

## 2023年数据保护领域值得关注的十大趋势和问题

### 前言

2022年是《个人信息保护法》和《数据安全法》生效后的第一年，数据领域的立法和执法在这一年全面、快速的发展和推进。一方面，中共中央、国务院发布提出构建数据基础制度的二十条政策举措<sup>1</sup>，另一方面，数据保护、数据出境规则开始落地实施，各行业机构、企业相应调整和加强了数据合规工作，一些企业因违规而被监管机关处罚。本文拟在回顾2022年重大事件的基础上，梳理和总结2023年与数据保护和网络安全立法和监管相关、值得关注的十大趋势和问题。

### 1. 数据领域基础制度逐步构建

2022年12月19日，中共中央、国务院发布关于构建数据基础制度更好发挥数据要素作用的意见，提出了二十条政策举措，从数据产权、流通交易、收益分配、安全治理四方面初步搭建我国数据基础制度体系。根据意见，数据基础制度包括四项制度：数据产权制度、数据要素流通和交易制度、数据要素收益分配制度、数据要素治理制度。在保障措施方面，意见提出鼓励有条件的地方和行业在制度建设、技术路径、发展模式等方面先行先试，鼓励企业创新内部数据合规管理体系，不断探索完善数据基础制度。

可以预计，未来构建数据基础制度体系的探索将持续，相关立法也将围绕该政策导向展开。数据基础制度的建立和完善将有助于促进数据合规和高效流通，充分实现数据要素价值。

### 2. 算法监管将逐渐深入且规则更加细化

2022年算法技术和服务的监管不断深化。国家网信办等部门先后发布《互联网信息服务算法推荐管理规定》和《互联网信息服务深度合成管理规定》，对算法推荐服务提供者和深度合成服务提供者规定了一系列义务。针对互联网平台的算法安全，市场监管总局、国家网信办、工信部等九部门联合发布意见，要求平台企业制定互联网信息服务算法安全制度。国家网信办公布了首批备案的算法，并开展了“清朗·2022年算法综合治理”专项行动。为响应监管要求，相关知名App均在3月上线了算法关闭键，允许用户在后台一键关闭个性化推荐。

我们预计，针对算法领域的立法和监管将在2023年继续深入开展，并可能针对不同算法技术的应用服务提出细化的监管要求，为企业利用算法技术、提供算法服务提供详细的合规指导。在2023年初ChatGPT等话题持续火热讨论的背景下，可以预计对相关算法监管的进一步探讨也会持续和深入。

### 3. 数据出境细则逐步落地、数据出境评估成为合规

<sup>1</sup>[http://www.gov.cn/zhengce/2022-12/19/content\\_5732695.htm](http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm)

## 内控重点

“数据出境”是 2022 年数据法律热点之一。国家网信办先后发布了《数据出境安全评估办法》和《数据出境安全评估申报指南（第一版）》，明确了数据出境安全评估的申报标准、申报程序和申请材料模板。国家网信办还发布了《个人信息出境标准合同规定（征求意见稿）》，但截至目前仍处于草案阶段，尚未生效实施。此外，信安标委发布了《网络安全标准实践指南个人信息跨境处理活动安全认证规范》，而后进行修订并发布了第二版规范<sup>2</sup>。该认证规范规定了跨境处理个人信息应遵循的基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面内容。

上述规定（草案）在一定程度上明确了《个人信息保护法》项下个人信息出境三条路径的实施细则，指导数据处理者更加规范开展个人信息跨境处理活动。我们预计，2023 年将会有更加详细、具体和明确的出境规则发布以支持“三条出境路径”的落地实施。企业内部的出境合规工作也将逐步落地并形成流程化内控制度。

## 4. 网络安全审查的力度可能进一步加强

2022 年 6 月，网络安全审查办公室宣布对知网启动网络安全审查。7 月，国家网信办发布针对滴滴的网络安全审查调查结果。滴滴因违反《网络安全法》、《数据安全法》、《个人信息保护法》被罚款人民币 80.26 亿元，相关负责人也被处以 100 万元罚款。国家网信办表示，下一步其将通过罚款、责令暂停相关业务、关闭网站、处理责任人等处置处罚措施，加大网络安全、数据安全、个人信息保护等领域的执法力度以及打击违法行为，并进一步强

调其将加大网络安全审查典型案例曝光力度，以起到警示和引导作用。<sup>3</sup>

随着 2022 年初修订后的《网络安全审查办法》正式生效施行，网络安全审查已深入影响了关键信息基础设施运营者和其他数据处理者的数据处理活动、网络产品服务采购活动以及国外上市活动。《网络安全审查办法》第 16 条规定，监管部门认为网络产品或者服务、数据处理活动影响或者可能影响国家安全的，网络安全审查办公室应当按照程序报国家网信办批准，并进行相应审查。两个重大案例也表明了监管部门加强对重要和敏感数据安全监管的态度，也预示着网络安全审查活动将持续展开和护航国家的网络安全。

## 5. 数据领域规则不断纵深细化、通过标准形成实践指引

2022 年，各相关行业领域特别是强监管领域进一步制定与所在行业密切相关的数据保护和网络安全法规。例如，在医疗行业，国家卫生健康委、国家中医药局和国家疾控局联合发布《医疗卫生机构网络安全管理办法》；在能源行业，国家能源局发布《电力行业网络安全管理办法》和《电力行业网络安全等级保护管理办法》；在工业和信息化领域，工信部发布《工业和信息化领域数据安全管理办法（试行）》。国家网信办还针对未成年人专门制定了《未成年人网络保护条例（征求意见稿）》。另一方面，各类与信息保护和安全相关的标准和指南文件也陆续起草、制定和发布，例如《信息安全技术 重要数据识别指南（征求意见稿）》，以及若干聚焦于隐私政策、移动智能终端所安装的 App 以及应用商店对拟上线 App 的审核管理等方面的国家标准草案。

<sup>4</sup>

<sup>2</sup> 《个人信息跨境处理活动安全认证规范 V2.0》

<sup>3</sup> [http://www.cac.gov.cn/2022-07/21/c\\_1660021534364976.htm](http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm)

<sup>4</sup> 详见《信息安全技术 互联网平台及产品隐私协议要求》（征求意见稿）、《信息安全技术 移动智能终端的移动互联网应用程序

（App）个人信息处理活动管理指南》（征求意见稿）和《信息安全技术 应用商店的 App 个人信息处理规范性审核与管理指南》（征求意见稿）。

我们预计，在 2023 年，不同行业、领域内的监管机构将基于本行业、领域的特点，继续制定所在行业和领域适用的数据保护规则和指南，这些监管规则和指南将趋向细节性和可操作性，为市场参与者提供更加明确的合规实践指引。

## 6. 数据领域相关监管执法力度将持续加大、执法流程更加明确

2022 年，个人信息保护的监管和执法活动进一步深入开展。整体上看，以日常通报违规 App 名单的监管活动为主，辅之以“回头看”、“安全检查工作”等专项整治行动，并呈现出常态化执法的特点。<sup>5</sup>

另外，国家网信办发布了《网络安全法》修订草案。修订草案提升了有关危害网络运行安全或内容管控的处罚额度，同时加大了对相关责任人的处罚力度，对于与个人信息相关的违法行为，修订草案建议转致采用《个人信息保护法》项下的个人信息保护法律责任制度。此外，国家网信办和工信部还分别发布行政执法程序规定的修改稿征求意见。总体而言，上述规定均是适应数据和信息化领域的发展和监管形势、贯彻落实《行政处罚法》的需要。

未来，随着上述法律法规的正式生效实施，网信部门和工信部门在网络安全、数据安全和个人信息保护领域的执法权限、范围和程序将更加明确，并在此基础上进一步加大网络执法监督检查工作力度，不断完善网络执法监督检查工作体系，强化网络执法日常监督检查。

## 7. 数安领域相关认证机制不断完善

国家网信办和市场监管总局于 2022 年 6 月和 11 月分别发布了关于开展数据安全认证和关

于实施个人信息保护认证的公告，并配套发布《数据安全认证实施规则》和《个人信息保护认证实施规则》。原则上，这两项认证均不是法律项下的强制性要求，但企业被鼓励取得该等认证作为数据安全合规工作和具备个人信息保护能力的证明，并且可在认证过程中识别相关数据安全风险管理以及与个人信息处理活动相关的风险，从而进行相应整改和完善。7 月，市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》，意在开展国家统一推行的网络安全服务认证工作，并鼓励网络运营者等广泛采信网络安全服务认证结果。此外，信安标委在 12 月发布了《个人信息跨境处理活动安全认证规范 V2.0》，该认证仅适用于未触发数据出境安全评估申报门槛的个人信息出境场景。

从 2022 年发布的上述认证公告和规则来看，国家在网络数据处理、个人信息处理、个人信息出境以及网络安全服务等方面陆续推动实施多项认证工作，并大力鼓励企业通过认证方式贯彻落实有关规定。我们预计，“认证”未来有望成为不同市场参与者在开展合规工作时可选择的路径之一。与此同时，认证规则，例如认证机构的确定、认证申请条件 and 流程等，还有待进一步完善和细化。

## 8. 地方持续开展数据相关立法，落地情况有待观察

随着国家层面的数据立法逐渐完善，部分省市结合地方实际发展情况，相继出台了地方数据条例。据不完全统计，截至 2023 年 1 月，包括上海、广东、深圳、浙江、山东、安徽、吉林、山西、海南、天津、贵州和沈阳在内的 24 个省市地区的数据相关地方条例已正式发布或实施。例如，《深圳经济特区数据条例》自 2022 年 1 月 1 日起施行，是国内

<sup>5</sup> 据统计，国家网信办及其地方网信部门在 2022 年查处 294 款存在违法违规处理个人信息行为的 App，全年累计下架 420 款违规 App。工信部在 2022 年上半年组织检测了 118 万款 App，责令整改 780 款 App，公开通报 255 款未按要求完成整改的 App，下半年对 227 款 App

(SDK) 提出整改要求，并公开通报 47 款未按要求完成整改的 App (SDK)。在地方层面，各地通信管理局和网信部门也结合本地情况陆续开展了 App 个人信息安全整治工作，对相关侵害用户权益和安全隐患的 App 进行通报。

数据领域首部基础性、综合性立法。《浙江省公共数据条例》自 2022 年 3 月 1 日起施行，是全国首部以公共数据为主题的地方性法规。

2023 年可能会有更多省市持续、有序推进地方数据立法。地方数据法规的生效实施时间均相对较短，各地具体落地实施情况及对企业的影响仍有待观察。

## 9. 个人信息相关民事诉讼增多，公益诉讼仍将持续

《民法典》距今实施已两年有余，司法实践中有关个人信息保护的民事诉讼案件也越来越常见。在近期最高院发布的人民法院贯彻实施民法典典型案例（第二批）<sup>6</sup>中，就包括“孙某燕与某通信公司某市分公司等隐私权、个人信息保护纠纷案”。而各级检察机关对于个人信息的公益诉讼案件也继续呈现增长趋势。根据最高检察院统计，2022 年全国检察机关立案办理公益诉讼案件 19.5 万件<sup>7</sup>，同比上升 15%，绝大多数案件在诉前解决了公益损害问题。此外，各地的互联网法院作为实践中处理个人信息保护纠纷案件的第一线裁判者，也经常发布个人信息相关典型案例。

随着数字经济快速发展和公民个人信息保护意识提高，预计未来将会出现越来越多与个人信息与隐私保护相关的民事诉讼案例。由于个人信息侵权案件常常因涉及大规模侵害个人信息行为具有

影响公共信息安全领域社会公共利益的性质，未来针对个人信息发起的公益诉讼也可能成为常态，值得持续关注。

## 10. 数据安全仍是合规重点、体系搭建成关键

数字化发展为社会和经济带来众多便利和机遇的同时，也带来了越来越严峻的网络安全和信息安全风险，这些风险不仅会影响个人财产和隐私安全，还会对社会公众利益和国家安全带来危害。2022 年国内发生了若干起与数据相关的安全事件。就 2023 年网络安全发展态势来看，企业面临的网络攻击风险不容小觑，防范数据泄露风险依然是数据合规工作的重点。建议企业应该结合自身情况，采取合理和适当的措施，建立数据安全治理体系，以最有效的方式保护数据的全生命周期安全。

## 结语

以上是在总结过去一年数据领域重大立法和执法事件的基础上，对 2023 年所做的一些展望，以期抛砖引玉，供相关从业人员进一步探讨。2023 年，中国将持续激发数据要素活力，全面发展数字经济，我国数据保护相关监管体系必将进一步完善和发展，我们将与各企业一同密切关注数据保护和网络安全领域立法动态和监管活动的新变化和新进展，并持续为客户提供及时有效的合规建议。

董 潇 合 伙 人 电 话：86 10 8519 1718

邮 箱 地 址：dongx@junhe.com

郭 超 律 师 电 话：86 10 8553 7733

邮 箱 地 址：guoch@junhe.com

本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息，敬请关注君合官方网站“[www.junhe.com](http://www.junhe.com)”或君合微信公众号“君合法律评论”/微信号“JUNHE\_LegalUpdates”。



<sup>6</sup><https://www.court.gov.cn/zixun-xiangqing-386521.html>

<sup>7</sup>[https://www.spp.gov.cn/zd gz/202302/t20230215\\_601611.shtml](https://www.spp.gov.cn/zd gz/202302/t20230215_601611.shtml)