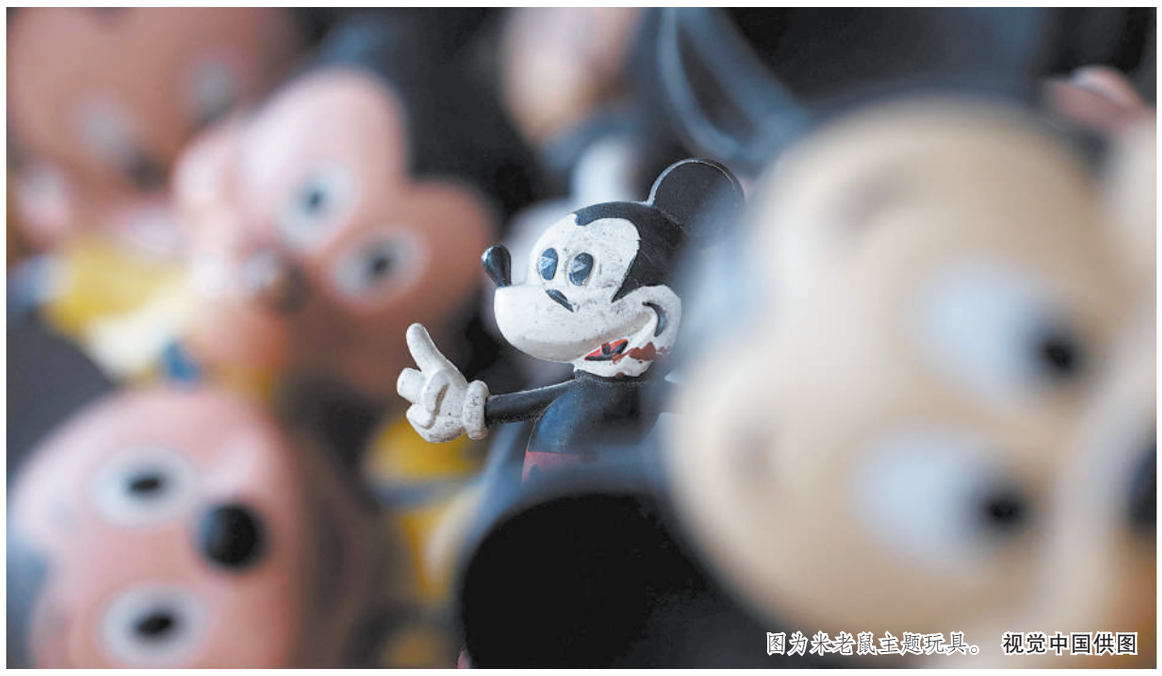
初版米老鼠“重获自由”引发版权保护热议

让保护更给力 为原创添活力

◎本报记者 孙 越 实习生 姚豆豆

据多家媒体报道，迪士尼公司的代表形象米老鼠已于2024年1月1日版权到期。这意味着，公众可以免费使用这个卡通造型。但到期的版权仅限于《汽船威利》中最初版的米老鼠设计，之后的修改版目前仍在版权保护期内。

一时之间，“米老鼠重获自由”这一话题引发热议。与此同时，版权保护问题再次进入公众视野。版权如何保护，保护的限度又在哪里？


图为米老鼠主题玩具。 视觉中国供图

米老鼠版权保护期两次延长

长期以来，“版权狂魔”迪士尼的硬核维权操作让它斩获“地表最强法务部”的戏称。米老鼠这个热门IP长达95岁的高龄就体现着迪士尼在版权方面的“疯狂”。

据了解，最初版米老鼠在1928年的有声卡通电影《汽船威利》中登场。按照当时美国的版权法，米老鼠拥有56年的版权保护期，即在1984年到期，之后任何人都可以免费使用米老鼠这一形象。

然而，在米老鼠版权即将到期前，迪士尼联合其他企业拼命地游说。很快，美国国会通过了1976年的版税立法，将版权保护期修改为75年，米老鼠版权保护期成功“续命”到2003年。

1998年，迪士尼使用了同样的方法，使美国的《桑尼·波诺版权期限延长法案》被签署。这一法案将米老鼠“续命”到了2023年，因此也被戏称为“米老鼠保护法案”。至此，米老鼠的版权总期限长达95年。迪士尼两次推动版权保护立法的操作，还引发了“经济学家大战‘米老鼠保护法案’事件”。知识共享组织的创始人之一艾瑞克·艾尔德雷德（Eric Eldred）认为，“米老鼠保护法案”违背了版权法和美国宪法“促进科学和实用艺术的进步”的初衷。

有专家同样认为，版权法的设立可以激发创作者的热情，促进文化市场的繁荣，但作品不能永远被垄断。

“自由”的作品也有使用边界

当艺术品的版权到期，它就成了全人类的公共财产。每年的年初，都有一大批书籍影音作品获得“自由”，脱离版权保护，进入公共领域。所有的创作者都可以不支付任何费用对这些作品进行二次创作。

迪士尼就是鼎鼎有名的“二创大户”。在它梦幻瑰丽的童话世界中，很多形象都来自于世界范围内的经典名著、童话故事和古老传说。例如，迪士尼将《美女与野兽》《白雪公主》《灰姑娘》等故事改编成电影，让流淌的文字变为瑰丽的画面。迪士尼也成为20世纪最伟大的“造梦机”。

版权具体包含多种权利。其中的署名权、修改权、保护作品完整权具有永久保护时限。但谈及修改权，中国人民大学法学院教授李琛认为：“修改权的效力并不在于‘禁止他人非法修改作品’，而体现为‘作者的修改不受妨害之权’。”

虽然作品超过版权保护时间限制之后，任何人都可以免费使用、传播和分享它们，但作品的使用场景仍为“是否构成侵权”的考量之一。以初版米老鼠为例，任何人都可以对米老鼠进行改编或二创，但不能让公众认为其与迪士尼有关，不能误导读者认为他们创作的米老鼠是原始版本。比如，如果将米老鼠的形象作为一款文具产品的标识，就有侵犯迪士尼商标权的可能。

上海大邦律师事务所律师游云庭说：“哪怕作品进入了公有领域，如果用米老鼠的形象拍摄一些低俗的，或者有其他不良含义的作品，米老鼠作者的继承人依旧可以进行维权。”

应分类看待二次创作作品

当前，注重版权保护已经成为社会共识。但也有人认为，过度保护可能会带来负面效应。在全媒体时代，互联网推动着文化繁荣。同时，网络上也出现了大量对文化作品的二创和改编。互联网平台上，短视频剪辑、电影电视混剪……二创作品和改编作品的火爆带来一系列讨论。有人认为，没有版权的改编和二创会损害原创作者的利益；也有人认为，如果出现版权过度保护会对创新环境造成一定影响。

2021年的“长视频反击战”就是版权方对中、短视频平台侵犯版权做出的反抗。“对这类短视频账号的打击主要涉及平台间的博弈。中短视频在影视方面的剪辑挤占了用户在长视频平台的使用时间，用户将大量时间花费在观看中短视频上，购买了版权的长视频平台反而成了配角。”游云庭说。

那么，如何守护版权？面对二次创作，又如何定义侵权？

上海交通大学媒体与传播学院副教授、数字平台与文化研究中心主任吴舫认为，应分类看待二次创作。IP粉丝基于剧情、节目的二次创作与通过截取搬运视频获利的侵权行为有本质不同。制作方对版权的主张应谨慎限制在观众集体层面的创作和消费。

著作权保护一直在路上

版权保护有利于激发创新活力。我国很早就注意到版权保护的重要性。在宋代，政府就有了规定：出版后的书如果有人翻印，就“追版劈毁，断罪施行”。这些手段不仅展示了当时社会对知识和劳动的尊重与保护，也对宋文化的繁荣有序产生了重要推动作用。

当前，我国的版权相关法律制度一直在修改完善，形成了以著作权法为核心，行政法规、地方性法规等为组成部分的版权法律体系。在互联网时代，数字作品的不断涌现给相关部门在加强互联网保护方面提出了新的要求。

相关部门一直在行动：2005年开始的“剑网专项行动”对网络侵权行为进行了严厉打击；2022年天津谭某某运营盗版网络文学App案标志着我国对盗版文学强势出手；近年来陆续开展的青少年版权保护季集中行动、冬奥版权保护集中行动等专项治理行动针对保护著作权作出努力。

“法律保护给力，原创更有活力。我国现行《著作权法》积极回应技术发展，引入了更有弹性、更加灵活的合理使用规则，在增强保护、鼓励创新的同时，兼顾作品使用人和广大社会公众的利益，为社会文化发展的繁荣提供了制度保障。”中国社会科学院法学所知识产权室主任管育鹰说。

“数字时代安全科技价值”专题研讨会举行

AI技术为安全治理提供“新工具箱”

◎本报记者 崔 爽

“数字化进入新阶段，我们面临着全新的安全挑战。”1月18日，中国社会科学院大学数字中国研究院举办“数字时代安全科技价值”专题研讨会，中国社会科学院大学数字中国研究院执行院长吕鹏在会上说，“安全风险呈现出快迭代、高智能、全覆盖的新特点。尤其是有了生成式人工智能以后，关注人工智能的安全风险更加紧迫。”

研讨会上发布了《数字时代安全科技价值报告》。该报告指出，未来，安全科技将成为公共品，与人工智能（以下简称AI）并列成为两项通用技术。具体来看，AI作为核心关键技术，将成为未来生产力的“发动机”。安全科技将作为“方向盘”，把新兴科技控制在向善的道路上。新的安全技术发展得越好，个人与社会为数字化转型所付出的代价也将越小。


图为郑州网络安全科技馆中，“手机安全的秘密”“移动终端安全”“钓鱼邮件”等展区。 视觉中国供图

安全科技将成为公共品

“当人们提到安全科技时，想到的往往是防病毒软件和防火墙软件。但全球安全科技的版图和技术工具已远远超过这个范围。”吕鹏介绍，“在网络安全、系统安全之外，还有数据安全、终端安全、AI安全、云安全等技术门类，也包括区块链、隐私计算、量子计算等前沿技术。”

浙江工业大学网络空间安全研究院院长宣琦指出，本质上，安全科技是一种伴生技术。它永远在面向新科技、新发展。比如，伴随AI发展提出智能安全，针对生物科技提出生物安全。新技术的发展有时非常快速，所以安全技术的发展和创新也同样在高速进行。

中国社会科学院科学技术和社会研究中心研究员段伟文认为，未来，安全科技必将成为公共品。整体来看，安全科技具有“压舱石”与“助燃剂”的双重价值：守住技术的安全底线，防御外部风险隐患，让技术“难作恶”；提高技术的安全上限，降低技术运行成本，让新技术得以规模化落地，让产业在安全的基础上“跑起来”。

吕鹏举例说明安全科技在产业发展中的应用。“北京中铁建工物资有限公司和蚂蚁蚁盾共建产业风控平台，用数据智能防范上下游的协作风险，产生了较好的效果。”吕鹏说，“工作效率提高了50%以上，产业授信额度的评定科学化、可量化程度也得到大幅提高。风险预测、预警、事后风险处置等都更好更精准。”

AI安全风险主要分三类

2023年，AI大模型安全风险凸显。AI技术在带来强有力的新工具的同时，也带来数据隐私、技术滥用、失控等安全问题。“加强对AI这一新兴技术的潜在风险研判和防范，确保AI安全、可靠、可控，已成为产业发展的核心要素。”吕鹏说。

在段伟文看来，AI安全风险目前来看主要可以分为三类：内生风险、衍生风险、外生风险。

在内生风险方面，AI存在技术本身的脆弱性、对数据的依赖性等自身缺陷带来的安全问题。比如，如果给数据库不断投喂带有特定价值观的数据，会对AI系统形成严重干扰，产生“数据偏见”“观点霸权”等问题。衍生风险是指AI系统因其自身脆弱性被利用或不恰当使用，可能引发其他领域的安全问题。例如生成虚假新闻、利用深度合成伪造进行诈骗等，这涉及人身安全、隐私保护等一系列社会治理挑战。外生风险也就是面向AI系统的外部网络攻击。

《数字时代安全科技价值报告》认为，当前，安全风险变得更加复杂隐蔽、强对抗、更具破坏力，将AI驱动的业务风控系统建设得更强、更智能，更好地应对大规模网络攻击与入侵，成为行业健康发展的必需。过去几年，通过应用AI来提高安全技术的效率和成功率，已经成为技术领先企业的常态。业界开始推出“大模型质检”类安全产品，成为推进大模型安全健康发展的方式之一。

“快”“慢”结合维护大模型安全

吕鹏指出，AI技术发展给安全治理增加挑战的同时，也形成AI安全治理的“新工具箱”。

谈到“用AI对抗AI”的具体产业实践，他介绍，一方面，可以使用智能对抗技术向大模型“投射问题”，观察模型生成的回答，以此实现对AI生成图片、视频等多模内容进行“真伪”辨别和安全性检测。另一方面，通过智能化风控技术，可以帮助大模型拦截外界的恶意提问，确保外部恶意诱导无法传入大模型。同时，对生成的回答内容能够进行风险过滤，保障大模型上线后从用户输入到生成输出实现整体安全防御。

整体来看，通过从已有数据中学习，AI可以更快地识别攻击的模式和趋势，从而预测未来攻击，并配置自动响应威胁功能，在更快的时间内对抗网络威胁。

吕鹏表示，维护大模型安全既要“快”也要“慢”。大模型安全防御方面要“快”，要能快速检测、查杀病毒，确保服务无毒害。大模型安全可信方面要“慢”，要能长远地、体系化地保证整个系统环境的可控、可信。

热点追踪

摆脱骚扰电话 还需用“魔法”打败“魔法”

◎新华社记者 颜之宏 赵 旭

现如今，骚扰电话越来越智能，像“长了眼”一样，对你的需求“了如指掌”。

骚扰电话“命中率”越来越高，背后有些什么猫腻？

骚扰电话对需求“了如指掌”

“我们这里有精选的几只股票，推荐您了解下呢！”接到这通电话后，厦门市民老杨直接挂断电话，把来电号码拉入“黑名单”。让老杨想不通的是，现在的骚扰电话都像“长了眼”一样，对自己的需求“了如指掌”。不久前，老杨下载了一款炒股软件，刚开始使用，当天就接到了荐股电话。“对方是机器人，说是有几只股票经过人工智能分析未来会有‘行情’。”老杨说，此后类似骚扰电话层出不穷，一天至少四五通，多的时候十来通。

无独有偶。这类骚扰电话也让北京市民李先生不堪其扰。“不接怕错过工作电话或快递电话，接了后也屏蔽、举报过，但没啥效果。”李先生说，这些由机器人拨打的骚扰电话会不停更换“马甲”来电，即使“拉黑”也没用。

在黑猫投诉平台上，有400余条有关“使用机器人向用户拨打骚扰电话”的投诉。

12321网络不良与垃圾信息举报受理中心公布的《2023年第三季度垃圾信息投诉情况盘点》显示，在2023年三季度骚扰电话投诉中，94.5%与商业营销相关。

记者了解到，利用人工智能开展电话营销正大行其道。在网络上搜索“外呼电销”，显示的搜索结果中大部分都是“人工智能外呼服务”。

“精准”骚扰背后的猫腻

现在的骚扰电话缘何越发精准？

在某二手交易平台上，记者使用指定关键词检索时发现，一些商家在商品简介中声称可以提供“精准客户手机号”。

一名商家向记者展示了其客户信息的采集渠道，包括两家短视频平台和一家“达人种草”类平台，每个客户的信息还包括其具体需求描述。当记者询问其数据来源是否合规时，该商家表示“您放心吧，我们不会干违法的事”。

“通过此类渠道获得的用户信息有可能是用户‘授权’提供的。”中国电子技术标准化研究院网安中心测评实验室副主任何延哲举例说，在一个二手车交易App里，客户想要了解某部车的底价，需填写手机号。如此一来，平台、二手车商、第三方销售人员可能都会获取该联系方式，“仔细查看软件的用户协议，会发现平台会要求用户‘授权’提供大量个人信息，甚至是以‘捆绑’方式向多方提供。”

记者发现，某“种草”类社交App的隐私政策提示，该App会将用户个人信息与“商业合作伙伴”进行“必要的共享”，这些“合作伙伴”包括但不限于平台第三方商家、第三方物流服务商、广告和统计分析类合作伙伴等。隐私政策还提示，当用户选择参加相关营销活动时，在“经过用户同意”后，会将用户姓名、性别、通信地址、联系方式、银行账号信息等与“关联方”或“第三方”共享。

“随着人工智能的使用，个人信息攫取和电话拨打效率大大提升了。”网络安全专家荣文佳说。

“你在购物App上的交易行为，在短视频App上的浏览习惯，在社交App上的发帖回复，背后都有人工智能在打‘电子标签’，也就是人们常说的‘用户画像’。”荣文佳解释说，这些“电子标签”会被脱敏并深度加工，而后分享给各大App的合作机构，而合作机构又能通过一些手段就这些“电子标签”与相应用户重新关联，这就是推送广告和推销电话都越来越精准的原因。

北京航空航天大学法学院副教授赵精武说，当前骚扰电话屡禁不止，主要治理难点在于个人信息泄露的来源难以确定，针对第三方营销公司业务人员故意或过失泄露客户信息的情况仍存监管难题。同时，部分App、网络平台等将个人信息买卖做成黑灰产业链，销售对象并不以特定行业为限，“用户无法确定自己的信息是从哪个平台泄露的，难以找到证据。”

如何治理骚扰电话“牛皮癣”

近年来，国家有关部门通过多种手段治理骚扰电话取得一定成效。2023年上半年，共拦截垃圾信息超90亿次，拦截涉诈电话14.2亿次和涉诈短信15.1亿条。工信部还推广“骚扰电话拒接”服务，强化电信网络诈骗一体化技防手段；印发《关于进一步提升移动互联网应用服务能力的通知》，加强App全流程、全链条治理。

此外，三家电信运营商已于2019年10月面向全国用户推出“骚扰电话拒接”服务。

北京邮电大学教授曾剑秋表示，骚扰电话根治存在难度，其根本原因在于商业推销需求长期存在。“骚扰电话成本低、可变现，这种经济利益驱使骚扰电话形成产业链，骚扰新方式层出不穷，给治理带来困难。”

根据个人信息保护法，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。不得以个人不同意为由拒绝提供产品或者服务。违反该法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。然而，因为个人信息泄露方式多样化，监管机构难以实现全面、及时、有效的监管。

赵精武建议，应加大对个人信息泄露投诉渠道的宣传推广力度，鼓励全社会增强个人信息保护意识，同时督促应用商店采取安全保障措施，对上架App是否存在非法收集个人信息行为进行事前核验、事中复查及事后屏蔽，做好问题上报工作。

曾剑秋建议，应加强网络技术投入和研发，实现信息贩卖、泄露可追踪、可取证，设置消费者“一键举报”等功能。

何延哲等专家还建议，相关电信服务提供商应强化运用人工智能等科技手段的监管能力，用“魔法”打败“魔法”，“人工智能提升了骚扰电话的拨打效率，有关平台同样应运用人工智能对此类行为深度学习，及早发现并阻断利用人工智能呼出骚扰电话的违法违规行为。”