法的需求。在新规频出之际，我们也希望结合新近出台的若干规章和规范文本，阐述我们的一些想法，以期作为相关规章在征求意见阶段的一些反馈声音。本文主要从监管权限、监管思路和监管规则协调等角度作一些初步的分析和思考，后续我们将尝试从规则层面做进一步的梳理和讨论。

一、《管理办法》的使命

从《管理办法》的内容来看，该文本部分可以看成是基于国标《个人信息安全规范》（“**《规范》**”）及《App 违法违规收集使用个人信息自评估指南》的前期实施经验所作的一次阶段性总结，把一些比较成熟的监管规则和实践以及实务中普遍关切的问题上升到立法层面，并通过规章的形式加以明确和确认。在条件成熟时将引导性的行为规则固化为具有强制力的法律规范，这也符合行政规章制定的一般规律。如此行政规章出台之后，执行和实施当中所遇到的阻力也会相对较小。

客观而言，《规范》作为一项推荐性国标，在实务中已获得了超乎其原本定位的广泛影响力和适用性，实践中似乎也很少有其他推荐性国标文件有如此的待遇。因此，在《规范》事实上已经成为一项“软法”[1]，而且《管理办法》中有关个人信息安全的规定也基本被《规范》及其 2.0 版本所覆盖的情况下，似乎并不足以解释是否需要再行出台一个《管理办法》。我们理解，《管理办法》应当是承载了更多的使命和“雄心”，尤其是数据安全方面的规定。

除了之前监管规则中不曾出现过网路爬虫抓取数据、定向推送、洗稿、数据出境审批以及平台运营者对第三方应用的过错推定责任等新规定而需要补充之外，另一个合理性解释，应该是按照《立法法》的规定，部门规章可以设定一定的行政处罚手段，通过将《规范》上升到部门规章层面，可以解决其作为推荐性国标并没有强制执行力的窘境，让那些已经实践验证确认行之有效的监管规则终于有了“牙齿”。

近期发布的《儿童个人信息保护规定》，除了标志着在儿童个人信息保护领域一项独立规则实现零的突破之外，赋予相关规定行政强制力也是一个重要的看点。虽然《儿童个人信息保护规定》中相当一部分内容在既有规定（尤其是《规范》）中都可以找到一些出处，但其第 24 条、第 25 条和第 26 条中所规定的行政管

[1] 有关《规范》在实务中的适用效力和实际运用，可参见许可：《<个人信息安全规范>的效力与功能》，载于《中国信息安全》2019 年第四期。

理措施和行政处罚手段，却是《规范》所不能实现的。

二、规则体系之间的协调

《网络安全法》出台以来，在网络安全、个人信息保护和数据合规领域，不同部门和机构已发布了一系列不同效力等级的文件，包括网信办等部委的规章和指引等规范性文件、各项国标、两高的司法解释、行业标准和指南以及执法行动文件等。此次《管理办法》中涉及的很多问题在上述这些文件其实已经多有涉及，因此，如何协调不同效力的规则体系之间的关系，给行业实践提供清晰的指引而不至于造成适用上的混乱甚至是冲突，就成为了一个不得不面对且日益棘手的问题。

需要考虑的是，按照立法规划，数据安全和个人信息保护两个议题已经确定会作为相对独立的立法议题并通过分别制定《数据安全法》和《个人信息保护法》来进行规制。此外，数据安全（或网络安全）与个人信息保护的立法侧重点也并不全完一致，前者更多是传统的网络安全三性（保密性、完整性和可用性）的问题，而后者更侧重保障个人自主、对个人信息的控制以及对个人信息符合个人信息主体预期的利用等问题。这次《管理办法》选择把这两个议题糅合在一起进行处理，虽然不能说完全不可以，但的确需要处理好前后立法衔接以及同一规章覆盖不同议题等情形中的立法技术问题[2]。

如前所述，如果《管理办法》部分是前期监管实践的一次阶段性总结的话，也相信其会在一定程度上在整个立法和监管规划中起到承上启下的作用，在前述完成阶段性总结的使命基础上，为后续《数据安全法》和《个人信息保护法》的起草和出台准备更丰富的监管经验和立法素材。

三、监管部门的执法权力

《管理办法》赋予了执法机关广泛的数据获取权限，其中第二十七条规定“网络运营者向他人提供个人信息前，应当评估可能带来的安全风险，并征得个人信息主体同意”，但“执法机关依法履行职责所必需”属于例外情形之一；第三十六条进一步规定“国务院有关主管部门为履行维护国家安全、社会管理、经济调控等职责需要，依照法律、行政法规的规定，要求网络运营者提供掌握的相关数据的，网络运营者应当予以提供。”

与《规范》第 5.4 条“征得授权同意的例外”中列出的具体情形[3]相比，《管理办法》的上述规定明显过于原则。“依法履行职责所必需”以及“履行维护国家安全、社会管理、经济调控等职责需要”，都是十分宽泛的表述。虽然说后者通过“国务院有关主管部门”进行了主体层级上的限定，但总体上仍赋予了监管部门相对广泛的执法裁量权。我们建议在后续定稿规范或在相关的法规规章中，对监管部门获取企业数据、个人信息的程序和权限加以规范，在实现国家安全和社会管理等利益的同时，维护程序正义，保护数据主体和收集数据企业的合法权益。

四、部门规章的立法权限

[2] 一个可以参考的立法案例是，2014 年 5 月原国家食药总局曾发布《互联网食品药品经营监督管理办法》（征求意见稿），试图将食品（含食用农产品、食品添加剂）、保健食品、药品、化妆品和医疗器械进行“五位一体”的统一立法，但由于这些产品类别之间的明显差异，监管政策的多样性，尤其是药品监管的特殊性，以及处方药网售是否开禁的巨大争议等，使得统一规定不仅在立法技巧上形成极大挑战，规章通过之后的实施效果也被严重质疑。经过数次审议，该办法最终不了了之，原国家食药总局最终也选择就不同品类产品出台单行的监管规则。

[3] 《规范》1.0 版本第 5.4 条和《规范》2.0 版本征求意见稿第 5.7 条。而且，《规范》里面除了国家安全和公共利益等事由之外，单独列明的是司法程序中的“犯罪侦查、起诉、审判和判决执行等直接相关”，而非《管理办法》中所述的“执法机关依法履行职责”。

《管理办法》第二十八条无疑是本次征求意见稿中尤为引人注目的一个条款，其中规定：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。向境外提供个人信息按有关规定执行。

就该事项，《网络安全法》第三十七条规定："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；法律、行政法规另有规定的，依照其规定。"

从条文来看，《网络安全法》仅仅将适用主体限定在了"关键信息基础设施运营者"，而且只需安全评估，没有规定须"报经行业主管监管部门同意"或"应经省级网信部门批准"。对于这个"突破"，到底是规章超越了上位法的授权权限新设了一个"行政许可"事项，或是增加了企业主体的义务，还是在上位法设定的权限范围内通过部门规章的形式细化了行政管理措施？这的确是很值得讨论的一个问题。当然，另一个解释路径是国家网信部门会同国务院有关部门依据《网络安全法》授权制定的评估办法中可能会明确此报批程序。

五、行政规制的活动方式

在网络安全、个人信息保护和数据合规立法领域，根据业界的普遍反映，每出台一项新的制度文件，基本都会给相关行业的企业实体增添新的义务和要求，并导致企业合规成本的不断增加。野蛮生长的草莽英雄时代，很多产业实践的确需要通过建立新的规则体系予以规制，但其中创新与约束、发展与规制、私利和公益等一系列矛盾诉求的权衡和平衡，必定是立法中非常具有挑战性却又无法回避的现实。

与传统的监督检查、定期汇报和审查批准等执法和监管方式相对应，近些年在社会经济活动的行政规制领域逐渐形成了社会共治和政府与企业合作治理的共识，并已经体现在众多的立法和执法活动中。在数据经济时代，大数据凸显其巨大的潜在利用价值，但又囿于个人信息和隐私数据保护的高度合规要求，因此合作治理和激励相容[4]的政策和监管模式，就尤其能体现其适用价值。值得欣慰的是，《规范》在其生效实施之后，在调动企业主体积极构建个人信息保护的内控合规制度、引导主动守法和降低执法成本等方面，都发挥了相当正向的作用。

本次《管理办法》第三十四条一定程度上也体现了这样的立法思路，其中规定："国家鼓励网络运营者自愿通过数据安全管理认证和应用程序安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的应用程序。国家网信部门会同国务院市场监督管理部门，指导国家网络安全审查与认证机构，组织数据安全管理认证和应用程序安全认证工作。"

我们有理由相信，如果有更多的类似规章和政策不断引导并形成良性推动，政府和企业各司其职，共同治理模式下的中国个人信息保护和数据安全治理环境值得期待。

六、规则设定与基础理论的支撑

[4] 有关激励相容治理模式的讨论，可参考周汉华：《探索激励相容的个人数据治理之道》，载于《法学研究》2018 年第 2 期。文章认为，传统法律理论认为，法律是主权者的命令，是必须遵守的规范，令行禁止是其基本特征。因此，传统立法规制方式通常是命令控制方式，表现为禁止性规范或者义务性规范，要求被管理对象不得或者必须为某些特定行为。这种规制方式有很多弊端，包括：要求很 强的执法能力，否则命令会被普遍漠视；由于信息不对称，这种命令可能与市场规律脱节，遏制市场主体创新能力与守法诱因；执法部门权力过大，可能会导致选择性执法或者"执法俘获"等问题。

法律即规则，法律体系由法律基础理论和法律具体规则构成。欧洲以基本人权理论为出发点构建了GDPR 为主导的严格的个人数据处理活动法律框架。美国也以 Fair Information Practice Principles（FIPP）为基础理论支撑，形成了极具美国特色的以 Federal Family Educational Rights and Privacy Act (FERPA)、Children's Online Privacy Protection Act (COPPA)、Fair Credit Reporting Act (FCRA)以及 Gramm-Leach-Bliley Act (GLBA，也即 Financial Modernization Act of 1999)等法律为基础的部门化立法模式。

与此相对应的，我国在个人信息和隐私数据保护方面的基础理论上却显得相对滞后——虽然 2009 年《侵权责任法》首次在法律中确立了隐私权的法律地位，以及 2017 年公布的《民法总则》首次对隐私权和个人信息采取了“二元”保护模式。总体而言，2017 年《网络安全法》出台以来陆续落地的一系列法规和规章文件，包括《管理办法》和《儿童个人信息保护规定》，立法和监管机构基本是以相对实用主义的路径设立了以现有互联网生态为主要规制对象的一套规则体系。随着《民法总则》人格权篇、《个人信息保护法》和《数据安全法》的陆续到位，个人信息、隐私权和数据资产等基本概念和理论框架的逐渐完备，相信我们国家可以建立一整套理论和规则协同配合的完整监管体系。

虽任重道远，但步伐坚定而清晰。

2、《个人信息出境安全评估办法》公开征求意见

作者：段志超丨蔡克蒙丨何雯

2019 年 6 月 13 日，国家互联网信息办公室（“**网信办**”）发布了被搁置已久的《个人信息出境安全评估办法（征求意见稿）》（“**办法草案**”），距此前发布备受争议的跨境传输指南草案已近两年。可能是基于重要数据[5]和个人信息这两类数据之间存在内在差异的考虑，办法草案排除了重要数据，但再次将个人信息出境的安全评估义务从关键信息基础设施运营者扩展到普通网络运营者，且统一要求境境外实体对数据出境进行事先评估。这两方面的规定可能会激起日常运营高度依赖跨境数据传输的公司的强烈反弹，特别是跨国公司或没有境内实体的境外互联网/数据公司。此外，尽管办法草案加强了数据主体权利，这些权利的实施和执行在现实中可能困难重重，同时还可能给境内数据控制者带来过重的负担。

一、扩展适用范围和事先政府评估

与此前的草案相同，此次办法草案规定所有网络运营者向境外提供个人信息之前均应进行安全评估，而不仅限于《网络安全法》第 37 条所规定关键信息基础设施运营者。在此基础上，办法草案还明确要求收集中国境内用户个人信息的境外运营者通过境内代表承担相同的义务[6]。

此外，办法草案扩展了政府评估的适用范围，要求所有网络运营者在向境外提供个人信息之前均应向省级网信部门申报个人信息出境安全评估。这一规定较此前草案更为严格，后者要求网络运营者定期进行自评估，仅在数据量达到一定量级或涉及某些敏感数据时，才需要向主管部门申请政府评估。

二、重视通过合同规制，增强数据主体权利

办法草案重视通过合同规制数据跨境传输。除个人信息出境安全风险及安全保障措施分析报告外，网络运营者在安全评估申请中还需要提交其与境外接收者之间的合同（“**传输合同**”）。传输合同应当包括以下条款：

- 数据主体是涉及数据主体权益条款的受益人，可以在发生侵权行为时直接向境内运营者或境外接收人或双方索赔；
- 除非数据已被销毁或匿名化处理，否则对个人信息的安全保护义务应在传输终止后继续有效；
- 境内运营者有义务向数据主体告知数据出境的类型、目的、接收方等具体情况，并根据数据主体的请求提供传输合同副本；
- 境外接收者有义务及时响应数据主体的合理请求；
- 当接收者所在国家法律环境发生变化导致接收者难以履行合同义务时，应终止合同。 否则，接收方应立即通知境内运营者，并通过后者申请政府重新评估；以及
- 原则上，除非境内运营者和境外接受者对数据主体的权利提供某些必要的保护措施，否则在出境后

[5] 《数据安全管理办法（征求意见稿）》规定：“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。”

[6] 方法草案第 20 条。

不得向第三方进一步传输个人信息。

实体上，办法草案重视合同监管的同时，亦将加强了数据主体权利的保护（如下文所详述）。

办法草案规定政府评估应侧重于：

- 是否符合国家有关法律法规和政策规定；
- 获得个人信息的合法性、正当性；
- 传输合同是否能够充分保障个人信息主体合法权益以及合同能否得到有效执行；和
- 境内运营者或境外接收者是否有损害数据主体合法权益的历史、是否发生过重大网络安全事件。

三、持续报告和监管

办法草案旨在建立持续的评估和监管机制，网络运营者需不断报告，接受有关部门持续监督，而非完成一次评估了事。同时，办法草案并不要求对相同主体之间在特定时间内跨境传输类似数据进行重复评估。

具体而言，网络运营者通过网信办安全评估后，在两年内无需就同一接收者后续的多次或连续的传输类似数据申请重新评估。然而，如果出境目的、相关数据类型和境外保存时间等发生变化时，则网络运营者需要申请重新评估。此外，网络运营者必须保存信息出境记录至少五年，每年向省级网信部门报告有关个人信息出境、传输合同履行情况的详情，并在发生严重的数据泄露事件时立即通知省级网信部门。

另一方面，如果境内运营者或境外接收者（1）发生严重的数据泄露或数据滥用事件，或（2）无法保护数据主体权益或个人信息的安全，网信部门有权随时暂停或终止数据出境。

四、跨国公司的难题

办法草案将对跨国公司的运营和管理构成重大挑战。

办法草案所规定的重合同的监管路径可能是借鉴了 GDPR 的经验，后者为跨国公司向海外主体传输数据提供了以下机制:（1）根据成员国数据保护机构一次性认证的有约束力的公司规则（Binding Corporate Rules，BCR）向境外集团内部关联方传输个人信息；或（2）基于欧盟委员会发布的标准合同条款（SCC）向集团以外的主体传输个人信息。

但办法草案所构想的评估机制与 GDPR 有显著差别。网络运营者向多个接收者传输个人信息时需分别申请安全评估，还需在获批的数据出境情况发生变化时申请重新评估。这会显著增加跨国公司的负担，并最终迫使其选择数据本地化。

办法草案要求基于跨境服务直接向境内数据主体收集数据的境外服务提供者通过境内代表（可能是境内分支机构或联系代理机构）申请政府评估。然而，办法草案中的许多条款系针对“境内运营者向境外接收者”传输数据（例如传输合同的要求）设计，因此直接向境内数据主体收集个人信息的境外服务提供商应如何适用这些条款仍不清楚。最后，同样重要的是，上述评估义务可视为对境外服务提供商在境内提供服务创设了许可要求，然而除了直接切断访问，网信部门如何将其管辖权延伸至此类境外服务提供商尚存疑问。

五、数据主体的权利执行

办法草案赋予了数据主体在传输合同下的第三方权利，数据主体可向境内运营者或直接向境外接收者

行使其数据主体权利并提出索赔请求。然而，鉴于向境外主体行使权利或索赔成本过高，数据主体对境外接收者的第三方权利在实践中可能意义有限。因此，办法草案要求境内运营者代数据主体向境外接收方进行索赔，并在索赔未成的情况下先行赔付数据主体。这样的要求将显著增加境内运营者的责任。考虑到境内运营者可能缺乏对境外接收方的有效控制手段和执行机制，这种严苛要求对于境内运营者是否公平尚值得商榷。

六、我们的观点

办法草案对从中国向境外传输个人信息提出了前所未有的严格限制，其一旦实施可能对数据相关业务产生深远影响。对于那些业务依赖境外数据处理或集中存储的公司而言，为了避免冗长的评估程序和与此相伴的不确定性，数据本地化可能是一个不可避免的昂贵选择。此外，统一要求网络运营者在个人信息出境前申请政府评估在实践中可能既难以实施，亦非必要。我们认为更为实际和可取的可能是代之以相对灵活的评估机制，结合如标准合同条款、具有约束力的公司规则、充分性决定以及同意机制等已经被其他国家或地区证明有效的跨境传输方式，辅以事后监管执法，这可以兼顾保护数据主体的权利和保护国家安全的需求。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86-10-8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86-21-6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86-755-3680 6518

Email：　jason.wang@hankunlaw.com

香港　陈达飞　律师：

电话：　+852-2820 5616

Email：　dafei.chen@hankunlaw.com