教职工政治学习参考资料

（2024 年第 5 期）

苏州大学党委宣传部编

2024 年 5 月 27 日

教职工政治学习参考资料

（2024 年第 5 期）

苏州大学党委宣传部编　　2024 年 5 月 27 日

● 学习内容

网络安全专题学习

● 参考资料

全国两会网络安全相关提案学习

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

摘要

“没有网络安全就没有国家安全”，随着互联网科技、经济社会、政治时局等多领域不断发展与变革，网络安全问题日趋严峻。

2024年全国两会上，网络安全仍是备受关注的话题，诸多全国人大代表、政协委员以及各行各业的专家、学者、企业大咖均对网络安全领域相关内容提出多项提案。其中包括AI安全、云安全、人工智能、数据安全、网络安全体系建设、个人信息安全等方面。

周　鸿　祎

全国政协委员、360 集团创始人兼董事长

PART　01

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案一： 鼓励兼具“安全和 AI”能力的企业解决通用大模型安全问题

1、建议国家更加重视通用大模型安全问题，给予兼具“安全和 AI”能力的企业专项扶持政策，更好发挥其解决通用大模型安全问题的重要作用。

通用大模型深刻影响经济社会的方方面面，安全问题至关重要，而目前国内的大模型安全问题不容乐观。一方面，国内大模型企业不熟悉内容安全、数据安全、科技伦理、网络安全等人工智能带来的安全挑战；另一方面，大部分安全公司又很少真正有能力深入大模型研究，上述两方面原因导致国内大模型安全领域成为整个产业链的薄弱环节。为此建议国家有关部门采用揭榜挂帅等方式，鼓励并扶持兼具“安全和 AI”能力的企业，给予专项扶持政策，支持企业担起大模型安全重担，聚焦攻坚，为解决通用大模型安全问题提供坚实保障。

提案一： 鼓励兼具“安全和 AI”能力的企业解决通用大模型安全问题

2、建议国家研究制定保障通用大模型安全的标准体系，推动通用大模型开展安全评测、接入安全服务，降低通用大模型安全风险。

现阶段，将安全模块作为大模型外挂的做法已不可行，安全需要贯穿通用大模型的整个构建过程，确保安全措施在系统的整个生命周期中得到充分考虑和实施。

建议国家在内容安全、数据安全、科技伦理、网络安全等细分领域，牵头研究制定安全检测标准，在规范的安全标准体系下，推动通用大模型的安全评测工作，通过接入安全服务来保障大模型的安全。

3、鼓励政府、央国企与兼具“安全和 AI”能力的企业在大模型安全领域展开深入合作。

政府、央国企对通用大模型的应用，具有更高的安全标准，不仅关涉商业安全，更关涉国家安全。

建议政府和央国企加强与兼具“安全和 AI”能力企业的合作，尤其针对被美制裁的企业，放宽与此类企业的市场准入条件，在政策和招投标条件上，给予更多合作机会，发挥此类企业在人工智能安全领域的优势作用，为国家安全贡献力量。

提案二：全面建设安全云、推广数字安全云化服务

1、统筹建设数字安全公共服务基础设施，集中数字安全能力。

建议国家发改委等相关部委牵头指导，建设数据安全、防国家级攻击、人工智能安全、数字城市安全等一系列以提供云化安全服务为目标的“安全云”基础设施。

2、改变重建设轻效果的思路，鼓励各单位购买数字安全云化服务，作为传统网络安全建设的升级路径。

建议财政部等相关部门明确指导“数字安全云服务”的可列支科目。建议相关部委研究出台配套标准和指导意见。

3、鼓励网络安全企业积极转型，以安全即服务的方式来为国家整体数字安全水平提升做出贡献，尤其是鼓励具备核心技术的被美制裁的龙头企业发挥更大作用。

建议财政部、国资委在招标采购相关的法律法规及相关政策流程中给予一定力度支持。

提案三：深化人工智能多场景应用，支持大模型向垂直化、产业化方向发展

1、场景很重要，大模型在垂直领域大有可为，建议政府、央国企率先提供更多应用场景，聚焦“小切口，大纵深”，推动大模型垂直化、产业化落地。企业用大模型不能冒进，而是要用 AI 逐步改造业务，循序渐进，积小胜为大胜。

在实践中要拆分场景具体分析，在业务流程上找准切入点，选择与大模型成熟能力匹配的业务环节切入，切入点虽小，但纵深推进，对业务影响很大，改造收效更大。

近期，国资委召开中央企业人工智能专题推进会，10 家央企率先倡议社会开放应用场景，建议政府和央国企持续提供更多应用场景，为发展垂直化、小型化、低成本的大模型开放更多“小切口、大纵深”的落地机会，助力百行千业数字化转型，实现数转智改。

提案三：深化人工智能多场景应用，支持大模型向垂直化、产业化方向发展

2、知识很重要，基于“暗知识”的垂直大模型能更好解决企业问题。

建议鼓励企业在定制 AI 前，做好知识管理，将企业大数据平台升级为企业知识平台。

大模型的数据、知识只是人类知识的冰山一角，企业还有大量的〝暗知识〞，如战略规划、产品设计图等企业具有的独特知识，只存在于特定企业中，在互联上难以找到。

建议鼓励企业构建知识平台，将〝暗知识〞汇总起来，打造企业专属知识库，做好管理，在此基础上，通过垂直训练，深入企业级场景，满足企业需求。

提案三：深化人工智能多场景应用，支持大模型向垂直化、产业化方向发展

3、业务融合很重要，建议鼓励和引导企业将大模型与数字化业务系统深度结合，同业务流程相结合，充分发挥大模型价值。

大模型像发动机，不是用来秀的，而是要与业务相结合，特别是传统制造业，大模型是推动数转智改的利器。

大模型与业务场景的融合，关键是智能体应用与企业数字化系统的连接打通。企业层面，通过打通组织、人员、业务、流程，构建业务协作平台，促进与大模型的全面融合。

国家层面，鼓励企业拿出一至两个业务场景与大模型融合，创造大量可落地推广的与业务紧密融合的大模型，推动这些大模型与数字化系统融为一体，这将对中国的产业数字化、新型工业化产生巨大作用，本质上成为新质生产力的重要部分。

杨　　杰

全国政协常委，中国移动党组书记、董事长

PART　02

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：全面推进“AI+”行动

在国家层面推动“AI+”行动，强化顶层设计和整体规划，统筹发展和安全，明确发展目标、主攻方向和关键任务，构建技术、服务和应用齐头并进、蓬勃发展的新局面，充分发挥人工智能在推动科技跨越发展、产业优化升级、生产力整体跃升方面的巨大潜能，为强国建设、民族复兴伟业提供有力支撑。具体建议如下。

1、统筹推进计算智能、感知智能、认知智能、运动智能的协同发展，夯实“AI+”发展根基。

目前，以逻辑运算分析为代表的计算智能、以感官信息交互为代表的感知智能、以人类思维模拟为代表的认知智能、以动作协调和复杂任务完成为代表的运动智能，正在成为全球AI创新突破的前沿方向。

杨杰认为，要强化〝四类智能〞的有机融合与系统创新，加快前瞻性基础研究、引领性原创成果的重大突破，促进AI具备更强大的认知力、判断力、创造力，为形成新质生产力注入强劲动能。

2、加快推动人工智能惠及千家万户、赋能千行百业，打造“AI+”产业高地。

当前，新型工业化正在成为新质生产力形成的主阵地，AI等战略性新兴产业正在成为新质生产力形成的关键领域。杨杰建议，要以推进AI全方位、深层次融入实体经济重点领域、核心环节为方向，聚焦人民群众在教育、医疗、养老、娱乐等领域的美好生活需要，加快布局超大型智算中心、人形机器人、无人驾驶、未来生物等战略性新兴产业和未来产业新赛道，培育多模态人机交互、智能助手、工业理解计算及代码生成等一批有需求、有效益、有前景的创新应用，让人工智能不仅会〝做诗〞、更要会〝做事〞，以产业的高质量发展带动生产力的深层次变革。

提案：全面推进“AI+”行动

3、探索打造企业为主体、产学研用深度融合的创新联合体，厚植“AI+”创新沃土。

AI发展是〝大科学+大工程〞的系统创新，涉及跨学科的交叉融合，以及基础研究、技术开发、产品培育等环节的贯通。杨杰认为，要充分发挥企业科技创新主体作用，打造国有企业、民营企业、高校及科研院所等广泛参与的产学研用创新联合体和新型研发机构，整合生产、教育、科研等优势资源，协调上、中、下游创新关键环节，完善科创评价体系和激励机制，营造鼓励创新、勇于突破、包容试错的良好氛围，广泛吸引全球AI领军人才和知名学者，培育一批面向国民经济重点行业的示范标杆应用，促进创新链、产业链、资金链、人才链深度融合，加速AI技术突破和应用普及。

4、深化构建可控可信的人工智能安全防护体系，筑牢“AI+”安全屏障。。

AI的快速发展也将带来一系列安全问题和潜在风险，防范化解好AI安全风险，让AI更好服务于社会，已成为当前最紧迫的议题之一。

杨杰建议，要以AI高水平安全保障AI高质量发展，全面审视技术基础架构、数据、模型、应用的安全规范和技术策略，系统锻造AI安全能力，布局内生安全、隐私计算、区块链等新型技术，增强内容风险管理、数据隐私保护、科技伦理规范等方面的治理效能，形成一体化全程可信的〝AI+〞安全体系。

曲　　伟

全国政协委员、

中国航天科技集团有限公司第十一院研究员

PART　03

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：用密态算力打通数据安全和共享瓶颈

1、统筹建设数字安全公共服务基础设施，集中数字安全能力。

数据产业迎来爆发式成长，数据隐私保护和数据安全也成了至关重要的环节。数据在汇集、加工、融合、应用链条上，每个环节都易出现问题、数据泄露扩散成本低，基本无约束，甚至违法、违规采集和应用数据的现象大量存在，还难以溯源追责，容易引发数据产品市场价格崩塌。但与此同时，数据要素流通主要是在企业、机构“内部循环”，打破“数据孤岛”是从政府到各行业亟待解决的问题。要实现数据要素跨主体、跨机构、跨行业、跨地域的外部循环，就要打破数据持有者不愿开放、不敢开放、不会开放的现状。数据的采集和使用，隐私和安全问题不解决，数据经济就难以满足大规模、复杂应用需求，做强做大数字经济就无从谈起。密态计算、密态算力具备数据要素的整合、利用、打通梗阻的能力。密态计算就是采用加密算法，在数据建模、计算、共享、应用、销毁的过程中，实现数据可用、好用，而使相关隐私问题的数据不可见，能在保证数据安全基础上，保证数据资源大循环。

密态算力是数据基础设施，是数字中国的重要组成部分。建议组织编制密算产业发展战略和规划、建立密态计算示范中心。打造和规范密态计算产业，提升密态算力势在必行。

提案：用密态算力打通数据安全和共享瓶颈

1、统筹建设数字安全公共服务基础设施，集中数字安全能力。

密态算力是数字中国的重要组成部分。只有密态算力的可持续发展，才能打通数字基础设施大动脉、畅通数据资源大循环，才能重点支持数据要素产业化发展，助力全面数字中国建设。这也是我国提出数据“2522”国家大战略的基本要求。与此同时，密态计算、密态算力产业的发展需要国家支持政策有效落地实施。相关指导原则，“原始数据不出域、数据可用不可见”“可控可计量”等，已经在《国务院办公厅关于印发要素市场化配置综合改革试点总体方案的通知》文件中明确。要实现产业跨越式提升，才能迈入数据密态时代，这是必须解决的痛点。

曲伟建议，应进行密态算力产业顶层设计，组织编制密算产业发展战略和规划。数据要素流通需要提供风险转移和经济补偿的保障，全面提升面向后果的用户数据安全防护能力，才能协同关联产业发展。战略和规划包括配套技术标准的制定、密态计算产业链布局、网络安全保险等。同时，推进密算政策落地，建立密态计算示范中心。密态计算中心应具备可信网络、密态算力等技术，集硬件、软件、开源协议、标准规范、机制设计等。密态计算中心主要解决数据要素在多点、多地、跨区域间的可信流通和调度问题，并结合数据分级进行分级密态计算，平衡安全与成本，向社会提供一体化的数据可信流通服务。

齐　向　东

全国政协委员、全国工商联副主席、

奇安信董事长

PART　04

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案一：大力探索“AI+安全”创新应用，抢占国家安全的人工智能战略制高点

1、从供给侧看，开展联合创新，围绕攻防实战和应用场景实现“AI+安全”尖端技术研发突破。

技术创新产品需要在应用中更新迭代走向成熟，特别是人工智能大模型，数据样本越丰富，成长速度越快。

建议鼓励各行业头部企业与专业安全厂商结成创新联合体，在关键行业选取典型场景开展联合创新，共同探索大模型安全创新产品在威胁检测、漏洞挖掘、指挥研判等方面的应用，在实战中推动〝AI+安全〞进入越用越强的良性循环。

2、从需求侧看，强化政策牵引，推动“AI+安全”技术创新产品在各行业落地应用。

把AI用于网络安全防护是新事物，政企机构面对大模型安全创新产品产生疑虑是正常的。积极的政策引导是推动新事物落地应用、成长壮大的催化剂。以新能源汽车产业的发展为例，最初消费者对其安全性有疑虑，密集出台的财税补贴、〝双积分〞制度等一系列政策，逐步改变了消费者观念，拉动了新能源汽车产业的发展和技术进步。建议像支持新能源汽车的发展一样，支持〝AI+安全〞发展，设置专项基金，对研发创新〝AI+安全〞产品的企业，给予政府基金、贴息贷款或科研项目等支持；对率先取得技术突破，实现成果转化的科研机构和企业给予奖励；对积极使用相关技术、产品和服务的企业给予相应补贴，推动〝AI+安全〞相关产业取得更多科技创新成果。

3、从人才侧看，壮大“AI+安全”领域的实战型、复合型人才队伍。

随着AI技术的普及和应用领域的不断扩展，我国AI人才严重短缺。工信部数据显示，人工智能不同技术方向岗位的人才供需比均低于0.4，其中智能语音和计算机视觉的岗位人才供需比分别为0.08、0.09，相关人才极度稀缺。建议充分发挥民营企业在人才培养上的优势，鼓励成立校企共同体，在实践中培养更多大数据、人工智能、网络安全等新兴产业领军人才，为我国抢抓人工智能机遇培育人才。

提案二：做好“科技金融”大文章，促进金融高质量发展

无科技不金融。这已经成为金融界的共识，也成为科创界的现实。金融高质量发展，科技创新既是动力也是服务对象。在统筹好发展和安全两件大事、推动金融高质量发展的过程中，也要防范化解各种安全风险，为中国式现代化作出贡献。新质生产力特点是创新，关键在质优，本质是先进生产力。民营企业是科技创新的主体，也是技术推广应用和产业升级的主体，所以民营企业是发展新质生产力的主力军。在数字经济时代，新质生产力离不开数据和网络，高质量发展离不开高水平网络数据安全，只有实现高质量发展和高水平安全的良性互动，才能支撑中国式现代化行稳致远。

王　　麒

全国人大代表、四川省工商联副主席、致公党四川省委常委、四川启阳汽车集团董事长

PART　05

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：进一步保障维护网络安全

通过企业和高等学校、职业学校等教育培训机构，加强开展网络安全相关教育与培训，通过举办国家网络安全宣传周及开展常态化宣传教育，宣传网络安全理念、普及网络安全知识、推广网络安全技能，采取多种方式培养网络安全人才，促进网络安全人才交流。进一步完善构建网络安全制度体系。加强关键信息基础设施安全保障能力建设，构建能够有效应对智能化网络攻击且具有灵活敏捷、高可靠特性的网络安全弹性体系，聚焦数字经济时代人工智能、量子计算、数字孪生、元宇宙等新技术新应用带来的安全挑战，强化重点问题研究，及时研究出台相关法规制度。

组织开展《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》《关键信息基础设施安全保护条例》等法律法规的执法监督检查，将法律法规规定的安全规范措施落实到位。

加强个人信息保护和数据安全管理。研究制定数据分类分级、数据安全审查、数据安全风险评估、数据安全应急处置、数据保护认证等方面的实施细则和标准规范，为数据安全管理提供遵循和指导。持续加大对个人信息贩卖等数据相关违法犯罪活动的打击力度，维护公民权益。

张　　敏

全国人大代表，

中国电信湖北公司党委书记、总经理

PART　06

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案一：加强基层网络安全建设

基层治理既是国家治理的“最后一公里”，也是民众感知公共服务质效和温度的“神经末梢”，要重视加强基层治理数字化能力建设，保障社会安全。受安全意识不足、资金等因素制约，基层单位无法独立有效解决数字化转型中面临的网络安全威胁。维护基层网络安全是一项长期的系统工程，建议从完善网络安全法律法规和政策体系、健全网络数据监测预警和应急处置工作体系等方面多方合作发力。

一方面，基层单位在进行数字化转型过程中需树立牢固安全意识，把数字安全能力纳入规划，强化网络安全技术措施同步规划、同步建设、同步使用要求，增强基层网络安全防护能力。

另一方面，构建扎根基层、分布式、多层级的一体化安全体系，面向基层主体、垂直行业及末梢单元等，提供涵盖云、网、端、边、应用以及合规性等网络安全服务支撑。张敏建议，进一步提升基于数据的治理效能，建设立体化智能化社会治安防控体系。例如，深化公共安全视频图像建设联网，加快图像识别、物联网、大数据、人工智能等数字技术在圈层查控、单元防控、要素管控等治安防控领域中的深度融合应用。同时，深化数据共享和业务协同，建设感知决策中枢，提升公共卫生、疾病防控、食品药品安全、生产安全、城市安全、自然灾害、快递物流等重点领域的风险防控能力；加强基层多层级运行态势感知和智能分析，支撑城市公共安全防控体系关口前移、精细管理和综合决策。

提案二：筑牢关键信息基础设施安全屏障

人工智能技术对于关键信息基础设施是一把“双刃剑”，为筑牢关键信息基础设施安全屏障，张敏提出建议：

增强人工智能技术安全应用的法治保障能力。加快推进《人工智能法》的立法；完善科技伦理审查和监管制度，推动人工智能技术创新；强化网络安全普法，严格落实网络安全保护条例等制度要求。

增强关键信息基础设施智能化安全合规的监管能力。强化人工智能系统的安全性评估，加强对人工智能算法和模型的审计。严格落实网络安全等级保护的基本要求，常态化开展安全威胁的智能化监测和处置；提升智能化防护水平，构建更加智能、安全的网络环境。

增强关键信息基础设施智能化全域方案的解决能力。要加大基于人工智能的网络安全核心技术攻关，提供一体化全域防护的安全产品及服务；要构建模拟真实复杂多变的智能网络环境，加强人工智能系统的防御机制和安全漏洞实战演练；要组建网络安全国家队，加强人机协同的智能运营，构建“全局、快速、智能”的监测能力和处置水平。

增强关键信息基础设施智能化保护人才的培养能力。可发挥湖北武汉国家网络安全人才与创新基地等现有研发基地的作用，联合华中科技大学和武汉大学等重点院校，积极开发和完善人工智能、网络安全及关键信息基础设施安全保护的交叉课程，打造更好的安全教育和培训体系，培养智能化网络安全复合型人才。

李　　君

全国人大代表

PART　07

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：继续加大网络空间系列乱象治理力度

随着互联网的快速发展，社会各种乱象从线下转至线上，各种低俗、暴力、色情、赌博、以丑为美、以恶为美、为了流量没有底线和下限的行为充斥在网络空间。同时，还有一些网络平台企业为谋取暴利，通过精心设计的玩法，来引诱、误导、“算计”青少年。网游、直播、打赏、赌博、网贷环环相扣、相互依托，以青少年为敛财对象，形成了规模巨大的网络灰产。不少学生为此花光了学费、生活费甚至陷入网贷深渊；有青年花光购房款甚至挪动巨额公款参与。相关网络直播灰产利益巨大，以各种玩法包装，不深入调查难以取证，目前司法实践中缺乏认定及判例，导致这些网络灰产收益大、风险低，很多直播间仍然蠢蠢欲动，很可能死灰复燃。

除了约谈、指导等手段，必须立规立法，明确认定，彻底取缔灰产链条中的关键环节，切实维护青少年权益，为国家和民族的未来护苗。李君还建议建立国家级举报平台，强化对网络游戏、网络直播、网贷、不良游戏的监管力度。完善游戏分级制度，进一步明确不良信息的范围及对应处罚。在执法层面，公检法形成合力，持续开展网络乱象治理，提高对网络犯罪的打击能力，对网络毒瘤进行彻底根治，净化网络空间。

唐　景　丽

全国人大代表，

河北省沧州市第十六中学校长

PART　08

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：提高未成年人网络素养是关键

1、关于网络内容，建议擦亮眼睛，明辨网络信息。

网络信息非常庞杂、良莠不齐，网络软件也很多、真假难辨。在未成年人身心尚未成熟、识别能力不强的情况下，需要家长去帮助识别。

未成年学生要使用正规的网络社交软件，做好个人隐私设置，不透露自己和家人、朋友的个人信息、隐私图像，不轻易添加、关注陌生人，不盲目相信网友提供的身份信息，不接受陌生网友线下见面的邀请。

家长要切实履行家庭教育责任，遵从青少年模式行为指引，教育好孩子自觉远离网吧等不适合未成年人进入的网络服务营业场所。未经学校允许不将手机、平板电脑等带入课堂，特殊情况经允许带到学校的，要交给老师统一管理。

2、关于上网时间，建议绿色上网，拒绝网络沉迷。

3、关于用网规则，建议遵守网络规则，传播社会正能量。

每个人每天都要面对两个世界，一个是现实世界，另一个是虚拟网络世界。两个世界规则是一致的，虽然网络无限，但自由有界。

恪守道德、遵守法律是现实世界和网络世界都要遵守的基本行为规范。每个人要规范好自己在网络上的言行，文明用语、文明言行。要抵制网络不良信息和不良行为，不信谣、不传谣。

同时利用网络平台传播正能量，为国家、为社会、为他人提供帮助、建言献策，在网络领域共同营造健康向上、向善的网络文化，让网络空间充满正能量。

潘　裕　萍

全国政协委员、四川省台联会长、成都市政协文化和文史资料委员会主任

PART　09

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案：推广“隐私面单”，加强快递个人信息保护

由于快递行业在这方面管理不规范，对客户个人隐私保护意识不强，过于注重派件效率而忽视技术投入等问题，致使快递行业存在泄露公民个人信息的极大风险。快递行业泄露个人信息的途径多种多样，最常见的就是：快递面单上以“扫码返现”“领红包”等二维码广告，为各种APP、公众号引流，获取扫码者个人信息。部分快递公司存在没有个人信息安全培训记录、没有定期销毁快递运单的记录台账、没有与快递员签订保密协议等问题；多个经营网点门前堆放大量快递，且无专人看管，有人随意翻看快递面单时也不制止。去年，《快递电子运单》《通用寄递地址编码规则》国家标准正式实施，对寄递中的个人信息保护提出了明确要求。但潘裕萍发现，由于是非强制性标准，两个标准并未得到有效执行。

潘裕萍认为，“违背国家标准”本身可能不用承担法律后果，但若是因违反标准进而导致违反《中华人民共和国标准化法》，就可以导致相应的法律后果。“寄递行业提供的是一种服务产品，因此，应当在配套法律法规上加以跟进。”

潘裕萍建议，政府和行业协会积极推广隐私面单技术，同时促进电商平台与寄递企业、寄递企业与驿站之间通过信息系统对接获取联系方式，以保障包裹顺利派送以及后续服务，平衡效率与个人信息保护之间的关系。

致公党中央

中国民主党派之一

PART 10

聚焦两会 • 关注民生 • 学习思想 • 热议话题 • 方针战略 • 推动发展

提案一：提升数据安全治理能力，有效平衡数据跨境交易效率与国家安全
提案二：治理网络暴力，打造清朗网络环境

提案一

建议提升政策操作性，建立多元主体联动协调的全周期监管机制。建立数据安全分类分级评估体系，对待出境数据实施分级管理，在北京、天津、海南、福建、广东推广〝负面清单〞管理模式，明确自贸区数据跨境流通专有通道细则，完善数据出境事前监管制度，并加强与国外政府与组织的跨境监管合作。

提案二

建议加大惩治力度，完善相关法律中的反网络暴力条款，并就预防和惩处网络暴力等作出具体化、明确化、体系化的规定。致公党中央在提案中列举了〝五难〞：查证难、预判难、投诉难、维权难、惩治难。网络虽然是虚拟的，但网络暴力给人造成的伤害却是真实的。然而，〝五难〞的普遍存在使不少遭受网暴的受害者〝知难而退〞，甚至让施加网暴者更有恃无恐。建议统筹健全刑法、行政法、民法及其相应的诉讼法中〝反网络暴力〞法律条款，并提供了两种方案：一方面，在侮辱、诽谤罪中增加〝情节特别严重〞的量刑档次，提高法律威慑力；另一方面，将网络侮辱、诽谤犯罪作为公诉犯罪，借助公权力帮助受害人及时维权。

感谢观看

深入贯彻全国两会精神

内容来源：公众号“网安头条”、“网信鄂尔多斯”

《个人信息保护法》案例及分析

一、《个人信息保护法》背景介绍

随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。

党中央高度重视网络空间法治建设，对个人信息保护立法工作作出部署。习近平总书记多次强调，要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益，对加强个人信息保护工作提出明确要求。《中华人民共和国个人信息保护法》（“个保法”）由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于2021年8月20日通过，自2021年11月1日起施行。

而自2021年1月1日起实施的《中华人民共和国民法典》（“民法典”）也在第四编人格权第六章专章对“隐私权和个人信息保护”进行了规定，其中第一千零三十四条规定：“自然人的个人信息受法律保护”。

二、个人信息安全的意义

从《网络安全法》的施行，到《民法典》的编纂出台，再到《数据安全法》的出台，在数字经济发展和法治建设进程中，我国个人信息保护法律制度逐步建立并不断发展完善。制定个人信息保护法，是进一步加强个人信息保护法制保障的客观要求，是维护网络空间良好生态的现实需要，是促进数字经济健康发展的重要举措。

《个人信息保护法》是及时回应广大人民群众的呼声和期待，落实党中央部署要求而制定的个人信息保护方面的专门法律，其制定和实施，对于织密个人信息保护的法治之网，将人民群众个人信息权益实现好、维护好、发展好，具有重要意义。

三、个人信息保护民事司法案例数据统计分析

那么《中华人民共和国个人信息保护法》（“个保法”）实施两年以来，个人信息保护司法运行情况如何？有多少案例，如何分布，有何特点？为此，大成（成都）律师事务所进行了案例检索和评析，检索式如下：

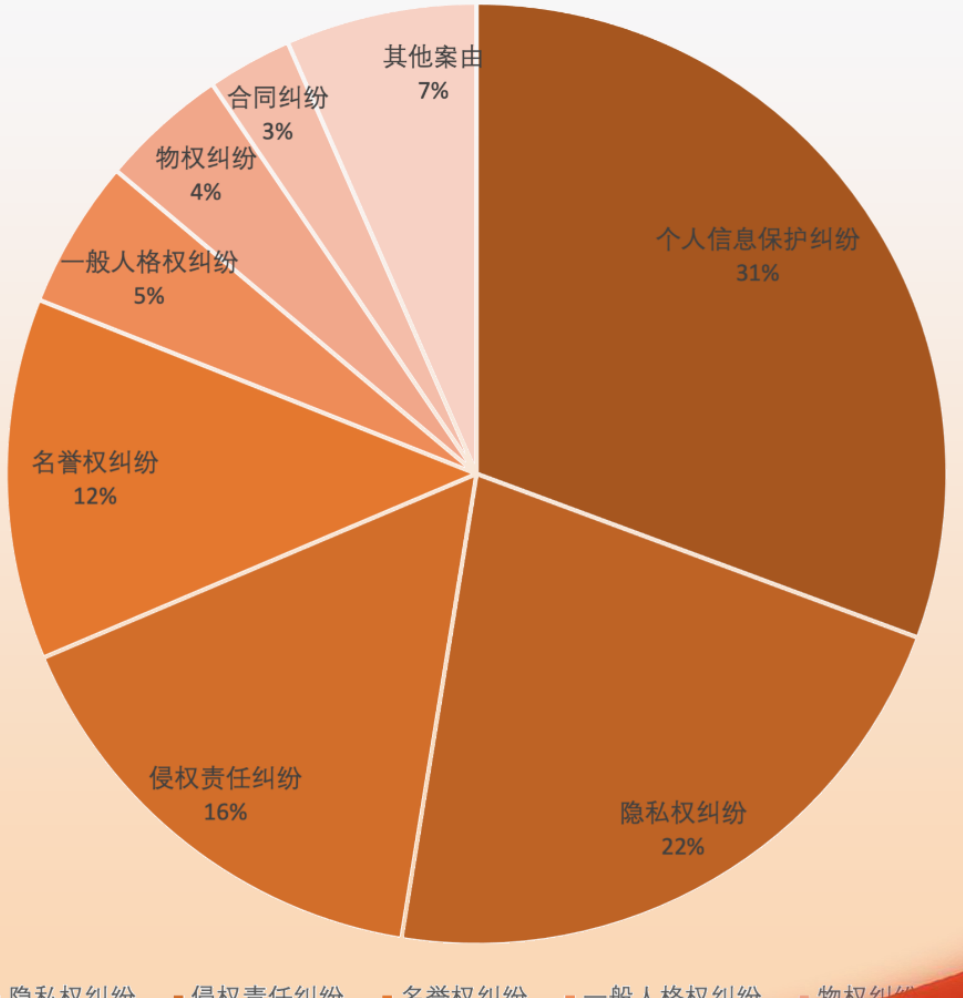
裁判日期：2021年11月1日至2023年10月23日，引用法条：中华人民共和国个人信息保护法｜中华人民共和国民法典第一千零三十四条，案由：民事。

通过以上检索式，共检索出民事一审、二审案件共150件，剔除无关案例（如错误引用）后共有案例137件。需要说明的是，由于检索式的限制，叠加司法案例公开渐少等因素，我们检索得到的案例数量将大大低于实际案例。

三、个人信息保护民事司法案例数据统计分析

（一）民事案由数据统计分析

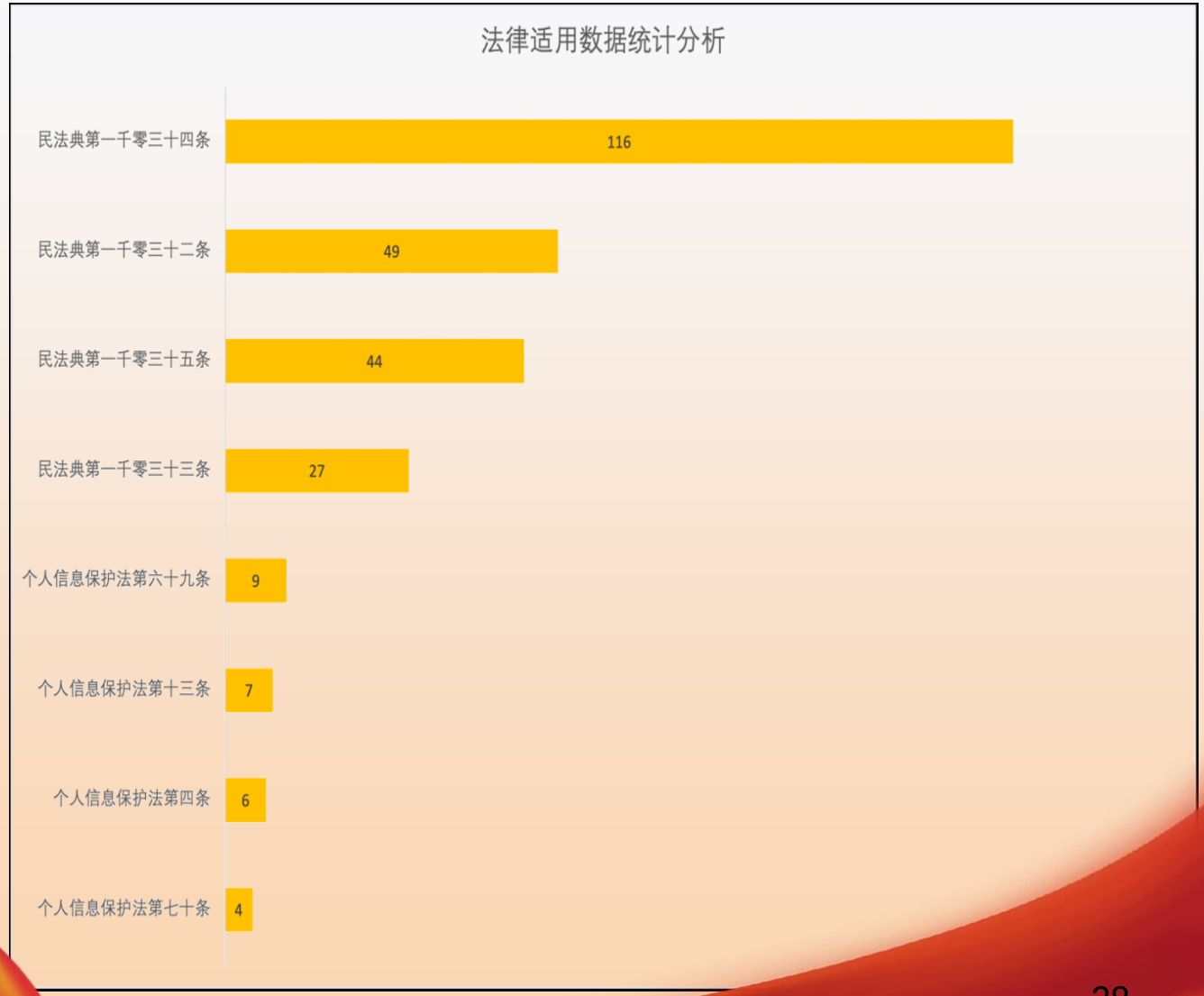
在检索的137份裁判文书中，个人信息保护纠纷案件42件，占案件总数的31%；隐私权纠纷案件30件，占案件总数的22%；侵权责任纠纷案件22件，占案件总数的16%，其中网络侵权责任纠纷案件12件，占案件总数的9%；名誉权纠纷案件17件，占案件总数的12%。需要说明的是，部分案件存在案由并列的情形，如个人信息保护纠纷与隐私权纠纷及或名誉权纠纷的并列，为了便于统计，前述情形均统计为个人信息保护纠纷。



三、个人信息保护民事司法案例数据统计分析

（二）法律适用数据统计分析

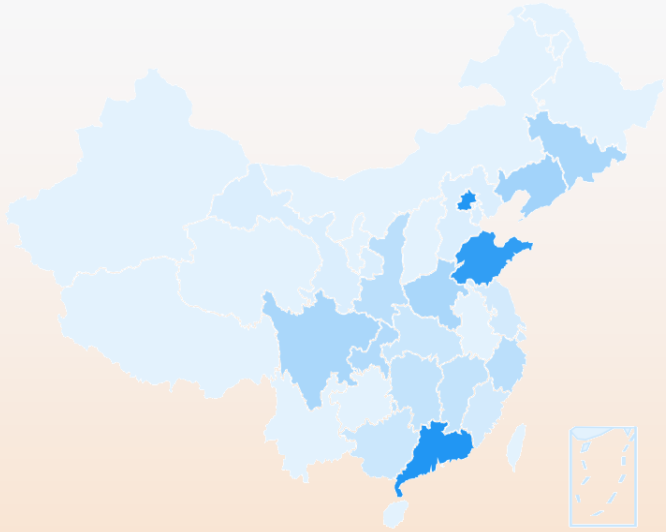
在检索的137份裁判文书中，法律适用主要集中在民法典第四编第六章：隐私权和个人信息保护。其中适用民法典第一千零三十四条【个人信息保护】的案件共116件，适用第一千零三十二条【侵害隐私权的行为】的案件共49件，适用第一千零三十五条【个人信息处理的原则】的案件共44件。相较于民法典而言，适用个保法的案例较少，适用法条也主要集中在第六十九条【过错推定及损失赔偿】、第十三条【个人信息处理条件】、第四条【个人信息的定义】。

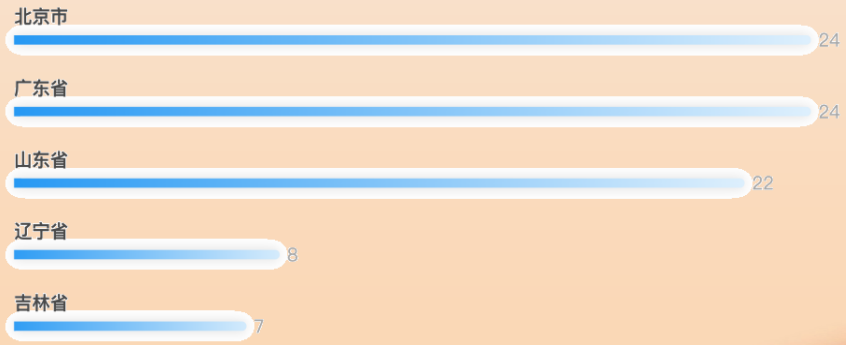


三、个人信息保护民事司法案例数据统计分析

（三）分布地区数据统计分析

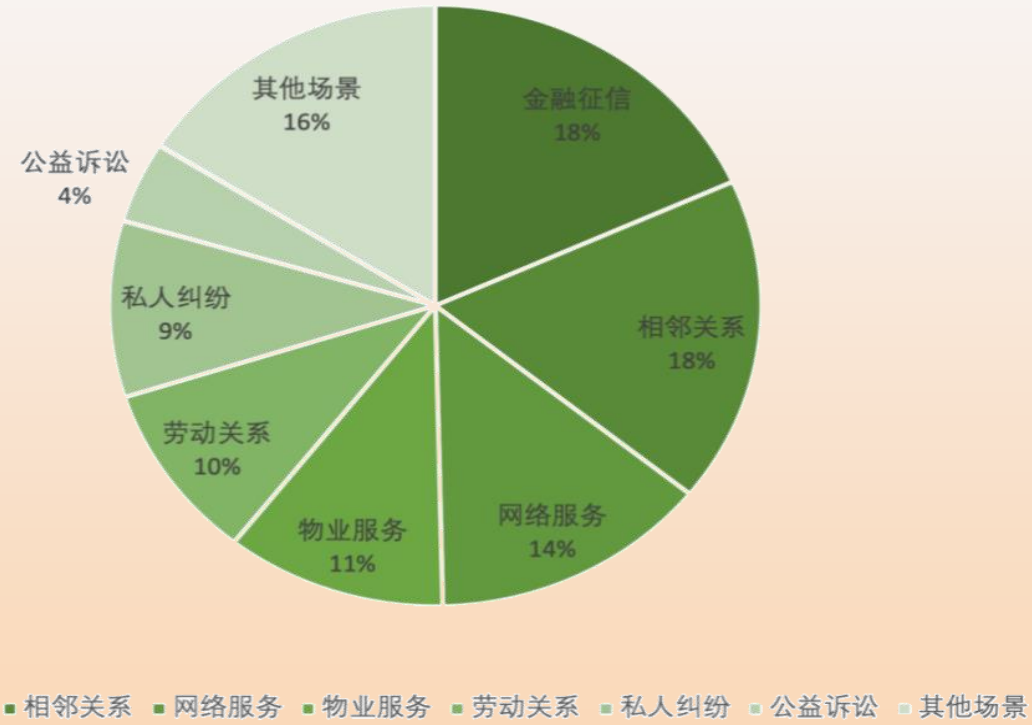
从分布地区来看，当前案例主要集中在北京市、广东省和山东省，占比分别为17.5%、17.5%和16%，累计案件占比51%。当然，如前文所述，由于近年公布的裁判文书逐渐减少，实际情况或许与该数据存在出入。





三、个人信息保护民事司法案例数据统计分析

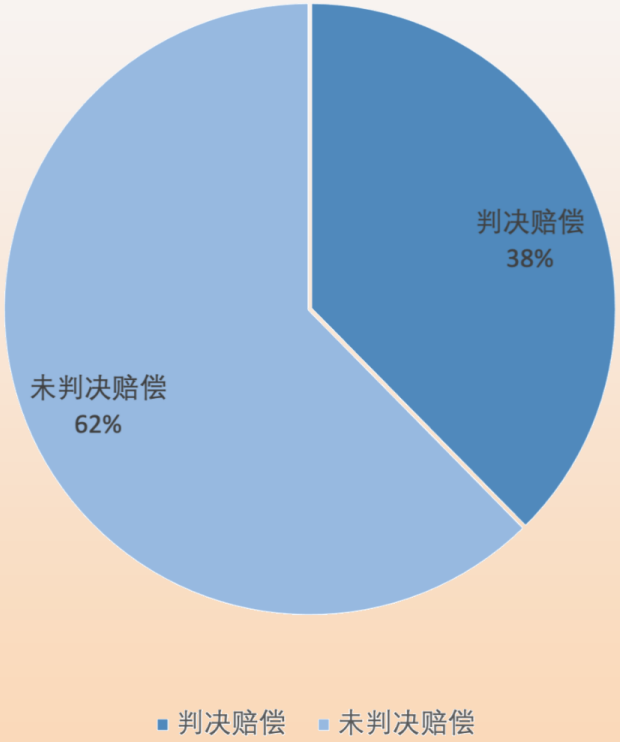
（四）侵权场景数据统计分析



个人信息侵权场景具有多样性和复杂性的特点，包括金融、物业、网络、劳动等多个领域，以及与家庭、社区和政府等各种关系。最终将检索案例中的个人信息侵权场景分为以下8类，分别为：网络服务、物业服务、相邻关系、金融征信、私人纠纷、劳动关系、公益诉讼、其他场景。其中发生在金融征信及相邻关系场景中的个人信息侵权案例在检索案例中占比最多，各占比18%，网络服务场景次之，占比14%。上述比例也反映了在数字化趋势日益发展的现代社会，侵犯个人信息的方式更加多样，且个人信息也更容易受到侵害。

三、个人信息保护民事司法案例数据统计分析

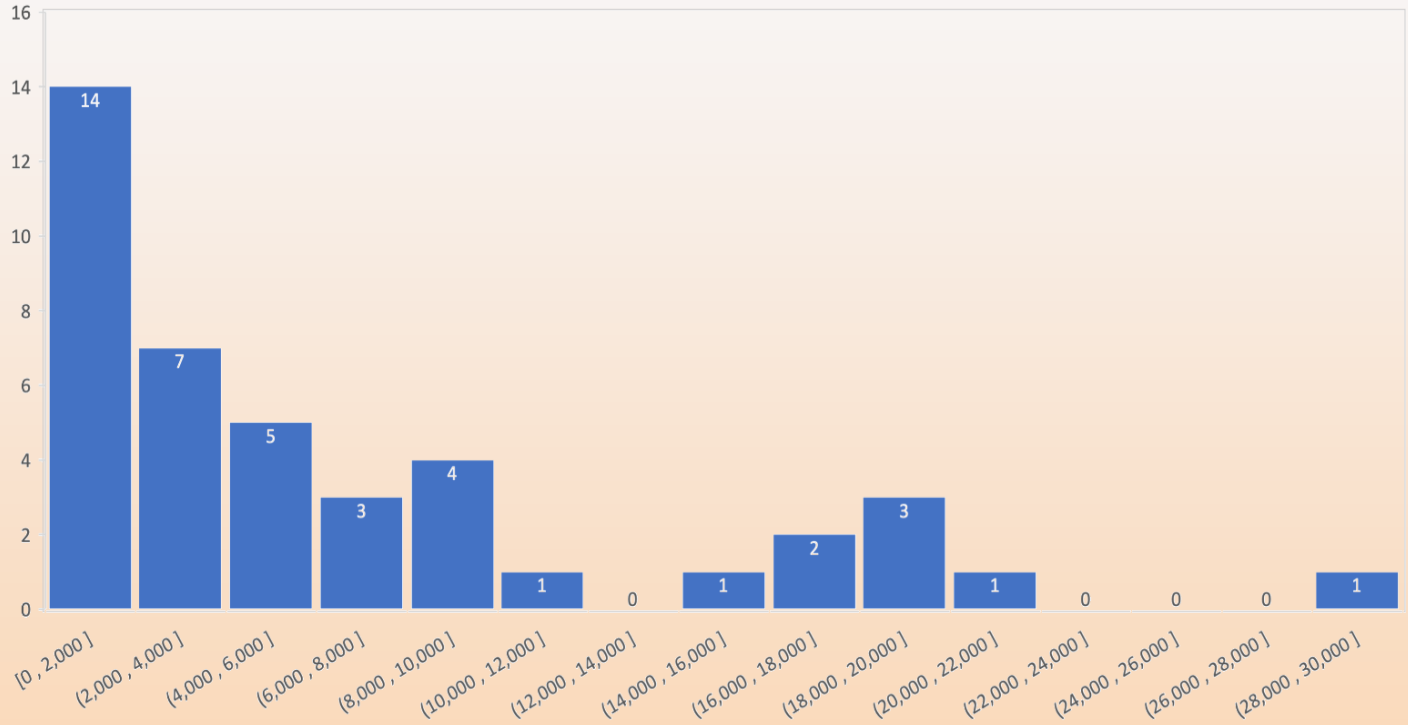
（五）赔偿情况数据统计分析



在判决确认侵权的101起案件中，判决赔偿的案件比例仅占38%。未予支持赔偿请求的原因主要是：法院认为原告关于损失赔偿/精神抚慰金的主张缺乏事实和法律依据；法院认为被告的侵权行为结合侵权时间、影响范围、过错程度等因素，不足以对原告造成（精神）损伤等，即主要基于证据不足的原因，法院对于大多数侵权案件的赔偿请求不予支持。

三、个人信息保护民事司法案例数据统计分析

（五）赔偿情况数据统计分析



个人信息侵权赔偿金额主要集中在10000元以下，其中2000元以下（包括2000元）占比最大，其中也不乏0.1元、1元等意义大于实质的“争口气”式主张被法院认可。而判决赔偿数额较高的案件普遍具有以下特点：个人生活遭受侵扰（频繁遭受电话骚扰、上门骚扰）、社会评价明显降低（附他人个人信息发布淫秽色情或其他社会禁忌性内容）、个人重大事项严重影响（报考志愿被篡改、无法正常缴纳社保）等。

四、个人信息保护民事司法案例典型侵权场景分析

（一）网络服务中的个人信息侵权案例分析

根据侵权行为将案件分为以下几类：

1、法律服务平台未经许可使用律师个人信息注册账户或进行展示

律师姓名、执业证号、代理案例等信息已由司法部门、人民法院公开，属于公开个人信息。个保法第二十七条确立了公开个人信息的处理规则，即个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

在检索的案例中，法院认为法律服务平台为实现自身的商业目的，针对已公开个人信息的处理行为不属于法定的合理范围，甚至存在虚构律师收费标准、通过平台成功承揽业务量等数据，构成对律师个人信息权益的侵害。另外，法院还认为某平台系专业提供法律服务的商业网站，其理应熟知个人信息保护的法律规定以及合理使用个人信息的范围，对于法律服务平台个人信息保护水平提出了更高的要求。

四、个人信息保护民事司法案例典型侵权场景分析

（一）网络服务中的个人信息侵权案例分析

2、侵害个人信息查阅、复制权

个保法第四十五条第二款规定：个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。此外，个保法在第四章专章规定“个人在个人信息处理活动中的权利”，企业如何响应个人提出的查阅、复制、更正、补充、删除等要求（DSR, Data Subject Request）将是合规的重点和难点。

关于个人信息处理者提供的个人信息查阅、复制方式，北京互联网法院认为：提供的信息形式在足以满足个人需求，且并没有为个人实现权利制造障碍的情况下，个人信息处理者可以依据其信息存储形式、存储能力，选择合理的提供信息的方式。对于特定类型的个人信息处理者是否可以按照用户的具体要求提供查阅、复制服务，是市场主体优化用户体验、加强市场竞争力的主动选择；是否应有相对统一、具体的提供方式，需要进一步的实践积累共识，形成相关标准或规范，司法不应在现阶段在个案中划定过于严苛的标准。

四、个人信息保护民事司法案例典型侵权场景分析

（二）物业服务中的个人信息侵权案例分析

在我们身边还存在一个大规模个人信息处理场景，就是物业服务。物业公司收集了大量业主的个人信息及隐私信息，但由于数据安全措施的不足，监管制约的缺乏，以及员工的不当行为，导致物业服务领域中个人信息侵权事件频发。在检索的137份裁判文书中，物业服务中的侵权案例就有15件，占比11%。通过梳理这15件侵权案例，可以按照侵权行为将其大致分为以下几类：

1、非法公开个人信息

个保法第二十五条规定：个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。但通过检索的裁判文书可以发现，很多物业公司存在非法公开业主个人信息的情况，具体表现形式为：在业主群内公开含有业主个人信息（姓名、出生日期、住址、身份证件号码、电话号码等）的起诉状、强制执行申请书；在楼道信息公示栏张贴含有业主个人信息的合同、通告；在微信公众号公开含有业主个人信息的判决书；物业公司工作人员制作的ppt中包含业主个人信息，该工作人员通过微信公开发布等。

四、个人信息保护民事司法案例典型侵权场景分析

（二）物业服务中的个人信息侵权案例分析

2、非法提供个人信息

民法典第一千零三十八条明确规定：未经自然人同意，不得向他人非法提供其个人信息。现实中也存在物业公司向其他业主提供同小区业主个人信息的情况，但司法实践中对于该行为并不完全做否定性评价。在（2021）湘0112民初7592号民事判决中，长沙市望城区人民法院就认为：案外人李某作为自然人，在与原告发生纠纷时，为维护自身利益，从被告处获取原告的个人信息，并以起诉的方式在合理范围内使用，以便于解决纠纷；被告宏德公司在合理范围内向其提供原告的身份信息，具有一定的正当性和合理性。从结果看，亦有利于通过民事诉讼的方式，正确处理其服务的业主之间的纠纷。而且原告亦未提供被告将上述材料向不特定他人予以泄露、扩散的相应证据。

当然，如果物业公司向他人提供业主个人信息的行为，后续已经影响到业主的正常生活，使业主遭受侵扰，发生物理层面以及心理层面的伤害，则该物业公司需要承担相应的侵权责任（如（2022）闽01民终5983号民事判决书）。

四、个人信息保护民事司法案例典型侵权场景分析

（二）物业服务中的个人信息侵权案例分析

3、人脸识别侵权

许多人员密集、安全防范难度较大的小区，物业公司出于业主精准识别、安全进出、智能管理的考量，采用了人脸识别功能进行门禁管理，甚至也存在不少小区将人脸识别作为出入小区的唯一验证方式。《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第十条规定：物业服务企业或者其他建筑物管理人以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式，不同意的业主或者物业使用人请求其提供其他合理验证方式的，人民法院依法予以支持。

在检索的案例中也发现确实有业主明确对人脸识别作为唯一验证方式提出异议，但由于物业公司没有妥善处理，业主诉诸法院的情况。在（2022）津01民终349号民事判决中，天津市第一中级人民法院认为，根据上述规定，物业公司关于业主已知情同意、业委会同意等抗辩均不能成立，并支持了业主关于删除其人脸信息并为其提供其他通行验证方式的诉讼请求。

上述案例也说明，物业服务公司需要加强数据保护措施、定期提供员工培训、明确隐私政策、遵循现行法律规范，以确保业主的个人信息得到妥善保护，让业主在家住得安全，睡得安心。

四、个人信息保护民事司法案例典型侵权场景分析

（三）相邻关系中的个人信息侵权案例分析

既让人意外又不出人意料的是，相邻关系中的个人信息保护案例竟多达24件，主要表现形式为安装摄像头侵犯他人个人信息及在业主群内公开他人个人信息。个保法第二十六条规定：在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。显然在住宅入户口或其他位置安装摄像头并不满足公共场所安装设备的要求，更不是维护公共安全所必需。因私人纠纷或者其他原因在业主群内公开他人信息也不属于正当理由。

1. 针对安装摄像头侵犯他人个人信息的情形，法院会结合摄像头位置，具体分析摄像头是否涉及个人信息或隐私权益侵犯。原告的诉讼请求通常为拆除相应的摄像头，在检索案例中还存在两个案例进一步主张删除相应的视频内容。

2. 针对业主群公开他人信息的情形，主要是一方未经许可将起诉状、裁判文书等资料发送至所在小区业主群，而起诉状、裁判文书未对当事人的姓名、出生日期、身份证号码等信息进行遮蔽，构成个人信息权益或隐私权的侵权。

四、个人信息保护民事司法案例典型侵权场景分析

（四）金融征信中的个人信息侵权案例分析

金融征信场景中的个人信息保护案例在整个检索案例中占比最高，达到18%，有25件案例。但仅有12件案例被认定为侵权，其中11件案例都是因为银行或者信用合作社错误报送征信信息，导致原告产生不良征信记录。但有意思的是，在案由选择上，大多数法院都选择了名誉权纠纷，认为征信信息的错误报送，导致征信系统对个人的诚信度不良记录和否定性评价，构成对名誉权的侵害。仅有2家法院以个人信息保护纠纷为案由立案审查，认为银行征信记录属于个人信息，应适用个人信息保护相关规定。

事实上，这一法律适用及案由选择争议民法典已经做出了明确规定，民法典第一千零三十条规定：民事主体与征信机构等信用信息处理者之间的关系，适用本编有关个人信息保护的规定和其他法律、行政法规的有关规定。

四、个人信息保护民事司法案例典型侵权场景分析

（五）私人纠纷中的个人信息侵权案例分析

私人之间因情感、家庭或其他纠葛也会涉及个人信息侵权问题，共检索到 12 件案例。当然业主群内公开他人个人信息本质上也属于私人纠纷，为了便于统计，将其归类至相邻关系。如果将这些案件归类至私人纠纷，可以看到私人纠纷场景下涉及个人信息侵权的案例不在少数。本类纠纷中涉及的具体情形较为丰富，如被告在诉讼中恶意使用原告地址作为本人地址，随着裁判文书的公开导致原告地址公开，从而受到侵扰。该案件侧面反映出裁判文书公开的个人信息也违背必要原则。常见的纠纷类型还有在朋友圈、抖音等社交媒体公开他人个人信息，如身份证照片、行政处罚文书等，通常情况下法院均会给与否定评价。

四、个人信息保护民事司法案例典型侵权场景分析

（六）劳动关系中的个人信息侵权案例分析

虽说是劳动关系中的侵权，但在该分类项下，发现更多案例是，在未建立劳动关系的前提下，用人单位使用他人的个人信息为其购买社保，一定程度上影响了他人的正常求职及社保缴纳。在检索的案例中甚至有6家企业在不同时间段为同一位未毕业大学生缴纳社保的情况，该社保缴纳行为将可能导致该学生无法以应届毕业生身份择业，最终该学生诉诸3家法院才完全解决其社保被错误缴纳的问题，严重影响了该学生的学习和生活，同时也带来了一定的精神困扰。

还有部分案例是用人单位未经劳动者同意，在公司微信群中公开了劳动者的个人信息（身份证号码、身份证地址、家庭地址、家庭成员手机号码等）；用人单位在劳动者离职后，将该劳动者实名注册且开通电信支付业务的手机号交由他人使用，且未协助劳动者办理手机号码关联人信息的变更。用人单位应加强对劳动者个人信息的管理和保护工作，做好入职前、工作中、离职后的个人信息全流程管理。

四、个人信息保护民事司法案例典型侵权场景分析

（七）公益诉讼中的个人信息侵权案例分析

个保法第七十条规定：个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和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。本次检索的案例中有 6 件由各地检察院提起的个人信息保护民事公益诉讼。被起诉的对象有运营商的工作人员、拥有相应权限的合作机构人员以及手机店的经营者，前述人员利用职务便利获取个人电话号码、验证码等信息，非法获利。判赔金额通常为被告非法获利金额。从检索的6 个案件来看，最高金额为 16700 元，其他多为数千元。

四、个人信息保护民事司法案例典型侵权场景分析

（八）其他场景中的个人信息侵权案例分析

除了上述七大场景外，还存在其他场景下的个人信息侵权，如利用他人个人信息修改他人报考志愿；在售楼处安装摄像头收集人脸信息进行判客；电影实景拍摄泄漏他人电话号码；冒用他人身份信息注册公司；未经他人同意，频繁向他人进行电话营销、微信推销；借用他人个人信息注册社媒账号，在他人撤回同意后仍然使用该社媒账号从事营利活动；未经他人同意，将其个人信息传输给第三方办理业务等。

这些案例分布在教育、经济、营销、文娱和社交媒体等各种领域，也反映了个人信息侵权问题的广泛性和复杂性。

五、个人信息保护法典型案例及法律解读

案例1、未依法履行个人信息保护义务

案例简介

2022年7月29日江苏常州公安机关在对常州某网络科技有限公司日常检查时，发现该公司运营一款为在校学生提供外卖配送及快递代取服务APP，采集储存大量会员姓名、手机号码等个人信息，但是该APP未对采集的公民个人信息采取相应加密、去标识化等安全技术措施，且没有制定内部管理制度和操作规程。江苏常州公安机关根据《个人信息保护法》第五十一条、第六十六条规定，对公司给予行政警告处罚并责令限期整改。

五、个人信息保护法典型案例及法律解读

案例1、未依法履行个人信息保护义务

法律解读

本案中，该公司未采取有效措施确保个人信息处理活动符合法律规定、防止未经授权的访问以及个人信息泄露、篡改、丢失，构成未依法履行个人信息保护义务，被公安机关依法给予行政处罚。违反国家有关规定，将提供服务过程中获取的公民个人信息出售或提供给他人，情节严重的，依据《刑法》第二百五十三条之一规定，以涉嫌侵犯公民个人信息罪立案查处。对于违反规定处理个人信息或者处理个人信息未履行保护义务的，尚不构成刑事处罚的，依据《个人信息保护法》第六十六条规定，以违法处理个人信息或处理个人信息未履行信息保护义务予以行政处罚。《个人信息保护法》通过全面强化行政责任效用，充分利用行政执法优势，积极主动地介入并制止尚未造成损害结果的违法行为，极大地强化了对个人信息的事前保护。该法第六十六条的规定，大幅提高了针对情节严重违法行为的罚款上限，在对单位责令改正、没收违法所得的基础上，并处5000万元以下或者上一年度营业额5%以下罚款，对直接责任主管人员和其他直接责任人员处10万元以上100万元以下罚款，同时可以对单位、个人作出限制性从业处罚，极大程度上增强法律权威性和震慑力。

来源：法青苑https://mp.weixin.qq.com/s/aPxxQTnnqJ9YjYlwjTfAvQ

五、个人信息保护法典型案例及法律解读

案例2、非法获取大量公民个人信息

案例简介

2023年2月，福建厦门公安机关接到某科技有限公司报案称，其公司信息系统被攻击导致大量用户信息泄露。经查，马某发现该公司开发的“跟单宝”系统中的交易记录等信息具有经济价值，指使杨某、陈某等人通过黑客手段入侵该系统，非法获取大量公民个人信息，并转卖至李某涛、刘某海、黄某南等人处。李某涛利用上述信息通过拨打骚扰电话、邮寄产品等方式向受害人进行精准营销。3月，厦门公安机关开展集中收网，抓获犯罪嫌疑人7名，涉案金额200余万元。此外，厦门公安机关还依法对该科技有限公司未履行网络安全保护义务行为给予行政处罚。

法律解读

各类企业和个人要贯彻落实《网络安全法》《数据安全法》《个人信息保护法》等法律法规要求，做好源头防控，切实履行主体责任，合法合规收集、储存、使用公民个人信息，采取必要管理措施和技术手段加强网络安全、数据安全和个人信息保护，防止未经授权的访问以及公民个人信息泄露、篡改、丢失。网信、公安等部门将坚决打击危害网络安全、数据安全乃至对国家安全构成威胁的违法行为。

来源：恩施人大

https://mp.weixin.qq.com/s/Ggb604PUdkNZcKdEdGgERw

五、个人信息保护法典型案例及法律解读

案例3、非法收集儿童个人信息

案例简介

某科技公司运营的某短视频App存在侵害众多不特定儿童个人信息的侵权行为，具体包括：1.未以显著、清晰的方式告知并征得儿童监护人有效明示同意的情况下，允许注册儿童账户，并收集、存储儿童网络账号、位置、联系方式，以及儿童面部识别特征、声音识别特征等个人敏感信息；2.在未再次征得儿童监护人有效明示同意的情况下，运用后台算法，向具有浏览儿童内容视频喜好的用户直接推送含有儿童个人信息的短视频；3.某短视频App未对儿童用户采取区分管理措施，默认用户点击“关注”后即可与儿童账户私信联系，并能获取其地理位置、面部特征等个人信息。

法律解读

面向儿童用户提供网络服务的互联网平台（信息处理者）在缺乏单独《儿童个人信息/隐私保护政策》和《儿童个人用户协议》，未采取合理措施通知监护人并征得监护人有效明示同意的情况下，处理儿童用户地理定位、联系方式、面部、肢体、声音等个人信息的，应认定为违法处理用户个人信息。

儿童个人信息的保护：收集儿童（未满14周岁未成年人）个人信息需①经监护人同意，②制定专门面向儿童的个人信息处理规则（《个人信息保护法》第31条、《儿童个人信息网络保护规定》第8、9条）。

来源：浙江法制

https://mp.weixin.qq.com/s/JtKgxM2ktO3yb57uGDJlXQ

五、个人信息保护法典型案例及法律解读

案例4、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

案例简介

2021年7月，张先生所在的小区物业通知，称门禁系统将改为人脸识别，要求业主办理人脸信息录入，否则无法进出小区。张先生不同意物业留存自己的人脸信息，多次沟通无果后将物业公司起诉至法院。法院审理认为，物业公司使用人脸信息应征得当事人同意，对于不同意提供人脸信息的业主应提供替代性验证方式。最终，物业公司为门禁系统增加了刷卡功能。

法律解读

《个人信息保护法》第16条：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；处理个人信息属于提供产品或者服务所必需的除外。违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，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；拒不改正的，并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。

来源：稀土高新政法 https://mp.weixin.qq.com/s/sRZP8JZC_YZJFVkb2jQqqQ

五、个人信息保护法典型案例及法律解读

案例5、个人信息非法买卖

案例简介

2023年1月，安徽宣城公安机关接群众举报，称其在一互联网借贷平台填写个人信息申请车辆贷款后，收到本地另一贷款公司的推广电话，怀疑个人信息被非法买卖。1月10日，警方抽调网安、刑侦等部门警种精干力量成立专案组。侦办期间，在安徽省公安厅网安总队的指导下，在宣城市公安局的指挥下，省、市、县三级公安机关联动，紧盯案件线索展开缜密侦查。经查，该举报群众申请贷款的平台既无借贷资质也不从事借贷业务，而是一家从事“居间助贷”的中介公司，该公司伪装成正规借贷公司在搜索引擎、网络短视频平台等发布广告，吸引有贷款需求人员填写公民个人信息后，在当事人未授权的情况下，通过代理将相关信息出售给贷款人归属地的贷款公司牟利。2023年5月，安徽宣城公安机关对该案开展集中收网，抓获犯罪嫌疑人39名，打掉涉嫌侵犯公民个人信息的“居间助贷”公司3家，涉案金额1600余万元。

法律解读

犯罪嫌疑人雷某等人合资注册的公司，既无借贷资质也不从事借贷业务，而是一家从事“居间助贷”的中介公司。为了吸引需要借贷人员的注意而事先精心设计网站，并伪装成正规借贷公司在网络社交平台上发布广告。一旦像汤先生这样的借贷需求人员在填写个人相关信息且在其本人(当事人)未授权的情况下，相关信息将被高价出售给借贷人归属地的借贷公司而非法获利，违反《个人信息保护法》。大家一定要擦亮双眼，非必要不透露个人信息，遇到类似情况要对违法犯罪分子坚决说“不”。

来源：网信恩施

五、个人信息保护法典型案例及法律解读

案例6、电信诈骗案例

案例简介

18岁女孩徐某某因为被一通电话骗走了为上学筹集的9900元学费，在报完案回家途中心脏骤停，不幸离世。经查明，此案嫌疑人攻破某省高考报名系统，通过获取徐某某个人详细信息进行诈骗。最终，法院以诈骗罪、侵犯公民个人信息等罪名对诈骗团伙七被告人分别判处无期徒刑和有期徒刑。

法律解读

个人信息泄露、电信诈骗严重侵害了人民群众的财产安全和其他合法权益，严重影响人民群众的安全感和社会和谐稳定。根据调查，本案个人信息泄露系黑客入侵数据库，并在QQ群里出售考生信息，犯罪性质恶劣，社会影响极大。根据《个人信息保护法》第十条任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

来源：网信恩施

https://mp.weixin.qq.com/s/eMDjEdlsXXAp6HEwHotlFQ

感谢观看

内容来源：公众号“大成成都办公室”

《数据安全法》案例及分析

《数据安全法》颁布背景

聚焦

近些年，因数据问题导致企业和公民的权益受到侵害的事件时有发生，结合当前数据业务发展态势，该类事件还会呈上升趋势，并未达到顶峰。这当然和数据主体(组织和个人）对于数据安全的意识在不断的提高有很大关系。另外，受利益驱使，某些组织或个人铤而走险，不当采集数据、滥用数据还是很常见的。因此，通过立法来维护数据主体的权益是非常有必要的。

2021年6月10日，《中华人民共和国数据安全法》（下文简称为《数据安全法》） 正式颁布，于2021年9月1日正式施行，作为我国数据安全领域的首部基础性法律，也是国家安全领域的一部重要法律，标志着我国以数据安全保障数据开发利用和产业发展全面进入法治化轨道。

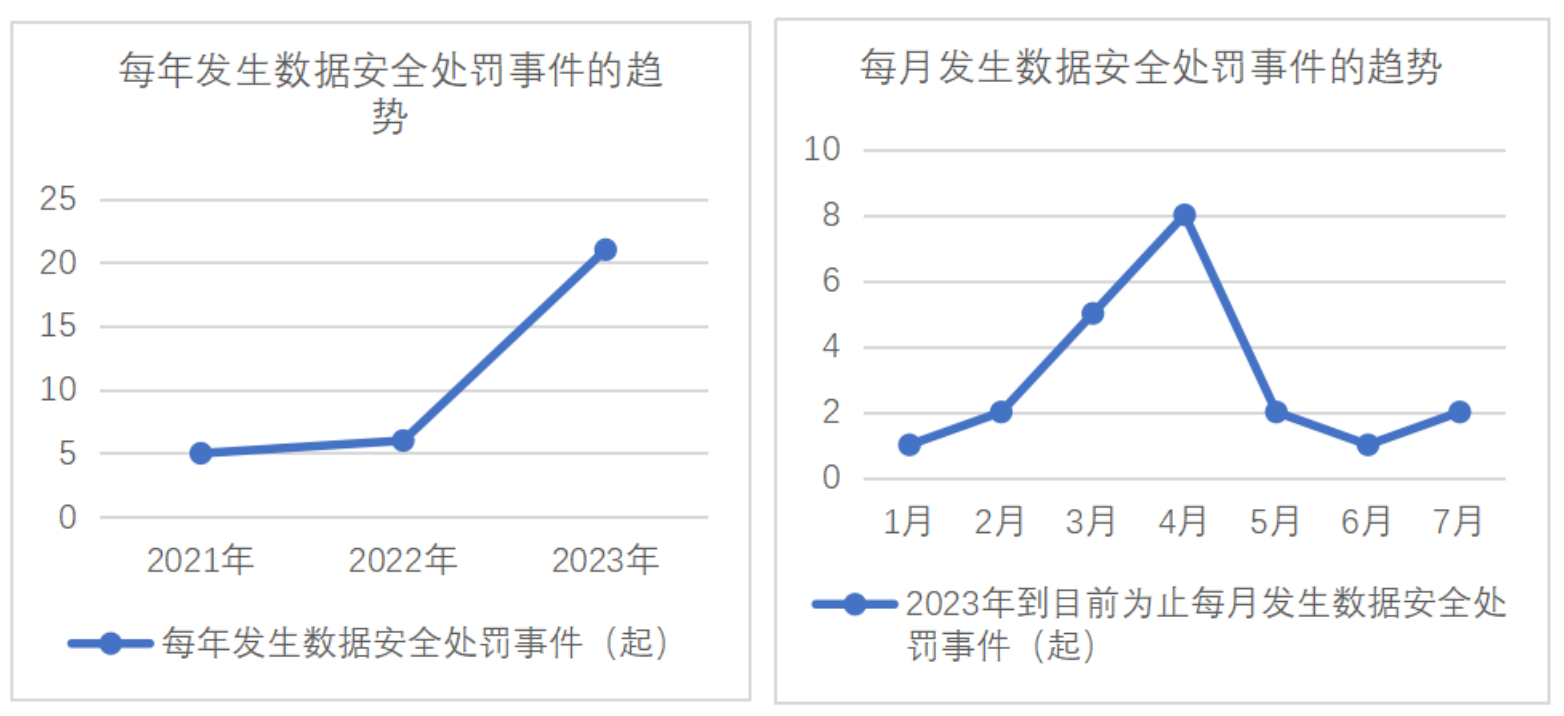
数据安全事件分析总结

聚焦

随着数字经济成为世界经济发展的新动力，推动数据量的高速增长，数据安全风险也在同步激增。同时传统的犯罪类型也借助新型技术不断形成新的变种，在侵犯数据权益的同时，对社会公共利益乃至国家安全也造成严重威胁。随着《数据安全法》的生效，不仅极大地保护了国家、社会和公民的数据安全，也表明了国家治理数据安全的决心。本文基于数据安全法实施近两年来，被公开作出行政处罚的典型案例32起，从不同维度对案例进行了分析总结。

数据安全处罚事件逐年升高，2023年呈爆发式增长

通过对近两年数据安全事件发生的时间进行汇总，2021年共发生5起，2022年共发生6起，2023年到目前为止已发生21起。相比前两年，2023年呈爆发式增长。并且2023年每个月都有处罚案例，在3月和4月分别达到5起和8起。说明随着《数据安全法》实施和相关配套体系的完善，相关部门正加大执法力度和频度。



聚焦

互联网行业是发生数据安全处罚事件的重灾区

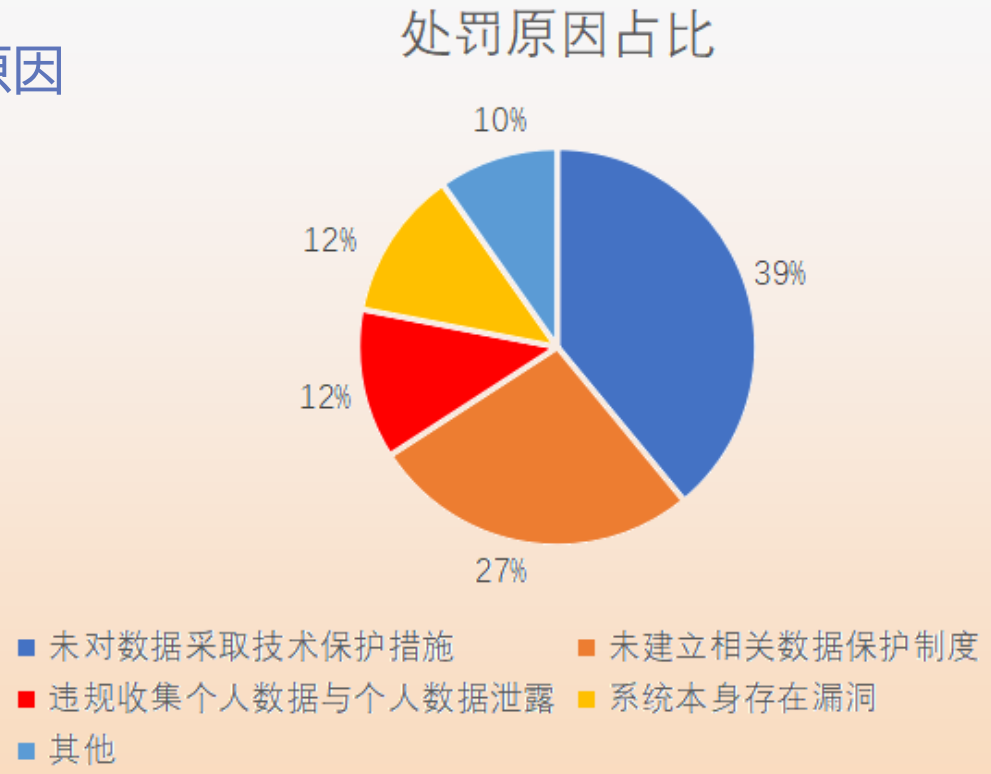
从行业分布来看数据安全处罚事件涉及互联网、医疗、金融等行业，其中互联网行业作为重灾区发生了10起数据安全处罚事件，占比32%。其中某些处罚是对多家单位的合并处罚，共包含了上百家运营主体。

数据安全事件分析总结

聚焦

未建立相应技术措施和管理制度为主要原因

通过对所有数据安全处罚事件进行归因分析，发现未对数据采取相应的技术保护措施和管理制度的占比为66%。原因是大多数企业或组织对于数据安全的认知和重视性不足，投入较少，存在侥幸心理。



涉及问题分类

可将所有违法行为和其对应的问题进总结归类为四类问题。

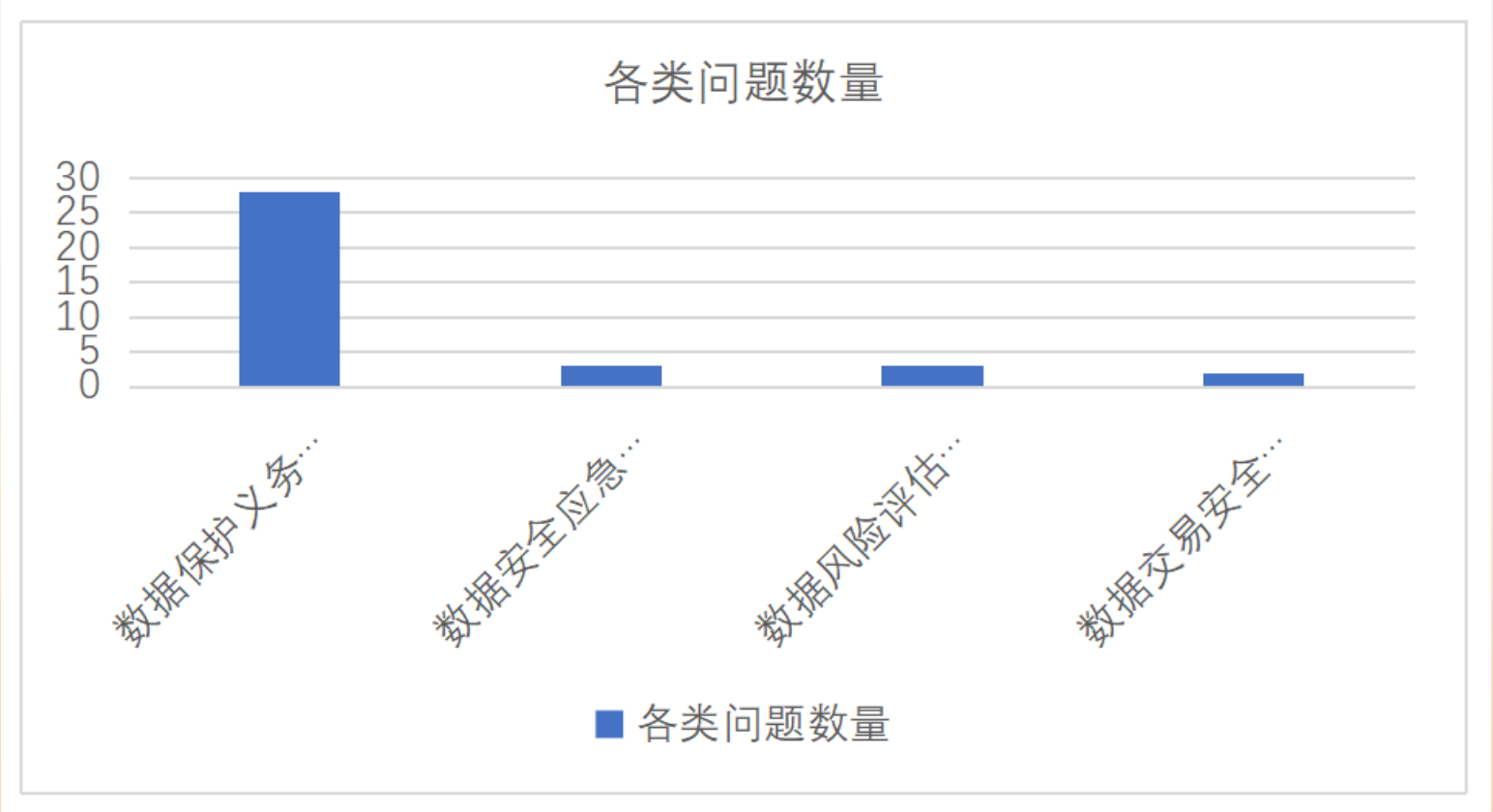
违法行为简述	对应问题
未对敏感数据采取去标识化和加密措施等技术保护措施，导致数据泄露或存在数据泄露风险。	数据安全保护技术
对已有漏洞不修复不管理，已经遭受攻击或被植入暗链、木马等。	数据安全漏洞扫描和修复
发生数据安全事件后不处置。	数据安全应急处置
数据处理者未遵守数据交易安全的规定，擅自向境外提供重要数据。	数据交易安全

数据安全事件分析总结

聚焦

涉及问题分类

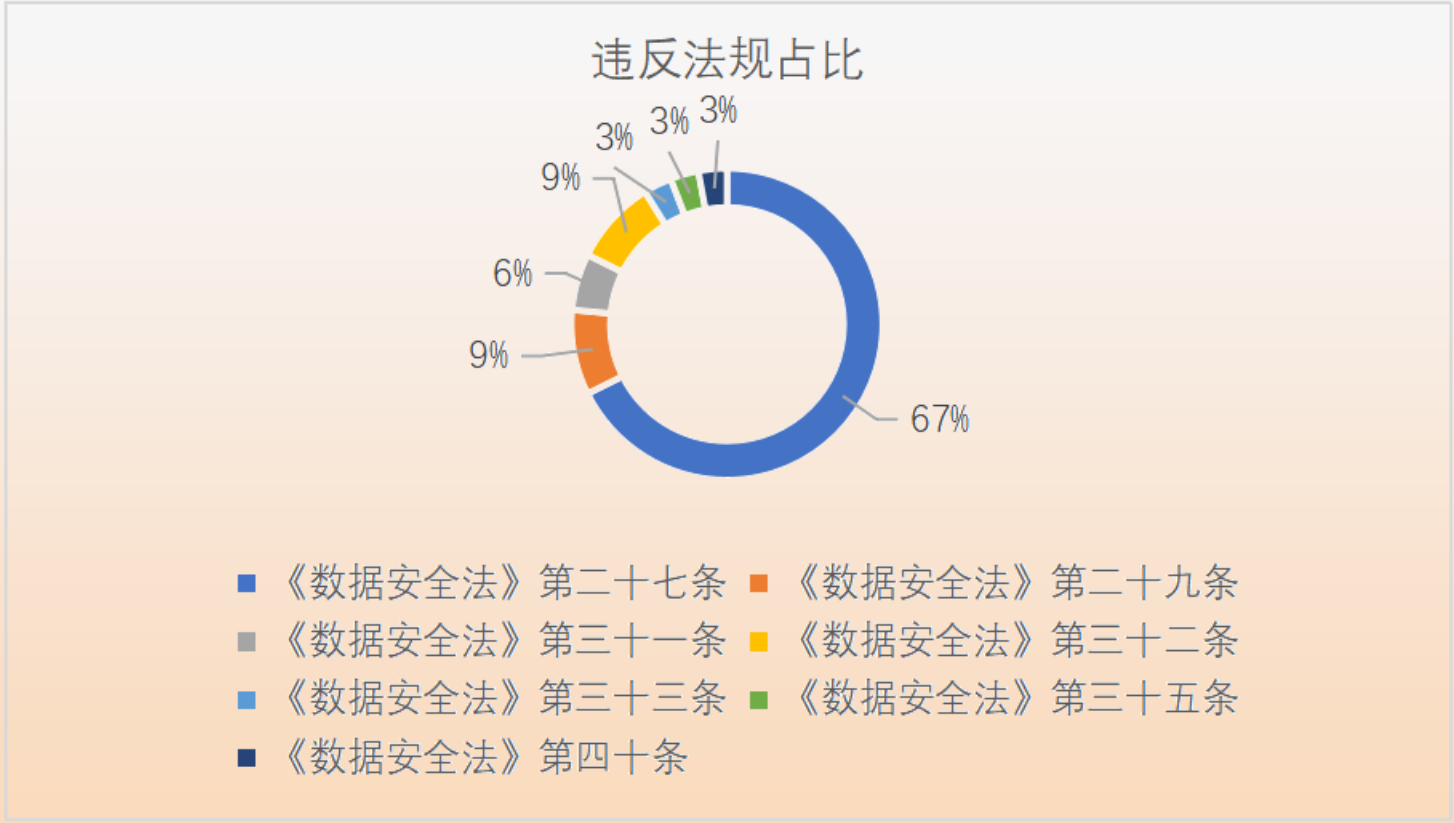
其中数据保护义务的问题多达28起，数据安全应急处置问题以及数据风险评估和监测的问题分别有3起，数据交易的安全问题2起。



数据安全事件分析总结

违反法规

通过对所有数据安全法处罚案例的总结，违反的法规条目主要有《数据安全法》第二十七条、二十九条、三十一条、三十二条、三十三条、三十五条、四十条。



数据安全事件分析总结

聚焦

违反法规	法规内容	案例数量
《数据安全法》第二十七条	开展数据处理活动应当依照法律、法规的规定，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，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。	23起
《数据安全法》第二十九条	开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。	3起
《数据安全法》第三十一条	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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。	2起

数据安全事件分析总结

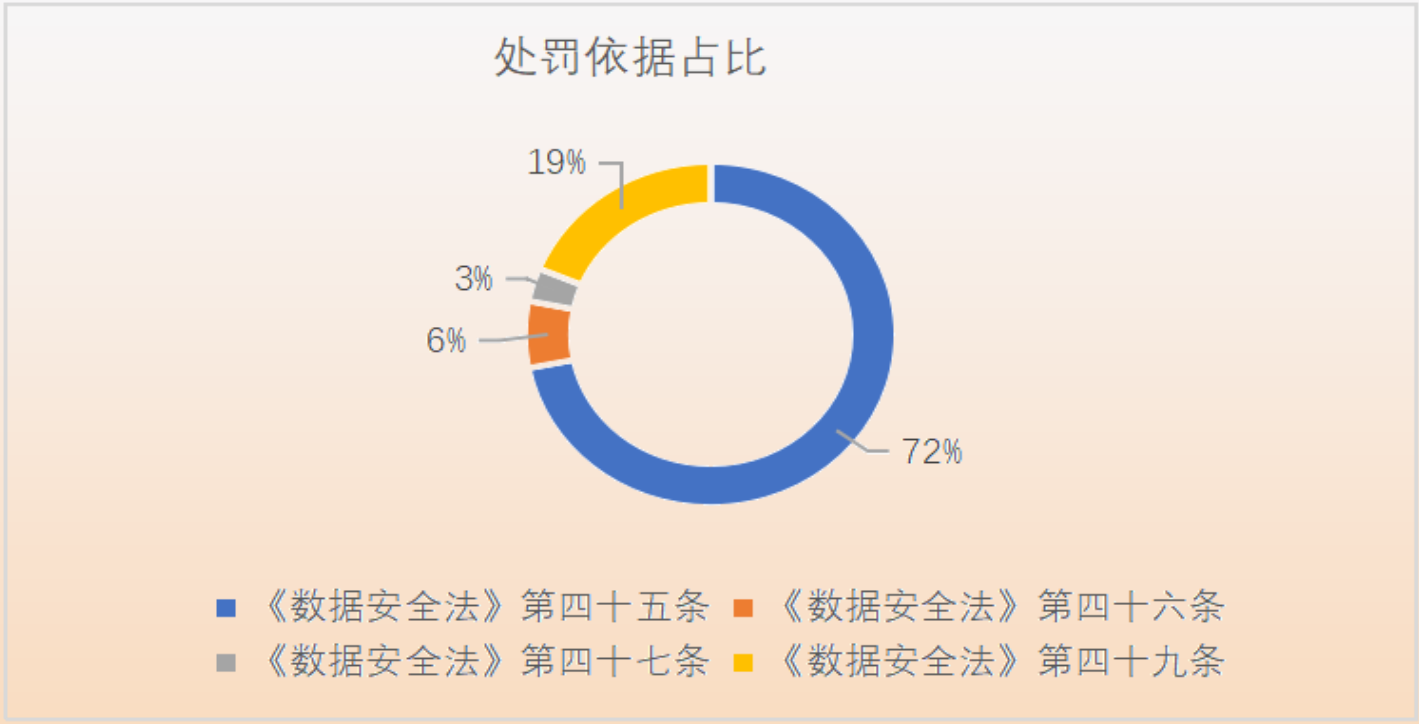
聚焦

违反法规	法规内容	案例数量
《数据安全法》第三十二条	任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。 法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。	3起
《数据安全法》第三十三条	从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。	1起
《数据安全法》第三十五条	公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。	1起
《数据安全法》第四十条	国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。	1起

聚焦

处罚依据

通过对所有数据安全法处罚案例的总结，处罚的法规条目主要有《数据安全法》第四十五条、四十六条、四十七条、四十九条。



处罚依据

处罚依据	法规内容	案例数量
《数据安全法》第四十五条	开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并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可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上二十万元以下罚款。 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，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。	23起

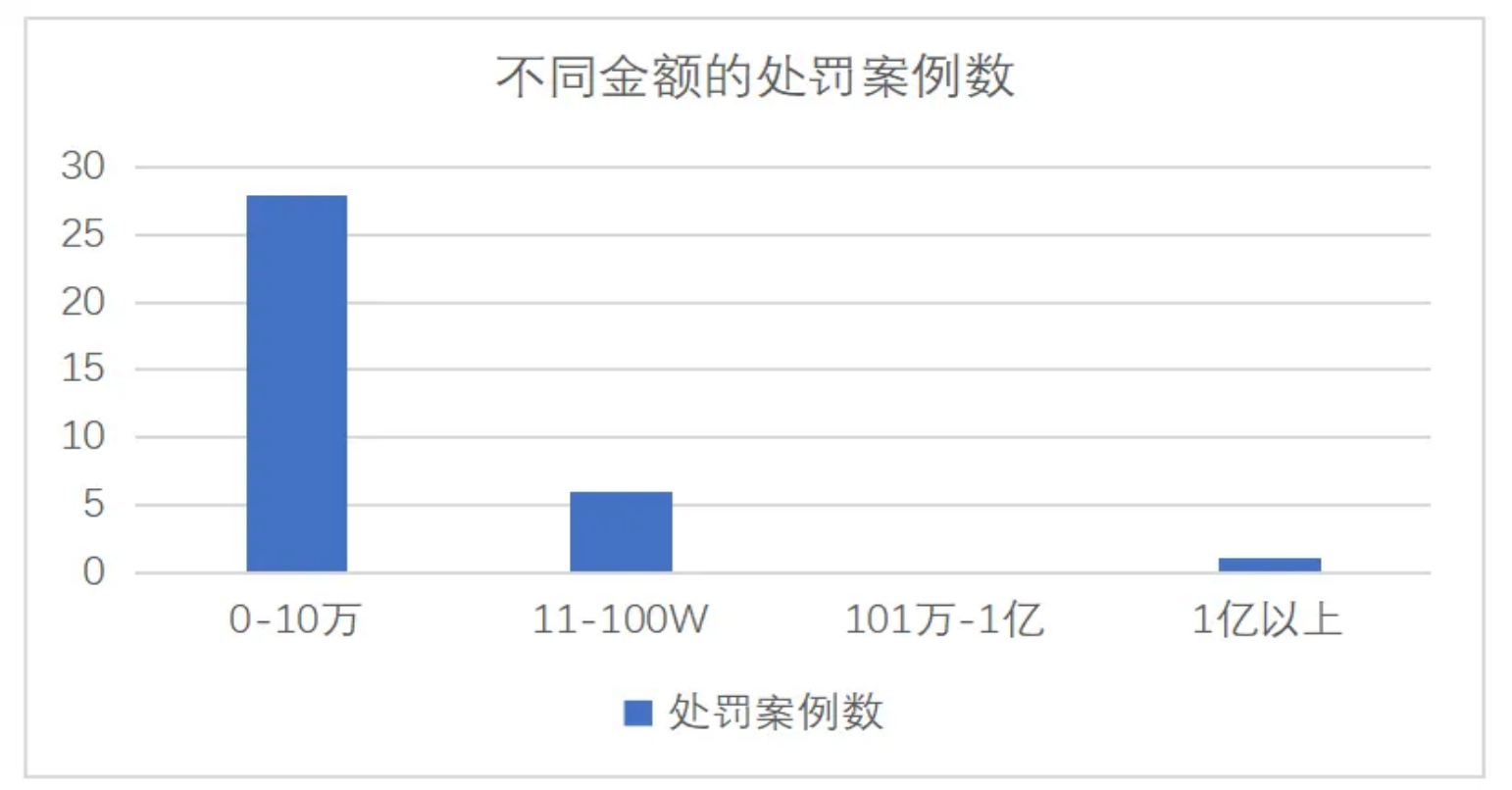
处罚依据

处罚依据	法规内容	案例数量
《数据安全法》第四十六条	违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、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。	2起
《数据安全法》第四十七条	从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、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。	1起
《数据安全法》第四十九条	国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。	6起

聚焦

对企业处罚金额最高达80.26亿元，对个人处罚最严重为刑拘

根据《数据安全法》对处罚的金额进行分析，可以发现金额跨度从几万到几十亿不等，且出现了“类案不同罚”的情况。这说明行政机关虽然是依据法律规定在法定处罚范围内作出处罚决定，但是行政机关在行使自由裁量权时遵循过罚相当原则，在全面衡量案件的综合情况的基础上决定处罚数额。



对企业处罚金额最高达80.26亿元，对个人处罚最严重为刑拘

根据处罚详情进行汇总，有21例处罚为0-10万或未披露处罚金额，占比66%，且都进行了行政处罚“给予警告，并责令限期改正”；已查明造成数据泄露或其他后果的数据安全事件罚款为10万至100万，共6例，占比19%；有1例数据安全事件对社会和国家造成极大危害，对其罚款高达80.26亿，占比3%。

其中，在上海某公司向境外出售高铁数据的事件中，由于上海某公司为境外公司搜集、提供的数据涉及铁路GSM-R敏感信号，且经国家安全机关调查，这家境外公司长期合作的客户包括某西方大国间谍情报机关、国防军事单位以及多个政府部门。所以，依据《中华人民共和国数据安全法》、《中华人民共和国刑法》、《中华人民共和国无线电管理条例》等法律法规对上海某公司的销售总监、销售及法定代表人执行逮捕。

数据安全事件分析总结

聚焦

通过以上报告分析可得，目前数据安全在我国仍面临较大的挑战，各企业和个人的数据安全意识不足，造成数据安全保护技术和管理上都有漏洞。同时，外部攻击也越来越组织化、体系化。

分析中还发现，对于不少公开的数据安全泄露事件，并没有公开处理结果。公开的这些案例中，大多数为未落实数据安全保护义务造成，虽未发生严重后果，但也给予了我们足够的警示。各企业或组织需尽快落实数据保护义务，防止重大数据安全事件发生，避免遭受处罚。

典型案例一：案情介绍

2023年6月，北京昌平公安机关在工作中发现，北京某软件有限公司研发的“某数据分析系统”存在数据泄露隐患。经查，该公司研发的“数据分析系统”内存有用户敏感数据。通过进一步核实，该系统内数据信息未采用加密措施，系统服务器未采取任何网络防护措施和技术防护措施，造成19.1GB个人敏感信息暴露在互联网。同时，该公司未制定数据安全管理制度、未充分落实网络安全等级保护制度。北京昌平公安机关根据《数据安全法》第二十七条、第四十五条第一款规定，给予该企业警告并处罚款五万元的行政处罚决定，责令限期改正。

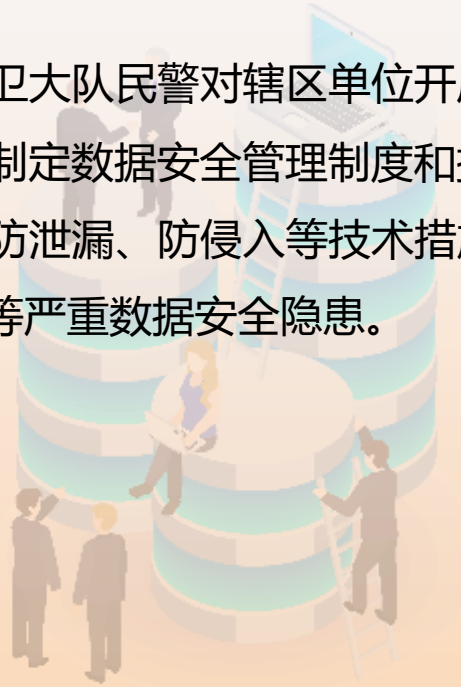
典型案例一：法律解读

本案中，该软件有限公司未依法采取数据保护措施、履行数据安全保护义务，导致大量个人敏感信息数据严重泄露，被公安机关依法给予行政处罚。

开展数据处理活动的组织、个人未依照法律、法规的规定履行建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施，保障数据安全义务的，依据《数据安全法》第二十七条、第四十五条第一款规定，以开展数据处理不履行数据安全保护义务予以行政处罚。《数据安全法》较《个人信息保护法》侧重保护个人信息、隐私而言，更加强调总体国家安全观，对国家利益、公共利益和个人、组织合法权益给予全面保护，标志着我国在网络与信息安全领域的法律法规体系得到进一步完善。

典型案例二：案情介绍

3月13日，邵东市公安局网络安全保卫大队民警对辖区单位开展网络安全和数据安全检查，在检查中发现某二类专科医院和某疫苗接种门诊没有制定数据安全管理制度和操作规程，没有对单位员工开展正规的数据安全教育培训，没有采取任何防篡改、防泄漏、防侵入等技术措施，没有对采集到的居民个人信息采取去标识化和加密措施，系统存在弱口令密码等严重数据安全隐患。



典型案例二：法律解读

该医院和门诊违反了《数据安全法》第二十七条开展数据处理活动应当依照法律、法规的规定，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，保障数据安全；利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务；重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

根据《数据安全法》第四十五条之规定，邵东市公安局对未履行数据安全保护义务的这两家单位依法予以行政警告处罚，两家单位负责人均表示接受处罚并且立即按要求整改到位，邵东警方将继续为数据安全治理作出积极探索和实践。

典型案例三：案情介绍

2022年5月12日，广州警方抓获一作案团伙，调查发现该团伙通过技术手段非法破解“驾培平台”系统，将虚假的培训数据包发送至平台服务器，对学员的学时进行修改，以达到帮助学员快速完成培训和驾校快速盈利的目的，牟利约35万元。在刑事打击非法入侵驾培系统代刷学时案的同时，广州警方检查发现，“驾培平台”系统存储了驾校培训学员的姓名、身份证号、手机号、个人照片等信息1070万余条，但该系统的开发公司没有建立数据安全管理制度和操作规程。因此在刑事打击的同时，警方启动一案双查，对该公司未履行数据安全保护义务的违法行为进行行政立案处罚。

处罚结果：行政处罚方面，警方对“驾培平台”系统开发公司处以警告并处罚款人民币5万元的行政处罚。

典型案例三：法律解读

根据《数据安全法》第二十七条规定，开展数据处理活动应当依照法律、法规的规定，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，保障数据安全。

本案中涉案公司对于日常经营活动采集到的驾校学员个人信息未采取去标识化和加密措施，系统存在未授权访问漏洞等严重数据安全隐患。系统平台一旦被不法分子突破窃取，将导致大量驾校学员个人信息泄露，给广大人民群众个人利益造成重大影响。广州警方对该公司未履行数据安全保护义务的违法行为，根据《数据安全法》四十五条依法处以警告并处罚款人民币5万元的行政处罚，是广东省公安机关适用《数据安全法》的首个案件。

公安同时肩负行政执法权和刑事侦查权，自2018年净网专项行动以来，公安机关对涉及网络的犯罪行为实施“一案双查”制度，即对网络违法犯罪案件开展侦查调查工作时，同步启动对涉案网络服务提供者法定网络安全义务履行情况的监督检查，自源头遏制网络违法犯罪案件发生。

典型案例四：案情介绍

2021年3月，马斯克承认特斯拉车内的摄像头可以监测车主，而民众更大的担忧来自特斯拉数据存储于海外服务器，可能导致国家安全信息、地理信息等关键敏感数据泄露。5月25日晚，特斯拉官方微博发布消息称：已经在中国建立数据中心，以实现数据存储本地化，并将陆续增加更多本地数据中心。所有在中国大陆市场销售车辆所产生的数据，都将存储在境内。特斯拉作为新能源汽车品牌，在处理交通领域相关数据时，鉴于所涉行业的公共利益特殊性以及数据处理体量，符合《数据安全法》第31条中的“关键信息基础设置的运营者”这一界定。

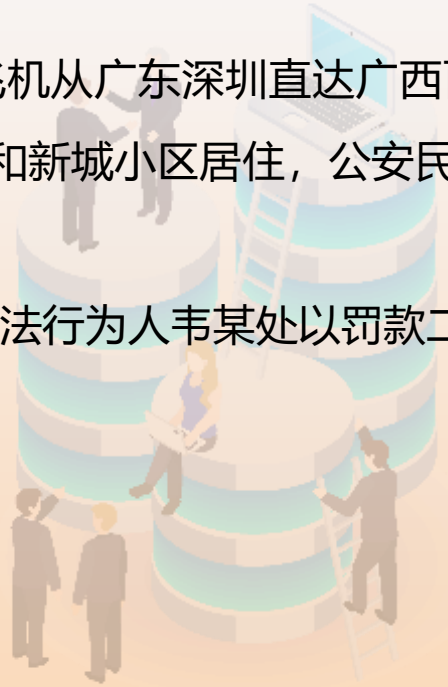
典型案例四：法律解读

《网络安全法》和《关键信息基础设施安全保护条例》规定，交通行业领域以及提供“云计算、大数据等大型公共信息网络服务”的单位，其运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围。因此，特斯拉作为新能源汽车品牌，其在处理交通领域相关数据时，鉴于所涉行业的公共利益特殊性以及数据处理体量，存在被界定为关键信息基础设施运营者的可能。而如若其在开发利用中华人民共和国境内运营收集和产生的重要数据过程中，擅自向境外提供重要数据，则很有可能面临《数据安全法》第四十六条第一款所规定的责令改正、警告、暂停相关业务、停业整顿、吊销许可证以及罚款等行政处罚措施。

典型案例五：案情介绍

2022年1月，违法行为人韦某乘坐飞机从广东深圳直达广西百色巴马机场，后由韦某堂哥韦建锋开车到巴马机场接送韦某回到田阳区田州镇万和新城小区居住，公安民警向韦某了解情况时，韦某却瞒报行程轨迹信息，后被公安民警查实。

根据《数据安全法》第35条，拟对违法行为人韦某处以罚款二百元的处罚。



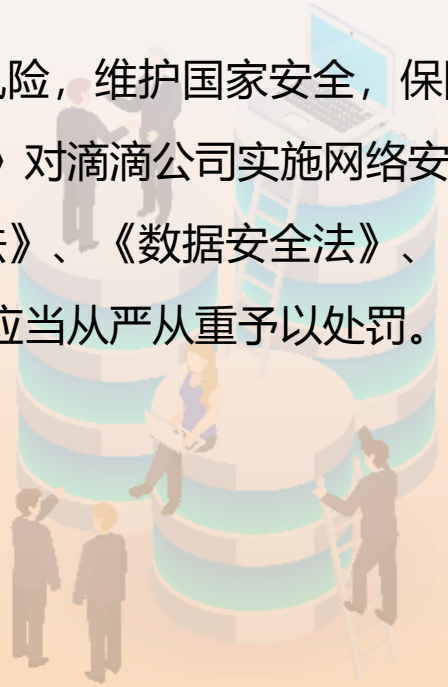
典型案例五：法律解读

《数据安全法》第三十五条规定，“公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。”《数据安全法》是我国首次从立法层面规定了国家机关的数据调取权和公民的配合调取义务。公民具有配合数据调取的义务，应当及时向公安机关和国家安全机关提供必要的工作支持与协助，降低国家机关的调查成本，以便国家安全工作的顺利进行。企业和个人拒不配合数据调取的，根据《数据安全法》第四十八条的规定，由有关主管部门责令改正，给予警告，并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。

典型案例六：案情介绍

2021年7月，为防范国家数据安全风险，维护国家安全，保障公共利益，依据《国家安全法》，网络安全审查办公室按照《网络安全审查办法》对滴滴公司实施网络安全审查。

经查实，滴滴公司违反《网络安全法》、《数据安全法》、《个人信息保护法》的违法违规行为事实清楚、证据确凿、情节严重、性质恶劣，应当从严从重予以处罚。



典型案例六：法律解读

此次对滴滴公司的网络安全审查相关行政处罚，与一般的行政处罚不同，具有特殊性。滴滴公司违法违规行为情节严重，结合网络安全审查情况，应当予以从严从重处罚。一是从违法行为的性质看，滴滴公司未按照相关法律法规规定和监管部门要求，履行网络安全、数据安全、个人信息保护义务，置国家网络安全、数据安全于不顾，给国家网络安全、数据安全带来严重的风险隐患，且在监管部门责令改正情况下，仍未进行全面深入整改，性质极为恶劣。二是从违法行为的持续时间看，滴滴公司相关违法行为最早开始于2015年6月，持续时间长达7年，持续违反2017年6月实施的《网络安全法》、2021年9月实施的《数据安全法》和2021年11月实施的《个人信息保护法》。三是从违法行为的危害看，滴滴公司通过违法手段收集用户剪切板信息、相册中的截图信息、亲情关系信息等个人信息，严重侵犯用户隐私，严重侵害用户个人信息权益。四是从违法处理个人信息的数量看，滴滴公司违法处理个人信息达647.09亿条，数量巨大，其中包括人脸识别信息、精准位置信息、身份证号等多类敏感个人信息。五是从违法处理个人信息的情形看，滴滴公司违法行为涉及多个App，涵盖过度收集个人信息、强制收集敏感个人信息、App频繁索权、未尽个人信息处理告知义务、未尽网络安全数据安全保护义务等多种情形。

感谢观看

内容参考：www.sohu.com/a/687390254_121123754
公众号来源： 谈思汽车|数达安全|数据长沙