Cooley科律

# 中国年末发布多项网络与数据安全重要法规征求意见稿

2025 年年末，中国在数据保护和网络安全领域再度迈出重要步伐。过去一个月，中国监管机构陆续发布了多项重要法规征求意见稿，面向公众征求意见。这些举措凸显了中国在应对日益严峻的数据安全风险方面投入的持续努力，以及对《网络安全法》、《数据安全法》和《个人信息保护法》强化执法力度的决心。

本文将聚焦三项最新发布的重要法规及其潜在影响：

- 《大型网络平台个人信息保护规定（征求意见稿）》（2025 年 11 月 22 日发布）
- 《公安机关网络空间监督检查办法（征求意见稿）》（2025 年 11 月 29 日发布）
- 《网络数据安全风险评估办法（征求意见稿）》（2025 年 12 月 6 日发布）。

## 《大型网络平台个人信息保护规定（征求意见稿）》（“LOP 规定”）

### 1. 大型网络平台（LOP）的适用范围

LOP 规定适用于在中国境内建设、运营的大型网络平台。国家互联网信息办公室（“网信部门”）与国务院公安部门等有关部门将综合考虑以下因素，认定平台是否属于 LOP：

- 注册用户 5,000 万以上或者月活跃用户 1,000 万以上；
- 提供重要网络服务或者经营范围涵盖多个类型业务；
- 掌握处理的数据一旦被泄露、篡改、损毁，对国家安全、经济运行、国计民生等具有重要影响；
- 国家网信部门、国务院公安部门规定的其他情形。

被认定为 LOP 的平台将被纳入由国家网信部门会同国务院公安部门等有关部门制定并动态更新的 LOP 目录中。

### 2. 指定“个人信息保护负责人”（DPO）

LOP 应当指定 DPO，并公开其联系方式。DPO 应当由 LOP 的管理层成员担任，具有中华人民共和国国籍，无境外永久居留权或者长期居留许可。此外，DPO 需具备个人信息保护专业知识且从事相关工作五年以上。

DPO 的职责包括但不限于：指导 LOP 合规开展个人信息处理活动；参与 LOP 个人信息处理事项相关决策，并对个人信息处理事项具有否决权；负责对个人信息处理活动以及采取的保护措施等进行监督；以及组织制定专门的未成年人个人信息处理规则。LOP 规定赋予 DPO 直接向国家网信部门、有关主管部门报告有关情况的权利。

### 3. 数据本地化与跨境传输要求

LOP 应当将在中国境内运营中收集和产生的个人信息存储在境内。确需向境外提供的，应当符合国家数据出境安全管理有关规定。此外，LOP 规定对存储数据的数据中心提出具体要求，包括：

- 数据中心设立在中国境内；
- LOP 具有中华人民共和国国籍，无境外永久居留权或者长期居留许可；
- 数据中心安全性符合国家有关标准要求。

LOP 还应当向国家网信部门等有关部门报送存储个人信息的数据中心的基本信息，包括管理团队和管理架构、内部个人信息保护管理制度、采取的安全措施、与第三方数据中心签署的合同文本等。

## 《公安机关网络空间监督检查办法（征求意见稿）》（“公安机关监督检查办法”）

新的公安机关监督检查办法确立了公安机关（即中国警察系统及公安局）的网络空间监督检查程序与标准，有望替代 2018 年发布的《公安机关互联网安全监督检查规定》。

### 1. 适用范围

公安机关监督检查办法允许公安机关对下列对象依法开展监督检查：

- 提供互联网接入、数据中心、内容分发、域名服务、信息服务等的互联网服务提供者；
- 公共上网服务提供者（如提供公共 Wi-Fi 连接的酒店、医院或其他公共场所）；
- 网络运营者（即拥有或使用网络来运营或提供服务的主体）及其建设者、维护者；
- 关键信息基础设施运营者及其建设者、维护者；
- 网络产品、服务的提供者；
- 数据处理者及个人信息处理者（即独立决定数据或个人信息处理目的与方式的主体）。

### 2. 公安机关检查权限

根据公安机关监督检查办法，公安机关可以通过“网络信息巡查”、“信息审核能力测试”（未明确定义，可能指内容管理能力）、漏洞扫描等方式，对被检查对象的网络安全、“信息安全”（未明确定义，可能指在线内容安全）及数据安全等情况进行线上及现场检查，以发现风险隐患。公安机关应当对被检查对象履行法定义务等情况进行监督检查，重点检查以下内容：

- 是否依法制定并落实网络安全、“信息安全”、数据安全管理制度和操作规程；
- 是否依法记录并留存用户注册信息和上网日志信息；
- 是否依法履行网络安全等级保护制度（MLPS）；
- 是否依法采取防范计算机病毒和网络攻击、网络侵入等技术措施；
- 是否依法为公安机关维护国家安全、防范调查恐怖活动、侦查犯罪等提供技术支持和协助。

Cooley 科律

## 《网络数据安全风险评估办法（征求意见稿）》（“风险评估办法”）

风险评估办法将网络数据安全风险评估定义为“对网络数据[i]和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动”。

处理“重要数据”[ii]的网络数据处理者[iii]（“重要数据处理者”）应当每年度对其网络数据处理活动开展风险评估。鼓励处理一般数据的网络数据处理者（即不处理“重要数据”的其他数据处理者）至少每 3 年开展一次风险评估。网络数据处理者可以自行或者委托第三方评估机构开展风险评估。除网络数据处理者主动开展的风险评估外，省级以上网信部门和有关部门发现网络数据处理者有以下情形之一的，应当要求其委托第三方评估机构开展风险评估：

- 网络数据处理活动存在较大安全风险的；
- 发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的；
- 网络数据处理活动可能危害国家安全、公共利益的；
- 国家网信部门或者有关部门规定的其他情形。

重要数据处理者开展年度风险评估应当按照风险评估办法附件模板编制评估报告，并报送有关主管部门（如重要数据处理者的主管部门不明确的，向网信部门报送）。省级以上网信部门和有关部门可对网络数据处理者的评估报告真实性、准确性进行抽查核验，网络数据处理者应当配合开展抽查核验。

## 后续措施

违反上述三项法规的行为将依据《网络安全法》、《数据安全法》和《个人信息保护法》的规定予以相应处罚。向中国客户和用户提供服务的公司应评估这些法规的适用性，并密切关注其最新进展。

---



作者：鲍家兴、于智精

[i] “网络数据”指通过网络处理和生成的电子数据。

[ii] “重要数据”指特定领域、特定群体或特定区域的数据，或达到一定准确性及规模的数据，一旦被篡改、破坏、泄露或非法获取使用，可能直接危及国家安全、经济运行、社会稳定、公共卫生与安全。

[iii] “网络数据处理者”指独立决定数据处理目的与方式的个人或组织。