漢坤律師事務所

汉坤法律评述

融贯中西 · 务实创新

2015 年 12 月 28 日

反恐法对互联网企业的冲击有多大？

许莹丨王晨

2015 年 12 月 27 日，旨在打击恐怖主义、维护国家安全及公共安全的《中国人民共和国反恐怖主义法》（以下简称“**《反恐法》**”）由十二届全国人大常委会第十八次会议表决通过并正式公布，该法将于 2016 年 1 月 1 日起施行。恐怖主义活动危害甚广，重拳打击实乃民心所向。但值得关注的是，总计共十章九十七条的《反恐法》中的部分条款针对电信业务经营者以及互联网服务提供者（以下统称“**互联网企业**”）做出了不少义务性或限制性的规定，其中不乏备受争议之处，我们梳理了如下：

1. 宣传教育义务

《反恐法》中规定，互联网企业同各级政府、学校、新闻传播媒体等单位一道，共同担负着向社会进行反恐怖主义宣传教育的义务。

2. 防止恐怖信息传播的义务

《反恐法》中明确规定了互联网企业应当有效落实网络安全监督、防范措施，防止恐怖信息、极端主义信息的传播，并及时删除且向公安部门等进行报告。违反本条规定的，互联网企业及直接责任人员可能被相关监管部门处以一定数额的罚款，情节严重的情况下直接责任人员甚至可能被处以行政拘留处罚。

值得关注的是，之前向社会公开征求意见的《反恐法》（草案）中规定的、且引起部分互联网企业较大不安的“互联网企业应当将相关设备、境内用户数据留存在中国境内”的规定，在正式公布的《反恐法》中已经被取消。对于互联网企业数据是否必须全部在境内存储和对于跨境存储和传输的要求，在法律法规层面目前尚未有明确规定，但此前的实践中不乏要求将数据信息（特别是敏感信息）存储在境内的要求。此次《反恐法》虽未有明确突破，但未来实践中会否依据《反恐法》而进一步加强对于互联网企业数据存储和传输的限制，仍未可知。

3. 协助调查义务

《反恐法》第十八条是备受境内、境外关注的一条，其明确规定了相关政府部门在防范、调查恐怖活动中互联网企业有提供技术接口和解密等协助调查的义务。

虽然上述规定并非中国首创，在美国、欧盟等国家和地区均有类似规定，但众所周知，互联网企业作为轻资产类企业，其最核心的竞争力即是技术资源，如何在与相关政府部门的沟通、对接中有效保持企业正常的运营并保护企业知识产权，需要互联网企业的特别关注以及与政府部门的有效沟通与协调。

4. 查验用户身份义务

《反恐法》中还规定了互联网企业在提供服务前应当对客户身份进行查验，否则不得提供相应服务。违反本条规定的可能被相关监管部门责令改正，拒不改正或者情节严重的情况下甚至可能被监管部门处以一定数额的罚款。

就上述规定，目前很多互联网管理的分项专门法规中已经不乏约定，但随着立法层面的加强（特别是有关罚则的进一步明确），互联网企业未来仍然应当更加注意完善客户身份查验工作并保存完整相应的查验数据，以便未来在与恐怖主义活动发生被动关联等不可控因素的情况下更有效地证明“本企业已尽合理努力进行了用户身份查验工作”。

此外，与之相关的，互联网企业还应当注意遵守《电信和互联网用户个人信息保护规定》等法律法规，包括但不限于：不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，应当对前述信息严格保密、不得出售或非法向他人提供等。

综上可以看出，《反恐法》对互联网企业在经营中的相关义务及限制做了更为清晰和细化的规定，未来工业与信息化部等互联网企业的直接监管部门是否会出台更为细化的法律法规尚不得而知，我们将持续关注并及时与您分享。

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**黄蓉（+8610-8525 4613; nancy.huang@hankunlaw.com**）联系。