

新规待出 数据出境“安全阀”将进一步拧紧

□ 陈 兵 杨懿林

随着国际数字贸易的飞速发展,数据跨境流动成为各国和地区数据信息交流和经贸往来的重要形式和通路。数据跨境流动的爆炸式增长在促进国际数字贸易繁荣的同时,也对个人信息安全、数据产业发展甚至国家数据安全带来了挑战,诸如个人信息泄露、商业数据违规披露、国家数据主权冲突等层见叠出,如何规范数据出境活动,促进数据跨境安全、自由流动,维护个人信息权益、国家和社会公共利益成为社会各界关注的热点与难点。

近日,《第一财经日报》记者了解到国家互联网信息办公室就《数据出境安全评估办法(征求意见稿)》(以下简称《征求意见稿》)向社会公开征求意见。《征求意见稿》共18条,内容囊括了数据处理者应当申报数据出境安全评估的具体情形、申报数据出境安全评估应当提交的材料、数据处理者风险自评估与监管部门安全评估、数据处理者与境外接收方订立合同要求、数据出境安全评估主管部门、重新申报评估情形以及相关法律责任等,对数据出境安全评估提供了明确的规则指引。

数据出境合规体系更加完善

在《征求意见稿》发布前,《中华人民共和国网络安全法》(以下简称《网络安全法》)《中华人民共和国数据安全法》(以下简

称《数据安全法》)和《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)从法律层面建立了数据出境合规机制,构建了科学系统的网络空间数据出境合规法律体系。然而,上述法律并未对数据出境评估规范进行细化规定,导致实践中对数据出境进行安全评估时缺乏具体实施规则,不利于依法规范开展数据出境安全评估,维护个人信息权益、国家和社会公共利益。

本次《征求意见稿》在遵循上述法律基本要求的前提下,对数据出境安全评估规范进行了细致的规定。《征求意见稿》第2条明确规定:数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和依法应当进行安全评估的个人信息,应当按照本办法的规定进行安全评估。

在适用对象上,《征求意见稿》并未采用《网络安全法》《数据安全法》《个人信息保护法》有关“关键信息基础设施运营者”“重要数据处理者”“其他数据处理者”的表述,而是统一采用“数据处理者”,在适用对象上更具广泛性和包容性。当然,也存在与现有法律如何衔接的问题,可能会引发对“数据处理者”这一概念的不同理解,不利于对数据出境活动中负有核心义务的数据处理者做规范化、系统化及法治化的认定。

数据出境或迎更安全保障体系

据悉,《征求意见稿》第3条

明确指出“数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合”,对数据出境评估流程进行了清晰的制度构建。其中,事前评估具体体现为风险自评估与安全评估制度,通过数据处理者对风险自评估与监管部门所做的外部安全评估,可及时发现并预判数据出境可能存在的潜在风险或已知风险,及时采取措施化解风险,降低数据泄露对个人信息权益、社会公共利益和国家利益的影响。

在持续监督方面,具体体现为数据出境评估结果有效期制度,根据《征求意见稿》第12条,数据出境评估结果有效期两年,如在有效期内出现本条规定的特定情形,数据处理者需要向监管部门重新申报数据出境安全评估。通过事前评估与持续监督“双管齐下”,《征求意见稿》建立了全流程、全链条、全周期的数据出境风险防范与化解机制,有助于灵活高效应对数据跨境流动中可能存在的治理难题,提升数据出境安全评估治理效能。

关于数据出境安全自评估与数据出境安全评估,《征求意见稿》规定了数据处理者向境外提供数据满足规定情形时的两类评估义务,即数据出境安全自评估与监管部门数据出境安全评估。第5条明确规定了数据出境风险自评估的具体事项,有助于数据处理者全面分析和预测数据安全风险,形成系统的数据出境风险自评估报告,为监管部门进行数

据安全评估提供参考,形成政府与企业数据出境安全评估交流的互动机制。

在数据安全保护责任方面,《征求意见稿》要求,数据处理者与境外接收方订立合同应当充分约定数据安全保护责任。境外数据接收方的技术安全能力,处理数据的用途、方式,以及出境数据是否会再转移等因素,均会影响数据保护水平,对数据跨境流动安全产生挑战。故在与境外接受方订立合同时,充分约定数据安全保护责任,是强化境外接收方按照我国法律履行数据安全保护义务的重要保障,有助于提供具有约束力的行权条款和争议解决条款,在境外接收方出现违约情形时,便于我国数据出境企业和权益受损的个人依法进行维权。

同时,数据安全保护责任也是监管部门数据出境安全评估以及重新申报数据出境安全评估的重要内容或影响因素,随着《征求意见稿》对境外接收方数据安全保护责任的规定,数据出境安全将迎来更加系统的安全保障体系,在日趋激烈的国际数据争夺战中,为维护我国数据主权、安全和发展利益提供强有力的法治保障作用。

保障数据出境安全需多措并举

数据的价值在于流动,只有在持续高质量的流动中才能充分发挥和挖掘数据价值,最大效能释放数据红利。作为数据出境安全评估的重要价值目标之一,《征求意见稿》第3条明确指出“保障数据依法有序自由流动”,然而,数据流动本身便意味着风险存在,在促进数据自由流动的同时,也应妥善应对和防范数据出境安全风险,实现数据流动与数据保护的平衡。故立足于我国数据出境流动治理的现实情况,建议多措并举保障数据出境安全,维护我国在全球数据经济活动中的合法权益。

第一,在制度建构层面,根据《数据安全法》《信息安全技术数据出境安全评估指南(征求意见稿)》等法律、国家标准的规定,尽快建立数据分类分级制度。根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者个人、组织合法权益造成的危害程度,对数据实行分类分级保护。对不同安全层级的数据采取不同层次的保护水平,降低数据出境对国家安

全、社会公共利益的影响,最大限度避免数据安全事件的发生。

第二,在国际合作层面,加强我国在数据跨境流动治理领域的国际合作。一方面,加紧推进国际合作渠道尤其是区域性合作渠道的建立,9月16日,中国正式申请加入《全面与进步跨太平洋伙伴关系协定》(CPTPP),CPTPP针对互联网规则和数字经济设定了较高标准,其中涉及数据跨境流动与数据本地化存储等问题,在正式加入后可能成为沟通我国与世界各国数据合作的纽带;另一方面,可以尝试将国际协定与国内治理进行衔接,率先与已经构建起良好协作关系的国家或地区进行数据跨境流通的先行先试,逐渐推动国内治理机制与国际规则的双向交互发展。

第三,在监管层面,完善数据跨境流动行业监管体系,建立数据安全监管平台。当前,数据安全风险更多地来源于数据运行周期的不可控性,数据安全风险存在于数据收集、存储、分析、加工、共享到销毁的每一环节。故有必要借助数据交易中心的建设,建立数据安全监管平台,做到对数据跨境流动全周期监控和实时预警,维护市场交易稳定与安全,推动数据市场健康发展。

第四,在行业自律和企业合规层面,切实发挥行业协会与企业的积极性与能动性,减轻政府对数据跨境流动风险审查的压力。在行业自律方面,应充分发挥行业协会自身优势,积极参与到维护数据安全、促进数据竞争的治理中,推动建立行业内部惩戒机制、健全行业自律规则、完善数据跨境流动规范,形成公平有序、开放竞争、安全可靠的数据跨境流动治理行业标准。

在企业合规方面,除积极引导企业开展合规工作外,还应建设企业合规的新工具,譬如,构建企业资质认证制度,对企业的数据保护能力及专门从事数据跨境传递业务的水平等资质进行考核评定,做好事前资质审查,避免等待审查、重复审查的情况出现。同时,针对数据出境不可逆的特性,企业应充分重视境外合规工作,通过加强与高校、科研机构的深入合作,准确把握境外接收方所在国家或者地区的数据治理法律制度,灵活应对域外法律环境的变化,采取有效措施避免或降低域外相应制度对我国数据利益的不当影响。

澳大利亚拟立法要求社交平台提供诽谤他人者的信息

本报讯 11月28日,澳大利亚总理莫里森宣布,为了治理网络空间中存在的诽谤与攻击性言论,澳政府将推动出台新的法规,要求社交平台公司对其平台上发布的诽谤性评论负责。

据澳大利亚广播公司(ABC)报道,根据拟议中的新法草案,澳大利亚政府将要求社交平台公司创建投诉机制,任何人若认为自己在社交平台上遭诽谤、霸凌或恶意攻击,可依法要求有关的社交平台删除恶意留言。倘若平台没有这么做,投诉人可寻求法院下令,强制涉事社交平台提供恶意留言者的身份详情等个人信息,以便对霸凌者采取行动。《华尔街日报》刊文指出,此举可能会让社交平台公司未来面临诉讼。

莫里森在一次电视新闻发布会上指出,收到投诉时提供上述细节的社交平台公司将能以不是其平台上评论的发布者为由进行辩护。“要保证社交平台公司有强硬手段,确保它们可以告诉人们发表伤害性言论的人到底是谁,这符合这些公司的利益。”莫里森说,“否则,这些社交平台公司将成为被告。”

“网络空间不应该成为机器人、偏执狂与霸凌者的‘狂野西部’,仗着匿名身份肆意中伤他人的这种行为不会发生在现实世界,同样也不应该存在于虚拟世界。”莫里森说。

《联合早报》报道指出,澳大利亚政府一直在寻求将推特、脸书这些社交平台公司纳入法律监管的框架。莫里森说:“社交平台,这些巨头,应该采取有效的措施来删除诽谤性言论。既然这些公司创造出了这样一个虚拟空间,那他们就应该确保这个空间是安全的。假使他们做不到,我们会诉诸法律。”(南博一)

涉嫌伪造医疗证明 意大利黑手党成员被捕受审

本报讯 向法官行贿以获得无罪释放;伪造医疗证明让原本被定罪的杀手逃脱牢狱之灾……从恐吓到造假,从贩毒到谋杀,这些触目惊心的犯罪行为,由意大利黑手党组织“光荣会”的数十名成员供述。这场审判从今年1月份开始,媒体近日曝光了这些惊人内幕。

据法新社11月28日报道,意大利最强大的有组织犯罪集团“光荣会”近日因355名成员受审成为舆论关注的焦点。除了臭名昭著的黑手党成员,被告还包括警察、法院工作人员、市长和其他官员。审判的核心人物是现年67岁的“光荣会”头号人物路易吉·曼库索,绰号“叔叔”。曼库索为黑手党家族实际控制人。此前,他因贩毒和有组织犯罪被判处19年徒刑,直到2012年获释。

法新社称,“光荣会”黑白通吃”,压迫当地民众,现在主导着欧洲的可卡因交易,并渗透到整个意大利乃至世界其他国家和地区。近日,58名黑手党线人通过视频连线向法院提供证词,更是曝光了该组织的各种罪行,也暴露了该组织在社会各阶层的潜在影响。351页起诉书指控也表明,“光荣会”为达目的不择手段。目前,这些被告被关押在卡拉布里亚南部的贫困地区。

法新社称,“光荣会”对当地经济的影响很大,几乎无法根除。但这次核心成员被捕受审,或许会对其造成致命打击。(刘洋)

受间谍软件丑闻影响 以色列限制对外出口网络科技

本报讯 据以色列财经媒体《经济学人报》报道,受“飞马”间谍软件丑闻的影响,以色列国防部已于11月初更新了网络科技出口许可范围,大幅缩减网络科技可出口国家的数量。

《经济学人报》称,以色列国防部将该国网络科技可出口国家的数量从102个减少到37个,以色列的新盟友阿联酋、沙特等国已经被踢出可出口名单,但之前被控使用“飞马”软件监控国内政治人士的印度却仍在名单上。

《经济学人报》没有透露其消息来源。不过,以色列国防部之后发表声明,对《经济学人报》的报道进行回应。声明称,将对违反出口许可的行为采取“适当措施”。不过以色列国防部没有在声明中明确禁止向哪些国家出口网络科技。

“飞马”间谍软件是以色列NSO集团开发的一款产品。今年7月,多家媒体爆出该软件涉嫌被用来监视多国领导人、记者和活动人士,还因此导致多个国家向以色列“兴师问罪”。NSO集团从未披露过其外国政府客户名单,且始终坚称该公司仅向政府提供“飞马”软件用于反恐和打击犯罪目的。不过,相关报道还是促使以色列重新审视其网络科技出口政策,该政策由国防部负责制定。

据《以色列时报》报道,“飞马”软件被认为是市场上最强大的网络监控工具之一,它能让操作人员完全控制被监控人的手机等电子设备,从上面下载所有数据,或者在被监控人不知情的情况下激活其设备的摄像头或麦克风。(甄翔)



国际观察

“加拿大鹅”陷退货风波 品牌信誉再遭质疑

□ 徐 驰

万元羽绒服商标绣错、面料味道刺鼻、部分脱线……从门店到总公司,消费者想要退货,却遭遇重重阻碍。近日,刚刚因虚假广告宣传被黄浦区市场监管部门罚款45万元并因此冲上热搜的“加拿大鹅”,这次又摊上事了。

有消费者向《新民晚报》反映,她在“加拿大鹅”门店购买的羽绒服存在一系列质量问题,却在维权过程中处处碰壁。“加拿大鹅”何时能拿出解决问题的应有诚意?消费者的合法权益是否能够得到保障?

门店衣服商标绣错

10月27日,上海市民贾女士

在上海国金中心商场下一层LG1-58号“加拿大鹅”门店,购买了一件型号为9512M的羽绒服,价格为11,400元。回到家中后,贾女士发现,这件“加拿大鹅”的商标竟然绣错了:中心太阳处多绣了一根弧线。

羽绒服缝线粗糙,挂着许多长长短短的线头;衣服口袋内布料边缘没有包边,有脱线现象;面料也有阵阵刺鼻的味道……贾女士说,当天,她在付款前,店员对于购买的商品不能退款退货等没有任何告知。“但当我刷完信用卡后,店员递给我一张纸,抬头为《更换条款》,要求我签名。”

据悉,这份《更换条款》上写明:除非相关法律另有规定,所有中国大陆地区专门店售卖的货品

均不得退货。“如果不签名,就不能拿衣服。”贾女士表示,当时,她只能在这份条款上签了字。

投诉维权处处碰壁

10月28日,贾女士向国金中心“加拿大鹅”门店店长投诉,同时拨打了“加拿大鹅”客服热线4001275066。可店长称,“我没有权力退货,需要总公司层面来解决。”

“我向店长要总公司电话,他却说没办法提供,要我自己去查。还说公司已经向市场监管局方面提供了这件衣服的报关单和合格的检测报告。他要求我提供给公司衣服不合格的检测报告,才可以退货。”贾女士说道。

11月14日,贾女士又撰写了

一份邮件,并将衣服的细节照片等凭证一同通过邮件附件的形式,发给“加拿大鹅”的检测中心邮箱(ce@canadagoose.com)。但随后,总公司在回信中却告知,现在,“加拿大鹅”方面不再通过照片提供产品认证。

律师称可提出赔偿

上海善法律师事务所高级合伙人秦裕斌表示,对于商品不符合要求的,消费者有权要求销售者对其修理、重做、更换、退货等。而商家在付款前不告知,在付款后让消费者签署所谓的《更换协议》,损害了消费者的合法权益。

秦裕斌直言,如果商品存在质量问题,消费者不仅可以要求退换,甚至完全可以要求厂家赔