《网络安全法（草案）》二次审议稿与境外企业的关注

何菁、侯磊

网络安全相关立法近年来成为中国立法机关和政府部门优先关切，先后颁布实施的《国家安全法》、《反恐怖主义法》等重要法律中均涉及网络安全的相关条款。中国全国人大常务委员会于 2015 年 7 月 6 日公布《中华人民共和国网络安全法（草案）》（“一审稿”），广泛征求社会各界意见，经过一年多时间的酝酿，又于今年 7 月 5 日进一步修改并发布了《中华人民共和国网络安全法（草案）》二次审议稿（“二审稿”）。

作为网络安全领域的基本法，未来发布生效的《网络安全法》将为中国信息通信产业中网络安全体系的建设、运营、维护和使用设立监管框架和基本规则，并对该领域的市场准入产生重大影响。因此，两个版本的网络安全法草案均引起了社会各界，包括国外产业界的广泛关注。目前对于草案中的部分规定在国外企业有着相当不同的认识，其中可能存在误解和偏差。但是对这些意见进行研究与探讨，可能对于完善未来的立法有些许价值。本文根据了解到的情况，尝试对国外企业关注的若干重点问题予以总结并初步评述。

一、 数据本地化的要求

从各国网络安全立法的实践来看，数据本地化要求是网络安全制度中的最为核心，但是也是最有争议的制度。一方面，数据本地化存储使得执法部门在紧急情况下能够及时掌握和调取数据，应对网络安全事件；但是另一方面，数据本地化的要求易于在各国之间形成“信息孤岛”，使得跨国的信息流动和存储受到阻碍。尤其是在以云计算和大数据为代表的新一代信息技术迅猛发展的背景下，如何设置数据本地化要求是各国网络安全法体系中必须要面临的问题。“随着信息技术全球化的普及，大数据、云计算应用更加广泛，数据留存体现的数据本地化要求与数据跨境常态性的客观现实产生冲突，执法机构在数据留存过程中的潜在风险也招致越来越多的非议。”[i]

近年来，中国政府机关的在信息本地化存储方面已经有若干零散的规定，《人口健康信息管理办法（试行）》第 10 条规定了人口健康信息实行分级存储的原则，同时规定“不得将人口健康信息存储在境外的服务器中，不得托管、租赁在境外的服务器”。《征信业管理条例》第 24 条也规定，征信机构在中国境内采集的信

息的整理、保存和加工，应当在中国境内进行。”[ii]《地图管理条例》第 34 条规定：“互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内”。这一系列规定体现了中国政府在金融，测绘，人口信息等领域加强信息流动的限制。

《网络安全法》进一步明确和扩展了关于数据本地化的规定。在一审稿第 31 条中，其要求“关键信息基础设施的运营者应当在中华人民共和国境内存储在运营中收集和产生的公民个人信息等重要数据”，确需要提供给境外的，需要通过“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”。在当前二审稿第 35 条的规定中，依然要求关键信息基础设施运营商“在中华人民共和国境内运营中收集和产生的公民个人信息和重要业务数据应当在境内存储”。尽管二审稿似乎将要求放松至仅在境内收集和产生的数据，但它在“公民个人信息”的基础上增加了“重要业务数据”，实际上可能会更加宽泛。

国外企业尤其会关注“重要业务数据”边界界定带来的不确定性：何种 “业务数据”会引发这些限制和要求？有的企业可能认为，数据本地存储的要求应当仅仅限制在最为敏感的数据上。认为推定网络安全和信息完整性在某一地理区域比另一地理区域更安全并无依据。从国际上的整体趋势来看，“数据留存法律制度的重心开始从本国留存数据过渡到对数据跨境的监管”。[iii]跨境数据流动对全球经济的发展是非常必要的，而中国在全球经济中扮演着关键角色。重点在于关注部署技术和程序安全措施以保护数据，而不在于数据存储的物理位置。当前的二审稿中虽然有关于安全评估的制度，但是依然非常不明确。例如，当一家公司“因业务需要而确需”向境外转移数据时，是否每次都需要进行安全评估？

事实上，数据本地存储的要求不仅仅对国外企业增加负担，该要求也将使得中国企业，尤其那些已经扩张或正希望扩张至全球市场的中小型企业面临困难，或者至少造成监管上的风险。

二、因执法活动和国家安全而获取数据

二审稿第 27 条要求网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。不同于一审稿，第 27 条的义务不再限制于“必要”的范围之内。国外企业由于对于中国执法系统的不熟悉和种种观念限制，对于这方面的规定肯定意见较大。

对于现有文本而言，一种意见认为，将义务限制在“必要”的支持和协助之内

是非常重要的，应当予以保留，以确保在执法需要、用户在线存储其个人数据时对隐私的合理预期以及网络运营者保护其用户数据的义务之间保持审慎的平衡。

另外，国外企业对于正当程序的关注是非常迫切的，认为程序保障对于确保法治和必要的透明性至关重要，在修改意见方面对提出一系列的要求，包括：

（1） 对做出此类要求的法律程序进行明确。

（2） 为与国际法律实践保持一致，执法机关强制网络运营者提供协助应当仅限于具备具体明确法律依据的情形，而且应当制定严格的程序以防止可能的权力滥用。

（3） 在企业没有掌握加密密钥的情况下，不应当要求他们提供解密信息

（4） 考量到运营商的利益，在数据访问要求与合同义务、依据中国其他法律应该对中国消费者履行的义务以及国外法律适用产生冲突的情形下就如何解决这些冲突提供指导性规定。

（5） 要求获取数据的行政决定应当受到司法审查的约束。

三、 关键信息基础设施

一审稿对关键信息基础设施做出了大量的重要规定。二审稿的第 29 条将关键信息基础设施界定为“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益”。二审稿随后规定“关键信息基础设施的具体范围和安全保护办法由国务院制定”。

相较于一审稿第 25 条用“用户数量众多”限定，通过列举信息系统清单的方式对关键信息基础设施进行的定义，二审稿的定义从概念范围上有所改进。

关键基础设施和关键信息基础设施的定义方式在包括欧盟、美国、日本等其他国家在内的国际实践中也是一种新兴事物。国外企业一般会希望中国参考国际实践，以确保所采用的方式既满足中国政府的特殊需要，也尽可能与国际通行规定保持一致。这当中一个主要的理由是，采用比较一致的定义，将便于技术和服务提供者开发和利用全球最佳技术，提高中国关键信息基础设施整体网络安全和网络恢复能力。

未来，国外企业会继续关注关键信息基础设施的进一步界定方式和保护办法。国外企业一般认为，只有用于支持关键资产和服务的网络和信息系统，才应当被认为是关键信息基础设施。同时应当明确的是，用于服务非关键或私人系统的同一信息网络不能仅仅因为其在其他情形之下被认为是关键基础设施的缘故，就认为其受《网络安全法》针对关键信息基础设施做出的相关规定的约束。

四、个人信息、通知和同意

不少国外企业认为，当前审议稿第四章网络信息安全中的很多内容最好是在关于数据隐私和个人信息保护的其他法律中单独规定。个人信息保护和数据隐私的问题尽管和网络安全相关，但超出了网络安全的范围，并且涉及到其他问题。单独制定一部数据隐私法能针对个人信息的全部所有权人、收集者、处理者和用户作出一致的规定并赋予权利和义务，而不是仅仅针对网络运营者。

数据控制者和数据处理者管理、处理、存储和转移个人信息时，他们与数据主体之间赖以交流、通知以及获取同意机制相关的各种问题，无法通过第四章中的具体条款得到解决。国外企业提出，中国可以考虑制定一部全面保护个人信息的法律。在这方面，亚太经合组织(“APEC”)隐私框架[iv]和跨境隐私框架(“CBPR”)在内的隐私框架[v]认可和完善的责任模型可供参考。

总体而言，上面四个方面集中代表了国外企业对于当前《网络安全法》的关注。部分国外企业总的思路是，认为有必要区分带有政治色彩的国家安全和一般意义上的商业安全问题。后者实际上更需要市场机制来解决，过度的控制和保护反而有可能因施加过度的限制而阻碍正常的商业活动，并最终损害网络安全的防护能力，符合市场规律的监管方式才能发挥最佳效果。

---

[i]《网络安全法》中数据留存法律制度的解构与建议，果园，《中国信息安全》 2016 年 06 期
[ii] 参见：http://www.ctex.cn/article/quanzi/qbzx/201605/20160500025821.shtml
[iii]《网络安全法》中数据留存法律制度的解构与建议，果园，《中国信息安全》 2016 年 06 期
[iv] 参见:
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
[v] 参见：http://www.cbprs.org/