国家工程研究中心和天枢智库联合出品

数字安全观察

DIGITAL SECURITY INSIGHT

数据安全专刊 No. 002(总第 102 期)

责编：钟力 zhongli1@360.cn

导　读

第二期《数字安全观察·数据安全专刊》发布在 2021 年底，以回顾总结全年的数据安全发展态势为重点，分为数字经济与数据安全形势、国内外政策法规分析、年度数据安全事件分析和专家观点四个板块，主要内容如下：

数字经济与数据安全形势方面，随着数据要素价值的凸显以及国家、地方和行业领域层面数据安全相关政策文件的颁布施行，我国数据安全产业迎来高光时刻。该部分从政策指导文件、数据安全开发利用、数据安全技术与产品、数据处理活动安全等四个维度，采用里程碑事件描述和综合评论的方式，梳理和展示了 2021 年数字经济和数据安全的演进脉络，以期清晰地为大家展示数据安全发展态势。

国内外政策法规分析方面，在经济全球化背景下，世界主要国家和地区数据立法竞相提速，随着《数据安全法》和《个人信息保护法》的颁布施行，国内数据安全监管管理框架逐渐形成，同时，各地积极出台数据条例，有效推动数据应用发展。该部分在政策法规概述基础上，重点对数据分类分级、数据出境安全、地方数据条例以及数据安全监管作出了深度的梳理与解读。

数据安全事件分析方面，主要基于大数据协同安全技术国家工程实验室 2021 年发布的系列《全球数据安全观察》周报中收录的数据安全事件，从多个维度进行梳理和总结分析。整体来看，2021 年发生的数据安全事件仍以数据泄露类型为主，在所有事件中占比最高；其

次，勒索攻击今年依旧比较活跃，占比为 27%；由于今年全球强监管的整体态势，数据合规事件也占到 8%的比例。从数据安全事件行业来源来看，信息传输、软件和信息技术服务业以 39%的比例位居行业之首，其次，政府机关、卫生和社会工作、金融业也都是数据安全事件频发的行业。

专家观点方面，本期汇聚了知名院士、业界专家、学界代表的精彩语录。聚焦数据安全发展热点，以主旨演讲以及研究观点精选的方式，给读者带来一次覆盖数据安全领域不同身份的观点合集，旨在展现数据安全行业新趋势，凝聚行业新气象，解读未来数据安全发展新风向。

目 录

第一部分 数字经济与数据安全形势

P1 法律法规和政策指导文件

P10 数据安全开发利用

P15 数据安全技术与产品

P23 数据处理活动安全

第二部分 国内外政策法规分析

P28 政策法规发展概述

P32 数据分类分级合规政策重点解读

P43 数据出境安全评估重点解读

P50 地方数据条例重点解读

P58 数据安全监管审计提上日程

第三部分 年度数据安全事件分析

P63 整体态势分析

P65 数据泄露事件分析

P69 勒索攻击事件分析

P71 数据合规事件分析

第四部分 专家观点

P72 互联网企业要加强数据安全意识

P72《数据安全法》为各行业数据安全提供了监管依据

P73 保障数据安全需建立主动免疫保障体系

P74 智能网联新能源汽车数据安全如何保障

P76 用好大数据，要运营安全两手抓

P77 广泛提升数据安全能力，保障数据权益，促进数据利用

P78 数据开放流通环境下的数据安全新问题

P80 做好数据分类分级的后半程

P82 构建基于 DSMM 的数据安全治理体系

P83 建设以数据为中心的安全保障体系

P84 全球数据安全：认知、政策与实践

P86 数据安全风险评估应具备时代特性

P86 从《数据安全法》视角探讨重要数据保护

一、数字经济与数据安全形势

2021 年被称为数据安全元年，《数据安全法》、《个人信息保护法》和《关键信息基础设施安全保护条例》正式发布实施，国家互联网信息办公室（以下简称“国家网信办”）对外发布《网络安全审查办法（修订草案征求意见稿）》、《数据出境安全评估办法(征求意见稿)》和《网络数据安全管理条例（征求意见稿）》公开征求意见，各部委、地方省市和行业领域也都纷纷发布数字经济和数据安全相关的政策文件，提出具体的行动方案并开展相关建设，我国数字经济与数据安全发展呈现一片欣欣向荣之势。本部分从**政策指导文件、数据安全开发利用、数据安全技术与产品、数据处理活动安全**等四个维度，采用里程碑事件描述和综合评论的方式，梳理今年数字经济和数据安全的演进脉络，希望能够清晰地为大家展示当前数据安全的发展态势。

（一）法律法规和政策指导文件

1、国家层面的法律法规和政策文件

（1）概述

2021 年国家陆续发布与数字经济和数据安全相关的法律法规和政策指导文件，保障数字经济健康持续发展。政策指导文件包含《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》、《提升全民数字素养与技能行动纲要》、《国家安全战略（2021—2025 年）》等；法律法规包含《数据安全法》、《中华人

民共和国个人信息保护法》、《关键信息基础设施安全保护条例》和《网络数据安全管理条例（征求意见稿）》等。同时，中国也积极寻求国际合作，促进世界数字经济和数据安全的发展，例如，与阿拉伯签署《中阿数据安全合作倡议》等。

（2）政策指导文件

2021 年 3 月 11 日，《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》正式发布。《纲要》指出，要加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。

11 月 5 日，中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》，对提升全民数字素养与技能作出安排部署，提出 2035 年基本建成数字人才强国，全民数字素养与技能等能力达到更高水平，高端数字人才引领作用凸显，数字创新创业繁荣活跃，为建成网络强国、数字中国、智慧社会提供有力支撑。行动纲要围绕七个方面部署了主要任务，一是丰富优质数字资源供给，二是提升高品质数字生活水平，三是提升高效率数字工作能力，四是构建终身数字学习体系，五是激发数字创新活力，六是提高数字安全保护能力，七是强化数字社会法治道德规范。

11 月 18 日，中共中央政治局召开会议审议《国家安全战略（2021—2025 年）》等文件。会议强调，必须坚持把政治安全放在首要位置，统筹做好政治安全、经济安全、社会安全、科技安全、新型领域安全等重点领域、重点地区、重点方向国家安全工作。要持续做好新冠肺

炎疫情防控，加快提升生物安全、网络安全、数据安全、人工智能安全等领域的治理能力。

11 月 30 日，工业和信息化部印发“十四五”大数据产业发展规划。提出推动建立市场定价、政府监管的数据要素市场机制，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系。培育大数据交易市场，鼓励各类所有制企业参与要素交易平台建设，探索多种形式的数据交易模式。该规划指出要强化大数据安全顶层设计，落实网络安全和数据安全相关法律法规和政策标准，开启数据安全铸盾行动。鼓励行业、地方和企业推进数据分类分级管理、数据安全共享使用，开展数据安全能力成熟度评估和数据安全管理认证。加强数据安全保障能力建设，引导建设数据安全态势感知平台，提升对敏感数据泄露、违法跨境数据流动等安全隐患的监测、分析与处置能力。

（3）法律法规

2021 年 9 月 1 日，《数据安全法》正式实施。360 大数据协同安全技术国家工程实验室从大数据安全开发利用的角度，对《数据安全法》进行了解读，认为《数据安全法》明确了几方面内容：一是，明确数据安全各方职责；二是，鼓励数据安全、合法、有序流动；三是，数据开发利用和数据安全相互促进；四是，建立数据安全管理制度；五是，确保政务数据安全；六是，法律责任更加明确，最大金额 1000 万。

9 月 1 日，《关键信息基础设施安全保护条例》（以下简称《条例》）正式施行。《条例》从关键信息基础设施的范围及认定、运营

者责任义务、保障和促进、法律责任等方面给出了明确的指导和要求，要求关键信息基础设施相关企业建立健全网络安全保护制度和责任制，制定网络安全应急预案，开展网络安全监测、检测和风险评估工作，采取安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用，违反本条例规定将会受到行政处罚、判处罚金甚至要承担刑事责任。

11 月 1 日，《中华人民共和国个人信息保护法》正式施行。作为中国首部针对个人信息保护的专门性立法，《个人信息保护法》明确，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；个人信息处理者利用个人信息进行自动化决策，不得对个人在交易价格等交易条件上实行不合理的差别待遇。同时，针对大数据杀熟和个人信息用户商业活动作出明确规定。对于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，该法特别规定了其需要履行的义务。

2021 年 11 月 14 日，国家网信办会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》，向社会公开征求意见。该条例是为落实网络安全法、数据安全法、个人信息保护法等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益而制定的。征求意见稿提出，国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，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。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。

（4）国际合作

2021 年 3 月 29 日，外交部副部长马朝旭同阿拉伯国家联盟首席助理秘书长扎齐举行中阿数据安全视频会议，双方签署并发表《中阿数据安全合作倡议》。双方一致认为，在当前数字经济迅猛发展、数据和网络安全风险突出背景下，达成《中阿数据安全合作倡议》具有重要特殊意义，标志着双方数字领域战略互信和务实合作进入新阶段。双方愿以此为契机不断深化合作，共同推动全球数字治理和国际规则制定。

2、地方层面的政策法规文件

（1）概述

各地方政府纷纷出台适合本地实际情况，与数据相关的法律法规和政策指导文件，保障各地数字经济和数据安全的发展。例如，广东省政府办公厅印发《广东省首席数据官制度试点工作方案》、深圳市印发《深圳市首席数据官制度试点实施方案》、国内数据领域首部综合性立法《深圳经济特区数据条例》正式颁布等等，已经有 11 个省份出台了与数据相关的条例。

（2）广东省

2021 年 5 月，广东省政府办公厅印发《广东省首席数据官制度试点工作方案》，鼓励试点单位先行先试，强化跨部门、跨层级、跨

领域统筹协同机制，为全面落实首席数据官制度积累可复制、可推广的经验做法。首席数据官的职责将侧重于统筹数据管理和融合创新，推进公共数据共享开放和开发利用；领导本行政区域内数据工作，对信息化建设及数据发展和保护工作中的重大事项进行决策，协调解决相关重大问题；组织制订数据治理工作的中长期发展规划及相关制度规范，推动公共数据与社会数据深度融合和应用场景创新。

6 月 29 日，《深圳经济特区数据条例》获深圳市七届人大常委会第二次会议表决通过，拟自 2022 年 1 月 1 日起实施。该条例内容涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，是国内数据领域首部基础性、综合性立法。针对 APP 过度收集个人信息、强制索要用户授权这一问题，率先提出“数据权益”，明确自然人对个人数据依法享有人格权益，包括知情同意、补充更正、删除、查阅复制等权益；自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益，可以依法自主使用，取得收益，进行处分。

8 月 9 日，深圳市人民政府办公厅关于印发《深圳市首席数据官制度试点实施方案》，旨在进一步完善公共数据共享协调机制，加强公共数据开发利用，推动公共数据与社会数据深度融合，加快培育数据要素市场。

8 月 31 日，珠海市正式发布《珠海市关于加强隐私计算在城市数字化转型中应用的指导意见》，成为国内首个以“隐私计算”命名的政策文件。它明确指出要充分发挥隐私计算在城市数字化转型中优

势，推动数据要素有序流通及利用，为珠海市建设新时代中国特色社会主义现代化国际化经济特区注入新活力和新动能。

（3）上海市

11 月 25 日，上海市第十五届人大常委会第三十七次会议 25 日表决通过了《上海市数据条例》（下称《条例》），为上海全面推进城市数字化转型提供基础性制度保障。据此，上海将健全公共数据治理体系，建立数据安全治理体系；上海将在浦东设立数据交易所，在临港新片区推进国际数据港建设。《条例》共十章九十一条，分为总则、数据权益保障、公共数据、数据要素市场、数据资源开发和应用、浦东新区数据改革、长三角区域数据合作、数据安全、法律责任和附则。数据作为一种新型生产要素，已和其他要素一起融入经济价值创造过程，成为推动经济高质量发展的新动能。对上海而言，全面推进数字化转型是实现超大城市治理体系和治理能力现代化的必然要求。

（4）其他省市

加强数据安全保护和监督管理制度建设，各地已经行动起来。目前，已有山东等 11 个省份出台了与数据相关的条例（包括大数据条例、数据条例、数字经济条例，统称为“数据条例”）。数字化发展时代，全社会数据总量将爆发式增长，而打通数据流动通道，提供快速的数据分析能力，离不开构建完善的数据产业生态，建设数字基础设施势在必行。

3、行业领域层面的政策文件和标准规范

（1）概述

各行业领域陆续发布适应本行业实际情况的政策指导文件和标准规范，保障本行业数字化转型和数据安全的健康持续发展，例如交通部发布《交通运输政务数据共享管理办法》、中国人民银行发布金融行业标准《金融数据安全　数据生命周期安全规范》和信安标委发布《汽车采集数据处理安全指南》等等。

（2）交通领域

4 月 6 日，交通运输部于印发《交通运输政务数据共享管理办法》。为规范交通运输政务数据共享，推动交通运输数字政府建设，加快建设交通强国，依据国务院关于政务数据共享管理要求，制定《交通运输政务数据共享管理办法》，用于规范交通运输部及部际、部省相关政务部门因履行职责需要提供和使用政务数据的行为。

2021 年 5 月 12 日，为加强个人信息和重要数据保护，规范汽车数据处理活动，根据网络安全法等法律法规，国家网信办会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》。这是我国首个汽车数据安全方面的管理规定，是中国构建智能网联汽车网络安全体系的重要一环。它聚焦于国家安全和公共利益，将加强个人信息和重要数据保护，对数据全生命周期的安全管理进行了框架设计。

8 月 12 日，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》。《意见》分为“总体要求、加强数据和网络安全管理、规范软件在线升级、加强产品管理、保障措施”共 5 个部分、11 项内容。《意见》明确管理范围为智能网联汽车生产企业及其产品，明确企业应落实主体责任，加强汽车数据安全、网络

安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性。

9 月 16 日，工业和信息化部发布《关于加强车联网网络安全和数据安全的通知》。通知指出，要加强智能互联车辆的安全防护，加强车联网安全防护，加强车联网服务平台的安全防护，加强数据安全防护，完善安全标准体系。在加强车联网网络安全防护方面，各相关企业应建立网络安全监测预警机制和技术手段，对智能车联网进行网络安全相关监测，车辆互联网服务平台和联网系统，及时发现网络安全事件或异常行为，并按规定保存相关网络日志不少于 6 个月。

标准方面，10 月 11 日，信安标委发布了《汽车采集数据处理安全指南》。该指南规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求，明确了其适用于汽车制造商开展汽车的设计、生产、销售、使用、运维，也适用于主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估。

（3）金融领域

2021 年 4 月 8 日，中国人民银行正式发布金融行业标准《金融数据安全　数据生命周期安全规范》（JR/T　0223—2021）。本标准在数据安全分级的基础上，结合金融数据特点，梳理数据安全保护要求，形成覆盖数据生命周期全过程的、差异化的金融数据安全保护要求，并以此为核心构建金融数据安全管理框架，为金融业机构开展数据安全保护工作提供指导，并为第三方安全评估机构等单位开展数据安全检查与评估提供参考。

9 月 30 日，央行发布《征信业务管理办法》，自 2022 年 1 月 1 日起施行，过渡期截至 2023 年 6 月底。该办法是《征信业管理条例》的配套制度，以征信业务全流程合规管理为主线，以明确征信业务边界、加强信息主体权益保护为重点，完善了数字征信时代的征信业法制框架。

（4）医疗领域

2021 年 4 月 6 日，为扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理安全开发利用，国家医疗保障局于印发了《加强网络安全和数据保护工作指导意见》。医疗保障信息化是医疗保障事业高质量发展的基础，是医保治理体系和治理能力现代化的重要支撑。为全面落实国家领导人总书记关于网络强国战略、大数据战略、数字经济的重要指示批示精神，以及党中央关于网络安全工作的总体部署，扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理安全开发利用，现就加强医疗保障网络安全和数据保护工作，提出《加强网络安全和数据保护工作指导意见》。

（二）数据安全开发利用

1、构建全国一体化大数据中心

2020 年 12 月 23 日，国家发改委发布了《关于加快构建全国一体化大数据中心协同创新体系的指导意见》。《意见》指出，加快构建全国一体化大数据中心协同创新体系，是贯彻落实党中央、国务院

决策部署的具体举措。以深化数据要素市场化配置改革为核心，优化数据中心建设布局，推动算力、算法、数据、应用资源集约化和服务化创新，对于深化政企协同、行业协同、区域协同，全面支撑各行业数字化升级和产业数字化转型具有重要意义。

2021 年 5 月 24 日，国家发改委、中央网信办、工业和信息化部、国家能源局联合印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》，明确提出构建国家算力网络体系。该方案提出试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率，给出了当前突破数据流通瓶颈的技术路径——促进以隐私计算为代表的数据流通技术的应用。

2、各地/区域大数据交易中心纷纷成立

为推动数据要素市场化配置和数字经济高质量发展，北京、上海、天津和贵州等地纷纷建立大数据交易中心，且贵州大数据交易中心促成了第一笔数据交易。数据交易是以技术促流通，以流通促创新，探索数字经济的新产业、新业态、新模式。

（1）北京国际大数据交易中心

2021 年 3 月 31 日，为推动数据要素市场化配置和数字经济高质量发展，助力推进首都“两区”建设，北京市经济和信息化局会同北京市金融局、商务局、网信办等部门，组织北京金控集团牵头发起成立北京国际大数据交易有限公司，并在京举办发布会。发布会上，北京国际大数据交易所成立，北京数据交易系统上线。这是国内首家基于“数据可用不可见，用途可控可计量”新型交易范式的数据交易所，

定位于打造国内领先的数据交易基础设施和国际重要的数据跨境流通枢纽。北数所植根北京，将在保护个人隐私和信息安全的前提下，发挥技术密集和数据密集的双轮驱动，以技术促流通，以流通促创新，探索数字经济的新产业、新业态、新模式。

（2）上海数据交易所

2021 年 11 月 25 日，上海数据交易所揭牌成立仪式在沪举行并达成了部分首单交易。上海数据交易所的设立，重点是聚焦确权难、定价难、互信难、入场难、监管难等关键共性难题，形成系列创新安排。一是全国首发数商体系；二是全国首发数据交易配套制度；三是全国首发全数字化数据交易系统；四是全国首发数据产品登记凭证；五是全国首发数据产品说明书。此次上海数据交易所的成立是贯彻落实中央文件《中共中央 国务院关于支持浦东新区高水平改革开放打造社会主义现代化建设引领区的意见》的生动实践，是推动数据要素流通、释放数字红利、促进数字经济发展的重要举措，是全面推进上海城市数字化转型工作、打造“国际数字之都”的应有之义，也将有望成为引领全国数据要素市场发展的“上海模式”。

（3）北方大数据交易中心

2021 年 11 月 3 日，天津市人民政府正式批复，同意在中新天津生态城设立北方大数据交易中心，按照市场监管部门核定的经营范围开展经营活动，形成全国领先的跨行业、跨区域的“数据汇津”流通交易生态系统，集聚大数据相关产业，建设具有天津特色的数字经济产业标杆。目前，该中心已启动建设，聚焦生态城智慧城市优势基础，

吸引更多生态伙伴，鼓励数据创新应用。中心建成后，将面向各级政府、企事业单位等提供基础信息及数据应用服务产品。与此同时，生态城将以数据交易为核心，以隐私计算、数据沙箱、区块链等创新技术为支撑，开展数据价值评估、数据交易技术研发，以及“数据可用不可见”“数据可算不可识”等数据交易模式创新，构建安全可信、管理可控、价值可计量的数据交易环境；委托第三方评估机构，对数据资产的价值与数据质量进行评估，为数据资产定价提供参考；健全数据要素市场规则，制定数据确权、隐私保护、交易流通、跨境流动等制度规范；强化数据交易监管体系，制定数据交易管理办法，明确数据交易监管主体和监管对象，建立跨部门协同监管机制；挖掘数据资源，促进数据要素市场化配置，推动产业数字化转型升级，打造辐射我国北方的全链条数据交易服务基地。

（4）贵州大数据交易中心

作为抢抓国家数据要素市场培育新机遇、落实“在实施数字经济战略上抢新机”要求的具体举措，近日，贵州省数据流通交易服务中心挂牌成立，采用隐私计算、联邦学习、区块链等新技术手段，以安全可信的开发利用环境为底座，搭建贵州省数据流通交易平台。10 月 11 日，贵州数据流通交易平台上线运行，标志着贵州数据流通交易进入 2.0 时代。通过贵州省数据流通交易平台，云上北斗（贵州）科技股份有限公司作为“买方”，向“数据商”北京帝测科技股份有限公司购买了贵阳市城区倾斜摄影数据产品，交易金额 225 万元。随着第

一笔实质数据交易撮合完成，贵州新的大数据交易中心正式“开所”运行。

3、数据分类分级成为数据安全开发利用的基础和前提

数据分类分级是数据安全治理和数据安全开发利用的基础和前提，已成为业内共识。从 2016 年贵州省发布政务数据分类分级指南标准，2020 年《工业数据分类分级指南（试行）》和 JR/T 0197-2020《金融数据安全 数据安全分级指南》发布，到 2021 年《数据安全法》明确提出国家建立数据分类分级保护制度，数据分类分级法规标准渐成体系并逐渐完善，目前各地和各行业领域具体落地的法规标准正在陆续制定和发布实施中。

9 月 23 日，国家标准《信息安全技术 重要数据识别指南》征求意见稿完成，其明确了识别重要数据的基本原则，提出了重要数据的特征，主要包括与经济运行相关、与人口与健康相关、与自然资源与环境相关、与科学技术相关、与安全保护相关、与应用服务相关、与政务活动相关等类别。

2021 年 9 月 30 日，国家标准《网络安全标准实践指南——数据分类分级指引（征求意见稿）》公开征求意见。该指南从国家数据安全管理视角，给出了数据分类分级的原则、框架和规则。其中，关于数据分类规则，明确了个人信息识别与分类、公共数据识别与分类和法人数据识别与分类三方面内容。关于数据分级，根据数据一旦遭到篡改、破坏、泄露后者非法获取、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，将数据从低到高分成公开

级（1 级）、内部级（2 级）、敏感级（3 级）、重要级（4 级）、核心级（5 级）五个级别。其中，重要数据属于重要级（4 级），国家核心数据属于核心级（5 级）。

（三）数据安全技术与产品

1、数据安全技术与产品的发展态势

数据安全技术近年来发展十分迅速，创新技术不断涌现，参考《国信证券 计算机行业 2021 年 8 月投资策略》和国家工信安全中心联合华为发布《数据安全白皮书》等资料，下面对国内数据安全技术发展趋势进行梳理和总结。

（1）数据安全强调数据全生命周期的保护

数据安全推动了数字化转型中内生安全的融入，即进入数据全生命周期的各个环节，不再只是后 IT 时期的修修补补。数据生命周期涉及采集、传输、存储、处理、交换、销毁。当前的网络安全建设，主要仍基于传输和存储两个环节，像“交换”之类敏感环节，并未成熟，才导致数据泄露和数据黑市的存在。因此传统及新兴数据安全技术有望得到迅速应用和发展，如数据加密（叠加当前国密改造）、脱敏；数据监测（态感、UEBA）、数据审计（堡垒、水印）；隐私计算；数据容灾等，当前也能看到持续的产品化及方案落地。

（2）隐私计算技术逐渐成熟，在数据安全领域应用越来越广泛

隐私计算交叉融合了密码学、人工智能、计算机硬件等多种技术，其中密码学包括混淆电路、秘密分享、不经意传输等底层技术，以及

同态加密、零知识证明、差分隐私等辅助技术。最终形成了三大隐私计算方向：多方安全计算（MPC）、联邦学习（FL）和可信执行环境（TEE）。从 2016 年开始，国内逐步有隐私计算商业化落地，并且已经进入快速发展期，越来越多的行业客户开始愿意尝试。根据中国信通院调研，2021 年上半年各隐私计算项目进展顺利，已经有 81%的隐私计算产品进入了试点阶段或实施阶段。在技术选择上，由于 AI 训练等需求较为明确，且有成熟的开源社区，运营商和金融科技公司大多选择联邦学习的路线开发隐私计算产品，占比高达 52%。对于各行业龙头企业，致力于打造平台化的多方安全计算基础设施，26%企业选择多方安全计算路线。

（3）人工智能技术是数据安全的倍增器

人工智能是数据安全的倍增器，广泛应用到数据安全各个方面。在数据分类分级的过程中，基于人工智能的方案可以对更加复杂的上下文进行分析。在认证访问控制以及检测响应的过程中，基于人工智能的方案可以更有效地发现攻击者的异常行为，提高检测的精准度和系统应对攻击的响应能力。人工智能应用在数据分类和合规分析上，在敏感数据挖掘、图片文件内容实时监控和标记、数据防泄漏等方面都有很好的效果。通过机器学习技术自动识别重要数据访问、复制、移动等可疑行为，并实施精准实时的修复措施，防范重要数据暴露及共享业务中的数据安全风险；数据分类分级利用人工智能提升数据分类的精准程度，并且可以支持自动生成多种法律法规的合规报告，提升数据安全治理的效率；数据分类分级可以在数据块维度进行多任务

并行处理，利用机器学习+语义分析生成训练模型，提高数据分类速度和精度，并提供数据特性及变化趋势展示。人工智能驱动加密流量分析方案，使用机器学习算法，在分析初始数据包特征以及后续数据包长度与时序等的基础上识别加密后的异常流量。借助机器学习技术来检测组织系统和网络中的异常行为，并根据异常信息来检测网络攻击，自动形成应对的操作，减少针对数据攻击的风险。

（4）API 安全管控引发关注

大数据时代，API 成为服务交付的必选，API 接口负责传输的数据量以及敏感性的增加，导致针对 API 的攻击变得越来越频繁和复杂，甚至成为不少公司的头号安全威胁。因此，企业亟需有效的解决方案对开放共享的数据核心资产提供保护。通过对 API 访问风险及数据传输风险进行持续监测，全面评估业务系统、数据接口、数据分类的数据安全风险态势，面向 API 安全风险，可弥补 API 网关方案的不足。

（5）数据防泄漏（DLP）向智能化发展

传统 DLP（Data leakage prevention，数据泄露防护）通常采取动态加密、访问阻断、数据库防火墙等技术，监控终端、网络以及服务器中动态传输的数据，发现和阻止数据泄露。目前 DLP 已经较为成熟，可以预见的是，大数据分析技术、机器学习算法的发展将推动数据泄露防护的智能化发展，实现数据的智能化分级保护，并形成终端、网络、云端协同一体的数据传输安全体系。

（6）数据加密技术向轻量级、密文操作、透明加密等方向发展

数据内部传输和存储、外部共享、上云上平台等过程都有数据加密需求，数据加密技术需考虑数据实时性、稳定性、可靠性等特殊要求，尽可能以轻量级的加密技术减少密码对计算、网络、存储等资源的消耗。同时，面对大规模复杂的加密数据，频繁的加解密存在占用带宽、耗时耗力等问题，对密文的检索、使用等需求不断增加，密文直接可操作技术也是研究热点方向。透明加密技术只有在用户读写的过程中才会进行解密，以明文形式呈现给用户，其核心在于解决数据加密防护和密钥管理引起的数据处理效率、系统部署和应用及工具改造的代价等问题，以及对数据自动化运维的影响。

（7）数据脱敏技术向动静结合脱敏、敏感字段定向脱敏、数据智能脱敏等方向发展

数据脱敏又称数据去隐私化或数据变形，是在给定的规则、策略下对敏感数据进行变换、修改的技术机制。在数据开放共享的大背景下，数据流动共享是推动组织发展的主要动力，是数据核心价值体现的关键环节，数据跨部门、跨企业、跨地域流动共享使用逐渐成为常态，其中涉及到的重要敏感数据则需在流动共享前采用数据脱敏技术等进行处理，确保数据安全共享和使用。而数据的脱敏技术需要适配大流量、高速流动、实时交互等需求，随着机器学习技术的应用，集敏感数据自动化感知、脱敏规则自动匹配、脱敏处理自动完成等能力于一体的数据智能脱敏技术将成为新趋势。

（8）数据溯源技术向跨组织追踪方向发展

数据采集阶段重点关注如何自动地生成正确的元数据以及其可追溯性，数据溯源显得尤其重要。数据多路径、跨组织的复杂传输流动模式，跨越了数据控制者和安全域，为保证数据安全，数据溯源应贯穿数据存储、使用、共享等全过程，跨系统、跨组织的数据追踪溯源技术将成为未来研究方向。

（9）流量识别技术保障数据全流程安全监测与防护

随着数据应用场景的增多，数据安全监测与防护需求增强，催生了以流量识别技术为基础的网络流量分析技术（Network Traffic Analysis，NTA），其统筹深度包检测、协议识别与还原、大数据采集和分析、安全检测引擎、漏洞挖掘和分析、渗透及攻防等技术，面向智能化生产、网络化协同、个性化定制和服务化延伸等网络交互场景，进行基于流监测的数据安全防护，支撑流量采集、协议识别和解析、敏感数据违规传输监测、数据泄露监测、数据安全事件检测、数据安全威胁溯源分析等具体应用场景。为了应对新兴技术和纷繁复杂的应用，面向私有协议、加密协议的未知协议识别技术、加密流量识别技术是未来发展方向。

2、主要机构和企业数据安全方案

（1）大数据协同安全技术国家工程实验室

大数据协同安全技术国家工程实验室是由北京奇虎科技有限公司牵头承建，我国大数据安全领域唯一的一个国家工程实验室。经过几年的探索与实践，实验室在数据安全方面已打磨形成了一套可行的“一体系、三支撑”数据安全整体解决方案。其中，“一体系”是指

基于数据安全能力成熟度模型（DSMM）的数据安全治理体系，实验室将通过数据安全咨询、培训和测评服务，帮助企业或组织体系化地提升数据安全能力成熟度；“三支撑”则是指面向大数据平台安全、大数据协同计算安全和大数据运营安全三大方向，为客户提供在数字经济不同应用场景下的数据安全解决方案、产品和服务。

实验室提供数据安全治理、数据安全合规、数据安全方案和数据安全运营四类咨询服务，从政策、策略、方法到技术、方案和具体建设运营的咨询指导来帮助企业或组织不断提升数据安全能力。提供 DSMM 测评服务，帮助企业或组织准确找到数据安全管理和技术方面的差距，以满足相应数据安全能力成熟度等级的要求。提供注册数据安全官、注册数据安全工程师和 DSMM 测评师培训，为社会提供专业的数据安全管理和技术人才。

实验室提供面向数据全生命周期的大数据平台安全解决方案，重点在数据分类分级、数据资产安全管理、数据处理安全和数据交换安全等方面创新发展新技术、新产品，帮助客户安全地管理大数据资源并提供各类大数据服务。建设大数据协同安全计算平台，对外提供隐私计算服务，作为可信第三方或参与方，探索数字创新应用开发和数据价值的挖掘。提供数据处理活动安全监管审计、数据安全威胁抵御和数据滥用防范等安全解决方案、产品和服务，支撑监管侧的安全监管工作，保障平台侧的大数据安全运营。

（2）360 公司发布大数据安全能力框架

2021 年 11 月 9 日，360 重磅发布 360 大数据安全能力框架，带来了面向不同场景的整体数据安全保护方案。这是一个覆盖监管侧、企业侧和城市侧的整体框架，实现监管单位常态化监管、企业防护能力提升、城市数据安全管控相统一，由基于数据安全大脑的数据安全治理、数据攻击面防护、数据访问控制、数据专家运营四部分组成。监管侧数据安全的目标是进行常态化的数据安全监管，需要数据安全监管平台、常态化的数据连接、标准化的数据接口，以实现监管部门对辖区内全网数据的地图展示、知识图谱、事件审计和态势感知。同时，还可以实现常态化的数据查询，在发生数据安全事件时，能够快速进行调查和取证。

（3）CCIA 发布《数据安全产品指南》

在“依法治数”的大趋势下，用户如何选择安全可靠的数据安全产品成为当下最为迫切的需求之一。2021 年 11 月 1 日，中国网络安全产业联盟（CCIA）征集并梳理数据安全领域有关产品，发布了《数据安全产品指南》。该指南从数据安全治理、个人隐私保护、数据库安全、数据脱敏、数据泄露保护、电子文档管理与加密、存储备份与恢复等方面，对网络安全企业推出的优秀数据安全产品进行分类、整理、展示，方便广大用户了解数据安全方面的前沿技术、管理理念和发展趋势，为各行各业在加强数据安全建设方面提供参考。

（4）炼石网络

2021 年 7 月，炼石网络 CEO 白小勇在第九届互联网安全大会（简称 ISC 2021）“数据安全与隐私保护战略峰会”作《DTTACK：以数据

为中心的安全技术框架》主题演讲，分享对数据安全的新框架、新战法的探索。从“以数据为中心”的角度提出 DTTACK 数据安全技术框架，全称是 Data-centric Tactics, Techniques And Common Knowledge（以数据为中心的战术、技术和通用知识）。DTTACK 框架尝试填补“以数据为中心”的安全技术体系的空白，它不是网络、服务器或应用程序安全性的模型，更强调数据本身的安全性，并从对数据的“应对式”防护，向“主动式”防护转变，重视从业务风险映射视角列举数据保护需求，可以为信息化建设、企业业务架构设计提供数据安全能力参考。

（5）北京安华金和科技有限公司

2021 年 5 月 21 日，在“第四届中国数据安全治理高峰论坛”上，安华金和公司牵头起草的《数据安全治理白皮书 3.0》发布。白皮书内容涵盖数据安全治理全球形势分析、理论技术研究、框架体系构建、行业实践案例、政策法规标准、未来趋势预测等，旨在为各行业数据安全治理工作提供更多经验总结与信息参考。物联网、云计算和人工智能技术的飞速发展，已经并仍在加速促进着从“数据”到“大数据”的由量变到质变的演进，大数据成为挖掘新信息和新知识的基础原材料，在经过统计分析和机器学习等技术和方法的发掘和利用后，既迸发出巨大价值，又预示着无限潜能。数据安全日益成为保障经济发展、社会稳定和国家安全的重要基石。

（四）数据处理活动安全

1、国家加强网络安全审查

2021 年 7 月 6 日，中办、国办公布《关于依法从严打击证券违法活动的意见》，这是资本市场历史上首次以中办、国办名义联合印发打击证券违法活动的专门文件，是全方位加强和改进证券监管执法工作的行动纲领。其中，在第十九条指出，要加强跨境监管合作，完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。加强跨境信息提供机制与流程的规范管理。坚持依法和对等原则，进一步深化跨境审计监管合作。而且，在第二十三条强调丰富证券执法手段，需有效运用大数据、人工智能、区块链等技术，建立证券期货市场监测预警体系，构建以科技为支撑的现代化监管执法新模式，提高监管执法效能，加强对严重违法隐患的排查预警，做到有效预防、及时发现、精准打击。

7 月 10 日，国家网信办发布关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知，相关上市要求条款体现了落实《数据安全法》第二十四条和《关于依法从严打击证券违法活动的意见》的要求。具体数据安全相关内容包括：（1）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；企业赴国外上市可能出现数据安全风险，这是国家数据安全审查制度实施的一种具体体现；（2）加强跨境监管合作，完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。

2、对网约车平台的网络安全审查

2021 年 7 月 4 日，国家网信办发布通知称“滴滴出行”App 存在严重违法违规收集使用个人信息问题，依据《网络安全法》相关规定，应用商店下架“滴滴出行”App。同时，要求滴滴出行科技有限公司严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。7 月 9 日，国家网信办发布公告称，根据举报经检测核实，“滴滴企业版”等 25 款 App 存在严重违法违规收集使用个人信息问题。依据《网络安全法》相关规定，通知应用商店下架该 25 款 App。7 月 16 日，国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴出行科技有限公司，开展网络安全审查。

9 月 1 日，交通运输部会同中央网信办、工业和信息化部、公安部、国家市场监管总局等交通运输新业态协同监管部际联席会议成员单位，对 T3 出行、美团出行、曹操出行、高德、滴滴出行、首汽约车、嘀嗒出行、享道出行、如祺出行、阳光出行、万顺叫车等 11 家网约车平台公司进行联合约谈。约谈要求各公司坚守依法合规经营底线，维护公平竞争市场秩序，保障司乘人员合法权益，落实安全稳定主体责任，保障用户信息和数据安全。各公司要严格落实用户信息和数据安全相关法律法规要求，认真履行个人信息保护责任，未征得用户同意，不得向第三方提供用户个人信息。在用户数据收集、传输、存储、处理等环节，应依法建立相关数据安全管理制度，采取必要的安全技术和管理措施。

3、数据出境安全评估

2021 年 10 月 29 日，为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，国家网信办发布《数据出境安全评估办法（征求意见稿）》并公开征求意见。数据有出境需求时，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。数据出境采取合法、正当和必要原则；评估境外接收方的数据保护水平和总体安全风险、数据安全和个人信息权益保障、数据出境相关合同、法律遵守情况以及其他事项。同时，规定了“安全评估”与“风险自评估”的相关要求，特别是在向境外提供数据前均应事先开展数据出境风险自评估。该办法适用的对象既包括关键信息基础设施的运营者，也包括处理个人信息和重要数据的一般处理者。

数据出境安全将重点评估的七大事项：合法、正当、必要原则，境外接收方的数据保护水平，总体安全风险，数据安全和个人信息权益保障，数据出境相关合同，法律遵守情况，以及其他事项。同时，分别规定了“安全评估”与“风险自评估”的相关要求，特别是在向境外提供数据前均应事先开展数据出境风险自评估。该办法适用的对象既包括关键信息基础设施的运营者，也包括处理个人信息和重要数据的一般处理者。

事实上，数据出境安全一直是我国高度关注的问题。早期我国强调数据的存储、处理和业务相关服务器应部署在境内，建立数据跨境风险防范机制。例如，2006 年银监会发布的《电子银行业务管理办

法》，2016 年由交通运输部、工信部等 7 部委发布的《网络预约出租汽车经营服务管理暂行办法》，以及 2016 年国家新闻出版广电总局、工业和信息化部发布的《网络出版服务管理规定》，均要求数据存储和业务服务器存放在中国境内。

至 2017 年，国家网信办发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，2019 年又发布了《个人信息出境安全评估办法（征求意见稿）》，已着力构建可操作性的数据出境安全评估制度。《网络安全法》和《数据安全法》的发布实施确立了重要数据出境的基本框架，即重要数据原则上应当在境内存储，确需向境外提供时应当进行安全评估。

对于数据出境安全评估的实施，2020 年 8 月，商务部发布《关于印发全面深化服务贸易创新发展试点总体方案的通知》，就明确提出北京、上海、海南等条件相对较好的地区，要求支持试点开展数据跨境流动安全评估，建立数据保护能力认证、数据流通备份审查、跨境数据流动和交易风险评估等数据安全管理机制。

根据北京、上海、浙江、海南等地的自贸试验区方案，各地都在加快数据跨境流动机制探索，并采取了一些创新性的举措。例如，北京明确要加强跨境数据保护规制合作，促进数字证书和电子签名的国际互认，探索制定跨境数据流动等重点领域规则，提出数据产品跨境交易模式，并设立了北京国际大数据交易所；上海明确要建立数据保护能力认证、数据流通备份审查、跨境数据流动和交易风险评估等数据安全管理机制，并提出依托国际光缆登录口构建跨境数据中心、新

型互联网交换中心，建设新型数据监管关口，设立新片区跨境数据公司。

二、国内外政策法规分析

（一）政策法规发展概述

1、世界主要国家和组织数据立法竞相提速

经济全球化背景下，人们对于隐私和数据保护的认知逐渐提高，世界各国纷纷采取行动，制定数据安全战略和政策。2020 年欧盟委员会发布《欧洲数据保护监管局战略计划》，旨在从前瞻性、行动性和协调性等方面加强数据安全保护。美国发布《联邦数据战略与 2020 年行动计划》，核心目标是将数据作为战略资产利用，致力于“维护全球数字化转型背景下的数字领导地位”。2018 年以来，各国的数据保护立法进度加快，但各地市场状况不同，数据保护立法的方向也不甚相同，形成了各具特色的法规，其中以欧盟和美国的政策法规更具代表性。

欧盟的数据安全立法无论是时间还是系统性上都处于全球领先位置。2018 年正式生效的《通用数据保护条例》（GDPR）是当前全球个人信息和数据保护方面最具代表性的立法。其主要目标是恢复个体对个人数据的控制，简化欧盟内部国际业务的通用规范。2020 年 11 月，欧盟委员会提出的《数据治理法案》是欧盟数字战略下的第一个成果，旨在促进九个共同数据空间的建立和发展，为欧盟经济发展提供更多具有使用价值的数据。2020 年 12 月，欧盟委员会发布的《数字市场法》及《数字服务法》草案作为欧盟数字战略的重要组成部分，为欧盟委员会加强数字领域监管提供了法律基础。

美国目前在联邦层面上，没有全面综合的数据保护法，各领域存在不同的法规进行数据保护。如消费者保护类有《联邦贸易委员会法》、医疗服务类有《健康保险便利与责任法》、金融类有《金融服务现代化法》等。州层面上，全美 50 个州都提出了数据保护相关法案，但目前仅内达华州、加州、缅因州、弗吉尼亚州和科罗拉多州的法案正式通过。其中具有标志性意义的是 2018 年 6 月颁布的《加州消费者隐私保护法》（CCPA），被认为是美国目前最综合的数据和隐私保护立法。为统一美国州隐私立法，2021 年 7 月，美国统一法律委员会通过了《统一个人数据保护法》，该法案预计将于 2022 年被州立法机构引入。

2、国内数据安全监管政策管理框架逐渐形成

2015 年，《中华人民共和国国家安全法》（以下简称“《国家安全法》”）将数据安全纳入国家安全范畴， 2017 年施行的《网络安全法》对基础设施及个人信息的保护进行强调，提出数据泄露通知、个人删除权、个人信息境内存储及出境评估等规定。

2021 年 6 月，《数据安全法》出台，作为我国首部数据安全领域的基础性立法，其聚焦数据安全领域的突出问题，确立了数据分类分级管理，建立了数据安全风险评估、监测预警、应急处置，数据安全审查等基本制度，对国内外数据竞争与保护的关键问题进行了回应，为企业数据经营合规、进一步有序挖掘数据价值提供了指引。8 月，《个人信息保护法》发布，立足于数据产业发展的实践和个人信息保护的迫切需求，确立个人信息保护原则和个人信息处理规则，规范个

人信息处理者义务及国家机关处理活动，并关注敏感个人信息保护与个人信息跨境流动，为个人信息处理制定了明确的法理依据和法律红线，为个人维护正当隐私权益提供了充分保障。11 月，《网络数据安全管理条例（征求意见稿）》发布，在《网络安全法》、《数据安全法》、《个人信息保护法》三部上位法的基础上，在操作实施、责任界定、惩罚措施等方面进行了更加清晰具体的细化，进一步强化数据处理者主体责任的落实，弥补了网络数据安全管理领域法律规则体系中行政法规层级制度的缺失，对“法律-行政法规-部门规章、地方性法规以及规范性文件”全位阶的法律规则体系作了进一步完善。

3、各地积极出台数据条例推动数据应用发展

随着《国家安全法》、《网络安全法》、《数据安全法》及《个人信息保护法》等法律的颁布与实施，我国在国家层面构筑了数据安全保护的基础性“法律堡垒”。各省市近年来结合自身发展情况，也积极制定出台了与数据发展相关的条例（包括大数据条例、数据条例、相关草案），目前与数据发展相关的有至少 13 部地方条例，如表 1 所示。

表 1 各省市数据发展相关条例

地区	条例名称	施行时间
贵州	贵州省大数据发展应用促进条例	2016 年 3 月 1 日
天津	天津市促进大数据发展应用条例	2019 年 1 月 1 日
海南	海南省大数据开发应用条例	2019 年 11 月 1 日

地区	条例名称	施行时间
山西	山西省大数据发展应用促进条例	2020 年 7 月 1 日
吉林	吉林省大数据发展应用促进条例	2021 年 1 月 1 日
安徽	安徽省大数据发展条例	2021 年 5 月 1 日
山东	山东省大数据发展促进条例	2022 年 1 月 1 日
深圳	深圳经济特区数据条例	2022 年 1 月 1 日
上海	上海市数据条例	2022 年 1 月 1 日
辽宁	辽宁省大数据发展应用促进条例（草案）	/
黑龙江	黑龙江省促进大数据发展应用条例（征求意见稿）	/
陕西	陕西省大数据发展应用条例（征求意见稿）	/
宁夏	宁夏回族自治区大数据产业发展促进条例（草案）	/

各地对“构建以数据为关键要素的数字经济”的号召均作出快速响应，出台数据发展相关条例后，又针对数据安全、数字经济、数据共享与开放等制定专项的条例、规范，对数据合法合规的有效利用、最大化发挥价值以促进经济发展提出更为全面、深入和具体的引导和约束，全方位加速推进我国数字化转型进程并提供强有力的支撑和保障。

（二）数据分类分级合规政策重点解读

1、数据安全分类分级背景

2021 年 9 月和 11 月，《数据安全法》和《个人信息保护法》相继施行，从国家层面为数据安全保护提供了法制保障。由于不同类型的数据，价值和级别均不同，需根据数据的重要性、价值属性等区别对待，因此要进行数据分类分级保护。数据分类是为了规范化关联，分级是安全防护的基础，不同安全级别的数据在不同的活动场景下，安全防护的手段和措施也不同。数据分类分级是数据治理的第一步，只有做好了数据的分类分级工作，才能进行后续的数据安全保护体系建设。

作为数据安全保护的前提，数据分类分级已成为国家法规政策标准中的明确要求。2021 年 6 月 10 日出台的《数据安全法》在第二十一条中明确规定了数据分类分级保护制度，要求“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”。2021 年 11 月 14 日国家网信办发布的《网络数据安全管理条例（征求意见稿）》在《数据安全法》的基础上进一步明确了数据分级要求，“按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，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”。

2、数据分类分级国家标准

2021 年 9 月 30 日，国家标准《网络安全标准实践指南 －数据分类分级指引（征求意见稿）》公开征求意见。它从国家数据安全管理视角给出了数据分类分级原则、框架和规则。分类分级框架如图 1 所示，数据分类分级按照数据分类管理、分级保护的思路，主要遵循以下原则：合法合规、界限明确、就高从严、时效性、自主性。对于数据识别与分类，征求意见稿主要提出以下几点：

1）数据分为公共数据、个人信息和法人数据三类。

2）直接标识信息、准标识信息和自然人属性级活动产生的信息均属于个人信息，分为一般个人信息、敏感个人信息和私密个人信息三类。

3）党政机关和企事业单位履行公共管理和服务职能中收集产生的数据属于公共数据，由各级单位自主分类。

4）不属于个人信息、公共数据的数据识别为法人数据，可分为业务数据、经营管理数据、系统运行和安全数据三类。

分级方面，主要根据数据危害对象和危害程度，将数据分级从低到高分成公开级（1 级）、内部级（2 级）、敏感级（3 级）、重要级（4 级）、核心级（5 级）五个级别。对于特定数据，征求意见稿中设置了最低级别：（1）国家核心数据定级不低于 5 级；（2）重要数据定级不低于 4 级；（3）敏感个人信息定级不低于 4 级，一般个人信息不低于 3 级，组织内部员工个人信息不低于 2 级，个人标签信息不低于 2 级；（4）有条件开放的公共数据定级不低于 2 级，禁止开放的公共数据不低于 4 级。

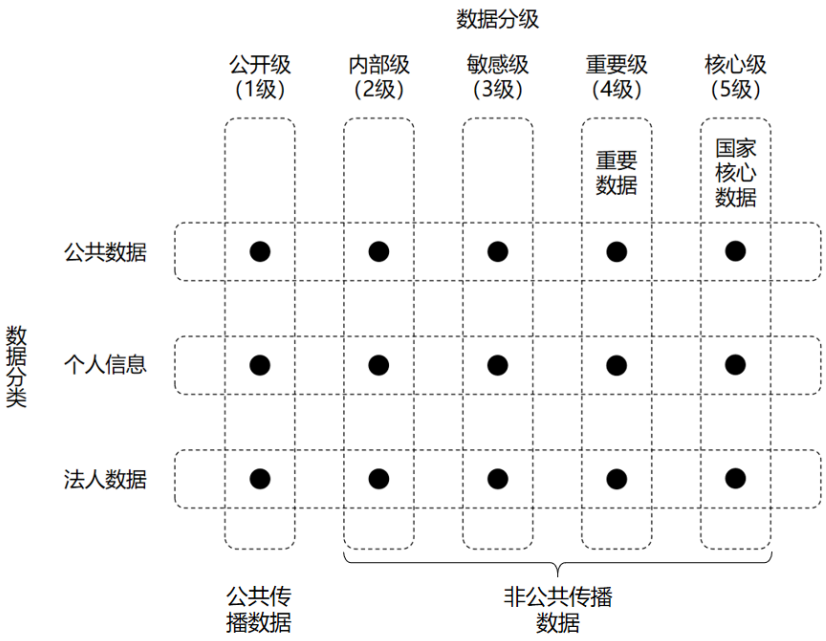


图 1 网络安全标准实践指南 －数据分类分级指引 数据分类分级框架

3、数据分类分级地方标准

近年来陆续出台的各省市数据条例均提出要将数据进行分类分级管理，举例如下：

表 2 各地数据条例关于分类分级要求

时间	发布机构	政策	要求
2019 年 8 月	贵州省人民代表大会常务委员会	《贵州省大数据安全保障条例》	采取数据分类、备份和加密等安全措施。
2020 年 4 月	内蒙古自治区市场监督管理局	《内蒙古公共大数据安全管理指南》	基于政策法规及公共数据共享和安全需求，确定组织机构内部的数据分类分级方法，对公共数据进行分类分级标识。
2021 年 7 月	深圳市人民代表大会常务委员会	《深圳经济特区数据条例》	法人、非法人组织应当建立健全数据治理架构和管理制度设置或委托专门数据管理机构，对数据实施分类分级保护和管理。
2021 年 10 月	广东省人民政府	《广东省公共数据管理办法》	行业主管部门应当根据国家、省、地级以上市公共数据分类分级相关规定，加强对本部门公共数据的管理。
2021 年 11 月	上海市人民代表大会常务委员会	《上海市数据条例》	本市按照国家要求，建立健全数据分类分级保护制度，推动本地区数据安全治理工作。

除数据条例中提到的分类分级要求外，部分省市对于公共数据也提出了具体分类分级指南，具体如下：

表 3 数据分类分级地方标准

时间	发布机构	政策
2021 年 2 月	上海市经济和信息化委员会	《上海市公共数据开放分类分级指南（试行）》
2021 年 4 月	烟台市大数据局	《烟台市公共数据开放分类分级指南（试行）》

2021 年 7 月	浙江省市场监督管理局	地方标准 DB33/T 2351—2021《数字化改革公共数据分类分级指南》
2021 年 10 月	重庆市大数据应用发展管理局	《重庆市公共数据分类分级指南（试行）》

公共数据是指公共管理和服务机构在履行职责和提供公共服务过程中获取的数据资源，涉及数据开放共享。各省市的条例以共享为原则，以不共享为例外，对公共数据采用目录制服务方式，鼓励通过目录进行数据发布，促进数据开放共享和交易利用。深圳、上海、陕西等地区按照无条件开放、有条件开放和不予开放进行数据分类，无条件开放数据可通过地区统一数据平台获取，有条件开放数据可向平台数据提供者提出申请。上海市公共数据开放类别说明如表 4 所示。

表 4 上海市公共数据开放分类分级指南 公共数据开放类别说明

开放类别	说明
非开放	涉及商业秘密、个人隐私，或者法律、法规规定不得开放的公共数据
有条件开放	对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据
无条件开放	除上述非开放和有条件开放以外的其他公共数据

公共数据开放的级别按照其描述的对象，从个人、组织、客体三个维度，分别对应了数据特征、开放类型和开放级别。对于不同级别的数据，采取对应的数据安全要求，并对需提供的申请材料进行详细说明。此外，《重庆市公共数据分类分级指南（试行）》和浙江省《数字化改革公共数据分类分级指南》中还按照采集、传输、存储、处理、

共享、开放、销毁等各阶段，对数据全生命周期分级管控措施按公共数据的级别做了详细要求，为当地公共数据分类分级管控提供了参考。

4、数据分类分级行业标准

各行业关于数据分类分级的行业标准也陆续出台，主要包括政府部门、金融行业及工业和信息化部，具体如下表所示。

表 5 数据分类分级行业标准

时间	发布机构	政策
2016 年 6 月	贵州省大数据发展领导小组	地方标准 DB52/T 1123—2016《政府数据 数据分类分级指南》
2018 年 9 月	中国证券监督管理委员会	金融行业标准 JR/T 0158—2018《证券期货业数据分类分级指引》
2020 年 2 月	工业和信息化部	《工业数据分类分级指南（试行）》
2020 年 9 月	中国人民银行	金融行业标准 JR/T 0197—2020《金融数据安全 数据安全分级指南》
2020 年 10 月	深圳市坪山区人民政府	《坪山区政务数据分级分类管理办法（试行）》
2020 年 12 月	工业和信息化部	通信行业标准 YD/T 3813-2020《基础电信企业数据分类分级方法》
2021 年 4 月	北京市经济和信息化局	《政务数据分级与安全保护规范（征求意见稿）》
2021 年 10 月	杭州市数据资源管理局	地方标准 DB3301/T 0322.3-2020《数据资源管理第 3 部分：政务数据分类分级》

（1）政务数据分类分级

各地制定的政务数据分类分级原则基本一致，遵照科学性、实用性、多维度的分类原则和自主定级、分级管控的分级原则进行政务数据分类分级。由于政务数据的复杂性，政务数据分类大都采用了多维度与线分类法相结合的方法，如贵州省出台的《政府数据 数据分类分级指南》要求“在主题、行业和服务三个维度对贵州省政府数据进行分类，对于每个维度采用线分类法将其分为大类、中类和小类三级。业务部门可以根据业务需要，对数据分类进行小类之后的细分”，深圳市坪山区出台的《坪山区政务数据分级分类管理办法（试行）》也要求“结合政务数据所特有的行业属性特征，采用多维度和线分类法相结合方法，从技术选型、业务应用和数据对象三个视角对政务数据进行分类，在分类原则确定的三个分类视角下，按分类维度对政务数据的每一维度的一级分类进行明确，然后参照各维度分类的标准规范，按线分类法划分一级分类下的二级分类和三级分类”。

数据分级方面，各地标准中基本都是按照政务数据的敏感程度，以及发生泄露、篡改、丢失或滥用后的影响对象、影响程度、影响范围中的几种相结合，将政务数据分为 3~5 级，并提出相应的等级管控要求。北京市的《政务数据分级与安全保护规范（征求意见稿）》将分级因素与安全等级的对应关系进行了详细描述，如表 5 所示。此外，由于政务数据涉及开放共享，各地的标准对于政务数据的共享也提出了相关要求。

表 6 政务数据分级与安全保护规范 分级因素与安全等级对应表

影响程度	影响范围		影响对象		
	影响规模	可控程度	党政机关、公共服务机构	自然人	其他机构
一般影响	较小范围	强可控	一级	一级	一级
		弱可控	二级	一级	一级
	较大范围	强可控	二级	二级	一级
		弱可控	三级	二级	二级
严重影响	较小范围	强可控	三级	二级	二级
		弱可控	三级	三级	三级
	较大范围	强可控	三级	三级	三级
		弱可控	四级	三级	三级
特别严重影响	较小范围	强可控	四级	四级	三级
		弱可控	四级	四级	四级
	较大范围	强可控	四级	四级	四级
		弱可控	四级	四级	四级

（2）金融行业数据分类分级

金融行业目前施行了两个数据分类分级行业标准，分别是 2018 年证监会公布实施的《证券期货业数据分类分级指引》和 2020 年中国人民银行公布实施的《金融数据安全数据安全分级指南》。

《证券期货业数据分类分级指引》对证券期货业数据分类、分级以及相应的前提条件、方法概述、关键问题处理等内容做了详细说明。提出数据分类分级的前提条件是要建立数据分类分级组织保障、数据分类分级管理制度、建立数据资产分类分级清单。另外还提供了数据分类分级方法的三个流程阶段：

第一阶段：业务细分。解决业务分类问题，同时确定数据的管理主体。数据管理主体的确定是数据分类准确性和定级准确性的基本保证。

第二阶段：数据归类。在明确数据管理主体和业务分类的基础上，重点解决数据分类问题。

第三阶段：级别判定。在数据分类基础上，进行数据定级。

对每个阶段的步骤进行了详细描述、示例说明和流程图解，且给出了典型数据分类分级模板，具有很强的规范指导作用。

《金融数据安全 数据安全分级指南》主要针对金融数据的分级做了规定。该指南分为六个章节，分别是：范围、规范性引用文件、术语和定义、目标原则和范围、数据安全定级和重要数据识别。指南中数据的范围不包括涉及国家秘密的金融数据和非电子形式的金融数据。数据定级主要根据数据安全性（保密性、完整性、可用性）遭到破坏后可能造成的影响对象和影响程度作为判断依据，给出了详细的数据安全定级工作流程图和典型数据定级规则参考表。

此外，标准提出数据的安全级别可能在数据脱敏、删除关键字段、汇聚融合等技术手段下发生级别变化，并给出了级别升降示例如下表，为其他行业的数据安全级别变更提供了参考。

表 7 金融数据安全 数据安全分级指南 数据级别调整表

措施	安全级别调整
汇聚融合	3 级升至 4 级
生产数据脱敏后用于金融业机构内部业务经营或管理工作	3 级降至 2 级
汇聚融合，特定机构特定时间或事件后信息具有高安全等级	2 级升至 4 级
脱敏，从数据中去除能够直接定位到个人金融信息主题的内容，删除涉及商业秘密的内容等，特定事件或事件后信息失去原有敏感性	4 级降至 2 级

（3）工信部数据分类分级

工信部目前施行的数据分类分级标准有《工业数据分类分级指南（试行）》和《基础电信企业数据分类分级方法》，分别对工业数据和基础电信企业数据的分类分级做出规定。

《工业数据分类分级指南（试行）》旨在指导企业全面梳理自身工业数据，提升数据分级管理能力，促进数据充分使用、全局流动和有序共享。明确了企业作为数据分类分级主体，以提升企业数据管理能力为目标，坚持问题导向、目标导向和结果导向相结合，企业主体、行业指导和属地监管相结合，分类标识、逐类定级和分级管理相结合。对于工业企业和平台企业的分类维度分别做了相应指导，分级方面根据数据遭篡改、破坏、泄露或非法利用后，对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级 3 个级别。另外还提出了数据分级的管理与防护规范。

《基础电信企业数据分类分级方法》关于数据分类，根据基础电信企业业务运营特点和企业内部管理方法，收集企业内所有部门的数据资源，梳理所有数据资源。按照线分类法，按照业务属性（或特征），将基础电信企业数据分为若干数据大类，然后按照大类内部的数据隶属逻辑关系，将每个大类的数据分为若干层级，每个层级分为若干子类，同一分支的同层级子类之间构成并列关系，不同层级子类之间构成隶属关系。所有数据类及数据子类构成数据资源目录树。数据分级方面，按照确定数据分级对象、确定数据安全收到破坏时造成影响的

客体、评定对影响客体的影响程度、确定数据分级对象的安全等级四个步骤进行。

5、分类分级对国家和企业的意义

对数据分类分级是企业当前首先要考虑的数据治理工作。企业可以按照数据安全法的原则以及本行业的具体指南开展具体的工作。对国家而言，数据分类分级是监测、管理、防范数据风险的基础，尤其对于国家核心数据和重要数据而言，若未进行分类分级则难以进行判断和针对性的安全管理。此外，数据作为生产要素，只有在流动、共享和加工处理的过程中才能发挥价值。对数据进行分类分级，有利于提高数据质量，使数据规范化和标准化，从而提升数据资源的价值。

对企业而言，日益复杂的数据处理活动导致企业内部数据难以得到有效保护，存在泄露、篡改等安全风险，对数据进行分类分级保护有助于企业梳理其内部数据，对不同重要程度的数据采取不同的保护措施，降低安全风险。另外，在国家的数据保护背景下，企业也承担着个人信息保护、数据出境合规等义务，对企业内部数据进行分类分级有利于企业履行数据合规义务。

（三）数据出境安全评估重点解读

数据跨境流动成为国际新常态，为全球经济活动、人类社会发展提供了支撑，但数据跨境流动从国家安全、产业安全、个人安全角度都是数据安全治理领域较为敏感、复杂的问题。下文从我国现有数据

出境政策法规和数据出境安全评估角度对我国数据出境政策进行分析解读。

1、我国的数据出境政策法规

（1）重要数据：原则上境内存储，确有必要出境提供

我国《网络安全法》和《数据安全法》确立了重要数据出境的基本框架，即重要数据原则上应当在境内存储，确需向境外提供时应当进行安全评估。可见，我国重要数据跨境流动制度的核心是数据出境安全评估。

1）数据出境安全评估旨在把控数据出境的安全风险

2017 年国家网信办发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，2019 年又发布了《个人信息出境安全评估办法（征求意见稿）》，着力构建可操作性的数据出境安全评估制度。根据上述办法，我国数据出境安全评估重点评估以下内容：

a）数据出境的必要性；

b） 涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

c）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

d）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

e）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险等。

2）金融等行业完善数据跨境流动制度

我国金融、卫生健康、交通运输等部门很早就结合行业需求对特定数据出境提出了要求，建立健全数据跨境流动规则和机制。相关要求主要集中在两个方面：

a）明确要求数据本地化存储。例如，2006 年银监会发布的《电子银行业务管理办法》第十条规定，中资银行业金瓯让机构的电子银行业务运营系统和业务处理服务器设置在中华人民共和国境内；2016 年由交通运输部、工信部等 7 部委发布的《网络预约出租汽车经营服务管理暂行办法》第二十七条规定，网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流；2016 年国家新闻出版广电总局、工业和信息化部发布的《网络出版服务管理规定》第十二条要求，申请从事网络出版服务应当提交网站域名注册证明、相关服务器存放在 中华人民共和国境内的承诺。

b）明确数据出境相关要求。这方面多数是笼统性的规定，缺乏操作性。例如，2013 年发布的《征信业管理条例》第二十四条规定，征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定；2019 年中国人民银行等四部委发布的《信用评级业管理暂行办法》第三十条规定，信用评级机构向境外组织或者个人提供信息，应当遵守法律法规以及信用评级行业主管部门和业务管理部门的有关规定；2021 年 5 月国家网信办发布的《汽车数据安全管理若干规定》第十二条规定，个人信息或者重

要数据应当依法在境内存储，确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。

3）地方加快探索数据跨境安全监管模式

2020 年 8 月，商务部发布《关于印发全面深化服务贸易创新发展试点总体方案的通知》，提出北京、上海、海南等条件相对较好的试点地区开展数据跨境传输安全管理试点，明确要求支持试点开展数据跨境流动安全评估，建立数据保护能力认证、数据流通备份审查、跨境数据流动和交易风险评估等数据安全管理机制。

根据北京、上海、浙江、海南等地的自贸试验区方案，各地都在加快数据跨境流动机制探索，并采取了一些创新性的举措。例如，北京明确要加强跨境数据保护规制合作，促进数字证书和电子签名的国际互认，探索制定跨境数据流动等重点领域规则，提出数据产品跨境交易模式，并设立了北京国际大数据交易所；上海明确要建立数据保护能力认证、数据流通备份审查、跨境数据流动和交易风险评估等数据安全管理机制，并提出依托国际光缆登录口构建跨境数据中心、新型互联网交换中心，建设新型数据监管关口，设立新片区跨境数据公司。

（2）个人信息：在数据主体同意的前提下，提供安全评估、认证等三种机制

我国《个人信息保护法》确立了三种个人信息跨境流动机制：（1）安全评估，由国家网信部门组织实施；（2）个人信息保护认证，国家网信部门出台相关规定，专业机构按照规定开展认证活动；（3）标准

合同文本，由国家网信部门制定标准合同文本，数据输出方和接收方订立合同，明确双方的权利和义务，并监督接收方的个人信息活动达到法律规定的个人信息保护标准。

2019 年国家网信办发布《个人信息出境安全评估办法（征求意见稿）》，安全评估工作由省级网信部门组织进行，重点评估以下内容：

1）是否符合国家有关法律法规和政策规定；

2）合同条款是否能够充分保障个人信息主体合法权益；

3）合同能否得到有效执行；

4）网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件；

5）网络运营者获得个人信息是否合法、正当；

6）其他应当评估的内容。

（3）数据跨境调取：奉行对等原则，并需经有关主管部门批准

在一国涉外司法或执法过程中，可能会需要调取他国境内数据或公民个人信息，这种数据跨境调取通常通过国际司法或执法协助进行。但 2018 年美国 CLOUD 法案规定，美国政府有权力调取存储于他国境内数据，而其他国家若要调取存储在美国的数据，则必须通过美国的“符合资格的外国政府”审查。这实质上采取了双重标准，并打破了国际司法或执法协助制度。

与美国不同，在数据跨境调取方面，我国《数据安全法》、《个人信息保护法》都奉行对等原则，明确我国根据有关法律和中华人民

共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求；非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。同时，对于从事损害我国公民个人信息权益等活动的境外组织、个人，以及在个人信息保护方面对我国采取不合理措施的国家和地区，法律还规定我国可以采取相应的对等措施。

2、数据出境安全评估

2021 年 10 月 29 日，国家网信办公开征求意见的《数据出境安全评估办法（征求意见稿）》为规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动方面提供了行政法规依据。评估包括安全评估和风险自评估，前者是指按要求向监管机关申报的评估，后者是数据处理者自行开展的内部评估。若干关键项如下：

（1）安全评估要求

触发申报的五种具体情形：（a）关键信息基础设施的运营者收集和产生的个人信息和重要数据；(b)出境数据中包含重要数据；(c)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；（d）累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息；(e)国家网信部门规定的其他情形。其中，(c)项和(d)项是《个人信息保护法》出台后首次明确涉及个人信息出境安全评估的标准。数据出境评估结果有效期为二年。在有效期内如有重大变更

(例如境外接收方处理数据的用途、方式发生变化)，应当重新申报评估。

重点评估的七大事项：(a) 合法、正当、必要原则。数据出境的目的、范围、方式等的合法性、正当性、必要性。(b) 境外接收方的数据保护水平。境外接收方所在国家或者地区的数据安全保护政策法规及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、行政法规规定和强制性国家标准的要求。(c) 总体风险。出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险。(d) 数据安全和个人信息权益保障。数据安全和个人信息权益是否能够得到充分有效保障。(e) 数据出境相关合同。数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务。(f) 法律遵守情况。遵守中国法律、行政法规、部门规章情况。(g) 其他事项。国家网信部门认为需要评估的其他事项。

数据处理者应当通过所在地省级网信部门向国家网信部门申报安全评估。申报数据出境安全评估，应当提交申报书、数据出境风险自评估报告、数据处理者与境外接收方拟订立的合同或者其他具有法律效力的文件等，以及安全评估工作需要的其他材料。国家网信部门自出具书面受理通知书之日起 45 个工作日内完成安全评估;情况复杂或者需要补充材料的，可以适当延长，但一般不超过 60 个工作日。评估结果以书面形式通知数据处理者。

(2) 自评估要求

无论数据处理者的数据出境活动是否触发安全评估申报的要求，其在向境外提供数据前均应事先开展数据出境风险自评估。自评估的重点评估事项与安全评估要求相对类似，包括：

1）数据出境及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；

2）出境带来的总体风险；

3）数据转移风险；

4）境外接收方的责任义务；

5）出境后续风险；

6）与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。

（四）地方数据条例重点解读

为加强数据监管管理与安全保护制度建设，保障数字经济的有序稳定发展，十余个省市陆续出台了与数据发展相关的条例（包括大数据条例、数据条例、相关草案），其中，最具代表示范意义的是贵州省 2016 年出台的《贵州省大数据发展应用促进条例》，深圳市 2021 年 7 月发布的《深圳经济特区数据条例》，上海市 2021 年 11 月发布的《上海市数据条例》。从这三部数据条例中，可以看到地方性法规对具体实施细节做出的规定和指引，并结合舆论热点、各地监管重点等加入了场景化的控制和约束，有利于保障数据安全和个人信息保护要求的全面落实，从而整体推动数据安全生态的发展。

1、第一个“吃螃蟹”的《贵州省大数据发展应用促进条例》

作为国内首部大数据地方法规，《贵州省大数据条例》中明确将大数据纳入地方经济社会规划，全力推进数据开放共享，引入负面清单制度，将依法不能向社会开放的公共数据形成目录向社会公布，提出隐私泄露有相应的法律责任和应急预案，填补了大数据行业的法规空白。

《贵州省大数据条例》共三十九条，分为总则、发展应用、共享开放、安全管理、法律责任、附则、共六章，紧扣贵州省大数据发展应用的现实需求和趋势，对贵州省大数据发展应用的原则、总体目标、发展重点、促进措施、安全管理以及法律责任等作出了宣示性、原则性、概括性和指引性规定。对大数据采集、存储、清洗、开发、应用、交易、服务单位提出了安全方面的要求，包括建立数据安全防护管理制度，制定数据安全应急预案，定期开展安全评测、风险评估和应急演练，并在发生重大数据安全事故时，应立即启动应急预案，及时采取补救措施，告知可能受到影响的用户，同时按照规定向有关主管部门报告等。

《贵州省大数据条例》淡化、回避了在数据交易、数据权属方面的问题，但在诸多方面进行了积极尝试和有效探索，为大数据产业发展立下了一块重要里程碑，为后来国家、地方等各个层面的大数据立法提供了有益参考。

2、数据领域综合性地方法规的风向标——《深圳经济特区数据条例》

《深圳经济特区数据条例》于今年 6 月 29 日颁布，自 2022 年 1 月 1 日起施行，共 100 条，分为总则、个人数据、公共数据、数据要素市场、数据安全、法律责任、附则七章。作为数据领域首个城市级综合性地方法规，《条例》未将视野局限于数据的某个方面，而是涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，开启了数据领域立法的多个首次，包括率先对数据权益范围与类型进行明确，首次确立数据领域的公益诉讼制度等，为后续其他地区的数据立法工作提供了显著的借鉴意义。

《条例》明确了自然人对个人数据享有知情同意、补充更正、删除、查阅等人格权益，以及“自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益”，在数据权益范围和类型的探索中对已经取得普遍共识的人格权益、数据财产权益做出了确定性要求。

为保障数据管理工作的有效开展和落实，《条例》明确了数据管理工作是由市数据工作委员会领导协调，市人民政府、市政务服务数据管理部门、市网信部门、市发展改革、工业和信息化、公安、财政、人力资源保障、规划和自然资源、市场监管、审计、国家安全等部门以及市各行业主管部门等各相关部门履行各自职责范围内数据管理工作的统筹、指导、监督等工作，

为全方位强化对个人数据的保护，《条例》制定了“处理个人数据应当充分尊重和保障自然人与个人数据相关的各项合法权益”的基本原则，确立以告知同意为前提的个人数据处理规则并明确告知要求，并针对敏感个人数据明确保护要求。同时该条例首次在立法中认可了数据处理者在自然人撤回同意前基于同意进行的合法数据处理的有效性，并要求建立个人数据保护监督管理联合工作机制、个人数据保护投诉举报处理机制。《条例》还规定除该生物识别数据为处理个人数据目的所必需且不能替代外，应当同时提供处理其他非生物识别数据的替代方案；要求数据处理者明示用户画像的具体用途和主要规则，且自然人有权拒绝基于提升产品或服务质量目的的用户画像或基于用户画像推荐的个性化产品和服务；同时严格要求未满十四周岁未成年的个人数据需遵循敏感个人数据要求，并限制数据处理者不得基于用户画像向未满十四周岁的未成年人推荐个性化产品或者服务。

针对公共数据的管理和使用，《条例》提出构建公共数据资源管理体系，建立以城市大数据中心及其分中心为核心的公共数据资源统一管理机制；实行公共数据分类管理制度，建立基础数据库、主题数据库和业务数据库；实行公共数据目录管理制度，按照公共数据资源目录编制规范要求，对公共数据进行目录管理。为推动公共数据最大限度开放、共享和利用，该条例提出公共数据应当以共享为原则；明确分类分级、需求导向、安全可控为公共数据开放应遵循的原则，并按照开放条件将公共数据分为无条件开放、有条件开放和不予开放三

类；提出应依托城市大数据中心建设城市智能中枢平台体系，为公共管理和服务以及各区域各行业应用提供统一、全面的数字化服务。

《条例》从多方面进行了数据要素市场的探索，包括建立健全数据标准体系，推动数据质量评估认证与数据价值评估，建立数据生产要素统计核算制度并推动将数据生产要素纳入国民经济核算体系，承认数据可交易并明确数据交易范围为“市场主体合法处理数据形成的数据产品和服务”，提出基于市场自由意志建立数据交易平台，同时对数据交易的公平竞争提出了规定。

《条例》进行了数据安全保护相关内容的进一步细化，包括确定由市人民政府负责统筹数据安全管理工作，由市网信部门统筹协调制定重要数据具体目录；明确数据处理者在数据收集、加工、存储、共享开放、销毁、委托处理、出境、风险评估等方面的安全管理责任，并落实对数据泄露、损毁、丢失、篡改等异常情况的监测与预警，以及数据安全事件应急处置工作；明确数据安全监督部门通过开展数据安全预警工作、对数据处理者进行数据安全管理认证和评估、约谈违规数据处理者等措施强化数据安全监督，并强调相关人员在履职过程中的保密责任。

数据侵权行为通常具有较高的隐蔽性，即便被侵权方发觉，取证困难、诉讼时间或经济成本等因素也加大了有效维权的难度。参考2020 年 9 月中华人民共和国最高人民检察院发布的《关于积极稳妥拓展公益诉讼案件范围的指导意见》中关于“将个人信息保护作为网络侵害领域公益诉讼的办案重点”的意见，《条例》在地方立法中首

次确立了数据领域的公益诉讼制度，提出对于“违反本条例规定处理数据，致使国家利益或者公共利益受到损害的”，人民检察院和法律、法规规定的组织可以依法提起民事公益诉讼；人民检察院还可以针对“违法行使职权或者不作为，致使国家利益或者公共利益受到损害的”数据监管履职部门，向其行政机关提出检察建议，若行政机关不依法履行职责的，人民检察院可以依法提起行政公益诉讼。

3、紧跟数据立法元年步伐的先行者——《上海市数据条例》

《上海市数据条例》于今年 11 月 25 日颁布，自 2022 年 1 月 1 日起施行，共 91 条，分为总则、数据权益保障、公共数据、数据要素市场、数据资源开发和应用、浦东新区数据改革、长三角区域数据合作、数据安全、法律责任、附则、共十章。《条例》吸收了其他地区的条例及草案经验，并通过“第六章 浦东新区数据改革”、“第七章 长三角区域数据合作”两个章节对浦东新区、长三角区域的发展提出数据层面的支持与推动。

《条例》规定了各级政府在数据发展和管理等方面的职责，明确由市政府办公厅负责统筹规划、综合协调全市数据发展和管理工作，市发展改革部门负责统筹本市新型基础设施规划建设和数字经济发展，市网信部门负责统筹协调本市个人信息保护、网络数据安全和相关监管工作，市经济信息化、公安、国家安全机关、财政、人力资源社会保障、市场监管、统计、物价、大数据中心等部门在各自职责范围内履行相关职责。同时，该条例提出“鼓励各区、各部门、各企业事业单位建立首席数据官制度”，明确市人民政府设立数据专家委员

会，并对数字基础设施规划和布局、人才建设、数据标准体系建设等提出要求。

在数据权益方面，《条例》明确“依法保护自然人对其个人信息享有的人格权益”，通过“依法保护自然人、法人和非法人组织在使用、加工等数据处理活动中形成的法定或者约定的财产权益”承认交易主体对数据本身的财产权益，而不局限于数据产品和服务，并强调“在数字经济发展中有关数据创新活动取得的合法财产权益”也将依法保护，以进一步鼓励与保护数据创新活动的产物。同时，该条例对数据收集、使用、交易、突发事件数据使用等活动提出原则性规定，以保障合法数据权益。

关于个人数据的保护，《条例》在数据处理同意的要求中，提出个人信息处理获得同意的相关规定，与《个人信息保护法》的明示同意、单独同意进行了呼应，并通过“明确拒绝”可对 “处理个人自行公开或者其他已经合法公开的个人信息”行使拒绝权、撤销权。该条例对个人信息处理告知事项、个人信息更正和补充权提出了要求，并明确了生物识别信息处理需单独同意的要求。同时，结合社会焦点，《条例》对于在公共场所及居住小区、商务楼宇等区域，安装图像采集、个人身份识别设备，提出了“应当为维护公共安全所必需”、“设置显著标识”的要求；对于“大数据杀熟”等利用个人信息进行自动化决策明确规定“不得对个人在交易价格等交易条件上实行不合理的差别待遇”，且个人“有权拒绝处理者仅通过自动化决策的方式作出决定”。

《条例》在公共数据的管理、开放和利用方面，与《深圳经济特区数据条例》保持了多项原则的一致性，包括：由市大数据中心统一管理公共数据；对公共数据实施分类分级管理；建立公共数据目录管理体系；公共管理和服务机构之间共享公共数据，应当以共享为原则，不共享为例外；公共数据按照开放类型分为无条件开放、有条件开放和非开放三类，明确相应开放方式与使用要求。

同时，《条例》明确提出“建立公共数据授权运营机制”，规定“市政府办公厅应当组织制定公共数据授权运营管理办法，明确授权主体，授权条件、程序、数据范围，运营平台的服务和使用机制，运营行为规范，以及运营评价和退出情形等内容”，体现了政府作为公共数据开放的先行角色。该条例中还对公共数据收集原则、按区域属性回传、归集方式、基础数据库建设、建立健全公共数据质量管理体系、共享和开放相关原则与机制等做出规定。

针对数据要素市场，《条例》确定“公平、开放、有序、诚信”为培育数据要素市场的总体要求，并提出“建立资产评估、登记结算、交易撮合、争议解决等市场运营体系”和“为数据交易提供数据资产、数据合规性、数据质量等第三方评估以及交易撮合、交易代理、专业咨询、数据经纪、数据交付等专业服务”，充分显示了上海市不止于建立数据交易所，而是构建从交易起点到争议解决的闭环交易圈，建立完整数据交易产业链的愿景。《条例》明确了数据交易服务机构管理要求，规定应建立数据资产评估制度，建立健全数据要素配置的统计指标体系，鼓励市场主体“通过实质性加工和创新性劳动形成数据

产品和服务”，并概述不得进行数据交易的情形，提出了数据交易方式可自主选择，以及数据交易活动按照自主与评估的原则进行价格确定。

为了发挥海量数据和丰富应用场景优势，《条例》提出“鼓励和引导全社会参与经济、生活、治理等领域全面数字化转型，提升城市软实力”。为了促进数据技术与实体经济、服务业和政府管理、服务、运行的深度融合，该条例明确“支持数据基础研究和关键核心技术攻关，发展高端数据产品和服务”，并提出鼓励企业开展数据融合应用、提高民生领域数字化水平、深化“一网通办”和“一网通管”建设等举措，以推动数据全面赋能数字化转型。

《条例》依法规定“实行数据安全责任制，数据处理者是数据安全责任主体”，明确数据处理者安全保护义务并要求重要数据处理者应开展风险评估，要求政府实施数据分类分级保护制度、建立重要数据目录管理机制、建立数据安全风险管理机制、建立健全数据安全应急处置机制。

《条例》明确规定了国家机关、履行公共管理和服务职责的事业单位的法律责任，并通过“违反本条例规定，依法受到行政处罚的，相关信息纳入本市公共信用信息服务平台，由有关部门依法开展联合惩戒”将违例行为纳入征信系统，以信用惩戒作为新的处罚措施；同时，该条例承袭《个人信息保护法》，明确“违反本条例规定处理个人信息，侵害众多个人的权益的，人民检察院、市消费者权益保护委

员会，以及由国家网信部门确定的组织，可以依法向人民法院提起诉讼”。

（五）数据安全监管审计提上日程

近年来，全球数据泄露、滥用等乱象频生，尤其在大型互联网平台企业的迅速发展下，数据垄断及导致的滥用、泄露等问题已威胁到社会稳定、国家安全，各国对大型互联网企业数据安全违法的惩治力度不断增大，例如美国针对 Facebook 违反用户隐私保护策略向其处以 50 亿美元罚款，爱尔兰因数据非法跨境传输对 Facebook 处以 28 亿美元罚款，法国因谷歌搜索引擎对 Cookie 的管理方式不当处以 1 亿欧元罚款。今年 7 月，我国网络安全审查办公室对“滴滴出行”、“运满满”、“货车帮”、“BOSS 直聘”等赴美上市公司展开了《网络安全审查办法》发布至今的首轮正式审查行动，并停止新用户注册；随后滴滴出行因存在严重违规收集使用个人信息等问题，旗下 25 个应用遭下架，股价疯狂下跌。

数字经济时代，数据成为经济发展的重要驱动力和关键生产要素，作为数字经济重要组成部分的平台经济，以数据驱动业务，使得数据成为互联网平台企业竞相争夺的资源，强制用户授权、过度索权、“大数据杀熟”等非法违规的行为在利益驱使下愈发严重。《数据安全法》第二十四条提出“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”，可见，形成我国有效的数据安全监管审计机制迫在眉睫。

1、《网络安全审查办法》修订稿强调数据安全审查

2020 年 6 月，十二部委联合发布《网络安全审查办法》，推动建立国家网络安全审查工作机制，以确保关键信息基础设施供应链安全，维护国家安全。今年 7 月，国家网信办在对滴滴等企业实施网络安全审查期间，发布了《网络安全审查办法（修订草案征求意见稿）》（以下简称《修订草案》），《修订草案》中针对数据安全审查进行了补充和强调。

（1）明确增加对数据安全的规范，落实数据安全审查机制

《修订草案》第一条中将《数据安全法》纳入制定依据，并在第二条中增加“数据处理者(以下称运营者)开展数据处理活动”，对规范主体与规范行为进行了扩大，直接表明本次修订主旨为加强对数据安全相关行为的规范，明确将数据安全纳入网络安全审查范畴。

（2）明确纳入数据处理活动及国外上市为需审查情形

《修订草案》对《数据安全法》中“影响或者可能影响国家安全的数据处理活动”进行了更具体的明确规定，包括新增第六条“掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”，第十条纳入“数据处理活动以及国外上市”为网络安全审查重点情形，并将“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”与“国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险”归为主要考虑因素，表明数据出

境前后、企业在国外上市前后，均需要持续性关注和防范因核心数据、重要数据或大量个人信息可能引发的风险。

2、《网络数据安全管理条例（征求意见稿）》明确数据安全审计

今年 11 月 14 日，国家网信办公布了《网络数据安全管理条例（征求意见稿）》，对数据安全、数据分级分类、数据处理者境外上市、数据出境等方面提出详细和有针对性的监管措施，明确了数据处理者在数据安全方面的义务要求，同时，《条例》对数据安全监管审计作出了进一步的明确和要求。

（1）明确数据安全审计制度

《条例》在第五十八条明确提出“国家建立数据安全审计制度”，要求“数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计”，并规定“主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况”。明确了数据安全审计制度的两种形式，一种是通过第三方专业数据安全审计机构针对数据处理者，在处理个人信息遵守法律、行政法规等数据安全方面的定期审计，另一种则是由主管、监管部门针对重要数据处理活动，在数据处理者履行法律、行政法规规定的义务等方面的审计。

（2）强调针对大型互联网平台的数据安全审计

《条例》在第五十三条提出“大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，

并披露审计结果”，第四十三条要求“日活用户超过一亿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”。该两条通过要求大型互联网平台以年为单位针对数据安全及使用情况开展第三方审计，以及发生重要规则、政策修订时引入监管部门的监督与许可，强化了相关企业在数据安全合规方面的保障。

（3）明确数据处理者的年度数据安全评估及报告义务

为落实《数据安全法》第三十条“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告”的要求，《条例》第三十二条规定“处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门”，以实现针对重要数据处理者和赴境外上市处理者企业内部数据安全管理情况的持续性监督与评估。

在数字化转型快速发展的进程中，数据愈发频繁的流动尤其是跨境流动同其汇聚、挖掘后愈发显著的经济价值、战略价值等，愈发受到各组织、行业、国家的关注和重视，随着我国数据安全监管体系的日益完善，对数据实施完备安全保护措施的同时，有效监管审计机制的建设也正提上日程，促进更高效的发现问题以防范各类数据风险，保障数字经济的高效有序发展。

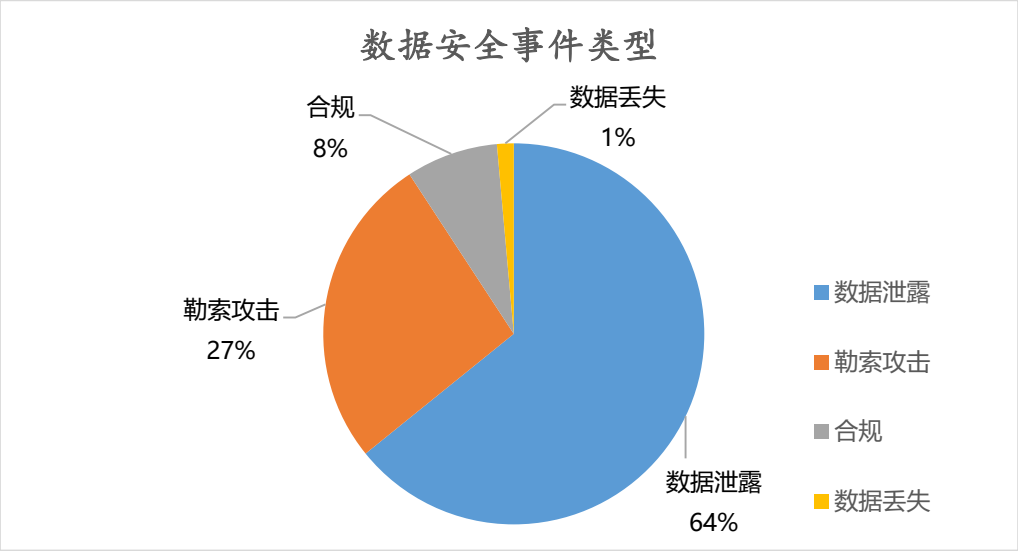
三、年度数据安全事件分析

本部分基于大数据协同安全技术国家工程研究中心 2021 年发布的《全球数据安全观察》周报中收录的数据安全事件，从多个维度对各类型数据安全事件进行梳理和总结分析。

（一）整体态势分析

1、数据安全事件类型占比

2021 年数据安全事件类型主要包括数据泄露、勒索攻击、数据合规、数据丢失四种类型，其它如数据损毁等因占比较少，不单独归为一类。



通过统计分析发现，2021 年发生的数据安全事件类型仍以数据泄露为主，占 64%，在所有类型中占比最高；

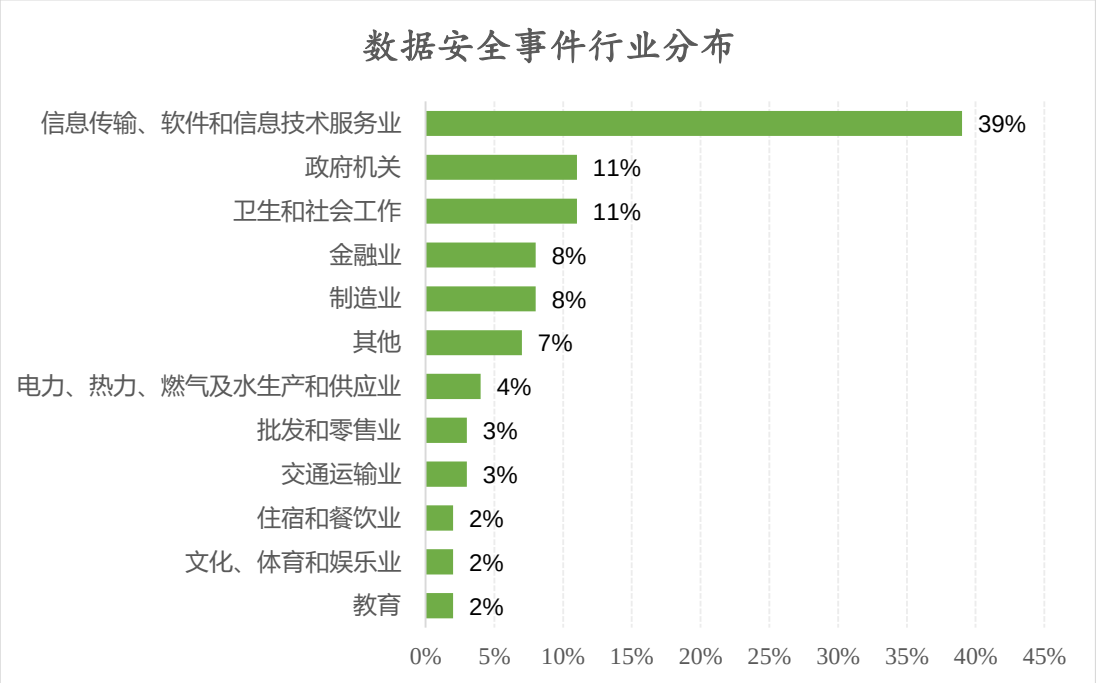
其次，勒索攻击今年变得比较活跃，该类事件也占有较大比重，为 27%；

数据合规类型事件主要指由于数据合规问题而遭受罚款的事件，该类事件占比为 8%；

数据丢失的占比最少，为 1%，此类型事件大多是由于自然灾害或人为恶意删除以及操作失误造成。

2、数据安全事件行业分布

本报告里事件所属行业的划分，主要参考《国民经济行业分类》（GB/T 4754-2017）。对 2021 年《全球数据安全观察》周报里收录的数据安全事件所属行业进行统计分析，结果如下：



信息传输、软件和信息技术服务业以占比 39%的比例位居行业之首，该大类主要包括互联网行业、软件和信息技术服务、电信、广播电视和卫星传输服务等；

政府机关排在第二位，占比为 11%。主要由于该行业是由国家组织发起的网络攻击的首要目标；

卫生和社会工作占比并列第二。受新冠疫情影响，医院、公共卫生服务、卫生组织、疫苗研究机构等都是黑客攻击的重点目标；

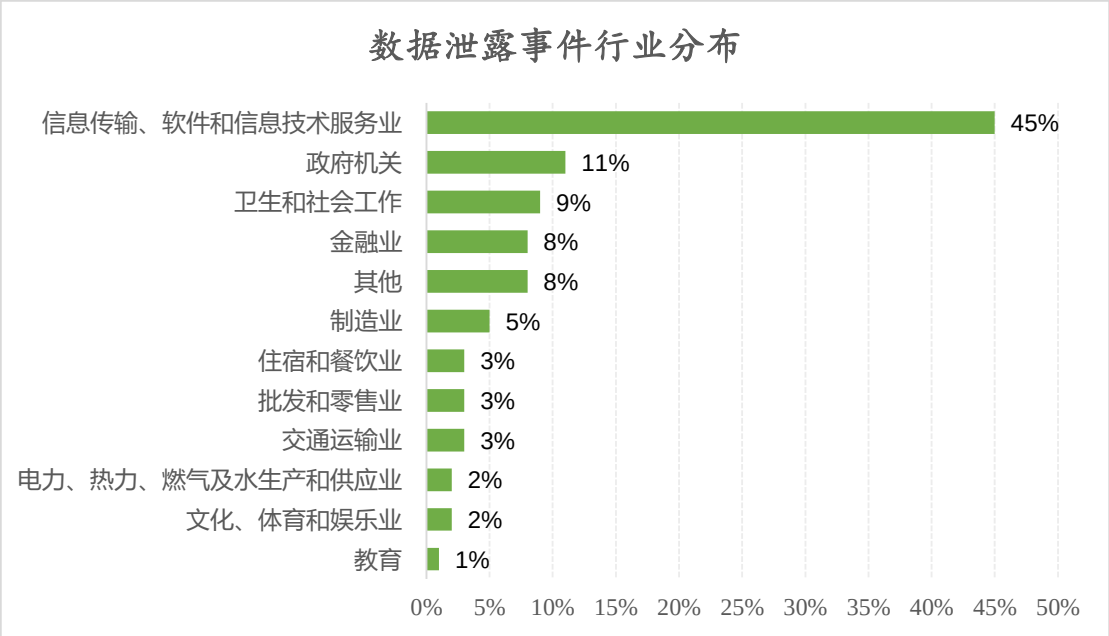
金融业、制造业、电力、热力、燃气及水生产和供应业也是数据安全事件频发的行业，其次，批发和零售业、交通运输业占比相当，均为 3%；住宿和餐饮业、教育、文化、体育和娱乐业在本次分析中占比最低，为 2%。

（二）数据泄露事件分析

对于数据泄露类型事件，下面从行业分布、泄露规模、泄露原因、泄露数据类型四个方面进行单独分析，结果如下。

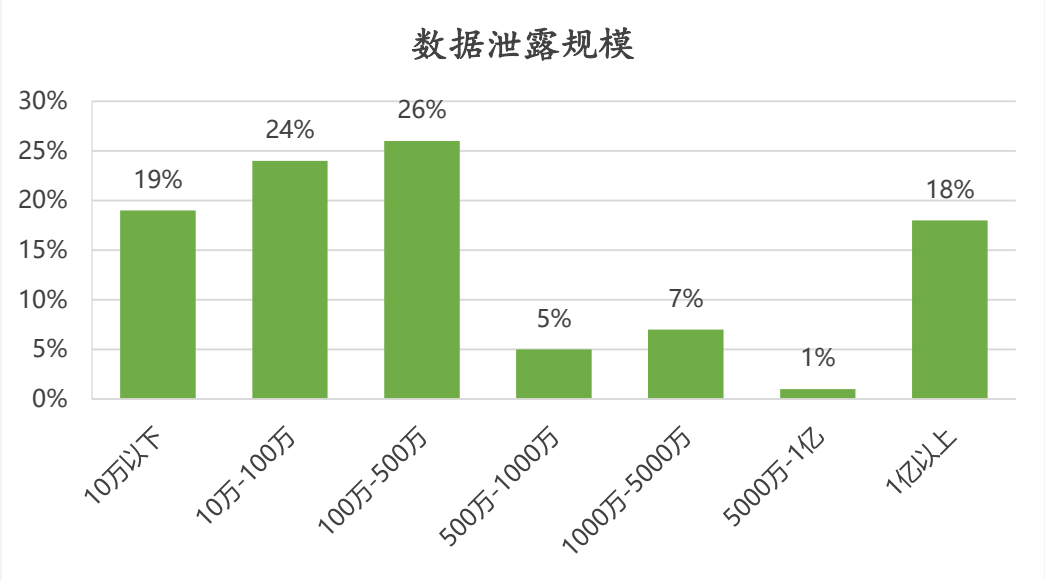
1、数据泄露事件行业分布

2021 年数据泄露愈演愈烈，数据安全形势依然不容乐观，同时，各行业之间也有较大差异。数据泄露事件发生最多的行业为信息传输、软件和信息技术服务业，占比高达 45%；政府机关数据泄露也较为严重，在所有行业中排名第二，占比为 11%；其次，由于黑客攻击和疫情原因，卫生和社会工作以及金融业也有较高比例，分别为 9%和 8%；教育行业在此次分析中，排名最低，占比仅为 1%。



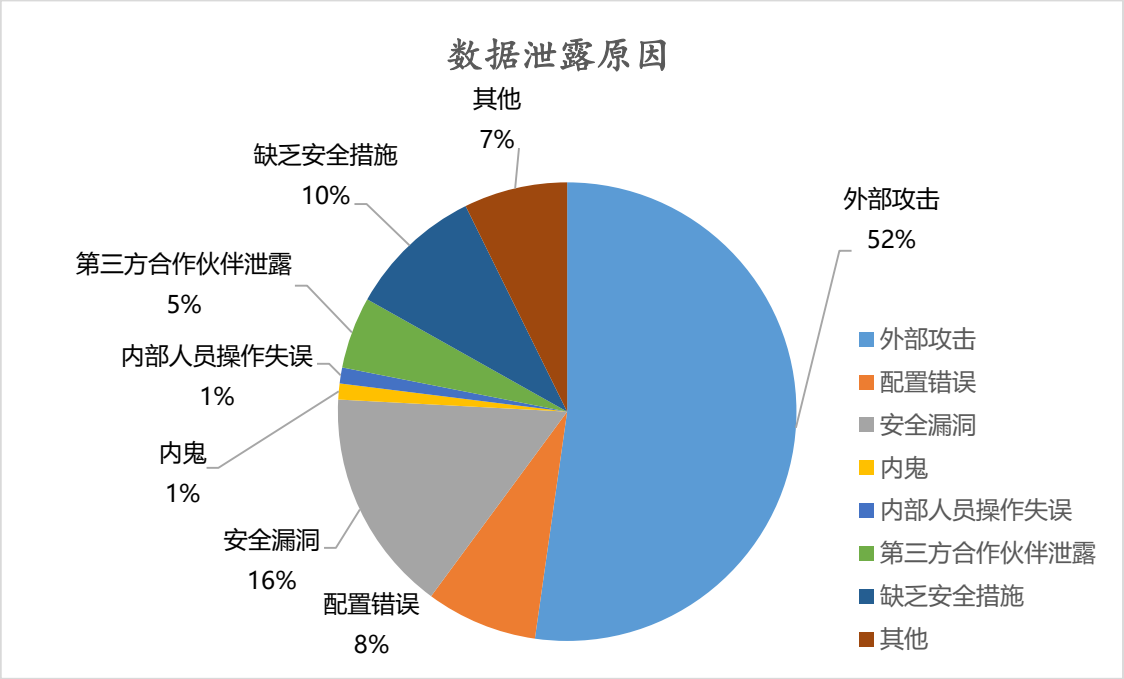
2、数据泄露规模

在所有数据泄露事件中，35%的事件未披露具体泄露数据规模，在披露数据规模的事件中，泄露的数据量在 100 万-500 万的占比最高，为 26%；10 万-100 万阶段占比次之，为 24%；泄露规模大于 1 亿条的以 18%的占比排名第三，可见，大规模数据泄露事件依旧层出不穷。



3、数据泄露原因

对数据泄露事件所发生的具体原因进行深入剖析，将主要原因归类为：外部攻击、配置错误、安全漏洞、内鬼、内部人员操作失误、第三方合作伙伴泄露、缺乏安全措施等，以下为主要结论。



外部攻击是大部分数据泄露的罪魁祸首。本报告中共有 52%的数据泄露事件可以归因为外部攻击，具体原因包括黑客入侵、网络钓鱼及未经授权访问等；

安全漏洞是导致数据泄露的第二大原因。本报告共有 16%的数据泄露事件由安全漏洞引起，该类型主要原因包括软件本身安全漏洞、安全机制缺陷、系统缺陷或数据库漏洞等；

缺乏安全措施类型占 10%，该类型主要由数据库或服务器未做任何加密等安全措施引起，使数据公开暴露而导致泄漏；

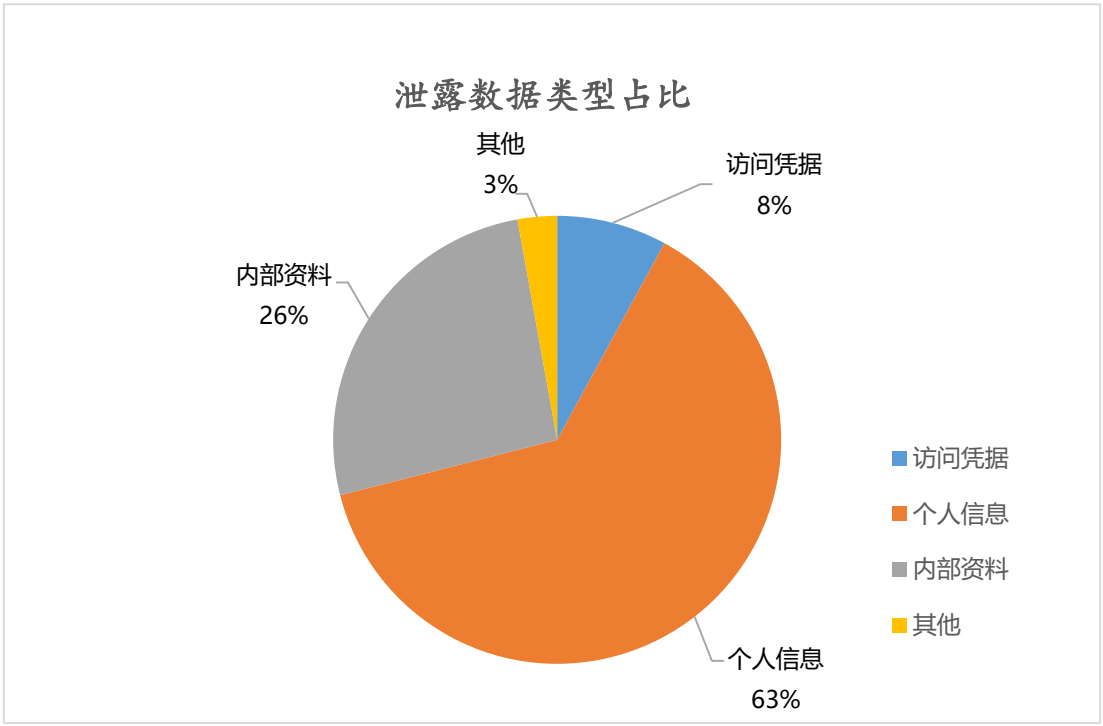
其次，配置错误也是重要原因之一，在本次分析中占有 8%的比例。主要原因包括服务器配置不当、云存储配置错误及开发人员错误配置等；由于第三方合作伙伴原因导致数据泄露的占 5%，内鬼和内部人员操作失误占比较小，仅为 1%。

4、泄露数据类型

从泄露的数据类型来看，个人信息泄露最为严重，占据了 63%的比例，主要涉及姓名、电话、身份信息、银行卡、地址等；

内部资料也是最常见的被泄露信息，26%的泄露事件涉及此类数据，其中，内部资料包括内部机密、企业商业机密信息、技术机密信息等数据；

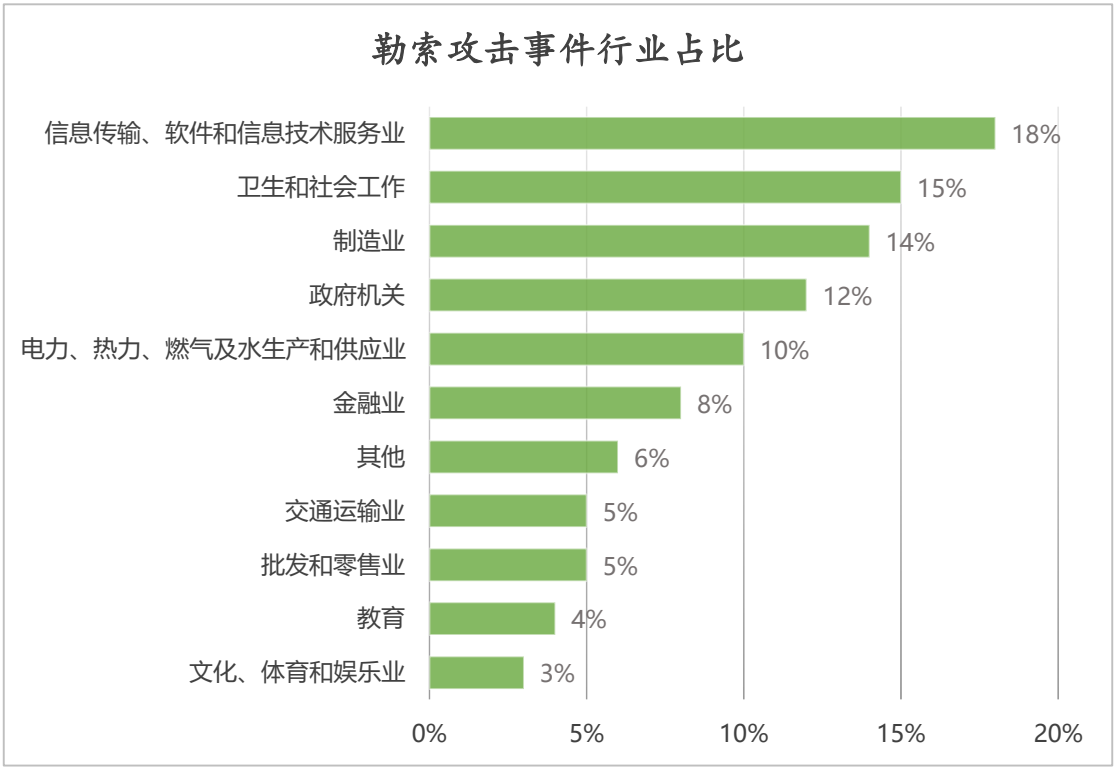
其次，8%的数据泄露涉及用户访问凭据，主要包括账号密码、口令信息、证书及其他证明身份的信息等。



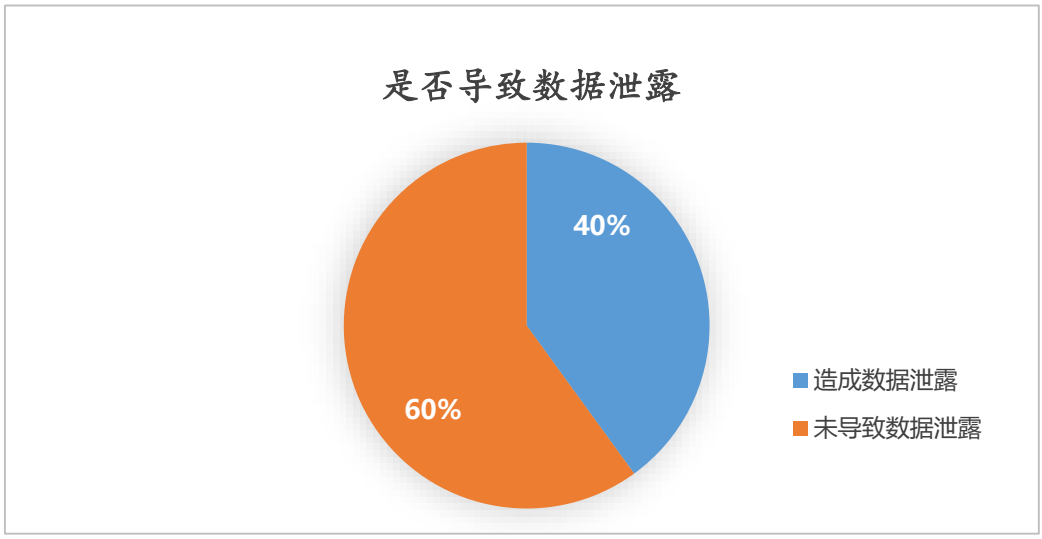
（三）勒索攻击事件分析

据统计，信息技术服务、医疗卫生和制造业是遭受勒索攻击事件占比最高的行业。在全球范围内，信息技术服务行业受勒索软件的影响较为严重，占攻击事件的 18%；针对医疗行业的攻击由于受执法机构高度关注和打击，情况稍有缓和，但在所有行业当中仍然占比较高，为 15%；制造业也同样成为勒索攻击的重点对象，占比达到了 14%，对于制造业公司而言，因为系统宕机问题所造成的损失无疑是巨大的。

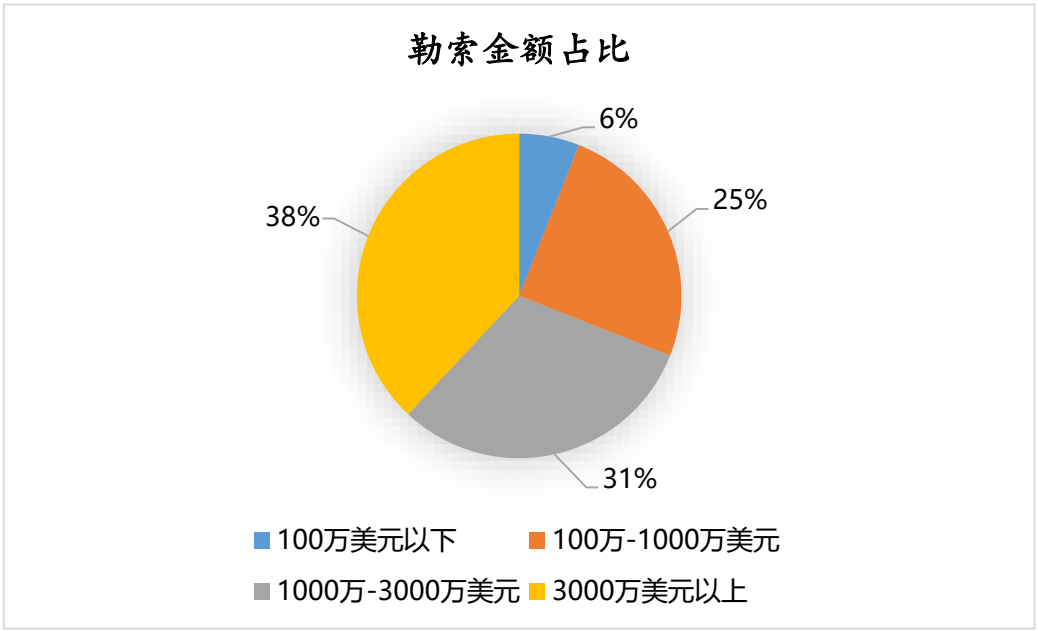
此外，政府机关、电力、热力、燃气及水生产和供应业、金融等行业也影响较重，占比均在 8%及以上。



在众多勒索攻击事件中，约 60%的勒索攻击伴随着数据泄露，以数据泄露问题威胁受害者支付巨额赎金。



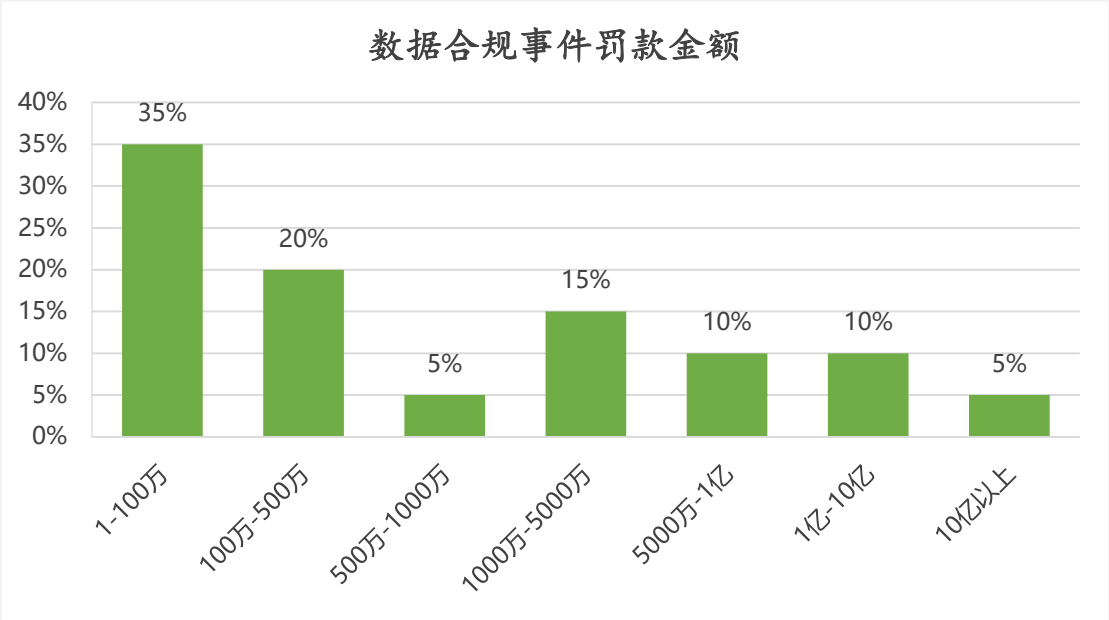
针对性勒索攻击的赎金规模不断上升，索要 3000 万美元以上勒索赎金的事件在所调查的勒索数额中占比最高，达到 38%。



据以往统计数据显示，2019 年最高勒索赎金金额仅为 1500 万美元，2020 年增长至 3400 万美元，而在 2021 年尚未结束之际，勒索赎金纪录竟再次被刷新，飙升至 5000 万美元。

（四）数据合规事件分析

2021 年，越来越多因为数据合规问题而导致罚款的事件为我们敲响了警钟，本年度该类事件越来越受重视，占比为 8%。



从罚款金额来看，在 100 万以内的占比最高，为 35%；其次是 100 万-500 万的占 20%；其中，大额罚款也不在少数，1000 万以上罚款的事件占总体的 40%,如亚马逊因违反欧盟数据保护条例遭重罚 8.87 亿美元、Facebook 侵犯隐私案签和解协议，赔偿 160 万用户 6.5 亿美元、WhatsApp 违反 GDPR 被罚 2.25 亿欧元等案例。

值得一提的是，在所有的数据合规事件中，因违反 GDPR 条例而导致罚款的占 45%，罚款原因如违反个人数据处理相关原则、处理用户个人信息未能充分告知、向境外非法传输个人数据、未采取安全措施保护用户个人信息等。

四、专家观点

互联网企业要加强数据安全意识

中国工程院院士 邬贺铨

中国互联网渗透到生活的方方面面，提升工作生活效率的同时，也增加了人们对互联网的依赖。中国工程院院士邬贺铨在第九届互联网安全大会（ISC2021）上提到，提升网络安全意识，加强国家安全、数据安全、客户隐私保护，互联网企业通常都是大数据企业，基于大量的用户数据和所服务的企业数据开展业务，这些数据不仅包含了用户隐私，也涉及国家敏感数据，但一些企业在自律能力、对客户的敬畏、对数据的保护等方面做得不够，给国家数据安全和国家安全带来巨大的风险。

互联网治理的一个重要方面是规范数据的使用和安全保护，作为互联网企业，在发展中一定要加强国家安全、数据安全、网民利益和隐私保护的的意识。

（来源：第九届互联网安全大会 ISC 2021）

《数据安全法》为各行业数据安全提供了监管依据

中国工程院院士 倪光南

《数据安全法》的出台正式以法律的形式将数据安全上升到国家安全的战略，并与《国家安全法》和《网络安全法》共同构成国家安全的基础性法律，形成国家整体安全观的三大基石。《数据安全法》在立法理念上强调国家总体安全观，坚持“国家风险防范与数字经济

发展并重”的数据安全立法原则；在立法维度上既明确了数据的安全又关注了数据发展；同时对全国数据安全工作做了统筹部署安排；在适用范围和适用主体上实现全覆盖并明确了域外管辖效力；强调了加强对数据出境管理；提出建立政府强制、平台自治、行业自律的合作治理模式；对违法行为提出了明确的处理方式；明确了政务数据的安全要求。

但是，数据本身又有其特殊性，在客观世界的物质、能量、信息这三种基本形态中，属于信息的范畴，因此，衡量数据安全显然也需要有专门的方法。为此需要制订对数据的监测和评估的标准，并设立或委托相应的机构予以实施。

（来源：中国网络社会组织联合会）

保障数据安全需建立主动免疫保障体系

中国工程院院士 沈昌祥

保障数据安全还需要建立主动免疫保障体系，只有这样才能保障数据安全。建立主动免疫保障体系涉及以下几个方面：

第一，要有新的计算模式，以密码为基因抗体实施身份识别、状态度量、保密存储等功能，及时识别自己和非己成分。我们要提高新的计算模式，一边计算，一边防护，从而破坏与排斥进入机体的有害物质，相当于为网络信息系统培育了免疫能力。

第二，要有“计算机体系结构+防护部件”。

第三，要构建科学的防护框架，即在可信安全管理中心支持下的主动免疫三重防护框架。

第四，落实等级保护要求，保障数字经济健康发展。据介绍，目前可信计算广泛应用于国家重要信息系统，如增值税防伪、彩票防伪、二代居民身份证安全系统、中央电视台全数字化可信制播环境建设，国家电网电力数字化调度系统安全防护建设等。我国等级保护要构建一个体系，即软件不能篡改，并行执行的程序需要一边执行一边可信检查，实行边执行边检查，而且要有动态的管理措施，解决现在“马后炮”的问题。

（来源：电子信息产业网）

智能网联新能源汽车数据安全如何保障

中国工程院院士 孙逢春

智能网联新能源汽车数据具有面广、量大的特征，其安全体系是一个复杂的系统工程，主要包括四个体系：法律法规体系、标准规范体系、监管体系、技术体系。

在政策法规层面，网络安全法、数据安全法和个人信息保护法成为我国网络治理和数据保护的三驾马车。但在具体操作层面，数据安全法律体系有待完善，智能网联新能源汽车或智能交通领域亟待出台专项实施细则。

在技术标准与规范等支撑体系方面，仍需从部门规范、行业标准、地方标准、企业标准、示范工程等多维度同步推进共性基础和通用技术标准的制定。

在监管方面，2021 年，国家出台了多项有关数据安全的管理规定。比如，《汽车数据安全管理若干规定（试行）》确定了汽车数据

定义、数据运营者权责和相关部门的监管准则；《关于加强智能网联汽车生产企业及产品准入管理的意见》对汽车数据安全提出了明确的管理要求。

在技术方面，数据安全主要涉及数据安全采集与分析、数据安全防护、数据安全测评技术等。在这方面，一是要建立端、管、云立体的威胁态势感知系统，确立数据安全评估机制，建立应急响应体系，加强安全监督检查；二是提升软件的安全加固技术能力，加快提升终端设备的安全水平；三是全面推进车载密码技术开发及生态系统应用；四是开发数据隐私与身份鉴别技术，通过通信安全、数据资产加密和数据安全共享，全方位保护敏感隐私信息，阻止未授权的操作。

关于智能网联新能源汽车数据的安全发展，中国工程院院士孙逢春有以下几点建议。第一，加快完善数据安全立法及法规体系建设。第二，全面推进数据安全标准规范支撑体系建设。第三，完善数据安全管理联动机制。第四，加快构建智能新能源汽车数据安全技术架构，设立智能新能源汽车数据安全科技专项。第五，在国家层面进行顶层设计，多部门协同制定智能汽车数据传输、接入以及使用等关键环节的规范和要求，将车辆用户信息、环境信息、位置信息按统一要求接入平台，进行规范化管理。

（来源：中国科学报）

用好大数据，要运营安全两手抓

360 集团创始人、董事长 周鸿祎

过去 10 年互联网公司是大数据的主角，在服务用户过程中收集积累了海量的数据；但是未来数字化的主战场是产业互联网、数字政府、智慧城市，物理世界和业务流程将全部数字化，未来互联网的主要流量来自于政府和传统产业。数字化时代已经来临，大数据是数字化的中心，要以数据运营为抓手做好大数据的开发利用，以网络安全为基础同步推进大数据开发利用和保护。

数据运营是长期持续的，不存在交钥匙工程。衡量一个城市、一个企业的大数据能力，重点不在于数据的数量、种类、新鲜度，而是看有没有数据持续运营的能力。除了做好运营外，安全也是大数据开发利用的“必答题”。当前，大数据面临网络攻击、勒索攻击、数据污染攻击、数据内部泄露等一系列威胁。此外，大数据的流动共享开放，放大了网络攻击风险。高级别网络攻击带来巨大挑战。传统的碎片化防护无法适应网络威胁的新挑战，需要建立体系化的协同联防体系。

（来源：新华网）

广泛提升数据安全能力，保障数据权益，促进数据利用

360 首席安全官、大数据协同安全技术国家工程实验室常务副主任 杜跃进

数据安全问题日益严重，各界对数据安全的重视程度显著提升，但是各相关方普遍存在不知所措、能力薄弱、心中没数的现象。这将

严重影响各方信心，阻碍数据有效利用和数字经济发展。数字经济的发展依赖于大范围的数据流动，仅仅提升个别企业行业或者地区的数据安全水平，对我国整体数据权益保护和数据利用促进的效果有限。另外，要达到良好的效果，也不是仅仅依靠几个技术或者标准就能解决的，而需要建立包括配套政策在内的完整体系。

鉴于上述情况，提出以下三条建议：

以能力成熟度为核心抓手，广泛提升我国整体数据安全水平。在发挥已有积累和保证整体协调的基础上，在全国加快推广数据安全能力成熟度测评咨询，以及数据安全专业人才如数据安全官培养；在确保风险可控的基础上，有序地进一步推广数据安全实网攻防能力的持续验证工作；建立国家级能力合作与支援体系，帮助各行业应对复杂和高级安全威胁。

研究建立更加科学的数据安全治理机制。例如建立**免责机制**，当发生安全事件时，对相关单位不存在失职但是安全攻击超出其能力范围的情况下，对其免责（解决简单“打板子”的问题）；建立安全**事件报告制度**，鼓励报告安全事件，但对瞒报情况严厉处罚（解决普遍“捂盖子”的问题）；建立**能力适配机制**，根据数据安全能力成熟度的水平决定一个机构能够处理的数据类型和范围（解决“没动力”的问题）；等等。

建立良好的社会合作与协同创新生态。数据安全挑战还在持续变化，需要发动社会力量，高效协同、持续创新，为此，需要研究如何结合体制优势和市场化优势、如何发动社会资源建立和运营开放创新

平台等，通过这些方法实现技术方法上的持续改进，和安全能力的持续提升。

通过以上措施，在 2-3 年内实现相关标准和最佳实践的普及和细化、相关人才满足重点需求，主要行业和重点地区综合能力成熟度达到中上等水平；十四五期间完成整体数据安全状况符合我国数字经济发展的总体要求，达到国际领先水平。

（来源：2021 年 11 月 11 日全国政协专题调研会上的发言）

数据开放流通环境下的数据安全新问题

复旦大学教授、大数据协同安全技术国家工程实验室副理事长 朱扬勇

长期以来，数据安全是指保护好数据免遭黑客入侵、网络攻击而造成数据泄露、数据损毁。这是数据封闭环境下的数据安全观，狭义地看其实是数据安全防御，即重点在防御。当前，数据作为数字经济的关键要素，数据在全社会流通、在全球流通的大趋势下，数据安全有了全新的内容，主要是保护国家数据安全和个人隐私、企业的数据价值等，大致分为三个方面的数据安全问题：

（1）数据生产方的数据安全问题

数据生产方有两大类，第一类是信息化工作带来的数据生产，第二类是专门的数据生产。

第一类数据生产方：目前，大部分数据生产方为第一类数据生产方。自从信息化开始以来，几乎每一个信息系统都在将业务信息化的同时，不断地生产数据。从计算机的视角看，信息化就是生产数据的过程。由于信息化涉及了全社会，因此个人、法人和非法人机构等任

何主体都是数据的生产方。信息化的目的是解决业务的问题，数据只是信息化的副产品，直到数据积累到了大量规模变成数据资源，才引起重视，所谓大数据的由来。

第二类数据生产方：当数据的价值被认识后，专门生产数据就成了一些企业的牟利手段。这类数据生产方也是专门的数据供给方，他们生产数据的目的就是向市场供给数据。

传统的数据安全技术主要是保护第一类数据生产方的数据，早期的目的是保护商业秘密或商业竞争力，现在延伸到了保护数据的价值，更重要是数据生产是否安全？是否获得相关数据的生产许可？

（2）数据供给方的数据安全问题

数据供给方是指向市场提供数据（包括数据产品或数据服务）的市场主体。数据私用和向市场提供数据是完全不同的概念。信息化过程中生产的数据在主体内部私用总体问题不大，一旦向市场供给数据，就意味着数据公开，意味着新的数据安全问题出现。首先是国家数据安全问题、其次是个人隐私问题、第三是数据价值保护问题。国家数据安全典型的情况是：在国外上市公司向上市国证券监管部门提交数据是否侵害到国家数据安全？这么多数据如何审查？个人隐私问题并不能简单地匿名化、脱敏、安全计算等技术就能够解决的。第三，作为数据供给方，实现数据价值才是数据供给的目的。数据安全新问题是：数据供给出去后，如何防止数据不被超范围使用、不被广泛传播？即数据价值保护问题。

（3）数据安全实现方式探索

数据作为数字经济关键要素已经形成共识，数据资源、数据资产、数据要素等持续创新和有序推进，数据要素市场建设如火如荼。现行的数据安全技术主要是面向数据封闭环境的，数据流通环境下的数据安全是新问题，需要新技术来解决。新技术需要解决：如何保护数据稀缺性不丧失、数据安全和隐私有保障的前提下实现数据合法有序流通。数据自治开放是指数据由数据拥有者在法律框架下自行确权和管理、自行制定开放规则（所谓数据自治），然后将数据开放给使用者，包括上载数据应用软件使用数据或下载数据到使用者的设备中（使用者没有数据治理权）。具体技术有：数据盒技术；数据权益保护、防泄露、防拼图等安全技术；数据使用标准、数据访问行为管控和数据使用审计等技术等等。

做好数据分类分级的后半程

大数据协同安全技术国家工程实验室副主任 钟力

数据分类分级的重要性不言而喻，既是对数据进行适度保护的依据，也是进行数据安全流通共享、充分挖掘数据要素价值的基础和前提。《数据安全法》提出国家建立数据分类分级保护制度，给出了数据分类分级的基本原则，并要求各地区、各部门建立所在地或行业领域的数据分类分级实施规范或细则，建立重要数据具体目录。近五六年来，贵州、广东、上海、金融和交通等很多省市和行业都发布了数据分类分级相关的标准规范，比如《广东省公共数据管理办法》、《金融数据安全 数据安全分级指南》。

刚发布的《网络数据安全管理条例（征求意见稿）》，是三部上位法的落地实践指导，将数据分为一般数据、重要数据、核心数据。国标《重要数据识别指南（征求意见稿）》给出了识别重要数据的指导方法，指出与经济社会运行相关、与科学技术相关等八类数据被认为是重要数据。国标《网络安全标准实践指南 数据分类分级指引（征求意见稿）》将数据分为公共数据、个人信息和法人数据三大类，分成公开、内部、敏感、重要、核心五个级别。总体上，数据分类分级的法规标准体系在逐步完善之中，分类相对清晰，分级总体还在探讨中，有分三级的、四级的、五级的，还没有形成一致的意见，但终归是会统一的。

但是，这也仅仅是数据分类分级的上半程。在具体实际操作层面，数据分类分级还有不少问题需要解决，很多数据拥有方、安全研究机构和安全公司等，还不知如何操作，数据分类分级的下半程才刚刚开始。比如很多安全公司在承担数据分类分级项目时，陷入到面对巨量数据、给数据打标签等繁琐细节中，人力投入大、工作效率很低。在这些问题当中，最关键的一个问题实际上是定级对象应该如何确定？这似乎被忽略了。就像信息系统的等级保护一样，首先要有一个定级对象，才好去谈后面的事情。因此，我们首先需要做的是确定定级对象，即要给什么样的一个数据对象（数据集）进行分级？

我们应采取依需求而定的定级对象确定，可以根据数据流通共享需求、数据交易需求或数据应用需求，来进行定级对象的确定。具体操作上，数据先默认地进行整体分级，或按照大类划分之后进行整体

分级，例如以一个企业或平台的数据集作为定级对象，这样做的好处是避免落入操作细节，同时数据也能够得到基本的保护。其次，如果有一个数据集要流通共享，那就以该数据集作为定级对象；如果要交易一个数据集，那就以该数据集作为定级对象，从而做到清晰定位数据和精准保护。第三，针对这个确定的定级对象（数据集），通过敏感数据识别、重要数据识别等技术手段识别与级别紧密相关的关键数据，并根据预先设置的定级策略，来确定定级对象的级别。未来几年，敏感数据扫描、重要数据识别等数据分类分级自动化技术与工具，将会与数据资产安全管理结合在一起，成为数据流通共享交易的基础性支撑平台。

构建基于DSMM的数据安全治理体系

贵州大数据安全工程研究中心副主任 刘东昊

数据安全应该是一个生态圈的安全，而不是单一组织的个体安全。当前，数据作为数字经济发展的重要生产要素。数据要素的流通交易，推动了数字经济的发展，但也面临着严峻的数据安全风险。在数据要素流通交易的动态过程中，数据安全问题并不取决于某一个组织的数据安全等级，而是需要确保整个数据流动涉及的供应商、服务商、建设方、需求方等相关方构成的数据生态圈的整体安全等级，这样数据生态圈里面的组织才能具备统一的安全等级。

数据安全治理应该构建“五维一体”的数据安全治理体系。数据安全治理是组织、人员、制度、技术等多维度的体系问题，技术产品

只能解决部分数据安全问题。还应依据国家相关法律，围绕国家/地方/行业相关标准来制定对应的管理办法，同时，在整个生态圈引入第三方评估与认证，建设统一安全水位。并且持续加强组织自身的团队建设，提升人员在数据安全方面的知识结构和能力水平，构建评估、认证、培训、技术、咨询“五维一体”的数据安全治理体系。与此同时，目前 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》国家标准能够有效的支撑和解决这五个维度的问题，成为数据安全治理领域的最佳实践。

建设以数据为中心的安全保障体系

中国信息安全测评中心 陈锦 王禹 成林 杜文越

针对数据安全面临的问题，需要构建以数据为中心的动态安全防控体系，通过数据治理、安全防护措施、风险识别和审计溯源等手段重点识别和控制数据访问、应用和流转等动态过程中的安全风险。

第一、数据治理。通过大数据治理实现数据分类分级、数据溯源，能够从全域的角度“看得见、看得清”所有的数据，包括数据存储、使用流转情况和对应的数据安全策略。掌握数据流动情况，包括表与表之间的流动、系统之间的流动、部门之间的流动、单位之间的流动等等；第二、部署安全防护措施。在大数据基础设施、数据挖掘分析和共享交易等方面采取安全防护措施，保障数据安全；第三、主动识别和控制风险。通过收集基础设施、用户操作、数据流转等方面的日志数据，重点识别用户对数据的异常操作风险和数据的异常流动风险；

第四、安全审计与溯源分析。通过细粒度的数据行为审计与溯源能力建设，形成事后可审计、可溯源、可追责的威慑体系。

（来源：中国信息安全）

全球数据安全：认知、政策与实践

中国现代国际关系研究院、上海国际问题研究院 李艳 章时雨等

数据安全问题复杂，涉及主体多元，领域广泛，包括国家、企业乃至个人的各方均是数据安全维护的主要实践者，虽然各有专长或专注领域，但彼此之间又有着紧密关联，共同构成不断发展的数据安全治理生态。首先，是国家层面“三条主线”。随着数据安全重要性日益凸显，世界各国都在维护数据安全方面进行了诸多尝试。一是推进数据本地化措施。二是加强数据跨境流动规制。三是围绕“长臂管辖”展开较量。

其次，行业层面“重点突出”。不同行业对于数据安全类型的侧重和维护方式均有所不同，所有需要和个人交互的行业都需要保护的个人隐私数据之外，重点是对各自“核心数据”采取相应措施大幅提升数据安全能力。一是加大数据安全管理架构优化力度，不再仅仅将数据安全作为简单的技术问题，而是通过涉及优化治理层、管理层、执行层和监督层四个层面促进整个数据安全治理体系的持续优化；二是不断加强数据安全风险评估力度，通过建立专门部门或工作小组的方式，将数据安全风险评估工作常态化与机制化；三是积极采取新技术手段，通过系统升级，部署人工智能、器学习、分析和其他形式的安全自动化技术，强化数据安全态势感知；四是加大人员数据安全能

力培训，通过打造针对技术、自动化与安全专业人才团队建设，维护和减少系统内部漏洞以避免外部恶意攻击；规范数据处理流程 ，对于企业内部人员进行数据安全培训与道德培训以降低内部无意识泄露的风险。

最后，国际层面“积极探索”。各国数据在跨境流动中，不断地通过机制对接，寻找流动与安全的平衡点。在此过程中，基于流动背景下的数据安全理念不断扩散，相应数据安全规则也在逐渐成形。虽然目前阶段各国囿于利益、价值观等方面的较大差异，短期内在联合国或 WTO 等多边机制下很难形成各方接受的单一数据流动规则，更遑论安全规则，但各主要国家都在探索可能的路径。

（来源：信息安全与通信保密杂志社）

数据安全风险评估应具备时代特性

中国信息安全测评中心 宋璟 邸丽清 杨光 都婧

在新时代背景下，数据安全风险评估也应具备时代特性。数据安全风险评估的发展一定是以《数据安全法》为根本出发点，以网络安全风险评估的理论框架为准绳，且风险评估的内容和指标将围绕数据为核心对象，以发现数据安全风险为主要目的。

数据安全风险评估核心内容包括：1. 数据识别安全评估 2. 数据安全法律遵从性评估 3. 数据处理安全评估 4. 数据环境安全评估 5. 重要数据出境安全评估。

目前，数据安全风险评估相关标准体系存在空缺，需尽快建立完善提供依据，数据资产识别和分类分级存在难度，急需行业主管部门

及企业自身统筹解决，数据安全风险评估的健康生态尚未建立，需各方协作助力生态建设。

（来源：中国信息安全）

从《数据安全法》视角探讨重要数据保护

北京邮电大学互联网治理与法律研究中心 谢永江

为了加强重要数据的保护，《数据安全法》在国家数据安全制度构建方面，除了规定建立数据分类分级保护制度，数据安全风险评估、报告、信息共享、监测预警机制，数据安全应急处置机制等基本制度外，还针对重要数据规定了重要数据目录制定、数据安全审查和数据出口管制等制度。

在数据处理者的数据安全保护义务方面，《数据安全法》除了规定建立健全全流程数据安全管理制度、组织开展数据安全教育培训、采取相应的技术措施和其他必要措施、风险监测、采取补救措施、数据安全事件报告等一般数据安全保护义务外，还特别针对重要数据规定了设置数据安全负责人和管理机构、风险评估和报告、出境安全评估等义务。

对此，应当坚持总体国家安全观，建立健全相关数据安全治理体系。为贯彻实施好《数据安全法》，建议重点做好以下几方面工作：

第一，抓紧出台行业领域的重要数据目录。第二，建立健全全流程数据安全管理制度，明确数据安全负责人和管理机构。第三，定期

开展风险检测评估，制作风险评估报告。第四，做好数据出境安全管理。第五，组织开展数据安全教育培训，提高数据安全意识。

（来源：中国教育网络）

《数字安全观察》版块

每周动态/政策解读/行业洞察/技术前瞻/事件分析

策略建议/国际智库精编/信创专刊/数据安全专刊/国防专刊

总编辑：杜跃进

执行编辑：韩李云 张义荣

编委会：360 天枢智库编委会

排版校对：唐会芳 韩露荻

如有反馈 邮件请至 dipperresearch@360.cn