漢坤律師事務所

汉坤法律评述

融贯中西 · 务实创新

2016 年 7 月 26 日

# 《中华人民共和国网络安全法（草案）》二次审议稿解读

唐志华丨孙冠绯

互联网时代，网络安全问题在全球范围内正日益成为各国立法与监管的焦点。中国全国人大常务委员会继 2015 年 7 月 6 日公布《中华人民共和国网络安全法（草案）》（“初审稿”）后，又于今年 7 月 5 日，结合当下建设、运营、维护和使用网络和相关监管的实际情况，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”），广泛征求意见，以期尽快正式出台一部网络安全的专门性法律，以规范网络信息保护，解决网络安全问题。

## 一、 我国网络安全立法的现状

我国目前尚没有一部生效的网络安全专门性法律，网络安全相关的立法主要还是围绕着用户个人信息的保护，散落在多部法律和法规等规范性文件之中，主要包括：《电信和互联网用户个人信息保护规定》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《网络交易管理办法》、《消费者权益保护法》和《规范互联网信息服务市场秩序若干规定》等。总体而言，上述法律法规要求收集和使用个人信息的公司，特别是涉及网络服务的公司，采取适当措施，以确保上述信息安全并阻止用户个人信息泄露、毁损或丢失；当发生或可能已发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

为适应互联网经济发展和网络安全全球化的趋势，我国全国人大常务委员会在 2015 年 7 月 6 日公布了初审稿，又于今年 7 月 5 日公布了二审稿，在征求意见后，有望在今年年末或明年年初正式颁行。

## 二、 二审稿主要内容和修订

二审稿适用于在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，基本延续了初审稿的框架与内容，主要内容包括：维护网络主权和战略规划、保障网络产品和服务安全、保障网络运行安全、保障网络数据安全、保障信息安全、监测预警与应急处理和监督管理与法律责任。

在初审稿基础上，二审稿主要有以下修订：

**1. 加大国家层面网络安全的保护与支持**

二审稿把网络安全提升到了国家层面的保护。例如，新增的第五条要求国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

同时，二审稿第十五条、十六条和十七条进一步要求国家支持和促进网络安全发展，要求各级政府推广安全可信的网络产品和服务；国家推进网络安全社会化服务体系建设，鼓励企业、机构开展网络安全认证、检测和风险评估等安全服务；并且，国家鼓励开发网络数据安全保护和利用技术，促进公共资源开放，推动技术创新和经济社会发展；支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

国家从网络安全保护和网络产品、服务提升与技术发展两方面予以鼓励与支持，坚持网络安全与信息化发展并重。

**2. 进一步规范网络运营者行为**

二审稿对作为网络安全源头的网络运营者增加了相应的责任。二审稿在总则中增加规定，网络运营者在开展经营和服务活动时，除了遵守法律法规，还应当遵守社会公德、商业道德，诚实信用，履行网络安全保护义务，接受政府和社会公众的监督，承担社会责任。

二审稿第二十条明确要求网络运营者留存网络日志的时间不少于六个月。而为维护网络秩序，规范网络运营者行为，第二十五条又要求网络运营者或其他机构、个人开展网络安全认证、检测、风险评估等活动，以及向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等安全信息，应该遵守国家规定。

网络运营者是网络产品和服务的提供者，以及网络运行安全和网络数据、信息保护的直接责任人，二审稿以道德和社会责任向网络运营者提出了更严格的要求，并进一步规范网络运营者的经营与服务，有利于从源头保障网络秩序，促进网络安全保护与技术发展。而对网络安全认证、风险评估活动的规范则有利于加强网络用户对网络安全体系的信赖及并促进其健康发展。但是，对于发布系统漏洞、计算机病毒、网络攻击、网络侵入等安全信息应遵守的国家规定，还有待进一步细化与明确。

**3. 加强关键信息基础设施及数据保护**

网络安全法律法规下，“关键信息基础设施”保护包括保护其运营安全和相关信息与数据安全，其对国家安全、各经济部门运行安全以及公民个人信息安全保护至关重要。

关于“关键信息基础设施”的范围，初审稿进行了列举，包括公共通讯、广播电视等基础信息网络，能源、水利、交通、金融、公共服务领域等重要信息系统，以及军事、政务网络和用户众多的网络和系统等，而二审稿第二十九条则删除了该等例举，把关键信息基础设施的具体范围和安全保护办法交由国务院另行制定。

对于“关键信息基础设施”相关数据与信息的保护，初审稿要求关键信息基础设施的运营者对运营中收集和产生的公民个人信息等重要数据境内存储，而二审稿第三十五条要求将其重要业务数据也列为需要境内存储的重要数据。二审稿第三十八条还要求国家网信部门和有关部门在保护关键信息基础设施中获取的信息，只能用于维护网络安全需要，不可用于其他用途，避免有关部门滥用职权危害信息安全。

显而易见，二审稿删除“关键信息基础设施”的定义范围，以后续行政规范予以界定的修订增加了作为设施与数据保护前提的“关键信息基础设施”的灵活性，便于今后根据不断变化的网络技术和环境对其进行调整，以利于更好地保护关键信息基础设施。当然，在《网络安全法》正式颁行后，国务院应尽快制定配套的文件，规定“关键信息基础设施”的范围，否则今后可能出现新法在该定义内涵的可操作性问题。

另外，二审稿建议网络运营者自愿参与关键信息基础设施保护，目的是加强网络运营者、专业机构和政府有关部门之间的网络安全信息共享，同时加强对这些信息的保护，但具体如何操作目前不得而知。

**4. 增加实名认证领域**

二审稿第二十三条在网络运营者提供网络接入、域名注册服务、固定电话和移动电话入网服务、信息发布服务时，要求用户提供真实身份信息之外，增加即时通讯等服务的实名认证要求。另外，二审稿要求国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。一方面扩大网络信息可追溯范围，倒逼网络用户遵守网络安全法律法规，另一方面通过技术开发便利身份认证，进一步加快身份信息认证进程，建立网络可信身份战略体系。

**5. 接轨大数据网络时代**

二审稿在第四十一条中规定网络运营者不得泄露、篡改、毁损其收集的公民个人信息；未经被收集者同意，不得向他人提供公民个人信息。但是，经过处理无法识别特定个人且不能复原的除外。在保护网络安全同时，为大数据技术对非敏感个人信息的收集与利用，提供了法律依据与支持。与此同时，前述国家鼓励开发网络数据安全保护和利用技术，支持对公共资源开放和网络技术创新，以及规范网络安全认证、风险评估等，同样是对云计算、大数据研究等技术发展和应用的支持。

**6. 加强危害网络安全行为惩戒力度**

二审稿第五十四条增加了对存在网络安全风险的网络运营者的法定代表人或负责人的约谈机制。第六十一条规定了终身行业禁入，即故意从事危害网络安全的活动受到治安管理处罚或者刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。另外，在原有责令改正、警告、暂停相关业务、停业整顿、关闭网站、吊销业务许可证以及吊销营业执照和罚款等处罚手段的基础上，二审稿第六十八条对违反该法的行为的，新增了将相关违法行为记入信用档案的规定。

很明显，二审稿意图通过加大对危害网络安全行为的惩戒力度，减少相关违法犯罪行为，在最大程度上预防风险，消除安全隐患。

## 三、 总结和建议

相比于初审稿，我们认为二审稿的修订进一步结合了网络信息保护实践经验和网络技术发展，与国家大力提倡的网络经济相互配套和促进。《网络安全法》的颁行将有助于理清当下复杂的网络安全监管情况和法规体系。当然，其正式出台和有效实施还有待进一步梳理、论证，也需要相关配套文件的出台和施行。我们也将持续关注《网络安全法》立法的最新进展。

在《网络安全法》正式颁行之前，我国现行有效的网络安全立法仍以用户个人信息保护为核心。因此，我们建议公司在处理任何形式的个人信息或管理个人信息时，采取合理的措施，例如：采取有效的技术措施和内部规章，以保障信息安全并阻止内部或外部的非法访问、获取和黑客入侵；涉及收集、使用和转移用户个人信息的，应向其明确披露并获取其书面或电子形式的同意，该等同意应当慎重措辞以保留在法律允许范围内处理的灵活性；对个人信息的收集、使用和转移应当被限定在同意和提供服务所必须的范围之内；在未获适当授权时，在任何情况下均不得转让或售卖个人信息；当信息泄露或黑客事件发生或可能已发生时，及时通知相关方并采取相应补救措施。

## 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**唐志华律师（+8621-60800905; david.tang@hankunlaw.com）**联系。