

上海

上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京

北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港

香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦

1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

制标治本——简评《网络数据安全标准化体系建设指南》

作者: 潘永建 | 邓梓珊

我国电信和互联网行业在释放数字经济发展潜力、促进数字经济加快成长的高速发展过程中, 面临着严峻的安全形势。数据泄露事件频繁发生, 过度收集、滥用用户个人信息问题大量存在, 非法数据共享与交易带来的安全挑战愈加严峻。随着《网络安全法》的出台以及各领域各项执法行动的有序铺开, 网络安全、数据安全以及个人信息保护相关法律法规的管理要求亟待补充和细化。4 月 10 日, 工业和信息化部(“工信部”)公布其组织起草的《网络数据安全标准体系建设指南(征求意见稿)》(“《建设指南》”), 旨在指导电信和互联网行业的网络数据安全标准化工作。

一. 背景和主旨

正如《建设指南》前言所述, 随着信息技术和人类生产生活交汇融合, 全球数据呈现爆发增长、海量聚集的特点, 大数据产业正值活跃发展期, 技术演进和应用创新并行加速推进, 数据资源已成为国家基础战略性资源和社会生产的创新要素。由于法律存在滞后性, 目前的标准化制定与实施存在着体系性不强、部分问题和重点领域存在标准的空白等问题。为应对复杂严峻的现实安全风险, 加速构建网络数据安全保障体系, 工信部拟通过《建设指南》, 加快落实网络数据安全制度的标准化工作。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

《建设指南》指出，到 2021 年，将初步建立网络数据安全标准体系，有效落实网络数据安全要求，基本满足行业网络数据安全保护需要，推进标准在重点企业、重点领域中的应用，研制网络数据安全行业标准将达到 20 项以上。到 2023 年，健全完善网络数据安全标准体系，标准技术水平、应用水平和国际化水平显著提高，有力促进行业网络数据安全保护能力提升，研制网络数据安全行业标准将达到 50 项以上。随着标准体系的完善，企业的网络数据安全技术管理、制度管理也将有据可依，有制可循；同时，也意味着监管部门对企业网络数据安全情况的监督管理有了“硬性”要求。一言以蔽之，《建设指南》是政府监管部门制标以治本的措施之一。

二. 网络数据安全标准体系

为加强网络数据全生命周期各环节的安全保护，针对各应用领域和业务场景形成闭环安全管理模式，落实网络安全与信息保护的各項法律法规要求，《建设指南》所提出的网络数据安全标准体系建设，包括**基础共性、关键技术、安全管理、重点领域**四大类标准。

1. **基础共性类标准**包括术语定义、数据安全框架、数据分类分级等，为各类标准提供基础性支撑。
2. **关键技术标准**从数据采集、传输、存储、处理、交换、销毁等数据全生命周期维度对数据安全技术进行规范。子标准的制定将涵盖数据清洗比对、数据质量监控、数据匿名化/去标识化、多方安全计算、数据溯源等内容。
3. **安全管理标准**从网络数据安全框架的管理视角出发，指导行业有效落实相关法律法规对网络数据安全的要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等标准。
4. **重点领域标准**结合相关领域的实际情况和数据安全保护的具体要求，指导行业有效开展重要领域网络数据安全保护工作。重点领域包括 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等。未来将结合行业发展情况，逐步覆盖其他重要领域。

《建设指南》四大类标准划分，贴合企业的网络数据安全实际需求。企业在实际进行网络安全、数据安全制度建设时，也应从数据来源的归类甄别、分类分级做起，完善数据全生命周期管理，落实技术措施的同时，加强管理(包括人员管理、数据安全评估、安全事件应急方案等)制度建设，结合自身所在行业特点制定针对性的网络数据安全保护计划。

三. 重点领域与重点问题

随着社会的发展和技术的更迭，网络的外延不断扩展，出现了云计算、大数据、物联网、工业控制系统等形态。这些新形态行业近年来也不断被曝出各类数据安全事件，如移动 APP 服务器遭撞库攻击、非法获取用户隐私；车联网技术缺陷造成车辆失控；物联网系统遭入侵导致设备财产损失；大数据平台公司遭员工删库，大量电商企业数据丢失；AI 人脸识别技术引发生物识别信息安全隐患等。企业需要针对新一代信息通信技术的特点，在满足通用安全要求的基础上，为不同业务场景制定差异化的安全标准、采取针对性的技术及组织管理措施。《建设指南》针对 9 大重点领域的特点，拟定了针对性的标准化建设方向：

1. **5G 领域:** 5G 安全机制在满足通用安全要求基础上, 为不同业务场景提供差异化安全服务, 适应多种网络接入方式及新型网络架构, 保护用户个人隐私, 并支持提供开放的安全能力。5G 领域的网络数据安全标准主要包括 5G 数据安全总体要求、5G 终端数据安全、5G 网络侧数据安全、5G 网络能力开放数据安全等。
2. **移动互联网领域:** 传统的移动互联网安全主要包括终端安全、网络安全和应用安全等方面。随着开放生态体系下移动操作系统的普遍应用和数据的大规模流动, 移动互联网的数据安全风险进一步凸显。移动互联网领域的网络数据安全标准主要包括移动应用个人信息保护、移动应用软件 SDK 安全等。
3. **车联网领域:** 车联网安全覆盖车内、车与车、车与路、车与人、车与服务平台的全方位连接和数据交互过程, 数据安全和隐私保护贯穿于车联网的各个环节。车联网领域的网络数据安全标准主要包括车联网云平台数据安全、V2X 通信数据安全、智能网联汽车数据安全、车联网移动 App 数据安全等。
4. **物联网领域:** 物联网安全涵盖物联网的感知层、传输层、应用层, 涉及服务端安全、终端安全和通信网络安全等方面, 数据安全贯穿于其中的各个环节。物联网领域的网络数据安全标准主要包括物联网云端数据安全保护、物联网管理系统数据安全保护、物联网终端数据安全保护等。
5. **工业互联网领域:** 工业互联网安全重点关注控制系统、设备、网络、数据、平台、应用程序安全 and 安全管理等。工业互联网领域的网络数据安全标准主要包括工业互联网数据安全保护、工业互联网数据分级技术等。
6. **云计算领域:** 云计算安全以云主机安全为核心, 涵盖网络安全、数据安全、应用安全、安全管理、业务安全等方面。云计算领域的网络数据安全标准主要包括客户数据保护、云服务业务数据安全、云上资产管理等。
7. **大数据领域:** 大数据安全覆盖数据全生命周期管理各环节, 涵盖对大数据平台运行安全功能保障及以数据为对象进行资产管理等。大数据领域的网络数据安全标准主要包括大数据平台安全、大数据资产管理等。
8. **人工智能领域:** 人工智能安全覆盖个人信息安全、算法安全、数据安全、网络安全等。人工智能领域的网络数据安全标准主要包括人工智能平台数据安全、人工智能终端个人信息保护等。
9. **区块链领域:** 区块链安全包括应用服务的安全性、系统设计的安全性(包含智能合约、共识机制)、基础组件的安全性(包含网络通信、数据安全、密码技术)三个维度。区块链领域的网络数据安全标准主要包括区块链隐私数据保护、区块链数字资产存储与交互保护等。

(就上述重点领域与重点问题的详细分析, 读者可参考通力合规团队撰写的系列法评文章: [《跨国公司遵守 APP 个人信息保护规则的五大要点》](#) [《不解内忧何以防外患——Zoom 事件的数据合规管理启示》](#) [《简析车联网应用下个人隐私保护难点与对策》](#) [《简析物联网应用中的网安数据合规问题》](#) [《区块链新规及其对我国区块链不同应用场景的影响》](#) [《区块链: 概念、应用及中国法》](#))

值得注意的是, 网络安全等级保护制度也采取了类似的体系建设思路。2019 年 12 月 1 日正式实施的等保 2.0 国家标准, 《信息安全技术 网络安全等级保护基本要求》, 将云计算、移动互联网、物联网、工业控制系统、大数据等新兴技术和应用场景纳入了等级保护范围, 采用“扩展要求”的形式, 在统一标准的基础上针对不同场景增加针对性要求。有关等保 2.0 的具体内容和特点, 可参见通力合规团队法评 [《等保 2.0 要点概览及合规建议》](#)。

四. 国标的制定现状及其效力

《建设指南》的附件 2 梳理了近年来已发布和制定中的百余项网络数据安全相关标准。正如《建设指南》编制说明中坦言,目前我国网络数据安全标准化制定存在着体系性不强、部分关键标准亟需制定、部分重点领域相关标准仍存在空白等问题。纵观《建设指南》附件 2,笔者注意到就关键技术类标准而言,“数据销毁”相关标准尚未制定,亦未进入“拟制定”阶段。在安全管理类规范中,针对数据安全规范,15 部处于不同制定阶段的国家标准有 13 部专门针对个人信息的管理。虽然这足见监管部门对于治理个人信息合规问题的决心,但也反映出制定中的国标全面性不足。

网络安全法的体系由数部法律,数十部行政法规、部门规章、司法解释、规范性文件及数百部国家标准构成。法律法规构建了网络安全法的原则性规定,国家标准则提供了具体的可操作性措施。目前有关网络数据安全的国家标准虽然多为推荐性国家标准,但其“替代规制功能”也不容小觑。以个人信息保护工作的监管为例,2017 年 8、9 月份,中央网信办、工信部、公安部、国家标准委四部门联合宣布启动隐私条款评审专项工作,主要以当时《信息安全技术 个人信息安全规范》的征求意见稿为评审依据。按照《信息安全技术 个人信息安全规范》之规定,在个人信息保护的专项法律法规缺位的情况下,国家标准可以适用于“主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估”。因此,监管部门可以参考国家标准对企业进行监督管理。实践中,监管部门亦将国家标准转化为具体监管要求。例如,2018 年 5 月 21 日中国银保监会发布的《银行业金融机构数据治理指引》中第 24 条明确要求:“银行业金融机构采集、应用数据涉及到个人信息的,应遵循国际个人信息保护法律法规要求,符合与个人信息安全相关的国家标准”。鉴此,企业应当认识到目前日趋严格的网络安全、数据安全监管形势,积极关注标准化制定进程,充分遵从各项标准的指导,在网络数据安全实践方面做到全方面全环节合规。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

T: +86 21 3135 8666
F: +86 21 3135 8600

北京

T: +86 10 8519 2266
F: +86 10 8519 2929

香港

T: +852 2592 1978
F: +852 2868 0883

伦敦

T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 本篇文章独家授权威科先行法律信息库发布，未经许可，不得转载。