

最新监管形势下中资企业境外上市相关法律问题简析

作者：蓝洁 高巍 霍超

引言

近日，相关监管部门先后对“滴滴出行”、“运满满”、“货车帮”、“BOSS直聘”等APP及其运营企业实施了网络安全审查措施，并拟出台或修订配套的制度规则，以进一步加强对境外上市企业网络安全、数据安全等方面合规监管要求。中共中央办公厅、国务院办公厅于2021年7月6日印发的《关于依法从严打击证券违法活动的意见》（以下简称“《意见》”）亦明确提出要“加强中概股监管”。本文旨在结合前述监管动态对新形势下中资企业境外上市涉及的相关法律问题初步探讨和简要分析。

一.关于赴美上市跨境信息提供的监管问题

赴境外上市的中资企业须同时适用境内及上市地两地的相关监管要求。其中，针对赴美上市的中资企业，中美两地监管要求对相关中介机构的工作底稿及其他相关文件、资料、信息等的跨境提供存在一定程度的冲突，相关要求主要如下：

中国监管相关规定	
数据安全法 2021年6月10日发布， 2021年9月1日生效	第三十六条：中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。
证券法（2019修订） 2019年12月28日发布， 2020年3月1日生效	第一百七十七条：境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得向境外提供与证券业务活动有关的文件和资料。
关于加强在境外发行证券与上市相关保密和档案管理工作的规定 2009年10月20日发布并生效	1. 证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内。工作底稿及国家秘密、国家安全或者重大利益的，不得在非涉密计算机信息系统中存储、和传输；未经有关主管部门批准，也不得将其携带、寄运至境外或者通过信息技任何手段传递给境外机构或者个人。 2. 境外证券监管机构提出对境外上市公司以及证券公司、证券服务机构进行非现场的，涉及国家秘密的事项、档案管理的事项、以及其他需要事先经其他有关部门的事项，境外上市公司、证券公司和证券服务机构均应当事先报相关主管部门批准才能提供给相关资料。
美国监管相关规定	
外国公司问责法案 2020年12月18日生效	1. 若在美上市公司聘用的审计师有以下情形，则上市公司需要向SEC提交文件以证没有被外国政府所有或控制，且相应审计报告包含年度被认定为“未检查年”：（1）审计师在外国司法辖区有办公室或者分支机构；且（2）由于该外国司法辖区所采立场，导致PCAOB无法完全检查或调查该审计师的，。 2. 如果连续三年存在“未检查年”的发行人，则该发行人的证券被禁止在美国证券交或受SEC监管的柜台市场等场所交易；发行人向SEC确认其将按要求任用可PCAOB完全检查的审计师后，SEC可以解除交易限制；解除后再次发生“未检查”形的，SEC将再次施加限制，直至最后一次限制满五年后，且发行人证明其已任受PCAOB检查的审计师的，可取消禁令。 3. 发行人需要在“未检查年”的年报中披露其受外国政府实体控制的股比、发行人或实体中含有执政党官员的姓名、发行人章程是否载有执政党章程的相关内容等。
萨班斯法案（其中对美国1933年、1934年证券交易法作出修订） 2002年7月30日生效	1. 会计监察委员会（PCAOB）有权要求审计师或任何有关人员，不论位于何处，提交工作底稿和文件；PCAOB可以检查审计师或有关人员的帐册、记录，以便确定的文件或材料是否准确。 2. 若上市企业的审计师基于外国会计师事务所的服务签发审计报告的，外国会计师事务所以及上市企业的审计师被视作同意向SEC提供审计相关的工作底稿，且外国会计师事务所被视作同意服从美国法庭关于提供工作底稿的命令。

由上述对比可见，中国监管要求为，若境外上市企业及其证券服务机构拟向境外提供任何涉及国家秘密、证券业务以及其他涉及前置审批事项的工作底稿及资料时，应当按照中国证券监管机构认可的口径，通过监管合作渠道提供交换信息。而美国SEC则要求赴美上市的中资企业所聘用的审计师必须按照SEC的监管要求，提供SEC认为必要的相关审计底稿文件。

《意见》中明确，“加强跨境监管合作。完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。加强跨境信息提供机制与流程的规范管理。坚持依法和对等原则，进一步深化跨境审计监管合作。”由此可见，中国有关监管部门将就境外上市中资企业的信息、资料跨境提供等事项与境外监管机构深化跨境合作。

二.拟修订的《网络安全审查办法》对企业境外上市的主要影响

基于近期对赴国外上市企业开展网络安全审查的规则需求，国家互联网信息办公室（以下简称“网信办”）于2021年7月10日公布了《网络安全审查办法（修订草案征求意见稿）》（以下简称“《办法意见稿》”）。结合前述《办法意见稿》的相关内容，计划境外上市的中资企业可能需要关注以下方面的事项：

1、触发网络安全审查的标准

根据《办法意见稿》，触发网络安全审查主要包括下列情形：（1）因关键信息基础设施运营者采购网络产品和服务而影响或可能影响国家安全的；（2）因数据处理者开展数据处理活动而影响或可能影响国家安全的；（3）掌握超过100万用户个人信息的运营者（即“关键信息基础设施运营者”或“数据处理者”）赴国外上市的。存在以上任意情形的，相关企业应当主动申报审查并提交相关材料。

此外，从网信办关于对“滴滴出行”等主体启动网络安全审查的公告内容看，《网络安全审查办法》赋予了网信办主动实施审查的权利，即便境外上市企业未主动申报进行审查，若网信办等监管机构认为其上市安排或经营活动存在国家安全或网络安全风险的，仍可依职权主动实施审查。

2、“关键信息基础设施运营者”与“数据处理者”的关系

“关键信息基础设施运营者”（即CIIO）是源自《网络安全法》的概念，就具体定义而言，“国家关键信息基础设施”是指一旦遭到破坏、丧失功能或数据泄露可能严重危害国家安全、国计民生、公共利益的信息设施，其运营者一般包括以下几类主体：（1）政府机关和能源、金融、卫生医疗、教育、环境保护等领域的单位；（2）信息网络以及提供云计算、大数据等单位；（3）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；（4）广播电台、电视台、通讯社等新闻单位；（5）其他重点单位。

“数据处理者”则源于《数据安全法》，具体指对数据实施收集、存储、使用、加工、传输、提供、公开等行为的主体。

相较于CIIO，“数据处理者”的范围更广泛，在CIIO开展数据收集、传输、

提供等行为时，其同样属于“数据处理者”而受到《数据安全法》的规制。

3、对“掌握超过100万用户个人信息”的理解

《办法意见稿》中将“掌握超过100万用户个人信息”作为赴国外上市企业触发网络安全审查的判断标准。“100万用户个人信息”，不论指用户数量，或指个人信息数量，对于运营者而言并不难判断。但对于构成“掌握”的标准，在现有规则尚未明确的情况下，容易导致不同的理解。若将用户个人信息相关业务进行剥离，委托他人管理，是否不构成“掌握”个人信息？相反，若仅为他人提供信息存储、数据保管服务，不进行数据使用、加工的，是否仍会被认定为“掌握”？

笔者认为，判断运营者是否“掌握”用户个人信息，关键在于其能否控制和处理该等信息数据。据此，将用户信息数据相关业务剥离到上市公司体外开展，可以在一定程度上解释上市公司对于该等信息数据未形成控制，从而降低境外监管机构以上市公司作为直接监管对象而要求其提供该等信息数据的可能。但该等方式能否获得监管认可，仍需结合《办法意见稿》正式落地文件中对于“掌握”标准的界定和实操中的监管情况。

需要注意，按照《办法意见稿》的规定，即便上市企业对用户个人信息未达到“掌握”的标准，仍有可能因参与数据处理（使用、传输、提供同样属于数据处理行为）、或因需向上市地监管机构跨境提供底稿资料而被网信办依职权主动实施安全审查。

4、对“赴国外上市”的理解

与《证券法》、《国务院关于股份有限公司境外募集股份及上市的特别规定》、《国务院关于进一步加强在境外发行股票和上市管理的通知》（以下简称“97红筹指引”）等文件中使用的“境外”上市表述不同，本次《办法意见稿》中使用了“赴国外上市”、“国外上市”的表述，而该等表述在此前涉及企业境外上市的相关法规、规章、规范性文件中并不常见。

基于该等区别表述，且鉴于中国对香港特别行政区行使主权，以及此前颁布的《香港特别行政区维护国家安全法》中对于危害国家安全行为已有严格的刑则规定，因此有市场人士将《办法意见稿》中采用“赴国外上市”的表述解读为赴香港地区上市不适用《办法意见稿》。笔者倾向于认同该观点，同时，鉴于《办法意见稿》中“赴国外上市”的表述已引起广泛热议，立法机构在正式出台的修订稿中对赴香港特别行政区上市是否需参照适用应会作出进一步

说明。满足新规规定标准的赴港上市企业是否需申报网络安全审查，仍需以最终落地的修订稿为准作出判断。

5、《办法意见稿》落地后对境外上市的主要影响

结合上述分析，笔者认为，《办法意见稿》修订生效后，可能对境外上市造成的主要影响如下：

（1）对拟上市企业而言，若涉及大量用户个人信息处理业务的，需结合最终落地规定、网信办等监管机构对“掌握超过100万用户个人信息”标准的解读、以及市场案例实操情况，判断是否需调整用户信息数据收集处理的业务模式，若监管认可将用户信息剥离至上市公司体外运营或进行托管作为解决方案的，拟上市企业可结合监管要求做相应调整，但同时需注意该等调整对公司营收情况、业务和人员稳定性的影响是否符合上市地的相关要求。

（2）对证券服务中介机构而言，在上市准备工作开展过程中，需对网络安全保护、数据合规、个人信息保护等方面开展更为详细、全面的尽职调查，保荐机构、发行人境内律师等证券服务机构需结合《数据安全法》、《个人信息保护法》、《网络安全审查办法》的出台和修订情况就相关法律问题发表专业意见。

（3）就上市地点的选择来说，若最终落地的《网络安全审查办法》修订稿中明确赴香港地区不适用该规定的，则相较于赴美等国外上市的企业，更加利好选择香港作为上市地的企业。

三、红筹架构企业到境外上市的监管趋势

《意见》中明确提出，“加强中概股监管。切实采取措施做好中概股公司风险及突发情况应对，推进相关监管制度体系建设。”

在现有监管体系下，属于“97红筹指引”中规定的中资控股境外注册公司拟在境外上市的，需按照规定取得相关政府部门的批准，以及报中国证监会进行核准或事后备案。“97红筹指引”颁布的背景主要是为了规范中资企业（特别是国有企业）通过境外窗口公司将境内资产转移到境外上市的行为，并且其规制的境外注册中资企业通常被理解为“境内企业”出境在境外投资设立的企业。此外，针对涉及境内权益的境外公司在境外发行股票和上市，在一定时期内，发

行人需通过其境内律师获得证监会出具的“无异议函”；随着2002年《行政许可法》的出台，国家明确规定未经法律和行政法规授权，不设行政许可项目，“无异议函”机制也被取消。目前，实践中，民营企业则通常是通过境内个人出境设立境外持股和上市平台的“小红筹”架构（包括利用VIE结构）申请境外上市，该等“小红筹”企业海外上市不再向境内证券主管部门履行审批程序。

《意见》的出台释放了一个明确的信号：“小红筹”企业的海外上市将会再度纳入境内监管的范围。《意见》同时要求：“建立健全资本市场法律域外适用制度。抓紧制定证券法有关域外适用条款的司法解释和配套规则，细化法律域外适用具体条件，明确执法程序、证据效力等事项。加强资本市场涉外审判工作，推动境外国家、地区与我国对司法判决的相互承认与执行。”事实上，2019年修订的《证券法》已对《证券法》的域外适用做出了明确规定，明确在我国境外的证券发行和交易活动，扰乱我国境内市场秩序，损害境内投资者合法权益的，将依照《证券法》追究责任。

笔者认为，《意见》的出台背景不仅仅有国际局势的变化、数据和网络安全的考量，也反应了中国的资本市场以及“中概股”在迅猛发展二十多年之后日益强大的市场影响力，以及历史过程中部分企业出现的证券违法行为对中国的资本市场和投资者的影响。这种影响跨越国界，给监管提出了更高的要求。因此，除了网络安全审查、数据处理等方面的监管之外，中国证券监管部门拟对“小红筹”企业采取何种监管方式，值得我们观察和期待。

四、拟境外上市企业的应对措施

1、对于已提交申请文件的赴港上市企业，我们理解，《办法意见稿》对其上市安排的影响有限，在最终落地的办法对赴港上市企业不设置额外审批要求的前提下，仍可按照原上市计划推进项目，但是发行人和中介机构也应密切关注拟议政策的落实和变化。

2、对于已提交申请文件的赴美、欧、新加坡等地上市的企业，建议尽快咨询境内外律师关于《办法意见稿》及近期监管要求对上市安排可能构成影响的专业意见，结合自身业务和数据情况综合判断风险，补充相关数据核查尽调并在申请文件中增加相关披露，如有必要可与境内网络安全审查部门积极沟通，并结合监管要求调整上市安排，避免因监管风险对境内经营造成实质影响。若

企业上市过程中《办法意见稿》按其现有内容落地生效的，达到审查标准的企业仍需在上市前按照办法要求进行申报并完成网络安全审查工作。

3、对于仍处于境外上市前期筹划阶段的企业，可从以下方面降低监管政策变化可能造成的影响：

（1）谨慎选择上市地点，评估A股、H股、以及红筹港股上市的可行性。若搭建境外架构上市为最优选择的，需综合判断不同上市地的监管风险，重视香港资本市场的特殊地位，尽可能降低因国际形势变化等因素对上市安排可能造成的不确定性；

（2）结合监管要求开展企业数据安全、网络安全的自查工作，根据自身数据属性就境外上市安排与境内监管机构积极沟通，为安全审查预留充足时间；

（3）持续关注监管机构对于网络安全审查以及红筹境外上市的监管政策变化情况，以便及时作出应对措施。

4、对于赴美上市企业而言，在中美之间就底稿资料跨境提供的监管要求尚需进行磋商的背景下，拟赴美上市的中资企业若无法针对向境外提供底稿资料的范围作出准确判断时，建议事先与中国境内监管机构充分沟通，确认向境外提供审计工作底稿及资料的具体监管要求。

结语

在监管趋严的态势下，对于中资企业而言，除需谨慎选择上市地点外，更重要的，一是要强化内部控制和合规管理，落实诚信责任，切实提升信息披露的质量，防范并尽量减少证券诉讼风险；二是尽快构建自身关于网络安全、数据合规的管理体系，通过内部人员、外部顾问等对公司数据合规情况作出全面梳理，建立必要的网络、数据安全应急机制，使自身能够在互联网和大数据时代从容应对外部监管环境的变化。

2021-07-16