汉坤法律评述

2019 年 6 月 9 日

漢坤律師事務所
HAN KUN LAW OFFICES

北京 | 上海 | 深圳 | 香港

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 | 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

[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。

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

[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”。

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

《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。"

[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。

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

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。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

朱敏

电话： +86-21-6080 0955
Email： min.zhu@hankunlaw.com