人脸识别技术应用的合法性边界：基于场景化分级审查的路径

杨博雅

山东理工大学，山东 淄博 255049

摘要：本论文探讨了人脸识别技术应用的合法性边界，重点分析了其在不同场景中的法律风险和治理挑战。论文从技术特性与应用场景的错位出发，探讨了人脸识别技术泛化应用带来的治理困境，结合《个人信息保护法》第 26 条进行三维透视的法律风险解构，揭示了技术发展与法律框架之间的适配问题。同时，基于场景化审查的思路，论文提出了分级审查路径，具体分析了安防、教育或办公、商业等不同场景下人脸识别技术的合法性边界，为人脸识别技术的规范应用提供法律上的合理框架和路径建议。

关键词：人脸识别技术；隐私权；场景化；分级审查

随着人脸识别技术的广泛应用，技术特性与场景适配的错位问题日益凸显，引发了隐私保护和法律合规的复杂困境。人脸识别技术作为生物特征识别的重要手段，其应用场景的泛化不仅带来了便利，也增加了隐私泄露和滥用的风险。基于《个人信息保护法》以及将于 2025 年 6 月 1 日实施的《人脸识别技术应用安全管理办法》，本文通过提出场景化分级审查机制对人脸识别技术的合法性边界进行细致划定，并结合“语境完整性理论”，为不同应用场景设计合适的审查标准和风险评估路径，以保障公民隐私权与技术应用的合规性。

1 人脸识别技术场景泛化应用引发的治理困境

随着人脸识别技术的成熟，人脸识别技术的应用场景在不断扩大，成为社会各行各业不可或缺的一部分。然而，如今人们对隐私保护问题的逐渐重视，如何平衡便利性和隐私保护将是未来发展的一个重要课题。

1.1 技术特性与场景适配的错位

随着科学技术和人工智能技术的不断完善和发展，人脸识别技术从公共安全到商业服务，几乎已被所有领域积极探索并利用。然而，这项技术的广泛应用也暴露出了其本身的局限性。

人脸识别技术不同于普通个人信息，其具有生物学上的唯一性和稳定性，相较于名字、身份证号等传统个人信息，人脸信息不可更改，因此其处理过程中的隐私风险远高于其他信息。人脸识别技术通过分析和比对一个人的面部特征，能够提取出一个独一无二的生物特征。每个人的面部信息是与生俱来的，并且在整个生命周期内都几乎不变，这使得人脸数据在个体识别中的唯一性远远超越了如名字、身份证号等传统信息。

1.2 基于《个人信息保护法》26 条的三维透视的法律风险解构

根据《个保法》第 26 条规定：“在公共场所安装图像采集、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；取得人单独同意的除外。”由此可见，我国《个保法》已经对人脸识别技术的应用提出了明确要求，指出在公共场所安装图

像采集、人身份识别设备应当遵守国家有关规定，并要求收集的个人图像、身份识别信息只能用于维护公共安全的目的[1]。然而，随着技术应用场景的泛化，这一规定面临着实际操作中的巨大法律风险。

1.2.1 目的限制原则的虚置化

目的限制原则要求个人信息的收集和处理应当明确并严格限定其用途。然而，技术中台化使得数据处理过程中的“目的漂移”现象愈加严重，一些安防数据虽然最初为公共安全目的而采集，但却被流向商业分析、用户行为预测等非安全领域，这种“目的漂移”现象严重违背了目的限制原则，并增加了数据滥用的风险。

GDPR（通用数据保护条例）作为全球最严格的数据保护法规之一，其中明确规定了个人数据的收集和处理应当遵循“目的限制原则”。在 2019 年，法国数据保护监管机构 CNIL 对 Google 提出处罚，理由是，在 GDPR 框架下 Google 未能充分告知用户其数据收集的所有目的，导致了目的漂移的风险[2]。

1.2.2 告知同意机制的失灵

告知同意是《个保法》中的重要机制，然而在实际应用中，这一机制的执行常常处于失灵状态。很多公共场所和企业并未充分告知用户其数据收集的目的与方式，且告知同意常常被形式化或隐性化。例如，在一些写字楼的闸机系统中，用户并未明确同意人脸信息的采集，而是通过物理场景的设置形成“默示同意”。这种方式存在潜在的法律风险，因为用户未明确同意数据采集和使用，可能违反了隐私保护相关的法律规定。例如，在许多司法管辖区，收集和处理生物识别信息如人脸数据要求数据主体明确知情同意。

1.2.3 单独同意要件的规避

根据《个保法》第 29 条规定，对于敏感个人信息的处理，必须获得用户的单独同意。然而，许多企业通过单一的、且用户无法自主选择的混合授权协议规避了这一要求，将人脸识别技术与其他服务捆绑，迫使用户在同意使用服务的同时也必须同意采集和使用人脸信息。事实上，现在大量平台或 APP 都是这样强制要求用户通过人脸验证登录，且无法提供密码登录等其他的替代方式，这种强制性、单一性的验证方式，不仅剥夺了用户选择的权利，并且违反了单独同意的原则。

以上问题无一不表明，如今人脸识别技术的应用必须从场景化角度出发，构建一套分级审查机制，根据不同的技术应用场景进行合理的合规性评估与风险管控。为解决人脸识别技术在不同场景中的合法性边界问题，Helen Nissenbaum 的“语境完整性理论”提供了重要的理论支持[4]。结合这一理论框架，我们可以对人脸识别技术的应用在不同场景进行分类审查，从而避免“一刀切”的机械应用模式带来的问题。

2 基于场景化审查分级审查的设想

随着《个保法》及相关政策的出台，确保技术合规不仅是法律要求，也是对公众信任和隐私权的尊重。从目的限制到告知义务的履行，再到特定群体的保护，每个环节都涉及个人信息的收集、使用与保护分析各领域的具体应用，探讨如何在技术进步与隐私保护之间找到平衡，并提出相应的法律和管理框架。

2.1 安防场景下人脸识别技术应用的合法性边界

人脸识别技术在安防领域的应用日益广泛，出于提升公共安全、及时处理突发事件、预防犯罪等目的，往往在大型公共场所如地铁、机场、商场等都会设有人脸识别装置。然而，在高频次、公众性强的场景中，如何确保人脸识别技术的合规性与合法性，成为亟需探讨的重要问题。根据《个保法》第 26 条，维护公共安全是个人信息处理的一项法定豁免情形，但如何合理界定该豁免情形的边界，仍然是当

前法治建设中的关键课题。

2.1.1 目的限制的穿透性审查

目的限制原则是隐私保护法律体系中的核心原则之一[5]。在安防场景中，对于人脸识别技术的应用，必须确保其使用目的与技术应用之间存在直接且必要的关联，任何针对公众进行的大规模人脸识别技术应用，应当清楚界定其具体目的，并证明该目的在保护公共安全方面具有高度的相关性。

以北京地铁为例，整个 2024 年度，北京地铁线网日均客运量为 986.36 万人次/日，作为一个人流密集且涉及公共安全的重要场所，人脸识别技术的引入可以有效提升安防水平和安防效率，尤其是在反恐、重大公共安全事件预警、以及快速定位失踪儿童等重要安防场景中。然而，这并不意味着随意进行大规模的人脸识别就是合理的、合法的。我们应当平衡好公共安全与个人隐私之间的关系，将人脸识别技术合理的应用于反恐重点人员筛查或失踪儿童识别等特定场景，而非全员监控。

2.1.2. 告知义务的履行标准

虽然《个保法》允许在某些情况下豁免单独同意的要求，但这并不意味着相关主体可以忽视对信息主体的基本的告知义务。根据《个保法》第 17 条规定，数据处理方应当在收集信息之前，明确告知信息主体其个人信息的处理方式和目的，并确保信息主体知悉其隐私权利的相关内容。

例如，在地铁入站口，数据方可以通过设置 LED 告知屏或在安检区域张贴清晰的告知声明，来告知乘客若进入特定区域，其面部信息就会被采集并用于相关公共安全的保障方案中。此外，服务站还可以提供纸质或电子说明文本，详细阐述数据的处理方式和目的及其合法性依据，这样不仅能够确保信息主体知情权得到保障，还能在出现数据处理争议时，提供明确的证据支持。

2.2 教育或办公场景下有限空间内的知情权保障

在教育和办公等相对开放的领域，隐私保护和合法性问题变得愈发严重。目前，一些高校已经采用人脸识别技术进行教室考勤，确保能够实时追踪学生的出席情况以及听课状态。然而，技术应用的普及并未平稳过渡，反而在一些高校内引发了较为复杂的法律争议。根据《人脸识别技术应用安全管理办法》（自 2025 年 6 月 1 日起施行，下面简称《办法》）第十三条规定：“任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。”因此，如何在此类应用场景中平衡技术发展与隐私保护，成为了亟待解决的问题。

2.2.1 必要性的动态评估

依据“语境完整性理论”，人脸识别技术的应用必须符合其所在场景的需求与规范，因此，审查框架首先应当对人脸识别技术在该场景应用的必要性进行评估[6]。尤其在教育场景这样的空间具有相对封闭的特征中的人脸识别系统，不能简单地将其应用于所有场所或所有时段，而是要根据不同场所不同时段的具体需求进行筛选使用，不能将人脸识别技术随意扩展至不必要的场所。

2.2.2 告知同意的复合模式

在知情同意方面，学校可以建立分层告知机制，确保学生的可以充分行使其知情权。例如，在基础的层面，学校可以通过“学生基本手册”或“学生基本准则”等学习手册进行概括性的告知，明确告知学校部署人脸识别系统的目的和用途，提醒学生及时关注个人信息保护问题[7]；从中层告知机制出发，在每学期开始时，学校可要求学生自愿签署相关知情同意书，详细列明人脸识别技术的应用范围及隐私保护措施，并充分考虑学生意见，考量学生需求；最后，在人脸识别设备的采集区域，学校应设置语音提示和可视化标识，提醒学生人脸识别设备正在采集个人信息，同时提供给学生

拒绝或退出的权利。这种分层告知机制的设立能够基本确保学生在不同层次上知情权的保障，并且学生能够在每个阶段作出相应的选择。

2.3 商业场景：落地“非唯一验证”原则

在低风险场景中使用人脸识别技术的合法性边界同样需要进行细致审查。尽管相较于安防等高风险场景，商业场景的潜在风险较低，但由于涉及个人隐私、消费行为以及企业的数据使用等合规问题，人脸识别技术应用界限问题仍然不容忽视。因此，为了确保人脸识别技术在商场系统以及类似商业场景中的合法应用，低风险场景的审查机制也需要通过细致的设计，确保对消费者的隐私进行了充分保护。

2.3.1 告知内容的精细化设计

在使用人脸识别技术前，商场应向顾客提供明确、透明的告知内容，应当明确告知顾客人脸信息的使用方式与范围，确保顾客了解其人脸数据在商场内部及特定服务范围内使用，不得被滥用或泄露给未经授权的第三方。同时应当建立知情同意机制，应当要求顾客对人脸识别的使用方式、目的以及风险进行明示同意，确保其自主选择是否参与该项服务。

同时要当告知消费者其能够随时要求注销其生物特征数据，并彻底删除相关记录商场应当提供简便的渠道，允许顾客随时删除其人脸数据，别不当保证数据的彻底删除，不应再被商场用于任何目的。

2.3.2 落地“非唯一验证”原则

根据《办法》第十条相关规定，当实现相同目的或达到相同业务需求时，如果存在其他非人脸识别的技术手段，可以不必仅依赖于人脸识别技术作为唯一的验证方式[8]。也就是说，人脸识别技术在多数场合并非唯一选择，如果有其他技术手段能够达到同样的验证效果，就应该考虑采用这些技术而非人脸识别技术。

同时《办法》第十一条指出，如果要应用人脸识别技术进行个人身份验证或辨识特定个人，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等已建立的渠道[9]。这条立法意在使用人脸识别时，国家鼓励优先使用一些官方和经过认证的公共服务系统，这样既可以确保身份验证过程的准确性和可信度，同时也能减少滥用和错误识别的风险。通过这些系统，可以更准确地比对和确认个人身份，增强安全性。

结语

随着人脸识别技术在不同场景中的应用日益广泛，相关法律法规不仅仅从数据保护的角度出发，还要考虑到不同应用场景的特殊性。因此，根据现实需求，应当构建一个场景化分级审查机制，根据人脸识别技术的应用场景不同，采取不同程度的审查和监管，确保在商业、公共安全等不同领域的技术应用中，既能够提高效率，又能够有效地控制风险。

通过这样的场景化分级审查机制，结合《人脸识别技术应用安全管理办法》的实施，既保障了技术的健康发展，又能切实维护公民的基本权利，确保技术的应用不会超越法律和伦理的界限。在社会发展日新月异的背景下，如何平衡技术进步与个人隐私保护、社会效益与风险管控，已经成为各国政府和技术公司共同面临的重要课题。只有在严格的法律框架和科学的监管机制下，人脸识别技术才能真正实现为社会提供便利的同时，保护好每个公民的隐私和基本权益。

参考文献

[1]郭帅.公共图书馆读者个人信息相关权利保护研究——以《个人信息保护法》为视角[J].图书馆研究与工作.2023（8）:55-58.

[2]陈纯柱,王唐艳.大数据时代精准广告投放中的隐私权保护研究[J].学术探索.2020

（4）:46-47.
[3]丁倩.个人信息保护中知情同意规则适用问题研究[D].兰州:甘肃政法大学,2023.
[4]李金霖.论纳税人涉税信息保护范围的界定——基于场景理论与风险管理[J].吉林工商学院学报.2023（5）:87-89.
[5]林巧巧.公共管理领域应用人脸识别的法律规制与路径完善[J].西部学刊.2025（6）:86-89.
[6]张恩典.人脸识别技术应用场景的法律规制研究[J].人权研究.2024（1）:66-68.
[7]范远芳.人脸识别技术在高校中的研究与应用[J].信息记录材料.2025（3）:20-24.
[8]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（1）:16-18.
[9]李玥.筑牢技术应用安全防线 守护公众“刷脸”尊严[N].人民邮电.2025-3-25（001）

作者简介：杨博雅（2003-），女，汉族，本科，研究方向：经济法，法理学。