Dispute Settlement 争议解决, 2025, 11(7), 87-95
Published Online July 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.117218

Hans汉斯

人脸识别技术在高校应用的法律风险与规制

李冰清

西南民族大学法学院，四川 成都

收稿日期：2025年6月4日；录用日期：2025年7月4日；发布日期：2025年7月11日

摘　要

人脸识别作为一种新型技术，在推动“智慧校园”建设中，发挥了诸多优势。然而，新技术的应用本是提升学校管理水平和维护学生安全，但其在采集和应用阶段暴露出学生合法权益存在被侵害风险、“告知－同意”规则被架空、缺乏对禁止适用场景的明确规定等问题。对此，面对新技术带来的冲击，有必要予以法治回应。针对当前我国高校实际情况，提出相关规制路径：健全人脸信息安全保护机制；增强“告知－同意”规则的有效性；设置禁止适用场景。探究高校使用人脸识别技术的法律问题，不仅保障学生个人权利，也有助于增强高校管理方式的合规性。从而，在法律和技术双重推动下，使校园管理场景下的人脸识别技术更加符合法治化的要求。

关键词

人脸识别，智慧校园，告知同意

Legal Problems and Regulations of Face Recognition Application in Universities

Bingqing Li

Law School, Southwest Minzu University, Chengdu Sichuan

Received: Jun. 4th, 2025; accepted: Jul. 4th, 2025; published: Jul. 11th, 2025

Abstract

As a new technology, facial recognition has played many advantages in promoting the construction of “smart campuses”. However, although the application of new technologies is supposed to enhance the management level of schools and maintain the safety of students, problems such as the risk of infringement of students’ legitimate rights and interests, the “notice-consent” rule being undermined, and the lack of clear regulations on prohibited application scenarios have emerged in the collection and application stages. In response to the impact brought by new technologies, it is

文章引用: 李冰清. 人脸识别技术在高校应用的法律风险与规制[J]. 争议解决, 2025, 11(7): 87-95.
DOI: 10.12677/ds.2025.117218

necessary to provide a legal response. In light of the current situation of universities in China, relevant regulatory paths are proposed: improving the mechanism for protecting the security of facial information; enhancing the effectiveness of the notice-consent rule; setting up prohibited application scenarios. Exploring the legal issues of universities' use of facial recognition technology not only protects students' personal rights but also helps to enhance the compliance of university management methods. Thus, under the dual promotion of law and technology, facial recognition technology in campus management scenarios will better meet the requirements of the rule of law.

Keywords

Face Recognition, Smart Campus, Informed Consent

1. 引言

随着信息技术的飞速发展，大数据、深度学习以及人工智能的蓬勃发展，人脸识别技术已经被广泛地运用到了各个领域，从个人设备上的刷脸解锁到刷脸支付，应有尽有。目前许多大学已经将人脸识别技术应用于学生的入学登记，使学生能够快速、方便地完成入学登记；为了方便学校的考勤，一些学校在课堂上设置了面部识别系统，可以检测到学生在课堂上玩手机、吃饭等行为；与此同时，越来越多的高校都已经安装了人脸识别闸机，学生们可以通过刷脸来进出宿舍、校门，甚至是在校内消费等。通过使用大数据和人脸识别技术，高校可以对校内人员的行为数据进行分析并对其进行建模，从而为学校对学生的安全管理、教学分析等提供基础数据支持。人脸识别技术的应用的确为学校的管理工作提供了许多方便和保障，但与此同时，人脸识别的应用存在诸多法律问题，如何确保信息主体信息安全，亟需进一步讨论。本文将聚焦于人脸识别技术在高校采集、存储、使用过程中可能引发的法律风险，并提出相关的应对策略。

2. 高校人脸识别应用概述

(一) 人脸识别技术概况

早在 19 世纪末至 20 世纪初，英国学者 Galton 便在《Nature》期刊上相继发表了两篇探讨面部特征识别的研究论文，然而这些文献均未涉及自动人脸识别(AFR)这一技术概念。直至 1965 年，Bledsoe 与 Chan 在 Panoramic Research Inc 机构发布的技术报告中，才首次系统阐述了 AFR 技术，这标志着该领域首篇具有学术价值的研究成果问世。从技术发展历程来看，人脸识别研究已历经半个多世纪的演进，然而该技术在我国各领域的实际应用推广，则是近年才逐步实现的重要突破。而目前国内围绕人脸识别信息的法律问题，主要聚焦于人脸识别信息的立法保护，较少讨论人脸识别信息收集的规则以及人脸识别信息合理使用问题。

人脸识别是利用面部特征信息进行身份认证的生物识别技术，其原理是通过对人脸特征信息进行深入分析和比较，以达到准确识别的目的。与之前的身份认证软件和传统的生物特征识别技术(如指纹、虹膜识别等)相比，人脸识别无需接触、采集简便、交互性好、特征稳定、高效快捷等众多优点，并被公认为是维护公共安全、信息安全、金融安全的富有成效的有潜力的工具[1]。目前，人脸识别技术已成为安保、金融、公共场所和司法系统中不可或缺的重要工具。人脸识别主要包括三类基本方式：一是“一对

一”的识别方式，如：电子支付，企业打卡，地铁进站等；第二类是“一对多”或“多对多”的识别方式，其重点在于监视、跟踪和识别某个特殊的群体；第三类为监视与侦测模型，如对公共场所的人流进行监视，其首要目标并不在于识别，而在于监视[2]。

本质上，人脸识别是以大数据为基础，算法为核心。人脸识别的核心逻辑系统分为三个环节，一是人脸图像的采集与预处理。该阶段需要获取大量的人脸信息样本，常用的采集方式包括批量导入和实时抓取两种模式。采集完成后需对原始图像实施预处理，包括灰度调整、滤波等操作，构建标准化的大规模人脸信息数据库。二是目标人脸的精准定位与特征捕获。该环节要求在特定位置安装人脸采集设备，通过人脸检测算法对目标对象进行定位，准确识别人脸区域并去除背景干扰，确保采集数据的准确性。三是跨模态人脸数据的深度比对与身份识别。在这一过程中需对检测到的人脸图像进行面部特征提取，再与人脸信息数据库中的特征模版进行相似性计算和筛选，最终完成身份识别[3]。

(二) 高校人脸识别的应用场景

早在2014年，西安交通大学、西南交通大学等高校相继引进了人脸识别技术，并将其应用于校内考勤、迎新等场景。此后至2018年，使用人脸识别技术的高校在逐年递增，一些高校为打造智慧校园也纷纷引进人脸识别技术，将其广泛应用于校门出入、宿舍门禁管理、课堂考勤监测以及图书借阅验证等多个场景，以提高校园安全保卫及教学工作的效率，为现代化校园管理提供有效的技术支撑。

人脸识别技术在高校的具体应用场景可分为门禁类、教学行政管理类、校园安全管理类和校园生活支付类四类。门禁类：通常是指高校校门、宿舍和图书馆等进出场所，教师和学生通过刷脸进出闸机，利用人脸识别技术进行身份识别、验证，防止非法人员进入学校。教学行政管理类：考勤打卡和教师授课等方式是应用最为广泛的。其中，考勤管理系统在教职工刷脸考勤或学生上课刷脸出勤监测中发挥着重要作用，由于人脸具有不可替代性，通过非接触式身份验证显著提升了考勤数据的精确度，考勤打卡可以为学校提供实时有效的学生基本情况及学习状态的监控。同时，随着智能教室的广泛普及，一些高校已经实现了部分教室的智能化建设，配备了一套完备的软硬件设备，教职工只需进行刷脸操作即可轻松启动设备。校园安全管理类：此功能主要是针对由校园摄像装备所记录的电子资料，通过电子数据中对人脸信息的处理，可以有效地进行批量面部信息的识别。校园生活支付类：一些高校已经实现了校内刷脸支付，并被广泛应用于学生食堂、澡堂、校园超市等多种场景下，这一便捷的支付方式也为全校师生带来了极大的便利。

3. 高校人脸识别应用的法律问题

(一) 学生合法权益存在被侵害风险

1、存在学生隐私权被侵害的风险

《民法典》第1032条[1]明确将隐私权纳入人格权保护范畴，确立了隐私保护的法律边界，为个人信息安全提供了基本的法律保障。高校运用人脸识别技术进行行政管理时，学生进出校门、宿舍等行踪信息将被实时捕获并储存于数据库之中。在课堂教学中，甚至通过课堂视频监控捕获学生的面部微表情，以此评估其课堂专注度。疫情期间，高校校门都采用了人脸识别技术来管理学生的出入，食堂也采用了人脸识别来检查员工是否佩戴着口罩。由于每个人的人脸信息具有唯一性，因此，通过对人脸特征的比较，可以获取他们的基本信息，这也导致了许多学生的个人信息被泄露。基于人脸识别系统的应用，学校教师得以实时掌握学生进出校园、宿舍的情况，同时还能通过教室的监控设备收集到学生的上课表现等信息。这的确存在着侵犯学生隐私和个人信息安全的风险。

[1]《中华人民共和国民法典》第一千零三十二条：“自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”

2、存在学生人身权被侵害的风险

人脸信息一旦被收集，很有可能会被长期保存，从而增加了不可控的风险。例如，在疫情防控期间，部分高校为加强校园管理，广泛采集了学生的人脸信息。然而，这些数据的存储期限、使用范围及管理规范往往缺乏明确说明，学生亦未获得充分告知。当前社会普遍存在的个人信息滥用问题，如频繁收到的垃圾短信和骚扰电话，表明互联网平台的用户数据并未得到有效保护，反而可能被非法交易或不当利用。若高校存储的人脸数据因安全漏洞遭到泄露，同样可能被不法分子用于恶意目的。由于人脸信息具有生物识别特性，能够直接关联到特定个体，因此其法律属性属于敏感个人信息。某些图像处理软件可能通过 AI 技术丑化或篡改他人肖像，构成对肖像权的直接侵害。更为严重的是，深度伪造等技术的滥用，例如将他人面部信息合成至不雅视频中，不仅侵犯肖像权，还会导致受害者社会评价受损，进而构成名誉权侵害。相较于普通个人信息(如手机号码)，人脸信息的泄露可能引发更严重的法律风险和社会危害，亟需加强监管与保护措施。

3、存在财产权被侵害的风险

面部信息作为一种生物特征信息，具有高度的敏感性，一旦被泄露或非法利用，将会对人们的财产权益造成严重的损害，甚至可能对人们的精神造成不可逆转的影响。目前大多数的大学都将人脸识别系统交给了厂商，并对其进行数据的采集和处理，学校内部也会有信息团队对其进行跟踪。在使用人脸识别技术的过程中，在采集后存储到的数据是非常巨大的。在数据的储存和传输过程中，若因技术或其他原因导致信息泄露或被非法截取，将会带来财产权益的潜在风险：1) 在当今这个信息技术高度发展的时代，很多个人银行软件和支付宝软件都可以使用面部识别来实现网上交易，如果不法分子对用户的身份进行了破解，并取消了对用户支付信息的限制，那么就有可能造成不正当的支付行为，从而造成财产的损害，甚至还会造成精神上的伤害。2) 作为重要的生物识别数据，人脸信息具有不可更改的特殊属性，其泄露可能导致严重的身份安全隐患。在个人信息被泄漏之后可能被不正当地利用，甚至被用在某些非法活动中，从而造成个人的权利被侵害。尤其是近年来，诸如电信诈骗、网络诈骗等违法犯罪行为变得更加严重[4]，因此，更应强化对人脸信息的保护力度。

(二) “告知–同意”规则被架空

个人信息处理的正当性依据在于取得信息主体的“告知–同意”，我国《个人信息保护法》第 14 条[2]作出明确规定，“告知–同意”规则的有效要件应当包括自由、具体、知情、明确以及形式等五个方面。在进行信息采集之前，高校和建设厂商必须获得学生的明确同意，同时，还须详细说明所采集的目的、使用范围、保存方式以及存储时间等方面的细节[5]。这就意味着，信息主体接受“告知–同意”这一规则，须在充分了解授权他人使用个人信息的目的和风险的前提下，每个人都有权以其充分的理性和主动性自由选择是否同意。高校相较于学生、教师等人拥有显著的主导地位，因此，高校在人脸识别信息采集的过程中，师生群体往往处于被动接受的地位。信息采集常常使得“告知–同意”这一核心原则的实际效力往往被严重削弱，常常以各种方式被架空[6]。

1、不明后果的同意

在网络环境下，被采集信息的主体往往面临着不明后果的“同意”、“告知”不充分和难以理解的情形。网络隐私协议通常具有内容冗长、语义模糊、授权目的模糊等问题，信息主体难以快速获取到有效信息。一项调查显示，美国人每年花 201 小时读各种冗长而内容复杂的个人信息保护条款，各种时间成本、能力以及信息不对称使丹尼尔·斯洛夫教授感叹道：“人们不会读隐私政策，即使阅读了，他们也不

[2]《中华人民共和国个人信息保护法》第十四条：“基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。”

理解；就算阅读并理解了，他们也缺乏充足的背景知识来做知情后的选择”[7]。而高校的人脸信息采集对象大多都是学生，以他们浅薄的阅历难以认识到人脸识别的后果和风险。

疫情期间，高校为限制校园人员流动普遍设置了“刷脸”进出闸机。而部分高校采用微信群或内部官网通知的方式，或者通过基层管理服务人员口头告知的方式，引入了刷脸机制。由于其无法提供明确的信息，这种通知方式注定无法全面呈现选择刷脸所带来的不良影响。即便被问及刷脸的风险，这些负责传达的基层管理服务者也并未提供一个全面而明确的回答。

2、别无选择的同意

在线上场景，据研究表明，在面对网络服务提供商时，学生群体作为数据主体往往无法真正行使个人信息自主权。他们在使用各类校园软件、APP (如企业微信、步道乐跑)时，必须提供个人信息，否则将无法使用其产品或服务[8]。在人脸识别领域，这种情形仍然存在。实践中，高校与 APP 运营商在用户协议中采用“要么同意要么不得使用”的强制性规定，实质剥夺了学生的选择自由权。例如，疫情防控期间，众多高校在研究生招生复试环节普遍采用了远程考核方式，考生被要求接受人脸识别验证，缺乏替代性的身份核验方案；如果拒绝进行人脸验证，就要丧失参与复试选拔的机会。这种缺乏协商余地的强制性要求，实质上构成了对个人信息自决权的限制。

随着时代的发展，越来越多的公共场所开始采用人脸识别技术，并将其视为唯一的身份验证方式，几乎每个人都在被动接受着人脸识别技术。在学校里，人脸识别也是如此。尽管学生内心或许并不情愿，但为了进入校园，他们不得不接受人脸信息的录入，这也是许多高校进入校园的必要条件。在新生入学时，许多高校都要求进行面部信息的采集，而“刷脸迎新”则成为了当时备受瞩目的话题。即使新生或许会有疑虑，但他们仍不得不顺从学校的安排，否则只能在独木桥上再次迎接高考的挑战。

(三) 缺乏对禁止适用场景的明确规定

张新宝、葛鑫学者认为，可以将人脸识别技术的适用领域进行二分，即公共安全适用场景和非公共安全适用场景，在此划分基础上充分结合人脸识别技术在不同场景中的适用目的和适用功能，对各场景实施精细化的利益衡量[9]。在高校应用人脸识别技术的过程中，“缺乏对禁止适用场景的明确规定”已成为当前法律规制体系中的显著缺陷。

从立法层面来看，虽然我国《个人信息保护法》确立了个人信息处理的基本原则，但针对高校这一特殊应用场景的禁止性规定却付之阙如。现行法律仅对公共场所安装图像采集设备作出原则性要求，却未能充分考虑教室、宿舍、心理咨询室等教育场所的特殊性，导致技术应用缺乏明确的禁止边界。例如，《民法典》第 1032 条虽然规定了隐私权保护，但未具体明确禁止在宿舍内部、卫生间等私密空间部署人脸识别设备，这使得部分高校得以“安全管理”之名，在宿舍走廊等准私密区域安装监控系统，实质上形成了对学生日常活动的持续性监控。

从实践层面来看，由于缺乏明确的禁止性规定，高校人脸识别技术的应用呈现出明显的泛化趋势。部分高校在教室部署具有“情绪识别”“专注度分析”功能的系统，其宣称的“提升教学质量”目的与设备的深度监控能力明显不成比例[10]。更值得警惕的是，某些高校将人脸识别与行为分析、轨迹追踪等技术叠加使用，构建起全方位的监控网络，这种技术聚合产生的监控效应远超单一技术，却因缺乏明确的组合应用禁止条款而处于监管真空。这种技术应用的泛化不仅违背了比例原则和最小必要原则，更可能异化为压制性的监控工具。

从权利保障角度来看，禁止性规定的缺失对特殊群体的权益保护尤为不利。高校中存在未成年人、留学生等特殊群体，《未成年人保护法》虽然要求处理未成年人信息需取得监护人同意，但未明确禁止在未成年人集中的教学场所使用人脸识别技术。实践中，部分高校在国际学院、留学生公寓等场所无差别部署人脸识别系统，不仅忽视了对特殊群体的差别化保护，更可能引发数据跨境流动的安全风险。此

外，现行规范未禁止将人脸识别数据用于学生评优评奖、贫困生认定等涉及重大权益的决策系统，这种技术化评判可能加剧算法歧视，严重违背教育公平原则。

从制度建构的深层次来看，禁止性规定的缺失导致高校人脸识别应用缺乏统一的负面清单制度。相较于金融、医疗等领域已经建立的场景化规制体系，教育领域的人脸识别应用仍处于规范真空状态。利用人脸识别技术分析学生课堂情绪状态、预测学业表现等行为，既超出《个人信息保护法》定义的“最小必要”范围，又违背“以学生为本”的教育理念，却因缺乏明确禁止规定而被某些高校冠以“教育创新”之名加以推行。这种规制缺失不仅使技术应用容易异化为监控工具，更可能对师生关系、校园文化产生深远的负面影响。

综上所述，高校人脸识别技术应用中“禁止适用场景规定缺失”的问题，本质上是由于未能基于比例原则和最小必要原则建立系统化的负面清单制度。这一立法空白不仅导致技术应用缺乏明确边界，更使得教育场景中的特殊隐私需求和伦理考量被严重忽视。要解决这一问题，亟需在制度层面构建层次分明、覆盖全面的禁止适用场景规则体系，为人脸识别技术在高校的合理应用划定清晰的法律红线。

4. 高校人脸识别应用的法律规制

今年 3 月，国家互联网信息办公室和公安部联合发布《人脸识别技术应用安全管理办法》(下称《办法》)，明确了应用人脸识别技术处理人脸信息的基本要求和处理规则、人脸识别技术应用安全规范、监督管理职责等内容。该《办法》的出台对人脸识别技术的风险治理是一大进步。

(一) 健全人脸信息安全保护机制

当前，大部分高校都把人脸识别系统的安装、采集、处理等工作交给了厂商，学校内部也有信息团队负责。高校应用人脸识别技术的过程中，若在采集、存储、使用等环节存在技术或者其他因素，可能会导致人脸信息的泄露或被非法截获，甚至造成难以估量的后果，所以高校应当对利用人脸信息的各环节予以健全和完善。

第一，限制人脸信息采集、使用的范围和目的[11]。《办法》第 4 条规定，应用人脸识别技术处理人脸信息，应当有特定的目的和充分的必要性，选择对个人权益影响最小的方式，并实施严格保护措施。高校采集人脸信息须遵循最小必要原则[12]，即高校对于人脸识别技术的应用必须严格限制在最小必要的校园管理范围内进行，在非必要的情况下，尽可能不使用该技术，以保证学生、教职工等主体个人信息安全。

现行采集人脸信息是为了维护校园安全、疫情防控、考勤打卡、监控等，对于上述目的都应重新审视。1) 用于维护校园安全。在用于身份认证的场景，对身份的认证存在可替代措施，例如登记身份证、准考证、校园卡、校园企业微信等。此外，高校在使用人脸数据时，可采取隐匿化技术以加强隐私保护。作为具有高度敏感性的生物识别数据，人脸信息包含多维度的个人特征，而实际应用场景往往仅需验证特定维度的信息，因此在必要的时候应进行隐匿化处理。在校园或宿舍进出口进行安装刷脸门禁设备时，确保仅显示身份验证所必需的最小化信息。以北京大学为例，其早期门禁系统在识别过程中会同步显示使用者的姓名、学号等敏感信息，经优化后已取消此类信息的实时展示，这一改进显著提升了个人信息保护水平。2) 用于疫情防控。在疫情防控期间的非正常状态下，为了不影响学校学生和教职工的身体健康，若不配合高校的采集活动，基本上无法开展校园活动，因此，入校进行身份验证，甚至是限制一些敏感信息权益、校门限制人员流动，都是非常有必要的。必须考虑的是，疫情结束后此时已缺失必要性。高校信息部门由于疫情防控而设置的刷脸设备、带有识别功能的摄像头和手机 APP 应该逐一下架，已录入的人脸信息也应随之删除。3) 用于考勤打卡。课堂要求学生“刷脸”来签到方式并不具有必要性，针对教学楼、实验室及体育场等教学区域，任课教师可选用传统点名或数字化签到等替代性考勤方式。4)

用于监控。高校为了维护校园公共安全，在校内安装用于防止学生打架斗殴的监控装置，目的正当且安装确有必要；若用于观察学生的出勤率和学习状态安装于教室的监控装置，并不是出于对校园公共安全的维护，可以其他管理方式代替。

第二，人脸信息的存储应尽到妥善保管的义务。重要人脸信息的处理者应当明确人脸信息安全主管人员和存储管理团队，落实人脸信息安全保护职责。近些年来，高校信息泄露事件频繁发生，甚至有可能导致学生违规申请信用卡或虚开工资等，因此在存储过程中必须高度重视其潜在的风险。在完成人脸信息数据的采集后，采集主体必须严格履行其所承诺的使用范围，确保人脸数据的处理行为既符合法律规定，又遵循行业制定的生物识别信息管理标准。一旦主体泄露个人隐私信息，将依据双方约定或相关法律条文承担相应的法律责任，情节严重的，相关责任主体还可能因触犯刑法而受到刑事处罚。

第三，落实保障删除权之制度与技术实现。我国《民法典》第 1037 条第 2 款、《个人信息保护法》第 47 条[3]均明确规定了信息主体享有删除权。当信息处理者违规处理用户的数据信息时，基于当事人之间信赖关系的破裂，为更好保护人脸信息的安全，即便协议未作明确约定，信息处理者也应主动履行数据删除义务。由于人脸信息具有高度敏感性和不可替代性，其一旦泄露并被不法利用将会造成不可估量的后果，因此，在特定情形下相关责任主体应当及时删除或销毁该信息，从根本上消除因数据留存可能导致的潜在安全风险。在具体实践中，高校对于毕业年级学生及退休、调任、辞任教职工在校期间收集的人脸信息数据，在其离校之后就不应当作其他的用途，而应在高校人脸信息库中将该人脸信息彻底删除。

(二) 增强“告知–同意”规则的有效性

第一，坚持以人为本，在进行人脸信息的采集、使用之前，必须严格遵守“告知–同意”规则，全面履行告知义务。根据《办法》第 6 条[4]的规定，处理敏感个人信息应当取得个人的单独同意。从法律性质上看，人脸信息属于人格利益的范畴，任何未经授权获取人脸信息的行为均构成对个人权利的侵害。“人脸”的变化性决定了人脸信息的特征，同时也增加了人脸识别技术的实施难度，故人脸信息在采集后能否被安全合理地使用，是采集主体应当依照法律法规对被采集人做出承诺、使被采集人知晓的义务之举。在采集个人信息前，采集主体应当严格履行法定告知义务，具体包括：采集信息的内容、范围、目的以及可能带来的风险，对于涉及责任限制的格式条款，采集主体必须进行重点提示和详细解释，避免采用任何形式的推定同意机制，如“默认同意”“默认授权”“告知不等于同意”，为规范双方权利义务关系，建议采集主体与信息主体通过书面协议的形式明确约定相关事项。对于已经部署运行的，及时通过协议修订或增补条款等方式弥补法律瑕疵。

高校作为行政机关在维护校园安全及师生信息安全方面有不可推卸的责任。在进行人脸信息采集前，高校应对被采集主体进行详细解释，其中包括采集的方式、范围、可能带来的风险，以及具体的责任承担方式，这样才能充分保证信息主体的知情权。当高校发布关于人脸识别信息采集的通知时，应该通过学校官网、学校微信公众号等公开平台来发布，并要求学院、班级负责人通知特定的人脸识别信息主体。同时加强对人脸识别技术相关法律法规知识的宣传与普及工作，从而提高师生对于这项技术的认识程度，确保他们能够全面、具体地了解采集情况。

[3]《个人信息保护法》第四十七条：“有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：（一）处理目的已实现、无法实现或者为实现处理目的不再必要；（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；（三）个人撤回同意；（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（五）法律、行政法规规定的其他情形。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。”

[4]《人脸识别技术应用安全管理办法》第六条：“基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。”

第二，人脸识别不能作为唯一的身份认证手段。《办法》明确规定个人拒绝采用面部特征识别方式，相关机构应当为其提供替代性的验证方案[5]。高校将人脸识别技术设定为唯一身份核验手段的做法，既不符合必要性原则，也难以针对人脸信息进行严格防护。高校在使用人脸识别技术时，学生抑或是教职工均有权拒绝“刷脸”。当他们拒绝“刷脸”时，高校应当提供其他替代性的认证方式，而非以拒绝人脸识别为由限制其正常使用校园设施或服务的权利[13]。在疫情期间，很多高校都采集到了学生人脸信息，清华大学仅刷紫荆码不刷脸的方式对维护师生个人信息权益更为有利。

人脸信息采集与存储环节可实施制度性规制，任何单一认证方式都不具有绝对的安全性，而双重或多重认证识别方式虽然代价高昂，却不失为提高安全概率的唯一途径。各种生物识别技术会在相当长的一段时间内共生并存，而目前的人脸识别技术无法达到人类期望的目的，人脸识别技术极易被不法分子破洞而身份造假。因此，在校学生、在任教师、后勤等其他需要频繁进出校园的人员可以选择通过其他方式进入校园、完成考勤打卡等，例如出示学生证、工作证等证明自己身份的证件，或者可以通过手机软件如企业微信或者校园一卡通扫码通过校园门禁以此代替刷脸入校。对于需要临时入校的人员可以选择出示临时入校证明，外来入校考试的考生可以出示准考证等有效证件。总而言之，拓宽人脸识别途径，通过多种生物特征识别技术的融合，进一步提升学生身份识别的整体安全性和识别率。

(三) 设定禁止适用场景

在高校推广应用人脸识别技术的过程中，设置禁止使用场景作为重要的规制手段，应当基于比例原则和最小必要原则，结合高校场景的特殊性进行系统性设计。该对策的实质是通过明确技术使用的负面清单，划定人脸识别技术不可逾越的红线，从而在源头上防范技术滥用引发的法律风险。具体而言，高校在部署人脸识别系统时，应当建立严格的场景准入机制，将以下几类场景明确纳入禁止使用范畴：

首先，涉及师生私密生活空间的场景应绝对禁止使用人脸识别技术。这包括但不限于学生宿舍内部、卫生间、浴室、更衣室等高度私密场所。在这些空间部署人脸识别设备，不仅可能侵犯《民法典》第1032条规定的隐私权，更可能构成对人格尊严的严重侵害[14]。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》第10条已明确将“在宾馆、商场等公共场所安装人脸识别设备”列为侵权行为，这一法理同样适用于高校的私密空间。其次，在教学管理领域，应当禁止将人脸识别技术用于非必要的监控目的。例如，通过人脸识别分析学生课堂抬头率、专注度等学习状态的做法，既缺乏教育管理的必要性，又可能违反《办法》第4条规定的目的限制原则[6]。更值得警惕的是，此类应用可能异化为“数字全景监狱”，对师生造成无形的心理压迫，与教育的人文关怀本质背道而驰。再次，在日常校园服务场景中，应当禁止强制使用人脸识别技术。如图书馆借阅、食堂消费、体育场馆出入等常规服务场景，必须保留校园卡、二维码等替代性验证方式。根据《个人信息保护法》第16条规定，个人信息处理者不得以个人不同意处理其个人信息为由拒绝提供产品或服务。高校作为特殊的公共服务机构，更应当遵循“技术非强制”原则，保障师生的选择权。此外，在特殊敏感场景下也应当设置使用禁令，如师生政治表达场所(如选举投票点、学术研讨会)、心理咨询场所、宗教活动场所等。在这些场景使用人脸识别技术，不仅可能触及宪法保障的基本权利，更可能产生寒蝉效应，抑制校园的思想自由和文化活力。

为确保禁止性规定的实效性，高校应当建立三层保障机制：其一，在技术采购环节将禁止场景写入合同条款；其二，组建由法学专家、教育专家、技术专家组成的伦理审查委员会，对拟应用场景进行必要性评估；其三，建立畅通的投诉举报渠道，鼓励师生对违规使用行为进行监督。唯有通过这样系统化

[5]《人脸识别技术应用安全管理办法》第十条：“个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式。”

[6]《人脸识别技术应用安全管理办法》第四条：“应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式，并实施严格保护措施。”

的禁止场景设置，才能在享受技术便利的同时，守护好高校这片育人的净土。

5. 结语

本文主要就高校人脸识别的法律风险与规制问题展开研究。在“智慧校园”的背景下，随着生物识别技术的飞速发展，人脸识别已经成为高校管理中不可或缺的工具之一，其被广泛应用于高校身份识别、教学行政管理、疫情防控、校园生活支付等领域，有效提升了学校管理水平，同时在保障学生安全、助力高校发展等方面扮演着至关重要的角色。不可否认，运用人脸识别技术对于提高工作效率具有至关重要的意义。然而，在该技术的应用过程中，不断涌现出新的难题和挑战，需要我们不断探索和创新。为了保障人脸识别信息应用的安全性，减少信息泄露的风险，必须在采集、存储和使用过程中实施严格的标准规范。只有通过前瞻性的规划和信息化的设计，才能充分发挥人脸识别技术在智慧校园建设中的独特作用。从而，在法律和技术双重推动下，使校园管理场景下的人脸识别技术更加符合法治化的要求。希望本文针对高校人脸识别应用的法律问题以及所提出的法律策略，可以为我国高校建设完整的人脸识别技术体系提供一个可行的方案。

参考文献

[1] 郭春镇. 数字人权时代人脸识别技术应用的治理[J]. 现代法学, 2020, 42(4): 19-36.
[2] 王鑫媛. 人脸识别技术应用的风险与法律规制[J]. 科技与法律, 2021(5): 93-101.
[3] 文铭, 刘博. 人脸识别技术应用中的法律规制研究[J]. 科技与法律, 2020(4): 9.
[4] 张莉莉. 人脸识别技术在治安管理中的应用及其规范路径[J]. 行政与法, 2022(3): 61-70.
[5] 石佳友, 刘思齐. 人脸识别技术中的个人信息保护——兼论动态同意模式的建构[J]. 财经法学, 2021(2): 60-78.
[6] 曾晨, 李汶龙. 人脸识别治理的进路完善: 从个人信息到社会公正[J]. 学术交流, 2024(10): 83-95.
[7] 王旭. 人脸识别准入规则的失灵风险与制度重构[J]. 大连海事大学学报(社会科学版), 2021, 20(6): 54-65.
[8] 林凌, 贺小石. 人脸识别的法律规制路径[J]. 法学杂志, 2020, 41(7): 68-75.
[9] 张新宝, 葛鑫. 人脸识别法律规制的利益衡量与制度构建[J]. 湖湘法学评论, 2021, 1(1): 36-51.
[10] 胡凌. 刷脸: 身份制度、个人信息与法律规制[J]. 法学家, 2021(2): 41-55+192.
[11] 陈姿君. 行政机关采集人脸信息活动的法治因应[J]. 行政法学研究, 2023(3): 153-164.
[12] 赵精武. 人脸识别技术应用的利益权衡与合法性认定[J]. 法律科学(西北政法大学学报), 2024, 42(1): 100-110.
[13] 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(5): 51-63.
[14] 王利明. 论《个人信息保护法》与《民法典》的适用关系[J]. 湖湘法学评论, 2021, 1(1): 25-35.