君合研究简讯

JUNHE

2023 年 3 月 30 日

网络安全与保护法律热点问题

网信执法程序颁布—网络安全与数据保护进入政府监管新阶段

2023 年 3 月 23 日，国家互联网信息办公室（“国家网信办”）公布了《网信部门行政执法程序规定》（“《程序规定》”），该规定将自 2023 年 6 月 1 日起施行。

在《网络安全法》、《数据安全法》及《个人信息保护法》三大法律框架下，在中国网络安全及数据安全立法领域最具代表性的“数据出境监管”规则逐一落地之后，《程序规定》的出台恰逢其时，其为网络与数据安全和个人信息保护事项进行“自上而下”地有序监管提供了程序指引---《程序规定》通过规范和保障网信部门依法履行职责，保护公民、法人的合法权益，维护国家安全和公共利益。

本文从以下角度，梳理并讨论《程序规定》中企业需重点关注的内容。

（一）地域管辖的广泛性

根据《程序规定》，行政处罚由“违法行为发生地”的网信部门管辖。“违法行为发生地”包括**违法行为人相关服务许可地或者备案地，主营业地、登记地，网站建立者、管理者、使用者所在地，网络接入地，服务器所在地，计算机等终端设备所在地**。与 2022 年 9 月发布的《程序规定》征求意见稿（“征求意见稿”）相比，最终定稿的《程序规定》对于“违法行为发生地”中的“相关服务许可地、备案地、主营业地”等不再限定为“网络运营者”相关地，而省略了主体身份，以违法行为人作为替换，显示以违法行为作为处罚依据（而非主体身份）的变化。

《程序规定》中对“违法行为发生地”的广泛定义，基本涵盖了各种情形下的网信执法管辖权。概括来讲，虽然因网络架构和数据流动具有全球性和复杂性的特点，但对于涉及中国因素（例如中国境内运营境外网络，境外收集处理来自中国境内数据等）的行为，从文义来看，网信部门均可能具有执法管辖权。

（二）执法类型的概括性

对于具体的执法事项，征求意见稿罗列了网信部门可以管辖“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。但最终的《程序规定》删除了相关表述，只是概括性规定了“县级以上网信部门依职权管辖本行政区域内的行政处罚案件”。考虑到《网络安全法》、《数据安全法》，《个人信息保护法》以及其他相关法规中的行政执法部门并不完全清晰，例如《数据安全法》第六章法律责任部分中的行政执法部门仅规定为“有关主管部门”，因此《程序规定》中的网信部门的执法事项范围存在一定的讨论空间。

（三）涉及国家安全案件的严肃性

《网络安全法》、《数据安全法》及《个人信息保护法》均涉及国家安全的保护以及对危害国家安全的处罚措施。《程序规定》规定了当案件涉及国家安全时，设区的市级以下网信部门应当及时报告上一级网信部门，必要时报请上一级网信部门管辖。

由此可知，国家安全问题属于网信部门的管辖

范围并重点关注（但基于其他法律规定，国家安全问题并非仅由网信部门管辖）。根据中国立法原则分析，企业的日常经营中，最有可能涉及“国家安全”的问题主要集中在“数据出境”合规领域，考虑到数据出境主要的路径（数据出境安全评估，标准合同，认证）已全部落地，企业应重点关注数据出境合规工作的落实以及后续针对核心数据、重要数据的识别工作。

（四）调查取证中的特殊性

相比于其他类型的行政执法，电子数据的取证是网络安全与数据保护领域执法调查的关键证据来源。根据《程序规定》第二十一条，“电子数据是指案件发生过程中形成的，存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或者存储介质中，以数字化形式存储、处理、传输的，能够证明案件事实的数据”。

《程序规定》赋予了网信部门通过**现场取证、远程取证和责令有关单位、个人固定和提交**等多种方式来收集和保存电子数据的权力。从技术角度来讲，执法人员具备对境外系统和服务器中的数据进行远程取证的可能性，且对于系统内数据在调查取证过程中很难进行区分对待。对于跨国公司全球系统内的数据，网信执法过程中对电子数据的收集一定程度上可能突破传统意义上的行政管辖（地域管辖）的范畴，具体有待在执法实践中明确。

此外，根据《程序规定》第二十八条，在证据可能灭失或者以后难以取得的情况下，经网信部门负责人批准，**执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存**，先行登记保存的设备和物品，网信部门应当在七个工作日内作出证据保全后返还、或送交鉴定、或解除保存、或予以没收等处理决定。如果有证据证明是用于违法个人信息处理活动的设备或物品，执法人员还可以采取查封或者扣押措施。

（五）免于处罚的可能性

《程序规定》规定了三种可能不予处罚的情形，分别是：（1）违法行为情节轻微并及时改正，没有造成危害后果；（2）初次违法且危害后果轻微并及时改正；（3）当事人有证据足以证明没有主观过错。

其中前两项都需要以当事人的“及时改正”作为前提条件。此时，企业应配合网信部门的执法工作，根据整改要求尽快采取改正措施。而对于第三项可能免于处罚的情形，需要证明当事人没有主观过错，则需要企业将具体工作贯彻于日常的合规工作中。考虑到网络安全与数据保护法规在近年来的频繁出台，数据出境规定涉及的大量且复杂的合规要求，相应合规工作的完善程度需要尽快评估，并补足实际工作与法律要求的差距。

结语

随着网络安全与数据保护立法与规则制度趋于完善，监管部门也会将重心逐步转移至日常的监督检查与执法工作中。《程序规定》的公布正式为网信部门的行政执法提供了程序依据，也标志着数据保护领域迈向“常态化”的政府监管时代。

孙　博　　合伙人　电话：86 21 2208 6216　邮箱地址：sunb@junhe.com
刘国君　　律　师　电话：86-21-2283 8289　邮箱地址：liuguojun@junhe.com