张弛有度：把握《网络安全审查办法》的边界与尺度

2022年1月4日，国家互联网信息办公室等十三部门联合修订发布了《网络安全审查办法》（“**2022**版”），新办法自2022年2月15日起施行。2022版的修订以《数据安全法》正式施行为背景，以保障网络安全和数据安全，维护国家安全为主要目的，一方面对网络安全审查范围的扩张秉持了审慎的态度，将“网络平台运营者”（而非“数据处理者”）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；另一方面对于赴国外上市这一焦点问题给予了明确回应，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。

《网络安全审查办法》尘埃落定。市场也精准地把握到了2022版的修订精髓，即：国外上市活动所涉数据处理行为对国家安全的影响或可能影响。本文从网络安全审查与数据安全审查的关系、需要主动申报网络安全审查的情形、网络平台运营者的界定、国家安全风险因素的理解这四大角度，对2022版的修法重点进行解读。

一. 依托既有网络安全审查制度，先行解决数据处理活动中已显现的国家安全隐患

2022版明确了网络安全审查制度和数据安全审查制度系两套制度，但现实中存在重叠之处。此次通过修订既有网络安全审查制度，着力解决现阶段数据处理活动中已显现的国家安全隐患。同时，为未来数据安全审查的进一步立法留有空间，达到提供法律手段和稳定市场预期的综合目标。

《数据安全法》规定了数据安全审查制度。《网络安全审查办法（修订草案征求意见稿）》（“**2021**版”）开宗明义将“数据处理者开展数据处理活动”纳入网络安全审查的适用范围，导致有观点认为数据安全审查制度系为网络安全审查所包含。2022版的两点变化：

1. **2022**版第**2**条将网络安全审查的适用前提之一由**“**数据处理者**”**修改为**“**网络平台运营者**”**开展数据处理活动，影响或可能影响国家安全的。考虑到在《网络数据安全管理条例（征求意见稿）》（“《条例》”）中“互联网平台运营者”属于一类特殊的“数据处理者”[1]，网信部门可能有意限缩了网络安全审查所规制的数据处理主体范围。值得注意的是，虽然赴国外上市场景下的主动申报主体限定为“网络平台运营者”，但监管依职权提出审查仍需着眼于数据处理活动是否影响或可能影响国家安全，此处所涉及主体范围可能包含其他类型的数据处理者。
2. **2022**版第**22**条增加国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定的要求。“另有规定，同时符合”的表述不同于“另有规定，依照规定执行”或者“另有规定，以本规定为准”。该条款说明数据安全审查制度具有独立性，未来对其审查事项应该会有进一步规定。

数据安全审查系一项法律制度，必定难以一蹴而就，但就合规实践而言市场仍对此

重要制度的架构有所期待：第一是合规成本问题。尽管各类安全审查可能有着不同的规范目的和归口部门，但从提高监管和市场效率的角度，仍期待后续立法能够避免审查程序的叠床架屋，尽量让市场主体因为同一事项“最多跑一次”。第二是立法技术问题。国家对网络安全审查的规定修改暂时落地，未来对数据安全审查另有规定的，需同时符合。该等情况下，避免相互间的逻辑矛盾情况可能会成为新的课题。

二．赴港上市无需主动申报审查，但主动排除数据安全风险或将成为必修课

2022版下需要主动申报网络安全审查的只有两种情况：（1）关键信息基础设施（“**CII**”）运营者采购网络产品和服务，影响或者可能影响国家安全的；（2）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。

“赴港上市**”**无需**“**主动申报**”**，但不等于无需考虑数据安全风险。《条例》将“数据处理者赴香港上市，影响或可能影响国家安全”纳入网络安全审查主动申报情形，虽然展现出对赴港上市的申报要求明显宽松于赴国外上市的监管态度，但因何谓“影响或可能影响国家安全”暂不明确而引发一定困惑。2022版未将“赴港上市”纳入“主动申报”范畴，但仍需考虑数据安全风险，原因可能在于：（1）监管认为影响或者可能影响国家安全的数据处理活动，可依职权开展网络安全审查。无论国外亦或赴港上市必然包含数据处理行为，其中的数据出境更是备受关注；（2）相较于主动申报，企业对于依职权审查的掌控度较低，一旦发生则微观于上市进程、宏观于企业运营必将产生重大影响，属于企业运营中难以承受之重；（3）《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》要求境内企业境外发行上市的，应当向证监会履行备案程序，而证监会在备案时应当会考察网络安全审查的适用问题。

2022版新增关于审查期间采取风险预防和消减措施的规定，[2]初步理解适用情形为依职权审查时。该等措施实践中可能表现为要求网络产品下架、停止新用户注册等。2022版未说明系何种启动方式下的“审查期间”，但考虑到本款系增设于依职权启动审查情形之下，依职权启动审查场景下企业被要求采取上述措施的可能性较高。

数据剥离方案对于降低国家安全影响有积极意义，但能否规避网安审查需依据剥离效果判断。境内企业赴境外上市前主动剥离境内数据，属于响应《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》合规要求[3]的积极举措。采取该等方案应有助于通过网络安全审查，但若期待以此规避网安审查则恐怕需要满足苛刻条件：（1）业务层面不具有处理被剥离数据的诉求，或仅于限定场景有所诉求且具备严格管控该等处理行为的机制；（2）技术层面不具有接触、使用该等数据的可能性；（3）托管方需具备保持数据处于隔离状态的技术能力与公信力。

三、**“**网络平台运营者**”**定义有待明确，**“**基础**”**与**“**连接**”**或为关键特性

2022版中未就**“**网络平台运营者**”**给出定义，如何界定网络平台运营者将成为实务的争点问题之一。

“服务的基础性**”**与**“**服务的连接性**”**可能成为界定平台的标准。网信部门与市场监管部门在各自所主导的立法中，对界定何为“平台”体现出了不同的路径偏好：网信部门侧重于从后果出发，更加关注**“**服务的基础性**”**，将信息发布、社交、交易、支付、视听等五种日常生活中高频使用的互联网服务界定为典型的“互联网平台服务”，并通过界定“平台服务”进而界定“平台”[4]；而市场监管部门侧重于从本质出发，更加关注**“**连接多方**”**的服务特性，将“互联网平台”界定为“通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态”[5]。

需注意的是，根据“连接”标准，在《电子商务法》[6]、《关于平台经济领域的反垄断指南》[7]等法律法规中的“平台”往往限于主体与主体之间的连接。但在市场监管总局10月所发布的《互联网平台分类分级指南（征求意见稿）》中，“平台”不再限于提供主体之间的连接，还可能包括人与物的连接（如云计算被视为“人与计算能力”的连接）[8]，如类似表述最终得以通过，则“平台”的范围可能进一步扩大。

在判定是否构成网络平台运营者时，**“**基础**”**与**“**连接**”**究竟是取其交集亦或并集，有待进一步观察，但建议具备**“**基础**”**或**“**连接**”**特性的网络运营者提前开展相应合规部署。“网络平台运营者”这一概念的弹性为监管机关提供了调节的“工具”，通过将“数据处理者”限缩为“网络平台运营者”，2022版在回应现实执法需求、提供执法依据的同时，也在监管机关干预市场活动的授权问题上秉持了克制的态度。监管机关在未来的实践中将如何界定“网络平台运营者”，尚不确定，企业不宜仅以自身不属于“网络平台运营者”为理由而认为无需进行网络安全审查。

四．国家安全风险因素有所扩张，但仍聚焦于有价值的数据和高风险的数据处理场景

“影响或者可能影响国家安全**”**始终是网络安全审查的前提条件与落脚点。从《国家安全法》初步构建针对网络信息技术产品和服务的国家安全审查[9]，到《网络安全法》确立针对CII运营者采购网络产品和服务的国家安全审查[10]、《数据安全法》确立数据安全审查制度[11]，再到最新的《网络安全审查办法》进一步细化针对CII运营者采购网络产品和服务、网络平台运营者开展数据处理活动的网络安全审查[12]，上述法律法规均强调审查对象对于国家安全的现实影响或潜在影响。

《网络安全审查办法》具象化了**“**影响或者可能影响国家安全**”**的考量因素。[13]对于网络安全审查中重点评估的国家安全风险因素，2021版在原《网络安全审查办法》（“**2020**版”）的基础上增加了针对数据处理活动的考量因素，2022版对2021版进行了微调，主要包括如下值得关注的特点。

1. 持续聚焦核心数据、重要数据、大量个人信息。2021版、2022版均对网络安全审查所关心的数据进行了限缩，核心数据、重要数据、大量个人信息这三类数据因其性质或数量，更有可能影响国家安全。并且，网络安全审查重点关注这三类数据被窃取、泄露、毁损、非法利用、非法出境的风险。

2. 重点关切赴国外上市活动。2021版、2022版均特别强调了赴国外上市的情形。在考察CII及上述三类数据因赴国外上市而被外国政府影响、控制、恶意利用的风险时，2022版将2021版的“上市后……的风险”改为了“上市存在……的风险”，即，网络安全审查也将考察上市准备与申请阶段的风险。此外，2022版除前述与国家安全强相关的风险外，还需考察网络信息安全风险，而《网络安全法》第四章“网络信息安全”涵盖了个人信息保护、网络诈骗、信息内容等多方面的规定，存在较大的解释空间。

3. 适度扩张对于网络安全和数据安全的考量。对于兜底性质的其他因素，2020版主要强调了CII安全，2021版增加了数据安全，2022版又增加了网络安全。2022版在三处（立法意旨与保护法益、国家安全风险因素、网络产品和服务的定义）均新增了对“网络安全和数据安全”的考量与保护[14]，而上位法《网络安全法》《数据安全法》均有着丰富的内涵。2022版将较为抽象的“国家安全”进一步落地至网络安全和数据安全，但其引申的边界有待实践的检验。

[1] 《网络数据安全管理条例（征求意见稿）》
第73条 本条例下列用语的含义：
（九）互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

[2] 《网络安全审查办法》（2022版）第16条网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。 为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

[3] 《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》第8条境内企业境外发行上市的，应当严格遵守外商投资、网络安全、数据安全等国家安全法律法规和有关规定，切实履行国家安全保护义务。涉及安全审查的，应当依法履行相关安全审查程序。 国务院有关主管部门可以要求剥离境内企业业务、资产或采取其他有效措施，消除或避免境外发行上市对国家安全的影响。

[4] 《网络数据安全管理条例（征求意见稿）》
第73条 本条例下列用语的含义：
（九）互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

[5] 《国务院反垄断委员会关于平台经济领域的反垄断指南》
第2条 相关概念：
（一）平台，本指南所称平台为互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

[8] 《互联网平台分类分级指南（征求意见稿）》
2.1 分类依据
对平台进行分类需要考虑平台的连接属性和主要功能。平台的连接属性是指通过网络技术把人和商品、服务、信息、娱乐、资金以及算力等连接起来，由此使得平台具有交易、社交、娱乐、资讯、融资、计算等各种功能。

[9]《国家安全法》第59条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

[10]《网络安全法》第35条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

[11]《数据安全法》第24条第1款 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

[12]《网络安全审查办法》（2022版）第2条第1款 关键信息基础设施运营者采购网络产品和服务，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的，应当按照本办法进行网络安全审查。

13《网络安全审查办法》（2022版）
第10条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：
（一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；
（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；
（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；
（五）核心数据、重要数据或者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；
（六）上市存在关键信息基础设施、核心数据、重要数据或者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；
（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。
《网络安全审查办法（修订草案征求意见稿）》（2021版）
第10条 网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑以下因素：
（一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险；
（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；
（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；
（五）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；
（六）国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险；
（七）其他可能危害关键信息基础设施安全和国家数据安全的因素。
《网络安全审查办法》（2020版）
第9条 网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，主要考虑以下因素：
（一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；
（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；
（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；
（五）其他可能危害关键信息基础设施安全和国家安全的因素。

[14]《网络安全审查办法》（2022版）
第1条 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。
第10条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：……
（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。
第21条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。