从数据合规到网安法的全面遵从

黄道丽 公安部第三研究所 副研究员 二级警督

我们的团队

◆公安三所网络安全法律研究中心

- 隶属于公安部第三研究所
- 跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用给网络管理带来的热点难点问题，为政府机构、企业等提供高质量的法律研究支撑
- 网络安全行政立法研究、大数据安全立法研究、安全漏洞法律规制、等级保护与关键信息基础设施立法研究等

目录

目录

安全态势

- 数据资源成为人类社会的生产要素
- 数据资源成为国家基础性战略资源
- 发达国家相继制定实施大数据战略
- 我国首次提出推行国家大数据战略
  - 国务院《促进大数据发展行动纲要》（国发〔2015〕50 号）
  - 《中华人民共和国国民经济和社会发展第十三个五年规划纲要》

安全态势

- 大数据时代面临着更为严峻的安全态势
  - 数据基础设施频受攻击
  - 新型网络威胁层出不穷
  - 个人信息丢失及泄露风险加大
  - 数据跨境流动监管机制不够完善
  - 数据资源、开放共享与安全保护矛盾

传统基于数据资产的风险管理机制尽管仍有着基本的保护作用，但已不能完全适应大数据技术和产业发展的需要

安全监管态势

◆不断完善国家顶层监管机制并落地实施，寻求在个人信息保护、数据安全保障、跨境数据传输等法律监管和大数据产业经济发展之间的平衡，安全监管态势呈现三大特点:

- ◆立法规范体系化
- ◆执法实践常态化
- ◆诉讼案例规模化

立法规范体系化

◆立法层面，相关规范制度已初具规模，并在逐步完善

◆个人信息保护。《关于加强网络信息保护的决定》《刑法》《民法总则》《消费者权益保护法》《测绘法》《征信管理条例》《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《电信和互联网用户个人信息保护规定》等法律法规中均明确了个人信息保护规范。立法层级逐步提升，可操作性逐步增强。

◆数据安全保障。2017年6月1日正式施行的《网络安全法》将实施多年的信息安全等级保护制度上升到国家网络安全等级保护制度层面，并首次明确建立了关键信息基础设施保护制度。《网络安全法》对数据安全保护在传统保护方式基础上，从关键信息基础设施保护、网络安全审查、数据本地化留存与跨境流动等方面强化对数据全生命周期的安全要求，并相继出台了一系列的配套措施。目前《关键信息基础设施保护条例》（征求意见稿）、《个人信息和重要数据出境安全评估办法》（征求意见稿）、《信息安全技术 数据出境安全评估指南》（征求意见稿）等配套规范仍在加紧推进中。

执法实践常态化

- ◆执法层面，相关执法实践逐步走向常态化
  - ◆侵犯公民个人信息犯罪仍处于高发态势，而且与电信网络诈骗、敲诈勒索、绑架等犯罪呈合流态势，社会危害及其严重，公安部多次部署全国公安机关打击整治网络侵犯公民个人信息犯罪专项行动。
  - ◆《网络安全法》实施之后，全国各地相继开展执法活动，违反网络安全等级保护规定的行政处罚案例、违反网络内容治理规定的处罚案例等执法案例相继涌现。

诉讼案例规模化

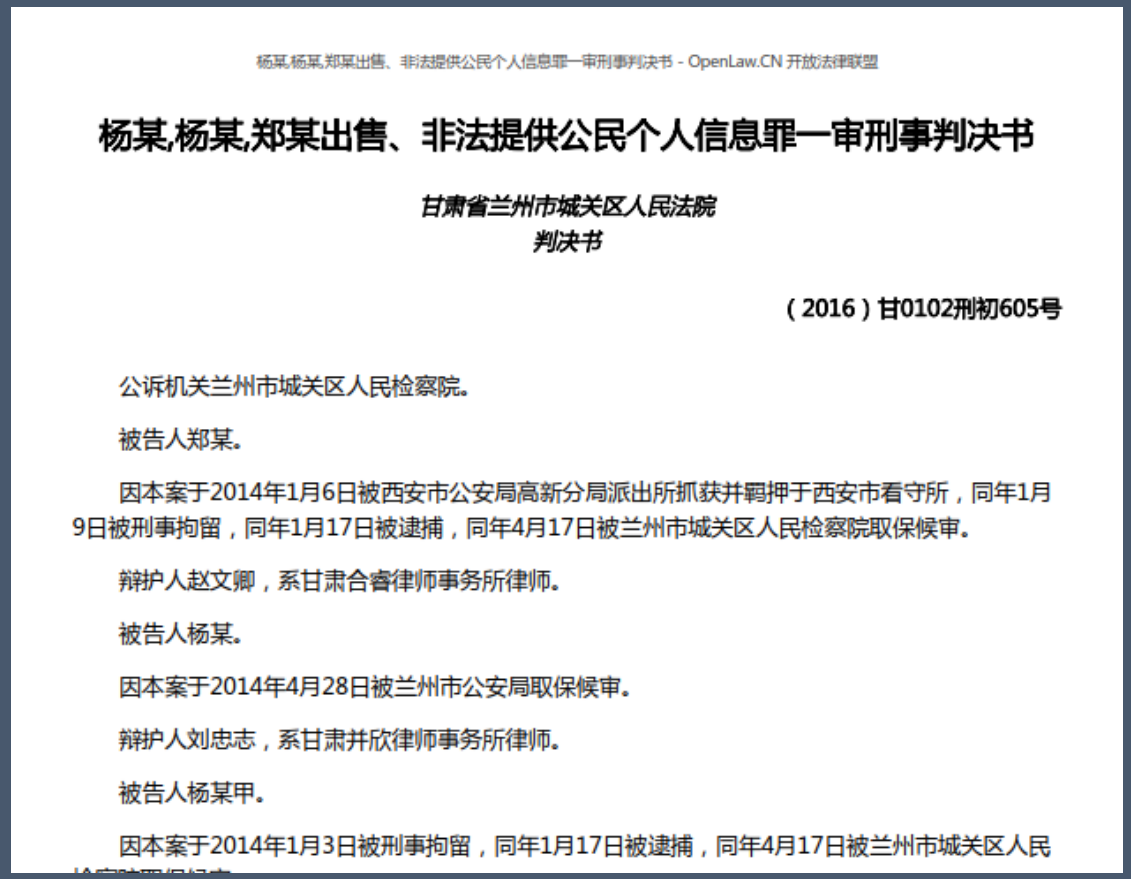
- 司法层面，相关诉讼逐步增多
  - 民事诉讼方面，我国先后出现了朱烨诉百度隐私权侵权案，周盛春诉阿里巴巴案 ，任甲玉诉百度案。
  - 刑事诉讼方面，《刑法修正案（九）》施行以来，各级公检法机关依据修改后的刑法规定，严肃惩处侵犯公民个人信息犯罪，案件数量显著增长。2015年11月至2016年12月，全国法院新收侵犯公民个人信息刑事案件495件，审结464件，生效判决人数697人。

数据合规的基础立法已经基本确立，初步构建了民事、行政和刑事保护相结合的立体框架，与此同时，基础立法有待指引和标准化落地

大数据安全合规态势

- 大数据安全合规风险三大特点：
  - 监管体系的配套制度、标准体系等尚待正式出台，合规不确定性
  - 宽严相济、张弛有度的“良性”执法体系尚未完全建立
  - 立法效果暂时无法进行有效的度量和改进

雀巢员工侵犯公民个人信息案



杨某,杨某,郑某出售、非法提供公民个人信息罪一审刑事判决书 - OpenLaw.CN 开放法律联盟

杨某,杨某,郑某出售、非法提供公民个人信息罪一审刑事判决书

甘肃省兰州市城关区人民法院
判决书

（2016）甘0102刑初605号

公诉机关兰州市城关区人民检察院。

被告人郑某。

因本案于2014年1月6日被西安市公安局高新分局派出所抓获并羁押于西安市看守所，同年1月9日被刑事拘留，同年1月17日被逮捕，同年4月17日被兰州市城关区人民检察院取保候审。

辩护人赵文卿，系甘肃合睿律师事务所律师。

被告人杨某。

因本案于2014年4月28日被兰州市公安局取保候审。

辩护人刘忠志，系甘肃并欣律师事务所律师。

被告人杨某甲。

因本案于2014年1月3日被刑事拘留，同年1月17日被逮捕，同年4月17日被兰州市城关区人民

◆二审法院：甘肃省兰州市中级人民法院，2017年5月31日判决

◆2011年至2013年9月，郑某等6名雀巢企业员工为推销配方奶粉，通过支付好处费等手段，从兰州市多家医院获取孕妇姓名、手机号等信息共计12万余条

雀巢员工侵犯公民个人信息案

- 法院充分认可雀巢企业所制定和实施的含有个人信息保护合规内容的《员工行为规范》等企业政策，认为其足以证明“雀巢企业禁止员工从事侵犯公民个人信息的违法犯罪行为”，并据此认定郑某等人的涉案行为属于个人行为
- 雀巢企业无刑事责任，免于单位犯罪
- 员工的合规意识是最终决定企业合规成败的关键，自上而下，以人为本，数据安全管理上，人是最大的风险，也是最好的尺度

目录

《中华人民共和国网络安全法》

- 2016年11月7日发布，自2017年6月1日起施行
- 第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑

核心价值目标之一：数据安全

数据安全：核心价值目标之一

◆在网络运行安全部分，《网络安全法》在传统保护方式基础上（数据分类、重要数据备份和加密）（第21条），从关键信息基础设施保护（第34条）、网络安全审查（第35条）、数据本地化留存与跨境流动（第37条）等方面强化数据全生命周期安全的要求。

◆在网络信息安全部分，《网络安全法》第40条到第45条规定了网络运营者对个人信息的全生命周期保护义务，要求网络运营者建立健全用户信息保护制度、信息安全投诉及举报制度，合法、正当、必要并经收集者同意后收集、使用其个人信息，强化个人信息安全保障，履行泄露告知、补救和报告等义务，保障个人的删除更正权，不得非法侵犯个人信息等。

数据安全：核心价值目标之一

◆法律责任部分，网络运营者、网络产品或者服务的提供者违反个人信息收集使用规则的，可能需要承担的行政处罚责任包括：责令改正、警告、没收违法所得、罚款；情节严重的，可能还会被责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等。窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，需要没收违法所得，并处罚款，没有违法所得的，处一百万元以下罚款。

《网络安全法》配套措施完善进行时

《网络安全法》配套规范一览表

文件类别	发布时间	文件名称	发布/制定单位
国家战略	2016.12.27	《国家网络空间安全战略》	国家互联网信息办公室
	2017.3.1	《网络空间国际合作战略》	外交部；国家互联网信息办公室
配套规章和规范性文件	2017.1.10	《国家网络安全事件应急预案》	中央网信办
	2017.5.2	《互联网新闻信息服务管理规定》	国家互联网信息办公室
	2017.5.2	《网络产品和服务安全审查办法（试行）》	中央网信办
	2017.5.31	《工业控制系统信息安全事件应急管理工作指南》	工业和信息化部
	2017.6.1	《网络关键设备和网络安全专用产品目录（第一批）》	国家互联网信息办公室；工业和信息化部；公安部；国家认证认可监督管理委员会
	2017.8.14	《一流网络安全学院建设示范项目管理办法》	中央网信办秘书局；教育部办公厅
立法草案	2017.4.11	《个人信息和重要数据出境安全评估办法（征求意见稿）》	国家互联网信息办公室
	2017.7.11	《关键信息基础设施安全保护条例（征求意见稿）》	
国家标准草案	2016.11.3	《信息安全技术 网络安全等级保护测评过程指南（征求意见稿）》	全国信息安全标准化技术委员会
	2016.11.3	《信息安全技术 网络安全等级保护测试评估技术指南（征求意见稿）》	
	2016.11.3	《信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求（征求意见稿）》	
	2016.12.20	《信息安全技术 个人信息安全规范（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护测评要求 第2部分：云计算安全扩展要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护基本要求 第3部分：移动互联安全扩展要求》	
	2017.1.11	《信息安全技术 网络安全等级保护基本要求 第4部分：物联网安全扩展要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护设计技术要求 第1部分：通用设计要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护设计技术要求 第2部分：云计算安全要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护设计技术要求 第3部分：移动互联安全要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护设计技术要求 第4部分：物联网安全要求（征求意见稿）》	
	2017.1.11	《信息安全技术 网络安全等级保护设计技术要求 第5部分：工业控制安全要求（征求意见稿）》	
	2017.5.24	《信息安全技术 网络安全事件应急演练通用指南（征求意见稿）》	
	2017.5.27	《信息安全技术 数据出境安全评估指南（草案）》	
国家标准立项	制定中	《信息安全技术 网络安全漏洞发现与报告管理指南》	全国信息安全标准化技术委员会
		《信息安全技术 关键信息基础设施网络安全保护要求》	
		《信息安全技术 网络产品和服务安全基本要求》	

《网络安全法》合规遵从9大模块

- 网络运营者
- 关键信息基础设施保护
- 网络安全等级保护
- 国家安全审查
- 配合、支持监管工作
- 个人信息保护
- 网络设备与服务认证
- 网络实名制
- 数据本地化存储与出境评估

《网络安全法》合规输出

- 适用法律清单
- 《网络安全法》各条款适用性
- 《网络安全法》差异分析结果与风险分布
- 个人信息和重要数据清单、分布
- 重要信息系统技术抽样评估结果
- 改进建议（与外部数据交互的建议）
  更新制度

目录

如何在有效利用数据促进业务创新增值、提升企业核心价值的同时，保障数据安全，完善内部控制，降低合规风险，成为当下企业亟需动态关注和直面解决的问题

2017年大数据安全合规白皮书（1.0版本）

2017 年大数据安全合规白皮书
（1.0 版本）

公安部第三研究所网络安全法律研究中心

2017 年 12 月 5 日

公安部第三研究所网络安全法律研究中心简介

公安部第三研究所网络安全法律研究中心（以下简称“中心”）是公安部第三研究所下设的专业法律研究机构。中心致力于服务网络安全中心工作需要，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用给网络管理带来的热点难点问题，为政府机构、互联网企业等提供高质量的法律研究支撑。

中心围绕网络安全法律问题展开了法学、计算机科学、公共管理与政策等跨学科交叉研究，承担上海市科委、公安部、中国工程院等省部级课题 6 项，参编著作教材 15 部，发表论文 40 余篇，多项研究成果被网络安全相关立法采纳。

中心对外运行“公安三所网络安全法律研究中心”公众号，定期发布立法研究成果和对外合作交流计划，欢迎业界同仁前来交流，共同创建高质量的交流平台。

联系地址：上海浦东张江华昇路 339 号 A 座 5 楼

电子邮箱：csplaw@stars.org.cn

联系电话：021-68571526

序 言

随着大数据安全态势的日益严峻，大数据安全监管机制的日趋加强，大数据安全合规也面临着诸多挑战和风险。大数据安全合规风险既有技术因素带来的风险，也有法律因素带来的合规风险。当下，大数据技术日新月异，新技术催生新的安全风险，同时也为数据安全合规带来了挑战。以企业的数据安全保障义务为例，随着新技术的层出不穷，新的威胁形态也不断涌现，如何应对新技术带来的新的安全威胁，切实落实安全保障义务，是企业合规需要解决的问题。此外，法律规则的不完善也为合规带来了挑战。

公安部第三研究所网络安全法律研究中心发挥优势力量，精心组织编写了《2017 年大数据安全合规白皮书》（1.0 版本），旨在为企业在个人信息保护、网络安全等级保护、数据本地化和出境评估三大核心问题上提供合规指引。鉴于《网络安全法》相关配套行政法规、部门规章、规范性文件和大量国家标准尚处于制定和征求意见稿阶段，本次发布白皮书 1.0 版本，其后将结合合规要求变化以及企业实践反馈予以改进和完善。

2017年大数据安全合规白皮书（1.0版本）

目 录

2017 年大数据安全合规白皮书（1.0 版本）

2017 年大数据安全合规白皮书（1.0 版本）

图表索引

合规工作指引

- 分析《网络安全法》各条款、《网络安全法》配套法律法规、标准等在企业的适用性，建立《网络安全法》合规管理框架；
- 依据合规管理框架，实施合规差距分析，识别企业在业务、IT等维度与《网络安全法》的差距，分析现有安全策略及安全控制措施针对《网络安全法》的有效性；
- 梳理个人信息和重要数据在企业重要信息系统的分布及流转过程，分析其安全控制手段的有效性；
- 识别数据跨境传输需求，梳理需要跨境传输的个人信息及重要数据，评估出境风险；
- 针对目前企业业务流程（包括外包业务）进行梳理，评估安全差异；
- 综合评估差距为企业带来的潜在业务风险与法律风险。

大数据安全合规风险控制

◆本白皮书从当下最关键的个人信息、等级保护及争议最大的数据本地化和出境评估制度出发，梳理了我国法律法规、规范性文件及相关标准的具体内容，以“从严为妥”的思路出发，为企业合规遵从提供参考和建议；

◆法律具有天然的滞后性，作为国家顶层设计的立法制度可能会与产业创新与发展的最佳实践磨合欠佳在短时间内是不可避免的事实，网络运营者应该本着“有法必依”的态度进行合规检查，全面遵从法律。

谢谢!

联系方式：
huangdaoli@stars.org.cn