



# NEWSLETTER

LIFANG & PARTNERS **立方观评**



关注更多精彩内容

## No.168

2020.08

### 立方网络安全与数据合规周报

## Weekly Cybersecurity and Data Protection Review

### No.22

#### 国内要闻 Domestic News

工信部发布《工业互联网标识管理办法（征求意见稿）》

MIIT Seeks Comments on the Draft Measures on the Management of Industrial Internet Identification

工信部发布《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》

MIIT Seeks Comments on the Draft Guidelines on Building Data Security Standards System in Telecommunication and Internet Industries

国家互联网应急中心发布《2019年中国互联网络网络安全报告》

CNCERT Publishes 2019 Report on China Internet Security

信安标委就两项关键信息基础设施国家标准征求意见

TC260 Invites Comments on Two Draft National Standards for Critical Information Infrastructure

《国家新一代人工智能标准体系建设指南》发布

Guidelines on Construction of Standardized Systems of National New Generation Artificial Intelligence Released

交通运输部将加强基础设施网络安全保护

MTC to Strengthen Infrastructure Cybersecurity Protection

交行、招行各被罚100万：对客户信息未尽安全保护义务

COMM and CMB Fined CNY 1m Respectively for Failure to Fulfill Obligations of Protecting Customers' Personal Information

工信部发布《关于开展纵深推进APP侵害用户权益专项整治行动的通知》

MIIT Launches Special Rectification Actions towards Infringement of Rights and Interests of Users by Apps

#### 海外动态 Overseas News

德国成立联邦网络安全机构以加强数字主权

Germany Launches Cybersecurity Agency to Strengthen Digital Sovereignty

欧洲数据保护专员公署：量子计算可能危害数据安全保护和通信机密

EDPS: Quantum Computing Could Undermine Data Security Protection and Confidentiality of Communications

因阻止数据主体访问其个人数据，荷兰信用登记局被罚83万欧元

Netherlands National Credit Register Fined EUR 0.83m for Personal Data Access Charges

Twitter涉嫌不当使用个人信息投放广告，或面临FTC 2.5亿美元罚款

Twitter Under FTC Investigation for Alleged Misuse of User Data with Potential Fine of USD 250m

## 国内要闻 Domestic News

### 工信部发布《工业互联网标识管理办法（征求意见稿）》

2020年8月14日，工业和信息化部（“工信部”）发布《工业互联网标识管理办法（征求意见稿）》（“《管理办法》”）并向社会公众公开征求意见。《管理办法》规定了工业互联网标识、标识服务和提供标识服务机构等概念，工信部和省级通信管理局对标识服务的监管职责，标识服务机构应当履行的义务（取得相应许可、确保系统对接、网络资源与用户信息合规等）及承担的法律責任等。征求意见截止日期为2020年9月13日。（[查看更多](#)）

### MIIT Seeks Comments on the Draft Measures on the Management of Industrial Internet Identification

On August 14, 2020, the Ministry of Industry and Information Technology of China (“MIIT”) published the *Measures on the Management of Industrial Internet Identification (Exposure Draft)* (“Measures”) for public comments. The Measures specifies the concepts of industrial Internet identification, identification services and identification services organizations, etc. The Measures also specifies the supervision responsibilities of the MIIT and provincial communications administrations on identification services, and the obligations (such as obtaining relevant licenses, maintaining system integration, compliance of network resources and users’ information) and legal liabilities of identification service organizations, etc. The deadline for submitting comments is September 13, 2020. ([More](#))

### 工信部发布《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》

2020年8月11日，工信部发布《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》（“《建设指南》”）并向社会公众公开征求意见。《建设指南》提出了电信和互联网行业数据安全标准体系框架、数据安全重点标准化领域及方向。《建设指南》还对术语定义和已发布、制定中、拟制定的数据安全相关标准进行了梳理，形成《数据安全相关标准项目明细表》。征求意见截止日期为2020年9月10日。（[查看更多](#)）

### MIIT Seeks Comments on the Draft Guidelines on Building Data Security Standards System in Telecommunication and Internet Industries

On August 11, 2020, the MIIT published the *Guidelines on Building Data Security Standards System in Telecommunications and Internet Industries (Exposure Draft)* (“Guidelines”) for public comments. The Guidelines specify the framework of data security standards system and the key standardization fields of data security in the telecommunication and Internet industries. The Guidelines also sorts out the definitions of certain terms as well as the data security-related standards that are released, under formulation and to be formulated, and compiles the latter into the *List of Data Security-related Standard Projects*. The deadline for submitting comments is September 10, 2020. ([More](#))

## 国家互联网应急中心发布《2019年中国互联网网络安全报告》

2020年8月11日，国家互联网应急中心发布其编写的《2019年中国互联网网络安全报告》（“《报告》”）。《报告》重点内容包括2019年网络安全状况综述、网络安全专题分析、网络安全事件案例详解以及网络安全关注方向与对策等，并对2020年网络安全热点问题进行预测。《报告》对计算机、移动互联网恶意程序传播和活动，网站安全监测，DDoS攻击监测，安全漏洞预警与处置，网络安全事件接收与处理等专业问题进行了深入分析。《报告》旨在为政府部门提供监管支撑，同时为互联网企业提供运行管理技术支持。（[查看更多](#)）

## CNCERT Publishes 2019 Report on China Internet Security

On August 11, 2020, The National Computer Network Emergency Response Technical Team of China (“CNCERT”) published the *2019 Report on China Internet Security* (“**Report**”). The Report mainly includes the overview of cybersecurity situations in 2019, thematic analysis of cybersecurity, detailed illustrations of cybersecurity cases, key focus of and potential counter measures for cybersecurity issues and projects the hotspot issues of cybersecurity in 2020. The Report undertakes in-depth analysis on issues such as the spread of malicious computers and mobile Internet programs and relevant conducts, website security monitoring, DDoS attack monitoring, security vulnerability warning and handling, and network security incidents’ reception and dispose. The Report aims to provide regulatory support for government departments and to provided technical support on operation and management for Internet companies. ([More](#))

## 信安标委就两项关键信息基础设施国家标准征求意见

2020年8月10日，全国信息安全标准化技术委员会（“信安标委”）发布两项关键信息基础设施国家标准的征求意见稿并向社会公众公开征求意见，具体包括：（1）《信息安全技术 关键信息基础设施安全防护能力评价方法》。该标准主要规定了关键信息基础设施安全防护能力评价模型与能力评价方法，适用于关键信息基础设施运营者对自身安全能力进行评价并完善自身安全管理建设；（2）《信息安全技术 关键信息基础设施边界确定方法》。该标准主要规定了关键信息基础设施边界识别基本原则以及关键信息基础设施边界的识别模型、方法和流程，适用于关键信息基础设施运营者开展关键信息基础设施边界识别工作。征求意见截止日期为2020年10月9日。（[查看更多](#)）

## TC260 Invites Comments on Two Draft National Standards for Critical Information Infrastructure

On August 10, 2020, the National Information Security Standardization Technical Committee, also known as the TC260, released the following two draft national standards for critical information infrastructure: (i) *Information security technology - The evaluation method for security protection capability of critical information infrastructure (Exposure Draft)*. This standard mainly specifies the safety protection capability evaluation model and method of critical information infrastructure, applicable to evaluating the safety capability and promoting the safety management construction of the critical information infrastructure operators; (ii) *Information security technology - Method of boundary identification for critical information infrastructure (Exposure Draft)*. This standard mainly specifies the basic principles, models, methods, and processes for the identification of critical information infrastructure’s boundary,

which applies to the identification of critical information infrastructure's boundary by critical information infrastructure operators. The deadline for submitting comments is October 9, 2020. ([More](#))

### 《国家新一代人工智能标准体系建设指南》发布

2020年8月7日，国家标准化管理委员会、中共中央网络安全和信息化委员会办公室等5部门联合发布《国家新一代人工智能标准体系建设指南》（“《指南》”）。根据《指南》，人工智能标准体系结构包括“A基础共性”、“B支撑技术与产品”、“C基础软硬件平台”、“D关键通用技术”、“E关键领域技术”、“F产品与服务”、“G行业应用”、“H安全/伦理”等八个部分。其中，人工智能领域的安全与隐私保护标准涵盖基础安全，数据、算法和模型安全，技术和系统安全，安全管理和服务，安全测试评估，产品和应用安全等六方面。 ([查看更多](#))

### Guidelines on Construction of Standardized Systems of National New Generation Artificial Intelligence Released

On August 7, 2020, the Standardization Administration of China and the Cyberspace Administration of China together with three other departments jointly issued the *Guidelines on the Construction of Standardized Systems of National New Generation Artificial Intelligence* (“AI”) (“**Guidelines**”). According to the Guidelines, the structure of AI standardized systems consists of eight parts, including: (i) basic generality; (ii) supporting technology and product; (iii) fundamental software and hardware platform; (iv) critical general technology; (v) critical area technology; (vi) product and service; (vii) industrial application; and (viii) security/ethics. Among those standards, AI security and privacy protection standards cover six aspects, including: (i) basic security; (ii) data, algorithm and model security; (iii) technology and system security; (iv) security management and service; (v) security testing evaluation; and (vi) product and application security. ([More](#))

### 交通运输部将加强基础设施网络安全保护

2020年8月6日，交通运输部发布《关于推动交通运输领域新型基础设施建设的指导意见》（“《指导意见》”），以推动交通基础设施数字转型、智能升级。《指导意见》指出，在网络安全保护方面，加快新技术交通运输场景应用的安全设施配置部署，强化统一认证和数据传输保护，加强关键信息基础设施保护。切实推进商用密码等技术应用，积极推广可信计算，提高系统主动免疫能力。加强数据全生命周期管理和分级分类保护，落实数据容灾备份措施。 ([查看更多](#))

### MTC to Strengthen Infrastructure Cybersecurity Protection

On August 6, 2020, the Ministry of Transport of China (“MTC”) issued the *Guiding Opinions on Promoting the Construction of New Infrastructure in the Transportation Field* (“**Guiding Opinions**”) to promote the digital transformation and intelligent upgrading of transportation infrastructure. The Guiding Opinions points out that, in terms of cybersecurity protection, it is necessary to (i) accelerate the deployment of security facilities for the application of new technology in the transportation scenario, strengthen the unified certification and data transmission protection, and strengthen the protection of essential information infrastructure; (ii) effectively promote the application of commercial cryptography and other technologies, actively promote trusted computing, and improve the active immunity of the



system; and (iii) reinforce data whole-life cycle management and data protection by different classification and grading, and implement data recovery and backup measures in case of any disaster. ([More](#))

### 交行、招行各被罚100万：对客户信息未尽安全保护义务

2020年8月5日，中国银行保险监督管理委员会上海监管局（“上海银保监局”）公布了其于7月28日分别对交通银行股份有限公司太平洋信用卡中心（“交行”）、招商银行股份有限公司信用卡中心（“招行”）的行政处罚信息公开表。上海银保监局认定，交行、招行对客户个人信息未尽安全保护义务，根据《中华人民共和国银行业监督管理法》第四十六条第（五）项，决定对交行、招行各罚款人民币100万元。（[查看更多](#)）

### COMM and CMB Fined CNY 1m Respectively for Failure to Fulfill Obligations of Protecting Customers' Personal Information

On August 5, 2020, the Shanghai Bureau of the China Banking and Insurance Regulatory Commission published two administrative punishment information disclosure forms in which it fined the Pacific Credit Card Centre of Bank of Communications Co., Ltd. (“COMM”) and the Credit Card Centre of China Merchants Bank Co., Ltd. (“CMB”) CNY 1m respectively for failure to fulfill their obligations of protecting the personal information of customers in accordance with Article 46 (5) of the *Law of the People's Republic of China on Banking Regulation and Supervision*. ([More](#))

### 工信部发布《关于开展纵深推进APP侵害用户权益专项整治行动的通知》

2020年8月2日，工业和信息化部（“工信部”）发布《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（“《通知》”）。根据《通知》，整治对象包括APP服务提供者、软件工具开发包（SDK）提供者和应用分发平台。整治行动涵盖APP、SDK违规收集、超范围收集、违规使用用户个人信息及强制用户使用定向推送功能，APP强制、频繁、过度索取权限和频繁自启动和关联启动，欺骗误导用户下载APP或者提供个人信息，应用分发平台商未明示APP收集、使用用户个人信息的内容、目的、方式和范围等多种行为。（[查看更多](#)）

### MIIT Launches Special Rectification Actions Towards Infringement of Rights and Interests of Users by Apps

On August 2, 2020, China's Ministry of Industry and Information Technology (“MIIT”) issued the *Notice on Launching the Deep Promotion of Special Rectification Action Against Infringement of Rights and Interests of Users by Apps* (“Notice”). According to the Notice, the targets of this action include Apps service providers, software development kit (“SDK”) providers and application distribution platforms. This rectification action targets at: (i) illegal collection, overrange collection and illegal use of users' personal information, and coercion to use the targeted push function by Apps and SDKs; (ii) compulsory, frequent and excessive request for permissions, and frequent self-starting and associated start-ups by Apps; (iii) deceit and misguidance that lead users to download Apps or provide personal information; and (iv) application distribution platforms' failure for notifying the content, purpose, method and scope of collection and use of personal information of users by Apps. ([More](#))

## 海外动态 Overseas News

### 德国成立联邦网络安全机构以加强数字主权

2020年8月11日，据德国之声报道，德国政府已决定成立一个旨在加强德国“数字主权”的联邦机构，以协调在网络安全方面的创新研究，并协助将其研究转化为打击网络威胁的可行方法。该机构将在2023年之前获得3.5亿欧元的初始资金，其总部将先设立在德国东部城市哈雷，之后将迁往莱比锡/哈雷机场。该机构的成立被视为德国信息技术系统保护的里程碑。（[查看更多](#)）

### Germany Launches Cybersecurity Agency to Strengthen Digital Sovereignty

On August 11, 2020, Deutsche Welle reported that the German government had signed up to create a federal agency to coordinate innovative research on cybersecurity and help turn it into practicable approaches to combat cyberthreats, aiming to strengthen Germany's "digital sovereignty". The agency, which will receive initial funding of EUR 350m up to 2023, is to be headquartered at first in the eastern city of Halle, before moving in the long term to the Leipzig/Halle airport. The creation of the agency is deemed to be a milestone in the protection of Germany's IT systems. ([More](#))

### 欧洲数据保护专员公署：量子计算可能危害数据安全保护和通信机密

2020年8月7日，欧洲数据保护专员公署发布一则科技电讯报告称，量子计算可能会危害数据安全保护和通信机密。原因是量子计算能够破解诸多的经典密码学，这将严重损害信息技术安全。该风险甚至会扩展到核心互联网安全协定，因此几乎当今所有要求安全、隐私或信任的系统都会受到影响。（[查看更多](#)）

### EDPS: Quantum Computing Could Undermine Data Security Protection and Confidentiality of Communications

On August 7, 2020, the European Data Protection Supervisor ("EDPS") published a TechDispatch report which opined that quantum computing could undermine data protection in terms of data security and confidentiality of communications. One reason is that quantum computing can break many of today's classical cryptography and as such harm severely IT security. The risk extends to the core internet security protocols. Nearly all of today's systems that demand security, privacy or trust, would be affected. ([More](#))

### 因阻止数据主体访问其个人数据，荷兰信用登记局被罚83万欧元

2020年8月6日，荷兰数据保护局对荷兰信用登记局（“BKR”）处以83万欧元罚款，原因是BKR阻止数据主体访问其个人数据。荷兰数据保护局查明，自2018年5月始，BKR对请求获取电子版个人数据的数据主体收取费用，并且数据主体每年只能免费一次获得其个人数据的纸质版本，这构成对隐私立法的侵犯。BKR已对该案提起上诉。（[查看更多](#)）

## Netherlands National Credit Register Fined EUR 0.83m for Personal Data Access Charges

On August 6, 2020, the Dutch Data Protection Authority (“**Dutch DPA**”) imposed a fine of EUR 0.83m on the Netherlands National Credit Register (“**BKR**”) for setting excessive obstacles for people wishing to access their data. Dutch DPA found that, in May 2018, the BKR began charging a fee to data subjects for requesting access to their data in a digital format, and data subjects could obtain a paper copy of their data for free only once a year, which was an infringement of privacy legislation. The BKR has appealed the case in court. ([More](#))

## Twitter涉嫌不当使用个人信息投放广告，或面临FTC 2.5亿美元罚款

2020年8月3日，Twitter在当日向美国证监会提交的文件中披露，其正受到美国联邦贸易委员会（Federal Trade Commission, “**FTC**”)的调查，原因是Twitter涉嫌不当使用用户个人信息以投放广告，并可能面临1.5亿至2.5亿美元的罚款。FTC发现，Twitter将出于安全目的收集的用户个人信息数据库链接至广告合作伙伴系统的行为可能违反了Twitter于2011年与FTC在消费者隐私方面签署的协议，该协议禁止Twitter在其消费者安全及其隐私保护措施方面误导消费者。（[查看更多](#)）

## Twitter Under FTC Investigation for Alleged Misuse of User Data with Potential Fine of USD 250m

On August 3, 2020, Twitter disclosed in its cooperate filing submitted on that day to United States Security and Exchange Commission that it was under investigation by the Federal Trade Commission (“**FTC**”) for potentially misusing personal information of users to serve ads and could face fines of USD 150m to 250m. The FTC found that Twitter linked a database of users’ personal information for security purposes with a system used by advertising partners, which may have violated a 2011 agreement that Twitter signed with the FTC over consumer privacy. Under the agreement, Twitter was restricted from misleading people about the measures it took to protect their security and privacy. ([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”

北京 | 上海 | 武汉 | 广州 | 深圳 | 韩国  
Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

 [www.lifanglaw.com](http://www.lifanglaw.com)  
 Email: [info@lifanglaw.com](mailto:info@lifanglaw.com)

 Tel: +8610 64096099  
 Fax: +8610 64096260/64096261