汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2016 年 11 月 9 日

《网络安全法》简评

唐志华 | 张驰 | 孙冠绯

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议，通过了历经三审稿的《中华人民共和国网络安全法》（“**《网络安全法》**”）。《网络安全法》全文共七章、七十九条，自 2017 年 6 月 1 日起施行。

《网络安全法》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。本文对《网络安全法》下的重要制度和亮点做了相关梳理和总结。

一、 强调网络空间主权和国家网络空间安全

随着互联网和信息技术的持续发展，国家网络空间主权面临严峻挑战。全球互联网环境表面风平浪静，实则暗涌波涛。网络空间安全已成为一项关乎国家主权、安全和利益的重大议题，全球范围内各国均在积极制定和构建维护网络空间安全方面的法律措施和监管体系。

以欧盟为例，欧盟最高司法机构欧洲法院于 2015 年 10 月作出判决，认定欧美 2000 年签署的关于自动交换数据的《安全港协议》无效；2016 年 4 月，欧洲议会通过了商讨近四年的《一般数据保护条例》，堪称史上最严格的个人数据保护条例；2016 年 7 月欧洲议会通过了《网络与信息安全指令》，标志欧盟层面首部网络安全法案正式出台。

在此背景下，我国于 2015 年 7 月通过了新的《国家安全法》，第一次明确“网络空间主权”概念。2016 年 7 月颁布的《国家信息化发展战略纲要》强调，在推进国家信息化建设过程中维护国家网络空间主权、安全和发展利益，并加快制定网络安全立法。

本次公布的《网络安全法》遵循了国家坚持网络安全与信息化并重的宏观发展思路，并在关键信息基础设施保护、网络信息安全、监测预警与应急处置以及法律责任等方面落实了相关规则和措施，尤其是在最终稿中追加针对境外主体的追责措施[1]，有利于增强网络空间主权的防御能力和威慑能力。

[1]《网络安全法》第七十五条，境外主体从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

二、 实施网络安全等级保护制度

《网络安全法》要求实行网络安全等级保护制度[2]。建立安全等级保护制度并非《网络安全法》首次提出的新要求。

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委在 2007 年制定《信息安全等级保护管理办法》第七条中，将信息系统的安全保护等级分为五级，信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作；信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合该办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评，并履行相应备案手续。

相关行业主管部门还在 2007 年《信息安全等级保护管理办法》的基础之上，出台了加强本行业信息安全工作的指引和规范，如教育部于 2009 年 11 月发布《教育部办公厅关于开展信息系统安全等级保护工作的通知》，要求高校及地市级以上教育行政部门三级以上的信息系统要在教育部教育管理信息中心和当地公安部门同时办理备案手续；卫生部于 2011 年 11 月发布《卫生行业信息安全等级保护工作的指导意见》，要求第二级以上（含第二级）信息系统，应当报属地公安机关及卫生行政部门备案。因此，属于特定行业的单位在其信息系统达到一定安全等级时，将归入公安部门和行业主管部门的双重监管之下。

此外，工业信息化部于 2010 年 1 月颁布的《通信网络安全防护管理办法》还要求中华人民共和国境内的电信业务经营者和互联网域名服务提供者，对本单位已正式投入运行的通信网络进行单元划分，按照各通信网络单元遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度由低到高分别划分为五级，并向电信管理机构履行相应的备案手续、落实安全防护措施和进行符合性测评。

《网络安全法》作为我国首部网络安全专门性法律，首次以法律形式要求国家实行网络安全等级保护制度[3]，但《网络安全法》并未明确网络安全等级制度所具体参照的办法和标准，所以在未来的实际操作上是沿袭目前公安部牵头、各行业主管部门辅助的双轨监管模式，还是会后续制定统一的网络安全分级管理办法，尚有待进一步观察。

三、 对关键信息基础设施实行重点保护

《网络安全法》引入了“关键信息基础设施”的概念，并在前述网络安全等级保护制度的基础之上实行重点保护。“关键信息基础设施”作为关乎国家安全和利益的战略性资源，其重要性无需多言，对“关键信息基础设施”在法律和制度层面进行重点保护乃是目前各国立法的大势所趋。

从一审稿到三审稿，“关键信息基础设施”的定义经历了一波三折的纠结过程。正式稿最终采用非穷尽式列举的方式对其进行了定义：“关键信息基础设施”是指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。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。前述定义，一方面通过行业列举大体勾勒出“关键信息基础设施”

[2]《网络安全法》第二十一条。

[3]《网络安全法》第二十一条。

的属性，另一方面也为国务院后续进一步界定“关键信息基础设施”的具体范围和制定安全保护办法保留了空间和灵活性。

《网络安全法》对“关键信息基础设施”主要采取了以下重点保护措施：

1. 第三十五条规定，关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查，同时在法律责任部分制定了对应罚则[4]。

   值得注意的是，涉及关键信息基础设施的国家安全审查并非是在《网络安全法》被首次祭出，在2015年初公布《外国投资法（草案）》[5]中，对我国关键基础设施和关键技术的影响即被列为外国投资国家安全审查应当考虑的因素。“关键（信息）基础设施”之于国家安全的重大战略性意义得窥一斑。

2. 第三十七条明确了关键信息基础设施相关信息跨境传输原则，即关键信息基础设施的运营者在中华人民共和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；法律、行政法规另有规定的，依照其规定。

至此，《网络安全法》成为目前首部限制数据向境外传输的法律，但该等限制仅针对关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据。值得注意的是，在《网络安全法》二审稿中，限制向境外传输的信息范围是“个人信息”和“重要业务数据”，最终稿将后者改为“重要数据”，限制境外传输的信息范围无疑有所扩大。

四、 完善个人信息保护制度

1. 受保护对象范围扩大：相比早前发布的《网络安全法》二审稿，《网络安全法》删除了“公民”在“个人信息”前的修饰，进而扩大了受保护对象范围，即包括所有使用我国网络服务的境内外个人，从而避免 “非公民”个人信息保护的立法真空。

2. 个人信息定义：《网络安全法》第七十六条规定，个人信息指以电子或者其他方式记录的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，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。上述对于个人信息范围的定义比较宽泛，但是相比2013年颁布的《电信和互联网用户个人信息保护规定》，《网络安全法》未包含可单独或结合其他信息识别用户使用服务的事件、地点等的信息[6]。

3. 大数据开发应用：《网络安全法》第四十二条规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；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。根据本条但书的规定，网络运营者似乎只要能对合法收集的个人信息进行脱敏处理以达到无法识别个人且不能复原的程度，那么对该等数据的处理和使用可不受个人信息保护规定的制约。由此可见，立法者有意从制度设计层面为大数据的应用留下可行性空间，以取得

[4]《网络安全法》第六十六条。

[5]《外国投资法（草案）》第四章。

[6]《电信和互联网用户个人信息保护规定》第四条。

个人信息保护和公众利益之间的平衡。

4. 明确网络运营者的信息安全义务：《网络安全法》整合了已经实施的《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》等法律法规中对于网络信息保护的规定。具体要求包括：公开收集、使用用户信息规则；按约定收集、使用信息；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，及时采取补救措施等。而对于个人发现网络运营者存在违法收集、使用个人信息，并要求予以更正时，网络运营者应当采取措施予以删除或者更正[7]。

   另外，《网络安全法》第四十九条规定，网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。但该条没有明确配合的限度和执法机关应当遵循的正当程序，从而在监督检查过程中可能会产生争议甚至诱发权力滥用。

5. 网络诈骗等违法行为惩治：《网络安全法》第四十六条规定，任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。监管机关可以依据第六十七条，对上述违法犯罪活动实施者进行处罚。原二审稿并没有该等条款，《网络安全法》正式出台后增加的这一规定，体现了立法和监管机关对目前泛滥的电信诈骗、电商乱象的整治决心。

五、 法律责任

《网络安全法》在二审稿基础上修改了部分处罚措施，将针对部分违法行为的罚金提高到原来的两倍。而对于从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，或者为上述活动提供服务的行为，差别化适用行业禁入惩戒措施：受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作[8]。

六、 其他亮点归纳

1. 关注未成年人保护：《网络安全法》第十三条要求研究开发利于未成年人健康的网络产品和服务，惩治利用网络危害未成年人身心健康的活动，并配套规定了相应罚则，旨在为未成年人提供安全、健康的网络环境。

2. “网络运营者”定义：《网络安全法》根据第七十六条的规定，“网络运营者”指网络的所有者、管理者和网络服务提供者。这一定义范围较广，几乎囊括了利用网络开展活动的各类主体，也就是说在我国境内提供或者利用通信网络、互联网络等提供产品与服务的各类营利性与非营利性主体，都属于《网络安全法》监管范围。

3. 实名制认证：《网络安全法》第二十四条提出实名制认证要求，规定为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，

[7]《网络安全法》第四十至四十五条。

[8]《网络安全法》第六十三条。

在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。相关网络服务提供者、网络运营者应注意严格遵守相关规定和标准。

4. 监管部门保密和合规使用义务：监管部门在相关日常监管、违法行为查处等活动中会接触到大量信息，因此《网络安全法》第三十条要求，有关部门在“履行网络安全保护职责”中获取的信息，只可用于维护网络安全需要。

   另外，《网络安全法》第十四条规定了违法行为举报相关事宜，并要求有关部门对举报人信息予以保密，以保护其合法权益。这也是立法鼓励良性举报，促进社会监督的体现。

5. 监测预警与应急处理：网络安全的保障应当从事前预警、事中防范以及事后处置三个方面进行规范。《网络安全法》要求网络运营者应当制定网络安全事件应急预案[9]。另外，第五章专章规定网络安全监测预警和应急处理制度建设，要求建立国家层面的网络安全监测预警和信息通报制度，强化网络安全事件风险防范机制，健全网络安全事件处置机制，并引入《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规。[10]

结语：

《网络安全法》是我国第一部网络安全专门性法律，其以法律形式提纲挈领地整合了众多相关下位法中对网络安全、信息保护的规定，并契合大数据、信息化发展的大背景，具有重要的里程碑意义。过去我国网络安全事件、信息泄露事件时有发生，一个重要原因在于立法缺位和执法不严。违法成本不高、处罚力度不大，导致网络运营者未对网络信息保护给予足够重视并采取充分的安全保护措施。

近年来，我国政府愈发重视网络安全监管，注重个人信息保护。因此，我国境内企业，不论是网络所有者、管理者还是广大的网络产品、服务提供者，都应当严格遵守《网络安全法》的要求，认真落实网络安全保护和用户个人信息保护。同时，《网络安全法》的完善还有待在实践中总结经验，进一步制定与之配套的法律、法规、管理办法和标准等，我们将持续关注相关规定的后续发展。

[9] 《网络安全法》第二十五条。

[10] 《网络安全法》第五章。

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。