汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2017 年 6 月 6 日

汉坤网络安全和数据合规系列之六：数据出境安全评估，操作指南来了！

唐志华 | 朱敏

为落实已经于 2017 年 6 月 1 日生效的《网络安全法》对个人信息和重要数据出境要求，全国信息安全标准化技术委员会（“**信安标委**”）于 5 月 27 日发布《信息安全技术 数据出境安全评估指南（草案）》（“**《评估指南》**”）公开征求意见。

信安标委由国家标准化管理委员会领导，业务受中央网信办指导，负责全国信息安全标准化工作。虽然信安标委发布的仅仅是推荐性国家标准（GB/T），不具有强制性效力，但在《网络安全法》和正在制定中的《个人信息和重要数据出境安全评估办法（征求意见稿）》（“**《评估办法》**”）对个人信息和重要数据出境评估仍留有空白的情况下，信安标委发布的《评估指南》可以在一定程度上反映监管态度，为数据出境评估提供更具有操作性的指引。

一、 《评估指南》和《评估办法》的关系

《评估办法》目前已经结束征求意见，如果顺利可能与《网络产品和服务安全审查办法（试行）》一样，经过一次公开征求意见后即快速正式发布，以配合《网络安全法》的生效实施。但如之前的评述所言，《评估办法》中还有很多不确定的地方，需要更具可操作性的配套措施。而《评估指南》基本参照《评估办法》的逻辑框架，对数据出境评估进行了细化和补充。

例如，《评估办法》针对不同情形规定了网络运营者自行评估和报请行业主管或监管部门组织安全评估等程序要求，《评估指南》第 4 部分“评估流程”，即是按照网络运营者开展个人信息和重要数据出境安全评估进行设计和要求；并同时明确，该标准适用于网络运营者，也适用于行业主管或监管部门的指导和监督等工作。

又如，第 5 部分“评估要点”，从“合法正当”和“风险可控”两个角度展开，即是对《评估办法》第八条所述数据出境安全重点评估内容的细化。《评估办法》在“重要数据”定义中也规定，其具体范围参照国家有关标准和重要数据识别指南，而《评估指南》作为信安标委制定的推荐性国家标准，尤其是其附录 A“重要数据识别指南”，便是对该重要定义的细化指引。

二、 重点关注内容

根据目前发布的《评估指南》草案文本，我们认为有如下内容值得特别关注：

1. 适用范围

《评估指南》指出该标准适用于网络运营者开展的个人信息和重要数据出境安全评估工作，与《评估办法》相同，并未将数据出境评估主体限定在关键信息基础设施（“CII”）运营者。但是，根据《网络安全法》施行前夕国家互联网信息办公室网络安全协调局负责人答记者问中所给出的信息，个人信息和重要数据的境内存储和出境评估要求仍然是针对关键信息基础设施运营者提出，而不是针对所有网络运营者。因此，对于个人信息和重要数据跨境传输的适用范围，仍存在较大的不确定性，有待《评估办法》等文件的正式出台。

2. 个人信息

除《网络安全法》和《评估办法》对“个人信息”的列举之外，《评估指南》延续了《网络安全法》之前《电信和互联网用户个人信息保护规定》等规定，认定自然人的位置和行为信息等也属于“个人信息”。这对目前使用广泛的手机 APP 等收集用户使用位置，特别是利用用户实时位置提供服务的各类 APP 提出了明确要求，即这些位置和行为信息在《评估指南》的语境下都属于个人信息。而鉴于《网络安全法》对个人信息本就是非穷尽式列举，在目前监管趋严的环境下，我们认为对个人信息宜做出宽泛解释，即自然人位置和行为信息也应当按照个人信息予以保护。

3. 数据出境和提供

《评估指南》明确了“数据出境”是指将在中华人民共和国境内收集和产生的“电子形式”的个人信息和重要数据，提供给境外机构、组织；而境外数据经由中国中转，未经任何变动或加工的，不属于数据出境。但是，除网络运营者主动提供或者通过其他途径发布数据的行为外，其用户使用网络运营者提供的产品或服务，向境外机构、组织或个人提供数据的行为也属于“提供”。

因此，一方面《评估指南》排除了部分行业人士对各种形式（包括非电子形式）出境的个人信息和重要数据出境都属于数据出境的顾虑。另一方面，网络运营者通过用户利用其产品和服务对外提供数据，也会被认定为网络运营者数据出境，如此则对部分网路运营者通过技术处理手段或交易架构设计等变通方法实现数据曲线出境的做法提出了监管要求。

4. 评估流程

按照《评估指南》，评估流程包括自评估启动、制定计划、评估计划（合法正当和风险可控）以及制作评估报告，其中评估报告至少保存 5 年。按照该项要求，评估报告无疑成为了网络运营者开展个人信息和重要数据出境安全评估的一份必备文件。而结合下文中要讨论的“评估要点”，从工作内容上而言，则该份评估报告又无异于是要求网络运营者对与其业务相关的网络安全和数据保护进行一项全面的尽职调查，其中涉及技术、法律和政策等多方面内容。

5. 评估要点

如上所述，评估要点从“合法正当”和“风险可控”两个角度展开。我们理解，“合法正当”相对简单，对网络运营者来说义务相对较轻，基本上从业务必要性角度就能论证成功。

而“风险可控”则要求相对较高。《评估指南》从数据属性（个人信息和重要数据）、业务主体能

力（发送方和接收方）以及宏观环境分析（接收方所在国的政治法律环境）等方面提出了综合评估要求。评估内容较多，覆盖面广，意味着较多的评估义务和工作，是网络运营者自行评估的难点。

其中，在个人信息和重要信息属性评估中，《评估指南》就范围都提出了“最小化原则”的要求。最小化原则要求信息或数据与出境目的相关业务有直接联系，即没有该信息参与，相应功能无法实现；并且传输频率（自动传输下）和数量都应当是与数据出境目的相关的业务功能所需的最低频率和最低数量。

6. 附录 A：重要数据

附录 A 规定，指南中的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，可能对国家安全、国家经济和金融安全、社会公共利益、个人合法权益等造成相关严重后果的数据。

除此之外，附录 A 详细列举了 27 个行业（领域）及其重要数据范围供参考。所罗列的行业和领域，明显比《网络安全法》和《网络安全检查操作指南》中所界定的 CII 重要行业和领域的范围广泛，基本涵盖了主要的行业领域，并且在最后规定了兜底条款，指出了其他行业判断重要数据的标准。据此，我们倾向于认为，数据境内存储和出境评估审查范围应在《网络安全法》既定框架下和不影响数据有序自由跨境流动的基础上，适当做扩大解释。

7. 附录 B：评估方法

《评估指南》附录 B 详细描述了评估方法。首先，评估个人信息出境对个人权益的影响等级、重要数据对国家安全和社会公共利益的影响等级，以及根据发送方和接收方安全保障能力，和接收方所在地政治环境，对安全事件可能性等级进行判定。其次，进行安全风险综合评估，根据上述个人权益和国家安全、社会公共利益受影响程度，以及安全事件可能性两个维度进行综合评价，将数据出境活动整体安全风险级别划分为“极高”、“高”、“中”和“低”四个等级。其中，经评估出境安全风险为“极高”或“高”的，个人信息和重要数据不得出境。

三、 结语

《评估指南》内容详细，实操性较强，适用时需要网络运营者对照自身情况具体分析。虽然目前《评估办法》和《评估指南》都在征求意见阶段，还未正式出台，但《网络安全法》所要求的数据本地化存储和数据出境评估已势在必行。因此，我们建议相关企业，不论是否是 CII 运营者，都应当对照《评估指南》对自身情况进行初步判定，提早进行准备以应对可能的数据出境评估要求。

汉坤网络安全和数据合规系列：

之一：健康医疗大数据领域的政策和法律问题

之二：《网络安全法》简评

之三：数据出境不再任性

之四：网安审查，大幕开启！

之五：个人信息保护，刑法的归刑法

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**唐志华律师（+8621-6080 0905; david.tang@hankunlaw.com**）、或**朱敏律师（+8621-6080 0955; min.zhu@hankunlaw.com**）联系。