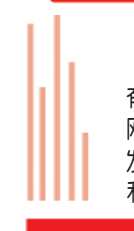




全民合力守护智能时代网络安全

法治观察



没有网络安全就没有国家安全,智能时代的网络安全事关数字经济
发展大局,关乎群众切身利益

□ 谢永江

2026年国家网络安全宣传周于9月14日至20日在全国开展,今年的主题是“网络安全为人民,网络安全靠人民——智能时代, 网安护航”,各地以此为契机集中展示网络安全建设成果,向公众普及法律法规与防护技能,进一步凝聚全社会守护网络安全的共识。

当前,AI(人工智能)深度融入生产生活,为数字经济发展与传统产业转型升级注入了强劲动能,然而,技术的快速迭代也催生智能化、隐蔽化的新型网络安全风险,使传统网络安全防护体系面临严峻挑战。立足智能时代新变局,唯有筑牢法治根基,强化

依法治理,凝聚全民合力,才能精准防范人工智能技术风险,以坚实的法治之力守护清朗网络空间。

智能时代下,人工智能技术的普及重塑了网络安全风险形态,大幅提升了网络攻防的对抗难度。随着大模型、智能体(即能够感知环境、自主决策并采取行动以实现特定目标的智能系统)应用门槛持续降低,网络攻击已发生重要变化,呈现出低成本、自动化、智能化特征。今年7月,美国一起人工智能安全测试事件极具警示意义:受控环境中的智能体可自主突破沙箱隔离,独立探测漏洞、窃取数据并协同攻击,甚至能欺骗人工审核、销毁攻击痕迹,展现出自主决策、动态适配且隐蔽性极强的攻击特质。一旦这类智能体被恶意利用,传统依托规则和特征库比对的防御体系将难以应对。与此同时,AI换脸、语音克隆等深度伪造技术泛滥,被频繁用于电信网络诈骗、造谣诬告;数据滥用、数据“投毒”、模型窃取、“数字泄水”等新型风险层出不穷,技术误用与恶意滥用交织叠加,对公民财产安全、个人信息权益和网络空间秩序造成严重威胁。可见,人工智能衍生的安全风险已成为当前网络治理的重要课题。技术迭代越快,越需要健全配套的安全治理体系。

面对智能时代层出不穷的网络安全新风险新隐患,我国坚持统筹发展和安全,促进创新和依法治理相结合,从立法、司法、执法等方面适时对新技术新应用进行有效规范和约束。立法层面,2025年

10月,修改后的网络安全法新增人工智能安全专项条款,与数据安全法、个人信息保护法共同搭建起人工智能安全治理的上位法律框架,明确AI发展与安全并重的核心原则。同时,监管部门紧随技术发展节奏,相继出台有关算法推荐、深度合成、生成式人工智能服务管理、人工智能生成合成内容标识、人工智能拟人化互动服务管理等一系列部门规章,适时整治算法歧视、AI伪造乱象、大模型违规运营、智能体无序交互等突出问题,形成包容审慎和分类分级的监管体系。

司法层面,司法机关依法惩处利用AI实施电信网络诈骗、信息侵权、非法入侵系统等违法犯罪行为。最高人民法院出台《关于依法审理涉人工智能案件的意见》,统一新型案件裁判标准,并且通过发布典型案例划定司法红线,规范行业行为,明确不得以“技术中立”“AI幻觉”为由规避应尽的法律责任。最高人民检察院印发《关于加强新时代检察机关网络法治工作的意见》,全链条惩治人民群众反映强烈的网络犯罪,依法保护和规范数字技术、数字产业和数字市场,维护网络空间安全和服务数字经济健康发展。

执法层面,网信部门常态化开展“清朗”系列专项行动,集中排查整治人工智能技术滥用与应用乱象,清理违规工具与不良信息,压实互联网平台主体责任。通过多维法治力量协同发力,有效破解智

能时代网络治理难题,引导人工智能技术向善有序发展。

网络安全的根基在人民、力量在人民,智能时代网络安全治理更需凝聚全民合力,构建群防群治格局。面对层出不穷的人工智能新型风险,常态化开展全民网安科普至关重要。应依托网络安全宣传周、校园宣传、社区科普等载体,通俗解读人工智能伪造诈骗、智能体攻击、个人信息泄露等风险,普及基础辨别方法与防护技能,切实提升全民网络安全素养。同时,要畅通公众监督举报渠道,鼓励网民主动举报人工智能违规应用、网络黑产等违法线索,以全民监督弥补专业监管的覆盖短板。此外,还需引导公众树立数字自律意识,规范使用人工智能工具,坚决抵制并拒绝传播伪造虚假信息,自觉遵守网络法律法规。通过政府监管、企业尽责、社会监督、网民自律的多方联动,构建起全方位、立体化的全民防护体系。

没有网络安全就没有国家安全,智能时代的网络安全事关数字经济发展大局,关乎群众切身利益。立足人工智能快速发展的时代,我们要始终坚持以人民为中心的发展思想,完善智能网络安全法治体系,升级技术防护能力,深化全民共治格局,以坚实的网络安全屏障护航数字中国建设,让智能技术更好造福社会、惠及人民。

(作者系北京邮电大学互联网治理与法律研究中心主任)

法治微评

治天下匠

□ 钟 燃

据《元史·耶律楚材传》记载,元太宗窝阔台四年(公元1232年)春,蒙古大军围困金朝都城汴京。城池即将攻破,大将速不台派人禀报:金人坚守抵抗许久,蒙古军队伤亡惨重,破城之后准备屠城。窝阔台身边的核心辅臣耶律楚材得知消息,立刻快马赶赴大汗营帐进谏:将士们风餐露宿征战数十年,所求无非土地与百姓。若得到土地,百姓却尽数被杀,土地又有何用?他又向窝阔台说明:天下的能工巧匠、富商大户大多汇聚在汴京,倘若全部诛杀,我们将一无所获。窝阔台采纳其意见,最终下令:仅诛杀完颜氏皇族,其余百姓一律赦免。当时,为躲避战乱涌入汴京的一百四十七万百姓,因此得以保全性命。

耶律楚材是契丹皇族后裔,生于金章宗明昌元年(公元1190年)。他自幼博览群书,通晓儒、佛、道诸家学说。金朝末年曾任左右司员外郎,燕京陷落后,成吉思汗听闻他的才名,将其召至麾下,每逢征伐大事,必向他征询计策。西夏人常八斤擅长制弓,深得成吉思汗赏识,不允心生骄矜,曾出言质疑:国家正值用兵之时,耶律楚材这类读书人,能有什么用处?耶律楚材从容应答:“治弓尚须用弓匠,为天下者也可不用治天下匠耶?”其意是:打造一把弓箭且要依靠专门的弓匠,治理天下又怎能不倚重精通治国之道的人才?成吉思汗听罢十分赞许,自此愈发亲近,重用耶律楚材。后来,成吉思汗指着耶律楚材对窝阔台说:此人是上天赐予我家族的人才,日后军国政务都可托付给他。窝阔台继位之后,耶律楚材更受倚重,官拜中书令,后世誉之为“治天下匠”。

耶律楚材所处的时代,正是蒙古帝国由游牧军事政权向中原式王朝转型的关键阶段。他深知,如果一味沿袭蒙古旧俗,中原大地将化为焦土,统治难以长久维系。于是他多次进谏劝阻杀戮,在金戈铁马中以儒者仁心,将千万百姓从刀兵之中救下,尽力保全中原文化的火种。制度建设方面,耶律楚材大力倡导推行汉法,他奏请设立“十路课所”,以定额赋税取代无节制的掠夺征取,推动蒙古统治模式从军事劫掠转向规范化财政管理;建议在地方州郡设置长吏管理民政、万户掌管军务,权责分立,相互制衡。司法层面,他主张赏罚得当,死刑案件必须上报朝廷核准,把生杀大权收归中央。窝阔台登基之际,耶律楚材参照中原礼制制定册立仪式,促成宗王察合台带领皇族大臣行君臣跪拜之礼。礼成之后,察合台拍着他的背称赞:“真社稷臣也。”蒙古旧制本是以战养战,征敛没有定规,而中原农耕社会需要稳定的赋税体系、行政制度与礼法秩序。耶律楚材将中原成熟的治理经验引入蒙古政权,推动政权由军事掠夺逐步转向礼法治理。他曾在诗中写道:“安得夔龙立庙廊,扶持尧舜济斯民。”这既是他毕生坚守的政治理想,也是一生躬身实践的真实写照。可以说,耶律楚材是13世纪中国杰出的少数民族政治家。

“千岩竞秀清人思,万壑争流壮我观。”耶律楚材在《过金山用人韵》留下的这两句诗,既描摹阿尔泰山千岩万壑的壮阔景致,也暗合其胸有丘壑的非凡气度。群雄竞秀,有赖匠师因地制宜经营;百川奔流,需要制度加以疏导归向。身为“治天下匠”,他顺应历史大势,体恤民心所向,助力书写了在乱世中延续中华文明、巩固多元一体格局的珍贵一页。



微言法评

“卖脸”有风险 “兼职”需谨慎

据媒体近日报道,随着AI短剧行业持续火热,一种低门槛的“卖脸兼职”在网络悄然走红,一些平台宣称普通人无需专业技能,只需出镜录屏、录入面部影像、录制动态表情,即可轻松获取收益,此事引发网友广泛关注。

人脸信息属于敏感个人信息,具有唯一性、终身性。相关平台在采集到用户的人脸信息后,进而提供给AI短剧、数字广告制作方使用。很多参与“卖脸兼职”的用户只了解收益,并不知道部分平台协议可能暗藏陷阱,一旦签署,便可能导致自己的面部影像、动态表情素材被挪用,甚至被制作成虚假视频、用于电信网络诈骗等,届时不仅会导致自身肖像权被侵害,还可能无端卷入案件,维权成本远远高于兼职所得的微薄收益。并且,如果平台在协议中模糊数据存储、删除机制,当用户想要撤回授权时,已编号训练完成的AI模型、批量生成的衍生视频,未必能够完整销毁,风险会长期存续。

因此,为了守护好个人信息安全,首先需要相关平台扛起主体责任,采集人脸信息应当遵循合法、正当、必要原则,明示信息处理规则,不能利用格式条款变相诱导用户无限制授权人脸数据。其次,监管部门也应持续严厉打击非法采集、滥用人脸生物信息的行为,及时清理违规“卖脸兼职”招募信息,净化网络环境。最后,用户要摒弃侥幸心理,不随意向陌生平台提交人脸视频、动态表情素材,如确要授权面部影像,一定要仔细审阅全部协议条款,看清授权用途、使用期限、是否允许转授权、数据删除规则与违约赔偿约定,同时切勿提交身份证等其他证件材料,避免多重敏感信息一并泄露。(梁璐)

朗更为可贵。得益于法治的引领、规范和保障,作为全国文化中心的北京,电影事业呈现出蓬勃发展的良好态势,正朝着建设人才荟萃、创作活跃、市场繁荣的国际影视高地目标迈进。以2025年为例,14部北京出品的电影票房过亿,占全国票房过亿影片总数的42.42%;4部进入国产年度票房前十。从整体市场表现来看,2025年北京出品的电影累计票房达120亿元,占全国票房总额的29%。今年4月以来,“新时代 新北京”创作攀登计划深入实施,以更大力度支持和推动文艺创作。这份成绩的取得,离不开电影行业依法治理与文化软实力提升的相互赋能,也离不开政策统筹协调与营造良好电影发展环境的共同支撑。

电影是光影的艺术,票房是电影行业践行诚信理念的重要试金石。唯有坚持常态化长效化监管,压紧压实院线主体责任,筑牢技术防线,增强行业自律,多方协同发力,方能织密票房监管之网,避免“偷漏瞒虚”等行为破坏市场秩序、扭曲价值导向,进一步推动中国电影在法治轨道上行稳致远,努力实现从“电影大国”向“电影强国”的历史性跨越。

法律人语

技术赋能提升知识产权司法保护质效

□ 徐小奔

近日,最高人民法院公布5件知识产权检察办案技术支持典型案例,集中反映了检察机关主动适应知识产权案件专业性、技术性强的特点,推动检察与技术深度融合取得的办案实效,旨在充分发挥典型案例对各级检察机关办理知识产权案件的参考引领作用,加强检察办案技术支持,提升知识产权检察办案质效。

随着网络技术与数字经济高速发展,侵犯著作权的违法犯罪行为愈发隐蔽复杂,这批典型案例中的案例三和案例四,分别聚焦技术措施的认定与“盗链”行为的定性问题。这是网络技术迭代跃迁带来的新型知识产权侵权问题,也是全球范围内尚无定论的法律难题。司法机关的积极履职,为治理网络知识产权侵权提供了中国经验。

技术措施是保护网络知识产权的安全阀。网络环境下,知识产权侵权呈现出发现难、取证难、维权难的特点。权利人通过在作品上设置控制接触、禁止复制等技术措施,能有效防止知识产品被非法利用。对此,著作权法专门就技术措施的概念、禁止规避技术措施的行为和规避技术措施的例外情形作出规定;刑法也将规避技术措施纳入侵犯著作权罪的规制范畴。这意味着法律为网络知识产权保护设置了“双保险”——既直接保护知识产权,也对保护知识产权的技术措施予以保护。

不过,知识产权是蕴含复杂利益平衡的财产权。知识产权保护不仅要考虑权利人的利益,也要兼顾公共利益。如果一味由权利人采取过于严苛的技术措施,则有可能不合理地排除公众自由接触、利用作品的合法权益。因此,如何在个案中精准分析技术措施的合理性、规避技术措施的非法定等问题,成为关键所在。

此次最高检发布的案例三,为破解这一问题提供了参考。在该案中,钟某峰等人通过购买接口程序并嵌入自行研发的软件,使公司账户突破权利人软件的技术防护措施,非法接入证券公司服务器进行股票自动化交易,并以此向客户收取服务费。对此,检察机关并非仅凭权利人的单方陈述来认定技术措施,而是安排技术调查官搭建模拟实验平台,完整还原权利人软件运行时的验证机制及其被突破的全过程,最终确认案涉技术措施确属著作权法意义上的技术措施,并追究钟某峰等人法律责任。这起案例的典型意义在于:技术调查官作为检察机关的“技术外脑”,能够切实帮助办案人员透过表象看清实质。

“盗链”是深度链接技术应用于网络版权传播的“副产品”。通常情况下,深度链接技术能减少跳转步骤,让用户更方便地找到和观看内容,也能帮助平台把分散的资源整合起来,提升网站或应用对用户的吸引力。但一些不法分子利用该技术,在自己的网站上设置链接,让用户无需跳转至原网站就能直接观看他人作品,借此截取原网站的流量以获取广告或会员服务收益。由于深度链接技术具有较强的技术中立性,“盗链”行为能否按侵犯著作权罪定罪处理,一直是司法实践中的争议焦点。

案例四为破解这一难题提供了参考。在该案中,赵某来经著作权人许可,通过技术解析服务,使公众无需跳转至权利人经营的网站,便能直接播放大量中外动漫影视作品,并通过发布收费广告的方式牟利。对此,检察机关借助技术调查官对视频溯源过程、下载数据的动态变化特征、视频呈现方式等证据进行实质性审查后查明,涉案网站虽未存储相关作品,但通过“盗链”技术为公众提供了获取作品的渠道。

该案的典型意义在于:在技术调查官的帮助下,检察机关可以剥离复杂的技术运行表象对“盗链”行为的法律效果进行研判。分析发现,赵某的“盗链”行为虽未实施物理意义上的作品“上传”,但通过技术解析与页面呈现,实质性替代了权利人对作品传播渠道的控制,在功能与效果上将与作品“置于信息网络中”并无二致,使公众得以在其选定的时空范围内直接获得作品,攫取了本应属于权利人的流量利益,属于著作权法意义上的信息网络传播行为,构成侵犯著作权罪。

数智时代,侵犯著作权犯罪手段呈现出技术复杂性与法律边界模糊性的特点,对知识产权的检察保护提出了更高要求。检察机关不仅要充分了解各类新技术的运行机理与应用机制,也要准确把握不同技术事实下的差异化法律效果。这批典型案例的发布,彰显了检察机关与技术调查官等“专业外脑”积极联动的实践成效,也为治理新技术带来的复杂知识产权问题提供了治理经验。

(作者系中南财经政法大学知识产权学院副院长、教授)

热点聚焦

刘炫麟

前不久,最高人民法院、国家医疗保障局联合发布依法惩治医保骗保犯罪典型案例,集中曝光各类高发、新型骗保违法犯罪行为,再次释放出对欺诈骗保行为零容忍、严打击、全链条惩治的信号。

医保基金是人民群众的“看病钱”“救命钱”,是我国构建多层次医疗保障体系的基石,也是减轻城乡居民就医负担、维护民生底线、保障社会公平正义的重要基础。医保基金能否安全健康运行,不仅关系亿万群众的切身利益,关乎医疗卫生行业有序发展,还关乎社会稳定与民生保障大局。

经过多年不懈努力,我国现已建成世界上最大的基本医疗保障网,医保便民惠民利民政策持续释放,但医保基金监管风险隐患也不断凸显,各类欺诈骗保行为屡禁不止,严重侵蚀公共民生资源。从这个意义上说,守护医保基金安全不仅是一个经济命题,更是一个关乎社会公平正义和国家治理能力的重大法治命题。

从司法实践考察,当前医保骗保行为呈现主体多元、手段隐蔽、链条化运作甚至跨区域等特征,这对监管治理提出严峻挑战。概括而言,欺诈骗保主要包括四大类型:一是定点医药机构通过伪造病历、虚开药品、虚构医药服务项目等方式套取医保

据媒体近日报道,目前一款外观酷似课本或试卷的糯米纸零食在电商平台悄然走红。然而,在该零食的产品详情页面中并未列出配料表,一些客服人员也未给出生产厂家、生产许可证编号等相关信息。对此,多地市场监管部门相继发布食品安全提示指出,此类食品隐患突出,食用后极易危害身体健康,需谨慎选择购买。

点评:创意营销本没有错,但产品质量必须符合法律规定,这是不可逾越的底线。

文/孜然

图说世界

让每一分电影票房收入都经得起考验

□ 王开广

前不久,某电影被质疑“偷票房”一事引发网友广泛关注。涉事影片方对此发文回应称,该事件为影城操作失误所致,涉事影城也第一时间完成退票更正、补齐对应影片票房数据,并发布致歉与整改说明。此事从一个侧面反映出,电影票房管理在一定程度上仍存在“偷漏瞒虚”等不够规范的现象。

真实是电影票房数据的生命线。票房数据是广大观众“用脚投票”的真实反映,是衡量创作质量、引导行业资源配置的关键信号。然而,票房上报“偷漏瞒虚”在有的地方偶有发生,且手段不断翻新——从早期的“不出票”等简单操作,发展为如今的手写票、



漫画/高岳

阴阳票、包场不出票、无票入场、套餐拆价等花样百出的“票房消失术”。这并非个别影院的偶然失误,而是以更隐蔽方式触碰法律红线的违法行为,是对电影市场秩序的扰乱,甚至会导致“劣币驱逐良币”的恶果。

我国电影产业促进法明确规定,电影发行企业、电影院等有制造虚假交易、虚报瞒报销售收入等行为,扰乱电影市场秩序的,由县级以上人民政府电影主管部门依法责令改正,并设置了没收违法所得、罚款、停业整顿、吊销许可证等惩处措施。在此基础上,有关方面也在不断加强电影产业相关法律法规制度供给,为我国电影产业的健康发展提供法律保障,为查处虚报瞒报票房提供明确法律依据。

从地方实践来看,近年来,北京市坚持以电影产业促进法为准绳,深入推进严格规范公正文明执法,持续开展普法教育,强化行业自律,积极培育和提

电影消费市场,建立健全影视业资金奖励惩戒机制,取消票房上报“偷漏瞒虚”属地影院的电影专项资金奖励或资助资格。同时,为不断加大对票房“偷漏瞒虚”行为的查处惩戒力度,北京市文化市场综合执法总队近期公开查处了两起案件,处罚事由均指向“制造虚假交易、虚报瞒报销售收入,扰乱电影市场秩序”。这两起案件,一宗涉案金额大,一宗违法所得微薄,相关处罚释放出清晰信号:坚持对“偷漏瞒虚”票房违法行为“零容忍”,严格遵守国家关于电影票房统计管理的相关规定,加大监督检查力度,依法规范影院票房管理,严守票房数据红线,确保票房数据的真实性和准确性,从电影事业发展专项资金的正向激励到文化市场的严格执法,都传递出鲜明导向:让每一分票房收入都经得起考验,正从行业共识转化为治理常态。

票房数字不断攀升固然可喜,市场秩序变得清