新法速递
中国新《网络安全法》生效

纽约
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

香港
Mark Johnson
mdjohnson@debevoise.com

上海
Philip Rohlik
prohlik@debevoise.com

华盛顿特区
Jeffrey P. Cunard
jpcunard@debevoise.com

Luke Dembosky
ldembosky@debevoise.com

2017 年 6 月 1 日，中国新《网络安全法》正式生效。在该法于 2016 年刚刚通过时，我们曾发表出版物评论：作为中国首部完全致力于网络安全问题的立法，该法将对中国境内经营企业创设重大义务。其中，最为重要的是有关“关键信息基础设施”运营者的义务，包括在中国大陆境内存储数据、就数据跨境转移进行安全评估，以及购买的特定网络产品或服务应经安全审查。[1] 我们还注意到，《网络安全法》将可能影响跨国公司的 IT 基础设施布局以及向境外转移数据的能力。

当时我们提到，《网络安全法》因语言的模糊宽泛引发质疑，并希望后续的实施办法可以澄清这些疑惑。[2] 然而，目前该法业已生效，但很多问题并未得到澄清。另外，与该法相关一项重要实施办法在未来 18 个月内不会实施生效。

今年上半年，中国最主要的互联网监管机关国家互联网信息办公室（“国家网信办”）公布了两项有关《网络安全法》的实施办法公开征求意见。其中一项，即《网络产品和服务安全审查办法（试行）》（“《安全审查办法》”）就特定网络产品和服务的安全标准提供了指导，并规定了一套由政府组织安全审查的流程。[3] 另外一项办法，即《个人信息和重要数据出境安全评估办法》（“《数据出境办法》”）旨在规制跨境数据传输问题，并详细制定了一套数据跨境转移的

[1] 根据《网络安全法》，关键信息基础设施运营者被定义为在“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域”以及一旦遭到破坏可能严重危害“国家安全、国计民生、公共利益”的行业和领域中的网络运营者。参见《网络安全法》第 31 条。

[2] “China Passes Network Security Law”（《中国通过<网络安全法>》），Debevoise Client Update（2016 年 11 月 10 日），http://www.debevoise.com/insights/publications/2016/11/china-passes-network-security-law.

[3] 《安全审查办法》第一稿于 2017 年 2 月公布公开征求意见。该《办法》最终稿于 2017 年 5 月 2 日出台，中文版本参见 http://www.cac.gov.cn/2017-05/02/c1120904567.htm.

安全评估流程。[4] 《数据出境办法》和《安全审查办法》均计划于 6 月 1 日生效，尽管众多日常运营中涉及向境外传输数据的企业认为这两项文件缺乏明确性。

2017 年 5 月，数十家跨国企业集团组成联盟要求中国推迟《网络安全法》及其实施办法的生效，提出《网络安全法》有可能妨碍市场准入，与世界贸易组织的条例相冲突。随后，国家网信办决定暂缓实施《数据出境办法》，实施日期推迟到 2018 年 12 月 31 日。而《安全审查办法》仍于 6 月 1 日生效。

《安全审查办法》

《安全审查办法》旨在规定《网络安全法》第 35 条的实施问题，要求关键信息基础设施运营者确保其购买的特定 "网络产品及服务" 通过 "安全审查"。

该《办法》项下的网络安全审查要求关注于产品和服务是否具有 "安全性" 和 "可控性"。审查必须评估一系列具体的风险，比如，产品和服务被非法控制、干扰和中断运行的风险。[5] 国家网信办将设立网络安全审查委员会（"委员会"）来负责审议制定网络安全审查的重要政策，并设立网络安全审查办公室负责具体进行实际审查工作。[6] 另外，委员会将聘请专家组成专家委员会评估安全风险。[7] 具体审查方法将包括实验室检测、现场检查、在线监测、背景调查等。[8]

《安全审查办法》并未提供太多具体的实践指导，而更多的是规定了一般性原则。比如，该《办法》并未明确审查流程的任何时间期限，也未说明相关安全风险将被如何评估。由于缺乏明确性，监管者将有较大的自由裁量空间。

《数据出境办法》草案

《数据出境办法》目前仍为 2017 年 5 月 2 日公布的草案版本，计划于 2018 年 12 月 31 日予以实施。《数据出境办法》的目的是针对《网络安全法》项下有关"数据本地化"和数据传输条款进行澄清。《网络安全法》第 37 条规定，关键

---

[4] 2017 年 4 月 11 日，《数据出境办法》第一稿于 2017 年 4 月 11 日出台公开征求意见，中文版本参见 http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. 2017 年 5 月 19 日，国家互联网信息办公室（"国家网信办"）邀请外国利益相关者参加研讨会讨论《数据出境办法》的更新版本。虽然该更新版本并未正式公布，本文所引用条款均为该版本内容。

[5] 《安全审查办法》第 4 条。

[6] 《安全审查办法》第 5 条。

[7] 《安全审查办法》第 6 条。

[8] 《安全审查办法》第 3 条。

信息基础设施运营者必须将在中国大陆境内运营中收集和产生的 “个人信息和重要数据” 在境内存储，如需向境外传输数据应进行 “安全评估”。

《数据出境办法》将《网络安全法》项下规定的“安全评估”的范围扩展至不仅涵盖关键信息基础设施运营者，还涵盖一般的“网络运营者”。[9] 《网络安全法》将“网络运营者”定义为“网络的所有者、管理者和网络服务提供者”[10]，而这一定义如此宽泛，几乎可以涵盖使用网络进行经营的任何实体，无论其所属行业类型。这意味着，例如，一家仅使用局域网收集雇员信息的公司也可能因其在集团内部的跨境数据传输需要进行安全评估。

两种类型的数据将受到安全评估要求约束：“个人信息” 和 “重要数据”。“个人信息”指能够单独或者与其他信息结合识别自然人个人身份的各种信息，比如，姓名、生日、身份证件号码等。[11] 而 “重要数据” 并非指对公司重要的数据，而是 “与国家安全、经济发展，以及社会公共利益密切相关的数据”。[12]

《数据出境办法》规定了两类评估流程：自行评估和监管机构组织的评估。一般来说，网络运营者有义务对其数据出境进行安全评估。[13] 行业主管或监管部门在特定情况下应进行安全评估，比如，如果数据出境涉及的个人信息量巨大（即，含有或累计含有 50 万人以上的个人信息），或者如果出境的数据与敏感事宜相关（比如，核设施、国防、海洋环境等）或涉及与关键信息基础设施相关的网络安全信息，或者出境涉及其他可能影响国家安全和社会公共利益的数据。[14]《数据出境办法》还详细规定了同时适用于自行评估和监管机构评估的实质性标准，包括评估涉及的方面（比如，所涉及个人信息的数量、范围、类型、敏感程度），以及在何种情况下数据将被禁止出境（比如，数据出境可能影响中国的国家安全或损害社会公共利益）。[15]

值得注意的是，《数据出境办法》强调了保护个人信息。根据《数据出境办法》第 4 条，个人信息出境，应向个人信息主体说明数据出境的 “目的、范围、内容、接收方及接收方所在的国家或地区”，并经其同意。此要求的唯一例外是当出

---

9 《数据出境办法》草案第 2 条。

10 《网络安全法》第 76(3)条。

11 《数据出境办法》第 15 条；《网络安全法》第 76(5)条。

12 《数据出境办法》第 15 条。

13 《数据出境办法》第 6 条。

14 《数据出境办法》第 7 条。

15 《数据出境办法》第 8 和 9 条。

现危及公民生命财产安全的紧急情况。《数据出境办法》还强调，个人信息出境未经个人信息主体同意，数据不得出境。[16] 由于这一规定不存在明示的例外情形，且“个人信息”的定义宽泛，因而可能给任何向境外的数据传输增加负担。因而我们希望这一问题可以在《数据出境办法》18 个月正式生效前得以解决。

未来展望

虽然《网络安全法》和《安全审查办法》已经生效，但有关如何遵守这两项法律文件尚不够清晰，而《数据出境办法》草稿何时将正式通过、是否会以目前的版本通过也尚不明确。另外，监管机构目前执行的首要目标，以及安全审查将被如何执行也尚未可知，但在关键产业领域经营的企业及供应商应对相关法律要求更为警惕。

在期待出台后续实施细则或指南的同时，我们建议受《网络安全法》约束的公司考虑：

- 持续与在华各国商会及其他商业组织共同合作以获取更多明确性；
- 根据自身的商业性质，所供应产业以及商业运营过程中收集、处理数据的性质和数量，评估公司是否符合关键信息基础设施运营者的定义；
- 审查当前的 IT 基础设施布局和数据合规程序，评估其是否符合数据本地化、跨境数据转移和产品服务安全审查的要求；
- 咨询法律专业人员，确定需要改进的方面以提高网络安全合规性；并
- 提前计划与监管机构可能发生的互动，规划危机管理策略。

* * *

如果有任何问题，请您随时联系我们。

[16] 《数据出境办法》第 9(2)条。