特别专题:重大疫情治理研究

重大疫情治理中人工智能的价值属性与隐私风险

——兼谈隐私保护的刑法路径

闫　立　吴何奇

[摘　要]　相关国家政策文件的出台为我国医疗人工智能的迅速发展夯实了政策基础,在重大疫情的治理过程中,以医疗大数据为基础的人工智能不仅能够提升诊断的准确率、缓解医务人员不足的困境,更能减少医务工作者感染疾病的风险。但由于人工智能的运作存在着对个人隐私侵犯的天然性,反思人工智能时代个人隐私保护的刑法路径也应同步于重大疫情的治理。我国刑法中并没有以隐私权为独立客体的法律条文,现有对隐私权的保护附属于刑法对市场经济秩序、公民人身权利与民主权利、社会管理秩序的保护,但这一体系下的个人隐私保护存在着制度设计上的缺陷。针对弊端,个人隐私保护刑法路径的建构首先应以对大数据背景下个人隐私的合理界定为逻辑前提,站在风险防范与利益平衡的立场,不以静态的视角界定隐私的边界,再以此展开个人隐私保护刑法路径的具体设计。

[关键词]　重大疫情治理;大数据;人工智能;隐私风险

一、人工智能治理重大疫情的价值属性

国家战略“互联网+”行动计划的提出,以及《全国医疗卫生服务体系规划纲要(2015—2020年)》《关于积极推进“互联网+”行动的指导意见》《促进新一代人工智能产业发展三年行动计划(2018—2020年)》等文件的相继出台,为医疗人工智能的快速发展提供了政策上的支持。伴随着《新一代人工智能发展规划》在2017年7月的正式发布,如何通过法律法规的建立更好地保障人工智能的健康发展被进一步强调。根据《规划》,国家希望通过对包括隐私权、信息安全利用在内的人工智能应用相关法律问题的研究,建构顶层设计以适应人工智能的发展。在此背景下,法学领域围绕人工智能的讨论呈现出百家争鸣的图景。作为“互联网+”健康命题下的核心构成,医疗人工智能即通过人工智能技术的应用,转变传统医疗的服务模式,以智慧医疗惠及全民。当前,我国医疗资源的供需严重失衡,①因此,医疗

闫立,法学博士,上海政法学院教授、博士生导师(上海 201701);吴何奇,上海财经大学法学院博士研究生(上海 200433)。本文系中央高校基本科研业务费专项资金资助(2018110301)的研究成果。

①奥比斯科技:《AI医疗:人工智能在医疗行业中的几大突破案例》,http://www.sohu.com/a/270645378_100119466,2020年1月21日。

人工智能的发展特别是其在影像、儿科等领域展现出的优势对于缓解当前医疗领域的燃眉之急具有重大意义。在未来,人工智能将赋予医疗技术深刻的变革,成为医学创新源源不断的驱动力。①

在世界卫生组织于2020年1月31日召开的紧急委员会会议上,中国的新型冠状病毒肺炎疫情被列为"国际关注的突发公共卫生事件"——世界卫生组织传染病应急机制中的最高等级。从2019年12月30日疫情公告首次发布之日起,新型冠状病毒肺炎的确诊数在一个月的时间里便超过了2003年SARS的确诊数,且至今仍在不断增加。② 疫情的集中爆发让湖北省绝大多数医院的医疗资源严重匮乏,众多危重患者难以在第一时间得到救治。对此,在中央全面深化改革委员会第十二次会议上,党中央强调要通过更好地发挥人工智能等数字技术以支撑疫情监测分析、病毒溯源、防控救治等方面。

当前,协助医生诊断的人工智能产品不再是以智能穿戴设备为核心,基于医疗大数据的算法成为提高医疗工作效率的重点。近年来很多国家对医疗信息化发展的积极推进缔造了人工智能在医疗领域的巨大发展,这一举措不光使得很多医疗机构有资金来做大数据分析,更体现了国家从头构建新的医疗数据应用生态的决心。

在此背景下,依靠不断积累的医疗数据与不断提升的数据分析功能,人工智能正给医疗保健带来范式转变。在治理类似于新型冠状病毒肺炎的重大疫情中,利用传感器对人体进行数字化,医疗人工智能不仅可以提前干预人体健康,降低发病几率。还能借助于医疗大数据实现对治疗路径的预测。例如通过对患者死亡概率的预测建议采取传统治疗还是临终关怀。③

当前,人工智能赋能医疗领域的场景中最典型的应用莫过于医学图像分析。④ 传统对新型冠状病毒肺炎患者的胸部影像的诊断采用的是两个医生同时查看的模式,在重大疫情爆发阶段,本就有限的医务人员在巨大的工作量面前显得捉襟见肘,卷积神经网络在医学图像领域的应用与推广针对的便是医学领域的这一痛点。在通过各种医学图像的训练并获取输入图像的基础上,这一深度学习的算法通过卷积、汇集等操作将输入图像的顺序转换为扁平向量,用以表示疾病存在概率的则是输出向量的元素。

利用人工智能诊断疾病不仅可以大大提升诊断的准确率、缓解医务人员不足的窘境,更能最大程度地预防和降低医患之间交叉感染的风险。如何应对"人传人"的病毒传播不仅是治理新型冠状病毒肺炎这一重大疫情的难点,更是保障医务人员生命健康的关键。医疗实践中,医务人员作为病毒的密切接触者,已成为感染新型冠状病毒肺炎的高风险人群。⑤ 在抗击重大疫情的过程中,医疗人工智能的运用不仅是对疫情监测分析、病毒溯源、防控救治的有力支持,更能降低甚至规避医务人员被感染的风险,这也重大疫情治理中人工智能价值属性的体现。

二、人工智能的运用对患者个人隐私的风险

值得注意的是,医疗人工智能提供的服务依赖于对医疗数据的深度挖掘与分析,在利用数据的同时如何保护患者的隐私不被侵犯具有研究的价值。毕竟,技术上的漏洞能够逐渐在技术本身发展

---

①王利明:《人工智能时代提出的法学新课题》,《中国法律评论》2018年第2期。

②截至2020年2月15日,根据国家卫健委发布的数据,确诊病例共计66580例,疑似病例8969例。

③W. N. Price & I. G. Cohen, "Privacy in the age of medical big data", *Nature Medicine*, vol. 25, 2019, pp. 37—43.

④由四万余块260核芯片组成的超级计算机"啄医生",将超算技术与人工智能结合,学习了10万多套肺片,在短时间内,迅速达到了有15年临床经验的影像科医生的阅片水平;吴恩达的斯坦福团队发布了一个基于深度神经网络CheXNeXt的X光诊断算法,该算法可以自动诊断14种疾病。在其中10种疾病的诊断上,AI的表现与放射科医生旗鼓相当,还有一种疾病的诊断效果甚至超过了人类。并且,这个AI诊断算法的诊断速度是人类的160倍;武汉同济医院在2016年就上线试用了AI-DR辅助诊断技术。短短5个多月,使用AI-DR技术共诊断X线片8093张。在测试实际病人X线片的过程中,AI-DR于160例病例中发现了两例医生诊断中遗漏的病灶。

⑤以武汉市卫健委于1月21日发布的权威通报为例,截至当日,武汉市已有15名医务人员感染新型冠状病毒肺炎。

的进路中得以抹平，但只要人工智能“深度学习”的基础依然是海量的数据，人工智能对患者个人隐私的风险就不会消除。因此，如何协调隐私保护和信息福利之间的张力，是人工智能发展进路上亟待解决的重要问题。在肯定人工智能能够出色地运用于重大疫情治理的同时，我们仍应思考数据价值的维持对人工智能的促进与个人隐私保护的平衡问题。

医疗人工智能水平的高低取决于其所掌握的医疗数据的多寡，而数据的积累、医疗大数据的分析以及智能化医疗诊断均以患者医疗数据的共享为前提，涉及患者诊断记录、用药效果、基因数据、家庭病史等个人医疗信息与医学诊断信息是医疗人工智能得以迅速发展的温床，但对海量数据的不断挖掘与分析，就会给个人隐私安全带来风险。无线网络便携性、开放性强，使得对它的安全管理面临很大困难。无线数据传输具有脆弱性和不稳定性，巨量的个人数据过于分散，使得团体组织无法对所有数据进行加密和保护。个人数据在信息时代被记录得越来越多，被侵扰、收集和利用也越演越烈已成为基本现实。医疗人工智能中对健康医疗大数据的收集、集成和运用，面临着科技进步与信息安全、隐私保护之间的突出矛盾。

具体到重大疫情治理的问题上，一方面，包括患者的诊断记录、病史甚至遗传信息在内的个人信息由医疗 AI 的系统收集并保存于云端或存储器中，一旦医院的网络服务器遭到黑客或网络病毒的攻击，病人的信息就会泄露，如果这些信息被不法分子用到不正当的途径，患者的隐私权就会遭到侵犯。2016 年，全国便有至少 275 例艾滋病感染者的信息被泄露。① 另一方面，人类无法奢求不具备情感的医疗人工智能像自然人那样对他人私密信息“守口如瓶”，计算机的加密措施在掌握破译算法技术的人面前也不堪一击。例如，由英国皇家慈济 NHS 信托基金运营的三家医院保管的涉及 160 万患者艾滋病病毒感染状况、堕胎信息和过去的吸毒过量等私密性的个人数据不经意间便被 DeepMind 公司破译并获取。② 诸多案例中，人工智能展现出来的隐私风险不言而喻。

医疗信息于不同患者而言，什么样的内容属于患者不愿为他人所知悉的隐私本就因人而异，譬如，外伤患者可能不会介意个人健康信息的泄露，但在重大疫情时期，肺炎患者则会担忧诊断信息的泄露对其生活的影响。试图从客观生硬的数据里筛选出属于患者隐私的内容加以封存不仅成本高昂，更未解决算法泄露隐私的外部性问题。现状下，对患者数据的利用与保护之间的平衡点若隐若现，难以为人类所掌握。此外，现实情况中绝大部分患者在享受医疗人工智能带来的便利时几乎没有个人隐私保护的意识，这让患者个人隐私遭到侵犯的风险更加难以规避。而患者的个人隐私一旦遭受侵害，结合大数据容量大、种类多、速度性、复杂性、可变性的特征，必然是对患者法益的重大侵害，③广大公民对信息技术的茫然与无知更让一种个人信息被泄露以及被非法利用产生的严重不安感成为整个社会挥之不散的阴霾。1981 年欧洲委员会修订的《个人数据自动化处理中的个人保护公约》将对隐私权的保护视为重中之重，而将那些严重侵犯隐私的行为规定为犯罪，则是刑法通过否定评价进而保护人权的价值所在。④ 因此，20 世纪末以降，各国刑法也开始对个人隐私的保护进行了积极介入。

三、人工智能时代个人隐私保护刑法路径的现状与缺陷

（一）法律规制中隐私概念的流变

人工智能时代，个人信息与个人数据在法律概念上逐渐趋同。尽管国际上鲜有立法文件将“个

①刘琪、谷笑颖：《医疗人工智能应用中的伦理困境及对策研究》，《医学与哲学》2019 年第 21 期。

②D. D. Mille & E. W. Brown，“Artificial intelligence in medical practice：The question to the answer?”，*The American Journal of Medicine*，vol. 2，2018，pp. 129—133.

③刘建利：《医疗人工智能临床应用的法律挑战及应对》，《东方法学》2019 年第 5 期。

④杨永志：《论隐私权的刑法保护》，《河北法学》2007 年第 12 期。

人信息”用于法律层面的称谓,但国内立法者对“个人信息”这一措辞的青睐要高于“个人数据”,相继颁布的规定与相关立法都以“个人信息”作为立法所规制的或保护的对象的名称。

一些学者将个人信息与数据的关系表述为内容与物化表现形式,[①]并强调后者只是前者的表现形式之一。[②] 然而,相比人们能够通过信息认识世界、改造世界,数据只是对现象的客观描述。据此,个人数据的范畴又宽于个人信息。值得注意的是,法律或规范性文件对个人信息与数据的界定并不符合二者在文字含义方面的区分。“个人信息”与“个人数据”只是表述上的差异,往往可以相互替换使用,[③]甚至互为解释对象,《通用数据保护条例》第4条便以数据主体的信息界定个人数据。[④] 采用类似用法的还有《个人数据保护指令》、《数据处理、数据文件及个人自由法》以及《联邦数据保护法》等立法文件。纵然二者的文字内涵有所差异,但法律规范中的含义既然已由法律人彼此约定俗成,[⑤]我们自然没有在法律概念上强行区分二者的必要。[⑥] 更何况,数据之所以在当下逐渐成为最重要的社会资源之一,在于其本身的内涵已不再局限于形式载体,被赋予多维度、完备性等新特质的数据不应当再被简单地理解为一种描述客观事物的未经加工的原始素材,是能将人类的智能问题转化为数据问题的桥梁。

关于隐私,《世界人权宣言》第12条规定与《欧洲人权公约》第8条规定是保护个人隐私方面最权威的国际法渊源。[⑦] 但总体而言,如何界定“隐私”以及如何区分隐私与个人信息的关系,在我国法律界尚未达成共识,而对上述内容的认知与审视是我国个人隐私刑法保护路径的必要前提。

“记录”与“识别”是《网络安全法》下个人信息的核心要素。[⑧] 前者是个人信息的状态要素,后者则属于个人信息的功能要素。在信息繁荣的今天,很难找到一个不能被记录的客体,但被记录下来的信息只有具有身份识别的功能属性才会被纳入个人信息的范畴。有学者认为隐私是未公开的个人信息,[⑨]但笔者认为,隐私的法律概念应是权利主体的主观需求与社会评价机制的耦合,个人信息未得以公开既不能反映出权利主体是否同意、默许公众知悉该信息的主观意愿,也不能体现出根据社会的普遍评价该信息是否属于应当被公开的内容。同理,就二者的关系而言,有的个人隐私是个人信息,但并不是所有的个人信息都属于隐私,个人信息中属于“隐私”的那部分,应当是个人信息中本人不希望且不应当被他人看到、知晓、干涉的内容。尽管个人信息这一概念远远超出了隐私权的范畴,[⑩]但个人信息与个人隐私的关系并非包含,而是交叉重合,即“不是所有的个人信息都是个人隐私,也不是所有的隐私都是个人信息”。[⑪]

(二)现状下个人隐私保护的刑法规制

早在19世纪,德国、法国的刑法典中就存在保护个人隐私的法律规制。[⑫]《西班牙刑法典》第十

---

①齐爱民:《个人资料保护法原理及其跨国流通法律问题研究》,武汉:武汉大学出版社,2004年,第4页。

②王鹏鹏:《论个人数据的静态与动态融合的私法保护》,《四川师范大学学报》(社会科学版)2019年第5期。

③马改然:《个人信息犯罪研究》,北京:法律出版社,2015年,第10页。

④Art. 4 GDPR Definitions: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject');

⑤林立:《法学方法论与德沃金》,北京:中国政法大学出版社,2002年,第151页。

⑥陈吉栋:《个人信息的侵权救济》,《交大法学》2019年第4期。

⑦《世界人权宣言》的第12条规定:“任何人对其隐私、家庭、房屋或者通讯均不受武断干扰,对其尊严或者名誉不受攻击。任何人均有权对这种干扰或者攻击获得法律保护。”《欧洲人权公约》第8条规定:“每个人都有权使其私人生活和家庭生活、其房屋和通讯受到尊重。”

⑧《网络安全法》第76条:“个人信息,是指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自然人个人身份的各种信息,包括但不仅限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”

⑨徐翕明:《“网络隐私权”刑法规制的应然选择——从“侵犯公民个人信息罪”切入》,《东方法学》2018年第5期。

⑩王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013年第4期。

⑪陈冉:《论大数据背景下隐私权的刑法保护》,《中国刑事法杂志》2017年第3期。

⑫德国1871年颁布的刑法典中设置了“侵犯私人秘密犯罪”一章,法国刑法典第226—1条也对侵犯个人隐私的行为予以规制。

编设置了“侵犯隐私、公开隐私和侵入住宅罪”。美国1962年《模范刑法典》第250.12条也专门规定了侵犯隐私行为的处理,[①]以及《意大利刑法典》设置了“非法干涉私生活罪”以禁止非法获取和向公众泄露或者传播他人私生活信息的行为。而刑事法领域,第一次对医生等特定职业的保密义务予以要求的立法是1794年的《普鲁士一般法》。自此,医生等特定职业的行为主体对患者个人隐私的泄露将面临刑罚的苛责。此外,日本《刑法》第134条“泄露秘密罪”也对医药行业的从业者在没有“正当理由”的前提下泄露“业务上所知悉的他人的秘密”的行为进行了规制,以此在限定的状况下对患者个人隐私进行保护。

我国宪法的第38条到第40条对公民人格尊严、住宅不受侵犯、通信自由以及通信秘密的宣告涉及保护公民隐私的意蕴,这是刑法保护个人隐私的宪法渊源。但不同于国外刑法典对个人隐私保护专章专节专门罪名的立法模式,我国尚未出台以具有独立地位的隐私权为客体或主要客体的刑法规制,即便是对个人信息的保护也不是立法者一以贯之的重点。刑法规范中的“个人信息”兼具个人隐私的人格权属性与用于商业运营、政府运作的经济属性,[②]因此,对个人信息的保护往往依附于刑法对超个人法益的保护,通过对国家法益、社会法益、商业秘密的保护附带地规制侵犯个人信息的行为。[③] 值得注意的是,我国对于隐私的保护采取的是德国式的人格权保护模式,刑法对公民个人信息的保护也基本采取了人格权保护的模式,因此,涉及保护个人隐私的刑法规制主要置于“侵犯公民人身权利、民主权利罪”之下。[④] 侵犯公民个人信息罪更是被视作当前保护个人隐私的刑法路径中的“金科玉律”。该罪经由《刑法修正案(九)》修改,对个人信息专属犯罪做了主体扩大化和行为多元化的修改。[⑤] 此外,市场经济秩序犯罪刑法规制下的“窃取、收买、非法提供信用卡信息罪”开创了我国刑法对个人隐私保护的先河;以及通过《刑法修正案(七)》将非法获取国家事务、国防建设、尖端科学技术领域以外的计算机信息系统数据的行为规定为犯罪。经过上述立法演进,分则相关罪名的设置基本回应了对个人隐私保护的总体需求。

(三)个人隐私保护刑法路径的缺陷

第一,刑法缺乏对隐私权的直接保护。在国外立法中,美国早在2003年生效的HIPPA法案中就对使用EHR系统(Electronic Health Records)时如何保护公民隐私作出了明确规定。例如,对EHR系统的使用取决于信息的建立机制、系统的维护主体以及当事人的具体情况,等等。[⑥] 我国的《网络安全法》第44条强调了个人和组织不得侵犯他人个人信息的禁止性义务,[⑦]最新审议通过的《中华人民共和国基本医疗卫生与健康促进法》也通过第92条和第105条体现了我国对个人健康信息保护的立法举措。[⑧] 较之于此,我国对于个人信息保护的法律规范多为一些原则性的宣示、排除性的规定,缺乏对侵犯隐私问题解决路径的指引。

---

①陈冉:《论大数据背景下隐私权的刑法保护》。

②文立彬:《个人信息犯罪的刑法规制——以内地和澳门为比较》,《北京邮电大学学报》(社会科学版)2015年第3期。

③于冲:《侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界》,《政治与法律》2018年第4期。

④“侵犯公民人格权犯罪问题”课题组、顾静薇:《论侵犯公民个人信息犯罪的司法认定》,《政治与法律》2012年第11期。

⑤李川:《个人信息犯罪的规制困境与对策完善——从大数据环境下滥用信息问题切入》,《中国刑事法杂志》2019年第5期。

⑥N. Terry, “Existential challenges for healthcare data protection in the United States”, *Ethics, Medicine and Public Health*, vol. 1, 2017, pp. 19—27.

⑦《中华人民共和国网络安全法》第四十四条:“任何个人和组织不得窃取或者以其他非法方式获取个人信息,不得非法出售或者非法向他人提供个人信息。”

⑧《中华人民共和国基本医疗卫生与健康促进法》第九十二条:国家保护公民个人健康信息,确保公民个人健康信息安全。任何组织或者个人不得非法收集、使用、加工、传输公民个人健康信息,不得非法买卖、提供或者公开公民个人健康信息;第一百零五条:违反本法规定,扰乱医疗卫生机构执业场所秩序,威胁、危害医疗卫生人员人身安全,侵犯医疗卫生人员人格尊严,非法收集、使用、加工、传输公民个人健康信息,非法买卖、提供或者公开公民个人健康信息等,构成违反治安管理行为的,依法给予治安管理处罚。

我国司法实践中较为典型的涉及侵犯他人隐私权案例包括2008年香港的“艳照门事件”,2009年“江国盛传播淫秽物品罪案”以及2015年北京的“优衣库事件”。其中,“艳照门事件”的电脑修理店员史某被判“因不诚实取用电脑罪”,“优衣库事件”嫌疑人邓某某虽因涉嫌传播淫秽物品罪被刑事拘留,但最终仅以违反治安管理处罚法第42条规定被处以行政拘留10日的处罚。上述司法实践反映出我国刑事立法缺乏对隐私权直接保护的现状,传播淫秽物品罪便正是社会法益保护基础上的一种间接保护公民隐私的体现。由《刑法修正案(七)》设置的非法获取公民个人信息罪经由《刑法修正案(九)》修改为侵犯公民个人信息罪,通过对犯罪主体以及侵犯个人信息行为的范围的扩张起到了进一步对公民个人隐私的保护。司法实践中,自侵犯公民个人信息罪设立以来,以该罪名定罪量刑的案件数急剧增加。参考中国裁判文书网提供的数据,2016年基层法院以该罪名作出判决的案件数为258起,2019年为1723起,犯罪的行为类型主要为基于进行市场营销或者技术研发的目的非法获取、使用个人信息。尽管侵犯公民个人信息罪的设置很大程度地缓解了这种寄托于社会法益来保护个人隐私的尴尬,但该罪的客体依然是公民的个人身份信息,较之于国外刑法典对公民个人隐私的直接保护仍有不小的差距。

第二,尚未形成与刑法典衔接的法律保护体系。在对具体法益的保护上,刑法机能的发挥不仅需要相关罪名的完备,还依赖于相关前置法律、配套法律的协调性。现状下,我国关于个人信息的相关法律、法规尚未健全,更不具备一个成熟的隐私保护法律体系,例如,根据我国刑法第253条之一的规定,行为“违反国家规定”是该罪成立的前提,然而,尽管《个人信息保护法》已经纳入十三届全国人大常委会的立法规划,但专门用以保护个人信息的立法目前尚未出台,而现行的《治安管理处罚法》甚至未将侵犯公民个人信息的行为作为行政违法行为,[①]换言之,现状下尚不具有统一、完备的行政法律制裁体系与刑事制裁相衔接。完备的法律体系,尤其是刑法前置法律的存在是保证刑法发挥效力的必要前提。个人信息行政制裁体系的欠缺必然对个人信息的保护产生深刻的不利影响。值得肯定的是,我国现行法律规范中间接起到保护个人隐私的条款正逐渐地丰富,但对于信息隐私的保护起步较晚,这使得当前的法律规范很难应对人工智能时代人工智能运用过程中潜伏的隐私风险。正如有学者所指出的,我国的隐私权法律保护体系既不像美国那样以不断丰富隐私内核的方式应对当前与未来的个人信息保护需求,又无健全的个人信息保护法律体系而无法像欧盟那样寄托于日渐臻熟的个人信息保护法律体系来应对人工智能时代所存在的隐私保护问题。[②]

四、人工智能时代个人隐私保护刑法路径的建构

(一)人工智能时代个人隐私保护刑法路径建构的逻辑前提

第一,个人信息去识别化规则的实践困境。“可识别性”是个人信息的功能要素,最高法、最高检发布的《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》的第三条的但书部分将“经过处理无法识别特定个人且不能复原的”信息排除出侵犯个人信息罪的构成要件。据此,只要对流通过程中被利用的个人信息进行去识别化的操作,就使得该信息不再是个人信息,从而规避了刑法的约束。个人信息的去识别化,即数据保有者采用技术手段,对其所保有的数据信息进行集中的筛查,将其中能够识别特定个人身份的数据信息予以删改的过程。从而实现在保留信息特定用途价值内容的同时,降低可能对信息主体的隐私造成的威胁或损害的风险。[③] 去识别化的处理之所以可以

①赵秉志:《公民个人信息刑法保护问题研究》,《华东政法大学学报》2014年第1期。
②郑志峰:《人工智能时代的隐私保护》,《法律科学》(西北政法大学学报)2019年第2期。
③张勇:《个人信息去识别化的刑法应对》,《国家检察官学院学报》2018年第4期。

作为个人信息利用的合法事由,存在形式和实质两个方面的解释路径。形式层面,对个人信息的去识别化处理消除了该信息的可识别性和关联性的特征,信息不再是个人信息,自然也就不符合“侵犯个人信息”的犯罪构成要件;实质层面,对去识别化信息的利用,实际上不具有泄露公民个人信息并对公民个人隐私造成侵犯的可能性,利用信息的行为自然不具备了被评价为犯罪的社会危害性。但这一规则同样存在难以攻破的症结,因为至少从目前的技术来看,对个人信息尤其是医疗领域的个人信息的去识别化往往会导致数据价值的“断崖式”下跌。① 因此,当前欧美国家在针对医疗数据中涉及患者隐私信息所作的规定也仅仅止步于对患者重要隐私的加密处理、数据访问权限的加强等层面。②

第二,同意原则的现实局限。被害人承诺与同意在刑法理论中源远流长,以被害人的承诺作为正当化事由排除行为违法性的依据滥觞于古罗马时期法学家乌尔比安所说的,“符合被害人意志的,不构成不法”。如今在刑法理论中广为流传的是后世法学学者对这句法谚的提炼,即“得承诺的行为不违法”。③ 据此,信息主体的同意原则上可以阻却个人信息收集、利用、提供甚至出售的违法性。“同意”被认为是个人信息的使用者规避刑法规制的绝佳路径。

在医疗的语境下,知情同意作为一个法律概念,展开于患者自主权的表述过程。随着社会信息技术的繁荣,它逐步延伸到个人信息保护的主体框架。④ 医疗信息的保护亦需依循传统个人信息保护的知情同意规范,即医院、疾病预防控制机构在收集信息主体的信息之前,应告知信息主体需要什么样的信息,如何处理和使用什么样的信息,只有依法取得信息主体的明确同意与授权,方才能对信息进行处理与运用。在传统的信息生态之下,个人医疗信息被信息控制者随意使用或传输给后续的控制媒介。受技术水平的限制,信息使用方式更为直接、简单,便于信息主体了解。因此,知情同意架构能够减少信息风险,保护信息主体对个人医疗信息的独立决定权。

然而,同意原则在个人信息领域的适用同样面临着实践中的障碍。在人们感受到个人隐私存在被他人觊觎的风险的时代背景下,能够确认或者征得信息主体同意的场合非常有限。尤其是医疗信息往往涉及到患者那部分难以启齿的个人隐私,患者对共享个人信息的反对更让医疗人工智能对数据的搜集难以开展。导致这一症结在现实中难以被克服的原因在于机器学习对数据处理结果不可预测性的提升使得信息主体往往无法获取数据处理的适当信息,在这一背景下,征求用户的有效同意自然也失去了意义。同时,通知同意机制下的通知大多难以有效到达、信息主体缺乏议价空间,更进一步使得该机制仅仅停留于理论层面而难以付诸有效实践。⑤

综上所述,基于数据对于人工智能的特殊价值,个人信息的去识别化规则难以在实践中发挥保护个人隐私的效果,现实中信息的不对等让同意原则无法成为信息使用者侵犯他人隐私的豁免理由,而导致上述症结的缘由在于当前社会对个人隐私的定位难以达成共识。

(二)人工智能时代个人隐私的理性定位

在使用公民个人信息的过程中,个人隐私保护与其他利益往往存在冲突,利益至上原则是解决冲突的主要理论工具。大数据对个人信息的利用主要集中在庞大的群体信息上,其目的和用途往往体现在技术创新或突发事件等公共领域。因此,人工智能时代个人隐私保护往往与其他利益的追求或保护存在难以协调的冲突。在个人隐私与社会公共利益发生冲突的情形下,为了实现社会整体的

---

①李丹丹:《论个人医疗信息的法律保护》,《吉首大学学报》(社会科学版)2015 年第 2 期。

②包桉冰、徐佩:《医疗人工智能的伦理风险及应对策略》,《医学与哲学》(A)2018 年第 6 期。

③王钢:《被害人承诺的体系定位》,《比较法研究》2019 年第 4 期。

④田野:《人工智能时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》,《法制与社会发展》2018 年第 6 期。

⑤郑志峰:《人工智能时代的隐私保护》。

更大利益，隐私权也被认为是一种具有可克减性的权利，在特定情况下，为了维护公共利益，可以对其加以一定的限制、甚至剥夺，在这种情况下就排除了侵权行为的违法性。但在隐私利益与公共利益发生冲突的情况下，不能简单地以保护公共利益为理由任意侵犯个人隐私。开展医学研究有利于提高全社会的医疗卫生水平，关系到全体公民的生命健康，具有重大的社会公益性。医学研究周期长、全局性强。医疗大数据在医学研究中的应用往往需要很长时间才能取得一定的成功，很难迅速直接影响到公众个人的切身利益。总的来说，与公民医疗信息的保护并不存在紧迫和不可调和的冲突。即使在某些情况下，医学大数据也不能被用于医学研究，因为没有患者同意或匿名处理，不会导致社会福利的不可避免和不可挽回的损失。在人工智能时代，为了提高医疗卫生水平而牺牲患者个人利益的观点受到了医学研究领域的批评，这反映出业界对医学研究的利益排序未能形成共识。因此，我们不能认为医疗研发的社会效益一定高于患者个人信息保护的利益。

提高信息、数据的安全性，加大对信息主体隐私的保护是医疗乃至整个人工智能领域进一步发展的关键。在倡导以法律尤其是刑法介入个人隐私保护之前，厘清个人隐私的时代内涵是开展任何一种制度设计的必要前提。如前文所述，对隐私的判断必须报以动态的视角，笔者认为，在大数据背景下对隐私抑或是隐私边界的界定应当摒弃对传统法律理据的机械适用。

人工智能时代，公民对于个人隐私总有一种岌岌可危的风险感或不安感，但另一方面，私人领域和公共领域的界限正在变得越来越模糊，个人隐私的价值正逐步被消解。近代资产阶级革命之后，隐私权成为一项关键的人身权利。从那时起，现代隐私的理论就牢牢地掌控在西方的话语权中。不同于过去，人工智能时代的我们似乎并不介意将自己的个人信息交给诸如外卖、社交平台、网购这样的机构抑或是公司。很大程度上，我们正逐渐将隐私的意义从西方文化的拘束之中解放出来，过往人们对隐私权的偏见观已然被刷新。这就是人工智能时代为我们以前的固有思维所带来的革新，让隐私这个概念在人们心中发生着微妙地改变。

在人工智能时代以一个静态的视角界定隐私之所以不可取还在于个人信息“识别”本身就是一个动态的过程，存在技术上的去识别与重新识别。① 既然人工智能对隐私存在天然的风险性，那么信息的“适当”流通、分享则是人工智能时代隐私场景公正性理论的逻辑起点。隐私规制不是以保护权利或制止侵权为目的，而是以社会整体利益为考量，以利益关系平衡为基础。② 隐私保护的顶层设计，应无碍于信息的流动和分配，从而提升信息资源的利用效率。因此，关于隐私权的争论，最后的解决方案不会一边倒，而是在风险防范与利益诉求中取得一个平衡，既不会允许肆无忌惮地侵犯个人隐私权，个人也不可能绝对的保有所有的隐私权。

不以静态的视角界定隐私的边界的依据不仅在于上述看似较为功利化的思维逻辑，还在于以固定的标准区分合理使用与侵权在当下已然不具有实践的可能。过往区分数据合理使用与侵犯隐私的边界是由美国学者桑德拉·彼的罗尼奥提出的隐私边界的三条规则，即“控制边界链接、掌握边界渗透和明晰边界所有权”。但当前，无处不在的媒介顷刻间便能使用户在不知不觉中将个人信息向外界表述。信息采集的途径日益隐蔽，也让用户几乎无法知道自己的哪些信息正在被泄露，以及以欧盟《通用数据保护条例》（GDPR）为代表的各国法律都对合理使用的保留极大地冲击着用户的边界所有权。③ 人工智能时代，这三条规则早已“消解殆尽”。

隐私权的本质是人格尊严的无比神圣，而隐私则是隐私主体不希望且不应当被他人看到、知晓、

---

①李源粒：《网络数据安全与公民个人信息保护的刑法完善》，《中国政法大学学报》2015 年第 4 期。

②李文姝、刘道前：《人工智能视域下的信息规制——基于隐私场景理论的激励与规范》，《人民论坛·学术前沿》2019 年第 6 期。

③李凌霄：《隐私悖论：万物互联与赛博人的隐私边界》，《传媒》2019 年第 19 期。

干涉的个人信息。“不希望”是权利主体需求的体现,“不应当”则是基于社会普遍价值立场作出的判断。但无论是前者还是后者,都具有主观上的恣意性,因此,对隐私权的界定必然是将个人对人格尊严的认识和公众对人格尊严的一般理解相结合得出的结论。① 上述逻辑同样适用于判断何为个人信息合理利用,即对个人信息的使用“是否符合用户的合理隐私期待”“是否造成了不合理的隐私风险”。前者属于隐私判断的主观标准,后者则是对隐私风险的客观评价。② 主客观判断标准的动态性显然更契合人工智能时代界定个人隐私的理性逻辑。

(三)人工智能时代个人隐私刑法保护的应然路径

第一,完善个人隐私保护的法律体系。一方面,应注重刑法与行政法、民事法的配合,注重刑事责任与行政责任、民事责任的衔接,③从而保证打击侵犯个人隐私行为民事责任、行政责任、刑事责任的统一。现代法律的发展规律就是形式理性化,换言之,伴随法学专门化进路的应是整个法律体系的合理性与一致性。④ 就隐私保护的法律体系而言,刑法、行政法与民法都是社会这一整体系统在多样化交织式构造的过程中产生的子系统,以各自的运作逻辑规范社会机理的有序运行。作为保障法的刑法,必须以前置法的相关规定作为其介入的必要前提,如果与前置法关于信息自决权的禁止性规定产生冲突,难免折损信息的完整性与可利用性。⑤ 但在信息即黄金的背景下,侵犯公民个人信息行为行政责任的缺位产生的规制风险便是刑事责任在社会秩序治理中的越位,而刑法的机能决定了只有那些严重危及隐私安全的行为才具有刑罚处罚的可能性。人工智能时代,个人隐私的法律规制应关注隐私保护与人工智能产业创新的协调发展,在遏制隐私泄露的外部性的同时保证个人信息交易市场的资源配置效率与秩序。刑法不是市场经济的宏观调控法,对犯罪化的克制是避免隐私规制对经济主体的限制而产生市场失灵的窘境。基于上述分析,构建一个相对成熟的隐私规制体系的大致思路应该是,由民法为人工智能的开发而利用个人信息的行为提供正当性的补充,依靠行政法与刑法的禁止性规定则更多的基于个人隐私的立场予以底线的设置。在对侵犯个人隐私的不法行为的制裁上,对于情节较轻、行为危害不大的那部分予以民事、行政的处罚手段,对于满足犯罪构成的部分再施以刑事处罚,即通过对刑、行、民处罚范围的明确与分配,建立“赔偿—处罚—刑罚”的阶梯式的制裁模式。

第二,打击犯罪和预防犯罪都是犯罪防治的重要内容。然而现实犯罪治理中,往往偏重对实然犯罪行为的打击,而忽视犯罪风险的预防。⑥ 在个人隐私保护领域同样应当凸显“预防为主”的风险防控思维,对隐私权的保护不能满足于事后惩罚。⑦ 台湾地区“刑法”第 28 章妨害秘密罪在保护个人的隐私领域时便设置了抽象危险犯的立法模式以提前刑法对侵犯个人隐私行为的规制时机,⑧德国刑法典中的“侵害私人生活及秘密罪”采用了相同的立法模式。⑨ 但我国刑法中涉及保护隐私权的罪名的成立要么要求“情节严重”才予以处罚,要么限定为“造成严重后果”才予以追诉,⑩刑法保护路径的启动在应接不暇的隐私侵犯与不断增加的隐私风险面前,显得被动且消极。此外,司法实践中,如何判断“情节严重”依托于刑法、司法解释明确、清晰的规定。但就像上文多次提到的,对隐私

①杨永志:《论隐私权的刑法保护》。
②房绍坤、曹相见:《论个人信息人格利益的隐私本质》,《法制与社会发展》2019 年第 4 期。
③汪明亮:《治理侵犯公民个人信息犯罪之刑罚替代措施》,《东方法学》2019 年第 2 期。
④周维明、赵晓光:《分化、耦合与联结:立体刑法学的运作问题研究》,《政法论坛》2018 年第 3 期。
⑤冀洋:《法益自决权与侵犯公民个人信息罪的司法边界》,《中国法学》2019 年第 4 期。
⑥张旭、阮重骏:《人工智能非法应用的犯罪风险及其治理》,《中国特色社会主义研究》2019 年第 4 期。
⑦王立志:《隐私权刑法保护研究》,北京:中国检察出版社,2009 年,第 176 页。
⑧许泽天:《刑法分则(下)人格与公共法益篇》,台湾:新学林出版股份有限公司,2019 年,第 302 页。
⑨徐久生、庄敬华:《德国刑法典》,北京:中国方正出版社,2004 年,第 104—107 页。
⑩李婕:《刑法如何保护隐私——兼评〈刑法修正案(九)〉个人信息保护条款》,《暨南学报》(哲学社会科学版)2016 年第 12 期。

的界定难以形成相对静态的共识。同理,以固定的标准区分“情节严重”在信息价值难以估量的人工智能时代存在降低相关条文在实践中的灵活性的风险。因此,对既有保护个人隐私的刑法条文的修正可考虑删除上述对启动处罚权甚至追诉权的限制,既可以保证刑法对严重危害个人隐私安全的行为的规制更加主动,又能保证刑法规制在保护个人隐私的司法实践中的灵活性。

第三,专属罪名的增设,提升刑法对公民个人隐私的保护力度。如前文所述,由于刑法并未以公民的隐私权作为独立保护的客体,当前对个人隐私保护的刑法路径依然附属于其他法益的保护。尽管侵犯公民个人信息罪的设置一定程度回应了公民希望通过强有力的法律手段应对人工智能时代隐私风险的迫切需求,但由于刑法中的个人信息与个人隐私在内涵上的部分交叉,该罪名也难以应对当下人工智能发展、运行过程中所产生的与日俱增的权利风险。由于现行刑法中涉及隐私权保护的罪名在犯罪客体、犯罪客观方面存在较大的差异,将直接或间接规制侵犯隐私权行为的条款集中起来再设章节难免破坏既有规范的体系性,因此,单独设立用以保护隐私权的专属罪名以加大对侵犯隐私权的犯罪行为的规制力度具有必要性。

(**责任编辑**:蒋永华　石亚兵)

The Value and Privacy Risks of Deploying AI in Handling a Public Health Emergency: Also on a Criminal Law-based Approach to Privacy Protection

YAN Li, WU Heqi

Abstract: The introduction of relevant state policies has laid a solid foundation for the rapid development of AI for medical purposes in China. In dealing with a public health emergency, AI technology based on medical big data can not only improve the accuracy of diagnosis, alleviate the shortage of medical personnel, but also reduce the medical workers' risk of infection. However, because the operation of AI will inevitably result in the invasion of personal privacy, the criminal law path to the protection of personal privacy in the era of AI should also be aligned with the governance of a public health emergency. In China's criminal law, there is no legal provision regarding privacy as an independent object, and the protection of privacy is attached to the protection of market order, citizens' personal and democratic rights, and social order. In view of the disadvantages, the construction of the criminal law path to personal privacy protection should first take as the logical premise a reasonable definition of personal privacy in the context of big data, and stick to the standpoint of risk prevention and interest balance, rather than defining the boundary of privacy from a static perspective. Only in this way can we carry out the specific design of a criminal law-based path to personal privacy protection.

Key words: public health emergency; big data; AI; privacy risks

About the authors: YAN Li, PhD in Law, is Professor in Shanghai University of Political Science and Law (Shanghai 201701); WU Heqi is PhD Candidate at School of Law, Shanghai University of Finance and Economics (Shanghai 200433).