数据保护

合规指引与规则解析

刘新宇◎主编

Data Protection:

Compliance Guidelines and Rule Analysis

- 数据保护相关新规解读
- 数据保护热点事件解析

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

数据保护：合规指引与规则解析

刘新宇　主编

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

图书在版编目（**CIP**）数据

数据保护：合规指引与规则解析/刘新宇主编.—北京：中国法制出版社，2020.8

（网络信息法丛书）

ISBN 978-7-5216-1214-1

Ⅰ.①数… Ⅱ.①刘… Ⅲ.①互联网络-个人信息-隐私权-法律保护-研究-中国 Ⅳ.①D923.04

中国版本图书馆CIP数据核字（2020）第134890号

策划编辑 李小草 韩璐玮（hailuwei666@163.com）

责任编辑 韩璐玮 王紫晶　　封面设计 李宁

数据保护：合规指引与规则解析

SHUJU BAOHU：HEGUI ZHIYIN YU GUIZE JIEXI

主编/刘新宇

经销/新华书店

印刷/

开本/710毫米×1000毫米 16开　印张/ 29 字数/ 378千

版次/2020年8月第1版　　2020年8月第1次印刷

中国法制出版社出版

书号ISBN 978-7-5216-1214-1　定价：89.00元

北京西单横二条2号

邮政编码 100031　　传真：010-66031119

网址：**http：//www.zgfzs.com**　编辑部电话：**010-66070084**

市场营销部电话：**010-66033393**　邮购部电话：**010-66033288**

（如有印装质量问题，请与本社印务部联系调换。电话：010-66032926）

编委会名单

序言

数据商业利用与个人信息保护之间存在的对立，无疑是数字社会发展中遇到的最大矛盾。合理的个人信息保护是数据商业交易不反噬个人私领域的基本保障和前提，而数据的自由流动与个人信息的正当使用则是数字社会健康发展的基础。这两者相辅相成、和谐发展方能带来数字社会的繁荣。如何平衡数据商业利用与个人信息保护之间的关系，最大效用地利用数据与信息，且能有效保护数据主体的最大权益，将是数据治理中的永恒核心议题。

在信息化趋势下，网络空间内安全威胁的范围不断扩大，具体表现形态也纷繁多样，网络安全形势愈发严峻。在此背景下的数据处理，尤其是其规模的不断扩大，也带来了更多的网络空间安全问题。如何通过高水平的立法应对网络安全威胁，保护关键信息基础设施和公民个人信息安全，维护国家利益和公民合法权益，进而推动我国网络空间国际治理能力的发展，亦成为在网络安全领域立法需回应的问题。

最近十年，“科技寡头”的快速扩张，时常会引发用户们对于自身的个人信息和数据是否能得到合理保护的担心，“支付宝年度账单事件”等与个人数据保护相关的事件和诉讼案件开始频繁涌现。这些与个人数据相关的议题，不断占据舆论热点。其中揭示的现实问题是：个人用户数据权利意识愈发强烈，企业的数据合规也愈发重要。这也使得企业个人数据的合规能力，正在和企业的商业信誉愈发紧密地捆绑在一起。在可见的未来，企业的数据合规将和企业名誉、利益甚至命运息息相关。甚至可以说，一个企业的信息合规能力，在未来会成为决定其综合实力的

重要影响因素。

刘新宇博士等作者前瞻且深刻地认识到，在数据商业运用广泛铺开的21世纪，数据本身的开放性、共享性和无形性，决定了法律人不仅会在学理层面遇到信息权利建构等各方面的挑战，而且更会让信息控制者和法律从业者，在实务的数据交易和数据运用中面对各种棘手的难题。面对这些问题，不仅立法者需要跳出传统法律体系的框架，面对新情况即时调整规范；法律从业者和个人信息持有者，也需要即时适应数据权利保护不断流变的法律框架，把握规范发展的脉络，甚至做出具有前瞻性的合规调整。

本书作为数据保护实务指引，凝聚了作者在长期法律研究和实务工作中的所见、所思、所得，紧跟数据保护热点、难点和重点，对数据合规相关问题的分析深入浅出，并从数据保护全生命周期的角度提出了具体的实务操作建议，具有较强的可行性，能够帮助读者在大数据时代，更好地应对新兴的数据合规挑战。这本书的亮点还在于收录了作者对数据保护相关新规的解析，方便读者在近两年数据保护新规不断出台的情况下，第一时间掌握新规的要点、难点，并为读者有效落实新规的要求提供了针对性的指导。

本书的几位作者均是在数据保护领域深耕多年的专家，熟悉各类数据商业应用的场景，对数据合规有着充分而深刻的理解。其中新宇跟我攻读博士期间便参与了跟我主持的国家社科基金重大课题“大数据时代个人数据保护与数据权利体系研究”相关的学术研究。其博士学位论文也是以《数据权利构建及其交易规则研究》为题，较为深入地研究了大数据时代下数据权属的认定、交易规则和数据权利构建等相关问题。可喜的是，他去年还在核心期刊上发表了《大数据时代数据权属分析及其体系构建》一文，指出目前以用户为中心的个人信息“绝对保护”框架，

已经无法有效地调整经营者和用户之间的复杂关系；而现代社会正愈发倾向于一种动态化的双向保护方式，以平衡个人信息权益与经营者数据资产权益。可以看出，他在执业之余，一直在数据法律领域坚持学习与研究。

本书作者尽管付出了艰辛努力，但对相关法律规章的解读还可更为细致些，对于案例的分析还可更为全面些，对一些基本概念或术语的介绍还可更加深入些。但瑕不掩瑜，本书丰富而系统的法律规章梳理，全面而富有针对性的条文解读以及对于典型案例的分析等，无论是对于数据企业，还是对于相关法律从业者，都会带来一定助益；也相信这本书对于企业数据合规体系在未来的构建，能够带来实际帮助。感动于作者在繁忙的实务工作中，不忘学习与研究！更期待新宇博士无论在实践业务，还是在学理知识上，继续努力与进步！

彭诚信

上海交通大学凯原法学院副院长、教授

2020年6月于凯原法学院

- 第一部分 我国数据保护现状概述
  - 一、引言
  - 二、数据保护立法现状
  - 三、数据保护监管部门梳理
  - 四、数据保护测评情况
  - 五、数据保护专项整治情况
  - 六、我国当前数据保护存在的问题
- 第二部分 数据保护相关法律规范
  - 一、法律、行政法规
  - 二、其他规定
  - 三、司法解释及其他规范性文件
  - 四、国家标准
- 第三部分 数据保护相关新规解读
  - 一、《互联网个人信息安全保护指南》与《互联网个人信息安全保护指引（征求意见稿）》和《个人信息安全规范》对比解读
  - 二、《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南（征求意见稿）》与《App自评估指南》和《App违法违规认定方法》逐条对比解读
  - 三、《网络安全审查办法》正式版与征求意见稿逐条对比解读
  - 四、《App违法违规认定方法》正式版与征求意见稿逐条对比解读
  - 五、《数据安全管理办法（征求意见稿）》逐条解读
  - 六、《个人信息出境办法（征求意见稿）》逐条解读
  - 七、《儿童个人信息网络保护规定》逐条解读
  - 八、《数据安全法（草案）》逐条解读

    - 九、《个人信息安全规范（征求意见稿）》十大主要变化解读
    - 十、《个人信息安全规范》正式版九大主要变化解读
- 第四部分 数据保护相关执法、刑事案例和热点事件解析
    - 一、数据保护相关执法案例解析
    - 二、数据保护相关刑事案例解析
    - 三、数据保护相关热点事件解析
- 第五部分 数据保护合规指引
    - 一、个人信息收集
    - 二、个人信息存储
    - 三、个人信息访问与使用
    - 四、个人信息委托处理、共享、转让和公开披露
    - 五、个人信息主体权利保护
    - 六、个人信息出境
    - 七、数据危机应对
- 第六部分 儿童个人信息保护的额外要求
    - 一、儿童的认定标准
    - 二、专门文本与专人负责
    - 三、监护人同意
    - 四、对外提供儿童个人信息的安全评估要求
    - 五、儿童个人信息保护的除外情形
    - 六、不得制作、发布、传播侵害儿童个人信息安全的信息
- 第七部分 个人信息保护组织管理要求
    - 一、个人信息保护责任部门与人员
    - 二、个人信息保护处理活动记录
    - 三、员工个人信息保护管理和培训
    - 四、个人信息安全影响评估
    - 五、个人信息安全审计

- 第八部分 爬虫使用合规指引
  - 一、爬虫相关概念及其应用场景
  - 二、爬虫治理盘点
  - 三、爬虫相关法律责任梳理
  - 四、爬虫使用合规指引
- 附录一 数据保护2019年回顾——规范、整治、前行
  - 规范篇
  - 整治篇
    - 一、专项整治行动盘点
    - 二、行政处罚盘点
    - 三、爬虫治理盘点
    - 四、刑事犯罪盘点
  - 前行篇
- 附录二 《个人信息安全规范（征求意见稿）》（2019.10.22版）与《个人信息安全规范》正式版全文比对

第一部分 我国数据保护现状概述

一、引言

当下，相关技术及市场的快速发展深刻改变着现有的生产和生活方式，正引发思维方式和社会形态的剧烈变革。数据有价，数据商品化的实现将数据使用和保护的平衡推到了信息化时代的台前，如何平衡数据的保护和利用并促进数据的流通成为新的关注点。一方面，民众权利意识的提升亟待法律的回应；而另一方面，企业和政府使用信息给民众带来巨大便利的现实，又不断提醒着我们，法律应当谨慎把控数据保护的力度，保障信息的流通自由。

现如今，数据，尤其是个人信息，对于实现风险控制、风险定价、精准营销、产品开发和战略分析等发挥着越来越重要的作用。但与此同时，其带来的风险也是不能忽视的。近年来，境内外数据安全事件频发，无论是Facebook的信息泄露事件、支付宝年度账单事件、顺丰员工转卖内部数据权限等重大数据安全事件，还是各类个人信息买卖案件、App个人信息侵权事件，在使社会公众信息安全和财产安全面临威胁的同时，也引发了政府和公众对数据安全的思考。

2020年5月28日通过的《民法典》将个人信息的相关规则写入民事立法中，确立了个人信息相关权利的法律地位及性质。而在此之前，2017年6月1日，《网络安全法》正式实施，其作为我国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，不仅是我国网络空间法治建

设的重要里程碑，也就数据和个人信息合规提出了许多框架性的要求。《网络安全法》实施以来，各类配套法规、规章和标准化文件不断出台。尤其是2019年以来，数据保护相关规范的出台速度明显加快，规则体系的框架已越发清晰，对应的合规要求也逐渐落向实处。随着我国政府数据安全意识不断加强以及个人信息主体自身权利意识的逐渐觉醒，做好数据保护已经成为面对着监管要求和舆情压力的企业在规划发展战略和开展日常运营工作的过程中不可忽视的重要环节。

二、数据保护立法现状

在现代社会治理中，将数据治理与个人信息保护放到更加重要的地位上已经成为国际社会的广泛共识。于我国而言，虽然聚焦于数据治理及个人信息保护的专门法律——《数据安全法》与《个人信息保护法》尚未出台，[1]但与数据保护相关的条文早在多年以前，便逐渐开始散见于法律、司法解释以及相关的部门规范性文件中，其具体的发展脉络梳理如下：

（一）民商事法律、法规、规章层面

2012年3月15日，工业和信息化部发布的《规范互联网信息服务市场秩序若干规定》正式施行，其明确规定，除非法律、行政法规另有规定，“能够单独或者与其他信息结合识别用户的信息”的收集、使用、提供必须“经用户同意”。就此，“可识别性”成为认定个人信息的核心标准，个人信息保护的客体开始逐渐明晰。2012年12月28日，全国人大常委会通过了《关于加强网络信息保护的决定》，明确了国家对于网络信息安全的保护，强调了公民个人信息收集过程中的合法、正当、必要原则以及防止个人信息泄露的义务，国家越发重视对于个人的网络信息保护。随后的两三年间，征信、工信、消费者保护等领域的立法都将个人信息保护纳入相应的法律文本中，如《征信业管理条例》《电信和互联网用户个人信息保护规定》《中华人民共和国消费者权益保护法》等。

2017年6月1日，《网络安全法》正式实施，作为我国网络和数据安全框架性的立法，它标志着我国网络安全保护相关的众多制度要求开始

逐步建立。在安全等级保护方面，《网络安全等级保护条例（征求意见稿）》《网络安全等级测评机构管理办法》等规章相继发布或生效；在关键信息基础设施保护方面，《关键信息基础设施安全保护条例（征求意见稿）》（以下简称《CII保护条例（征求意见稿）》）发布；在数据出境方面，《个人信息出境安全评估办法（征求意见稿）》（以下简称《个人信息出境办法（征求意见稿）》）等规范性文件的制定标志着数据跨境传输方面的制度要求逐渐完善。此外，国家网信办还于2019年5月28日发布了《数据安全管理办法（征求意见稿）》。

伴随着《网络安全法》的施行和相关监管实践活动的开展，在积累了较为充分的监管经验的前提下，更具针对性的数据立法开始大量发布。如2019年10月1日起施行的《儿童个人信息网络保护规定》对于儿童的个人信息的保护采取了更加严格的手段，并基于儿童个人信息保护的特殊性对儿童个人信息保护进行了专门的规定。而针对一些App过度收集用户个人信息，隐私条款不完善等问题，国家网信办、工信部、公安部、国家市场监管总局四部委也于同年11月28日联合发布了《App违法违规收集使用个人信息行为认定方法》（以下简称《App违法违规认定方法》）。该文件既为监管部门认定App违法违规收集使用个人信息行为提供了参考，也为App运营者自查自纠和网民社会监督提供了具体的实务指引。

我国不同地区的网络条件及技术能力存在较大差异，不同地区数据保护情况可能存在区别。实践中，部分地方政府也尝试通过制定地方法规的方式对数据处理活动进行规范。例如，天津市网信办于2019年6月26日发布了《天津市数据安全管理办法（暂行）》，并于2019年8月1日开始正式施行，开启了地方监管机关开展监管探索的尝试。此后，《重庆市政务数据资源管理暂行办法》《贵州省大数据安全保障条例》等地

方法规也相继出台，地方政府基于区域特点进行数据方面的针对性监管或将成为今后的立法趋势。

此外，随着新业务的出现和发展，数据保护亦在不同行业的立法中表现为专业化和精细化的特征。如随着“网约车”、物流行业的发展，《网络预约出租汽车经营服务管理暂行办法》《寄递服务用户个人信息安全管理规定》等管理办法应运而生，其中涉及大量旨在规制行业中数据收集和使用等问题的具体条文。这类法规及规章进一步充实了数据治理的相关规则体系。同时，2020年发布的《民法典》将“隐私权和个人信息保护”单列一章，对隐私和个人信息进行特别的规定，从基本法律的层面体现了对个人信息的重视。

（二）国家标准层面

我国数据立法的一个鲜明特征便在于通过大量的国家标准的制定来为企业合规经营提供指引。国家标准在制定程序上相对更为灵活，更能贴近不断发展变化的数据活动的实践需要。2013年2月1日，《信息安全技术　公共及商用服务信息系统个人信息保护指南》（GB/Z　28828-2012）正式实施。这是我国关于个人信息保护的首个国家标准，该文件确立了信息处理的基本原则（目的明确原则、最少够用原则、公开告知原则等），明确将个人信息区分为个人敏感信息和一般个人信息，并区别规制。

2017年12月29日，《信息安全技术　个人信息安全规范》（以下简称《个人信息安全规范》）由全国信息安全标准化技术委员会（以下简称信安标委）发布，并于2018年5月1日正式实施。该标准系我国个人信息保护领域最重要、影响最为广泛的国家标准，其对于个人信息的相关名词进行了系统化、专业化的定义，并对于个人信息控制者在收集、保

存、使用、共享、转让、公开披露等信息处理环节中的相关行为进行了规制。根据实践中个人信息收集、使用的变化及《个人信息安全规范》（2017）在实施过程中出现的问题，信安标委分别于2019年2月1日、6月25日及10月22日发布了《个人信息安全规范（草案）》和两次征求意见稿，不断根据监管实践中发现的用户画像、个人生物识别信息收集等相关新问题对规范的内容进行调整，并于2020年3月6日发布了修改后的《个人信息安全规范》正式版，将于2020年10月1日正式施行。

在《网络安全法》确立的具体制度方面，许多制度框架正是通过国家标准来搭建和完善的。例如，在网络安全等级保护方面，《GB/T 22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）》（以下简称《网络安全等级保护基本要求》）、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护实施指南》、《信息安全技术 网络安全等级保护安全设计技术要求》等多部国家标准均已在实施当中，以全力推动我国网络安全等级保护制度从“等保2.0”向“等保3.0”时代演进。再如，在《网络安全法》和《个人信息安全规范》搭建的一系列收集、使用个人信息制度的基础上，《信息安全技术 个人信息去标识化指南》（以下简称《个人信息去标识化指南》）、《信息安全技术 大数据安全管理指南》（以下简称《大数据安全管理指南》）、《信息安全技术 个人信息安全影响评估指南（征求意见稿）》、《信息安全技术 个人信息告知同意指南（征求意见稿）》（以下简称《个人信息告知同意指南（征求意见稿）》）等配套国家标准也相继生效或发布，为数据安全及个人信息保护提供了更加详细和具体的指引。

（三）刑事层面

在立法层面，我国对数据和个人信息的保护存在着“刑法先行”的立法模式。1997年修订的《刑法》便已经规定了破坏计算机信息系统罪，侵入他人计算机删除、修改、增加数据信息的行为开始受到刑事处罚。2009年2月28日，《刑法修正案（七）》开始正式施行，其增设了出售、非法提供公民个人信息罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪等罪名。《刑法修正案（七）》不仅采用刑事手段规制金融机构等单位工作人员提供、获取、交易个人信息的行为，也是首次将侵入非国有计算机仅获取数据的行为也纳入刑事规制的范围之内，对于他人计算机信息的删改行为不再成为入罪的必须要件，刑法对于数据保护的力度得以加强。2015年施行的《刑法修正案（九）》则修改了刑法第253条之一，将犯罪主体的限制放宽，提升了法定最高刑的刑期，并规定对于在履行职责或者提供服务过程中获得的公民个人信息，非法出售或提供的行为，可以从重处罚。修改后，“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”被整合为“侵犯公民个人信息罪”。同时，《刑法修正案（九）》也增设了非法侵入计算机信息系统罪、破坏计算机信息系统罪等罪名的单位犯罪规定。

除《刑法》外，最高人民法院、最高人民检察院和公安部也出台了一系列与数据和个人信息犯罪相关的司法解释，以指导相关刑事案件的侦查、检察和审判。2013年4月23日，最高人民法院、最高人民检察院和公安部联合发布了《关于依法惩处侵害公民个人信息犯罪活动的通知》，要求坚决打击侵害公民个人信息犯罪活动。该通知明确规定侵害公民信息犯罪的定罪量刑应当综合考量非法出售、提供、获取个人信息的次数、数量、手段和牟利数额等因素，与此同时，该文件也对于具有可识别性的个人信息进行了较为细致的列举，如姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历等。2014年10月10日，最高人民法院发布的《关于审理利用信息网络侵害人身权益民事纠纷案件适用

法律若干问题的规定》正式施行，全方位地确定了利用信息网络侵害个人信息案件的审理流程与审判要点，提高了个人信息相关刑事案件的审判工作水平，也变相推动了司法机关对个人信息相关犯罪的打击力度。

2017年6月1日，最高人民法院、最高人民检察院联合发布的《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》（以下简称《侵犯公民个人信息刑事案件解释》）正式施行。该司法解释对于侵犯公民个人信息罪的构成要件、量刑标准和具体法律适用问题进行了系统性的规定。其后两年中，最高人民检察院发布的《检察机关办理侵犯公民个人信息案件指引》和《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（法释〔2019〕15号）（以下简称《网络犯罪解释》）则对于侵犯公民个人信息案件的几个具体构成要件，列出了更为细致的证据审查要求与更加清晰的定罪量刑之标准。

（四）数据保护相关法律、法规、规章、规范性文件及国家标准汇总

当前我国数据保护相关的重要法律、法规、规章、规范性文件及国家标准参见下表：

序号	文件名称	发布机构	生效时间	法律状态
A. 数据保护相关的重要法律、法规、规章及规范性文件				
1	《消费者权益保护法》第14条、第29条、第50条、第56条	全国人大常委会	2014年3月15日	现行有效
2	《刑法修正案（七）》	全国人大常委会	2009年2月28日	现行有效
	《刑法修正案（九）》第17条、第28条		2015年11月1日	

续表

序号	文件名称	发布机构	生效时间	法律状态
3	《网络安全法》	全国人大常委会	2017 年 6 月 1 日	现行有效
4	《民法典》第 111 条、第 1032 ~ 1039 条	全国人大	2021 年 1 月 1 日	尚未生效
5	《电子商务法》第 5 条、第 23 条、第 25 条、第 32 条	全国人大常委会	2019 年 1 月 1 日	现行有效
6	《密码法》	全国人大常委会	2020 年 1 月 1 日	现行有效
7	《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》	最高人民法院	2014 年 10 月 10 日	现行有效
8	《侵犯公民个人信息刑事案件解释》	最高人民法院、最高人民检察院	2017 年 6 月 1 日	现行有效
9	《网络犯罪解释》	最高人民法院、最高人民检察院	2019 年 11 月 1 日	现行有效
10	《征信业管理条例》	国务院	2013 年 3 月 15 日	现行有效
11	《电信和互联网用户个人信息保护规定》	工信部	2013 年 9 月 1 日	现行有效
12	《中国人民银行金融消费者权益保护实施办法》	中国人民银行	2016 年 12 月 14 日	现行有效
13	《儿童个人信息网络保护规定》	国家网信办	2019 年 10 月 1 日	现行有效
14	《App 违法违规认定方法》	国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅	2019 年 11 月 28 日	现行有效
15	《网络安全审查办法》	国家网信办	2020 年 6 月 1 日	现行有效
16	《App 违法违规收集使用个人信息自评估指南》	App 违法违规收集使用个人信息专项治理工作组	2019 年 3 月 3 日	非法律文件
17	《数据安全法（草案）》	全国人大常委会	2020 年 7 月 3 日（发布时间）	正式版未发布，未生效

续表

序号	文件名称	发布机构	生效时间	法律状态
18	《CII 保护条例（征求意见稿）》	国家网信办	2017 年 7 月 10 日（发布时间）	正式版未发布，未生效
19	《网络安全等级保护条例（征求意见稿）》	公安部	2018 年 6 月 27 日（发布时间）	正式版未发布，未生效
20	《数据安全管理办法（征求意见稿）》	国家网信办	2019 年 5 月 28 日（发布时间）	正式版未发布，未生效
21	《个人信息出境办法（征求意见稿）》	国家网信办	2019 年 6 月 13 日（发布时间）	正式版未发布，未生效
22	《网络安全漏洞管理规定（征求意见稿）》	工信部	2019 年 6 月 18 日（发布时间）	正式版未发布，未生效
B. 数据保护相关的重要国家标准				
23	《网络安全等级保护基本要求》	市场监管总局、国家标准化委员会	2019 年 12 月 1 日	已生效
24	《信息安全技术　网络安全等级保护测评要求》	市场监管总局、国家标准化委员会	2019 年 12 月 1 日	已生效
25	《个人金融信息保护技术规范》	中国人民银行	2020 年 2 月 13 日	已生效
26	《个人信息去标识化指南》	市场监管总局、国家标准化委员会	2020 年 3 月 1 日	已生效
27	《大数据安全管理指南》	市场监管总局、国家标准化委员会	2020 年 3 月 1 日	已生效
28	《信息安全技术　网络安全等级保护实施指南》	市场监管总局、国家标准化委员会	2020 年 3 月 1 日	已生效
29	《个人信息安全规范》	市场监管总局、国家标准化委员会	2020 年 10 月 1 日	尚未生效
30	《个人信息安全影响评估指南（征求意见稿）》	信安标委	2018 年 6 月 11 日（发布时间）	正式版未发布，未生效

续表

序号	文件名称	发布机构	生效时间	法律状态
31	《信息技术　安全技术　生物特征识别信息的保护要求（征求意见稿）》	信安标委	2019年6月25日（发布时间）	正式版未发布，未生效
32	《个人信息告知同意指南（征求意见稿）》	信安标委	2020年1月20日（发布时间）	正式版未发布，未生效
33	《信息安全技术　移动互联网应用程序（App）收集个人信息基本规范（征求意见稿）》	信安标委	2020年1月20日（发布时间）	正式版未发布，未生效
34	《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南（征求意见稿）》	信安标委	2020年3月19日（发布时间）	正式版未发布，未生效

综合上表来看，现阶段我国对于数据保护的立法中，已经有相当一部分较为具体、可操作的规定。但是由于缺少较高位阶的法律加以统一，整体的法规和规范性文件依然处在一个较为分散和松散的状态，缺少系统性。当下，《个人信息保护法》《数据安全法》等法律法规已经被列入人大法工委2020年度立法工作计划之中。可以预见，在不远的将来，立法对数据的保护会进一步完善，覆盖的广度和深度会进一步加强，数据和个人信息保护的重要性将会进一步提升。

三、数据保护监管部门梳理

自《网络安全法》实施以来，网络安全相关的执法检查日益常态化。对于企业来说，充分了解各监管部门的职责范围和行政执法重点，能够帮助其更加依法合规地开展业务、面对监管检查。

1.行政执法主体

根据国务院于2004年印发的《全面推进依法行政实施纲要》（国务院令第十号）第7条第22项：“行政执法由行政机关在其法定职权范围内实施，非行政机关的组织未经法律、法规授权或者行政机关的合法委托，不得行使行政执法权……”可以认为，行政执法主体包括：（1）在法定职权范围开展行政执法行为的行政机关；（2）由法律、法规授权或者行政机关委托行使行政执法权的非行政机关。

具体到网络安全、个人信息安全保护领域，结合《网络安全法》等相关规定以及当前的执法实践可以看出，相关行政执法事项主要由网信部门、工信部门、公安部门以及市场监督管理部门负责。

尽管各部门有其法定的职责权限，其行政执法的对象和范围也各有侧重，但在具体开展行政执法的过程中，仍然存在一些困境。2017年12月24日举行的十二届全国人大常委会第三十一次会议上，关于检查网络安全法、加强网络信息保护的决定（即“一法一决定”）实施情况的报告明确指出：网络安全监管“九龙治水”现象仍然存在，权责不清、各自为战、执法推诿、效率低下等问题尚未有效解决，法律赋予网信部门的统筹协调职能履行不够顺畅。一些地方网络信息安全多头管理问题比较突

出，但在发生信息泄露、滥用用户个人信息等信息安全事件后，用户又经常遇到投诉无门、部门之间推诿扯皮的问题。不少网络运营单位反映，行政执法过程中存在不同执法部门对同一单位、同一事项重复检查且检查标准不一等问题，不同法律实施主管机关采集的数据还不能实现“互联互通”，经常给网络运营商增加额外负担。

针对前述问题，除了依照相关法律法规及政策文件规定、在实践中进一步明确各职能部门的权责界限以外，各部门也越来越多地采用了联合协作等方式开展行政执法工作，以加强资源整合、信息共享，打破数据壁垒。例如，2019年初，中央网信办、工信部、公安部、市场监管总局共同发布了《关于开展App违法违规收集使用个人信息专项治理的公告》，联手在全国范围组织开展App违法违规收集使用个人信息专项治理行动。2019年5月至12月，前述四部门又联合开展全国范围的互联网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。

此外，具体到各个细分行业，不少行业主管部门也逐渐承担起对所在行业的网络信息安全的管理责任。例如，在金融行业，中国银行保险监督管理委员会、中国人民银行等会配合对金融相关的数据合规问题进行监督管理；在教育行业，教育部、国家新闻出版署等相关部门会参与到个人信息保护相关的治理行动中；其他领域的行政主管部门，如国家质量监督检验检疫总局、国家食品药品监管总局、国家宗教事务局、国家版权局等，也同样针对各自领域内的数据和信息进行相应的规范。

2.行政执法行为

从中共中央办公厅、国务院办公厅发布的《行政执法类公务员管理

规定（试行）》[2]，以及国务院办公厅印发的《推行行政执法公示制度执法全过程记录制度重大执法决定法制审核制度试点工作方案》（国办发〔2017〕14号）[3]等文件中均可以看出，行政执法行为应当包含行政许可、行政处罚、行政强制、行政征收、行政收费、行政检查六类。

在网络安全、个人信息安全保护领域，最主要和最常见的行政执法行为是行政检查和行政处罚，当然部分情况下也会涉及行政许可和行政强制。

从行政处罚措施上来看，根据《行政处罚法》第8条规定：“行政处罚的种类：（一）警告；（二）罚款；（三）没收违法所得、没收非法财物；（四）责令停产停业；（五）暂扣或者吊销许可证、暂扣或者吊销执照；（六）行政拘留；（七）法律、行政法规规定的其他行政处罚。”其中，就责令停产停业这一处罚，在互联网环境下，除了常规的停业整顿外，还包括关闭网站、关闭通讯群组、暂停系统运行、暂停新用户注册等形式。

（一）网信部门

1.部门简介

网信部门在中央/国家层面包括中央网信办和国家网信办。国家网信办与中央网信办是“一个机构两块牌子”的关系，列入中共中央直属机构序列[4]。

中央网信办，即中共中央网络安全和信息化委员会办公室，其前身是于2014年2月27日成立的中央网络安全和信息化领导小组，由中共中央总书记、国家主席、中央军委主席习近平担任组长；2018年3月，中

共中央印发《深化党和国家机构改革方案》，将中央网络安全和信息化领导小组改为中央网络安全和信息化委员会，中央网信办为该委员会的办事机构。中央网信办自成立之初，即开展了“扫黄打非·净网2014”专项行动、打击整治“伪基站”专项行动、“剑网2014”专项行动等。

国家网信办，即中华人民共和国国家互联网信息办公室，是经国务院批准设立的互联网信息监管机构，成立于2011年5月初。《网络安全法》为国家网信部门设定的职责主要包括：

序号	职责	依据
1	统筹协调网络安全工作和相关监督管理工作。	《网络安全法》第8条
2	会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认。	《网络安全法》第23条
3	关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，会同国务院有关部门组织的国家安全审查。	《网络安全法》第35条
4	对关键信息基础设施运营者将其在境内运营中收集和产生的个人信息和重要数据向境外提供的，会同国务院有关部门制定办法进行安全评估。	《网络安全法》第37条

续表

序号	职责	依据
5	统筹协调有关部门对关键信息基础设施的安全保护采取下列措施： （一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估； （二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力； （三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享； （四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。	《网络安全法》第39条
6	和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。	《网络安全法》第50条
7	统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。	《网络安全法》第51条
8	协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。	《网络安全法》第53条

此外，2014年8月，国务院发布《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》（国发〔2014〕33号），授权国家互联网信息办公室负责全国互联网信息内容管理工作，并负责监督管理执法。

2017年5月，国家网信办又发布《互联网信息内容管理行政执法程序规定》（以下简称《程序规定》），从部委规章的层面将互联网信息内容管理的执法工作进行了程序上的统一协调安排。特别值得关注的是，《程序规定》第21条和第29条分别对“网络巡查”和“远程取证”等新型执法手段作了规定，在针对互联网领域的行政执法实践中更加具有可操作性。

2.行政执法情况

针对互联网信息内容管理，网信部门进行了一系列专项执法检查和行政处罚。

2019年初，国家网信办启动网络生态治理专项行动，分为启动部署、全面整治、督导检查、总结评估四个阶段，剑指各类网站、移动客户端、论坛贴吧、即时通信工具、直播平台等重点环节中12类违法违规互联网信息，集中解决网络生态重点环节突出问题。

2019年，全国网信系统通过约谈、警告、限期整改、暂停更新网站，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，会同有关部门依法查处网上各类违法信息和违法行为，移送司法机关相关案件线索等方式，持续加大行政执法力度。例如：

序号	执法主体	处罚对象	处罚原因	处罚措施
1	北京市网信办	搜狐	搜狐 WAP 网、搜狐新闻客户端传播低俗庸俗信息、破坏网上舆论生态等。	约谈相关负责人，责令整改。整改期间，搜狐 WAP 网“新闻频道”、搜狐新闻客户端“新闻频道”自 2019 年 1 月 3 日 15 时起暂停更新一周。
2	北京市网信办	新浪网	对用户发布违法违规信息未尽审查义务，持续传播炒作导向错误、低俗色情、虚假不实等违法有害信息。	约谈相关负责人，责令其全面深入整改，整改期间对“新浪博客”“新浪看点”平台暂停更新 1 个月，对“新浪新闻”“新浪博客” App 下架 1 个月。
3	上海市网信办	华尔街见闻简书网	未获得互联网新闻信息服务资质，违规登载新闻信息，内容导向存在偏差等扰乱网络信息传播秩序。	约谈相关负责人，责令其停止违法违规行为，开展全面深入整改，依法作出罚款处罚。
4	杭州市网信办（浙江省网信办指导）	花瓣网	历史存量信息中存在违法不良有害信息内容。	约谈“花瓣网”相关负责人，责令“花瓣网”全面开展自查整改，全站暂停信息内容更新 15 天。
5	天津市网信办会同江苏省和北京市网信办	视觉中国	违规从事互联网新闻信息服务、违规与境外企业开展涉及互联网新闻信息服务业务的合作。	约谈网站负责人，责令两家网站立即停止违法违规行为，进行全面整改。整改期间，两家网站暂停服务。
	上海市网信办	IC photo		

地方各级网信办也积极开展各项行动，例如深圳市网信办于2018年5月组织开展“一法一令”（《网络安全法》和《互联网新闻信息服务管理规定》）落实情况专项检查行动，对腾讯公司、果酱直播等单位的法律法规落实情况进行执法监督检查。

同时，针对关键信息基础设施，近两年来，各地网信办也积极组织开展网络安全检查工作，通过现场查看、技术检测、查阅资料、座谈交