人脸识别技术的隐私问题探析

蒋鹏宇　杜严勇

摘要：人脸识别技术在身份验证、社交、娱乐等方面存在滥用的现象，其隐私保护需要考虑技术应用的全生命周期。它的非接触式特点使隐私风险变得更为隐蔽，面对技术的强大力量，人们丧失了人脸信息自主权。在“语境完整性”的视角下，人脸识别技术隐私问题产生的原因主要有信息属性的不匹配、数据管理者对信息传输规范的控制以及技术自身的漏洞。为了降低隐私风险，技术应用应当以“技术功能与语境相匹配”这一必要性原则为指导，同时也要改变用户在数据管理中的弱势地位，强化隐私保护的技术手段。

关键词：人脸识别技术；隐私；语境完整性；隐私保护技术

中图分类号：N031　　**文献标识码**：A　　**文章编号**：1000—8691（2023）04—0063—07

人脸识别技术的普遍应用让人们的数字化生活变得更为丰富。在这样一个数字化时代，基于认知计算的数据智能使单个人从统计平均意义上的个体转变为可被单独进行数据解析的对象，这一变化预示着数据解析社会的到来。[①] 个人信息是解析个人的关键，而人脸信息在个人信息中最具可识别性，它的泄露将可能导致多方面的不良后果。人脸识别技术的隐私问题已经引起人们的高度关注。因遭到消费者集体投诉，Facebook 于 2021 年 11 月决定关停人脸识别系统。欧洲议会于 2021 年 10 月通过决议，禁止警方在公共场所或边境检查中实施大规模人脸识别。在中国正式实施《个人信息保护法》之后，事关人脸识别技术的新闻报道也在逐渐增加。人脸识别技术的隐私伦理问题已经成为科技伦理关注的焦点之一。本文介绍了隐私问题的具体表现，以人脸信息的传播为切入点，在“语境完整性”的视角下，探究隐私问题背后的原因，尤其从前瞻性的角度对技术滥用进行了反思，进而初步提出相应的治理路径。

一、人脸识别隐私问题的具体表现

与其他生物信息识别技术如指纹识别、虹膜识别、DNA 识别等相比，人脸识别的优点主要体现在其非接触式采集没有太多的侵犯性。[②] 自 2014 年汤晓鸥及其团队发布 DeepID 系列算法，人脸识别技术的准确率大幅提高，随后在各个领域迅速发展。在具体的技术实践中，人脸识别技术中的隐私问题主要表现在三个方面。

首先，人脸识别技术的滥用增加了隐私保护的复杂性。相比于其他生物识别技术，人脸识别技术的

基金项目：本文是国家社会科学基金重大项目“人工智能伦理风险防范研究”（项目号：20&ZD041）的阶段性成果。

作者简介：蒋鹏宇，男，上海交通大学马克思主义学院博士研究生，主要从事人工智能伦理研究。

杜严勇，男，同济大学人文学院特聘教授、博士生导师，国家社会科学基金重大项目首席专家，主要从事人工智能伦理研究。

① 段伟文：《人工智能与解析社会的来临》，《科学与社会》2019 年第 1 期。

② 段锦：《人脸自动机器识别》，北京：科学出版社，2009 年，第 13 页。

实现设备通用并且简单，只需设备具备摄像功能即可，不需要像指纹或瞳孔识别那样搭配专用信息接收器。这带来的优势是应用人脸识别技术的成本较低，一些本就带有摄像头的设备只需接入人脸识别系统即可，然而这一优势容易导致人脸识别技术的滥用。除了政府对人脸识别的广泛使用，越来越多的私人和商业活动也在使用人脸识别。在随意采集人脸信息的同时，这些组织的信息管理能力却参差不齐。在手机和电脑这类个人设备上，人脸的采集尚可以有“知情同意”的选项，门禁和摄像头这些公共设备却很难落实“知情同意”原则。大多商用人脸识别在收集人脸信息时并未就其收集方式、范围、目的、存储时间等做任何告知，更遑论征求用户同意。[①] 人脸识别设备的滥用使得隐私保护需要考虑技术应用的全周期过程，包括技术应用本身的正当性、技术实践中的伦理指导以及技术产生的社会效应等，隐私保护的复杂度大大增加。

其次，人脸识别技术的隐私风险更为隐蔽。它的非接触式特点不仅为公众提供了便利，也为隐私侵犯提供了便利。相较于其他生物信息，人脸信息的获取容易且隐蔽。人脸信息作为人与人交流的基础，在网络世界往往作为一种公共信息存在，人们早已习惯在社交平台分享个人照片或视频。但一旦将人脸信息从社交语境中抽离，尤其是对网络暴力的受害者而言，它就会成为一种重要的隐私信息，关涉个人尊严。网络上的各种换脸视频已经证明，从网络世界获取并加工人脸信息已经成为现实，这些人脸信息有可能会欺骗人脸识别系统，在当事人不知情的情况下损害当事人的权益。这表明，人脸识别技术产生的隐私问题具有很强的隐蔽性，个人往往只有在损害发生后才意识到隐私信息的泄露，这是隐私保护的一大挑战。

最后，人脸识别技术使人们丧失人脸信息自主权。在数字时代，决定谁可以以及怎样处理个人信息本就非常困难，人脸识别技术的滥用以及隐私风险的隐蔽更是让人们难以控制自己的人脸信息。它既是隐私又不是隐私，这取决于具体情境，个人拥有转换人脸信息属性的权力。然而人脸识别技术的使用削弱了这一权力。在公共空间，人们无法意识到人脸信息的采集与识别发生在何时何处，无法决定某时某刻人脸信息作为何种类型信息存在。在一些技术应用场景中，本是作为隐私存在的人脸信息却被技术当作非隐私信息进行处理。人脸识别技术的滥用同时也造成了人脸信息的单一属性倾向，即仅作为非隐私信息存在，如人脸识别在售楼处、相册分类和门禁中的使用。人们不能决定人脸信息是否属于隐私，也不能控制人脸信息属性的转换，人脸信息一旦被采集，信息的传播与使用完全由信息存储者决定，用户丧失了人脸信息自主权。

二、人脸识别隐私保护中的“语境完整性”

长久以来，对隐私概念的定义一直都是一个难题。1890 年塞缪尔 • 沃伦（Samuel Warren）和路易斯 • 布兰代斯（Louis Brandeis）首次较为系统地论述隐私权，认为个人对自身事务的公开、揭露具有决定权，强调隐私是人们不受外界干扰的独处权。[②] 对隐私概念的讨论随着时代的不同一直在变化。信息技术的出现使信息成为讨论隐私的核心要素，隐私逐渐转变为个人、群体或机构所享有的决定在何时、以何种方式以及在多大程度上将其信息对别人公开的权利。[③] 信息技术使隐私从绝对的不受外界干扰转变为信息的适当披露，如今，数据已经成为新的生产要素，这就要求隐私信息需要更多地参与到信息流通之中。面对越发复杂的信息系统与相关实践活动，海伦 • 尼森鲍姆（Helen Nissenbaum）提出了一种基于语境的隐私理解，隐私的含义因具体语境而异。基于语境的信息规范规定了特定语境下的个人信息流动，当这些规范被违反时，语境完整性遭到破坏，如果这些信息是隐私信息，这也就意味着是对隐私的侵犯。[④] 人脸

① 蒋福明、曾慧平：《人脸识别技术应用中的隐私伦理问题及其消解路径》，《山西高等学校社会科学学报》2020 年第 9 期。

② Samuel Warren, Louis Brandeis(1890). The right to privacy, *Harvard Law Review*, 1890, 4(5), 193-220.

③ Alan Westin(1967). *Privacy and freedom*, New York: Athenum, 7.

④ Helen Nissenbaum(2010). *Privacy in context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press, 127.

信息作为一种个人信息，在社交语境下，它作为人际交往的重要元素，并不被视为隐私信息，但在一些网络暴力中，它又作为重要的隐私信息存在。在当前这样一个以数据为基础的技术环境下，公共空间与私人空间越来越多地融合在一起，隐私信息不再绝对地是一种私人信息。尼森鲍姆提出的 “基于语境的隐私”可以针对具体的技术实践做出调整，使人们较为清晰地认识到隐私侵犯如何发生，可以更有效率地对隐私侵犯行为进行治理。

与语境相关的信息规范包含四个关键因素：语境、参与者、属性和信息传播规范。[①] 语境就是信息规范的背景，不同的语境都有一套独特的规则来管理信息流。以就医为例，在就医的语境下，参与者有病人、医生和医院，病人是信息主体和信息发送者，医生和医院是信息接收者，信息的属性是病人的健康信息，传播规范有“医生应当保证病人的健康信息不被他人知晓”和“医院应当保证病人健康信息存储的安全”等。当这样一种语境完整性得到较好的维持时，就认为没有隐私侵犯产生。如果医生询问病人与就医无关的信息，信息的属性并不属于当前语境的信息规范，语境完整性遭到破坏，就认为发生了隐私侵犯。

在研究人脸识别技术的伦理问题时，当前的学术研究主要聚焦于以“身份验证”为主要用途的人脸识别技术，对“非身份验证”的人脸识别关注并不多。除了身份验证，人脸识别也被广泛应用于人脸信息的获取、处理和分析，如网络照片的搜集、换脸视频的制作、人物心理的分析等。人脸识别技术产生隐私问题的核心原因在于，它处理的是敏感的人脸信息，因此，以人脸信息的传输为切入点，从“语境完整性”的角度可以更加清晰地认识到所有人脸识别技术实践中隐私问题的产生原因。在这样一种“语境完整性”的视角下，人脸识别技术产生隐私问题的原因主要有三类。

（一）信息属性与语境的不匹配

许多语境并不需要敏感信息的介入，技术的滥用却使人脸信息在各种语境下随意传播。小区、动物园、售楼处等都开始配备人脸识别，诚然，技术固然解决了住户认证、游客认证、客户认证等问题，但却产生了更大的隐私问题，引发社会各界的讨论。在这些语境下，人脸信息并不是必要信息，长远来看，强制使用人脸信息产生的积极作用小于消极作用。以动物园为例，人脸识别并没有带来游客认证效率和游客舒适度的大幅度提升，反而因采用敏感的人脸信息增加了游客的隐私危机。动物园需要的只是一些敏感程度较低的个人信息，如手机号、票据等。人脸识别技术的强制应用导致用户的选择权丧失，形成技术霸权，信息属性的不匹配使语境完整性遭到破坏，隐私问题极易发生。

人脸识别技术的滥用反映出，相关组织在决策之前，对应用人脸识别技术的风险缺乏前瞻性评估。一般在讨论责任时，负责任是指成为反应态度的正当目标，也就是说你已经做了某事，为此你应该接受赞扬或谴责。[②] 由于现代信息技术的强大力量，除了追溯性的责任，责任伦理学同时也要求人们承担一定的前瞻性道德责任，相关责任人应当在应用技术之前进行必要的思考。与其他价值相比，虽然隐私不是处于核心地位，但它却是核心价值——安全的体现。[③] 因此，评估人脸识别技术所使用的信息属性即人脸信息与具体语境是否匹配，是相关责任人在应用人脸识别技术之前应当负有的责任，人脸识别技术的滥用现象反映了这一责任的缺失。不仅仅是这些技术管理者，一些用户也并不能认识到人脸信息对个人隐私的重要性，从而无法做到恰当的前瞻性评估，大多用户默许人脸识别技术的使用，不会对它进行怀疑。因为这些错误评估，人脸信息与许多语境不匹配，即使在技术使用之后建立一些制度标准进行限制，依然无法从根源上解决问题。面对此类问题，需要做的是彻底消解技术的不合理性，即取消技术的使用。

（二）数据管理者对信息传输规范的控制

在合适的情境下使用人脸识别技术依然会产生隐私伦理问题，如因人脸信息的让渡引发的算法歧视、信息自主权缺失、知情同意缺失等问题。面对个人信息的传播与处理，政府和各大企业平台都制定了相

① Helen Nissenbaum, *Privacy in context: Technology, Policy, and the Integrity of Social Life*, 141.

② 杜严勇：《人工智能伦理引论》，上海：上海交通大学出版社，2020 年，第 198 页。

③ 刘佳明：《人脸识别技术正当性和必要性的质疑》，《大连理工大学学报（社会科学版）》2021 年第 6 期。

应的信息传输规范。《个人信息保护法》规定个人信息的处理需要取得个人的同意，并且个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务。在这类规范的指导下，数据管理者制定隐私政策，在提供服务之前征求用户的同意。然而这些“告知”或是出现于不起眼的地方，或是含糊不清，并且因不同意而无法使用的情况依然很普遍。

在当前的技术架构下，隐私政策由拥有信息的数据管理者制定，这就使数据管理者掌握着信息传输规范的最终解释权。而作为信息主体的用户除了被动的接受，还要承担隐私风险。大多数据管理者也许能认识到隐私问题的存在，但因为数据已经成为新的生产要素，面对数据蕴含的巨大价值，他们所制定的信息传输规范自然不会以用户为中心，这就导致语境完整性的维持并不稳定。人类具有自利的本性，但在肯定这一本性的同时，也能够通过游戏规则的塑造使自利服务于人性，从而实现使人达致人性化的伦理目标。[①] 然而如果自利者控制着游戏规则的制定，隐私保护的目标将永远无法实现。即使用户感知到隐私风险，数据管理者仍可以借助信息传输规范做出解释。想要避免他们对人脸信息的隐蔽式使用，需要让用户也参与到信息传输规范的制定中，改变用户的弱势地位。如何平衡个人信息的适当流通和用户的信息自决权是解决该类问题的最大难点。

（三）人脸识别技术自身的漏洞

此类问题的边界最为清晰，人脸识别需要数据库存储用户的人脸信息，数据库的安全程度由技术条件决定，技术自身的不稳定也就导致了语境完整性的不稳定，数据的泄露会带来不必要的信息接收者，从而破坏原有语境的完整性。不法分子利用技术漏洞获取数据库信息的案例时有发生，如 2018 年 12 月 Facebook 曝出由于软件漏洞，6800 万用户的私人照片遭到泄漏。人脸信息数据库的泄漏对社会的影响往往是巨大的，泄漏事件一方面会导致人们的利益受损，另一方面也会降低公众对数据管理者的信任。公众对技术安全的理解很简单，即从结果上看技术保护了与个人密切相关的信息隐私数据。[②] 公众往往以结果为导向，只有减少信息泄露事件的发生，才能提高公众对技术和数据管理者的信任。技术保护往往只能由新的技术来实现。在技术保护方面，科技人员已经进行了各类尝试。例如，隐私增强技术在人脸识别阶段使用安全多方计算，对服务器隐藏生物信息和验证结果，从而实现了对人脸信息的保护。[③] 虽然不存在绝对安全的技术，但在人们可以接受的安全风险下使用人脸识别是可以实现的。相比于前两类问题，如何解决技术漏洞导致的隐私问题也更加清晰。

三、人脸识别隐私问题的应对路径

究其本质，技术实践对信息语境完整性的破坏反映了人文文化与科技文化的冲突。技术的强大力量引诱人们过度关注工具理性，忽视了价值理性，造成各种隐私问题的出现。隐私保护的难题就是怎样处理两种文化的关系问题，最重要的是重建价值理性和工具理性的关系，以价值理性熔铸工具理性。[④] 人脸识别技术所反映的科技文化追求人脸信息高效、准确的识别作用，以人脸信息代表一个具体的人，甚至仅以人脸信息代表个人。尊重隐私、尊重人之技术将始终作为人类寻求幸福生活的手段而存在。对个人隐私的保护并不是出于技术的安全与发展，而是出于人的价值，这正是人文文化的追求。以价值理性熔铸工具理性，需要始终以个人隐私信息背后的人文价值为中心，而不是过多强调隐私信息的经济价值。基于此，解决人脸识别技术的隐私问题，应当以伦理原则为指导，改变用户在数据管理中的弱势地位，将隐私保护意识融入技术的开发中。

① 甘绍平：《伦理学的当代建构》，北京：中国发展出版社，2015 年，第 373 页。

② 杨庆峰：《数据共享与隐私保护——一种技术方案的哲学论证》，《自然辩证法研究》2018 年第 5 期。

③ Zekeriya Erkin, Martin Franz, Jorge Guajardo, et al.（2009），“Privacy-Preserving Face Recognition,” in Ian Goldberg and Mikhail Atallah, eds., *Privacy Enhancing Technologies*, Heidelberg: Springer, 236.

④ 王金柱、张旭：《隐私研究的“困难”审视》，《自然辩证法研究》2020 年第 6 期。

（一）必要性原则：技术功能与语境相匹配

在分析人脸识别技术的隐私问题时，当前的学术讨论多是聚焦于技术实践产生之后的问题，对人脸识别技术的前瞻性讨论比较少。人脸识别应用依然因循着“先应用后治理”的新技术应用思路。[①] 然而在许多语境下，人脸识别技术一经介入就会打破原有的信息传输规范，技术应用本身就是问题。技术实践产生的社会影响是实然层面的，具有一定的主观性，有些人可以接受人脸识别门禁，有些人却无法接受。但对技术功能的描述是一个应然层面的概念，具有客观性。因此，在技术实践产生之前，从功能上对人脸识别技术进行考察，可以得到较为客观的结论。人脸识别在安防与金融领域的应用虽然也有一些问题，但相比之下，伦理争议比较少。原因就在于两者的使用语境与人脸识别的技术功能较为匹配。技术功能决定了特定技术必然存在一定的应用范围，在对技术应用进行前瞻性评估时，以“技术功能与语境相匹配”这一必要性原则为指导，有助于规避人脸识别技术的错误应用。

人脸识别技术的功能是识别人脸信息。在安防领域，公安警察的职责是在人群中寻找犯罪嫌疑人，“身份验证”是这一过程的核心，人脸识别可以让安防人员高效识别人脸，这就与语境高度匹配。反观中国的“人脸识别第一案”，动物园入园检票是为了筛选游客是否已经购买门票，这一过程主要识别票的真伪，身份验证已经出现在购票阶段，检票阶段再次使用人脸识别进行身份验证就造成了技术的过度使用，导致原有的语境完整性存在被破坏的风险，从而产生隐私风险。

要实现技术功能与语境的匹配，存在两个过程。一是能够正确认识技术的功能。了解人脸识别技术的功能对人们来说并不困难，重要的是认识功能背后附带的隐私价值。人脸信息不仅属于普通数据，它关乎人格权与财产权，对人脸信息的保护应优先于数据流通的价值变现。[②] 相关技术企业应当避免对产品的过度宣传，不仅要让使用者了解技术的强大能力，还应对技术可能存在的隐私风险做必要的说明。二是能够正确认识使用语境。在选择使用人脸识别技术之前，要了解语境的核心要素，即参与者、信息属性和信息传输规范。问题看似简单，但使用者恰恰容易忽略这些考量。以换脸视频为例，使用他人的人脸信息制作视频，信息发送者并非信息主体，由于当前这类语境下的信息传输规范依然比较缺乏，在没有严格的信息传输规范保护信息主体隐私的情况下，即使使用公众人物的人脸信息制作换脸视频，制作者也应当承担由于不能正确认识语境所导致的隐私责任。大多用户往往有一些认知偏差，当用户感知隐私披露的收益是立即能享受到时，他们更倾向于认为此行为是风险更低而利益更高，不能敏感地认识到隐私泄露所带来的长远性风险。[③] 因此，想要在应用人脸识别技术之前就意识到其背后巨大的隐私风险是十分困难的。要实现这一目标，不仅需要在不同语境下进行多方面的评估，还需要相关使用者克服认知偏差。在用户的认知水平无法正确认识语境时，就需要信息传输规范以及隐私保护技术的介入。

（二）改变用户在数据管理中的弱势地位

技术平台借助于技术的强权，在技术实践中占据着主导地位。用户一旦将人脸信息录入系统，由于信息传输规范由平台制定，相关平台就拥有了数据的绝对控制权，用户的隐私安全完全取决于平台的数据管理能力。在责任伦理的视角下，平台对技术的使用具有一种“前瞻性道德责任”，他们大多能够认识到他们应当承担的责任，但问题在于有些人不愿意去履行这种道德责任，责任仅仅停留在理性认知层面，不能成为鲜活的责任实践。[④] 因此，问题的解决仅仅通过约束技术平台是无法实现的。为了改变用户的弱势地位，需要进一步细化法律法规，同时还要赋予用户更多的数据管理权力。政府、平台和用户三方共同努力去优化数据管理才能促使责任实践成为可能。

第一，强化技术平台的社会责任。对技术平台而言，法律法规是处理个人信息的底线，作为技术发

① 段伟文：《人脸识别：“裸奔”时代的我们》，《商学院》2021 年第 1 期。
② 林凌、贺小石：《人脸识别的法律规制路径》，《法学杂志》2020 年第 7 期。
③ 刘婷、邓胜利：《国外隐私悖论研究综述》，《信息资源管理学报》2018 年第 2 期。
④ 龙静云、吴涛:《新责任伦理: 技术时代美好生活的重要保障》,《华中师范大学学报（人文社会科学版）》2021 年第 5 期。

展的主导者，除了追求经济利益，遵守基本法律，还应主动承担起较高的社会责任，应当以经济利益与技术服务并重。经济利益固然重要，它是技术进步的资本，但当某一技术被普遍应用于社会各个领域时，技术平台就应当担负更多的社会责任。相比于钻法律法规漏洞和制造技术霸权，优秀的技术服务不仅能带来长久的经济利益，也可以获得公众的普遍信任。大卫•科斯（David Coss）和古佩特•狄伦（Gurpreet Dhillon）通过分析实验数据，提出了云计算技术的 6 个隐私保护目标，其中“提高对技术提供者的信任”和“最大限度承担信息管理的责任”[①] 对任何信息技术来说都是适用的，人脸识别技术也不例外。信息泄漏事件的时常发生使用户对技术的信任度并不高，数据管理者以用户为重才能体现出所承担的信息管理责任，才会提高用户的信任。

第二，细化法律法规。对政府而言，制定法律法规是保护公众隐私的有效手段。《个人信息保护法》要求个人信息处理者应当采取一些措施保护个人信息，如制定管理制度、对个人信息分类管理、采取安全技术、对从业人员进行教育和培训等。但在具体实践中，个人信息处理者的落实仍不够全面，App 隐私说明隐晦、不同意则无法使用、用户反馈通道不明晰、广告针对性投放等问题依然存在。最高人民法院于 2021 年 7 月 28 日发布了《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》。2021 年 10 月，欧洲议会通过决议，也禁止了警方在公共场所或边境检查中实行大规模人脸识别。可见各国政府已经在加紧对人脸识别技术进行更加细致的规范，不再只是通过宏观原则保护人们的隐私。

第三，落实用户更多的数据管理权力。对用户而言，虽然无法涉足技术的开发以及管理环节，但作为信息主体，用户应当参与具体技术实践的信息传输规范的制定。伦理与法律法规都强调了用户的知情、撤销、更改、删除等权力，但在许多技术实践中依然缺乏具体的实现机制，如许多小区仍不能提供删除人脸信息的选择。此外，人脸识别技术的透明度较低，用户大多没有什么技术基础，对人脸信息存储在哪里、人脸信息的接收者有哪些、信息是否已经删除等几乎是无知的，知情权无法落实。当用户真正拥有这些数据管理权力时，才能实现个人数据个人控制。同时，许多用户并不能清晰地意识到自己所拥有的数据管理权力，根据人民智库的调查，公众的隐私意识属于中等稍高水平，公众隐私意识平均值为 58.69，满分 100。虽然超过八成的受访者认为私人信息是有价值的，但仅仅有 28.89% 的人“主动地采取保护措施”[②]，公众的隐私防范意识仍有待提升。

（三）强化隐私保护的技术手段

技术平台除了技术运营，往往还担任着技术开发和维护的角色。技术的隐私安全度越高，隐私问题就会越少。保护隐私的人脸识别技术可以体现在人脸信息的采集阶段和识别阶段。

在人脸信息的采集阶段，一种采用差分隐私的人脸识别技术可以对人脸信息进行数据扰动，经过这一过程，存储在第三方数据库的人脸信息将不再是原始信息。经过数据扰动，数据库即使遭到泄漏，不法分子得到的也只不过是一些杂乱信息。通过实验，该技术在相应隐私标准下可以显示出约 70%—90% 的分类准确率。[③] 差分隐私技术直接降低了数据库中人脸信息的敏感度，大幅度提高了用户人脸信息的存储安全。基于该技术，用户在使用人脸识别技术时没有产生新的真实人脸信息，同时又能保证技术的正常使用，这不仅降低了人脸信息被盗取所产生的威胁，也可以提高用户对技术管理者的信任度，对解决隐私问题起到了较大作用。

在人脸识别阶段，前文提到的安全多方计算可以对服务器隐藏生物信息和验证结果，这一隐私增强

① David Coss, Gurpreet Dhillon(2019), Cloud privacy objectives a value based approach, *Information & Computer Security*, 27(2), 189-220.

② 张捷：《当前公众的信息安全意识与隐私观念调查报告》，《国家治理》2020 年第 14 期。

③ Mahawaga Chamikara, Peter Bertok , Ibrahim Khalil, et al. (2020), Privacy Preserving Face Recognition Utilizing Differential Privacy, *Computers & Security*, 97,1-12.

技术采用了一个高度优化的加密协议，不需要共享真实信息即可以在多方之间进行信息交流。此外，对社交平台中的人脸信息进行技术保护也是必要的，人脸识别容易在用户不知情的情况下发生，社交平台上的个人照片随时都可能被人脸识别技术进行识别分类，一种匿名化人脸信息技术可以帮助用户对抗人脸识别算法，同时又可以保留更多的原始信息使得人类仍然可以进行识别。[①] 匿名化可以干预人脸识别技术的识别结果，在对抗人脸识别技术强制使用的同时，又不影响人们在社交网络中分享个人照片。

随着 Web3.0 的发展，个人数据个人存储在技术层面也成为可能。在 Web3.0 的架构下，数据不再由平台存储，个人拥有真正的身份自主权、数据自主权和算法自主权。平台之间通过分布式协议连接，用户可以通过极小的成本从一个服务商转移到另一个服务商，用户与建设者平权，不存在谁控制谁的问题。任何人都可以在智能合约中设立他们自由定义的所有权规则和交易方式。[②] 在 Web3.0 这一分布式基础设施的框架下，用户摆脱了原有的弱势地位，拥有真正的数据自主权，隐私问题将大幅解决。

不管是采用何种方法，技术人员早已关注到了人脸识别技术中的隐私问题，也已探索出很多保护隐私的技术手段，这些技术的成熟与普及对解决隐私问题至关重要。

总而言之，不管是在道德领域还是法律领域，隐私对人们的重要性不言而喻。人脸识别技术在身份验证、社交、娱乐等方面都存在滥用现象。在技术应用之前，人们对它的前瞻性评估还比较缺乏。“语境完整性”视角可以帮助人们提前预知可能存在的隐私风险，可以针对信息主体、信息属性、信息接收者和信息传输规范进行及时的隐私治理。只有人脸识别技术与语境相匹配时，技术应用才不会增加人们的隐私风险。同时，在技术实践产生之后，隐私问题的应对需要技术平台、政府以及用户共同努力。在现有技术架构下，法律法规的细化、对平台的严格约束、落实用户的数据管理权、强化技术手段都可以有效降低隐私风险。未来，当个人数据真正属于个人时，有了真正的数据自主权，个人数据的隐私价值也就拥有了对抗工具价值的力量，人文文化与科技文化的隐私冲突也将得到有效改善。

An Analysis of Privacy Issues of Face Recognition Technology

JIANG Peng-yu[1] & DU Yan-yong[2]

(1.School of Marxism, Shanghai Jiao Tong University, Shanghai, 200240;

2.School of Humanities, Tongji University, Shanghai, 200092)

Abstract: Face recognition technology is abused in authentication, social networking, entertainment and other aspects and its privacy protection needs to consider the whole life cycle of technology application. The non-contact feature of face recognition makes the privacy risk more hidden. Facing the power of technology, people have lost the autonomy of face information. From the perspective of “contextual integrity”, the main reasons for the privacy problems of face recognition technology are the mismatch of information attributes, the control of data managers over information transmission principles and the defects of the technology itself. Based on the need to reduce privacy risks, the technology application should be guided by the necessity principle of “matching the technology function with the context”. In addition, we also should change the weak position of users in data management and strengthen the technical means of privacy protection.

Keywords: Face Recognition Technology, Privacy, Contextual Integrity, Privacy Protection Technology

[责任编辑：谢雨佟]

① Benedikt Driessen, Markus Dürmuth(2013), “Achieving Anonymity against Major Face Recognition Algorithms,” in Bart Decker, Jana Dittmann, Christian Kraetzer, et al. eds., *Communications and Multimedia Security*, Heidelberg: Springer, 19.

② 姚前：《Web3.0：渐行渐近的新一代互联网》，《中国金融》2022 年第 6 期。