

人脸识别应用下的公民权利保护

陈志娜, 钟浩龙

广东工业大学法学院, 广东 广州

收稿日期: 2026年6月22日; 录用日期: 2026年7月22日; 发布日期: 2026年7月30日

摘 要

当前, 人脸识别技术在我国得到了广泛的应用。然而随着人脸识别技术的越加普及, 技术的滥用与公民个人信息的窃取盗用带来了安全之忧, 公民的个人生物识别信息安全面临着一定程度的威胁, 公民权利遭受侵权之殇。要实现技术的发展和公民权利的保障之间的平衡, 立法与司法等层面的规制及其制度完善刻不容缓。因此, 需要对人脸识别技术的应用与公民权利的保护有更深一步的认识。文章将分为以下四个部分: 一是简述了人脸识别的技术概况; 二是通过我国人脸识别第一案对其背后的公民权利之忧展开论述; 三是讲述人脸信息与多项公民权利之间的关系; 最后对有关人脸识别信息保护的困境以及人脸识别技术应用与公民权利保护平衡的完善路径进行探究。

关键词

人脸识别, 生物识别信息, 公民权利, 法律规则

Civil Rights Protection under the Application of Face Recognition

Zhina Chen, Haolong Zhong

School of Law, Guangdong University of Technology, Guangzhou Guangdong

Received: June 22, 2026; accepted: July 22, 2026; published: July 30, 2026

Abstract

At present, face recognition technology has been widely used in China. However, with the increasing popularity of face recognition technology, the abuse of technology and the theft and theft of citizens' personal information have caused security concerns. Citizens' personal biometric information security is facing a certain degree of threat, and citizens' rights have suffered from infringement. In order to achieve the balance between the development of technology and the protection of civil rights, it is urgent to improve the regulation and system at the legislative and judicial levels. Therefore, it

is necessary to have a deeper understanding of the application of face recognition technology and the protection of civil rights. The article will be divided into the following four parts: First, it briefly describes the technical overview of face recognition; the second is to discuss the worries of civil rights behind the first case of face recognition in China; the third is about the relationship between face information and multiple civil rights; finally, it explores the dilemma of face recognition information protection at the legislative and judicial levels in China and the improvement path of the balance between the application of face recognition technology and the protection of civil rights.

Keywords

Face Recognition, Biometric Information, Civil Rights, Legal Rules

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

近年来,生物识别技术在众多领域快速发展并推广,但该类技术在开发利用中暴露出诸多数据安全风险,加之戴口罩人脸识别等新技术的广泛应用,使得公民个人相关权利的保护成为学术研究热点。人脸识别是通过识别人类面部特征验证个体身份的科学技术,已在各领域广泛应用,正逐渐渗透到社会生活的方方面面。人脸信息是个体与生俱来的身份标识,具有唯一性、不可变性与强烈的人格属性,若被不法分子获取,将为其实施违法犯罪活动提供便利,严重侵害公民个人权利,亟须法律严加保护。基于此背景,笔者就人脸识别技术概况、相关公民权利的论述、部分法律规制的问题等发表浅见,以期平衡人脸识别技术应用与公民权利保护提供思路。

2. 人脸识别技术手段概述

2.1. 人脸识别的定义与特点

人脸识别技术是一种通过收集人的面部表征信息,进行比对分析后完成个体身份识别验证的技术。该技术的核心在于人的脸部特征信息,相较于普通个人信息,人脸信息具有以下几方面突出特点:

首先是技术性,人脸信息数据需通过生物识别技术、算法等手段获取并固定,其利用离不开相关技术支撑;但一旦不法分子非法利用这类信息谋取不当利益,就可能引发民事侵权或刑事犯罪。

再有是隐私性。人脸信息通过技术手段获取,集合了个体特征,使其成为公民个人的“数据身份证”。在技术发展初期,相关信息数据或许适宜公开,但随着人脸识别技术的广泛应用,难免有心之人非法泄露不宜公开的隐私信息,这在一定程度上可能造成个体歧视等社会不公现象。

人脸信息还具有易侵性。随着现代数字媒体的高度发达,过度收集、非法采集乃至非法泄露人脸数据的现象已不再是个例,再加上暗中偷拍等手段层出不穷,人脸数据不仅唾手可得,其安全更是岌岌可危。

2.2. 应用领域与技术步骤

2.2.1. 应用领域

作为人工智能的典型应用,人脸识别技术近年来已深度渗透至社会生活各领域,其应用场景从车站、机场等公共场所,迅速拓展至移动支付等日常金融交易之中[1]。具体而言,人脸识别技术现已广泛应用

于证件核验、入口控制及安保领域。证件核验方面,在汽车站、火车站、机场等公共交通站点,乘客通过人脸识别与身份证件照片的比对进出乘车站口,实现了证件检验的自动化管控;入口控制领域,许多小区物业安装了人脸识别门禁系统,住户预先在系统中提交人脸照片,经计算机系统转化为人脸数据后,日常进出时即可刷脸通行;安保领域中,无论是场所监控的视频识别与定位追踪,还是公安机关对嫌疑人的追击逮捕,人脸识别技术都是高效便捷的工具。

2.2.2. 技术步骤

人脸识别技术主要包含人脸检测、人脸特征定位与提取、人脸识别三个核心步骤。具体而言,考虑到人脸识别场景中环境的复杂性,技术流程的第一步是从拍摄的图像中检测并提取人脸的图像及位置信息,以此排除背景环境的干扰;第二步为人脸特征点的定位与提取,即在完成人脸整体检测后,系统需进一步细化提取人脸的细节特征,即先对人脸的多个特征点进行定位,再将人脸图像量化处理,把各项特征信息转化为对应的特定数值;第三步则是最终的人脸识别环节,经过前序步骤的图像处理,系统已获取基础分析数据,此时输入待识别的人脸特征,系统即可精准定位并呈现匹配度最高的人脸信息。

2.3. 人脸信息的法律属性

最高人民法院在 2021 年 7 月 28 日发布的《最高人民法院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》中第一条第三款明确了人脸信息的法律属性,确定其属于我国民法典第一千零三十四条规定的“生物识别信息”¹。个人信息、个人敏感信息、生物识别信息与人脸信息四者之间是从大到小的范围包含关系。

公民个人信息作为包含关系中含义范围最广的概念类型,是指可用以区分、识别某个自然人个人身份及其专属个人情况的各种资料信息的总和,在数字化时代,个人信息往往以电子数据的方式存在,诸如姓名、身份证件号码、家庭住址、联系方式等。在此框架下,生物识别信息因其高度敏感性而被置于特殊保护地位。欧盟采取统一严格的立法模式,以《通用数据保护条例》(GDPR)为核心,将生物识别数据列为特殊类别予以原则性禁止处理,仅允许在明确同意等例外情形下使用²。相较之下,美国则呈现分散式规制格局,联邦层面尚未建立统一的生物识别隐私立法,主要依赖州级法律发挥实质约束作用,其中尤以伊利诺伊州《生物识别信息隐私法案》(Biometric Information Privacy Act,简称 BIPA)最具代表性。BIPA 要求企业在收集生物识别标识符前必须履行书面告知义务、获取数据主体的书面知情同意,并制定公开的数据保留与销毁政策,同时赋予个人强大的私人诉权,使其成为制约企业行为的关键机制³。

在我国,根据《中华人民共和国个人信息保护法》⁴(后文简称《个人信息保护法》),个人敏感信息是一旦被泄露或者被非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,其包括生物识别信息、医疗健康信息、生物识别信息等等。生物识别信息作为个人敏感信息,较深程度地体现自然人的生理和行为特征,具体包括个人基因、指纹、声纹、掌纹、耳郭、虹膜、面部识别特征等,其中表现面部识别特征的信息即为文章所要探析的人脸信息。随着科技发展,人脸识别技术为社会生活带来诸多便利,但该技术的应用离不开人脸信息的收集。看似单一的人脸信息,实则关系到

¹<http://gongbao.court.gov.cn/Details/118ff4e615bc74154664ceaf3bf39.html>

²参见《欧盟通用数据保护条例》(《General Data Protection Regulation》)第 9 条第一款, <https://gdpr-info.eu/>, 2026 年 7 月 3 日访问。

³参见 US Law Explained: 《Biometric Information Privacy Act (BIPA): The Ultimate Guide》, <https://uslawexplained.com/biometric-information-privacy-act-bipa>, 2026 年 7 月 3 日访问。

⁴《中华人民共和国个人信息保护法》第二十八条:敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息。

公民多项合法权利的行使, 客观上对人脸信息权益构成了一定程度的威胁, 因此完善人脸识别侵权的法律保障具有重要意义。作为防范社会风险、赋能公共服务的重要技术手段, 人脸识别的应用必须因场景而制宜, 同步强化对个人人脸信息的保护, 实现技术与权益保障的和谐共进[2]。

3. 人脸识别技术背后的公民权利之忧

3.1. 我国人脸识别第一案

2019年, 大学教授郭兵将杭州野生动物世界诉至法院。郭兵主张, 动物园取消原指纹识别、启用人脸识别技术的行为未充分保护用户隐私, 已违反《消费者权益保护法》, 遂向杭州市富阳区人民法院提起侵权诉讼⁵。最终, 法院判决杭州野生动物世界向郭兵赔偿合同利益损失及交通费, 并删除其办理指纹年卡时提交的含照片在内的面部特征信息; 但驳回了郭兵的其他诉讼请求。这一案件引发社会舆论广泛关注, 其中围绕个人生物识别信息安全展开的讨论, 发人深思。

近年来, 人脸识别等生物识别技术在诸多领域得到应用与发展, 戴口罩人脸识别、红外体温检测等新技术也逐步普及。然而, 生物识别信息的独特属性使其在开发利用过程中暴露出不少数据安全风险[3]。人脸识别技术采集的面部信息属于个人生物识别信息, 与姓名、身份证号码等普通个人信息不同, 具有更强的唯一性和不可更改性。一旦此类信息泄露, 将对公民造成不可逆的损害。此外, 随着动态人脸识别、无感采集等新技术的涌现, 人脸信息侵权形态日趋复杂, 司法实践亦在积极回应。例如, 在无感采集与强制刷脸场景中, 司法明确强化了知情同意与非唯一性原则。在浙江平阳一起售楼处“无感抓拍”客户人脸信息案中, 法院认定开发商未经同意以人脸识别系统截图作为证据, 因取证方式严重侵害他人合法权益, 对该证据不予采纳⁶。此外, 2025年, 中山市检察机关针对游戏游艺设备“强制刷脸”“无感采集”“默示同意”等问题提起行政公益诉讼, 推动行业整改并促成自律倡议出台⁷。上述判例表明, 司法实践正通过个案裁判逐步回应技术发展带来的挑战, 在知情同意、合规处理、安全保障的全链条侵权认定体系基础上, 进一步将规制触角延伸至深度伪造、算法滥用等新兴领域, 为技术向善划定清晰边界。

我国“人脸识别第一案”中, 人脸识别技术应用背后的“安全隐忧”——公民合法权利遭受侵害的相关问题, 具有深入探究的价值。由于人脸识别技术的先进性, 公民权利保护出现漏洞的可能性随之增加, 多项相关权利可能时刻面临被损害的威胁。

3.2. 法定人脸识别侵权行为种类

最高人民法院发布的《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》中列举了人脸识别侵权行为的具体情形, 共包含以下八类: 一是公共场所经营管理者违规使用人脸识别技术; 二是未履行告知义务, 即未公开处理规则, 或未明确告知处理目的、方式及范围; 三是未就人脸信息处理取得单独同意或法定书面同意; 四是超出明示或约定的处理范围; 五是未充分履行信息安全保障义务, 导致人脸信息泄露、篡改或丢失; 六是违规或违约向他人提供人脸信息; 七是处理行为违背公序良俗; 八是其他违反合法、正当、必要原则的处理行为。该八类情形的规定, 以类型化的方式将人脸识别中个人信息处理的原则性规范具体化, 形成了从事前告知同意、事中合规处理到事后安全保障的全链条侵权认定体系。其不仅为法院裁判提供了清晰明确的法律适用依据, 有效统一了司法裁量标

⁵参见《郭兵与杭州野生动物世界有限公司服务合同纠纷一审民事判决书》, 载中国法学会网络与信息法学研究会官网, <https://cyberlaw.chinalaw.org.cn/portal/article/index/id/540.html>, 2026年6月27日访问。

⁶参见《开发商擅自采集客户人脸作诉讼证据 浙江平阳县法院: 侵害他人合法权益的证据不予采纳》, 载中国法院网, <https://www.chinacourt.cn/article/detail/2023/06/id/7372751.shtml>, 2026年7月3日访问。

⁷参见《中山检察1案例入选! 广东省人民检察院发布“3·15”消费者权益保护检察公益诉讼典型案例》, 载中山检察在线网, <https://www.zhongshan.jcy.gov.cn/article/view/cateid/16/id/19056.html>, 2026年7月3日访问。

准, 也通过划定行为红线, 强化了对信息处理者的程序性约束, 充分体现了在技术应用与权利保护之间寻求平衡的规范意图, 对于应对人脸识别技术广泛使用所带来的法律挑战具有重要的实践指导意义。

3.3. 人脸识别技术侵权表现形态

3.3.1. 人脸数据信息收集过程中的侵权

人脸识别技术的首要环节是人脸图像收集, 而在此过程中, 技术应用方常存在通知与告知义务履行不到位的问题。以上文提及的郭兵案为例, 动物园要求入园游客进行人脸识别时, 仅通过简单告示进行单方通知。这种方式难以确保所有游客在被拍摄人脸图像前, 充分了解自身人脸信息将被收集的事实^[4]。部分游客甚至可能因未注意到告示, 在毫无察觉的情况下就被录入了脸部信息。人脸数据收集本质上是对个人私密特征信息的获取, 由于生物识别信息相较于普通个人信息具有更强的确定性与唯一性, 因此在收集人脸图像时, 更应充分告知被采集者相关信息, 使其在相对完全知情的前提下, 行使个人信息权并做出是否同意的决定。

例如前文提及的我国人脸识别第一案中, 这种形式上的“知情同意”实际上侵犯了信息主体的信息决定权; 当公民在对自身提供的相关信息缺乏充分认知的情况下做出决定时, 其决定的效力难免令人质疑。

此外, 人脸识别与其他生物识别技术存在差异, 例如人脸信息的收集相较于指纹信息的收集缺乏交互性。具体而言, 指纹收集需公民将手指按压至指定接触面, 收集方才能获取相关生物识别信息; 而人脸图像的收集无需公民将脸部接触任何平面, 这种收集方式虽更为便利, 但也导致在许多情况下, 公民尚未意识到自身脸部图像信息已被收集完毕。

3.3.2. 人脸数据信息处理过程中的侵权

当公民的面部信息完成整体检测后, 相关处理系统需进一步提取面部细节特征, 将其整合为数值集合并进行比对与存储。在此过程中, 信息收集方对数据泄露风险的把控存在不确定性。近年来, 人脸识别技术应用愈发广泛, 但对大规模人脸信息的处理与存储, 反而导致安全风险持续攀升。同时, 在社会执法领域, 若公务机关未能平衡公民私权与社会公权的关系, 便可能在信息处理环节侵犯公民个人信息, 引发非法公开个人信息、数据泄露等问题。

3.3.3. 人脸数据信息使用过程中的侵权

人脸数据信息的收集与使用具有必然的强关联性, 因此, 数据信息的使用范围应严格限定于原始收集目的, 超出该范围的使用行为属于违法行为。人脸识别的最终科学目标并非简单的身份验证, 而是通过收集和处理个人面部信息实现对个体的预测。例如, 在海量人脸数据库中, 技术人员将面部信息与信息主体的个人病史、过往经历等隐私数据关联整合并分类, 可能在数据库中形成将人类划分等级的风险。在就业领域, 这类经过分析分类的数据可能被用于筛选应聘者, 从而引发严重的就业歧视。相较于数据泄露, 这种类型的“人脸识别”应用才更令人担忧。

4. 人脸数据信息与公民权利的关系

4.1. 公民隐私权

从相关法律规定来看, 公民个人不愿公开且与社会公共利益无关的信息, 属于公民个人隐私。由此可见, 隐私权的构成需满足两大要素: 一是信息未经披露, 二是不涉及公共利益。然而, 在人脸识别技术的应用中, 对公民面部信息的收集行为本身, 就意味着这些信息已被对外披露。正是通过这种披露, 人脸识别信息的收集方才能够整合人脸数据, 并在识别过程中实现精准匹配。其次, 公民个人隐私信息

本应与社会公共利益无关,但近年来,人脸识别技术已成为防疫、执法等领域的重要技术手段,公民面部信息与社会重大公共利益的关联性正日益增强。

人脸识别技术通过各类科技手段,表面上似乎仅涉及对公民肖像权的侵犯,但其背后的技术逻辑实则会导致公民其他信息的透明化,包括内心情绪、情感波动等深层状态都可能被清晰捕捉。换言之,技术能够将人们的内心活动转化为可被处理和呈现的外在信息,公民的隐私边界也因此受到侵害^[5]。此外,隐私权属于消极性权利,即公民仅在该权利受到他人侵犯时才能行使,这意味着隐私权的救济方式偏重于事后救济,要求具备“实际损害结果”这一构成要件。然而,人脸识别技术引发的侵权行为,其当下造成的“损害”可能并不显著,正如上述案例中的郭兵,并未因动物园采用人脸识别技术而遭受严重损害。

综上,笔者认为以隐私权保护来应对人脸识别这类生物识别信息技术的侵权问题,其精准性与妥当性均有所不足;但若对这类技术简单采取“一刀切”式的禁止,又会抑制有益的信息识别技术发展,这显然有悖于人类社会的发展规律。

4.2. 公民肖像权

我国宪法赋予每个民事主体肖像权,其内容包括肖像制作专有权、肖像使用专有权及肖像利益维护权。人脸识别技术通过科技手段收集自然人的生物特征信息,并将数据传输至对应数据库存储,在此过程中,信息收集环节易被他人利用以谋取非法利益,进而侵害公民对自身肖像的专有使用权。在人脸识别中,肖像是实现该技术的载体,通过技术手段非法利用人脸信息,本质上就是对公民肖像的非法使用,无疑构成对肖像权的侵犯。

人脸识别的侵权行为与肖像权密切相关,这一点毋庸置疑。然而笔者认为,肖像权的保护范围相对有限,难以充分满足受害者及维权者的核心诉求。实际上,权利人真正在意的并非仅仅是形象被盗用或丑化,而是担忧他人非法利用其人脸信息冒用身份实施不法行为,导致无端承担不良后果;同时也担心个人身份验证信息在系统中出现错误,给社会生活与工作带来困扰。安全感源于权利人对自身生物识别信息的掌控力,而这正是肖像权保护无法提供的。

4.3. 公民个人信息权

由上文可知,公民隐私权的适用性不强、肖像权的保护范围有限,相比之下,公民个人信息权才更符合人脸识别维权保护的属性。从权利内容来看,信息主体享有“信息决定权、信息知情权、信息保有、信息保护权”等多项权利,对其个人生物数据信息拥有绝对控制力;另一方面,当生物识别信息受到侵害时,公民还可主张人格权请求权,通过对精神利益与财产利益的双重保护,确保权利人获得充分救济。

前文提及的“郭兵案”中,动物园采集并使用当事人的面部数据时,仅以告示形式告知人脸识别的使用方式,既未直接征得当事人同意,也未能确保其知情,这种单方通知的做法,显然难以让公众安心提供面部信息。在权利人未有效行使信息知情权、决定权等个人信息权的情况下,数据利用方的行为是否构成侵权、相关信息的储存与处理是否安全,均无从知晓。笔者认为,郭兵案恰恰暴露了个人信息权保护的漏洞,也提醒公民及相关公权力主体应加强对这一权利的关注。

5. 人脸识别技术应用与公民权利保护的平衡

5.1. 人脸识别技术应用与公民权利保护平衡的困境

5.1.1. 立法方面

首先,在宪法层面,尽管宪法明确规定公民的人格尊严不受侵犯,并确立了对通信自由与通信秘密

的保护规范, 但我国目前针对个人生物识别信息的规定尚未统一, 且缺乏专门立法, 相关内容仅分散于部分法律法规及规范性文件中。

其次, 《中华人民共和国民法典》《个人信息保护法》等多部法律均涉及公民个人信息保护。目前我国尚未对公民个人生物识别信息进行细化分类, 相关立法部门应对人脸信息范畴等作出进一步规定。

依上可见, 我国对人脸识别技术应用的信息保护虽已实现有法可依, 但现有立法仍存在完善空间: 一方面, 相关立法内容较为碎片化, 条文规定抽象, 专门性与针对性不足, 尤其在人脸识别信息的收集、处理、使用等全流程规范方面, 立法尚待细化; 另一方面, 法律法规之间衔接性较弱, 有效的救济途径不够健全, 导致法律救济体系的发展滞后于信息技术的迭代。

5.1.2. 司法方面

首先, 司法救济程序的诉讼周期较长。以郭兵一案为例, 根据媒体公开信息, 该案于 2019 年 10 月由法院受理起诉, 2020 年 11 月基层法院作出一审判决, 2020 年 12 月中级人民法院受理上诉, 直至 2021 年 4 月 9 日才作出终审判决——两个程序合计用时近 17 个月。案件的诉讼周期太过于漫长, 这对于当事人而言, 维权成本太高, 难度也随之增加。

其次, 受侵权人在人脸信息案件中面临举证困境。人脸识别技术流程复杂, 其信息收集、处理与使用环节涉及的潜在侵权主体具有不确定性, 各环节均可能发生侵权行为, 导致公民在诉讼时难以明确被告身份。此外, 原告多为普通公民, 对信息技术处理手段的了解和掌握相对有限, 这使得维权者在证据收集上面临重重困难。更重要的是, 一些非法收集人脸信息的主体常通过隐蔽方式获取数据, 被收集者往往对此毫不知情, 人脸信息在不知不觉中被盗取, 信息主体既无法察觉也难以取证。

最后, 部分法院审理人脸信息侵权案件的能力有待提升。在我国民事审判中, 法官是案件事实认定的核心角色, 这要求审理人脸信息侵权案件的法官具备相应的专业素养。此类案件的审理焦点通常集中于梳理侵权行为、判断权利侵害的结果与程度、分析行为与损害结果的因果关系等方面, 而要准确完成这些工作, 法官必须具备一定的专业技术知识, 才能作出更贴合客观实际的事实认定与价值判断。然而现实情况是, 我国受理此类案件最多的是基层人民法院, 而基层法官的知识背景往往以法律为主, 较为单一, 这导致他们在审理这类案件时可能力不从心。

5.2. 人脸识别技术应用与公民权利保护平衡的完善路径

5.2.1. 制定专门的个人生物识别信息保护法

如前文所述, 我国人脸信息保护立法存在碎片化问题, 相关条文规定较为抽象, 专门性与针对性不足。为此, 立法层面需对人脸信息等敏感个人生物识别信息的法律概念进行界定与分类, 并细化数据整合处理等环节的规范要求; 同时应区分公民姓名、住址等一般个人信息与人脸数据等特殊个人信息, 针对人脸识别技术制定特殊规则, 明确其使用主体及相关权利, 以及人脸数据控制方、处理者与监管机构的义务和责任。

5.2.2. 设立专门的监管部门监督各方对人脸识别技术的使用

公安部、网信办等部门均应对人脸识别技术的规范与保护承担相应责任。然而, 当前各部门仅针对各自业务领域开展监管, 尚未形成对人脸识别技术的统一专项管制。基于此, 可设立专门且独立的行政监管机构, 负责公民个人信息及个人生物识别信息的保护工作, 明确其监管职责, 对公私主体使用人脸识别技术过程中的各类技术行为实施严格的行政监管。

5.2.3. 确立特殊证明责任分配制度, 完善电子证据制度

在人脸信息侵权案件中, 由于争议焦点常涉及复杂的技术原理与运算逻辑, 各方主体在信息技术能

力及取证举证能力上往往存在显著差距。对此, 可通过举证责任倒置来平衡这种能力差异[6]。但并非所有此类案件都固定适用这一规则, 而应根据具体案情区别处理: 若案件涉及公权力主体, 公民在证据收集等方面显然与公权力主体存在巨大悬殊, 此时应适用举证责任倒置; 若双方均非公权力主体, 则需综合评估主体间的能力差距, 将举证责任分配给更具举证能力的一方。

当前技术迭代迅猛, 司法实践亦需与时俱进。人脸信息侵权案件的证据多以电子数据形式存在, 其收集成本高、技术要求复杂。为破解取证难题, 可考虑从数据平台方切入, 借助平台网络数据存储后台的侵权行为数据备份进行证据收集。

6. 结语

在大数据时代, 人脸识别技术已广泛应用于社会生活与工作的各个领域。然而, 人脸信息具有唯一性、敏感性和易受侵害性等特征, 一旦被非法利用, 将对公民权利造成重大影响。因此, 有必要在深入了解人脸识别技术原理的基础上, 分析技术发展与公共利益、公民私权之间的关系, 进而研究我国人脸识别技术规范的法治路径, 探索实现技术规范、公民人脸数据保护与国家公共安全、社会经济发展之间平衡的法治优化方案。

参考文献

- [1] 王立志, 刘汴鹤. 我国个人生物识别信息刑法保护的理念偏差与纠偏完善[J]. 南开学报(哲学社会科学版), 2026(2): 152-166.
- [2] 王业亮. 人脸识别技术法律规制的国际比较与场景化重构[J]. 行政法学研究, 2026(4): 82-94.
- [3] 刘汴鹤. 生物识别信息安全风险的多维度治理研究[J]. 科学决策, 2025(8): 161-178.
- [4] 劳东燕. “人脸识别第一案”判决的法理分析[J]. 环球法律评论, 2022, 44(1): 146-161.
- [5] 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.
- [6] 倪楠, 王敏. 人脸识别技术中个人信息保护的法律规制[J]. 人文杂志, 2022(2): 121-131.