



它们为何被实施“网络安全审查”

赴美国上市涉及我国信息出境,数据安全再次成为关注焦点

掌握大量用户隐私数据 关联关键信息基础设施

“滴滴一下,美好出行”。作为中国最大的出行平台,“滴滴出行”的下架整改,让这句广告词变了滋味。

7月4日,国家互联网信息办公室发布公告称,经检测核实,“滴滴出行”App存在严重违法违规收集使用个人信息问题。“滴滴出行”随后回应称,将严格按照有关部门的要求下架整改,并积极配合网络安全审查。目前,“滴滴出行”App已暂停新用户注册,并下架整改。

一天后,网络安全审查办公室发布关于对“运满满”“货车帮”“BOSS直聘”启动网络安全审查的公告。

对这几家企业启动网络安全审查,原因是什么?

记者查看“运满满”企业官网时发现,该公司成立于2013年,隶属于江苏满运软件科技有限公司,是国内基于云计算、大数据、移动互联网和人工智能技术开发的货运调度平台。官网称,“运满满已经成为全球出类拔萃的整车运力调度平台和智慧物流信息平台”。“货车帮”公司官网则介绍,“货车帮”是中国最大的公路物流互联网信息平台,建立了中国第一张覆盖全国的货源信息网,并为平台货车提供综合服务,致力于做中国公路物流基础设施。

相比于这两家公司,“BOSS直聘”或许更为广为人知。招股书显示,2021年3月,“BOSS直聘”月活跃用户数达3060万,服务630万家认证企业,其中82.6%为中小企业。官网介绍称,该平台应用人工智能、大数据前沿技术,提高雇主与人才的匹配精准度,缩短求职招聘时间,从而提升求职招聘效率。

综合来看,这几家企业都掌握大量用户隐私数据,并且业务与关键信息基础设施有关联。

“上述几家被审查的企业,分别为日常出行、网络货运及大众求职领域的头部平台,至少掌握了所属行业领域80%以上的深度数据。这些数据可以直接或间接地反映我国各区域人口分布、商业热力、人口流动、货物流动、企业经营等情况。”江苏省大数据交易和流通工程实验室副主任李可顺表示。

赴美上市需披露信息 可能导致重要数据泄露

值得注意的是,这几家被审查的企业有着共同的特点:近期赴美上市。

记者查阅资料发现,2021年6月11日,“BOSS直聘”于美国上市;6月22日,拥有“运满满”和“货车帮”的满帮集团于美国上市;6月30日,国内最大的移动出行平台滴滴于美国上市。

滴滴接受网络安全审查的消息,迅速在网络上发酵。

汇业律师事务所高级合伙人李天航认为,滴滴作为一家主要在中国经营的企业,所有数据首先是存储在本地的。但是,在美国上市将不可避免地涉及数据出境问题。

去年6月份,美国参议院提出了《外国公司问责法案》,该法案规定,如果外国公司连续三年未能通过美国公众公司会计监督委员会

7月6日,中共中央办公厅、国务院办公厅公开发布《关于依法从严打击证券违法活动的意见》。意见提出,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。

近日,国家网信办连续发布了对“滴滴出行”“运满满”“货车帮”“BOSS直聘”实施网络安全审查的公告。审查期间,以上App均已停止新用户注册。

多家互联网企业接受网络安全审查,一时间,数据安全再次成为关注焦点。



企业应及时调整经营、运维和治理理念

近几年,大数据、云计算、物联网等技术和应用高速发展,互联网企业在为人们生活带来便利的同时,跨境数据流动、用户数据泄露等问题,也受到广泛关注。

在赵淑钰看来,“一方面,造成侵犯用户个人信息的风险,目前过度收集、滥用用户个人信息的情形依然多发高发;另一方面,也会对国家安全产生影响,随着数据分析技术的飞跃发展,互联网企业在运营过程中产生的巨量数据通过大数据分析能够反映出我国整体经济运行情况等涉及国家秘密的信息,对总体国家安全构成重大安全威胁。”

“近两年,一些互联网企业在用户个人信息泄露方面发生的问题屡见不鲜,原因之一是我国数据安全保护机制的建设还不是特别完善。”刘典表示,这与互联网行业的高速变化不无关系。“新业态不断推陈出新,监管对象在不停变化,规模不断扩大,给治理带来了一定的难度。”

互联网企业的数据安全问题也可能从不同方面影响国家安全。类似地图数据、位置数据等重要数据,同样需要保护。

在刘典看来,当前国家在互联网领域和数据安全领域的主导,符合推动高质量发展的内在要求。“过去一些互联网企业在野蛮高速增长的状态下,主要从商业利益的角度出发进行数据的开发利用,对数据合规的投入相对较小。随着数据保护问题成为一个社会焦点,国家开始不断加强对数据监管和数据安全合规的监管。虽然从短期来看,会对互联网企业的发展模式带来一定冲击,但这也是由高速发展转向高质量发展的必由之路。”刘典说。

在李天航看来,将来所有企业的所有经营行为,都必须受到国家安全法、网络安全法、数据安全法和个人信息保护法这四部法律为纲的立体法律框架体系的规范。他建议,企业要有前瞻性,调整自己的经营、运维和治理理念,甚至重塑自身业务模式。

数据安全已被提升至国家安全层面

“6月10日,十三届全国人大常委会第二十九次会议表决通过数据安全法,将数据安全提升到了国家安全的层面,同时对重要数据出境安全管理也提出了相应要求。”李可顺表示。

数据安全法第三十一条明确了重要数据出境安全管理制度,“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理,适用《中华人民共和国网络安全法》的规定;其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法,由国家网信部门会同国务院有关部门制定。”

此外,数据安全法还严格规制面向境外司法或者执法机构的数据出境活动。该法第三十六条规定,“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。”

“这一条款制定的背景是近年来数据管

辖权冲突日益激烈的国际环境。”中伦律师事务所顾问贾申刊文指出,在这一背景下,数据安全法的规定再度明确了我国对境内数据的管辖权,充分体现了我国维护数据主权和国家安全的决心。

“值得一提的是,数据安全法还特别明确了未经主管机关批准向境外的司法或者执法机构提供数据的法律责任,包括对企业和直接负责的主管人员的罚款,以及责令企业暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照等。这一明确的法律责任形式,不仅意味着第三十六条的规定是企业应严格履行的一项数据合规义务,也使得企业在对抗境外执法或司法机构可能的数据调取要求时,拥有了可援引的有力的法律规则。”贾申表示。

没有网络安全就没有国家安全,就没有经济社会稳定运行,广大人民群众利益也难以得到保障。

的审计,将被禁止在美国任何交易所上市。而有关信息披露,可能导致重要数据、个人信息的泄露。今年3月份,美国证券交易委员会表示,通过了《外国公司问责法案》最终修正案。

“美国证券市场对于上市公司有很高的信息披露要求,包括必须根据美国公认会计原则编报其财务报表,必须根据美国证券法律规定,对公司重大信息及时披露等,这势必涉及一些该公司在中国境内的经营情况数据是否能够出境的问题。”李天航说。

我国正在不断完善网络和数据法律法规体系

“我国在网络安全和数据治理方面的立法体系不断构建完善,为开展网络安全和数据治理工作提供了充分的立法保障。”中国信息通信研究院互联网法律研究中心研究员赵淑钰告诉记者。

2017年6月1日,《中华人民共和国网络安全法》施行,填补了我国综合性网络信息安全基本大法、核心的网络信息安全法和专门法律的三大空白。

此次几家互联网企业接受审查的依据之一,是2020年6月1日正式实施的《网络安全审查办法》。该办法为开展网络安全审查提供了重要的制度保障和法律依据。

中国人民大学重阳金融研究院副研究员刘典告诉记者,网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险,包括: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;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;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;产品和服务提供者遵守中国法律、行政法规、部门规章情况;其他可能危害关键信息基础设施安全和国家安全的因素。

“通常情况下,网络安全审查在45个工作日内完成,情况复杂的会延长15个工作日。进入特别审查程序的审查项目,可能还需要45个工作日或者更长。”刘典说。

2021年3月,《中华人民共和国个人信息保护法(草案)》提请全国人大常委会审议。目前,该草案已处于审议阶段,业界普遍认为,该法距离面世并生效实施已经为期不远。

2021年6月,《中华人民共和国数据安全法》全文公布,并将于9月1日起正式实施。“数据安全法明确了由中央国家安全领导机构‘统筹协调国家数据安全的重大事项和重要工作,建立国家数据安全工作协调机制’,这是亮点之一。”刘典告诉记者。

“网络安全法、数据安全法和个人信息保护法这三部法律出台后,中国互联网领域基础性的法律法规框架体系就已完成,其他法律、法规、部门规章、地方性法规等等,都会在这三部法律组成的体系之下,继续细化具体的内容,逐步覆盖互联网、个人信息和数据活动的方方面面。”李天航说。

据《中国纪检监察报》

据《中国纪检监察报》