网络安全、数据治理与反垄断合集（上篇）

金杜律师事务所
KING&WOOD MALLESONS

网络安全、数据治理与反垄断合集（上篇）

有关本出版物的咨询及意见和建议，请联系：
publication@cn.kwm.com

序 言

2021-2022 年，对于中国网络安全数据保护和反垄断，都是应当被铭记的。

首先，在法律层面上，《数据安全法》和《个人信息保护法》于 2021 年下半年生效，与《网络安全法》共同构筑了中国网络空间安全、数据 / 个人信息保护的骨架。《反垄断法》在实施 14 年后修法，于 2022 年 8 月 1 日生效，并明确了经营者不得利用算法、数据或平台规则从事垄断行为。

与法律相配套的国家标准、部门规章在数据安全个人信息保护方面纷至沓来，《关于平台经济反垄断指南》等，也都在细化规则上，显示着立法者对于实施法律的耐心、决心和努力。各地方政府和人大，在地方立法上也百舸争流，对于数据产权交易、数字经济促进、创新，对于地方优势产业及其数字化转型，都在做出非比寻常的努力，地方法规和鼓励政策纷纷出台，显示出地方政府对地方数字经济的巨大热情与信心。

金杜反垄断与网络安全、数据合规及治理团队，从参与立法到深度实践，我们始终与立法、执法、产业、学界一起，研究最前沿的法律问题，并在数据与反垄断法律问题结合点上，寻求平衡，探讨诸如人工智能、大数据、云计算等新兴技术与竞争的关系，算法是否可以成为新的合谋方式，隐私保护是否可以成为竞争法下的合理理由。

《反垄断法》是有趣的，《网络安全法》《数据安全法》《个人信息保护法》是有趣的，二者相加相结合，更是有趣的。我们的团队就是在这有趣的法律领域中自由践行，并成此集以记心得。

《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）于 2022 年 12 月 19 日公布，涉及数据产权、流通交易、收益分配、安全治理四个方面，初步搭建了我国数据制度体系，以赋能实体经济，促进高质量的发展。这些问题，既是数据安全 / 治理需要探讨的问题，也是反垄断需要探讨的问题。

我们身在其中，乐在其中，也希望成于其中！

2022 年 12 月 22 日 壬寅冬至日

宁宣凤

合规业务部管理合伙人
金杜数字经济国际法律服务中心负责合伙人

金杜数字经济国际法律服务中心

作为引领未来的新经济形态，数字经济已成为推动我国经济高质量发展的重要引擎。“十四五”期间，中央推出新的政策和举措，扶植数字经济的发展，明确将数据作为新型生产要素，在国家层面正式确认数据的基础资源地位，正式开启数字经济社会新阶段。在数字经济社会发展的同时，社会各界亟需从理论和实践角度研究和分析数字经济社会产生的法律关系，例如分享经济中的灵活用工劳动关系、个人信息处理者与个人信息主体的委托关系、智慧城市构建中多主体的法律责任和权益等。

作为国内首家专注数字经济领域法律研究和法律服务的国际化创新型综合法律服务平台，金杜数字经济国际法律服务中心（以下称“数字中心”）整合行业头部资源，组成跨学科、跨法域的研究战队，致力于内容、产品和业务模式的创新。数字中心运用智慧和经验，为数字经济立法和规则制定提供极具价值的专业研究成果，同时将前沿研究转化为具有商业价值的法律服务和产品，帮助企业客户成功应对数字经济浪潮新挑战。

数字中心依托金杜律师事务所在法律实践和平台资源的领跑优势，结合数字经济的无疆界特点拓展全新服务平台和产品，将“法律 + 数字经济”的构想付诸实践。

目录

个人信息保护

法律前沿

“潮平两岸阔，风正一帆悬”——2022年金杜网络安全与数据合规治理领域年度法律观察

宁宣凤 吴涵 姚敏侣 吴真恺

开篇词

2022年全球网络安全与数据合规治理格局纵深推进，欧盟加速数据保护和数字经济一体化进展，年末在推进与美国的跨境数据传输协议中又迈出重要一步，以数据主权理念为基础的数据保护规则进一步扩大国际影响力，建立数据保护共识的“朋友圈”。同时，我们也看到诸如印尼等东南亚国家数据安全立法出现新变化，数据保护的工具箱也显现出多样化的趋势。在趋同存异的国际大环境下，**我国网络空间治理框架不仅逐步成型，而且在“以安全促发展”的目标下平稳落地**。数据安全和个人信息保护出台更加细节化的规则，如何通过数据保护促进数字经济发展也具备明确的指导方向。

如同习近平主席指出，当前，世界之变、时代之变、历史之变正以前所未有的方式展开。在国际规则的迎合和差异化之间，数据保护与数字经济增长的平衡之上，动态的博弈将是长期的时代命题，“在分裂的世界中加强合作”将是国际竞争的主旋律。

在新的一年以及可预见的未来，我们理解，国际数据竞争将持续在法律、贸易、冲突等各个领域愈演愈烈，而同时我们也将依然警惕以数字化为基础的深度智能化对个人主体性以及社会群体认知的消磨和冲击。要认识和把握数字社会的规律，力争与新型社会形态的自洽和共处，我们需要及时地“回头看”来总结经验，“抬头看”以鉴往知来，确保“潮平”与“风正”，期待我国的数字经济发展能“一帆风顺”的同时，也祈盼世界各国在向智能化社会的转变中“云共千帆舞，浪淘万里沙”。

一、具化：安全工具箱的丰富与成熟

（一）网络安全审查

自2022年2月15日开始施行的新《网络安全审查办法》，无疑是过去一年中在国家安全和网络安全合规领域中的一个里程碑；而随着新法规修订后正式实施接近一周年，最集中的变化在于人们对于“什么是网络安全审查”“何时需要进行网络安全审查”和“怎么进行网络安全审查”有了更加全面和深入的认识。规则的确定和透明化，将更有助于形成稳定的发展预期。其中，除了关键信息基础设施供应链安全保障措施之外，市场最为关注的规则便是新《网络安全审查办法》第七条将安全审查的适用范围拓展至“掌握超过100万用户个人信息的网络平台运营者赴国外上市”的情形。该新增条款沿用了《网络安全法》的法律定义，规定了网络平台运营者应当主动向有关主管部门申报网络安全审查的客观条件。

由于与市场主体上市活动密切相关，网络安全和数据合规成为相关主体活动中的重要环节，数据合规与企业上市的互动愈加频繁。根据《< 网络安全审查办法 > 答记者问》，网络平台运营者应当在向国外证券监管机构提出上市申请之前，申报网络安全审查。因此，国外证券机构对于上市主体的监管规则及其对于我国国家安全和境内用户利益的影响，成为网络安全审查中重点关心的对象。在与上市监管合规的规则衔接方面，我国证监会于 2022 年 4 月 2 日就《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定》面向社会公开征求意见，尽管该规定目前仍未正式生效，但显然已经对上市主体在上市过程中绷紧网络安全的神经、压实数据安全责任产生了深远的影响。

《网络安全审查办法》实施的最终目的，是在确保国家安全的前提下支持境内企业依法依规合理利用境外资本市场融资发展。2022 年，在境内外上市监管合作方面也取得了进展。根据官方消息，我国证监会和财政部通过与 PCAOB 签署审计监管合作协议并启动相关合作试点的形式，推动解决中概股企业此前在美国上市的监管冲突问题，以期在确保数据安全的前提下维护我国企业海外上市利益。

2022 年网络安全审查规则日渐明确，官方监管合作不断推进，给予了投资者和市场以更多的信心。但需要注意的是，我国境外上市企业仍然应当积极承担网络数据安全主体责任，根据《数据安全法》《个人信息保护法》及一系列已确立和执行的配套规则充分做好内部的数据合规工作，在配合证券监管和提交审计材料之前对于涉及国家安全和公共利益事项的国家秘密信息、行业重要数据和核心数据，以及用户敏感个人信息履行保密义务和脱敏责任。根据我们的行业观察，目前不少企业已经逐渐意识到并建立起了框架成熟、行之有效的审计文件数据合规审阅制度和流程。我们理解，这将会进一步助力企业合法合规发挥境外资本的利用效率。

（二）关键信息基础设施保护

2021 年 7 月 30 日，国务院发布《关键信息基础设施安全保护条例》（《条例》），并自 2021 年 9 月 1 日起施行。《条例》明确了监管体制、关键信息基础设施范围和认定程序、保护工作部门职责、运营者责任义务、保障和促进措施、法律责任等内容，为关键信息基础设施保护工作提供了法制保障。**如今，《条例》颁布实施已有一周年之余，我国关键信息基础设施领域的法治保护也取得了初步成效**。

首先，《条例》相关系列配套标准陆续公布，我国关键信息基础设施安全保护标准体系开始布局。2022 年 11 月 7 日，国家标准《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）发布，并将于 2023 年 5 月 1 日起实施。这是我国第一项关键信息基础设施安全保护的国家标准，该标准提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防的关键信息基础设施安全保护 3 项基本原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置 6 个方面提出了 111 条安全要求，为运营者开展关键信息基础设施保护工作提供了强有力的标准保障。[1] 围绕上述核心标准，我国关键信息基础设施相关在研的配套标准目前已经初步涵盖了总体要求、识别认定、安全防护、检测评估、监测预警和事件处置等方面，主要用于指导运营者、网络安全服务机构等相关单位共同构建关键信息基础设施安全保障体系。[2]

其次，在关键信息基础设施认定方面，《条例》界定的关键信息基础设施涉及行业领域众多，运行状态、防护需求各异，相关行业认定规则和操作标准有待继续出台。值得注意的是，《条例》施行一年以来，交通、能源、证券期货业等行业和领域主管部门加快推动关基保护工作在本行业、本领域的落地实施。例如，交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》，就公路水路的关保工作进行专项规定；国家卫生健康委等部门发布《医

[1] https://www.cqn.com.cn/zj/content/2022-11/09/content_8878030.htm
[2] 《专题·关基保护 | 关键信息基础设施安全国家标准进展》，https://mp.weixin.qq.com/s?__biz=MzA5MzE5MDAzOA==&mid=2664166817&idx=1&sn=fd8e05811d4bd685205d4f093e70cac9&chksm=8b5ef758bc297e4e6637d4b424b0a86ed767612c7c5e4f37e660828474b192ec02359d888fce&scene=27。

疗卫生机构网络安全管理办法》、中国证监会发布《证券期货业网络安全管理办法（征求意见稿）》、国家能源局发布《电力行业网络安全管理办法（修订征求意见稿）》，将关键信息基础设施运行安全作为重要内容之一。[3] 其中，电力行业关键信息基础设施的认定规则，已经在制定中。2022 年，国家能源局安全监管司已向电力行业企业对相关文件征求意见。以发电侧为例，认定规则分为火电、水电、新能源、向计划单列市提供电力的发电厂（站）4 种。[4] 不难看出，以电力行业为代表的国家重点行业领域关键信息基础设施的识别认定工作也将陆续开展，相关重点行业可持续关注监管动向。

（三）重要数据识别与保护

2021 年末，全国信息安全标准化技术委员会发布的《网络安全标准实践指南——网络数据分类分级指引》（以下简称《网络数据分类分级指引》）对行业领域数据分级的原则与方法提出了一系列指导原则。2022 年 1 月，《信息安全技术 重要数据识别指南（征求意见稿）》也相继发布，进一步界定了重要数据的特征。该稿要求从国家安全、经济运行、社会稳定、公共健康和安全等角度识别重要数据，通过对数据分级，明确安全保护重点，使一般数据充分流动，重要数据在满足安全保护要求前提下有序流动，释放数据价值。

在此背景下，相关企业应根据是否涉及人口健康，资源环境、科技与政务等多方面特征对现有业务涉及数据，利用《网络数据分类分级指引》提供的原则方法进行有效地识别梳理，主动推进数据合规管理流程。尽管《网络数据分类分级指引》中对工业、电信与金融行业做出了行业区分，但当前各垂直行业重要数据识别尚待看到细致的标准性指导，这也需要各企业配合行业主管部分在实践中积极沟通落实。**我们建议企业密切关注重要数据识别方面的国家法律法规与相关标准文件的指导，为数据合规建立动态管理机制，并加强与主管部门的标准共建等工作**。

（四）数据跨境合规

1. 数据跨境合规三大机制基本成型

随着《网络安全法》《数据安全法》以及《个人信息保护法》三大法律的确立，以及相关法律法规征求意见稿的出台，**我国数据跨境制度法律框架已经完成了基础性搭建**。具体而言，若数据处理者因业务等需要确需向境外传输数据的，可以通过国家网信部门组织的安全评估、经专业机构进行个人信息保护认证、与境外接收方订立合同这三种途径来满足数据跨境的合规要求。

（1）通过国家网信部门组织的安全评估

数据出境安全评估制度在我国的数据跨境制度中占据相当重要的地位。2022 年 9 月 1 日正式生效的《数据出境安全评估办法》（下称《评估办法》）对数据处理者在数据出境申报中的程序性规则与实体评估内容均作出详尽规定，标志着我国数据出境安全评估制度正式迈入实践阶段。一方面，《评估办法》明确了评估流程，主要包括评估材料、评估流程、评估时间等，能够帮助数据处理者定位其申报进度；另一方面，就具体评估内容而言，《评估办法》第 5 条、第 8 条确立了风险自评估与安全评估相结合的评估原则，划定自评估与安全评估重点事项，第 9 条也对与境外接收方订立的数据跨境法律文件（合同）进行了规制，要求其应当明确约定数据安全保护责任义务等。

此外，国家网信办在《评估办法》生效前一夜发布了《数据出境安全评估申报指南（第一版）》，具体说明了申

[3] 《专题·关基保护｜国家关键信息基础设施安全保护的法治进展》，https://baijiahao.baidu.com/s?id=1747014241321549982&wfr=spider&for=pc。
[4] 《安恒观察：电力行业出新令，工业信息安全迎来风口》，http://stock.10jqka.com.cn/20221216/c643661335.shtml。

报流程与明确了各项申报材料，并提供申报模板以帮助企业规范、有序开展数据出境安全评估申报工作。

（2）经专业机构进行个人信息保护认证

国家市场监督管理局与国家网信办于 2022 年 11 月共同发布的《个人信息保护认证规则》，以及全国信息安全标准化技术委员会于同月发布的《个人信息跨境处理活动安全认证规范（V2.0 征求意见稿）》，对通过进行个人信息保护认证实现数据跨境的机制进行了明确规定，具体也包括个人信息保护认证的适用情形、具体流程及重点内容等。

（3）根据标准合同与境外接收方订立合同

国家网信办于2022年6月30日发布了《个人信息出境标准合同规定（征求意见稿）》（下称《标准合同规定》）和《个人信息出境标准合同》（下称标准合同）。作为《个人信息保护法》的配套制度与文件，《标准合同规定》与此前发布的《评估办法》《网络数据安全管理条例（征求意见稿）》（下称《网数条例》）等规范中有关数据跨境的规制内容互为补充。具体而言，其中包括了标准合同的适用情形与主要内容、与个人信息保护影响评估的协作、向网信部门进行事前备案及确立主管部门与监管职权等内容进行了规定。虽然该标准合同仍处于征求意见阶段，暂未落地实行，但总的来说，未来标准合同的正式实施将极大提高《个人信息保护法》中有关个人信息跨境合规措施的可执行性，并保障个人信息主体的合法权益。

2. 数据跨境合规在实践中应注意的要点

当企业根据法律法规要求判断需通过向网信部门进行数据安全评估的方式以满足数据跨境合规要求时，根据实践经验，我们提醒需注意以下事项：

第一，判断自身是否为适格的申报主体。一方面，企业应先梳理在开展涉及数据出境业务过程中的数据处理关系，在申报审查的数据处理场景中区分和明确数据处理者角色。另一方面，企业还应梳理其是否满足《评估办法》第四条规定的应当进行数据出境安全评估申报的情形。举例而言，若企业处理个人信息数量没有达到但却十分接近申报标准的情况下，企业也可相应作申报准备以充分满足合规要求。

第二，梳理待评估客体，特别是涉及出境的数据是否有可能构成重要数据。一方面，《网络安全法》《数据安全法》等规定均对重要数据的本地化提出了原则性要求，《评估办法》亦将重要数据的出境作为需进行申报的法定情形，因此无论企业作为数据处理者或受托处理者，其业务场景中的数据出境活动若涉及重要数据的，应优先就场景进行申报；另一方面，鉴于当前法律法规对重要数据的定义和分类的颗粒度较粗，企业应持续关注立法动态，特别是其涉及数据出境业务所在的行业动态。

第三，分析数据出境活动的合法性、正当性和必要性，并评估是否需要进行整改并给出具体的整改意见。具体而言，若企业属于法律法规规定的应进行申报的情况但就具体涉及数据出境的业务场景的上述问题分析中存在瑕疵，则企业应在申报材料中提供具体的整改方案以满足数据出境的合规要求，并尽量在整改期内完成整改工作。

第四，与境外接收方签署如《个人信息跨境提供协议》等法律文件以约定数据安全保护责任义务。尽管目前标准合同仍未落地，但企业在与境外接收方签署相关法律文件时若参照目前的网信办发布的《个人信息出境标准合同》内容，

则可以帮助企业在评估申报时提升数据安全保护权利义务约定的充分性，降低合规风险。

3. 数据跨境合规给跨国公司及出海企业的影响

对跨国公司及出海企业而言，数据跨境合规的落地对其在业务开展和经营管理的过程中提出了新的要求，**既是挑战，也是机遇**。具体而言，为了满足《个人信息保护法》《数据出境安全评估办法》等对数据跨境传输的合规要求，企业需对其进行全方位的数据盘点和挖掘，若符合数据安全评估申报的情况，则需及时向网信部门开展相关申报工作。若跨国公司和出海企业在进行数据盘点和盘点时发现存在暂不满足数据跨境合规要求的，需尽快开展整改工作，其次还需要充分关注其他国家或地区的数据保护法律环境等。**不可否认，数据跨境合规会对跨国公司及出海企业的具体业务开展和整体经营管理均可能产生客观和长远影响**。

但同时我们也应该认识到，一方面跨国公司和出海企业在完成并通过申报后，可充分确保其在开展涉及数据出境的业务时能充分满足监管的合规要求，因而获得了较稳定的发展环境，同时也是企业自身数据安全保护能力的一大有力证明。另一方面，**企业中心化管理的数据系统显然已经与国际数据保护发展趋势产生了明显冲突**，就企业发展长远战略来说，借由数据跨境合规的机遇，企业有望在“分布式部署”和“区域化管理”上先行一步，抢占区域全球化发展的市场先机。

（五）个人信息保护（以移动互联网应用安全为例）

1. APP 监管合规进入成熟期

2022 年是中国 App 个人信息保护立法与监管逐渐走向成熟的一年。随着《个人信息保护法》生效一年多，随着个人信息保护监管力度加强，App 合规治理受到不同机构的多方监管。目前 App 个人信息保护领域的立法除了《个人信息保护法》和国家网信办制定的规范性文件外，还包括一系列国家标准，实践中，App 个人信息保护涉及国家网信办、工业和信息化部通信管理局、公安机关和国家市场监督管理局，以及各行业领域的监管部门，针对个人信息保护监管越来越普遍适用，国家出台了《App 违法违规收集使用个人信息自评估指南》《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等一系列法律法规供企业参考与自查自纠，**移动互联网应用程序个人信息保护领域逐渐形成“立法立规——监管检查——企业自查”的合规体系**。

2. 立法更新：逐渐细化要求

2022 年以来，个人信息保护领域立法呈现日趋细化的趋势，最新立法进一步明确和扩大责任主体范围，逐渐形成治理生态圈并呈现不断扩大监管范围的趋势，对 App 数据合规提出新的升级要求。

就业务功能而言，2022 年 4 月 15 日发布的 GBT 41391-2022《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》延续监管思路，按 App 功能区分所需收集必要个人信息范围，将 App 业务功能区分为基本业务功能与扩展业务功能，多功能高度集成的 App 将实现用户主要使用目的的业务功能划分为基础业务，并按照为实现基本业务功能所收集的信息确立必要个人信息的范围。

就监管范围而言，2022 年 6 月 13 日，信安标委发布《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）》，该指南将个人信息保护监管范围扩大至 App 所依托的移动智能终端及其上操作系统，对移动智能终端的权限、预置应用软件、敏感个人信息处理等作出规定，规定了移动智能终端对 App 个人信息处理活动的管理应遵循的原则，对 App 进行安装、启动、运行、更新、退出、停用 / 卸载全生命周期管理。针对移动智能终端提供了 App 个人信息安全功能设计、管理个人信息安全风险的指南，以增强 App 收集个人信息行为的明示程度，并为 App 用户提供更多个人信息保护方面的控制机制。

就责任主体而言，2022 年 6 月 14 日，国家网信办发布《移动互联网应用程序信息服务管理规定》强化应用程序提供者与应用程序分发平台的合规义务，规定了应用程序分发平台的多项合规义务，包括按类别向省级网信部门备案上架的应用程序、健全信息内容审核管理机制、建立健全管理机制和技术手段、对申请应用程序进行审核、公开管理规则等。将应用程序分发平台纳入监管范围，体现了我国 App 个人信息保护领域治理逐渐成熟化、体系化，有利于形成成熟的治理生态圈。

3. 行业实践：“隐私设计”成为新风尚

隐私设计（Privacy by Design）原则指在产品开发阶段就考虑隐私保护问题，将个人信息保护要求纳入产品服务的设计中，隐私设计是域外立法中提出的数据保护原则，在《个人信息保护法》第五十一条等条款中有所体现，2022 年 10 月 14 日，GBT 41817-2022《信息安全技术 个人信息安全工程指南》发布，该指南给出了在需求分析、产品设计、产品开发、测试部署、运行维护等系统工程阶段的个人信息保护实施指南，并且在附录中针对常见行业给出了具体的产品设计合规要点，可作为产品“隐私设计”开发落地的参考框架。**随着用户和大众对隐私的逐渐重视和隐私保护理念的普及，“隐私设计”已经形成新风尚，我们预计未来“隐私设计”将会成为企业竞争的阵地。**

4. 未来趋势：常态化的持续监管机制

我们留意到，国家工信部于 2022 年 12 月 27 日发布《工业和信息化部关于进一步提升移动互联网应用服务能力的通知（征求意见稿）》，要求从规范安装卸载行为、落实 App 开发运营者主体责任、强化平台分发管理、规范 SDK 应用服务等多维度提升全流程服务感知，保护用户合法权益。我们预计未来针对互联网应用的常态化持续监管会成为趋势，此前，工信部亦表示在“十四五”期间针对 App 治理，将细化实化监管举措，建立全链条监管体系。凡涉及 App、小程序等应用程序的企业应当关注行业立法动态，依据当前法律框架和行业实践开展自查自纠，提前做好合规部署。

（六）互联网信息内容安全

2022 年，国家网信办发布了多项互联网信息内容治理新规，对在跟帖评论、账号信息管理、弹窗信息推送等领域加强互联网信息服务提供者和互联网用户的主体责任，加强互联网信息内容管理是维护意识形态安全、社会公平公正和网民合法权益的需要，也是防范化解国家安全风险、维护网络空间良好生态的需要。

- 2022 年 6 月 17 日，公布《互联网跟帖评论服务管理规定（修订草案征求意见稿）》（以下简称《修订稿》），向社会公开征求意见。

- 2022 年 6 月 27 日，国家网信办发布《互联网用户账号信息管理规定》（《规定》），《规定》在 2022 年 8 月 1 日起正式施行。

- 2022 年 9 月 9 日，国家网信办、工业和信息化部、国家市场监督管理总局联合正式发布《互联网弹窗信息推送服务管理规定》。

我们可以预见，在未来随着移动互联网用户不断增长，监管部门会不断深化对于互联网信息内容的治理，维护健康清朗的网络生态环境。

（七）依法行政：网信部门执法程序规定

2022 年 9 月 8 日，国家网信办对《网信部门行政执法程序规定（征求意见稿）》（《执法规定》）公开征求意见。《执法规定》明确了网信部门的执法程序，并就管辖权问题作出清晰划定。随着网络安全与数据合规领域相关法律法规的不断完善和细化，配套的执法和调查依据也不断更新，《执法规定》将取代网信办此前公布并生效的《互联网信息内容管理行政执法程序规定》，明确网信部门的行政执法范围由原来单一的互联网信息内容扩大至网络信息内容、网络安全、数据安全、个人信息保护等领域，指出网信部门在办理个人信息保护案件时可以采取查封、扣押等行政强制措施，对网信部门执法程序进行规范，同时也赋予了当事人要求举行听证、申请行政复议等权利，规范和保障网信部门依法履行职责。

二、深化：发展逻辑下的协调与平衡

（一）代表行业：“以安全促发展”及“以发展保安全”

1. 电信与互联网

作为数字经济发展的先导区，工业和信息化领域数据安全管理的重要性不言而喻。2022 年 12 月 8 日，工业和信息化部印发了《工业和信息化领域数据安全管理办法（试行）》，进一步规范工业和信息化领域数据处理活动，保障数据安全、促进数据开发利用。具体而言，其从监管范围、监管机构、监管措施三个问题出发，涵盖法律适用、数据分级、特殊保护、数据生命周期合规要求等方面。就监管范围而言，规定了工业和信息化领域数据包括工业数据、电信数据和无线电数据，工业和信息化领域数据处理者则包括工业数据处理者、电信数据处理者和无线电数据处理者；就监管机构方面，搭建了“工业和信息化部、地方行业监管部门”两层不同监管机制，分管不同工作，细化工作内容；就监管措施方面，建立了数据分级保护的原则，并体系化地明确了安全保护要求。

2. 自动驾驶

在自动驾驶监管领域，2022 年各类立法新规层出不穷，旨在全方位、多维度规制自动驾驶可能涉及的合规问题，包括但不限于自动驾驶可能涉及的道路测试、准入要求、测绘行为、数据安全、交通事故责任认定等。就当前自动驾驶的监管格局而言，存在在中央统一管理的基础上，不同部门之间协同监管、地方试点不断突破等特点。

2021 年，国务院办公厅在《关于进一步优化营商环境更好服务市场主体的实施意见》中提出应当“完善对新业态的包容审慎监管”，并以智能网联汽车为例，提出一系列鼓励和发展智能汽车行业发展的新政策。在中央的支持下，地方政府也陆续推出针对自动驾驶的监管方案，包括北京、上海、广州等多地均展开自动驾驶路测活动，并出具相关文件试水，力求产生示范标杆效应。例如，北京市出台了《北京市智能网联汽车政策先行区自动驾驶出行服务商业化

试点管理实施细则（试行）》，并于 2022 年 4 月设立了我国首个智能网联汽车政策先行区，推动道路测试、示范应用和商业运营服务，并率先发布无人配送车上路、高速公路测试、无人化测试等政策。2022 年 8 月，《深圳经济特区智能网联汽车管理条例》生效。该条例从道路测试和示范应用、准入和登记、使用管理、车路协同基础设施、网络安全和数据保护、交通违法和事故处理等多个维度对自动驾驶技术进行了细化规定。作为国内首部规制自动驾驶活动的地方性法规，该条例的出台标志着我国的自动驾驶立法迈出了关键性的第一步，同时也将促进其他地区乃至全国层面加快自动驾驶立法进程。

自动驾驶业务涉及大量汽车数据，并很可能涉及重要数据。考虑到自动驾驶业务可能包含不同类型、不同风险等级的数据，针对不同的数据可能有不同监管要求，如果对自动驾驶数据进行无差别管控，一方面可能难以达到合规要求，另一方面可能造成企业资源浪费，最终甚至影响自动驾驶业务的可持续性。因此，自动驾驶业务相关公司应当对数据实施分级分类管理，加强个人信息与重要数据保护。

由于自动驾驶涉及对车外道路、建筑、地形等数据进行收集，同时会获取汽车定位和途经路径并进行统一处理，因而可能因被认定为测绘行为而为自然资源部门所监管。2022 年 8 月 30 日，自然资源部发布《关于促进智能网联汽车发展维护测绘地理信息安全的通知》（以下简称《地理信息安全通知》），该规定标志着我国对自动驾驶的监管进一步加强。如企业开展自动驾驶业务，并收集处理空间坐标、影像、点云等数据，则可能构成测绘行为。考虑到我国对测绘活动实行测绘资质管理制度，我们建议相关企业依法取得测绘资质证书，并在测绘资质等级许可的专业类别和作业限制范围内从事测绘活动。

3. 人遗与医疗

医疗行业大数据的发展，天然地离不开大量敏感个人信息和重要数据的合法合规使用。2022 年，《医疗卫生机构网络安全管理办法》正式颁布，该办法主要明确和规定了我国医疗卫生机构在网络安全和患者数据安全方面的责任和义务。从内容上看，该办法将“网络安全”和“数据安全”作为两章专门规定内容进行独立设置，一方面在《网络安全法》《密码法》等法律的基础上，要求卫生医疗机构严密落实《关键信息基础设施安全保护条例》和网络安全等级保护制度要求；另一方面，明确要求各级卫生医疗机构加强数据全生命周期安全管理，并确立原则上应在境内开展全生命周期数据处理活动，进一步细化了《数据安全法》《个人信息保护法》在医疗卫生领域的各项实践规范。

而作为我国生物资源安全相关的重要领域，**人类遗传资源的保护和发展**向来受到我国相关主管部门的重视，随着近些年相关领域法规更新和执法举措要求，行业内的企业也普遍谨慎地对待我国人类遗传资源的安全管理，尤其是涉及境内人类遗传资源的国际合作和出境合规。此外，《人类遗传资源管理条例实施细则（征求意见稿）》于 2022 年初公开发布，该细则在沿用和细化我国《人类遗传资源管理条例》相关规则的基础上，最为突出的地方在于更加细化了“外方单位”的认定方法，特别是为企业对于判断何为境外组织、个人“实际控制”情形提供了判断依据，主要是持股比、表决权和通过协议或相关安排足以施加重大影响的多种客观类型。我们理解，待该细则正式文本发布，需要行业内相关企业及时对此做好数据合规调整，特别是在人遗资源合作方式和数据权属安排层面，做好境内外风险的事前隔离预案设计。

4. 金融、保险与征信

我国个人金融信息的保护呈强监管趋势，个人金融信息合法合规收集使用成为金融业机构不可触碰的红线，也是各监管部门关注的重点。多监管部门发文，全面梳理和排查行业内个人信息保护方面的问题和漏洞，深入整治侵犯个

人金融信息主体权益乱象，督促各行业机构建立个人金融信息主体保护机制。

具体而言，《金融科技发展规划（2022-2025 年）》《征信业务管理办法》《银行保险机构消费者权益保护管理办法（征求意见稿）》《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知（银保监办法〔2022〕80号）》等针对金融、征信与保险类行业个人金融信息保护的法律法规的相继出台。就从宏观政策层面而言，提出了建设具有中国特色与国际接轨的金融数字化之路，要助力经济社会全面奔向数字化、智能化发展时代；就行业层面而言，针对性地规定了信用信息的采集、整理、保存、加工、提供、使用和保障信息安全的基本办法；就具体业务开展而言，也有如要求银行保险机构针对个人信息处理问题进行整改等。

（二）数据要素市场发展与数据交易

数据要素、数据价值化与数据资产、数据交易，这些名词或概念成为 2022 年炙手可热的讨论话题。随着数据作为生产要素自上而下地在市场经济领域内被确立、突出和强调，对于数据如何促进生产力发展、提升数字经济效率的探讨也更为深入。2021 年底，国务院印发《要素市场化配置综合改革试点总体方案》，提出要“探索建立数据要素流通规则，完善公共数据开放共享机制，建立健全数据流通交易规则，拓展规范化数据开发利用场景，加强数据安全保护”；2022 年底，中共中央和国务院正式印发《关于构建数据基础制度更好发挥数据要素作用的意见》（俗称“数据二十条”），要求构建数据产权制度、数据要素流通和交易制度、数据要素收益和分配制度、数据要素治理制度。根据国家发改委相关负责同志说法，“数据二十条”以解决市场主体遇到的实际问题为导向，创新数据产权观念，淡化所有权、强调使用权，聚焦数据使用权流通，创造性提出建立数据资源持有权、数据加工使用权和数据产品经营权“三权分置”的数据产权制度框架，构建中国特色数据产权制度体系。[5]

除了中央政策对数据要素作用和数据基础制度作出全国一盘棋的统一部署之外，各地也纷纷通过颁布地方法规条例的方式，先行先试，创新数据流通和交易规则。据相关公开数据统计，截至 2022 年 8 月，全国已有 18 省市颁布“数据条例”[6]，进一步促进地方数据要素市场化改革和数字经济发展。值得关注的是，历经三个多月的社会公开征询意见，北京市于 2022 年 11 月 25 日正式发布了《北京市数字经济促进条例》。该条例中明确提出，支持在依法设立的数据交易机构开展数据交易活动。数据交易机构应当制定数据交易规则，对数据提供方的数据来源、交易双方的身份进行合规性审查，并留存审查和交易记录，建立交易异常行为风险预警机制，确保数据交易公平有序、安全可控、全程可追溯。由此可见，数据交易成为数据要素化和数据资产管理的未来发展方向。

与政策法规不断推进保持步调一致，**行业实践也在不断深化对数据要素权益配置的认知**。实现数据要素化和资产化，需要解决数据权益如何分配的前置性难题。对于该问题，在 2022 年 7 月第三届数据治理研讨会发布的《2022 年数据治理研究报告——数据要素权益配置路径》中尝试作出解答，尤其是对数据要素权益配置的基本内涵、关键症结、机制探索和路径实现等进行了研究和观察。[7]

对于数据交易而言，2022 无疑是承前启后的关键年份；**依托数据交易平台，数据要素流通市场和交易生态圈逐渐显现**。目前，多数数据交易所或者大数据交易平台以提供数据交易备案、撮合和数据资产登记为主要功能服务，为数据供需双方或多方提供了正规化和便利化的磋商途径。不过，随着数据交易平台逐渐参与或主导制定数据交易合规指引、数据交易服务指南，以及数据资产化登记、确认和备案要求等标准或规范，突出数据交易机构在数据交易市场生态圈的核心角色作用。随着数据交易入局者不断增多、交易规则更加明确，我们有理由期待一个更为丰富、成熟和体系化

[5] 人民日报海外版：《“数据二十条”对外发布，构建数据基础制度体系——做强做优做大数字经济》，载“中国政府网”，http://www.gov.cn/zhengce/2022-12/21/content_5732906.htm，最后访问日期：2023 年 1 月 2 日。
[6] 贵州省大数据发展管理局：《18 省市公布『数据条例』》，https://dsj.guizhou.gov.cn/xwzx/gnyw/202206/t20220602_74591935.html，最后访问日期：2023 年 1 月 2 日。
[7] 金杜作为参编单位之一，也在其中分享了观点，有兴趣的读者可以进一步点击链接详细了解，https://mp.weixin.qq.com/s/PoJKEu2Q0J9p7dvx6mw6wQ。

的数据交易市场，一个融合兼顾了数据安全合规和自由流通的市场化业态。

（三）合规防线：“数据合规不起诉”

常说“司法”是社会公平正义的最后一道防线，而 2022 年在数据合规司法领域有了新的举措。2022 年 5 月，上海市普陀区检察院通过官方微信号向社会公示了我国首起数据合规不起诉案件基本情况。对于全国首起“数据合规不起诉”案例的聚焦和讨论，为涉嫌数据违法违规企业提供了一套通过主动合规实现自我防御的“保护盔甲”。通过观察，我们认为“数据合规不起诉”的价值主要体现在两方面，一是能够在确保日常经营业务不受数据合规问题影响，帮助企业防范和化解潜在的违法经营风险；二是通过数据合规体系的搭建，培育数据安全和合规的市场竞争力，以合规创造品牌和竞争价值。但“数据合规不起诉”并非是零门槛或者说轻而易举的，在该案检察院制发的检察建议书中，围绕“管理、技术和制度”三个维度，对数据合规不起诉的条件提出了对应的标准要求。而对于数据合规体系的搭建，需要利用系统性思维和全局观理念，在企业数据处理风险识别和整改的基础上，需强化制度规范建设与顶层方案设计，并且实现企业数据合规体系的日常维护和有效执行、监督。[8]

三、演化：智能社会法律的视野前瞻

（一）算法合规

1. 推荐算法合规

2022 年 3 月 1 日，国家网信办、工信部等联合发布的《互联网信息服务算法推荐管理规定》（以下简称《算法管理规定》）正式施行，由此开启中国算法治理的元年。《算法管理规定》首次明确了算法分级分类安全管理制度，建立健全企业主体算法安全责任制度，推动算法公开透明，并要求具有舆论属性或者社会动员能力的算法推荐服务提供者进行算法备案。算法备案是推荐算法合规治理的第一步，是对国家网信办联合其他部委联合发布的《关于加强互联网信息服务算法综合治理的指导意见》中有序推进算法备案相关工作要求的有效延续。为了顺利开展算法备案工作，国家网信办还开发了互联网信息服务算法备案系统，企业可通过该备案系统申报算法主体信息、算法信息、产品及功能信息从而完成备案。

就备案主体而言，并非所有算法推荐服务提供者均需履行备案义务，具有舆论属性或者社会动员能力的算法推荐服务者才是适格义务主体；就备案内容而言，需要提交服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示的内容等；就备案时间而言，备案主体需要在提供服务之日起十个工作日内完成备案；就备案注销而言，算法推荐服务提供者终止服务的，应当在终止服务之日起二十个工作日内办理注销备案手续，并作出妥善安排。

国家网信办在其官网持续更新算法备案清单。目前，国家网信办于 2022 年 8 月、2022 年 10 月分别发布的《境内互联网信息服务算法备案清单》显示，已备案的算法分别有 30 个和 70 个，涉及的算法类别具体包括个性化推送类、排序精选类、检索过滤类、生成合成类、调度决策类。其中，同一推荐算法服务提供者可能分别就数个算法进行备案。例如，北京网易传媒有限公司分别就其网易传媒信息推送算法、网易传媒信息搜索算法以及网易传媒信息流推荐算法进行备案。

[8] 我们在《苟日新，日日新，又日新——首例数据合规不起诉案例评述》一文中详细分享了金杜在“数据合规不起诉”制度运行的观察和看法，有兴趣的读者可以点击链接阅读全文，https://mp.weixin.qq.com/s/xYuMQB3VunmTyaw6y1hr1w。

2. 算法审查机制

2022 年 12 月 19 日，中共中央、国务院对外公布《关于构建数据基础制度更好发挥数据要素作用的意见》，其要求建立数据要素生产流通使用全过程的合规公证、安全审查、**算法审查**等制度。算法审查机制在《算法管理规定》中初具雏形，有待进一步明确和完善。目前，《算法管理规定》初步规定了**安全评估、算法检查**两种算法审查机制。

- **安全评估**：《算法管理规定》第 8 条和第 27 条均提到了算法服务提供者对算法审核评估、安全评估的义务，即应当完善算法推荐服务管理机制，对算法推荐服务日志等信息进行留存，留存期限不少于六个月，并在相关执法部门依法查询时予以提供。若相关算法推荐服务提供者未按上述要求完成安全评估或日志留存等义务，则按照有关法律、行政法规和部门规章的规定予以处理。**但安全评估的问题在于，规定里没有明确评估是自评估还是第三方评估，也没有明确的评估要求，还需要进一步明确和落实**。

- **算法检查**：《算法管理规定》第 28 条第 2 款规定了算法检查，即算法推荐服务提供者应当配合有关主管部门依法实施的安全评估和监督检查工作，并提供必要的技术、数据等支持和协助。对于违反者按照有关法律、行政法规和部门规章的规定予以处理。这意味着主管机构在进行安全评估和检查工作时，**算法推荐服务提供者可能需要向其提供数据、算法模型等，以供其查验**。

（二）算力规划

2022 年，**云计算的规划与发展持续走向主流视野，占据数字经济发展的重要地位**。国务院发布的《“十四五”数字经济发展规划》强调，云计算是重点产业之一。具体而言，规划要求优化升级数字基础设施，推进云网协同和算网融合发展，加快构建算力、算法、数据、应用资源协同的全国一体化大数据中心体系。中国人民银行于 2022 年 1 月印发的《金融科技发展规划（2022-2025）》说明，五年发展目标之一即金融业数字化转型深化，其阐述道，金融业数字化从多点突破迈入深化发展新阶段，全局性、系统性数字思维深入人心，数字化转型的理论、方法、评价体系基本形成，上云用数赋智水平稳步提高，金融机构数字化经营能力大幅跃升。

为了支持算力发展，国家采取了一系列举措。2022 年 2 月，“东数西算”工程全面启动，国家在京津冀、长三角、粤港澳、成渝、宁夏等地建设算力枢纽节点，规划了张家口等 10 个数据中心集群，完成全国一体化大数据中心体系总体布局设计。2022 年 6 月，中国算力网正式上线，未来全国各地的人工智能计算中心、超算中心、“东数西算”枢纽节点均可接入，由此开启全国算力资源的协同调度与共享。此外，国务院于 2022 年 10 月 28 日第十三届全国人民代表大会常委会第三十七次会议发布的《关于数字经济发展情况的报告》显示，我国算力基础设施已达到世界领先水平，截止 2022 年 6 月，我国数据中心机架总规模已超过 590 万标准机架，建成 153 家国家绿色数据中心。与此同时，我国建成一批国家新一代人工智能公共算力开放创新平台，以低成本算力服务支撑中小企业发展需求。

（三）科技与人工智能伦理发展

1. 深度合成、深度伪造技术合规

在我国，“辨伪求真”是十九大报告提出的“营造清朗的网络空间”总任务的一部分。为了规制深度伪造技术，国家网信办于 2022 年 1 月 28 日发布了《互联网信息服务深度合成管理规定（征求意见稿）》，并于同年 12 月 11 日

发布《**互联网信息服务深度合成管理规定**》，从**信息内容治理、数据安全保障以及算法技术合规**等多方面进行规制。该规定于 2023 年 1 月 10 日起施行。

- **明确各方责任主体法律定义与义务**：规定限缩“深度合成服务提供者”的内涵至在中国境内提供深度合成服务的组织、个人，以风险为导向细化其主要合规义务；明确了“深度合成服务技术支持者”的外延，缩减其信息内容治理义务，仅施加了履行数据安全保障义务、算法技术合规义务，以及协助发展有关深度合成技术的行业自治规范的义务；强化了应用程序分发平台等其他责任主体的信息安全义务，例如要求深度合成服务使用者仅能以单独同意作为合法性基础从而使用人脸等生物识别信息编辑功能。

- **完善“事前预防”与“事后应对”相结合的全流程治理模式**：就事前预防而言，新规要求深度合成服务提供者设立信息发布审核管理制度，细化了审核合成服务的算法备案要求，明确算法备案和变更、注销备案的要求仅适用于具有舆论属性或者社会动员能力的深度合成服务。就事后应对而言，规定要求深度合成服务提供者与应用程序分发平台设置应急处理管理制度，作为信息安全事件的关键救济机制。此外，深度合成服务提供者必须记录并保存相关网络日志，这一举措有助于监管部门及时对深度合成服务中的违法违规现象采取执法措施。

- **打造多元化监管格局**：深度合成服务的治理未来将由网信部门、电信主管部门以及公安部门协同进行；如果深度合成服务提供者和技术支持者是为从事网络出版服务、网络文化活动等，还应当同时符合新闻出版、文化和旅游、广播电视主管部门的规定。

2. 人工智能与科技伦理审查

2022 年 3 月，中办、国办印发《**关于加强科技伦理治理的意见**》（《意见》），这是我国首个国家层面的科技伦理治理指导性文件，着力解决我国科技伦理治理体制不健全、制度不完善、发展不平衡等突出问题，对科技伦理治理作出顶层设计和系统部署。《意见》中提出了包括“**伦理先行**”“**依法依规**”“**敏捷治理**”等五项人工智能与科技伦理审查治理要求。其中提到：

- **合理控制风险**：科技活动应客观评估和审慎对待不确定性和技术应用的风险，力求规避、防范可能引发的风险，防止科技成果误用、滥用，避免危及社会安全、公共安全、生物安全和生态安全。

- **压实创新主体科技伦理管理主体责任**：根据实际情况设立本单位的科技伦理（审查）委员会，并为其独立开展工作提供必要条件。**从事生命科学、医学、人工智能等科技活动的单位，研究内容涉及科技伦理敏感领域的，应当设立科技伦理（审查）委员会**。

- **建立科技伦理审查和监管制度**：明确科技伦理审查和监管职责，完善科技伦理审查、风险处置、违规处理等规则流程。建立健全科技伦理（审查）委员会的设立标准、运行机制、登记制度、监管制度等。

目前，法律法规层面，《算法管理规定》已经对科技伦理审查的具体内容进行了规定，其要求科技伦理审查制度至少包含以下两方面的内容：（1）定期审核、评估、验证算法机制机理、模型、数据和应用结果等；（2）不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。

3. 企业应着手准备的事项

首先，涉及科技与人工智能技术的企业需要**初步建设和完善人工智能伦理体系，根据技术风险清单内部梳理公司现有的可能涉及高风险 AI 技术应用场景和业务条线，同时厘清相关 AI 技术公司所承担的主体角色**。根据目前的规定，我们建议将涉及推荐算法技术（生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类），尤其在自动驾驶、智慧交通、生物识别、深度伪造或者深度学习等自动化决策领域内涉及的算法模型和人工智能系统进行梳理。梳理的过程中需注意厘清在相关高风险人工智能技术应用中企业所承担的“研究开发、设计制造、部署应用和使用”四个维度下的具体角色和职责。

其次，**优先落实对现有业务算法推荐技术备案、深度合成类算法使用的风险评估和风险提示等硬性合规义务**。具有舆论属性或者社会动员能力的算法推荐服务提供者应当将服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息履行备案手续。基于此，企业需在识别相关高风险人工智能技术应用场景的基础上，进一步深入开展自评估和备案工作。此外，企业还需跟踪深度机器学习、深度伪造和虚拟现实等人工智能管理规范的最新动态，在涉及提供相关服务时，通过更新用户协议文本、隐私政策或者产品内公告等合适方式，为用户增强风险提示。

最后，**筹划组建科技伦理委员会或者人工智能伦理治理委员会，建立问责机制、落实主体责任**。参考现有的行业实践，企业可以考虑由内部多部门（技术研发、信息安全、法律合规）以及外部专家或者第三方专业机构共同组建成立的科技伦理委员会（或者人工智能伦理治理小组），作为第一责任机构，对外负责对接相关主管部门对人工智能技术的监管指导和官方出口，对内负责人工智能治理原则规则制定、具体决策事项、理念宣传以及推动人工智能伦理具体举措落实等。而就人工智能的内部责任主体而言，保证算法与人工智能系统正常运作相关责任应当落实到具体的组织 / 部门与具体的岗位个人。

结语

过去的一年，网络安全和数据合规法律服务的各个细分领域，都朝着精细化治理的方向不断延展和深入。在立法者已经搭建起的网络空间治理法律框架的基础上，执法者和司法者逐渐地丰富和熟练地掌握使用了治理工具，从而维系了整个行业的健康运转；与此同时，决策者在这个年度将关于数据注意力和想象力的眼界放得更为长远，在把握安全和发展的辩证关系上，逐步勾勒出对于数据作为生产要素和价值资产的设计蓝图；而面对智能化社会的一步步靠近和所带来的挑战，我们不再是未雨绸缪而是已经开始着手应对。

2022 年，告别野蛮生长、承受来自内外部的压力，我们看到了中国互联网与数字经济发展中的韧劲和适应转变的速度，我们乐见于秩序更为稳健、规则更为明确的网络空间治理体系，为在虚拟世界构建人类命运共同体、贡献我们的智慧方案而拍手叫好。自由、平等、开放和共享，我们曾拥护和奔走呼号这样的互联网精神，如今迈入 2023，我们仍抱以“合规创造价值”的信仰，诚挚地期盼一份笃定和踏实。

感谢实习生刘畅、陈琳珺和董方倩对本文所作的贡献。

数据合规

苟日新，日日新，又日新——首例数据合规不起诉案例评述

宁宣凤　吴巍　吴涵　刘艳洁　赵妍　姚敏侣

2022 年 5 月，上海市普陀区检察院公开了全国首例数据领域刑事合规不起诉案件情况[1]。该案件涉及日前企业普遍关心的数据安全和刑事合规问题，同时案件背后所折射出的数据安全和刑事合规不起诉制度的有效运作和配合，值得我们从事企业法律合规相关人士思考和寻味，我们期待数据合规不起诉制度成为数字经济健康高度发展和网络空间治理的平衡器及指南针。

一、Z 网络科技公司通过数据领域专项整改，获得不起诉决定

Z 公司是一家网络科技公司。因运营需要，2019 至 2020 年间，该公司首席技术官陈某某在明知 Z 公司未获授权许可的情况下，指使多名技术人员通过数据爬虫技术，非法获取某外卖平台数据，给外卖平台造成 4 万余元的直接经济损失。

4 万元的金额看似不高，但却足以引发严重后果。根据《刑法》第 285 条及相关司法解释，违法国家规定，采用技术手段，获取计算机信息系统中存储、处理或者传输的数据，造成经济损失一万元以上便属“情节严重”，涉嫌非法获取计算机信息系统数据罪。如违法行为查证属实，陈某某及 Z 公司不仅会面临三年以下有期徒刑、罚金等严厉的刑事处罚，陈某某个人及 Z 公司后续发展也必将受到重挫。

在此情况下，Z 公司了解到最高检正在推行涉案企业合规改革，符合条件的企业可以通过合规整改免除刑事责任。为此，Z 公司积极赔偿损失，取得外卖平台谅解，并主动向普陀区检申请适用合规监督考察程序。

获准适用后，Z 公司结合普陀区检提出的检察建议，围绕管理、技术、制度进行自查整改，并聘请专业律师制定数据合规整改计划，扎实推进。经过数月努力，顺利通过合规考察验收，以及听证员、侦查人员、合规考察第三方组织、被害单位和 4 名全国人大代表等出席的“云听证”。通过合规整改，Z 公司不仅获得不起诉决定，使公司重新回到正轨，还提高了公司合规管理水平，增强了竞争软实力。

[1] 详情请见 https://mp.weixin.qq.com/s/WG-u1ZaHiOn9yX00irS35w。

二、数据经济发展与合规的矛盾

数据合规是新的合规领域，同时也是国家网络空间治理的重点领域。数字经济的发展使得作为生产要素之一的数据成为争先利用的对象，而由于数据本身可复制、易传播的特点，使得数据泄露、滥用等社会现象层出不穷，其引发的刑事犯罪也屡见不鲜。**数据有序利用发展是全球社会亟需解决的问题，而重点在于如何平衡数据领域立法滞后和数据使用方式日新月异的矛盾。**

（一）数据合规的法律法规基本框架成行，但仍待完善

近年来，我国高度重视数据合规在立法中的顶层设计，并且通过加强有关方面的监管，不断强化和落实责任主体的义务。尤其是随着 2021 年《数据安全法》《个人信息保护法》等相关上位法的出台和实施，加之此前《网络安全法》，我国在网络安全与数据合规领域，形成三股有效合力。但不得不承认，尽管网络安全与数据合规的立法框架已经初步成型，但相关的配套措施以及指南性文件仍然有待补充，比如“重要数据”“关键信息基础设施”等重要概念的范围和评价标准等还未正式公布。

（二）数据合规领域需要动态管理和敏捷治理

数据合规领域的监管趋势主要呈现出以下两个基本特征：

一方面，**规范动态制定与实时合规工作相伴而行**：由于需要对三大立法各大制度加以具体细化，各种立法、标准制定工作正在紧锣密鼓地进行中，因而陆续出现大量的尚未生效的征求意见稿，典型的如统合三大法律数据保护制度的《网络数据安全管理条例（征求意见稿）》，抑或是专门规制 App 领域个人信息的《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》等。这些征求意见稿确定了数据出境等相关制度的具体规制措施和方向，同时对于责任主体来说，这些合规工作的开展也在持续动态变化中。

另一方面，**垂直行业专门化与精细化监管同步深入**：出现了针对特定领域、特定场景的专门规范，立法立规工作逐渐向精细化监管趋势发展。三大立法奠定了数据合规的基本框架，但是鉴于数据合规的工作因不同领域和场景从而具有不同的特殊性，因此需要针对这些不同点进行有针对性的规制。从领域上看，立法已经延伸至金融、汽车、互联网、生物医药等领域。从场景上看，国家有关监管部门还对以 App 为主的互联网移动应用产业链或生态圈进行了大量的执法活动。

尽管数据合规领域的监管在不断加快速度并且日益深化，数据领域的技术和经济发展速度仍在拉开距离。企业作为数字经济的主体之一，**如何在创新的刚需中把握“合法合规”的底线，是企业亟需监管部门予以动态及敏捷指导的痛点。**

（三）数据不合规利用方式引发的多样化刑事责任

数据合规涉及到数据全生命周期的处理，在任意阶段的不正当行为都有可能引发多类刑事责任。比如，尽管爬虫是一项中立的技术工具，但非法爬虫可以作为一种犯罪手段来非法获取数据。以“爬虫”和“数据”作为全文关键词，北大法宝数据库进行检索，共检索出 78 份刑事案件。在分布上，罪名集中在侵犯公民个人信息罪（20）、非法获取计算机信息系统数据、非法控制计算机信息系统罪（14）、侵犯著作权罪（9）以及诈骗罪（8）。

与爬虫技术的利用相关案件只是个例子，具体而言，数据领域典型的刑事犯罪还有可能包括：

罪名	案件数	统计年限
侵犯公民个人信息罪	12547	2015-2022
非法获取计算机信息系统数据、非法控制计算机信息系统罪	2057	2013-2022
破坏计算机信息系统罪	1663	2013-2022
拒不履行信息网络安全管理义务罪	6	2018-2022
帮助信息网络犯罪活动罪	24138	2015-2022

表 3：近几年涉及相关罪名案件的绝对数量统计 [2]

从案件统计来看，相较于其他各类型案件，帮助信息网络犯罪活动罪被认定的数量更大。在积极犯罪中，侵犯公民个人信息罪是最常被认定成立的罪名。拒不履行信息网络安全管理义务罪作为一种消极犯罪，其被认定的情形不多。这可以从该罪的构成要件来进行解释，不履行信息网络安全管理义务通常表现为由不担当行政责任而导致的刑事责任，成立该罪名通常以拒不改正的行为并且导致所规定的危害结果作为犯罪构成要件。

除了以上常见的数据合规领域常见罪名以外，根据实际具体的犯罪构成要件的论证，数据有关的违法犯罪行为也有可能构成上述典型犯罪以外的其他罪名。譬如，上海某信息科技公司因受到巨大利益诱惑，为境外组织采集和提供采集中国铁路信号数据，包括物联网、蜂窝和 GSM-R，也就是轨道使用的频谱等数据。由于该等数据涉及国家基础信息、国家核心数据，因此该公司的王某、迟某等涉嫌为境外刺探、非法提供情报罪被执行逮捕。[3]

三、合规监督考察，救济数据违法行为的新路径

2022 全国两会后，最高检会同全国工商联等部门召开专题会议，宣布涉案企业合规改革在全国范围内推开。国有企业、民营企业、外资企业在生产经营活动中涉及的经济犯罪、职务犯罪等案件均在改革范围之内。数据合规领域常见的非法获取计算机信息系统数据罪、侵犯公民个人信息罪等罪名均可适用。而且，无论是单位犯罪案件，还是企业实际控制人、经营管理人员、关键技术人员等实施的与生产经营活动密切相关的犯罪案件，均可适用该项改革。由此可见，适用合规监督考察程序，通过合规整改免除刑事责任，将成为为涉嫌数据违法行为的企业的新的救济路径。

根据现行规定，获准适用合规监督考察程序的企业，需要开展内部自查，深入分析案发原因，识别违法行为背后的管控漏洞，并在此基础上明确合规整改措施，制定《合规计划》。《合规计划》经第三方组织及检察院确认后，涉案企业需严格执行，按照计划，积极开展、落实各项整改工作，并定期向第三方组织及检察院汇报，接受阶段性现场检查。最终，顺利通过第三方组织的验收及检察院组织的听证后，涉案企业才能获得不起诉决定。

[2] 数据来源：北大法宝。
[3] https://tv.cctv.com/2022/04/13/VIDE0FR1IT8DudSltL6poIRg220413.shtml

由此可知，涉案企业合规监督考察程序关注的重点，是涉案企业的合规整改与合规建设。在 Z 公司非法获取计算机信息系统数据案中，普陀区检也对 Z 公司提出了明确的合规建设要求。

第一，构建数据合规管理体系。设置专门的数据合规管理部门，特别针对数据来源合法性，制定并不断完善数据合规计划，消除内部管理盲区。

第二，提高数据合规风险识别、应对能力。规范技术汇报审批流程，建立技术应用合规评估制度，避免技术滥用。

第三，稳健数据合规运行。建立数据合规咨询机制与数据不合规发现机制，建立数据分级分类管理制度及员工数据安全管理制度，填补制度空白。

Z 公司也是通过合规整改，符合了上述合规建设要求，才能够顺利通过验收及听证，获得不起诉决定。

四、企业数据合规体系的搭建及其注意事项

结合普陀区检的检察建议，我们理解涉案企业在搭建数据合规体系时应关注以下核心要点。这些要点与企业搭建日常数据合规体系时所需关注的要点，有一定共通之处。

首先是数据合规问题的发现、风险识别与整改。目前，《网络安全法》《数据安全法》和《个人信息保护法》的数据合规领域上位法框架规则基本成型，对于企业现行数据处理方案中的合规问题，需要进行一次全面和彻底的盘点、梳理和识别。根据检察建议书，**“规范技术汇报审批流程，建立技术应用合规评估制度，避免技术滥用”**成为相应的客观要求，而配合此要求，**《数据安全法》规定的数据处理风险监测、重要数据处理定期风险评估，**以及**《个人信息保护法》要求在特定情形时开展的个人信息保护影响评估，**企业均需要形成行之有效的内部运行机制，并与自身业务规则相适应，将法律合规义务嵌入审批和管理流程，从而帮助企业完成风险识别以及后续的整改落地。

其次是数据合规制度规范建设与顶层设计。不难发现，构建成熟有效的数据合规管理体系，是本次涉案企业在合规不起诉案件中得以成功申请并通过听证的关键原因。从一般的企业数据合规体系构建实践视角来说，一个达到法律要求和预期目标的数据合规制度规范体系，至少要在顶层制度、配套规范和执行工具三个层面进行构建、完善与维护。

第一，在顶层制度上，企业需要以**统一的纲领性制度文件，**并且至少从管理或责任部门、组织架构、数据安全与个人信息保护原则，以及基本技术和操作要求等维度展开对该内部纲领性制度文件的搭建。该文件应当通过公司内部的员工大会或者其他依法形式公开发布，并且成为员工应当严格遵守的内部纪律制度。

第二，在配套规范上，企业需要根据相关法律分别对“网络运营者”“数据处理者”和“个人信息处理者”，乃至“关键信息基础设施运营者”等不同主体施加的不同网络安全和数据保护义务，**建立起可供业务和管理职能参照日常执行和监督的指引性规范和规定。**例如，企业数据分类分级管理规定、企业数据来源合法合规性审查规范、员工数据安全与权限管理规范、个人信息加密和去标识化指引、数据出境安全管理要求、网络数据安全应急响应预案及流程规定等等。其中，本次涉案企业所接受的检察建议中，对于数据来源合法性确认程序和员工信息安全意识管理提出了专门要求。

第三，在执行工具上，由于数据合规的涵盖面和工作事项较为广泛且多样，因此**一套配合有效的数据合规表单记**

录类工具或模板成为能够节省合规成本、提高合规效率的重要帮手。在这方面，例如个人信息处理记录义务、个人信息保护评估义务以及数据出境安全评估义务等均可以通过设计相对通用的合规工具，以在确保完成度的基础上尽可能提高合规工作的效率。

最后是数据合规体系的日常维护和执行监督。本次涉案企业经办案检察机关要求，设置了专门的数据合规管理部门，同时建立了数据合规咨询机制。在作出合规不起诉决定前，由监管部门、安全企业和社会组织等多方组成的相关第三方组织成员，进行了三方监督评估和整改情况调研工作。由此可见，对于企业拟搭建的数据合规体系而言，还需要分别在“内部体系维护”和“外部独立监督”两个方面下功夫。

其一，对于内部体系维护而言，如果符合相关法律规定的应当设立网络安全、数据安全和个人信息保护专门部门和负责人的情况或条件，则企业应当履行法定义务，**确认相关主管负责部门及同事**，切实担当起企业整体的数据合规责任。此外，根据现行法律要求，内部主管部门应当还需要定期对数据安全和个人信息保护情况进行“合规审计”。可以预见，**以自行或者委托第三方专业机构为主、相关主管部门强制审计为辅的数据领域合规审计工作**，将成为日后维系企业数据合规体系日常有效运转的重要内容。

其二，对于外部执行监督而言，**建议企业建立起稳定和畅通的数据合规咨询渠道**，包括与相关主管部门、专业第三方组织（如数据合规律师或律所团队）定期沟通与咨询合作机制，尽可能在风险还未生成或对企业经营产生重大影响前及时规避或化解；此外，根据《个人信息保护法》及相关规定，对于符合“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”，应当按照国家规定成立**主要由外部成员组成的独立机构**对个人信息保护情况进行监督，同时定期发布个人信息保护社会责任报告，接受社会监督。

企业数据合规体系的构建显然是一项系统性工程，企业需要从现有或计划开展的经营业务现实出发，借助专业第三方组织的力量并结合专业人士的意见，制定可行有效的数据合规体系搭建方案，并有计划、分步骤地展开落地和执行工作。从我国首例数据合规不起诉案件中，我们有理由认为，我们所探讨的合规体系构建工作的现实意义将日趋强化，高质量、精细化的数据合规工作也将进一步为现代企业的数字化开拓发展创造全新的价值。

感谢实习生吴仁浩对本文作出的贡献。

以安全促发展——《数据出境安全评估办法》解读

宁宣凤 吴涵 姚敏侣

各国关于数据出境的监管要求一直是各国数据监管的风向标，不仅体现国家对于数据安全的重视程度，也能意会出国家对于数据竞争的态度以及数字经济发展的思路。例如欧盟《通用数据保护条例》（GDPR）设定的个人数据出境的限制，规定在第三国具备充分保护水平的前提下可将个人数据向第三国传输，而如第三国不具备充分保护水平的，控制者或处理者只有在提供了适当的保障措施，并为数据主体提供了可执行的权利和有效的法律救济措施的条件下，才可将个人数据传输至第三国。上述内容是对于个人数据出境的特殊监管要求，也是解决欧盟单一数字经济发展面临制度障碍的尝试。

数据出境的监管对于数字经济蓬勃发展的中国也尤为重要。一方面需要树立数据监管的价值观，另一方面数据出境监管的制度设计将直接影响跨国企业以及出海企业的日常运营，更深刻的影响数字经济的发展进程。随着《网络安全法》、《数据安全法》以及《个人信息保护法》三大法律的确立，以及相关法律法规征求意见稿的出台，我国数据跨境制度法律框架已经完成了基础性搭建。其中，数据出境安全评估制度在我国的数据跨境制度中占据相当重要的地位。2022 年 7 月 7 日，《数据出境安全评估办法》正式颁布，这意味着，我国数据出境安全评估制度在效力上，从概念的制度向实践的制度迈出了重要的一步。本文在回顾我国数据跨境制度的历史沿革基础上，对《数据出境安全评估办法》的自评估方法进行操作化的解读，为企业等各数据处理者提供自评估合规指引。

一、数据跨境制度的规则导向

而就国内而言，《网络安全法》的生效，初步确立了以安全评估制度为核心的数据跨境的基本规则；随着《数据安全法》《个人信息保护法》等法律法规的出台，数据跨境制度的法律框架逐渐完善，安全评估制度在数据跨境制度中的定位也逐渐清晰。在此期间，为有效落地法律层面的制度规范，国家网信办等有关部门、标准制定单位等陆续发布了不同层级的数据跨境细则、标准指南等草案文件，明晰了数据跨境合规的监管和实践方向。

效力层级	法规名称	时效性	生效时间 / 颁布时间
法律	网络安全法	现行有效	2017.06.01
	数据安全法	现行有效	2021.09.01
	个人信息保护法	现行有效	2021.11.01

效力层级	法规名称	时效性	生效时间 / 颁布时间
行政法规	关键信息基础设施保护条例	现行有效	2021.09.01
	网络数据安全管理条例	征求意见	2021.11.14
部门规章 / 部门规范文件（包括历史文件）	数据安全管理办法	征求意见	2019.05.28
	个人信息和重要数据出境安全评估办法	征求意见	2017.07.14
	个人信息出境安全评估办法	征求意见	2019.06.13
	个人信息出境标准合同规定	征求意见	2022.06.30
	数据出境安全评估办法	现行有效	2022.07.07
标准 / 行业指南	信息安全技术 数据出境安全评估指南	征求意见	2017.08.30
	网络安全标准 个人信息跨境处理活动认证技术规范	征求意见	2022.04.29

二、我国数据跨境安全评估制度的历史沿革

在国内数据跨境制度的发展过程中，数据出境安全评估作为数据跨境的合规途径贯穿始终，并随着规则草案的颁布而逐渐细化。以下我们就数据跨境安全评估制度的历史沿革总结如下：

（一）数据跨境安全评估制度的开端——以《网络安全法》作为标志

1.《网络安全法》奠定数据跨境安全评估制度基础

从时间上看，最开始对数据跨境提出安全评估要求的是 2017 年的《网络安全法》（《网安法》）。《网安法》第 37 条对关键信息基础设施运营者（CIIO）提出了在境内收集和产生的个人信息和重要数据的本地化要求，确需出境的应当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。不过，对于上述条文中对“关键信息基础设施运营者”“重要数据”“个人信息”三个核心概念均未进行界定，同时并没有相应的国家层面的安全评估规定，这使得《网安法》的规定与数据跨境安全评估制度实际落地仍有较大距离。因此于同年，国家网信办就《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见，国家标准委随后也就《信息安全技术 数据出境安全评估指南（征求意见稿）》（《数据出境安全评估指南（征求意见稿）》）公开征求意见。两文件均不同程度地对《网安法》所奠定的数据跨境安全评估框架进行了进一步的深入和细化。

2. 阶段性征求意见稿明确方向

《个人信息和重要数据出境安全评估办法（征求意见稿）》的贡献在于确立了数据跨境制度之下的安全评估程序的基本流程。该《办法》对需要进行安全评估的情形、安全评估需要重点评估的内容、负责安全评估的主管部门等方面进行了具体的规定，并确立了以自评估为前置流程，申请评估为正式环节，重新评估为可持续性支持的安全评估流程。其中，还值得注意的是安全评估适用范围的拓展。它将适用主体拓展适用于任何符合第 9 条条件的网络运营者，同时将数据类型拓展至具有一定体量的数据。而《数据出境安全评估指南（征求意见稿）》则是对数据跨境、重要数据、核心数据等基本概念进行了界定和列举，同时提供了极具可操作性的，以影响程度等级和安全事件可能性等级为判断维度的安全评估落实方案。

随后经过大约两年时间，《数据安全管理办法（征求意见稿）》以及《个人信息出境安全评估办法（征求意见稿）》相继公开征求意见。《数据安全管理办法（征求意见稿）》纳入个人信息的有关内容，将包括个人信息在内的数据的收集、处理使用、安全监督管理进行了规定。《数据安全管理办法（征求意见稿）》区分重要数据和个人信息，涉及重要数据跨境的，网络运营者应进行评估，并报经同意或批准；个人信息则按照其他规定执行。

随之而来的《个人信息出境安全评估办法（征求意见稿）》中，个人信息的出境限制比数据出境更为严格，根据第 3 条的规定，凡涉及个人信息跨境，均需要进行个人信息出境安全评估申报。《个人信息出境安全评估办法（征求意见稿）》可以视为先前《个人信息和重要数据出境安全评估办法（征求意见稿）》的细化版本，其对申报材料、安全评估期限、救济渠道等内容进行细化规定，并强调网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件（统称合同）中所应规定的，保障个人信息权利以及网络运营者、个人信息接收者责任义务的要求。在该文件中，合同审核成为了安全评估的重点内容。

这一阶段，数据跨境安全评估制度得到了较高程度的讨论与细化，奠定了该制度在数据跨境制度中的重要地位。

（二）数据跨境安全评估制度的重要更新——以《数据安全法》《个人信息保护法》为标志

1. 数据跨境安全评估制度的适用日益多元化和具体化

随着《数据安全法》（《数安法》）以及《个人信息保护法》（《个信法》）相继出台并生效，我国的数据跨境制度的基本法律框架得以进一步厘清。《数安法》第 31 条在 CIIO 向境外提供重要数据时延续了《网安法》的规定，还为非 CIIO 的数据处理者在向境外提供重要数据提供了制度留白。《个信法》则是在数据处理者的基础上，进一步界定了个人信息处理者，并规定了“个人信息跨境提供的规则”专章来专门针对个人信息跨境构建规则框架。在《个信法》下，个人信息跨境场景下的安全评估制度有了更多的细化规定。

适用主体上，《个信法》继承了《网安法》和《数安法》的规定，将属于 CIIO 的个人信息处理者纳入需要安全评估的责任主体范围。在此基础上，《个信法》第 36 条和第 40 条还加入两个需要进行安全评估的责任主体，分别是国家机关和处理个人信息达到国家网信部门规定人数的个人信息处理者（下称“大型个人信息处理者”）。《个信法》对上述三者提出了个人信息本地化要求，因需要确需出境的，则需要进行安全评估。其中，CIIO 作为长期存在的概念，其概念界定、认定标准以及认定程序在《关键信息基础设施保护条例》中有了相对明确的规定。各主体

可以根据该条例的要求，对自身是否可能会被认定为 CIIO 进行自评估，可能会被认定为 CIIO 的，宜以 CIIO 的标准开展数据跨境合规工作。可以看出，在整个数据出境制度体系中，数据出境安全评估占据十分重要的位置。因为对于特定主体而言，安全评估并不是《个信法》第 38 条第 1 款所规定的“选择性义务”，而是第 36 条、第 40 条所规定的“强制性义务”；不是《网络数据安全管理条例（征求意见稿）》第 35 条中数据出境的“选择性义务”；而是第 37 条所规定的“强制性义务”。而同时，“处理个人信息达到国家网信部门规定数量的个人信息处理者”尚需进一步界定。

2. 后续规则草案尝试制度落地

《网安法》《数安法》以及《个信法》三驾马车的形成，为后来的《网络数据安全管理条例（征求意见稿）》的制定提供了上位法基础。《网络数据安全管理条例（征求意见稿）》将数据跨境统一处理，将个人信息跨境制度框架扩展成为数据跨境制度的一般框架，其基本上遵循了《个信法》的制度架构，但同时对三大法律的规定进行了细化，形成制度补充。在延续性地将数据出境安全评估作为数据出境的一种条件的基础上，《网络数据安全管理条例（征求意见稿）》尝试就数据出境安全评估的触发条件做进一步明确，除 CIIO 情形外，还包括了出境数据中包含重要数据、处理一百万人以上个人信息的数据处理者向境外提供个人信息。

现今生效的办法在统一处理数据出境的基础上，对统一的安全评估制度做了进一步更新。其第 4 条对《个信法》“处理个人信息达到国家网信部门规定数量的个人信息处理者”进行了补充界定，在“处理个人信息达到一百万人的个人信息处理者向境外提供个人信息”的基础上，补充了“自上年 1 月 1 日起累计向境外提供超过十万人个人信息或者一万人敏感个人信息”的数据处理者的情形，较为显著地扩大了数据出境安全评估制度的适用范围。

在具体的评估流程上，《数据出境安全评估办法》明确了**自评估——申请评估——重新申报评估**的评估流程框架，并对部分细节进行了更新。例如，在有效期上，《数据出境安全评估办法》规定了 2 年的固定有效期，2 年有效期届满均需要进行安全评估，并且规定有效期内需要重新评估的情形。在评估时限上，《数据出境安全评估办法》充分考虑到了安全评估工作的复杂性，例如根据第 10 条的要求，国家网信部门受理申报后，需要根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估，因而整个过程需要多部门协同以及具有较高的专业性。

在该办法中，数据跨境合同等法律文件仍然是重要的评估内容，与《个人信息出境安全评估办法》相比，《数据出境安全评估办法》综合了的个人信息处理情况、个人信息权利保障以及网络运营者和接收者的责任义务于一体，并补充再跨境条款和争议解决条款的要求，因而更为简洁，同时也更强调标准合同的可行性、周全性以及可执行性。

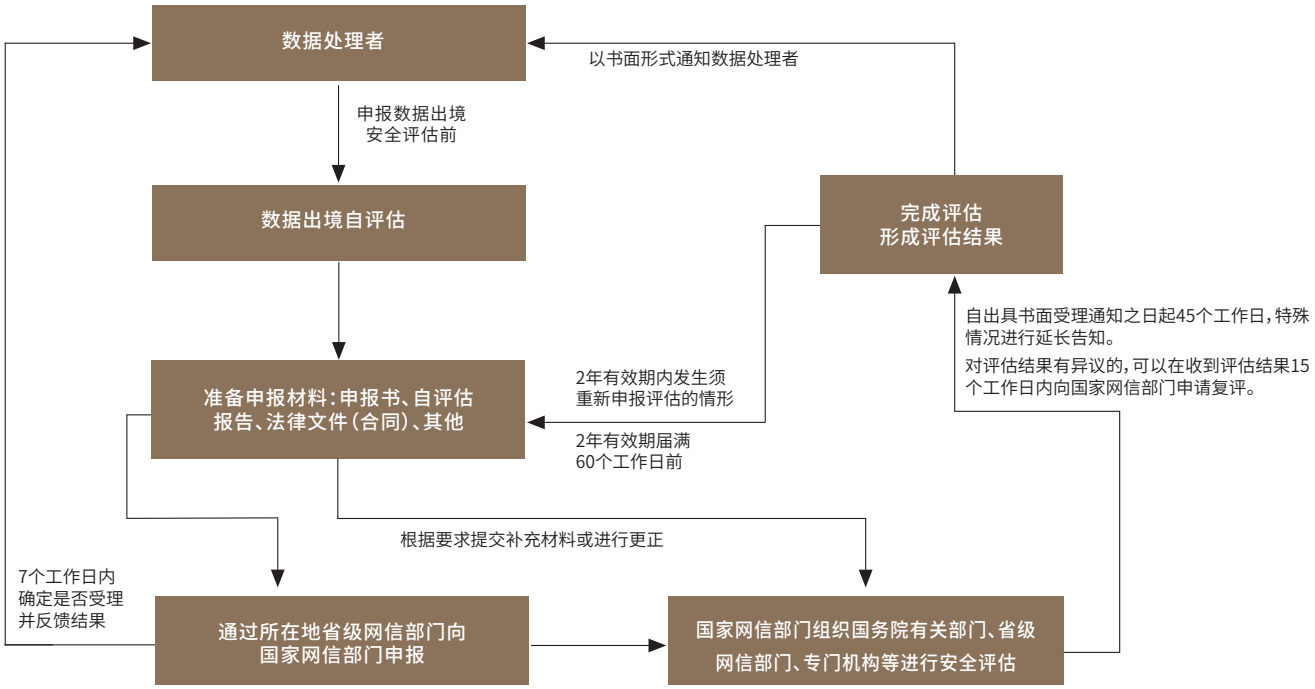
以上可以看出，《数据安全法》《个人信息保护法》生效之后这一时期的跨境制度，立法者逐渐梳理清楚了数据和个人信息之间的关系，搭建了基本统一的数据跨境法律制度框架。这一时期的个人信息跨境制度的构建拓展了多种允许数据跨境的路径。在众多路径中，安全评估仍然是数据合法跨境的最为重要的路径，也是特定数据处理者的强制性义务。同时，安全评估作为我国特色的数据跨境制度，其具体的落实应给予足够的关注和重视。而《数据出境安全评估办法》的最终生效，象征着我国数据出境安全评估制度的进一步落地，为数据处理者在开展数据安全评估工作提供了确定可操作的法律依据，因而具有里程碑式的意义。

三、《数据出境安全评估办法》内容解读

（一）数据出境评估情形与流程

数据出境评估情形与条件
数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：
（一）数据处理者向境外提供重要数据；
（二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；
（三）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；
（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。

从整体体例来看，《数据出境安全评估办法》对安全评估的程序性规则和实体评估内容均进行了规定。办法中所规定的自评估—申请评估—重新评估，以及评估材料、评估时间、评估通知、评估材料补充更正、评估结果撤销均属于程序性的规定。这些规定能够帮助数据处理者定位自己在开展数据出境安全评估工作中所处的时间点位。



（二）数据出境评估内容

上述环节中，数据处理者的自评估与网信部门等有关部门安全评估构成整个评估流程中相对关键和重要的内容。《数据出境安全评估办法》第 5 条、第 8 条及对自评估及安全评估的重点事项进行了列举说明。

值得注意的是，对于数据出境安全自评估是否为企业的强制性法律义务，在《数据出境安全评估办法》中也给出了相应的倾向性回答。我们注意到，《数据出境安全评估办法》正式稿第 5 条改变了企业需履行“自评估”的法定条件，将原先征求意见稿中“数据处理者在向境外提供数据前”改为“数据处理者在申报数据出境安全评估前”，因此我们理解，对于明显不符合或者不属于需向网信部门等相关部门申报数据出境安全评估的情形，数据出境安全风险自评估可能并非强制性法律义务，但这并不代表企业在向境外提供数据前无需进行任何内部自主判断，因此企业依然可以通过自评估的方式，对于是否满足数据出境安全评估的要求进行自证。此外，《个人信息保护法》第 55 条仍然对企业向境外提供个人信息的行为，需履行个人信息保护影响评估的法定义务。

自评估重点事项	安全评估重点事项
• 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性； • 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险； • 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全； • 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等； • 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务； • 其他可能影响数据出境安全的事项。	• 数据出境的目的、范围、方式等的合法性、正当性、必要性； • 境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求； • 出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险； • 数据安全和个人信息权益是否能够得到充分有效保障； • 数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务； • 遵守中国法律、行政法规、部门规章情况； • 国家网信部门认为需要评估的其他事项。

除上述之外，《数据出境安全评估办法》第 9 条对数据跨境法律文件（合同）应当包含的内容也进行了说明；法律文件条款的设置也将构成自评估和安全评估的重要组成部分 [1]。

数据出境法律文件评估
• 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等； • 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施； • 对于境外接收方将出境数据再转移给其他组织、个人的约束性要求； • 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施； • 违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式； • 出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

[1] https://mp.weixin.qq.com/s/fADcGdPeIUG0QZe1g3_hJw

以上可以看出，自评估与安全评估的重点事项在内容上有一定重叠，安全评估将重点关注数据出境活动对国家安全、公共利益、个人或组织合法权益带来的风险，并将基于此额外考虑境外接收方所在国家或地区的政策、法律、网络安全环境对出境数据安全的影响，以及数据出境活动及所涉相关方遵守中国法律、行政法规、部门规章情况。

（三）企业开展自评估的维度及要求

正如前文所述，本文认为数据处理者在正式开展评估工作时，应充分将申请评估阶段和合同等法律文件条款评估纳入到自评估的内容中。但鉴于这些评估内容在表述上仍较为宽泛，本文在对《数据出境安全评估办法》评估内容进行总结的基础上，进一步细化其颗粒度，争取为自评估工作提供一个更为清晰的指引。根据《数据出境安全评估办法》第 5 条、第 8 条和第 9 条的内容，本文认为可以从以下几个维度分别开展自评估工作：数据处理者维度、数据接收方维度、数据出境风险维度，以及合同约束维度。分别整理如下：

自评估维度	法规依据
数据处理者维度	第 8 条： （六）遵守中国法律、行政法规、部门规章情况
数据接收方维度	第 5 条： （三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
	第 8 条： （二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；
数据出境风险维度	第 5 条： （一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性； （二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险； （四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
	第 8 条： （一）数据出境的目的、范围、方式等的合法性、正当性、必要性； （三）出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险； （四）数据安全和个人信息权益是否能够得到充分有效保障；

自评估维度	法规依据
法律文件约束维度	第 5 条： （五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务；
	第 8 条 （五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；
	第 9 条 （一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等； （二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施； （三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求； （四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施； （五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式； （六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。
其他	第 8 条： （七）国家网信部门认为需要评估的其他事项。

根据上述整理，本文结合业务实践，尝试提出具有针对性的可落地和可操作性的评估内容。并结合上述的自评估流程，给出完成对应评估项的评估阶段，厘清各评估维度的流程定位。当然，评估内容的结构逻辑也可以根据实际情况进行灵活调整：

评估维度		评估内容
数据处理者维度	基本情况	企业基本信息
		分支机构、股权结构和实际控制人
		组织架构情况
		数据安全管理部门信息
		整体业务与数据情况
	数据安全保障能力	数据安全管理保障能力
		数据安全技术保障能力
		数据安全保障措施有效性说明
		遵守中国法律、行政法规、部门规章情况

评估维度		评估内容
数据接收方维度	基本情况	企业基本信息及企业所在地
		出境数据传输中和传输后情况
	数据安全保障能力	数据安全管理和技术措施及有效性、数据安全事件应急处置能力、个人信息权益保障情况等
	接收方所在地政治法律环境	境外接收方所在国或地区政策、法律、网络安全环境分析
数据出境风险维度	出境所涉业务基本情况	出境数据所涉相关业务基本情况
		出境数据所涉相关业务的数据资产信息
		出境数据的境内外数据中心信息
		数据出境涉及的系统平台信息
		出境数据流转路径及相关信息
	数据出境风险	数据出境的场景，包括数据出境的目的、方式和范围及其合法性、正当性、必要性
		出境数据属性（个人信息 / 重要数据）及数量、频率、范围、种类、敏感程度等
		出境数据在境内的存储地点、基本的保护措施、访问权限等
法律文件（合同）约束维度	法律文件（合同）内容	数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等
		数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施
		限制境外接收方将出境数据再转移给其他组织、个人的约束条款
		境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导致难以保障数据安全时，应当采取的安全措施
		违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款
		发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道

结语

出境数据在第三国的安全保障历来是国际层面诸多司法辖区数据跨境制度的关注重点，同时也随着法律对经济的影响而不断调整。比如，随着欧盟法院在 Schrems II 案中因担忧欧盟公民个人数据因可能被美国当局有关部门获取

而无法得到有效保障，决定欧美“隐私盾协议”无效，欧盟对其数据跨境制度中个人数据在第三国是否得到有效保障予以了重新审视，并于 2021 年 6 月发布了新版的标准合同条款（SCC）。而此后，欧盟数据保护委员会（EDPB）发布了《关于数据跨境转移的补充措施最终建议》（Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data），明确数据出境方在适用适当保护措施的情况下进行个人数据跨境时应进行数据跨境影响评估，评估第三国的现行法律和 / 或惯例中是否有任何内容可能影响数据出境方所采取的出境工具的适当保护措施的有效性，且须包含对第三国政府机构获取数据能力的评估。这一做法与我国的数据出境安全评估制度有异曲同工之处，表明欧盟当局通过数据出境方的影响评估，以补强论证适当保护措施有效性的监管意图。

《数据出境安全评估办法》的颁布，标志着我国距离数据安全评估制度的落地有了长足的进步，为数据处理者开展数据出境安全评估提供了确定性的法律依据。数据处理者应根据《数据出境安全评估办法》第 5 条、第 8 条和第 9 条的内容，严格按照规定程序开展工作。其中，自评估对各数据处理者的数据出境合规提出了更为细致且实际的要求，不仅可以成为数据安全评估制度的基础性、前提性工作，同时也有助于各数据处理者开展日常的数据流转梳理，对促进数据处理者数据管理的规范化、个人信息权益保护有巨大助益。

最后，从《数据出境安全评估办法》的落地我们也能看出国家对于数据安全监管的决心，“以安全促发展”将成为数字经济发展的首要指导原则之一。在数据安全上升到国家安全的今天，企业需要理解和体会国家数据监管的格局和基础原则，在原有的国际化发展的惯性中找到合规与商业的平衡点，寻求新型的国际化发展方向，在安全、合规的主旋律中奏响数字经济的新篇章。

感谢实习生吴仁浩对本文作出的贡献。

网络安全

“安全为本，发展为先”：《网络安全审查办法》正式发布

宁宣凤 吴涵 潘驰 姚敏侣

引言

2022 年的首个工作日，中央网络安全和信息化委员会办公室（中央网信办或者网信办）在其官网全文公布了《网络安全审查办法》（《办法》）。在《网络安全审查办法（修订草案征求意见稿）》（《修订草案》）面向社会各界公开征求意见六个多月后，备受市场关注的《办法》正式出台，帮助正在筹划或进行资本商业化运作的各家企业和中介机构**进一步廓清了“网络安全审查”的法律依据、适用主体、主管部门、审查内容以及周期流程等基本内容**。

总体来看，此次出台的《办法》释放出了主管部门对赴外上市企业坚持贯彻国家、网络和数据安全为本，同时兼顾社会经济发展整体利益的“利好信号”。本文在《办法》正式出台的背景下，**对其中重点关切问题进行梳理、分析和归纳，以期更好地理解和适用《办法》**。

一、《办法》的制定依据和审查体系

《办法》第一条清晰列明了其制定的上位法依据为《中华人民共和国国家安全法》（《国家安全法》）、《中华人民共和国网络安全法》（《网络安全法》）、《中华人民共和国数据安全法》（《数据安全法》）、《关键信息基础设施安全保护条例》（《关保条例》），同时表明，《办法》的立规宗旨目标为“确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全”。相比于《修订草案》，“网络安全和数据安全”成为新增内容，也表明《办法》将审查相关适用主体的特定活动下对于影响或者可能影响网络、数据和国家安全的多种因素。

考虑到《关保条例》已经于 2021 年 9 月 1 日起正式施行，因此，相比于《修订草案》，此次正式出台的《办法》中，将《关保条例》作为列明的上位法依据之一。此外，已经于 2021 年 11 月 1 日实施的《中华人民共和国个人信息保护法》（《个人信息保护法》）并未被列在《办法》的上位法依据中。不过，从立法立规的定位角度出发其实不难理解，《个人信息保护法》旨在保护个人信息主体基于个人信息所享有的相关人格权益，并以多种制度约束和规范个人信息处理活动，以实现促进个人信息合理利用为目标，而《办法》则主要侧重于网络、数据和国家安全利益保障。**但这并不意味着网络安全审查与个人信息保护完全不存在内在的关联**，例如当《个人信息保护法》下为个人信息处理者创设的诸多安全保障义务未得到履行和落实，从实质角度理解，相关企业仍然可能因大量的用户个人信息未得到合法合规处理而被判定为存在影响数据安全的客观风险，继而可能也无法通过审查。

在上位法依据中，《国家安全法》中规定了“国家安全审查”制度和机制，即“国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险（第五十九条）。”而《网络安全法》《数据安全法》

分别从网络安全和数据安全两个维度，在各自运行的领域内细化规定了适用于关键信息基础设施运营者采购网络产品和服务的网络安全审查、适用于数据处理活动的数据安全审查制度。从相关法律的体系解释角度来看，网络安全审查、数据安全审查并不完全等同，两者对于审查的内容、对象或许各有侧重，**但究其实质，前两者的内核与最终目标可能均为提前预判和审查影响或者可能影响国家安全的客观情形或者因素，因而共同构成“国家安全审查”体系下的两个关键面向和制度构成**。

二、《办法》的审查主体和主管机构

《办法》第四条未对《修订草案》进行调整，在中央网信办的领导下，包括国家网信办、国家发展和改革委员会、国家工信部等在内的十三个主管部门或者机构共同建立国家网络安全审查工作机制，并且由网络安全审查办公室具体负责制定网络安全审查相关制度规范，组织网络安全审查。**根据官方答记者问的情况说明[1]，网络安全审查的具体工作将由网络安全审查办公室委托中国网络安全审查技术与认证中心承担**。

值得注意的是，中国证券监督管理委员会（证监会）作为网络安全审查的主管部门之一，将参与到制度运行和审查工作中来，并可能将对企业赴外上市活动中影响或者可能影响国家安全的因素进行重点审查。结合此前发布的《国务院关于境内企业境外发行证券和上市备案管理办法（征求意见稿）》和证监会《境内企业境外发行证券和上市备案管理办法（征求意见稿）》，发行人在境外首次提交首次公开发行（IPO）上市申请文件后的三个工作日内，应当向证监会提交包括有关部门出具的安全评估审查意见在内的备案材料。又根据《网络安全审查办法》答记者问，网络平台运营者应当在向国外证券监管机构提出上市申请之前，申报网络安全审查。由此我们理解，证监会将在网络安全审查和备案管理两个工作机制上，形成新的监管连接点。

三、《办法》的适用对象

最终通过的《办法》将申报或者接受国家网络安全审查的适用对象限定为“关键信息基础设施运营者”和“网络平台运营者”。**与《修订草案》略有不同，《办法》将适用对象的合称调整为“当事人”而非“运营者”**，这对于从概念上准确把握和厘清与《网络安全法》下业已存在的“网络运营者”和“关键信息基础设施的运营者”有所帮助。

与《修订草案》中采用“数据处理者”的描述方式不同，《办法》中将掌握一百万以上用户个人信息赴国外上市必须申报网络安全审查的对象范围，限缩为“网络平台运营者”。对于何为“网络平台运营者”，我们在此前的团队文章《< 网络数据安全管理条例（征求意见稿）> 系列解读之网络安全审查篇》[2] 中进行了相对详细的解释，而对于此次调整中所涉及两个主体之间的关系，网络平台运营者基于其提供互联网信息或者其他服务的基本属性，其首先必定属于数据处理者；而对于掌握超过一百万以上用户个人信息的“非网络平台运营者”的国外上市活动，理论上而言的确不属于需要主动申报网络安全审查的范围。不过，一方面，从实践中看，结合《网络数据安全管理条例（征求意见稿）》以及相关规范，网络数据的定义和涵盖范围非常广泛，纯粹的、不通过网络提供产品和服务的数据处理者实则较为少见；另一方面，如果依据《办法》第七条便得出“非网络平台运营者在任何情况下都无需进行网络安全审查”的结论，也有失偏颇，这是因为根据《办法》，需要进行网络安全审查的适用情形也并非仅有“主动申报”一种；而只要在上市活动中存在影响或者可能影响国家安全的情形，网络安全审查制度也可能因有关部门的主动提请而触发。

总而言之，**我们判断是否适用主动申报或者接受有关部门网络安全审查的基本标准，仍是企业的经营活动（包括上市）以及相应的数据处理活动是否影响或者可能影响国家安全**，而仅从审查对象的边界或者范围进行判断可能仍然是不够充分的。

---

[1] 中国网信网：“《网络安全审查办法》答记者问”，载“中央网信办官网”，http://www.cac.gov.cn/2022-01/04/c_1642894602460572.htm，最后访问日期：2022 年 1 月 4 日。
[2] https://mp.weixin.qq.com/s/O04rbN5JelpYi14oOV9c5g

四、《办法》的适用情形与特定条件

（一）主动申报网络安全审查的法定义务

作为一种法定义务，当符合《办法》规定的条件时，企业应当主动申报网络安全审查。根据《办法》第五条至第七条，目前在：1）关键信息基础设施运营者采购网络产品和服务，经预判该产品和服务投入使用后可能带来的国家安全风险，对于影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查；2）掌握超过一百万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查，前述两种情形下企业负有向有关部门主动申报网络安全审查的法定义务。对于违反前述要求的，有关部门可以依据《网络安全法》和《数据安全法》的规定予以处罚。

对于国外上市活动中涉及触发“主动申报”情形的规定，主要有以下几个值得关注的地方。首先，较为一目了然的是，**中国香港特别行政区作为直辖于中央人民政府的地方行政区域，并非《办法》中规定的“国外”，因此并不属于《办法》第七条规定的需要企业主动申报网络安全审查的情形；其次，依然延续《修订草案》的用法，《办法》将“掌握”（而非“处理”）超过一百万用户个人信息的企业作为主动申报网络安全审查的义务主体**。初步理解，由于“掌握”并非属于固定的法律概念，因此其更倾向于采取“实质认定”的方法，以对用户个人信息实际的控制力或者影响力为衡量，对于超过一百万用户的个人信息有实质的控制力，或者较大的影响力的企业应当符合该条规定的条件，但仍然不能完全排除接受委托处理大量个人信息的企业仍需主动申报的可能性。

此外，我们注意到部分企业在境外上市准备阶段，可能将某些涉及大量用户个人信息的业务从上市体系内剥离至上市体系外的独立数据公司，进而主张不构成掌握一百万用户个人信息的网络平台运营者，进而无需主动申报网络安全审查。对此，完成剥离与否并不必然意味着是否“掌握”了用户个人信息，是否需要主动申报网络安全审查，还需基于数据公司与上市实体间的独立性、上市实体在剥离后对于数据的权限等多个维度进行判断。**但前述剥离措施依然具有较为积极的作用**。一方面，参照《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》第八条第二款规定，国务院有关主管部门可以要求剥离境内企业业务、资产或采取其他有效措施，消除或避免境外发行上市对国家安全的影响，因此，**企业在国外上市前主动采取剥离措施并非是对于网络安全审查制度或者规则的规避，而是对于监管重点关注的因上市引发国家安全风险的提前响应与预防，是一种积极的降低乃至消除潜在影响的举措，同时也有可能被认定为企业采取了《办法》第十六条中规定的“预防和消减风险的措施”**；另一方面，在完成剥离后，公司如未来国外上市后面临境外政府调取数据要求，能够具备对于相关数据不具备控制权从而无法提供的主张，**从而避免企业上市后所掌握用户信息遭到境外政府影响、控制或调用而违背境内法律的客观困境**。基于上述主张，公司亦可在申报材料中就所采取的剥离方案及未来应对国外监管调取数据要求的答复口径进行说明，从而能够一定程度加大公司通过网络安全审查的可能。

如上所述，网络安全审查制度是基于网络、数据和国家安全风险的实质判断所创立的，未来有关部门也将遵循实质风险审查和预防原则贯彻执行制度，因而企业应当摒弃任何企图通过改变上市结构等形式上规避网络安全审查的方法，而回归实质性地梳理、预判和解决相关安全风险因素的本质矛盾中来。

（二）接受有关部门网络安全审查的情形

从《办法》中可以很明确地发现，触发《办法》进行网络安全审查的情形、条件**并非仅限于**关键信息基础设施运营者采购网络产品和服务，以及掌握超过一百万用户个人信息赴国外上市这两种属于需要企业“主动申报”的情形。根据《办法》第十六条和第十九条，网络安全审查工作机制成员单位认为存在影响或者可能影响国家安全的网络产品

和服务以及数据处理活动（包含上市活动），经提请审批后可以开展网络安全审查。此外，网络安全审查办公室通过接受举报等形式发现前述情形的，也可以依法和依照相关程序，对相关主体和数据处理活动进行审查。

承前讨论，虽然企业赴港上市很可能不属于《办法》中规定的需要向有关主管部门“主动申报”网络安全审查的法定情形，**但是我们仍然建议，企业在赴港上市应当履行《网络安全法》《数据安全法》等基本的网络安全、数据安全要求，并且注重识别和防范自身经营实践或者上市前后可能存在网络和数据安全风险**。根据《办法》相关条文的解释，赴港上市活动其本身作为数据处理活动的具体形式之一，如果网络安全审查机制成员单位认为企业赴港上市过程中存在影响或者可能影响国家安全的因素的，可以依据《办法》第十六条提请审查。此时，企业需要积极配合相关审查流程。与此同时，该情形下接受审查的对象可能也不限于《办法》第七条规定的“网络平台运营者”。我们初步理解，在通常情况下，对于拟赴港上市的企业在进行国家安全分析时，需综合考虑所掌握的数据量级、数据敏感程度（是否涉及国家核心数据、重要数据）、企业自身所在的经营范围或者行业领域的特殊性，以及是否在日常经营或者上市前后涉及向境外提供数据等具体因素。

值得注意的是，《办法》第十六条中新增了“**为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施**”的相关要求。从条文解释来看，该条事实上规定有关主管部门可以依照相关要求，在进行网络安全审查期间要求企业采取特定类型的预防和消减风险措施，以避免审查程序延误风险防范的根本目标的实现，便于提前确保国家安全。从相关实践角度，前述可以选择的措施可能包括但不限于暂时停止提供网络产品和服务、暂时移除下载链接或者停止新账号注册等。

五、《办法》的审查内容与重点事项

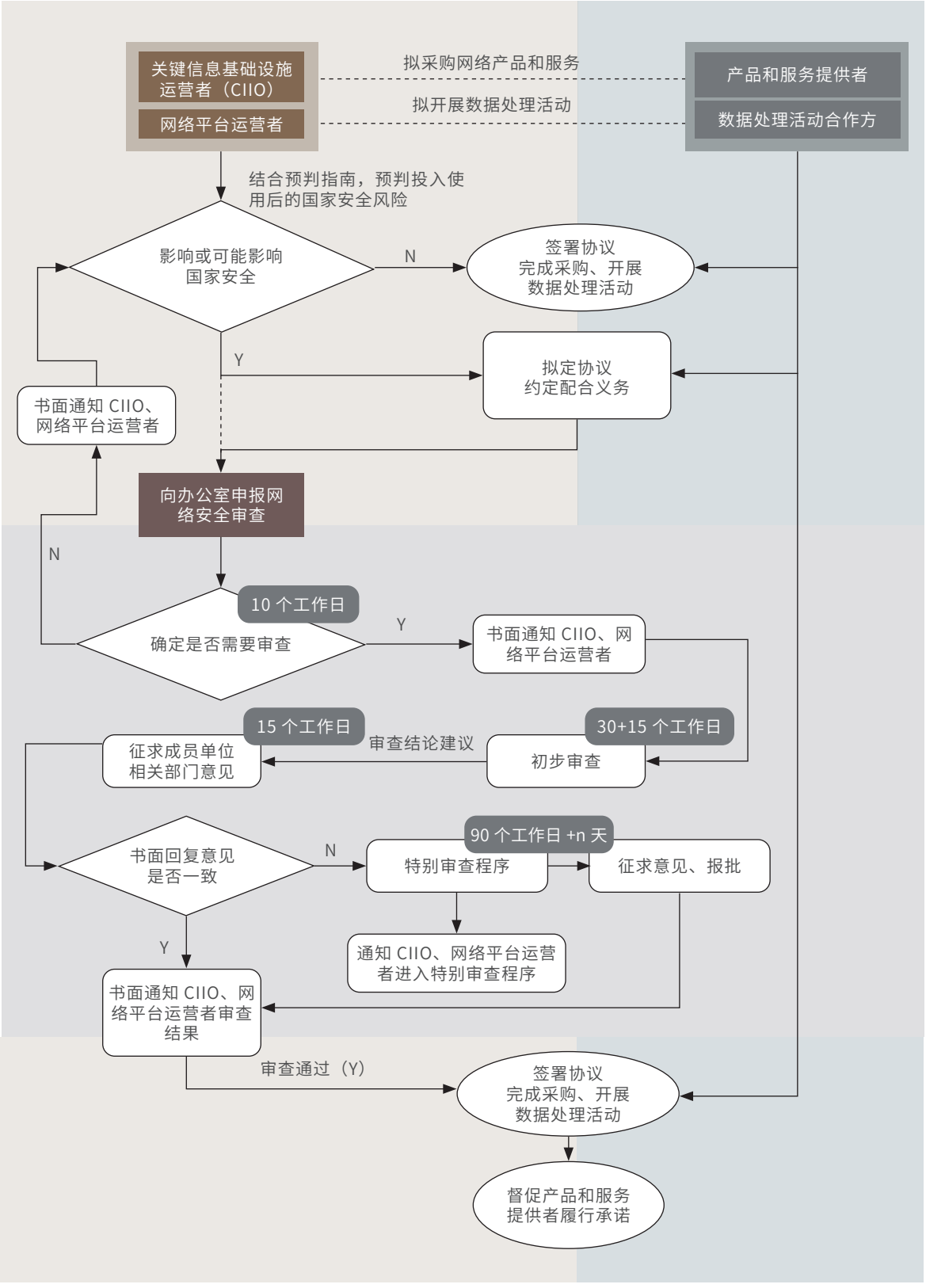
相较于《修订草案》，《办法》第十条对于关键信息基础设施运营者网络产品和服务采购的重点评估因素并无实质修订，但对于数据处理活动及企业国外上市的评估要素做了进一步明确与扩充，具体而言：

- **明确核心数据、重要数据或大量个人信息是否“非法”出境为评估因素**：相较于《修订草案》将核心数据、重要数据或大量个人信息是否出境作为评估因素，《办法》进一步明确网络安全审查重点关注的是企业非法出境行为所造成的潜在安全风险，而如企业能够按照《网络安全法》《数据安全法》《个人信息保护法》以及其他出境数据监管或行业监管要求，落实包括安全评估、获取用户同意在内的合规要求，对该等企业的数据出境行为将很可能不落入网络安全审查的评估范畴；

- **增加“网络信息安全风险”作为企业上市评估因素**：就如何理解网络信息安全风险，我们理解《网络安全法》作为《办法》的上位法，其第四章“网络信息安全”中所规定的内容应当是评估网络信息安全风险的重要参考因素，即主要包括企业个人信息的处理及保护措施的合规情况，以及上市阶段及上市后网络信息内容传播的安全风险。

六、《办法》规定的审查周期和流程

根据修订后的《办法》，网络安全审查办公室应当自收到符合《办法》第八条规定的审查申报材料起 10 个工作日内，确定是否需要审查并书面通知当事人。认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长 15 个工作日。网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门自收到审查结论建议之日起 15 个工作日内向运营者书面回复意见。网络安全审查工作机制成员单位意见不一致的，按照特别审查程序处理，特别审查程序一般应当在 90 个工作日内完成，情况复杂的可以延长。



网络安全审查流程周期图示

可以看出与《修订草案》相比，《办法》对于网络安全审查程序的流程及时间并未进行明显调整，仅将特别审查程序的一般审查时间由 3 个月修订为 90 个工作日，一方面从时间计算方式上与前文保持统一，另一方面进一步延长了特别审查程序的时间周期。因此我们初步计算：

- **一般程序所需时间自申报开始，最长需要 10+30+15+15=70 个工作日；**

- **而对于特别审查程序，最长需要 70 个工作日 +90 个工作日 +n=160+n 个工作日，即实际所需时间很可能达到 8 个月以上。**

对于拟国外上市企业而言，有必要结合企业业务实践情况在上市准备阶段评估是否适用网络安全审查、审查可能适用程序及预计所需时间，并结合上述网络安全审查程序安排上市计划及时间表。

七、《办法》与其他安全审查制度的衔接协调

相较于《修订草案》，《办法》第二十二条进一步规定，国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。我们理解，上述新增规定进一步明确了尽管同属于国家安全审查的范畴，但网络安全审查、数据安全审查及外商投资安全审查从监管对象、适用标准上可能仍存在一定差别。

而对于拟国外上市企业而言，我们理解上述三类审查存在同时适用的可能。这一观点也在近期公开的《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》中得到反映，其中第八条规定：境内企业境外发行上市的，应当严格遵守外商投资、网络安全、数据安全等国家安全法律法规和有关规定，切实履行国家安全保护义务。涉及安全审查的，应当依法履行相关安全审查程序。具体而言：

- **网络安全审查**：如前所述，《办法》第七条规定，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

- **数据安全审查**：根据 2021 年 9 月 1 日实施的《数据安全法》在第二十四条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。我们理解，如企业国外上市准备过程中同时存在影响或可能影响国家安全的数据处理活动，则有可能受到相关监管部门开展的数据安全审查。当然由于《办法》第二条同样将“影响或者可能影响国家安全的网络平台运营者所开展的数据处理活动”列入网络安全审查范围，因此数据安全审查与网络安全审查间的关系与衔接可能仍有待相关立法进一步明确。

- **外商投资安全审查**：根据 2021 年 12 月 27 日发改委商务部联合发布的最新 2021 年负面清单，禁止投资领域业务的境内企业到境外发行股份并上市交易的应当经国家有关主管部门审核同意。因此，如本身涉及从事外商投资准入限制行业的企业（例如测绘、义务教育等）计划赴国外上市，还应同时通过有关主管部门的审核同意。

总结

自《网络安全法》时代以来，我们渐渐地认识到，与网络文明进步相伴的往往也是新型安全风险与隐患，而原来仅聚焦于关键信息基础设施运营者采购网络产品和服务中安全防范的网络安全审查制度，也需要随之更新，并不断丰富风险应对的工具箱。在落实总体国家安全观下的指引下，此次修订调整后的《办法》的正式颁布和出台，无疑将在网络安全、数据安全等非传统安全问题的治理领域，为保护国家安全筑起一道更为坚实的防护墙。

而此次网络安全审查制度的调整和落地，对于企业而言也意味着新的机遇。深入认识和提前预防在网络运营、数据处理乃至上市活动中的相关国家安全风险，在满足条件或者符合要求时积极履行申报或者接受网络安全审查义务，秉持安全为本的理念下不断促成和实现自身发展与社会总体福利增长，将成为一个负责任的社会参与者、建设者和贡献者应当肩负起的法律职责。

回首峥嵘尽，连天草树芳——《网络安全法》首次修订的回顾与展望

宁宣凤　吴涵　张浣然

前言

2022 年 9 月 14 日，国家网信办在《中华人民共和国网络安全法》（《网安法》）实施五年后，发布了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（《意见稿》）。本次修订聚焦于《网安法》第六章的“法律责任”部分，旨在“做好《网安法》与新实施的法律之间衔接协调，完善法律责任制度，进一步保障网络安全”，将全面增强《网安法》的可操作性，确保《网安法》持续生命力，重申以安全促发展的原则。

日前，国家网信办亦发布以《网安法》为上位法依据之一的《网信部门行政执法程序规定（征求意见稿）》（《执法规定》），明确了网信部门的执法程序，并就管辖权问题作出清晰划定。《意见稿》与《执法规定》的联系与呼应将进一步为修订后的《网安法》落地实施提供坚实保障。

因此，本文将在梳理《意见稿》的重点修订内容的基础上，思考本次修订在我国网络空间治理层面和企业合规层面的建设性意义，并作出立法展望。

一、《网安法》的重点修订内容

《意见稿》共计作出六项修订。本部分以《关于修订〈中华人民共和国网络安全法〉的决定（征求意见稿）》中载明的四个修订面向为索引，基于修订前后的法条对比，就《意见稿》中六项修订的重点内容进行逐项梳理。

总体而言，可以认为《意见稿》的主要修法路径为理顺立法逻辑，弥补立法疏漏，增强与其他法律、法规衔接度，提升处罚幅度与立法精细度，包括引入“上一年度营业额百分之五”作为“情节特别严重”的处罚标准之一。我们同时也留意到，“情节特别严重”的处罚应当由省级以上有关主管部门作出，这是对《执法规定》中“省、自治区、直辖市网信部门依职权管辖本行政区域内重大、复杂的网络信息内容、网络安全、数据安全、个人信息保护等行政处罚案件”之职责划分的回应。

（一）完善违反网络运行安全一般规定的法律责任

从立法逻辑来看，《意见稿》第一项和第二项修订，均分别对违反《网安法》第三章中关于网络运行安全一般规定，包括未履行网络安全等级保护义务、网络产品和服务安全义务、违反用户身份管理规定等行为的法律责任进行整合；另一方面，第一项修订将违反第四十八条关于“电子信息、应用软件不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息”的罚则剥离，并在第五项修订中整合至同样规定网络信息安全保护义务的四十七、四十九条设立罚则。此外，还就违反第二十三条（网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求）和第二十八条（网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助）

的行为设定法律后果，整体上弥补了立法疏漏、优化了立法逻辑。

从处罚标准来看，第一项修订在原有的一般违法、情节严重的情形基础上，增设“情节特别严重”这一加重情形，对此处“一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款”。我们理解，该项用营业额进行处罚的规定承继《中华人民共和国反垄断法》《个信法》《网络数据安全管理条例（征求意见稿）》（《网数条例》），《意见稿》的第二至六项修订亦采取这一标准，大幅提升了原有的处罚标准，可对违反行为起到较强的震慑作用。

从处罚类型来看，第一项修订增设“通报批评”和“限制从业”两种处罚类型，“通报批评”是实践中广泛采用的处罚方式，而“限制从业”即可以“禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”，充分发挥《网安法》的指引作用，提高从业者的合规意识。具体内容对比如下：

原法条	修订后法条	修订重点
第一项 对于第五十九条至第六十二条的修订		
第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，**处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款**。 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正**或者导致危害网络安全等后果**的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。 第六十条 违反本法第二十二条第一款、第二款和**第四十八条第一款**规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者**导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款**： （一）设置恶意程序的； （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的； （三）擅自终止为其产品、服务提供安全维护的。 第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，**处五万元以上五十万元以下罚款**，并可以由有关主管部门**责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款**。 第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门**责令改正，给予警告**；拒不改正或者情节严重的，**处一万元以上十万元以下罚款**，并可以由有关主管部门**责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款**。	违反本法第二十一条、第二十二条第一款和第二款、**第二十三条**、第二十四条第一款、第二十五条、第二十六条、**第二十八条**、第三十三条、第三十四条、第三十六条、第三十八条规定的网络运行安全保护义务或者导致危害网络运行安全等后果的，由有关主管部门责令改正，给予警告、**通报批评**；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，**情节特别严重的**，由省级以上有关主管部门责令改正，**处一百万元以上五千万元以下**或者**上一年度营业额百分之五以下罚款**，并可以责令停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，**并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**	• **理顺立法逻辑** 一方面，整合了未履行等保义务、网络产品和服务安全义务、违反用户身份管理规定等行为的法律后果； 另一方面，将违反第四十八条的罚则剥离，并在第五项修订中整合至同样规定网络信息安全保护义务的四十七、四十九条设立罚则。 • **弥补立法疏漏** 就违反第二十三条和第二十八条的行为设定法律后果。 • **调整处罚标准** 增设“情节特别严重”这一加重情节； 整体提高处罚额度。 • **增设行政处罚类型** 对于一般违法行为增设“通报批评”； 情节特别严重则可以作出从业禁止决定。

原法条	修订后法条	修订重点
第二项 对于第六十三条和六十七条的修订		
第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，**可以并处五万元以上五十万元以下罚款**；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。 第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，**可以并处一万元以上十万元以下罚款**；情节较重的，处五日以上十五日以下拘留，可以并处**五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。** 单位有前款行为的，由公安机关处**十万元以上五十万元以下罚款**，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	违反本法第二十七条、第四十六条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，或者设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处**十万元以上一百万元以下罚款**，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。	• **整合规定** 整合违反二十七条、四十六条之规定的处罚措施。 • **提高处罚力度** 一方面，提高对个人违反第四十六条规定的处罚力度，即一般情况下的 1-10 万元提高至 5-50 万元；情节严重的情形则从 5-50 万元提高至 10-100 万元； 另一方面，提高对单位的处罚上限，从 10-50 万元提高至 10-100 万元。

（二）修订关键信息基础设施安全保护的法律责任制度，衔接数据出境安全管理体系

《意见稿》第四项修订了针对关键信息基础设施运营者（CIIO）违反国家安全审查规定采购网络产品或服务的行为的法律责任，增设“处上一年度营业额百分之五以下罚款” 与原有的“处采购金额一倍以上十倍以下”择一适用。

此外，将 CIIO 未履行数据出境安全评估等数据跨境安全管理义务的法律责任修改为转致性规定。鉴于《数安法》《个信法》已对中国数据跨境传输提出了统领性规定，与《网数条例》《个人信息出境标准合同规定（征求意见稿）》《数据出境安全评估办法》等配套法律法规共同构成数据出境安全管理义务群，明确了数据出境安全管理的义务与罚则，本次修订亦将增强《网安法》与我国数据出境安全管理体系的衔接度。

原法条	修订后法条	修订重点
第四项 对于第六十五条和六十六条的修订		
第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下**或者上一年度营业额百分之五以下罚款**，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	• **调整处罚标准** 新增“上一年度营业额百分之五以下罚款”与原有的“处采购金额一倍以上十倍以下”择一适用。
第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，**由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。**	关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，**依照有关法律、行政法规的规定处罚**。	• **增强与我国数据跨境安全管理制度体系的衔接度** 将 CIIO 违反数据跨境安全管理义务的法律责任修改为转致性规定，即适用《数安法》《个信法》的罚则。

（三）调整网络信息安全法律责任制度，增设兜底条款

《意见稿》第五项和第六项均是对网络信息安全法律责任制度的调整。其中第五项与第一项的修法思路相类似，亦从整合同类违法行为之责任、弥补立法疏漏、调整处罚幅度和增设行政处罚类型四个方面作出修订，具体可见以下对比表格。

第六项对于第七十条之修订，则可以从两方面进行理解：

（1）与第五项修订的关联性：由于本项修订对应的违法行为（第十二条第二款）与第五项修订（六十八条、六十九条）同属未履行网络信息安全保障义务的行为，处罚梯度与处罚标准与第四项修订保持一致具备合理性；

（2）设置兜底条款：即在无法律、行政法规明确规定的情况下，也可依据本条款对发布传输违法信息的行为进行处罚。我们理解，尽管 2020 年实施的《网络信息内容生态治理规定》对于禁止发布的违法信息作出列举式规定，但由于互联网内容生态具备多样性，对其生态治理难以作出穷尽式规定，因此，设置兜底条款具有前瞻性意义。

原法条	修订后法条	修订重点
第五项 对于第六十八条和六十九条的修订		
第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。 第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款： （一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的； （二）拒绝、阻碍有关部门依法实施的监督检查的； （三）拒不向公安机关、国家安全机关提供技术支持和协助的。	违反本法第四十七条、**第四十八条、第四十九条规定的网络信息安全保护义务**，或者不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取停止传输、消除等处置措施的，或者不按照有关部门的要求对网络存在较大安全风险和发生安全事件采取措施的，由有关主管部门责令改正，给予警告、**通报批评**，没收违法所得；拒不改正或者情节严重的，**处一百万元以下罚款**，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 **情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**	• **整合网络信息安全法律责任** 合并原第六十八条、六十九条的规定。 • **弥补立法疏漏** 新增违反第四十八条、第四十九条规定的网络信息安全保护义务的法律责任。 • **调整行政处罚幅度** 一方面增设“情节特别严重”这一加重情节； 另一方面整体提高处罚金额。 • **增设行政处罚类型** 对于一般违法行为增设“通报批评”； 情节特别严重则可以作出从业禁止决定。
第六项 对于第七十条的修订		
第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。	发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。 **法律、行政法规没有规定的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。** **情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**	• **增设兜底条款** 在无法律、行政法规明确规定的情况下，也可依据本条款对发布传输违法信息的行为进行处罚。 • **区分处罚梯度** 就一般情形、拒不改正或者情节严重、情节特别严重三种情形设置处罚，包括罚款、警告、通报批评和从业禁止等行政处罚类型。

（四）修订个人信息保护法律责任制度，设置转致性规定

《意见稿》第三项主要为对个人信息保护法律责任制度的修改，规定违反《网安法》第四章“网络信息安全”中对于个人信息的相关要求的法律责任直接适用《个信法》，有效增强了与《个信法》的衔接度，促进《网安法》《数安法》《个信法》“三驾马车”运行畅通。

原法条	修订后法条	修订重点
第三项 对于第六十四条的修订		
第六十四条 【违反个人信息保护相关规定的法律后果】 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，**由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。** **违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。**	网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十四条规定，侵害个人信息依法得到保护的权利的，**依照有关法律、行政法规的规定处罚。**	• **增强与《个信法》衔接度** 将个人信息保护的法律责任修改为转致性规定。

二、《网安法》修订之思考与立法展望

（一）关于我国网络空间治理和企业合规的思考

自《网安法》于 2017 年 6 月生效实施以来，时隔五年即迎来首次修订。本次修订有力回应了实务与学界就《网安法》对于企业的威慑力不足，与后续制定的《个信法》等法律之间的衔接度亟待提高的法律实效问题，有利于充分发挥《网安法》在我国网络空间治理的筑基作用，实现安全与发展“双轮驱动、两翼齐飞”。

对于企业而言，有必要理解从《意见稿》的修订内容、《执法规定》的发布以及国家网信办近期举办全国网信系统行政执法培训班等立法、执法动向中折射出的强监管、促实效之确保《网安法》持续生命力，促使企业加强自身网络安全建设和数据合规制度，采取主动合规路径的深意。

（二）立法展望

由于网络安全事项内在的复杂性与更迭频繁性，秉持着深入理解《网安法》的规范意涵并避免法律适用模糊性的问题意识，我们亦期待如下问题能够乘修订之东风，得到进一步释明。

就《意见稿》的六项修订内容而言：

（1）择一处罚的适用原则

整体来看，《意见稿》共计在四种情形下新增以“上一年度营业额百分之五以下罚款”与“一百万元以上五千万元以下”或“处采购金额一倍以上十倍以下”择一适用作为处罚标准，**但尚未明确采取就高或是就低原则进行适用**。

（2）处“上一年度营业额百分之五以下罚款”的合理性

一方面，除针对 CIIO 违反国家安全审查规定采购网络产品或服务的行为的法律责任进行修订的第四项修订以外，其他三项修订均以“情节特别严重”作为该等处罚的适用条件。

我们理解，**尽管对于关键信息基础设施运营者设定的网络安全保障义务应当高于一般的网络运营者，但考虑到 5% 的处罚幅度相当可观，且该违法行为不包含主观要件，是否亦当考虑设置特定情节或行为后果为该等处罚设定门槛**。

另一方面，对于“百分之五”这一比例作为“情节特别严重”情形之处罚的合理性需结合同样设置该比例的《个信法》《网数条例》进行分析论证，具体而言：

- **该处罚与《个信法》中“情节严重”的处罚标准相同**

  我们理解，尽管违反网络安全保护义务与违反个人信息保护义务的违法后果、对于个人和企业合法权益、公共安全造成的影响可能在一定程度上具有相当性，但由于《网安法》是捍卫我国网络空间主权、维护国家安全的法律重器，对于违反《网安法》“情节特别严重”的违法行为的处罚**可能需要考量对国家安全的影响，论证《个信法》采取同一处罚标准的合理性**。

- **该处罚与《网数条例》部分处罚规定一致**

  《网数条例》在两种情况下规定了营业额百分之五的处罚标准：数据处理者违法个人信息保护相关规定，情节严重的（第六十一条）；以及互联网平台运营者拒不改正的，处上一年度销售额百分之一以上百分之五以下的罚款（六十八条）。

  我们理解，对于第一种情况与《个信法》协调一致，在此不予赘述；但就第二种情况，对应的违反行为包括互联网平台运营者利用数据以及平台规则损害用户合法利益，利用数据误导、欺诈、胁迫用户，无正当理由限制用户访问其他互联网平台，利用个性化推送算法不符合规定等行为，且以“拒不改正”为适用情形。**考虑到“情节特别严重”对国家安全、社会公共利益造成的影响可能较“拒不改正”更为严重，故与《网数条例》的对比视角来看，《意见稿》该等处罚的合理性亦需进一步考量**。

（3）对于“情节特别严重”的适用标准考量

如前所述，“情节特别严重”情形的处罚标准较高、幅度较大，立法者**或可考虑列举“情节特别严重”的情形，**

以促进行政处罚裁量权合理行使，确保《网安法》实施执行的一致性和法律实效。

（4）对于“从业禁止”处罚的期限考量

- **从业禁止“一定期限”的期限考量**

《意见稿》第一项、第五项和第六项修订均增设了“从业禁止”处罚。2021 年修订的《行政处罚法》增设了限制从业这一行政处罚类型，可以反映立法者对实践中广泛存在的不允许从事某种职业等管制措施法治化问题的立法回应。我们理解，《网安法》要求网络运营者设置网络安全负责人、关键信息基础设施运营者设置专门安全管理机构和安全管理负责人，由于实务中通常该等职责均由企业的高管担任，因此增设限制从业呼应了这一要求，符合网络安全治理以控制和预防为抓手的治理思路。

然而，由于“一定期限”的规定较为模糊，或可考虑设定一定年限作为上限，或规定期限区间。

- **保留终身从业禁止规定的合理性**

《意见稿》第二项修订延续了《网安法》的规定，即违反第二十七条规定，受到刑事处罚的人员，不得从事网络安全管理和网络运营关键岗位的工作。我们理解，我国数部法律和行政法规中，从业禁止的期限从二年、三年、五年、十年[1]到终身不等，即从业禁止期限在立法实践中存在较多区间。

因此，考虑到二十七条中“明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助”的行为打击面广，从“受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作”之五年期限跃至终身，可能过于侧重处罚措施的惩戒性面向，不利于企业内部进行人员任用安排的自主性，亦恐损伤处罚措施的精准性，或可考虑采取如“五年至终身”的区间安排。

就与本次修订存在内在联系，但并未直接受到调整的《网安法》部分规范而言：

（1）“个人信息”等定义与《个信法》协调一致

《网安法》将个人信息定义为“以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息”，与《个信法》对于个人信息的定义存在一定程度的差异。考虑到《修订稿》的意旨之一在于增强与《个信法》之间的衔接度，**则对于“个人信息”定义的差异可能引发解读争议，影响法律适用效果。**

进一步而言，《网安法》第二十二条第三款规定，网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。从该规定的文义解释来看，用户信息分为个人信息和非个人信息。因此，虽然《意见稿》第三项修订使得针对用户信息中的个人信息的违法行为可以依据《个信法》进行处罚，**但这同时意味着用户信息中的非个人信息缺乏对应的处罚标准。**

[1] 例如《药品管理法》第一百二十二、一百二十三条，规定了十年内禁止从事药品生产经营活动；第一百二十三条、第一百二十四条，则规定十年直至终身禁止从事药品生产经营活动，可以看到从业限制的梯度设置。

我们理解，《网安法》中除此之外仅存在一处提及“用户信息”，即第四十条规定，“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。”由于在制定《网安法》时《个信法》尚未出台，**故该问题可能并非立法疏漏，而可能涉及不同法律之间定义与术语之间的协调一致，或可考虑将“用户信息”修改为“用户个人信息”来消除理解障碍。**

（2）对于《网安法》第三十七条的考量

《网安法》第三十七条规定，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个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当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；法律、行政法规另有规定的，依照其规定。

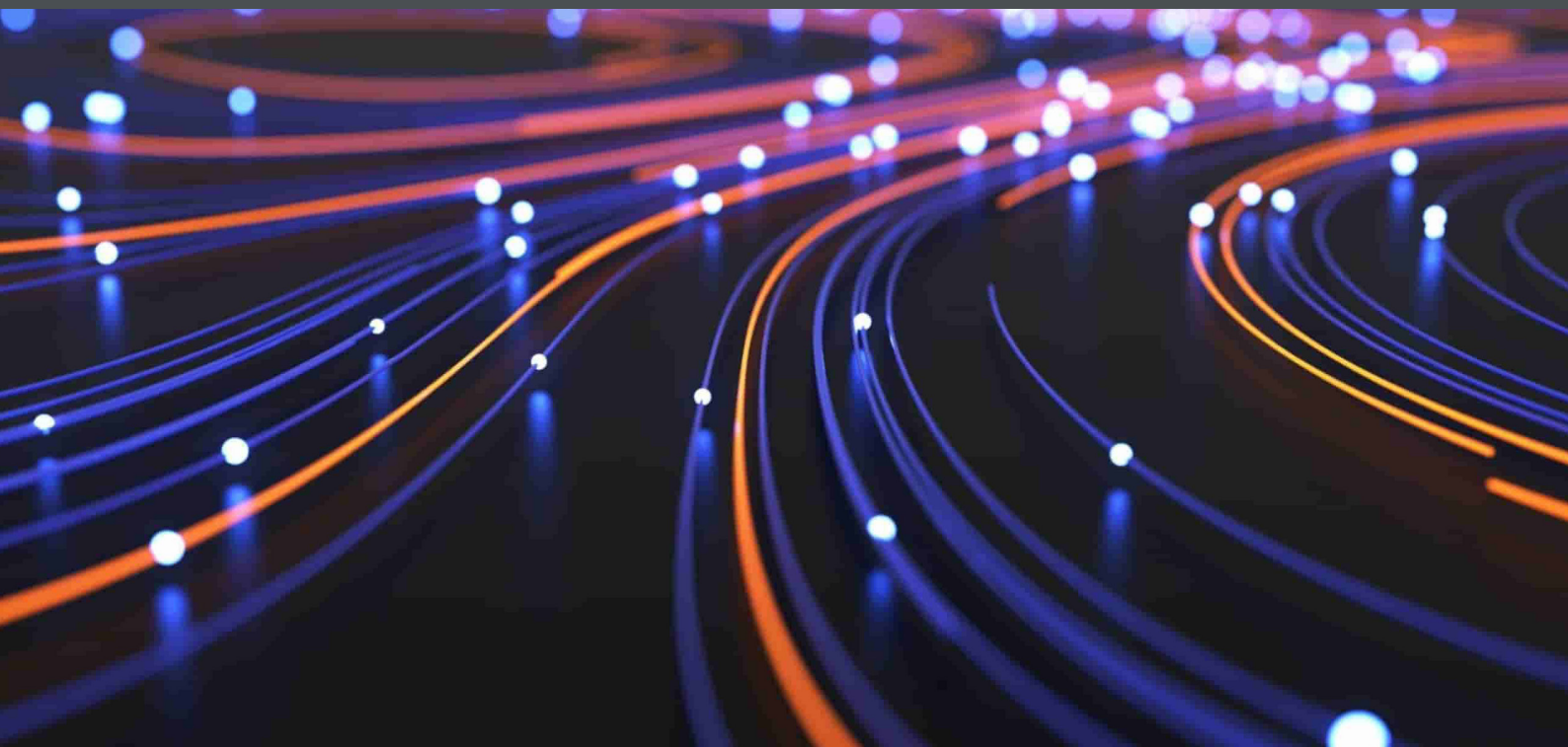
我们理解，由于《网安法》对于 CIIO 的规制相对严格，相关规定往往受到企业较高关注，故该条在实务中具备相当程度的争议，亟需就**“境内运营”的概念和外延予以进一步明确**，且由于 CIIO 也可能运营非关键信息基础设施，在其中产生的数据可能敏感程度相对较低，**或可考虑以“运营关键信息基础设施”为限制性条件。**

结语

在过去的五年，《网安法》作为网络空间治理的重要基础性法律弥补了网络安全的监管缺位问题，但《网安法》也同样需要顺应网络经济发展而更新，以延续《网安法》蓬勃的生命力，确保这部基础性法律的时效性和严肃性。

本次修订使《网安法》进一步落到实处，也与其他网络空间治理的规则保持同步更新，在日益丰富的网络法律中继续作为“中流砥柱”支撑起网络空间安全的屏障。企业的任务则在于准确理解修订的内在基础以及探讨空间。企业应当以修订为契机，加强对于《网安法》的规范理解，积极反思与加强自身的网络安全与数据合规体系建设，以新实践、新态度迎接未来可能生效的规范变化。

算法治理



算法治理之互联网信息服务推荐算法管理

宁宣凤　吴涵

2021 年 8 月 27 日，国家网信办发布了针对互联网信息服务算法推荐的专门管理规范《互联网信息服务算法推荐管理规定（征求意见稿）》（《征求意见稿》）并公开征求意见[1]。2022 年 1 月 4 日，在结束征求意见三个月后，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布《互联网信息服务算法推荐管理规定》（《规定》），对互联网信息服务算法推荐活动进行全面规范，以促进互联网信息服务健康发展。《规定》自 2022 年 3 月 1 日起施行。

继《个人信息保护法》《数据安全法》等法律法规概括性地从数据新技术的开发应用、自动化决策等角度进行规范[2]后，2021 年 9 月 17 日，国家互联网信息办公室联合中央宣传部、教育部、科学技术部、工业和信息化部、公安部、文化和旅游部、国家市场监督管理总局和国家广播电视总局联合发布《关于加强互联网信息服务算法综合治理的指导意见》（《指导意见》），首次在规范层面明确“算法治理”的概念并提出系统性、全面性的规范要求，标志着我国正式进入“算法合规”的新时代。

《指导意见》提出我国将利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局，并以此为基础明确提出算法治理的十五个主要目标。本次《规定》从监管内容、监管方式等多角度对该等目标进行了贯彻和落实。在《指导意见》的监管态度与规范思路下，《规定》以互联网信息服务算法推荐活动为切入点，从信息服务规范、用户权益保护、监督管理、法律责任等角度首次针对算法推荐应用提出具体规范要求。本文将结合《指导意见》的监管思路对《规定》的重点内容进行梳理和解读，从《规定》相比《征求意见稿》的修订内容分析监管趋势，并为企业提示初步合规建议。

一、《规定》重点内容梳理与解析

《指导意见》中关于算法治理的十五个主要目标在《规定》中均有体现，我们梳理出企业需要重点关注的落地规则，供大家参考。

（一）明确企业主体责任

对于“算法致损应由谁负责”这一问题，《指导意见》给予了明确答复，要求企业应强化责任意识，对算法应用产生的结果负**主体责任**。《规定》在此基础上进一步明确算法推荐服务的责任主体为在中国境内利用算法推荐技术（包括生

[1] 对《征求意见稿》的解读详见团队文章《积跬步，至千里——算法治理之互联网信息服务算法推荐管理》，https://www.chinalawinsight.com/2021/09/articles/uncategorized/%E7%A7%AF%E8%B7%AC%E6%AD%A5%EF%BC%8C%E8%87%B3%E5%8D%83%E9%87%8C-%E7%AE%97%E6%B3%95%E6%B2%BB%E7%90%86%E4%B9%8B%E4%BA%92%E8%81%94%E7%BD%91%E4%BF%A1%E6%81%AF%E6%9C%8D%E5%8A%A1%E7%AE%97/。

[2] 例如，《数据安全法》第二十八条规定，开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法[3]）提供互联网信息服务的算法推荐服务提供者。

关于责任内容，《指导意见》明确企业应建立算法安全责任制度和科技伦理审查制度，《规定》在第七条、第八条、第九条对该等制度提出了进一步的细化要求。

企业主体责任	具体责任内容
算法安全责任制度	建立健全相关管理制度和技术措施，包括： 1) 算法机制机理审核； 2) 信息发布审核； 3) 反电信网络诈骗； 4) 数据安全和个人信息保护； 5) 算法安全评估监测； 6) 安全事件应急处置。
	加强信息安全管理，建立健全违法信息和不良信息识别与应对机制，具体而言包括： 1) 违法信息 • 建立健全违法信息特征库，完善入库的标准、规则和程序； • 发现违法信息的，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信部门和有关部门报告； 2) 不良信息 • 建立健全不良信息特征库，完善入库的标准、规则和程序； • 发现不良信息的，应当按照网络信息内容生态治理有关规定予以处置。
科技伦理审查制度	建立健全科技伦理审查制度，科技伦理审查制度内容包括： 1) 算法推荐服务提供者应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等； 2) 不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。

（二）算法安全风险监测

鉴于算法的应用结果与输入数据、训练模型、应用场景等具有较高关联，《指导意见》明确企业应当对算法的数据使用、应用场景、影响效果等开展日常监测工作，以提前感知算法应用可能存在的安全隐患及伦理问题。《规定》对日常监测的要求进行细化，要求算法推荐服务提供者定期对算法的机制机理、模型、数据和应用结果等进行审核、评估和验证。我们理解，根据《规定》的立法目的，**企业应对该等算法的审核、评估和验证应当以算法的鲁棒性、公平性、透明程度以及数据使用的最小必要等方面作为评价维度**。

（三）推动算法公开透明

结合《指导意见》与《规定》的相关要求，我们理解整体而言可以从以下三个维度提高算法应用的透明度：

[3] 对该等算法含义的解读详见团队文章《积跬步，至千里——算法治理之互联网信息服务算法推荐管理》，https://www.chinalawinsight.com/2021/09/articles/uncategorized/%E7%A7%AF%E8%B7%AC%E6%AD%A5%EF%BC%8C%E8%87%B3%E5%8D%83%E9%87%8C-%E7%AE%97%E6%B3%95%E6%B2%BB%E7%90%86%E4%B9%8B%E4%BA%92%E8%81%94%E7%BD%91%E4%BF%A1%E6%81%AF%E6%9C%8D%E5%8A%A1%E7%AE%97/。

（1）在算法的设计与开发阶段，通过使用透明度较高的算法模型、简化算法逻辑等方式优化检索、排序、选择、推送、展示等规则的透明度和可解释性；

（2）在算法的使用阶段，及时、合理、有效地公开算法基本原理、优化目标、决策标准等信息，具体而言可以通过显著方式告知用户算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图、主要运行机制等；

（3）在算法的使用阶段，设立投诉申请与意见反馈机制，为公众或个人提供算法解释与意见响应的渠道，以提高公众对算法的接受程度。

（四）积极开展算法安全评估

《指导意见》要求企业组织建立专业技术评估队伍以深入分析算法的机制机理，并从算法的设计、部署和使用等全生命周期应用环节评估缺陷和漏洞，研判算法应用产生的意识形态、社会公平、道德伦理等安全风险，提出针对性应对措施。针对这一要求，《规定》除在第七条、第八条要求对算法进行安全评估监测并定期评估算法机制机理、模型、数据和应用结果之外，还对具有舆论属性或者社会动员能力的算法推荐服务提供者提出了算法安全评估的特殊要求，明确其应当按照国家有关规定开展安全评估。此外，鉴于该等算法推荐服务提供者应当履行备案的义务，在其填报备案系统信息时需提交算法自评估报告，我们理解该等算法推荐服务提供者需履行相应算法自评估的义务。

（五）算法分级分类体系及算法备案制度

《指导意见》中明确国家将建立算法备案制度并有序地推进算法备案的相关工作，以梳理算法备案的基本情况，并在此基础上健全算法分级分类体系。《规定》在第二十四条、二十五条、二十六条对算法备案制度进行明确。具体内容包括如下：

（1）备案主体的范围：具有舆论属性或者社会动员能力的算法推荐服务提供者；

（2）备案需填报信息：服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息；

（3）备案方式：通过互联网信息服务算法备案系统填报；

（4）备案时间：在提供服务之日起十个工作日内；

（5）备案公示：完成备案后应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接；

（6）备案变更：备案信息发生变更的，应当在变更之日起十个工作日内办理变更手续；

（7）备案注销：算法推荐服务提供者终止服务的，应当在终止服务之日起二十个工作日内办理注销备案手续，并作出妥善安排。

同时，《规定》也在第二十三条对算法的分级分类制度进行进一步明确，对算法进行分级分类的影响因素包括但不限于如下：

（1）舆论属性或者社会动员能力，我们理解包括例如人脸识别算法；

（2）内容类别；

（3）用户规模；

（4）算法推荐技术处理的数据重要程度，我们理解对此因素的判断可以参考企业现有的数据分级分类方法与标准，通常包括个人信息、敏感个人信息、生物识别信息、重要数据等维度；

（5）对用户行为的干预程度。

（六）充分保障网民合法权益

《规定》以专章的形式对用户权益保护提出要求，并结合《个人信息保护法》等相关法律法规的要求，对算法推荐服务提供者设定义务，主要包括如下内容：

（1）标签管理：

- 加强企业自有的用户模型和用户标签管理：完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息；
- 为用户提供自主标签管理的渠道：向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能；

（2）提高算法应用的透明度：以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等；

（3）用户选择退出权：向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项；

（4）设置面向用户和公众的投诉反馈渠道：设置便捷有效的用户申诉和公众投诉、举报入口，明确处理流程和反馈时限，及时受理、处理并反馈处理结果；

（5）向特定人群提供服务的特殊要求：

- 向未成年人提供服务的特殊要求：通过开发适合未成年人使用的模式、提供适合未成年人特点的服务等方式，便利未成年人获取有益身心健康的信息。此外，不得向未成年人推送可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息，不得利用算

法推荐服务诱导未成年人沉迷网络；

- 向老年人提供服务的特殊要求：充分考虑老年人出行、就医、消费、办事等需求，按照国家有关规定提供智能化适老服务，依法开展涉电信网络诈骗信息的监测、识别和处置；

- 向劳动者提供工作调度服务的特殊要求：保护劳动者取得劳动报酬、休息休假等合法权益，建立完善平台订单分配、报酬构成及支付、工作时间、奖惩等相关算法。

二、《规定》相比《征求意见稿》修订内容体现的监管趋势

《规定》相比《征求意见稿》并未进行大面积修订，在较大程度上延续了《征求意见稿》中的相关内容，但我们理解以下修订之处体现了相应的监管趋势：

（一）多部门联合执法

与《征求意见稿》中将国家互联网信息办公室（网信办）作为单一的主导监管部门不同，《规定》贯彻落实了《指导意见》中“强化统筹协同治理”的监管思路，规定由网信办会同工业和信息化部、公安部和国家市场监督管理总局联合负责统筹和监管。我们理解，上述部门一方面在监管中多领域、多方面的协同合作，另一方面也加入了技术支持以作为技术审查的支撑，同时具备了实质的强制执行力，因此我们理解多部门的合作体现了算法治理中技术与规范并行、下沉式、严格化的监管趋势。

（二）强调科技伦理审查

相比《征求意见稿》，《规定》在多处通过添加或修改表述的方式强调算法的科技伦理审查，体现了监管针对“技术中立”性以外的思考。换言之，算法并不因为其天然的技术属性而不具有价值谴责的可能性。根据相关法律法规及国际监管现状，我们理解在算法推荐的场景下常见的科技伦理审查维度包括内容向善、公平公正、透明公开、科学合理、可信等。对算法进行评估或日常监测以审查其科技伦理将成为算法合规的重要内容。

（三）向老年人提供服务的特殊要求

相比《征求意见稿》，《规定》首次针对向老年人提供服务的场景提出特殊要求。我们理解，在专门针对老年人提供特定适老性服务或产品的情况下，鉴于该服务或产品主要的受众群体为老年人，因此企业仅需在该服务和产品的研发、设计和使用阶段将上述关于老年人的特殊要求进行贯彻即可。但在一般场景下，某一服务或产品可能并非专门针对老年人设计和研发，因此为履行相关义务，企业可能需要识别所使用服务或产品的用户是否为老年人。如何在合法合规的前提下达到该识别目的可能需要进一步探讨。

三、企业需要重点履行的合规义务

《指导意见》与《规定》的相继出台与生效标志着我国正式进入算法治理的新时代，算法也逐渐成为监管所关注的执法焦点之一。基于此，涉及算法研发、设计和使用的企业需根据监管要求逐步建立并完善算法合规制度和体系。

在现阶段，我们理解企业应当采取的措施包括但不限于如下方面：

（1）指定算法合规管理机构负责企业的算法合规管理工作；

（2）建立健全算法合规内部制度，包括算法机制机理梳理与审核、用户注册审核、信息发布审核、反电信网络诈骗等。其中应重点关注算法安全评估监测，通过定期测试并评估算法的鲁棒性、透明程度、公平程度等监测算法的潜在风险；

（3）梳理企业内部涉及算法推荐服务的核心业务以及所使用的核心算法，包括其所使用的数据类型及敏感程度、算法模型（例如是基于规则的逻辑推理模型还是机器学习模型等）、舆论属性或者社会动员能力、所涉及的用户规模、对用户行为的干预程度等，并在此基础上进行初步分级分类；

（4）基于上述梳理，重点关注其中具有舆论属性或者社会动员能力的算法，并梳理其服务形式、应用领域、算法类型、拟公示内容等信息，并形成初步的算法自评估报告，以供后续备案使用；

（5）对于核心业务所使用的核心算法，梳理其基本原理、目的意图和主要运行机制，并在官网、App 交互界面等位置进行公示。对于使用机器学习模型等较为复杂的算法模型，我们理解可以尽可能告知算法设计的基本思路（包括设计目的及设计逻辑）、对该算法输出结果会产生影响的因素等；

（6）建立用户及公众提出异议和进行投诉的渠道并设置相应的反馈机制。例如通过公示算法咨询的热线电话、邮件或通过客服交互界面等方式为用户提供咨询或投诉渠道，并设置内部的话术模板、反馈机制（如由哪些部分负责协调与支持，以及在何种情况下需要相关部门介入等）、反馈期限等。

“算法”已从最初的概念宣传逐步发展至生活中方方面面的应用和实践，渗透到每一个领域和场景之中，对我们的生产生活产生巨大影响。监管部门在规制数据的基础上逐步开始关注算法应用，是法律拥抱技术变革的重要体现，也是保障技术健康有序发展的必要措施。“算法合规”的时代已经到来，我们有理由相信监管与企业及各方将共同努力，持续助力算法新时代的建设与发展。

感谢实习生张子谦对本文作出的贡献。

“假作真时真亦假”——数字社会中辨伪存真的挑战

宁宣凤 吴涵 屈尘 徐梦悦

前言

数字社会的发展将不可避免地带来新的社会问题。虚拟空间与物理社会融合发展中的重要挑战之一在于如何平衡“以假乱真”的技术发展趋势和“辨伪存真”的社会治理要求。

2019 年，“AI 换脸”的风潮将深度合成技术带入大众视野。用户只需要上传一张自己的照片，便可以在各种影视剧的经典场面中“出镜”。但除了众人所熟知的“AI 换脸”外，作为一种基础计算机技术，深度合成技术还包括语音合成、人脸替换、图像生成等，与近期网络空间发展的其他概念和技术比如元宇宙、虚拟人、AR/MR/VR/CR/XR 等息息相关。然而，不可否认的是，深度合成技术的滥用同时也引发了诸如“以假乱真”、信息泄露等一系列合规风险。

自党的十九大报告提出“营造清朗的网络空间”的总任务要求以来，2020 年 12 月 7 日，中共中央即在《法治社会建设实施纲要（2020-2025 年）》提出了对网络空间进行依法治理、推动现有法律法规延伸适用到网络空间的积极号召。其中，针对算法推荐、深度伪造等新技术应用制定相关规范管理办法，被视为完善网络法律制度的关键步骤之一。

在此背景下，2022 年 1 月 28 日，国家互联网信息办公室发布《互联网信息服务深度合成管理规定（征求意见稿）》（《深度合成服务规定》）。《深度合成服务规定》旨在规范互联网信息服务深度合成活动，促进深度合成技术依法、合理、有效利用，并在已经出台的《网络信息内容生态治理规定》《互联网信息服务算法推荐管理规定》《网络音视频信息服务管理规定》等相关部门规章和规范性文件的基础上，进一步厘清、细化了深度合成技术应用场景，明确了深度合成服务提供者与使用者信息安全义务，并以“促进深度合成服务向上向善”为总体要求，提出了一系列具有系统性、针对性和可操作性的要求。本文将结合境内外立法实践，对《深度合成服务规定》进行深度解读，并对深度合成服务提供者等主体的合规义务进行释明。

一、深度合成技术概述

从技术层面看，深度合成技术（Deep Synthesis）即深度伪造（Deepfake），是深度学习（Deep Learning）与伪造（Fake）二者的组合词，该技术主要依托于“生成式对抗网络（Generative Adversarial Networks，GAN 算法）”及自动编码机（Autoencoders）。[1] 具体而言，GAN 算法上同时搭载着两个神经网络，即生成器与识别器，前者可基于一个数据库自动生成模拟该数据库中数据的样本，后者可评估生成器生成的数据的真伪，两者在互相博弈学

[1] 参见曹建峰：《AI 生成内容发展报告 2020—“深度合成”（Deep synthesis）商业化元年》，载腾讯研究院公众号，2020 年 5 月 11 日，https://mp.weixin.qq.com/s/RNZIq87DnT-V5L-OKUESOag。

习中产生大规模和高精确度的输出。而自动编码器则是一个人工神经网络，用于对输入数据进行重建以实现数据合成。[2] 随着深度合成技术的不断成熟和日益复杂化，无论是图像还是声音、视频都可以通过深度合成技术进行伪造或自动合成，且达到以假乱真的程度。

《深度合成服务规定》则在法律层面上，明确了深度合成技术的概念，即“**以深度学习、虚拟现实为代表的生成合成类算法制作文本、图像、音频、视频、虚拟场景等信息的技术**”[3]，并且通过列举的方式明确了纳入规制范围的技术种类。我们在此对各类深度合成技术在实践当中的运用场景加以总结：

《深度合成服务规定》规制的深度合成技术种类	常见实践应用
篇章生成、文本风格转换、问答对话等对文本内容进行生成或者编辑的技术	短文本摘要、智能对话生成、诗歌创作、评论文本生成 [4]
文本转语音、语音转换、语音属性编辑等对语音内容进行生成或者编辑的技术	语音合成、数字配音、有声读物、个性化语音播报 [5]
音乐生成、场景声编辑等对非语音内容进行生成或者编辑的技术	虚拟演唱会
人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等对图像、视频内容中人脸等生物特征进行生成或者编辑的技术	AI 换脸、AI 主播、数字虚拟人、虚拟歌手、数字试穿 [6]
图像增强、图像修复等对图像、视频内容中非生物特征进行编辑的技术	电影后期制作、沉浸式体验、3D 影像
三维重建等对虚拟场景进行生成或者编辑的技术	元宇宙、沉浸式体验

从以上定义不难看出，监管机构并未采取穷尽列举的方式，这是由于深度合成技术处于不断发展、持续演进的过程中，而《深度合成服务规定》所采取了“概念 + 分类”的定义方式既能够概括说明深度合成技术的特点，又能够通过具体的示例具象化相关技术手段。我们理解，深度合成技术的特点包括：

- **高度技术化**：高质量、高仿真的深度合成技术需要大量的专业技术人员和专业工具参与；
- **应用领域广**：高度仿真能力的深度合成技术已经广泛应用在影视、娱乐、教育、医疗、社交、电商、内容营销、艺术创作、科研等诸多领域中；
- **发展潜力大**：随着深度合成技术工具的不断发展，深度合成内容的应用规模和使用范围也变得更大，内容的说服力也更强。[7]

[2] 同注 1。
[3] 《互联网信息服务深度合成管理规定》第二条第二款。
[4] 参见张晨阳，杜义华：《短文本自动生成技术研究进展》，载《数据与计算发展前沿》2021 年第 3 期。
[5] 同注 1。
[6] 同注 1。
[7] 参见王劭方：《浅析深度合成技术与电子信息数据安全》，载《网络安全技术与应用》2021 第 12 期。

二、深度合成技术的监管背景

在数字化社会，以算法为核心、以数据为资源、以平台为基础的发展格局逐步形成，这一新型网络格局涵摄政治、经济、文化与社会发展的数字化生态，塑造出以数据和算法为基础的新型法权关系，为法律制度和司法体系带来极大冲击和“破窗性”挑战。[8]作为第四次工业革命和数字经济发展的核心驱动力之一，算法所带来的变革需要法律予以回应。具体而言，算法的广泛应用可能引发歧视性风险、责任性风险，以及误用和滥用风险等极具挑战性的治理风险。[9]具体到深度合成领域，对深度合成技术的不当使用可能导致一系列治理风险，最为核心的三种风险是技术异化风险、信息失真风险和数据泄露风险。[10]

技术异化是指对技术的使用脱离了其“以人为本”的初衷。例如，“AI 换脸”技术诞生的初衷是出于娱乐目的，但逐渐变成了“色情复仇”的手段。2017 年 12 月，名为“Deepfake”的账号在社交新闻网站 Reddit 上发布了一段利用人工智能技术将名人面孔合成的色情视频，受害者皆为知名女性艺人。即便 Reddit 随即禁止未经同意使用人工智能将他人面孔植入色情视频和图像，深度合成技术依然引发了社会的强烈关注。[11]此后，随着深度合成技术在知名开源及私有软件项目的托管平台 GitHub 被开源以及各软件开发爱好者对其代码进行不断迭代与改良，该技术在精准度不断提升的同时，造成的恶劣影响也在不断扩大与加深。2019 年 12 月全网共有 14678 个深度合成视频，其中 96% 属于色情性的深度合成视频，主要存在于色情网站。[12]

信息失真是指深度合成技术可能导致假新闻泛滥，扰乱视听甚至导致真相终结。[13]由于深度合成技术的核心在于“以假乱真”，因此通过深度合成技术伪造的消息往往不会令人起疑，这使得当真假消息同时出现时，社会公众往往无法辨认其真实性。美国大法官霍姆斯曾经在 Abrams v. United States 案中提出“观念市场”（marketplace of ideas）的概念[14]，即真理和谎言同在自由的信息空间中传播，通过一系列竞争与辩论，真相终将胜利。然而，在互联网领域，考虑到网络传播的开放性、匿名性、交互性、复杂性和主观性，真假难辨的信息可能导致观念市场的失灵，从而使得真相进一步消弭。尤其是，当公众长期处于观念市场失灵的社会环境中，容易导致政府公信力下降，从而引发信任危机。

个人信息等数据泄露是深度合成技术最为直接的风险。以常见的“AI 换脸”技术为例，该技术服务自上线起，关于其“侵犯隐私”的质疑便层出不穷。为此，2019 年 9 月，工信部约谈了某 AI 换脸服务提供商，要求其组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。[15]此外，国家网信办、公安部于 2021 年 3 月 18 日指导地方网信部门、公安机关依法约谈了 11 家未履行安全评估程序的语音社交软件和涉深度伪造技术的应用开发企业。[16]此外，考虑到深度合成技术可能带来的巨大风险，《中华人民共和国民法典》第 1019 条明确规定，任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。

综上所述，综合考虑深度合成技术的广泛应用及其可能带来的一系列治理风险，通过专门的监管文件对其进行规制存在合理性和必要性。

---

[8] 参见马长山：《智能互联网时代的法律变革》，载《法学研究》2018 年第 4 期。
[9] 参见贾开、薛澜：《第四次工业革命与算法治理的新挑战》，载《清华管理评论》2021 年第 4 期。
[10] 参见万志前、陈晨：《深度合成技术应用的法律风险与协同规制》，载《科技与法律》2021 年第 5 期。
[11] See Erin Carson: Reddit cracks down on ‘deepfake’ pornography, publish on CNET, Feb. 7, 2018, https://www.cnet.com/news/reddit-cracks-down-on-involuntary-pornography-deepfakes/.
[12] 同注 1。
[13] 参见万志前、陈晨：《深度合成技术应用的法律风险与协同规制》，载《科技与法律》2021 年第 5 期。
[14] *Abrams v. United States*, 250 U.S. 616 (1919).
[15] 参见《工信部约谈陌陌：要求对 ZAO App 数据安全问题自查整改》，载新浪科技，2019 年 9 月 4 日，https://tech.sina.com.cn/i/2019-09-04/doc-iicezueu3281126.shtml。
[16] 参见《隐私泄露、AI 换脸存风险 11 家企业被约谈》，载北京商报，2021 年 3 月 19 日，http://epaper.bbtnews.com.cn/site1/bjsb/html/2021-03/19/content_463629.htm。

三、境外立法现状

（一）美国

美国是对深度伪造技术最早开展治理的国家之一，且相关治理行动也较为积极。总体而言，多项联邦及州立法就深度合成技术的应用提出了**不得制作与发布政治干扰、色情报复等犯罪及侵权内容与信息、对深度合成内容与信息进行披露与标记、鼓励监测及鉴别技术工具的研发、获得他人同意**等规制要求，违反者或面临包括罚款、监禁等行政或刑事责任。以下我们就联邦层面与州层面的部分立法进行分别举例说明：

- **《恶意深度伪造禁止法案》（Malicious Deep Fake Prohibition Act of 2018）**，该法案规定，为引发联邦法、各州法或地方法所规定的犯罪和侵权行为而制作深度伪造内容者，以及在明知有关视听记录内容为深度伪造的前提下，为引发联邦法、各州法或地方法所规定的犯罪和侵权行为而分发该视听记录内容者，将面临罚款及高达 2 年监禁的刑事责任；如果前述行为导致联邦、各州或地方，包括选举、外交关系处理在内的任何行政、司法及立法程序遭受影响的，或者出现煽动暴力的情况的，违法者还面临罚款及高达 10 年监禁的刑事责任。[17]

- **《深度伪造报告法案》（Deep Fake Report Act of 2019）**，该法案要求国土安全部以深度合成技术、种类及其演变情况，深度学习技术成果的应用场景、风险及益处，美国非政府组织将如何使用深度伪造技术，外国政府利用深度伪造技术对美国国家安全及个人权益所可能造成损害，以及应对深度伪造技术的策略等内容为主题，在本法案生效后一年内出具报告，并在此后以 5 年为频率再度提供报告。[18]

- **《深度伪造责任法案》（Deep Fakes Accountability Act）**，该法案要求任何创建深度伪造视频媒体文件的人，必须用“不可删除的数字水印以及文本描述”，对相关媒体文件属于篡改或生成的这一情况进行披露，违反者将面临罚款、最高五年监禁或两者并用的刑事责任。[19]

- **《识别生成对抗网络法案》（Identifying Outputs of Generative Adversarial Networks Act）**指示美国国家科学基金会和美国国家标准与技术研究院，为可对生成对抗网络或其他合成操纵技术所输出的内容和信息的真实性进行检查、验证的技术工具的相关研究进行支持。[20]

- **《2018-2020 财年情报授权法》（Intelligence Authorization Act for Fiscal Years 2018, 2019 and 2020）**指示国家情报总局通过举办相关竞赛计划并颁发奖项的方式，刺激与鼓励那些用于检测机器学习技术所创建的虚假音视频的技术的研究、开发及商业化进程。[21]

- **《2020 财年国防授权法案》（National Defense Authorization Act For Fiscal Year 2020）**则要求国家情报局负责人在该法案生效后的 180 日内，就潜在的影响国家安全的深度伪造技术、以及为外国用以实施传播虚假信息等恶意行为的深度伪造技术的潜在与实际影响，向国会情报委员会进行汇报；此外，该法令还指示以实施技术竞赛并提供奖励的方式，刺激深度伪造技术监测工具的进一步开发与商业化。[22]

---

[17] <Malicious Deep Fake Prohibition Act of 2018>, SEC. 2. § 1041. See S.3805 - 115th Congress （2017-2018）: Malicious Deep Fake Prohibition Act of 2018 | Congress.gov | Library of Congress.
[18] <Deepfake Report Act of 2019>, SEC. 3. See S.2065 - 116th Congress （2019-2020）: Deepfake Report Act of 2019 | Congress.gov | Library of Congress.
[19] <Deep Fakes Accountability Act >, SEC. 2. § 1041. See H.R.3230 - 116th Congress （2019-2020）: DEEP FAKES Accountability Act | Congress.gov | Library of Congress.
[20] < IOGAN Act>, SEC. 3, SEC. 4, See Text - S.1790 - 116th Congress （2019-2020）: National Defense Authorization Act for Fiscal Year 2020 | Congress.gov | Library of Congress.
[21] < Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020>, SEC. 707. See Text - H.R.3494 - 116th Congress （2019-2020）: Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 | Congress.gov | Library of Congress.
[22] <National Defense Authorization Act For Fiscal Year 2020>, SEC. 27. See Text - S.1790 - 116th Congress （2019-2020）: National Defense Authorization Act for Fiscal Year 2020 | Congress.gov | Library of Congress

在州一级层面，作为美国首批将未经同意的深度合成图像及视频分发行为作为刑事犯罪的州之一，弗吉尼亚州2019 通过修订《非同意色情法案》（Nonconsensual Pornography Law），将制作、分发裸体或性视频或图像，以恐吓、威胁他人的“复仇色情（Revenge Porn）”行为定义为 1 级轻罪，违反者面临最高 12 个月的监禁和 2500 美元的罚款。美国加州在《AB-602 法案（Assembly Bills 602）》中明确禁止未经个人同意对其面部图像进行编辑的行为，而《AB-730 法案（Assembly Bills 730）》则为防止选举中出现误导性，将制作、传播对政客产生负面影响的虚假恶意音视频的行为视为犯罪。[23]

（二）欧盟

总体而言，欧盟对深度合成技术的治理尚未系统建立，但《人工智能法案》（Artificial Intelligence Act）将深度伪造列为“高风险”人工智能技术，欧洲议会认为该归类的合理性来自于深度合成技术对个人基本权利及安全的威胁。因此，一方面，深度伪造技术的提供者需要面临包括但不限于遵守风险评估、记录、人工监督与确保高质量的数据集等规制要求，另一方面，在鼓励监测技术开发的基础上，深度合成技术的应用面仍应当受到限制。[24] 欧盟境内有关深度伪造的规定或意见主要为：

- **《人工智能法案》（Artificial Intelligence Act）**，该法案规定，对于生成的或操作的、与真实内容明显相似的图像、音频或视频内容，提供者应有义务披露该内容是通过自动方式生成的。[25]

- **《应对线上虚假信息：欧洲方案》（Tackling online disinformation: a European Approach）**，该意见总体上提出改进信息来源及提供信息传播透明性的目标，并强调了假新闻和虚假信息对各级政府构成共同威胁，总体上鼓励政府开展媒体素养运动，以防止假新闻和虚假信息的传播。[26]

- **《欧盟通用数据保护条例》（General Data Protection Regulation）**，从原则上禁止处理可以识别自然人的生物数据，除非是获得个人关于在特定处理目的下的明确同意等其他法定基础。[27] 并且，数据主体有权获得关于自动化决策所得出决定的解释性说明。[28]

四、《深度合成服务规定》主要规定内容

《深度合成服务规定》第二条规定，中华人民共和国境内应用深度合成技术提供互联网信息服务，以及为深度合成服务提供技术支持的活动，适用本规定。总体而言，《深度合成服务规定》的治理规则根植于国家此前提出的互联网信息服务与算法治理的总体思路，但又以深度合成技术及相关互联网信息服务应用场景的特点为基础，演化出更加个性化、具象化、细节化的治理规则。

就深度合成服务中相关主体的义务问题，《深度合成服务规定》作出了明确规定。一方面，鼓励相关行业组织加强行业自律，建立健全行业标准、行业准则和自律管理制度，督促指导深度合成服务提供者制定完善服务规范、加强信息内容安全管理、依法提供服务并接受社会监督；另一方面，《深度合成服务规定》还分别对深度合成服务提供者、

[23] Douglas E. Mirell and Joshua Geller: AB 602 and AB 730: Curbing “deepfakes” in pornography and elections, Daliy Journal, Jan 8, 2020, see https://www.dailyjournal.com/articles/355794-ab-602-and-ab-730-curbing-deepfakes-in-pornography-and-elections.
[24] European Parliament, Tackling deepfakes in European policy, Think Tank, 30 July 2021, see https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039.
[25] <Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS>, COM/2021/206 final, Annex III. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
[26] <Tackling online disinformation: a European Approach>, CDR 3908/201, see https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach.
[27] <General Data Protection Regulation> Article 9.
[28] <General Data Protection Regulation> Recital 71.

深度合成服务使用者及应用商店服务提供者等主体的义务予以释明。

（一）深度合成服务提供者义务

根据《深度合成服务规定》，深度合成服务提供者作为法定的信息安全责任主体，需要满足遵守法律法规，尊重社会公德和伦理，坚持正确政治方向、舆论导向、价值取向，促进深度合成服务向上向善，以及不得利用深度合成服务从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人名誉权、肖像权、隐私权、知识产权等合法权益等法律法规禁止的活动。我们理解，深度合成服务提供者需要遵守**信息内容治理义务、数据安全保障义务及算法技术合规义务**。

1. 信息内容治理义务

（1）建立深度合成信息内容标识管理制度

《网络音视频信息服务管理规定》提出，网络音视频信息服务提供者和网络音视频信息服务使用者利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播非真实音视频信息时，应当以显著方式予以标识的要求[29]；《互联网信息服务算法推荐管理规定》亦规定，算法推荐服务提供者发现未作显著标识的算法生成合成信息的，应当作出显著标识后，方可继续传输。[30]我们理解，前述规定针对生成合成类信息内容仅提出了概括性的标识义务规定。相对而言，此次《深度合成服务规定》则就深度合成服务提供者对深度合成信息的标识义务提出更为具体规定，要点包含：

- **标识不应当影响用户使用**：深度合成服务提供者对使用其服务所制作的深度合成信息内容，应当通过有效技术措施在信息内容中添加不影响用户使用的标识，依法保存日志信息，使发布、传播的深度合成信息内容可被自身识别、追溯。[31]

- **使用显著方式进行标识或提供进行标识的功能**：首先，对生成或者显著改变信息内容的深度合成信息内容，如智能对话、智能写作、合成人声、仿声、人脸生成、人脸替换、人脸操控、姿态操控等虚拟人物图像、视频、沉浸式拟真场景应当使用显著方式进行标识，向社会公众有效提示信息内容的合成情况；其次，对其他深度合成信息内容，应当提供进行显著标识的功能，并提示使用者可以自行标识。[32]

- **停止传输未标识的信息内容**：深度合成服务提供者发现深度合成信息内容未进行显著标识的，应当立即停止传输该信息，按照规定作出显著标识后，方可继续传输。[33]

与美国《深度伪造责任法案》类似，《深度合成服务规定》的规定也强调了深度合成内容的标识义务。但值得注意的是，《深度伪造责任法案》中该义务的主体为内容制作者，即深度合成技术的使用者，而《深度合成服务规定》则将该义务聚焦于深度合成服务提供者。考虑到深度合成服务提供者大多数情况可能属于平台型企业，《深度合成服务规定》承继了互联网平台监管的思路，通过对平台责任的设置，进一步降低深度合成服务使用的风险。但值得关注的是，与信息内容管理等平台责任不同的是，视频、音频、文字等内容的真实性判断与鉴别所要求的技术和审查能力可能更高。如何平衡在隐蔽性更强、技术要求更高的深度合成领域平衡平台责任和新型平台发展将值得我们进一步思考。

---

[29] 《网络音视频信息服务管理规定》第十条。
[30] 《互联网信息服务算法推荐管理规定》第九条。
[31] 《互联网信息服务算法推荐管理规定》第十三条。
[32] 《互联网信息服务算法推荐管理规定》第十四条。
[33] 《互联网信息服务算法推荐管理规定》第十五条。

（2）加强深度合成信息内容管理

就网络信息内容的治理方案而言，《网络信息内容生态治理规定》第八条针对所有网络信息内容服务平台提出了“履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化”的总体要求，并通过第九条、第三十四条为网络信息内容的治理工作设置了一套整体生态治理机制，即：信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度，并对违规者采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。[34]《深度合成服务规定》再次巩固了深调深度合成服务提供者的前述管理责任，具体举措为：

- **深度合成信息内容审核**，即采取技术或者人工方式对深度合成服务使用者的输入数据和合成结果进行审核。[35]
- **建立违法内容特征库**，即建立健全用于识别违法和不良深度合成信息内容的特征库，并完善入库标准、规则和程序。[36]
- **采取违规处置措施**，即对违法和不良信息依法采取相应处置措施，并对相关深度合成服务使用者依法依约采取警示、限制功能、暂停服务、关闭账号等处置措施。[37]

（3）建立辟谣、申诉与公众投诉机制

当发现深度合成信息服务使用者利用深度合成技术制作、复制、发布、传播虚假信息的，深度合成服务提供者应当及时采取相应的辟谣措施，并将相关信息报网信等部门备案；另外，还应当设置便捷有效的用户申诉和公众投诉、举报入口，公布处理流程和反馈时限，及时受理、处理并反馈处理结果。前述要求在《移动互联网应用程序信息服务管理规定》[38]《网络音视频信息服务管理规定》[39]《互联网信息服务算法推荐管理规定》[40]等规定中同样有迹可循。

2. 数据安全保障义务

（1）建立健全信息安全制度

《深度合成服务规定》总体上要求深度合成服务者设立用户注册、数据安全与个人信息保护、未成年人保护、从业人员教育培训等管理制度，并采取具有与新技术新应用发展相适应的安全可控的技术保障措施。[41]前述规定可被视为是我国《网络安全法》《数据安全法》《个人信息保护法》《网络信息内容生态治理规定》等网络安全及数据保护规范的呼应。

（2）提示深度合成服务使用者获得个人信息主体的单独同意

作为《深度合成服务规定》的亮点之一，深度合成服务提供者被要求在提供人脸、人声等生物识别信息的显著编

[34] 《网络信息内容生态治理规定》第八条、第九条、第三十四条。
[35] 《互联网信息服务算法推荐管理规定》第十条。
[36] 《互联网信息服务算法推荐管理规定》第十条。
[37] 《互联网信息服务算法推荐管理规定》第十条。
[38] 《移动互联网应用程序信息服务管理规定》第十条。
[39] 《网络音视频信息服务管理规定》第十三条、第十五条。
[40] 《互联网信息服务算法推荐管理规定》第二十二条。
[41] 《互联网信息服务深度合成管理规定》第七条。

辑功能时，应当提示深度合成服务使用者依法告知并取得被编辑的个人信息主体的单独同意。[42]《个人信息保护法》第二十九条规定，处理敏感个人信息应当取得个人的单独同意。[43] 而生物识别信息作为敏感个人信息，对该等信息的处理行为应当获取用户的单独同意，而深度合成服务提供者的提示义务则旨在促使使用者获取被编辑主体的单独同意。我们理解，该规定不仅是《个人信息保护法》就个人生物识别信息的特殊要求在深度合成服务下所衍生出的应然要求，在实践层面，此举也将有效控制此前因攫取与滥用人脸数据而产生的非法获取个人信息、侵害个人隐私、敲诈勒索、散布虚假消息等社会问题。

（3）加强训练数据管理

《深度合成服务规定》**首次对深度合成服务提供者提出加强训练数据管理的义务**，以确保数据处理合法、正当，采取必要措施保障数据安全。尤其是，该规定强调当训练数据包含涉及个人信息数据的，还应当遵守个人信息保护有关规定，不得非法处理个人信息。[44]

此前，工业和信息化部办公厅发布《新一代人工智能产业创新重点任务揭榜工作方案》，一方面指出到 2020 年基础语音、视频图像、文本对话等公共训练数据量大幅提升的趋势，另一方面鼓励在工业、医疗、金融、交通等领域汇集一定规模的行业应用数据，用于支持创业创新。[45] 在此基础上，对个人信息在内的大量训练数据的使用将触发一系列合规管理义务。因此我们理解，《深度合成服务规定》此处对训练数据管理的规定，不仅是对国家互联网信息内容治理及个人信息保护工作所进行响应，也是对前述合规管理义务的回应，从源头上、最大化避免因训练数据的大面积使用对个人信息所造成的风险，并减少后期治理的成本。

（4）履行制定与公开管理规则和平台公约

《网络信息内容生态治理规定》总体上对所有网络信息内容服务平台提出了“制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责”的要求。[46] 此次《深度合成服务规定》第八条，不仅重申“应当制定并公开管理规则和平台公约，完善服务协议”，还特别提出“以显著方式提示深度合成服务使用者信息安全义务”的要求。[47] 另外，《网络数据安全管理条例》第四十三条对互联网平台运营者提出了建立与数据相关的平台规则、隐私政策和算法策略披露制度，从而保障平台规则、隐私政策、算法公平公正的合规要求。[48] 我们理解，考虑到当前监管部门对平台算法治理的重视，不排除前述“公开管理规则与平台公约”包含算法策略的可能性。

值得注意的是，我们理解《深度合成服务规定》第二条规定的“深度合成服务提供者”同时包含“提供深度合成服务的主体”以及“为深度合成服务提供技术支持的组织”两种主体。因此，对于仅提供深度合成技术支持的技术提供商而言，考虑到其并不会直接面向用户，其是否仍属于“网络信息内容服务平台”，以及是否同样需要根据此第八条的规定以落实公开管理规则和平台公约的管理职责，或需要相关法律法规作进一步的说明。

（5）认证用户真实身份

实名认证义务是《网络安全法》所规定的基本义务。网络运营者为用户提供信息发布、即时通讯等服务，在与用

[42]《互联网信息服务深度合成管理规定》第二十二条第二款。
[43]《个人信息保护法》第二十九条。
[44]《互联网信息服务深度合成管理规定》第十二条。
[45]《新一代人工智能产业创新重点任务揭榜工作方案》第二条第四款。
[46]《网络信息内容生态治理规定》第十五条。
[47]《互联网信息服务深度合成管理规定》第八条。
[48]《网络数据安全管理条例》第四十三条。

户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。考虑到深度合成技术与信息发布关系密切，《深度合成服务规定》强调深度合成服务提供者应当依法对深度合成服务使用者进行真实身份信息认证。[49] 类似地，《网络音视频信息服务管理规定》要求网络音视频信息服务提供者基于组织机构代码、身份证件号码、移动电话号码等方式对用户真实身份信息进行认证[50]，而《互联网宗教信息服务管理办法》就互联网宗教信息传播平台与平台注册用户签订协议、核验注册用户真实身份信息等义务作出规定。[51]

3. 深度合成服务提供者的算法技术合规义务

（1）建立健全算法机制机理审核

2021年9月17日，《关于加强互联网信息服务算法综合治理的指导意见》在“积极开展算法安全评估”部分提出了“组织建立专业技术评估队伍，深入分析算法机制机理”的要求。[52]《互联网信息服务算法推荐管理规定》也规定了算法推荐服务提供者应当落实算法安全主体责任，建立健全算法机制机理审核、科技伦理审查的义务。[53] 此次《深度合成服务规定》就相同义务对深度合成服务提供者进行了重申，这也是“以人为本”的科技施政理念的体现。

（2）安全评估义务

《网络音视频信息服务管理规定》要求网络音视频信息服务提供者基于深度学习、虚拟现实等新技术新应用上线具有媒体属性或者社会动员功能的音视频信息服务，或者调整增设相关功能时均需开展安全评估。[54]《网络数据安全管理条例》也概括性地要求利用人工智能、虚拟现实、深度合成等新技术开展数据处理活动的互联网平台运营者，应按照国家有关规定进行安全评估。[55] 相比前述规定，《深度合成服务规定》进一步明确需要开展安全评估以预防信息安全风险的触发情形，即：

- 提供具有对**人脸、人声等生物识别信息**或者可能涉及**国家安全、社会公共利益**的模型、模板等工具的[56]；
- 开发上线**具有舆论属性或者社会动员能力**的新产品、新应用、新功能的。[57]

我们理解，由于深度合成技术的概念十分广泛，若对所有涉及应用深度合成技术的算法与服务开展安全评估，可能对相关服务提供者施加较重的合规义务，《深度合成服务规定》之要求在一定程度上缓解了深度合成服务提供者的合规压力。

（3）履行算法备案手续

此次，《深度合成服务规定》规定，深度合成服务提供者应当按照《互联网信息服务算法推荐管理规定》的有关规定，在提供服务之日起十个工作日内履行备案手续。[58] 而根据《互联网信息服务算法推荐管理规定》，具有舆论属性或者社会动员能力的推荐算法服务提供者应当履行备案手续。具体而言，算法服务提供者需要通过算法备案系统填报服务提

[49] 《网络安全法》第二十四条。
[50] 《网络音视频信息服务管理规定》第八条。
[51] 《互联网宗教信息服务管理办法》第二十条。
[52] 《关于加强互联网信息服务算法综合治理的指导意见》第三条第八款。
[53] 《互联网信息服务算法推荐管理规定》第七条。
[54] 《网络音视频信息服务管理规定》第十条。
[55] 《网络数据安全管理条例》第五十四条。
[56] 《互联网信息服务深度合成管理规定》第十一条。
[57] 《互联网信息服务深度合成管理规定》第二十条。
[58] 《互联网信息服务深度合成管理规定》第十九条。

供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息。[59] 然而，我们理解，该规定是否表明深度合成技术算法将被直接归类于具有舆论属性或者社会动员能力的算法，可能还具有一定争议。

自 2021 年 9 月，国家发布《关于加强互联网信息服务算法综合治理的指导意见》，对开展算法备案工作提出了“建立算法备案制度，梳理算法备案基本情况，健全算法分级分类体系，明确算法备案范围，有序开展备案工作”[60] 的指导方向后，“算法备案”开始成为热议话题。我们理解，备案制度为监管机构提供了从源头开展算法治理和监督工作的切入点，是国家所提出的“推动治理原则贯穿人工智能产品和服务全生命周期，对未来更高级人工智能的潜在风险持续开展研究和预判，确保人工智能始终朝着有利于社会的方向发展”的“敏捷治理”[61] 方式的重要表现形式。

（二）其他主体

《深度合成服务规定》还就深度合成服务使用者与应用商店服务者所应当承担的义务进行了说明。

对于深度合成服务使用者而言，其仍应当履行遵守法律法规，尊重社会公德和伦理，坚持正确的政治方向、舆论导向、价值取向，促进深度合成服务向上向善的总体义务。同时，使用者还需配合深度合成服务提供者履行真**实身份信息认证义务**，针对于违规者，深度合成服务提供者将拒绝为其提供信息发布服务。[62] 另外，深度合成服务使用者有义务在使用人脸、人声等生物识别信息的显著编辑功能前，**取得被编辑的个人信息主体的单独同意**。[63] 我们理解，虽然该义务属于服务使用者，但服务使用者往往是以用户的身份使用具有深度合成功能的应用软件。因此，在该场景下如何帮助服务使用者合规地获取他人的单独同意便成为服务提供者在应用设计和开发过程中需要考虑的问题。

针对互联网应用商店服务提供者，其主要义务为**履行安全管理责任**，即依法依约核验深度合成应用程序的安全评估、备案等情况，对违反国家有关规定的，应当及时采取不予上架、暂停上架或者下架等处置措施。[64] 我们理解，上述规定与《移动互联网应用程序信息服务管理规定》等文件中规定的“督促应用程序提供者履行信息保护”“发布合法信息及发布合法应用程序”等信息安全的管理责任相呼应，在深度合成技术服务领域强调互联网应用商店服务提供者的义务。

五、重要意义

《深度合成服务规定》是我国互联网信息服务治理、人工智能与算法治理的宏观版图中的重要组成部分。面对新技术的挑战，《深度合成服务规定》一方面表明了政府与监管者所采取的审慎包容的态度，另一方面，也同时展现了在以人为本、有序治理的大前提下，国家对新型技术的支持。总体而言，我们认为《深度合成服务规定》在以下三个方面有着重要意义：

（一）由点及面的立法布局

当前在数据保护领域，我国已出台一系列法律法规和国家标准，以全方位规制数据的全生命周期。然而，相较于数据立法，我国在算法层面出台的文件数量有限。但从目前已出台的《数据安全法》《个人信息保护法》《深度合成服务规定》以及《互联网信息服务算法推荐管理规定》等文件，可以管窥监管机构由点及面的立法布局。具体而言，从整体上看，《数据安全法》第 28 条提出，开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，

[59] 《互联网信息服务算法推荐管理规定》第二十四条。
[60] 《关于加强互联网信息服务算法综合治理的指导意见》第三条第九款。
[61] 《新一代人工智能治理原则——发展负责任的人工智能》，载新华社，2019 年 6 月 17 日，http://www.gov.cn/xinwen/2019-06/17/content_5401006.htm。
[62] 《互联网信息服务深度合成管理规定》第九条。
[63] 《互联网信息服务深度合成管理规定》第十二条。
[64] 《互联网信息服务深度合成管理规定》第十六条。

增进人民福祉，符合社会公德和伦理；同时，《个人信息保护法》《电子商务法》等也就自动化决策等算法问题进行规定，上述法律法规构成算法治理的核心要求。而目前针对推荐算法、深度合成技术等新兴技术的立法则旨在从具体的应用场景出发，规制特定的算法类型。不同监管文件之间环环相扣，形成紧密的逻辑链条。待未来相关法规逐渐丰富，多维谱系的法律法规能够使监管机构使用多种监管工具全方位、多层次地对算法问题进行规制。

（二）以人为本的监管思路

为了防止技术的异化风险，算法服务提供者和技术支持者应当始终将技术创新和以人为本作为根本目的。因此，倡导“科技向善”成为推动数字社会福祉最大化的必然要求。2019 年，国家新一代人工智能治理专业委员会《新一代人工智能治理原则——发展负责任的人工智能》提出了和谐友好、公平公正、包容共享、尊重隐私等原则。[65] 许多科技企业也相继发布有关人工智能治理方面的白皮书，明确人工智能在安全、 隐私、 公平等方面的伦理原则，还有企业成立了人工智能道德委员会，以期解决人工智能和算法带来的道德风险。而《深度合成服务规定》对“尊重社会公德和伦理，坚持正确政治方向、舆论导向、价值取向，促进深度合成服务向上向善”的强调，正是以人为本的“科技向善”的体现。

（三）敏捷治理的监管策略

从监管策略上看，《深度合成服务规定》在一定程度上体现出“敏捷治理”的基本思路。首先，《深度合成服务规定》明确了算法备案、审核、评估等制度，算法备案制度和安全评估制度是实现敏捷治理目标可优先考虑的制度设计，一方面可以让监管机构及时了解算法的具体内容，另一方面能够提高深度合成服务提供者的责任意识和安全意识。此外，《深度合成服务规定》还规定了深度合成技术的监管机构与相关法则，即：国家网信部门与地方网信部门负责统筹协调全国及各行政区域内的深度合成服务治理和相关监督管理工作，并规定违反相关规定者可能面临警告，责令限期改正，一万元以上十万元以下罚款等处罚方式，或依法承担民事责任、治安管理处罚及刑事责任。我们理解，上述中央与地方统筹协调、协同治理，多种惩罚手段并用的方式同样是敏捷治理的体现。

相较于传统由政府作为治理主体的单一治理方式，敏捷治理所提倡的多主体参与的多元治理能够进一步完善算法规制策略。对于将深度合成技术作为驱动商业利益的重要依托的服务提供者而言，在敏捷治理的背景下，除应当注意“慎始而后行”，还可以进一步探讨如何在合规前提下尽可能激发深度合成技术的商业潜力。换言之，深度合成服务者除了被动履行《深度合成服务规定》所规定的，包括但不限于信息安全主体责任、深度合成信息内容标识、审核深度合成信息内容、建立健全算法机制机理审核机制、加强训练数据管理及履行自评估等义务外，还可**相应积极推动检测识别技术的研发、检测标识和标注工具的开发等配套技术**，同监管机构一同促进深度合成技术的妥善运用，在防范风险的同时为对抗性技术和鉴别技术的发展提供计划。[66]

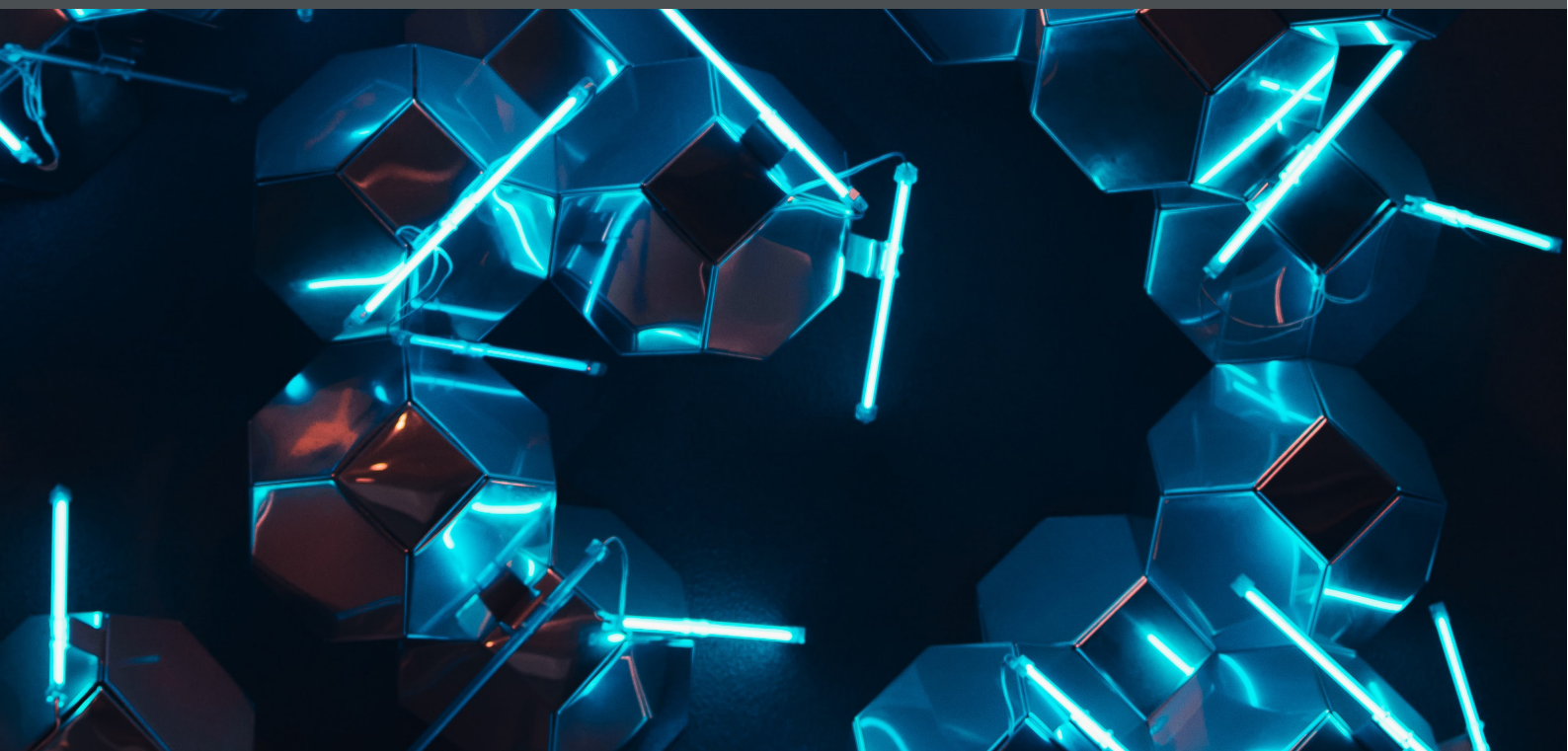
结语

对于深度合成领域的新监管要求是迎接数字社会发展挑战的一次重要尝试，可以预见的是，对于数字社会中“虚实”和“真伪”的事实辨别和价值判断将是动态变化的过程。正所谓“假作真时真亦假，无为有处有还无”，我们对数字社会治理规则的发展应当抱有积极开放的心态和审慎的精神，在追求社会发展和人性进步的历程中，恪守本心。

感谢实习生邓立山、綦浩彤对本文作出的贡献。

[65]《新一代人工智能治理原则——发展负责任的人工智能》，载新华社，2019 年 6 月 17 日，http://www.gov.cn/xinwen/2019-06/17/content_5401006.htm。
[66] 同注 1。

个人信息保护



千钧将一羽，轻重在平衡——试论个人信息权利保护纠纷中的自由裁量

吴涵　刘迎　孙乐怡　姚敏侣

一、企业如何协助个人信息主体行使权利

《个人信息保护法》是保护个人信息权益的基本法，对个人信息权利进行了定义，全面构建了个人在信息处理活动中享有的法定权利，包括知情权、决定权、限制权、拒绝权、查阅权、复制权、可携带权、更正权、删除权等。但是目前仅有《个人信息保护法》的概念性规定仍不足以明晰这些权利的内涵、边界、权利行使方式等问题。

权利与义务相对应而存在，企业作为个人信息收集、处理的主体往往成为个人行使这些个人信息权利时的相关义务承担者。个人向企业主张行使这些大数据时代的新兴权利时，企业又应当如何履行相应义务也有较大的争议。

以个人信息查阅权、复制权为例，实践中应如何理解“查阅”、“复制”的含义？“查阅”、“复制”是否必须采取某种指定形式？企业如何做才可以既能一一满足成千上万的用户查阅、复制个人信息的要求，同时又不至于使企业陷入无止境的义务履行负担中？如果主管部门、行业协会等已经在个人信息查阅、复制方面进行了指引和要求，且企业也符合现有的主管部门、行业协会等关于个人信息查阅、复制的要求，用户向企业提出的个人信息查阅、复制请求如果超出了主管部门、行业协会等的规定，企业是否还有义务响应？应如何响应？以互联网移动应用程序（APP）为例，通常 APP 会通过交互式页面设计在“个人中心”里展示用户自行填写的一些个人信息，这也是 APP 行业规范所要求的满足个人信息查阅的方式。如果某位用户向 APP 运营者主张查看 APP 后台存储的这些个人信息对应的全部原始数据，并要求为其提供专门的文档以便复制，这种要求是否属于个人信息查阅权、复制权的合理行使？ APP 运营者是否有义务去满足？如果是，APP 运营者又应当如何满足这种权利主张？

上述疑问是我们在相关案件办理过程中以及企业在个人信息合规工作中切实遇到的问题。对这些问题的思考和回应有利于个人信息纠纷定纷止争，从而更好地实现个人信息保护的目标。

二、个人信息保护纠纷中实现利益平衡的必要性

围绕个人信息权利产生的个人信息保护纠纷中，核心争议往往为个人信息权利是否受到侵害或者个人信息处理者是否保障了个人信息主体的个人信息权利。这一问题的判断离不开对个人信息权利与义务边界的划分。但是由于目前《个人信息保护法》尚未出台具体的实施细则，如果在个人信息纠纷处理中仅偏重于个人主体的诉求是否得到满足，而忽略个人信息主体诉求的出发点、动机以及企业实现诉求的成本，没有保护各方利益平衡，将价值天平一味向某一方倾斜，这样的处理结果是否反而导致不公和失衡，甚至限制数字经济的发展？

（一）利益平衡原则、比例原则与成本原则

利益平衡既是一项立法原则，也是一项司法原则，在法律层面上，利益平衡是指“通过法律的权威来协调各方面冲突因素，使相关各方的利益在共存和相容的基础上达

到合理的优化状态”[1]。社会生活中不同主体存在不同的利益诉求，而社会资源有限，不同利益主体之间很容易发生冲突。当不同利益主体之间发生冲突又不能两全时，法律只能进行不同利益之间的权衡，评估不同法律制度对各方利益的影响，选择更符合利益最大化的相应法律规则。[2]

利益平衡原则在法律制度中的典型应用就是知识产权法。一方面，知识产权法鼓励知识创新和促进知识扩散，保障知识产权人的专有权，另一方面社会公众在知识产权法中也存在合法的权益需要保障。知识产权法需要协调知识独占和知识共享的冲突，实现个人利益与公共利益的平衡或者至少使两者趋于平衡。著作权法中的合理使用制度、避风港原则，专利有限保护期制度等就是利益平衡原则的典型体现。[3]

与利益平衡原则相关联的另一原则是比例原则。比例原则是个人信息处理中的重要原则，是指信息处理活动中在必要性、适当性以及目的与手段之间合乎比例等要件的前提下，基于实现信息自由目的可以对权利进行一定的排除或限制。比例原则发源于 18 世纪末期德国警察法，它是行政法的核心原则，原旨在对限制私权利的立法权或行政权力进行限制，基本要义是强调对私权利进行限制应具备合理性。[4] 如今比例原则已成为域外个人信息保护立法和判例法中的重要原则。欧盟《通用数据保护条例》（GDPR）的序言第四项规定：“The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.”该规定明确了个人数据保护权不是绝对权，必须根据比例原则，考虑其在社会中的功用与其他基本权利保持平衡，是欧盟国家处理的基本要求。我国《个人信息保护法》第五条中规定了处理个人信息应当遵循合法、正当、必要和诚信原则，第六条规定处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。这些规定体现了比例原则和利益平衡原则在我国《个人信息保护法》中的运用。

此外，在平衡个人信息主体行权时多方利益的过程中，不容忽视的是行权成本的考虑。行权成本，既包括个人信息主体向个人信息处理者提出诉求时的门槛和条件，也包括个人信息处理者响应和满足个人信息主体权利要求时的花费和成本。在个人信息的人格尊严价值已经得以保障和体现时，成本原则应当成为判断个人信息主体行权要求合理性的重要标准之一。成本原则在我国的推荐性国家标准 GB/T35273-2020《信息安全技术 个人信息安全规范》中实则已有所体现。在该规范第 8.7 条中明确，对一定时期内多次重复的个人信息权利行使请求，企业可视情收取一定成本费用；直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，允许企业向个人信息主体提供替代方法。

（二）信息利用过程中涉及多元主体利益需要平衡

从《个人信息保护法》的名称中可以看出，该法的主旨在于“保护”，保护个人就个人信息享有的合法权益。但是从信息的属性来看，信息是无形的，被称为“信息论之父”的克劳德·香农（Claude E. Shannon）曾表示：“信息是用来消除随机不确定性的东西。”当一个人掌握了信息，就比其他不掌握该信息的人具有确定性，所以信息的价值在于拥有信息的主体可以传播、共享信息，以消除不确定性。[5] 信息在社会交往活动中进行传播、利用的过程中才能发挥作用。简单地讲，信息不是为了保护而存于世间的，相反恰恰是为了利用。所以除了“保护个人信息权益”这一立法宗旨外，“促进个人信息合理利用”也应是立法目的所在。

个人信息虽然是个人的信息，但是在个人信息的利用过程中，会涉及个人、政府、企业等不同的利益主体。例如在疫情防控、人口统计等社会治理领域，政府有必要掌握一定的公民个人信息并有权在特殊情况下无需个人同意利用个人信息，成为个人信息的利益主体。《个人信息保护法》第 13 条规定为履行法定职责或者法定义务所必须、为应对突发公共卫生事件或者紧急情况下为保护自然人的生命健康和财产安全所必需、为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理个人信息等情形，可

[1] 冯晓青：《知识产权法的利益平衡原则：法理学考察》，载《南都学坛》2008 年 3 月，第 28 卷第 2 期。
[2] 范小华、周琳：《基于利益平衡视角的的个人信息法律保护探析》，载《行政管理改革》2020 年第 3 期。
[3] 冯晓青：《知识产权法的利益平衡原则：法理学考察》，载《南都学坛》2008 年 3 月，第 28 卷第 2 期。
[4] 齐爱民、李仪：《论利益平衡视野下的个人信息权制度——人格利益与信息自由之间》，《法学评论》2011 年第 3 期。
[5] 申卫星：《论个人信息保护与利用的平衡》，载《中国法律评论》2021 年第 5 期。

以无需取得个人同意处理个人信息。该条规定实际上就是在个人利益与公共利益之间进行了一定的平衡。

除上述围绕个人信息产生的个人利益和公共利益外，企业通常以个人信息收集、处理者的身份牵涉其中，成为个人信息的重大利益相关主体。企业可以对其投入了劳动加工处理后的信息成果享有权益，已经逐渐成为立法和司法实践的共识，这种信息成果实际上也是基于个人信息聚合加工而成。而对于此类经过企业加工、分析和增值的个人信息产品或成果，在已经采取适当方式确保了个人信息主体对其享有的基本人格权益外，个人在多大程度或范围上享有对企业的个人信息产品或成果的财产权利要求，目前来看可能也缺少非常明确的答案。而企业与个人的信息权属划分规则，实际上也体现了司法在作为个人信息处理者的企业利益与个人信息主体利益之间的一种平衡。

而关于企业和企业之间就个人信息之上的相关权益划分，也需要一定的利益平衡，这一点虽然在国内外司法实践中不完全一致，但均间接认可了企业对于个人信息处理的相关合法权益。基于信息流通价值和保护价值的不同侧重，国外如美国法院对 HiQ vs. LinkedIn 的最新判决表明对于具有公开流通属性的个人信息，各家平台之间可能拥有相同的使用和竞争性权益，而我国此前在“新浪诉脉脉不正当竞争案”中确立的“三重授权原则”，除个人对个人信息的控制或决定权利以外，还强调了在线平台对于其用户个人信息的竞争性权益和价值。

从上述企业与个人、企业与企业之间的利益冲突与平衡实践来看，我们不难发现，应该承认个人信息之上除了人格权益之外，企业对于个人信息财产价值的分配合法性与正当性。正如欧盟《通用数据保护条例》（GDPR）第六条中，将“合法利益”（legitimate interests）作为个人信息处理的合法性依据所折射出的立法考量，企业在个人信息处理活动中合法、正当的利益应得到尊重和承认。

尽管我国现行的《个人信息保护法》中并未将 GDPR 中的“合理利益”作为一项单独的合法处理个人信息的情形加以规定，但企业对于用户个人信息客观上享有的，基于自由诚信经营、市场公平竞争以及其他正当的财产性权利或合法权益，进而在合理范围内处理个人信息的行为，应当被视作个人信息处理合法合规性评估的重要衡量因素。这一点，在中国科学技术法学会牵头制定和发布的团体标准 T/CLAST 001-2021《个人信息处理法律合规性评估指引》中已经得到认可和体现。在该指引中，“合法利益公平处理”要求，当能够有说服力地论证个人信息处理具体场景下，要求个人信息主体事先同意将使得合法利益无法实现或者要求付出与收益不成比例的成本时，个人信息处理可以通过法律合规性评估。

当然，相比于取得个人信息主体的知情同意，作为个人信息合法处理的例外情形，企业基于合法利益进行个人信息处理前，参照上文提及的团体标准，往往需要企业运用比例原则，基于具体的个人信息处理场景进行多因素的利益平衡或者合法利益的比较，进行所谓的“平衡性测试”，以达到“充分论证”个人信息处理的合法利益显著高于个人信息主体的利益保护价值之目的。“通过个案衡量方式为数据保护留下了灵活的操作空间，是个人信息保护与促进信息流动之间的重要平衡器。”[6]

（三）个人信息权利义务的边界划分需注重利益平衡

企业作为个人信息处理者可能会处理海量的用户个人信息，例如我国某些购物类 APP 注册用户数多达几亿人，每一个用户都有权向 APP 运营者行使其个人信息的相关权利。仍以个人信息查阅权、复制权为例：

如果个人信息查阅权、复制权行使方式不合理不明确，每位用户都有权要求企业按照其指定的方式去满足用户查阅、复制个人信息的要求，那么企业将需要逐一专门采取措施去满足不同用户们查看、复制信息的需求。

如果个人信息查阅权、复制权没有合理的范围，用户可以随时要求企业披露其存储的与该用户有关的全部信息和原始数据，企业将需要大量时间并占用宝贵的服务器资源在海量数据库中不断为用户检索相关数据。互联网企业在存储用户数据时并非以用户账号为单位制作数据表单进行存储，而是按照不同的数据类型制作数据表单存储数据，例如所有的用户注册信息会存储在一起，所有的用户日志信息会存储在一起，这种数据存储逻辑下用户信息并非天然的在企业后台被按照用户账户整理

[6] Paolo Balboni, et al., *Legitimate Interests Of Data Controller New Data Protection Paradigm: Legitimate Grounded On Appropriate Protection,* International Data Privacy Law, vol.3, no.4 (2013). 转引自：谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019 年第 1 期。

存放，企业需要经过在数据库中检索的动作才能将相应信息提取出来。如果被检索的数据库较小，检索相应信息的时间成本很低，但是如果需要检索的数据库非常庞大，则检索的时间成本会线性增长，同时运行相关检索任务需要占用的服务器资源也会随之增长，比如为用户提供某账号注册以来的全部日志信息，因互联网行业每日产生的日志信息数量可以亿为单位，检索全部日志信息任务就需要花费一定的成本。

上述情境下，仅满足单个用户的需求产生的成本对企业来说尚足以承担，但是企业作为个人信息处理者需要面对无数用户，如果每一个用户都可以向企业提出上述请求，满足这些请求的成本累计起来将难以估量。此时，在基本满足个人信息主体的人格尊严保障要求下，成本原则应该派上用场。在个人信息保护义务承担方面，企业处于一对多的地位，如果个人信息权利的行使方式、边界等不明确或不合理，使企业承担严苛的、不合理的成本和风险，有可能反向打击企业履行保护个人信息职责的积极性，不利于个人信息保护的发展。因此有必要通过立法或司法裁判规则明确合理的个人信息权利行使方式，实现个人信息处理者与个人信息主体之间的利益平衡。

三、如何在个人信息纠纷中实现利益平衡

厘清《个人信息保护法》规定的新兴个人信息权利与义务的边界、权利行使方式以及个人信息处理者的义务承担方式具有现实意义。尤其是在日益频发的个人信息纠纷中，不仅需要明确权利义务边界定纷止争，更需要进行合理的划分和界定实现个体权利与他人利益、社会利益的平衡，才能使个人信息保护制度真正发挥作用。当下个人信息权利义务边界仍有待立法和实践进一步探索，我们结合所处理过的个人信息纠纷案件经验及实践中此类纠纷的常见争议焦点，对如何在个人信息纠纷中合理平衡企业与个人利益，尝试提出一些建议，抛砖引玉：

（一）处理个人信息纠纷时应当尊重和关注相关行业发展阶段和技术发展现状

在以往的数据不正当竞争纠纷中，法院通常会结合相关行业的发展阶段对当事人间的权利义务关系进行分析，例如（2018）浙 01 民终 7312 号案件中，法院认为“由于互联网经济作为新型市场形态正处在形成与新兴过程中，调整网络运营者与网络用户相互间权利义务关系的专门性法律规范尚处在探索创立阶段，目前对于网络运营者与网络用户间的利益分配与权利冲突，应当秉持‘合法、合理、公平’的原则，综合考量法律规定、双方间法律关系属性以及有利于社会公共秩序与社会公众利益维护等因素予以评判。”

技术发展现状也会影响义务的分配程度，例如（2020）浙 01 民终 4847 号案件中，法院认为“由于互联网征信行业仍处于发展的起步阶段，相关行业规范尚未成熟，应当以鼓励数据共享流通、兼顾各方利益为原则，并正视海量数据处理的技术困境，合理确定注意义务。一方面，从事企业征信的互联网征信企业运用大数据技术优势，将公共领域碎片化的局部数据整合起来，较为完整的反映企业经营信用状况，实现了面向整个市场的信息共享，解决了商业信息滞后、信息不对称的市场困境，在降低信息收集成本，增加交易行为的透明度，促进社会诚信体系建设方面具有积极作用。由于受到数据共享范围、获取成本的限制及数据有效抓取技术的局限，在司法裁判上，不宜为互联网征信企业赋予过高的注意义务，对于普通的信息偏差，应当允许其通过事后救济的方式进行修正。”

因此，个人与企业之间发生个人信息纠纷时，双方权利义务的合理划分不能仅囿于法律文本的分析，亦有必要结合当下相关行业的发展阶段以及有关的技术现状。如果脱离了行业和技术背景，有可能会对相关企业苛以其实际上难以做到的义务，起到揠苗助长的负面效果。

（二）个人信息权利义务的行使方式不能脱离大数据和互联网时代需求和特征

大数据时代，企业作为个人信息处理者要面对大量的信息主体，需要处理的个人信息也是海量的，这一特征使得个人信息权利义务关系与传统的民商事权利义务关系有所不同。在衡量个人与企业围绕个人信息纠纷可能产生的受益或损失时，不能仅仅局限于单个的用户与企业之间的利益平衡，也应当适当关注这一权利义务推及于全部用户后企业可能面临的负担与风险。

而且在互联网时代，个人信息权利义务的履行也应当与时俱进，不能局限于传统的履行方式，应当允许并鼓励企业运用互联网技术通过便捷的交互式页面方式或其他灵活方式为用户提供自助行使个人信息权利的途径，这也是当前行业发展趋势。在企业已经通过 APP 交互式页面设计为用户提供了个人信息的查阅、复制、删除、更正等功能时，用户再单独要求企业以指定方式满足其个人信息查阅、复制、删除、更正等需求，比如为其提供一份专门的纸质文件披露个人信息，用户的这种需求是否合理、企业是否有义务满足是值得商榷的，至少不应该苛责企业对用户关于个人信息权利行使的任何需求都做到一味满足。

（三）将企业保障个人信息权利的义务与主管部门、行业协会等制定的要求合理衔接

在《个人信息保护法》颁布之前，就有不少主管部门、行业协会就该行业企业如何做好个人信息保护制定了不少规范、指引，其中不乏关于个人信息权利、义务履行方式的细化规定。

例如国家市场监督管理总局、国家标准化管理委员会于 2020 年 3 月 6 日发布了国家标准《信息安全技术 个人信息安全规范》，对个人信息处理者如何响应个人信息主体的请求、如何保障个人信息主体的权利进行了详细规定。比如该规范第 8.1 条个人信息查阅，规定了个人信息控制者应向个人信息主体提供查阅的信息范围，也明确如果个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。根据该规定，我们理解，也并非用户所有查阅个人信息的请求企业都有义务予以满足。

工业和信息化部作为行业主管部门也多次发布关于个人信息保护的通知，对有关企业如何保障个人信息权利、履行个人信息保护义务进行了要求。例如工信部在《关于开展信息通信服务感知提升行动的通知》（工信部信管函〔2021〕2 号）中要求企业建立已收集个人信息清单和与第三方共享个人信息清单（“双清单”），在 APP 二级菜单中展示，方便用户查询。在企业已经按照工信部要求制作双清单以供用户查阅有关信息后，如果某位用户要求企业为其披露有关该用户个人信息向其他第三方共享的具体信息内容清单，企业是否应当满足用户的要求？

我们认为，在行业主管部门、行业协会等已经对企业如何保障具体的个人信息权利有明确要求时，企业按照相关要求采取措施就可以视为已经履行了《个人信息保护法》下保障个人信息权利的义务。在当前《个人信息保护法》中的个人信息权利规定仍较为粗疏的情况下，尽管行业主管部门、协会等有关规范、通知的法律效力层级较低，也有必要参照、尊重这些专业性的规范文件，将企业保障个人信息权利的义务与主管部门、行业协会等制定的要求衔接，来合理确定个人信息权利应当如何保障和落实。

四、企业如何更好地应对个人信息权利主张？

实践中，用户通常会以与客服电话、留言沟通、向企业专门邮箱发送电子邮件等方式向企业提出行使个人信息权利的主张，比如要求企业披露某些个人信息、为其提供个人信息副本等，如果企业对这些请求置之不理或处理不当，在《个人信息保护法》实施后将有面临被用户提起个人信息侵权纠纷的诉讼风险。面对这类用户请求，企业如何应对才能降低侵权风险到达合规要求？结合我们的相关案件经验和为企业提供个人信息合规服务的经验，对此有以下几点建议：

（1）按照行业主管部门规定和行业协会的各项要求进行个人信息合规建设，并按照有关要求优化网站、APP 等平台的设计和功能，以便捷的、行业通用的方式保障用户个人信息相关权利，尽可能避免因违规遭受主管部门的批评、通报或处罚等。

（2）明确并完善个人信息响应制度，在接到个人用户关于行使个人信息权利的主张时，应及时予以答复、说明相关理由，可以降低因未答复或答复不及时而被认定为侵权的风险。

（3）在答复用户关于行使个人信息权利的主张时，应

注意核验用户的真实身份，如果用户未主动提供其真实身份信息，企业可主动要求其提供身份信息以供核验或者告知用户核验身份的途径、方式。

（4）如果用户关于个人信息权利的请求，已经可以在网站、APP 等平台上由用户自助实现请求内容，企业可在答复中明确告知用户相关渠道和方式，或将上述内容在用户协议中予以公示。如果企业认为用户的请求不合理或难以满足，企业应向用户进行解释说明。

为了在个人信息保护与流通价值之间做好平衡，其核心在于法理上确定个人信息附着的各项权益，并就各项权益对应的利益进行合理分配。但值得注意的是类似的分配制度依然有可能是动态变化的过程，比如个人信息主体对不同类型的个人信息享有的人格权益程度有所不同（比如个人财产信息和身高信息），因此对应权利边界未来也有所差异。再如企业对于不同类型个人信息投入程度的差异（用户基本信息和用户浏览记录）可能会导致其财产权益的变化，甚至影响其履行个人信息义务的边界。

在当前法理上仍未有定论的情形下，如何既能“保护个人信息权益”，又能“促进个人信息合理利用”，是需要裁判机关在相关个人信息权利要求案件中积极调动司法能动性，在具体的个人信息处理场景下，充分发挥利益平衡原则的艺术，尊重和保护企业基于合法利益进行的个人信息处理活动，支持企业自主作出拒绝滥用权利、超出合理范围行使个人信息权利要求的决定。唯有此才能适应法律甚至法理滞后，而数字经济高速发展的现状，更好地利用司法判决保护企业的数据资产和合法利益，给予企业以推动数字经济发展的信念和信心。

我们期待随着我国个人信息保护实践的发展和法律运用的成熟，当下的疑惑在未来，答案会逐渐明朗，个人信息的全面保护并非个人诉求的无止尽满足，只有企业、个人等各方利益都能得到合理的关照和平衡，才能更好地实现个人信息保护的目标。

“言不信者行不果”——全面解读《互联网用户账号信息管理规定》

宁宣凤　吴涵　姚敏侣

2022 年 6 月 27 日，国家互联网信息办公室（国家网信办）发布《互联网用户账号信息管理规定》（《规定》），并宣布《规定》将在 8 月 1 日起正式施行，为企业留下了一个月的整改适应期。《规定》对于互联网信息服务提供者为用户提供的账号注册和使用服务，明确了信息安全管理的规范，提出了基本的监管框架，并且突出了其中对互联网用户账号信息的全生命周期管理要求和主体责任。

与此同时，《规定》通过搭建用户账号信息安全和账户信用管理机制，助力网络空间的诚信体系和良好生态建设。制定《规定》是规范互联网用户注册、使用和互联网信息服务提供者管理账号信息行为的需要，是维护意识形态安全、社会公平公正和网民合法权益的需要，也是防范化解国家安全风险、维护网络空间良好生态的需要。[1] 本文将对《规定》的立规沿革、重点制度以及企业义务进行多场景和全方位的分析。

一、《规定》的出台背景与基本概念

（一）历史沿革与上位法依据

《规定》最初源于 2015 年国家网信办发布的《互联网用户账号名称管理规定》。按照“后台实名，前台自愿”的原则，《互联网用户账号名称管理规定》对注册、使用和管理互联网用户账号名称提出了要求。不过，当时的规定只将用户账号名称作为规制的范围。但在现实生活中，随着互联网信息服务提供者提供服务的多样化和网络信息技术的进步，互联网用户除了用户名称以外，还有更多的在公共网络场景展示用户个性化信息的空间。这些用户信息对外展示时如同一张名片。而一些不法分子通过篡改、仿冒或者利用用户账号信息进行虚假宣传、招摇撞骗，乃至实施网络暴力等违法犯罪活动，对国家、社会、组织和个人的合法权益保护以及我国诚信清朗网络空间的建设带来了极大的危害。立规者敏锐地观察到了用户账户信息亟待进一步全面规制的现实需求，于 2021 年出台《互联网用户账号名称信息管理规定（征求意见稿）》（《规定（征求意见稿）》），该规定是对《互联网用户账号名称管理规定》的修订，包括用户名在内，将用于标识用户账号的信息（名称、头像、封面、简介、签名、认证信息等）纳入了规制的范围。

而此次《规定》约束对象由“账号名称”进一步向“账号信息”丰富和扩展。“用户账号名称”和“用户账号信息”在表述上不同，或可以理解为相关部门已经关注到“名称”和“信息”可能并非并列关系而是包含关系，从而最终确定使用“用户账号信息”的表述。在范围上，《规定》第 23 条明确表示互联网用户账号信息为“用于标识用户账号的信息”，与《规定（征求意见稿）》保持了一致。不过，最终出台的《规定》规定条款中并未明示与《互联网用户账号名称管理规定》之间作何衔接或处理，就目前来看，两个规定将同时处于有效状态并适用，而非替代关系。

与《规定》规范内容较为相近的相关规定还有**《互联网用户公众账号信息服务管理规定》。但需要注意的是，两个规定所规制的对象可能并不相同。**《规定》是将“互联网用户账号信息”作为主要的规制对象；后者则是聚焦于“在运营公众账号从事内容生产发布”的行为。由于互联网用户账号信息发布的平台未必都是公众账号，但同样要受到《规定》的规制。

从上位法依据看，和 2015 年《互联网用户账号名称

[1] 国家互联网信息办公室发布《互联网用户账号信息管理规定》，载“国家网信办”官方网站，http://www.cac.gov.cn/2022-06/26/c_1657868775333429.htm。

管理规定》相比，在《网络安全法》《个人信息保护法》《互联网信息服务管理办法》等法律法规相继出台之后，《规定》有了更加扎实的上位法基础。依托《网络安全法》构建的网络信息安全制度、《个人信息保护法》构建的个人信息处理和安全保护制度，以及《互联网信息服务管理办法》所规范的互联网信息管理制度，《规定》中各项条款约束的范围和依据相较于原来有了较大篇幅的新增，各项规定也自然考虑得更为全面，内容上更为详尽。

（二）《规定》的效力范围、规制行为和对象

1. 效力范围：位于境外的互联网信息服务提供者是否受《规定》约束？

《规定》第 2 条第 1 句规定：互联网用户在中华人民共和国境内的互联网信息服务提供者注册、使用互联网用户账号信息及其管理工作，适用本规定。该条实质上规定了《规定》的效力范围和规制行为。

在适用范围上，《规定》的要求是“**在中华人民共和国境内的互联网信息服务提供者**”。就此，似乎容易理解为《规定》只适用于在中国境内成立或者依据中国境内法律登记和注册的互联网信息服务提供者所提供互联网信息服务中包含的用户账号信息。但结合《规定》相关上位法、参照《电子商务法》第 2 条之规定，我们理解，**位于境外或者依据境外法律设立的互联网信息服务提供者，当其以面向中国境内用户提供互联网信息服务为目的，从事互联网信息服务活动的，也理应落入本《规定》规制范畴之中**。例如，在部分跨境电商场景中，虽然电子商务平台经营者可能并非在中国境内登记并设立，但若其有意识地主动地面向中国用户提供互联网信息服务，便需要履行《规定》有关作为互联网信息服务提供者的义务。当然，对于这种情形下是否最终需落实《规定》相关要求，还需根据客观情况和具体情形进行个案判断。

2. 规范对象：互联网用户账号信息与个人信息之间的联系与区别？

在规范行为上，《规定》规制的行为是“互联网用户在中华人民共和国境内的互联网信息服务提供者注册、使用互联网用户账号信息及其管理工作”，因此包含两个主体的行为，**其一是互联网用户在互联网信息服务提供者注册、使用互联网用户账号信息；其二是针对前述行为的管理工作**。

其中，尤其需要关注的是 “互联网用户账号信息”这一关键概念的内涵和外延。根据《规定》第 23 条，互联网用户账号信息，是指互联网用户在互联网信息服务中注册、使用的名称、头像、封面、简介、签名、认证信息等用于标识用户账号的信息。但请注意，**“互联网用户”与“个人 / 自然人”并非是完全等同的概念。根据《规定》第 7 条的规定，互联网用户区分为个人用户和机构用户。**因此不论是用于标识个人抑或是机构用户账号的信息，均属于“互联网用户账号信息”。

就互联网个人用户的互联网用户账号信息而言，在我国实名制的要求之下，这些信息和已识别或可识别的特定个人相关联，因此属于《个人信息保护法》第 4 条所定义的个人信息。因此，这类信息除了受到本《规定》的规制，互联网信息服务提供者在处理这些信息时还应遵守《个人信息保护法》的有关规定。但互联网用户账号信息的主要作用是用户在公共网络空间起到标识的作用，因此可能并非所有因账号产生或账号关联的信息均构成本《规定》中的互联网用户账号信息。例如，目前各互联网企业基于业务和管理之便，往往会为用户配置 UID 等仅供内部使用的用户唯一标识符，但由于这类信息仅由系统根据特定或随机算法生成的字符串，也仅作内部账号管理和映射使用，并不具有对外标识的作用，所以从规范意义上，这类信息虽然属于个人信息，但可能不属于《规定》所指称的互联网用户账号信息。

3. 义务主体：如何理解互联网用户和互联网信息服务提供者的定义？

互联网用户和互联网信息服务提供者是《规定》的两大义务主体。互联网用户在《规定》中未见专门定义。在网信办出台的部门规章及相关规范性文件中，使用“互联网用户”这一概念的有《互联网用户公众账号信息服务管理规定》《电信和互联网用户个人信息保护规定》，以及《互联网用户账号名称管理规定》等，但这三个规定也未

对“互联网用户”进行明确定义。而《互联网用户账号名称管理规定》除在标题使用“用户”这一措辞之后，全文也均以“互联网信息服务使用者”这一类型化的法规概念进行表述。**我们认为，《规定》中的“互联网用户”，指的是通过注册和使用互联网用户账号信息，以接受和使用互联网信息服务的自然人、法人或者非法人主体，包括个人用户和机构用户。**

与“用户”这一概念不同，《规定》为“互联网信息服务提供者”提供了明确的定义：是指向用户提供互联网信息发布和应用平台服务，包括但不限于互联网新闻信息服务、网络出版服务、搜索引擎、即时通讯、交互式信息服务、网络直播、应用软件下载等互联网服务的主体。**这一概念以描述式定义和列举式概括的方式，外延实则较为宽泛，囊括了现有提供互联网信息服务的多种业态，因此不论具体的信息服务内容类型如何，通过互联网提供信息发布和应用平台服务产品的企业一般均属于《规定》的互联网信息服务提供者。**从上位法来看，《互联网信息服务管理办法》第 3 条还专门规定了互联网信息服务的定义，包括经营性（通过互联网向上网用户有偿提供信息或者网页制作等服务活动）和非经营性两类（通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动）。由此看来，《规定》在界定互联网信息服务提供者时，并未突破《互联网信息服务管理办法》的有关定义，但是对其进行了更具场景化和类型化的描述。

二、《规定》的热点问题与重点制度

（一）账号信息的真实性核验

《规定》第 7 条和第 9 条分别规定了账号信息真实性核验和实名认证制度。账号信息真实性核验主要源于《互联网用户公众账号信息服务管理规定》第 9 条的规定。具体而言，个人用户涉及职业信息的，应当与个人真实职业信息相一致；机构用户账号信息，应当与机构名称、标识等相一致，与机构性质、经营范围和所属行业类型等相符合。《互联网用户公众账号信息服务管理规定》第 9 条的规定在内容上更接近于《规定》第 11 条的特定行业的账号认证机制。因此可以理解为《规定》将该要求拓展至了用户账号信息的管理方面，并作出了更加一般性的规定。不过，第 7 条的规定对个人用户和机构用户也进行了区别处理。个人用户只有在含有职业信息的时候才存在对应要求；较此而言，机构用户的账号信息则必须保证其真实性。

（二）实名认证制度

《规定》第 9 条并非首次规定实名认证要求。《互联网用户公众账号信息服务管理规定》以及《互联网用户账号名称管理规定》均对用户实名制进行了规定。在互联网信息服务提供者为互联网用户“提供信息发布、即时通讯等服务”时，明确需履行实名认证义务。

但需注意的是，注册用户履行实名制要求，系由于不论是信息发布还是即时通讯服务，都体现出用户能够利用该服务对外生产和交换信息内容的特征。换言之，**企业不得以实名制认证等法定要求，强迫非注册用户（不属于《规定》定义下的“互联网用户”）提交实名认证信息。**这其中的考虑，实际上协调的是《个人信息保护法》“个人信息收集的最小必要原则”和《常见类型移动互联网应用程序必要个人信息范围规定》等规定之间的关系。《个人信息保护法》第 16 条规定，不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；《常见类型移动互联网应用程序必要个人信息范围规定》中相当多的 App 类型（例如浏览器类、输入法类）无需个人信息即需提供基本功能。因此，如果《规定》一方面要求互联网信息服务提供者需对所有注册或非注册的用户履行实名认证义务，要求用户提供实名制的个人信息，另一方面又要求其不能收集非必要个人信息，则会一定程度上出现两者不协调乃至矛盾的情况。

由此，对于涉及用户能够对外生产和交换内容信息的服务，互联网信息服务提供者应遵守《规定》的要求，强制要求用户进行实名制认证。而对于非上述范围内的互联网信息服务，尽管互联网信息服务提供者仍需要根据《互联网用户账号名称管理规定》等履行实名制认证义务，**但是否进行注册应交由使用者自行决定，不能因为使用者拒绝注册成为用户而拒绝提供服务。**由此，《规定》的要求便能够和《个人信息保护法》《常见类型移动互联网应用程序必要个人信息范围规定》取得协调。

（三）特定行业的账号认证机制

1. 特定行业的账号认证机制

除了《规定》第 7 条外，第 11 条还规定了特定行业的账号认证机制：对于互联网用户申请注册提供互联网新闻信息服务、网络出版服务等依法需要取得行政许可的互联网信息服务的账号，或者申请注册从事经济、教育、医疗卫生、司法等领域信息内容生产的账号，互联网信息服务提供者应当要求其提供服务资质、职业资格、专业背景等相关材料，予以核验并在账号信息中加注专门标识。

例如，根据《出版管理条例》第 36 条规定，通过互联网等信息网络从事出版物发行业务的单位或者个体工商户，应当依照本条例规定取得《出版物经营许可证》。就其中的新闻出版而言，还要根据《新闻出版许可证管理办法》获取新闻出版许可证。而针对特别的行业领域，对生产这类信息内容的账号进行认证是有必要的，这类信息往往可能产生较大的社会影响力，该举措一定程度上能够保证这类信息的权威度和真实性，以防止良莠不齐的网络信息对公共利益造成不良影响。

2. 与特定行业的账号认证机制与实名认证的区分

首先，**两者认证的触发条件不同**。《规定》的实名认证要求在用户需要对外生产信息内容之前强制触发。**但特定行业的账号认证仅是在需要实名认证的基础上，基于特殊的法律规定、特定行业的对外信息内容生产用户进行**。因此，如果一个用户虽然涉及对外生产内容信息，但并没有特殊法律规制，也不属于特定行业，则只需进行实名认证，而无需进行特定行业的账号认证。

其次，**两者的公示程度不同**。对于特定行业的账号认证中涉及的部分用户账号信息，需要根据《规定》第 13 条的规定，以一定的形式在合理范围内进行公示。而实名认证机制，往往是互联网信息服务提供者对用户的一种管理要求，遵循“后台实名，前台自愿”的原则。这意味着用于实名认证所需的个人电话号码、身份证号等信息乃至隐私信息无需也不能对外公开披露。

3. 选择性职业认证和强制性职业认证

就个人用户而言，《规定》第 7 条和第 9 条均涉及了对职业的认证。我们理解，第 7 条第 1 款的规定是一种选择性的职业认证，是否进行认证交由个人用户自行决定；而第 9 条则更倾向于属于强制性职业认证，当该个人用户申请注册从事经济、教育、医疗卫生、司法等领域信息内容生产的账号，则必须提供职业资格、专业背景等相关材料进行认证，由互联网信息服务提供者强制要求个人用户进行。

不过，不论是选择性职业认证和强制性职业认证，一旦触发职业认证机制，则互联网信息服务提供者必须采取一定的手段核验这些信息的真实性。不过，正如前文所述，个人用户账号信息属于个人信息范畴，因此宜遵循最小必要原则，把握对“职业认证”的方式。在《规定》出台之前，互联网平台已经就职业认证进行了充分的实践。例如，某社交平台的职业认证中，基本的认证材料需求为在职证明、执业证明和职业资格证书。其中，在职证明需要用户提供单位的地址、联系人和联系电话，以确保身份的真实性。某知识类分享平台的职业认证需要用户提交身份证明、工作证明、职业资格证明。对材料则要求包括：材料需为原件、清晰、有效、公开渠道可查。[2]

综合各种实践，我们理解，在进行职业认证时，可能需要要求用户提供执业资格、持续、有效的执业状态、以及真实身份以及验证其职业资格的真实关联性三个维度进行把控。同时应注意避免收集过多的，与职业认证无关的个人信息，从而触及《个人信息保护法》收集个人信息最小必要性的问题而引起纠纷。为此，建议互联网信息服务提供者在开展此项工作时，开展充分的前期调查，了解特定行业的行政许可要求、特定行业的从业资格证书类型等，建立针对各行各业的认证清单，将认证工作流程化、规范化。

（四）信息内容安全管理制度

《规定》第 8 条规定了互联网用户注册、使用账号信息时，不得出现的 8 种情形。这位互联网信息服务提供者在审核账号信息时提供了较为清晰的指导。

[2] https://zhuanlan.zhihu.com/p/96956163

需要特别注意的是，该条第 1 项将《网络信息内容生态治理规定》中第 7 条的违法信息和第 8 条的不良信息作了统一的要求，即一律要求不得在注册、使用账号信息的情形下出现。《规定》将两者统一作为“不得”出现的内容，**意味着对用户账号信息的内容要求更为严格**。我们理解，这是因为账号信息作为标识和展示用户，往往具有更强的公开信息属性，因此公众对这些信息的依赖程度更高，而《规定》认为互联网信息服务提供者在对用户账号信息内容的管理上，可能负有更高的信息内容安全注意义务。

（五）互联网用户账号信用体系

《规定》第 18 条规定，互联网信息服务提供者应当建立健全互联网用户账号信用管理体系，将账号信息相关信用评价作为账号信用管理的重要参考指标，并据以提供相应服务。该条并没有为互联网信息服务提供者提供具体的措施，为市场主体如何履行该义务，留下了较大的自主空间。

1. 互联网用户账号信用管理体系的目的？

互联网用户账号信用管理体系的建立是为了进一步防范、打击同一不法主体利用互联网用户账号从事网络违法犯罪活动。通过该机制，互联网信息服务提供者能够根据其识别和判断用户账号信用情况，进而拒绝提供相应的服务。

该体系通过分类分级的方式进行。根据种类和严重程度不同来决定拒绝提供多大范围、多大程度上的服务。同时，由于这类处理对用户的权益影响较大，在并非极其严重的情形下，互联网信息服务提供者宜审慎把握各类永久措施。

例如，近期出台的**《关于进一步规范网络直播营利行为促进行业健康发展的意见》中，明确要求加强网络直播账号分级分类管理**。网络直播平台应当严格按照有关法律法规要求，建立并严格执行网络直播账号分级分类管理制度；对违反相关法律法规的网络直播账号，依法依规采取警示提醒、责令限期改正、限制账号功能、暂停账号使用、永久关闭账号、禁止重新注册等处置措施，保存有关记录并按要求及时向有关部门报告。

2. 针对用户账号抑或是针对用户个人？

我们理解，从本质上来看，《规定》所要求的互联网用户账号信用管理体系应需针对具体的用户主体。因为并非用户账号，而是使用用户账号的本人才是具体的信息内容生产者，才是需要被纳入信用管理的实际对象。对于一些经常利用互联网用户账号从事不法活动的个人和机构，应当建立长效机制，有效防范这类用户频繁“转移阵地”，采取不断更换用户账号等方式继续从事不法活动。

3. 是否需要跨平台协作实现？

互联网用户账号信用管理体系可能会以跨平台的方式实现。这意味着，一个在 A 互联网信息服务的用户账号信用情况，在未来可能将会和 B 等其他互联网信息服务实现共享，从而实现全互联网信用协同。一个用户在一个互联网信息服务的行为，将会影响到其他互联网信息服务对其提供的服务。

这一思考在构建诚信网络空间的方向性把握上具有较强的指导意义，而且也并非完全没有现实基础。此前，中国信通院曾推出手机号“一键解绑”功能，通过其旗下微信公众号“一号通查”功能，可解除本人持有号码前（即号码注销重启前）号码注册绑定的互联网账号关联关系（本人持有号码期间绑定的互联网账号不受影响）。该功能覆盖多款常用 App。[3] 虽然通信院提供的仅是解绑功能，但功能背后实现的是以手机号码为纽带的多互联网平台的信息共享。因此，实现全网络平台的互联网用户账号信用管理体系，并非完全是“空中楼阁”。

不过，《规定》第 18 条的义务是否仅限于互联网信息服务提供者自身内部的用户账号信息，或许还有点进一步细致的论证研讨。虽说技术上实现全平台的信息共享不无可能，但是这可能也会给各平台增加一定的技术协调成本。而若仅由某一个或几个平台承担账号信用信息汇集和梳理工作，则跨平台共享用户账号信息管理也可能存在超出乃至滥用个人信息处理“权限”的嫌疑。从用户权益上看，如果仅因某个用户的某个不当行为而引起全网连锁反应，也可能会影响该用户在其他互联网信息服务的正当使用。因此，为了符合“比例原则“的要求，未来用户账号信用体系的跨平台建设，可能是个值得多方参与、贡献智

[3] http://finance.people.com.cn/n1/2022/0608/c1004-32441591.html

慧的重要课题。

三、《规定》下企业的法定义务与责任

（一）对用户账号信息的全生命周期审查义务

纵观《规定》五章共计二十四条的条款规定，不难发现，对于“互联网用户账户信息”的网络信息安全管理方面也贯彻了事前、事中和事后的全生命周期监管要求。总结来看，企业作为互联网信息服务提供者，**应当至少在用户账号信息的管理上履行“事前严格审查”、“事中动态审查”和“事后定期审查”等多个里程碑节点的法定义务**。

1. 对一般用户账号注册前的审查义务

《规定》第 10 条第 1 款实际上规定了互联网平台应当在用户账号进行注册（包括通过手机号码实现用户首次“一键登录”）前应当履行的核验义务。根据该条规定，我们理解，应当核验的维度至少应当包含《规定》第 7 条、第 8 条和第 9 条所规定的内容，进行实质性的核验，以尽可能保证用户账号信息的真实性、完整性和准确性。在目前的行业实践中一般可能采取机器自动化核查（如关键词屏蔽）和人工审查相结合的方式，以达成前述法定义务的预期履行效果。

遵循对应用户账户风险等级对应信息分类分级管理的基本思路，《规定》第 10 条第 2 款专门对包含“中国”“中华”“中央”“全国”“国家”等内容，或者含有党旗、党徽、国旗、国歌、国徽等党和国家象征和标志的用户账号信息，要求以从严标准进行核验。初步理解，对于“国字号”相关机构称谓或者带有党和国家象征的相关标志的使用，应当遵循诸如《中国共产党党徽党旗条例》《国旗法》《国歌法》《国徽法》等相关法律、法规和国家规定，特别是其中的禁止性使用条件或规范，进行逐条审查和核对。

2. 对强制关闭账号的高关联账号注册时的从严核验义务

而值得注意的是，《规定》第 10 条第 3 款要求“**防止依法依约关闭账号重新注册**”，以及**与前述账号关联度高的账号信息进行从严核验的特殊规定**。考虑到互联网信息服务的匿名性强、流动性大，网络违法犯罪活动和不良信息的复现率比较高，由此《规定》对于已经依法依约强制关闭的账号信息，以及与该被强制关闭的账号具有较高关联性的账号信息，施以互联网信息服务提供者以更高的注意义务和防范责任。

对于该款的解读，**主要在于“防止重新注册如何理解”以及“关联性如何判断”**两个关键问题上。

首先，我们认为不得重新注册的账号应该限于依据法律法规、用户使用协议等存在较为严重的违法违约行为而导致已经被采取强制措施关闭的账号。该规定的本质在于杜绝违法违约账号改头换面后的“死灰复燃”，从而避免违法或者不良信息、网络信息违法犯罪活动“卷土重来”。但对于注册已被关停的账号的个人或者机构而言，并不当然属于该条所被禁止“重新注册”账号之列。但是，对于具有被强制关闭账号的用户个人或机构而言，其需要接受更为严格的审查核验。

其次，哪些“关联度高”的用户个人或者机构需要受到“从严核验”的约束，换言之，如何判断“关联性高”？《规定》暂未作出明确要求。从互联网信息服务行业实践来看，如果属于同一自然人用户在同一或关联平台注册的新账号，或者相同和具有紧密关联关系（如具有直接股权控制或在利益关系上归属于同一集团）的组织机构用户在同一或关联平台上注册的新账号，应当被理解为归属于前述需严格核验的账号信息范畴。

3. 对正常使用和存量用户账号的动态核验义务

《规定》第 15 条规定了互联网信息服务提供者应当建立账号信息动态核验制度，“适时核验存量账号信息”。对于企业而言，应当关注动态审核机制的触发条件或情形，以及可被视作动态核验的相关措施。

联系《规定》第 10 条，当用户在申请或者主动变更账号信息时，应当被视作触发动态审查的具体情形之一。目前行业中不少平台均在用户重新上传头像、更改昵称或者个性化签名等资料信息时，提示用户将进行机器或部分人工审核的机制。当然，当用户账号行为出现部分标志性

信号时，如用户常用登录 IP 地址出现跨境或者敏感地区变化，或者用户账号在同一段时间内出现明显不合理地频繁登录等情形时，可以考虑通过再次要求用户提交核验信息的方式，以达成动态核验的要求。当然，当用户主动寻求“找回账号”等时间点契机上，也可考虑加入动态核验机制，以在尽可能避免干扰用户正常使用的同时强化账号信息的常态化监督。

此外，对于“沉默账号”的处理一直是互联网信息服务提供者较为苦恼的问题。结合目前行业实践，在不少平台的业务部门进行沉默用户“召回 / 促活”的过程中，我们也建议嵌入账号信息的定期盘点和核验机制。对于同时可能存在信息安全问题的长久沉默账号，根据《规定》要求应当暂停提供服务，并以应用内通知、通知栏消息以及授权后短信等合理方式，通知用户限期改正。

（二）用户账号信息公开展示与持续监督义务

在《规定》第 7 条、第 9 条和第 11 条的基础之上，第 12 条和第 13 条进一步规定了用户账号信息公开制度。其中，第 12 条要求互联网信息服务提供者应当在互联网用户账号信息页面展示合理范围内的互联网用户账号的互联网协议（IP）地址归属地信息，便于公众为公共利益实施监督。第 13 条要求互联网信息服务提供者应当在互联网用户公众账号信息页面，展示公众账号的运营主体、注册运营地址、内容生产类别、统一社会信用代码、有效联系方式、互联网协议（IP）地址归属地等信息。

可以看出，第 12 条和第 13 条在内容上存在一定的重合，都提及了互联网协议（IP）地址归属地信息的公示要求。我们理解，就互联网协议（IP）地址归属地信息而言，第 13 条规定了互联网信息服务者对此具有强制公示义务；第 12 条则是规定了公示互联网协议（IP）地址归属地信息的目的以及限制。

1. 公开 IP 归属地信息的合法性基础研讨

自从 2022 年 4 月 28 日，某社交平台发布将公开 IP 地址归属地信息以来，就该信息是否属于个人信息，公开该信息是否具备《个人信息保护法》个人信息处理合法性等问题引发了较大范围内的讨论。[4] 此前，也存在用户以某社交平台强制公开用户 IP 地址归属地信息侵犯个人信息权利为由进行起诉的案例。就此，我们理解，《规定》第 12、第 13 条一方面将公开 IP 地址归属地信息以互联网信息服务提供者义务的形式确定了下来，另一方面也说明该行为具有为公共利益进行舆论监督的性质，因此具备个人同意以外其他公开个人信息的合法性基础。

对于个人用户而言，公示 IP 地址或者归属地信息，无疑属于一种在客观上“未经个人同意”处理个人信息的情形，因此会受到合法性挑战。为此，第 12 条说法是“便于公众为公共利益实施监督”，意为该方式是为公众提供一个舆论监督的渠道。该规定是为了确认互联网信息服务提供者未经用户同意便可处理个人信息（公示 IP 地址归属地信息）的合法性。《规定》在效力上属于部门规章，不属于法律和行政法规，因此无法直接将《个人信息保护法》第 13 条第 7 项的要求作为合法性依据，但该合法性基础或可尝试从该条第 5 项中得以援引。

借鉴新闻传播领域的专业观点，舆论监督的主体可能为新闻媒体或者普通公民，其中，媒体是公民实现舆论监督的媒介。不过，由于互联网信息技术的发展，公民可通过在互联网平台上发表意见和评论，以体现公民作为实现舆论监督的主体。**就此而言，在广泛意义上理解《个人信息保护法》第 13 条第 5 项，新闻媒体并非舆论监督的唯一主体，公众更是舆论监督的直接参与者。**[5] 在这一层面上，《规定》认为公示互联网协议（IP）地址归属地信息是为了实现《个人信息保护法》中规定的为公共利益实施新闻报道、舆论监督等行为，为该种义务设定相应寻求了合法性依据。并且，根据 12 条的表述，该信息的公开需要在“合理范围内”，这一要求也和《个人信息保护法》的要求相互吻合。**这同时也要求互联网信息服务提供者在公示 IP 地址归属地信息时不能过于精确，以避免与其他信息结合轻易识别到具体个人，对个人产生其他权益影响。**

2. 公开 IP 归属地信息时的“合理范围”平衡

在根据《规定》第 12 条公示 IP 地址归属地信息时，

[4] 翟嘉诗：《IP 地址信息的法律属性分析》，载《互联网天地杂志》公众号，https://mp.weixin.qq.com/s?__biz=MzIxMTc4Mzc2NA==&mid=2247486810&idx=1&sn=a6f303e219c9ac8fb760a19e4c0e9fbe&chksm=97515461a026dd77ffb84b80fc3fc438d289970a7b2908dd50e2b4b36ed6d2204c75644f5a02&scene=27。

[5] 李延枫：《舆论监督：概念辨析与重新认识》，载《新闻与传播学术前沿》公众号，https://mp.weixin.qq.com/s/tQvPazVYTw2qi1wn9HDN5Q 。

应同时符合《个人信息保护法》第 13 条第 5 项的要求。简言之，一是要确保公示该信息确有保护公共利益，能够起到促进舆论监督的作用; 二是要将公示的程度限制在“合理范围”内。

就公共利益而言，已经有学者对公示 IP 地址归属地信息能否真正起到良好的舆论监督提供了辩证的观点。一方面公示 IP 地址归属地信息的确能够在一定程度上起到识别、防范“境外水军”的风险，但同时也可能产生地域歧视等潜在问题，对于真正试图限制的对象，使用技术手段篡改上述信息也并非没有可能。互联网信息服务提供者在履行该项义务时，也应仔细考量公开信息与目的实现之间的匹配关系。例如，用户在某搜索引擎上注册账号。但由于用户在搜索引擎中并不对外生产和交互信息内容，其在搜索引擎进行搜索的行为也不涉及公共利益，在这种场景下仍强制公开用户账号的 IP 属地信息是缺乏必要性的。

就合理范围而言，客观存在基于公共利益进行舆论监督的必要性的基础上，公示的范围应遵循目的限制原则，仅限于实现目的的范围内。如今颁布的《规定》和之前的征求意见稿相比，删去了公示用户 IP 属地信息的细节规定，转而要求平台在“合理范围内”公开该信息。这表明《规定》意识到了在不同场景下，合理公开与否、范围均是不同的，不能幻想给出一套“放之四海而皆准”的细节性规范。为此，可以考虑从调整强制公开的阶段、限定强制公开的对象、缩小强制公开的范围等方面合理控制公开的范围。[6]

（三）企业互联网账号信息管理的主体责任

《规定》第 14 条规定，互联网信息服务提供者应当履行互联网用户账号信息管理主体责任，配备与服务规模相适应的专业人员和技术能力，**建立健全并严格落实真实身份信息认证、账号信息核验、信息内容安全、生态治理、应急处置、个人信息保护等管理制度**。由此，《规定》在用户账号信息这一规范对象上，形成了对互联网企业的管理主体责任要求。

根据《规定》第 21、22 条，企业账号信息管理方面的主体责任，可以从“执法抓手”和“法律后果”两个方面体现出来。一方面，网信部门可依据相关规范对互联网信息服务提供者管理互联网用户注册、使用账号信息情况实施监督检查，而互联网信息服务提供者应当予以配合，并提供必要的技术、数据等支持和协助；另一方面，对于存在较大网络信息安全风险的，省级以上网信部门**可以要求企业采取暂停信息更新、用户账号注册或者其他相关服务等**措施，企业应当按照要求采取措施，进行整改，消除隐患。

关于处罚责任，考虑到《规定》归属于部门规章法效层级，根据《行政处罚法》相关规定，可以在法律、行政法规规定的给予行政处罚的行为、种类和幅度的范围内作出具体规定。**若尚未制定法律、行政法规的，国务院部门规章对违反行政管理秩序的行为，可以设定警告、通报批评或者一定数额罚款的行政处罚**。罚款的限额由国务院规定。《规定》第 22 条中所规定的罚则条款，便遵循了该规定，在遵从已有法律、行政法规规定处罚的前提下，为了更为全面的压实企业对用户账号信息安全的主体责任，还专门规定了未有法律、行政法规规定情形下的“警告”“通报批评”“责令限期改正”以及“罚款”的处罚要求。对于这种可能面临的行政处罚责任情况，值得引起互联网企业的重视。

结语

理解上述《规定》所体现和折射的立规价值取向和基本立场定位，我们认为相关主管部门对于互联网信息服务提供者对于互联网用户账号信息安全的审核和管理要求进行了全面的调整和升级，对于相关特定情形的安全保障义务和责任也进行了细节性和常态化的规定。特别是在厘清相关概念和义务要求的前提下，企业需要建立起针对互联网用户账号信息的全生命周期管理流程、体系和机制，主动配合相关部门对于账号信息安全的管理和执法要求，尤其是在实践中探索一套既符合业务实际需求、又能够确保网络空间生态治理和诚实信用体系建设的企业规则。这或许是我们期待《规定》所能够达到的“规则指引实践，实践丰富规则”的积极局面。

感谢实习生吴仁浩对本文作出的贡献。

[6] 彭錞：《IP 属地信息公开：如何平衡个人隐私与网络秩序》，载《五马社》公众号，https://mp.weixin.qq.com/s/Jh8a8DSeO3FvKiPy6qR-IQ 。

映日荷花别样红——中欧个人信息出境标准合同（条款）对比分析

宁宣凤 吴涵 徐梦悦

为规范个人信息出境活动，保护个人信息权益，促进个人信息跨境安全、自由流动，国家互联网信息办公室于2022年6月30日发布了《个人信息出境标准合同规定（征求意见稿）》（《规定》），并附《个人信息出境标准合同》（标准合同）。作为《个人信息保护法》（《个保法》）的配套制度与文件，《规定》与此前发布的《数据出境安全评估办法（征求意见稿）》（《评估办法》）、《网络数据安全管理条例（征求意见稿）》（《网数条例》）等规范中有关数据跨境的规制内容互为补充，提高《个保法》第三十八条有关个人信息跨境规的可执行性。

考虑到涉及个人信息出境的场景通常涉及多司法个人信息保护交叉要求，本文在初步总结《规定》与标准合同内容的基础上，拟以比较法的观察角度，浅析《规定》与标准合同的内容与欧盟《通用数据保护条例》（GDPR）下规定的标准合同条款的异同，以为国际化企业提供参考。

一、《规定》及标准合同的要点总结

为对标准合同的适用搭建一整套合规机制，《规定》就标准合同的适用情形与主要内容、与个人信息保护影响评估的协作、向网信部门进行事前备案及确立主管部门与监管职权等内容进行了规定。

（一）明确标准合同的适用情形

《规定》第四条明确了标准合同的适用前提，如果个人信息处理者不构成关键信息基础设施运营者、处理个人信息不满100万人、自上年1月1日起累计向境外提供未达到10万个人信息或1万敏感个人信息，方可以签署标准合同作为满足《个人信息保护法》第三十八条有关个人信息跨境传输的要求。

而针对未落入以上适用情形的个人信息跨境传输场景，个人信息处理者仍应当依据《个保法》《评估办法》等相关规范，以向相关网信部门申报数据出境安全评估、按照国家网信部门的规定经专业机构进行个人信息保护认证等方式作为合规路径。

（二）强调标准合同与个人信息保护影响评估的协作机制

《个人信息保护法》第五十五条规定，向境外提供个人信息时，个人信息处理者应当事前就个人信息跨境传输所涉及的处理目的、处理方式的合法性、正当性与必要性; 对个人权益的影响及安全风险; 以及所采取的保护措施是否合法、有效并与风险程度相适应等维度进行个人信息保护影响评估。

《规定》第五条不仅重申了个人信息处理者在实施跨境传输应当进行个人信息保护影响评估的义务，且第七条还要求个人信息处理者在履行标准合同备案义务时同步提交相关个人信息保护影响评估报告的要求。

（三）设立标准合同的备案义务

我们理解，为便于主管部门就个人信息跨境传输实现敏捷监管，及时对个人数据跨境传输过程所可能产生的安全风险进行掌控，作为一种典型的事前监管手段，《规定》第七条提出了个人信息处理者在标准合同生效后向所在地省级网信部门进行备案的义务。但**值得注意的是，备案与个人信息跨境传输的开展并不具备直接关联，后者仅以标准合同的生效为前提**。此外，《规定》第八条还以个人信息跨境传输情况的“变化”为关键词，就缔约双方应当重新签订合同并再次履行备案义务的情形进行了列举。

同时，因向监管部门履行备案或涉及到个人信息跨境传输中相关个人隐私、个人信息、商业秘密、保密商务信息的对外披露，《规定》第九条对应就参与标准合同备案的机构及人员在履行职责过程中应当遵守的保密义务进行了规定。

（四）明确标准合同的主要内容

《规定》第六条明确了标准合同所应当具有的内容，包括但不限于缔约双方的基本信息、个人信息跨境传输的基本情况、所采取的技术与管理的安全保障措施、境外接收方所在国家相关政策法规对履约的影响、个人信息主体的权利保护以及作为民事合同的部分标准条款，如救济、合同解除、违约责任与争议解决等。前述内容与《评估办法》第九条规定的，数据处理者与境外接收方订立的合同所应当包含的内容具有较高协同性，是对《评估办法》的承继与呼应。

而具体就标准合同的具体内容而言，该合同共有九大条款，以个人信息处理者的义务、境外接收方的义务、个人信息主体的权利保护及事先确认个人信息出境目的地政策法规对合同影响等内容为关键维度，对个人信息跨境场景下的各方角色（如个人信息处理者、境外接受与个人信息主体）的权利义务进行约定：

就个人信息处理者的权利义务而言，标准合同精准反映《个保法》等相关法规对个人信息处理者在跨境传输个人信息所施加的一般性及特殊性的法定义务，包括但不限于履行境外接收方信息披露义务、获得单独同意的法定基础、保障境外接收方处理个人信息的活动达到《个保法》规定的个人信息保护标准等内容。

就境外接收方而言，标准合同未区分其具体数据处理角色，但原则上要求接收方履行按照约定处理个人信息、采取有效的技术和管理措施、发生信息泄露时向个人信息主体及监管部门进行告知与报告、配合个人信息主体履行义务及接受中国监管机构的监督管理等义务。

就个人信息主体而言，标准合同主要是通过确立“第三方受益人”角色以保护其权益，在此身份下，**个人信息主体可直接向个人信息处理者或境外接收方要求获取合同副本、主张合同中约定权利与《个保法》下的各项个人信息权利。**

二、我国标准合同与欧盟标准合同条款的对比

与我国出台的《规定》及标准合同具有较强比较法意义的域外法规定，主要包括欧盟标准数据保护条款。根据欧盟 GDPR 第 46 条的规定，签署欧盟委员会认可的标准数据保护条款作为一种适当的保护措施，是为将个人数据跨境传输至欧盟经济区外第三方国家的合规要件之一。在此基础上，欧盟委员会于 2021 年 6 月 4 日以发布（EU）2021/91 号执行决定的方式（《决定》）提供了最新版本的向第三国转移个人数据的标准合同条款（Standard Contractual Clauses，SCC）。此最新版本的 SCC 总共分为 4 个部分、18 大条款，主要内容围绕个人数据跨境传输过程中数据出境方与数据进口方各自应当采取的数据保护措施、数据主体的权利保护、转委托处理者的注意事项、合同终止条件与法律适用等方面。

纵观我国标准合同与 SCC 的内容及形式，我们理解，我国标准合同在吸收各司法辖区共识的同时，也结合中国个人信息保护的特点，提出新的理念和要求。

（一）共识与呼应

1. 确认第三方受益人权利保护

个人信息跨境传输事关个人信息主体的相关利益，因此，除对数据出境方与数据进口方的权利义务进行规定外，SCC 与标准合同均制定了有关第三方受益人保护的条款，相关内容具有较高一致性。具体内容对比如下：

共性	欧盟 SCC	我国标准合同
第三方受益人	数据主体作为第三方受益人、可直接对数据出境方与数据进口方援引并执行 SCC 条款的权利，包括但不限于： • 向缔约双方主张 GDPR 下规定的数据主体权利； • 确认目的地第三国适用于数据进口方处理个人数据的法律和惯例对数据进口方履行 SCC 的影响； • 确保通过投诉、申诉与诉讼方式获得救济； • 在数据进口方无法继续履行等法定原因产生时要求终止合同等。	要求个人信息处理者向个人信息主体告知其与境外接收方通过本合同将其约定为第三方受益人，基于此，个人信息主体可向标准合同缔约双方要求： • 执行合同中关于个人信息保护义务； • 提供标准合同副本； • 确认境外接收方所在国有关个人信息保护的政策法规对履行标准合同履行的影响； • 通过投诉、诉讼等方式获得救济； • 在法定要件发生时主张解除标准合同等。

2. 通过合同承诺接受长臂司法管辖

我们理解，GDPR 与《个保法》均未就数据跨境传输下境外数据进口方是否直接受制于前述法律提供明确规定，实务中不乏关于二者域外适用力的探讨。当前，SCC 与标准条款均在此问题提供了可借鉴的规定，即境外数据进口方

将通过签署 SCC 与标准合同承诺受制于数据出境方所在地的监管要求。具体内容对比如下：

共性	欧盟 SCC	我国标准合同
合同承诺接受长臂司法管辖	• 数据进口方同意服从欧盟主管监管部门的管辖并与之合作，特别是，数据进口方同意回应询问、接收审计和遵守监管部门采取的措施，包括损害赔偿和补偿措施。 • 数据出境方应当就数据进口方已经采取的必要行动以书面方式向监管部门进行确认。	• 境外接收方同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问，配合监管机构检查，服从监管机构采取的措施或做出的决定。 • 就提供已采取必要行动的书面证明。 **值得注意的是，标准合同的规定是对境外类似长臂管辖要求的回应。**

3. 确认数据跨境目的地数据监管法律对合同履行的影响

为确保数据跨境过程中有关数据的安全性保障要求得到贯彻与落实，SCC 与标准合同均以专章形式，就数据出境方与数据进口方在开展个人信息跨境传输过程前，应当对目的国关于个人信息保护的法规政策对 SCC 或标准合同履行所产生的影响进行审慎判断的义务进行了规定。具体内容对比如下：

共性	欧盟 SCC	我国标准合同
确认数据跨境目的地数据监管法律对合同履行的影响	• 数据出境方与数据进口方均应保证其没有理由相信，目的地第三国适用于数据进口方处理个人数据的法律和惯例，包括披露个人数据的任何要求或授权公共当局查阅的措施，会妨碍数据进口方履行该等条款规定的义务。 • 为证明该审慎义务的履行，双方应当承诺其就数据跨境的具体处理情况、目的地的法律和惯例、已经采取的保障措施予以了充分的考虑。 • 数据进口方保障在上述过程中已尽最大努力向数据出境方提供了相关信息。	• 个人信息处理者与境外接收方需保障，经过合理努力仍不知晓境外接收方所在国家或者地区的个人信息保护政策法规（包括任何提供个人信息的要求或授权公共机关访问个人信息的规定），会阻止境外接收方履行本合同规定的义务。 • 在提供上述保证时，双方应当声明已经就数据出具的具体情况、境外接收方所在国家或者地区的个人信息保护政策法规以及境外接收方安全管理制度和技术手段保障能力进行了考量。

（二）对比下的中国特色

1. 设定缔约主体权利义务的不同基础

最新版 SCC 分别以 GDPR 下有关数据控制者及处理者的角色划分为维度，根据数据出境方与数据进口方所可能形成的不同法律关系为基础划分了四种个人数据跨境传输的模式，分别为：（1）控制者向控制者传输的“C-C 模式”；（2）控制者向处理者传输的“C-P 模式”；（3）处理者向处理者传输的“P-P 模式”以及（4）处理者向控制者传输的“P-C 模式”。在此基础上，根据 SCC 签署双方在不同模式下所形成的具体数据处理法律关系，数据出境方与数据进口方将面临不同种类的合同权利义务。

而我国标准合同并未就个人信息跨境场景下数据出境方与境外接收方所形成的数据处理法律关系做进一步划分，

而是以统一将数据出境方归纳为“个人信息处理者”、数据进口方定义为“境外接收方”的方式作为构建基础，对缔约双方在个人信息跨境过程中所享有和承担的权利义务进行了一致性的规定。具体内容对比如下：

个性	欧盟 SCC	我国标准合同
	以数据处理法律关系为基础区分合同权利义务	以个人信息处理者为轴心统一设定合同权利义务
设定缔约主体权利义务的不同基础	根据 SCC 签署双方在不同模式下所形成的具体数据处理法律关系，数据出境方与数据进口方将面临不同种类的合同权利义务，例如： • 在 C-C 模式中，数据进口方因同时作为数据控制者，将背负更高程度的合规义务，如就个人数据跨境获取数据主体的同意等合法性基础、履行告知等透明性义务、直接响应数据主体权利主张以及在发生数据泄露事件时向数据保护机构进行汇报等； • 就 C-P 模式、P-P 模式而言，作为数据处理者的数据进口方除了具有协助作为数据控制者的数据出境方履行前述法定义务的职责外，基本上仅具有按照控制者要求处理数据与保障数据传输及处理过程之安全性的义务； • 在较为特殊的 P-C 模式下，因数据出境方为欧盟境内的数据处理者，需受到 GDPR 等数据监管要求的管辖，故作为数据控制者的数据进口方还存在不得妨碍数据出境方履行前述监管要求的合同义务。	• 就个人信息处理者而言，应当统一遵守包括但不限于：最小必要等处理原则；实施个人信息保护影响评估；获得个人信息主体的单独同意；对个人信息跨境传输采取技术与管理层面的安全保障措施；接受监管机构询问及向个人信息主体提供合同副本等要求。 • 就境外接收方而言，应当统一遵守包括但不限于：在统一遵守在约定范围内处理个人信息；采取有效的技术和管理措施确保个人信息的安全；在发生个人信息泄露时向个人信息主体进行通知并向中国监管机构进行报告、确保自动化决策使用的合规性等义务等要求。 • 境外接收方所享有的豁免性内容：作为受托处理者时，无需向个人信息主体履行个人信息泄露通知义务，转而由个人信息处理者履行该义务。

2. 开展事前监管的不同路径

《决定》允许 SCC 的缔约方对 SCC 进行个性化的修订，但其效力前提为获得数据保护机构的批准。实践中，这种基于对 SCC 的进一步修订所形成的合同条款通常被称之为定制合同（Hoc contract）。目前，如微软、谷歌、亚马逊等科技公司均采用此种定制后的、经过相关数据保护机构批准的数据传输协议模板，此种定制化的传输协议可使得公司在 SCC 的基础上设置灵活性更高的数据保护条款，一方面以更好地保护个人数据，另一方亦可降低自身的违约风险。

《规定》与标准合同本身均为就个人信息处理者与境外接收方是否可以对标准合同进行个性化修订进行说明，亦未说明经过个性化修订的标准合同应当以履行何种程序作为生效前提。其次，针对已经实际投入使用的标准合同，《规定》采取了具有自身特色事前监管方式，即要求个人信息处理者在标准合同生效之日起的 10 个工作日内向所在地省级网信部门进行备案。

个性	欧盟 SCC	我国标准合同
	经过修订后的 SCC 需要经过当地数据保护机构的事前批准	所有标准合同均需经过备案
事前监管的不同方式	• 在不直接或间接地与 SCC 相抵触或损害数据主体的基本权利或自由的前提下，数据出境方与接收方可以自由地将 SCC 纳入更广泛的合同，并增加其他条款或额外的保障措施。 • 针对数据出境方与数据进口方所使用的此种临时定制合同，GDPR 第 57、58 条赋予了各欧盟成员国的监管机构局对其进行批准的职权。	• 《规定》与标准合同本身均为就个人信息处理者与境外接收方是否可以对标准合同进行个性化修订进行说明，亦未说明经过个性化修订的标准合同应当以履行何种程序作为生效前提。 • 针对已经实际投入使用的标准合同，《规定》采取了具有自身特色事前监管方式，即要求个人信息处理者在标准合同生效之日起的 10 个工作日内向所在地省级网信部门进行备案。

在此基础上，我们理解，与欧盟数据保护机构对定制合同进行事前审批的监管方式相比，我国网信部门对标准合同的备案应当被视为一种形式审查机制，其主要目的在于为监管部门后期开展数据跨境治理铺垫基础，并不直接或间接地表明标准合同具有可被修订的空间，亦未在此基础上建立定制化合同的审批机制。

3. 对目的国监管行为的不同监督态度

SCC 第 15 条约定了数据进口方在面临当地监管部门根据目的国法律所提出的执法要求时所应当履行的义务。而标准合同第四条第五款规定，在境外接收方所在国家或地区更改法律或者采取强制性措施导致境外接收方无法履行本合同的情况下，境外接收方方具备立即通知个人信息处理者的义务。我们理解，该通知义务是以“结果”而非“行动”为基础，换言之，《规定》与标准合同并未以境外接收方所在地监管部门实施的数据监管行为本身为基础，规定境外接收方所应当实时采取的、与中国境内个人信息处理者进行及时沟通与协作的相关措施。

个性	欧盟 SCC	我国标准合同
	谨防目的国监管行为对合同履行造成影响	未形成目的国监管行为的监督机制
对目的国监管行为的不同监督态度	数据进口方在面临当地监管部门根据目的国法律所提出的执法要求时，应当： • 通知数据出境方、数据主体及欧盟监管，并在面临禁止通知的当地监管要求时尽最大努力获得豁免； • 审查目的国执法要求的合法性、确认相关执法要求是否在其职权范围内，并在产生质疑时寻求上诉的可能性。	• 在境外接收方所在国家或地区更改法律或者采取强制性措施导致境外接收方无法履行本合同的情况下，境外接收方具备立即通知个人信息处理者的义务。 • 并未以境外接收方所在地监管部门实施的数据监管行为本身为基础，规定境外接收方所应当实时采取的、与中国境内个人信息处理者进行及时沟通与协作的相关措施。

我们理解，我国《个保法》第四十一条在原则上提出了“非经中华人民共和国主管机关批准，个人信息处理者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个人信息”的要求。但是，从文本释义的角度出发，本限制性条款仅适用于个人信息处理者，并不直接适用于境外接收方。因此，可以合理推测的是，在境外接收方实际上作为个人信息受托处理者从中国境内获取了个人信息的情形下，如果境外接收方所在国监管机构根据当地法律向境外接收方开展了数据监管行动，位于中国境内的个人信息处理者可能难以实时知悉和评估相关执法过程个人信息跨境传输所造成的影响。

4. 对约定适用法律与境外司法管辖权的不同态度

就适用法律而言与境外司法管辖权归属上，SCC 在区分四种个人数据跨境传输模式的基础上，附条件允许缔约双方就适用法律与境外司法管辖地进行约定。而我国标准合同第九条第（一）款列明“本合同适用于中华人民共和国相关法律法规”，对于缔约双方是否可选择其他国家法律作为法律适用法未置可否。并且，标准合同第（五）款表明个人信息处理者与境外接收方在产生合同纠纷时，仅可就争议解决的方进行式是为仲裁或诉讼进行选择，但可选择的仲裁机构与司法机构亦基本限缩在中国境内。

个性	欧盟 SCC	我国标准合同
	附条件允许适用法律约定与境外司法管辖地	要求适用中国法并限制境外司法管辖权
对约定适用法律与境外司法管辖的不同态度	• 要求数据出境方与数据进口方在 C-C 模式、C-P 模式及 P-P 模式下仅能在欧盟境内选择适用特定成员国的法律。但在 P-C 模式下，缔约双方则可在达成合意的基础上，超出欧盟这一司法辖区的限制选择适用境外国家法律，但该选择范围的限制性条件为第三方受益人的权利不得受到减损。 • 在 C-C 模式、C-P 模式及 P-P 模式下，SCC 对缔约双方可选择的争议解决地进行了限制，也即数据出境方与数据进口方仅能就特定欧盟成员国的法院进行选择。而在 P-C 模式下，数据出境方与数据进口方亦可就欧盟之外司法辖区的法院进行选择。	• 要求标准合同适用于中华人民共和国相关法律法规。 • 对于双方因合同产生的纠纷以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，应由双方协商解决；协商解决不成的，任何一方可以采取下列第 X 种方式加以解决（如选择）： （1）将争议提交中国国际贸易仲裁委员会等机构进行仲裁，或； （2）依法向中国有管辖权的人民法院提起诉讼。

以上，我们理解，根据《中华人民共和国涉外民事关系法律适用法若干问题的解释（一）》第六条规定：“中华人民共和国法律没有明确规定当事人可以选择涉外民事关系适用的法律，当事人选择适用法律的，人民法院应认定该选择无效”。因此，由于《个保法》等个人信息监管规定并不存在允许个人信息处理活动中相关法律主体在涉外民事关系中自主选择适用法律的相关规定，我们理解，作为下位法的《规定》及标准合同将适用法与司法管辖限制于中国境内，且体现出我国个人信息监管整体环境对涉外司法管辖权所持有的强限制性态度。

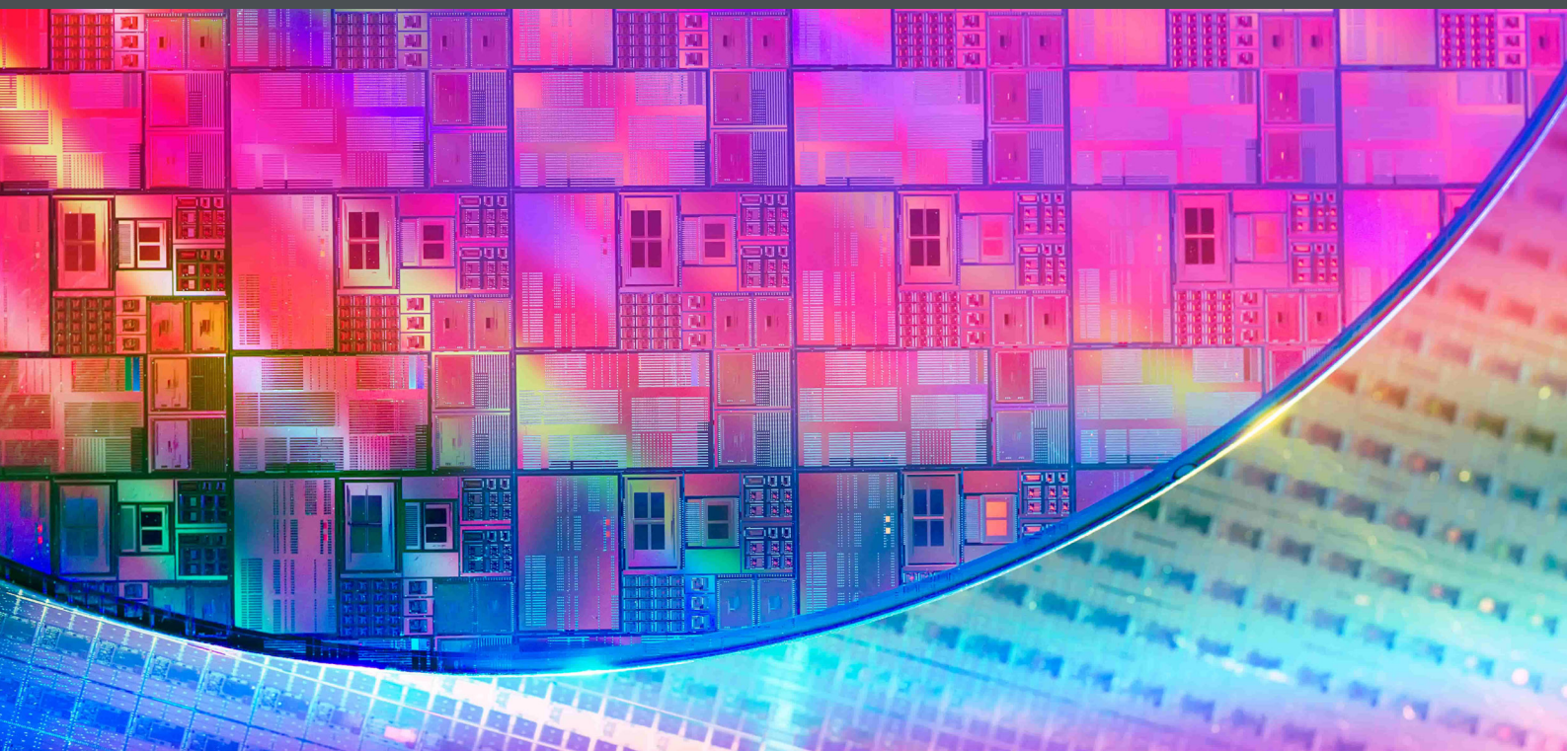
结语

各国数据跨境传输制度不仅是保护个人信息主体权益与社会利益的重要举措，并逐渐成为各国争夺数据主权的国家策略，因此，包括个人信息在内的数据出境活动已不再是以局限于以民事主体自主决策为主的商事活动，其亟待成为我国自上而下的重要监管领域。

作为我国数据跨境传输治理工具的《规定》与标准合同，呈现出我国对数据跨境传输开启“事前 - 事中 - 事后”的全流程监管模式与合理排斥域外法适用及司法管辖的强监管态度。我们期待在征求意见期间，各界能进一步就标准合同的内容与形式提出更多补充性意见，让标准合同更为饱满和充实。

感谢实习生王储对本文作出的贡献。

法律前沿



1. Relevant legislation and competent authorities

1.1 What is the principal data protection legislation?

There are three major principal data protection laws, i.e., the Cybersecurity Law (the "**CSL**"), the Personal Information Protection Law (the "**PIPL**") and the Data Security Law (the "**DSL**").

1.2 Is there any other general legislation that impacts data protection?

Yes. Both the general civil and criminal legislation in China provide requirements on data protection.

In particular, the Civil Code, which took effect on 1 January 2021, establishes the right to privacy and the principles of personal information protection. It mainly provides a definition of personal information and sets out basic requirements for personal information processing, the obligations on the personal information processors and the rights of individ u als to their personal information. Most of the provisions in the Civil Code are restatements of requirements contained in the CSL. National Standards such as the Information Security Technology – Personal Data Security Specification (the "**Standard**") also have an impact on the authorities' enforcement on data protection practices.

The Criminal Law also sets forth offences relating to infringing personal data and privacy, e.g., the offence of infringing citizens' personal information in Article 253-(1), the offence of refusing to fulfil information network security responsibilities in Article 286-(1), and the offence of stealing, purchasing or illegally disclosing other people's credit card information in Article 177-(1). The Interpretation of Several Issues Regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information Handled by the Supreme People's Court and the Supreme People's Procuratorate issued in 2017 provides further explanation regarding the offences relating to infringing personal data and privacy.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. There are various pieces of sector-specific legislation that impact data protection, including but not limited to medical and health, telecommunications, e-commerce and automobiles. For example, the Commercial Bank Law requires banks to keep confidential on depositors' personal savings deposit businesses. The People's Bank of China ("the **PBOC"**) has released the Implementing Measures of the People's Bank of China for Protection of Financial Consumers' Rights and Interests, which provide basic requirements on protection of financial information (including personal information) of individual customers. The Biosecurity Law and the Administrative Regulations on Human Genetic Resources set out requirements on processing of human resource information. The E-commerce Law restates the principle of personal information protection in the field of e-commerce industry. There are also various legal requirements on protection of personal information and data in automobile industry, such as the Several Provisions on Automotive Data Security Management (for Trial Implementation). Furthermore, the Provisions on Protecting the Personal Information of Telecommunications and Internet Users set out obligations of telecommunication and Internet information service providers.

1.4 What authority(ies) are responsible for data protection?

As for personal information protection, China has no single authority responsible for enforcing provisions.

The Cyberspace Administration of China (the "**CAC"**) is responsible for coordinating the protection of personal information and relevant supervision and administration work, while other departments of the State Council, such as the Ministry of Industry and Information Technology (the "**MIIT**"), the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.

For example, the Ministry of Public Security (the "**MPS**") and its local branches are entitled to impose administrative penalties and are also in charge of criminal investigations against the unlawful obtaining, sale or disclosure of personal information.

The MIIT and its local branches are responsible for the supervision and administration of personal information in the telecommunications and Internet sector.

Also, the State Administration for Market Regulation (the

"**SAMR**") and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the Law on Protection of the Rights and Interests of Consumers.

There are also industrial-specific data protection requirements which are mainly enforced by relevant industrial authorities. For example, the PBOC and the China Banking and Insurance Regulatory Commission promulgate and enforce legal requirements on the protection of personal financial information. The National Health Commission and Ministry of Science and Technology supervise the processing of medical and health data.

2. Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal data"**

  Pursuant to the PIPL, personal data/personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding information processed anonymously.

- **"Processing"**

  Pursuant to the PIPL, the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.

- **"Controller"**

  The PIPL does not use the term "controller(s)" to refer to entities that hold or handle personal information. Instead, it names such entities as "personal information processor" considering their engagement in processing personal information. Pursuant to the PIPL, a personal information processor is defined as an organisation or individual that independently determines the purpose and method of the processing of personal information.

- **"Processor"**

  The PIPL does not define "processor" in the same way as under the General Data Protection Regulation ("the **GDPR**"). However, the PIPL sets out the scenario of entrusted processing of personal information, where a personal information processor may entrust an entity with such processing.

- **"Data subject"**

  The PIPL does not define "data subject". However, both the Civil Code and the PIPL provide that a natural person's personal information shall be protected by law. It is widely understood that a natural person/individual identified by the personal information shall be regarded as a data subject.

- **"Sensitive personal data"**

  Pursuant to the PIPL, sensitive personal data/sensitive personal information refers to personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts, as well as the personal information of minors under the age of 14.

- **"Data breach"**

  The CSL, PIPL and DSL do not define "data breach". The National Contingency Plan for Cyber Security Incidents issued by the CAC defines "Cybersecurity incidents", which refers to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. Cybersecurity incidents can be divided into hazardous programme incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents and other incidents.

- **Other key definitions**

  Under the PIPL:

  - "**De-identification**" refers to the process in which personal information is processed so that it is impossible to identify certain natural persons without the aid of additional information; and

  - "**Anonymisation**" refers to the process in which personal information is processed so that it is impossible to identify certain natural persons and cannot be recovered.

3. Territorial scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Under the CSL, relevant authorities are entitled to monitor, prevent and manage cybersecurity risks and threats from other jurisdictions. Pursuant to Article 50, if any information from other jurisdictions is found to be prohibited by law, the CAC and competent authorities may take measures to block the transmission of such information. Pursuant to Article 75, the law applies to an overseas institution, organisation or individual that engages in activity that also endangers Critical Information Infrastructure ("CII"). Further, companies operating under the offshore model but providing services to Chinese clients/users may also be subject to the personal data protection rules established by the CSL, especially those on the cross-border transfer of data. However, the law does not clearly specify how to realise the sanctions. As such, the extent to which these provisions will be enforced abroad against overseas companies remains unclear.

The PIPL provides similar rules to the GDPR regarding its jurisdiction over businesses located outside of China. Article 3 provides that the law shall apply to the processing of personal information of natural persons who are in China under any of the following circumstances, where the processing happens outside of China:

1) where the purpose is to provide domestic natural persons with products or services;

2) where the activities of domestic natural persons are analysed and evaluated; and

3) other circumstances as prescribed by laws and administrative regulations.

Furthermore, according to Article 42 of the PIPL, where an overseas organisation or individual engages in personal information processing activities that infringe upon the personal information rights and interests of citizens of the People's Republic of China or endanger the national security and public interests of the People's Republic of China, the CAC may include such organisation or individual in the list of subjects to whom provision of personal information is restricted or prohibited, announce the same, and take measures such as restricting or prohibiting provision of personal information to such organisation or individual.

The DSL also empowers relevant authorities with the power to investigate the liabilities of entities that process data outside of China that damages the national security, public interest or the legitimate rights and interests of citizens and organisations.

4. Key principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Article 41 of the CSL stipulates that network operators shall make public the rules for collecting and using personal data, and expressly notify the purpose, methods and scope of such collection and use. The same principle has also been included in the PIPL. According to Article 7, the principles of openness and transparency shall be observed in the processing of personal information; the rules for the processing of personal information shall be publicly disclosed, and the purpose, manners and scope of processing shall be explicitly indicated.

- **Lawful basis for processing**

  Article 41 of the CSL and Article 1035 of the Civil Code require network operators to abide by the "lawful, justifiable and necessary" principles when collecting and using personal information. The PIPL similarly requires that the processing of personal information shall follow the principles of lawfulness, legitimacy, necessity and good faith, and processing personal information by misleading, fraud, coercion or otherwise is not permitted.

  Furthermore, Article 13 of the PIPL provides various legal grounds for processing of personal information, including:

  1) the consent of the individual concerned is obtained;

  2) it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resource management in accordance with the labour rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;

  3) it is necessary for the performance of statutory

duties or statutory obligations;

4) it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;

5) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest;

6) processing within a reasonable scope of personal information that is publicly disclosed in accordance with the PIPL; or

7) other circumstances prescribed by laws and administrative regulations.

- **Purpose limitation**

  Article 41 of the CSL requires that network operators shall not collect any personal information that is not related to the services it provides. PIPL similarly requires that the processing of personal information shall be for a definite and reasonable purpose and be directly related to the purpose of processing.

- **Data minimisation**

  Article 6 of the PIPL provides that the processing of personal information shall be conducted in a way that minimises the impact on personal rights and interests, and shall be limited to the minimum scope for achieving the purpose of processing. It is prohibited to excessively collect personal information.

- **Proportionality**

  There is no explicit rule providing for a "proportionality principle" under the CSL or the PIPL, but the data minimisation principle under the PIPL is similar in essence to the "proportionality principle", emphasising "processing of personal data only within a proper and necessary scope", and "shall be conducted in a way that minimises the impact on personal rights and interests".

- **Retention**

  Pursuant to Article 19 of the PIPL, unless otherwise stipulated by laws and administrative regulations, the retention period of personal information shall be the minimum period necessary for achieving the purpose of processing.

- **Other key principles**

  - **Data quality and accuracy** – Article 8 of the PIPL provides that the quality of personal information shall be ensured in the processing of personal information to avoid the adverse impact on personal rights and interests caused by inaccurate or incomplete personal information.

  - **Accountability** – Article 9 of the PIPL requires a personal information processor to be responsible for its processing of personal information and take necessary measures to ensure the security of the personal information processed.

5. Individual rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  Both the Civil Code and the PIPL entitle an individual to consult or copy his/her personal information from a personal information processor.

- **Right to rectification of errors**

  The PIPL provides that where an individual finds that his/her personal information is inaccurate or incomplete, he/she is entitled to request the personal information processor to make corrections or supplements. The Civil Code and the CSL provide similar rules.

- **Right to deletion/right to be forgotten**

  The PIPL requires a personal information processor to delete personal information actively or under the request of relevant individuals in any of the following circumstances:

  1) where the purpose of handling has been achieved, it is impossible to achieve such purpose, or it is no longer necessary to achieve such purpose;

  2) where the personal information processor ceases to provide products or services, or the storage period has expired;

  3) where the individual withdraws his/her consent;

  4) where the personal information processor processes personal information in violation of laws, administrative regulations or the agreement; or

5) other circumstances stipulated by laws and administrative regulations.

- **Right to object to processing**

  Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.

- **Right to restrict processing**

  Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.

- **Right to data portability**

  Pursuant to Article 45 of the PIPL, where an individual requests to transfer his/her personal information to a personal information processor designated by him/her, which meets the conditions stipulated by the CAC, the personal information processor shall provide a way for the transfer.

- **Right to withdraw consent**

  Article 15 of the PIPL provides that where the processing of personal information is based on the consent of the individual concerned, the individual is entitled to withdraw his/her consent. The personal information processor shall provide a convenient method for the individual to withdraw his/her consent.

- **Right to object to marketing**

  Section 8.4 of the Standard stipulates that data subjects have the right not to receive commercial advertisements that are based on their personal data. Furthermore, regarding marketing by means of automated decision making, the PIPL requires the processor to provide convenient rejection ways to relevant individuals.

- **Right protecting against solely automated decision-making and profiling**

  The PIPL provides that where a processor makes use of personal information to make an automatic decision, it shall ensure the transparency of the decision-making and the fairness and impartiality of the results, and shall not impose unreasonable discriminatory treatment on individuals in respect of the transaction price and transaction conditions. In a scenario in which there is information pushing and commercial marketing to an individual through automated decision-making, the processor shall in parallel provide options that do not target the individual's personal characteristics, and provide convenient means of rejection to relevant individuals. On the other hand, an individual shall have the right to require the personal information processor to make an explanation and to reject such explanation only through automatic decision-making where such decision has a significant impact on an individual's rights and interests.

- **Right to complain to the relevant data protection authority(ies)**

  The right for individuals to complain to data protection authorities has been recognised in a number of pieces of legislation. For example, Section IX of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection provides that any organisation or individual has the right to report to the relevant authorities regarding the illegal or criminal conduct of stealing or otherwise unlawfully acquiring, selling or providing to others a citizen's personal electronic information. Further, the CSL provides in Article 14 that one could report acts that endanger network security to the CAC, telecom and public security authorities.

  Under the PIPL, any organisation or individual shall have the right to complain or report illegal personal information processing activities to the authorities performing duties of personal information protection.

- **Other key rights**

  The PIPL protects the rights of close relatives of the deceased. Where a natural person dies, his/her close relatives may, for the purpose of their own lawful and legitimate interests, exercise such rights as consulting, copying, correcting and deleting the relevant personal information of the deceased as prescribed in this chapter, unless otherwise arranged by the deceased prior to his/her death.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There are similar rules under the PIPL. Article 70 of the PIPL provides that where any personal information processor processes personal information in violation of this Law, which infringes upon the rights and interests of a large number of individuals, the People's Procuratorate, the consumer organisations specified by law and the organisations determined by the CAC may bring a lawsuit to a people's court.

6. Children's personal data

6.1 What additional obligations apply to the processing of children's personal data?

Under the PIPL, personal information of children under the age of 14 shall be regarded as sensitive personal information, the processing of which shall be subject to additional legal requirements. Pursuant to Article 31 of the PIPL, processing personal information of children under the age of 14 requires the consent of the children's parents or other guardians, and specialised rules shall be formulated for such processing.

Besides, the CAC has promulgated a special regulation regarding the protection of children's personal information, i.e., the Provisions on the Cyber Protection of Children's Personal Information. Network operators that process children's personal information shall formulate special data protection rules and user agreements and designate persons as responsible for the protection of such information.

7. Registration formalities and prior approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the CSL, PIPL and DSL, transferring personal information or important data abroad may trigger such obligation in certain circumstances. As for operators of CII ("**CIIOs**"), a security assessment shall be conducted pursuant to the measures developed by the CAC and/or competent departments of the State Council, if the personal information or important data generated or collected by them within the territory of China needs to be transferred abroad for business purposes. Personal information processors whose quantity of processing reaches that as prescribed by the CAC will also be subject to such obligation according to the PIPL. As for other personal information processors, there are some other ways provided by the PIPL to compliantly transfer personal information outside China, among which the processors can choose to pass the security assessment organised by the CAC.

According to the DSL, processors of important data shall, in accordance with the relevant provisions, carry out risk assessments on their data processing activities on a regular basis and submit a risk assessment report to the relevant competent authority. On an industrial-specific basis, the CAC has issued a regulation on the security protection of automotive data, in which the CAC requires that an automotive data processor shall conduct risk assessments and submit an assessment report to the cyberspace administration at provincial level and other relevant authorities for its processing of important data. Such processor is further required to submit its annual automotive data security management report to these authorities by December 15 of each year. Furthermore, the international transfer of important data by the processor shall also be subject to the assessment organised by the CAC and relevant authorities.

The CAC also sets out legal requirements on the application of algorithm recommendation technologies for provision of Internet information services, where an algorithm recommendation service provider with public opinion attribute or social mobilisation ability shall, within 10 working days from the date of provision of services, go through record-filing formalities.

Additionally, where the processing of data raises national security issues, such activities may further trigger a cybersecurity review. According to the Cybersecurity Review Measures released by the CAC and a number of other national departments, the purchase of network products and services by CIIOs and the data processing activities carried out by online platform operators, which affect or may affect national security, shall be notified to the relevant authorities for cybersecurity review. Online platform operator holding personal information of more than 1 million users shall also declare for cybersecurity review when they enter into an initial public offering ("**IPO**") in other countries.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

For the security assessment of international transfer of personal information and important data, according to relevant draft regulations, the notification is designed to be specific, covering various aspects such as legitimacy, fairness, necessity of the transfer, categories, quantity, sensitivity of the data, security risk, etc.

The report by automotive data processors is also required to be specific. Processors are requested to provide details of the processing activities, such as the type, scale, purpose, and necessity of the processing of

automotive data, the measures for security protection and management of automotive data, provision of automotive data to third parties, data security incidents and the handling thereof, etc.

The filing of algorithms needs to be conducted via the Internet information service algorithm record-filing system operated by the relevant authorities, where detailed information such as the service provider's name, service form, application field, algorithm type, algorithm self-assessment report and content shall be provided.

The cybersecurity review is also conducted in a detailed manner. Relevant data processors need to file (including but not limited to) an assessment report analysing in detail the risk factors concerning national security.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

For international data transfer, according to relevant draft regulations, the assessment has a two-year period of validity. When such period expires, the assessment shall be renewed. Furthermore, during the two-year period, the assessment will need to be renewed if: (i) any change occurs to the purpose, method, scope, or type of the data to be transferred, or the use or method of data processing by the overseas recipient, or the period for overseas storage of personal information and important data is extended; (ii) there is any change in the legal environment of the country or region where the overseas recipient is located, any change in the actual control of the data processor or the overseas recipient, or any change in the contract between the data processor and the overseas recipient that may affect the security of the outbound data, or other circumstances affecting the security of outbound data; or (iii) there are other circumstances that have an impact on the security of data transfer.

For automotive data, each processor (who conducts important data processing) is required to file a report of its overall automotive data processing activities. Similarly, the filing of algorithms shall be conducted by each relevant service provider, and if any change occurs to the information filed, the service providers shall make modifications within 10 working days.

As for cybersecurity review, as mentioned above, the review process is initiated when a CIIO purchases network products and services that affect or may affect national security, or when an online platform operator's certain data processing activity affects or may affect national security, or when an online platform operator holding personal information of more than 1 million users enter into an IPO in other countries.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to questions 7.1 and 7.3.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to question 7.2.

7.6 What are the sanctions for failure to register/ notify where required?

CIIOs that fail to notify their cross-border transfer of personal information and important data, according to the CSL, shall be warned and ordered by the competent authority to make rectifications, and shall be subject to confiscation of illegal earnings and a fine ranging from RMB 50,000 to RMB 500,000, and may be subject to a suspension of related business, winding up for rectification, shutdown of website, and revocation of business licence, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000. As for personal information processors, pursuant to the PIPL, the authorities may order them to make corrections, give a warning to them and confiscate their illegal gains. If they refuse to make corrections, a fine of not more than RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made

to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data processor failing to report may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes serious consequences such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

With respect to any algorithm recommendation service provider with the attribute of public opinions or the ability to mobilise the public who has obtained record-filing by concealing relevant information, providing false materials or other improper means, its record filing shall be revoked, a warning given, or a notice of criticism circulated; if the circumstances are serious, it shall be ordered to suspend information updating and impose a fine of not less than RMB 10,000 but not more than RMB 100,000.

CIIOs using products and/or services that have not undergone or have failed in the security review shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than one but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000.

7.7 What is the fee per registration/notification (if applicable)?

Currently, it remains unclear. Normally, such notifications are free of charge.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to questions 7.1 and 7.3.

7.9 Is any prior approval required from the data protection regulator?

For the international data transfers mentioned in question 7.1, it is widely recognised that prior approval is required, where applicable. As for important data processing, there is no requirement of prior approval in the DSL. The same goes with the filing of algorithms.

For cybersecurity review, it is understood that prior approval is needed.

7.10 Can the registration/notification be completed online?

The filing of algorithms is conducted online. It remains unclear whether other notifications can be completed online.

7.11 Is there a publicly available list of completed registrations/notifications?

Since the laws and regulations are newly issued, currently there is no public channel established to list completed notifications.

7.12 How long does a typical registration/notification process take?

For the security assessment of international data transfers, the draft regulations provide that the CAC shall complete a security assessment of outbound data within 45 working days commencing from the date of issuing the written notice of acceptance; if the circumstance is complex or supplementary materials are required, the said time limit may be extended appropriately, but generally shall not exceed 60 working days.

For the filing of algorithms, relevant authorities shall, within 30 working days upon receipt of the record-filing materials submitted by the record-filing applicants, grant record-filing, issue record-filing numbers and make public the record-filing; if the materials are incomplete, record-filing shall not be granted, and the record-filing applicant shall be notified, with reasons stated, within 30 working days.

The cybersecurity review follows a period of "30+15+15" working days for an ordinary review procedure. Where a special procedure is needed, the review shall generally be completed within 90 working days, and the time limit may be extended for complicated cases.

8. Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PIPL, where the quantity of personal

information processed reaches that specified by the CAC, the personal information processor shall designate a person in charge of personal information protection to be responsible for supervising the activities of processing of personal information and the adopted protection measures. Currently, the threshold is yet to be made public.

Under the DSL, processors of important data shall specify the person(s) responsible for data security and the management body, and implement the responsibility of data security protection.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Under the PIPL, the authorities may order the processor to make corrections, give a warning to it and confiscate its illegal gains. If it refuses to make corrections, a fine of not more than RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data processor failing to appoint a data security officer may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes serious consequences such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If a Data Protection Officer ("**DPO**") fails to perform his or her duty with due diligence, then he or she may be accused of administrative or even criminal liabilities in respect of his or her role as a DPO.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law and relevant rules do not specify whether a business can appoint a single DPO to cover multiple entities.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Section 11.1 of the Standard specifies that the DPO shall be a person with relevant management experience and professional knowledge of personal information protection.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please refer to the response to question 8.1. Furthermore, Section 11.1 of the Standard provides that the DPO's responsibilities include but are not limited to:

1) direct responsibility for, and comprehensive and overall implementation of, the organisation's personal data security;

2) organising the formulation of a personal information protection work plan and supervising its implementation;

3) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;

4) establishing, maintaining, and updating the list of personal data held by the organisation (including the type, amount, origin, recipient, etc. of the personal data) and authorised access policies;

5) conducting a personal data security impact assessment, proposing countermeasures and suggestions for personal information protection, and urging the rectification regarding security risks;

6) organising personal data security training;

7）conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data;

8）announcing information such as complaint or reporting methods and promptly accepting the complaint and report;

9）conducting safety audits; and

10）communicating with supervisory authorities, and reporting on personal information protection and incident handling, etc.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Under the PIPL, yes. The personal information processor shall make public the contact information of the person in charge of personal information protection and submit their name and contact information to the authorities.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. Please refer to question 8.7.

9. Appointment of processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Under the PIPL, where a personal information processor entrusts others with the processing of personal information, it shall agree with the agent on the purpose, time limit and method of entrusted processing, type of personal information and protection measures, as well as the rights and obligations of both parties, and supervise the personal information processing activities of the agent.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Please refer to question 9.1.

10. Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Pursuant to Article 43 of the Advertisement Law, no organisation or individual shall, without obtaining the consent or request of the parties concerned, distribute advertisements to them via electronic means. Advertisements distributed via electronic means shall state the true identity and contact details of the senders, and the method for the recipients to refuse acceptance of future advertisements. Article 44 further provides that advertisements published in the form of pop-up windows on the website shall show the “close” sign prominently.

Article 13 of the Administration of Internet Electronic Mail Services provides that the word “advertisement” or “AD” must be indicated in the email subject, and it is prohibited to send emails containing commercial advertisement without the express consent of the receivers. Article 14 provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such emails, the sender shall stop sending such emails, unless otherwise agreed by the parties. The receivers shall be provided with the contact details for the discontinuation of the receipt of such emails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The Advertisement Law as well as the Administration of Internet Electronic Mail Services Procedures do not specify whether they are only applicable to business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Section VII of the Decision of the Standing Committee of the National People’s Congress on Strengthening

Network Information Protection provides that any organisation or individual shall not send commercial electronic messages to the fixed-line, mobile telephone or email inbox of an electronic message receiver without the prior consent or request of the receivers or if the receivers explicitly express rejection.

The operators of an e-commerce platform, when displaying search results of goods or services, shall mark "advertisement" for bid-ranked products or services, pursuant to Article 40 of the E-commerce Law. Furthermore, Article 18 provides that e-commerce business operators who provide search results based on consumers' preference or consumption habits shall in the meantime provide options not targeting consumers' personal characteristics.

As for marketing by means of automated decision making, the PIPL requires the relevant processor to provide options not specific to individuals' characteristics simultaneously, or provide methods for individuals to refuse such marketing or push.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Advertisement Law and the E-commerce Law apply to operators providing products and services within the territory of China, while for foreign operators providing products or services to China on an offshore model, the law does not further elaborate whether it will apply or not. However, according to Article 3.2 of the Draft Security Assessment Guidelines on Cross-border Data Transfer, business operators not registered in China but providing products or services to China using the Chinese language, making settlement by the RMB, and delivering products to China are considered to be "providing products or services to China", in which case it is possible that the relevant provisions will apply.

The PIPL applies to the processing of personal information of natural persons within China for the purpose of providing products or services to them or analysing or assessing their conduct. Therefore, marketing sent by a personal information processor from other jurisdictions could be subject to the PIPL if it falls into the cases above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Administration for Market Regulation is mainly responsible for the enforcement of marketing restrictions. There are recent cases where authorities such as the Administration for Market Regulation are taking action. For example, in 2017, Shanghai Paipaidai Financial Information Service Co., Ltd. was fined RMB 800,000 for its infringement of the Advertisement Law, the breaches including, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

If the source of the marketing lists is legitimate and lawful and the data subject has consented, then it is not prohibited. Otherwise, it is illegal to do so, as network service providers and other enterprises, public institutions and their employees are obligated to keep strictly confidential a citizen's personal electronic information collected during their business activities, and may not disclose, falsify, damage, sell or illegally provide such information to others, as provided in the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 63 of the Advertisement Law provides that sending direct marketing communications without obtaining the consent of the target may result in a fine of up to RMB 30,000.

E-commerce platforms that do not clearly mark "advertisement" for bid-ranked products may face a fine of up to RMB 100,000, pursuant to Article 81 of the E-commerce Law and Article 59 of the Advertisement Law.

In addition, Article 77 of the E-commerce Law provides that e-commerce business operators who provide search results in violation of Article 18 as described in question 10.3 shall be ordered to make the correction within a stipulated period, their illegal income shall be confiscated, and a fine ranging from RMB 50,000 to RMB 200,000 may be imposed. In serious cases, a fine ranging from RMB 200,000 to RMB 500,000 should be imposed concurrently.

As for the penalties under the PIPL, please refer to question 8.2.

11. Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no legislation addressing the use of cookies explicitly. Given that cookies may fall within the definition of personal information, it is understood that the general regulations on personal data apply to the use of cookies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The law does not distinguish between different types of cookies at this stage.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There are no administrative actions on the use of cookies. Nonetheless, in 2015, the search engine Baidu's use of cookies to personalise advertisements aimed at consumers when they enter certain third-party websites was found by the court not to infringe an individual's right to privacy.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please refer to the maximum penalties for other general breaches.

12. Restrictions on international data transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The CSL, PIPL and DSL have set out requirements on international data transfer. For restrictions on international transfer of personal information and important data, please refer to questions 7.1–7.12.

In October 2021, the CAC issued an updated draft regulation, i.e., the Draft Measures for the Security Assessment of Cross-border Data Transfer, according to which data processors are required to conduct security assessment when they provide important data collected and generated overseas during their operation within the territory of the People's Republic of China and personal information that shall be subject to security assessments according to law. The draft regulation is still under review by the relevant authorities and may be subject to further revision.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The PIPL provides several methods that a business can adopt to compliantly transfer personal information abroad, including the following:

1) passing the security evaluation organised by the CAC (for CIIOs and processors whose quantity of processing of personal information reaches that as prescribed by the CAC);

2) obtaining certification by a specialised agency for protection of personal information in accordance with the provisions of the CAC;

3) entering into a contract with the overseas recipient under the standard contract formulated by the CAC, specifying the rights and obligations of both parties; or

4) meeting other conditions prescribed by laws, administrative regulations or the CAC.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In certain circumstances, prior notification or approval is needed. As mentioned in Section 7, CIIOs and personal information processors, whose quantity of processing personal information reach that as prescribed by the CAC, shall pass the security assessment organised by the CAC when transferring personal information collected within China abroad. According to the Draft Measures for the Security Assessment of Cross-border Data Transfer, if a personal information processor has processed personal information of more than 1 million people, or if it has transferred personal information of more than 100,000 people or sensitive personal information of more than 10,000 people overseas accumulatively, the transfer by such processor shall be subject to security assessment.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

This is not applicable.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

This is not applicable.

13. Whistle-blower hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PIPL provides that any organisations and individuals shall have the right to file complaints or reports about illegal personal information processing activities with relevant authorities. The authorities receiving complaints or reports shall handle them without delay and notify the complainants and informants of the handling results.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The PIPL does not explicitly prohibit anonymous reporting. Anonymous reporting is generally permitted.

14. CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Article 12 of the Public Security Video Image Information System Administrative Regulations (exposure draft, hereinafter the "**CCTV Regulations**"), which was issued by the MPS and regulates the use of CCTV for public safety purposes, stipulates that anyone who uses CCTV for public safety purposes shall notify the local public security department of the type and location of the camera installed.

14.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to Article 6 of the CCTV Regulations, it is prohibited to obtain state secrets, work secrets or trade secrets from a public security video image information system, or infringe on citizens' privacy by using such a system. Organisations that construct and use CCTV are required to keep in confidence the basic information (e.g., the system design, equipment type, installation location, address code) and collected data concerning state secrets, work secrets and trade secrets and shall not illegally disclose CCTV data concerning citizens' privacy. Such CCTV data shall not be bought or sold, illegally used, copied or disseminated, pursuant to Article 22. According to Article 21, investigative, procuratorial and judicial powers, public security and national security organs, as well as the administrative departments of the government at or above town level, may inspect, copy or retrieve the basic information or data collected through CCTV. Under circumstances of the security services, Article 25 of the Regulations on Administration of Security Services provides that the using of CCTV equipment shall not infringe on the legitimate rights and interests or privacy of individuals.

It is worth noting that the PIPL provides restrictions on image capturing, and personal identification equipment installed in public places. Such data collection activities shall be necessary for maintaining public security, comply with the relevant provisions of the State, and conspicuous prompting signs shall be set up. An individual's personal image and personal identification information collected may only be used for the purpose of maintaining public security and shall not be used for any other purpose, except with the individual's separate consent.

15. Employee monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

On the one hand, Article 8 of the Labour Contract Law provides that employers are entitled to know about basic information of the worker in direct relation to the labour contract between them; therefore, some types of employee monitoring are permitted, though no specific rule explicitly addresses employee monitoring. On the other hand, it is prudent that the monitoring does not

infringe the employee's privacy.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the PIPL, consent may not be needed if the processing of personal information is necessary for the implementation of human resources management in accordance with the internal labour rules and regulations and the collective contract concluded. While the processing of employees' personal information exceeds the human resource management scope, consent is still needed unless the processing falls in other legal bases as prescribed in Article 13 of the PIPL.

In practice, employers usually choose to add a provision in the labour contract or in the employee handbook or similar documents to inform employees of the processing of their personal information, and where necessary, to obtain their consent.

15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Article 4 of the Labour Contract Law requires employers to discuss with the employee representatives' congress or all employees, and negotiate with trade unions or employee representatives when formulating, revising or deciding on matters directly involving the vital interests of workers such as remuneration, working hours, rest periods and days off, labour safety and health, insurance and welfare, staff training, labour discipline and labour quota administration, etc. Article 43 further provides that employers shall notify the trade union when they unilaterally rescind a labour contract. However, such notifying or negotiating circumstances may not directly relate to employers' monitoring or processing of employees' personal data.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

If consent has been obtained from such employee, then yes. If the employer attempts to process such information without obtaining consent, it may go with the legal ground of "necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency". In spite of this, it is worth noting that whether an employer could process an employee's such information on the legal ground other than consent shall be assessed on a case-by-case basis.

16. Data security and data breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Under Article 40 of the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of personal data they collect, and to establish and improve the system for user information protection. However, if the network operator as a controller appoints a third party to process personal data on its behalf, it shall ensure that such processor will provide an adequate level of protection to the personal data involved, as provided in Section 8.1 of the Standard.

The PIPL provides in its Article 9 that the personal information processor shall be responsible for its processing of personal information and take necessary measures to ensure the security of the personal information processed. For the definition of personal information processor in the PIPL, please refer to question 2.1.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Under Article 42 of the CSL, in case of (possible) divulgence, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority.

Under the PIPL, where personal information has been or may be divulged, tampered with or lost, the personal information processor shall immediately take remedial measures and notify the relevant authorities and the individuals concerned. The notice shall include the following matters:

1) the types, reasons and possible harm of the information that has been involved or may be involved in the divulgence, tampering with or loss of personal information;

2) the remedial measures taken by the personal information processor and the measures that can be taken by the individuals to mitigate harm; and

3) the contact information of the personal information processor.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, please refer to question 16.2. Furthermore, according to the PIPL, where the personal information processor has taken measures to effectively avoid harm caused by divulgence, tampering with or loss of information, the personal information processor may opt not to notify the individuals concerned. If the authorities performing duties of personal information protection believe that harm may be caused, they may require the personal information processor to notify the individuals concerned.

16.4 What are the maximum penalties for data security breaches?

Under Article 64 of the CSL, in case of severe violation, an operator or provider in breach of data security may face fines of up to RMB 1 million (or 10 times the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any website(s) and revocation of a business licence. The persons directly in charge may face a fine of up to RMB 100,000.

As for the penalties under the PIPL, please refer to question 8.2.

17. Enforcement and sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The PIPL has defined the scope of the "authorities performing duties of personal information protection", including the following:

1) the CAC, which is responsible for coordinating the protection of personal information and relevant supervision and administration work;

2) other relevant national departments (such as the MIIT, the MPS, and the SAMR), which are responsible for protecting, supervising and administering the protection of personal information within the scope of their respective duties; and

3) relevant departments of local people's governments at or above the county level.

These authorities perform the following data protection duties:

1) carrying out publicity and education on personal information protection, and guiding and supervising personal information processors to protect personal information;

2) accepting and handling complaints and reports related to personal information protection;

3) organising the evaluation of applications and other organisations on the protection of personal information, and disclosing the evaluation results;

4) investigating and handling illegal personal information processing activities; and

5) other duties stipulated by laws and administrative regulations.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, and no court order is needed. For example, pursuant to Article 50 of the CSL, if any information prohibited by laws and administrative regulations from release or transmission is found, the CAC and other competent authorities may require the network operator to stop the transmission of such information, take measures such as deletion and keep the records. If any such information is from overseas, they may block the transmission.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CAC and relevant data protection authorities may issue a ban in the form of an administrative penalty, together with other punitive measures such as a fine, an order to rectify, etc. In the recent special rectification action on app providers, the CAC, MIIT and its local branches usually issue a list of app providers and describe their illegal processing of personal information (such as excessive collection, lack of notification to users), and in cases where the app providers fail to make rectifications, the CAC, MIIT and relevant authorities may

even request the apps to be removed from app stores.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

So far, there is no public record of Chinese data protection authorities exercising their powers directly against companies established in other jurisdictions. In most cases, authorities may talk with the local subsidiary of an international company for its violations of the CSL or other data protection regulations.

18. E-discovery / Disclosure to foreign law enforcement agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Both the PIPL and DSL prohibit processors of personal information/data from providing personal information/data to foreign judicial or law enforcement authorities without the approval of competent authorities. If there are treaties or agreements in relation to judicial assistance or cooperation entered into between China and the respective foreign country, the relevant companies may respond to such requests following such treaties or agreements. Any entity or responsible person in violation of such requirement may be subject to administrative penalties.

18.2 What guidance has/have the data protection authority(ies) issued?

The CAC has not issued any guidance particularly concerning e-discovery requests from foreign law enforcement agencies.

19. Trends and developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As mentioned in Section 8, regulations on automotive data processing and algorithm recommendation services have been the major enforcement focus of the CAC in recent years. In terms of the automotive data, it is said that the CAC has conducted a pilot project regarding the annual report of automotive data security management by automotive data processors. Regarding the filing of algorithms, the CAC has recently launched the algorithmic filing system which has been available since March 1, 2022. It is expected that algorithm recommendation service providers file information regarding the algorithms they applied through this system.

Cross-border data transfer is another point of the CAC's recent enforcement activities. As mentioned above, the Draft Measures for the Security Assessment of Cross-border Data Transfer issued in October 2021 aim to specify the rules and procedures on restrictions of cross-border data transfer. Meanwhile, it is said that the CAC is preparing the standard contract that can be used by companies to ensure that the transfer of personal information is compliant with relevant laws.

Furthermore, the cybersecurity review is also a hot topic. In July 2021, the Cybersecurity Review Office, a unit of the CAC, announced the cybersecurity review into a well-known ride-hailing company Didi, which has set a precedent for how the government will handle national security issues related to cybersecurity and data. Meanwhile, the updated Cybersecurity Review Measures have added that online platform operators holding personal information of more than 1 million users shall declare for cybersecurity review when they enter into IPOs in other countries. Since then, companies seeking to enter into an IPO overseas shall pay additional attention to the requirements on cybersecurity and evaluate whether their activities may raise national security concerns.

19.2 What "hot topics" are currently a focus for the data protection regulator?

Please refer to question 19.1.

CHAMBERS - CYBERSECURITY 2022 (CHINA)

1. Basic national regime

1.1 Laws

The Civil Code of the PRC (Civil Code) is a periodic legislative response to the problem of personal information (PI) protection. The personality rights chapter of the Civil Code adopts a special section to provide protection on both PI and privacy right, recognising the personality attributes of PI. In addition, the Civil Code preliminarily stipulates the definition and types of PI, the legal basis for processing PI, and the rights of PI subjects, etc. The provisions on PI are periodical and general, therefore remaining to be further refined and implemented by subsequent legislation.

As compared to the scattered provisions set forth by the Civil Code, the Cybersecurity Law (CSL) of the PRC acts as the overarching construct of the cybersecurity regime in China and sets forth specific requirements in various cybersecurity segments. The CSL applies to network operators (NOs) in China, a term defined as any entities that own or administer a network or provide network services, setting forth liabilities of violation in the form of fines and injunctions against the network operators and/or their responsible personnel.

The subject matter regulated by the CSL, supplemented by relevant regulatory documents (including drafts), can be summarised in two main categories: (i) network operation security, which addresses the security of operation, structure and management of a network system; and (ii) network information security, which mainly focuses on measures and structural arrangements to protect PI and important data. The specific requirements of the two categories can be divided into the following major segments.

In addition, the Data Security Law (DSL), which was released on 10 June 2021 and came into effect on 1 September 2021, articulates specific security requirements for data processing. The DSL for the first time explicitly articulates extra-territorial jurisdiction in the Chinese data regulation regime, applying to overseas data processing activities that jeopardise China's national security or the interests of the state or citizens. The DSL contemplates a variety of state data protection mechanisms from an overarching architecture perspective, such as classified data protection system, state data security certification and standardisation, data transaction system, state open data system, and others, with implementation measures to be later promulgated by state and municipal regulatory authorities.

Lastly, the Personal Information Protection Law (PIPL), which was released on 20 August 2021 and became effective on 1 November 2021, building upon the general principles and rules established under the CSL, provides detailed personal information protection requirements. The PIPL, while recognising consent is still the cornerstone of personal information processing activities, provides other lawful bases, such as the necessity for enacting and performing contracts in which the individuals are a party. Additionally, the PIPL put forward requirements in sensitive personal information protection, cross-border transfer, personal information protection impact assessment, compliance audits, separate consent and liabilities.

The CSL, the DSL and the PIPL form the three "pillars" of China's cybersecurity and data protection regime. Moving forward, we expect a series of implementing regulations, measures, and standards to be drafted and finalised.

Network operation security

Multi-level protection scheme (MLPS)

A classified cybersecurity protection scheme (also known as the multi-level protection scheme or MLPS) is recognised as the basic legal system to ensure structural network security in China. Under the MLPS, network operators must be classified by one of five levels according to their security impact if the system is damaged, with classification levels ranging from one to five. Progressively stringent requirements for network security and filing obligations with authorities

are imposed on network operators at higher MLPS classification levels. Please refer to **4.3 Critical infrastructure, networks, systems** for further details of MLPS.

Security requirements

Certain security requirements are imposed on the suppliers of network products and services, such as taking remedial actions to correct security vulnerabilities and continuing provision of security maintenance services. Any identified key network equipment and specialised cybersecurity product must pass security certification before being put into the market. Network product suppliers and organisations or individuals who detect, collect and publish security vulnerabilities of network products (Vulnerabilities Publishing Platforms) are obligated to report any identified security vulnerabilities to the National Vulnerabilities DataBase. NOs are also encouraged to report such vulnerabilities. Please refer to **5.7 Requirements for secure software development**, 'Network product security' for further details of the security vulnerabilities.

Critical information infrastructures (CIIs)

Critical information infrastructures (CIIs) are defined as important network facilities and information systems, in industries and sectors such as: telecommunications and information services; energy; transportation; water conservancy; finance; public service; e-government; national defence; science, as well as any other important network facilities and information systems that may severely endanger national security, social welfare and public interests upon sabotage, malfunction or data breach. CIIs are afforded additional and strict security protection requirements and there are obligations regarding security management mechanism, training, technical measures of cybersecurity protection, procurement of network products and services, emergency response plans, and others. As a fundamental principle, protection measures shall be implemented simultaneously when designing, setting-up and using the CIIs.

In addition, in the event that procuring network products and services by CII operators (CIIOs) may affect national security, competent authorities must conduct cybersecurity review of such procurement.

Monitoring, etc

Network operators shall set up cybersecurity monitoring, early warning and emergency response plans to mitigate cybersecurity risks and timely notify relevant parties upon the occurrence of cybersecurity incidents.

Network information security

Legitimate processing

NOs shall process (collection, storage, use, handling, transfer, provision, disclosure, deletion, etc) personal information lawfully, legitimately, in good faith, and only to the extent necessary, and obtain informed consent from the PI subjects regarding the purpose, methods and scope of processing. NOs shall also take necessary measures to ensure the security of PI it collects and promptly inform PI subjects and relevant authorities upon discovering possible or identified PI security incidents.

NOs shall take measures to respond to legitimate request from PI subjects related to their PIs. In particular, based on the PIPL, depending on their different roles in PI processing, NOs are categorised as personal information processors (PIPs) – defined as any entity or individual capable of determining the purpose and method of PI processing – and entrusted processors (EPs) – defined as entities or individuals processing PI on behalf of PIPs.

When PI contains sensitive personal information (SPI), additional security requirements are imposed on PIPs, such as obtaining separate consent and encryptions. Please see **4.1 Personal data** for details of PI protection requirements for NOs, PIPs and EPs.

Important data

Important data refers to data that may potentially harm national security, economic security, social stability, public health and security, which might include undisclosed government information, information regarding mass population, genetic health, geographical and mineral resources, as well as production and operation information of CIIs. Entities responsible for processing important data are subject to various security obligations under DSL, such as conducting periodic risk assessments and filing the relevant reports as well as adopting technical measures, such as encryption, back-up and monitoring. The scope of important data will be defined by regulatory authorities of different industries and regions in upcoming legislations. Please see **4.2 Material business data and material non-public information** for details on important data protection requirements.

Cross-border data transfer

CIIOs must store PI and important data within China and obtain the approval on an authority-led security assessment before transferring such data out of China. PIPs, who processed personal information reaching a threshold to be determined by the Cyberspace Administration of China (CAC), are subject to the same localisation and security assessment requirement. Data processors, defined as those with ability to determine the purposes and means of data processing activities, similarly are subject to the security assessment requirement.

According to the current draft regulations on cross-border data transfer, data processors shall conduct a self-risk assessment before transferring PI and important data cross-border. The self-risk assessment and the authority-led security assessment may cover the nature of data to be transferred, the data recipient's data security protection abilities, the security measures taken to protect data in-transit, the receiving country or region's political and legal environment of data protection, and evaluation of the impact to PI subjects, national security and social interests by such transfer, etc. Cross-border data transfer is prohibited if it threatens national security or public interests. For detailed cross-border data transfer descriptions, please see "Cross-border data transfer" under **3.1 De Jure or De Facto standards**.

The CSL and relevant regulatory documents are mainly enforced by the CAC, the Ministry of Industry and Information Technology of China (MIIT), the Ministry of Public Security of China (MPS), and the State Administration for Market Regulation (SAMR). It is worth mentioning that regulatory documents in drafts are commonly applied as an important reference for cybersecurity enforcement.

State secrets

The Guarding State Secrets Law of PRC ("State Secrets Law") classifies state secrets into three tiers and articulates respective protection requirements, which generally prevail over other data protection requirements when data is identified as a state secret.

Restrictions on state activities

Under DSL and other implementing regulations, governmental authorities bear confidentiality obligations with respect to the personal information, trade secret and other business confidential information disclosed by NOs.

Other laws and regulations

Various other laws and regulations also contribute to other segments of the cybersecurity regime as illustrated below.

The Cryptography Law

The Cryptography Law, mainly enforced by the Cryptography Administration of China (SCA), sets forth requirements for supplying and adopting various encryption, in particular the commercial encryption which plays a key role in network security required by the CSL. The law also sets forth the civil liabilities of violation.

The Provisions on the Ecological Governance of Network Information Contents

The Provisions on the Ecological Governance of Network Information Contents takes network information contents as the main governance objects, and, by aiming at establishing and perfecting a comprehensive network governance system, creates a clean cyberspace and builds a sound network ecosystem.

The Criminal Law

The Criminal Law of the People's Republic of China (Criminal Law) recognises the various cybercrimes infringing PI or computing systems and crimes utilising networks, and the crime of failure to perform cybersecurity obligations, punishable by imprisonment and/or fines. The above-mentioned Criminal Law provisions are enforced by MPS and its local agencies.

1.2 Regulators

All key regulators of cybersecurity in China – namely the CAC, MIIT, MPS and SAMR – have regulatory authorities at the national level and their branch agencies at the county level or above that exercise their authorities within their respective geographic jurisdiction, including audits and investigations of NOs regarding violation of cybersecurity-related laws and regulations.

CAC has the overarching responsibility of planning and co-ordinating cybersecurity regulation. It is the most active regulator in terms of enacting cybersecurity regulatory documents, and its enforcement focuses on the governance of the "internet ecology" and network information content.

The MPS is the key regulator and enforcement authority of the MLPS and network operation security, and

responsible for investigating and preventing crimes related to computing system and PI infringement.

The MIIT oversees the telecommunication and information technology industry and thus administers the licences of the market participants in this industry. Its enforcement focuses on PI protection, especially telecommunication value-added services.

The SAMR is responsible for the protection of consumer rights, including consumers' rights in PI and fair market competition.

In addition to the four key regulators, some national regulators focus on specific areas of cybersecurity-related matters, as detailed below.

- The National Security Commission of the Communist Party is responsible for overseeing and formulating state data security strategies under DSL.
- The Ministry of State Security (MSS) is responsible for safeguarding national security of data processing activities.
- The National Information Security Standardisation Technical Committee (TC260) is responsible for the promulgation of cybersecurity-related national standards.
- The National Administration of State Secrets Protection (NASSP) is responsible for MLPS classification and protection related to state secrets.
- The SCA is responsible for regulation and enforcement in relation to encryption activities.
- The China Securities Regulatory Commission (CSRC), the China Banking and Insurance Regulatory Commission (CBIRC), the China Insurance Regulatory Commission (CIRC) and the China Banking Regulatory Commission (CBRC) also regulate cybersecurity matters in their respective financial areas.

1.3 Administration and enforcement process

In general, the penalties that cybersecurity regulators or data protection authorities impose on the investigated entities or individuals must comply with the liabilities articulated by the CSL, the DSL, the PIPL and, in case where criminal culpability arises, the Criminal Law.

As for regulator-specific administrative process, the Provisions on Internet Security Supervision and Inspection by Public Security Organs (Public Security Provisions) set forth the standard administrative process of cybersecurity enforcement by the MPS and its branch agencies. The Public Security Provisions limit the scope of the targeted network service providers and the contents of supervision and investigation by public security agencies. It also articulates two methods of supervision and investigation, namely on-site inspection and remote inspection, and sets forth procedural requirements for each method.

Other due process and appeal rights issues not contemplated by the above-mentioned laws and regulations shall, in theory, apply the administration laws of China, namely the Administrative Penalty Law, the Administrative Reconsideration Law, the Administrative Litigation Law, etc. In practice, we are not aware of any remedies under the aforementioned administration laws initiated by respondents. Thus, further observation is advised regarding the applicability of the administration laws to cybersecurity-related administrative process and enforcement.

1.4 Multilateral and subnational issues

Currently, most cybersecurity enforcement actions are based on laws and regulations at the national level. Regulations at provincial or municipal level are comparatively limited in number and lack uniformity and consistency in subject matter and legal effectiveness. Although, such regional regulations may only specify but not exceed the requirements already contemplated by the CSL, these regional regulations can shed lights in interpreting the CSL. For example, the Shanghai Public Security Bureau issued the Administrative Penalty Guidance of Cybersecurity Management, setting detailed rules for issuing administrative penalties for violations of the CSL.

Agencies at the subnational level play a piloting and critical role in cybersecurity enforcement activities. For example, the Beijing Cyber Police Department in 2021 launched administrative inspections and issued penalties concerning cybersecurity for 2,775 companies. The Cyber Police Departments of Shanghai and Shenzhen are also very active in launching such inspections on companies of all sizes, including multinational corporations. Furthermore, following the effectiveness of the PIPL, enforcement actions have expanded to include public interest class actions initiated by local Procuratorates. On 1 November 2021, the Hangzhou Internet Court issued its decision for a public interest class action brought by the Gongshu District Procuratorate, where the defendant

was found to infringe the personal information rights and interests.

1.5 Information sharing organisations and government cybersecurity assistance

The National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNERT) is a national non-government cybersecurity information-sharing organisation that has played the key co-ordinating role in China's cybersecurity emergency response community since 2001.

CNERT runs the two databases that monitor, alert and provide solutions for information vulnerabilities and malware, namely the China National Vulnerability Database (CNVD) and the Critical Information Infrastructure Security Response Centre (CII-SRC), both of which are joint efforts of information system operators, telecommunication operators, cybersecurity service providers and internet service providers.

In addition, the China National Vulnerability Database of Information Security (CNNVD) is a central government-funded database that has analysed, alerted and responded to information vulnerabilities since 2009.

As required by the Administrative Provisions on Security Vulnerabilities of Network Products (Vulnerability Regulation), the MIIT established the National Vulnerabilities Database (NVDB) in 2021 to collect and publicise the vulnerabilities reported by NOs, network product suppliers and vulnerabilities publishing platforms.

1.6 System characteristics

While the scope of the cybersecurity regime in China is comparatively comprehensive and diverse in subject matter, it is still under development, with more supplemental measures expected to be released. Cybersecurity enforcement in China has been active and aggressive, especially since 2019, usually focusing in specific areas, such as the mobile application data protection campaign in 2019, 2020 and 2021. Enforcement is expected to expand in scope and enhance in extent in 2022, focusing on app stores and software development kits (SDKs) interpreted within mobile applications. In 2021, the CAC also initiated a series of enforcement actions on public listing on foreign securities markets, namely, the Cybersecurity Review, expanding the scope of enforcement actions.

The cybersecurity legal system in China absorbs some security protection mechanisms from both the US and the EU systems, while maintaining its distinctive designs. For the network security perspective, China affords special protection to CII, a concept derived from the critical infrastructure in both the EU and the US systems; China also sets forth requirements for emergency response, similar to the EU and the US systems. However, the methodology to identify CII and its boundaries in China differs from that used in the EU and the USA; in addition, security requirements for CII is more expansive in China as they are organically connected to other cybersecurity segments, such as security review, MLPS, and cross-border data transfer.

As for data protection, China is similar to most other jurisdictions in the respect that consent of PI subjects is still the cornerstone of PI protection while affording other limited lawful bases, yet it is different in at least four major respects:

- currently, commercial transactions of PI are criminal offences;
- consent by the PI subject is absolutely central to the legal system in China, and thus the dominant source of the lawfulness of PI processing, save for other limited lawful bases provided by the PIPL, such as processing activities necessary for the compliance of legal obligations;
- the China regime affords additional protection to important data, a concept that the EU or the US systems do not explicitly contemplate; and
- although cross-border data transfer is encouraged, localisation and authority approval is required if regulators deem the transfer may affect national security and public interests.

1.7 Key developments

In the prior 12 months, a series of key laws and regulations (including drafts) were released or came into force, including the following.

- The DSL was released on 10 June 2021 and came into effect on 1 November 2021. Please see **1.1 Laws** for further information.
- The PIPL was released on 20 August 2021 and came into effect on 1 November 2021, marking China's first comprehensive legislation to define, establish, and integrate the provisions regarding PI protection. Please

see **1.1 Laws** for further information.

- The Critical Information Infrastructure Security Protection Regulation (CII Security Regulation) came into effect on 1 Sept 2021, clarifying CII identification rules and providing CIIOs' network protection obligations.
- The Cybersecurity Review Measures was passed in November 2021 and came into effect on 15 February 2022, expanding the scope of cybersecurity review to companies planning to do public offerings in foreign securities markets.
- The Provisions on Several Issues concerning the Application of Law in the Trial of Civil Cases related to the Use of Factual Recognition Technology to Process Personal Information came into effect from 1 August 2021, providing detailed instructions to courts when considering cases involving facial recognition.
- The Algorithmic Recommendation of Internet Information Service Measures, was passed in November 2021 and came into effect on 1 March 2022; this is the first regulation in China that specifically targets the use of artificial intelligence.

As for significant law enforcement activities, the special enforcement campaign against mobile applications illegally collecting and processing PI has discovered thousands of mobile applications infringing PI and ordered violators to rectify accordingly, marking the trend of increasing and extensive enforcement activities by joint forces of regulators. The "Jingwang 2021" campaign against internet-based crimes and PI infringement also marks the continuous strengthening of elevated cybersecurity enforcement by the MPS.

1.8 Significant pending changes, hot topics and issues

The CAC released the Network Data Security Management Regulation (Data Security Regulation) for public comments on 14 November 2021, aiming to provide an overarching implementing regulation for the CSL, the DSL and the PIPL. The Data Security Regulation expected to be a game-changer in the cybersecurity and data protection area, because the Regulation would provide clarification in many pending issues, such as:

- the reporting time after identifying security incidents;
- the scope of important data and obligations of important data processors;
- threshold of PI localisation;
- the rights and obligations of data security officers;
- prerequisites of PI portability rights.

Furthermore, measures for cross-border transfer, such as procedures of security assessment and standard contractual clauses template are also expected to be finalised within 2022.

A number of draft industry-specific regulations and national standards are likely to be finalised this year, such as the draft Data Security Management Measures of Industry and Information Technology Sector (MIIT Data Security Measures) issued by the MIIT.

Hot topics of enforcement emerging since the second half of 2021 include:

- the lawfulness of collecting data from third parties by technical measures, in particular software development kit (SDK);
- processing PI within the scope of necessity, in particular since the release of Provisions on the Scope of Necessary Personal Information of Common Mobile Internet Applications in March 2021;
- the perception of personal information processing activities; and
- cybersecurity review on companies planning (or already) to be listed in the foreign public offering process.

Lastly, sectors such as financial services, automotive and internet services have experience heightened regulatory scrutiny in 2021.

2. Key laws and regulators at national and subnational levels

2.1 Key laws

As mentioned in **1.1 Laws**, the CSL, along with the DSL and the PIPL, lay the foundation of the cybersecurity legal system in China that applies to all kinds of data, systems and information infrastructures, supplemented by a series of implementation measures and other laws and regulations as listed below and sorted by cybersecurity segments.

Network operation security

A1: MLPS – Regulation on Graded Protection of

Cybersecurity (Draft for Comments) (Draft MLPS Regulations).

A2: CII Protection – CII Security Regulation; Cybersecurity Review Measures, as amended.

A3: Cybersecurity Review and Emergency Response – Cybersecurity Review Measures, as amended.

A4: Encryption – the Cryptography Law and the Law on Guarding State Secrets.

Network information security

B1: Personal Information Protection – Civil Code, PIPL, draft Data Security Regulation, Provisions on the Scope of Necessary Personal Information of Common Mobile Applications and Provisions on the Cyber Protection of Children's Personal Information.

B2: Important Data and State Secrets – DSL, Law on Guarding State Secrets.

B3: Cross-border Data Transfer – DSL, PIPL and Cross-border Data Transfer Security Assessment (draft).

B4: Internet Information Content Administration – Provisions on Governance of Network Information Content Ecology, Algorithmic Recommendation of Internet Information Service Measures, Provisions on the Administration of Blockchain Information Services, Provisions for the Administration of Internet News Information Services, and others.

In addition, Articles 253(1), 285, 286, and 287(2) of the Criminal Law apply to the crimes related to cybersecurity.

2.2 Regulators

Please refer to **1.2 Regulators** for their respective responsible area of cybersecurity.

2.3 Over-arching cybersecurity agency

Under Article 8 of the CSL, the CAC is the overarching cybersecurity regulator and agency in China. Please refer to **1.2 Regulators** for its specific regulatory role.

2.4 Data protection authorities or privacy regulators

The CAC, MIIT, MPS and SAMR at the national level, and their branches at the county level or above, are the major data protection authorities and privacy regulators. Please refer to **1.2 Regulators** for their respective role in data protection. The TC260 is also an important privacy regulator that focuses on the promulgation of data protection-related national standards, and most of the national standards are not legally binding but serve as important reference in legal enforcement activities.

2.5 Financial or other sectoral regulators

The CSRC administers a series of securities-related financial activities in China, including initial public offering (IPO), corporate restructuring, and related transactions. Data compliance of listing companies has become one of the key factors in CSRC approving such activities and contributes to CSRC's rejection of IPO listing application in some cases. In a new draft regulation issued by the CSRC in December 2021, the regulators specifically required issuers to comply with cybersecurity and data protection requirements when planning to be listed in foreign securities markets.

The CBIRC, CIRC and CBRC also regulate cybersecurity matters in their respective responsible financial areas. In particular, the CBIRC takes an active regulatory role, as it issued the Guidelines for Data Management of Banking Financial Institutions in May 2018 and is currently promoting the legislation regarding personal financial information protection. The People's Bank of China (PBOC) is also a key regulator over financial institutions, and released Implementing Measures of the PBOC for Protection of Financial Consumers' Rights and Interests, which came into force on 1 November 2020 as well as the Personal Financial Information Protection Technical Specification, an industry best practice standard.

2.6 Other relevant regulators and agencies

Other key regulators include the NASSP and the SCA, as discussed in **1.2 Regulators**.

3. Key frameworks

3.1 De Jure or De Facto standards

Key frameworks

A series of national standards and government announcements have been released. Although some of them were finalised in 2021, many documents are still in draft form for public comments and currently all such national standards are not mandatory. However, in practice a number of these documents are commonly deployed as guidance for law enforcement and corporate compliance, such as the following.

MLPS and network security in general

The Information Security Technology – Baseline for

Classified Protection of Cybersecurity (GB/T 22239-2019) (MLPS Baseline Standards) and the Information Security Technology – Classification Guide for Classified Protection of Cybersecurity set forth specifications encompassing the MLPS classification and evaluation process and the respective requirements for systems at each MLPS classification level. Guidelines on the Protection of Information Security of Industrial Control Systems (ICS Guidelines), promulgated by the MIIT, set forth security protection for industrial control systems (ICS) in various aspects, such as physical environment, authentication, remote access and emergence response.

CIIs

The Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure (Draft for Comments), the Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Draft for Comments), and the Information Security Technology – Indicator System of Critical Information Infrastructure Security Assurance (Draft for Comments) all contemplate the requirements of the identification, inspection, evaluation and security of CIIs.

Emergency response

The National Cybersecurity Incident Emergency Response Plan, promulgated by the CAC, sets forth emergency response measures to various cybersecurity incidents by authorities. The Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, promulgated by the MIIT, sets forth emergency response measures applicable to internet industry participants. The draft Data Security Regulation proposes the time limit as well as procedures for reporting the incidents.

Personal information

The PIPL provides an expanded definition of PI and specifies rules for PI processing activities, PI protection measures and rights for PI subjects. The PIPL is regarded as the fundamental legislation that put in place a key building block of the personal data protection. However, national standard PI Specifications are still practical guidance to PI protection-applicable PIPs and are referred to in data protection compliance practice and enforcement. Guidelines for Internet Personal Information Security Protection, promulgated mainly by the MPS, provides guidance of PI protection tailored to internet companies. Measures for the Identification of Collecting and Utilising Personal Information by Apps in Violation of Laws and Regulations, jointly issued by the CAC, MPS, MIIT and SAMR, sets forth methods of identifying unlawful PI processing by mobile applications. Provisions on the Scope of Necessary Personal Information of Common Mobile Applications, released in 2021, identifies the scope of necessary PI for the basic services of 36 categories and prohibits apps from refusing to provide basic service when users refuse to provide non-necessary PI.

Cross-border data transfer

As mentioned above, under the CSL and the DSL, unless otherwise required by laws and regulations, CIIOs are required to localise PI and important data obtained from operations in China, conduct cross-border transfer of such data only when necessary, perform security assessment requirement beforehand. For general PIPs intended to conduct PI cross-border transfer, pursuant to the PIPL, the PIPs shall inform the PI subjects concerned and obtain their separate consent. The PIPs shall also conduct a personal information impact assessment (PIIA) with regard to the necessity, legitimacy and lawfulness of the transfer, impact on PI subject, security risk and corresponding measures to mitigate the risk. Moreover, PIPs shall satisfy at least one of the following conditions:

- conducting security assessment (if meeting the localisation threshold);
- obtaining PI protection certification by qualified entities;
- entering into standard contracts recognised by the state with the PI receiver; or
- other conditions provided by applicable regulations.

3.2 Consensus or commonly applied framework

The major commonly applied framework for required "reasonable security" are the regulations and national standards related to the MLPS. Please see **2.1 Key laws** and **3.1 De Jure or De Facto standards** for further details.

3.3 Legal requirements

The following illustrate the legal requirements and applicable standards for specific cybersecurity sectors.

Written information security plans or programmes

China has not established any legal requirements regarding written information security plans or programmes. However, NOs are generally required to provide PI subjects with written documents, usually in the form of privacy policies or consent letters, to inform them of the purpose, methods, and scope of PI collection and processing, the NOs' PI security protection mechanisms, PI subjects' approaches of asserting PI-related claims, risks of PI processing, and others.

Incident response plans

The CSL requires that relevant government authorities formulate emergency response plans for their respective industries and fields. Such emergency response plans shall comply with the National Cybersecurity Incident Emergency Response Plan, which classifies cybersecurity incidents into four categories according to their severity and articulates the respective responses to each level. Consistent with the CSL, the DSL requires the competent authority to initiate the incident response plan, take the corresponding emergency response measures, and timely report to the public in the event of a data security incident.

As for private sectors, the PIPL put forward the same obligations by requiring PIPs to formulate incident response plan for PI security incident. It is worth mentioning that, systems classified at MLPS level 2 or above must formulate their own emergency response plans, provide training to its relevant personnel and conduct drills. The Emergency Response Plan for Cybersecurity Incidents in the Public Internet Network also sets forth response requirements for foundational telecommunication companies.

The Data Security Regulation proposes more detailed requirements concerning this mechanism by specifying that PIPs shall notify interested parties and authorities within three working days. Where the incidents involve important data or more than 100,000 individuals' personal information, PIPs shall report to authorities within eight hours.

Appointment of chief information security officer or equivalent

Under the CSL and MLPS-related regulations, each NO shall appoint an officer with the general responsibility of overseeing the NO's cybersecurity and MLPS-related arrangements. The CIIOs shall, in addition to appointing such officer, also conduct a security background check of the officer. Further, DSL set out that processors of important data shall appoint a data security officer to be in charge of the data security protection. The PIPL requires a personal information protection officer to be designated if PIPs processes PI reaching a threshold specified by the CAC.

Involvement of board of directors or equivalent

In China, there is no general legal requirement for direct involvement of the board of directors or equivalent in the cybersecurity matters of a company. However, the fiduciary duty of board of directors under the Company Law of the PRC may give rise to the board's obligations to establish and maintain an effective cybersecurity systems and to take corresponding security measures, depending on the circumstances – for example, the company's affiliated industry or the significance of cybersecurity risks.

The Provisions on the Administration of Informatisation of Insurance Institutions issued by CBIRC require institutions to appoint an executive to be fully responsible for informatisation matters including cybersecurity, under the direct leadership of the board of directors.

The draft Data Security Regulation similarly also propose that the data security officer role shall be assumed by someone at the executive level.

Conducting internal risk assessments, vulnerability scanning, penetration tests, etc

- MLPS national standards and draft regulations set forth a large variety of risk-assessment requirements, such as periodical security assessments taken by systems at level 3 or above.
- The CII Security Regulations require that the CIIOs establish and maintain a CII risk assessment mechanism and conduct assessment at least annually to rectify security risks discovered in a timely manner and report to the competent authority as required.
- According to the PIPL and other draft regulations, PIPs conducting PI cross-border or DPs transferring important data abroad may be required to conduct security assessments.
- Under the PIPL, as mentioned above, PIPs shall conduct PIIA in certain circumstances such as processing sensitive PI, utilising PI for automatic decision-making,

entrusting, sharing, or transferring PI to a third party or publicly disclosing PI, and cross-border transferring PI. The assessment factors shall include the lawfulness, legitimacy and necessity of processing, the risks of adverse effect to PI subjects and the effectiveness of corresponding security measures. The Information Security Technology – Guidance for Personal Information Security Impact Assessment defines the framework, methods and processes of the PI security impact assessment under different scenarios.

Multi-factor authentication, anti-phishing measures, ransomware, threat intelligence

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user identity using passcodes, encryption, biometric technologies and/or other technical measures, in which at least one factor must be encryption; and
- all systems shall install counter-malware software, update malware code database regularly, and establish internal policies of malware countermeasures.

Insider threat programmes

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user, in which at least one factor must be encryption; and
- all systems shall install and maintain updated counter-malware software and establish internal policies correspondingly.

Vendor and service provider due diligence, oversight and monitoring

Obtaining PI from vendors and service providers is recognised as indirect collection of PI. The PI Specifications articulate that PIPs indirectly collecting PI shall request the PI providers to clarify the source of PI, the lawfulness of the source, and the scope of PI subjects' consent, and obtain supplemental consent from PI subjects if the intended processing exceeds the scope of consent.

When PIPs provide their vendors or service providers with PI, their activities constitute the entrusting, sharing, or transferring of PI. The PIPL set forth a series of requirements for such PI provision, such as obtaining informed separate consent from PI subjects, conducting PIIA, contracting with and monitoring PI recipients, and assisting PI subjects to assert lawful requests.

In the event of providing PI to vendors and service providers abroad, PIPs shall ensure the PI would be subject to the same protection level as afforded by the PIPL by satisfying the requirements listed in **3.1 De Jure or De Facto standards**, "Cross-border data transfer".

When procuring network products or services from vendors or providers, under MLPS, the NOs shall ensure that the products or services comply with applicable regulations and standards, and systems at level 3 or above shall conduct inspections before procurement and regularly update and review the list of candidate products. In addition, CIIOs shall ensure that the products or services procured have passed the cybersecurity review by the state if such procurement may affect national security.

Use of cloud, outsourcing, offshoring

The use of cloud is mainly regulated from the MLPS aspect. The MLPS national standards articulate complex and extended security requirements for cloud computing at each MLPS level, covering various aspects of cloud computing security, such as physical environment, network structure, access control, audits, authentication, data integrity and back-up, internal management and service providers. Cloud computing systems at level 2 or above shall maintain their servers physically within China. When the use of cloud involves PI, PICs shall keep such PI physically stored within China.

Outsourcing PI processing is recognised as entrusting, sharing or transferring of PI to third parties. Please see "Vendor and Service Provider Due Diligence, Oversight and Monitoring" (above) for details.

Offshoring mainly concerns cross-border data transfer. Please see the discussion of this topic in **1.1 Laws** for details.

Training

Under the CSL, CIIOs are required to conduct cybersecurity education, technical training and skill assessment for employees on a periodical basis. In line with CSL, both PIPL and DSL demand DPs to carry out personal information protection and data security

education and training for the relevant employees on a regular basis. It is worth mentioning that the Data Security Regulation proposes that DPs with important data shall provide no less than 20 hours of data security training for technical and managerial personnel per year.

3.4 Key multinational relationships

On 16 September 2021, China sent a formal request to join the regional alliance of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP is the largest regional trade agreement to date, setting out rules on e-commerce to ensure that government regulations in CPTPP markets do not unnecessarily impede cross-border data flows, or impose localisation requirements that force businesses to place data servers in individual markets as a condition for serving consumers in that market.

China has entered into Regional Comprehensive Economic Partnership (RCEP) in 2020 covering 15 countries. RCEP establishes regional consensus on cross-border data transfer and limits its members' restrictions on the international digital trades, which facilitates the regional free circulation of data. The RECP has been effective in China since 1 January 2022.

China has entered into bilateral agreements on mutual legal assistance in civil, commercial or criminal matters with a number of countries. These treaties set forth due process requirements of bilateral international legal assistance, which lays the foundation of China's participation in multinational co-operation, such as international co-operation in combating internet-related crimes and frauds.

In addition, China has been actively participating in activities of the establishment of international standards initiated and organised by the International Organisation for Standardisation (ISO).

4. Key affirmative security requirements

4.1 Personal data

The information security requirements in the CSL focus on the following areas – de-identification, secure transmission, deletion and contingency plan. The internal department or personnel in charge of cybersecurity must keep any and all PI, privacy and business secrets obtained during their performance of duties in strict confidence.

Aligned with CSL, the PIPL demands PIPs to take corresponding security measures to ensure the security of PI processed. The aforesaid security measures include: implementing Ma multi-level protection scheme; adopting encryption and de-identification; adopting access control; and formulating an incident response plan. The DSL requires DPs to adopt data security measures covering every step of data processing activities.

De-identification

PI should be immediately de-identified after being collected by PIPs, and technical and managerial measures should be taken to separately store the de-identified data and information that can be used to restore the identification; it should be ensured that no particular individual will be identified during subsequent processing of such data.

Safe transmission

According to the PIPL and PI Specifications, in principle, PI is not encouraged to be shared or transferred except with a solid legal basis and appropriate safety measures. If sharing or transfer by the PIPs is necessary, PIPs shall perform a PIIA beforehand, obtain PI subjects' separate consent after proper notification, and accurately record the sharing or transferring of PI. Particularly, SPI shall be transferred and stored using encryption and other security measures.

As to the issue of PI cross-border transfer, please refer to **1.1 Laws** ("Cross-border transfers") for details.

Deletion

PIPs shall take the initiative to delete PI under any of the following circumstances:

- where the purpose of processing has been achieved or is impossible to achieve, the PI is no longer necessary to achieve the purpose;
- where the PIP ceases to provide products or services, or the retention period has expired;
- where the PI subject withdraws consent; or
- where the PIP processes PI in violation of laws, administrative regulations or countersigned agreements.

PI subjects may request the PI to delete relevant PI, if the PIP has failed to do so. Furthermore, where the lawfully mandated minimum retention period has not expired,

or the deletion is technically difficult to realise, the PIP shall stop all processing activities except storage and necessary security protection measures.

Emergency response plan

Please refer to **3.3 Legal requirements** ("Incident response plans") for details.

4.2 Material business data and material non-public information

In general, NO's internal department or personnel in charge of cybersecurity must keep all business secrets obtained during their performance of duties in strict confidence. Data protected by China's cybersecurity regime can generally be divided into categories of PI, important data, trade secrets, commercial encryption and others.

Enterprises are advised to first identify whether its material business data and material non-public information would fall under the definition of PI or important data. If both categories do not apply, such data may, if applicable, fall under the scope of trade secrets, the identification and protection of which are set forth by the Anti-Unfair Competition Law of the PRC.

For security requirements of business data or non-public information identified as PI, please refer to **4.1 Personal data**.

If material business data is recognised as important data, according to the CSL, NOs are required to take measures such as back-up and encryption of important data. Besides, the DSL also provides the protection system for important data. Article 21 states that each region and department shall formulate the specific catalogue of important data for the region, department, related industry and sector, and focus on the protection of data listed. Article 27 (2) further mandates important data processors to appoint a data security officer and set up a management institution in charge of data security. Article 30 requires such processor to carry out risk assessment on data processing activities on a regular basis, and submit the risk assessment report to the relevant competent department. Additionally, the draft Data Security Regulation as well as the draft Data Security Management Measures for Industry and Information Technology Sector both propose that important data processors shall file the identified important data with the competent authorities.

Various requirements are imposed by the Cryptography Law when enterprises adopt commercial encryption to protect data. The commercial encryption products closely related to national and social public interests shall be certified by qualified inspection agencies before marketisation. CIIOs adopting commercial encryption shall conduct security assessments by themselves or by qualified inspection agencies. When CIIOs' procurement of network products or services adopting commercial encryption may affect national security, a security review of the procurement shall be conducted by relevant state authorities.

4.3 Critical infrastructure, networks, systems

Under the MLPS, in principle NOs are required to:

- formulate internal security management systems and operation instructions to determine the person in charge of cybersecurity and define accountabilities for cybersecurity;
- take technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitor and record network operation and cybersecurity events, and maintain cyber-related logs for no less than six months as required; and
- take measures such as data classification, back-up and encryption of important data.

MLPS protects generic information networks, ICS, cloud computing platforms, internet of things (IoT), big data platforms, mobile communication systems and others network systems (MLPS subjects). NOs have different filing and self-assessment obligations for their MLPS subjects at each of the five protection levels – the higher level the classification is, the higher compliance obligations the NOs have.

In addition to the above requirements applicable to all NOs, CIIOs are in principle identified as level 3 or above, and have additional general obligations to:

- establish a dedicated security management department, appoint a cybersecurity officer, and carry out security inspection of such cybersecurity officer and people in key positions;
- provide periodic cybersecurity education, technical training and assessments for its employees;
- maintain back-up for important systems and databases

in anticipation of catastrophes; and

- formulate emergency response plans for cybersecurity breach incidents and conduct periodic drills.

In the scenario of cross-border data transfer by CIIOs, please refer to **1.1 Laws** ("Cross-border transfers") for details.

In addition, the CII Security Regulations further specify the requirements on the security protection of CII, encompassing the identification of CIIs, response to security incidents, daily operation and security maintenance, security monitoring and inspections, security assessment security of network products and services procurement, and others.

Following the issuance of the Practical Guide to the Multi-level Protection Scheme and Critical Information Infrastructure Security Protection System (Practical Guide) by MPS, the basic framework of CII protection will be gradually set by series of supporting standards, including the identification, security, monitoring and warning, testing and evaluation and incident handling of CII, and important industries and sectors will simultaneously make preliminary progress in establishing the CII identification mechanism based on characteristics of each sector. Overall, the regulatory efforts focus on the CIIOs' obligation of multi-level assessment and CII protection.

4.4 Denial of service attacks

Apart from the general security requirements for NOs under the CSL – described in **4.3 Critical infrastructure, networks, systems** – the Draft MLPS Regulations contemplate general MLPS monitoring requirements related to preventing denial of service attacks. Particularly, while NOs shall monitor and record their network security status, operators of MLPS subjects at level 3 or above shall in addition adopt further precautionary and monitoring measures and timely file the results with local public security bureaus.

With regard to the technical specifications of preventing denial of service attacks, the MLPS Baseline Standards prescribe respective requirements for MLPS subjects at each level regarding the security protection capacity in the four key technical aspects: secure management centre, secure network, safe regional boundary and safe calculation environment.

4.5 Internet of Things (IoT), software, supply chain, other data or systems

Apart from overarching guidelines in the CSL and supporting regulatory documents, there are laws and regulations in particular industries or sectors that also touch on the topic of cybersecurity, as exampled below.

- The Law of the People's Republic of China on Guarding State Secrets mandates that hierarchical protection measures shall be adopted for the computer information systems which are used for storing or processing state secrets and organs and agencies shall enhance their control over the secret-involved information system.
- The Administrative Regulations on Maps prescribes that entities engaging in internet map services shall establish the management system as well as protection measures for the data security of internet maps.
- According to Measures for the Administration of Population Health Information (for Trial Implementation), population health information shall be subject to hierarchical storage. Entities in charge shall establish a reliable working mechanism for disaster back-up of population health information, and conduct back-up and recovery inspections on a regular basis.
- The Cybersecurity Review Measures requires CIIOs to conduct cybersecurity review prior to the purchase of network products and services that affects or may affect national security to ensure the supply chain security of critical information infrastructure and safeguard national security. It also applies to data processing activities by online platform operators when the processing activities impact or may impact national security.

5. Data breach reporting and notification

5.1 Definition of data security incident, breach or cybersecurity event

According to the National Cybersecurity Incident Emergency Response Plan, "cybersecurity incidents" refer to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. They can be

categorised as hazardous program incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents, and other incidents. Furthermore, cybersecurity incidents are graded into four levels, namely: severely material, material, relatively material and general cybersecurity incidents.

5.2 Data elements covered

For the purpose of data security incident or breach regulations, generally all types of data may be covered. In addition to general types of protected data – namely, PI, important data, trade secrets and data contemplated under the National Cybersecurity Incident Emergency Response Plan – other data that may be covered include state secret information, important sensitive information, critical data or other data whose loss would pose certain threats to or have certain impacts on national security, social order, economic construction and public interests.

5.3 Systems covered

The legal construct of data security incident or breach covers:

- systems involving important network and information systems that undertake business closely related to national security, social order, economic development and public interest; and
- network and information systems that would pose threats to or incur impacts on national security, social order, economic construction and public interests upon being damaged.

5.4 Security requirements for medical devices

The Guidelines for Technical Review of Medical Device Network Security Registration articulate general security requirements for the applicants for medical device network registration, such as:

- paying continuous attention to cybersecurity issues during the whole life cycle of medical device production;
- perfecting the user access control mechanism; and
- notifying users of relevant cybersecurity information in a timely manner.

5.5 Security requirements for industrial control systems (and SCADA)

The fundamental security requirements for ICS (including SCADA) can be found in the ICS Guidelines which list 11 protection requirements, covering:

- security software selection and management;
- configuration and patch management;
- boundary security;
- physical and environmental security;
- identity authentication;
- remote access security;
- security monitoring and emergency drills;
- asset security;
- data security;
- supply chain management; and
- responsibility implementation.

In addition, the MLPS Baseline Standards provide security requirements specifically for ICS, such as outdoor control equipment protection, network structure security, dial-up usage control, wireless use control and control equipment security. The Guidelines for Categorisation and Classification of Industry Data (Trial), circulated by the MIIT, put forward preliminary guidance on categorising data in combination with industrial manufacturing models and service operation models, and graded the industrial data into three levels by considering the potential impacts on industrial production and economic benefits after different types of industrial data are distorted, destroyed, disclosed or illegally used.

5.6 Security requirements for IoT

MLPS Baseline Standards provide security extension requirements for IoT such as the physical protection of sensor nodes, device security of sensor nodes, device security of gateway nodes, management of sensor nodes and data fusion processing. Other national standards also serve as reference for IoT security, such as the security technical requirements for data transmission.

The Guidelines for the Construction of Basic Security Standard System of Internet of Things 2021 puts forward the framework of the basic security standards, key standardisation fields and directions of the basic security of IoT, including overall security requirements, terminal security, gateway security, platform security and security management.

The Guidelines for Construction also proposed to set up the basic security standard system of the IoT in 2022 and promoted the formation of a relatively complete system of IoT basic security standards in the next three years. It specifically defined the security requirements for key basic fields such as IoT terminals, gateways and platforms. The requirements include system construction, safety organisation, personnel management, operation safety, asset management, configuration management, remote maintenance safety, vulnerability detection, emergency response, and management and disaster recovery.

5.7 Requirements for secure software development

Certification

Administrative Measures on Testing and Sales Permits for Products Dedicated for the Security of Computer Information Systems released by MPS in 1997, proposed that the term "the products dedicated for the security of computer information systems" shall refer to the hardware and software products dedicated for the security of computer information systems. Selling security dedicated products in China is subject to the sales permit system.

Furthermore, Implementing Measures on Security Certification for Critical Network Equipment and Specialised Network Products provides that the specialised products for network security require security certification. The specialised products for network security are divided into 15 categories, according to the Catalogue of Critical Network Equipment and Network Security Products (First Batch) 2017, including WAF, IDS, IPS and network comprehensive audit system.

Network product security

The Vulnerability Regulation requires network product suppliers, Nos, and vulnerability publishing platforms to establish unimpeded channels for receiving vulnerability information, and timely verify and complete the repair of vulnerabilities. Meanwhile, the Vulnerability Regulation also provides specific time periods for network product suppliers to report vulnerabilities and their obligations to provide product users with technical support. For vulnerability publishing platforms, the Vulnerability Regulation specifies eight requirements, such as allowing them to disclose product vulnerabilities in advance upon assessment and negotiation, prohibiting them from releasing details of network operators' vulnerabilities, simultaneously releasing remedial and preventive measures, and prohibiting them from providing undisclosed vulnerabilities to overseas organisations or individuals other than product providers.

5.8 Reporting triggers

Government authorities

Under the Cybersecurity Law, concerned NOs shall report incidents that threaten cybersecurity to the competent authority. For instance, the following.

- The Automotive Data Security Management Measures requires the automotive data processor that conducts important data processing activities shall, before 15 December of each year, submit the annual automotive data security management report, including the automotive data security incidents and the handling thereof, to the provincial CAC and relevant authorities.
- The Promulgation of the Administrative Measures on Regulatory Data Security (Trial Implementation), issued by the CBIRC, prescribes that in case of occurrence of significant security risks relating to regulatory data, the business department or entrusted organisation concerned shall immediately take emergency response measures and report to the Statistics Information Department of the CBIRC within 48 hours.
- According to Regulations of the PRC on the Security Protection of Computer Information System, users of a computer information system shall report any case arising from such system to the local public security bureau at county level or above within 24 hours.
- The Telecommunications Regulations of the PRC prescribe that telecom operators shall report to the relevant national authorities upon discovery of illegal transmission of information contents as described in Article 56 in the course of their public information services.
- The draft Data Security Regulation proposes that for any data security incident – such as leakage, damage or loss – DPs shall report to interested parties within three business days. Where important data or more than 100,000 individuals' personal information is involved, the DPs shall report to the municipal CAC and relevant authorities within eight hours of the occurrence of the security incident. DP should also submit an investigation and assessment report covering the cause of the incident, the consequence of

harm caused, the accountability and the improvement measures taken, among other information, to the district city-level cybersecurity authority and other relevant authorities within five business days of the disposal of the incident.

As for CII, authorities in charge shall establish the cybersecurity monitoring mechanism and information reporting mechanism for specific industries/sectors within their respective jurisdictions.

In case of increasing risk of cybersecurity events, governments at provincial level and above shall take measures to require authorities, agencies and personnel concerned to promptly collect and report necessary information and enhance monitoring of cybersecurity risks.

In accordance with the CSL, PIPL and DSL, China has established a national cybersecurity information reporting mechanism led by the CAC and MPS, while multi-ministries/bureaus – including MIIT, NDRC and the secrecy bureau – are also participating.

Individuals

Under the CSL, in case of disclosure, damage or loss (or possible disclosure, damage or loss), NOs are obligated to notify the affected users promptly. In addition, for any risk, such as security defect or bug in network products or service, the product/service providers concerned shall inform the users of such risk. In addition, according to the PIPL, in case of PI security incident, affected PI subjects shall be notified of information related to the incident.

Other companies or organisations

Duty to report to other companies may be triggered by contractual obligations.

Industry organisations may determine reporting obligations to its members, under Article 29 of the CSL. Other industry self-regulated obligations to report to information-sharing organisations, as described in **1.5 Information sharing organisations**, may also exist.

5.9 "Risk of harm" thresholds or standards

There are various thresholds and standards of notification in China's cybersecurity regime.

For instance, according to the Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, the lowest level of network security incident is the general network security incident which shall suit one of the following conditions:

- a large number of internet users within one municipality are unable to access the internet normally;
- the leakage of the information of more than 100,000 internet users; and
- other incidents that cause or may cause general harm or effect.

It could be implied at least the same level of threshold of cybersecurity harm is applicable to data breach incident notification.

In addition to the harm to cybersecurity, notification obligations are also triggered when personal information is "likely to be divulged, damaged or lost" under the CSL.

6. Ability to monitor networks for cybersecurity

6.1 Cybersecurity defensive measures

According to the Measures for Monitoring and Handling Threats to the Cyber Security of Public Internet, telecommunications authorities (including MIIT and provincial communication administrations) are in charge of monitoring cybersecurity threats. Thereafter, Information Security Technology – Basic Requirements and Implementation Guide of Network Security Monitoring 2018 sets out the framework and baselines for network security monitoring, which contemplate that network security monitoring are conducted through real-time collection of network and security equipment logs, system operation data and other information.

6.2 Intersection of cybersecurity and privacy or data protection

The intersection of cybersecurity and privacy illustrates the conflict arising from the intertwined interests of the community and of individuals/entities. For instance, from the commercial practice perspective, as companies impose confidentiality obligations on their employees, an employee reporting the vulnerability of his or her company's network system to a third party is in conflict with their confidentiality obligations.

Although it is difficult to clearly define the boundaries between the two, the state tries to balance the scales. For example, in the PIPL, the processing of PI by state organs to perform their statutory functions shall be carried out in accordance with the authority and procedures provided

in laws and administrative regulations, and shall not exceed the scope and limits necessary for the statutory functions, which means public authorities may only collect and use personal information upon data subjects' authorised consent or statutory authorisations by laws or administrative regulations, even when cybersecurity threat is involved. Generally speaking, we understand that only circumstances of certain criminal investigations or threats to national security may trigger such statutory authorisation.

Additionally, under the CSL, DSL, PIPL, and the implementing regulations, authorities and their staff bearing relevant regulatory authority must carefully keep strict confidentiality of any PI, privacy information and business secrets obtained in their performance of duties. Furthermore, Article 30 of the CSL prescribes that cyberspace administrations and authorities concerned shall only use the information accessed in performance of their duties for cybersecurity protection purposes.

7. Cyberthreat information sharing arrangements

7.1 Required or authorised sharing of cybersecurity information

Please refer to **5.8 Reporting triggers** ("Government authorities") for details of this matter.

7.2 Voluntary information sharing opportunities

With regard to Article 29 of the CSL, the state supports the co-operation among network operators in collection, analysis and notification of cybersecurity information and emergency response, in order to improve their cybersecurity protection capacities. The relevant industry organisations shall establish and improve respective cybersecurity rules and co-ordination mechanisms, enhance analysis and assessment on cybersecurity risks, regularly release risk alerts to their members, and assist their members with coping with cybersecurity risks.

In China, users, suppliers and research institutions are encouraged to report any potential system vulnerabilities identified to the CNVD, as described in **1.5 Information sharing organisations and government cybersecurity assistance** , so as to gather, verify and warn against any security vulnerabilities and to establish an effective and co-ordinated emergency response mechanism among all operators.

Also, there are scenarios where system vulnerabilities shall be mandatorily reported, as described in **5.7 Requirements for secure software development**.

It is worth noting that a major cloud service provider had been suspended by MIIT, with their partnership ending in 2021, because of failing to meet the mandatory reporting obligation.

8. Significant cybersecurity and data breach regulatory enforcement and litigation

8.1 Regulatory enforcement or litigation

In the field of administrative supervision, app governance is still the most important work for regulatory authorities in the field of data protection in 2021. MPS further promoted the special action of "Jingwang 2021" and achieved remarkable phased results, with more than 37,000 illegal activities related to network being detected. In the meantime, MIIT issued a notice on launching actions for improvements to the perception of information and communications service. It is required to establish the list of collected personal information and a list of personal information shared with third parties, and display the same in the secondary menu of the app.

As of September 2021, MIIT has issued a total of 19 batches of "app notification on infringement of user rights", of which five batches were issued in 2021. The notified apps concern many fields, and the listed problems focus on the illegal collection of PI compulsory access to authority, etc.

8.2 Significant audits, investigations or penalties

Since last year, the regulatory authorities have significantly strengthened their supervision over the protection of personal information security. The CBIRC released an administrative penalty notice on its official website, indicating that China CITIC Bank received a fine of CNY4.5 million for several violations of laws and regulations, such as enquiring about and then providing transaction information of a customer's personal bank account to a third party without the authorisation of the customer.

The PBC has issued more than 31 penalty decisions involving personal information security (including institutions and individuals). Most of the punishment decisions are for the violation of enquiring about personal information without the subject's consent, including enquiring about individual credit reports or loan information without the subject's consent and

negligent disclosure of personal information.

8.3 Applicable legal standards

Please refer to **1.3 Administration and enforcement process** and **1.4 Multilateral and subnational issues**.

8.4 Significant private litigation

A WeChat user filed a lawsuit, claiming that the Weishi app (operated by Tencent) used the plaintiff's personal information in WeChat without authorisation, including region, gender and WeChat relationship. Upon trial of the second instance, the court held that the Weishi App's compulsory acquisition of the user's region and gender information did not satisfy the principle of necessity of collecting user information.

Further, in the scenario that the plaintiff uninstalled the Weishi App and re-used the same account to log in to the Weishi App without consent and authorisation, the user had reasonable grounds to believe that it no longer authorised the Weishi App to use the WeChat friend relationship. Weishi's continuous use of the stored WeChat friend relationship in the back-end did not meet the user's "reasonable expectation" of the consequences of his authorisation. Therefore, the Weishi App's continuous use of the plaintiff's WeChat friend relationship did not meet the lawfulness principle when the plaintiff downloaded the app for the second time.

8.5 Class actions

Article 70 of the PIPL establishes the foundation of public interest litigation for the protection of personal information. The Procuratorate, the consumer organisation as provided by law, or the organisation determined by the CAC may file a lawsuit with the court in accordance with the law. In addition, the Supreme People's Procuratorate (SPP) promulgated the Circular on Implementing the Law on the Protection of Personal Information and Promoting the Procuratorial Work of Public Interest Litigation on the Protection of Personal Information, clarifying the key points of handling public interest litigation on the protection of personal information.

9. Due diligence

9.1 Processes and issues

The process of diligence in corporate transactions mainly concerns the security and the asset aspects of data.

For the security aspect, MLPS classification and evaluation of a company's information system are the first steps of due diligence. Comprehensive assessments of cybersecurity based on MLPS classification will then be conducted to perform gap analyses of various security-related matters, including emergency response, PI protection, cross-border data transfer security and CII protection.

As for the asset aspect, due diligence will focus on confirming the legitimacy of the corporate data and identifying the legal boundary of corporate data assets. As security and compliance of data are the premises of data assets, taking data mapping as reference, assessment reports will be issued to review the corporate compliance of data regarding various matters, such as PI processing, internal corporate systems related to cybersecurity and data compliance, information content administration, and others. Identifying the boundary of the company's data and the claims the company has over them will be the next step to confirm the company's proprietary rights on the corporate data.

9.2 Public disclosure

The National General Response Plans for the Public Emergency Incidents set forth local government authorities' obligations to report public emergency incidents to higher level authorities. Cybersecurity risks that constitute a public emergency incident may be disclosed and reported to various level of authorities for emergency alerts and responses. The Emergency Response Law of the PRC also requires that all entities shall timely report their potential emergency incidents to local authorities in accordance with applicable laws and regulations. In the financial area, the Measures for the Administration of Initial Public Offering and Listing of Stocks and other similar IPO administration measures require that any information that may have any major impact on the investors' decisions on investment shall be disclosed in IPO prospectuses.

However, entities should note that the disclosure of cybersecurity information may be subject to certain limitations under recent draft measures by the CAC, as described in 1.5 Information sharing organisations.

10. Insurance and other cybersecurity issues

10.1 Further considerations regarding cybersecurity regulation

Considering the extraterritorial jurisdiction of PRC

cybersecurity regulations, "domestic operation" also entails an enterprise's acts that are intended to provide goods or services to individuals within the PRC.

11. Trends and developments

11.1 Overview

The year 2021 marked a significant development in China's cybersecurity and data protection legislative regime. The long-awaited Data Security Law (DSL) and the Personal Information Protection Law (PIPL) were both finalised and came into effect in 2021. These two laws, together with the Cybersecurity Law (CSL), which has been effective since 2017, form the overarching legislative framework of cybersecurity and data protection.

Regulators also finalised many implementing regulations. For example, after seven months of public consultation and deliberation, the Cybersecurity Review Measures (CRM), as amended, came into force on 15 February 2022, signalling that China's cybersecurity enforcement has moved into a new era. The CRM mandates that (i) critical information infrastructure operators (CIIOs) procuring network products and services, and (ii) network platform operators carrying out data processing activities that affect or may affect national security shall be subject to cybersecurity review organised by the competent authorities.

Another example is the Critical Information Infrastructure Security Management Regulation ("CII Security Regulation"), which was adopted on 1 September 2021; it lays down the fundamental security compliance obligations for CIIOs, ensuring the CIIOs are well protected in cyberspace.

A series of implementing regulations are expected to be released or finalised in 2022. Aside from the traditional cybersecurity regulations, regulators in various industries are expected to issue cybersecurity-related regulations focusing on industry-specific issues. These regulations are expected to address pending issues and provide more practical guidance.

As such, the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (albeit with certain specific compliance requirements) generally act as fundamental laws, while regulators in each industry are tasked to promulgate respective implementing regulations.

11.2 The Data Security Law

The Data Security Law (DSL) that came into effect in September 2021 represents the legislation's first effort at the state level to regulate data processing activities by balancing the security and the utilisation aspects. The DSL provides the fundamental legal basis for the Cyberspace Administration of China (CAC) and other competent authorities to ensure data processing activities do not harm state security, public interests and private interests.

The DSL contemplates extraterritorial jurisdiction over offshore data activities affecting state security, public interests and private interests within the PRC; it operates in conjunction with the Cybersecurity Law (CSL) in many areas. For instance, the DSL requests data processors to perform data security protection on top of the multi-level protection scheme as prescribed by the CSL.

The DSL contemplates a general principle of data categorisation and classification based on the importance of data and the damage incurred upon data breach. Some industry regulators have issued national and industry standards for their respective sectors, such as finance and healthcare. In December 2021, the National Information Security Standardisation Technical Committee (TC260) issued the Cybersecurity Standard Practical Guidance – Network Data Categorisation and Classification, a non-binding guideline, which provides general and universal guidance on conducting data categorisation classification.

The DSL requires governments at different levels to issue catalogues of important data to identify and provide heightened protection to such data, including periodical risk assessment. Although there have been several attempts to provide straightforward criteria, the specific scope of "important data" is to be determined. The new draft regulations now propose to require data processors to self-identify important data and then file the identification result with the industry regulators. Hence, it is likely that the scope of important data will become clearer in 2022 or early 2023.

The DSL requires that data security reviews should be conducted on data processing activities that may affect state security. Although the cybersecurity review system has been established, the data security review is a different review process. The implementing regulation thereof is likely to be issued in the new future.

11.3 The Personal Information Protection Law

The Personal Information Protection Law (PIPL) came into effect in November 2021. While primarily focusing on protecting personal information (PI), the PIPL also supplements the network information security requirements under the CSL.

In essence, the PIPL aims to work as an independent legislature specifically focused on PI protection, which significantly changed under the CSL. The PIPL contemplates extraterritorial jurisdiction over offshore processing of the PI of natural persons within the PRC if the action is intended to provide goods or services to such person or assess such person's behaviour. This illustrates the legislation's response to the trend of extraterritorial jurisdiction worldwide, such as the GDPR in the EU and the CCPA in the USA, to afford individuals within the PRC equal protection. Foreign companies should be mindful of the extraterritorial jurisdiction when dealing with individuals within the PRC.

The PIPL lines up with the terminology used in the Civil Code, and defines the entity or individual capable of determining the purpose and methods of PI processing as the "PI processor", rather than the "controller" concept used in other jurisdictions such as the EU. In addition, the "entrusted processor" under the PIPL is comparable to the "data processor" in the GDPR.

Besides the consent and requirement laid down by other laws and regulations, the PIPL introduces additional legal bases including:

- necessity for executing or performing contracts where the individual is a party;
- necessity for human resources management based on lawfully enacted labour rules and collective bargain agreements;
- protection of public health in an emergency; and
- certain reasonable acts to protect the public interest.

It is a drastic expansion from the CSL's framework, and grants enterprises much more flexibility.

The PIPL also introduces the first attempt to regulate the cross-border transfer of PI by general entities at the statute level, compared to the cross-border transfer provisions applicable to CIIOs in the CySL. Specifically, it extends the scope of data localisation and mandatory security assessment for outbound PI transfer, previously only applied to transfers conducted by CIIOs, to mass-volume PI processors (the standard is to be determined by regulators). For transfers conducted by other entities, it also provides several new approaches of compliant outbound PI transfer as compared to the sole approach of security assessment under the current cross-border security transfer rules. In general, foreign enterprises processing a large volume of user data may incur legal risks if providing service to PRC users without deploying the server within the PRC. It also requires PI processors to obtain independent consent from PI subjects, which is different from explicit consent under the GDPR.

In sum, the PIPL reflects the legislation's attitudes and objectives in PI protection that elevates requirements for PI protection while endeavouring to strike a nuanced balance between PI rights and market participants' interests in processing PI in the evolving era of the digital economy.

11.4 The draft Network Data Security Management Regulation

In order to harmonise the requirements under the CSL, the DSL and the PIPL, the CAC released the draft Network Data Security Management Regulation ("Data Security Regulation") on 14 November 2021. This Regulation proposes to implement the high-level instructions contained in the aforesaid laws. For instance, the laws all require companies to develop an emergency plan for security incidents and report the incidents to the competent authority, but do not specify the time limit of the reporting obligation. The Data Security Regulation proposes that if a security incident has caused harm, companies shall notify the interested parties within three business days. Moreover, if the security incident involves important data or more than 100,000 individuals, the companies shall report to competent authorities within eight hours upon the occurrence of the security incident.

Although filled with detailed contents, duties imposed by the Data Security Regulation can be generally categorised into four aspects: record, assessment, review and filing/report in relation to data processing activities, which provide regulators with regulatory tools that are practical and down-to-earth. For example, as evidenced by the automotive industry, after the local MIIT branches received the annual automotive data security report, the regulator would approach the companies to discuss high-risk data processing activities and request remedial measures.

However, if the Data Security Regulation is finalised

as is, companies may face unprecedented compliance burdens. Therefore, the draft Regulation has led to heated discussions, and many proposed requirements are likely to be modified. However, the Regulation provides valuable insights into the CAC's view of how companies should manage data processing activities.

11.5 Cybersecurity review

As a crucial aspect of national security review, a cybersecurity review was enacted to protect national security interests by examining the network products or services to be procured by CIIOs, whose network products and associated information systems, by definition, may have national security interests.

In July 2021, the CAC issued an amendment to the CRM, expanding the scope of cybersecurity review to data processing activities that may affect national security. Particularly, because public offerings in foreign securities markets involve a significant volume of cross-border data transfers, the amendment requires data processors, who possess more than one million individuals' personal information, to proactively file for a cybersecurity review when planning to be listed in a foreign security market. The amendment was passed in November 2021 and came into force on 15 February 2022. Although the finalised CRM changed the terminology from data processors to network platform operators, it is likely that these terms have similar scopes.

The cybersecurity review focuses on two aspects. The first aspect is the procurement of network products or services by CIIOs, including:

- the risk of any CII being illegally controlled, tampered with or harmed after using the network products or services;
- the risk of any CII's supply of network products or services being interrupted;
- the security, openness, transparency, diversity of sources and reliability of the supply channels of network products or services, as well as the risk of the supply chain being interrupted due to political, diplomatic, trade or other factors; and
- the compliance situation of the suppliers with the RPC laws and regulations.

The second aspect is data processing activity, including: the risk of core data, important data or a large volume of personal information being stolen, leaked, destroyed and illegally used or transferred abroad; the risk, during and after the public offering, that CII, core data, important data or a large volume of personal information might be affected, controlled or maliciously used by foreign governments, as well as any network information security risk.

The cybersecurity review process may take a month to complete if it is initiated by the Cybersecurity Review Office (CRO) under the CAC, but when a CIIO or a network platform operator proactively applies for cybersecurity review, the CRO should conduct a pro forma review and notify the applicant in writing whether or not a full-blown cybersecurity review will be conducted within ten business days upon receiving application materials.

It is worth noting that it is not clear whether CRM is applicable to foreign companies. Based on the legislative intent of mitigating risks incurred by data processing activities, it is still likely that the CAC may require such a foreign company to file for a cybersecurity review if the company has a significant operation in China.

11.6 Multi-level Protection Scheme (MLPS)

The MLPS requirements and standards generally remained the same in the year of 2021, but the draft Data Security Regulation proposes that all systems processing important data must be qualified as MLPS level three, creating an interoperative link between cybersecurity and data security.

Additionally, we have observed that an increasing number of multinational companies (MNCs) are considering conducting MLPS. This trend suggests that these companies partially localised their networks because MLPS can only be conducted for domestic networks.

11.7 The CII Security Regulation

Section 2 of the CSL has envisaged a framework of operation security of CII by setting out basic principles, imposing basic security protection obligations on CIIO, and requesting localisation of the PI and important data collected by CIIO.

In line with the CSL, the CII Security Regulation lays down detailed responsibilities and obligations for CIIOs to undertake, supportive measures for protection authorities to adopt and the legal liability for violation. Significantly, the CII Security Regulation put forward several factors to consider in identifying CII, namely:

- the importance of the network facility and information system;

- the degree of harm that might be caused in the event of destruction, loss of function or leak of data; and
- the impact on the relevant industries and sectors

Additionally, the Regulation specifies that industry regulators are charged with the responsibility to identify the CII, and notify the operator thereof about the identification result.

Because CIIOs are subject to heightened compliance obligations, some of which may affect how they should interact with other companies (eg, procurement), companies should be mindful of any notices from relevant regulators and the CIIO status of the business clients.

11.8 Industry-specific regulations

Cybersecurity regulations are moving toward a sectoral model, where industry regulators are implementing the laws with industry-specific issues.

On 23 January 2022, the financial regulators issued a five-year plan to advance the standardisation of financial sectors. The plan, by recognising the cybersecurity and data risks brought by the digitalisation of financial services, aims to improve network security standards in the financial sector, such as financial CII protection standard, financial network security assessment, etc, so that financial service providers are well equipped against cybersecurity threats. In particular, the plan contemplates financial information technology outsourcing evaluation, financial data classification and commercial cypher codes standards.

The Ministry of Industry and Information Technology (MIIT) issued the Administrative Provisions on Security Vulnerabilities of Network Product on 12 July 2021. Network product suppliers, network operators and vulnerability publication platforms are required to set up a communication channel to receive reports of network products' security vulnerability, and keep the log of the received security vulnerability for at least six months. Additionally, network product suppliers are required to report identified vulnerability information to the National Vulnerability Database within two days.

Furthermore, the MIIT has twice sought public comments for the Data Security Management Measures of Industry and Information Technology Sector – in September 2021 and February 2022 – indicating MIIT's commitment to establishing detailed data security rules. The Measures first divides data into three categories: normal data, important data and core data, then provides the identification criteria, based on the degree of impact on national security, public interests and private interests. The Measures also offer detailed requirements for each category of data through every step of data processing activities. Similar to the draft Data Security Regulation, the Measures require companies to file the important data identification result with the regulators.

Switching to the automotive sector, the CAC and four other regulators, including the Ministry of Transportation, issued the Automotive Data Security Management Measures in August 2021. For the first time, the Measures provide a clear definition of important data, including more than 100,000 individuals' personal information and geographic information of sensitive areas such as government buildings. The Measures also require automotive data processors to file an annual data security management report with the competent authorities, specifying the types, volume, purposes and necessity of automotive data processing activities, as well as the implemented protective measures.

Conclusion

Starting from the CSL, security obligations are determined based on different legally prescribed roles, and potential impact on national security, public interests and private interests, such as that CIIOs are subject to higher security protection obligations compared to network operators. Although the overall enforcement actions are not as frequent as those in other fields, it demonstrates that regulators are taking a prudent approach in regulating cybersecurity. The cybersecurity review, MLPS and finalised (as well as proposed) filing requirements all provide regulators with effective regulatory tools and serve as bridges between cybersecurity and data security.

As such, the offshore model adopted by MNCs is likely to face more compliance burdens and may attract regulatory scrutiny. Therefore, in addition to data localisation, the possibility of network localisation should also be evaluated.

CHAMBERS - ARTIFICIAL INTELLIGENCE 2022 (CHINA)

1. General legal framework

1.1 General legal background framework

China has developed a large number of laws and regulations that systematically address AI-related issues, as well as rules regulating particular AI-related subject matters.

At the level of national laws, AI – as a technology that highly relies on the use of internet and data – will be subject to the three basic laws in the information technology field, namely:

- the Cybersecurity Law of the People's Republic of China (CSL);
- the Data Security Law of the People's Republic of China (DSL); and
- the Personal Information Protection Law of the People's Republic of China (PIPL).

They are enacted to guarantee cybersecurity and regulate data (including personal information) processing activities.

Under these basic laws, the State Council, the Cyberspace Administration of China (CAC) and other authorities responsible for cybersecurity and data protection within the scope of their respective duties are tasked to develop and enforce specific regulations. For example, the CAC has issued a number of rules/draft rules concerning internet information services, especially including the use of AI technologies in such fields.

At regional levels, local governments have enacted relevant cybersecurity and data regulations in conjunction with the actual development of their respective regions, with 12 representative provinces and cities such as Shanghai and Shenzhen since 2021.

Apart from general cybersecurity and data protection laws, laws and regulations of other legal sectors also apply to AI if the application of AI touches specific issues regulated in these other legal sectors, including consumer protection law, anti-monopoly law and industrial-specific laws.

2. Industry use of AI and machine learning

2.1 AI technology and applications

AI and machine learning have become the key force in promoting the development of the financial industry, according to a report issued by the China Academy of Information and Communications Technology (CAICT). In the banking industry, AI technology is widely used in biometric identification, credit risk prevention and intelligent customer services (such as chatbots). According to the CAICT, as of September 2021, one of China's state-owned banks had collected and used 40 PB of data assets and implemented more than 1,000 AI applications.

Another noteworthy application of AI technology is automated driving. The investment and financing of the automated driving industry are increasingly active in China. Robotaxis are the top priority. For example, in 2021, Baidu and Pony.ai became the first two domestic enterprises to be allowed to carry out commercial robotaxi services in Beijing. The commercial use of low-speed automatic vehicles is also accelerating. In May 2021, approximately 100 automatic delivery vehicles from JD.com, Meituan, and Neolix were issued with official vehicle codes in Beijing; in September 2021, the automatic express car developed by JD.com was put into trial operation on the roads in Qionghai City to provide delivery services to communities within 3 km.

Since 2020, while bringing havoc to the markets and industries in China, the COVID-19 outbreak has also revealed unprecedented opportunities for the AI industry. To respond to the pandemic control policies in China, the market has seen a high demand for products and services based on AI technology, AI-powered medical research and diagnosis, pandemic

control decision-making, a uniform national "Health Code" platform that traces individuals' health status for pandemic control, and internet-based convenience services powered by AI, such as food delivery, online shopping and internet hospitals.

3. Executive developments

3.1 Policies

At the national level, China has drawn up comprehensive plans for the development and application of AI. In December 2021, the Ministry of Industry and Information Technology (MIIT), along with seven other state ministries released the 14th Five-Year Plan for the Development of Intelligent Manufacturing (the "Plan"), which listed AI as one of the core technologies in China's intelligent manufacturing.

The Plan also emphasises strengthening research on the application of specific AI technologies in certain industries. In the finance sector, for example, the China Banking and Insurance Regulatory Commission (CBIRC) issued the Guiding Opinions on Promoting the Highquality Development of Banking and Insurance Industries, encouraging banking and insurance institutions to make full use of emerging technologies such as AI, big data, cloud computing, blockchain, biometrics and other technologies to improve service quality.

In addition, the Chinese government is also making efforts on establishing a national standard system for AI technology. In August 2020, the State Standardisation Administration, the CAC, and other state ministries jointly released the Guidance on Establishing the New Generation of National AI Standardisation System (the "AI Standards Guidance"), aiming at setting up a preliminary national AI standardisation system by 2023. The Opinions on Accelerating the Construction of a National Unified Market, issued by the Central Committee of the Communist Party of China and the State Council in 2022, has made it clear that it is necessary to strengthen the standard system in fields including AI.

3.2 National security

It is a common issue for AI operators that they may collect a large amount of data to feed their AI system. Since China's laws and regulations on data processing have a clear concern for national security, AI companies are also advised to be aware of related legislative requirements.

Critical Information Infrastructure (CII)

The Regulation on Protecting the Security of Critical Information Infrastructure has defined CII as network facilities and information systems in important industries and fields that may seriously endanger national security, the national economy and people's livelihood, and public interest in the event of being damaged or losing functionality. CII Operators (CIIO) are required to take protective measures to ensure the security of the CIIs. Furthermore, the CSL imposes data localisation and security assessment requirements on cross-border transfer of personal information and important data for CIIOs.

Important data

The DSL have defined important data as data the divulging of which may directly affect national security, public interests, and the legitimate interests of citizens or organisations, and certain rules impose various restrictions on its processing. The DSL contemplates security assessment and reporting requirements for the processing of important data in general.

Cybersecurity review

On 28 December 2021, the CAC, together with certain other national departments, promulgated the revised Cybersecurity Review Measures, aiming at ensuring the security of the CII supply chain, cybersecurity and data security and safeguarding national security. The regulation provides that CIIOs that procure internet products and services, and internet platform operators engaging in data processing activities, shall be subject to the cybersecurity review if their activities affect or may affect national security, and that internet platform operators holding more than one million users' personal information shall apply to the Cybersecurity Review Office for a cybersecurity review before listing abroad.

4. Legislative developments

4.1 Enacted legislation

Currently, legislations regulating particular AIrelated subject matters in China include the following:

Data protection

The CSL and DSL directly address the national strategy for enhancing cybersecurity and data security. As for personal information protection, there are three overarching statutes setting forth general principles:

- the PIPL, enacted on 1 November 2021;

- the Civil Code, released in May 2020; and
- the CSL, articulating requirements for personal information protection.

The PIPL proposes to extend the legal basis of processing personal information, as compared to the Civil Code and the CSL, in order to adapt to the complexities of economic and social activities. Since 2019, when multiple departments in China jointly issued the Announcement on Special Treatment of Illegal Collection and Use of Personal Information by App, the current trend shows that the enforcement of app personal information protection has continued to be enhanced, especially in the areas of small programs, SDK (software development toolkit) third-party sharing and algorithmic recommendation as the focus of regulation.

Antitrust

Concerning the Antitrust Guidelines for the Platform Economy, concerted conduct may also refer to the conduct whereby undertakings do not explicitly enter into an agreement or decision but are co-ordinated through data, algorithms, platform rules or other means. As such, AI operators shall also comply with the Anti-Monopoly Law, which requires that competitors are prohibited from reaching monopoly agreements of price-fixing, production or sales restrictions, market division, boycott, or other restraining behaviours. Moreover, dominant market players are also prohibited from conducting discriminatory activities against their counterparties by means of algorithm.

Consumer protection

Business operators providing products/services to consumers by means of algorithms shall be subject to the Law on Protection of Consumer Rights and Interests, which acts as the basic consumer protection legislation. As for e-commerce businesses, they should further comply with the E-commerce Law, in which there are specific rules dealing with personalised recommendations.

Information content management

The Provisions on Ecological Governance of Network Information Content issued by the CAC, effective in January 2020, articulate requirements for content provision models, manual intervention and user-choice mechanisms when network information content providers feed information to users by adopting personalised algorithms.

In December 2021, the CAC issued the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (the "CAC Algorithm Recommendation Rules") to provide special management regulations on algorithmic recommendation technology. The CAC Algorithm Recommendation Rules mark the CAC's first attempt to regulate the use of algorithms, in which internet information service providers are required to use algorithms in a way that respects social morality and ethics, and are prohibited from setting up any algorithm model inducing users to become addicted or to over-consume.

For industrial-based regulations, please refer to **9. AI in Industry Sector**s.

4.2 Proposed legislation

During the past two years, the data protection authorities in China have issued a large number of draft regulations, aiming at providing detailed implementation guidance for national legislations about data processing activities. For example, the draft Regulations for the Administration of Network Data Security, as a supporting regulation of the CSL, DSL and PIPL, clarifies specific issues in the field of data security management and supplements the basic principles in the national legislations. The draft of Measures on Security Assessment of the Cross-border Transfer of Data articulates in greater detail the framework of cross-border data security review.

For AI-related rules, the CAC released the draft Provisions on the Administration of Deep Synthesis of Internet Information Services in February 2022, which provides specific rules for providers of deep synthesis technologies in the context of information content management.

5. AI regulatory regimes

5.1 Key regulatory agencies

In China, the CAC is responsible for the overall planning and co-ordination of cybersecurity, personal information protection and network data security, and has issued a number of regulations concerning the application of AI technology in terms of internet information services. There are also many other departments – such as departments in the industrial sector, telecommunications, transportation, finance, natural resources, health, education, science and technology – and other departments undertake the duty

to ensure cybersecurity and data protection (including that related to AI) in their respective industries and fields. Public security authorities and national security authorities also play an important role for network and data security within their respective purviews.

5.2 AI definitions

The practice guidance issued by the National Information Security Standardisation Technical Committee (TC260) – ie, Practice Guide for Network Security Standards-Guidelines for Prevention of Ethical Security Risks in Artificial Intelligence – has defined AI as the simulation, extension or expansion of human intelligence by using a computer or its controlled equipment, through the methods of perceiving the environment, acquiring knowledge and deducing.

Another draft standard, the Information Security Technology-Security Specification and Assessment Methods for Machine Learning Algorithms, also released by TC260, defines machine learning algorithms as algorithms that solve problems by using a limited and orderly set of rules to generate classification, to reason, and to predict based on the input data.

5.3 Regulatory objectives

It is a normal practice for the CAC and other departments to co-operate in rule-making and enforcing the laws. Most of the data protectionrelated rules are jointly issued by multiple regulatory agencies including the CAC, the MIIT, public security authorities and other related departments. These laws and regulations have played a key role in ensuring network and data security, and the protection of personal information. In particular, the CAC recently promulgated a series of rules or drafts on the application of AI technology, with an aim to promote the positive and good application of algorithms. These laws and regulations also aim to protect the social and public interests and national security involved in the network and data fields from being endangered.

6. Proposed EU Artificial Intelligence law

6.1 Jurisdiction commonalities

The matter is not applicable in the jurisdiction.

6.2 Jurisdiction conflicts

The matter is not applicable in the jurisdiction.

7. Standard-setting bodies

7.1 Standards

The State Standardisation Administration (CSA) is responsible for approving the release of national standards, and TC260 (as mentioned above) is one of the important standard-setting bodies on AI technology. So far, TC260 has issued a series of recommended national standards and practical guidelines containing provisions regarding the use of AI-related technology. For example, the national standard Information Security Technology – Personal Information Specificationprovides rules on automated decision-making similar to the PIPL, which states that controllers adopting automated decision-making that may influence data subjects' interests should conduct security assessments of personal information ex ante and periodically, and should allow data subjects to opt out of such automated decision-making.

The draft standard Information Security Technoogy – Security Specification and Assessment Methods for Machine Learning Algorithms specifies the security requirements and verification methods of machine learning algorithms in the stages of design and development, verification testing, deployment and operation, maintenance and upgrading, and decommissioning, as well as the implementation of security assessment of machine learning algorithms.

In addition, there are standard-setting bodies to formulate AI-related standards in specific industries. The PBOC, along with the Financial Standardisation Technical Committee of China (TC 180), which is the CSA-authorised institution to engage in national standardisation, plays a leading role in writing AI-related standards in the financial field. The recommended industry standard of Personal Financial Information Protection Technical Specification, which was issued in the name of the PBOC, sets forth requirements for financial institutions to regularly assess the safety of external automated tools (such as algorithm models and software development kits) adopted in the sharing, transferring and entrusting of personal financial information. The PBOC also released the Evaluation Specification of Artificial Intelligence Algorithm in Financial Application in 2021, providing AI algorithm evaluation methods in terms of security, interpretability, accuracy and performance.

In automated driving, the recent recommended national standard Taxonomy of Driving Automation for Vehicle s sets forth six classes of automated driving (from L0 to L5) and sets forth respective technical requirements and the

roles of the automated systems at each level. The TC260 released the Security Guidelines for Processing Vehicle Collected Data, which specify the security requirements for automobile manufacturers' data processing activities such as transmission, storage and export of automobile data, and provides data protection implementation specifications for automobile manufacturers to carry out the design, production, sales, use, operation and maintenance of automobiles.

8. General technology-driven AI legal issues

8.1 Algorithmic bias

From a technical perspective, algorithms may be biased due to a number of reasons. The accuracy of an algorithm may be affected by the data used to train it. Data that lacks representativeness or, in essence, reflects certain inequalities may result in biases of the algorithms. The algorithm may also cause bias due to the cognitive deficits/bias of the R&D personnel. Besides, due to the inability to recognise and filter bias in human activities, algorithms may indiscriminately acquire human ethical preferences during human-computer interaction, increasing the risk of bias in the output results.

For example, the provision of personalised content by digital media has raised serious concerns on the so-called "information cocoon" – a phenomenon where people get more and more limited information selected, based on automatic analysis of their previous content preferences. Another example is the concern of "big data killing", where different consumers are charged significantly different prices for the same good. According to the China Consumers Association, certain companies use algorithms to make price discriminations over different groups of consumers.

Having been aware of the harm to society and consumers' interests caused by algorithm bias, the Chinese government is trying to regulate the proper application of algorithm both on an industrial-specific basis and on the general data protection side. According to the E-commerce Law, where an e-commerce business operator provides consumers with search results for goods or services based on consumers' preferences or consumption habits, it shall, in parallel, provide consumers with options that are not targeted at their personal characteristics. Similar rules have been set in the PIPL regarding automatic decision-making, where transparency and fairness requirements are explicitly stipulated (see **8.4 Automated decision-making**).

The newly issued regulation concerning internet information services, the CAC Algorithm Recommendation Rules, further provide that an algorithm-recommended service provider which sells goods or provides services to consumers shall protect their right to fair transactions, and shall not use algorithms to commit unreasonable differential treatment and other illegal acts in respect of transaction prices and other transaction conditions based on their preferences, transaction practices and other characteristics. "Big data killing" is also under the scrutiny of the Anti-monopoly Law, by which a dominant market player is prohibited from discriminating against its counterparties (including consumers) by means of automatic decision-making programs.

8.2 Facial recognition and biometrics

Under the PIPL, facial recognition and biometric information are recognised as sensitive personal information. Separate consent is needed for processing such information and the processing shall be only for specific purposes and with sufficient necessity. Facial information collected by image collection or personal identification equipment in public places shall only be used for maintaining public security, unless separate consent has been obtained.

This gives rise to concerns of intelligent shopping malls and smart retail industries where facial characters and body movement of consumers are processed for purposes beyond security, such as recognising VIP members and identifying consumers' preferences so as to provide personalised recommendations. Under the PIPL, companies must consider the necessity for such commercialised processing and find feasible ways to obtain effective "separate consent".

In the automobile industry, images or videos containing pedestrians are usually collected by cameras installed on cars. This is a typical data source for automobile companies engaging in autonomous driving or providing internet of vehicles services. While training their algorithms and providing relevant services, automobile data processors must consider the mandatory requirements both in the PIPL and the recently issued Several Provisions on the Management of Automobile Data Security (for Trial Implementation), in which videos and images containing facial information are considered as important data. Processors having difficulty obtaining consent for its collection of personal information from outside a vehicle for the purpose of ensuring driving safety shall conduct anonymisation for such information,

including deleting the images or videos that can identify the natural person, or conducting partial contour processing of facial information.

The Supreme People's Court also provides its judicial view regarding the processing of facial information and clarifies scenarios that may cause civil liabilities, such as:

- failing to comply with laws when conducting facial verification, recognition, or analysis in business premises and public places;
- failing to disclose rules on the processing of facial information or failing to explicitly state the purposes, methods and scope of such processing;
- failing to obtain the separate consent;
- failing to take proper measures for ensuring the security of facial information which results in leaks, distortion or loss of facial information.

Companies failing to perform obligations under the PIPL and related regulations are also faced with administrative penalties and even criminal liabilities (ie, for infringing citizens' personal information).

8.3 Transparency

In China, chatbots are usually deployed by e-commerce platforms or online sellers to provide consulting or after-sale services for consumers. While there has not been a special regulation targeting the compliant use of chatbots or similar technologies, it does not mean that such use avoids the scrutiny of current effective laws. For example, under the regime of consumer protection law, companies using chatbots to address consumers' questions or requests must ensure the rights and interests of consumers are properly protected; where chatbots are enabled to make decisions based on a user's personal information, the PIPL shall apply.

Furthermore, chatbots providing (personalised) content recommendations may also need to comply with the rules issued by the CAC Algorithm Recommendation Rules. Companies shall pay special attention to the recent CAC Algorithm Recommendation Rules, if their chatbots are equipped with automated content push functions.

Relevant laws have set out transparency requirements on the use of AI-related technology. If such technology involves processing of personal information, processors are required to notify individuals of such processing. There are also transparency requirements for automated decision-making (see **8.4 Automated decision-making**). Users of internet information services involving AI technology are also entitled to be informed of the provision of algorithm-recommended services in a conspicuous manner. According to the CAC Algorithm Recommendation Rules, relevant service providers are required to appropriately publish the basic principles, purposes and main mechanics of algorithm-recommended services.

8.4 Automated decision-making

There are specific rules for automated decisionmaking in the PIPL. Firstly, automated decisionmaking using personal information shall be subject to transparency requirements; processors are required to ensure the fairness and impartiality of the decision, and shall not give unreasonable differential treatment to individuals in terms of trading price or other trading conditions.

Where information feed or commercial marketing to individuals is carried out by means of automated decision-making, options not specific to individuals' characteristics shall be provided simultaneously, or convenient ways to refuse shall be provided to individuals. Individuals whose interests are materially impacted by the decision made by automated means are entitled to request relevant service provider/processor to provide explanations and to refuse to be subjected to decisions solely by automated means.

8.5 Theories of liability

There have been hot debates on the allocation of liabilities in an AI scenario. In a traditional view, the civil law – including tort law – deals with legal relationships between/among civil subjects such as natural persons, companies or other organisations; thus, it seems difficult to treat AI, which is developed by humans through computer programming, as a liability subject. However, such consensus might be challenged considering the strengthened self-learning and independent decision-making ability of AI technology, both now and in the foreseeable future.

From a tort law perspective, the owner of AIenabled technology that harms the interest of others should be directly liable. However, the application of AI technology usually involves a number of roles, such as the AI developer, the product/service manufacturer, the seller and even the user. It must be prudent when defining who is the proper "owner" that should be liable.

Secondly, liability is usually established on the fact

that the infringer is at fault. This brings difficulty when the decision that harms others' interest is made by AI technology which goes beyond the control of the technology user – a typical example is the driver of a car equipped with an autopilot program. Furthermore, even discussing the liability of the developer or provider of the AI technology, it remains a problem for the plaintiff to prove at a technical level that there is an internal design defect in the AI technology, particularly considering the ability of autonomous deep learning of AI as well as the complexity of the external environment that may interfere with AI's decision-making during the interaction.

Therefore, the attribution of responsibility in an AI scenario shall be conducted with sufficient consideration and proper definition of the duty of care of different subjects, combining with the state-of-art, as well as objective factors that may affect the computing process of the AI technology.

9. AI in industry sectors

9.1 Healthcare

As for AI technologies that act as a medical aid during the process of diagnosis and treatment, the Department of Health (currently named the National Health Commission) has issued technical specifications for robot-assisted cardiac surgery in 2012. Apart from that, in 2021, the State Food and Drug Administration issued the Guiding Principles for the Classification and Definition of Artificial Intelligence Medical Software Products, which clearly defines AI medical software as "independent software that uses AI technology to realise its medical use based on medical device data", and medical device data as "the objective data generated by medical devices for medical purposes and in special cases includes the objective data generated by general equipment for medical purposes".

On the other hand, the adoption of AI technology involving processing of data shall also be subject to the data protection laws. As for information related to patients, apart from personal information protection requirements, companies must pay additional attention to rules in the medical and health sector, whereby the use, sharing of patients' medical record is strictly restricted. The use and transfer of medical data may also trigger legal obligations in bio-security laws and may even raise national security issues.

9.2 Financial services

The application of AI technology in the financial sector may have a significant impact on the rights and interests of individuals. For example, it is a common practice for financial institutions to evaluate the credit situation of individuals through automated decision-making. In such case, the rules on automated decision-making in the PIPL shall apply, whereby individuals have the right to refuse the decisions solely by automated means. Financial companies are suggested to make appropriate manual intervention in the decision-making process of AI. In addition, the legality of the data on which the application of AI technology in financial sector is based should be carefully checked. Obtaining information related to personal credit by illegal means may lead to serious liabilities, including even criminal liability.

Apart from these general rules, the People's Bank of China (the PBOC) and other financial regulators jointly issued the Guidance Opinions on Regulating Asset Management Business by Financial Institutions in April 2018, which articulate qualification requirements and human intervention obligations for financial institutions providing asset management consulting services based on AI technologies. In addition, the newly promulgated Implementation Measures for Protection of Financial Consumers' Rights and Interests of the People's Bank of China and Financial Data Security Data Lifecycle Security Specification also form a differentiated financial data security protection requirement covering the whole data life cycle based on data security grading.

9.3 Autonomous vehicles

The Several Provisions on the Manage ment of Automobile Data Security (for Trial Implementation), issued by the CAC jointly with other departments, specified the rules for use of automobile data and identified the scope of important data in automotive industry. The MIIT and other ministries jointly issued the Trial Administrative Provisions on Road Tests of Intelligent Connected Vehicles, effective in May 2018, to regulate the qualification, application and procedure requirements of automated driving road tests and liabilities incurred by road test accidents. At local government level, companies engaging in autonomous driving road tests are required to apply for a professional review for their testing plans and get approvals before implementing a road test. Currently, more than 20 cities have issued their administrative measures for automated driving road test qualifications.

Additionally, road testing of autonomous driving inevitably involves the processing of road and geographic data, which are further subject to the laws regarding surveying and mapping activities.

10. AI and employment

10.1 AI in corporate employment and hiring practices

As businesses turn to automated assessments, digital interviews and data analytics to parse job resumes and screen candidates, the use of AI technology in recruiting has been increasing.

One of the main benefits of AI recruiting is its ability to quickly organise candidate resumes for employers. AI is able to sift through hundreds of resumes, scour candidates for relevant past experience, or other qualities that might be of interest to employers, and ensure the best candidates are screened within minutes. This greatly reduces the time required to review applications.

On the other hand, however, without a broadly representative dataset, it might be difficult for AI systems to discover and evaluate suitable candidates in a fair manner. For example, if the positions in the company have been dominated by male employees for the past years, the historical data on which the AI recruitment system is based may lead to a gender bias, making women who would otherwise be qualified for the job excluded from the candidates list.

As resumes usually constitute personal information, employers using AI technology to process candidates' information shall be subject to the transparency and related requirements under the PIPL, and shall ensure the fairness and rationality of the decision-making process. To best avoid bias, employers are suggested to establish a regular review and correction mechanism for the AI technology used for recruiting and endeavour to mitigate the risk of unfair and unreasonable decision-making. Further, human participation in the entire recruitment process should be guaranteed, so that the interview, evaluation and decision on whether the candidate is qualified shall be mainly processed by humans.

11. Intellectual property

11.1 Applicability of copyright and patent law

When AI-enabled technology/algorithms are expressed in the form of computer software, the software code of the whole set or a certain module can be protected in China under the Regulation on Computers Software Protection. While AI-enabled technology/algorithms are expressed through a technical scheme, it can be protected as a process patent. The latest revision of the Patent Examination Guidelines in 2020 specifically adds provisions for the examination of invention applications that include algorithmic features. In addition, if the development and use of the algorithm is of high confidentiality, such algorithm might be protected as a trade secret or technical know-how.

As for the datasets, it remains unclear in law whether companies or persons could successfully establish ownership over such intangible assets. Recent judicial cases have affirmed the competitive rights of platform operators in the user data they hold from the perspective of the Anti-Unfair Competition Law, and regulations made by certain local governments have tried to formulate a right/interest system for data that involves individuals and enterprises. However, given that different types of data (personal information, important data, state secrets, etc.) are subject to restrictions in different legal regimes, challenges still exist for ownership protection over data, from both a legislative and a practical perspective.

There remains hot debate on whether machines can be the holder of any intellectual property rights. In China, one of the well-known local courts, Shenzhen Nanshan District People's Court, determined in a copyright infringement case in 2020 that articles automatically generated by an AI-written assistant software shall be copyrightable and constitute a work of the legal entity that owns the software. Although recognised as one of the top ten cases in 2020 by People's Court Daily, the court's opinion on whether automatically generated contents are copyrightable still remains controversial, especially considering that an opposite decision has been made by the Beijing Internet Court in another similar case.

12. E-discovery and litigation

12.1 E-discovery and litigation support services

In 2017, the State Council issued the New Generation Artificial Intelligence Development Plan and proposed to establish "smart courts" – that is, "to establish a smart court data platform that integrates trials, personnel, data applications, judicial disclosure and dynamic monitoring

to promote the application of artificial intelligence in evidence collection, case analysis, and legal document reading and analysis".

In this context, various places have begun to make beneficial explorations of artificial intelligence in judicial practice. At present, the use of speech recognition technology to assist in the recording of court proceedings has become a common practice of many domestic courts. For criminal cases, intelligent assistant case-handling systems have been developed and applied at local level, with an attempt to unify evidence standards, formulate evidence rules, and build evidence models. In civil litigation scenarios, certain local courts have adopted a smart trial platform which allows the parties to participate in trials without being in the court, and even without being present at the same time. The AI assistant judge can act as the host of the trial. As long as the parties are online, the AI assistant will guide the parties to present evidence, crossexamination, etc.

It is foreseeable in the future that AI technology will be used in a wider scope for litigation. Trained with a huge amount of case data, artificial intelligence technology will play a greater role in unifying case trial standards and many other aspects.

13. Advising directors

13.1 Advising corporate boards of directors

Regarding the scenario of companies' governance, automated decision-making may more directly and frequently affect shareholders' vested interests and the operation of the business as a whole. It needs to be established whether automated decisions are attributed as decisions by the board of directors or shareholders' meeting. In general, as the automated decision-making scheme is introduced to the company mainly by decisions of the board, there is consensus that such decision shall be considered as a decision of the board or the shareholders' meeting.

Therefore, if there is any adverse impact on shareholders or the whole business operation, the board or the shareholders' meeting shall be responsible.

To mitigate relevant risks, from a technical perspective, ensuring the traceability of automated decision-making results would be a top priority. From a managerial perspective, companies are advised to assess potential risks in business before implementing the automated decisionmaking system, limit the applicable scope of such system if a material adverse impact would incur, and set up a manual review mechanism to check and ensure the accountability of final decisions. Furthermore, to neutralise potential bias that may be inserted in or evolved through the algorithm, it is also advisable for companies to set up an AI ethics committee to overview the internal use of AI.

14. Other

14.1 Hot topics and trends on the horizon

The ethical issue of AI technology has always been a major concern and is hotly discussed in many countries. In September 2021, the National New Generation Artificial Intelligence Governance Professional Committee issued the New Generation Artificial Intelligence Ethics Code, proposing that, when providing AI-enabled products and services, operators should fully respect and help vulnerable and other special groups, and provide corresponding alternatives as needed.

It is also necessary to ensure that humans have full autonomy in decision-making, and that AI shall be always under human control. Under the State Council's New Generation AI Development Plan, the state government intends to initially establish a legal, ethical and policy system of AI regulation by 2025. It is foreseeable that the government will engage more in AI governance, and specific regulations, such as institutional rules on AI ethics, will gradually become clearer.

15. Trends and developments

15.1 Introduction

Artificial intelligence (AI) has become one of the most revolutionary technologies in human history. As summarised by the State Council in its New Generation AI Development Plan, after more than 60 years of evolution – especially driven by new theories and technologies such as mobile internet, big data, supercomputing, sensor networks and brain science, as well as the strong demand for economic and social development – AI has been developing rapidly.

AI industries in China benefit from various market advantages, such as gigantic amounts of data available for machine learning, diverse and huge demand for market applications, and strong policy support.

The Chinese government also actively embraces AI technology and recognises it as a key focus of future economic development. As estimated by the International Data Corporation (IDC), by 2025, the total size of China's AI market is expected to exceed USD18.4 billion and China will account for approximately 8.3% of the global total, ranking second among individual countries.

15.2 Application and development of AI industry

The Chinese Academy of Science recognises eight key AI technologies that have achieved breakthroughs and has identified specific areas of application, including:

- computer vision;
- natural language processing;
- trans-media analysis and reasoning;
- intelligent adaptive learning (which provides each student with a personalised education that suits their character);
- collective intelligence;
- automated unmanned systems;
- intelligent chips; and
- brain-computer interfaces.

Among the industries adopting AI in China, the computer user vision market remains one of the biggest contributors, and machine learning, where intelligent decision-making plays a major role, will be consolidated and achieve growth as the importance of data as a model production factor increases. In addition to the AI technology track, the training and reasoning demand of AI chips that serve as underlying computing power support contributes a lot to the increasing size of the AI industry.

From an academic view, the AI Index 2022 Annual Report released by Stanford University shows that, despite rising geopolitical tensions, the USA and China had the greatest number of crosscountry collaborations in AI publications from 2010 to 2021, increasing five times since 2010. The report further pointed out that, in 2021, China continued to lead the world in the number of AI journals, conference and repository publications.

The Chinese government recognises AI as an important component of national strategy and plans to establish an AI regulatory system shortly. AI is one of the seven key areas of digital industrialisation in the 14th Five-Year Plan, and intelligent transformation will also be the focus of state-owned enterprises in the next three years.

Since 2020, the COVID-19 outbreak has greatly changed the way people live and work; simultaneously, it has also brought great opportunities for the application of AI technology. In terms of pandemic prevention and control, AI has played an important role in monitoring and analysis, personnel and material management and control, medical treatment, drug research and development, logistics support, and resumption of work and production.

15.3 Regulation updates regarding AI

Currently, the regulation over AI is usually combined with specific sectors where AI technology is applied or is closely related. For example, the E-Commerce Law requires operators of e-commerce to provide the consumer with options not targeting their identifiable traits when providing the results of a search for commodities or services for a consumer based on their hobbies, consumption habits, or any other traits thereof. There are similar requirements in the Personal Information Protection Law (PIPL) regarding automated decision-making by use of personal information. There are also rules in the automated driving, medical and financial sectors. For the relevant laws and regulations, please refer to the Artificial Intelligence 2022 China Law & Practice[1].

The year 2021 has been called "the first year of algorithm governance in China". In August 2021, the Cyberspace Administration of China (CAC) issued a public consultation on the Regulations on the Administration of Algorithm Recommendations for Internet Information Services (Draft for Public Comments), which re-stated that users should be provided with options that do not target their personal characteristics or be provided with convenient ways to close them. Subsequently, the CAC and nine other ministries and commissions issued the Guidance on Strengthening the Comprehensive Governance of Internet Information Service Algorithms ("Guidance on Governance of Algorithms"), announcing that China would establish a comprehensive algorithm governance system within three years.

The year 2022 began with the release of the Regulations on the Administration of Algorithm Recommendations for Internet Information Services ("CAC Algorithm Recommendation Rules"), which came into effect in March. Based on internet information services, the regula tion puts forward specific and detailed requirements for

[1] https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2022/china

algorithm recommendation services from the perspective of algorithm fairness and information content management, and clarified the scope of "algorithm recommendation technology", the regulatory principles and rules of algorithm recommendation services, as well as specific classification, filing, security assessment and other regulatory means.

15.4 Law enforcement and judicial practices regarding AI

The abuse of algorithms has received increasing attention from the regulators of different sectors. Based on the Guidance on Governance of Algorithms, the CAC initiated a special action of Clear Algorithm Abuse Governance, and conducted algorithm inspections on more than 300 internet companies across the country, including news media, e-commerce platforms, and video websites. With the coming into force of the Regulations on the CAC Algorithm Recommendation Rules, the CAC continued its enforcement in 2022 and has started the annual special action for algorithm governance, together with other relevant authorities.

This annual action aims to deeply investigate and rectify the algorithm security problems of internet enterprise platforms, evaluate the algorithm security capabilities, with a special focus on examining large-scale websites, platforms and products with strong public opinion attributes or social mobilisation capabilities.

Enforcement activities in other legal fields reflects the multi-dimensional regulation over the application of algorithms. From an antitrust view, the abuse of algorithm by a dominant market player may cause serious consequences, damaging the interests of consumers and market competition.

On 8 October 2021, the State Administration for Market Regulation (SAMR) announced an administrative penalty decision against Meituan, which was found to have abused its dominant market position within the Chinese online food delivery service market. According to SAMR's investigation, Meituan forced its merchants into exclusive co-operation agreements by charging differential rates and slowing down their approvals to list on the app. Meituan also required its merchants to "pick-one-from-two" among Meituan and other rival platforms by charging exclusive co-operation deposits, adopting algorithms, data and other technical means, as well as various punitive measures. All of the above acts constitute an abuse of a dominant market position under Article 17 of the Anti-Monopoly Law (AML), as they have forced, "without justifiable reasons", their trading counterparts to make transactions exclusively with themselves.

Meituan is not the only internet platform behemoth to be imposed with a fine as a result of its "pick-one-from-two" activities via manipulation of algorithms and data. In December 2020, SAMR issued administrative penalties against Alibaba, which was fined CNY18, 228 billion for abusing its dominant position in the domestic online retail platform service market. This was the highest penalty amount in China's antimonopoly enforcement history.

In terms of court decisions, in April 2021, the first case related to face recognition technology ushered in the final verdict. The plaintiff was dissatisfied with a wildlife park's change to the way of entering the park for annual card users, from fingerprint recognition to face recognition, and he brought the park to court on the grounds of infringement of privacy and breach of service contract. The court of second instance decided that the wildlife park's unilateral change in the way annual card users enter the park constitutes a breach of contract, and its intention was to use the customers' photos to expand the scope of information processing goes beyond the purpose for data collection stated previously, indicating that there is a possibility and danger of infringing on the personal interests of the plaintiff. Furthermore, as the park had ceased to use fingerprint gates, the court finally ordered the wildlife park to delete the plaintiff's facial character information as well as his fingerprint recognition information.

This case reflects the judicial protection of personal information in the AI application scenario, which has paid sufficient attention to the principle of "lawful, proper and necessary" for enterprises to process personal information by means of AI technology.

15.5 Focus on AI governance: ethical norms

In AI governance, legal constraints and flexible ethical norms usually go hand-in-hand. Compared with laws and regulations, ethics codes reflect more of a general direction and universal guidance. In China, the National Professional Committee on the Governance of New Generation Artificial Intelligence released the Code of Ethics for New Generation Artificial Intelligence on 25 September 2021, proposing six basic ethical requirements:

- promoting human welfare;
- promoting fairness and justice;

- protecting privacy and security;
- ensuring controllability and trustworthiness;
- strengthening responsibility; and
- enhancing ethical literacy.

The Code thereby aims to integrate ethics into the whole life cycle of artificial intelligence and provide ethical guidelines for natural persons, legal persons and other related institutions engaged in AI-related activities.

Recently, in March 2022, China's State Council issued the Opinions on Strengthening Ethical Governance of Science and Technology, proposing that during the 14th Five-Year Plan period, the government will focus on strengthening the study of legislation on the ethics of science and technology in the fields of life sciences, medicine and artificial intelligence, and timely promote the elevation of important ethical norms of science and technology into national laws and regulations.

Official institutions are endeavouring to establish ethical standards for algorithms. The China Academy of Information and Communications Technology issued the White Paper on AI Governance ("CAICT White Paper"), which lays out ethical standards for using AI, such as that algorithms should protect individual rights. The CAICT White Paper proposed that AI should treat all users equally and in a non-discriminatory fashion and that all processes involved in AI design should also be non-discriminatory. AI must be trained using unbiased data sets representing different population groups, which entails considering potentially vulnerable persons and groups, such as workers, persons with disabilities, children and others at risk of exclusion.

Enterprises, on the other hand, are the protagonists in implementing ethical codes. In recent years, the establishment of ethics-related departments has become an important manifestation of corporate self-regulation. At the 2019 National Congress, Baidu proposed to accelerate AI ethics research and encouraged companies to implement AI ethical principles in product design and business operations. At the 2020 World AI Conference, Megvii proposed three principles for companies to uphold when practising AI governance:

- no absence – deep involvement in it;
- no confrontation – the development of tech- nology, the application of business and the formulation of rules should be complemen- tary; and
- action speaks louder than words – every step of AI governance should be reflected in daily work.

It is foreseeable that more and more technology companies will follow the fast-paced flow of policies and regulations to establish a more complete system and mechanism for the ethical review of AI technology.

AI technology is still in the early stages of industrial application, and many deep-seated ethical issues and their implications have not yet been fully revealed. Therefore, the Chinese authorities are closely tracking the frontiers of technology and widely incorporating the opinions and suggestions of experts and scholars from different disciplines and fields, as well as enterprises and consumers, in order to make scientific and dynamic adjustments to ethical regulations.

Conclusion

At present in China, legislation and law enforcement in many fields have touched on the legal issues arising from the current application of AI technology, including data protection, consumer rights protection and anti-monopoly issues. It is foreseeable that the cross-use of various AI technologies and the updating and iteration of such technologies will inevitably lead to more complicated legal issues.

General questions such as whether AI can qualify as a "human" in a legal sense, as well as specific issues such as whether the "creation" of AI can be protected – and how to assign responsibilities for AI infringing upon the rights and interests of others – will be discussed in depth with the wider and deeper penetration of AI in different industries. On the other hand, ethical and moral requirements will also constitute an important tool for constraint over AI technology.

作 者

宁宣凤

susan.ning@cn.kwm.com

吴涵

wuhan@cn.kwm.com

吴巍

wuwei@cn.kwm.com

刘迎

liuying3@cn.kwm.com

姚敏侣

yaominlv@cn.kwm.com

张浣然

zhanghuanran@cn.kwm.com

徐梦悦

xumengyue@cn.kwm.com

刘艳洁

liuyanjie@cn.kwm.com

赵妍

zhaoyan8@cn.kwm.com

孙乐怡

sunleyi@cn.kwm.com

金杜律师事务所

金杜律师事务所被广泛认为是全球最具创新力的律所之一，能够提供与众不同的商业化思维和客户体验。金杜拥有 3000 多名律师，分布于全球 30 个城市，借助统一的全球平台，协助客户了解当地的挑战，应对地域性复杂形势，提供具有竞争优势的商业解决方案。

作为总部位于亚洲的国际领先律师事务所， 我们为客户发掘和开启机遇，协助客户在亚洲市场释放全部潜能。凭借卓越的专业知识和在核心市场的广泛网络，我们致力于让亚洲走向世界，让世界联通亚洲。

我们始终以伙伴的合作模式为客户提供服务，不止步于满足客户所需， 更关注实现客户目标的方式。我们不断突破已取得的成就，在重塑法律市场的同时，打造超越客户预期的律师事务所。

金杜法律研究院是由金杜律师事务所和金杜公益基金会联合发起成立的非营利性研究机构。自设立以来，一直致力于打造具有国际影响力的中国特色新型智库，依托于金杜律师事务所过往二十多年来服务国家经济建设和法治建设过程中所积累的丰富执业经验和专业洞见，对企业“走出去”战略中面临的重要问题进行分析研究，以提供具有建设性和实操性的政策建议和咨询意见。

金杜研究院
KWM_CHINA