汉坤法律评述

2019 年 6 月 13 日

漢坤律師事務所
HAN KUN LAW OFFICES

北京 | 上海 | 深圳 | 香港

《个人信息出境安全评估办法》公开征求意见

作者：段志超 | 蔡克蒙 | 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[1]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[2]。

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；

[1] 《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。”

[2] 方法草案第 20 条。

- 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：

段志超

电话： +86-10-8516 4123
Email： kevin.duan@hankunlaw.com