2021
NO. 07

数据合规资讯月报

Data Compliance Monthly Newsletter

天达共和律师事务所

East & Concord Partners

摘 要

尊敬的各位客户、同仁：

欢迎参阅天达共和律师事务所数据合规团队为您呈现的《数据合规资讯月报》2021 年第七期，本期月报主要内容包括：

- **立法动态**

  介绍 2021 年 6 月 26 日至 2021 年 7 月 25 日期间及前后境内外数据保护立法动态，并针对部分立法动态提供简要评论。

- **执法聚焦**

  介绍 2021 年 6 月 26 日至 2021 年 7 月 25 日期间及前后境内外部分典型执法案例，并针对部分执法活动提供简要评论。

- **行业新闻**

  精选 2021 年 6 月 26 日至 2021 年 7 月 25 日期间及前后互联网及相关行业与网络安全和数据保护有关的新闻资讯。

- **热点评述**

  《数据安全法》将于 2021 年 9 月 1 日正式生效施行。滴滴事件发生后，我国启动了《网络安全审查办法》修订工作，数据安全问题引起了社会各界的广泛关注。本数据合规团队申晓雨合伙人律师应新闻媒体“健康界”邀请，为《〈数据安全法〉出台后，AI、大数据企业如何自处？》一文提供专业观点支持，对 AI 智能企业风控提出前瞻建议，其中涉及介绍及评述《数据安全法》《网络安全审查办法（修订草案征求意见稿）》的一些重点内容。

目 录

立 法 动 态

➢ 境内立法

- 6 月 28 日，中华人民共和国工业和信息化部（“工信部”）发布《2021 年汽车标准化工作要点》（“《工作要点》”）。《工作要点》强调，在智能网联汽车领域要加快推进整车信息安全、软件升级、自动驾驶数据记录系统等强制性国家标准的立项和制定工作；强化基础性标准支撑，完成智能网联汽车术语定义推荐性国家标准征求意见，启动并持续推进信息安全工程、操作系统等基础类标准制定工作。《工作要点》同时指出要深化国际合作，发挥多双边合作机制作用，促进国内外标准化机构间的对话合作，积极推动中国标准“走出去”，深度参与全球技术法规制定。

  （https://www.miit.gov.cn/jgsj/zbys/gzdt/art/2021/art_074e096a8b7a44b1945ab57d962aada9.html）

  简析：可以预见，智能网联汽车产业拥有广阔的发展空间。智能网联汽车收集处理的信息含有敏感信息，强化智能网联汽车的信息及系统安全将成为产业发展监管的一个重要方面。智能网联汽车产业链相关企业有必要关注智能网联汽车信息及系统安全的有关强制性国家标准的制定情况，以便为合规运营做好准备工作。

- 7 月 2 日，国家市场监督管理总局（“市场监管总局”）发布了《价格违法行为行政处罚规定（修订征求意见稿）》（“征求意见稿”），正式向社会公开征求意见。征求意见稿重点规制了新兴业态下的价格违法行为，新增第十三条，明确禁止电子商务平台经营者利用算法等技术手段，根据用户偏好、交易习惯等实施价格歧视行为；征求意见稿将现行《价格违法行为行政处罚规定》处以 500 万以下不等罚款的规定，修改为“可以处违法行为发生期间销售额或所囤积货值 1%以上 10%以下的罚款”，罚款金额可能大幅提高，最高可能达到经营者上一年度销售额的 10%。

  （http://www.samr.gov.cn/hd/zjdc/202107/t20210702_332196.html）

- 7 月 6 日，深圳市人民代表大会常务委员会正式公布了《深圳经济特区数据条例》（“《条例》”），《条例》自 2022 年 1 月 1 日起施行，内容涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，是国内数据领域首部基础性、综合性的地方立法。《条例》主要内容和创新包括以下几个方面：率先在地方立法中探索数据相关权益范围和类型；合理限制生物识别数据的处理；规范用户画像和个性化推荐的应用；提升公共数据处理水平，建立公共数据治理体系、推动公共数据最大限度开放利用；探索培育数据要素市场；参考最高人民检察院《关于积极稳妥拓展公益诉讼案件范围的指导意见》中关于“将个人信息保护作为网络侵害领域公益诉讼的办案重点”的意见，在地方立法中首次确立了数据领域的公益诉讼制度。

  （http://www.szrd.gov.cn/szrd_zlda/szrd_zlda_flfg/flfg_szfg/content/post_706636.html）

  简析：《条例》规定自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及条例规定的财产权益，但不得危害国家安全和公共利益，

不得损害他人的合法权益。该规定是从立法层面确认企业对合法处理的数据享有财产权益，为构建数据要素市场奠定基础。

关于数据要素市场,《条例》明确规定市场主体对合法处理数据形成的数据产品和服务，可以依法自主使用，取得收益，进行处分；关于数据要素市场培育，规定：（1）市人民政府应当组织制定数据处理活动合规标准等地方标准；（2）探索构建数据资产定价指标体系，推动制定数据价值评估准则；（3）推动建立数据交易平台，引导市场主体通过数据交易平台进行数据交易；（4）数据处理者可以委托第三方机构进行数据质量评估认证；（5）市场主体合法处理数据形成的数据产品和服务，可以依法交易。但是，有下列情形之一的除外：交易的数据产品和服务包含个人数据未依法获得授权的；交易的数据产品和服务包含未经依法开放的公共数据的；法律、法规规定禁止交易的其他情形。

《条例》作为地方性立法具有制度创新和实践探索方面的积极意义，值得予以关注。

- 7 月 6 日，据新华社北京电，中共中央办公厅、国务院办公厅于近日印发了《关于依法从严打击证券违法活动的意见》（“《意见》”）。《意见》主要为依法查处证券违法犯罪确立了基本原则；提出了完善资本市场违法犯罪法律责任制度体系的要求；指出要进一步加强跨境监管执法司法协作，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，压实境外上市公司信息安全主体责任。
（http://www.gov.cn/zhengce/2021-07/06/content_5622763.htm）
简析：根据我国《网络安全法》以及即将于 2021 年 9 月 1 日起实施的《数据安全法》，关键信息基础设施运营者在境内运营中收集或产生的重要数据出境应按照国家网信部门会同国务院有关部门制定的办法进行安全评估；其他数据处理者在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。关于境外执法机构调取数据的要求，《数据安全法》的规定是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的国际条约、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的请求。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。此外，《个人信息保护法（草案二次审议稿）》也对向境外提供个人信息设定了须满足的前提条件。

境外上市公司在境内运营中收集和产生的数据是否包含重要数据、个人信息，这些数据是否将流向境外，境外上市公司应给予充分重视和关注，确保符合境内的合规要求。

- 7 月 6 日，中国支付清算协会发布《关于印发〈多方安全计算金融应用评估规范〉和〈移动金融基于声纹识别的安全应用评估规范〉的通知》。《多方安全计算金融应用评估规范》（“《多方安全计算评估规范》”）是我国首个金融领域针对多方安全计算技术的评估标准。多方安全计算作为一种隐私计算技术，在我国数据合规监管要求趋严的背景下，备受关注。《多方安全计算评估规范》适用于多方安全计算的金融应用机构、技术服务和解决方案提供商，明确了多方安全计算金融应用的基础要求、安全要求以及性能

要求。《移动金融基于声纹识别的安全应用评估规范》（“《声纹识别评估规范》”）在《移动金融基于声纹识别的安全应用技术规范（JR/T 0164-2018）》基础上制定，为金融行业安全建设和金融行业主管部门对声纹识别的安全技术评估提供参考，为第三方评估机构的安全检测评估提供指导和依据，对于降低互联网金融的 IT 风险、保证互联网金融业务的连续性等具有非常积极的意义。

（http://www.pcac.org.cn/eportal/ui?pageId=598261&articleKey=612680&columnId=595085）

- 7 月 7 日，工信部公布了与国家标准化管理委员会组织编制的《工业互联网综合标准化体系建设指南（征求意见稿）（2021 版）》（“征求意见稿”），以推进工业互联网标准体系建设的部署要求，加强工业互联网标准化工作，公示截止日期为 2021 年 8 月 5 日。征求意见稿由以下章节组成：技术与产业发展现状、总体要求、标准体系结构图和框架图、建设内容、组织实施组成，另有两个附件——附件 1 为工业互联网相关缩略语，附件 2 为已发布、制定中和待制定的工业互联网标准。征求意见稿指出我国的建设目标是到 2023 年，基本形成工业互联网标准体系，制定术语定义、通用需求、供应链/产业链、人才等基础标准 15 项以上；“5G+工业互联网”、信息模型、工业大数据、安全防护等关键技术标准 40 项以上；面向汽车、电子信息、钢铁、轻工家电、装备制造、航空航天、石油化工等重点行业领域的应用标准 25 项以上。

  （https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_10e736506cbc41d6be0d826158244b7b.html）

- 7 月 10 日，国家互联网信息办公室（“国家网信办”）发布《网络安全审查办法（修订草案征求意见稿）》（“征求意见稿”），正式面向社会公开征求意见。征求意见稿第二条规定实质性地扩大了适用网络安全审查的范围，其中包括：关键信息基础设施运营者采购网络产品和服务，以及数据处理者开展数据处理活动，影响或可能影响国家安全的情形；增加证监会作为网络安全审查工作机制的成员单位；第六条规定掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。第十条进一步增加了网络安全审查中考虑的国家安全风险因素，规定了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。

  （http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm）

  简析：根据以上修订草案，只要数据处理活动影响或可能影响国家安全，不论数据处理者是否属于关键信息基础设施运营者，都落入网络安全审查范围。另，企业赴国外上市的，如其掌握超过 100 万用户个人信息，应进行网络安全审查。数据处理者需要识别其所处理数据的类型和数量，评估其承载数据的系统遭到破坏、丧失功能或数据泄漏是否可能影响国家安全，并对《网络安全审查办法》的修订保持持续关注。

- 7 月 12 日，工信部、国家网信办、公安部联合发布《网络产品安全漏洞管理规定》（“《规定》”），自 2021 年 9 月 1 日起施行。《规定》重点内容包括：第一，明确规制对象。中华人民共和国境内的网络产品（含硬件、软件）提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，应当遵守《规定》。第二，规定网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安

全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于 6 个月。第三，网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。第四，提出了网络产品提供者的漏洞验证、信息报送及补救义务。《规定》要求网络产品提供者对发现或获知其所提供的网络产品漏洞应立即采取措施并进行验证，评估安全漏洞的危害程度和影响范围，对属于其上游产品或组件存在的安全漏洞则立即通知有关产品提供者，并于 2 日内向工信部报送漏洞信息，并及时进行修补，将修补方式告知可能受影响的产品用户。第五，提出漏洞收集平台实行备案管理。

（http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm）

简析：《规定》细化了《网络安全法》关于网络安全漏洞方面的规定。《规定》出台的主要目的是为了维护网络安全、保护网络产品和网络系统的安全稳定运行，将有助于推动网络产品安全漏洞管理工作的规范化，提高有关主体的网络安全漏洞管理水平。由于网络产品提供者、网络运营者以及从事网络产品安全漏洞发现、收集、发布等活动的组织或个人均受到《规定》的规制，这些主体应各自参照《规定》梳理合规要求，确保漏洞接收及/或处置方面符合《规定》。对于网络运营者而言，应设置网络安全产品漏洞信息接收渠道，配备有关漏洞接收、处理机制及其人员，包括验证漏洞、修补漏洞。

- 7 月 21 日，商务部、中央网络安全和信息化委员会办公室（“中央网信办”）、工信部联合印发《数字经济对外投资合作工作指引》（“《工作指引》”）。《工作指引》适用于企业在数字经济领域开展对外投资合作，由企业自觉遵守，同时适用于地方商务、网信办、工信部主管部门对我国企业开展对外投资的指导、管理和服务。《工作指引》鼓励数字经济企业完善内部合规制度，严格落实我国法律法规有关数据出境安全管理的规定，遵守东道国法律法规及国际通行规则，妥善应对数据经济领域审查和监管措施，健全数据安全管理制度，采取必要技术措施保护数据安全和个人信息。

  （http://www.ltcjzx.org.cn/article/cq/202107/20210703180522.shtml）

- 7 月 28 日，《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》发布，于 2021 年 8 月 1 日施行，适用于因信息处理者违反法律、行政法规的规定或双方的约定使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息所引起的民事案件，并从物业服务、格式条款效力、违约责任承担等角度对人民群众普遍关心的问题予以回应。

  （http://www.court.gov.cn/fabu-gengduo-16.html）

  简析：人脸信息是生物识别信息中社交属性最强的个人信息，具有唯一性、不可更改性、高度敏感性，一旦泄漏将对个人人身和财产带来严重危害。人脸识别技术的飞速发展，不应成为个人必须提供人脸用于验证身份等场景的唯一手段（法律、行政法规另有规定的除外）。涉及人脸信息采集、人脸识别相关应用的企业需要重视该司法解释。

➢ 境外立法

✧ 美国

- 7 月 7 日，美国科罗拉多州州长签署了《科罗拉多州隐私法案》（Colorado Privacy Act，CPA），科罗拉多州成为继加利福尼亚州和弗吉尼亚州之后美国第三个颁布全面隐私立法的州。该法案规定了消费者享有个人数据访问权、纠正权、删除权以及拒绝收集、使用和出售个人数据等权利，数据控制者或处理者则需要履行说明告知、数据保护评估等数据保护义务，将于 2023 年 7 月 1 日生效。
（https://www.jdsupra.com/legalnews/colorado-privacy-act-3182596/）

- 7 月 9 日，《纽约市生物识别法》生效。该法要求商业机构收集、保留或共享用户的生物识别信息必须向用户披露，即“在所有用户入口附近放置清晰显眼的标志，以通俗易懂的语言告知用户”。此外，该法明确禁止将生物识别信息用于交易，“出售、出租、交易、分享生物识别信息以换取任何有价值的东西或以其他方式从生物识别信息交易中获利”均为非法行为。该法还规定了一项私人诉讼权，受害方能够对每起侵权行为请求 500 美元到 5000 美元不等的法定损害赔偿金。
（https://iapp.org/news/a/nyc-biometric-law-enters-into-force/）

✧ 欧盟

- 6 月 28 日，欧盟承认英国的隐私规则达到欧盟所认可的充分保护水平的条件，欧盟和英国之间可进行数据的转移和流动。此前欧盟与英国曾于 2020 年 12 月达成英国脱欧后的贸易协议时，引入了一个为期六个月的临时解决方案，以保持跨境数据的流动。本月 28 日，欧盟委员会正式通过两项 “充分性 ”认定，也承认英国的数据保护法与欧盟法律相称。但是，欧盟首次加入了一项 “日落条款”，这意味着这些决定将在生效四年后到期。同时，如果在前述决定生效期间英国在数据标准上与欧盟存在重大分歧，欧盟委员会表示可能会进行干预。
（https://www.cnbc.com/2021/06/28/eu-uk-personal-data-flows-set-to-continue-after-adequacy-deal.html
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en）

- 6 月 29 日-30 日，欧洲专利局行政理事会批准通过了欧洲专利局（EPO）的新数据保护框架。EPO 发布了新的《数据保护规则》（Data Protection Rules，DPR），并将在 EPO 服务条例中引入数据保护的概念，以实现与最高国际标准、最佳实践和欧盟数据保护立法保持一致。DPR 规定了数据保护的基本原则、个体数据权利和数据保护全流程，将于 2022 年 1 月 1 日正式生效。
（https://www.epo.org/news-events/news/2021/20210702.html）

执 法 聚 焦

➢ 境内执法

- 6 月底，浙江省“亮剑 2021”消费安全综合执法行动收官。本次专项执法行动重点围绕消费信息安全、食品安全等四大领域，共立案查处 10558 件案件，罚没款项 1.46 亿元，移送 134 件。在浙江省市场监督管理局（“浙江省市场监管局”）公布的“亮剑 2021”消费安全综合执法行动十大典型案例中，三起案例涉及侵犯消费者个人信息权益。其中，宁波杭州湾新区泛海置业等 20 家房地产公司因非法收集消费者人脸识别信息被罚；丽水亚上信息技术等 7 家公司通过潜入家长微信群非法收集学生、家长个人信息并销售给网络教育培训机构，最终 58 人被捕；兰溪市爵庭家居经营部等 6 家单位因通过同行互换、线下活动等渠道违法收集 5 万余条消费者个人信息被罚。
（参考来源：浙江省市场监管局官方微信公众号“浙江市场监管矩阵”）
（https://mp.weixin.qq.com/s/1wzjoqkq0XzaGIUb0clvFg）

- 7 月 2 日，网络安全审查办公室按照《网络安全审查办法》对“滴滴出行”启动网络安全审查，审查期间“滴滴出行”App 及小程序停止新用户注册。7 月 4 日，国家网信办经检测核实“滴滴出行”存在严重违法违规收集使用个人信息问题，通知应用商店下架“滴滴出行”App，要求滴滴出行科技有限公司（“滴滴”）严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。7 月 9 日，国家网信办经检测核实“滴滴企业版”等 25 款 App 存在严重违法违规收集使用个人信息问题，通知应用商店下架上述 25 款 App，要求相关运营者认真整改存在的问题。各网站、平台不得为“滴滴出行”和“滴滴企业版”等上述 25 款已在应用商店下架的 App 提供访问和下载服务。7 月 16 日，国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴，开展网络安全审查。
（http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm
http://www.cac.gov.cn/2021-07/04/c_1627016782176163.htm
http://www.cac.gov.cn/2021-07/09/c_1627415870012872.htm
http://www.cac.gov.cn/2021-07/16/c_1628023601191804.htm）
简析：滴滴事件中，“滴滴出行”App 因存在严重违反违规收集使用个人信息，被通知应用商店下架 App，深刻体现出《网络安全法》等法律法规下除了行政罚款之外的其他行政处罚方式的威力。网络运营者若存在个人信息方面的违法违规行为，被通知应用商店下架 App 或被撤销营业执照或许可，都会给企业正常运营带来严重影响。滴滴事件为广大网络运营者确保履行个人信息合规要求的重要性敲响了警钟。

由于国家有关部门已联合进驻滴滴开展网络安全审查，“滴滴出行”App 是否属于关键信息基础设施以及现行有效的《网络安全审查办法》及其修订稿有关条款引发了诸多讨论。现行有效的《网络安全审查办法》的制定目的是为确保关键信息基础设施供应链安全，维护国家安全，且规定对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，根据该办法进行网络安全审查。不过，对于其他企业来说，《网络

安全审查办法》修订稿草案如正式通过，则意味着不论是否属于关键信息基础设施运营者，均需关注其数据处理活动是否可能影响国家安全，其采购网络产品和服务应当预判该产品和服务投入使用后可能带来的国家安全风险，如影响或者可能影响国家安全，应当向网络安全审查办公室申报网络安全审查。企业需要持续保持对《网络安全审查办法》修订情况的关注。

- 7 月 5 日，网络安全审查办公室按照《网络安全审查办法》，对“运满满”“货车帮”“BOSS 直聘”启动网络安全审查。为配合网络安全审查工作，防范风险扩大，审查期间“运满满”“货车帮”“BOSS 直聘”App 停止新用户注册。上述被列入网络安全审查的相关运营企业均为六月赴美上市的公司。其中，“运满满”“货车帮”隶属的满帮集团于 6 月 22 日在美国纽交所上市，“BOSS 直聘”所属企业北京华品博睿网络技术有限公司于 6 月 11 日在美国纳斯达克上市。
（http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm）
简析：结合我国《网络安全法》《数据安全法》等法律法规以及《网络安全审查办法》修订草案，企业有必要识别所持有的数据是否为境内运营中收集和产生的以及这些数据是否涉及出境，数据处理活动（包括数据出境）是否可能影响国家安全，是否需要申请进行网络安全审查，以及整体评估境外上市的有关风险及可行性。

- 7 月 7 日，绍兴市柯桥法院开庭审理携程“大数据杀熟”第一案，最终判决被告上海携程商务有限公司（“携程”）退一赔三。该案中，胡女士作为享受 8.5 折优惠价的携程钻石贵宾用户，发现其通过携程 App 预定的酒店房间比酒店实际挂牌价贵了一倍。对此，胡女士以采集其个人非必要信息，进行“大数据杀熟”等为由将携程诉至柯桥法院。法院判决认为携程 App 存在虚假宣传、价格欺诈和欺骗行为，判决被告携程退一赔三，且被告应在其运营的携程旅行 App 中为原告增加不同意其现有《服务协议》和《隐私政策》仍可继续使用的选项，或者为原告修订携程旅行 App 的《服务协议》和《隐私政策》，去除对用户非必要信息采集和使用的相关内容（修订版本需经法院审定同意）。
（参考来源：微信公众号“柯桥法院”）
（https://mp.weixin.qq.com/s/DZ7RCKCd6sbsqka26gfRKw）

- 7 月 8 日，工信部发消息称大力推进 App 开屏弹窗信息骚扰用户问题整治。工信部表示，近期对用户反映强烈投诉较多的“弹窗信息标识近于无形、关闭按钮小如蝼蚁、页面伪装瞒天过海、诱导点击暗度陈仓”等违规行为进行了集中整治，督促企业重视用户诉求，解决好在开屏信息页面中存在利用文字、图片、视频等方式欺骗误导用户跳转等问题。截至目前，百度、阿里巴巴、腾讯、新浪微博、爱奇艺等 68 家头部互联网企业已按要求完成整改。2021 年第二季度，开屏弹窗信息用户投诉举报数量环比下降 50%，误导用户点击跳转第三方页面问题同比下降 80%。
（https://wap.miit.gov.cn/jgsj/xgj/gzdt/art/2021/art_5f841d495ab74e9a9aaf6e95c033d2ad.html）

- 7 月 19 日，工信部发布了《关于侵害用户权益行为的 App 通报（2021 年第 6 批 总第 15 批）》，此前工信部组织第三方检测机构针对用户反映问题较多的医疗健康、电子商

务、实用工具等类型手机应用软件进行了专项检查并通知相关企业进行整改，截至目前尚有 71 款 App 未完成整改。各通信管理局按工信部 App 整治行动部署，积极开展手机应用软件监督检查，辽宁省、浙江省、广东省、四川省、宁夏回族自治区通信管理局检查发现仍有 74 款 App 未完成整改。上述 145 款 App 应在 7 月 26 日前完成整改落实工作。逾期不整改的，工信部将依法依规组织开展相关处置工作。

（https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_0f974eeec513414aa56b1dac1797cf9b.html）

- 7 月 24 日，市场监管总局依法对腾讯控股有限公司（“腾讯”）2016 年 7 月收购中国音乐集团股权涉嫌违法实施经营者集中一案作出行政处罚决定，责令腾讯及关联公司采取三十日内解除独家音乐版权、停止高额预付金等版权费用支付方式、无正当理由不得要求上游版权方给予其优于竞争对手的条件等恢复市场竞争状态的措施。本案为我国《反垄断法》实施以来对违法实施经营者集中采取必要措施恢复市场竞争状态的第一起案件，责令腾讯解除独家版权等措施将重塑相关市场竞争秩序，降低市场进入壁垒，使竞争者均有公平触达上游版权资源的机会，有利于保障消费者选择权，促进网络音乐产业规范创新健康发展。

  （http://www.samr.gov.cn/xw/zj/202107/t20210724_333016.html）

- 7 月 26 日，工信部发消息称正式启动为期半年的互联网行业专项整治行动，聚焦扰乱市场秩序、侵害用户权益、威胁数据安全、违反资源和资质管理规定等四方面 8 类问题，涉及 22 个具体场景。在扰乱市场秩序方面，重点整治恶意屏蔽网址链接和干扰其他企业产品或服务运行等问题；在侵害用户权益方面，重点整治应用软件启动弹窗欺骗误导用户、强制提供个性化服务等问题；在威胁数据安全方面，重点整治企业在数据收集、传输、存储及对外提供等环节，未按要求采取必要的管理和技术措施等问题；在违反资源和资质管理规定方面，重点整治“黑宽带”和未履行网站备案手续等问题。

  （https://wap.miit.gov.cn/jgsj/xgj/gzdt/art/2021/art_b86f1d15c9824f3297090330353ce2f3.html）

  简析：据工信部官网消息，工信部启动的此次互联网行业专项整治活动是工信部在前期 APP 专项整治的基础上，进一步梳理的互联网行业内社会关注度高、影响面广和群众反应强烈的热点、难点问题。从数据安全方面，整治数据处理活动未按要求采取必要的管理和技术措施等问题，释放出监管执法对于数据安全问题的关注。预计《数据安全法》施行及《网络安全审查办法》修订稿通过之后，各主管部门将加强数据安全等方面的监管执法。作为数据处理者的企业有必要识别、评估其数据处理活动的现状，结合履行网络安全等级保护的情况，判断是否具备相应数据安全管理制度及采取了相应合适保护水平的技术措施，确保履行数据安全合规义务。

➢ 境外执法

✧ 意大利

- 7 月 5 日，意大利数据保护机构 Garante 对西班牙的一家外卖平台 Foodinho 处以 260 万欧元的罚款。Garante 认为 Foodinho 的应用程序可能存在算法歧视，违反欧盟《通用数据保护条例》的透明度和处理原则，同时还违背了意大利最新颁布的关于保护使用数字平台的劳动者权益的立法。对于上述问题，Garante 给予 Foodinho 150 天的时间进行必要的整改，并计划对其母公司 Glova 的全球数字平台展开调查。
（https://www.dataguidance.com/news/spain-aepd-fines-individual-€1500-disclosing-personal）

✧ 澳大利亚

- 7 月 23 日，澳大利亚信息专员及隐私专员（Australian Information Commissioner and Privacy Commissioner）Angelene Falk 认定 Uber（Uber Technologies, Inc. 及 Uber B.V.）妨碍了约 120 万澳大利亚人的隐私；Uber 由于未能妥善保护澳大利亚消费者和司机的个人信息，导致个人信息在 2016 年 10 月和 11 月遭受网络攻击被获取。Uber 要求黑客销毁了数据且无证据表明存在进一步的数据滥用，澳大利亚信息专员办公室（the Office of the Australian Information Commissioner, OAIC)的调查聚焦在 Uber 是否采取了预防性措施以保护澳大利亚用户的数据。Falk 专员认定 Uber 违反了《1988 年隐私法案》，未能采取合理措施保护澳大利亚用户的数据免于受到未经授权的访问，未按要求销毁或采取去标识化措施确保数据不能识别个人。Uber 将近一年后即于 2017 年 11 月才公开披露该数据泄漏事件。Falk 专员责令 Uber：（1）准备、执行及维持数据保留及销毁制度、信息安全计划、事件应急预案以确保符合澳大利亚隐私法；（2）任命一名独立的专家审核、报告前述制度、计划的执行情况，并向 OAIC 提交报告，并根据报告建议作出任何必要的调整。
（https://www.oaic.gov.au/updates/news-and-media/uber-found-to-have-interfered-with-privacy/）

行 业 新 闻

➢ 境内新闻

- 6 月 25 日，我国 SM4 分组密码算法正式成为 ISO/IEC 国际标准，是继 SM2/SM9 数字签名算法、SM3 密码杂凑算法、祖冲之密码算法和 SM9 标识加密算法之后，我国又一个商用密码算法被纳入 ISO/IEC 国际标准正式发布，标志着我国商用密码算法国际标准体系进一步完善，展现了我国先进的密码科技水平和国际标准化能力，对提升我国商用密码产业发展、推动商用密码更好的服务“一带一路”建设具有重要意义。
（https://www.oscca.gov.cn/sca/xwdt/2021-07/08/content_1060866.shtml）

- 7 月 8 日，英国《金融时报》报道中国运动社交平台 Keep、博客平台喜马拉雅均已搁置赴美 IPO 计划，同日医疗科技公司零氪科技也搁置了赴美 IPO 计划。业界认为，多家企业紧急取消赴美 IPO 计划可能与此前国家网信办下架“滴滴出行”App 事件有关，并预测国家可能加大对 VIE 架构公司在境外上市的监管力度。
（https://www.ft.com/content/7123266e-94c1-45cb-a133-8f1c0b907c25
https://businesshala.com/exclusive-chinas-linkdoc-shelves-211-mln-us-ipo-after-regulatory-crackdown/）

- 7 月 13 日，根据上海证券交易所《科创板上市委 2021 年第 48 次审议会议公告》，云从科技集团股份有限公司（“云从科技”）符合发行条件、上市条件和信息披露要求。云从科技定位为提供高效人机协同操作系统和行业解决方案的人工智能企业，在业界与北京市商汤科技开发有限公司、上海依图网络科技有限公司、旷视科技有限公司被合称为“AI 四小龙”。本次云从科技上市获批，将成为国内 AI 领域第一家上市企业。
（http://kcb.zqrb.cn/html/20210720/news-334-488048.html）

- 7 月 13 日至 15 日，由中国互联网协会主办的 2021（第二十届）中国互联网大会“新阶段、新理念、新格局——互联网引领数字经济新发展”在北京国家会议中心召开。论坛上，中国互联网协会、工业与信息部相关领导为首批签署《互联网平台经营者反垄断自律公约》的阿里巴巴、腾讯、字节跳动、华为、百度、京东、科大讯飞等 33 家互联网企业授牌。400 余位政府部门领导、院士、国内外行业专家及企业代表针对 5G 应用、工业互联网、数字政府、数据安全、数据治理、数字孪生、未成年人保护、知识产权等热门话题发表了精彩观点。
（参考来源：南方都市报，记者黄莉玲）
（https://mp.weixin.qq.com/s/AlmkS-OCGz49kvAl0_ARcg）

- 7 月 20 日，以“携手应对数据安全威胁挑战”为主题的 2021 年中国网络安全年会在北京成功召开。本届中国网络安全年会由国家网信办指导，国家计算机网络应急技术处理协调中心（CNCERT/CC）主办，会上发布了《2020 年中国互联网网络安全报告》（“《报

告》”）。《报告》汇总分析了 CNCERT 自有监测数据和网络安全应急服务支撑单位数据，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。

（http://www.cac.gov.cn/2021-07/21/c_1628454189500041.htm）

- 7 月 22 日，人力资源社会保障部同国家发展改革委员会、交通运输部、应急部、市场监管总局、国家医疗保障局、最高人民法院、中华全国总工会八部门共同制定的《关于维护新就业形态劳动者劳动保障权益的指导意见》（“《意见》”）正式公布。近年来，平台经济迅速发展，创造了大量就业机会，依托互联网平台就业的网约配送员、网约车驾驶员、货车司机、互联网营销师等新就业形态劳动者数量大幅增加。《意见》针对新就业形态劳动者面临的痛点、难点问题，从劳动报酬、休息、劳动安全、社会保险等多方面补齐了制度短板。

  （参考来源：人民日报，记者李心萍）

  （http://www.mohrss.gov.cn/SYrlzyhshbzb/dongtaixinwen/buneiyaowen/rsxw/202107/t20210723_419155.html）

- 7 月，中国信息通信研究院云计算与大数据研究所发布《企业数字化治理应用发展报告（2021 年）》（“《报告》”）。《报告》指出数字经济时代，企业作为社会治理体系中重要的一环，在数字经济时代加速数字化转型的过程中，同时面临着严峻的治理挑战。《报告》包括四章及其附录，分别对企业数字化治理提出了包含治理目标、数字化治理战略、数字化治理机制、数字化治理应用、数字化治理对象等层面的企业数字化治理的体系；从各关键领域产生背景、最新理念和最佳实践入手，以技管结合为主线总结归纳典型应用现状和典型特征；详细分析了各关键领域发展过程中的关键问题、重难点问题，并针对性提出实施建议；从多元共治的角度提出企业数字化治理应用发展建议。附录中针对各领域数字化治理行业优秀实践进行了筛选和归纳，提炼案例核心特色和价值。该《报告》对企业数字化治理具有重要参考意义。中国信息通信研究院 7 月还发布了《可信人工智能白皮书》《云计算白皮书》《区块链基础设施研究报告》《医疗物联网安全研究报告》等研究成果。

  （参考来源：中国信息通信研究院）

  （http://www.caict.ac.cn/kxyj/）

➢ 境外新闻

✧ 美国

- 7 月 4 日，雅虎财经报道称，美国律师事务所 Labaton Sucharow 宣布将代表滴滴的全球股东调查潜在的证券索赔。此前在滴滴上市未及 48 小时，中国监管部门宣布对“滴滴出行”实施网络安全审查后其股价应声下跌。而 Labaton Sucharow 则试图通过提起集体诉讼挽回股东的损失。
  （参考来源：微信公众号“经济新工场”）
  （https://finance.yahoo.com/news/didi-alert-national-law-firm-140000975.html）

- 7 月 12 日，网络安全类媒体 CyberNews 报道，领英 （LinkedIn）在过去四个月内第三次遭遇恶意进行的大规模数据抓取。从数亿 LinkedIn 用户个人资料中收集的数据档案再次出现在黑客论坛上，目前正在以未公开的价格出售。据该论坛帖子的作者称正在出售从 6 亿份领英个人资料中收集的信息，并宣称此次的数据较以往更新，质量更好。
  （https://cybernews.com/news/threat-actors-scrape-600-million-linkedin-profiles-and-are-selling-the-data-online-again/）
  简析：社交媒体等平台类公司对于用户信息应尽到何种程度的保护义务，是否应该限制第三方抓取数据值得持续关注。美国 HiQ Labs 抓取 LinkedIn 用户数据的重审案件，值得关注。

✧ 英国

- 7 月 6 日，据路透社报道，英国航空公司 42 万名客户及员工数据泄露案件已达成保密和解协议。此前，英国数据保护监管机构信息专员办公室（ICO）曾就该案对英国航空公司处以 2000 万英镑（约 1.7 亿人民币）的最终罚款，成为英国历史上最大数据违规处罚案，但 ICO 的罚款并不包括对数据泄露受害者的任何赔偿，随着和解协议的达成，这起集体诉讼案件或许迎来最终结局。
  （https://www.reuters.com/business/aerospace-defense/british-airways-reaches-settlement-with-customers-over-2018-data-breach-2021-07-06/）

热 点 评 述

《数据安全法》将于 2021 年 9 月 1 日正式生效施行。滴滴事件发生后，我国启动了《网络安全审查办法》修订工作，数据安全问题引起了社会各界的广泛关注。本数据合规团队申晓雨合伙人律师应新闻媒体“健康界”邀请，为《〈数据安全法〉出台后，AI、大数据企业如何自处？》一文提供专业观点支持，对 AI 智能企业风控提出前瞻建议，其中涉及介绍及评述《数据安全法》《网络安全审查办法》（修订草案征求意见稿）的一些重点内容。

《数据安全法》出台后，AI、大数据企业如何自处？

日前，滴滴在上市前夕被国家互联网信息办公室实行网络安全审查，在这之前，有媒体称讯飞输入法因违规收集个人信息遭下架……这一切，都与不久前发布的《数据安全法》不无关联。

一时之间，《失控》作者凯文·凯利曾经的“大数据缔造大公司”理论正在遭受挑战，“数据石油”似乎正在变成“数据梦魇”。

人工智能三要素为算力、算法与模型。数据是其中必要的信息通路。但是，我国数据相关法规远滞后于技术发展，长期以来，AI 医疗一直在“摸着石头过河”，甚至是“半黑不白”。

廊坊市第四人民医院信息科主任郝振兴告诉健康界，由于没有数据分级分类目录、没有开放权限门槛，医疗机构只能成立伦理委员会，自行制定数据管理制度。

“随着相关法律的出台，一些人工智能公司为训练模型，采取的获取医疗数据的模式将面临合规性的考量，医疗机构在与其合作时也需要加强合规性管理。”某医院信息中心主任白晶表示。

那么，这场风波是否会波及到 AI 医疗企业？对《数据安全法》，医疗机构、产业界怎么看？

最快法规出台，试解数据开放难题

2020 年 6 月 28 日公布草案，到 2021 年 6 月 10 日通过，《数据安全法》历经三次审议，并于 2021 年 9 月 1 日正式施行，可见数据安全立法的急迫性。

四川省律师协会医药卫生法专业委员会副主任邓明攀律师表示，“加快推进数据安全立法进程的背后，是行业普遍数字化转型发展的必然要求，也是加强数据保护、强化数据全流程管理、规范数据产业发展的应有之义。”

数据，是 AI 公司的“硬通货”，根据国家药监局《深度学习辅助决策医疗器械软件审核要点》，数据收集在合规基础上，要尽可能来自多家、不同层级的临床机构，以保证数据多样性，提高算法泛化能力。

《数据安全法》出台，AI 医疗企业是否将面临数据合规风险？北京中医药大学法律系医药卫生法学副教授邓勇给了健康界肯定的答案：“堪忧！AI 医疗企业的合规意识普遍不是很强，对数据安全的研判不够。”

“很多人工智能、大数据企业，都有过度收集数据的倾向，如何规范获取数据，合规地存储和使用数据，需要公司法人和管理者认真考量。”白晶说道。

但是，对于这种判断，产业界却另有说法。

“医疗数据合规审查很早就开始了，从 2019 年开始，对数据安全、网络安全和用户隐私保护的监管开始升级，大家的数据保护意识一直在增强。同时，当 AI 的模型成熟之后，需要的产品颗粒度很细，大量收集数据对 AI 企业来说价值并不大。”汇医慧影 CIO 张路说道。

商汤科技副总裁张少霆告诉健康界，商汤在内部成立了人工智能伦理委员会与数据安全委员会，在使用医疗数据进行产品研发和临床试验时，都经过医院严格的伦理审核，并由医院完成数据脱敏工作，再经过商汤伦理委员会审核，才能用于产品研发和临床试验使用。

“我们的数据是绝对不出院的”“数据使用都经过了伦理委员会”“医院签订了知情同意书，所有数据都知情同意”是相关企业的普遍回应。

行业方和产业方各执一词，为何会出现这种现象？医疗数据的使用边界在哪里？《数据安全法》的出台，对产业将带来什么影响？

医疗机构“战战兢兢”

在强监管的医疗行业，医疗数据主要存储在医疗机构和政府平台。

AI 公司数据获取方式包括三类，一是公开的多中心数据集；二是企业自行收集；三是通过医院获取。

“2016 年左右，隔一段时间就会有几家 AI 公司来跟医院要拿数据合作，AI 与医疗结合很火热。”西安交通大学附属第一医院首席科学家钱步月向健康界介绍，医疗 AI 公司从医院获取数据的方式分为两类，科研项目立项或提供软件使用。

由于医院欠缺数据分析能力，会与第三方企业共同选定科研课题，企业在医院内部部署服务器，通过处理、分析医疗数据来验证产品模型。为保护数据安全，大部分医院都会要求

AI 医疗公司将服务器部署在医院本地，通过 web service 方式提供接口，同时，敏感数据请求需要伦理委员会通过。

“虽然是本地服务器，但高级运维人员权限很高，如果医院没有应用堡垒机，对数据的操作不会留痕，有些部门到医院检查需要把数据库的备份带走，虽然跟医院报备过，但因为缺乏数据保护规定，还是存在风险的。”郝振兴告诉健康界。

某医院信息中心主任李雷表示：“有一些 AI 企业，会以系统免费或低价的形式与医疗机构合作，但会在合约中要求医院将相关数据上传平台，这是一种变相购买数据。虽然合作签定了合同，合同的签定流程也是合规的，但在数据保护的细节处理上还是有不尽如人意的地方，即使对个人信息做了脱敏处理。”

此外，健康界了解到，AI 医疗火热时期，还出现了一批第三方数据公司。“这些数据公司不止是卖医疗数据，包括人脸识别、个人信息他们都卖，他们的医疗数据来源主要是县域医院，虽然单个医院患者体量不大，但汇集起来还是有价值的。”

某企业负责人王超向健康界透露，第三方数据公司在 2017 年左右最为活跃，隔三差五就会有第三方数据公司给 AI 公司打电话兜售数据。这些第三方数据公司提供的数据普遍体量不大，但颗粒度较小，能够涵盖 AI 医疗的热门领域，肺结节、糖网等。

“还有一些云影像平台，以提高患者下载速度为由要求医疗机构把影像数据批量上传到平台，无论患者使用与否。这些数据会被平台截留和利用，如卖给 AI 公司。”李雷说道。

一面是 AI 医疗企业“狂热”的合作意愿，一面是医疗机构“泼凉水”的合作态度。健康界分析认为，这背后，是此前数据法律缺位，企业与医疗机构合作只能“摸着石头过河”，医疗机构处于担忧之中：担心开放数据程序不合规；担心不合规的数据开放；担心开放数据给不合规企业；担心合规开放数据被泄漏。

苏州大学附属儿童医院质量管理办公室主任朱晨与上海市锦天城（苏州）律师事务所魏灿灿在联合撰文中，对医疗机构的“数据风险”进行了详述：

“未脱敏的个人信息在共享时将会导致个人信息的泄露。即使经过了脱敏，但实践中脱敏到何种程度并没有明确的标准，而且大量的非敏感数据聚合后也可能会产生敏感数据。医疗机构与第三方合作的过程中，如果未能进行充分的合规审查，也会增加患者个人隐私的安全风险，比如未对第三方的资质进行评估、未对双方数据对接的方案进行安全评估、未对数据传输的方式进行技术控制等。”

AI 公司直面合规挑战

“大数据是早晚延伸的趋势，打破医院的围墙，一定要讲究互联互通的应用。”北京大学肿瘤医院信息部主任衡反修曾在接受《财经网》采访时表示。

诚然，如何打破围墙，让数据安全流动，发挥数据资产最大价值，是产业界与医疗机构的共同愿望，但也是个足够复杂的议题。

早在 2018 年，《财经网》就撰文表示，医疗 AI 公司获取数据，是在法规“红线”上舞蹈。对此，邓勇告知健康界，这部分源于人工智能企业法律意识淡薄。

第一，AI 医疗企业大部分是 IT 出身，合规意识不强。对医疗行业相关法规，例如《生物安全法》《网络安全法》等健康医疗相关法规风险识别不够清晰。

第二，数据所有权不明确，属于“拿来主义”。数据获取之后，直接进行挖掘分析、清洗、加工、提炼、商业转化，在监管主体、监管手段、监管方式上不是很先进，也不及时。

第三，商业模式构建缺乏数据考量。企业更多的时间和精力集中在商业模式的设计上，从盈利最大化角度来考虑。在商业模式的合规数据安全、患者隐私保护上，关注相对较少。

“企业务必行动起来！”邓勇建议，一方面，需要加强数据相关法规学习，对照法规对内部数据进行合规审查；另一方面，需要聘请第三方科研或学术机构，学习国内外产品成熟模式，在商业模式盈利最大化与产品合规之间取得平衡。

“企业如果触碰过‘红线’，我们建议要尽快对自身的数据安全能力和数据合规体系进行加强和完善。亡羊补牢，为时未晚。从我国行政处罚体系和措施来看，整改也正是一种重要的行政监管手段。”北京市天达共和律师事务所律师申晓雨表示，AI 企业的“红线”有两点，一是要根据数据流动方向（医疗机构也可能是数据接收方），符合收集的“告知-同意”原则；二是需要符合数据安全规定。

申晓雨告诉健康界，从目前数据安全立法整体情况来看，呈现出个人信息保护立法和非个人信息类数据保护立法发展不甚平衡的局面。由此，在医疗数据收集、使用、流转过程中，企业应当特别注意的“红线”，主要参考个人信息数据交互时，数据提供方与数据接收方的权责：

作为数据提供方，在《个人信息保护法》正式颁布前，“告知-同意”是最主要的数据处理的合法基础，即收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体或其监护人的同意。

作为数据接收方，根据《个人信息安全规范》和相关司法实践，需要遵循三重授权原则，即：1.数据提供方已经取得数据主体合法有效授权；2.数据提供方对数据接收方进行适当授权；3.数据接收方超出数据主体对数据提供方的原始授权范围使用数据的，应当重新取得数据主体的授权。

申晓雨表示，无论是数据提供方，还是数据接收方，如果没有满足上述要求，就有可能

因侵犯个人信息而被个人信息主体提出侵权赔偿主张，或受到行政主管部门的行政处罚，严重时还可能触犯刑法并因侵犯公民个人信息而承担刑事责任。

在 7 月 10 日，网信办发布了《网络安全审查办法（修订草案征求意见稿）》（下称征求意见稿），根据该征求意见稿，网络安全审查制度的使用对象不再仅限于 CIIO（关键信息基础设施运营者），而是将数据处理者也纳入到监管范围内，只要数据处理者开展数据处理活动，影响或可能影响国家安全的，都需要进行网络安全审查，由此实现《数据安全法》第二十四条规定的数据安全审查制度的落地。

该征求意见稿还明确规定，掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。根据该征求意见稿，对于数据处理活动可能带来的国家安全风险，主管部门将主要考虑以下因素：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；国外上市后核心数据、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；其他可能危害国家数据安全的因素。

“医疗大数据企业普遍掌握海量个人信息，其中不乏重要数据甚至核心数据。鉴于此，即便未被认定为 CIIO，未来医疗大数据企业受数据安全审查制度规制的可能性仍然较大。”申晓雨研判。

在新冠疫情期间，某 AI 医疗企业多项技术和用户数据被黑客在网上公开售卖，虽然从数据体量来看，患者信息未被泄漏，但也暴露出 AI 医疗企业数据安全治理能力欠缺的问题。

对此，申晓雨表示，无论在数据交互中的角色如何，根据《网络安全法》和《数据安全法》的规定，AI 医疗公司或医疗机构都必须承担法定的网络安全保护义务和数据安全保护义务，采取必要的技术和组织措施加强对其网络和数据的安全保护，防止数据泄露、毁损、丢失。

在实践中，如果发生数据泄露或类似网络安全、数据安全事件，主管部门通常会遵循“一案双查”的原则，同时对侵害方和被害方展开调查。“如果被害方未能履行网络安全保护义务或数据安全保护义务，也同样将面临《网络安全法》《数据安全法》甚至《刑法》所规定的相应后果并承担法律责任。”申晓雨说道。

划不清楚的“红线”

除了人工智能企业需加强数据安全意识，申晓雨分析，我国医疗数据的立法尚未形成体系，不同法规之间的衔接、交叉和相互支撑存在瑕疵。由此，产生了划不清楚的“红线”，给企业在医疗数据合规制度建设，以及主管部门对医疗健康数据安全的监管方面都造成一定困难，综合多方内容，其中有三点原因：

第一，正如前文提及，从目前数据安全立法整体情况来看，呈现出个人信息保护立法和非个人信息类数据保护立法发展不甚平衡的局面。个人信息保护的立法走得更快。

第二，医疗数据安全保护专门立法存在空白。与美国 HIPPA 相比，截至目前，我国尚未制定一部关于医疗数据安全保护的专门立法，而关于医疗数据的收集、使用等问题，散见在与医疗医药、大健康产业有关的法律法规、规范性文件、国家或行业标准及政策中。

第三，在监管主体上存在部分空白。《中国医学伦理学》日前对此详细撰文，摘录如下：

国家药品监督管理局医疗器械技术审评中心发布的《深度学习辅助决策医疗器械软件审评要点》中，要求数据采集时将个人信息脱敏以保护患者隐私，并要求在算法设计中考虑网络安全防护。但是国家食药监局的这些要求仅针对人工智能医疗产品的设计而提出。而国家食药监局的评审人员，是否具备就人工智能医疗产品的数据安全和隐私保护的评审能力，亦存有疑问。此外，就人工智能医疗产品上市后的数据安全和隐私保护，国家食药监局并无监管权限，由此出现监管主体的空缺问题。

那么，本次《数据安全法》的出台，能够缓解医疗机构的质疑，同时提振行业信心吗？答案是，不好说。

正向来看，本次《数据安全法》的出台，延续了健康医疗大数据的监管逻辑，保护与发展并重，这鲜明体现在《数据安全法》的第十四条和第十六条。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

同时，《数据安全法》作为数据安全顶层立法的重要组成部分，规制范围十分广泛，对各行业、领域均具有约束力。

在适用对象上，《数据安全法》打破了从数据处理主体角度进行规制的思路，明确规定，该法适用于在中国境内开展的所有数据处理活动及其安全监管，以及在境外开展的损害我国国家安全、公共利益或者公民、组织合法权益的数据处理活动，覆盖了数据全生命周期和各个数据处理场景。

对医疗大数据产业而言，《数据安全法》中提出的数据分类分级保护制度、数据安全审查制度等都是刚需。

《数据安全法》出台促进了医疗机构、产业对于数据安全的重视。众多人工智能、医疗大数据企业，医疗机构均在加强对《数据安全法》的学习，并开启内部数据合规性审查。“《数据安全法》是一部既讲保护又讲发展的法律，在法律规定上有不少创新，但同时给企业数据合规带来了一系列挑战。”商汤产业研究院撰文表示。

但从另一方面来看，某医疗企业信息安全负责人陈皓向健康界表示，《数据安全法》类似于母法，更多是从法律层面让大家充分重视，提高警惕。《数据安全法》的出台，需要行政部门出台更多细则和规章。滴滴案后，数据安全法已经在执法中被引用。

2021 年 7 月 1 日，期盼已久的《信息安全技术健康医疗数据安全指南》已经正式实施。

《指南》共 11 个部分，包括医疗数据的分类体系、使用披露原则、安全措施、安全管理指南、安全技术指南等，并对代表性场景数据安全进行分析。其中，医疗器械数据安全作为典型场景之一，就涵盖了人工智能辅助决策医疗器械软件。

当然，作为指南，其中措辞只以“适宜”出现，并非强制性行政命令。什么时候能从“宜”“应”，到“需”，值得期待。

1 HIT 专家网—【医疗机构数据合规系列之一】强监管背景下医疗机构的数据合规之路
2 中国经营报—【等深线】数据安全“紧箍咒”
3 财经网—医疗 AI 公司如何获取数据?和医院结盟，在法规“红线”上舞蹈
4 中国医学伦理学—医疗领域的人工智能:法律问题与规管挑战
5 大成上海办公室—浅析健康医疗大数据的法律合规问题丨大成·实践指南