汉坤法律评述
2024 年 10 月 2 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约

好风借力，扬帆当时：简评《网络数据安全管理条例》

作者：段志超 | 王雨婷 | 金今 | 邹奕

引言

2024 年 9 月 30 日，国务院总理李强签署第 790 号国务院令，公布《网络数据安全管理条例》（以下简称“**《网数条例》**”），自 2025 年 1 月 1 日起施行。自 2021 年 11 月国家互联网信息办公室（以下简称“**网信办**”）公布《网络数据安全管理条例（征求意见稿）》（以下简称“**《征求意见稿》**”）以来，《网数条例》连续三年被写入国务院立法工作计划，受到社会各界广泛的关注和讨论。主管部门汇聚各方反馈意见、总结近年来有关网络数据安全的立法和监管实践，最终形成了《网数条例》这一网络数据安全领域首个行政法规级文件。

概括而言，《网数条例》针对上位法（即《中华人民共和国网络安全法》（以下简称“**《网络安全法》**”）、《中华人民共和国数据安全法》（以下简称“**《数据安全法》**”）、《中华人民共和国个人信息保护法》（以下简称“**《个人信息保护法》**”））以及现行部门规章中的重要概念与合规要求进行了明确与细化，虽然新增了部分网络数据处理者的合规义务，但基本与近年来网络数据领域的主流行业实践保持一致，总体上针对《征求意见稿》中的各项细化要求进行了适度的调整与放宽，体现了立法者谦抑的态度与促进数据合法有效利用的决心。

本文将通过对《网数条例》重点内容的初步梳理，解读其与现行网络数据领域法律法规之间的关系，识别与企业密切相关的重点合规义务。

一、《网数条例》适用范围

（一）何为“网络数据”

《网数条例》旨在规范“网络数据处理活动”。对此，《网数条例》附则第 62 条将“网络数据”界定为“通过网络处理和产生的各种电子数据”。该定义的范围理论上小于《数据安全法》和《个人信息保护法》有关“数据”和“个人信息”的界定，即“以电子或其他方式记录的信息”。相比之下，《网数条例》的适用聚焦于“通过网络”处理“电子数据”的行为，排除了使用纸张等传统物理介质记录的数据信息。但由于通过网络形式进行电子数据的处理已经成为当今企业开展业务的常态，因此，《网数条例》对于绝大部分企业均具有适用性。

（二）何为“网络数据处理者”

《网数条例》附则第 62 条进一步明确，“网络数据处理者”指的是“在网络数据处理活动中自主决定处理目的和处理方式的个人、组织”，基本采取了《个人信息保护法》对“个人信息处理者”的界定思路，突出“处理者”对处理活动的控制权。

事实上，《网数条例》出台前，网络数据安全领域的数个部门规章都使用了“数据处理者”这一概念，但缺少统一、明确的定义，导致难以界定部分法律义务的责任主体。例如，在数据跨境场景下，实际处理数据的企业（如个人信息处理受托方）是否需要履行相关评估备案义务并不明确。因此，《网数条例》的此番定义将帮助在网络数据处理链条上不同角色的企业更好地厘清权责划分边界，促进数据要素的有序流通。

（三）《网数条例》的地域范围

《网数条例》第 2 条延续了《数据安全法》和《个人信息保护法》中有关域外适用效力的规定。一方面，在中华人民共和国境内开展网络数据处理活动应当适用《网数条例》；另一方面，在中国境外处理境内自然人个人信息且符合《个人信息保护法》第 3 条第 2 款规定情形的，也应当适用《网数条例》，在中国境外开展网络数据处理活动且危害我国国家利益、公共利益的，将被依法追究责任。因此，位于境外的网络数据处理者若直接面向境内个人提供境外服务并处理个人信息，也需要遵守《网数条例》的有关规定。

二、《网数条例》的一般规定

《网数条例》第二章明确了有关网络数据处理活动的基本原则，向上综合了上位法中有关网络运营、数据处理和个人信息保护的要求，向下则统领了近年来网络数据领域发布的重要部门规章，并对网络数据处理的焦点问题（如爬虫、人工智能）划定了红线，充分体现出《网数条例》作为行政法规“承上启下”的定位。

（一）一般网络数据处理者

1. 网络数据的收集和使用：以“合法性”为前提

《网数条例》承接《数据安全法》第 32 条、《网络安全法》第 44 条等规定，重申了网络数据处理活动中的“合法性”原则，即不得非法收集、获取数据，也不得非法出售、利用数据，或为此类行为提供帮助。特别的，相较于《征求意见稿》中“不得侵害他人名誉权”、“不得危害国家安全”等细节描述，《网数条例》概括地使用了“任何个人、组织不得利用网络数据从事非法活动”的表述，给予了该条款更广泛的适用性，也能确保《网数条例》可以适应未来数字经济的不断发展以及日益复杂的数据处理活动。

2. 网络数据的存储和安全：以“主体责任”为基础

《网数条例》综合《网络安全法》第 21 条、《个人信息保护法》第 51 条等要求，提出网络数据处理者应当对“所处理网络数据的安全承担主体责任”。实际上，在近年来我国网络数据领域的监管实践中“主体责任”一词频繁出现。网络数据处理者，特别是具有庞大的用户群体并开展复杂处理活动的大型网络平台，是维护个人隐私、数据安全、网络安全的第一道防线。网络数据处理者应尽快将数据处理全生命周期的每一个环节都纳入合规管理体系，方可切实保障所处理数据的安全。对此，《网数条例》所提到的重点合规义务包括：

- 落实网络安全等级保护要求，包括开展等级保护备案和测评；
- 建立网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施；
- 开展网络安全事件管理，包括建立相关应急预案，处置网络数据安全事件，按照规定向有关主管部门报告，并视情况通知利害关系人。

需要说明的是，《征求意见稿》曾要求在发生安全事件的 3 个工作日内通知利害关系人；在发生涉及 10 万人以上安全事件的 8 个小时内报告市网信办等主管部门。鉴于国家网信办已于 2023 年 12 月发布《网络安全事件报告管理办法（征求意见稿）》，拟针对网络安全事件报告进行专门立法，因此《网数条例》并未保留《征求意见稿》的相关规定，以避免与该等部门规章产生重复或不一致，降低企业的合规负担。

3. 网络数据的传输和提供：以“权责分配”为抓手

在数字经济蓬勃发展的今天，数据处理活动很可能存在较长、较复杂的链条，涉及多方主体。因此，《网数条例》第 12 条明确要求在提供或委托处理个人信息或重要数据时通过合同约定分配双方权责义务，并强调网络数据处理者应对接收方履行义务的情况进行监督。同时，应记录提供或委托处理数据的情况并保存相关记录至少 3 年。该等要求与《个人信息保护法》第 21 条的规定基本一致，并将对接收方的监督义务扩展到委托处理以外的“提供”行为。《网数条例》这一规定将使得网络数据在不同企业之间的流动更加“有迹可循”，最终促进数据的合规流通、释放数据要素价值。

4. 网络数据处理的处理：以“国家安全审查”为防线

《征求意见稿》曾规定“数据处理者赴香港上市，影响或者可能影响国家安全的”，应申报网络安全审查。由于香港上市并非《网络安全审查办法》规定的“赴国外上市”，《征求意见稿》这一规定一度为企业赴香港上市是否有义务申报网络安全审查造成了一定程度的不确定性。

《网数条例》第 13 条概括规定，网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。这一规定一方面扫清了市场对于港股上市网络安全审查风险的顾虑，另一方面也扩展了数据领域国家安全的保障机制，除了网络安全审查外，外商投资安全审查等国家安全审查机制均可成为数据领域保障国家安全的重要防线。

（二）其他特定网络数据处理者

1. 网络产品、服务提供者

与《网络安全法》的要求基本一致，网络产品、服务提供者负有保障产品安全，报告安全漏洞的义务。不过，《网数条例》进一步要求，若网络安全漏洞可能影响国家安全、公共利益的，应当在 24 小时内向主管部门进行报告，2021 年发布的《网络产品安全漏洞管理规定》和《征求意见稿》均未涵盖该等具体要求。我们理解《网数条例》这一要求可能与近年来频繁出现的安全漏洞事件有关。为消除安全隐患并切实履行“安全主体责任”，提供网络产品和服务的企业有必要加强内部管理并建立相关的响应机制和监管报告流程。

2. 政务相关服务提供者

《网数条例》在衔接《数据安全法》和《网络安全法》的基础上，进一步明确了为政府部门、关键信息基础设施运营者等重点企事业单位提供服务时应当注意履行的义务，特别是安全和保密要求，即

“未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析”。企业为此类企事业单位提供数据处理服务的，应当采取更高更严的安全保护水平，同时加强客户数据处理相关的内部管理要求，避免在重点企事业单位客户不知情的情况下超出授权范围使用相关数据。

3. 人工智能相关企业

人工智能也是近两年来的热点议题。对此，《网数条例》从两个维度明确了相关企业的基本原则：

- 在收集的环节，若涉及使用爬虫等自动化工具采集数据，应当进行影响评估并确保不得非法入侵、不得干扰被爬取网页的正常运行。特别的，针对人工智能企业可能存在大量爬取数据用于模型训练但难以获取用户同意的这一实践难题，《网数条例》在第 24 条要求网络数据处理者删除个人信息或者进行匿名化处理。因此，当前阶段，人工智能企业在获取训练数据时，“匿名化”仍然是主要的合规手段；
- 在使用环节，相关企业应当加强对训练数据和训练数据处理活动的安全管理。这一要求与此前公布的《生成式人工智能服务管理暂行办法》相比，主要强调了数据处理活动的“安全”要求，与《网数条例》第二章的整体基调保持一致。

三、个人信息保护

《网数条例》在结合行业实践的基础上进一步细化了《个人信息保护法》关于告知同意、个人信息权利等有关规定，具体包括：

（一）新增个人信息处理的告知要求，强调个人注销账号的权利

相较于《个人信息保护法》,《网数条例》对个人信息处理规则的内容提出了如下额外披露要求:（1）个人信息保存期限或确定保存期限的方法，以及到期后的处理方式，（2）个人信息权利的具体类别，包括查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意，（3）以清单形式列明向其他网络数据处理者提供个人信息的情况。

（二）新增个人信息删除场景

《网数条例》第 24 条规定，若（1）因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，或（2）个人注销账号的，应删除或匿名化处理相关个人信息。如如上文分析，《网数条例》将自动化采集场景纳入规制范围，实则认可在应用爬虫技术或海量数据采集情形下难以在收集阶段落实告知同意的实践困难，允许网络数据处理者通过事后删除或匿名化处理等方式实现个人信息合规。

（三）细化个人信息转移的具体条件

《个人信息保护法》创设性规定了个人信息转移权，但由于缺少权利行使的法定条件，这一个人信息权利在实践中通常难以实现。未来，网络数据处理者需根据《网数条例》规定的下述个人信息转移权行使条件调整内部的权利请求响应流程，以保障个人信息主体的合法权利：（1）能够验证请求人的真实身份，（2）请求转移的是本人同意提供的或者基于合同收集的个人信息，（3）转移个人信息具备技术可行性，（4）转移个人信息不损害他人合法权益。

（四）明确境内代表信息的报送渠道

基于《个人信息保护法》第 3 条第 2 款域外适用效力而落入《个人信息保护法》管辖范围的境外网络数据处理者应在境内设立专门机构或者指定代表，并应根据《网数条例》的规定，将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门。

与此同时，《网数条例》将个人信息类重要数据的认定数量门槛从 100 万提升为 1,000 万，规定处理 1,000 万人以上个人信息的网络数据处理者，还应履行重要数据安全管理义务（第 30 条）与合并、分立、解散、破产等情形下的重要数据处置方案与接收方报送义务（第 32 条），但无需履行重要数据风险评估与报送义务（第 33 条）。

四、重要数据保护

在重要数据保护方面，《网数条例》融合了《网络安全法》《数据安全法》与《工业和信息化领域数据安全管理办法（试行）》针对关键信息基础设施以及重要数据提出的若干安全管理要求，并结合《汽车数据安全管理若干规定（试行）》在汽车行业试行重要数据风险评估机制的经验，细化了重要数据的处理者应履行的安全管理义务，重点包括：

- 制定实施网络数据安全管理制度、操作规程；
- 定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训，制定网络数据安全事件应急预案，及时处置安全风险与事件；
- 受理并处理网络数据安全投诉、举报；
- 任命符合条件的网络数据安全负责人，网络安全负责人应属于网络数据处理者管理层成员；
- 掌握特定种类或规模的重要数据的，应针对网络数据安全负责人和关键岗位的人员进行安全背景审查；
- 在提供、委托处理、共同处理重要数据前进行风险评估，除非属于履行法定职责或者法定义务；
- 重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案以及接收方信息；
- 每年度对网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告。

五、数据跨境

《网数条例》重在梳理、重申《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》（**“《数据跨境流动规定》”**）等部门规章项下个人信息、重要数据出境的合法条件及责任义务，并未实质性增设新的合规义务。

（一）新增“履行法定义务”作为个人信息出境的合法条件

《个人信息保护法》第 38 条与《数据跨境流动规定》包含若干个人信息跨境的合法条件，在此基础上，《网数条例》新增“为履行法定职责或者法定义务，确需向境外提供个人信息”作为合法路径之一，但其适用范围仍有待进一步明确。

（二）从行政法规层面认可《数据跨境新规》项下的豁免场景为个人信息出境的合法条件

以《个人信息保护法》第 38 条第 1 款第 4 项作为上位法依据，《网数条例》第 35 条将《数据跨境流动规定》规定的豁免场景纳入个人信息出境的合规路径，即为订立或履行合同所必需、人力资源管理所必需、紧急情况下保护生命健康及财产安全所必需，从行政法规层面进一步完善个人信息出境立法体系。值得注意的是，《数据跨境流动规定》第 5 条规定的“10 万以下非敏感个人信息”豁免场景并未同步被《网数条例》吸纳，我们理解该等情形属于第 35 条第（八）项的兜底情形，这一立法体例有利于主管部门根据数据出境监管实践灵活调整小规模个人信息出境的数量豁免门槛。

（三）强调数据出境规模变更对安全评估的影响

《数据出境安全评估办法》第 14 条规定，在数据出境安全评估有效期内向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息境外保存期限的，应当重新申报安全评估。《网数条例》在此基础上新增“规模”这一要素，要求网络数据处理者在数据出境安全评估明确的数据出境规模范围内开展个人信息与重要数据出境活动。

六、网络平台服务提供者义务

承袭《征求意见稿》，《网数条例》亦通过专章对网络平台服务提供者进行单独规制，并将规制对象从“互联网平台经营者”调整为“网络平台服务提供者”，虽然其具体定义仍待进一步明确。重点内容如下：

（一）相较《征求意见稿》更为宽松的义务体系

《网数条例》并未沿袭《征求意见稿》针对网络平台服务提供者繁杂严苛的规定，而是以平台对服务接入者的监管义务作为主要抓手，体现监管对企业实践的关注。其中，第 40 条明确网络平台服务提供者及智能终端设备生产者需通过合同对服务接入方进行监督管理。针对接入平台或提供预装应用程序的第三方产品服务提供者违反法定、约定义务的违规行为，服务提供者、平台方、终端设备生产方均需承担相应责任。值得注意的是，《网数条例》删除了《征求意见稿》中用户可以先行向平台索赔的规定，一定程度上减轻了平台方的赔偿责任。

（二）大型网络平台服务提供者的特殊义务

《网数条例》第 62 条从定量和定性两个角度明确了“大型网络平台服务提供者”的定义，即“注册用户 5,000 万以上或者月活跃用户 1,000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台”。在定量维度上，《网数条例》新增月活用户数作为并列的评价指标；在定性维度上，相较于《征求意见稿》侧重对市场运行的影响，《网数条例》的认定因素更加宽泛，考虑对经济、安全、社会的综合影响。针对大型网络平台服务提供者的加强义务包括：

- 每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等；
- 禁止滥用网络数据、算法以及平台规则，包括禁止违法处理用户数据、无合理理由限制用户访问或使用网络数据、对用户实施不合理的差别待遇。

七、监督管理与法律责任

《网数条例》专门设置“监督管理”章节，针对主管部门的执法活动进行规范，例如第 51 条要求有关

主管部门在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途。第 52 条要求主管部门合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。这些规定有助于提升主管部门执法活动的效率，也有利于提升社会公众对主管部门透明、公正执法的信任。

在法律责任方面，《网数条例》针对违反数据安全保护义务、数据处理危害国家安全、违反重要数据管理规范等三类违法活动分别规定了对应的罚则，其中，未依法进行国家安全审查的可能面临高达 1,000 万元的罚款。即便如此，鉴于《网数条例》第 58 条同时引致《个人信息保护法》《网络安全法》《数据安全法》等对于法律责任的规定，违反《网数条例》的行为仍可能突破条例本身明确的罚则上限，以上位法为依据处以更加严苛的处罚。

八、结论

作为《网络安全法》、《数据安全法》和《个人信息保护法》的细化和配套，最终落地的《网数条例》相较于《征求意见稿》做了大幅的简化和调整，旨在避免繁复且一定程度上有所冲突的规定给企业合规带来的困境，体现了立法者日渐成熟的监管思路。作为从业者，我们乐见《网数条例》和《数据跨境流动规定》等近期出台的法规文件一起，在坚守安全底线的同时促进数据流通利用，为企业的数字化和人工智能化转型提供更具操作性的合规指引。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com