医学人文

医疗机构应用人脸识别技术的法律风险与规制研究

张 瑞[1]，班艺源[2]
1. 南京师范大学中国法治现代化研究院，江苏 南京 210023；2. 山西大学法学院，山西 太原 030012

摘 要：人脸识别技术极大地提高了医疗机构运营管理效率，同时也伴生了潜在的技术应用与法律风险。在主体合规层面，医疗机构并不是应用人脸识别技术的天然合规主体；在具体实践中，置身视频监控人脸识别设备审视下的医生的诊疗自主性存在被侵蚀的风险；在信息权利的保障上，患者相对人的知情同意权也有被实质架空的风险。这就意味着必须针对法律风险完善相应的规制进路：强化医疗机构应用人脸识别技术的合规性，区分人脸识别技术在医疗机构应用的不同场域，切实保障患者相对人的知情同意权利等方面着手补充。

关键词：数字时代；人脸识别技术；医疗机构；规制困境；知情同意权
中图分类号：R-052 **文献标志码**：A **文章编号**：1671-0479(2024)04-369-006
doi：10.7655/NYDXBSSS240244

随着医疗机构在医疗、服务、管理“三位一体”智慧医院建设的不断推进，人脸识别技术在“智慧服务”“电子病历”“智慧管理”等应用领域发挥了重要作用。具体来说，从身份验证、预约挂号和自主缴费，到就诊检查、打印报告和医保结算，人脸识别技术通过综合运用生物识别、人工智能比对、大数据算法等技术要素，广泛地应用于全过程的医疗场景。2020年7月，国务院办公厅印发《深化医药卫生体制改革2020年下半年重点工作任务》，鼓励开展基于大数据的医保智能监控，推广视频监控、人脸识别等技术应用。2021年6月，国家卫健委发布《国家卫生健康委办公厅关于实施进一步便利老年人就医举措的通知》，鼓励在就医场景中应用人脸识别等技术。2021年7月，国家医保局发文鼓励推广运用人脸识别技术，实现参保人“刷脸”就医住院。在此背景下，各地医疗机构普遍将人脸识别技术作为推动医疗机构数字化转型，提高数字化质效的有力提升点。2023年4月，河南省医疗保障局印发了《关于全面推进医疗保障智能场景监控系统应用的方案》，要求市县乡三级覆盖应用智能场景监控系统和感知设备，运用“视频监控+人脸识别”技术，实现诊疗数据和服务影像的事实对比，同步在线监控。

其间，应用人脸识别技术情境下患者大量的个人信息（如姓名和身份信息，人脸虹膜等生物学信息，病史病症和就诊记录等隐私信息）被收集到人工智能的算法数据库中进行数据分析、人脸比对和算法处理。在这个过程中，医疗机构应用人脸识别技术确实存在着一定事实争议和法律风险。例如，人脸信息泄露风险、人脸识别技术应用不透明带来的患者知情同意权利受损风险等。尤其是，医疗机构所承载的社会职能和相对人具有一定的特殊性、不可替代性和复杂性，要求患者相对人的个人权益必须受到格外重视。因此，本文将基于人脸识别技术在医疗机构应用的特殊场域语境，就人脸识别技术应用的法律风险和规制路径进行分析和阐释，以期充分保障患者相对人的人格尊严和个人信息安全，为医事活动的有序开展提供智识资源。

一、医疗机构应用人脸识别技术的法律厘定

人脸识别技术是综合运用计算机视觉技术和算法模型，基于人脸信息所具有的独特性、直接识别性、不可更改性、易采集性、不可匿名性等特征[1]，

基金项目：中国法学会部级法学研究（自选课题）“人工智能的公法规制研究”[CLS(2023)D70]；中国法学会民法学研究会青年学者研究项目“大数据时代个人信息侵权‘损害’概念研究”（2022MFXH014）
收稿日期：2024-06-05
作者简介：张瑞（1992— ），男，山东东营人，博士研究生在读，研究方向为卫生健康法学、法治现代化，通信作者，prisoner24601@163.com。

通过将人脸识别设备采集到的人脸图像及面部特征与数据库中的数据信息进行对比，从而精准识别和验证相对人身份信息的一种新质数字技术，在保障公共安全、维护社会秩序、便捷身份验证等治理层面具有显著优势[2]。进入数字时代以来，数字化场景赋能成为新质数字技术与现实医疗应用场景结合的普遍选择，在极大地提高了医疗机构运行效率的同时，也带来了诸如安全性的疑问。因此，在分析医疗机构应用人脸识别技术的法律风险之前，首先要明晰人脸识别技术的医疗应用场景，同时对人脸识别信息的法律性质予以界定。

（一）人脸识别技术应用的法学研究概述

从现有人脸识别技术的相关法学研究来看，学界对人脸识别技术应用和人脸识别信息的法律保护、法律规范和制度建构已经进行了一定的研究和论证，相关细节的讨论也比较充分。例如，有学者从人脸信息是个人生物识别信息的角度，主张规范个人生物识别技术的研发和应用，确定侵犯个人生物识别信息权利的法律责任，构建危害生物信息安全的制裁体系[3]；有学者从公共场所视频设备应用人脸识别技术的维度出发，主张应遵守个人敏感信息处理的有关准则，保护信息主体的选择权，承担具有结果义务性质的信息安全义务[4]；有学者从侵权责任认定损害的角度论证非法收集和滥用人脸信息者的侵权责任[5]；有学者试图通过从应用层、系统层、技术层、信息层着手进行人脸识别技术应用的分层治理，以期规避人脸识别技术对个人基本权利和社会公共利益的威胁[6]；更有学者从刑事案件实证分析的角度，分别从非法获取、提供、出售人脸识别信息和破解人脸识别核验的角度，分析涉及人脸识别的犯罪行为的刑事规制路径[7]；也有学者从欧美法律模式比较评价的角度探讨生物识别信息商业应用的立场与进路[8]。

总结分析来看，虽有上述学者从多个维度对人脸识别技术的应用进行了阐释和论证，但现有的研究大多基于人脸识别技术的商业应用场景展开，或是就人脸识别信息是隐私权、肖像权、财产权抑或某种新兴权利进行分析和证成，对医疗机构这一特殊的主体和场域应用人脸识别技术的智能应用场景的相关法学研究相对较少，也几乎没有学者就医疗机构应用人脸识别技术的法律风险给出具体的应对策略或解决方案。

（二）人脸识别技术的医疗应用场景分析

围绕医疗机构应用人脸识别技术的具体问题开展卫生法学领域的具体研究，首先需要明确的是人脸识别技术的医疗应用场景，也即回答“人脸识别技术在医疗机构中是如何应用的”这个问题。根据2022年10月国家市场监督管理总局和国家标准化管理委员会发布的《信息安全技术 人脸识别数据安全要求》（GB/T 41819—2022），人脸识别技术的典型应用场景主要有人证比对、解锁支付、核对身份等几个主要应用场景。

通过对几家医疗机构的走访调研可以发现，目前医疗机构中人脸识别技术的应用场景主要有以下几个方面：第一，医疗机构通过运用人脸识别技术获取特定范围群体的人脸数据信息，用于职工考勤、院区管理、门禁出入等权限管理；第二，人脸识别技术在医疗机构的挂号缴费和医保支付环节也发挥了重要作用，不少医疗机构应用由第三方服务运营商提供服务运行维护的人脸识别设备，对患者的医保账户或其他支付账户予以支付和核销；第三，医疗机构是人流密集的重点公共场所，出于公共安全需要，公安部门会在部分出入口和重点地区，统一设置安装具有人脸识别功能的“天眼系统”等治安摄像头和高空摄像头，并运用人脸识别技术扫描和追踪重点人群。而根据《关于全面推进医疗保障智能场景监控系统应用的方案》要求，未来医疗机构将全场景覆盖“视频监控+人脸识别”设备，这就使得进入医疗机构的每个公民个体都将成为人脸识别技术的审视对象，人脸识别技术在医疗机构的应用场景外延将不断开拓。从这个意义上讲，政府和企业都越来越能够追踪、分析、预测、监控个人的行为，并且这种能力达到了一个前所未有的程度，如不加以有效约束，这些科技发展会给人的尊严、自主性、隐私和一般意义上的人权带来重大的风险[9]。

（三）生成人脸识别信息的法律性质界定

从学理层面分析来看，目前学界就现实中人脸识别技术应用所生成的相关人脸识别信息的法律性质界定，有着关于人脸识别信息究竟是隐私权还是肖像权，是人身权利还是财产权利等诸多争议。但基于现有的法律框架和法律定义话语的规范表达，可以对人脸识别信息的法律性质予以基本明确。具体而言，《信息安全技术人脸识别数据安全要求》将人脸识别信息界定为生物识别信息。而根据《中华人民共和国民法典》的表述，个人信息的范围包括生物识别信息。因而，人脸识别信息作为生物识别信息的范围之一，在法律性质上属于个人信息的范畴。而根据《中华人民共和国个人信息保护法》对“个人信息”所作出的定义，“个人信息”是以电子或者其他方式记录的，能够单独或者与其他信息结合，识别特定自然人身份或者反映特定自然人活动情况的各种信息。简单来说，这些个人信息能够直接或者间接地指向确定的主体[10]。而人脸信息因“人脸”所具有的天然唯一性可以直接指向确定的相对人个体，因此人脸识别信息符合个人信息

所须具有的全部特性。同时,虽然我国现行有效的法律法规暂未对个人信息的财产权利属性作出具体规定,但在《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》中明确倡导“探索数据分享价值收益”,也即在某种意义上以规范性文件的形式通过承认个人信息数据在数字时代背景下具有一定的经济价值,变相认可了个人信息的财产权利属性。因此,人脸识别信息是一种具备财产权利属性的个人信息。

二、医疗机构应用人脸识别技术的法律风险

从医疗机构应用人脸识别技术的实践来看,许多医疗机构将其作为数字化赋能医疗的亮点工作,如不少医疗机构陆续投入使用了“数字化病区管理人脸识别系统”“人脸识别非接触式无纸化系统”等数字化应用程序,来改善和提升患者的就医体验。也有地区,如四川省的助产机构、出生医学证明办理机构须根据《四川省卫生健康委员会关于进一步加强出生医学证明管理的通知》(川卫办妇幼便函〔2024〕2号)的要求,通过人脸识别确保“人”“证”一致。在人脸识别技术在医疗机构场景得到广泛应用的同时,也要辩证地看到其存在着法律风险。

(一)医疗机构存在技术应用主体合规风险

首先,在传统的公法实践中,个人信息的采集主体是行政机关、政府部门等公权力主体。这些公权力主体主要是基于行政职权、法律法规授权或委托,依照其行政职权范围和上级行政机关的命令要求,依法依规按法定程序采集和利用公民相关个人信息,以满足特定的行政管理需要,而医疗机构显然不具备公权力外观。在现实语境下,由于我国东西部地区之间存在的经济社会发展差异,医疗机构的法律性质也较为复杂。但从占多数的情况来看,我国的公立医疗机构多为公益性事业单位,并无行政执法权和对外的行政管理职权,私立医疗机构多为企业和非企业单位,同样不具备公共主体资格。因而在这个意义上讲,医疗机构并不具备公法意义上出于公共管理职能和目的去安装图像采集、个人身份识别设备的天然合规权限,不是应用人脸识别技术的合规主体。其次,《中华人民共和国个人信息保护法》第二十六条规定:“在公共场所安装图像采集、个人身份识别设备,应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的,不得用于其他目的;取得个人单独同意的除外。”而医疗机构应用人脸识别技术的目的并不仅仅是为了公共安全需要,前述医疗机构人脸识别技术的应用场景也多是出于便利医疗机构内部行政和人事管理,提高医疗机构运营效率的需要。同时,在市场经济背景下医疗机构也容易受到经济人假设的驱使,为谋取更高经济利益回报而将获取的人脸识别信息应用于商业目的,或因不当人脸识别算法的使用对患者带来实质意义上的价格歧视。最后,《中华人民共和国民法典》第一千零三十三条规定:“除法律另有规定或者权利人明确同意外,任何组织或者个人不得实施下列行为:(三)拍摄、窥视、窃听、公开他人的私密活动;(五)处理他人的私密信息;(六)以其他方式侵害他人的隐私权。”也即明确禁止任何组织和个人通过拍摄方式侵害自然人的隐私权。现实语境下,尽管医疗机构在常识意义上属于公共场所,但患者相对人具体的私人就诊行为本身即具有天然正当的私密属性,患者相对人进行医学检查和接受医学诊断的客观需要,也决定了医疗机构内的部分场所(如病房、检查诊室等)不宜也不应具有开放性。而部分地区的卫生健康主管部门以“视频监控+人脸识别”设备全覆盖作为目标,要求医疗机构无死角安装和应用人脸识别技术设备,无疑会拍摄到患者相对人的个人隐私,进而侵害自然人的隐私权利。因此,在人脸识别设备“谁来装”这个问题上,医疗机构存在主体合规的风险。

(二)医生诊疗行为存在自主性被侵蚀风险

在医疗机构传统的诊疗模式下,患者相对人基于对医生和医疗机构资质等级、专业资格的信赖和认可,通过挂号和分诊向医生寻求诊疗帮助,医生基于患者的病情病症和相关检查结果做出具体的医疗诊断。假使按照《方案》要求,三级医疗机构将全场景覆盖“视频监控+人脸识别”设备,则医生开展医事诊疗服务的自主性有被侵蚀的风险。

首先,在医疗机构的空间场域内全部覆盖应用人脸识别技术,则意味着医患双方将在具备人脸识别功能的视频监控设备的审视下阐述病情和开展工作,摄像头的凝视势必会加剧医患双方的紧张感,降低患者对医生和医疗机构的信任。其次,人脸识别技术的应用将动摇基于面诊形式的诊疗模式。实践中,医生通过听取患者对自身病症的主诉,结合检查报告和自身医学经验做出正确的医事诊断。而在视频监控设备的审视下,就诊室将不再是密不透风的安全堡垒,患者基于自身隐私安全和私密因素考量可能不会如实、全面地讲述自己的病症表现,这类“难言之隐”的情形势必会影响医生诊断的准确性和科学性。最后,在理想的良好的医患关系下,医生彻底信任患者就必须使医生在专业判断出错时还能受到保护,即不会面临投诉、索赔或面对医疗委员会的质询[11]。医事活动作为因人因病情而异的特殊的具有不确定性的社会活动,本身即具有相当复杂性和风险性。而在人脸识别技术

和视频监控设备全覆盖的情况下，一方面，患者会对医生和医疗机构产生一定程度上的抵触心理，不利于患者如实全面地陈述病情；另一方面，医生基于空间场所内实时视频留痕的外部环境因素，可能在医疗结果的诊断过程中片面追求诊断结果不出错，做出保守的诊断而非追求诊断结果的正确，从而规避潜在的医事责任和执业风险。在这个意义上讲，人脸识别和监控设备在医疗机构中的存在会侵蚀医生从事诊疗行为和医事活动的积极性，从而造成医生和患者“双输”的局面。

（三）患者相对人存在知情同意被架空风险

在数字时代背景下，由于个人无法按照自己的意志控制信息的产生、存储、转移和利用[12]，自然人个体只要置身社会生活之中就会不断生成各类信息数据。因此，为了有效保障自然人的信息权利，《中华人民共和国民法典》《中华人民共和国个人信息保护法》专门设定了“知情同意原则”。也即，在对自然人的相关个人信息进行采集时，要确保相对人“知情同意”。例如，医疗机构应用人脸识别技术采集相对人相关个人信息，就要在程序上对相对人进行明确的告知，确保相对人充分了解医疗机构采集相关个人信息的目的、方法、用途和相关风险，在确保相对人知情的基础上获取相对人同意医疗机构应用人脸识别技术的明确意思表示。而事实是，实践中理应作为医疗机构应用人脸识别技术前提条件的“知情同意”原则有被架空的风险。

首先，《中华人民共和国民法典》规定使用人脸识别技术须以相对人的明确同意为前提并设置显著的提示标识。而在实践中的绝大多数情况下，患者相对人并未被告知也无从得知其进入医疗机构的空间范围内，就意味着要接受人脸识别技术和视频监控设备的拍摄和识别。其次，即便患者相对人就医疗机构应用人脸识别技术相关情况充分“知情”，但患者相对人并无就此提出异议或是反对的实质权利和具体途径。从医患关系的角度分析，患者相对人前往医疗机构寻求医学救助，时间上往往具有紧迫性；且医疗机构是患者相对人寻求医疗救助的近乎唯一选择，空间上具有不可替代性。因此，患者相对人在医患关系中处于相对弱势地位，即便患者相对人不同意人脸识别技术对自身人脸和相关个人信息的识别和采集，但其在医疗机构面前并无太多议价和选择的空间。最后，医疗机构并未为患者相对人提供除了接受人脸识别身份验证之外的其他途径。实践中医疗机构往往将人脸识别和身份信息实名验证作为进入医疗机构场所空间的第一步，也即医疗机构以全有或全无的方式剥夺了患者相对人在不同意人脸识别情况下进入医疗机构内的其他可能性。在这个意义上讲，患者相对人进入医疗机构也就意味着其同意接受医疗机构对其进行的人脸识别和信息采集，人脸信息的权利让渡在某种意义上成为就医的代价，患者相对人的知情同意权利在实质意义上被架空。从而使得进入医疗机构场域内的每个自然人个体的隐私权、个人信息权利、人格尊严等合法权益有受到侵害的风险。

三、医疗机构应用人脸识别技术的法律规制

健康自古以来便是人的基本需求[13]，在人脸识别技术这类新质数字技术更多地应用在医疗机构场域的新情境下，健康的实现不应以患者的权利受到潜在侵害为代价。因此，必须采取有效措施消除这类技术应用带来的法律风险[14]，更好地满足人民群众不同层次健康需求，进一步提高服务效率和质量[15]。

（一）强化医疗机构人脸识别合规性

在医疗机构业已普遍应用人脸识别技术的现实语境下，已无再去纠结人脸识别技术是否可以在医疗机构中应用的必要，而是应当从完善技术应用规范和管理制度合规的角度，对人脸识别技术应用的规范性予以强化。通过制度明确有权进行人脸信息采集、保存、使用的合规主体，以事前准入、事中控制和常态监管为切入点全流程加强人脸识别技术应用的合规性监管。

在事前准入阶段，可以参考借鉴美国立法模式中的“情境脉络完整性”理论，也即充分尊重信息原始收集阶段和制度创设时的具体语境和最初动因，在后续信息元素的传播及利用阶段不得超出最初的情境脉络。在实践中，不难发现囿于资金、技术水平、重视程度的差异，不同等级的医疗机构在人脸识别技术应用层面所采集、利用、存储的相关人脸信息的质量、规模各不相同，对相关人脸信息的保护力度和数字化能力也存在较大差异。因此，应结合实际设置人脸识别技术应用的准入门槛，加强医疗机构应用人脸识别技术的资格管理。具体来看，设置准入门槛机制能够最大限度地剔除没有人脸识别技术应用能力和信息保护能力的医疗机构，避免人脸识别技术的滥用，消除由此给患者相对人造成的信息泄露风险。

在事中控制阶段，应遵循信息最小化原则，将人脸识别信息的采集和应用控制在必要的最低限度和最小范围。应定期对具有人脸识别技术应用资质的医疗机构进行常态化监管和巡查。同时，根据国家互联网信息办公室发布的《人脸识别技术应用安全管理规定》，医疗机构作为存储超过1万人的人脸识别技术使用者，应就处理人脸信息的必要性进行说明，并将人脸信息的处理目的、处理方式和

安全保护措施，人脸信息的处理规则和操作规程，个人信息保护影响评估报告等相关内容向所属地市级以上网信部门备案。

在常态监管阶段，应根据实际从内部监管和外部监管两个层面予以合规强化。一方面在医疗机构内部应建立人脸识别技术应用影响评估机制、人脸识别信息储存数据安全保障机制、技术失范应急处置机制等常态化的运行监管体系。另一方面，医疗机构的上级主管和卫生监管部门、履行信息保护职责的行政机关、其他政府监管部门应密切协调，对医疗机构建立起常态化监管机制，对违反个人信息保护的行为和超越权限进行人脸识别采集的医疗机构进行处罚和打击。

（二）区分人脸识别技术的应用场域

在医疗机构应用人脸识别技术的具体细节上，应根据医疗机构不同场域作用功能的不同，对人脸识别技术的应用细节和权限管理予以具体区分。例如，根据医疗机构场域内部的功能空间来具体划分人脸识别技术的应用区域，将人脸识别技术的应用区域分为公开区域、半公开区域和限制区域。

医疗机构应用人脸识别技术的公开区域，也即医疗机构功能空间图景中依法依规可以不加限制应用人脸识别技术的公共区域[16]，如面向“不特定之人”开放的具备“公用性”或者说是满足“公共出入性”的区域，这类区域主要包括公共进出通道、公共停车区域、公共服务区域等公众可以共享共用的公共活动区域。这类区域人群流量较大，情况也较为复杂，结合医疗机构作为重点场所所承载的公共安全、公共利益和公共卫生需要，可以由公安机关依法依规布设具备人脸识别功能的治安摄像头，通过人脸识别技术联通图像收集终端和执法数据库，以比对发现违法犯罪人员[17]。

同时，视频监控的范围和时长加深对公民个人生活的入侵程度，与维护个人生活安宁和不受打扰存在一定程度的对立[18]。因此，为了保障患者相对人的生活安宁和个人隐私，在医疗机构功能应用图景中，应划分不适宜全程应用视频监控和人脸识别技术的半公开区域，和应予完全禁止使用人脸识别技术的限制区域。尤其是实践中部分医疗机构错误理解了行政主管部门关于场景监控、诊疗数据和服务影像同步全覆盖的具体要求，在涉及患者相对人病情诊断、检查诊疗等有关个人隐私的半公开场所，甚至高度私密的场所也设置了视频监控和人脸识别设备。这些行为不仅曲解了政策本意，更使患者相对人陷入对自身隐私权时刻遭受侵犯的担忧之中，进一步恶化了就诊体验和医患关系。因此，在医疗机构开展诊疗服务的场所，如医院病房、医生问诊室应限制人脸识别监控设备的安装和使用，限制人脸存储等高阶功能或关闭人脸识别权限。在医疗机构进行身体检查和疾病诊断的检查室等这类涉及患者相对人个人隐私的空间区域，应禁止具备人脸识别功能的视频监控设备的安装和使用。

（三）保障患者相对人的知情同意权

从医疗机构的数字化转型来看，智慧医院建设过程中人脸识别技术的综合运用已是不可逆转的数字化浪潮，断无因噎废食“开倒车”的道理。鉴于患者相对人知情同意原则被架空的现实可能性，必须采取措施切实保障患者相对人对于应用人脸识别技术的知情同意权，真正将其作为技术应用的首要原则和前提条件。

首先，医疗机构在患者相对人进入人脸识别信息采集区域时应当充分尽到提醒义务。在具体设置上，医疗机构在安装人脸识别设备时要“设置显著的提示标识”，包括但不限于通过标志标识、语音告知、风险提示等，以足够明显的方式对患者相对人尽到提醒和告知义务。在具体告知内容上，应包括相对人对人脸识别技术的具体使用授权，明确告知患者相对人人脸识别信息的收集、储存、使用方式。

其次，医疗机构应建立完善患者相对人意思同意表示机制。从域外经验来看，欧盟《数据保护指令》将数据主体的“同意”定义为“数据主体在被充分告知信息的情况下自由做出的、明确表明其同意处理与其有关的个人数据的意思表示”[19]。在我国，《中华人民共和国个人信息保护法》要求公共场所非因公共安全目的的人脸识别需取得个人单独同意。在实践语境下，“个人单独同意”意味着医疗机构必须使患者相对人以积极、明确、作为的方式表示其同意医疗机构应用人脸识别技术作为一项程序性设置。例如，患者相对人在使用刷脸设备就诊前医疗机构应向其获取明确授权说明，并要求患者相对人以点击确认或签字授权的方式做出“同意”的意思表示，从而保障患者相对人对医疗机构应用人脸识别技术的知情同意权利。

最后，医疗机构应为患者相对人提供不同意适用人脸识别技术时的其他就诊方式。在数字时代背景下，数字弱势群体可能因数字鸿沟无法享受数字生活的便利，但绝不能因数字技术发展被剥夺就医等基本生活权利和人格尊严。医疗机构作为提供医疗服务的机构在社会功能上具有不可替代性。因此，医疗机构应确保患者相对人尤其是数字弱势群体在不适用人脸识别技术时也能享受到同等水平和质量的医疗服务，以此保障患者相对人的就诊权利。

参考文献

[1] 邢会强. 人脸识别的法律规制[J]. 比较法研究，2020（5）：51-63

[2] 张重生. 人工智能:人脸识别与搜索[M]. 北京:电子工业出版社,2020:8-12
[3] 张勇. 个人生物信息安全的法律保护——以人脸识别为例[J]. 江西社会科学,2021(5):157-168
[4] 石佳友. 公共视频设备应用中的个人信息保护[J]. 江苏社会科学,2022(3):90-101
[5] 焦艳玲. 人脸识别的侵权责任认定[J]. 中国高校社会科学,2022(2):117-128
[6] 洪延青. 人脸识别技术应用的分层治理理论与制度进路[J]. 法律科学(西北政法大学学报),2024,42(1):89-99
[7] 韩子璇. 涉人脸识别犯罪行为的规制困境与突破——基于67例刑事案例的实证分析[J]. 江西警察学院学报,2023(6):47-54
[8] 商希雪. 生物特征识别信息商业应用的中国立场与制度进路——鉴于欧美法律模式的比较分析[J]. 江西社会科学,2020(2):192-204
[9] POWER D J,HEAVIN C,O'CONNOR Y. Balancing privacy rights and surveillance analytics:a decision process guide[J]. J Bus Anal,2021,4(2):155-170
[10] 于冲. 网络刑法的体系构建[M]. 北京:中国法制出版社,2016:218
[11] PARKER J. Too much medicine:not enough trust?A response[J]. J Med Ethics,2019,45(11):746-747
[12] 吴伟光. 大数据技术下个人数据信息私权保护论批判[J]. 政治与法律,2016(7):116-132
[13] 毋文文. 法治国家的健康观[J]. 南京医科大学学报(社会科学版),2023,23(5):415-422
[14] 周晗,储著源. 中国式现代化视野下健康中国的价值探微[J]. 南京医科大学学报(社会科学版),2023,23(6):510-516
[15] 李昕钰,陶林,沈瑞林. 试论习近平关于卫生健康重要论述的科学内涵和实践路径[J]. 南京医科大学学报(社会科学版),2023,23(2):168-172
[16] 胡建淼,岑剑梅. 论公共摄像监视——以隐私权为中心[J]. 法律科学(西北政法大学学报),2008,26(4):23-30
[17] 纵博. 隐私权视角下的大规模监控措施类型化及其规范[J]. 中国刑事法杂志,2020(6):55-71
[18] 李延舜. 公共视频监控中的公民隐私权保护研究[J]. 法律科学(西北政法大学学报),2019,37(3):54-63
[19] 库勒. 欧洲数据保护法——公司遵守与管制[M]. 旷野,杨会永,译. 北京:法律出版社,2008:71

(本文编辑:姜 鑫)

Legal risk and regulatory research on the application of facial recognition technology in medical institutions

ZHANG Rui[1], BAN Yiyuan[2]
1. Institute for Chinese Legal Modernization Studies, Nanjing Normal University, Nanjing 210023; 2. Law School, Shanxi University, Taiyuan 030012, China

Abstract: Facial recognition technology greatly enhances the operational and management efficiency of medical institutions, it also brings potential technological application and legal risks. In terms of subject compliance, medical institutions are not the natural compliant entities applying facial recognition technology. In practical application, there is a risk that the diagnostic autonomy of doctors under the scrutiny of video surveillance and facial recognition devices may be compromised. In terms of information rights protection, the informed consent rights of patients are at risk of being substantially violated, which means it is necessary to refine corresponding regulatory approaches to address these legal risks. Efforts can be made to enhance the compliance of medical institutions in applying facial recognition technology, differentiating between different application scenarios of facial recognition technology within medical institutions, and ensuring patients' informed consent rights.

Key words: digital era; facial recognition technology; medical institutions; regulatory dilemmas; informed consent right