中国新《网络安全法》可能会影响中国境内外公司运作：你准备好了吗？

中国网络运营者，尤其是关键信息基础设施所面对信息保护法规日渐增多，将给网络运营者的服务合同造成负担，甚至影响到中国境外的数据传播。

徐辉、郭威君著

美国瑞生律师事务所

重点：

- 中国新《网络安全法》加强了对网络安全和个人隐私的保护。
- 具有收集个人信息功能的中国网络运营者需要建立保护用户信息安全的制度。
- 公司内部法律顾问应协助企业应对不断变化和发展的《网络安全法》。

在过去数月，中国网络运营者面对着日益严峻的数据保护挑战。中国备受期待的《网络安全法》及其相关规则和标准的颁布，相比其他法律措施，将对数据保护带来最深远的影响。

《网络安全法》及其相关法规自2017年6月1日生效以来，不仅为中国网络数据的保护和安全制定多项重大规定，也为国内外的企业带来持续挑战。近期有报道称国家互联网信息办公室（CAC）多次开展了数据保护执法行动，例如审阅中国网络运营者的隐私政策及其实施情况，这表明中国数据保护和网络安全风险正被日益重视。本文将概述公司内部法律顾问应如何遵守这些法规以应对相关挑战。

夯实网络安全管理系统基础

《网络安全法》适用于中国的网络运营者（即网络的所有者、管理者以及网络服务提供者），网络运营者必需依法制定相关内部政策流程以保障其在中国境内的网络安全。依据《网络安全法》未履行网络安全管理职责的违规者不但会受到行政处罚，如被责令暂停相关业务、关闭网站、吊销相关业务许可证或营业执照、企业或相关人员被处行政罚款等；若违规行为情节严重，还可依照中国《刑法》承担相应的刑事责任，如有期徒刑、拘留及/或刑事罚款等（例如泄露用户信息而导致严重后果）。

公司内部法律顾问需要和公司内部的相关职能部门密切合作，来确保企业遵守《网络安全法》的相关规定，包括在网络安全制度中加入网络安全措施。例如，中国的网络运营者应施行以下各项措施：

- **网络安全措施。**实施技术措施防止电脑被入侵并监督网络运作；安排网络安全负责人落实网络安全保护责任；按照规定留存相关网络日志不少于六个月；备份和加密重要数据；及制定和演练网络安全事件应急预案（例如应对电脑病毒、网络攻击与网络入侵等危机）

- **用户信息保护。**收集用户信息前应当向用户明示并取得同意；建立用户信息保护制度以严格保密用户信息；建立适当机制使用户可以在某些情况下删除或更改其个人信息；如发现或怀疑用户个人信息被泄露、损坏或遗失，应及时采取补救措施并通知用户及相关主管部门

- **线上内容管理。**向用户提供网络内容发布及传播的相关服务（例如为用户办理网络接入、域名注册服务、固网电话或移动电话入网手续、信息发布或即时通讯服务）前应核实用户的真实身份和信息；加强对用户提供的网络信息管理，防止非法信息散布

- **网络产品及服务要求。**网络产品及服务要求。网络产品和服务供应商必需确保提供的网络产品和服务符合国家相关的强制性规定；在法规规定或各方同意的期间内提供安全支持；发现网络安全危机需即时采取补救措施并通知用户和有关主管部门

预期当局将加强对关键信息基础设施的监督从而对中国境内外的业务与数据传输造成影响

除了上述适用于网络运营者的规定外，被认定为关键信息基础设施的企业需要遵守更严格的网络安全规定，例如实施更严格的网络安全措施、对个人信息和重要数据实施本地存储，遵循数据出境要求并在采购网络产品和服务时通过国家安全审查等。

关键信息基础设施的定义尚处发展阶段

虽然《网络安全法》及其相关规则（尚处征求意见阶段）载列了关键信息基础设施的行业描述，但其详细定义仍有待当局进一步界定。

徐辉

《网络安全法》不仅为中国网络数据保护与安全提供重要法律依据，也为国内与国际企业带来了持续挑战。

郭威君

下表载列了《网络安全法》与CAC在2017年7月10日对外发布的《关键信息基础设施安全保护条例（征求意见稿）》中对关键信息基础设施的定义：

	《网络安全法》	《关键信息基础设施安全保护条例（征求意见稿）》
关键信息技术设施的定义	1.公共信息和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域	1.政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领
		2.电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位
		3.国防科工、大型装备、化工、食品药品等行业领域科研生产单位
		4.广播电视、电视台、通讯社等新闻单位
	2.其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施	5.其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的单位

虽然《关键信息基础设施安全保护条例（征求意见稿）》对于《网络安全法》中给出的关键信息基础设施的定义可能作出进一步说明，从而致使界定某一企业是否属于关键信息基础设施仍存在不确定性，但是《关键信息基础设施安全保护条例（征求意见稿）》的发布（尽管只是征求意见稿）还是有助于我们进一步了解监管机构对于关键信息基础设施的界定范围。《关键信息基础设施安全保护条例（征求意见稿）》还规定国家网信部门将会与相关政府机关制定关键信息基础设施识别指南，这显然会从各行业的角度来更加明确关键信息基础设施的涵盖范围。有报告指出相关政府机关已将数百家企业认定为关键信息基础设施运营者，当中大部分为中国国有企业。相关政府机关已通知这些国有企业其已被认定为关键信息基础设施运营者并告知其应当遵守的相关合规要求。一旦相关政府机关公布关键信息基础设施运营者初步名单和关键信息基础设施识别指南，企业可望于近期内进一步明确对关键信息基础设施的认定准则。

关键信息基础设施应遵循更严格的相关数据要求

根据《网络安全法》，关键信息基础设施运营者应当履行更严格的网络安全保护义务，例如设置专门安全管理机构和安全管理负责人、定期对从业人员进行网络安全教育、技术培训和技能考核，以及对重要系统和数据库进行分类、容灾备份和备份等，其中最受关注和争议的网络安全要求是关键信息基础设施运营者需遵守《网络安全法》下的数据出境规定。

具体而言，《网络安全法》规定关键信息基础设施运营者在中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，应当按照主管部门制定的办法进行安全评估。除了数据出境规定外，

《关键信息基础设施安全保护条例（征求意见稿）》还规定关键信息基础设施的运行维护应当在中国境内实施，因业务需要确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。

随着更多国内和跨国企业将可能落入关键信息基础设施（范围仍然不断说明）的监管范围，它们可能会受到数据只准在境内储存/传送这一规定所带来的限制和掣肘，其境外进行远程业务维护也可能遭受限制（正如《关键信息基础设施安全保护条例（征求意见稿）》所规定的）。因此，企业必需密切关注相关法规的发展，预先做好准备，避免违规所带来的法律后果。

个人信息保护的范围不断扩大

《网络安全法》及其相关法规另一个引人注目的发展在于加强对个人信息的保护。虽然之前多项法规从各个角度做出过类似的规定，但唯独《网络安全法》以其完整严密的结构重申了相关规定，要求网络运营者建立健全用户信息保护制度，以加强对用户信息的保护。因此公司法律顾问及时了解和审查公司内部是否在各方面做到依据《网络安全法》的要求对用户信息进行保护就显得尤为重要。

新法规强调网络运营者需要建立一套健全的用户信息保护制度，凡收集、储存、处理和转移个人信息，应明确与被收集者沟通，并在进行上述操作前得到被收集者同意。具体而言，根据《网络安全法》，网络运营者收集、使用、转移和分享个人信息，应当遵循网络运营者与用户之间的协议，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。此外，《网络安全法》规定，网络运营者未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者成为重点整顿对象已经反映在最近针对网络运营者隐私政策的执法行动中。最近有新闻指出，中国当局已经对至少十家领先的网络服务供应商的隐私政策进行审查并提出意见。据报道，中国一家移动地图应用运营者将会采用以《个人信息安全规范》（该规范征求意见稿预期将会在短期内公布）为基础的新网络隐私政策。此外，工业和信息化部还颁布了《移动互联网综合标准化体系建设指南》，要求网络运营者在制定网络隐私政策时，内部法律顾问应参考其规定的“用户个人信息保护指南”。

由于《网络安全法》可能会为企业和个人带来刑事责任，内部法律顾问应审查和自我评估公司现行的网络隐私政策与保护个人信息的基础设施建设，以识别潜在的违规漏洞并加以纠正。

你准备好了吗?

总而言之，中国不但正在加强对互联网活动和数据保护的监管，对网络运营者和用户也在施加更多责任。明智的企业应采取措施对已经发生的和即将发生的改变做好准备。

本文特别鸣谢美国瑞生律师事务所华盛顿办公室合伙人Jennifer C. Archie。

文章翻译自2017年10月《Asian-mena Counsel》出版的英文原版。

LATHAM&WATKINS LLP
hui.xu@lw.com
lex.kuo@lw.com
http://www.lw.com