



# 5G与数据治理全球态势

吴沈括

北京师范大学互联网发展研究院院长助理

北京师范大学网络法治国际中心执行主任

联合国网络安全与网络犯罪问题高级顾问

中国互联网协会研究中心秘书长

邮箱 [shenkuo.wu@hotmail.com](mailto:shenkuo.wu@hotmail.com)

手机 13311546373

# 5G与数据治理全球态势

- 一、新一代信息技术及其相关机遇和风险态势
- 二、数据治理新维度：2018年ICDPPC《人工智能伦理与数据保护宣言》
- 三、数据治理新框架：2019年欧洲委员会《人工智能与数据保护指南》
- 四、数据治理新挑战：2019年《布拉格提案》
- 五、数据治理中国路：从政策战略到法律规范



# 一、新一代信息技术及其相关机遇和风险态势

一方面，围绕5G与数据的利用，在新一代信息技术的普及应用过程中，人们不断拥抱更多的发展机遇；

另一方面，围绕5G与数据的保护，我们也面对着来源更为广泛、程度更为深刻的安全风险。

# 一、新一代信息技术及其相关机遇和风险态势

根据中国互联网络信息中心2018年发布的《第41次中国互联网络发展状况统计报告》显示，我国的网民规模已达到7.72亿，手机网民规模达到7.53亿，互联网普及率为55.8%，境内外上市互联网企业数量达到102家，总体市值达到8.97万亿人民币。而就信息基础设施而言，我国服务器部署数量也已达到118万台。

Norton（诺顿）于2018年1月发布的一项关于网络安全及数据安全的研究报告，该报告统计分析了中国在内的20个世界主要国家和地区在2017年遭受网络犯罪的情况。根据该报告，2017年全世界约有9.78亿人受到了网络犯罪的影响，全世界的消费者因黑客攻击共遭受了约1720亿美元的损失。

## 1、新一代信息技术与相关机遇

(1) 新的技术支持：大数据、5G、人工智能等

(2) 新的组织样态：云计算、物联网等

(3) 新的应用内容：安保监控、远程诊疗、金融理财、生活娱乐等

## 2、新一代信息技术与风险态势

(1) 技术要素风险：木马、病毒、僵尸网络等

(2) 组织管理风险：电信网络诈骗等

(3) 在线内容风险：色情信息、暴恐信息、虚假信息等

## 3、焦点风险区域

(1) 非刑事责任：数据获取、处理（使用）、流转...

(2) 刑事责任：数据获取、流转、安全事件（泄露） ...



## 二、数据治理新维度：2018年ICDPPC《人工智能伦理与数据保护宣言》



**第40届数据保护与隐私专员国际大会  
(40th ICDPPC,  
2018.10.22-26, 布鲁塞尔)  
中文译本**

**吴沈括、周 洁、杨滢滢 / 译**

- 1、应根据公平原则，在基本人权层面设计、开发和使用人工智能和机器学习技术
- 2、应确保对人工智能系统的潜在影响和后果的持续关注和警惕以及确立问责制
- 3、应改进人工智能系统的透明度和可理解度，以实现有效施行
- 4、作为整体“设计伦理”方法的一部分，应通过默认应用隐私原则和设计隐私来对人工智能系统进行负责任地设计和开发
- 5、应促进赋能每个人，并应鼓励行使个人权利，为公众的参与创造机会
- 6、应当减少和减轻因使用人工智能数据而可能导致的非法偏见或歧视

### 三、数据治理新框架：2019年欧洲委员会《人工智能与数据保护指南》



斯特拉斯堡，2019年1月25日

T-PD(2019)01

个人数据自动化处理中的个体保护公约咨询委员会

(第108号公约)

人权与法治总司

人工智能与数据保护指南

(中译本)

吴沈括

译

胡 涵

I.一般指引

II.研发者、制造商和服务提供者指引

III.立法者与政策制定者指引



## 四、数据治理新挑战：2019年《布拉格提案》

布拉格 5G 安全大会

“布拉格提案”

布拉格，2019 年 5 月 3 日

吴沈括 胡涵 译

吴沈括，北京师范大学网络法治国际中心执行主任

胡涵，北京师范大学刑科院暨法学院硕士研究生



### - 前言：全球数字化世界中的通信网络

#### - 关于5G网络安全的重要性

#### - 提案指向

A.政策

B.技术

C.经济

D.安全、隐私和弹性

- 1、政策战略
- 2、法律规范
- 3、其他规范
  - (1) 最高司法机关
  - (2) 国家网信部门

### A、政策战略

1. “互联网+” 行动计划
2. 中国制造2025
3. 《关于促进大数据发展行动纲要》
4. 网络强国战略
5. 《“十三五” 国家信息化规划》
6. 《国家网络空间安全战略》
7. 《网络空间国际合作战略》
8. 《新一代人工智能发展规划》



### B、法律规范

- 网络安全法
- 电子商务法
- 个人信息保护法（拟）
- 数据安全法（拟）
- 电信法（拟）

### C、其他规范

#### (1) 最高司法机关

1. “两高一部” 电信网络诈骗《意见》(2016.12.20)
2. “两高” 侵犯公民个人信息刑事司法解释 (2017.06.01)
3. “两高” 扰乱无线电通讯管理秩序刑事司法解释 (2017.07.01)
4. “两高” 关于网络犯罪的司法解释 (2019)

### C、其他规范

#### (2) 国家网信部门

1. “微信十条” (2014.08.07)
2. “约谈十条” (2015.04.28)
3. “直播规定” (2016.11.04)
4. “网安标准化工作意见” (2016.08.12)
5. 网络产品和服务安全审查办法（试行） (2017.05.02)
6. 互联网新闻信息服务管理规定 (2017.06.01)
7. 互联网信息服务内容管理行政执法程序规定 (2017.06.01)
8. 个人信息出境安全评估办法（征求意见稿） (2019.06.13)

# 2019 《网络安全审查办法》(征求意见稿)

共计21条

- 1、《网络安全审查办法》的出台背景
- 2、《网络安全审查办法》的制度要点
- 3、《网络安全审查办法》的规范亮点



# 2019 《网络安全审查办法》(征求意见稿)

## 1、《网络安全审查办法》的出台背景

(1) 数字化发展加速，安全可控的关切突显

(2) 全球化程度加深，供应链安全问题普遍

## 2019《网络安全审查办法》(征求意见稿)

### 1、《网络安全审查办法》的出台背景

网络安全审查坚持防范网络安全风险与促进先进技术应用、增强公正透明与保护知识产权相统一，坚持事前审查与持续监管、企业承诺与社会监督相结合，从产品和服务安全性、可能对国家安全带来的风险隐患等方面进行综合分析评判。（第3条）

# 2019《网络安全审查办法》(征求意见稿)

## 2、《网络安全审查办法》的制度要点

- (1) CII运营者形成风险报告
- (2) 4种情况下申报网络安全审查
- (3) 网络安全审查办公室受理后完成初步审查(30+15个工作日)

分为通过审查、附条件通过审查、未通过审查三种情况

- (4) 审查结论建议送网络安全审查工作机制成员单位征求意见 (15个工作日)

A、意见一致：办公室以书面形式将审查结论反馈运营者

B、意见不一致：进入特别审查程序并通知运营者

# 2019《网络安全审查办法》(征求意见稿)

## 2、《网络安全审查办法》的制度要点

### (5) 特别审查程序

A、网络安全审查办公室应进一步听取相关部门、专业机构、专家意见，进行深入分析评估，形成审查结论建议，征求网络安全审查工作机制成员单位意见后，按程序报中央网络安全和信息化委员会批准。

B、特别审查原则上应在45个工作日内完成，情况复杂的可以延长。



# 2019《网络安全审查办法》(征求意见稿)

## 2、《网络安全审查办法》的制度要点

### (6) 事中事后监督与依照职权启动审查

A、网络安全审查办公室通过抽查、接受举报等形式加强事中事后监管。

B、网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务采购活动、信息技术服务活动，网络安全审查办公室按程序报中央网络安全和信息化委员会批准，依照本办法进行审查。

## 2019 《网络安全审查办法》(征求意见稿)

### 3、《网络安全审查办法》的规范特点

(1) 职能架构：三层次架构 (第4、5条)

(2) 实体事项：供应链安全 (第6、10条)

(3) 程序期限：日期的限制 (第9、11、13、14条)

## 2019 《数据安全管理办法》(征求意见稿)

共计5章40条

- 1、《数据安全管理办法》的制度背景
- 2、《数据安全管理办法》的框架特色
- 3、《数据安全管理办法》的规范侧重

## 2019 《数据安全管理办法》(征求意见稿)

### 1、《数据安全管理办法》的制度背景

国家坚持保障数据安全与发展并重，鼓励研发数据安全保护技术，积极推进数据资源开发利用，保障数据依法有序自由流动。(第3条)

# 2019 《数据安全管理办法》(征求意见稿)

## 2、《数据安全管理办法》的框架特色

涵盖数据处理全生命周期:

- (1) 数据收集
- (2) 数据处理使用
- (3) 数据安全监督管理



# 2019 《数据安全管理办法》(征求意见稿)

## 3、《数据安全管理办法》的规范侧重

### (1) 数据收集

- A、知情同意原则
- B、透明同步原则
- C、服务保障原则
- D、未成年人保护原则
- E、非歧视原则
- F、间接收集同等保护
- G、经营目的收集备案
- H、自动收集（数据爬取）限制
- I、DPO

# 2019 《数据安全管理办法》(征求意见稿)

## 3、《数据安全管理办法》的规范侧重

### (2) 数据处理使用

- A、技术安保措施
- B、保存删除义务
- C、查询、更正、删除或注销权利
- D、“定推”限制
- E、“合成”限制
- F、用户标识要求
- G、向他人提供个人信息的要求
- H、风险评估
- I、数据处理主体变更

# 2019《数据安全管理办法》(征求意见稿)

## 3、《数据安全管理办法》的规范侧重

### (3) 数据安全监督管理

- A、约谈
- B、数据安全认证和应用程序安全认证
- C、数据安全事件处置
- D、数据提供义务
- E、行政刑事责任衔接

### 主要启示：

- (一) 安全理念的转变
- (二) 风控策略的设定
- (三) 核心权益的维护
- (四) 关键风险的管控

## (一) 安全理念的转变

新理念：“设计安全” (Security by design)



## (二) 风控策略的设定

### 1. 消极维度

网络企业自身遵循法律条文引入的各行为规范从而确保免受法律处罚

### 2. 积极维度

根据法律规范授权发现、纠正侵害网络企业乃至网络产业利益的不合规行为

### (三) 核心权益的维护

《网安法》第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

### (三) 核心权益的维护

1. 注意法律规范的体系化综合运用;
2. 充分利用法律赋予的正当化机制。

## (四) 关键风险的管控

1. 《网安法》第六十三条 违反本法第二十七条规定，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。
2. “单位犯 (...) 罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照(...)的规定处罚。”

## (四) 关键风险的管控

### **“责任阻断机制” 建设**

- 1.横向：定岗定人，明确厘定行为人主观认识与客观行为的边界；
- 2.纵向：定岗定责，界分业务作业层级切断单位法律责任因果链。



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that create a sense of depth and movement, resembling a stylized grid or wave pattern.

# 谢谢！

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE





CAICT  
中国信通院

# 5G发展与安全高峰论坛

推进5G发展，共建安全未来

主办单位：中国信息通信研究院

协办单位：中国通信学会网络空间安全战略与法律委员会

支持单位：中国互联网协会互联网应用创新工作委员会

中国云安全与新兴技术安全创新联盟

联合国世界丝路论坛网络空间国际合作委员会