国盟信息安全通报

2021 年 03 月 14 日第 235 期

全国售后服务中心

国盟信息安全通报

（第 235 期）

国际信息安全学习联盟

2021 年 3 月 14 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 488 个，其中高危漏洞 196 个、中危漏洞 244 个、低危漏洞 48 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 43%），其中互联网上出现“UltimateKode Neo Billing 跨站脚本漏洞、PHPSHE SQL 注入漏洞（CNVD-2021-14156）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 6101 个，与上周（4894 个）环比增加 25%。

主要内容

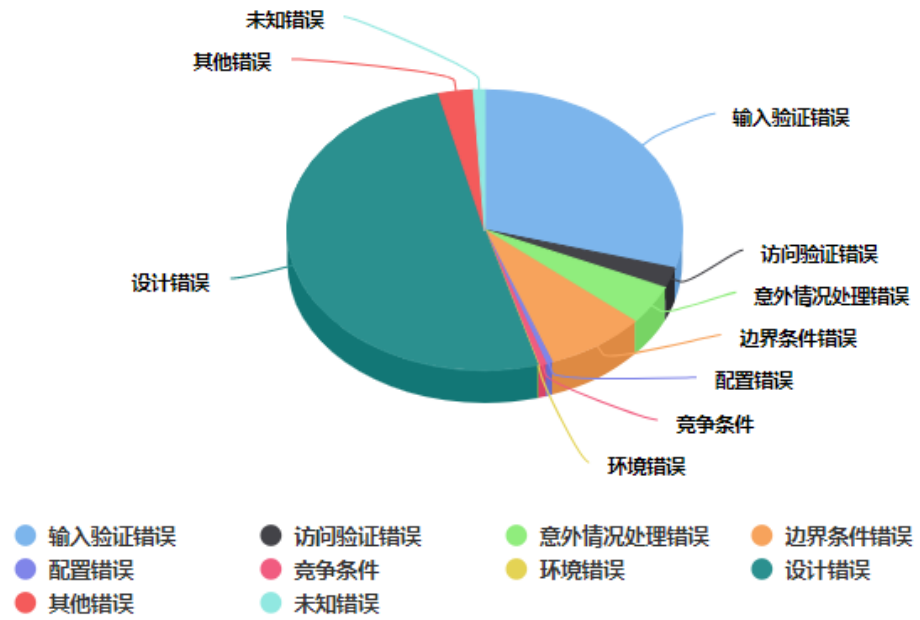
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

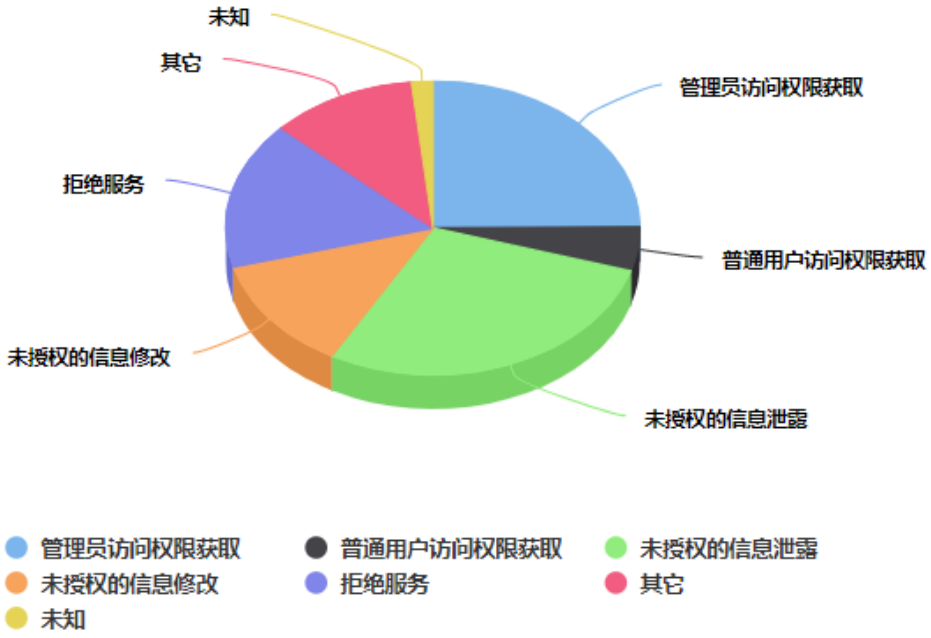
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 488 个，其中高危漏洞 196 个、中危漏洞 244 个、低危漏洞 48 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 43%），其中互联网上出现“UltimateKode Neo Billing 跨站脚本漏洞、PHPSHE SQL 注入漏洞（CNVD-2021-14156）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 6101 个，与上周（4894 个）环比增加 25%。

二、安全漏洞增长数量及种类分布情况

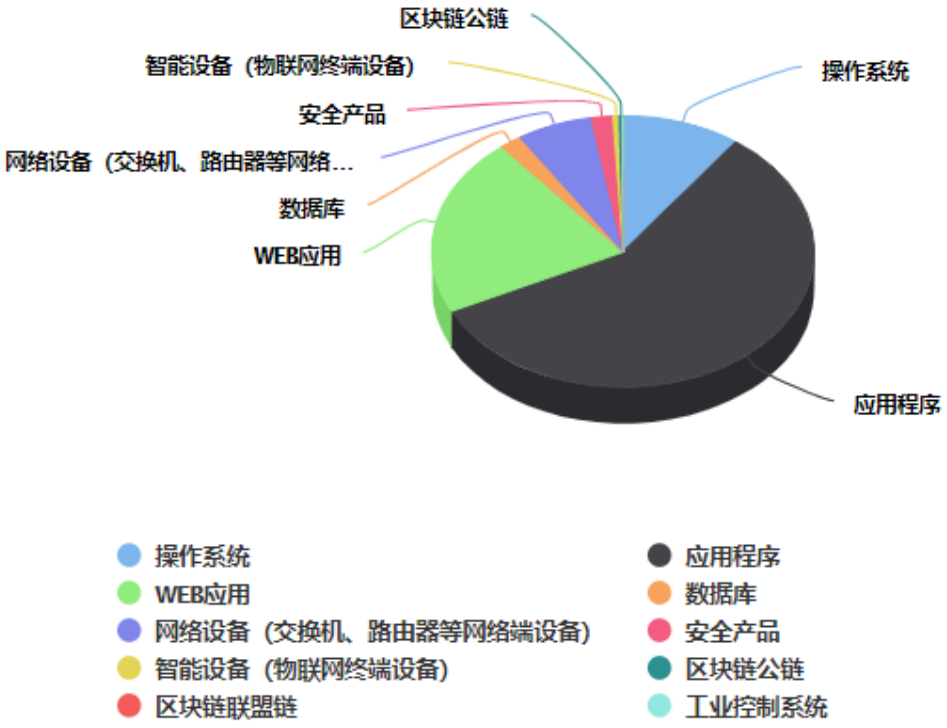
➢ 漏洞产生原因（2021 年 3 月 1 日—2021 年 3 月 14）



➢ 漏洞引发的威胁（2021 年 3 月 1 日—2021 年 3 月 14）



➢ 漏洞影响对象类型（2021 年 3 月 1 日—2021 年 3 月 14）



三、安全产业动态

➢ “十四五”规划纲要发布！关于网信有哪些内容?

据悉，《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》已于 3 月 12 日由新华社受权于发布。十三届全国人大四次会议 3 月 11 日表决通过了关于国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要的决议，决定批准这个规划纲要。

纲要共分为 19 篇：“开启全面建设社会主义现代化国家新征程”“坚持创新驱动发展　全面塑造发展新优势”“加快发展现代产业体系　巩固壮大实体经济根基”“形成强大国内市场构建新发展格局”“加快数字化发展　建设数字中国”“全面深化改革　构建高水平社会主义市场经济体制”“坚持农业农村优先发展全面推进乡村振兴”“完善新型城镇化战略　提升城镇化发展质量”“优化区域经济布局　促进区域协调发展”“发展社会主义先进文化　提升国家文化软实力”“推动绿色发展　促进人与自然和谐共生”“实行高水平对外开放　开拓合作共赢新局面”“提升国民素质　促进人的全面发展”“增进民生福祉　提升共建共治共享水平”“统筹发展和安全　建设更高水平的平安中国”“加快国防和军队现代化　实现富国和强军相统一”“加强社会主义民主法治建设　健全党和国家监督制度”“坚持‘一国两制’　推进祖国统一”“加强规划实施保障”。

下面我们来看看，纲要中有哪些关于网信的内容：

第一篇 开启全面建设社会主义现代化国家新征程

第三章 主要目标

第一节 2035 年远景目标

展望 2035 年，我国将基本实现社会主义现代化。经济实力、科技实力、综合国力将大幅跃升，经济总量和城乡居民人均收入将再迈上新的大台阶，关键核心技术实现重大突破，进入创新型国家前列。基本实现新型工业化、信息化、城镇化、农业现代化，建成现代化经济体系。基本实现国家治理体系和治理能力现代化，人民平等参与、平等发展权利得到充分保障，基本建成法治国家、法治政府、法治社会。建成文化强国、教育强国、人才强国、体育强国、健康中国，国民素质和社会文明程度达到新高度，国家文化软实力显著增强。……

第二篇 坚持新驱动发展 全面塑造发展新优势

第四章 强化国家战略科技力量

制定科技强国行动纲要，健全社会主义市场经济条件下新型举国体制，打好关键核心技术攻坚战，提高创新链整体效能。

第一节 整合优化科技资源配置

以国家战略性需求为导向推进创新体系优化组合，加快构建以国家实验室为引领的战略科技力量。聚焦量子信息、光子与微纳电子、网络通信、人工智能、生物医药、现代能源系统等重大创新领域组建一批国家实验室，重组国家重点实验室，形成结构合理、运行高效的实验室体系。优化提升国家工程研究中心、国家技术创新中心等创新基地。推进科研院所、高等院校和企业科研力量优化配置和资源共享。支持发展新型研究型大学、新型研发机构等新型创新主体，推动投入主体多元化、管理制度现代化、运行机制市场化、用人机制灵活化。

第二节 加强原创性引领性科技攻关

在事关国家安全和发展全局的基础核心领域，制定实施战略性科学计划和科学工程。瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。从国家急迫需要和长远需求出发，集中优势资源攻关新发突发传染病和生物安全风险防控、医药和医疗设备、关键元器件零部件和基础材料、油气勘探开发等领域关键核心技术。……

第三篇 加快发展现代产业体系 巩固壮大实体经济根基

第八章 深入实施制造强国战略

第一节 加强产业基础能力建设

实施产业基础再造工程，加快补齐基础零部件及元器件、基础软件、基础材料、基础工艺和产业技术基础等瓶颈短板。依托行业龙头企业，加大重要产品和关键核心技术攻关力度，加快工程化产业化突破。实施重大技术装备攻关工程，完善激励和风险补偿机制，推动首台（套）装备、首批次材料、首版次软件示范应用。健全产业基础支撑体系，在重点领域布局一批国家制造业创新中心，完善国家质量基础设施，建设生产应用示范平台和标准计量、认证认可、检验检测、试验验证等产业技术基础公共服务平台，完善技术、工艺等工业基础数据库。……

第九章 发展壮大战略性新兴产业

第一节 构筑产业体系新支柱

聚焦新一代信息技术、生物技术、新能源、新材料、高端装备、新能源汽车、绿色环保以及航空航天、海洋装备等战略性新兴产业，加快关键核心技术创新应用，增强要素保障能力，培育壮大产业发展新动能。推动生物技术和信息技术融合创新，加快发展生物医药、生物育种、生物材料、生物能源等产业，做大做强生物经济。深化北斗系统推广应用，推动北斗产业高质量发展。深入推进国家战略性新兴产业集群发展工程，健全产业集群组织管理和专业化推进机制，建设创新和公共服务综合体，构建一批各具特色、优势互补、结构合理的战略性新兴产业增长引擎。鼓励技术创新和企业兼并重组，防止低水平重复建设。发挥产业投资基金引导作用，加大融资担保和风险补偿力度。

第二节 前瞻谋划未来产业

在类脑智能、量子信息、基因技术、未来网络、深海空天开发、氢能与储能等前沿科技和产业变革领域，组织实施未来产业孵化与加速计划，谋划布局一批未来产业。在科教资源优势突出、产业基础雄厚的地区，布局一批国家未来产业技术研究院，加强前沿技术多路径探索、交叉融合和颠覆性技术供给。实施产业跨界融合示范工程，打造未来技术应用场景，加速形成若干未来产业。……

第十一章 建设现代化基础设施体系

统筹推进传统基础设施和新型基础设施建设，打造系统完备、高效实用、智能绿色、安全可靠的现代化基础设施体系。

第一节 加快建设新型基础设施

围绕强化数字转型、智能升级、融合创新支撑，布局建设信息基础设施、融合基础设施、创新基础设施等新型基础设施。建设高速泛在、天地一体、集成互联、安全高效的信息基础设施，增强数据感知、传输、存储和运算能力。加快 5G 网络规模化部署，用户普及率提高

到 56%，推广升级千兆光纤网络。前瞻布局 6G 网络技术储备。扩容骨干网互联节点，新设一批国际通信出入口，全面推进互联网协议第六版（IPv6）商用部署。实施中西部地区中小城市基础网络完善工程。推动物联网全面发展，打造支持固移融合、宽窄结合的物联接入能力。加快构建全国一体化大数据中心体系，强化算力统筹智能调度，建设若干国家枢纽节点和大数据中心集群，建设 E 级和 10E 级超级计算中心。积极稳妥发展工业互联网和车联网。打造全球覆盖、高效运行的通信、导航、遥感空间基础设施体系，建设商业航天发射场。加快交通、能源、市政等传统基础设施数字化改造，加强泛在感知、终端联网、智能调度体系建设。发挥市场主导作用，打通多元化投资渠道，构建新型基础设施标准体系。……

第四篇 形成强大国内市场 构建新发展格局

第十三章 促进国内国际双循环

第二节 提高国际双向投资水平

坚持引进来和走出去并重，以高水平双向投资高效利用全球资源要素和市场空间，完善产业链供应链保障机制，推动产业竞争力提升。更大力度吸引和利用外资，有序推进电信、互联网、教育、文化、医疗等领域相关业务开放。全面优化外商投资服务，加强外商投资促进和保护，发挥重大外资项目示范效应，支持外资加大中高端制造、高新技术、传统制造转型升级、现代服务等领域和中西部地区投资，支持外资企业设立研发中心和参与承担国家科技计划项目。鼓励外资企业利润再投资。坚持企业主体，创新境外投资方式，优化境外投资结构和布局，提升风险防范能力和收益水平。完善境外生产服务网络和流通体系，加快金融、咨询、会计、法律等生产性服务业国际化发展，推动中国产品、服务、技术、品牌、标准走出去。支持企业融入全球产业链供应链，提高跨国经营能力和水平。引导企业加强合规管理，防范化解境外政治、经济、安全等各类风险。推进多双边投资合作机制建设，健全促进和保障境外投资政策和服务体系，推动境外投资立法。

第十四章 加快培育完整内需体系

第二节 拓展投资空间

优化投资结构，提高投资效率，保持投资合理增长。加快补齐基础设施、市政工程、农业农村、公共安全、生态环保、公共卫生、物资储备、防灾减灾、民生保障等领域短板，推动企业设备更新和技术改造，扩大战略性新兴产业投资。推进既促消费惠民生又调结构增后劲的新型基础设施、新型城镇化、交通水利等重大工程建设。面向服务国家重大战略，实施川藏铁路、西部陆海新通道、国家水网、雅鲁藏布江下游水电开发、星际探测、北斗产业化等重大工程，推进重大科研设施、重大生态系统保护修复、公共卫生应急保障、重大引调水、

防洪减灾、送电输气、沿边沿江沿海交通等一批强基础、增功能、利长远的重大项目建设。深化投融资体制改革，发挥政府投资撬动作用，激发民间投资活力，形成市场主导的投资内生增长机制。健全项目谋划、储备、推进机制，加大资金、用地等要素保障力度，加快投资项目落地见效。规范有序推进政府和社会资本合作（PPP），推动基础设施领域不动产投资信托基金（REITs）健康发展，有效盘活存量资产，形成存量资产和新增投资的良性循环。

第五篇 加快数字化发展 建设数字中国

迎接数字时代，激活数据要素潜能，推进网络强国建设，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。

第十五章 打造数字经济新优势

充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，壮大经济发展新引擎。

第一节 加强关键数字技术创新应用

聚焦高端芯片、操作系统、人工智能关键算法、传感器等关键领域，加快推进基础理论、基础算法、装备材料等研发突破与迭代应用。加强通用处理器、云计算系统和软件核心技术一体化研发。加快布局量子计算、量子通信、神经芯片、DNA 存储等前沿技术，加强信息科学与生命科学、材料等基础学科的交叉创新，支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。

第二节 加快推动数字产业化

培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，提升通信设备、核心电子元器件、关键软件等产业水平。构建基于 5G 的应用场景和产业生态，在智能交通、智慧物流、智慧能源、智慧医疗等重点领域开展试点示范。鼓励企业开放搜索、电商、社交等数据，发展第三方大数据服务产业。促进共享经济、平台经济健康发展。

第三节 推进产业数字化转型

实施“上云用数赋智”行动，推动数据赋能全产业链协同转型。在重点行业和区域建设若干国际水准的工业互联网平台和数字化转型促进中心，深化研发设计、生产制造、经营管理、市场服务等环节的数字化应用，培育发展个性定制、柔性制造等新模式，加快产业园区数字化改造。深入推进服务业数字化转型，培育众包设计、智慧物流、新零售等新增长点。加快发展智慧农业，推进农业生产经营和管理服务数字化改造。

第十六章 加快数字社会建设步伐

适应数字技术全面融入社会交往和日常生活新趋势，促进公共服务和社会运行方式创新，

构筑全民畅享的数字生活。

第一节 提供智慧便捷的公共服务

聚焦教育、医疗、养老、抚幼、就业、文体、助残等重点领域，推动数字化服务普惠应用，持续提升群众获得感。推进学校、医院、养老院等公共服务机构资源数字化，加大开放共享和应用力度。推进线上线下公共服务共同发展、深度融合，积极发展在线课堂、互联网医院、智慧图书馆等，支持高水平公共服务机构对接基层、边远和欠发达地区，扩大优质公共服务资源辐射覆盖范围。加强智慧法院建设。鼓励社会力量参与“互联网+公共服务”，创新提供服务模式和产品。

第二节 建设智慧城市和数字乡村

以数字化助推城乡发展和治理模式创新，全面提高运行效率和宜居度。分级分类推进新型智慧城市建设，将物联网感知设施、通信系统等纳入公共基础设施统一规划建设，推进市政公用设施、建筑等物联网应用和智能化改造。完善城市信息模型平台和运行管理服务平台，构建城市数据资源体系，推进城市数据大脑建设。探索建设数字孪生城市。加快推进数字乡村建设，构建面向农业农村的综合信息服务体系，建立涉农信息普惠服务机制，推动乡村管理服务数字化。

第三节 构筑美好数字生活新图景

推动购物消费、居家生活、旅游休闲、交通出行等各类场景数字化，打造智慧共享、和睦共治的新型数字生活。推进智慧社区建设，依托社区数字化平台和线下社区服务机构，建设便民惠民智慧服务圈，提供线上线下融合的社区生活服务、社区治理及公共服务、智能小区等服务。丰富数字生活体验，发展数字家庭。加强全民数字技能教育和培训，普及提升公民数字素养。加快信息无障碍建设，帮助老年人、残疾人等共享数字生活。

第十七章 提高数字政府建设水平

将数字技术广泛应用于政府管理服务，推动政府治理流程再造和模式优化，不断提高决策科学性和服务效率。

第一节 加强公共数据开放共享

建立健全国家公共数据资源体系，确保公共数据安全，推进数据跨部门、跨层级、跨地区汇聚融合和深度利用。健全数据资源目录和责任清单制度，提升国家数据共享交换平台功能，深化国家人口、法人、空间地理等基础信息资源共享利用。扩大基础公共信息数据安全有序开放，探索将公共数据服务纳入公共服务体系，构建统一的国家公共数据开放平台和开发利用端口，优先推动企业登记监管、卫生、交通、气象等高价值数据集向社会开放。开展

政府数据授权运营试点，鼓励第三方深化对公共数据的挖掘利用。

第二节 推动政务信息化共建共用

加大政务信息化建设统筹力度，健全政务信息化项目清单，持续深化政务信息系统整合，布局建设执政能力、依法治国、经济治理、市场监管、公共安全、生态环境等重大信息系统，提升跨部门协同治理能力。完善国家电子政务网络，集约建设政务云平台和数据中心体系，推进政务信息系统云迁移。加强政务信息化建设快速迭代，增强政务信息系统快速部署能力和弹性扩展能力。

第三节 提高数字化政务服务效能

全面推进政府运行方式、业务流程和服务模式数字化智能化。深化“互联网+政务服务”，提升全流程一体化在线服务平台功能。加快构建数字技术辅助政府决策机制，提高基于高频大数据精准动态监测预测预警水平。强化数字技术在公共卫生、自然灾害、事故灾难、社会安全等突发公共事件应对中的运用，全面提升预警和应急处置能力。

第十八章 营造良好数字生态

坚持放管并重，促进发展与规范管理相统一，构建数字规则体系，营造开放、健康、安全的数字生态。

第一节 建立健全数据要素市场规则

统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。建立健全数据产权交易和行业自律机制，培育规范的数据交易平台和市场主体，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。加强涉及国家利益、商业秘密、个人隐私的数据保护，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。完善适用于大数据环境下的数据分类分级保护制度。加强数据安全评估，推动数据跨境安全有序流动。

第二节 营造规范有序的政策环境

构建与数字经济发展相适应的政策法规体系。健全共享经济、平台经济和新个体经济管理规范，清理不合理的行政许可、资质资格事项，支持平台企业创新发展、增强国际竞争力。依法依规加强互联网平台经济监管，明确平台企业定位和监管规则，完善垄断认定法律规范，打击垄断和不正当竞争行为。探索建立无人驾驶、在线医疗、金融科技、智能配送等监管框架，完善相关法律法规和伦理审查规则。健全数字经济统计监测体系。

第三节 加强网络安全保护

健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统

安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。加强网络安全宣传教育和人才培养。

第四节 推动构建网络空间命运共同体

推进网络空间国际交流与合作，推动以联合国为主渠道、以联合国宪章为基本原则制定数字和网络空间国际规则。推动建立多边、民主、透明的全球互联网治理体系，建立更加公平合理的网络基础设施和资源治理机制。积极参与数据安全、数字货币、数字税等国际规则和数字技术标准制定。推动全球网络安全保障合作机制建设，构建保护数据要素、处置网络安全事件、打击网络犯罪的国际协调合作机制。向欠发达国家提供技术、设备、服务等数字援助，使各国共享数字时代红利。积极推进网络文化交流互鉴。

第六篇 全面深化改革 构建高水平社会主义市场经济体制

第十九章 激发各类市场主体活力

第一节 加快国有经济布局优化和结构调整

围绕服务国家战略，坚持有进有退、有所为有所不为，加快国有经济布局优化、结构调整和战略性重组，增强国有经济竞争力、创新力、控制力、影响力、抗风险能力，做强做优做大国有资本和国有企业。发挥国有经济战略支撑作用，推动国有经济进一步聚焦战略安全、产业引领、国计民生、公共服务等功能，调整盘活存量资产，优化增量资本配置，向关系国家安全、国民经济命脉的重要行业集中，向提供公共服务、应急能力建设和公益性等关系国计民生的重要行业集中，向前瞻性战略性新兴产业集中。对充分竞争领域的国有经济，强化资本收益目标和财务硬约束，增强流动性，完善国有资本优化配置机制。建立布局结构调整长效机制，动态发布国有经济布局优化和结构调整指引。……

第五节 促进民营企业高质量发展

鼓励民营企业改革创新，提升经营能力和管理水平。引导有条件的民营企业建立现代企业制度。支持民营企业开展基础研究和科技创新、参与关键核心技术研发和国家重大科技项目攻关。完善民营企业参与国家重大战略实施机制。推动民营企业守法合规经营，鼓励民营企业积极履行社会责任、参与社会公益和慈善事业。弘扬企业家精神，实施年轻一代民营企业家健康成长促进计划。

第二十章 建设高标准市场体系

第一节 全面完善产权制度

健全归属清晰、权责明确、保护严格、流转顺畅的现代产权制度。实施民法典，制修订物权、债权、股权等产权法律法规，明晰产权归属、完善产权权能。健全以公平为原则的产权保护制度，依法平等保护国有、民营、外资等各种所有制企业产权。健全产权执法司法保护制度，完善涉企产权案件申诉、复核、重审等保护机制，推动涉企冤错案件依法甄别纠正常态化机制化，畅通涉政府产权纠纷反映和处理渠道。加强数据、知识、环境等领域产权制度建设，健全自然资源资产产权制度和法律法规。

第二节 推进要素市场化配置改革

建立健全城乡统一的建设用地市场，统筹推进农村土地征收、集体经营性建设用地入市、宅基地制度改革。改革土地计划管理方式，赋予省级政府更大用地自主权，探索建立全国性的建设用地、补充耕地指标跨区域交易机制。建立不同产业用地类型合理转换机制，增加混合产业用地供给。健全统一规范的人力资源市场体系，破除劳动力和人才在城乡、区域和不同所有制单位间的流动障碍，减少人事档案管理中的不合理限制。发展技术和数据要素市场。健全要素市场运行机制，完善交易规则和服务体系。深化公共资源交易平台整合共享。……

第四节 健全社会信用体系

建立健全信用法律法规和标准体系，制定公共信用信息目录和失信惩戒措施清单，完善失信主体信用修复机制。推广信用承诺制度。加强信用信息归集、共享、公开和应用，推广惠民便企信用产品与服务。建立公共信用信息和金融信息的共享整合机制。培育具有国际竞争力的企业征信机构和信用评级机构，加强征信监管，推动信用服务市场健康发展。加强信用信息安全管理，保障信用主体合法权益。建立健全政府失信责任追究制度。

第二十一章 建立现代财税金融体制

第三节 深化金融供给侧结构性改革

健全具有高度适应性、竞争力、普惠性的现代金融体系，构建金融有效支持实体经济的体制机制。建设现代中央银行制度，完善货币供应调控机制。稳妥推进数字货币研发。健全市场化利率形成和传导机制，完善央行政策利率体系，更好发挥贷款市场报价利率基准作用。优化金融体系结构，深化国有商业银行改革，加快完善中小银行和农村信用社治理结构，规范发展非银行金融机构，增强金融普惠性。改革优化政策性金融，强化服务国家战略和规划能力。深化保险公司改革，提高商业保险保障能力。健全金融机构公司治理，强化股东股权和关联交易监管。完善资本市场基础制度，健全多层次资本市场体系，大力发展机构投资者，提高直接融资特别是股权融资比重。全面实行股票发行注册制，建立常态化退市机制，提高

上市公司质量。深化新三板改革。完善市场化债券发行机制，稳步扩大债券市场规模，丰富债券品种，发行长期国债和基础设施长期债券。完善投资者保护制度和存款保险制度。完善现代金融监管体系，补齐监管制度短板，在审慎监管前提下有序推进金融创新，健全风险全覆盖监管框架，提高金融监管透明度和法治化水平。稳妥发展金融科技，加快金融机构数字化转型。强化监管科技运用和金融创新风险评估，探索建立创新产品纠偏和暂停机制。

第二十二章 提升政府经济治理能力

第一节 完善宏观经济治理

健全以国家发展规划为战略导向，以财政政策和货币政策为主要手段，就业、产业、投资、消费、环保、区域等政策紧密配合，目标优化、分工合理、高效协同的宏观经济治理体系。增强国家发展规划对公共预算、国土开发、资源配置等政策的宏观引导、统筹协调功能，健全宏观政策制定和执行机制，重视预期管理和引导，合理把握经济增长、就业、价格、国际收支等调控目标，在区间调控基础上加强定向调控、相机调控和精准调控。完善宏观调控政策体系，搞好跨周期政策设计，提高逆周期调节能力，促进经济总量平衡、结构优化、内外均衡。加强宏观经济治理数据库等建设，提升大数据等现代技术手段辅助治理能力，推进统计现代化改革。健全宏观经济政策评估评价制度和重大风险识别预警机制，畅通政策制定参与渠道，提高决策科学化、民主化、法治化水平。……

第三节 推进监管能力现代化

健全以“双随机、一公开”监管和“互联网+监管”为基本手段、以重点监管为补充、以信用监管为基础的新型监管机制，推进线上线下一体化监管。严格市场监管、质量监管、安全监管，加强对食品药品、特种设备和网络交易、旅游、广告、中介、物业等的监管，强化要素市场交易监管，对新产业新业态实施包容审慎监管。深化市场监管综合行政执法改革，完善跨领域跨部门联动执法、协同监管机制。深化行业协会、商会和中介机构改革。加强社会公众、新闻媒体监督。……

第八篇 完善新型城镇化战略 提升城镇化发展质量

第二十九章 全面提升城市品质

第三节 提高城市治理水平

坚持党建引领、重心下移、科技赋能，不断提升城市治理科学化精细化智能化水平，推进市域社会治理现代化。改革完善城市管理体制。推广“街乡吹哨、部门报到、接诉即办”等基层管理机制经验，推动资源、管理、服务向街道社区下沉，加快建设现代社区。运用数字技术推动城市管理手段、管理模式、管理理念创新，精准高效满足群众需求。加强物业服

务监管，提高物业服务覆盖率、服务质量和标准化水平。……

第十篇 发展社会主义先进文化 提升国家文化软实力

第三十六章 健全现代文化产业体系

第一节 扩大优质文化产品供给

实施文化产业数字化战略，加快发展新型文化企业、文化业态、文化消费模式，壮大数字创意、网络视听、数字出版、数字娱乐、线上演播等产业。加快提升超高清电视节目制播能力，推进电视频道高清化改造，推进沉浸式视频、云转播等应用。实施文化品牌战略，打造一批有影响力、代表性的文化品牌。培育骨干文化企业，规范发展文化产业园区，推动区域文化产业带建设。积极发展对外文化贸易，开拓海外文化市场，鼓励优秀传统文化产品和影视剧、游戏等数字文化产品“走出去”，加强国家文化出口基地建设。……

第三节 深化文化体制改革

完善文化管理体制和生产经营机制，提升文化治理效能。完善国有文化资产管理体制机制，深化公益性文化事业单位改革，推进公共文化机构法人治理结构改革。深化国有文化企业分类改革，推进国有文艺院团改革和院线制改革。完善文化市场综合执法体制，制定未成年人网络保护、信息网络传播视听等领域法律法规。……

第十二篇 实行高水平对外开放 开拓合作共赢新局面

第四十章 建设更高水平开放型经济新体制

第二节 提升对外开放平台功能

统筹推进各类开放平台建设，打造开放层次更高、营商环境更优、辐射作用更强的开放新高地。完善自由贸易试验区布局，赋予其更大改革自主权，深化首创性、集成化、差别化改革探索，积极复制推广制度创新成果。稳步推进海南自由贸易港建设，以货物贸易“零关税”、服务贸易“既准入又准营”为方向推进贸易自由化便利化，大幅放宽市场准入，全面推行“极简审批”投资制度，开展跨境证券投融资改革试点和数据跨境传输安全管理试点，实施更加开放的人才、出入境、运输等政策，制定出台海南自由贸易港法，初步建立中国特色自由贸易港政策和制度体系。创新提升国家级新区和开发区，促进综合保税区高水平开放，完善沿边重点开发开放试验区、边境经济合作区、跨境经济合作区功能，支持宁夏、贵州、江西建设内陆开放型经济试验区。……

第四节 健全开放安全保障体系

构筑与更高水平开放相匹配的监管和风险防控体系。健全产业损害预警体系，丰富贸易调整援助、贸易救济等政策工具，妥善应对经贸摩擦。健全外商投资国家安全审查、反垄断

审查和国家技术安全清单管理、不可靠实体清单等制度。建立重要资源和产品全球供应链风险预警系统，加强国际供应链保障合作。加强国际收支监测，保持国际收支基本平衡和外汇储备基本稳定。加强对外资产负债监测，建立健全全口径外债监管体系。完善境外投资分类分级监管体系。构建海外利益保护和风险预警防范体系。优化提升驻外外交机构基础设施保障能力，完善领事保护工作体制机制，维护海外中国公民、机构安全和正当权益。

第四十一章 推动共建“一带一路”高质量发展

坚持共商共建共享原则，秉持绿色、开放、廉洁理念，深化务实合作，加强安全保障，促进共同发展。

第一节 加强发展战略和政策对接

推进战略、规划、机制对接，加强政策、规则、标准联通。创新对接方式，推进已签文件落实见效，推动与更多国家商签投资保护协定、避免双重征税协定等，加强海关、税收、监管等合作，推动实施更高水平的通关一体化。拓展规则对接领域，加强融资、贸易、能源、数字信息、农业等领域规则对接合作。促进共建“一带一路”倡议同区域和国际发展议程有效对接、协同增效。

第二节 推进基础设施互联互通

推动陆海天网四位一体联通，以“六廊六路多国多港”为基本框架，构建以新亚欧大陆桥等经济走廊为引领，以中欧班列、陆海新通道等大通道和信息高速路为骨架，以铁路、港口、管网等为依托的互联互通网络，打造国际陆海贸易新通道。聚焦关键通道和关键城市，有序推动重大合作项目建设，将高质量、可持续、抗风险、价格合理、包容可及目标融入项目建设全过程。提高中欧班列开行质量，推动国际陆运贸易规则制定。扩大“丝路海运”品牌影响。推进福建、新疆建设“一带一路”核心区。推进“一带一路”空间信息走廊建设。建设“空中丝绸之路”。……

第十五篇 统筹发展和安全 建设更高水平的平安中国

坚持总体国家安全观，实施国家安全战略，维护和塑造国家安全，统筹传统安全和非传统安全，把安全发展贯穿国家发展各领域和全过程，防范和化解影响我国现代化进程的各种风险，筑牢国家安全屏障。

第五十二章 加强国家安全体系和能力建设

坚持政治安全、人民安全、国家利益至上有机统一，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，不断增强国家安全能力。完善集中统一、高效权威的国家安全领导体制，健全国家安全法治体系、战略体系、政策体

系、人才体系和运行机制，完善重要领域国家安全立法、制度、政策。巩固国家安全人民防线，加强国家安全宣传教育，增强全民国家安全意识，建立健全国家安全风险研判、防控协同、防范化解机制。健全国家安全审查和监管制度，加强国家安全执法。坚定维护国家政权安全、制度安全、意识形态安全，全面加强网络安全保障体系和能力建设，切实维护新型领域安全，严密防范和严厉打击敌对势力渗透、破坏、颠覆、分裂活动。

第五十三章 强化国家经济安全保障

强化经济安全风险预警、防控机制和能力建设，实现重要产业、基础设施、战略资源、重大科技等关键领域安全可控，着力提升粮食、能源、金融等领域安全发展能力。……

第三节 实施金融安全战略

健全金融风险预防、预警、处置、问责制度体系，落实监管责任和属地责任，对违法违规行为零容忍，守住不发生系统性风险的底线。完善宏观审慎管理体系，保持宏观杠杆率以稳为主、稳中有降。加强系统重要性金融机构和金融控股公司监管，强化不良资产认定和处置，防范化解影子银行风险，有序处置高风险金融机构，严厉打击非法金融活动，健全互联网金融监管长效机制。完善债务风险识别、评估预警和有效防控机制，健全债券市场违约处置机制，推动债券市场统一执法，稳妥化解地方政府隐性债务，严惩逃废债行为。完善跨境资本流动管理框架，加强监管合作，提高开放条件下风险防控和应对能力。加强人民币跨境支付系统建设，推进金融业信息化核心技术安全可控，维护金融基础设施安全。……

第五十五章 维护社会稳定和安全

第二节 推进社会治安防控体系现代化

坚持专群结合、群防群治，提高社会治安立体化、法治化、专业化、智能化水平，形成问题联治、工作联动、平安联创的工作机制，健全社会治安防控体系。继续开展好禁毒人民战争和反恐怖斗争，推动扫黑除恶常态化，严厉打击各类违法犯罪活动，提升打击新型网络犯罪和跨国跨区域犯罪能力。坚持打防结合、整体防控，强化社会治安重点地区排查整治，健全社会治安协调联动机制。推进公安大数据智能化平台建设。完善执法司法权力运行监督和制约机制，健全执法司法人员权益保障机制。建设国门安全防控体系。深化国际执法安全务实合作。

第十六篇 加快国防和军队现代化 实现富国和强军相统一

第五十七章 促进国防实力和经济实力同步提升

同国家现代化发展相协调，搞好战略层面筹划，深化资源要素共享，强化政策制度协调，完善组织管理、工作运行、政策制度、人才队伍、风险防控体系，构建一体化国家战略体系

和能力。推动重点区域、重点领域、新兴领域协调发展，集中力量实施国防领域重大工程。促进军事建设布局与区域经济发展布局有机结合，更好服务国家安全发展战略需要。深化军民科技协同创新，加强海洋、空天、网络空间、生物、新能源、人工智能、量子科技等领域军民统筹发展，推动军地科研设施资源共享，推进军地科研成果双向转化应用和重点产业发展。强化基础设施共建共用，加强新型基础设施统筹建设，加大经济建设项目贯彻国防要求力度。加快建设现代军事物流体系和资产管理体系。加强军地人才联合培养，健全军地人才交流使用、资格认证等制度。优化国防科技工业布局，加快标准化通用化进程。推进武器装备市场准入、空中交通管理等改革。完善国防动员体系，加强应急应战协同，健全强边固防机制，强化全民国防教育，巩固军政军民团结。维护军人军属合法权益，让军人成为全社会尊崇的职业。（来源：新华社）

- **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**
- **全文：**http://www.xinhuanet.com/2021-03/13/c_1127205564.htm

➢ 最高法解读工作报告：不得过度收集个人信息

2021 年 3 月 8 日下午，最高人民法院举办 2021 年全国两会《最高人民法院工作报告》系列解读全媒体直播访谈第一场活动，**最高人民法院副院长贺小荣在线解读工作报告**。互联网时代，人们在通过手机下载安装某些 App 时，往往会被索取定位、访问设备照片、通讯录、脸型及指纹信息等与下载目的无关的内容，不同意则无法正常下载使用，同意则会给后续生活带来不必要烦恼，人民法院如何应对过度收集个人信息的问题？报告中表示，“审理手机软件侵害用户个人信息、人脸识别纠纷等案件,加强个人信息保护,维护数据安全。”

不得过度搜集个人信息

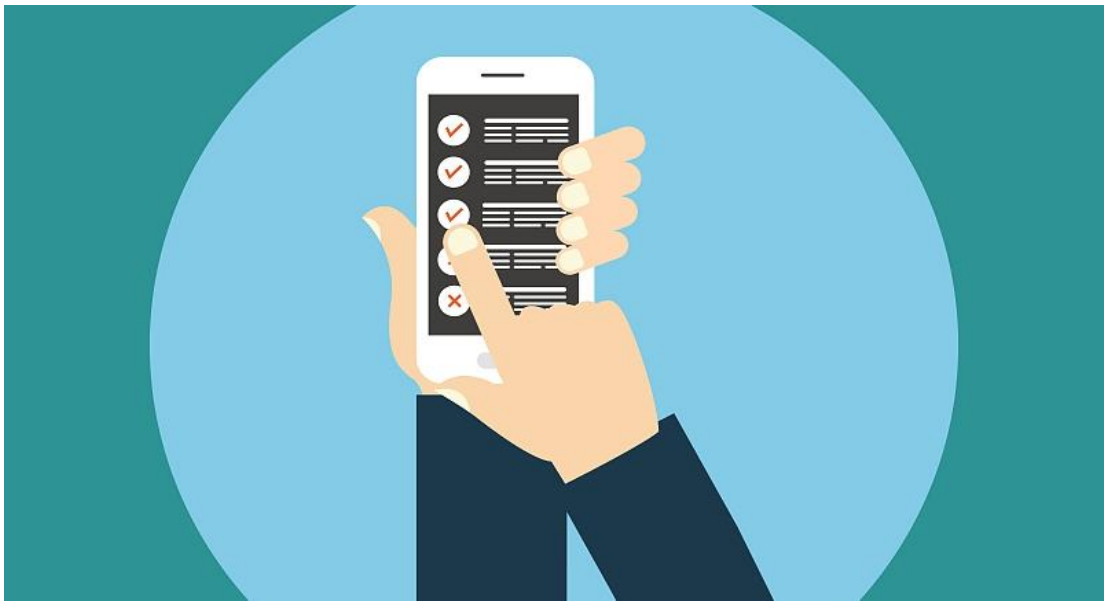
贺小荣在回答记者提问时强调，“互联网并非法外之地，App 运营商提供服务时必须遵守法律规定”。我国《网络安全法》第 41 条第 2 款规定，网络运营者不得收集与其提供的服务无关的个人信息。《民法典》第 1035 条第 1 款规定，处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理。

据此，贺小荣表示，App 运营商在提供某 App 下载服务时，依法不得收集与该应用软件无关的个人信息，否则便构成违法。个人若在下载 App 过程中被收集与该应用软件无关的信息，提起诉讼要求删除相关个人信息的，人民法院将依法予以支持。

同时，他也提到，为公共利益需要，适度处理个人信息依法免责。依据《民法典》第 1036 条第 3 项的相关规定，为维护公共利益，合理处理个人信息的，行为人不承担民事责任。

他强调，由于公共利益涉及国家利益和不特定多数人的利益，为了公共利益整体考虑，个人的权利应当受到适当限制。当然，公共利益是个弹性极大的概念，为避免滥用，应当严格限制适用范围，而为了公众的健康安全需要，则无疑属于公共利益的范畴。

贺小荣举例称，在我国去年抗击新冠肺炎疫情的过程中，政府主管职能部门运用大数据技术，及时准确搜索患者的每一个接触者，并采取适当的安全隔离措施，最终取得抗击新冠肺炎疫情的胜利，表明我国关于个人信息权益保护和维护公共利益之间平衡的法律制度，具有相当的科学性和合理性，应继续坚持。



在贺小荣看来，净化网络空间，需要各方共同努力。就政府主管部门而言，2019 年 11 月，中央网信办、工信部、公安部和市场监管总局四部门联合启动开展 App 违法违规收集使用个人信息专项治理工作，制定印发了《App 违法违规收集使用个人信息行为认定方法》《App 违法违规收集使用个人信息自评估指南》，对用户规模大、问题突出的 260 款 App，有关部门采取曝光、约谈、下架等措施。

就 App 运营商而言，应当秉持法治意识，自觉遵守法律规定运营，自行整改违法违约的运营模式，否则将承担相应的法律责任。就自然人个人而言，也应当具有依法维权意识，对于违规收集个人信息的 App,应当有意识地收集证据，及时投诉或者举报，并可以依法提起诉讼，人民法院将依法维护自然人的合法权益。

保护外卖、快递小哥的权益

互联网平台经济快速发展，新业态用工法律关系、外卖快递员权益保障等问题引发社会

各界广泛关注。访谈中贺小荣坦言，“技术前进一小步，管理难度增加一大步。互联网平台经济是近年来发展迅猛的新的经济组织方式，对于优化资源配置、推动产业升级、拓展消费市场尤其是增加就业，都有重要作用。特别在抗击新冠肺炎疫情中，互联网平台发挥了不可替代的积极作用，成为推动我国经济社会发展的重要力量”。

据不完全统计，目前全国外卖骑手达到了 600 万（美团、饿了么、闪送等），快递员从业人员约 350 万，滴滴驾驶员 270 万。每一个骑手、快递员的背后都是一个家庭，因此保护这些从业者的合法权益尤为重要。

贺小荣表示，新的经济业态，必然会产生新的矛盾纠纷。当前，面对互联网平台用工引发的大量纠纷案件，依法保护平台从业者的合法权益。“平台从业者与传统劳动者不同，他们没有固定的工作场所和工作时间，工作安排相对自由，工作场所流动，劳动时间和劳动空间趋向松散”。

因此，贺小荣表示，“人民法院审理相关案件时，对于平台与从业者之间能否构成劳动关系，要根据劳动者的工作时长、工作频次、工作场所、报酬结算、劳动工具等，企业对劳动者的监督管理程度、惩戒措施等因素来综合认定。构成劳动关系的，应当依法保障这部分人的劳动者相关待遇”。前段时间发生了骑手发生交通事故造成第三人损害等事件，贺小荣称，这表明新业态用工制度亟待规范。我们在司法政策制定或者案件审理过程中，一方面要依法认定劳动关系或者劳务派遣关系，同时也要引导平台企业落实好安全保障责任，通过购买从业相关保险等方式分担损失。贺小荣还透露，下一步，最高人民法院将在广泛调研和听取社会各界意见的基础上，制定出台审理外卖快递等相关案件的司法解释。

法律护航“良善之举”

“理念是行动的先导，任何一个国家的司法裁判都是在其价值观的指导下作出的。当法官将抽象的法律条文与具体的案件事实相连接时，其信仰和遵循的价值观将起着十分重要的作用”。贺小荣表示，近年来，最高人民法院高度重视社会主义核心价值观对人民法院审判工作的指引作用。据其介绍，自 2016 年以来，最高人民法院先后发布四批弘扬社会主义核心价值观的典型案例，涵盖家庭美德、社会公德、英烈保护、公序良俗、友善互助、诚实信用、环境保护等各个方面，通过这些典型案例的释法说理弘扬真善美、鞭笞假丑恶，赢得普遍社会赞誉。

贺小荣表示，近年来，从惩戒“老赖”助推诚信社会建设，到整治“霸座”“抢公交车方向盘”树立规矩意识；从办理维护英雄烈士荣誉、名誉案件，到强调过错责任、反对“和稀泥”……一个个生动案例有效树立了社会新风尚，凝聚了中华民族“精气神”。

浙江省宁波市北区人民法院审判了一个“照顾邻居分得一半遗产案”，现场连线了承办法官张海娟。张海娟法官表示，“远亲不如近邻！本案的老徐照顾邻居老人长达几十年，实在是难能可贵，不管于理于情于法都应予以肯定。而且，《民法典》第 1131 条也规定，继承人以外的对被继承人扶养较多的人，可以分给适当的遗产。表明本案的调解结果完全符合法律的规定。我们认为，对于邻居老徐的弘德扬善之举，人民法院应当从弘扬社会主义核心价值观的角度，进行正向激励，树立价值导向。”

贺小荣表示，弘扬社会主义核心价值观是人民法院司法裁判的永恒主题和价值追求。我国民法典第一条开宗明义，将弘扬社会主义核心价值观作为制定民法典的目的。

比如，《民法典》第 184 条规定的“好人条款”，该条规定，“因自愿实施紧急救助行为造成受助人损害的，救助人不承担民事责任。”贺小荣举例称，最近，济南中院审理的“代接朋友孩子意外造成损伤免赔案”。张女士骑电动车替朋友接孩子，将朋友的孩子安排在座位上，而自己的孩子站在脚踏板上，这种“先人后己”的体贴做法，可以说“仁至义尽”，且朋友也确认这是一起意外，尽管后座孩子因摔伤用去医疗费 7757.04 元，一审判赔 5000 多元，二审改判免赔。贺小荣强调，当一个法官在判断一种行为是否违背公序良俗时，就需要法官运用自身的知识、经验和价值观来判断何为“善良风俗”、何为“好人”、何为“善举”。

（来源：新浪科技）

➢ 商业银行隐私与数据保护实施路径探析

当前“后大数据时代”，个人隐私与数据保护问题已上升至国家高度。2020 年 10 月召开的“十三届全国人大常委会第二十二次会议”对《中华人民共和国个人信息保护法（草案）》进行了初次审议，并已公开征求社会意见。中国的隐私与数据保护立法时代已经开启。在此时代背景下，商业银行如何建立全面有效的个人信息保护体系，做好充分准备来迎接我国《个人信息保护法》的正式生效，已成为亟待解决的重要问题。本文面向《个人信息保护法（草案）》提出 8“O”解读视角，并立足于商业银行实践提出“POSTER”框架，以期为国内同业隐私与数据保护实践提供有益的探索。

《个人信息保护法（草案）》背景及简介

个人隐私权的概念最早于 1890 年由美国法学界提出，进入信息化时代后，隐私权赋予了自然人控制、管理、披露和保护自己个人信息的权利。全球 130 多个国家相继出台了专项

法律法规。2016 年欧盟发布了《通用数据保护条例》（简称“GDPR”），并于 2018 年 5 月生效，因其具备内容全面、要求严格、处罚严厉等特征，成为各国个人信息保护立法的参照典范。

我国的《中华人民共和国民法典》已于 2021 年 1 月 1 日正式实施，其中明确了对个人隐私、个人信息以及个人数据的保护原则及立场。《个人信息保护法》将是个人信息和隐私保护领域中与民法典相配套和并行的法律，运用民事、行政、刑事等综合性手段对个人信息加以保护。草案编写过程中，参考了国内外相关经验与实践，目前虽然处于审议阶段，但草案具有一定的成熟度，可作为各类机构、组织、企业提前进行个人信息保护合规的参考依据。

基于 8“O”视角的《个人信息保护法（草案）》要点解读

本次提交的草案共八章七十条，内容详实。文本基于 8“O”视角进行解读，将需要重点关注的内容明确如下。

1.保护对象及适用范围（Object）。保护对象为中华人民共和国境内自然人。适用范围包括在中华人民共和国境内处理自然人个人信息的活动，以及在境外向境内个人提供产品或服务或者分析、评估境内个人行为的活动。

2.明确个人信息处理的基本规则（Operation）。确立了以“告知—同意”为核心的个人信息处理一系列规则，处理个人信息应当采用合法、正当的方式，遵循诚信原则，处理限于实现处理目的的最小范围，公开处理规则等。

3.明确个人作为信息主体的权利（Ownership）。草案对个人的各项权利进行了明确，包括知情权、决定权、查询权、更正权、删除权等。

4.明确信息处理者的义务（Obligation）。信息处理者须采取必要的管理、技术、监督措施确保个人信息处理活动符合法规规定，防止未经授权的访问以及个人信息泄露或被窃取、篡改、删除等。

5.对敏感个人信息、未成年人信息、个人公开信息等进行了额外规定（Other Rules）。草案规定处理敏感信息时需特别向个人告知处理的必要性和影响；处理不满 14 周岁未成年人个人信息，应当取得其监护人的同意；处理已公开的个人信息，应当符合该信息被公开时的用途。

6.数据境内存储以及出境要求（Overseas）。应当将在中华人民共和国境内收集和产生的个人信息存储在境内，确需向境外提供个人信息，应当通过国家网信部门组织的安全评估。

7.延续多头监管的格局（Ongoing Regulation）。明确国家网信部门负责个人信息保护工作的统筹协调，国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。

8.处罚形式多样，惩处力度加大，并记入信用记录（On record）。处罚形式包括责令改正、没收违法所得、给予警告、罚款、责令暂停业务、停业整顿、吊销业务许可或营业执照、治安处罚和刑事处罚等，并且违反行为将记入信用档案，予以公示。

综上，《个人信息保护法（草案）》旨在为我国个人信息的处理、共享、应用等方面建立全面的法律约束和屏障。

商业银行个人信息保护合规依据及参考

银行业金融机构须满足央行、银保监会的行业监管要求，并符合我国相关国家法规、标准等。目前已生效的主要法律、规范等参见表 1。

表 1 商业银行需遵守的主要个人信息保护法律、规范、标准

制定方	法律/规范/标准名称	实施日期
全国人大常委会	《中华人民共和国消费者权益保护法》	1994 年 1 月 1 日
	《中华人民共和国反洗钱法》	2007 年 1 月 1 日
	《中华人民共和国民法典》	2021 年 1 月 1 日
国家互联网信息办公室（网信办）	《金融信息服务管理规定》	2019 年 2 月 1 日
中国人民银行	《中华人民共和国金融行业标准 JR/T 0171—2020 个人金融信息保护技术规范》	2020 年 2 月 13 日
银保监会	《银保监会关于银行保险机构加强消费者权益保护工作体制机制建设的指导意见》	2019 年 11 月 2 日
国家市场监督管理总局、国家标准化管理委员会	《中华人民共和国国家标准 GB/T 35273—2020 个人信息安全规范》	2020 年 10 月 1 日
	《中华人民共和国国家标准 GB/T 36618—2018 信息安全技术金融信息服务安全规范》	2019 年 4 月 1 日

商业银行个人信息保护体系“POSTER”框架

以中国人民银行《中华人民共和国金融行业标准 JR/T0171—2020 个人金融信息保护技术规范》为目标，借鉴银保监会的《关于银行保险机构加强消费者权益保护工作体制机制建设的指导意见》，本文将商业银行的个人信息保护工作概括为图 1 中所示的“POSTER”框架。

图 1 个人信息保护管理体系——“POSTER”框架

1.Policy&Protection，隐私策略及个人信息保护体系。（1）对内：建立自上而下的治理管控体系。制定全行的个人信息保护政策及规划，建立个人信息保护委员会，指派牵头管理部门及专职管理人员，建立自上而下、由内而外的全面个人信息保护体系。（2）对外：树立良好的保护形象，明确委托关系中的权责边界。一方面，完善和优化银行各种个人信息收集渠道中的隐私声明，达到隐私声明的信息完备的同时，提高可读性和用户友好程度。另一方面，对数据处理委托的业务和委托方进行梳理，加强对信息处理委托方的约束和监督。

2.Operation&Awareness，将个人信息保护融入全员意识和运营操作当中。（1）将个人信息保护在业务操作中进行落地。将个人信息保护的具体要求结合各岗位操作特点融入各操作流程及规范中，并纳入员工考核内容。（2）提升全员的个人信息保护意识。进行个人信息保护专业人员培养，并将个人信息保护纳入全行全员常态化意识培训内容中。特别需要说明的是，个人信息保护不仅是对客户的信息进行保护，也包括对本行员工、服务提供商、合作伙伴等个人信息进行保护，需将个人信息保护体现在各个管理细节中。

3.Standard Certification，开展国际、国内标准认证。（1）持续对标国际相关标准。目前与个人信息保护相关的国际标准主要有《ISO/IEC29151：2017 信息技术—安全技术—个人身份信息保护实务准则》《ISO/IEC27701：2019 安全技术—ISO/IEC27001 与 ISO/IEC27002 隐私信息管理的扩展—安全与指南》等。（2）满足国内相关标准与认证。我国的国家标准《中华人民共和国国家标准 GB/T35273—2020 个人信息安全规范》、金融业标准《中华人民共和国金融行业标准 JR/T0171—2020 个人金融信息保护技术规范》已发布。

4.Techniques&Tools，个人信息保护技术与工具的研发。（1）信息处理技术的研究与应用。大数据背景下的数据保护技术已处于研究和实践中，如：联邦学习、多方安全计算技术等。在保证数据安全性方面，系统和数据的抗攻击技术也有很大研究空间。（2）个人信息保护工作的相关工具。个人信息及个人数据保护过程中需要依赖各种管理工具和技术工具，才能实现对数据的有效管理、控制与保护。常用工具总结如下（见表 2）。

表 2 个人信息保护工作中的相关工具

类型	工具	主要功能
管理类	隐私趋势与法规管理工具	提供及时更新的国家以及全球隐私保护动态和相关法律法规要求
	隐私保护工作管理工具	实现并记录个人信息保护工作“计划、执行、监督、反馈”闭环，为银行提供个人信息保护工作的有效证明
评估类	评估管理平台工具	开展定期的、持续的隐私影响评估及合规风险评估等
	隐私风险评估工具	识别、分析个人数据的风险，以制定合理的保护措施及风险应对措施
权益保障类	用户授权管理工具	记录、维护用户对数据使用的同意授权，实现可选择、可撤销、可更新的用户同意
	网站工具	管理 cookies 设置、APP 授权等
事件管理类	数据泄露事件响应工具	及时发现、响应数据泄露风险及事件，快速控制影响范围，及时上报监管，以及妥善进行客户沟通
	行为监控、身份保护工具	对可能已泄露的数据，监控网络中的个人信息售卖、身份冒用、盗用行为，保护客户权益
数据技术类	数据映射工具	通过手动或自动表单填写来帮企业勾勒出数据流图，实现数据全生命周期的可控处理
	数据防泄露工具	监控个人信息被谁访问，做了什么操作，并提供阻断等控制措施
	数据发现工具	扫描数据，根据规则进行分级分类，便于企业梳理存量数据，作为隐私风险合规及管控的基础
	反识别 / 匿名化 / 脱敏工具	对个人数据实现脱敏保护，对沉淀数据实现匿名化保护，实现数据可用不可见

5.Emergency Reaction，建立对信息安全事件的高效应对能力。（1）数据泄露事件的及时响应和处置能力。将数据泄露事件作为信息安全事件中的重要一类，在全行形成高效的事件评估与决策机制，以及覆盖行内的业务、科技、客服、品牌等部门和行外的合作伙伴、关联机构、主要媒体等全面联动事件应对预案。（2）适时适度进行数据泄露事件的沟通与披露。对于可能对个人产生较大风险的数据泄露，及时采用有效沟通渠道与受影响的个人沟通事件的性质、可能的影响、已采取的措施等信息，并提供风险防范的协助与支持。

6.Regulator Communication，与监管部门的积极沟通。（1）紧跟监管机构的法规和监管动态。近几年我国个人信息保护法规和标准密集发布，逐步形成与《个人信息保护法》配套的法制强监管体系。商业银行应进行监管法规的跟踪、解读和预判，及时为行内个人信息保护的规划和执行工作提供建议和依据。

由于我国个人信息保护多头监管的格局，因此商业银行应关注多个相关机构的监管政策和行动进展动态，及时满足和回应各监管部门的相关工作要求。

（2）进行积极的监管沟通。根据相关法规要求，作为收集和处理大量个人信息的金融机构，商业银行应指定个人信息保护责任人和责任机构，并在多种业务场景下积极向监管部门进行上报和咨询。

结语

个人信息保护是一项综合、复杂、长期的工作，需要纳入商业银行的治理框架中，融入日常管理、运营、监督审计等过程中。各商业银行亟待完善个人信息保护体系，以迎接我国个人信息保护的法治与强监管时代。（作者：金融电子化）

➢ 《个人信息保护法（草案）》的立法评析与完善思考

2020 年 10 月 21 日，《个人信息保护法（草案）》（以下简称草案）在中国人大网正式向社会公布并征求意见。继个人信息保护相关规定散布于《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国刑法》《消费者权益保护法》《网络安全法》《民法典》等法律法规之后，我国即将迈入个人信息保护专门立法、统一规范的新时代。在全球数字经济迅猛发展，国际社会围绕数据控制力与主导权的博弈日趋激烈，国内加快培育数据要素市场的背景下，草案是具有中国特色个人信息保护思路的集中体现。草案对个人信息的处理规则、个人权利和处理者义务、跨境流动、监督管理、侵权救济、法律责任等作出了明确规定，为数字时代的个人信息权益保护、个人信息有序、自由流动确立了基本框架。

一、《个人信息保护法（草案）》的中国特色

近年来，在国外欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）掀起的全球个人信息保护立法浪潮盛行，国内个人信息非法采集、滥用、泄露等形势严峻的背景下， 我国不断强化对个人信息保护的监管与执法力度，并进行制度探索。

一方面，国家相关立法快速推进，《网络安全法》《民法典》相继出台，在基本法层面构

建了个人信息保护的行政和民事基本规范。另一方面，部门规范、地方规范、标准规范等自下而上的制度探索全面展开。国家互联网信息办公室相继发布《数据安全管理办法（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》。地方层面围绕数据跨境、数据安全保障、数据开放、数据权等问题积极先试先行，典型如《天津市数据安全管理办法（暂行）》《贵州省大数据安全保障条例》《深圳经济特区数据条例（征求意见稿）》《中国（上海）自由贸易试验区临港新片区总体方案的通知》《海南自由贸易港建设总体方案》等。标准规范层面，国家标准《信息安全技术 个人信息安全规范》出台并实施， 充分发挥标准与行业的良性互动作用。

在个人信息保护执法层面，围绕个人信息非法采集和滥用、数据三性破坏等活动的数据安全专项治理行动空前有力。App 违法违规收集使用个人信息专项治理行动全面展开，公安部、市场监管总局、工信部、网信办等部门充分发挥监管、主管职责开展个人信息保护专项行动。为保持对侵犯公民个人信息违法犯罪的高压严打态势，形成源头治理、综合治理、系统治理的工作格局，2020 年 4 月，经中央领导批准，公安部与中央网信办牵头，建立打击危害公民个人信息和数据安全违法犯罪长效机制。

正是在这样的背景下，我国《个人信息保护法（草案）》出台。从现有规定来看，草案吸收了近年来个人信息保护的国际经验以及国内前期《网络安全法》《民法典》等立法、标准和实践经验，使得草案既与国际接轨，又不乏中国特色。尤其是与欧盟 GDPR 相比，草案在个人信息处理的合法性基础、信息主体权利、个人信息处理者义务的规范方面引入了欧盟 GDPR 的理念和相关规定，但同时也具有鲜明的中国特色：

第一，以“个人信息处理者为中心”的监管思路。GDPR 从概念上对数据控制者和数据处理者进行区分，并分别对其设置了个人信息保护义务。草案中的委托方、受托方基本对应于 GDPR 中界定的数据控制者和数据处理者概念。但与 GDPR 对数据处理者同样设置个人信息保护义务的规定不同，草案将个人信息保护义务集中于“个人信息处理者”，明确个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全（第 9 条）。草案还设专章规定个人信息处理者义务（第 5 章）。根据草案第 69 条的规定，“个人信息处理者”是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人。根据这一界定， 不能自主决定处理目的、处理方式的受托者并不属于“个人信息处理者”。从这一立法思路来看，所有的监管均围绕“个人信息处理者”为中心展开。

第二，数据本地存储和跨境提供问题。跨境数据流动已经成为时代发展的必然要求。但与此同时，其所带来的隐私保护问题、数据主权问题、国家安全问题使得各国在此问题上存在诸多分歧，不同主权国家法治传统与制度环境的差异导致跨境数据流动的规制冲突日益严重。据美国信息技术创新基金 2017 年 4 月统计， 除信息化水平较低的非洲外，绝大多数国家均已实施了不同程度的数据本地化政策。数据本地存储和跨境提供是《网络安全法》诸多制度设计中一直难以落地的关键问题之一。草案细化了个人信息本地化和跨境传输的要求，目前规定的部分内容突破了《网络安全法》第 37 条规定，本地存储的义务主体既包括国家机关、关键信息基础设施运营者，还包括处理个人信息达到规定数量的个人信息处理者。

二、制度定位：保障个体权益兼顾数据要素市场培育

个人数据作为大数据的重要基础资源，具有重大的商业价值和社会价值。在个人信息保护立法过程中，“不同于传统隐私权从个体出发为个体提供单一向度的权利保护，个人信息需要从保护和利用两个角度兼得的视角加以考量”。其是在中央将数据与土地、资本、劳动力、技术并列为五大生产要素的背景下，个人信息保护立法应当在关注个人信息人格属性保障的同时，兼顾其经济价值和社会价值的释放，为数据要素市场化建设提供制度支撑。从全球范围来看，无论是欧盟的 GDPR 还是美国《加州消费者隐私法》（California Consumer Privacy Act，CCPA）的规则设计，其在考虑对信息主体进行保护的同时，也将数字经济发展作为重

要考量因素之一。这要求立法的制度建设需从增强用户（信息主体）信任和企业激励机制两个维度着手。

从草案目前版本来看，立法者已经注意到了这一点，并在部分制度建设中有意平衡个体权利保护和企业责任承担之间的关系。例如草案在“知情—同意”之外增加了“为订立或者履行个人作为一方当事人的合同所必需”等其他四项个人信息处理的合法性基础。在数据泄露通知方面，规定个人信息处理者采取措施能够有效避免信息泄露造成损害的，可以不通知个人，这大大降低了企业的通知成本。但草案仍存在以下问题亟待解决：

第一，部分场景仍坚持“同意为王”的治理模式。个人信息保护制度中的“知情—同意”框架偏向于通过信息主体自治以保护个人信息，这一路径选择对信息的合理流通和利用构成了严苛的限制，实践中也存在形式化问题。此外，过于严苛的“同意”规则会造成数据企业经营成本的增加，制约数据经济的发展。在此背景下，各国纷纷开始重新审视同意规则在个人数据保护中的实际效用，探索新时代语境下同意规则的合理性及适用问题。

从当前国际通行做法来看，增强信息主体对个人信息的控制力、重视对信息处理者的过程规制、强化事后问责都是可行路径。草案也在很大程度上秉承了这一监管理念。值得肯定的是，草案在个人信息处理的合法性基础方面，除了规定同意之外还增加了其他合法事由，这在一定程度上可缓解当前真正的同意难以实现，反而可能为个人信息处理者提供免责事由损害信息主体利益的情况。

但需要指出的是，草案在诸多场景下， 仍然实质上坚持用户“同意为王”的治理模式。例如个人信息处理者因合并、分立场景下，接收方变更原先的处理目的、处理方式的（草案第 23 条）、接收个人信息的第三方变更原先的处理目的、处理方式的（草案第 24 条）、个人信息的公开（草案第 26 条）等。

第二，缺乏对个人信息处理者“合法利益”的保障。在数据要素化背景下，在不侵犯信息主体基本权利及自由的前提下，立法上承认个人信息处理者对其处理的个人信息享有合法利益，对于激励企业挖掘数据潜能具有重要意义， 也是《个人信息保护法（草案）》在保障个体权益的同时，为数据要素市场化建设提供的重要制度支撑。在个人信息处理者对个人信息处理投入大量的人力、物力、财力的现实情况下，信息处理者对此类衍生数据享有一定的合法利益具有立法上的正当性。这一点在国际立法上也有例可考，如欧盟 GDPR 将“数据控制者或第三方为追求合法利益目的而进行的必要数据处理”作为数据处理的合法基础之一。

第三，未区分“去标识化”个人信息与一般个人信息处理规则。当前“匿名化”“去标

识化”在数据处理中广泛应用。草案对“匿名化”“去标识化”作出了明确界定，并规定匿名化的信息不再属于个人信息。但对于“去标识化”的法律效果并没有作出与一般个人信息处理规则不一样的规定。在实践中，“匿名化”往往难以实现，使得去标识化作为一种安全技术应用得更为广泛。“去标识化”个人信息在不借助额外信息的情况下无法识别特定自然人的特点决定了其与一般个人信息存在较大差别。立法对其处理规则未做特殊规定，忽视了二者之间的差异， 一方面可能会导致个人信息保护效果适得其反， 如已去标识的个人信息要求获得信息主体的同意意味着再次对信息主体进行识别。另一方面也难以对企业进行去标识化处理形成激励效应。

三、体系定位：做好规范体系协调

我国个人信息法律保护近年来发展迅速，早期个人信息保护领域《中华人民共和国刑法》先行，而民事、行政立法薄弱的问题得以缓解，尤其是随着《网络安全法》《民法典》的出台， 个人信息保护的民事、行政立法逐渐充实。在学术界，由于个人信息的特殊性质，个人信息保护近年来成为不同法律部门与理论研究的热点，也产生很多争议，包括个人信息保护的本质究竟是权利还是权益，个人信息的权益属性究竟是人格权还是财产权，《民法典》人格权编与个人信息保护法的关系，个人信息民法保护、行政法保护与刑法保护之间的关系等。个人信息保护法即将出台，该法如何与《民法典》《网络安全法》《中华人民共和国刑法》以及未来即将出台的《数据安全法》等立法进行有效衔接与协调，都是当前亟待解决的问题。

3.1 与《民法典》的协调

作为民事领域的基础性法律，《民法典》将个人信息保护问题纳入“人格权编”，并对个人信息处理规则、合理使用、责任承担等作出明确规定，为个人信息作为“人格利益”予以保护以及保护机制提供重要依据。作为一部以保护“个人信息权益”为重要目标的立法，如何与《民法典》进行规范性协调是个人信息保护法面临的一个核心问题。

草案诸多条款以《民法典》的规则为基础，例如个人信息共同处理者的连带责任就是以民事共同侵权理论为基础；个人信息处理委托方与受托方、转委托规则也以民事委托合同规则为基础；侵犯个人信息权益的赔偿标准是因人身权益受侵害遭受财产损失的赔偿标准，等等。与《数据安全法》《网络安全法》更加侧重国家安全与公共安全不同，草案更加侧重对个体个人信息权益的保障。例如草案确立的以个人“知情—同意”为核心的数据处理规则。专章规定的个人权利，对应的个人信息处理义务章节也是以保护个人信息权益为导向。草案还采用了《民法典》“个人信息处理”的概念，遵循了《民法典》确定的信息处理者管理思路。

从这一角度看，可以说，草案是以《民法典》所确立的个人信息民事权益为基础，从国家监管角度， 用公权力细化、落实个人信息民事合法权益的保障法。基于此，草案的许多规定还需要与《民法典》相协调。例如目前草案第 15 条规定的“以 14 岁为界”需要与《民法典》第 1035 条进一步协调。同时，“敏感信息”处理规则如何与《民法典》中的“私密信息”规定进行协调也是需要考虑的问题。此外，公开个人信息的处理规则也需要注意与《民法典》相关规定的有效衔接。

3.2 与《网络安全法》《数据安全法》等的协调

作为网络安全领域的综合性立法，2017 年《网络安全法》将数据安全纳入网络安全范畴， 基于网络安全保障目的，为个人信息保护与数据安全的部分重要、核心制度奠定了基础。《网络安全法》施行已经三年有余，国际国内形势变化、新技术新应用发展都对数据安全和个人信息保护问题提出了非常迫切的法律要求。从国家顶层设计来看，《网络安全法》《数据安全法》，以及正在制定的个人信息保护法将是支撑国家网络安全保障工作的重要支柱。

当前，草案部分规定与《网络安全法》存在需要协调之处。例如草案第 62 条违反处理个人信息规则的行政处罚规定与《网络安全法》第 64 条网络运营者和网络产品服务提供者违反个人信息处理规定设定的行政处罚在处罚条件、罚款最高额度方面的规定皆不相同，二者发生竞合时如何适用？草案确立的数据本地化与跨境流动规则与《网络安全法》第 37 条规定的不一致，未来将如何协调？草案第 40 条将关键信息基础设施运营者与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并列，未来在关键信息基础设施的认定中，系统中的“个人信息”数量是否将成为认定关键信息基础设施的考量因素以及如何适用这一标准则需要与本条衔接协调。此外，还需做好个人信息安全评估、认证与其他网络安全检测、认证、评估之间的内容衔接，尽可能避免重复检测、认证和评估。

除个人权益保障之外，草案也注意到了个人信息处理对公共安全、国家安全乃至国际竞争的影响。如草案第 10 条禁止性规定，纳入了国家安全和公共安全的考量因素，第 41 条关于国际执法协助规定，第 42 条规定个人信息提供负面清单制度；基于公共安全和国家安全的考量，可以实施第 43 条对等原则。上述规定与《数据安全法（草案）》在规制思路上存在相似之处但也有所差异。与《数据安全法（草案）》第 33 条国际执法协助的规定相比，草案还增加了行政执法协助的规定，这些差异都需要在两部立法的制定过程中予以协调。

3.3 与《中华人民共和国刑法》的协调

大数据时代的到来，使得对个人数据的法律保护面临重大的冲击。无论是作为整体的法

律体系还是作为部门法的刑法，都莫不如此。因此，无论是正在制定中的个人信息保护法还是已实施许久的刑法，在相应的规则制定或落实中都应当着眼于整个法律体系走向，置于整个立法体系的视野之中予以考虑。

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称两高解释）将“未经被收集者同意，将合法收集的公民个人信息向他人提供的”认定为“违反国家有关规定，提供公民个人信息”的行为。随着草案在同意之外增加了其他几项合法处理的事由，上述提供行为是否必然属于非法提供还需根据具体情况来进行判定。虽然草案第 24 条对个人信息处理者向第三方提供行为仍然坚持同意规则，并要求单独同意。但该条本身与第 13 条合法性基础的规定存在逻辑上不能自洽的问题。

此外，两高解释对行踪轨迹信息、通信内容、征信信息与财产信息这四类信息的定罪情节作出了不同于一般个人信息的从严要求，但没有对生物数据等更为敏感的个人信息给予更高程度的刑法保护。这一点如何与草案规定的包括“种族、民族、宗教信仰、个人生物特征”等在内的敏感个人信息保护规则进行协调也需要通盘考虑。

四、完善思考

4.1 明确监管部门权责分工，避免多头监管

草案第 56 条明确国家网信部门负责个人信息保护工作的统筹协调，同时规定，国家网信部门和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。其规定未能解决网络安全保护、数据安全治理领域长期存在的监管体制机制问题，建议进一步明确各监管部门之间的权责分工和界限，避免立法施行后因权力范围重叠出现管理和执法尺度不一，影响个人信息保护监管执法的实际效能。

4.2 细化罚款标准，避免执法主体自由裁量幅度过大

草案第 62 条规定了个人信息违法处理的法律责任，其处罚规则借鉴了欧盟 GDPR 的监管思路。为惩治个人信息违法处理乱象，加强法律惩治力度，增加违法成本的做法值得肯定。但现有规定在最高额五千万元以下或者上一年度营业额百分之五以下罚款的幅度内，未能确立相对明确、细化的罚款等级标准，给予监管部门自由裁量空间过大，可能会带来执法上的诸多问题。

4.3 敏感个人信息的界定应当纳入动态评估因素

将“敏感个人信息”予以特殊保护是当前国际通行做法，如何设计敏感个人信息的处理规则以平衡个人信息保护与利用的关系是立法亟须解决的问题。草案第二章第二节专门规定“敏感个人信息的处理规则”，第 29 条界定了敏感个人信息的内涵与外延。事实上，个人

敏感信息的判定基于风险评估，在不同的场景、不同的行业、不同的适用条件下很难统一作立法上的区分。

正如西米蒂斯（Simitis）教授所言：“所有数据信息的评估都必须建立在充分考虑其使用背景的基础上。数据控制者的特定利益、数据的潜在接受者、收集数据的目的、收集数据的条件以及可能对数据主体产生的影响等整个数据处理过程中的因素要综合起来进行考察，以此确定相关信息的敏感程度。”因此， 敏感个人信息的界定应当是一个动态评估的过程，建议采用“列举+动态评估”规则。此外，个人敏感信息的界定与适用还需考虑与《民法典》《网络安全法》《中华人民共和国刑法》及其司法解释中的相关概念之间的协调，实现民法、行政法与刑法在个人信息保护上的一体化衔接。

4.4 自动化决策重大影响判定宜采用客观标准

草案第 25 条明确了利用个人信息进行自动化决策的要求，强调自动化决策的透明度和处理结果的公平合理，并规定了个人的救济途径。当前，自动化决策技术广泛应用于商业经营及社会治理中具有巨大的经济价值和社会价值。与此同时也对人的主体性、公平性等带来挑战。鉴于自动化决策中也会涉及个人信息的利用， 立法确需在自动化决策应用中平衡个体权益、商业利益和社会公共利益。基于此，草案第 25 条自动化决策是否会“对个人权益造成重大影响”的判定宜采用客观标准，而不宜采用当前条款中类似“个人认为”的主观标准。

五、结论

自 2012 年全国人大常委会通过《关于加强网络信息保护的决定》以来，我国无论数据产业还是数据规范都取得了突飞猛进的发展。此次发布的《个人信息保护法（草案）》也在一定程度上体现了对近年来立法、执法等经验的总结，回应了产业发展的现实需求。但仍可以注意到，目前的版本在数据处理合法性基础、监管机制设置、敏感数据保护等制度构建上有待进一步完善。在中央将数据作为生产要素的背景下，个人信息保护立法应在关注个人信息人格属性保障的同时，兼顾其经济价值和社会价值的释放，为数据要素市场化建设提供制度支撑。在当前已出台《网络安全法》《民法典》，未来还将出台《数据安全法》的背景下，个人信息保护立法应做好不同立法间的规范协调，推动构建个人信息保护刑事、行政、民事全方位法律保护体系。（来源：信息安全与通信保密）

四、政府之声

➢ 个人信息频频泄露，工信部：拒不接受整治的 App 要坚决下架

2021 年 3 月 1 日上午，在国务院新闻办举行的工业和信息化发展情况新闻发布会上，工信部相关负责人表示，2020 年工信部对手机 App 开展了专项整治，可能是个人信息保护得最好的一年。今年将会继续整治，对拒不接受整治的 App 要坚决下架。

工信部介绍，目前个人信息应用丰富多彩，手机 App 的数量非常大，保守估计在 250 万以上，在此过程中，个人信息保护方面需要迅速加强、提高。2020 年，工信部对群众反映强烈的问题进行了专项整治，总体来讲效果比较明显。2021 年，工信部将继续延续这样的整治，尤其是群众反映的重点领域，坚持“最小可用”的原则来处理 App 的发展过程，对拒不接受整治的 App 要坚决下架。同时，在监管方面，要提高技术装备的能力，首先要确保能够检测出信息保护的漏洞，以及对广告信息有效拦截。

在备受关注的 5G 网络建设上，工信部表示，到 2020 年底，累计开通 5G 基站 71.8 万个，5G 手机终端连接数突破 2 亿户;IPv6 规模部署纵深推进，活跃连接数达到 13.9 亿，4G 网络 IPv6 流量占比从无到有，超过 15%，今年继续有序推进 5G 网络建设，加快 6G 的布局，推动网络优化的升级，确保网络安全。在宽带普及上，工信部数据则显示，截至 2020 年底，我国固定宽带家庭普及率已达到 96%，移动宽带用户普及率达到 108%。（来源：央视新闻）

➢ 中国人民银行发布《金融业数据能力建设指引》

2021 年 2 月 9 日，中国人民银行正式发布《金融业数据能力建设指引》（JR/T0218—2021，以下简称《指引》）金融行业标准。

《指引》规定了数据战略、数据治理、数据架构、数据规范、数据保护、数据质量、数据应用、数据生存周期管理能力域划分，明确了相关能力项，提出了每个能力项的建设目标和思路。《指引》的发布有助于引导金融机构深挖数据要素潜能，全面提升数据管理和应用水平，切实将数据规划好、治理好、应用好、保护好。

本标准由全国金融标准化技术委员会归口管理，由中国人民银行科技司提出并负责起草，行业内有关单位共同参与。标准经过广泛征求意见和论证，并通过了全国金融标准化技术委员会审查。（来源：中国人民银行）

- **《金融业数据能力建设指引》（JR/T0218—2021）**
- **全文：**http://www.cfstc.org/bzgk

➢ 重庆市 6 部门联合印发《重庆市工业信息安全管理实施办法（试行）》

2021 年 2 月 8 日，重庆市经济和信息化委员会、中共重庆市委网络安全和信息化委员会办公室、重庆市公安局、重庆市应急管理局、重庆市通信管理局、重庆市密码管理局 6 个部门关于印发重庆市工业信息安全管理实施 办法（试行）的通知渝经信规范〔2021〕1 号。

通知要求：各区县（自治县）人民政府，市政府有关部门，有关单位：为贯彻落实《中

华人民共和国网络安全法》、《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168 号），建立健全工业信息安全工作机制，加强工业信息安全指导、监督和管理工作，我们制定了《重庆市工业信息安全管理实施办法（试行）》，经市政府同意，现印发给你们，请认真贯彻实施。

《重庆市工业信息安全管理实施办法（试行）》：主要为加强全市工业信息安全保障和应急管理工作，落实企业工业信息安全主体责任，加快构建工业信息安全保障和应急体系，建立健全工业信息安全工作机制，提高应对工业信息安全事件的组织协调和应急处置能力，依据《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》《中华人民共和国密码法》《国务院关于深化制造业与互联网融合发展的指导意见》《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》，以及工业和信息化部等十部门《加强工业互联网安全工作的指导意见》、工业和信息化部《工业控制系统信息安全事件应急管理工作指南》等法规政策，制定本办法。（来源：重庆市经济和信息化委员会）

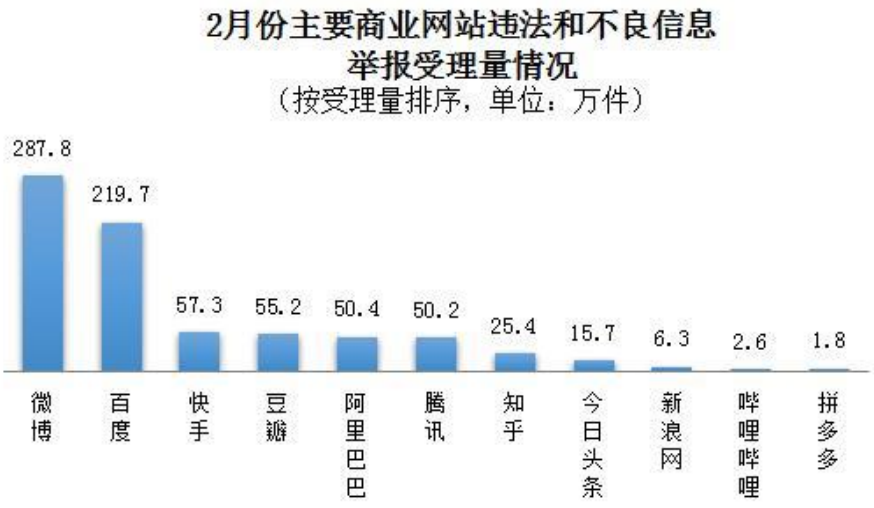
- **重庆市工业信息安全管理实施办法（试行）**
- **全文：**https://jjxxw.cq.gov.cn/zwgk_213/zcwj/xzgfxwj/202102/t20210224_8931328.html

➢ 今年 2 月全国受理网络违法和不良信息举报 984.5 万件

2021 年 3 月 10 日，网信办网站公布 2021 年 2 月，全国各级网络举报部门受理举报

984.5 万件，环比下降 12.1%、同比下降 6.4%。其中，中央网信办（国家互联网信息办公室）违法和不良信息举报中心受理举报 18.9 万件，环比增长 6.9%、同比增长 6.2%；各地网信办举报部门受理举报 90.3 万件，环比下降 15.7%、同比下降 13.8%；全国主要网站受理举报 875.3 万件，环比下降 12.1%，同比下降 5.8%。

在全国主要网站受理的举报中，微博、百度、快手、豆瓣、阿里巴巴、腾讯、知乎、今日头条、新浪网、哔哩哔哩、拼多多等主要商业网站受理量占 88.5%，达 774.9 万件。



在各级网信部门指导下，目前全国各主要网站不断畅通举报渠道、受理处置网民举报。欢迎广大网民积极参与网络综合治理，共同维护清朗网络空间。（来源：网信办网站）

五、本期重要漏洞实例

➢ 关于 Microsoft Exchange Server 存在多个高危漏洞的安全公告

发布日期：2021-3-08
更新日期：2021-3-08
受影响系统：
Exchange Server 2013
Exchange Server 2016
Exchange Server 2019
Exchange Server 2010
描述：

CVE(CAN) ID: CNTA-2021-0009
2021 年 3 月 4 日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-14768、CNVD-2021-14769、CNVD-2021-14770，对应 CVE-2021-26854、CVE-2021-26412、CVE-2021-27078）、Microsoft Exchange Server 任意文件写入漏洞（CNVD-2021-14810、CNVD-2021-14811，对应 CVE-2021-27065、CVE-2021-26858）、Microsoft Exchange Server 反序列化漏洞（CNVD-2021-14812，对应 CVE-2021-26857）、Microsoft Exchange Server 请求伪造漏洞（CNVD-2021-14813，对应 CVE-2021-26855）。攻击者综合利用上述漏洞，可在未授权的情况远程执行代码。目前，部分漏洞细节已公开，微软官方已发布新版本修复漏洞，建议用户尽快更新至最新版本进行修复。Exchange 是微软公司开发的一套电子邮件服务组件。Exchange 不仅支持传统的电子邮件的存取、储存、转发功能，新版本产品中还支持语音邮件、邮件过滤筛选和 OWA 等辅助功能。
2021 年 3 月 2 日，微软公司发布了关于 Exchange 服务的紧急安全更新，修复了 7 个相关漏洞：1）Exchange 服务端请求伪造漏洞（CVE-2021-26855）：未经授权的攻击者利用该漏洞，可发送任意 HTTP 请求并通过 Exchange 服务身份验证。2）Exchange 反序列化漏洞（CVE-2021-26857）：具有管理员（administrator）权限的攻击者利用该漏洞通过发送恶意请求，实现在 Exchange 服务器上以 SYSTEM 身份的任意代码执行。该漏洞单独利用须具备较高的前提条件。3）Exchange 任意文件写入漏洞（CVE-2021-26858/CVE-2021-27065）：经过 Exchange 服务身份验证的攻击者，利用该漏洞，可实现对服务器的任意目录文件写入。4）Exchange 远程代码执行漏洞（CVE-2021-26412/CVE-2021-26854/CVE-2021-27078）：攻击者利用此漏洞，可获得目标服务器的权限，最终在服务器上的任意代码执行。CNVD 对上述漏洞的综合评级为“高危”。
CNVD 组织技术支撑单位对 Microsoft Exchange 服务在我国境内的分布情况进行了分析统计，数据显示我国大陆地区共有 27825 个 IP（IP 端口）开启了 Exchange 服务。我平台以 Exchange 服务端请求伪造漏洞为例开展了漏洞普测工作，结果显示我国大陆地区共有 1466 台服务器（IP 端口）存在该漏洞，受影响比例约为 5.3%。
建议：

厂商补丁：
目前，微软公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本，避免引发漏洞相关的网络安全事件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://msrc.microsoft.com/update-guide/en-us

➢ Google Chrome Network Internals 代码执行漏洞

发布日期：2021-3-04
更新日期：2021-3-04
受影响系统：
Google Chrome <89.0.4389.72
描述：

CVE(CAN) ID: CVE-2021-21179
Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。
Google Chrome Network Internals 存在代码执行漏洞。远程攻击者可以利用此漏洞在系统上执行任意代码或造成拒绝服务情况。
建议：

厂商补丁：
Google
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html

➢ SAP Enterprise Financial Services 权限提升漏洞

发布日期：2021-03-09
更新日期：2021-03-11
受影响系统：
SAP Enterprise Financial Services 800
SAP Enterprise Financial Services 618
SAP Enterprise Financial Services 617
SAP Enterprise Financial Services 616
SAP Enterprise Financial Services 606
SAP Enterprise Financial Services 605
SAP Enterprise Financial Services 604
SAP Enterprise Financial Services 603
SAP Enterprise Financial Services 600
SAP Enterprise Financial Services 105
SAP Enterprise Financial Services 104
SAP Enterprise Financial Services 103

SAP Enterprise Financial Services 102
SAP Enterprise Financial Services 101
描述：

CVE(CAN) ID: CVE-2021-21486
SAP Enterprise Financial Services 是德国思爱普（SAP）公司的一套企业财务服务解决方案。
SAP Enterprise Financial Services 101、102、103、104、105、600、603、604、605、606、616、617、618 和 800 版本存在权限提升漏洞。该漏洞源于程序未对经过身份认证的用户执行正确的授权检查。攻击者可利用该漏洞提升权限。
建议：

厂商补丁：
SAP
目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107

➢ Cisco SD-WAN vManage SQL 注入漏洞

发布日期：2021-03-03
更新日期：2021-03-04
受影响系统：
Cisco SD-WAN vManage < 20.4.1
Cisco SD-WAN vManage < 20.3.2
Cisco SD-WAN vManage < 19.2.4
描述：

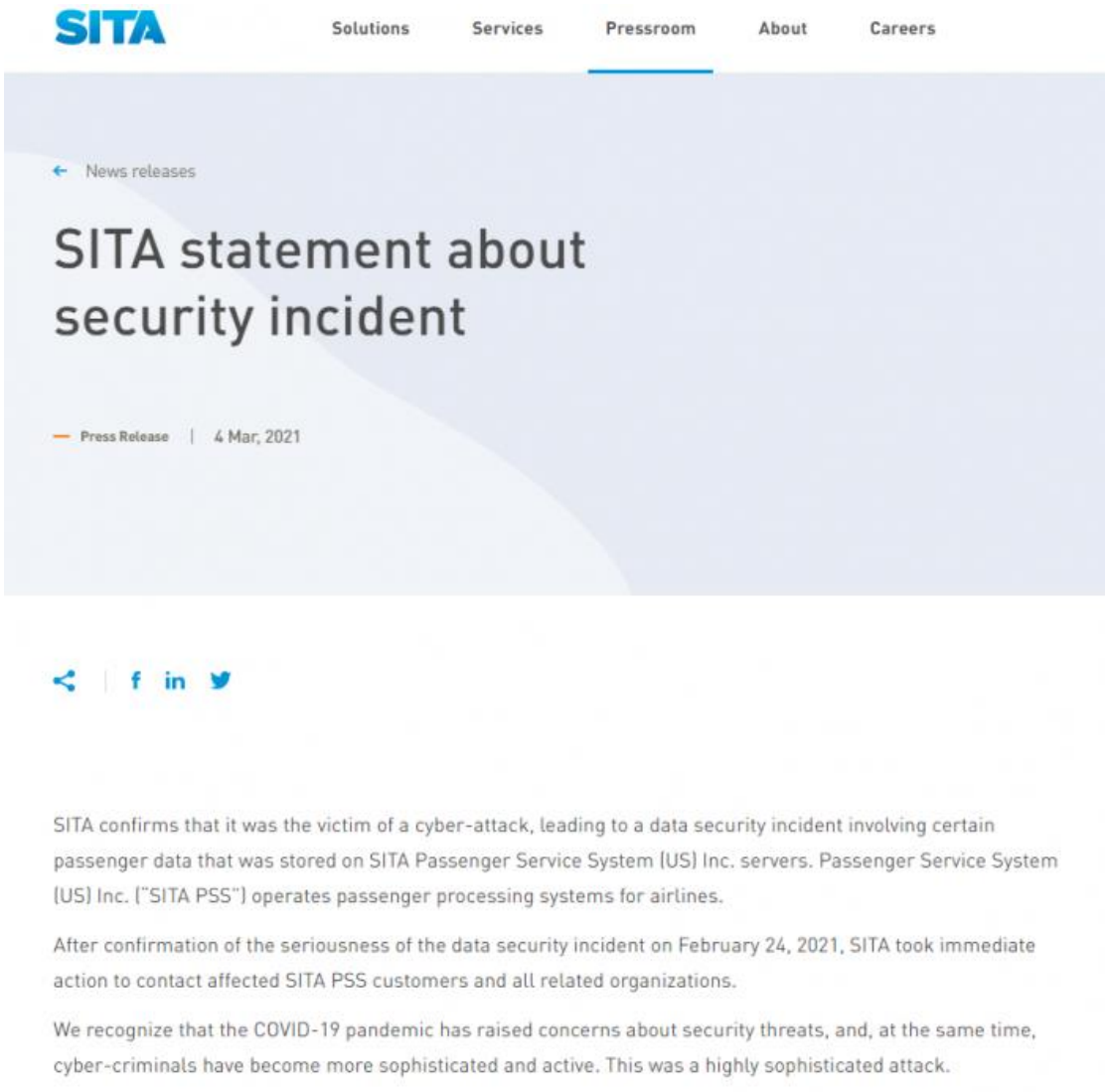
CVE(CAN) ID: CVE-2021-1470
Cisco SD-WAN vManage 是美国思科（Cisco）公司的一款可提供软件定义网络功能的软件。该软件为网络虚拟化的一种方式。Cisco SD-WAN vManage Software 存在 SQL 注入漏洞。该漏洞源于程序未对 SQL 查询的输入进行正确验证。攻击者可通过发送恶意 SQL 查询利用该漏洞修改 vManage 数据库或基础操作系统上的值，或从 vManage 数据库或基础操作系统返回值。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-sqlinj-HDJUeEAX
建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-sdw-sqlinj-HDJUeEAX）以及相应补丁：
cisco-sa-sdw-sqlinj-HDJUeEAX：Cisco SD-WAN vManage SQL Injection Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-sqlinj-HDJUeEAX

六、本期网络安全事件

➢ 全球航空运输数据巨头 SITA 航空客运系统遭遇数据泄露事件

2021 年 3 月 5 日，球航空运输数据巨头 SITA 公司已经证实了一起涉及乘客数据的数据泄露事件。**该公司周四在一份简短的声明中表示**，该公司已成为“网络攻击的受害者”，存储在其美国服务器上的某些乘客数据已被泄露。2 月 24 日该公司证实了这一网络攻击事件，之后其联系了受影响的航空公司。



SITA 是全球最大的航空 IT 公司之一，为全球约 90%的航空公司提供服务，这些航空公司依靠该公司的旅客服务系统 Horizon 来管理订票、售票和飞机起飞。但目前仍不清楚到底有哪些数据被访问或被盗。当联系到 SITA 时，SITA 发言人 Edna Ayme-Yahil 以正在进行的调查为由，拒绝透露被盗取的具体数据。该公司表示，该事件“影响到全球各个航空公司，而

不仅仅是美国的航空公司”。

SITA 确认已经通知了几家航空公司：这包括马来西亚航空;芬兰航空;新加坡航空;以及韩国的济州航空，这些航空公司已经就此次事件发表了声明。但 SITA 拒绝透露其他受影响的航空公司的名字。在 TechCrunch 看到的一封给受影响客户的电子邮件中，新加坡航空公司表示，它不是 SITA 的 Horizon 乘客服务系统的客户，但约有 50 万名常旅客会员的会员号和层级身份被泄露。该航空公司表示，转移这类数据是“为了能够验证会员层级状态，并在旅行时给予会员航空公司的客户相关优惠”。该航空公司表示，乘客的行程、预订、票务和护照数据没有受到影响。

SITA 是航空市场上少数几家为航空公司提供客票和预订系统的公司之一，与 Sabre 和 Amadeus 并列。Sabre 在 2017 年年中报告了一起影响其酒店预订系统的重大数据泄露事件，黑客获取了超过 100 万张客户信用卡数据。这家总部位于美国的公司在 12 月同意 240 万美元的和解协议，并在泄露事件发生后对其网络安全政策进行修改。2019 年，有安全研究人员发现，法航、英航和澳航等公司使用的 Amadeus 乘客预订系统存在漏洞，这使得该公司很容易更改或获取旅客记录。（来源：cnBeta）

➢ 海底捞包间装摄像头引争议 律师:需提前告知消费者

2021 年 2 月 27 日，一则“海底捞在包间里安装摄像头”的消息引发网友热议。对于安装摄像头是否会侵犯隐私，网友各执一词。此前有消息称，海底捞多个门店包间内安装了摄像头。记者走访海底捞位于北京市朝阳区的多家门店，确实在包间里看到了云台式摄像头。随后，记者走访部分其他品牌餐饮企业发现，饭店包间装摄像头的现象，并不罕见。在走访的 8 家餐厅里，有 3 家包间都有摄像头。不过，部分包间内没有“内有监控”等相关提示。

3 月 1 日，海底捞总部客服回应称：海底捞确实有在北京部分门店内的包间里安装摄像头，初衷是为了保护消费者用餐安全，“我们不会滥用摄像头，有相应的管理制度，我们遵照了国家的相应法律法规。”前述海底捞总部客服强调，部分门店里会有摄像头的明确提示，海底捞也会告知消费者在包间内安装了摄像头，不过“各个门店执行起来有差异。”前述客服称，目前暂无法告知具体哪些门店安装了摄像头，“但是会有标志提示，会告知顾客”。

3 月 1 日记者随机询问位于湖南长沙等地的 5 家海底捞门店，对方均表示在包间内安装了监控摄像头。部分门店称，有监控的地方都有温馨提示。其中一家海底捞分店客服说，海底捞在大厅内的包间里确实安装了监控，没有明确的标识，如果有顾客需要用监控，需要领导提前批准。

如果海底捞告知消费者安装了摄像头，算侵犯隐私吗？

上海正策律师事务所律师虞元坚称，如果海底捞提前告知则不属于侵犯隐私权。根据《民法典》第一千零三十二条规定，隐私的范围强调了“是否愿意为他人知晓”这一主观心态，消费者明知行为可能会被观看，而不介意，就不存在侵犯隐私。虞元坚表示，对经营者来说，安装监控摄像头可以规避很多麻烦。对于封闭式包厢，摄像头建议安置在明显易于发现的位置，或者有所提示。如果视频未经允许流出，消费者可根据对自身造成的侵权后果，而选择是否起诉处理。（来源：互联网综合整理）

➢ 利用微信“清粉”软件非法获取微信用户信息，8 人获刑

2021 年 3 月 7 日报道，去年九月，南通市通州公安破获全国首例利用微信“清粉”软件非法获取微信用户信息的案件，八名犯罪嫌疑人落网。3 月 3 日，该案进行了集中宣判。张某某等八名被告人，犯非法获取计算机信息系统数据、非法控制计算机信息系统罪而获刑。公诉人介绍，被害用户当初扫描这款“清粉”二维码，目的是想给微信好友通讯录“瘦身”，释放内存空间，不料个人信息泄露。八名被告人则以刷阅读量、售卖微信群聊二维码等方式非法获利 200 多万元。

案件回溯

为图省事和方便，部分微信用户会选择“清粉”服务。事后，有的用户却发现有陌生人通过自己分享的二维码扫码进群，或者自己被拉入了一些广告群。2020 年 6 月，南通市公安局网安支队民警在工作中发现，部分微信朋友圈和群聊中散播的“清粉”软件存在很大安

全隐患。

民警介绍，“清粉”软件的原理，就是通过应用集群控制软件控制微信账号，自动向所有好友群发消息，再由软件自动识别哪些是“僵尸粉”并予以删除。但犯罪嫌疑人在取得微信账号的控制权限后，却借机非法获取用户微信群聊二维码信息，并将这些群聊二维码以图片形式保存在服务器上，再倒卖给下游的诈骗、赌博等犯罪团伙获利。

2020 年 7 月 3 日，南通市公安局成立由网安、法制、通州区公安局等部门组成的专案组，并指令通州区公安局为主侦办此案，全力开展工作。专案组研判发现，2020 年 2 月以来，多个地区频繁出现陌生人扫码进群散布赌博、营销等非法广告，甚至实施诈骗，关联案件达 1500 余起，涉及 20 多个省市。腾讯公司反馈，微信群聊二维码泄露现象发生后，他们依法配合多地公安机关抓获了多个出售和利用微信群聊二维码作案的犯罪团伙。通过对大量“清粉”软件开展侦查实验，专案组最终锁定一款名为“微清”的软件有重大嫌疑。该团伙精心制作了‘极速清粉’的广告图，号称官方认证，只需要 1 分钟检测完毕。为吸引人使用，这款软件打着官方清粉团队的旗号，通过各种途径在微信用户群体中传播，一旦有人点击扫描登录检测，就可以通过后台服务器直接登录受害人的微信，并获取所有的用户权限。

虽然犯罪嫌疑人使用的是非实名信息注册，以期逃避公安机关打击。但侦查员重新梳理线索后，在已停用的服务器上取得重大突破，成功挖出团伙成员刘某、何某等人的真实身份。2020 年 7 月 22 日，专案组民警兵分三路，在广东韶关、仁化，湖北天门等地公安机关的支持下，将涉案的 5 名犯罪嫌疑人全部抓获归案。

经查，该犯罪团伙分工明确，由张某、刘某、何某负责系统开发和维护，李某负责出售二维码牟利，谭某负责为微信公众号引流牟利。据众人交代，所谓的官方认证、放心访问只是为了降低使用者的警惕心理，他们并没有获得官方授权，而是租用服务器自行搭建系统，在骗取用户授权登录后，通过这些外挂软件系统批量获取微信群聊二维码，批量关注、阅读、点赞等。

该犯罪团伙平台化、专业化、精细化程度高，隐蔽性极强。从非法获取微信用户的相关个人信息，到下游的广告、营销和其他网络犯罪，相关的网络黑灰产已经形成一个各环节相互独立又紧密协作的产业链。这起案件系全国首例，没有经验借鉴，办案民警通过分析作案手法、犯罪事实，在腾讯公司和南京森林警官学院的支持配合下，最终案件得以成功告破。

提醒：一旦同意使用这类“清粉”软件，就意味着自己的账号完全让人“接管”，不法分子将轻易获取相关个人信息，建议广大网友尽量不要使用破坏官方软件协议或具有外挂功能的插件和软件，有效规避可能遇到的安全风险。网络安全为人民，网络安全靠人民。（来源：扬子晚报）

➢ 赔偿 1.59 亿员工携商业秘密跳槽，与“新东家”被判侵权或涉刑事犯罪

2021 年 2 月 26 日，随着最高人民法院知识产权法庭的法槌落下，一起重大商业秘密侵权案迎来终审判决，法院最终认定涉案的王龙集团公司（以下简称王龙集团）、王龙科技公司（以下简称王龙科技）等共同实施了侵害嘉兴中华化工（以下简称中华化工）商业秘密的行为，令其停止侵权并赔偿经济损失 1.59 亿元人民币。1.59 亿的天文数字，使该案成为人民法院史上判决赔偿额最高的侵害商业秘密案件。那么，这起纠纷究竟因何而起？判赔金额又是如何计算得出的呢？

案情回顾：车间副主任携商业秘密跳槽

本案中，双方的争议焦点是一款名为“香兰素”的香料技术秘密。香兰素(Vanillin)又名香草醛，是一种广泛使用的可食用香料，可在香荚兰的种子中找到，也可以人工合成。2002 年起，中华化工与上海欣晨公司（以下简称上海欣晨）共同研发了乙醛酸法生产香兰素工艺，并将之作为技术秘密保护。中华化工因香兰素相关技术被评为高新技术企业，并成为全球最大的香兰素制造商，占据了香兰素全球市场约 60%的份额。

但是，好景不长，香兰素为公司招来巨大商机的同时，也引来了觊觎的目光。虽然中

华化工为保护商业秘密采取了一些防范措施，但千防万防，家贼难防。2010 年，中华化工香兰素车间副主任傅某某在获得王龙科技给予的 40 万元报酬以后，将“老东家”的香兰素技术秘密披露给对方，并在离职后进入王龙科技，成为其核心业务骨干。此后，王龙科技按照载有涉案技术的图纸，订购香兰素生产设备组建生产线，正式生产香兰素。2011 年至 2017 年，王龙集团、王龙科技等利用涉案技术秘密，每年生产销售香兰素至少 2000 吨。

法院认定：被告承担侵权连带责任

遭到侵权后，中华化工、上海欣晨以王龙集团、王龙科技等为被告，诉至浙江省高级人民法院，请求判令被告停止侵权并赔偿 5.02 亿元（当时浙江省诉讼标的额 5 亿元以上的一审民事案件由高级人民法院管辖）。浙江省高院作出判令被告停止侵权并赔偿 350 万元的判决后，该案各方当事人又上诉至最高人民法院。二审中，原告请求的赔偿额降至 1.77 亿元。最高法综合考虑涉案技术秘密商业价值巨大、侵权规模大、侵权时间长、侵权者拒不执行生效行为保全裁定等因素，改判王龙集团、傅某某、王龙科技及其法定代表人王某某等连带赔偿权利人经济损失 1.59 亿元。法庭同时决定将本案涉嫌犯罪线索向公安机关移送。这一判决值得关注。除根据案件事实依法判决侵权方赔偿 1.59 亿元之外，最高法还判令跳槽员工和侵权企业法定代表人承担连带责任，精准有效打击了侵权行为主导者，彰显出人民法院严格保护知识产权，严厉打击恶意侵权行为的鲜明态度。

做好“人防”：严格保护企业商业秘密

本案作为人民法院判决赔偿额最高的侵害商业秘密案件，引发社会舆论的广泛关注。同时，也让不少“身怀绝技”的企业为之震慑，迫切寻找保护商业秘密的“药方”。毕竟在实践中，企业的保密措施常常因人员流动大、保密制度震慑性弱等因素得不到有效落实。

这其中，又以员工携商业秘密跳槽“新东家”的情况最常见也最具杀伤力。

由此看来，做好“人防”应是企业加强商业秘密保护的重中之重，必须予以高度重视。把牢“入口”。企业在招聘时，应对重点岗位的员工进行全面考察，除考察工作能力外，也需结合其从业经历等情况考察员工是否具备良好的品德品行。在员工入职签订劳动合同时，企业应与员工约定商业秘密保护条款，告知其保护企业商业秘密的重要性以及泄露商业秘密可能导致的严重后果。

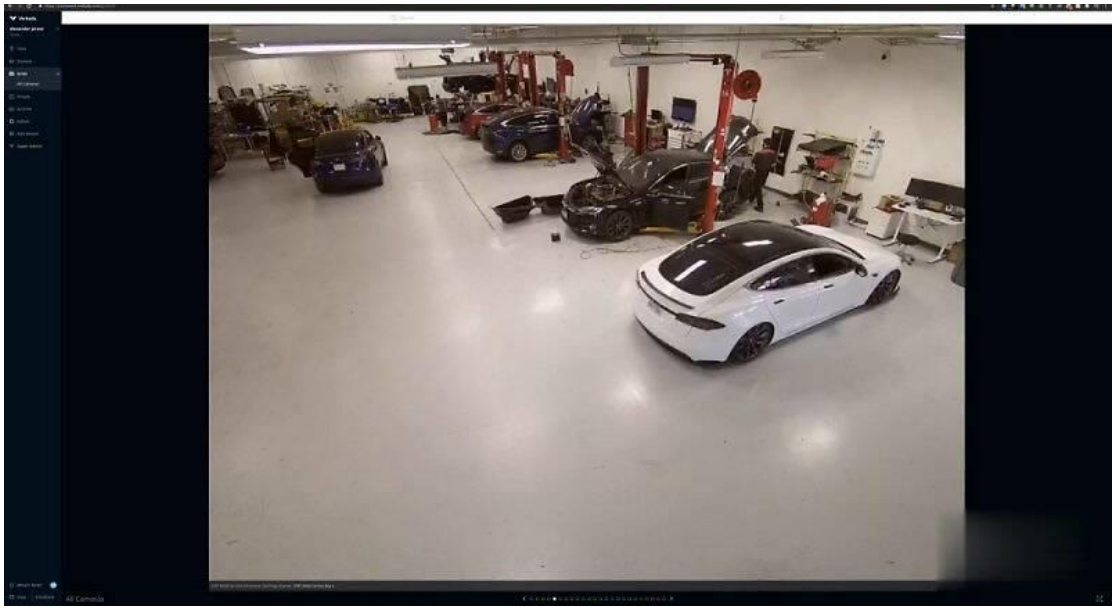
重视过程。员工选择在企业长久发展，一方面是认可企业的发展前景，另一方面则在于认同企业文化。因此，企业加强重点岗位员工保密管理，可以从三方面入手：一是定期组织与业务相结合的保密宣教培训，如上岗保密培训、出国（境）保密培训等，确保员工在认同企业文化的基础上，掌握保密知识技能并严格遵守保密制度；二是提高人文关怀，为保密专员等提供保密津贴，在工作考核中予以政策倾斜，多了解其思想和工作状况；三是强化监督管理，如组织定期检查，及时发现隐患并认真整改，从源头上遏制侵害商业秘密行为发生。

严把“出口”。若曾掌握商业秘密的员工离岗离职，企业应对其“特殊关照”，如保证其彻底、及时地交还工作资料；与离职员工谈话，了解其离职动机和去向；与其签订竞业限制条款等。主动维权。企业一旦发现有离职员工侵害商业秘密的情况，应积极开展维权措施，如联系律师、会计师等专业人员收集资料、固定证据，向有关部门反映遭侵权情况以及向法院提起诉讼等，以切实保障企业合法权益。（来源：保密观）

➢ 黑客攻破 Verkada 品牌 15 万个视频监控摄像头

2021 年 3 月 10 日消息，一群黑客表示，他们已经入侵了硅谷监控创业公司 Verkada 收集的海量监控摄像头数据，能够看到医院、公司、警局、监狱以及学校内部的 15 万个监控摄像头的实时录像情况。

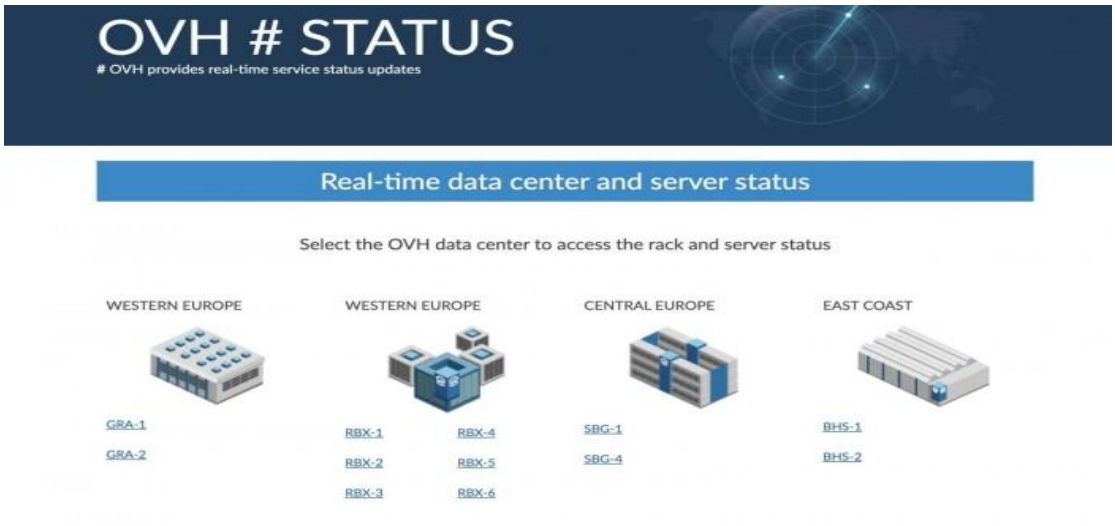
监控视频被曝光的企业包括特斯拉、软件提供商 Cloudflare。此外，黑客还能够看到女子卫生诊所、精神病院以及 Verkada 本身办公室内部的视频。其中一个视频拍摄自特斯拉上海仓库内部，能够看到装配线上的工人。黑客称，他们能够访问特斯拉工厂和仓库内的 222 个摄像头。



Verkada 代表在一份声明中称：“我们已经禁用了所有内部管理员账户来防止任何未经授权的访问。我们的内部安全团队和外部安全团队正在调查这一潜在问题的规模和范围。”据了解，Verkada 成立于 2016 年，主营业务是销售监控摄像头，用户可以通过网络对其进行访问和管理。（来源：凤凰科技）

➢ 法国斯特拉斯堡 OVH 数据中心遭遇火灾 诸多客户遭遇严重打击

2021 年 3 月 11 日 Bleeping Computer 报道称，一次史无前例的重大事故，导致位于法国斯特拉斯堡的 OVH 数据中心被大获烧毁。作为欧洲最大、世界第三的托管服务提供商，这家云计算企业有为客户提供 VPS、专用服务器、以及其它 Web 服务。由状态页面可知，本次事故已导致多个数据中心离线，且对全球网站也造成了冲击。



Bleeping Computer 指出，大火摧毁了 OVH 斯特拉斯堡 SBG2 数据中心，但 SBG1、SBG3 和 SBG4 也都被迫关闭，以免受到火灾的附带影响。

该公司在声明中称：我司位于斯特拉斯堡的数据中心遭遇了重大事故，SBG2 号建筑物中发生了火灾。尽管消防人员立即抵达了现场，但遗憾未能控制这里的火势。目前整个站点都已被隔离，因而对 SBG1、SBG3 和 SBG4 上的所有服务也造成了影响。如果您在此处托管了生产服务，建议立即激活灾备恢复计划。我司所有团队正在与消防员携手努力，当有更多信息可分享时，我们也将及时发布更新。

据悉，在事件发生后的几个小时内，Bleeping Computer 就看到 SBG 和 SBG3 从 OVH 状态页面的列表中完全离线。受此事件影响，OVH 的许多大客户都表示自家的 Web 服务已无法访问，包括网络威胁情报公司 Bad Packes、免费国际象棋服务器 Lichess.org、视频游戏制造商 Rust、加密货币交易所 Deribit 的博客和文档站点、电信公司 AFR-IX、加密实用程序 VeraCrypt、新闻媒体 eeNews Europe、蓬皮杜艺术中心等。

后续 Deribit 告知，本次中断仅影响了他们的文档和博客网站，交易所的服务并未受到影响。然而视频游戏制造商 Rust 就没有那么幸运，据说本次事故已导致数据全损且无法恢复。OVH 创始人兼董事长 Octave Klaba 在转发 Bad Pockets 推文时表示，公司已确认 OVH 数据中心大火导致重大损失，目前正在尝试更换受影响的服务器，但数据显然无法得到有效恢复。

截止 2021 年 3 月 10 日凌晨，虽然大火已经得到了控制，但至少在今天，他们仍预计无法提供服务 ——“大火已灭，消防员仍在浇水冷却建筑物。但因维护人员无法进入，SBG1、SBG3 和 SBG4 无法在今日重新启用”。庆幸的是，截止目前，我们尚未见到有关大火造成人员伤亡的报案到。不过在 OVH 努力重启服务时，所有客户也应立即实施他们的灾备恢复计划。（来源：cnBeta）

信息安全意识产品服务

021-33663299