立律
方師
NEWSLETTER
LIFANG & PARTNERS 立方观评
关注更多精彩内容

No.133

2020.04

立方网络安全与数据合规周报
Weekly Cybersecurity and Data Protection Review

国内要闻 Domestic News

工信部发布《网络数据安全标准体系建设指南》（征求意见稿）

MIIT Publishes the Guidelines on the Construction of Standardized System of Network Data Security

中共中央、国务院《关于构建更加完善的要素市场化配置体制机制的意见》

China to Promote Market-Based Allocation of Production Factors

信安标委发布2020年第一批推荐性网络安全国家标准计划项目清单

NISSTC Issues List of the First Batch of Recommended National Standards for Cybersecurity in 2020

百度App部分频道因严重违规暂停更新，负责人被约谈

Baidu App Inquired into Serious Violations and Suspends Some of its Channels

海外动态 Overseas News

EDPB第二十次全体会议 – 关于制定抗疫数据处理指南

Twentieth Plenary Session of the EDPB - Scope of Upcoming Guidance on Data Processing in the Fight Against COVID-19

FTC与加拿大智能锁制造商就其在安全措施上欺骗消费者的指控达成和解协议

Canadian Maker of Smart Locks Settles FTC Allegations That It Deceived Consumers about its Security Practices

Zoom曝出重大安全漏洞

Zoom is Leaking Peoples’ Email Addresses and Photos to Strangers

国内要闻 Domestic News

工信部发布《网络数据安全标准体系建设指南》（征求意见稿）

2020年4月10日，工业和信息化部（“**工信部**”）发布《网络数据安全标准体系建设指南》（“**《建设指南》**”），向社会公开征求意见。该《建设指南》落实了《中华人民共和国网络安全法》等法律法规要求，旨在保障电信和互联网行业网络数据安全、促进网络数据合理有序流动。《建设指南》构建了网络数据安全标准体系框架，分为基础共性标准、关键技术标准、安全管理标准、重点领域标准四部分。其中，基础共性标准是网络数据安全保护的基础性、通用性、指导性标准，包括术语定义、数据分类分级等；关键技术标准是数据采集、传输、存储、处理、交换、销毁等环节中网络数据安全关键技术的标准；安全管理标准主要是指导行业落实法律法规以及政府主管部门的管理要求，包括数据安全评估标准等；重点领域标准是指在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、区块链等重点领域的网络数据安全标准。（查看更多）

MIIT Publishes the *Guidelines on the Construction of Standardized System of Network Data Security*

On April 10, 2020, the Ministry of Industry and Information Technology of China (“**MIIT**”) published the *Guidelines on the Construction of Standardized System of Network Data Security* (“***Guidelines***”), to solicit opinions from the public. The *Guidelines* implements the *Cybersecurity Law* and other laws and regulations, aiming at protecting network data security in the telecommunications and Internet industries and promoting the rational and orderly flow of network data. The *Guidelines* constructs the standardized system of network data security, including basic generic standards, critical technology standards, security management standards, and major area standards. Specifically, basic generic standards are the basic, universal and guiding standards in the protection of network data security, including the definitions of terms and the standard for data grading and classification; critical technology standards are security standards related to the processes of data acquisition, transmission, storage, processing, exchange, destruction, etc.; security management standards are mainly to guide the industry to implement laws and regulations as well as the management requirements of the competent authorities, including data security assessment standards, etc.; major area standards refer to the network data security standards in 5G, mobile Internet, Internet of vehicles, Internet of things, industrial Internet, cloud computing, big data, artificial intelligence, blockchain, and other key areas. (More)

中共中央、国务院《关于构建更加完善的要素市场化配置体制机制的意见》

2020年4月9日，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》（“《意见》”）。该《意见》指出要加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护。《意见》强调，应支持构建农业、工业、交通、教育、安防、城市管理、公共资源交易等领域规范化数据开发利用的场景，发挥行业协会商会作用，推动人工智能、可穿戴设备、车联网、物联网等领域数据采集标准化。在数据管理与保护方面，探索建立统一规范的数据管理制度。制定数据隐私保护制度和安全审查制

度。推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。（查看更多）

China to Promote Market-Based Allocation of Production Factors

On April 9, 2020, the Communist Party of China and the State Council issued the *Opinions on Improving the Market-Based Allocation Mechanism of Production Factors* ("***Opinions***"). The *Opinions* indicates that it is necessary to accelerate the establishment of data factors market, advance the open sharing of government data, promote the value of society data, and strengthen the integration and security protection of data resource. The *Opinions* also emphasizes the necessity of supporting the construction of standardized data development and utilization scenarios in the fields of agriculture, industry, transportation, education, security, urban management, public resource trading, etc., attaching great importance to the role of industrial associations and chambers of commerce, and promoting the standardization of data collection in the fields of artificial intelligence, wearable equipment, Internet of vehicles, Internet of things, etc. In terms of data management and protection, China will establish a unified data management system, develop data privacy protection and security review systems, promote the formulation of security protection system via data grading and classification in the context of big data, and strengthen the protection of government data, business secrets and personal information. (More)

信安标委发布2020年第一批推荐性网络安全国家标准计划项目清单

近日，国家标准化管理委员会下达了2020年第一批推荐性国家标准计划。2020年4月7日，全国信息安全标准化技术委员会（“信安标委”）下达了由其归口的标准项目共计16项，详见下表。（查看更多）

表一：2020年第一批推荐性网络安全国家标准计划项目清单

编号	计划号	项目名称
1	20201686- T-469	信息安全技术 网络脆弱性扫描产品安全技术要求
2	20201687- T-469	信息安全技术 政府门户网站系统安全技术指南
3	20201688- T-469	信息技术 安全技术网络安全 第3部分：参考网络场景——风险、设计技术和控制要素
4	20201689- T-469	信息技术 安全技术网络安全 第4部分：使用安全网关的网间通信安全保护
5	20201690- T-469	信息安全技术 信息安全风险管理指南
6	20201691- T-469	信息安全技术 信息安全服务 分类
7	20201692- T-469	信息安全技术 云计算服务安全能力要求
8	20201693- T-469	信息安全技术 云计算服务安全指南
9	20201694- T-469	信息技术 安全技术 个人可识别信息（PII）处理者在公有云中保护PII的实践指南
10	20201695- T-469	信息安全技术 可信计算密码支撑平台功能与接口规范
11	20201696- T-469	信息安全技术 分组密码算法的工作模式
12	20201697- T-469	信息技术 安全技术抗抵赖第 2 部分：采用对称技术的机制
13	20201698- T-469	信息安全技术 公钥基础设施标准一致性测试评价指南
14	20201699- T-469	信息安全技术 网站数据恢复产品技术要求与测试评价方法
15	20201700- T-469	信息安全技术 网络入侵检测系统技术要求和测试评价方法
16	20201701- T-469	信息安全技术 数据备份与恢复产品技术要求与测试评价方法

NISSTC Issues List of the First Batch of Recommended National Standards for Cybersecurity in 2020

Recently, the Standardization Administration issued the first batch of recommended national standards plans for 2020. On April 7, 2020, the National Information Security Standardization Technical Committee (“**NISSTC**”) then issued a total of 16 cybersecurity standard items, as shown in the following table. (More)

Table 1: List of the First Batch of Recommended National Standards for Cybersecurity in 2020

No.	Plan No.	Name of Standard
1	20201686- T-469	Information security technology—Security technical requirements for network vulnerability scanners
2	20201687- T-469	Information security technology—Security technology guidelines for web portal system of government
3	20201688- T-469	Information technology—Security techniques—IT network security—Part 3: Reference network scenario—Risk, design techniques, and control factors
4	20201689- T-469	Information technology—Security techniques—IT network security—Part 4: Securing communications between networks using security gateways
5	20201690- T-469	Information security technology—Guidelines for information security risk management
6	20201691- T-469	Information security technology—Information security service—Category
7	20201692- T-469	Information security technology—Security capability requirements of cloud computing services
8	20201693- T-469	Information security technology—Security guide of cloud computing services
9	20201694- T-469	Information technology—Security techniques—Practice guide for PII (Personal Identifiable Information) processors to protect PII in the public cloud
10	20201695- T-469	Information security techniques—Functionality and interface specification of cryptographic support platform for trusted computing
11	20201696- T-469	Information technology—Security Techniques—Modes of operation for a block cipher
12	20201697- T-469	Information technology—Security techniques—Non-repudiation—Part 2: Mechanisms using symmetric techniques
13	20201698- T-469	Information security technology—Public Key Infrastructure—Testing and evaluation guide on standard conformance
14	20201699- T-469	Information security technology—Technical requirements and testing and evaluating approaches of website data recovery products
15	20201700- T-469	Information security technology—Technical requirements and testing and evaluation approaches for network-based intrusion detection system
16	20201701- T-469	Information security technology—Technical requirements and testing and evaluating method for data backup and recovery products

百度App部分频道因严重违规暂停更新，负责人被约谈

2020年4月7日，国家互联网信息办公室指导北京市互联网信息办公室，针对百度App多个频道存在严重违规问题，严肃约谈百度公司负责人，要求立即停止违规行为。北京市互联网信息办公室有关负责人指出，百度App违反国家有关互联网法律法规和管理要求，落实主体责任不力，大量传播低俗庸俗信息、密集发布“标题党”文章、公众账号注册管理及内容审核不严，传播秩序和生态问题突出，社会影响恶劣。百度App相关频道自4月8日上午9时起暂停更新，清理违规内容，开展深入整改。（查看更多）

Baidu App Inquired into Serious Violations and Suspends Some of its Channels

On April 7, 2020, the Cybersecurity Administration of China ("**CAC**") instructed Beijing CAC to inquire Baidu's relevant person-in-charge about the serious violations of several channels of Baidu App and demand it to cease the violations. The relevant person in charge of Beijing CAC indicated that Baidu App was in violations of relevant Internet laws, regulations and management requirements, failing to fulfill its main responsibilities and strictly review the registration and contents of public accounts, spreading vulgar information and intensively publishing "clickbait" articles, which led to chaotic communication order, ecological problems and caused bad social impact. Baidu App's relevant channels were required to be suspended from 9:00 a.m. on April 8 to clean up the illegal contents and carry out in-depth rectification. (More)

海外动态 Overseas News

EDPB第二十次全体会议 – 关于制定抗疫数据处理指南

2020年4月7日，欧盟数据保护委员会（European Data Protection Board，"EDPB"）发布新闻称，在当日举行的第20次全体会议上，其已向专家小组分配了具体工作任务，要求制定抗疫数据处理方面的指南。指南的两个议题为：（1）疫情背景下地理定位和其他追踪工具－已授权技术专家小组负责该项工作；（2）疫情背景下以科研为目的的健康数据处理－已授权合规、电子政务和健康专家小组负责该项工作。考虑到这两个议题的高度优先性，EDPB决定暂时推迟在疫情期间开展远程办公工具使用及实操的指导工作。（查看更多）

Twentieth Plenary Session of the EDPB - Scope of Upcoming Guidance on Data Processing in the Fight Against COVID-19

On April 7, 2020, the European Data Protection Board ("**EDPB**") announced that during its 20th plenary session, it assigned concrete mandates to its expert subgroups to develop guidance on several aspects of data processing in the fight against COVID-19. The two topics were as follows:

1. geolocation and other tracing tools in the context of the COVID-19 outbreak – a mandate was given to the technology expert subgroup for leading this work;

2. processing of health data for research purposes in the context of the COVID-19 outbreak – a mandate was given to the compliance, e-government and health expert subgroup for leading this work.

Considering the high priority of these 2 topics, the EDPB decided to postpone the guidance work on teleworking tools and practices in the context of the COVID-19 outbreak, for the time being. (More)

FTC与加拿大智能锁制造商就其在安全措施上欺骗消费者的指控达成和解协议

2020年4月6日，美国联邦贸易委员会（Federal Trade Commission，"**FTC**"）发布新闻称，其已就Tapplock公司谎称其联网智能锁"牢不可破"，并且采取了合理措施保护收集的用户数据的指控，与该公司达成和解协议。FTC指出该公司的锁是不安全的，其未能采取合理的预防措施或遵循行业最佳做法来保护收集的消费者数据，此外，该公司未能设置安全程序或采取其他可能有助于该公司发现锁的电子漏洞的防护措施。根据该和解协议，FTC要求Tapplock制定并实施全方

位的安全程序，每两年进行一次评估，禁止Tapplock歪曲其采取的隐私和安全措施，并且对信息安全程序每两年进行一次第三方评估，FTC有权任命评估人员。（查看更多）

Canadian Maker of Smart Locks Settles FTC Allegations That It Deceived Consumers about its Security Practices

On April 6, 2020, the Federal Trade Commission (“**FTC**”) announced that a Canadian company Tapplock, Inc. (“**Tapplock**”) had settled FTC allegations that it deceived consumers by falsely claiming that its Internet-connected smart locks were designed to be “unbreakable” and that it took reasonable steps to secure the data it collected from users. The FTC alleged that the company’s locks were not secure and that Tapplock failed to take reasonable precautions or follow industry best practices to protect the consumer data it collected. The FTC also alleged that Tapplock failed to implement a security program or take other steps that might have helped the company discover electronic vulnerabilities with its locks. The settlement required Tapplock to implement a comprehensive security program and obtain independent biennial assessments of the program. In addition to the security program provision, the proposed settlement prohibited Tapplock from misrepresenting its privacy and security practices. Tapplock also was required to obtain third-party assessments of its information security program every two years. In addition, the FTC had authority to approve the assessor for each two-year assessment period. (More)

Zoom曝出重大安全漏洞

2020年4月1日，据Vice报道，视频会议软件Zoom大量用户的个人信息遭泄露，包括电子邮件、照片，并且陌生人能够尝试通过Zoom与用户进行视频通话。该事件的发生与Zoom“公司目录”设置有关，其自动将使用同一域名电子邮件进行注册的用户互相设置为联系人。当域名是单个公司时，可以轻松地找到要视频呼叫的同事。但大量用户表示当他们使用个人邮箱注册时，Zoom将他们与成千上万的其他用户放在一起，好像大家都在同一家公司上班，这无疑暴露了个人信息。上周，Zoom更新了iOS系统的App，3月30日，一名用户对Zoom数据泄露问题提起了集体诉讼。（查看更多）

Zoom is Leaking Peoples’ Email Addresses and Photos to Strangers

On April 1, 2020, the *Vice* reported that popular video-conferencing Zoom was leaking personal information of at least thousands of users, including their email address and photo, and giving strangers the ability to attempt to start a video call with them through Zoom. The issue lied in Zoom’s “Company Directory” setting, which automatically added other people to a user’s lists of contacts if they signed up with an email address that shared the same domain. This can make it easier to find a specific colleague to call when the domain belongs to an individual company. But multiple Zoom users said they signed up with personal email addresses, and Zoom pooled them together with thousands of other people as if they all worked for the same company, exposing their personal information to one another. Last week, Zoom updated the iOS version of its app. On March 30, a user filed a class action lawsuit against Zoom for the data transfer. (More)

立方律师事务所编写《立方观评》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。

This Newsletter has been prepared for clients and professional associates of Lifang & Partners. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

Subscribe to our WeChat community

扫码关注公众号“立方律师事务所”和“竞争法视界”

北京 ｜ 上海 ｜ 武汉 ｜ 广州 ｜ 深圳 ｜ 韩国

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com

Email：info@lifanglaw.com

Tel：+8610 64096099

Fax：+8610 64096260/64096261