“十四五”新征程

数据安全保护的中国方案

——从数据安全法正式施行透视我国数据安全保护与治理

■本报记者　佟欣雨

“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。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。

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，该法与网络安全法以及即将施行的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”。

在中国科学院可持续发展大数据国际研究中心，科研人员在“可持续发展大数据平台系统”监测平台运行情况。该平台是国内首个面向可持续发展目标的大数据云服务基础平台，可为不同用户提供“一站式”数据计算、分析、展示、共享服务等可持续发展目标服务和数据公共产品。

新华社记者　金立旺摄

从“附加题”到“必答题”

法制体系撑起数据安全的“防护罩”

刷脸支付、刷脸过闸机……人脸识别技术的商业化应用越来越普遍，在给人们日常生活带来便捷的同时，背后的安全风险也不容忽视。今年央视“3·15”晚会曝光，部分门店通过布局人脸识别摄像头，在未告知消费者的情况下采集人脸信息，以此对客户进行分类，进而采取不同的营销策略精准促销。

不断进步与创新的科学技术本身是无害的，但若缺乏完善的制度与强有力的监管，就会越过边界带来危害。与有形的资产相比，规模不断扩大的无形数据更易陷入“灰色地带”。今年7月，在第二十届中国互联网大会数据安全论坛上，中国信息通信研究院安全所信息安全部主任魏薇表示，据统计，2020年全球数据泄露的数量已经超过过去15年的总和，数据安全风险的影响范围从个人、企业逐步辐射到产业甚至国家，问题非常突出。

数字经济的“巨轮”行稳致远，离不开数据安全这块“压舱石”，近年来，国家相关领域法律法规相继出台。2018年9月，全国人大常委会将数据安全法列入立法规划；2020年6月，初稿提交全国人大常委会审议；2021年6月，最终稿表决通过；9月1日，数据安全法正式施行。这部法律的出台，为国家重要数据保护和各行业数据安全监管提供了依据，标志着我国在数据安全领域有法可依。

数据安全法的亮点之一就是建立数据分类分级保护制度，“根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。”其中，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，实行更加严格的管理制度。

专家认为，作为该领域的基础性法律，数据安全法从顶层设计的角度提出数据分类分级，成为今后维持数据保护和利用之间平衡的一个重要依据，为细化政务数据、企业数据、工业数据和个人数据的保护措施奠定法律基础。未来将对数据全生命周期状态进行梳理，根据不同的数据敏感等级以及数据使用状态，统筹规划相应数据保护策略，确保数据安全全程可控。

“可用不可见”

推动关键技术创新自主可控

早在20世纪80年代，中国科学院院士姚期智曾提出一个著名的“百万富翁”设想：两位百万富翁在街头相遇，他们想比一比谁更有钱，但是出于隐私，都不想让对方知道自己到底拥有多少财富。如何在不借助第三方力量的情况下，让他们知道谁更有钱？

这个看似无解的难题，反映了数据使用权和所有权之间的矛盾。经过近40年的发展，由这个设想搭建的理论框架逐步变为现实，使用加密处理、多方计算等方法来处理用户隐私数据的计算方式——隐私计算，助力实现数据“可用不可见”，目前已应用于政务服务、金融、医疗等领域。

数据安全防护关键技术是数据安全和隐私保护的基础。从软件到硬件，从互联网边界到内部，从事先防范到事后追溯，数据安全防护的全流程和全领域都离不开关键技术的应用与突破。

走进超市，进口冰激凌、奶酪等销售专区都贴上了“北京冷链”专属二维码。消费者扫描二维码，可以查询进口冷链食品的质量安全和产品追溯信息，入境货物检验检疫证明、核酸检测报告、消毒信息等内容一目了然，为新冠肺炎疫情常态化防控增添一重保障。

今年1月，北京市开始发放首套电子印章。新开办企业在获得电子执照的同时，可以免费获得包括法定名称章、发票专用章、财务专用章等在内的一套电子印章，与实物印章具有同等法律效力，实现签章应用信息可查、可控、可追溯。

这些场景的应用都依托国内首个自主可控区块链技术体系——“长安链”，目前支持食品安全链、电子印章、碳交易等200余个应用场景。值得一提的是，“长安链”已实现软硬件全部由国内自主研发。

数据安全产品的核心技术是数据安全的“砝码”。数据安全法的正式施行，有利于推动数据安全防护技术的研究和应用，推动数据基础设施的基础软件自主可控，拿出数据安全的中国方案。

从安全产品的简单堆砌到数据安全的全流程治理，从提供产品到提供服务，不仅需要技术手段创新，更离不开专业化技术人才队伍。统计显示，未来10年间我国信息安全人才总需求量为140万人，而当前人工智能、密码学等相关领域高校毕业生仅3万余人，人才缺口高达98%。近年来，我国各部门正通过设立相关学科与研究院、开展培训考核、建设大数据安全人才培养基地等方式，加强数据安全人才队伍建设。

行业风口已现

我国数据安全产业链初步形成

如果将数据安全治理手段组合成金字塔状的稳定结构，相关领域的法律法规就像塔尖，从顶层设计的角度对应用数据要素的各项行为加以规范；不断突破和创新的关键技术可以实现数据全生命周期的防护，为数据搭建起完备坚固的“金钟罩”；作为金字塔最坚实、面积最大的地基，则应是数据安全的产业基础。

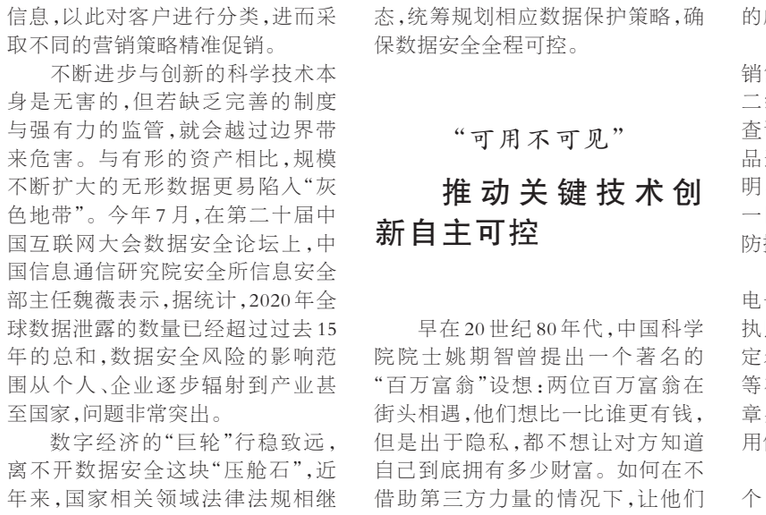
“加强数据安全的意义是让数据要素在全生命周期得到保护，最终实现价值变现，促进数字经济健康发展。”不少专家表示，没有安全健康的产业基础作为支撑，数据要素和数字经济就是空中楼阁，数据安全就失去了依托。

数据资源的价值通过数据的流通与交易实现，这是数字经济发展的基础。而在此过程中，数据使用又必须明确数据保护的责任，特别是对个人信息的保护。为此，数据安全法将数据安全与发展放在同等重要的位置：“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。”

近年间，企业数据安全产品和解决方案在行业场景和新基建中的应用不断落地，数据安全防护在政务、金融、交通、医疗等各行各业都逐渐得到广泛应用。

2018年，贵州省贵阳经济技术开发区创建全国首个“大数据安全认证示范区”，截至2020年，全区已聚集大数据安全企业和相关机构约120家，初步构建起产业发展生态体系。工业和信息化部数据显示，到2023年，我国网络安全产业规模将超过2500亿元，年复合增长率超过15%。

可见，我国数据安全产业链已初步形成，随着数据安全法的颁布实施，产业链将朝着更高阶段迈进。专家认为，这势必要求打通数据孤岛，构筑开放、公正、安全、合作的产业生态，促进数字经济健康发展。



斩断“杀熟刀”

同一平台上的同一款产品或服务，对“熟客”的报价可能要比新用户更高。近年来，一些商家通过收集、分析个人信息进行“大数据杀熟”，受到社会各界诟病。8月20日全国人大常委会表决通过的个人信息保护法，对“大数据杀熟”等问题作出规定。　新华社发

保护经济社会运行的“神经中枢”

——国务院政策例行吹风会解读《关键信息基础设施安全保护条例》

关键信息基础设施是经济社会运行的“神经中枢”，是网络安全的重中之重。今年9月1日，与数据安全法同时施行的还有《关键信息基础设施安全保护条例》（以下简称《条例》）。日前举行的国务院政策例行吹风会上，相关部门负责人对此进行了解读。

什么是关键信息基础设施

《条例》第二条明确，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

关键信息基础设施安全保护面临怎样的形势和问题

当前，关键信息基础设施面临的网络安全形势依旧严峻复杂，网络攻击威胁上升，特别是新冠肺炎疫情发生以来，高级持续性威胁、网络勒索、数据窃取等事件频发，危害经济社会稳定运行。

《条例》确立的保护工作总体思路和责任体系是什么

国家互联网信息办公室副主任盛荣华表示，《条例》的施行进一步压实各方责任，包括运营者的主体责任、保护部门的监督管理责任以及社会各方面的协同配合和监督责任。

其中，运营者的主体责任是基础和关键，《条例》设置专章细化有关规定和要求，提出运营者应当设置专门安全管理机构、每年至少进行一次网络安全检测和风险评估等。

（本报综合各媒体报道）

图解　我国数据安全的法治建设之路

近年来，我国陆续发布了一系列数据及其安全相关的法律法规和标准规范，数据资产价值得到确认。政府部门、企业持续加大在数据治理、数据存储、数据保护、数据加密等方面的重视程度和投资力度。

2020年3月

全国信息安全标准化技术委员会发布《信息安全技术 个人信息安全规范》标准，针对个人信息安全问题，规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的行为，禁止个人信息非法收集、滥用、泄露等。

2020年4月

2020年4月《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》发布，首次明确数据成为继土地、劳动力、资本和技术之外的第五大生产要素。

2020年6月

12部委联合发布的《网络安全审查办法》实施，推动建立国家网络安全审查工作机制，明确关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应按照有关要求进行网络安全审查，确保关键信息基础设施供应链安全。

2021年8月

十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，明确通过自动化决策方式向个人进行信息推送、商业营销，应提供不针对其个人特征的选项或提供便捷的拒绝方式；处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息，应取得个人的单独同意。

个人信息保护法将于11月1日起施行

2021年9月1日

数据安全法正式施行，从法律层面清晰定义数据活动、数据安全，提出国家将对数据实行分类分级保护、开展数据活动必须履行数据安全保护义务承担社会责任等。

国家安全法、网络安全法、数据安全法、个人信息保护法与其他规范形成配套组合，为保护国家关键数据资源安全和个人信息数据安全提供法律依据。

资料来源：国家工业信息安全发展研究中心、《数据安全白皮书》

资料整理：佟欣雨　　制图：扈 硕