欢迎关注《中国商报·法治周刊》官方微信

《中国商报·法治周刊》官方微信平台

扫一扫 更精彩

中国商报

法治周刊

欢迎关注《中国商报·法治周刊》头条号

《中国商报·法治周刊》官方头条号

扫一扫 更精彩

2022 年 3 月 1 日 星期二 总第 7580 期 邮发代号 1-18

新修订的网络安全审查办法正式施行

筑牢数据安全防线 助力平台经济健康发展

许睿 本报记者 李海洋

2 月 15 日，由国家互联网信息办公室等十三部门联合修订发布的网络安全审查办法（以下简称办法）正式施行。专家表示，办法的施行，对数据处理、抵御数据安全风险、国外上市等活动提供了审查的依据，为保障国家安全提供了扎实的工具，为我国依法治网揭开了新篇章。

审查制度不断完善

网络安全审查是网络安全领域的重要法律制度。原办法自 2020 年 6 月 1 日施行以来，通过对关键信息基础设施运营者采购活动进行审查和对部分重要产品等发起审查，对于保障关键信息基础设施供应链安全、维护国家安全发挥了重要作用。

国家互联网信息办公室有关负责人表示：“2021 年 9 月 1 日，数据安全法正式施行，明确规定国家建立数据安全审查制度。我们据此对网络安全审查办法进行了修订，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，并明确要求掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查，主要目的是为了进一步保障网络安全和数据安全，维护国家安全。”

国家互联网应急中心最新报告显示，近年来，网络产品和服务供应链安全形势愈加严峻，针对关键信息基础设施的信息窃取、攻击破坏等恶意活动持续增加，针对数据的网络攻击以及数据滥用问题日趋严重，数据安全风险将更加突出。

“出于适应国际国内网络安全新形势、促进平台经济稳定健康发展的需要，适时地进行制度修订和调整，体现了制度不断向前发展的趋势，持续完善的网络安全审查制度将为维护国家安全作出更大贡献。”中国网络安全审查技术与认证中心工程师齐越说。

我国各类互联网平台众多，既有为社会提供金融支付、通信交流等基础性服务的互联网平台，也有专注于视听、求职、打车、货运、购物等的领域性互联网平台。中国网络安全审查技术与认证中心高级工程师唐旺表示，这些平台或掌握了海量公民个人数据，或在一个领域内掌握具有垄断性的用户信息。互联网平台掌握的数据一旦发生泄露，将会严重危害公民个人信息安全，给不法分子实施诈骗、非法营销等活动提供便利。

据中国网络安全审查技术与认证中心工程师刘金芳介绍，网络安全审查重点评估的国家安全风险因素增加了两方面内容：一是重点评估核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；二是重点评估上市存在关键信息基础设施、核心数据、重要数据或大量个人信息被外国政府影响、控制、恶意利用的风险。

记者注意到，此次办法修订在扩大审查范围的同时，也对审查的工作机制、工作流程等进行了适当调整。调整内容包括：增加证监会作为网络安全审查工作机制成员单位，明确网络安全审查办公室收到合格申报材料的时间为审查开始时间，增加上市申请文件作为上市审查申报材料的一部分，增加上市活动带来的数据安全风险作为国家安全风险考虑的因素，延长特别审查的工作时限至 90 个工作日等。齐越表示，从总体上看，审查机制和流程沿用了原有审查制度框架，针对新纳入赴国外上市审查这一变化进行了有针对性的优化，审查制度在实践中不断得到完善。

赴国外上市严审查

唐旺表示，上市对于互联网平台具有特殊意义。国内互联网平台大多以上市，特别是赴国外上市作为发展的主要目标。但是，如果一个互联网平台不遵守国家有关网络安全要求，不落实重要数据和个人信息保护责任义务，滥用数据，上市后在金融力量的加持下无序扩张，网络安全风险和威胁将成倍扩大。同时，一些国家出于保护本国投资者的目的，通过法律要求在其国内上市的企业披露业务经营数据。这个理由一旦被滥用，索要数据的边界将不受限制，会给国家安全带来很大威胁。

办法将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者，赴国外上市必须向网络安全审查办公室申报网络安全审查。同时，申报网络安全审查可能有以下三种情况：一是无须审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

《中国互联网络发展状况统计报告》显示，2021 年上半年，工业和信息化部网络安全威胁和漏洞信息共享平台接报网络安全事件 49605 件。图为江苏省海安市公安局网安大队民警在向孩子们讲解网络安全知识。 *CNSPHOTO 提供*

一个数据严监管的时代正在到来。新修订的网络安全审查办法针对数据处理活动，聚焦国家数据安全风险，明确运营者赴国外上市的网络安全审查要求。该办法既是贯彻落实网络安全法、数据安全法等一系列法律法规的有效实践，也是不断完善国家网络安全审查制度、适应国际国内网络安全新形势的重要举措，更是保障人民群众切身利益和维护国家安全的现实需要。

办法要求，关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

在供应链安全风险评价的基础上，办法增添了针对国家数据安全风险因素的评价。企业在开展对外活动时，大量个人信息、核心数据、重要数据一旦被窃取、泄露、损毁、非法利用，将直接影响国家安全和公共利益安全。比如，有大型网络公司汇聚了大量涉及国家安全、公共利益和个人权益的信息，如果在大数据运用过程中出现泄露，大量的敏感数据将被国外势力窃取，一旦被解析或者共享、发布，将对我国国家安全、公共利益及个人利益造成不可估量的损失。

鉴于企业海外上市存在的风险，本次修订办法时增加了证监会的职能表述，以针对企业赴国外网络平台上市活动实施审查，也增加了将企业上市材料纳入网络安全审查申报范围的规定。

专家表示，办法的实施提醒有关企业，在开展涉及大量个人信息、核心数据、重要数据的活动时，一定要加强国家安全意识，先行判断活动可能带来的国家安全风险，要及时向网络安全审查办公室汇报情况，主动配合安全防范措施。

安全风险如何化解

第 48 次《中国互联网络发展状况统计报告》显示，2021 年上半年，工业和信息化部网络安全威胁和漏洞信息共享平台接报网络安全事件 49605 件。

“网络安全审查的主旨在于网络风险的识别与防范，是国家安全审查的重要组成部分。网络平台运营者是维护网络安全、国家安全的重要责任主体。”北京航空航天大学工业和信息化法治研究院研究员雷震文表示，保障数据安全与网络安全，要防患于未然。

对此，雷震文建议，网络平台运营者化解网络安全风险、国家安全风险，应该注意以下三个方面：首先，应提高安全意识、法治意识，尤其应正确理解和处理维护网络安全与促进自身发展之间的关系，坚持安全发展理念，筑牢网络安全的基石；其次，应不断增强对自身运营安全的管理和评估，积极对照网络安全法和数据安全法的相关规定以及办法第 10 条列出的安全风险因素，做好安全风险的预判和评估、管理工作；最后，积极主动申报和配合网络安全审查，凡符合办法规定的审查条件的当事人都应负有主动申报并配合审查办公室做好安全审查工作的义务。

“关键信息基础设施运营者应采购安全可信的、供应渠道可靠的网络安全产品和服务，基于此构建具有全面感知、智能协同、动态防护能力的安全保障体系。”天融信科技集团 CEO 李雪莹认为，关键信息基础设施运营者采购网络安全产品和服务，是为了获得并持续提升其网络和数据安全保护能力。因此对于所采购的网络安全产品和服务，在自身安全可信的基础上，还应具备有效对抗威胁、防范风险的安全能力。

除了在自身关键信息基础设施方面做到合规建设外，安恒信息首席科学家刘博则认为，企业和机构还需要考虑建设体系化的数据安全能力，重视数据安全的体系规划。刘博建议企业从“管理、技术、运营”三个维度，建立相应的管理体系、技术保障以及常态化的数据安全运营机制，以实现利用数据安全技术更好开展业务的目的。

针对如何保护数据安全这个核心问题，360 安全专家表示，要以数据为中心，以组织为单位，以能力成熟度为抓手，从传统的管理体系转向社会化治理体系，建立复合机制，从只有处罚转变为处罚、帮助、奖励并举。

目前，行业中数据安全工作普遍面临的难点在于数据如何分类分级，亟待行业和企业一起将标准定义出来，以标准为基础不断优化。此外，各企业员工的安全意识如何提高也是比较棘手的问题，需要通过培训、制度及流程等持续影响。数据安全专家表示，数据安全建设要从组织、制度、流程及安全能力方面进行建设；数据安全运营是一项持续的工作，数据安全是一个过程，需要不断优化，以业务为主体进行持续的运营，这也是安全工作的重中之重。

链接 〉〉〉

数据成网络安全审查重点

我国网络空间安全立法不断推进，目前已经形成了包括网络安全法、数据安全法和个人信息保护法等三部基本法律为纲的治理框架。三法相继生效，标志着我国的网络安全工作从技术安全、内容安全完成了对新维度的拓展——数据安全。

在对数据安全认识的逐步深化及国际博弈的巨大压力之下，网络安全审查制度将数据安全涵盖其中，恰逢其时。针对数据安全，网络安全审查制度重点关注以下两类风险：“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险”，以及“上市存在关键信息基础设施，核心数据、重要数据或大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险”。

前者主要关注关键信息基础设施所采购的网络产品和服务提供者利用提供产品和服务的便利条件，非法收集、存储、利用、向境外提供关键信息基础设施所处理的“核心数据、重要数据或大量个人信息”的风险。换言之，网络产品和服务提供者除了其对外宣称和向用户展示的“规定动作”之外，不应偷偷地进行关于数据的“自选动作”，更不应该损害其用户对自己信息的自主权、支配权。后者是指因赴境外或国外上市而导致被外国法律管辖，进而引发外国政府能够通过执法、司法方面的法律规定和权力，对境内网络平台运营者所掌握的“核心数据、重要数据或大量个人信息”施加“影响”、主张“控制”，并随之“恶意利用”，导致我国主权、安全、发展利益受损的风险。“掌握超过 100 万用户个人信息的网络平台运营者”，因在此方面的数据安全风险突出，新版的网络安全审查办法规定，“赴国外上市，必须向网络安全审查办公室申报网络安全审查”。

在新一轮数据治理中，国家不仅仅作为制度供给者，也作为独立的利益主体登场，全球数据治理立法均充分考量国家的利益诉求，各国的数据战略都服务于大数据时代的综合国力竞争，既包括维护国家安全利益的防御性诉求，也包括促进本国数字经济全球竞争，并通过规则治理抢占全球数据规则话语权。因此，我国数据安全法、个人信息保护法，乃至于新版的网络安全审查办法并非局限于技术安全问题，而是在更加宽泛的意义上理解数据安全，核心目的都在于保障作为基础性战略资源的数据，能够在将来被管好、用好，服务于我国的主权、安全和发展利益。

2 月 17 日，安徽南部地区普降大雪，合肥铁路公安处绩溪北站派出所启动恶劣天气应急预案，加强站区重点部位巡查，全力维护旅客乘降秩序，热情为民服务，确保旅客出行安全。图为民警在为携带大量行李的旅客搬运行李。 童革苗 / 摄

主编：李海洋 新闻热线：010-83128830 投稿邮箱：zgsbfzzk@163.com 广告代理：北京法行天下文化传播中心