



# NEWSLETTER

LIFANG & PARTNERS **立方观评**



关注更多精彩内容

No. **137**

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

国家网信办、国家发改委等12部门联合发布《网络安全审查办法》

12 Departments Jointly Release the *Cybersecurity Review Measures*

国家互联网应急中心发布《2019年我国互联网网络安全态势综述》

CNCERT Publishes the *Overview of China's Internet Cybersecurity State in 2019*

国家发改委首次明确“新基建”范围

NDRC First Defines the Scope of the New Infrastructure

一季度全国网信行政执法工作有序推进

CAC Releases the Results of Administrative Enforcement on Cyberspace in the First Quarter

#### 海外动态 Overseas News

EDPB第二十三次全体会议 – 进一步起草抗疫指南

Twenty-third Plenary Session: EDPB Adopts Further COVID-19 Guidance

加拿大隐私专员办公室发布疫情期间有效隐私措施评估框架

OPC Publishes Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19

## 国内要闻 Domestic News

### 国家网信办、国家发改委等12部门联合发布《网络安全审查办法》

2020年4月27日，国家互联网信息办公室（“国家网信办”）、国家发展改革委（“国家发改委”）、工业和信息化部、公安部等12个部门联合发布了《网络安全审查办法》（“《办法》”），将于2020年6月1日起正式实施，同时2017年6月1日起施行的《网络产品和服务安全审查办法（试行）》废止。《办法》以《国家安全法》、《网络安全法》为基础，规定了针对关键信息基础设施运营者采购网络产品和服务的安全审查机制。关键信息基础设施运营者在采购网络产品和服务前需要预判产品和服务投入使用后可能带来的国家安全风险，如果影响或可能影响国家安全，应当进行事前主动申报网络安全审查。《办法》具体明确了申报主体和责任主体、主管部门、以及申报材料、审查内容及流程，并且明确了违反该《办法》的后果及责任。（[查看更多](#)）

### 12 Departments Jointly Release the Cybersecurity Review Measures

On April 27, 2020, 12 departments, including the Cyberspace Administration of China (“CAC”), the National Development and Reform Commission (“NDRC”), the Ministry of Public Security, jointly released the *Cybersecurity Review Measures* (“*Measures*”), which will come into force on 1 June 2020. The *Measures on Security Examination for Online Products and Services (Trial Implementation)* effective on 1 June 2017 shall be repealed simultaneously. Based on the *State Security Law* and the *Cybersecurity Law*, the *Measures* stipulates the security review mechanism for the critical information infrastructure operator (“CIIO”) to purchase network products and services. Before purchasing, the CIIO shall predict the possibility of national security risks when products and services are put into use. If they affect or are likely to affect national security, the CIIO shall apply for the cybersecurity review in advance. The *Measures* specifies the subject of notification, the competent departments, the notification materials required, the content and process of security review, as well as the consequences and responsibilities of violations. ([More](#))

### 国家互联网应急中心发布《2019年我国互联网网络安全态势综述》

2020年4月20日，国家互联网应急中心发布《2019年我国互联网网络安全态势综述》报告（“《2019年网安综述》”）。《2019年网安综述》涉及2019年典型网络安全事件、网络安全新趋势及日常网络安全事件应急处置实践等内容，主要分为四个部分：（1）总结2019年我国互联网网络安全状况。重点包括APT攻击、安全漏洞、数据安全、移动互联网安全、互联网黑灰产等七个方面；（2）预测2020年网络安全热点。认为国家关键信息基础设施安全、重要数据和个人信息保护、国家级网络对抗、精准网络勒索、远程协同安全风险、5G等新技术安全将成为2020年网络安全领域值得关注的热点；（3）结合网络安全态势分析提出对策建议。《2019年网安综述》从强化关键信息基础设施保护、加快网络安全核心技术创新突破、提升数据安全管理和个人信息保护力度、扩大国内外网络安全合作等五个方面，对进一步做好我国网络安全工作提出建议；（4）梳理网络安全监测数据。（[查看更多](#)）

## CNCERT Publishes the *Overview of China's Internet Cybersecurity State in 2019*

On April 20, 2020, the National Computer Network Emergency Response Technical Team (“CNCERT”) published *the Overview of China's Internet Cybersecurity State in 2019* (“Overview”). The *Overview* includes the aspects of typical cybersecurity incidents in 2019, new trends of cybersecurity and practices of handling daily cybersecurity emergencies, etc., which includes four parts: (i) the summarization of China's Internet cybersecurity state in 2019, which involves seven aspects, that is, APT attack, security vulnerability, data security, mobile Internet security, Internet black & grey production chains, etc.; (ii) the prediction of cybersecurity hotspots in 2020, which is believed that great attention will be caught on the national critical information infrastructure security, critical data, personal information protection, national cyber-confrontation, accurate cyber-blackmail, remote collaborative security risks and new technologies like 5G in 2020; (iii) some suggestions put forward by analyzing the state of cybersecurity. The *Overview* puts forward suggestions for further improving China's cybersecurity work from five aspects: strengthening the protection of critical information infrastructure, accelerating the innovation and breakthrough of core technologies, improving data security management and personal information protection, and expanding domestic and foreign cybersecurity cooperation, etc.; (iv) sorting out cybersecurity monitoring data. ([More](#))

## 国家发改委首次明确“新基建”范围

2020年4月20日，国家发改委举行4月份新闻发布会，会上首次明确新型基础设施的范围。会议指出，目前来看，新型基础设施主要包括3个方面内容：一是信息基础设施。主要是指基于新一代信息技术演化生成的基础设施；二是融合基础设施。主要是指深度应用互联网、大数据、人工智能等技术，支撑传统基础设施转型升级，进而形成的融合基础设施；三是创新基础设施。主要是指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施。下一步，国家发改委将联合相关部门重点做好四方面工作：一是加强顶层设计；二是优化政策环境；三是抓好项目建设；四是做好统筹协调。 ([查看更多](#))

## NDRC First Defines the Scope of the New Infrastructure

On April 20, 2020, the NDRC held the April press conference, at which the scope of the new infrastructure was defined for the first time. The NDRC indicated that at present, the new infrastructure involves three aspects: (i) the information infrastructure, which mainly refers to the infrastructure formed on the basis of new information technology; (ii) the converged infrastructure, which is formed by the deep application of Internet, big data, artificial intelligence and other technologies and the support of the transformation and upgrading of traditional infrastructures; (iii) the innovation infrastructure, which mainly refers to the public welfare infrastructure supporting scientific research, technological development and product development. Next, the NDRC will work with relevant departments in four aspects: first, to strengthen the top-level design; second, to optimize the policy environment; third, to work harder on project constructions; fourth, to improve overall coordination. ([More](#))

## 一季度全国网信行政执法工作有序推进

2020年4月16日，国家网信办公布了一季度全国网信行政执法工作情况。一季度，全国网信系统不断加大行政执法工作力度，各级网信部门会同有关部门，坚决查处网上危害国家安全类违法

信息和违法行为，依法关闭一批存在违法违规为社会影响恶劣的网站平台，通过约谈整改、行政处罚、公开曝光等手段，依法加大监管执法力度。据悉，全国网信系统一季度累计约谈网站1143家，警告网站848家，暂停更新网站117家，会同电信主管部门取消违法网站许可或备案、关闭违法网站816家，移送司法机关相关案件线索3520件；有关网站平台关闭各类违法违规账号群组3.3万个。（[查看更多](#)）

## CAC Releases the Results of Administrative Enforcement on Cyberspace in the First Quarter

On April 16, 2020, the CAC released the results of administrative enforcement on cyberspace in the first quarter. In the first quarter, the national cyberspace departments continued to strengthen the administrative enforcement. The cyberspace departments at all levels, together with relevant departments, resolutely investigated and punished illegal information and behaviors endangering national security, closed a number of websites in violation of laws and regulations with severe social impact, and strengthened law enforcement and supervision through interview, rectification, administrative punishment and public exposure, etc. It was reported that there were 1,143 websites inquired, 848 websites warned, 117 websites suspended from updating, 816 illegal websites cancelled or put on record by cyberspace departments together with competent telecommunication authorities, 3,520 clues of relevant cases transferred to judicial organs, 33,000 illegal account groups closed by relevant website platforms. ([More](#))

## 海外动态 Overseas News

### EDPB第二十三次全体会议 - 进一步起草抗疫指南

2020年4月21日，欧洲数据保护委员会（“EDPB”）在第23次全体大会上宣布，EDPB通过了新冠肺炎疫情期间为科学研究目的健康数据处理指南和新冠肺炎疫情期间定位及其他追踪工具指南。新冠肺炎疫情期间为科学研究目的健康数据处理指南旨在阐明与使用健康数据有关的最紧迫的法律问题，例如为科学研究目的的处理及进一步处理健康数据的法律依据、实施适当的保障措施以及数据主体权利的行使等问题。新冠肺炎疫情期间定位及其他追踪工具指南旨在阐明在何种情况及原则下可以合理利用定位数据以及接触者追踪工具。该指南有两个目的：（1）通过建立病毒传播模型，利用定位数据评估疫情期间限制出行措施的总体有效性；（2）利用接触者追踪，尽早通知新冠确诊患者的密切接触者以切断传染链。指南强调，GDPR和《电子隐私指令》均包含允许使用匿名或个人数据的条款，以确保欧盟成员国和欧盟的机构及其他参与方能够采取相关行动监控和防止新冠病毒的传播。此外，EDPB还在指南附件中增加了接触追踪APP的指南。（[查看更多](#)）

### Twenty-third Plenary Session: EDPB Adopts Further COVID-19 Guidance

On April 21, 2020, the European Data Protection Board (“EDPB”) announced that during its 23rd plenary session, the EDPB adopted guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak and guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak. The guidelines on the processing of health data for research purposes in the

context of the COVID-19 outbreak aim to shed light on the most urgent legal questions concerning the use of health data, such as the legal basis of processing, further processing of health data for the purpose of scientific research, the implementation of adequate safeguards and the exercise of data subject rights. The guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak aim to clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes: (i) using location data to support the response to the pandemic by modelling the spread of the virus in order to assess the overall effectiveness of confinement measures; (ii) using contact tracing, which aims to notify individuals who may have been in close proximity to someone who is eventually confirmed as a carrier of the virus, in order to break the contamination chains as early as possible. The guidelines emphasize that both the GDPR and the ePrivacy Directive contain specific provisions allowing for the use of anonymous or personal data to support public authorities and other actors at both national and EU level in their efforts to monitor and contain the spread of COVID-19. In addition, the EDPB adopted a guide for contact tracing apps as an annex to the guidelines. ([More](#))

### 加拿大隐私专员办公室发布疫情期间有效隐私措施评估框架

2020年4月17日，加拿大隐私专员办公室（Office of the Privacy Commissioner, “OPC”）发布了一份评估框架，旨在协助政府机构应对新冠危机。该份政策文件旨在指导以减轻疫情影响为目的的有效隐私措施的发展。该评估框架规定了一些重要的隐私原则：（1）法律依据：提出的措施必须具有法律依据；（2）采取的措施必须在必要的限度之内，必须具有科学依据以及是为了达到具体目的所必需；（3）目的限制：个人信息的使用必须以保护公众健康为唯一目的；（4）尽可能使用去标识数据或者总体数据；（5）特别措施必须是有时间限制的，收集到的数据应在疫情结束之后销毁；（6）公开透明以及责任制：政府需了解适用于特别措施的依据以及条款并对此负责。该框架对此前发布的指南起到了补充的作用，帮助需遵守联邦隐私法规的政府及机构更好地在新冠疫情期间了解其隐私保护的相关责任。 ([查看更多](#))

### OPC Publishes Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19

On April 17, 2020, the Office of the Privacy Commissioner of Canada (“OPC”) published an assessment framework intended to assist government institutions faced with responding to the COVID-19 crisis. The policy document is designed to guide the development of privacy impactful initiatives that seek to alleviate the effects of the pandemic. The framework sets out some key privacy principles, including: (i) legal authority: the proposed measures must have a clear legal basis; (ii) the measures must be necessary and proportionate, and, therefore, be science-based and necessary to achieve a specific identified purpose; (iii) purpose limitation: personal information must be used to protect public health and for no other purpose; (iv) use de-identified or aggregate data whenever possible; (v) exceptional measures should be time-limited and data collected during this period should be destroyed when the crisis ends; (vi) transparency and accountability: government should be clear about the basis and the terms applicable to exceptional measures, and be accountable for them. The framework complements previously issued guidance to help departments and organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 outbreak. ([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](http://www.lifanglaw.com)  
 Email: [info@lifanglaw.com](mailto:info@lifanglaw.com)

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