简评《中华人民共和国网络数据安全管理条例》

作者：杨迅 | 黄欣荣

2024 年 9 月 24 日，中国国务院公布了《网络数据安全管理条例》(以下简称“**《网络数据条例》**”)，该条例将于 2025 年 1 月 1 日起施行。它标志着在《网络安全法》、《数据安全法》和《个人信息保护法》等的基础上，数据保护又有了重要的立法进展。

本文将简要概述《网络数据条例》如何发展了数据法律框架，还将讨论《网络数据条例》在创新数据业务中的应用，并概述网络数据处理者的合规义务。

一. 《网络数据条例》对数据法律体系的发展

《网络数据条例》在数据法律领域树立了一个重要的里程碑，协调了有关数据安全、数据出境和个人信息保护的分散规定，进一步细化了关键领域的规则。

2017 年，全国人大常委会通过了《网络安全法》，标志着数据相关事务大规模立法活动的开始。随后一系列有关数据的国家标准和部门规章引入。2021 年，全国人大常委会通过了《数据安全法》和《个人信息保护法》，分别加强了《网络安全法》下的数据保护和个人信息保护规定。在 2023 年，数据出境的安全评估和标准合同备案措施最终确定，而个人信息保护合规审查方面的规则则继续演进，一个全面的数据保护体系开始形成。

然而，数据法律体系仍然存在一些问题，需要进一步发展，《网络数据条例》旨在解决这些挑战。

第一，《网络数据条例》协调了保护个人信息和非个人信息的规则。以前的数据安全和个人信息保护由不同的法律和规章规制。然而，在实践中，企业经常处理结合了个人和非个人元素的数据，需要统一方式的数据立法。《网络数据条例》努力统一这两种类型的数据规则。

第二，《网络数据条例》补充了《数据安全法》和《个人信息保护法》。尽管部门规章和国家标准进行了许多立法修正，但是在数据保护方面仍然存在不足。例如，尽管《个人信息保护法》授予数据主体可携带权，但缺乏行使这一权利的详细规定。同样，《数据安全法》要求对处理重要数据进行风险评估，但没有提供进行此类评估的详细指南，《网络数据条例》填补了这些空白。

第三，《网络数据条例》根据现实世界的做法“修订”现有规则。一些与数据相关的规则过于严格，难以执行。例如，《个人信息保护法》要求只收集必要的信息，这一规定在使用自动数据收集技术时可能难以遵守，该技术可能会附带收集不必要的数据。《网络数据条例》协调这些技术或实际挑战，并建立规则以适应它们。

第四，《网络数据条例》引入了创新技术和其应用的规则。例如，《网络数据条例》第 18 条和第 19 条概述了自动化数据收集技术(例如网络爬虫)和人工智能的使用规定。

二. 《网络数据条例》的主要内容

网络数据管理规定涵盖网络数据活动的全过程，包括收集、存储、利用、处理、传输、提供、发布和删除。其中，“网络数据”被定义为通过网络处理和产生的各种电子数据。这些规定总结如下:

(一) 数据治理

《网络数据条例》在《数据安全法》和《个人信息保护法》的基础要求上，为建立有力的数据保护治理提供了详细指南。

在处理中国境内个人的个人信息方面，《网络数据条例》要求依照《个人信息保护法》在境内设立专门机构或者指定代表。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。

网络数据处理者处理 1000 万人以上个人信息的，《网络数据条例》将此类活动等同于处理重要数据。重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，有权直接向有关主管部门报告网络数据安全情况。《网络数据条例》还概述了网络数据安全管理机构的责任，包括:

(1) 制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案;
(2) 定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件;
(3) 受理并处理网络数据安全投诉、举报。

(二) 数据收集的同意规则

《网络数据条例》细致地概述了在管理个人信息管理方面征得个人同意的规则，强化了《个人信息保护法》确立的“知情同意”原则。《网络数据条例》指定了必须向个人披露的信息，包括:

(1) 网络数据处理者的名称或者姓名和联系方式;
(2) 处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响;
(3) 个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法;
(4) 个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。

此外，《网络数据条例》明确网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定:
(1) 不得通过误导、欺诈、胁迫等方式取得个人同意;
(2) 处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意;
(3) 处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意;
(4) 不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息;
(5) 不得在个人明确表示不同意处理其个人信息后，频繁征求同意;
(6) 个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。

(三) 数据传输

《网络数据条例》厘清了传输个人和非个人重要数据的规定。

《网络数据条例》规定，网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当:(1)通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等;(2)对网络数据接收方履行义务的情况进行监督;(3)向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存 3 年。网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

此外，《网络数据条例》将其范围扩展到合并、分立、解散、破产等原因下的网络数据转移，从而确保非个人数据的传输也受到与个人数据同样严格的规则的约束。因此，《网络数据条例》要求，在此类公司过渡期间网络数据接收方承担相关的数据安全保护义务。

此外，《网络数据条例》详细规定了个人行使数据可携带权的程序。对符合下列条件的个人信息转移请求，网络数据处理者应当为个人指定的其他网络数据处理者访问、获取有关个人信息提供途径:
(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。

请求转移个人信息次数等明显超出合理范围的，网络数据处理者可以根据转移个人信息的成本收取必要费用。

(四) 跨境数据传输

在与《个人信息保护法》目标保持一致的基础上，《网络数据条例》结合实践，统一数据出境的审查标准。

《个人信息保护法》概述了出口个人信息的三条主要路径：通过安全评估、标准合同备案和专业认证。它进一步授权网络安全管理机构根据需要建立额外的渠道。在 2023 年的实践中，管理层认识到审查每个数据出口场景是不切实际的，因此豁免了某些低风险出口情况的严格审查。《网络数据条例》将这些豁免情形编纂成法律，明确了以下情况：

(1) 为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；
(2) 按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息；
(3) 为履行法定职责或者法定义务，确需向境外提供个人信息；
(4) 紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；

因此，《网络数据条例》实现了一种平衡的方法，既维护了数据安全，又适应了合法和低风险的国际数据传输要求。

(五) 风险评估

与处理个人信息的规则一致，《网络数据条例》为处理重要数据时的风险评估制定了全面指南。

类似于《个人信息保护法》要求在各种情况下进行个人信息保护影响评估，《网络数据条例》对处理重要数据制定了同等的要求。重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估。风险评估应当重点评估下列内容：

(1) 提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；
(2) 提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；
(3) 网络数据接收方的诚信、守法等情况；
(4) 与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；
(5) 采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；

此外，重要数据的处理者应当每年度对其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。

风险评估报告应当包括下列内容:

(1) 网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等;

(2) 处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身;

(3) 网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性;

(4) 发现的网络数据安全风险，发生的网络数据安全事件及处置情况;

(5) 提供、委托处理、共同处理重要数据的风险评估情况;

(6) 网络数据出境情况。

(六) 安全事件管理

《网络数据条例》整合了数据处理者安全事件管理的责任，明确并加强了《数据安全法》和《个人信息保护法》先前概述的规定。义务包括:

(1) 网络数据处理者应当建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患。

(2) 网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人。

(3) 按照规定向有关主管部门报告。

(4) 网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案。

此外，网络数据处理者发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；涉及危害国家安全、公共利益的，网络数据处理者还应当在 24 小时内向有关主管部门报告。

(七) 创新技术的应用

《网络数据条例》针对创新技术的应用提出了具体规定:

(1) 爬虫技术: 针对使用爬虫技术进行数据收集的普遍做法，《网络数据条例》为爬虫技术的使用设定了界限。网络数据处理者使用自动化工具访问、收集网络数据，应当评估这些工具对网络服务带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。

(2) 人工智能: 《网络数据条例》针对提供生成式人工智能服务的网络数据处理者，要求加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。

(3) 自动化采集技术：《网络数据条例》认识到自动化采集技术可能会采集到非必要的个人信息或者超出同意范围的数据。它并未禁止自动化采集技术。相反，它要求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，网络数据处理者应当删除个人信息或者进行匿名化处理；如果删除、匿名化处理个人信息从技术上难以实现的，网络数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

(4) 自动化决策：网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

三. 企业的应对建议

《网络数据条例》的实施标志着数据保护立法领域的一个重要里程碑，企业现在必须确保准备遵守它。

(一) 风险评估程序

《网络数据条例》强调进行健全的风险评估程序的必要性，标志着向更细致和更主动的数据保护合规方法的战略转变。它要求网络数据处理者在各种情况下进行潜在风险的自我评估，从而使其合规工作适应运营的具体情况。

从本质上讲，这些运营商的任务是评估其数据处理活动或其提供的网络服务带来的风险。在发现重大风险的情况下，运营商有义务采取措施以减轻这些风险。此外，如果风险超过了数据处理活动或网络服务带来的利益，则必须重新审定是否开展该数据活动。

《网络数据条例》规定了几个需要进行风险评估的场景：

(1) 个人信息保护影响评估：在处理敏感个人信息、进行自动化决策、数据委托处理、数据提供、公开披露个人信息以及将个人信息传输给境外实体之前，必须进行评估，这是《个人信息保护法》和《网络数据条例》的要求。

(2) 重要数据风险评估：处理重要数据的运营商必须在对外提供、委托或共同处理此类数据之前进行风险评估。这一评估主要包括对数据处理的合法性、正当性和必要性以及对国家安全、公共利益和个人或组织的合法权益的潜在风险。

(3) 跨境数据传输风险评估：在跨境传输网络数据时，尤其是个人和重要数据，必须进行彻底的安全评估。这一评估必须确定传输的目的、方法和范围是否合法、正当和必要，并且必须考虑潜在风险。

(4) 定期风险评估：《网络数据条例》强制要求处理重要数据的运营商每年对其网络数据处理活动进行风险评估，并要求向相关省级或以上的主管机关提交风险评估报告。

(5) 使用自动化工具的风险评估：使用自动化工具访问和收集数据的网络数据处理者必须评估这些工具对网络服务的潜在影响，确保不干扰或侵入他人的网络。

尽管需要风险评估的不同场景多种多样，但考虑的基本因素是一致的。将风险评估程序整合到运营商的内部管理系统中可以简化流程。这种整合将允许在常规内部审查和决策过程中进行评估，防止对相同因素的重复评估，从而提高整体效率。

(二) 合规审查

《网络数据条例》要求运营商进行自主合规审查，并将合规考虑纳入产品开发生命周期。这一规定加强了《个人信息保护法》对个人信息保护合规审计的要求，《网络数据条例》重申并扩大了这一必要性。处理重要数据的风险评估程序也包括评估遵守数据处理规定的情况。

此外，《网络数据条例》坚持网络产品和服务的合规性。运营商必须保证其产品符合强制性国家标准，并积极解决任何发现的漏洞。此外，对于向公众提供网络产品和服务的运营商，建立接收投诉和报告的渠道是必要的。这意味着运营商必须将这些渠道纳入其产品和服务的设计阶段。

网络产品和服务的运营者有义务遵守接入平台的要求和分发服务的第三方协议。根据《网络数据条例》，网络平台服务提供者有义务明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促该等义务的执行。同样，提供应用程序分发服务的服务提供者，有义务建立应用程序核验规则并开展网络数据安全相关核验。不遵守这些规定可能导致相关产品从平台断开连接或暂停其销售。因此，除法律和监管要求之外，运营者还必须确保其网络产品或服务的设计符合平台规则和分销规则。

(三) 保留记录

根据《网络数据条例》，数据处理者有法律义务保留详细记录，以便于政府检查。这些记录不仅有助于履行法律义务，而且可能作为关键证据，有助于应对因数据相关事件而产生的索赔。
根据《网络数据条例》的规定，数据处理者必须保留以下记录:

(1) 数据处理活动记录。包括: (a)对于经同意收集的个人信息，同意的记录;(b)对于数据提供、委托或共同处理数据，与数据接收方的合同记录以及监督数据接收方活动的文件;以及(c)对于处理重要数据，年度风险评估的记录。

(2) 合规审查记录。包括: (a)对于个人信息处理，合规审计的记录;(b)对于可能影响国家安全的任何数据处理活动，国家安全审查的记录;以及(c)证明履行尽职调查的全面风险评估报告的完整收集。

(3) 事件管理记录。包括: (a)应急计划以及与该计划相关的培训会议记录;(b)执行应急计划以防止损失扩大和减轻风险的文件。

这些详尽的记录保留要求确保数据处理者透明、负责，并能够阐释其运营过程中可能出现的任何问题。

(本文系作者 A Brief Review of PRC Administrative Regulation of Network Data Security 一文的中文翻译)

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野