君合专题研究报告 JUNHE

2022 年 9 月 23 日

数据合规领域政府执法及调查的响应与配合

近年出台的《网络安全法》《数据安全法》《个人信息保护法》及其他相关法律法规对中国的网络数据安全和个人信息保护事项进行“自上而下”的有序监管，并授权多个政府机构对以企业为主的监管对象进行监督和检查，以促进企业和个人遵守网络数据安全和个人信息的保护要求。

2022 年 9 月 8 日，国家互联网信息办公室（“**国家网信办**”）发布《网信部门行政执法程序规定（征求意见稿）》（“**《程序规定》**”），进一步规范国家网信办和地方互联网信息办公室（统称“**网信部门**”）依法履行监管职责。鉴于执法调查案例和实施细则的逐步释出，本文拟从《程序规定》的文件要点切入，对数据合规领域（包括网络安全、数据安全和个人信息保护）执法调查的主要依据、实施部门和执法活动的类型作梳理总结，以对企业的响应与配合要点进行提示。

一、《程序规定》出台背景与要点

2017 年 5 月 2 日，国家网信办发布《互联网信息内容管理行政执法程序规定》，以在《行政处罚法》与《网络安全法》的基础上，加强互联网信息内容管理执法体系建设。2017 年至今，数据合规领域相关法律法规陆续出台或更新，相应地，网信部门执法和调查依据不断细化，执法范围也逐渐从互联网信息内容管理，扩展至更广义的网络安全、数据安全及个人信息保护等领域。2022 年 9 月发布的《程序规定》整体上细化了数据合规领域的执法要求，文件的基本要点如下：

- **执法范围：**明确各级网信部门依职权管辖的案件范围包括网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。[1]
- **行政强制措施：**指出网信部门在办理个人信息保护案件时可以采取查封、扣押等行政强制措施。[2]
- **执法要求：**细化立案、调查取证、听证约谈、行政处罚决定的作出与送达、执行与结案等环节中的网信部门执法要求，例如明确调查取证人员应具有行政执法资格并主动出示执法证件、对于涉及重大公共利益等特殊情况的行政处罚决定增加法制审核程序、细化行政处罚案件办理期限等。

二、数据合规领域的主要执法与调查依据

数据合规领域的主要执法与调查依据由实体法规则与程序法规则共同构成。《网络安全法》《数据安全法》《个人信息保护法》等基础法律规定，对相关主体在网络运营、数据处理以及个人信息保护方面的权利义务以及法律责任进行了详细规定。同时，《互联网信息内容管理行政执法程序规定》《程

[1] 参见《程序规定》第二章。

[2] 参见《程序规定》第三十二条。

序规定》等程序性规则，为执法部门开展行政处罚　　的程序以及管理要求提供了规范。

法律法规名称	主要内容
《网络安全法》	规定了网络运营者、网络产品或者服务的提供和关键信息基础设施的运营者的网络运行安全义务和网络信息安全义务，以及主管部门的网络安全保护和监督管理职责与权限。
《数据安全法》	规定了个人、组织与数据有关的权益，开展数据处理活动的组织、个人的数据安全保护义务，以及国家机关的安全监管职责与权限。
《个人信息保护法》	规定了个人信息主体的权利，个人信息处理者在个人信息生命周期不同环节应遵守的规则与义务，以及主管部门的保护职责与权限。
《网络安全审查办法》	规定了关键信息基础设施运营者、网络平台运营者配合网络安全审查的义务、范围以及程序，以及审查人员的职责和权限。
《互联网信息内容管理行政执法程序规定》	规定了互联网信息内容管理部门对违反有关互联网信息内容管理法律法规规章的行为实施行政处罚的相关程序。
《网信部门行政执法程序规定（征求意见稿）》	规定了网信部门处理有关网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件的相关程序。

此外，近年来，各地在中央立法的指导下陆续出台地方数据条例，为数据合规执法提供了区域性的细化规则。此外，以《信息安全技术 个人信息安全规范》为代表的国家标准、行业标准、地方标准等文件亦成为数据合规领域执法与调查的重要参考。

三、主要实施部门及职责

数据合规领域主要监管执法、检查和调查体系呈现“自上而下”、“联合执法检查”、“一案双查”等特点或工作要求。以移动互联网应用程序（“**APP**”）监管为例，网信、工信、公安、市场监管等部门均有不同程度的参与。

实践中，多部门综合监管与执法的情况可能给企业配合监管要求、完善数据合规体系带来一定挑战。我们尝试基于近年的法律法规文件和监管实践，将数据合规领域较为常见的监管与执法部门及各自职责总结如下。

- **国家网信办：**统筹协调网络安全、网络数据安全、个人信息保护工作；网络信息安全监督管理；网络安全审查；组织数据出境安全评估、规定个人信息保护认证、制定个人信息出境标准合同等。
- **网信部门：**管辖职责范围内的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件。
- **公安部、地方公安机关（统称“公安部门”，包括内部网络警察总队/支队、网安总队/支队等网络安全保卫机构）：**监管危害网络安全活动、网络违法犯罪活动、非法获取、提供个人信息等行为；开展职责范围内的数据安全监管工作，以及监管恶意程序设置、违法信息处置行为等其他职责。
- **工业和信息化部、地方工业和信息化部门以及地方通信管理局（统称“工信部门”）：**协调维护国家信息安全和国家信息安全保障体系建设；指导监督政府部门、重点行业的重要信息系统与基础信息网络的安全保障工作；协调处理网络与信息安全的重大事件等。
- **国家市场监督管理总局、地方市场监督管理局：**

监督和管理 APP 个人信息处理活动、数据安全管理认证工作等。

- **中国银行保险监督管理委员会及地方派出机构（统称“银保监会”）：**负责银保监会监管数据安全工作，组织实施监管数据安全评估和监督检查；监管银行业金融机构数据治理工作等。
- **国家卫生健康委员会、地方卫生健康行政部门：**开展健康医疗数据、人口健康信息等标准、安全和服务管理与监督工作。
- **科学技术部、地方科学技术行政部门：**人类遗传资源采集、保藏、国际合作科学研究、材料出境等审批工作；人类遗传资源国际合作临床试验、对外提供或开放使用等备案工作等。

四、常见的监管执法、调查与检查活动

从近年来监管与执法实践来看，常见的数据合规领域监管执法、调查与检查活动包括：

（一） 日常检查与执法

前述主管部门开展的日常检查（包括定期或随机形式），具体的检查时间、方式和主体依检查和执法目标会有不同。

例如，工信部会定期组织第三方检测机构对 APP 及第三方软件开发工具包（SDK）进行检查，并相应提出整改要求。[3] 地方公安机关也会针对当地网络安全重点保卫单位开展网络安全监督检查。[4] 同时，相关监管执法部门也会针对检查或执法对象特点采取针对性的行政执法措施，例如下架 APP、取消网站许可或备案、关闭违法网站等。

（二） 专项行动

专项行动指由网信部门、公安部门、工信部门等部门牵头开展的网络与数据安全专项行动，例如国家网信办“清朗”系列专项行动、公安部“净网”系列专项行动。[5]

（三） 安全审查

《网络安全法》规定了关键信息基础设施运营者采购网络产品和服务，可能影响国家安全的，应当通过国家安全审查。类似的要求在《数据安全法》中也有出现。

此外，根据《网络安全审查办法》，关键信息基础设施运营者或网络平台运营者在特定情形下需主动申报进行网络安全审查，同时，网络安全审查办公室亦可依职权启动审查。[6]

（四） 事后监管

数据合规领域典型的事后监管体现在对网络安全事件的监管与调查中，根据《国家网络安全事件应急预案》，在发生网络安全事件后，事发单位应按要求实施处置并及时报送信息，并应由相关部门组织调查处理和总结评估。[7]

部分行业监管部门对该领域的网络安全事件事后监管进行了细化规定，如对于证券期货业网络安全事件，中国证监会或者其派出机构将督促相关机构落实整改措施，同时可采取听取报告、询问当事人、调阅系统日志等工作方式。[8]

---

[3] 参见工信部通报 47 款侵害用户权益 APP 和 SDK：https://mp.weixin.qq.com/s?__biz=MjM5OTUwMTc2OA==&mid=2650869326&idx=1&sn=8cccd5d658af8a8e71258e0f7114aa67&chksm=bccf24e98bb8adffe5153dae37135bcac8953485827383d3a5b2339082e3d83d157288a3afa7&mpshare=1&scene=1&srcid=0914pdRYbLgmDlO2xukx5JFF&sharer_sharetime=1663150203314&sharer_shareid=591c1ae68629a4e27d557cd984dfcbe6#rd

[4] 参见网警在行动丨开展网络安全专项检查，让网络安全不留死角：https://baijiahao.baidu.com/s?id=1728978626957327468&wfr=spider&for=pc

[5] 参见 2022 年“清朗”系列专项行动举行新闻发布会：http://www.cac.gov.cn/2022-03/17/c_1649125522577850.htm；参见公安部新闻发布会通报部署全国公安机关开展“净网 2021”专项行动的工作举措和取得的成效等情况：https://www.mps.gov.cn/n2253534/n2253535/c8329772/content.html

[6] 参见《网络安全审查办法》第五条、第七条、第十六条。

[7] 参见《国家网络安全事件应急预案》第五条。

[8] 参见 《证券期货业网络安全事件报告与调查处理办法》第二十四条、第二十六条。

（五） 刑事处罚

数据合规相关刑事案件亦属于监管执法重点，近年公安机关严厉打击危害网络安全、数据安全与个人信息权益的违法犯罪活动。2021 年，公安机关网安部门便重点打击了非法采集、提供、倒卖个人信息违法犯罪，以及破坏计算机信息系统数据、非法获取计算机信息系统数据类犯罪。[9]

五、企业如何响应与配合政府执法工作

基于前文对数据合规领域监管执法、调查的梳理和总结，我们结合过往经验，将企业在响应与配合政府执法调查过程中的两方面要点做初步提示。

（一） 跨境数据泄露或安全事件的响应

在特定国家或地区发生数据泄露或安全事件可能涉及多个不同国家或地区境内自然人的个人信息，在此类场景中，企业如何快速厘清不同法域的数据泄露或安全事件监管要求并协调不同法域的处置方案对企业提出一定的考验。

例如，境外数据泄露或安全事件涉及企业收集或管理的员工或消费者个人信息时，企业需要考虑的重点事项诸如：如何判断事件的真实性以及影响程度，如何实施不同国家或地区的报告和披露要求（如报告时间、内容详尽、前期判断等），以及应当组建何种事件响应团队（包括但不限于熟悉当地数据安全法规的律师、专业的网络数据安全事件调查人员、企业内部 IT 和数据管理人员等），以期对事件的处理实现遵守适用的法律法规要求，并符合企业商业和社会责任等多重目标。

（二） 检查与执法活动的响应与配合

就国内政府机构的检查与执法活动而言，根据《程序规定》，网信部门在正式立案之前，可以采取询问、勘验、检查、鉴定、调取证据材料等措施。在监管实践中，相关部门也可能采取随机或定期检查。中国数据合规领域“多部门执法”的特点导致企业在面临随机检查时，需注意区分不同执法部门的监管权限与审查重点，并确定可保留数据/文件的范围。

虽然数据合规领域政府执法与调查具有一定的特殊性，企业仍可借鉴一般政府执法与调查的准备措施，例如完善沟通接待的策略与指引、配合数据搜集与员工访谈、合理行使当事人权利、适时邀请律师介入与协助等，并结合具体执法部门、执法事项、所涉数据等情况，配合相关执法与调查活动。

刘晨光 合伙人 电话：86-21-22086088 邮箱地址：liuchg@junhe.com
孙 博 合伙人 电话：86-21-22086216 邮箱地址：sunb@junhe.com
马晓媛 律 师 电话：86-21-22086114 邮箱地址：maxiaoyuan@junhe.com
徐钱燕飞 电话：86-21-22838357 邮箱地址：xuqyf@junhe.com

[9] 参见数据安全步入法治化轨道（来源：人民日报）：https://baijiahao.baidu.com/s?id=1720246978595568299&wfr=spider&for=pc。