公诸于世

创作自由还是侵权行为?
记者调查AI生成内容乱象

随着人工智能技术的飞速发展,多元化的艺术重构形式被催生,从影视二次创作、AI歌手翻唱到绘画风格模仿,AI生成内容(AIGC)在拓宽创作边界的同时,也让“合理使用”与“侵权”的界定愈发模糊。AI生成内容的法律责任究竟如何划分?

AI“魔改”层出不穷

从《泰坦尼克号》的经典镜头,到《让子弹飞》的“敢杀我的马”;从周润发的美元点烟,到张敏的回眸一笑,没有什么照片是不能“吉卜力化”的。吉卜力风格,是指日本吉卜力动画工作室(由宫崎骏等人创办)的艺术风格,具有手绘动画、色彩柔和等特点。“吉卜力化”在社交平台刷屏背后,OpenAI的GPT-4o模型“立大功”,用户只需借助图像生成功能便可生成吉卜力风格的照片。

有业内人士解释,AI模型能够生成吉卜力风格的图片,和模型前期的训练数据相关,大模型对海量数据中所包含的知识进行了学习。利用版权作品训练AI模型是否属于合理使用,以及从网络爬取内容用于数据库是否构成侵权,这些问题目前仍处于法律的空白地带,尚未有明确的法律定论。

付费改编仅需数元

记者调查发现,用AI工具“魔改”影视作品的门槛并不高。在某交易平台上,有大量标题为“付费AI‘魔改’视频”的帖子,称只需几元至十几元便可请人制作一段AI视频,时长在3秒钟到3分钟之间,改编内容覆盖大量动漫、影视作品。“Muse AI歌曲代创作”则只需3.5元便可生成一首歌曲,“风格、语言、人声和性别都可以指定”。卖家直言:“用明星脸也行,但容易被告。”

受访专家指出,对影视改编作品的侵权判定,需深究其性质,综合多方因素衡量考虑。华东政法大学知识产权学院特聘副研究员姚叶说:“对于经典影视作品,我们需要具体判断二创作品的性质,比如究竟侵犯了原作的什么权利?它对原作的使用范围、数量和质量有没有形成一种例外?如果仅停留在戏谑调侃方面,那么一般认为是合理使用,如果通过恶意剪辑扭曲情节、诋毁原作名誉,则可能侵犯了原创者的信息网络传播权或其他权利。”

在京都律师事务所竞争法律事务部主管合伙人王菲看来,此类视频以经典剧集为根基,显然涉及对原作的侵权,但在法律责任界定的角度,AIGC产品的研发者、服务者以及使用者三方是否同样需要对“魔改”视频侵权行为承担责任,成为相关部门判定时的棘手难题。同时,生成视频通过算法对素材重新组合、加工后,将经典影片原有叙事节奏与结构进行了颠覆性调整,传达出截然不同的情感与寓意,其所呈现出的独创性又让相关作品是否侵权难以被轻易裁定。

受访专家认为,当AI成为“创作者”,关于版权边界的共识应该是:创新不能践踏原创的土壤,技术中立更不意味着责任真空。唯有守住这条底线,AI才能真正成为艺术进化的伙伴,而非埋葬创意的铲子。

□ 赵丽 殷增梓
《法治日报》4月26日

情理法理

山西『十岁男孩被生母继父虐死案』宣判

4月28日,山西运城临猗县“10岁男孩被生母继父虐死案”在运城市中级人民法院开庭并宣判:该案被害人张某某继父王某虎被判处死刑、生母谢某朵被判处无期徒刑。

2023年5月初,张先生得知10岁的儿子张某某离家出走后失踪,在社交平台多次发布寻人信息。孩子失踪前,由其生母谢某朵和继父王某虎抚养,两人也在社交平台发布寻人启事,哭诉找不到孩子。

2023年5月8日,山西临猗县公安局发布协查通报称,接到谢某朵报案,称其儿子张某某在临猗县临晋镇下豆氏村离家出走。临猗警方表示,如有线索请与临猗县公安局刑侦大队联系,公安机关经核实后给予1万元奖励。

临猗县公安局于同年5月23日找到失踪人员张某某,已确认死亡。犯罪嫌疑人谢某朵、王某虎被临猗县公安局抓获。

据该案起诉书显示,2023年5月2日22时许,王某虎指使谢某朵取来三角带并将已熟睡的张某某叫醒带到客厅进行“管教”,二人先后持三角带殴打张某某,迫使张某某承认偷拿家中现金。5月3日凌晨,张某某大便失禁,几小时后谢某朵发现孩子身体冰凉无呼吸。5月4日凌晨,王某虎将张某某的尸体掩埋至其祖父的坟墓中,指使谢某朵报案称孩子离家出走。5月15日,二人恐罪行败露驾车逃至外省,7天后被警方抓获。

经鉴定,被害人张某某符合腰背部、臀部、四肢等部位被钝性外力长期反复多次击打致软组织缺血、挫伤、变性、坏死引起肾脏等器官功能减退合并创伤性休克而死亡。

检察院认为,被告人王某虎、谢某朵系共同犯罪,在共同犯罪中均起主要作用,均系主犯。犯罪手段极其残忍,犯罪后果极其严重,并且均一人犯数罪,应当数罪并罚。以故意伤害罪、虐待罪对两人提起公诉。

起诉书显示,被告人谢某朵、王某虎于2022年2月登记结婚,在此后长达一年多的时间里,二人对其子张某某进行了长期虐待。

2021年,谢某朵与张先生离婚。张先生称,谢某朵出轨,还经常问他要钱后失联,养不起她,不得不离婚。次年,谢某朵与王某虎登记结婚,被害人张某某跟随二人生活。

□ 舒隆焕 孔文龙
综编自极目新闻、东方网、《新民晚报》4月28日

讲法问津

扫码多付1.9万余元竟是洗钱套路

警方揭穿“跑分水军”猫腻

一台抽水泵的售价为300元,男子在购买时扫码支付显示的结果却为19999元,他称多出来的钱是公司发的工资,让老板退给他。这件事看似正常又有点让人感觉奇怪,老板有些为难。思考片刻,决定让警方来“评判”此事。而警方经过调查后,这名男子和同行的3名同事被“一窝端”。

据四川省资阳市公安局雁江区分局消息,经查,上述男子实为“跑分水军”的一个小组,其先用押金“承包”下境外诈骗团伙的赃款,然后开车到全国各地寻得线下商户的收款二维码后,提供给诈骗团伙转移受害群众的“血汗钱”。目前,初步查获的涉案金额共计22.26万元。犯罪嫌疑人覃某宏、覃某炜、劳某龙、陈某威已被警方刑事拘留。

据覃某宏、覃某炜、劳某龙、陈某威交代,四人均来自广西南丹县,系初中同学,覃某宏是“跑分车队”的队长。3月6日至3月13日,覃某宏4人在贵州省安顺市、泸州市、自贡市、内江市、资阳市等地,通过线下寻找商户提供收款二维码后,提供给诈骗团伙转移诈骗资金,涉案金额共计22.26万元。让四人铤而走险的背后是所谓的高收益。几人分工明确,覃某宏负责联系上家,覃某炜、劳某龙、陈某威分头随机选择商家拍摄收款二维码,每完成一单覃某宏抽成23%,队员则抽成20%。

目前,四人已被资阳市公安局雁江区分局刑事拘留,案件正在进一步侦办中。

犯罪嫌疑人指认现场

四川省资阳市公安局雁江区分局
四川长安网4月28日

我们的隐私如何流入“黑市”?

因为一句“不称心”的评论,个人隐私信息就被人挂上网,本人和亲友遭到部分网民的无端骚扰和人身攻击。常常接到的骚扰电话,甚至是诈骗电话,让人不堪其扰。这些都意味着个人隐私已被泄露,由此产生“隐私焦虑”。近年来,有关部门陆续出台多部保护个人隐私信息的法律法规和政策文件,有效遏制个人信息大肆泄露,但普通群众的“隐私焦虑”仍会因为个案发生被反复激发,我们该如何保护个人隐私?

普通人的“隐私焦虑”

前不久,一网民因对某位艺人一句看似稀松平常的评论,就遭到“人肉开盒”引发的网暴。“简单来说,‘人肉开盒’就是过去的‘人肉搜索’,不法分子通过非法渠道获取你的个人信息,并在网上曝光,从而达到实施网络暴力的目的。”中国科学技术大学网络空间安全学院教授左晓栋说,个人信息的“盒子”,一旦被居心叵测的人打开,当事人的户籍身份、生活轨迹、亲友关系网等个人隐私都可能被公开,继而不得不承受来自网络世界的恶意和敌视。

“开盒”的门槛并不高,任何人都可能成为“被开盒”的对象,公众对此普遍存在焦虑。“开盒并没有什么技术含量,一些未成年人参与其中,有的是为了炫技,有的则是寻找自己在虚拟世界中的存在感。”浙江大学计算机科学与技术学院院长任奎说,网络世界具有一定的匿名性,这也让施暴者产生了“只要我躲在屏幕后面你就找不到我”的错误认知,进而实施违法犯罪活动。

记者调查发现,用以“开盒”的个人隐私信息大多来自海外“社工库”(一种由泄露数据打造的信息查询库),不法分子根据买家需求提供“有偿查询”。一份由某卖家提供的“报价单”显示,500元可购买指定人员的“全家身份证号和照片关系”、3300元可购买“开房(带同住人)信息”、5000元则可获得指定人员的“日常生活轨迹信息”。

“个人信息的买卖一般是新的旧的‘一起卖’,真的假的‘混着卖’。”一位业内人士告诉记者,因为所有兜售的个人信息都是通过非法途径获取的,不少卖家手里的信息也是“二手”甚至“多手”信息,所以有的信息是“陈年信息”,有的信息则是编造的“虚假信息”,甚至是打着“兜售隐私”名义的诈骗。

隐私流入网络“黑市”

一张外卖单、一个快递盒、一次街头活动随手填写的个人信息,都可能成为“被开盒”的素材。

——外卖和快递是个人隐私泄露的重灾区。“我的外卖和快递从来不填到具体的门牌号,就近放快递驿站或者外卖柜就行。”从事多年网络安全工作的荣先生告诉记者,在个人信息保护法等相关法律法规对企业加以限制以前,网络黑灰产业能把一家企业的用户数据库整个“拖库”,造成手机号、收件人姓名、地址等信息泄露,“还有一些不法分子会专门搜集快递面单,其目的是获取面单上的收件人地址等隐私信息”。

——“海投”简历也可能造成个人隐私泄露。公安部发布的案例显示,吉林长春公安机关查明,2024年1月以来,以王某明为首的犯罪团伙伪造工商营业执照,在招聘网站发布虚假招聘信息骗取求职者简历,并出售给电信网络诈骗等犯罪团伙牟利。“求职者一定要擦亮眼睛,一方面要在权威求职网站上求职,另一方面不要随意海投简历,防止敏感个人信息被不法分子截胡。”左晓栋说,求职简历包含多重敏感信息,求职者也要通过多种渠道查查招聘企业的“底”,防止不法分子盗用个人隐私。

——贪小便宜,参与“拿小礼品扫二维码”的街头活动会将你的个人隐私拱手相让。“扫码领小礼品”的街头活动,可能是为了“提升品牌知名度”的商业推广行为,也可能是不法分子在以极低的价格套取个人信息。“面对‘街头诱惑’,不听、不信、不透露,就是保护自己的最好方式。”厦门市打击治理电信网络新型违法犯罪中心民警洪恒亮说,被套取的个人信息可能被用以实施针对个人的精准电信网络诈骗,由此造成的后果可能比“人肉开盒”更为严重。

多方合力方能堵住“黑洞”

堵住个人隐私的泄露“黑洞”,不仅需要国家在立法和执法层面更有作为,也需要社会和个人相向而行。

近年来,网络安全法、数据安全法、个人信息保护法等法律法规相继出台并实施,两高出台《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》,明确“侵犯公民个人信息罪”的定罪量刑标准,非法获取行踪轨迹信息50条以上即构成犯罪,非法获取普通信息5000条以上可入刑。2024年,全国公安机关深入推进“净网”专项行动,捣毁一批个人信息交易平台,全年共侦破相关案件7000余起。

任何人都不能在非法隐私交易中独善其身,数据高度集中的政企机构更应关注合规要求。北京康达(厦门)律师事务所张翼腾律师认为,有关机构应设立数据保护官和独立监督机构,严格落实国家有关公民个人信息保护规定,设计一套风险硬隔离的运行机制,杜绝“内鬼”内外勾结的可能。

应从小培养个人信息保护意识,加强未成年人网络行为的法治教育。任奎等专家建议,针对当前一些未成年人参与“开盒”的网络暴力事件,有关部门应主动作为,在普法教育中建立有效的家校联动机制,既要教育未成年人远离隐私买卖“黑洞”,也要通过一定的教育形式,帮助误入歧途的未成年人重回法律正轨。

在任何可能涉及个人隐私交互的领域,尽可能隐匿个人信息的有效片段。基层民警建议,普通人在点外卖、寄送快递、线上招聘等场景下,填写个人身份信息时,要学会隐去诸如居住地门牌号、身份证号等信息,对于无需实名的场合,可有选择性地使用化名,防止不法分子将非法获取的个人信息相互串联。

□ 颜之宏
半月谈网4月25日