决策参考 2021年11月第18期
（总567期 半月刊）

目录 Contents

编者按：“数据是21世纪的石油。”海量的数据资源与流动规模推动数字经济的蓬勃发展，也带来巨大的安全隐患。大数据时代，数据安全越来越重要。从个人隐私防护到国家关键数据信息保护，数据安全已成为数字经济时代最紧迫、最基础的安全问题，加强数据安全治理已成为维护国家安全和国家竞争力的战略要求。也因此，近年来世界各国都普遍对数据安全保障倾注更多关注和行动。

习主席强调：“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”

今年9月1日起施行的《中华人民共和国数据安全法》是我国首部独立将数据作为保护对象的基础性法律，该法将数据安全工作首次升至国家安全最高监管层级。

随着11月1日《个人信息保护法》的正式开始实施，中国在网络安全和数据保护方面的法律“三驾马车”正式成型。《网络安全法》、《数据安全法》和《个人信息保护法》一起，搭建起我国数据安全治理与保护的“四梁八柱”。

本期推出“数据安全”专题，有针对性选取相关文章，希望能为盐城市相关政府部门提供一些有意义的参考、思索和方向。其他栏目的文章也祈盼引起您阅读的兴趣。

本期专题·数据安全

热点关注

悦读时光

主　　管：盐城市文化广电和旅游局
主　　办：盐城市图书馆
刊头书法：臧　科
主　　编：黄兴港
副 主 编：张安红
责　　编：祁　杰

地　　址：盐城市城南新区府西路6号
邮　　编：224005
电　　话：0515-69971581　18762528568
邮　　箱：1015873743@qq.com
网　　址：www.yctsg.cn

设计制作：江苏凤凰盐城印刷有限公司
印刷单位：江苏凤凰盐城印刷有限公司
印刷日期：2021年11月30日
印　　数：9200-9400

筑牢数据安全防护网

日前，由国家互联网信息办公室会同相关部门研究起草的《网络数据安全管理条例（征求意见稿）》对外公布。

这是国家加强网络数据法治化的又一重要举措，对数据处理企业、数字化转型企业而言，将在搭建数据架构、完善数据合规体系等方面具有促进作用。

数据产生于网络之中，其资源属性也因网络而放大。对数据处理者来说，一方面，掌握的数据越多，平台推荐就越精准，客户黏性就越高；另一方面，掌握的数据越多，数据安全保障责任就越大，数据合规建设更显迫切。

近年来，《网络安全法》《数据安全法》《个人信息保护法》等法律相继出台，对数据安全管理作出明确规定，相关配套法规相继更新完善。

对标法律法规，如何将其落实到企业运营与交易的实际中去，既是企业长期要做且必须做的事，同时企业在实操过程中也产生不少困惑。

数据合规，首先明确了行为边界，知其有所为、有所不为。国家网信部门依照数据安全法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。此次征求意见的条例草案既明确监管部门职责，也对数据处理者提出明确要求，划定行动范围、行为方式、应尽义务等。

从企业运营层面看，以精细化管理保障平台规则、隐私政策、算法公平公正，可以说是数据合规的要义之一。条例草案的规定直接回应“大数据杀熟”、平台“二选一”、低价策略、个人信息保护等热点问题。

值得关注的是，条例草案首次提出，平台规则、隐私政策制定或者对用户权益有重大影响的修订，互联网平台运营者应当在其官方网站、个人信息保护相关行业协会互联网平台面向社会公开征求意见。这是推动数据管理公开透明的创新举措。此外，平台不得在平台规则、算法、技术、流量分配等方面设置不合理的限制和障碍，限制平台上的中小企业公平获取平台产生的行业、市场数据等，阻碍市场创新。

对企业交易层面而言，面临的是数据合规的全链条全过程监管。形成常态化数据安全保障机制，是数据合规的要义之二。

不管是合并、重组、解散、破产，还是境外上市等各类交易场景，都要接受数据监管。今后，企业交易行为触发网络安全审查的门槛将越发严格，符合条件的不仅要主动向监管部门申报、报告，而且每年开展一次数据安全评估。“向境外提供个人信息和重要数据的数据处理者，应当在每年1月31日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况”等规定，都是明确时间节点的“规定动作”，进一步加强了企业自身的数据安全保障责任。

以总体国家安全观为指引，国家构建起保障数据安全的法治体系。数据安全从立法到执法强力推进，监管则日趋精细化、法治化。企业按照数据分级分类管理，做到精细化防护，才能更好落实网络数据安全责任。毕竟，保证企业经营交易行为的正当性、合法性，事关企业发展大计，不可不察，不可不慎。

（2021-11-22　经济日报）

一文读懂《网络安全数据管理条例》

（征求意见稿）

2021年11月14日，国家网信办发布了《网络安全数据管理条例》（征求意见稿）（以下简称《条例》），共九章七十五条。

概括来说，《条例》是在《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三部上位法的基础上制定，在实施细则、责任界定、规范要求、惩罚措施等方面更加清晰细致，同时也增加了一些新的内容，进一步强化和落实数据处理者的主体责任，共同保护重要数据和个人信息的安全。

制定目的

规范网络数据处理活动，保障数据安全，保护个人、组织在网络空间的合法权益，维护国家安全、公共利益。

法律依据

《条例》的制定是以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三部上位法为依据。

数据定义

重要数据：一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

核心数据：关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。

公共数据：国家机关和法律、行政法规授权的具有管理公共事务职能的组织履行公共管理职责或者提供公共服务过程中收集、产生的各类数据，以及其他组织在提供公共服务中收集、产生的涉及公共利益的各类数据。

主体定义

数据处理者：在数据处理活动中自主决定处理目的和方式的个人和组织。

互联网平台运营者：为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

大型互联网平台运营者：用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

适用范围

以向境内提供产品或者服务为目的；分析、评估境内个人、组织的行为；涉及境内重要数据处理。

部门职责

国家网信部门：统筹协调数据安全和监督管理工作。

公安机关、国家安全机关：承担数据安全监管职责。

行业主管部门：承担本行业领域数据安全监管职责。

《网络安全数据管理条例》（征求意见稿）全文解读

一、用好数据，保护数据

“数据开发利用和保障数据安全并重”是《条例》的基调，即我们不仅要促进数据的使用，更要保护数据的安全。

在《网络安全法》《数据安全法》和《个人信息保护法》三驾马车的基础上，《条例》个人信息保护、重

要数据安全、数据跨境安全管理、互联网平台运营者义务等方面进一步细化，将对企业合规风控工作产生广泛的指导意义，也将会对互联网产业和数字生态、数字经济带来深度的、生态性的重组和改造。

二、明确数据分类分级分类保护制度

《条例》第五条明确提出，“国家建立数据分类分级保护制度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。”

众所周知，数据分类分级是数据使用、管理和安全防护的基础，也是数据安全治理中的难点和重点。虽然此前发布的《网络安全法》《数据安全法》《个人信息保护法》已经提及了数据分级分类，以及“重要数据”和“核心数据”的概念，但始终缺乏明确的定义。《条例》进一步界定了一般数据、重要数据和核心数据的区别，同时增加了个人信息保护的范畴。例如，为了进一步明确重要数据的定义，《条例》在第七十三条列举了七大具体类型数据，可为数据合规提供指引，企业可参考相关规定执行。同时，由于不同行业、不同地区数据分类分级的具体规则和考虑因素差异巨大，《条例》还强调“各地区、各部门应对本地区、本部门以及相关行业、领域的数据进行分类分级管理。”其意在于将数据分级分类的标准制定权限下放，制定出针对性的分级分类标准，真正将分级分类落在细处。

三、数据保护措施进一步明确

《条例》对于数据保护技术合规措施进行了详细的说明。

第九条提出，数据处理者应当做好等保工作，重要数据原则上要满足等保三级，以及关键信息基础设施安全保护要求，重要数据和核心数据还需使用密码进行保护。第十条提出，“数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取补救措施。”第十一条提出“数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患，并且要在三个工作日内向关系人进行说明，涉及犯罪者向公安机关报案。如果涉及重要数据或 10 万人以上的个人信息事件，数据处理这还应在八小时内向网信部门或主管部门汇报；事件处置完毕后五个工作日内向网信部门和主管部门再次汇报处理调查报告。

四、网络安全审查范畴进一步扩大

和 2020 年 4 月印发的《网络安全审查办法》相比，《条例》进一步扩大了需要接受网络安全审查的范畴。除“掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”以外，“大型互联网平台运营者实施合并、重组、分立”；“数据处理者赴香港上市，影响或者可能影响国家安全的”；都需要申报进行网络安全审查。同时，“大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。”

五、大型互联网平台迎更强监管

在数据保护上，《条例》体现出“抓大放小”的原则。

无论是“数据处理者合并、重组、分立”还是“发生解散、被宣告破产等情况”，只要涉及重要数据和一百万人以上的个人信息，都应该向设区的市级主管部门或网信部门报告。《条例》还强调，“日活用户超过 1 亿的大型互联网平台运营者平台规则、隐私政策制定或者对用户权益有重大影响的修订的，应

当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。”这意味着，掌握着大量个人信息的大型互联网平台将迎来更强的监管，尤其是国内头部互联网平台企业更是如此。其平台规则和隐私政策将是制度性的，涉及群体利益和公众利益时必定是牵一发而动全身，平台自主性将收到明显限制，企业必须提前做好相应的准备。值得一提的是，《条例》第十八条要求数据处理者“当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。”毫无疑问，《条例》第十八条规定进一步将数据安全放在了明处，彻底改变了以往“普通民众无法了解数据保护的现状”，同时也进一步促进企业规范使用数据，保护数据，减少数据黑箱操作的可能性。

六、个人信息保护

在个人信息保护方面，《条例》主要来源于《个人信息保护法》，但对其中的内容进行了细化，从用户的角度出发，维护了用户应有的权利，让他们可以对企业的不合理要求说“不”。同时也对企业提出了具体的要求，促进它们做好安全合规工作。

1、知情同意权

《条例》的三部上位法都在一定程度上明确了用户的“知情同意权”，在此基础上，《条例》进一步提出了细则，对企业提出了更加具体的要求，进一步明确了用户的知情同意权。《条例》第二十条规定，“数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗。”此举将有效改变当下信息收集“服务协议”和“隐私政策”又长又难懂的情况，要“以清单形式列明”每项功能收集信息的目的、用途等等，用户可以一目了然，不再需要去阅读密密麻麻的文字，对于用户来说无疑是一件幸事。同时，集中展示的内容还包括“个人查阅、复制、更正、删除”等敏感操作的途径；向第三方提供个人信息情形及其目的等；个人信息安全问题的投诉、举报渠道及解决途径，个人信息保护负责人联系方式等；以及产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称和信息收集的规则。《条例》第二十一条规定，“处理个人信息应当取得个人同意”，同时明确“不得使用概括性条款取得同意”；“敏感个人信息应当取得个人单独同意”；“处理不满十四周岁未成年人的个人信息，应当取得其监护人同意”；“不得以胁迫、误导、欺诈、捆绑、批量处理、频繁征求等方式获取个人同意处理器个人信息等。”此外，当“个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。”总的来说，《条例》在个人信息保护上花费了大量的篇幅，详细的叙述了用户享有的知情同意权，将三部上位法个人信息保护的内容以更加浅显、直白地进行告知。

2、信息处理权

《条例》赋予用户自由处理自己信息的权利，包括查阅、复制、更正、补充、限制处理、删除其个人信息、人信息转移等权利。《条例》第二十三条规定，对于以上的操作，企业应执行对应的规定，保障用户拥有信息处理权，包括“不得以时间、位置等因素对个人的合理请求进行限制；不得设置不合理条件；应当在十五个工作日内处理并反馈等。”在转移个人信息时，企业应确定这些个人信息的范畴，包括确定是本人信息，或已获得且不违背他人意愿的他人信息，在信息转移时还需要确认请求人的合法身份，给予相应的风险提示，避免因此造成个人信息泄露事件。

3、不得将人脸、指纹作为唯一认证方式

《条例》第二十五条规定，“不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。”这意味着日后所有互联网产品及线下产品都应提供人脸等生物特征认证以外的其他认证方法。

七、重要数据安全

分类分级的目的就是为了区分一般数据、重要

数据和核心数据，以便采取不同的数据安全保护措施。其中，重要数据作为大多数企业占比最大的数据种类，常成为企业重点保护对象，也是《条例》中需要重点关注的内容。

1、数据安全负责人的地位提升

《条例》第二十八条提出，“重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构，数据安全管理机构在数据安全负责人的领导下履行职责。”这意味着重要数据的识别与保护再次得到加强，从文件上规定了企业内部设立数据安全负责人和管理结构的义务。同时，“数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况”，积极做好事情的决策建议、应急预案、风险监测、宣传培训、处置投诉等安全工作。该规定大大提升了数据安全负责人的在企业内部的地位和权利，也体现出数据安全的重要性。

2、重要数据安全合规要求进一步明确

在提升数据安全负责人的地位后，《条例》对于企业的重要数据也提出了一些列的合规要求，督促数据处理者完成备案、培训、上报等关键操作。其中，第二十九条提出，“重要数据的处理者，也要在识别其重要数据后的十五个工作日内向设区的市级网信部门备案。备案内容包括数据处理者基本信息，处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，以及其他规定的备案内容。”第三十条提出，“重要数据的处理者，应当制定数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。”第三十二条提出，“每年一度自行或委托数据安全服务机构开展数据安全评估，在 1 月 31 日前将上一年评估报告上报至市级网信部门并保存至少三年等。”从上面的规定中不难发现国家对于重要数据安全的重视，对于企业的合规要求直接细化到了最低的颗粒度，其中包括详细的备案内容，以及不少于 20h/y 的安全培训工作等。此外，这样也给企业满足重要数据安全合规指出了具体的方向，企业只需要按照规定完成即可。

3、多项工作需网信部门或主管部门同意

除此之外，政府部门还对企业重要数据处理提出了其他的合规要求。比如开展共享、交易、委托处理、向境外提供重要数据的安全评估，一旦评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。第三十三条提出，“数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。”第三十四条提出，“国家机关和关键信息基础设施运营者采购的云计算服务，应当通过国家网信部门会同国务院有关部门组织的安全评估。”这意味着，当某些操作涉及重要数据时，企业已经不能再完全按照自身意愿处理，而是要在国家政策的同意之下方能进行。

八、数据跨境安全管理

针对数据跨境安全管理，《条例》做出了十分完善的规定，对于数据出境增加了许多限制条件，体现出我国对数据跨境的高度重视。

例如《条例》第三十五条明确提出，数据可以跨境流通，但是首先要通过网信部门组织的数据出境安全评估和满足《网络安全审查办法》的要求，以及其他审查需求，包括数据接收方、合同订立、权利与义务等都需要进行审查和满足规定的条件。该规定进一步明确了数据处理者在数据跨境传输活动中的责任与义务，也给数据跨境提出了具体的实现方式：数据出境后数据处理者依旧要承担数据安全保护的责任，同时还需要向涉及到的每一个用户发布公告并获得同意。这将给企业数据跨境增加了不少限制条件，尤其是涉及国计民生的信息，跨境所面临的难度将会非常高，凸显出我国坚持数据安全大前提的战略构想。此外，《条例》还要求展开数据出境活动的数据处理者应每年编制数据出境安全报告，并在 1 月 31 日前向市级网信部门报告上一年度的数据出境情况，报告应包括接收方的名称与联系方式、数据

出境后再转移的情况、数据在境外的存放地点、存储期限等。

九、互联网平台运营者义务

1、互联网平台合规要求更加明确

《条例》花费了大量的篇幅来说明互联网平台应该满足的合规要求，除了将其可能影响国家安全的数据处理行为纳入网络安全审查范畴外，还对平台规则、隐私政策修订等提出要求。《条例》第四十三条提出，互联网平台的平台规则、隐私政策发生重大更新时需要公示三十日，并广泛听取用户的建议；日活超过一亿的大型平台还“应当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。”同时互联网平台运营者还需要承担第三方数据安全管理责任，且“第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿”，这点对于移动通信终端和预装 APP 同样适用。近年来，因第三方而导致的数据泄露事件层出不穷，很多第三方平台缺乏必要的数据安全防护措施。《条例》的出现将会有效改变这一现状，能否保证数据安全将会成为互联网平台运营者选择第三方合作商的衡量指标之一，并且会体现在合同中，倒逼第三方提高数据安全保护能力。

2、杀熟将被禁止

互联网平台运营者通过已掌握的数据杀熟，定制化推荐广告已经不是什么秘密，针对这些热议的问题，《条例》做出了明确的规定。第四十六条提出，禁止向用户提供产品和服务差异化定价等损害用户合法利益的行为；禁止利用数据诱导用户的行为；禁止最低价销售等损害公平竞争的行为；禁止限制中小企业获取资源等。同时，对于人们关心的定制化推荐广告的行为，第四十九条提出，互联网平台运营者要“对推送信息的真实性、准确性以及来源合法性负责”，且“应取得个人单独同意”，还应该“设置便捷易懂的一键化关闭选项，允许用户重置、修改或调整针对其个人的定向推送参数”，和“允许个人删除定向推送信息服务收集产生的个人信息”。《条例》第五十三条提出，大型互联网平台运营者应每年对平台数据安全进行审计，并将审计结果进行披露。这意味着，大型互联网平台数据安不安全以及数据使用情况，已经不仅仅是企业自己的事情，而是需要接受第三方监督，避免企业出现阳奉阴违的情况，这也是企业需要完成的合规义务之一。

十、执法职责清晰，处罚日渐严格

正如文章开头部门列举出来的一样，《条例》对于各部门的监督和执法职责有了明确的划分，避免出现职责不清的情况。《条例》第五十五条提出，“国家网信部门负责统筹协调数据安全和相关监督管理工作；公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责；工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。”同时还明确了各监督、执法部门的工作范畴，包括“对数据安全进行监督检查”，“对重要数据处理活动的审计”，以及“制定数据安全行为规范，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。”针对互联网平台运营者的违法行为，《条例》也列举出详细的处罚措施，包括不履行《条例》处以金额不等的罚金；对违法处理个人信息的应用程序，责令暂停或者终止提供服务，最高可以处以上一年营业额百分之五的罚金，吊销营业执照，追究直接负责人和直接主管人员的责任，并处罚金。第七十条更是明确指出，“数据处理者违反本《条例》规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任”，值得企业和个人警醒。

十一、总结

随着大数据、物联网、人工智能等新兴技术的发展和应用，数据的价值正在不断上升，不仅是驱动企业发展的核心要素，也直接关系到我国的经济发展、公共利益和国家安全。《条例》的出台，不仅是对《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三部上位法的补充和说明，也进一步明确了网络数据安全管理的具体细则，进一步增加企业和社会对于数据安

中国数据保护官制度存在的问题与应对策略

2021年，数据保护官制度的相关概念频繁出现于大众视野。《个人信息保护法》（以下简称《个保法》）和《数据安全法》接连公布，明确设立个人信息保护负责人或数据安全负责人的必要性；5月13日发布的《广东省首席数据官制度试点工作方案》在全国范围内具有示范引领意义。数据保护官制度在中国立法和试点的土壤中得到滋养，不断完善和发展。然而由于中国数据保护官制度起步较晚，法律制度、监管部门和资质认证体系尚未完善，因此在制度落实、责任平衡、专业人才供给方面出现了一些问题。对此，本文从现存问题入手，从完善相关立法、建立专门部门、完善认证体系、建立行业协会四个方面提出建议，为完善数据保护官制度献言献策。

特别声明，本文中数据保护官制度分为企业和政府两个主体，其中企业为主体的数据保护官职称是“个人信息保护负责人”，政府为主体的数据保护官职称是“首席数据官”。

一、中国数据保护官制度现存问题

中国数据保护官制度主要受2018年欧盟通过的《通用数据保护条例》（GDPR）中设置“数据保护官（DPO）”的影响，现存一些亟需解决的问题。第一，中国数据保护官制度在各企业管理机构和政府部门中没有强制落实；第二，企业的个人信息保护负责人所承担责任重大，而政府的首席数据官则没有承担责任的明确规定；第三，高素质信息保护专业人才稀缺，出现人才供给失衡。

1、数据保护官制度没有强制落实

中国数据保护官制度没有强制在各企业管理机构和政府部门中落实。相较于欧盟GDPR明确规定所有公共机关和符合设立条件的私营企业或组织必

全的认知，进一步巩固了国家数据主权，体现出我国对于数据安全这个大前提不动摇的战略决心。对于个人来说，《条例》的出台让用户进一步了解了对自己的数据拥有哪些权利，强化了个人信息的重要性，使得用户不会再像以前一样放任个人信息滥用而没有任何办法，这将大大缓解当下日渐严峻的个人隐私信息泄露、数据泄露事件的发生。对于企业来说，《条例》详细列举了企业的合规要求，有的甚至已经精确到了小时，也明确了该向哪些部门进行报告等，使得企业能够在合规建设中有的放矢，某种程度上也会强化企业的数据安全防护能力。同时也对当下大数据野蛮发展的乱象进行约束，杜绝大数据杀熟、平台二选一，中小企业获取资源受限等问题，打造一个公平公开的数据市场，促进行业健康、有序的发展。

（2021-11-24　FreeBuf）

须依法设立数据保护官，国内现有的《个保法》、《数据安全法》以及2021年6月2日公布的《深圳经济特区数据条例(征求意见稿)》中，设置数据保护官的法定条件较为有限，且在措辞上都以“应当明确”、“应当制定”为主，缺乏强制性。对于没有设立数据保护官的企业机构或政府部门，现有法律中并没有相应的责罚机制，因此数据保护官的设立存在惰性，难以起到监管数据处理、开展风险评估、进行安全审计、加强数据安全教育的效用。

2、政府数据保护官与企业数据保护官承担责任不平衡

数据保护官在政府和企业两种主体中所承担的责任不平衡，提升了企业中推广普及数据保护官制度的困难程度。《个保法》与《数据安全法》中明确指出，对于不依法履行数据安全保护义务的企业个人信息保护负责人及其主管部门，根据情节严重程度，将被采取从责令改正到吊销业务许可证不等的处罚措施，并加以罚款。而政府部门，目前仅有广东省试点方案在推行首席数据官，且只规定了职责范围，没有相应的法律责任说明。

3、高素质个人信息保护专业人才稀缺，供给失衡

高素质信息保护专业人才稀缺是中国信息安全领域长期存在的问题，企业对人才的争夺加剧人才供给失衡。2017年的一项调查表明，中国近年高校教育培养的信息安全专业人才仅3万余人，而信息安全人才总需求则超过70万人，缺口高达95%，可见人才稀缺的严重程度。而随着相关法律的公布，以及广东试点方案的出台，数据合规行业蓝海到来，个人信息保护负责人、首席数据官职位炙手可热，高素质信息保护专业人才再次成为企业争夺的目标，市场上公开的薪资水平甚至已超过了同等年限的法务或律师，并出现人才供给失衡的现象。

二、中国数据保护官制度为何问题重重

中国数据保护官制度现存问题的主要原因包括法律完善、部门设置、认证体系三个方面。第一，由于中国数据保护官制度起步较晚，数据保护官相关法律尚未完善，仍有值得改进之处；第二，中国监管体系中缺乏个人信息保护部门，因此政府的首席数据官缺少隶属部门、企业的个人信息保护负责人缺乏监管部门；第三，注册个人信息保护专业人员认证体系在项目细化和持续教育政策方面有待完善。

1、数据保护官相关法律尚未完善

(1)设置数据保护官的法定条件存在缺陷。《个保法》第五十二条规定：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应当指定个人信息保护负责人。这项法定条件中只从所需处理的个人信息数据的规模数量出发，没有涵盖需要处理特殊类型、特殊分级数据的组织或机构。

(2)数据保护官的独立履职权缺乏法律保障。根据欧盟GDPR中对于数据保护官法定地位的规定，数据保护官应当拥有独立履职权，即其受聘于数据控制者或数据处理者这一事实不得影响其独立地位。但在中国《数据安全法》和《个保法》中都没有关于确保独立履职权的法条，或将无法避免数据保护官与企业利益勾结的现象，进而可能导致个人信息保护失效。

2、中国监管体系中缺失个人信息保护部门与数据保护官对接

中国现有的数据安全行政监管体系中，公安部负责网络安全保卫，网信办和工信部负责网络安全风险评估，唯独缺失对应监管个人信息保护的专门部门。《数据安全法》第六条规定：国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。这增加了国家网信部门的监管负担，不利于个人信息保护监管的高效进行。同时，个人信息保护部门的空白使得数据保护官制度无法与其对接：首席数据官分散在政府各级部门当中，不隶属于统一监管部门，缺少标准化的执行规定；个人信息保护负责人由企业聘用而在企业缺少有效的宏观监管机制。

3、注册个人信息保护专业人员认证体系尚未完善

注册个人信息保护专业人员(CISP-PIP)是中国目前唯一的国家级个人信息保护专业人员资质评定。对标国际影响力较大的个人信息保护认证项目

“国际隐私专业人员协会”(IAPP)认证,CISP-PIP 仍存在两方面的不足。

(1)资质认证单一,难以直接对应政府和企业数据保护官的不同需求。IAPP 认证作为目前全球顶级的隐私保护认证,包括隐私保护专业人员认证(CIPP)、隐私保护经理认证(CIPM)和隐私保护技术专家认证(CIPT)3 个项目。相比之下,CISP-PIP 认证项目较为笼统,“个人信息保护专业人员”的概念没有细化,较难直接对口个人信息保护负责人和首席数据官的不同需求。

(2)缺乏直接个人信息保护专业人员认证持续教育政策。IAPP 采用持续隐私教育(CPE)政策维持认证证书的有效性。而 CISP-PIP 白皮书中只强调了“资质证书有效期为 3 年,证书失效后需要重新申请”,没有领取资质证书后的持续教育的相关规定,难以有效维持和提高个人信息保护专业人员的专业技能。

三、解决中国数据保护官制度现存问题的建议

根据上文阐述的中国数据保护官制度现存问题与可能原因,本报告主要从完善相关立法、建立专门部门、完善认证体系、建立行业协会四个方面提出建议。

1、完善数据保护官制度相关法律

完善设置数据保护官的法定条件。在现有对于处理个人信息数据的规模数量的条件上,增加对于个人信息数据类别或级别的条件规定:当数据控制者或处理者的司法身份是法院以外的公共机构,其需要对数据主体进行大规模系统和常规化监控的处理操作,核心业务包括对诸如与健康有关的个人数据的特殊类别数据或与刑事定罪和犯罪有关的个人数据进行大规模处理的部分时,必须设立数据保护官。

立法保障数据保护官的独立履职权。个人信息保护负责人受聘于企业这一事实不得影响其独立地位,其履行职权时不受企业高层管理人员的立场或利益关系左右;各级首席数据官受各级部门领导小组任免这一事实不得影响其独立地位,报最高政务服务数据管理部门备案。

2、推动中国个人信息保护监管部门的建立

在公安部、网信办和工信部之外,建立个人信息保护监管部门,减轻原国家网信部门承担的监管压力。个人信息保护监管部门作为政府首席数据官的最高隶属机关,负责定期监管各省常态化首席数据官工作沟通机制、开展各省政务数据部门的绩效评估及复审数据官履职评价等工作;同时,对企业个人信息安全负责人进行宏观监控,与相关行业协会共同建立标准化、合理化的数据保护官行业规定。

3、完善注册个人信息保护人员专业认证体系,加强人才培养

进一步细化 CISP-PIP 项目。可借鉴 IAPP,择机将 CISP-PIP 扩展至 2 类资质认定项目:个人信息保护专业人员,主要适用于企业个人信息保护法律法规、合规审查、信息管理、数据治理、人力资源等领域的从业人员;数据保护专业人员,主要面向来自政府、监管部门以及企事业单位等从事个人信息保护项目管理人员。

逐步建立中国个人信息保护专业人员认证持续教育政策。持续教育主要用于支撑认证证书有效期的维持,也可以服务于国内个人信息保护相关教育、培训等需求,提高专业人才的数量和质量。

4、建立个人信息安全负责人行业协会,使行业规定标准化、合理化

针对高素质信息保护专业人才成为企业争夺的目标、薪资乱抬高、人才供给失衡的问题,可以成立个人信息安全负责人行业协会,建立起有效沟通政府与企业之间个人数据安全监管体系的桥梁,与 CISP-PIP 认证体系一起监督个人信息安全负责人的专业质量和制定薪资标准、数量要求,并积极配合政府监管部门和 CISP-PIP 认证体系展开企业个人信息安全教育与培训、提供咨询服务、举办展览、定期组织会议等等,使个人信息安全负责人行业规定标准化、合理化,形成良好的行业文化和行业氛围。

(2021-11-19 澎湃新闻)

《数据安全法》简析与对贯彻落实工作的建议

经过三次审议，2021 年 6 月 10 日，第十三届全国人大常委会第二十九次会议通过了《数据安全法》。该法于 2021 年 9 月 1 日起施行。

作为我国第一部数据安全领域的专门法律和我国国家安全领域的重要法律，《数据安全法》为保障国家、企业及个人的数据安全，促进数据的开发利用，维护组织和个人的合法权益提供了坚实可靠的法律依据，有助于推动国家数字经济安全健康发展。

《数据安全法》出台的背景

数据安全已成为关乎国家安全与经济社会发展的重大问题。《数据安全法》的出台，既顺应了国际发展趋势，也是保障我国社会经济高质量安全发展的必然要求。

（一）顺应国际发展趋势的需要

各国政府和企业对数据资源的价值与意义已经形成共识，新一轮大国竞争在很大程度上是通过数据增强全球影响力和主导权。各国政府对数据安全的认知，已经从传统的个人隐私保护上升到维护国家安全的高度，而出台数据安全领域的专门立法，则已成为各国各地区保护本国本地区数据的国际惯例。

近几年，美国、欧盟、日本、新加坡、新西兰等国家和地区纷纷出台或修订数据保护法，针对数据发展的新形势新问题，从法律层面加强对本国或本地区的数据安全保护。我国出台《数据安全法》，有助于在国际竞争激烈、跨境活动频繁的国际背景下，维护我国政府、企业和公民的数据安全。

（二）符合国家战略的要求

数据泄露、数据贩卖等数据安全事件频发，给我国社会安全、经济安全、政治安全甚至国家安全带来严重隐患。党中央已经就加强数据安全治理做出一系列重要部署。我国在相继发布的《促进大数据发展行动纲要》（2015）、《科学数据管理办法》（2018）、《关于构建更加完善的要素市场化配置体制机制的意见》（2020）等文件中，均提出发展数字经济、加快培育发展数据要素市场，应把保障数据安全放在突出位置的重要思想内涵。《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出，要“加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护”。出台《数据安全法》，着力解决数据安全领域的突出问题、提升我国数据安全治理能力，是贯彻落实总体国家安全观、切实保障国家数据安全、促进数字经济发展的必然要求。

《数据安全法》的特色

《数据安全法》共七章五十五条，围绕数据安全与发展、数据安全制度、数据安全保护义务等提出系列要求，在进一步完善我国数据安全保护制度的同时，也为企业未来数据合规指明了道路。

（一）坚持安全与发展并重

《数据安全法》最鲜明的特色之一，就是将数据

安全与数据开发利用提升至同等重要的高度。该法设立专章，明确提出“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”，并从技术研发、标准体系建设、检测评估认证、数据交易管理、教育培训、人才培养等多方面，体现数据开发利用和数据安全治理并行的思想内涵。该法虽名为数据安全法，但却不只局限于安全，而是安全与发展并驾齐驱，通过提升数据安全治理能力和数据开发利用水平，共同促进数字经济安全健康高质量发展。

（二）首次确立“国家核心数据”概念

《数据安全法》自一审稿起，便针对不同类型、不同级别、不同危害程度的数据，确立了数据分类分级保护的重要思想。相较于前两次的审议稿，正式出台的《数据安全法》首次确立了“国家核心数据”这一概念，明确关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，并增加了相应处罚措施，规定违反国家核心数据管理制度，危害国家主权、安全和发展利益的，最高可罚一千万元。

2016 年发布的《网络安全法》，首次提出了重要数据的概念，而《数据安全法》在“重要数据”之外又新增了“国家核心数据”概念，更加彰显了贯彻对数据实行分类分级保护的思想，对未来出台数据分类分级统一标准或细则提供了更加精细化的设计思路。此外，从国家安全的角度明确“国家核心数据”概念，并加大违法行为的惩处力度，也反映出国家对数据安全的高度重视。

（三）首次以法律形式明确保护数据权益

《数据安全法》第七条提出：“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展”。这是首次以法律形式提出对数据权益进行保护，为保障相关主体合法权益、规范数据处理活动、培育完善数据要素市场奠定了法律基础。虽然数据权益并非《数据安全法》的主要关注点，但是，其仍将成为未来数据权益保护的重要法律遵循，亦将为后续各地方开展相关立法、明确数据权益等提供上位法依据。

对贯彻落实工作的几点建议

《数据安全法》的出台为我国开展系列数据安全保护工作提供了重要的法律遵循，为进一步推动其落地，有效提升我国数据治理能力，建议做好以下工作。

（一）加快制定数据分类分级原则规范

《数据安全法》提出，要建立数据分类分级保护制度。但是，对于如何分类分级，还没有做出具体的规定。

我国目前正在工业互联网、证券期货等领域探索根据数据价值、敏感程度、危害后果等进行数据分类分级。为推动《数据安全法》相关制度落实到位，建议加快制定数据分类分级原则规范，厘清重要数据的概念和范畴，明确其与国家核心数据的关系，为各行业主管部门制定本行业标准细则提供指导，推进各部门各地区重要数据目录、行业数据重点保护目录以及国家数据分类分级保护目录的形成。在网络安全等级保护、关键信息基础设施重点保护等工作基础上，根据数据处理过程中的安全风险，制定数据分级分类保护指南。

（二）加强数据出境安全管理

多国出于掌控数据资源、维护数据主权等目的，对跨境数据流动做出限制。我国《数据安全法》明确要求，加强重要数据出境安全管理，并对向境外提供重要数据的违法行为设置高额罚款，增强威慑力显著提升。为进一步加强重要数据和个人信息出境管理，防止数据流向境外危害国家安全、主权和发展利益，建议加快研究制定数据出境管理办法，对关键信息基础设施运营者处理个人信息达到规定数量的，建立数据出境安全评估机制；对收集掌握重要数据和个人信息的机构，进行数据出境安全审查。开展数据跨境传输安全管理试点，分阶段分步骤有序推进离岸数据中心试点研究。

（三）积极开展数据安全教育培训

数据安全是公众数字素养教育的重要内容，是数字经济时代公民不可或缺的基本技能。《数据安全法》提出，国家支持开展数据安全相关教育和培训，

《个人信息保护法》实施，如何用好这部法？

11月1日，《个人信息保护法》正式施行。这是一部保护公民个人信息的专门法律，与《网络安全法》《数据安全法》《电子商务法》《消费者权益保护法》等法律共同编织成一张消费者个人信息“保护网”。

近日，围绕我国在个人信息保护和数据安全方面的现状、存在的短板以及如何加强保护等议题，新京智库联合中国法学交流基金会新兴产业发展及法治环境建设专项基金共同举办主题为“《个人信息保护法》落地实施，如何用好这个‘法’”的研讨会，来自北京大学、中国社科院及工业和信息化部网络安全产业发展中心等机构的相关专家参与研讨。

以具体典型案例推动规则落地

新京智库：《个人信息保护法》实施后将发挥哪些作用？如何落实到位？

王利明：《个人信息保护法》要和《民法典》相结合，才能够形成有效适用的一个规则体系。事实上《个人信息保护法》对于个人信息保护规则仍然有限，还有大量的保护规则，必须要从《民法典》里去寻找，所以《民法典》才是兜底性法律。例如，精神损害赔偿，禁令制度等等，《个人信息保护法》就没有具体规定。凡是在《个人信息保护法》里面找不到的保护规则，都得回归到《民法典》去寻找。有人认为《个人信息保护法》已经足以满足对个人信息保护的规定，那这个理解显然是不妥当的，不利于对个人信息的全面有效保护。

薛军：《个人信息保护法》的立意非常好，但它的一些规则还需要去明确和细化。在实施中，可以通过一些具体典型案例来推动规则落地。比如手机的运动数据，单独来看其未必就一定要被界定为个人信息。

现在一些手机名义上叫手机，但实际上是虚拟机。有些网络黑灰产集团利用这种虚拟机来薅羊毛，商家和平台深恶痛绝。对此，一个很重要的识别方法就是收集手机的运动数据，来分析其是否属于正常

并于第二十七条中将其明确为开展数据处理活动的安全保护义务。

建议在以下四个方面加强数据安全教育培训：一是推动将数据安全纳入国民教育体系，加快推进网络安全、数据安全“进校园”，提升中小学生数据安全意识和素养。二是支持高等院校加强数据安全相关学科专业建设，加强课程体系研究、教材编制、教师培训、培养模式创新等工作，支持承担国家重点和专项科研任务。三是支持重点面向关键信息基础设施、掌握大量个人信息和重要数据等单位人员，开展数据安全社会教育和技能培训。四是运用生动案例，网上网下相结合，面向全社会特别是青少年和老年人，加强个人信息保护、数据安全等方面的宣传引导，提升公众数据安全保护意识。

（2021年第7期 《中国信息安全》）

的收集。但如果要经过用户同意才能收集数据，那“羊毛党”通过设置，平台可能就收集不到这些数据，从而影响通过这种方法来识别一些与“猫池”里的虚拟机关联的黑灰产账号。某种意义上这样会损害商业效率。

这就说明在界定个人信息的范围时，一定要根据现实的情况，基于良好的利益衡量来进行界定。通过具体的类似于杭州野生动物园刷脸入园案、微信读书案等个案的精细打磨，慢慢把诸如个人信息的范围和分类的问题具体化，落实下来。在这个过程中，法院是一个很好的抓手，监管部门的专项治理活动等也能发挥积极作用。同时，消协等组织也要发挥积极作用。

《个人信息保护法》的出台，尽管提供了一个很好的法律框架，但目前仍然存在一些问题，需要进一步通过条例、法院裁判规则等加以完善、填充和落地。

《个人信息保护法》的有些条款比较粗线条、框架性，实操性不够；有些则是存在多种理解方式。这些对企业的实际运营而言，都有非常大的影响。

比如该法中一方面强调，企业在为用户提供服务前，要让用户明确是否同意采集个人信息；但同时又规定，如果用户拒绝同意，企业依然需要为用户提供服务。

这对企业而言就是一个难题。因为有些软件的功能，缺乏相应的个人信息是无法正常运行的。值得注意的是，该法更多地体现了监管思维，结合中国当前的语境，其实需要更多地从民法的视角、从损害赔偿的角度，从受害者救济的角度出发。

谢鸿飞：个人信息的损害赔偿是需要及时跟上的必要环节。如果缺乏相应的损害赔偿，那么对于企业而言，可能会将与之相关的大量成本外部化，而非企业本身消化。

《民法典》明确了隐私信息，《个人信息保护法》明确了敏感信息，但在这些之外还存在一般信息。这些信息应不应该保护，保护到何种程度，是个很大问题。尤其是，当这些一般信息被泄露，却既不构成隐私权的损害，也不构成财产权或人格权的损害时，能否从民法上找到对应的损害，就是个问题了。

而在诸如电信诈骗的案例中，受损人无法确定是谁导致了个人信息被泄露，到目前为止，没有看到有个人主动提起诉讼的案例。尽管检察机关有代表受害人提起一些公益诉讼，但这些诉讼的诉求主要是赔礼道歉和删除个人信息等，没有见到有关任何赔偿的内容。这些手段都只是防御、保护性手段。

法律体系要综合运用起来，行政监管和司法必须齐头并进。目前来看，法律的适用或者执法过程中，偏重于行政监管。在目前存在大量个人信息违法的情况下，仅依靠行政监管发挥很大作用是不太现实的。

促进数字经济相关产业发展

新京智库：《个人信息保护法》实施对相关产业将带来什么影响？

李新社：过去，我们不知道平台或者是应用提供方收集了哪些数据，收集这些数据的目的是什么，他们怎么利用这些数据。《个人信息保护法》出台后，明确了不能过度收集无关的个人信息。《个人信息保护法》《数据安全法》的出现，对于产业的推动作用是明显的。

比如，过去人们去酒店住店，要刷脸、要身份证等信息，这些信息都保存在酒店。现在已经有公司在做第三方认证。以后，可能顾客在酒店住店的时候，酒店只需要确认站在面前的这个人是真实存在的，而不需要了解其他个人信息。从产业的角度来讲，这推动了安全产业的发展。

《个人信息保护法》出台实施，一方面提醒了广大消费者注意个人信息，也提醒了企业不能按照过去的玩法过度收集个人信息。从产业发展的角度来讲，又催生了第三方验证，保障信息不泄露、不被滥用等。因此，《个人信息保护法》的意义是相当大的。

许可：《个人信息保护法》绝不只是个人信息保护的法律，还是一部促进数字经济发展的法律。

在过去几年，企业存在着滥用个人信息的行为。但另一方面也要注意到，当数据成为新的生产要素，成为数字经济推动力的时候，个人经过数据化加工后的信息，也成为其中重要的生产要素。对此，企业

实际上也是可以利用的，但非常重要的是，要给企业很重要的激励，让其摒弃滥用和错误的利用，走向正确的利用。这要进一步明确合规免责边界，推动企业用个人信息做好事，而不是做坏事。

《个人信息保护法》第 13 条，在《民法典》的基础之上，增加了六项个人信息处理的正当性事由，体现出在平衡个人信息保护和数字经济发展上非常重要的考量。第 13 条因此也被称为《个人信息保护法》的法眼之所在。所以这部法律是推动中国数字经济健康稳健发展的重要基础。

孙轩：个人信息保护需要负面“处罚”与正面“引导”相结合。除了注意个人信息安全的制度，也可考虑个人信息合法合规利用的疏导。比如对公司、企业是否可以进行使用个人信息的评价体系。如果一个企业使用个人信息非常规范，符合《个人信息保护法》等法规要求，可将其评为“五星”，而做得差的企业，会面临淘汰压力。

方兴东：过去中国互联网行业的发展是“隐私驱动”型的。《个人信息保护法》等法律实施后，会推动互联网行业回归到以科技创新驱动的正常轨道。此外，这还将有助于中国互联网的全球化。互联网巨头必须在个人信息保护方面达到欧美标准，才可能在国外合法经营，持续发展，真正实现全球化。

中国互联网巨头要经历一个估值的重新调整，这个过程跟这些法律会直接相关。目前的几次专项治理行动并不是调整的长期因素，而这些法律会是一个长期的因素。

新法普及增加的企业成本需内部消化

新京智库：企业在网络安全和个人信息保护方面做得如何？今后有哪些新要求？

许可：《个人信息保护法》是一部对企业经营发展非常重要的法律规范。比如，以营业额 5%的金额处罚，比欧盟 GDPR 的 4%还要高，这会是一个非常大的威慑。政府对互联网企业采取强监管的态势，这使得企业将高度重视个人信息保护工作。

《个人信息保护法》实施之后，对企业也提出了一些新的运营要求。比如“单独同意”原则，之前无论是《网络安全法》，还是《信息安全技术个人信息安全规范》，都没有涉及“单独同意”规则。这次针对高风险的个人信息处理行为，比如将个人信息向第三方提供，涉及敏感个人信息，个人信息的公开等，都需要经过个人的“单独同意”。

各个企业内部需要进一步去完善自己的合规体系，有一些企业要设立个人信息保护负责人，一些超大企业要设立个人信息保护委员会，还有的要根据算法要求设立算法隔离委员会等。这些都成为企业落实《个人信息保护法》重要的一环。

《个人信息保护法》是中国对于个人信息保护的一个非常郑重的声明。“这具有积极的信号作用，反映了我国保护个人信息的一种决心。”

《个人信息保护法》第 11 条指出，形成一个政府、企业、社会组织、公众共同参与的个人信息保护的体系，这种各方共同参与的个人信息保护体系也是落实《个人信息保护法》的核心。

相关社会组织可发挥作用。首先，一些行业协会可以发挥标准制定的作用。其次，通过行业形成一些值得学习和借鉴的最佳实践。再者，科技的发展推动最近几年相关的技术得到大量关注。从根本上来说，个人信息的保护来自于科技的完善、发展，这也是解决个人信息保护的重要途径。

公众参与也很重要。公众并不是个人信息的弱者，公众某种意义上说是个人信息能不能被收集的关卡。对公众来说，第一要提升个人信息的素养，不要把一些信息轻易交出去。一些预装的软件、一些明显来源不明的网址不要去打开。第二，《个人信息保护法》充分提升了个人信息的权益，包括查询、查阅、更正、删除、可转移等一系列的权益。个人可以积极去行使这些权益，保护自己在数字空间中的个人信息。第三，适当的情况下，公众可以向相关监管机构提起举报甚至可以发起民事诉讼。

李新社：从保护的角度来讲，《个人信息保护法》起到了保护作用；从产业角度来讲，推动了一些技术创新。

谢鸿飞：《个人信息保护法》肯定会增加一些运行成本，但这是企业必须承担的。《个人信息保护法》规定的一些行为规范，企业在数据合规方面的一些义务，是有利于个人利益和公共利益的。对企业来说，这部分成本应该内部消化，而不应该由外部来消化。

薛军：作为市场主体，企业对于生效的法律都有遵守、落实的责任，这是不容置疑的。但企业普遍存在的一个潜在担忧是，是否会存在某种形式的劣币驱逐良币问题？因为《个人信息保护法》的大量规定，缺乏可操作性的规定，这可能使得一些企业处于观望状态，要看看友商是怎么做的，看看竞争对手是怎么做的。因为对企业而言，做数据合规的成本是很高的，如果大家不是处于同一合规水准之上，做得好的企业，反而可能构成对其市场竞争力的伤害。

我相信企业并没有去做违法行为的内在动力，很多人认为企业好像不监管就一定会违法，其实是不客观的。企业的行为模式其实是服从于市场竞争的逻辑，当企业明确知道某一法律的执行，将会是严格的、公平的，不具有任何选择性的，这时他们都会认真遵守法律。但是当法律的执行带有选择性或者模糊不清的问题时，企业在经营时就可能心存侥幸，主要还是担心自己合规而别人不合规，从而在市场竞争中处于劣势。从这个角度看，执法标准的公平、透明以及统一是极端重要的，是培养企业合规文化的基础。

李新社：如果企业严格遵守了行业规范，但是与商业利益之间存在冲突该怎么办？所以需要在遵纪守法的前提下推动企业发展，这才是立法的根本要求。如果立法后，企业什么都不干了，或者不能干了，不发展了，那就是有问题的。

《个人信息保护法》等一系列法规出台后，企业一方面不能再用过去的思维无限度地扩大自身收集数据的权利。另一方面，企业还需要在法律规范框架内，收集数据、应用等，而且还要做得比原来更好，推动产业发展。

这一方面取决于企业遵纪守法的过程，同时还有一个监管的过程，不能说法律规范出台后企业就会自动去遵守。怎么监管，如何利用监管平台？对企业持续经营、产业长足发展来说，这都是一个挑战。

从政府角度而言，如何在法律出台之后，能够健康快速推进产业长足的发展，也是值得关注的。因为数据是将来社会的基础资源，个人信息作为数据的一部分，也会成为社会资源的一部分。企业如何利用好这些资源给社会创造更大的财富，这需要一个过程。

许可：有句话说，100 次普法不如一次执法。相信在未来两到三个月会有一系列的相关执法行动。

孙轩：随着数字化时代的到来，我们还要考虑怎样基于算法、程序、考评机制等塑造一个全新的数字化社会。即我们一方面要不断完善法律规范，另一方面又要提供一系列服务，执法与服务并举，创建一个更加完善的市场机制以促进经济的发展。当然，很多内容还需要政府、社会、企业来共同合作完成。

国外企业在合规下的经营经验值得借鉴

新京智库：国外在个人信息、数据安全方面有哪些值得借鉴的地方？

薛军：相关法律的适用需要注意一些具体的语境，要考虑国家合规经营的土壤，更要与政府的法治水平相适应。不能把国外一些个人信息保护的问题和相应的做法，跟国内进行简单的横向比较，如果不重视国内的具体情况，单纯把国外的制度挪用过来，有很大的风险性。

谢鸿飞：每个国家都必须考虑自己本土的政治、经济、文化等的情况，但是我们也必须承认，在个人信息保护这个领域，中国和其他国家也有一些共同的地方，这个时候参考域外法的一些方案，还是有启发意义的。

孙轩：欧美国家在个人信息保护问题上的态度一直是比较明确的，执法力度也非常大，使得整个社会都形成了一种产业、行业的自觉性，就是有意识、主动地保护个人隐私。

颁布法律主要是提供一种行为准绳、行为准则，国外的这种个人信息保护的文化值得我们学习。

方兴东：《个人信息保护法》在很多方面借鉴了

长三角一体化发展，如何破局？

以下文章来源于中欧国际工商学院，作者芮萌。

2018 年，长三角一体化上升为国家战略，三省一市的发展进入了新阶段。作为中国区域经济发展蓝图中的先行者，长三角区域一体化建设成果可圈可点。2020 年，长三角地区 GDP 总量已达 24.47 万亿元。随着一体化的持续推进，其辐射广度和深度仍在不断拓展。

在中欧近期举办的 2021 年首届长三角高质量一体化发展论坛上，中欧金融与会计学教授芮萌就区域化经济高质量发展这一主题发表了主旨演讲。芮萌教授认为，区域高质量发展即要达到经济发展的效率和分配公平的最优边界，处理好效率和公平之间的平衡。同时，市场要素自由流动能够加速推动长三角一体化发展。

国际趋势：“大国大城”时代

在百年未有之大变局的背景下，我国提出了双循环战略。其中强调，科技是第一生产力。发展科技，

欧盟《通用数据保护条例》（GDPR）。中国要像过去几十年学习美国的技术创新能力一样，认真学习欧洲在个人信息保护方面的制度创新能力，这不仅直接决定了我们在此方面的更新速度，甚至还决定未来在这方面赶超速度的快慢。

李新社：对企业来说，需要学习借鉴欧盟企业如何在合规的情况下合理合法地做经营。GDPR 颁布之后，很多企业为了合规性在内部做了大量的技术改造工作。这就是法律最终对于市场和发展的一些影响，这是值得中国企业借鉴的。从数据安全角度来讲，我们也应该考虑哪些问题会对国家安全产生影响。这方面西方有些实践对中国有借鉴意义。

许可：中国的《个人信息保护法》对应欧盟来看，有两个非常重要的特点，一个是很多条款过于原则，缺乏可操作性，需要未来出台更细的规则加以补充和落实。第二是没有贯彻基于风险的规制思路，最典型的问题就是对于去标识化的个人信息，没有给予风险减免。

中国可以借鉴韩国和新加坡相关立法，这些国家在某种程度上是吸收了很多欧洲国家的个人信息保护做法，同时又增加了促进数字经济发展的行业规制。

典型的例子就是新加坡对于个人信息保护增加了一个非常重要的合理性事由，那就是基于创新的个人信息的使用。对于企业来说，如果真的是创新活动，就可以使用个人信息。

方兴东：《个人信息保护法》本质上并不是仅仅为了解决当前面临的一些问题，最核心的还是面向未来，这是人类在数字时代面临的共同机遇和挑战。中国在借鉴其他国家经验的同时，并不妨碍突出中国的特色，更不影响中国以后站在别人的肩膀之上去贡献制度创新。

（2021-11-23　新京智库）

就要发展新基建。

未来新一轮基建主要包含“五新”，即新领域、新地区、新主体、新方式、新内涵。新地区即在人口流入的都市圈和城市群适度超前基建，推动区域化发展。

在以上的大图景下，我们可以看到，区域化发展是国家高质量发展的重要抓手。

我们的目标从2018年的“加快培育新生中小城市”到2019年“推动大中小城市协调发展”，这表明城市化发展正迎来一个重要的方向改变。

也就是说，未来城镇化的发展方向不再是中小城市全面而分散的发展模式，而是更加顺应市场规律，在中心或者说在核心大城市圈集中加速城镇化的发展。

2019年4月，国家发改委发布了《2019年新型城镇化建设重点任务》，确定了京津冀、长三角、粤港澳三大都市圈的优先建设地位，今天中国的城市化建设已经进入到大城市化的“大国大城”时代。

这与国际趋势也是相吻合的。目前，区域化发展已经成为全球经济发展的主要模式。

从国际经验来看，人口不断从农村流向城市，从城市流向大城市，是各个国家城镇化普遍的规律。这就是区域经济的趋势。

例如，日本东京的人口占了全国人口的32%，韩国首尔都市圈人口占了总人口的23%。中国也一样，一线城市人口流入远远超过二、三、四线城市的人口流入，区域化经济是未来国家经济发展的主要模式。

那么从经济学角度看，其背后的逻辑是什么？

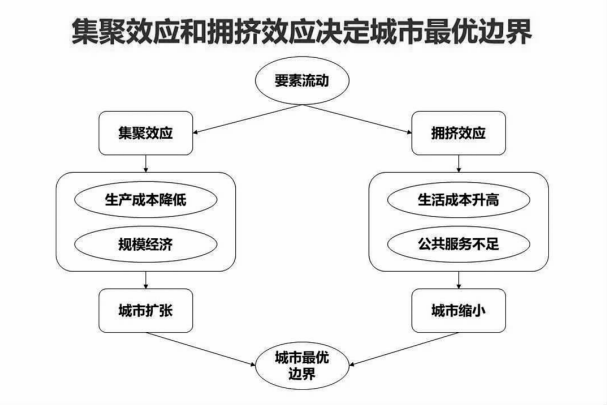
要素流动，有好的一面，也有坏的一面。

好的一面就是集聚效应，集聚效应主要反映在因为规模效应带来的生产成本的降低，这就促进了城市的扩张，也就是都市圈的概念。

不好的一面即拥挤效应，拥挤效应造成了公共服务不足，生活成本升高，这就导致了城市的缩小，所以什么是城市最优的边界，取决于集聚效应和拥挤效应。

从今天的发展来看，集聚效应远远大于拥挤效应，所以各个国家都采取了区域发展这个选择。

七年前，我读到经济学家陆铭教授所著的《大国大城》这本书，给我留下了深刻印象，书里面提了几个观点。



第一，城市化的过程发生得越晚，城市化的速度就会越快，且在城市化率达到70%之前，速度不会慢下来。

第二，城市人口分布有规律可循——Zip’s Law：一个国家第N大城市的城市人口是首位城市人口的1/N。中国城市人口的分布也越来越接近这个规律。首位城市人口跟国土面积没有多少关系，跟本身面积直接相关；跟一国的经济对外开放度直接相关；跟服务业的发展程度有关。

有人担心，“大国大城”时代，人口向大城市集中，一定会带来城市病，这本书指出，城市病主要是技术和管理的问题，和城市的规模不一定正相关。

那么，什么是“大国大城”时代的核心？

“大国大城”时代是一个国家经济高质量发展的时代。

由于规模效应、交易成本、物流成本等，大多数产业具有聚集效应，服务业、高新技术、金融业、制造业表现得更为明显。

人随产业走，人口自然向城市群都市圈集聚，向经济更发达、收入水平更高、更能提供就业机会的地区流动聚集。

“大国大城”时代的核心是高质量的发展，我觉得是要达到经济发展的效率和分配公平的最优边界，即处理好效率和公平之间的平衡。

以往的模式造成了四种差距，即区域差距、贫富差距、城乡差距、行业差距，这是中国目前的情况。我们要通过区域化的经济，弥合过去发展模式引发的差距，提高中国经济增长质量，实现高质量发展。

东京都市圈的案例

区域化发展是国家提高经济增长质量的有效方法。我们可以看一下东京都市圈的发展。

东京都市圈的发展经过了七个阶段，从1956年的《首都圈整备法》开始，从东京都向外延伸100–120公里，形成了当时的首都圈，这是东京湾区的雏形，到1958年第一次首都圈基本规划，限制东京无序蔓延，提出外围地区建立工业卫星城市的构想，到1999年共进行了五次基本规划。

日本东京湾都市圈能够为我们的高质量发展提供什么借鉴意义？

从1999年开始，东京湾都市圈建设了差不多二十年。

首先，随着东京湾区一体化建设的推进，区域内产业结构逐步调整，完成了产业转移和产业升级。东京湾建设的初期，神奈川、东京、埼玉的制造业占比较高，随着湾区建设，制造业向外围县市转移，东京第三产业比重稳步提升。1999年，东京作为核心城市，第三产业占比远高于东京湾其他城市。

第二，东京湾成为了日本国内经济的增长引擎。从1976年到1990年，东京湾GDP增长速度遥遥领先日本全国，经济增量占全国经济增量的比重常年保持在35%以上，同时人口不断聚集在东京湾区域。

第三，区域内收入差距减小，绝对水平高于全国。东京湾区建设初期，山梨县人均收入仅为东京的60.1%；随着区域一体化发展，其余城市的收入水平均提高至东京的70.5%—77.5%，并高于全国平均水平。

我国也基于国际经验，提出了未来区域经济发展的蓝图。

根据该蓝图，我们率先发展三大核心区域，即粤港澳大湾区、长三角一体化、京津冀协同发展，接下来是成渝地区的双城经济圈、海南的自由贸易港、新时代西部大开发，最后整合成黄河流域、长江流域高质量发展。其中，长三角是蓝图中的先行者。

长三角一体化发展有哪些优势？

长三角是中国经济的引擎。从经济总量、人均GDP、GDP增速来看，都领先于全国。2019年长三角地区GDP升至24万亿元，占全国24%（2020年占22%）。

产业结构持续优化。2000–2019年间，长三角地区第一、二、三产业的占比由11:49:40逐步发展为4:41:55，产业结构优化显著；同时战略性新兴产业布局加快，在66个国家级战略新兴产业集群名单中，长三角地区有14个产业入选。

高新技术、战略新兴产业发展迅速。2015–2019年间，江苏、浙江、安徽三省高新技术产业产值/增加值高于规模以上工业平均水平两个百分点。

科创资源丰富，研发投入增加。2014–2018年，长三角地区的研发投入达到了2.4万亿元，取得了很多的成就，比如从发明专利上来看，2008–2018年，长三角地区的发明专利授权量占全国的比重从12%上升到了26%；此外，还拥有上海张江、合肥两个综合性国家科学中心（全国共四个）。

区位优势突出，改革开放走在前列。立足通江达海、承东启西、连南接北的区位优势，长三角地区一直是我国对外开放的前沿阵地，国际联系紧密，对外开放程度高。

制造业在全国领先。长三角地区在电器、机械制造、高端制造、汽车各方面都领先于全国。其中通用设备制造业营业收入占全国45%，电器、机械和器材制造业占全国42%。

区域内的部分产业已经形成完整产业链。以新能源汽车零部件制造为例，长三角地区动力电池生产企业主要分布于浙江临安、江苏南通、安徽芜湖等城市，电动机主要分布于浙江杭州、绍兴等城市，汽车装配则主要分布于安徽芜湖等。

怎样高质量发展：要素自由流动

推动长三角高质量发展，我们需要加速推进区域内协同创新。借助产业发展，加强区域内协同创新，形成科技创新与产业发展的互相促进。目前，长三角区域已加大联合科技攻关力度。2019年4月，上线长三角科技资源共享服务平台（试运行），截至2020年8月初该平台已整合2425家服务机构的3.1万台（套）大型仪器设施，价值逾360亿元。

科创走廊建设是区域内创新协同发展的重要体现。G60科创走廊是沿着G60高速公路建设产城融

合的走廊，立足于人工智能、集成电路、生物医药、高端装备、新能源、新材料、新能源汽车七大战略性新兴产业。

另外，打造世界级生物医药产业集群。2010–2018年间，长三角地区生物医药营业收入占全国的比重从24%提高到27%，对应年均复合增速达11%。目前已经形成产业布局。

加大开放力度，打造国际一流营商环境。从体系建设上，对标国际通行或者更高标准的市场规则体系，打造公平、稳定、透明的营商环境，吸引海外优质投资者植根长三角。从执行上，从国际优质人才引进到货物快速通关，长三角地区从人流、物流、资金流方面不断加大开放力度，增强吸引力。

此外还包括加快都市圈一体化建设，打造数字长三角等等。

政府层面要有机制，并推动市场要素的自由流动，既有政府的手，又有市场的那只手。

在政府机制层面，将现有的机制精简、打通。

市场要素自由流动，推动各城市梯形发展。要素自由流动包含了监管、环境、土地、财政、税收、金融、医疗、异地养老、教育均等化等等。

在监管层面，做到规划协调，标准统一互认。如区域规划共同编制、共同批准、联合印发；实现食品安全、信用体系、环境保护、高新技术成果、执法监控等领域的标准统一和资格互认。

资金层面的一体化方向包含财政投资、税收分配、金融等。如区域内重大基础设施建设、园区合作进行成本分担；对于区域内企业税收按比例分成，激励地方政府推动产业转移；推进区域支付清算、异地存储、信用担保等业务同城化等。

人员层面的一体化方向包括户籍制度、人才认证、社会保障、医疗结算、医疗治疗等。如进一步放开区域内一般县城和建制镇甚至绝大多数中小城市的落户限制；设立社保一卡通制度，实现区域内社保账户互认互通等等。

对标国际都市圈

长三角区域的发展需要与国际都市圈对标。

根据法国地理学家简－戈特曼对城市群的定义，至少2500万人口规模和每平方公里250人以上的人口密度，目前全球有六大公认的世界级城市群，分别是：美国东北部大西洋沿岸城市群、北美五大湖城市群、日本太平洋沿岸城市群、英伦城市群、欧洲西北部城市群、中国长三角城市群。

2017年长三角26城GDP总量为16.54万亿元，2020年GDP总量为24.47万亿元，与其他城市群处于同一级别。

国际城市群

长三角城市群和世界主要城市群对比（长三角数据为2017年，其余为2015年）

城市群	长三角城市群	美国东北部大西洋沿岸城市群	北美五大湖城市群	日本太平洋沿岸城市群	欧洲西北部城市群	英国伦敦城市群
面积（万平方公里）	21.2	13.8	24.5	3.5	14.5	4.5
人口（亿人）	1.52	0.65	0.50	0.70	0.46	0.37
GDP（万亿美元）	2.45	4.03	3.36	3.38	2.10	2.01
人均GDP（美元/人）	16,093	62,030	67,200	48,315	45,652	55,305
经济密度（万美元/平方公里）	1,146	2,920	1,370	9,662	1,448	4,485

资料来源：Wind，国务院《长江三角洲城市群规划》，中信证券研究部

那么，在推动长三角一体化发展的进程中，有哪些行业可以受益？

主要受益行业包括先进制造业、现代服务业等，其中包含了电子信息、生物医药、现代金融、现代物流等重点产业。

这些产业也与前文所述未来新一轮基建中“新领域”所涵盖的行业有所呼应，即在补齐铁路、公路等传统基建的基础上大力发展5G、人工智能、大数据中心、教育、医疗等新型基建，为企业的发展指明方向，提供潜在的巨大的合作空间。

（2021–11–28　新京智库）