智能体重点应用领域有哪些？

近日，国家网信办、国家发展改革委、工业和信息化部联合印发《智能体规范应用与创新发展实施意见》（以下简称《实施意见》）。《实施意见》从夯实发展基础、守牢安全底线、强化应用牵引、建设创新生态4个方面提出举措。

在强化应用牵引方面，《实施意见》提出积极稳妥推动智能体典型场景应用，牵引技术产品优化提升，探索形成可复制、可推广的智能体落地应用模式。其中一共提到五个方面19种场景。

科学研究

科研探索。研发理论推演、模拟仿真等智能体，挖掘潜在技术路径。强化智能体信息关联整合、知识体系构建等能力，提升自然科学、哲学社会科学研究发现能力。

研发辅助。发展软件开发智能体，提升需求分析、架构设计、代码生成与测试等全流程开发能力。

产业发展

智能制造。研发生产管理智能体，动态优化生产排程、资源分配和工序衔接，推动智能体在工业互联网领域应用，提升企业精细化管理水平。

能源资源。研发大气、水体、土壤、噪声等环境要素感知智能体，提升自然灾害、环境污染等风险预警能力。

交通运输。研发交通安全监管、应急指挥调度等智能体，提升违章违规行为识别、交通基础设施风险预警、重点车辆（船舶）监管、事故快速响应等能力。

农业生产。研发农业服务智能体，开展农技指导、病虫害诊断与防治等服务。

金融服务。研发金融风控智能体，提升信贷审批、交易监控、账户安全等环节风险识别能力。

提振消费

终端应用。推动智能体赋能互联网应用及服务，优化在线购物、出行导航、生活缴费、日常办公等服务体验。

文化旅游。研发文学、音乐、绘画、视听、演艺等内容创作智能体，促进优秀文化传播推广。

商业服务。提升智能体客服能力，提供7×24小时咨询、预约、售后等服务。发展导引、清洁、仓储、配售等具身智能体，提升餐饮、零售、住宿、物流等商业场所的运营效率。

民生福祉

教育教学。探索课件生成、作业批改、学情分析等智能体，提高教师工作效率。

医疗健康。提升医学影像分析、疾病诊断推理、定制化诊疗方案生成等医疗辅助智能体性能，探索药品管理、手术排程、病历管理等智能体，提升医疗服务效率。

人力资源。探索智能体在就业促进、技术技能人才培养评价、劳动关系公共服务等领域应用，提升就业服务能力。

信息服务。探索智能体在网络内容建设管理中的应用，鼓励信息发布部门和内容传播平台研发用户分析、选题策划、采编加工、分发推荐、智能审核、舆论引导、情绪疏导、实时翻译等智能体。

社会治理

政务服务。探索事项辅助审批智能体，推动政务审批流程智能化。

司法服务。探索全流程办案辅助智能体，提升案件材料梳理、案件信息录入、证据审查、辅助法律文书生成等能力。

公共安全。探索监测预警、应急处置、救援调度、协同治理等智能体，提升安全生产监管和防灾减灾救灾等能力。提升智能体异常行为识别、潜在威胁预警、动态防控处理能力，维护公共安全。

城市治理。探索智能体在城市规划、建设与治理环节应用，支撑智能建造、房屋管理、城市基础设施安全运行等工作。

招标投标。探索招标投标智能体，实现招标投标活动全链路智慧管理，保障全过程规范高效。

在守牢安全底线方面，《实施意见》明确坚持以人为本、智能向善、多元共治、安全稳妥，营造规范发展、鼓励创新的制度环境，促进智能体健康有序发展。比如明确决策权限方面，《实施意见》要求在遵守法律法规、尊重社会公德和伦理规范前提下，厘清仅限用户本人决策、需由用户授权决策和智能体自主决策等各种决策方式的合理边界及所需权限。确保用户对智能体自主决策享有知情权和最终决策权，智能体执行操作不得超出用户授权范围。

另外，《实施意见》明确，要发挥专业机构内容资源和审核把关优势，确保智能体行为符合法律法规及主流价值观。防止智能体利用数据优势、人格化技术实施传播不良价值观、算法压榨等行为，防范未成年人、老年人沉迷成瘾、情感依赖等风险。

中国普法

戴智能手表跑步，致重要机密泄露

近日，某国发生一起因智能穿戴设备导致的军事机密泄露事件，引发全球关注。当时该国某重要军事装备正在执行任务，一名军官跑步时佩戴的智能运动手表持续记录并公开了高精度GPS数据，致使该军事装备实时位置等重要敏感信息泄露，给该国国防安全造成难以弥补的重大损失，也让智能穿戴设备的泄密风险再次走入人们的视线。

风险频发，警钟长鸣

智能穿戴设备引发的泄密事件并非偶发个案，近年来在全球范围内反复上演，已然成为信息安全领域的突出痛点。

公开案例1：某团队汇总全球某智能手环6460名用户的健身数据，还原出48处核武器存储场所、18处情报机构办公场所等众多敏感信息。

公开案例2：某国领导人出访前，安保人员在其即将下榻酒店附近跑步并留下数字足迹，致使酒店位置信息提前泄露。

公开案例3：某国特工执勤期间佩戴智能穿戴设备记录跑步路线，致使重要会晤的酒店位置遭到泄露。

公开案例4：境内多个健身APP存在违规收集个人信息问题，可能导致个人位置、工作单位等信息泄露。

从国家层面的军事机密、涉密信息，到社会层面的机构数据、个人隐私，都可能因为一次智能穿戴设备的不当使用而出现泄密，需引起全社会的高度重视。

数据失守，挑战加剧

当前，各类商业APP通过获取用户的位置信息、终端设备、使用习惯等广告标识数据，能够精准构建用户画像，进而有效提升用户黏性和市场转化率。但部分商业公司大批量、长时段、全方位收集用户信息，可能会增加信息泄露风险。如果这些数据被别有用心之人加以分析，就会给国家安全带来威胁。

——特殊身份暴露。境外间谍情报机关可能将智能穿戴设备数据，作为渗透策反的突破口，通过抓取各类数据，精准锁定涉密人员、公职人员、科研从业者等目标，直接危害国家安全。

——涉密信息外泄。智能穿戴设备会持续采集位置、环境等数据，若在军事管理区、涉密科研院所、党政机关办公区等敏感区域使用，极易泄露涉密敏感信息。

——隐私安全失守。智能穿戴设备采集的家庭住址、日常通勤、健康数据、消费轨迹等隐私信息，一旦被不法分子窃取，可能危害个人财产安全与人身安全。

多维防护，防患未然

智能穿戴设备本是便利生活的助手，但使用不当就会带来风险。我们要在享受科技便利的同时，绷紧安全之弦、守住保密底线。

——严控使用场景，敏感区域“慎触碰”。涉密人员及敏感岗位人员，要安全规范使用智能穿戴设备，避免运动轨迹标记出敏感坐标，危害国家安全。

——严控权限开关，“精打细算”给权限。定期审查智能穿戴设备的APP权限，遵循“最小必要”原则，对多数应用“仅在使用期间允许”定位，最小化运动日记、轨迹图的被访问权限，彻底关闭公开访问通道。

——严控数据分享，织牢信息“防护网”。审慎对待每一次运动成果分享，清除地理位置信息。注册时使用虚拟身份信息，不填写真实姓名、家庭住址、工作单位等隐私数据。定期删除APP内以及云端存储的运动历史记录、位置轨迹信息。

中国科普

本版图片为资料图片

“开盒”网暴、窃取患者隐私……

这些行为被严惩

随着犯罪技术迭代更新，个人信息泄露问题日益突出，犯罪分子利用非法获取的个人信息精准实施诈骗、敲诈勒索、“开盒”等违法犯罪，形成侵犯公民个人信息犯罪黑灰产业链，严重侵害公民人身、财产安全，也严重危害公共安全和社会秩序。

5月8日，最高人民法院发布人民法院审结的侵犯公民个人信息犯罪及关联犯罪典型案例。

案例一：外包公司窃取患者隐私——博某软件有限公司、何某某等侵犯公民个人信息案

【基本案情】

2015年至2020年间，被告单位博某软件有限公司负责为某医院开发、维护网上挂号系统，被告人何某某系公司法定代表人。在提供服务过程中，何某某暗中收集从后台非法获取的该医院挂号用户相关个人信息，并安排公司员工被告人熊某、罗某某将所获取的信息数据导入公司自建数据库。2021年初，熊某又安排人员在为该医院开发的软件上安装接口，自动将挂号用户个人信息导入公司自建数据库。案发后，在公司服务器、自建数据库及何某某家中设备内均提取到包含有挂号用户的个人信息，数据去重后合计2878070条。

【裁判结果】

江苏省无锡市锡山区人民法院审理认为，被告单位博某软件有限公司在提供服务过程中非法获取公民个人信息，情节特别严重，已构成侵犯公民个人信息罪，应依法惩处。被告人何某某等人为被告单位直接负责的主管人员和其他直接责任人员，均已构成侵犯公民个人信息罪。综合本案事实、情节、后果等，对被告单位博某软件有限公司以侵犯公民个人信息罪判处罚金人民币三十万元；对被告人何某某等人以侵犯公民个人信息罪判处有期徒刑五年六个月至一年六个月不等，并处罚金人民币十万元至一万元不等。

【典型意义】

针对医疗信息、患者隐私等个人信息犯罪案件高发，应强化医疗机构数据安全体系建设，严厉打击泄露、非法获取患者医疗信息犯罪。互联网企业在为医疗卫生领域提供服务过程中，应当严格依照法律法规、企业经营范围、合同约定及隐私协议等，在服务和授权范围内合理合法地处理公民个人信息。互联网企业利用为医疗机构提供服务的便利，非法获取患者信息、医疗数据的行为，属于《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》第四条规定的在“提供服务过程中收集公民个人信息”的情形，情节严重，应依法惩处。人民法院追究被告单位和直接负责的主管人员、其他直接责任人员的刑事责任，同时适用财产刑，体现了依法从严惩处的态度。

案例二：严惩“开盒”网暴行为——林某某、王某某侵犯公民个人信息、非法利用信息网络案

【基本案情】

2023年至2025年间，被告人林某某、王某某通过加密通讯工具等互联网渠道非法获取公民个人信息数据，后以虚拟货币收款等方式出售牟利。经查，林某某非法获取公民个人信息数据6亿余条，王某某非法获取公民个人信息数据3亿余条。2025年间，林某某、王某某伙同王某（另案处理）将非法获取的公民个人信息数据搭建“社工库”网站，经查，该网站数据库中的公民个人信息数据共计1.7亿余条，被告人利用网站非法提供公民个人信息1300余次，网站访问人次共计10余万次。

2025年间，被告人林某某伙同王某（另案处理）等人，利用加密通讯工具设立群组，担任群组管理员，在群组中发布针对他人侵犯隐私、侮辱谩骂等违法犯罪信息。该群组成员共计2000余人。

【裁判结果】

北京市海淀区人民法院审理认为，被告人林某某、王某某伙同他人违反国家有关规定，非法获取、出售公民个人信息，情节特别严重，均已构成侵犯公民个人信息罪；林某某伙同他人设立用于实施违法犯罪活动的群组，发布违法犯罪信息，情节严重，已构成非法利用信息网络罪，均应予惩处。林某某一人犯数罪，应当数罪并罚。综合本案事实、情节、后果等，对被告人林某某以侵犯公民个人信息罪判处有期徒刑六年六个月，并处罚金人民币六万元；以非法利用信息网络罪判处有期徒刑一年，并处罚金人民币一万元，决定执行有期徒刑七年，并处罚金人民币七万元。对被告人王某某以侵犯公民个人信息罪判处有期徒刑五年六个月，并处罚金人民币五万元。

【典型意义】

近年来，部分不法分子通过非法手段批量获取公民身份证件、家庭住址、社交媒体账号、交通住宿信息等公民个人信息，在网络上公开发布煽动网民针对特定人员攻击谩骂，或者提供有偿查询、帮助他人定向“开盒”，给被害人及其家人的身心健康和人身安全造成极大伤害，严重侵害公民合法权益、扰乱网络空间秩序、助长社会戾气、破坏和谐稳定。网络不是法外之地，“开盒挂人”针对性强，传播范围广，构成犯罪的，应依法严惩。个人信息安全关乎每个公民的生活安宁，人民法院依法保护公民个人信息、严厉打击“开盒”行为，是维护网络空间秩序、营造良好网络生态的必然选择。

中国普法