中国人工智能产业发展联盟
Artificial Intelligence Industry Alliance

人脸识别产业
法律治理研究报告

中国人工智能产业发展联盟安全治理委员会

编写单位

对外经济贸易大学数字经济与法律创新研究中心

中国信息通信研究院人工智能研究所

百度公司

前 言

人脸识别技术是对静态或视频中的人脸图像进行特征提取与分类，从而用于个人身份鉴别、验证与分析的当代信息技术。作为最广泛使用的生物识别技术之一，人脸识别技术以数据为体、以人工智能算法为用、以人类自身为对象，具有不可复制性、非接触性、可扩展性、快速性、多维性等优势，目前已与安防、金融、医疗、支付、教育、文娱等行业深度融合，不但推动链接大数据与人工智能的新型产业悄然成型，而且为我国数字经济与社会发展带来了新机遇。

在人脸识别产业突飞猛进的同时，人脸识别技术滥用的风险也在不断加剧，给个人、组织的合法权益保护以及国家安全带来巨大挑战。随着生成式人工智能时代的来临，人脸信息被广泛采集、分析，进而合成、生成人脸信息的崭新业态开始涌现。如何保护个人人脸信息、防范虚假信息、维护公共利益，成为人脸识别产业必须面对的重大议题。

面对种种挑战，我国《个人信息保护法》将人脸识别信息作为敏感个人信息予以严格保护，并在第 62 条进一步强调了人脸识别信息的特殊性，要求有关部门针对人脸识别制定专门的个人信息保护规则、标准。《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》重点规定了滥用人脸识别的侵权责任、合

同规则、诉讼程序。2023 年 8 月 8 日，国家互联网信息办公室（以下简称为“国家网信办”）公布《人脸识别技术应用安全管理规定（试行）》（征求意见稿）从更宏观的维度规定应用人脸识别技术的安全管理要求，采取了不同参与者、多种场景和细化技术标准相呼应的生态治理方法。

本研究报告立基于产业生态治理的思路，强调综合“人—技术—社会”三维视角，对人脸识别技术进行整全性治理。以产业生态参与各方的角色分工为切入，将主体类型化为：作为源头活水的技术提供者、作为中心枢纽的人脸产品/服务提供者、作为最后关卡的人脸识别产品/服务使用者；从数据安全、个人信息保护、算法治理、产品质量等各维度，细化不同主体的系统性义务与责任。此外，生成合成场景是人脸识别信息的重要应用场景之一，鉴于我国对深度合成算法、生成式人工智能等采取专门立法规制，研究报告特别关注了该场景下的人脸识别治理问题。

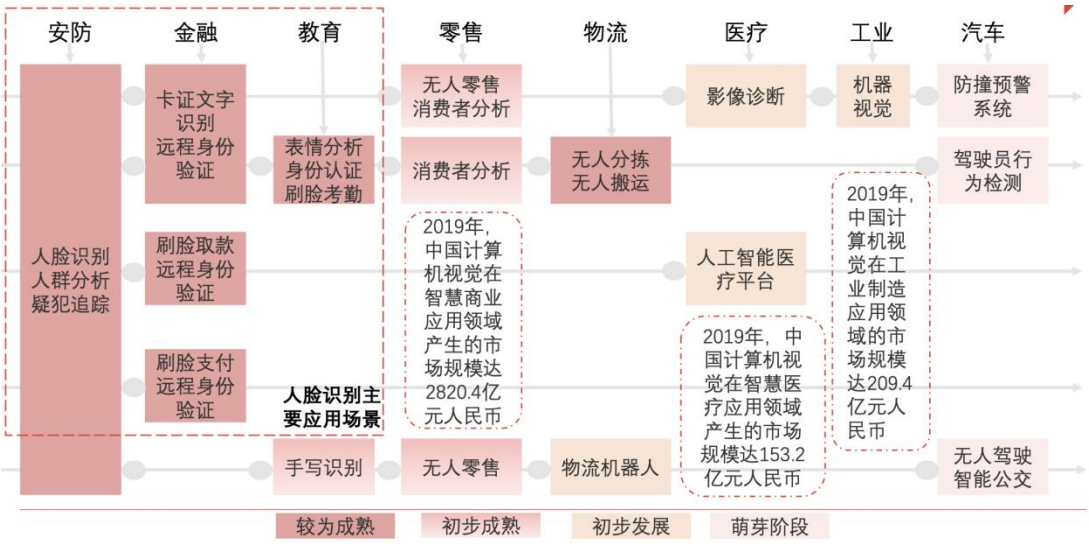
人脸识别产业的治理需要监管机构、司法机关、市场主体、行业组织、专家社群、社会公众的共同参与，本研究报告汇聚各方智慧，探索技术、法律、最佳实践、产业倡议多维一体的治理架构，希冀有裨于未来的立法、司法与执法，并为我国人脸识别产业的行稳致远贡献绵薄之力。

目 录

第一章　人脸识别产业的生态图谱

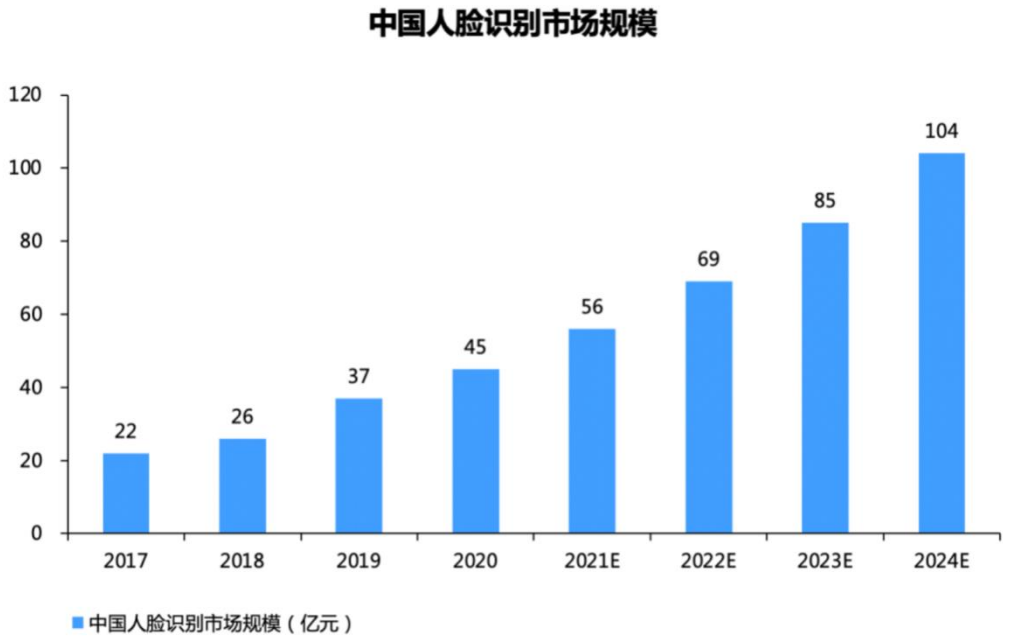
人脸识别（Face Recognition Technology, FRT）是一种基于个体脸部特征信息的生物识别技术，其将静态图像或视频图像中检测出来的人脸图像，同已知人脸图像进行比较，找到匹配的人脸，从而用于身份验证、识别和分析。人脸识别技术所具有的不可复制性、非接触性、可扩展性、快速性，使之成为多种生物识别技术中的明珠。2014 年以来，人脸识别技术在安防、金融、医疗、支付、教育、文娱等诸多领域中实现应用落地，广泛应用于设备解锁、身份验证、上班打卡、社区、考勤、乘车、购物等诸多场景，为数字经济社会发展和人们日常生活带来了新机遇。

图 1：人脸识别产业发展



数据显示，2021 年中国人脸识别市场规模为 56 亿元，预计到 2024 年突破 100 亿元；年均保持 23%增速。其中，人脸识别应用最多的是安防占 54%，其次是金融占 16%，此

后分别是娱乐 10%、医疗 7%、电商零售 6%、出行 3%、政务 2%、其他 2%。



资料来源：罗恩咨询, 行行查整理

作为数字经济的集合，人脸识别产业是一个复杂的生态系统。基于不同的参与主体，其包括了人脸识别技术生态、人脸识别产品/服务生态和人脸识别服务应用生态。

一、人脸识别技术生态

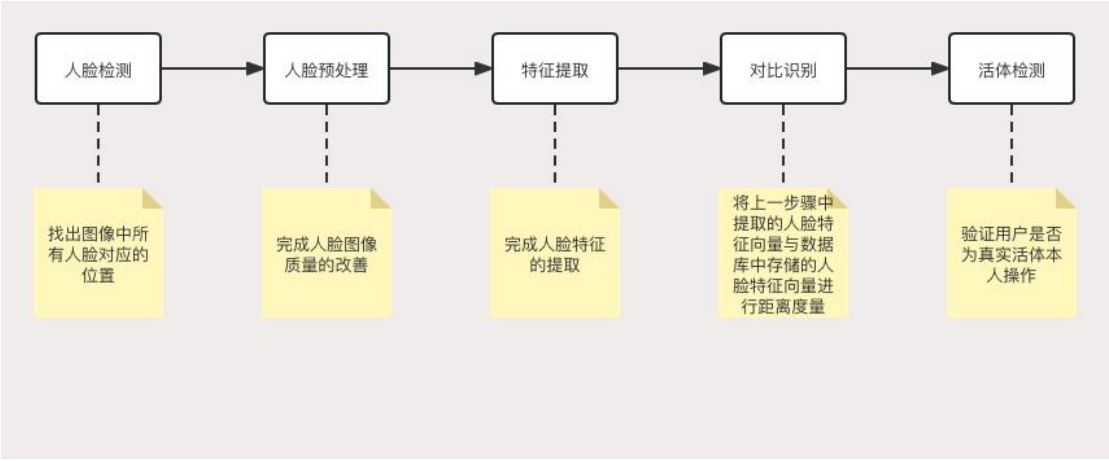
（一）技术提供者

人脸识别产业的技术提供者是提供包含**视频人脸识别、图片人脸识别和数据库对比检验**等技术的提供方。人脸识别技术主要包括**人脸检测、人脸预处理、特征提取、对比识别、活体检验**五大步骤，是推进服务应用的前提与关键[1]。目前人脸识别技术提供厂商主要包括**大型互联网企业**，如腾讯、阿

[1] 参见智慧芽&罗思咨询：《人脸识别行业研究报告》，2021 年。

里巴巴、百度、微软等，**电子设备厂商**，如华为、三星、苹果等，以及**其他科技公司**，如火山引擎、商汤科技、依图科技、旷视科技、格灵深瞳等。

人脸识别技术的五大步骤：**人脸检测**作为人脸识别算法的第一步，目标是找出图像中所有人脸对应的位置。**人脸预处理**模块主要完成人脸图像质量的改善，包括提高图像对比度、消除噪音等。**特征提取**模块完成人脸特征的提取，同时如何提取稳定和有效的特征是识别系统成败的关键[2]。**对比识别**模块根据特征提取模块输出的特征向量与数据库中存储的人脸特征向量进行距离度量，阈值内最小距离即识别为同一人[3]。**活体检测**主要是验证用户是否为真实活体本人操作，通过眨眼、张嘴、摇头或点头等动作进行判别[4]。



（二）产业实践

百度智能云依托领先的深度学习人工智能前沿技术框

[2] 吴玲：《人脸识别中的图像预处理技术》，载《中南论坛》2010 年第 4 期，第 116-118 页。
[3] 李怀宇等人：《基于人脸识别的智能立体车库控制系统设计》，载《工业控制计算机》2022 年第 7 期，第 1-3 页。
[4] 刘琴：《基于人脸识别的塔机身份管理系统》，载《建设机械技术与管理》2022 年第 5 期，第 69-71 页。

架和强大的端云计算能力，准确识别图片和视频流中的信息，提供高效、稳定的服务支持，助力各行业实现智能化升级和创新发展，同时采用多项安全技术，包括 AI 领域的算法技术保障、工程安全保障等，全方位守护数据安全。商汤科技依托于原创的计算机视觉技术以及深度学习底层算法平台，赋能于智能安防及其他领域，在多个垂直领域市场赋能多行业，为不同领域提供产品与解决方案，包括 SenseID，SenseUnity，SensePass，SenesKeeper，SenesNebula，SenesRadar 等。阿里巴巴利用三大核心技术，即生物特征自主感知和学习系统，结算意图识别和交易系统，以及目标检测与追踪系统，采用计算机视觉和传感器感应，并叠加了一些非配合生物识别技术，以降低误判率，广泛应用于政务、金融、直播、游戏、数字藏品、共享出行、教育、招聘、房地产等众多行业领域[5]。

（三）人脸识别技术价值

作为一项研究已有半世纪之久的技术，人脸识别技术是人脸识别技术应用不断发展的源头活水，也是保护人脸信息的技术核心。一方面，人脸识别技术以光学成像技术为基础，集合人工智能、机器识别、机器学习、模型理论、专家系统、视频图像处理等多种专业技术，其关键在于是否拥有尖端的核心算法，并使识别结果具有实用化的识别率和识别速度，

[5] 参见前注 1。

因此其不但是人工智能应用的主要领域之一，也是弱人工智能向强人工智能转化的环节。另一方面，在“基于设计的隐私保护”的架构下，人脸识别技术要求技术提供者从开发前期就应保障合规团队与开发、设计团队相互合作，在设计伊始即考量个人信息保护和隐私问题，将较能保护个人信息的做法列为预设机制，使之在信息系统中，得以受到系统的“自动”保护。

二、人脸识别产品/服务生态

（一）产品/服务提供者

产品/服务提供者根据具体应用场景的需要，提供**相应的软件服务、软硬件一体终端产品及服务等**，常见的人脸识别产品及服务包括离线 SDK、在线 API、人脸识别一体机等。例如，在**安防领域**，服务提供者按照需求研发提供楼宇、园区、地铁等场景下的门禁闸机；在**零售领域**，服务提供者提供支付场景下的 1 对 1 的人脸识别移动终端；在**金融领域**，服务提供者提供 API 调用接口，使用云端对比识别，在服务商完成数据处理。目前产品提供厂商与技术提供厂商重合度较高，它们包括阿里巴巴、百度、腾讯、火山引擎、商汤科技、海康威视、云从科技、华为、滴滴等。

（二）产业实践

人脸识别产品提供者主要为研发人工智能产品的科技公司，其提供的服务与产品形态也更加多样化，以满足各个

场景下的不同需求。

以百度为例，人脸识别技术灵活应用于金融、泛安防、安全生产等行业场景，满足身份验证和反欺诈、通行考勤、企业智能化治理等业务需求。传统制造企业厂区规模大、作业环境复杂、设备操作安全等级要求高，需对作业人员日常操作、穿戴安全进行及时监控及预警。同时，由于现场从业人员较多，员工管理面临排班复杂、流动性大。百度度目智能应用平台综合 AI+物联网+大数据分析能力,提供智能园区管理、能源生产安全管理、企业运营管理等服务，可广泛应用于企业园区及大型厂区，预警安全风险[6]。

在安防领域，科技公司提供人脸识别产品形态包括设备终端与系统性解决方案。例如，海康威视提供包括云计算、门禁、摄像机、软件平台、一体机等人脸识别终端设备以及系统性解决方案，致力于打造平安城市、平安乡镇、平安社区。格灵深瞳围绕视觉计算系统打造了囊括云到端到边缘侧的多形态产品，具体包括：高密度的视觉计算服务器、灵活部署的边缘服务器、嵌入式的智能前端视觉计算引擎以及云服务。依图科技主要研发智能安防产品，建立了十亿级的全球最大的人脸识别系统[7]。

在销售领域，科技公司提供人脸识别产品形态主要为智能化的解决方案。例如，腾讯提供腾讯云智能货柜解决方案。

[6] 参见前注 1。
[7] 参见前注 1。

该方案整合了先进的图像识别技术、微重力感应技术、RFID技术，可灵活自定义扫描策略，做到用户随意取货也能精准判断商品，在保障用户体验的同时有效控制货损率[8]。

在金融领域，科技公司提供人脸识别产品形态主要为人脸认证系统。例如，依图自主研发双目活体检测认证系统，为无卡取款业务用户提供身份核验功能，实现刷脸取款功能，现已应用于多家银行的 ATM 机[9]。

在直播等新兴产业，科技公司提供人脸识别产品形态主要为响应系统，辅助产业可靠发展。例如，火山引擎自主研发的实名认证系统，通过对用户的个人信息（姓名、身份证号、人脸）进行校验，增加用户身份可信度。目前已在抖音、头条等 APP 的直播、支付等涉及用户实名认证的场景完成落地。（内容来自调研）

（三）人脸识别产品价值

作为人脸识别系统与其他系统、设备的集成者，产品/服务提供者需按照产品应用者的要求进行集成开发，并且产品最后将直接面向用户，因此与产品应用者和用户也具有更加紧密的联系。人脸识别产品有着积极的社会价值。在公共安全领域，人脸识别技术配合人体特征、行为分析和事件分析，可将被动安防推向主动安防，在刑侦追逃、罪犯识别以及边防安全等领域具有重要的实战价值，比如，在视频监控

[8] 参见前注 1。
[9] 参见依图官网：https://www.yitutech.com/cn/business/smart-retail

系统中嵌入交通事件检测、人脸识别、违停抓拍及行人闯红灯抓拍等模块，并结合安防云和交通云，可大力提升社会治安防控体系建设的科技含量。

从技术的发展角度来看，技术产品化是实现技术价值、探索技术边界的必经之路，良好的产品设计需要充分考虑应用场景的差异和最终用户的需求。从法律关系角度来看，产品提供者不仅应当按照合同向产品接收者履行义务，在产品面向自然人提供涉及用户个人信息等具有敏感性的服务时，还应当向用户作出真实的说明和明确的警示，防止危害后果的发生。

三、人脸识别服务使用生态

（一）服务使用者

服务使用者是指将人脸识别技术实际应用于生活场景中的使用方，按照应用场景可以划分为**智慧安防、智慧金融、手机娱乐、出行交通**等多个领域的使用者。**在安防领域**，房地产商通过人脸识别一体机降低“飞单率”，公安机关通过公安平台进行刑侦打击犯罪；**在金融领域，**银行自主研发人脸识别系统，为用户提供高安全性的人脸识别服务；**在销售领域，**零售企业人脸识别与无人零售结合，开拓销售新场景新模式；**在交通领域，**车企利用人脸识别技术提升人机交互的体验感；**在家具领域，**家具企业通过人脸识别技术研发智能开锁产品，提高产品的智能性。

（二）产业实践

人脸识别服务使用者主要按照场景需求开展产业实践，主要以金融领域为代表。度小满采用动作配合式活体，在客户端做质量和活体检测，业务自动审核率超过90%。工商银行以前瞻性、系统性、安全性为指导，进行顶层架构设计，采用分层架构设计，建设多元化特征并行发展，云边端纵向分层解耦，提供生物特征客户统一视图的企业级生物识别服务，以兼顾不同场景和部署环境需求[10]。微众银行自主研发的人脸识别系统，集成于微众银行APP，为用户提供高安全性的人脸识别服务。在用户使用微众银行APP进行开户、添加银行卡、重置交易密码、注销账户等重大操作时，微众银行人脸识别系统会作为前置安全保障的步骤进行服务调用和识别验证，搭配密码输入、短信验证等组合验证，确认操作用户身份的真实性。

（三）人脸识别服务使用价值

人脸识别技术使用是产业成果落地实践的关键，也是与用户交互的纽带，在促进科技成果有效转移转化落地、加快产业化进程等方面发挥了不可或缺的作用。

服务应用方是具体部署产品使用和处理的关键，重点应当聚焦人脸信息保护的实践需求，按照业务进行流程化的管理设计，贴合实际需要。

[10] 参见中国工商银行金融科技研究院：《商业银行生物识别技术应用实践及趋势分析》，2022年9月。

四、人脸生成合成生态

生成式 AI 在人脸生成合成领域的应用可以分为两大类四小类：一是人脸生成，生成现实中不存在的人脸。二是人脸合成，针对已有人脸进行修改，包括：1.人脸身份合成，更改图像或视频中人物的身份；2.人脸动作合成，改变人物原有的面部动作；3.人脸属性合成，对原始人脸的某些属性进行编辑。

人脸生成合成技术被广泛应用于影视、娱乐、教育、医疗、社交、电商、内容营销、艺术创作、科研等领域。在影视领域，人脸生成合成技术用于影视作品的后期制作的翻拍、补拍、数字复活已故演员等；在电商领域，人脸生成合成技术可以构建虚拟主播、让用户实现在购买前“数字试穿”等；在广告营销领域，合成不存在但具有吸引力的人脸作为代言人或广告角色，可以降低广告成本和侵犯肖像权的风险等；在医疗领域，生成与真实影像无异的医学图像来训练 AI 系统，可以解决数据不足、病人隐私保护等问题；在游戏领域，人脸生成合成技术主要用于 NPC 外形生成、模拟对手对战训练等。

人脸生成合成生态包括三类主体：技术提供者、产品/服务提供者、服务应用者。其中技术提供者包括两类：一是大模型技术提供者。它们通过受控 API、开源等方式输出大模型能力，如 OpenAI、Stability AI、 Google、Meta、百度、

字节跳动、昆仑万维等。二是各垂直领域/行业模型（小模型）的技术提供者。它们在预训练模型基础上，通过专门的调试和训练，快速抽取形成垂直化、场景化、定制化的小模型和应用工具层。如科大讯飞、商汤、旷视、依图、格灵神瞳等。产品/服务提供者即提供生成式 AI 应用的服务商，如百度大脑人脸融合、瑞莱智慧公司人脸安全防火墙 RealOasis、无界 AI、计算美学、万兴科技、影谱科技、启元世界、Deepfake、FaceSwap、ZAO、Midjouney、DALL-E 等。

第二章 人脸识别产业的治理经验

一、美国人脸识别的治理经验

（一）美国人脸识别治理的立法

美国在人脸信息保护上采用的是通过专项立法进行保护的模式，侧重隐私权保护。在联邦层面，尽管已有若干法律提案，但目前还无统一法律规范人脸信息的收集和使用。相形之下，各州对人脸识别产业的规制走在联邦的前列，呈现“拼凑式”的立法特点，其中较为突出的是伊利诺伊州和加利福尼亚州。伊利诺伊州的《生物信息隐私法案》（Illinois Biometric Information Privacy Act，以下简称“BIPA”）是美国境内第一部规范生物识别信息的法律，并且由此催生 Facebook 生物识别信息隐私权诉讼等集体诉讼案件；加利福尼亚州接连颁布的《加利福尼亚州消费者隐私法》（The California Consumer Privacy Act，以下简称“CCPA”与《加州隐私权利法案》（California Privacy Rights Act，以下简称“CPRA”）同样也影响深远。

总体而言，各法案内容主要涉及以下三方面：第一，以限制处理人脸信息为核心，给予数据生命周期的强化保护。当私人实体在采集、存储、使用与销毁生物信息过程中，应严格遵守合法权源等义务、处理必要性等原则。第二，注重

信息披露、外部问责和监督机制。[11]第三，在治理人脸识别技术时避免将算法偏见、自动化决策负面影响纳入考量。[12]

层级	文件名称	内容简介
联邦层面	《道德使用人脸识别法案》（Ethical Use of Facial Recognition Act）（2020.2.12）	本法案第四节规定禁止政府机构使用人脸识别技术。美国政府机构不得安装任何与人脸识别技术相连接的摄像机，不得在未经授权的情况下获取或使用通过人脸识别技术获得的个人信息，不得在没有逮捕令的情况下使用人脸识别技术来识别特定个人。 第五节提供了人脸识别技术侵害权利的司法救济。任何人如果认为美国政府机构违反规定使用人脸识别技术使自己遭受侵害的，均可向相应的美国地方法院提起民事诉讼，以获取禁止令或者宣告性救济。 第六节提及制定人脸识别技术使用规则：（1）在未经许可的情况下，人脸识别技术是否可以在私人或公共场所适当使用；（2）商业化使用人脸识别技术的情形和限制是什么，个人对于其数据所享有的权利是什么；（3）在何种情形下，政府官员可以未经许可使用人脸识别技术；（4）考虑个人对于保护隐私或匿名的合理期望，应采用何种规则来控制通过人脸识别技术对于人脸图像的获取；（5）在何种情形下，个人能够选择退出或选择使用人脸识别技术；（6）需要采取什么保障措施以防止人脸识别技术的滥用；（7）当人脸识别技术被滥用时有哪些适当的救济措施；（8）个人应享有哪些与人脸识别技术所产生的数据及他们肖像的使用相关的权利。
	《国家生物识别信息隐私法案》(National Biometric Information Privacy Act of 2020)(2020.08.03)	以 BIPA 为蓝本，规范生物识别信息的收集、保留、披露和销毁。主要包括私人实体：（a）不能通过贸易获取个人或客户的生物识别信息，除非实体提供服务或其他有效商业用途，以书面形式告知并获得书面许可（不得与其他同意，包括就业协议相结合）；（b）应以合理的谨慎标准和保护其他机密和敏感信息的方式存储、传输和保护生物识别信息等。
	《商业人脸识别隐私法案》(Commercial Facial Recognition Privacy Act of 2019)	法案主要规范商业使用人脸识别技术，要求在使用前获得个人的同意，在未经同意情况下禁止将人脸识别数据共享给非关联第三方。具体内容包括：一是要求收集人脸识别数据获得明确同意；二是对人脸识别数据的处理提出限制性要求：（a） 原则上禁止使

[11] 例如，加州法案规定企业应保存内外部审计机构就生物识别系统的安全性、隐私性作出的审计记录，审计测试与测试数据库须经政府部门批准，定期将审计结果向社会公示。同时，亦注重外部问责．针对企业采用的生物识别系统进行年度外部审计，就收集数据的期限是否合理、精确度是否达标、是否对个人产生不利的歧视性影响开展审计问责。

[12] 例如，《商用人脸识别隐私法草案》中规定禁止使用人脸识别技术对用户进行歧视化对待。

	(2019.03.14)	用该技术收集人脸识别数据，除非获得明确同意并提供通知；禁止歧视、更改使用目的及未经明确同意与非附属第三方（an unaffiliated third party） 共享人脸识别数据，（b） 若对某一服务而言该技术的使用非必需的，不可因终端用户同意放弃隐私权服务或没有提出明确同意而终止或拒绝提供服务；三是明确可使用人脸识别技术的例外情形；四是要求对人脸识别技术的准确性进行独立第三方测试。
	《人脸识别技术授权法案》（Facial Recognition Technology Warrant Act）（2019.11.14）	法案旨在限制联邦调查局、移民与海关执法局等机构通过人脸识别技术开展持续监视，持续监视是指利用人脸识别技术在公共场所跟踪被识别个人的身体运动超过 72 小时，无论是实时的还是使用该技术进行历史记录，明确只有在支持执法机构的活动中，取得法院命令等情况下才能将人脸识别技术用于持续监视。 此外，持续监视获取的证据的使用具有限制，若信息是非法获得的、授权获取信息的法院发出命令的理由不充分、与法院命令授权使用的目的不相符等情况下不得在诉讼中申请使用。 最后，政府机构要对使用人脸识别技术得出的结论进行人工审查，并与美国技术和标准研究院（NIST）协商建立人脸识别系统测试程序，定期对系统性能进行独立测试。
	《2018 年外国投资风险审查现代化法案》《关于外国人在美国进行特定投资的规定》《出口管制条例》	通过外商投资安全审查、出口管制等手段对人工智能关键技术、敏感个人数据等采取相关跨境限制措施。 1.直接或间接收集或持有美国居民敏感个人数据的美国企业属于敏感行业美国企业（TID U.S. Business）。 2.外国投资者针对敏感行业美国企业的非控制权投资交易可能落入 CFIUS 的审查范围，并属于强制申报的情形。
	《2022 年面部识别法案》（提案）	美国马里兰州众议员 Ted Lieu 提出了《2022 年面部识别法案》。该法案包含规范面部识别技术在公共和私营部门的必要使用的条款。它还规定了透明度要求、年度评估和围绕执法部门使用情况的报告。 （一）对政府执法部门使用 FRT 进行严格限制和禁止： 1. 将执法部门使用人脸识别技术的情况限制在获得搜查令的情况下，搜查令应说明某人可能犯下严重暴力重罪的可能原因。 2. 禁止执法部门使用 FRT 来记录个人如何表达宪法所保障的权利，如合法抗议。 3. 禁止将 FRT 匹配作为确定搜查、逮捕或其他

		执法行动的合理理由的唯一依据。 4. 禁止执法部门使用 FRT 来执行移民法。 5. 禁止将 FRT 与包含非法获得的信息的数据库以及人体摄像头、仪表盘摄像头和飞机摄像头一起使用。 6. 禁止使用 FRT 追踪具有实时或存储视频片段的个人。 7. 确保该法案中的任何内容都不妨碍州或地方政府禁止或暂停使用 FRT。 （二）为个人提供透明度并提供救济路径: 1. 为因使用 FRT 而受到伤害的个人建立了私人诉讼权等救济途径。 2. 要求执法部门向作为 FRT 搜查对象的个人提供通知，并提供法院命令的副本和/或其他关键数据点。 3. 要求执法部门每六个月从 FRT 逮捕照片数据库中清除 18 岁以下、无罪释放、被撤销指控或被宣告无罪的个人照片。 （三）确保对执法部门使用 FRT 的情况进行年度评估和报告: 1.要求对执法机构使用的 FRT 系统进行定期审计，对审计不合格的机构进行停职处理。对审计不合格的机构进行暂停。 2.要求每年对执法部门采用的任何 FRT 系统进行独立测试。 3.要求详细的 FRT 司法和检察报告，以及数据收集。
伊利诺伊州	《生物信息隐私法案》 (Illinois Biometric Information Privacy Act, BIPA) (2008)	1.知情同意，收集个人生物识别信息需获得知情的书面同意；2.保留准则，企业须制定书面政策设定生物识别数据的保留时间表，且当收集数据的目的已达到或距信息主体与企业最后一次联络已满三年时（以先发生者为准），应当摧毁该数据；3.禁止获利，生物识别数据不得出售；4.有限披露，且除非获得相关自然人的同意或法律规定的特定例外情况不得对他人披露；5.BIPA 要求私人实体行业内的合理的注意标准（不同行业的注意标准不尽相同）；6.对生物信息的保护至少等同于“机密和敏感信息”的保护；7.允许公民对违反其规定的行为提起私人司法诉讼。
德克萨斯州	《捕获或使用生物识别符法案》 (Texas Capture or Use of Biometric Identifier Act,CUBI) (2009)	1.除非事前通知并收到同意外，任何人不得出于商业目的获取生物特征识别信息；2.规定除完成个人要求或授权金融交易等四种特殊情形外，不得向他人出售、出租或以其他方式透露已获取的生物特征识别信息；3.应该以合理谨慎的态度存储、传输、保护生物识别标识符。

华盛顿州	《生物识别隐私法》(Washington Biometric Privacy Law,WBPL)(2017.07)	从问责、人工审查、测试等机制来规范人脸识别服务使用。1.控制者必须获得消费者的同意，才能部署面部识别服务；2.在可能会对消费者产生法律或类似的重大影响的情况下，必须包括有意义的人类审查；3.禁止使用面部识别技术进行歧视；4.必须向消费者提供描述技术能力和局限性的文件；5.开发人员可在线使用的面部识别技术必须为第三方提供独立测试的技术能力。
加利福尼亚州	《人脸识别技术法》(Assembly Bill 2261: Facial recognition technology)(2020.02.14)	该法在加州民法典隐私保护部分增加人脸识别章节，内容上主要涉及人脸识别信息的收集和处理、政府机构使用人脸识别服务的限制性要求。一是收集人脸识别信息应当征得个人同意；二是建立人脸识别服务的人工审查和测试机制；三是建立政府机构使用人脸识别服务的问责机制；四是限制政府机构对人脸识别服务的使用。
	《加利福尼亚州消费者隐私法》(The California Consumer Privacy Act,CCPA)	CCPA 虽被称为全美最严厉的隐私保护立法，但其对收集个人生物信息的规制比较宽松，没有专门针对生物特征识别信息收集与使用的规定条款，与对一般个人信息的规制基本无异。[13]
	《加州隐私权利法案》(California Privacy Rights Act,CPRA)(2020.11.3)(2023.1.1)	在 CCPA 的基础上，进一步赋予个人一些新的权利。CPRA 在 CCPA 的内容上进行了多处修改，但许多细节需要通过法规加以澄清和定义。例如，建立针对全面选择退出偏好标志及其他选择退出机制的技术要求、定期提交个人信息处理风险评估报告（报告内容应当包括该处理行为是否涉及处理个人敏感信息）等。 1.CPRA 区分敏感个人信息和一般个人信息。消费者可以限制对于除必要服务和必需产品外敏感个人信息的商业使用。值得注意的是，对于敏感个人信息的规定不适用于公开信息[14]或者非用于分析消费者特点[15]而收集或处理的敏感个人信息。 2.CPRA 主要规制三类主体收集、处理消费者个人信息的行为，包括企业[16]、承包商[17]、服务提供方[18]。

[13] 在“公开可用”上略有不同，公开可用不意味着企业可以在消费者不知情的情况下收集关于消费者的生物信息。

[14] 根据 1798.140 第(v)款第(2)项的规定，公开获取的敏感个人信息不视为敏感个人信息，甚至也不视为个人信息。1798.140 第(v)款第(2)项中个人信息不包括公开获得的信息，或合法获得的、真实的、引起公众关注的信息。就本项而言“可公开获得”是指：从联邦、州或地方政府记录中合法获得的信息，或者某企业有合理理由认为是由消费者合法地向公众公布的，或从广泛传播的媒体获取的；或者如果消费者没有将信息限定于特定的受众，则由消费者已经向其披露了信息的人提供的信息。“可公开获得”并不意味着企业在消费者不知情的情况下收集的关于消费者的生物识别信息。

[15] 第 1798.121 条(d)项规定不以推断消费者特征为目的收集或处理的个人敏感信息不受本条约束，但上述信息仍应被视为个人信息。

[16] CPRA 只针对满足一定条件的大企业。即在加州开展业务的营利组织，并满足：(1)上一年度年收入总额超过 2500 万美元；或(2)单独或与他人合并，每年购买、出售、共享消费者的个人信息或家用设备数量达到 10 万以上；或(3)50%以上的收入来自出售、共享消费者的个人信息。

		CPRA 要求承包商和服务提供方与企业签订的书面合同需要以下条件：禁止出售、共享该个人信息；禁止超范围、超限度使用、处理该个人信息；原则上禁止将从企业处获取的消费者个人信息与从其他企业处获得的个人信息相结合用于个性化营销目的。此外，合同中须包含的合规承诺，以及授权企业对其个人信息处理活动的监督、审计等权利。涉及敏感个人信息的情况，如果消费者要求企业限制使用其敏感个人信息，企业应告知相关服务提供商或承包商。服务提供商或承包商在收到企业指示后，应停止使用相关消费者的敏感个人信息。即服务提供商和承包商对于企业的限制性使用指示有响应、配合义务。 3.Opt-out 机制的实现 企业可以通过多种方式向消费者提供“Opt-out”功能，但根据 CPRA 的要求，企业应在其网站主页、线上隐私政策中都提供清晰、明显且分开的“不得出售或共享我的个人信息”链接和“限制使用我的个人敏感信息”链接，供消费者点击选择。一旦消费者作出 Opt-out 选择，企业在此之后 12 个月内不得再次要求该消费者授权企业出于其他目的使用、披露消费者的敏感个人信息。

（二）美国人脸识别治理的典型案例

1.谷歌用户起诉谷歌违反 BIPA

2016 年 3 月，用户向谷歌提起集体诉讼，认为谷歌对用户在“谷歌照片”中上传的照片进行分析并建立面部模型，既没有公布收集用户生物识别信息的政策，也未获得用户的书面同意，违反了 BIPA 的规定。2019 年 1 月，法官以原告无法证明因谷歌公司的行为造成“具体损害”而驳回了原告起诉。

2. Rosenbach v. Six Flags Entertainment Corp.

2017 年 12 月，伊利诺伊州一位市民因其儿子办理六

[17] 与企业签订书面合同，企业出于商业目的向承包商提供消费者个人信息。
[18] 以企业的名义处理个人信息的个人并根据书面合同从企业或代表企业接收用于商业目的的消费者个人信息的主体。

旗主题公园（Six Flags）的季卡时被要求提供指纹信息而向法院提起诉讼，认为六旗主题公园既没有公布收集用户生物识别信息的政策，也未获得用户的书面同意，违反了 BIPA 的规定。伊利诺伊州上诉法院判决认为，原告未能证明合法权利受到损害，未支持原告的诉讼请求。伊利诺伊州最高法院在 2019 年 1 月推翻了原审法院的判决，认为生物特征隐私是一项基本的民事权利，个人无需证明受到实际损害就可起诉自身权利受到侵害。[19]

3.多名用户针对 Facebook 的图片标签功能提起集体诉讼

2016 年 5 月，多名用户针对 Facebook 的图片标签功能提起集体诉讼，认为 Facebook 未经用户同意收集用户生物识别信息，并存储在 Facebook 面部识别数据库中。只要用户上传照片，Facebook 的系统就会自动分辨出镜头中的面孔与之前上传照片中的人脸匹配，最后鉴别出个人身份。2019 年 8 月，美国第九巡回上诉法院驳回了 Facebook 要求撤销集体诉讼的请求，将该案退还给旧金山地方法院进行审理。案件最终达成和解协议，Facebook 将向符合条件的伊利诺伊州用户支付 5.5 亿美元，并支付原告的诉讼费。

4.Snap Inc.公司违规收集个人生物特征信息

2022 年 9 月，在伊利诺伊州，针对视频通讯应用软件

[19] Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019).

Snapchat 违规收集用户生物特征信息的集体诉讼案（Boone, et al. v. Snap Inc.案）初步达成了庭外和解（最高可达 3500 万美金赔偿、波及超 35 万人的和解动议）。在这起集体诉讼中，Snap Inc. 被指控违反了 BIPA。原告称，Snap Inc. 的隐私政策（Privacy Policy）中没有说明用户的面部信息会被收集，而且公司在没有得到用户书面授权的情况下，通过用户使用滤镜和特效镜头扫描了用户人脸。作为被告的 Snap Inc.虽然选择庭外和解，并同意支付最高 3500 万美元的和解费用，但不接受以上任何一项指控。Snap Inc.表示：“软件在使用镜头时不会收集可用于识别特定人员或进行面部识别的生物特征数据，例如，镜头可将眼睛或鼻子识别为面部的一部分，但不能将眼睛或鼻子识别为属于任何特定的人。”同时还表示，镜头功能使用的数据不会发送到他们的服务器，而是保留在用户的设备上，因此公司不应在 BIPA 管辖之列。

5.Instagram 违法收集处理人脸信息

2015 年 4 月，多位美国伊利诺伊州用户针对 Instagram 提起集体诉讼，指控该软件使用的生物识别技术违反了 BIPA。该法律严格限制企业收集、使用和共享生物信息，禁止企业在未经用户同意的情况下收集生物信息。同时，该法要求企业需要以书面形式告知用户收集生物信息的目的、用途以及存储和销毁的时间。诉讼称 Instagram 通过面部标记工具采集用户面部数据，并将创建的“面部数据”储存在数据库中。

Instagram 会在未经用户同意的情况下，自动使用面部标记工具来获取信息。对此，Instagram 声称其面部识别功能开启时，作用仅为通过建立个人面部模板来查找用户在 Facebook 等软件上的照片和视频，从而实现打标签、记录发布内容和特征的目的。然而，伊利诺伊州用户认为，Instagram 及其母公司 Meta 此举实际上在未获得用户知情同意的情况下，收集和使用其生物特征信息。

该案被诉至美国库克县巡回法院，后被移交至芝加哥联邦法院和加利福尼亚州联邦法院。此案审理期间，2021 年 11 月，由于用户对生物识别技术的安全性愈发担忧，Meta 宣布关闭其面部识别功能，同时删除存储的超过十亿个面部识别模板。2023 年 3 月，Instagram 与多位原告达成和解，决定为在 2015 年 8 月 10 日至 2023 年 8 月 16 日期间使用该软件的伊利诺伊州用户支付共计 6850 万美元的和解金，用户需在 9 月 27 日之前提交索赔申请，不想接受和解条款的人需在 8 月 16 日之前提交信函请求排除；想要留在和解集体中但反对和解或与和解相关的支出的人，需在 8 月 16 日前向法院提出异议。和解协议的最终批准听证会定于 10 月 11 日举行，每位索赔用户能获得多少赔偿将取决于提交索赔申请的总人数以及用户在规定期限内使用 Instagram 的时长。在向该案代理律师、税务、和解事务处理小组以及诉讼代表支付费用后，赔款将按一定比例发给受此事件影响的用户，

不论是成年人还是未成年人。但和解协议的最终批准听证会已从 10 月 11 日推迟到 11 月 21 日，官方没有给出推迟解释。如果和解协议获得批准且所有上诉被解决后，索赔人预计将在 90 天内（即 2024 年 2 月）开始获得自己应得的赔偿份额，但具体付款时间还需法院确定，仍具有不确定性。

总之，该案显示了 BIPA 作为一个真正强大的机制和执法工具的重要性，凸显了私人诉权在确保隐私制度执行方面的工具价值，体现了 BIPA 在人脸识别技术的使用和部署过程中所发挥的重要作用。

二、欧盟人脸识别的治理经验

（一）欧盟人脸识别治理的立法

欧盟对于人脸信息保护采取综合立法保护模式，初期以《一般数据保护条例》（以下简称“GDPR”）中生物信息保护为核心，近期则延伸到人脸识别应用人工智能算法上。与美国不同，欧盟尝试着在区分人脸识别产业中不同主体的基础上，采取差异化的义务与责任规制。例如，《关于人脸识别的指南》分别对开发和销售人脸识别技术、私营实体使用人脸识别技术两种情形进行指引；作为全世界第一部通过议会程序、专门针对人工智能的综合性立法，《人工智能法案》分别规定高风险 AI 系统提供商、高风险 AI 系统用户的义务；《欧盟人工智能责任指令》区分高风险 AI 系统提供者和用户的证据、因果关系推定的规则。

总体而言，欧盟对人脸识别产业保持非常谨慎的态度，对其设置了多重限制，包括但不限于（1）使用目的和使用场景的限制：人脸识别技术的使用只能在受控环境中进行验证、认证或分类；（2）数据处理的限制：数据处理的合法性，要求获得同意、透明、公平、数据最小化、存储时间有限；（3）数据准确性的限制；（4）数据安全的限制；（5）组织流程的限制：企业应设立内部审查委员会和数据安全保护官（DPO），定期开展数据影响评估，以评估、批准涉人脸识别数据的处理活动。

此外，虽然没有直接针对人脸识别技术开发的规定，但人脸识别技术被《人工智能法案》确定为高风险 AI 系统，《人工智能法案》从高风险 AI 系统应符合的标准和系统提供商的义务两个维度，提出对高风险 AI 系统技术要求和组织措施：强制性的风险管理系统、高质量数据训练集、技术文件和记录保存、明确的透明度、确保能对系统进行人为监督、确保 AI 系统能够达到适当的准确性、鲁棒性和网络安全、售后监控。

根据目前公布的最终版法案，AI 工具将依照本身技术特性，按照风险等级匹配监管规则，其中值得一提的是《人工智能法案》将严格禁止对人类安全具有不可接受风险的人工智能系统（Unacceptable risk AI），例如公共场合的“实时”或“事后”的远程生物识别系统、使用敏感特征（如性别、

种族、民族等）的生物识别分类系统、从互联网或闭路电视录像中无目标地抓取面部图像以创建或扩展面部识别数据库的人工智能系统、通过分析先前犯罪行为，试图预测未来非法活动的预测性警务系统，以及在执法、边防、工作场所和教育机构等领域中用于推断自然人的情绪识别系统等。

上述明令禁止的内容中，禁止使用生物识别系统这一条文备受争议。拥有人脸与生物辨识技术的 AI 公司可以通过社交媒体或电视影像对民众的外观信息进行大规模搜集与分析，严重威胁了个人隐私；面部识别技术甚至可以作出种族定性，可能危及有色人种或弱势少数民族公民的个人自由。最终版《人工智能法案》禁止出于执法目的在公共场所使用“实时”远程生物识别系统，除非使用该系统对于以下目的之一必须的：（1）寻找绑架、贩卖或性剥削的受害者，以及失踪人员；（2）防止对于生命或身体安全的特定的、重大的和紧迫的威胁或恐袭；（3）出于调查、检控或执行惩罚的目的定位或识别严重犯罪的嫌疑人。

2024 年 3 月 13 日，欧盟议会以 523 票赞成，46 票反对和 49 票弃权的压倒性票数通过了《人工智能法案》。该法案是世界上“第一部”针对人工智能的全面且具有约束力的法规，这一里程碑式法案的通过，有助于欧盟在监管人工智能方面走在世界的前列，即使《人工智能法案》的管辖范围只能覆盖欧盟成员国，但其针对人工智能监管的规范却可以

成为其他国家的参考。由是观之，如欧盟《人工智能法案》通过，该法案或许将同欧盟《一般数据保护条例》（GDPR）一样，影响世界各国家或地区的立法和实践。

文件名称	内容
《一般数据保护条例》（General Data Protection Rules）	人脸识别信息属于GDPR规定的个人敏感数据。除了数据控制者对一般信息的保护义务，如遵守合法、合理和透明原则、目的限制原则、最小化原则、准确性原则、限期储存原则、完整保密原则和权责一致原则等，GDPR对敏感数据的保护提出更严格的要求，原则上禁止处理。对于人脸识别技术的商业应用而言，可适用的唯一例外情形是“数据主体已明确表示同意”，且同意须“自由、明确、具体”。GDPR还对敏感数据控制者或处理者单独规定了必须设立DPO（第37条）和必须进行数据保护影响评估的义务（第35条）。 根据GDPR的规定，照片不当然构成个人敏感数据，但在通过特定技术方法对照片进行处理，使其能够识别或认证特定自然人时，也属于处理个人敏感数据（第51条）。
《欧盟人工智能法案（草案）》（EU Artificial Intelligence Act）（2020.2.19）	《欧盟人工智能法案（草案）》（以下简称“《草案》”）明确将人脸识别列为高风险AI系统。 1.针对高风险AI系统提供商（技术研发者）而言，需要重点关注《草案》第三编第2章对高风险AI系统本身的要求、第3章中关于高风险AI系统提供商的义务，以及第八编第61条提供商的入市后监测义务。 第三编第2章第9条—第15条规定了强制性的风险管理系统、高质量数据训练集、技术文件和记录保存、明确的透明度、确保能对系统进行人为监督、确保AI系统能够达到适当的准确性、鲁棒性和网络安全。 第三编第3章第16条罗列了高风险AI系统提供商义务，第17条—23条详细阐述前述义务的具体要求，其中包括：保证并证明其AI系统符合对高风险AI系统的要求（具体见该草案第2章）、建立质量管理体系、编制技术文档、保留AI系统自动生成的日志、确保系统投放前经过合格评定程序、采取纠正措施等义务。 第八编第61条规定了提供者负有建立售后监

	控系统的义务，需通过该系统评估 AI 系统的持续合规性。 2.针对技术应用者，《草案》第 3 章第 29 条规定了高风险 AI 系统用户的义务，包括：按照系统附带的使用说明使用系统；监督系统运行；在自己控制范围内确保输入数据是与高风险 AI 系统的预期目的相关的；保留该高风险 AI 系统自动生成的日志；进行数据保护影响评估。 除此之外，技术应用者也可能被认定为构成技术供应商，从而承担技术研发者相同的责任。《草案》第 3 章第 28 条规定了经销商、进口商、用户或任何其他第三方应被视为提供者的情形：（a）以自己名称或商标将高风险 AI 系统投放市场或投入使用；（b）修改已经投放市场或投入使用的高风险 AI 系统的预期目的；（c）对高风险的 AI 系统进行了实质性的修改。 3.针对产品制造商，《草案》规定以产品制造商的名义与根据该法律行为生产的产品一起投放市场或投入使用时，产品制造商应对 AI 系统符合本条例的规定承担责任，并就 AI 系统而言，负与本条例下供应商所负义务相同的义务。 4.《草案》规定了人脸识别技术进口商和经销商的义务，系统服务者如果有进口或经销人脸识别技术的业务，需要履行《草案》规定的相应义务。
《欧盟人工智能法案》 （EU Artificial Intelligence Act） （2024.3.13）	本法案将公共场合的“实时”或“事后”的远程生物识别系统归为具有不可接受风险的人工智能系统，对于人脸识别采取严格谨慎的态度，这也与《欧盟人权公约》中规定的隐私权、思想自由、禁止歧视等内容相符。具体涉及人脸识别的相关条文如下： **Recital 8:** 本条例中使用的“远程生物识别系统”的概念应从功能上加以定义，这是一种人工智能系统，用于在自然人没有主动参与的情况下，通常是在一定距离之外，通过将一个人的生物数据与参考数据库中的生物数据进行比较，从而识别其身份，而不论所使用的生物数据的特定技术、程序或类型如何。这种远程生物识别系统通常用于同时感知多个人或其行为，以便在没有自然人主动参与的情况下极大地便利对自然人的识别。这不包括用于生物验证，包括用于鉴别的人工智能系统，相应系统，单纯出于获得服务、解锁设备或安全进入场所的目的，其唯一目的是确认特定自然人就是他或她声称的那个人，以及确认自

	然人的身份。这种排除的理由是，与远程生物识别系统相比，这类系统对自然人基本权利的影响可能较小，因为远程生物识别系统可用于处理许多人的生物数据，而无需这些人的积极参与。在“实时”系统中，生物数据的采集、比对和识别都是在瞬间或接近瞬间进行的，或在任何情况下都没有明显的延迟。在这方面，不应存在通过设定轻微的延迟来规避本条例关于“实时”使用有关人工智能系统的规则的空间。“实时”系统涉及使用“现场直播”或者“近乎现场直播”的材料，如摄像机或其他具有类似功能的设备生成的录像片段。相比之下，“事后”系统则是生物数据已经得到采集，只有在延迟之后才进行比对和识别。这涉及在对有关自然人使用该系统之前已经生成的材料，如闭路电视摄像机或私人设备生成的图片或录像 **Recital 18:** 在公共场所为执法目的使用“实时”远程生物识别系统，每次使用都应得到司法机关或其决定对成员国具有约束力的独立行政机关的明确和具体授权。 这种授权原则上应在使用该系统识别特定的个人或多人之前获得。在有正当理由的紧急情况下，即在需要使用有关系统，因而实际上和客观上不可能在开始使用之前获得授权的情况下，这一规则应允许例外。在这种紧急情况下，使用应限制在严格必要的最低限度，并受制于适当的保障措施和条件，这些措施和条件由国家法律确定，并由执法机关本身在每个紧急使用的个案中具体规定。 此外，在这种情况下，执法机关应在提出申请的同时，说明未能及早提出申请的原因，不得无故拖延，最迟应在 24 小时内提出申请。如果这种授权被拒绝，则应立即停止使用与该授权有关的实时生物鉴别系统，并应弃置和删除与这种使用有关的所有数据。这些数据包括人工智能系统在使用过程中直接获得的输入数据，以及与该授权相关的使用结果和输出。这不应包括根据其他国家或欧盟法律合法获取的输入数据。在任何情况下，不得仅根据远程生物识别系统的输出结果做出对个人产生不利法律影响的决定。 **Recital 24:** 在使用人工智能系统进行生物识别时涉及的生物数据和其他个人数据的任何处理，除与本条例规定的为执法目的在公共场所使用“实时”远程生物识别系统有关外，应继续遵守 2016/680 号指令第 10 条规定的所有要求。对

	于执法以外的目的，2016/679 号条例第 9 条第 1 款和 2018/1725 号条例第 10 条第 1 款禁止处理生物数据，但这些条款规定的有限的例外情况除外。在适用 2016/679 号条例 第 9 条第 1 款时，远程生物特征识别用于执法以外的目的的已经落入国家数据保护机关的禁止决定之下。 **Recital 26 b:** 应禁止将人工智能系统投放市场、为这一特定目的提供服务或加以使用，这些系统通过从互联网或闭路电视录像中无针对性地获取面部图像来创建或扩大面部识别数据库，因为这种实践会增加大规模监控的感觉，并可能导致严重侵犯基本权利，包括隐私权。 **Article 3 – paragraph 1 – point 36:** “远程生物识别系统”系指一种人工智能系统，其目的是在没有自然人主动参与的情况下，通常通过将一个人的生物数据与参考数据库中的生物识别数据进行比较，远距离识别自然人的身份; **Article 3–paragraph 1–point 37:** “‘实时’远程生物识别系统”是指一种远程生物鉴别系统，在该系统中，生物数据的采集、比较和识别都是在没有明显延迟的情况下进行的。这不仅包括即时识别，还包括有限的短暂延迟，以避免规避本条例。 **Article 5 – paragraph 1:** (da) 投放市场、提供服务或加以使用人工智能系统，对自然人进行风险评估，以评估或预测自然人实施刑事犯罪的风险，而这完全是基于对自然人的画像或对其个性特征和特点的评估；这一禁令不适用于这样的人工智能系统，其根据与犯罪活动直接相关的客观且可核实的事实，支持人类对特定个人是否参与犯罪活动的评估。 (db) 投放市场、为此特定目的提供服务或加以使用人工智能系统，通过从互联网或闭路电视录像中无区别地爬取面部图像来创建或扩展面部识别数据库; (dc) 投放市场、为此特定目的提供服务或加以使用人工智能系统，在工作场所和教育机构领域推断自然人的情绪，但出于医疗或安全原因，有意将人工智能系统提供服务或投放市场的情况除外; (de) 投放市场、为此特定目的提供服务或加以使用生物分类系统，根据生物数据对自然人进行个体层面的分类，以推导或推断其种族、政治观点、工会成员身份、宗教或哲学信仰、性生活

	或性取向。 这项禁令不包括根据生物数据对合法获取的生物数据集，如图像，进行标注或过滤，也不包括在执法领域对生物 数据进行分类。 **Article 5 – paragraph2:** 在公共场所为执法目的使用“实时”远程生物识别系统，除非这种使用相应是为下列目标之一所严格必要的: (i) 有针对性地搜寻特定的绑架、贩卖人口和性剥削受害者，以及搜寻失踪人员; (ii) 防止对自然人的生命或人身安全构成确切、重大切紧迫的威胁，或防止真实存在或真实可预见的恐怖袭击威胁;
《欧盟人工智能责任指令》（AI Liability Directive）（2022.9.28）	《指令》的目的是通过协调成员国的过失责任规则，以确保因人工智能系统对其造成的损害而要求赔偿的人，享有等同于在没有人工智能系统参与的情况下而要求损害赔偿的保护水平。在涉及人工智能的侵权案件中，由于人工智能系统不透明、自动化决策和复杂性等特征，可能会使受害者难以证明过错、因果关系。 其中跟高风险人工智能提供者有关的规则主要包括：披露相关证据的规则[20]、风险管理系统在确认技术开发者过错方面的重要性[21]、针对高风险人工智能系统提供者提起的诉讼规定了可推定因果关系的情形[22]。
《关于通过视频设备处理个人数据的 3/2019 指引》（Guidelines 3/2019 on processing of personal data through video devices）（2020.1.29）	GDPR 区分了人脸识别数据和照片，未提及视频监控。但实际中视频监控通常可以收集大量的高度个人化甚至特殊类型的个人数据。《指引》旨在就如何通过视频设备根据 GDPR 处理个人数据提供指导。 1.细化并补充 GDPR 第 9 条当视频监控系统用于处理特殊类型数据时，数据控制者应该确认该行为是否符合 GDPR 第 9 条规定的豁免情形及第 6 条规定的合法基础；但数据控制者不能依据第 9(2)（e）条规定的豁免情形——涉及数据主体明示公开的个人数据，处理视频监控系统得到的

[20] 对于高风险人工智能系统，《人工智能法案》规定了具体的文件、信息和记录要求，但没有规定受伤害者有权获得这些信息。而获得涉嫌造成损害的特定高风险人工智能系统的信息，是确定是否要求赔偿和证实赔偿要求的一个重要因素，因此，为确定赔偿责任，应当规定有关人员披露相关证据的规则。这也应该为遵守《人工智能法案》中规定的相关要求提供额外的激励，以记录或保存相关信息。

[21] 在确定提供者是否遵守了本指令中提到的《人工智能法案》的相关要求时，应考虑提供者在风险管理系统中采取的步骤和风险管理系统的结果，即决定采取或不采取某些风险管理措施。提供者根据《人工智能法案》建立的风险管理系统是一个持续迭代的过程，贯穿于高风险人工智能系统的整个生命周期，提供者据此确保遵守旨在减少风险的强制性要求，因此可以作为评估其合规性的有用因素。

[22] 该系统不是在符合《人工智能法案》第 10(2)至(4)条所指质量标准的训练、验证和测试数据集的基础上开发的；不符合透明度的要求；不允许自然人对该系统有效监督；未达到适当的准确性、鲁棒性、网络安全水平。

	数据，进入摄像范围的事实行为并不意味着数据主体有意公开与其相关的特殊类型数据。 2.提出了一些降低处理生物识别信息所面临风险的措施，包括: 一是遵照数据最小化原则，确保不过多提取用于构建生物模板的数据，并采取措施防止模板在不同生物识别系统之间转移；二是必须存储生物特征数据时，数据控制者必须考虑数据存储的最佳位置，应存储在用户单独控制的设备上（例如智能手机或身份证）或以加密形式存储在只有用户拥有密钥的集中式数据库（centralized database）；三是应采取一切必要的预防措施保持所处理数据的可用性、完整性和机密性，在传输和存储过程中进行数据隔离，明确加密和密钥管理策略，整合欺诈检测的组织性和技术性措施，将完整性代码与数据关联（例如签名或哈希），并禁止任何外部访问生物特征数据；四是对人脸识别数据等原始数据进行删除，并确保删除的有效性。如果数据控制者需要保存原始数据，必须探索如水印等“加性噪声（noise-additive）”的保护方法。
《人工智能研究报告———通往卓越和信任的欧洲路径》 (On Artificial Intelligence – A European approach to excellence and trust) （2022.2.19）	针对使用人脸识别等高风险人工智能系统提出了严格的限制，如训练人工智能的数据应符合要求、保留部分记录和数据、告知使用者相关信息、确保技术鲁棒性、接受人工监控、投入使用前应接受事前合规审查。
《关于人脸识别的指南》 （Guidelines on Facial Recognition） （2021.1.28）	1.《指南》对人脸识别技术的开发商、制造商和服务提供商的指引主要包括确保人脸识别技术准确性和数据保护两个方面: (1) 技术要求，以减少偏差、确保人脸识别技术的准确性。确保所用数据的代表性、定期更新数据以训练改进所使用的算法、确保算法的有效性，具体操作措施如算法必须使用合成数据集来开发、记录、检测可靠性百分比记录等。 (2) 数据保护方面的义务。在内部：在人脸识别产品的设计和架构要纳入数据保护相关的原则、规则，也要把数据保护方法纳入组织工作中，如指定专门的工作人员，为员工提供隐私培训，以及进行数据保护影响评估。在外部：帮助使用技术的实体提升透明度并尊重隐私如为他们的隐私政策提供示例语言，或推荐清晰、易懂的标记表明人脸识别技术已部署在特定空间中。

	2.《指南》主要围绕数据保护对人脸识别应用者（使用人脸识别技术的实体）提出要求。 (1) 正面明确指出人脸识别技术的使用只能在受控环境中进行验证、认证或分类目的，还列举情绪识别等禁止性目的; (2) 《指南》还要求实体确保人脸识别技术使用的公平性、透明性和准确性，以及遵守目的限制、数据最小化以及存储时间的原则；[23] (3) 细化了数据保护影响评估的规定；[24] (4) 在组织措施方面，《指南》也给了实体指引，如发布关于特定使用人脸识别技术的透明性报告、成立内部审查委员会，以评估和批准任何涉及人脸识别数据的处理等。 3.《指南》还指出如果使用人脸识别技术时，完全根据人脸识别技术的结果做决定，则可被视为自动化决策，也需遵守法律对自动化决策的要求。
法国数据保护机构（CNIL）发布《机场的面部识别：有哪些挑战和需要遵循的主要原则》报告 （2019.11）	CNIL 并没有对人脸识别技术持否定态度，而是认为在适用该技术时不仅要考虑到保护公民的隐私权以及个人数据权，还要激发公民对已经实施技术的信任。 报告指出有关机场面部识别必须遵守的主要原则：1.说明拟采取的面部识别系统的必要性和相称性、征得乘客事前同意以及保障同意有效的技术和组织措施；2.必须将生物识别数据完全置于有关乘客的控制之下；3.必须进行数据保护影响评估（DPA）。
《执法领域面部识别技术指南》（Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement） （2023.4）	2023 年 4 月 26 日，经过公众咨询意见，EDPB 通过了其在执法领域的面部识别技术准则的最终版本。该准则为欧盟和国家立法机关以及执法部门提供了实施和使用面部识别技术的系统指导。 该准则强调，面部识别工具的使用应严格遵守执法指令（LED）。此外，正如《基本权利宪章》所规定的那样，只有在必要和相称的情况下才能使用这种工具。在指导方针中，EDPB 再次呼吁禁止在某些情况下使用面部识别技术，这是它在 EDPB-EDPS 关于人工智能法提案的联合意

[23] 《指南》明确对使用目的和使用环境做出限制，即人脸识别技术的使用只能在受控环境中进行验证、人证或分类目的；《指南》强调使用人脸识别技术要获得明确、具体、自由和知情的同意，在此内涵上进一步延伸提出处理者提供使用人脸识别技术的替代方案、不能当然处理公开照片；就透明度而言，《指南》详细给出告知数据主体的内容；数据存储方面，《指南》要求处理者确保不同的存储限制期限适用于处理不同的阶段；

[24] 包括内容（使用人脸识别技术，应当将必要性，目的性、比例性，以及对数据主体权利的影响一起进行评估）、评估主体、评估出风险的处理规则、公开评估结果等。

	见中提出的要求。 在公开征求意见后，对准则进行了更新，并增加了进一步的澄清意见。 对于执法背景下的个人数据保护，必须满足 LED 的要求。关于 FRT 的使用，LED 规定了一定的框架，特别是 LED 第 3 (13) 条 （术语生物识别数据），第 4 条 （与个人数据处理有关的原则）第 8 条 （处理的合法性），第 10 条 （特殊类别个人数据的处理） 和 LED 第 11 条 （自动个人决策）。 1.对特殊类别数据的处理，如生物识别数据，只能被视为“绝对必要”（第 10 条 LED）。 2.在使用 FRT 之前进行数据保护影响评估 (DPIA) 是一项强制性要求，参见 LED 第 27 条。 3.部署 FRT 的当局应在部署该系统之前咨询主管监督机构。 4.鉴于生物识别数据的独特性质，实施和/或使用 FRT 的当局应根据 LED 第 29 条，特别注意处理的安全性。 5.记录（参见 LED 第 25 条）是核实处理的合法性的重要保障，包括内部（即相关控制人/处理人的自我监督）和外部监督机构。在面部识别系统方面，建议对参考数据库的变化和识别或验证尝试进行记录，包括用户、结果和信心分数。 6.呼吁禁止某些类型的处理：（1）在公共场所对个人进行远程生物识别；（2）人工智能支持的面部识别系统，根据个人的生物特征，按照种族、性别、政治或性取向或其他歧视理由，将其归类; (3) 使用面部识别或类似技术来推断自然人的情绪，以及（4）在执法背景下处理个人数据，这将依赖于通过大规模和不加区分地收集个人数据而填充的数据库，例如通过搜刮的方式。例如，通过刮取网上可获得的照片和面部图片。
ISO/IEC WD 9868《远程生物识别系统——设计、开发和审核》（标准）	该标准为远程生物特征识别系统提供了建议和要求，进一步细化《欧盟人工智能法案（草案）》中的相关规定，如系统部署后测试的要求等。

（二）欧盟人脸识别治理的典型案例

1. 案例一：收集人脸信息应符合最小必要性原则

2019 年 8 月瑞典数据保护机构对 Anderstorps 中学做出

20 万瑞典克朗的罚款[25]，因其在学校教室里面安装人脸识别设备进行学生考勤。在该案中，瑞典数据保护机构认为，学校采用人脸识别技术收集、处理学生面部特征信息的行为违反了 GDPR 第五条规定的“数据处理最小必要性原则”和第六条规定的“数据处理合法依据”，具体体现在两个方面：一是该中学收集、处理学生面部特征信息所取得的同意并非学生及其家长自由作出的。因为学生要在学校接受教育，学校与学生及其监护人处于明显不平等的地位，在此情况下学校征得的同意违背了 GDPR 第七条规定的“同意须为自由作出（freely given）”这一要求。二是该中学收集的信息类别不符合最小必要性原则。为实现考勤这一目的，学校本可以采取其他更为保护学生个人信息的方式进行，且学校所收集的学生面部特征信息并不是 GDPR 第五条第一款要求的“为了实现数据处理目的而适当的、相关的和必要的”，因而该学校违反了 GDPR 所要求的最小必要性原则。

2.案例二：处理公开的人脸信息应获得同意

法国的数据保护机构——国家信息与自由委员会（CNIL）向美国 Clearview AI 开出了 2000 万欧元的罚单，指控其违反了 GDPR。

Clearview AI 从许多网站包括社交媒体上收集照片。它

[25] 参见瑞典数据监管机构于 2019 年 8 月 20 日对涉事高中作出的处罚决定书，“Tillsyn enligt EU:sdataskyddsförordning2016/679 ansiktsigenkänning för närvarokontroll avelever ” https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

收集所有可在这些网络上直接访问的照片（即无需登录账户即可查看的照片）。图片也从所有平台上的在线视频中提取。因此，该公司已经在全球范围内收集了超过200亿张图片。由于这种收集，该公司在市场上以搜索引擎的形式访问其图像数据库，在其中可以用照片搜索一个人。该公司向各国执法当局提供这项服务，以确定犯罪者或受害者。为了使人脸识别技术达到根据照片就可以找到一个人的效果，该公司建立了一个“生物识别模板”，即一个人的身体特征（在这种情况下是面部）的数字表示。这些生物识别数据非常敏感，因为它们与我们的身体身份（我们是什么）有关，使我们能够以独特的方式识别自己。然而，绝大多数图像被收集到搜索引擎的人都不知道这个特征。

2020年5月，CNIL收到个人对Clearview AI的人脸识别软件的投诉，并展开调查。2021年5月，隐私国际协会也就这一问题向CNIL发出警告。

CNIL进行的调查显示，Clearview有几个违反RGPD的行为：1.非法处理个人数据（违反GDPR第6条），因为生物识别数据的收集和使用没有法律依据；2.未能以有效和令人满意的方式考虑到个人的权利，特别是对其数据的访问请求（违反GDPR第12、15和17条）。

2021年11月26日，CNIL主席决定向Clearview AI发出正式通知：1.在没有法律依据的情况下，停止收集和使用

法国境内人员的数据；2.为个人权利的行使提供便利，并满足删除的要求。

Clearview AI 原本有两个月的时间来遵照监管要求调整其行为，并向 CNIL 说明其理由。然而，它并没有对这份正式通知作出任何回应。因此，CNIL 限制委员会决定根据 GDPR 第 83 条，对其进行最高 2000 万欧元的经济处罚。

三、中国人脸识别的治理经验

（一）中国人脸识别治理的立法

中国对人脸识别治理呈现出多部法律交叉、软法硬法共治的格局。一方面，尽管《民法典》《个人信息保护法》《网络安全法》《消费者权益保护法》分别从隐私权、个人信息权益、消费者权益、合同权利等不同维度对人脸信息予以保护，但就人脸识别的治理，目前尚无统一的法律规范。另一方面，《信息安全技术 远程人脸识别系统技术要求》《信息安全技术 人脸识别数据安全要求》《公共安全重点区域视频图像信息采集规范》《公共安全人脸识别应用图像技术要求》等国家标准、行业规范相继出台，凸显了软法先行的特点。

类型	名称	主要内容
法律	《民法典》	《民法典》在第四编人格权编规定了个人信息保护的基本原则和框架，在第 1034 条将“生物识别信息”纳入个人信息范畴，并在 1035 条具体规定个人信息处理者应当遵循的原则和处理环节，包括应遵循合法、正当、必要原则，不得过度处理，应取得个人或监护人同意、公开处理信息的规则，以及明示处理信息的目的、方式和范围等

		要求。
	《个人信息保护法》	作为我国首部专门针对个人信息保护的综合性法律，《个人信息保护法》第 2 章第 28 条至第 32 条专门规定了个人敏感信息的处理规则。《个人信息保护法》第 28 条第 1 款明确将生物识别信息列为首要的敏感个人信息，以凸显其重要地位，并在该条第 2 款对敏感信息的处理设定了严格的法律规则；在第 29 条明确了**处理人脸识别信息须获得个人同意的要求，**并且明确要求国家网信部门统筹协调其他部门，针对人脸识别的应用制定专门的个人信息保护标准和规则；与《民法典》规定类似，《个人信息保护法》在第 5 条和第 6 条明确处理个人信息的原则与要求，并在 26 条强调公共场所人脸识别设备的使用目的仅限“维护公共安全”。
	《网络安全法》	该法采用专章模式对网络信息安全作出规定，将“可识别性”作为公民个人信息认定的实质性标准，明确网络运营者收集、使用个人信息的原则，采取必要措施、防止信息泄露等。 此外，该法还特别明确了用户对自己数据的“自我决定权”。该法第 43 条规定，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。
	《消费者权益保护法》	该法第 29 条第 1 款规定了经营者在收集、使用消费者个人信息情景下应当**遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意；**并在第 56 条规定若经营者存在侵害消费者个人信息的情形时，需要承担的民事、行政责任。
	《电子商务法》	该法第 23 条规定电子商务经营者在收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。
	《中华人民共和国刑法》	《刑法》将侵犯公民个人信息罪置于第四章“侵犯公民人身权利、民主权利”部分，彰显个人信息保护的重要意义。该罪构成要件包括违规向他人出售或者提供公民个人信息、违规将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人、窃取或者以其他方法非法获取公民个人信息，并将责任主体扩展至单位犯罪。
司法解释	《最高人民法院、最高人民检察院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》	**该解释扩张了个人信息的保护范围，在第 1 条规定**公民的个人信息包括身份识别信息和虽不具有身份识别功能但能够反映特定自然人活动情况的信息。 同时，**在第 9 条**规定了网络服务提供者若不履行法律、行政法规规定的信息网络安全管理义务，因故意或过失致使用户的公民个人信息泄露，造成严重后果的，面临

		以拒不履行信息网络安全管理义务罪定罪的刑事处罚风险。
	《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》	作为我国专门针对人脸识别应用进行规制的第一部法律文件。此《规定》主要针对实践中反映较为突出的人脸识别技术被滥用问题，从侵权责任、合同规则以及诉讼程序等方面规定了16个条文。第1条规定人脸信息属于《民法典》第1034条规定 的“生物识别信息”；第2条至第9条明确了滥用人脸识别技术处理人脸信息行为的侵权性质及法律责任。[26] 在主体责任上，首先，《规定》将经营场所和公共场所违法违规使用人脸识别技术，未公开人脸信息处理规则或未明示处理目的、方式、范围，未征得个人或其监护人单独或书面同意，未采取必要措施确保人脸信息安全，违背公序良俗处理人脸信息，违反合法、正当、必要原则处理个人信息等情形认定为属于侵害自然人人格权益的行为。其次，《规定》指出物业服务企业或者其他建筑物管理人不应将人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式，应为不同意的业主或者物业使用人提供其他合理的验证方式。最后，《规定》还明确了数据处理者通过合同取得的无期限限制、不可撤销、可任意转授权等权利应被认定为无效，信息处理者违反约定处理自然人的人脸信息，无论是否约定了信息删除，自然人都有权请求删除人脸信息。
部门规章	《人脸识别技术应用安全管理规定（试行）》（征求意见稿）	明确“非必要，不使用”原则，不得滥用人脸识别技术。使用人脸识别技术应告知个人获取同意，并遵循自愿原则。明确数据“最小存储”原则，除取得单独同意外，不得存储原始人脸图像。
	《商业银行互联网贷款管理暂行办法》(银保监会令2020年第9号）	第18条规定商业银行应当按照反洗钱和反恐怖融资等要求，通过构建身份认证模型，采取联网核查、生物识别等有效措施识别客户，线上对借款人的身份数据、借款意愿进行核验并留存，确保借款人的身份数据真实有效，借款人的意思表示真实。商业银行对借款人的身份核验不得全权委托合作机构办理。
	《互联网信息服务深度合成管理规定》	在第三章数据和技术管理规范中，《规定》明确深度合成服务提供者和技术支持者提供人脸、人声等生物识别信息编辑功能的，应当提示深度合成服务使用者依法告知被编辑的个人，并取得其单独同意。与此同时，深度合成服务提供者和技术支持者还应当加强技术管理，定期审核、评估、验证生成合成类算法机制机理。
	《证券期货业网络和信息安全管理办法》	在第三章投资者个人信息保护中，《办法》明确核心机构和经营机构利用生物特征进行客户身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、

[26] 参见张勇：敏感个人信息的公私法一体化保护，载《东方法学》,2022(01):66-78.

		指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息。
	《医疗卫生机构网络安全管理办法》	在第三章数据安全管理中，《办法》明确各医疗卫生机构开展人脸识别或人脸辨识时，应同时提供非人脸识别的身份识别方式，不得因数据主体不同意收集人脸识别数据而拒绝数据主体使用其基本业务功能，人脸识别数据不得用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等。各医疗卫生机构应采取安全措施存储和传输人脸识别数据，包括但不限于加密存储和传输人脸识别数据，采用物理或逻辑隔离方式分别存储人脸识别和个人身份信息等。
国家标准	GB/T35273《信息安全技术 个人信息安全规范》	该标准在 2017 年旧版的基础上，细化与完善了个人生物识别信息特殊保护，严格规范其在收集、存储、传输、共享以及转让方面的规则。 第 5.4 条规定，网络运营者收集个人生物识别信息应征得个人信息主体的明示同意。即使已取得个人信息主体的同意，网络运营者仍应仅收集达到目的所需的最少个人生物识别信息，以最大限度降低损害风险。 第 9.2 条对个人金融信息特定类别作了特殊规定：网络运营者确因业务需要，确需共享、转让的，应单独向个人信息主体告知目的并征得其明示同意、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等。
	GB/T38671-2020《信息安全技术 远程人脸识别系统技术要求》	该标准是全国首个使用人脸识别技术进行身份鉴别的网络安全国家标准。标准提出了以人脸识别为手段、以密码技术为保障的人脸识别系统，在远程可信环境中为信息系统提供用户身份标识与鉴别服务的安全框架，重点解决了前端可信环境、活体检测、服务端人脸库安全等关键环节的标准化问题。
	GB/T 41819-2022《信息安全技术 人脸识别数据安全要求》	该标准规定了人脸识别数据的安全通用要求以及收集、存储、使用、传输、提供、公开、删除等具体处理活动的安全要求。 该标准适用于数据处理者安全开展人脸识别数据处理活动。
	GB 37300-2018《公共安全重点区域视频图像信息采集规范》	该标准规定了公共安全重点区域视频图像信息采集部位和采集种类、技术要求和采集设备要求、安全要求。
	GB/T 35678-2017《公共安全人脸识别应用图像技术要求》	该标准规定了公共安全人脸识别应用中图像技术要求，具体而言包括注册图像和识别图像的格式、表情、遮挡等要求。

	《网络安全标准实践指南——人脸识别支付场景个人信息保护安全要求（征求意见稿）》	该标准针对室内外区域中的人脸识别支付场景，提出个人信息保护要求。 该实践指南不适用于用户在其自有手机或其他自有智能移动终端上进行的人脸识别支付。
行业标准	JR/T 0171—2020 中国人民银行《个人金融信息保护技术规范》	该文件主要约束金融机构和获取个人金融信息的非金融机构，在个人金融信息范围、收集使用行为、安全技术标准、机构安全岗位设置等方面作出了细致的规定。
	YD/T 4087-2022《移动智能终端人脸识别安全技术要求及测试评估方法》	该标准规定了移动智能终端人脸识别的安全技术要求和测试评估方法，包括安全目标、安全威胁分析、安全技术要求、测试评价方法和安全能力分级等。 该标准适用于支持人脸识别技术的移动智能终端，个别条款不适用于特殊行业、专业应用、其他终端也可以参考使用。
团体标准	T/TAF 077.7-2020《APP 收集使用个人信息最小必要评估规范 人脸信息》	该标准规定了移动应用软件对人脸信息的收集、使用、存储、销毁等活动中的最小必要规范和评估方法，并通过个人信息处理活动中的典型应用场景来说明如何落实最小必要原则。
其他	中国支付清算协会《人脸识别线下支付行业自律公约（试行）》	该公约指出，用户开通刷脸支付时，会员单位应以显著方式提示用户注意服务协议中与其有重大利害关系的事项，采取有效方式确认用户充分知晓并清晰理解相关权利、义务和责任，提示方式包括但不限于隐私政策、格式条款、短信提示等。

（二）中国人脸识别治理的典型案例

类型	名称	基本案情	裁判结果
民事案例	中国人脸识别第一案: 郭某诉杭州野生动物世界有限公司服务合同纠纷案[27]	2019 年 4 月浙江某大学教授郭某花费 1360 元购买了一张杭州野生动物世界“畅游 365 天”的双人卡，并确定以指纹识别的方式入园游览。同年 10 月，园方将指纹识别升级为“刷脸”入园，并要求游客录入人脸信息，否则无法入园。郭某认为人脸信息属于高度敏感的个人隐私，野生动物世界无权采集，并要求园方退卡。园方则认为，从指纹识别升级人脸识别是为了提高效率。双方协商无果，郭某将野生动物世界告上法院。	一审判令野生动物世界赔偿郭某合同利益损失及交通费共计 1038 元。删除郭某办理指纹年卡时提交的包括照片在内的面部特征信息，驳回郭某的其他诉讼请求。 二审维持一审判决第一项第二项，即判决野生动物世界赔偿郭某合同利益损失及

[27] 参见杭州市富阳区人民法院（2019）浙 0111 民初 6971 号判决书、浙江省杭州市中级人民法院（2020）浙 01 民终 10940 号判决书。

			交通费共计 1038 元，判决生效十日内履行，删除郭某办理指纹年卡时提交的包括照片在内的面部特征信息。 二审新增判决：删除指纹识别信息，判决生效十日内履行，驳回郭某的其他诉讼请求。
	孙长宝与北京搜狐互联网信息服务有限公司等人格权纠纷案[28]	原告孙某在百度网站搜索其名字，发现百度网站非法收录并置顶了原告在“chinaren 校友录”网站上传的个人账户头像（个人证件照）。	一审法院判决被告北京百度网讯科技有限公司向原告孙某赔偿经济损失 1 元；被告北京百度网讯科技有限公司向原告孙长宝赔偿维权费用 40 元。
	刘嘉龙与沈榕隐私权纠纷案[29]	刘某与沈某系邻居关系，沈某在自家房门外墙上安装了一款有人脸识别和录像功能的智能门铃。原告主张智能门铃对其一家进出家门和在走廊通道内的活动进行了长时间、连续的拍摄，并自动上传到 360 门铃云端，事实上产生了进行持续性、高强度、近距离监视拍摄的结果。	二审法院撤销原判，认为沈某的门口系刘某出入家门的必经之地，沈某安装在门外的门铃摄像头对刘嘉龙及其家人的出行规律、人员流动等进行了记录，该处虽处于公共楼道，但对于刘某及其家人的正常生活产生了一定影响，应予以拆除。同时驳回刘某的其他诉讼请求。
	朱莎丽与中国人民银行衢州市中心支行、深圳前海微众银行股份有限公司名誉权纠纷案[30]	原告朱某因被案外人郭某欺骗完成了借 款刷脸认证，导致存在逾期未还款记录，产生不良征信记录。	一审法院认为被告前海微众银行报送涉案逾期信息是正常履行职务的行为，并非违法行为该行为不存在侵犯原告民事权利的主观故意和过错。虽然刑事判决书认定该笔贷款不是由原告操作，但被告对郭某使用

[28] 参见北京互联网法院（2019）京 0491 民初 10989 号孙长宝与北京搜狐互联网信息服务有限公司等人格权纠纷一审民事判决书。

[29] 参见北京市第二中级人民法院（2020）京 02 民终 1641 号刘嘉龙与沈榕隐私权纠纷二审民事判决书。

[30] 参见衢州市柯城区人民法院（2019）浙 0802 民初 5880 号朱莎丽与中国人民银行衢州市中心支行、深圳前海微众银行股份有限公司名誉权纠纷一审民事判决书。

			原告手机申请贷款的行为无法预见、无法预知，为确认申请贷款人的身份，被告已经发起了人脸识别验证，且原告本人配合完成了动态指令，被告已经尽到了审查义务。因此驳回原告的诉讼请求
检察公益诉讼案例[31]	江苏省无锡市新吴区人民检察院督促保护服务场所消费者个人信息行政公益诉讼案	江苏省无锡市新吴区某健身房使用具有人脸识别、指纹识别等功能的信息管理系统，强制要求会员刷脸或录入指纹进入。由于该管理系统采用分级分层、前后端分离等技术，消费者在前端平台界面仅能看到被采集的个人身份信息，未被告知个人信息收集清单及权限。在部分会员明确拒绝人脸采集识别后，该健身房擅自将会员办卡时提供的照片录入系统作为刷脸进出凭证，且在会员要求删除照片等信息时，以无管理权限为由拒绝删除，其行为侵害众多消费者合法权益，损害社会公共利益。	检察院审查认为，消费者的人脸、指纹等属于生物识别类敏感个人信息，涉案服务场所系公共场所，非维护公共安全必需且未取得消费者单独同意，强制采集、非加密传输、违法存储、未定期删除敏感个人信息的行为，损害了众多消费者合法权益。新吴区院于2022年8月12日向新吴区市场监督管理局制发行政公益诉讼诉前检察建议，督促对涉案服务场所依法处理，切实履行保护消费者合法权益的职责；开展行业规范整治，加大监管力度，建立长效机制，防范类似违法行为发生。
	湖南省长沙市望城区人民检察院督促保护个人生物识别信息行政公益诉讼案	湖南省长沙市望城区卫生健康局（以下简称区卫健局）为推进数字化门诊建设，自2019年7月12日起，要求长沙市望城区辖区内17家医疗卫生机构陆续使用电子签核系统推送疫苗接种知情告知书，疫苗受种者或监护人点击“同意”时系统自动采集指纹和人脸识别信息，收集电子数据的存储及主机均由各社区卫生服务中心管理。截至2022年3月11日，上述机构共收集83万余条涉及指纹、人脸识别等个人生物识别信息。	检察院审查认为，望城区17家医疗卫生机构违反个人信息处理的合法、正当、必要和诚信原则，过度收集服务对象指纹和人脸等个人生物识别信息，未按要求解决电子签核系统的弱口令、数据未加密等安全漏洞，未能防患未经授权的访

[31] 参见《最高人民检察院发布8件个人信息保护检察公益诉讼典型案例》，2023年3月30日发布。

			问及个人信息泄露、篡改、丢失等高风险，未落实网络安全等级保护制度要求，对敏感个人信息保护的内部管理不到位。望城区卫健局和区公安分局对上述医疗卫生机构收集、处理敏感个人信息活动未尽到监管职责。
	浙江省湖州市检察机关诉浙江G旅游发展有限公司侵害公民个人信息民事公益诉讼案	A景区由浙江G旅游发展有限公司（以下简称G公司，其控股股东是某国有公司）负责实际运营。2020年7月，A景区通过招标委托浙江H科技有限公司（以下简称H公司）建设完成人脸识别系统，并投入运行。系统使用期间，A景区在采集游客人脸信息时未依法履行告知义务，存在强制要求购票游客录入人脸信息、“刷脸”入园的情形，且景区未对采集到的人脸信息定期予以删除，致使游客个人信息被侵害，损害了社会公共利益。	浙江省院、湖州市院、南浔区院会同当地旅游度假区管委会、G公司等景区运营主体，同时邀请了浙江省消费者权益保护委员会相关工作人员和法律专家，围绕涉案人脸信息被侵害问题召开磋商会，就G公司删除景区前期采集储存的人脸信息数据，规范人脸信息的收集和使用等事项达成共识。同时，湖州市院与湖州市网信办开展磋商，网信部门对G公司提出整改要求。同年11月18日，湖州市院向G公司制发检察建议，督促G公司积极整改，确保依法运营。
法案例	小鹏汽车违法采集人脸信息	小鹏汽车购买具有人脸识别功能的22台摄像设备安装在其旗下门店，用于采集消费者的面部识别数据，并将数据上传至后台系统，通过算法对面部数据进行识别计算，以此进行门店的客流统计和客流分析，包括进店人数统计、男女比例、年龄分析等。	上海市徐汇区市场监督管理局责令当事人改正上述违法行为，并决定罚款人民币100000元。

	“ZAO”换脸软件过度收集个人信息[32]	2019年，一款名为“ZAO”的AI换脸软件在国内爆火，用户可以通过APP实现换脸自由，但其用户协议中要求获得用户人脸照片“完全免费、不可撤销、永久、可转授权和可再许可的权利”，ZAO及其关联公司有权对用户上传的内容进行全部或部分的修改并享有修改后的内容著作权。这一系列规定涉嫌过度收集用户个人信息与转嫁侵权责任，具有较高的法律风险。	
刑事案例[33]	李某侵犯公民个人信息案	被告人李某，某网络科技有限公司软件开发人员。 2020年6月至9月，李某制作了一款可以窃取安装者手机内的照片的软件。当手机用户下载安装该软件打开使用时，软件就会自动获取手机相册的照片并且上传到李某搭建的服务器后台。李某将该软件发布在暗网某论坛售卖，截至2021年2月9日，共卖得网站虚拟币30$。后李某为炫耀技术、满足虚荣心，又将该软件伪装成“颜值检测”软件，发布在某论坛供网友免费下载安装，以此方式窃取安装者手机相册照片1751张。其中，含有人脸信息、姓名、身份证号码、联系方式、家庭住址等100余条公民个人信息。 2020年9月，李某又用虚拟币在该暗网的论坛购买“社工库资料”并转存于网盘。2021年2月，李某为炫耀自己的能力，明知“社工库资料”含有户籍信息、车主信息等，仍将网盘链接分享到“业主交流”QQ群（150名成员）。经去除无效数据、合并去重后，该“社工库资料”包含公民个人信息共计8100余万条。 2021年3月9日，公安机关将李某抓获。经侦查，因“社工库资料”内容庞大且存储于境外网盘，未查到有人下载使用。	奉贤区人民法院审理认为，李某具有坦白情节，且自愿认罪认罚，对其依法从宽处理，以侵犯公民个人信息罪判处李某有期徒刑三年，缓刑三年，并处罚金。

中国人脸识别技术和应用发展不断成熟，需要技术提供者、产品/服务提供者、服务应用者共建一个良性的生态治理

[32] 参见王四新：《“ZAO”背后的社会管理难题》，载《环球时报》，2019-09-02(015).
[33] 参见《最高人民法院关于发布第35批指导性案例的通知》，2022年12月26日公布。

环境，虽然中国目前尚未开展生态治理工作，但在近期新出台的规章中体现了未来生态治理的趋势。国家网信办、工业和信息化部、公安部联合发布《互联网信息服务深度合成管理规定》，将深度合成服务提供者和技术支持者都纳入到了监管对象中，并且强化深度合成服务的使用者与应用程序分发平台这类主体的信息安全责任义务。

第三章　人脸识别产业法律治理图景

一、人脸识别产业生态治理的基本原理

人脸识别产业生态治理，旨在减少“人—技术—社会”的割裂，主张技术、专业人士、各种组织都是科技系统中的互动实体，发挥着独立作用，从而共同构成了产业生态的“无缝之网”（Seamless Web）。立基于此的人脸识别产业生态治理，在科技系统的建构和解构的双向运作中，抽离出人脸识别的行动者、场景、算法、数据等系统组件，以人脸识别产业生态的人类行动者为中心，凭借共同优化原则，实现法律和技术的同频共振。

《人脸识别技术应用安全管理规定（试行）（征求意见稿）》（以下简称《人脸识别管理规定》）恰恰建立在这一范式之上。该规定第一条开宗明义地将立法依据扩展到《网络安全法》《数据安全法》《个人信息保护法》，充分说明其不再是根据《个人信息保护法》第 62 条“针对人脸识别制定专门的个人信息保护规则、标准”授权而制定的下位法，而是从宏观维度对人脸识别技术的系统性规范，相关条款的展开更鲜明体现了不同参与者、多种场景和细化技术标准相呼应的生态治理方法。

二、人脸识别技术生态治理

（一）技术提供者的数据安全义务

人脸识别技术以数据为驱动力。典型的人脸识别系统包括“训练”和“识别”两个部分，其中训练部分主要包括人脸数据库、人脸检测与定位、人脸图像预处理、特征提取与选择、训练五个环节；识别部分包括人脸信息采集、图像像素数据化、数据库比对识别等环节。据此，人脸识别的技术提供者在数据训练、存储、传输、删除等环节均应具有保证技术研发可靠安全的义务。[34]

1.训练环节的数据安全义务

技术提供者在训练、验证和测试人脸数据库时，应遵守适当的数据治理和管理规范。应特别关注：（a） 有关设计选择；（b） 数据采集；（c） 数据准备处理操作，例如注释、标记、清洗、充实和汇总；（d） 制定有关数据应衡量和代表的信息的假设；（e） 事先评估所需数据库的可用性、数量和适用性；（f） 对可能存在的偏见进行检查；（g） 确定任何可能的数据空白或不足，以及如何解决这些空白和不足。技术提供者应当确保训练、验证和测试数据库是有代表性的、没有错误且完整的。它们应具有适当的统计属性，特别是拟识别人群有关的属性。

2.存储环节的数据安全义务

技术提供者应采取加密或去标识化的安全技术措施。例如，采取技术措施生成不可逆的可更新的人脸特征后再存储，

[34] 参见中国信通院：《人脸信息处理合规操作指南》。2022 年 1 月。

可通过特征提取算法、密码学技术、假名标识符技术等技术实现。再如，对不同用户采用不同密钥的方式对人脸信息加密，将用户本人密钥存储在安全设备中；对不同设备采用不同密钥的方式对人脸信息加密，密钥与设备唯一绑定；在不同应用场景采用不同的密钥对人脸信息加密，不同密钥间隔离存储。此外，存储环境应提供分类管理的机制，保证人脸信息与人脸信息主体的身份相关信息分开存储与管理。例如，可采用对人脸信息与身份信息设置不同访问权限控制、隔离的物理机房或在独立数据系统中存储、两套数据有解耦等隔离手段。

3.传输环节的数据安全义务

技术提供者应确保传输环境安全，建立安全的人脸信息传输通道，在传输或接受传输前，应对通信双方的真实身份进行鉴别和认证，并采用防火墙、事前检测等安全技术或设备，确保人脸信息在安全的通道中传输。技术提供者应确保传输过程安全，人脸信息及识别决策结果的传输应有安全防护措施，如加密传输、数字签名、网络安全检测、逻辑保护等，确保人脸信息和识别决策结果的完整性和保密性，不被窃取或篡改。

4.删除环节的数据安全义务

技术提供者应确保做到及时删除人脸信息处理。同时，系统应具备删除后防止恢复的技术手段，宜采取慢速格式化、

Secure-Delete 指令、Dod 5220.22-M、Gutmann 算法等方法。

（二）技术提供者的算法可信义务

人脸识别技术作为一种高风险算法，技术提供者应当在技术研发伊始，就将算法可信理念植入需求分析和系统详细设计等规划设计的关键环节中，从而使后续的研发测试和运营能够始终符合可信人工智能的核心要求。

1.算法准确性、鲁棒性、安全性义务

技术提供者可以通过备份或故障安全计划等技术冗余解决方案来实现其鲁棒性，并应确保在投入使用后仍会持续学习的开发方式，使之用作未来操作输入的输出而产生的可能有偏差的输出（“反馈循环”）并且采取适当的缓解措施。同时，对于未经授权的第三方利用系统漏洞来更改其使用或性能的尝试，人脸识别系统应具有复原性，可以应对系统或系统运行所处的环境内可能发生的错误和故障，特别是由于其与操作人员或其他系统的相互作用所致。最后，技术提供者还可以采取对抗训练，以预防试图操纵训练数据集的攻击措施，防范导致模型出错的输入或模型缺陷。

2.算法安全评估、审计、备案的义务

为明确责任方面，技术提供者应定期审核、评估、验证人脸识别算法的机制机理，全面审计人脸识别系统的实现流程，提升系统可追溯能力，确保系统及服务的源头可信。审计主要包括模型训练和模型评估。其中，模型训练环节是为

人工智能系统赋予“智能”的关键，对硬件平台、软件框架、算法选择、调参过程等训练的关键环节进行全面审计，能够帮助对人工智能系统进行追溯。模型的评估很大程度上能够反映人工智能系统在实际应用中的性能表现和泛化能力，标准严谨的评估过程往往能够发现错误，衡量模型质量，并判断其是否能满足设计要求，帮助回溯系统实现过程中存在的问题从而进行不断改进，因此需要详细审计模型在验证集和测试集上的指标表现和变化。[35]在必要时，可以通过算法备案，落实上述算法安全评估和审计义务。

三、人脸识别产品/服务生态治理

人脸识别产品/服务提供者是人脸识别产业的中坚力量，其上连接技术提供者，下启人脸识别服务应用者，发挥着承上启下的枢纽作用，构成了人脸识别产业治理的关键一环。据此，人脸识别产品/服务提供者应承担如下义务:

（一）产品/服务提供者的质量管理义务

人脸识别产品/服务提供者作为供应商应建立质量管理体系，包括（a）监管合规性策略，包括合规性评估程序和系统修改管理程序；（b）用于人脸识别产品/服务的质量控制和质量保证的组织和程序;（c）应用的技术规范和标准;（d）数据治理的组织、系统和程序，包括数据收集、数据分析、数据标记、数据存储、数据过滤、数据挖掘、数据聚合与数

[35] 中国信息通信研究院、京东探索研究院：《可信人工智能研究报告》。

据删除；（e）风险管理系统；（f）售后监测系统；（g）严重事故和故障的应急程序；（h）支持监管机构监督和执法系统；（i）记录所有相关文件和信息的系统和程序；（j）问责制框架，用于明确管理层和其他员工的责任。

（二）产品/服务提供者的人工监督义务

为防范和降低风险，产品/服务提供者应使用适当的人机界面工具，使人脸识别系统在运行过程中可以由人介入和监督。为此，人脸识别系统应具备人脸信息访问控制功能，对于人脸信息的复制、下载等重要操作应具备严格的控制措施，应具备要求特定人员执行、操作过程验证身份、及时收回执行人员操作权限的功能。同时，负责监督的人员应当充分了解人脸识别的功能和局限性，能够对其运行进行适当监控，以便尽快发现并解决功能异常和意外性能的故障；并能意识到自动依赖或过度依赖人脸识别系统产生的“自动化偏差”以及其他风险，可以采取快速接管或通过“一键关停”的方式终止服务。

（三）产品/服务提供者的算法日志记录义务

产品/服务提供者应当确保人脸识别系统具有系统运行时自动记录事件（日志）功能。日志记录应确保人脸识别系统在其整个生命周期中的功能可追溯性水平，并包括如下内容：（a）记录系统每次使用的时间（每次使用的开始日期和时间以及结束日期和时间）；（b）系统已针对其检查输入

数据的参考数据库；（c）搜索导致匹配的输入数据；（d）确定参与结果验证的自然人的身份。

（四）产品/服务提供者的起草技术文件的义务

产品/服务提供者应确保其系统在投入使用之前符合法律和标准，为此，其应当编制技术文件，并向国家监管机构提供所有必要信息，以评估其合规性。

四、人脸识别服务使用生态治理

作为面向公众提供的主体，服务使用者是人脸识别的终端，承担着最终责任。据此，人脸识别服务使用者负有如下义务:

（一）服务使用者的个人信息保护义务

为了保护个人信息，服务使用者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，方可使用人脸识别技术处理人脸信息。实现相同目的或者达到同等业务要求，在同等实现成本的情况下存在其他非生物特征识别技术方案的，应当推荐使用非生物特征识别技术方案。

服务使用者需要保证在与用户交互时用户个人信息权利得以保障。在收集人脸信息时，应提供单独弹窗、单独提示等方式进行告知的功能，供人脸信息处理者用于告知收集人脸信息事宜以及处理人脸信息保护政策；应提供便于查看人脸信息保护政策的功能；应提供用户撤回同意、单独同意或拒绝的功能，并且在用户单独同意后才进行收集；应能够

针对意外收集的非注册用户人脸信息进行及时删除或匿名化处理。在存储人脸信息时，应确保能够到期自动删除。此外，应确保人脸信息主体行使个人信息权利能够及时响应。

此外，根据《个人信息保护法》第55条、56条的规定，服务使用者应对人脸识别开展个人信息影响评估，分别从人脸信息的处理目的、处理方式等是否合法、正当、必要；对“影响个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“个人财产受损”等权益影响及安全风险；以及所采取的保护措施是否合法、有效并与风险程度相适应等方面形成个人信息影响评估报告。

（二）服务使用者的算法解释义务

服务使用者是人脸识别算法的首要解释义务人。在卢米斯诉威斯康星州一案（Loomis v. Wisconsin）中，卢米斯通过辩诉交易承认了没有得到主人同意的情况下驾驶摩托车和企图逃离交管员管控这两项轻罪，最终却被判决6年徒刑和5年延期监督（Extended Supervision）。这是因为在量刑阶段，威斯康星惩教署引用了“罪犯矫正替代性制裁分析管理系统”（COMPAS）的风险评估结果，将卢米斯的危险等级认定为“高风险”。卢米斯向初审法院提交了定罪后的缓解动议，认为被告人有权知道被控告的理由，法院依据COMPAS的评估对其加以判决侵犯其正当程序权利。[36]在“算

[36] Loomis v. Wisconsin, Petition for certiorari denied on June 26, 2017, http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/.

法服务应用者”和“算法技术提供者”二分架构下，开发COMPAS系统的Nortpointe公司并不负有解释算法的义务，而威斯康星惩教署作为决定卢卡斯个人信息使用方式和用途的控制者，应说明其算法原理。与此类似，在我国健康码的场景下，腾讯、蚂蚁金服等技术提供者对民众无解释义务，相反，使用健康码的政府机关须承担算法解释的义务和解释不能的后果。

服务使用者的解释义务包括如下方面:

1.人脸识别数据的解释义务

个人有权要求人脸识别应用者在合理范围内，展示输入算法变量(人脸信息)的权利。此处输入变量的“合理范围”，由相应算法所处理的个人信息所准确界定。在某种意义上，这可视为个人信息保护中已有规定的延伸——解释主体需告知用户，收集或处理个人信息的目的，是用于优化上述目标，进而达到采用算法的目的。如果算法之输入包含非个人信息变量，解释主体可灵活决定是否展示。在展示过程中，主体既可以采取简单的文字列表方式，也可以采取符合认知特点的可视化方式。对儿童、老年人或残疾人等或有不便的群体，鼓励专门设计符合认知特点的展示方式。

2.算法逻辑的解释义务

个人有权要求人脸识别使用者在合理的范围内，说明相应算法变量（人脸信息）对自动化决策结果产生何种影响的

权利。在具体实施层面，可作如下四方面展开。（1） 这里的“相应变量”仅包括上一层次已经涵盖的个人信息中参与实际分析推断的信息；（2）决策结果需要在具体场景中界定，包括但不限于诊疗结果、信用分数、信贷决定，等等；（3）“影响”有必要进一步细化。在输入（个人信息）与输出（决策结果）均可排序的场合，[37]应用者可以展示数字化变量间的“正相关”与“负相关”，说明当输入信息（在一定范围内）上升/下降时，输出结果的高低变化。而在输入或输出无法排序的场合，可允许其灵活处理，既能显示全局相关，也可展示局部相关，只需说明相应相关性的作用范围即可。（4）使用者应选择用户友好形式解释说明。针对个人，应帮助其理解特定信息如何影响决策结果，从而成为后续知晓并对抗算法歧视问题的重要依据；针对公众，应帮助其了解富含不同社会价值的信息类型以何种方式影响输出，有利于更精细地评估算法是否恰当平衡了各方社会利益。在解释理论层面，此处要求的统计相关解释，可作为过于灵活、难以准确界定的实用主义解释的补充。

3.算法评估的解释义务

“算法审计”要求应用者针对模型、数据和决策结果留有明确记录，从而在变动对应因素后，使算法输出特定决策，以备监管部门、第三方机构或法院的核查，最终判断算法是

[37] 可以排序的情形包括：数字变量；二元变量（例如男女，可用一对数字量化，数字的具体大小不重要）；以及，其它具备自然排序的变量（例如信用评级的分等）。

否将会导致歧视性或其他不当后果。[38]与之前两个层次的权利不同，该权利更倾向于事后的验证、测试和问责。为此算法主体应当建构出一套具有交互诊断分析能力的系统，通过检视输入数据和重现执行过程，来化解人们可能的质疑。“反事实解释”成为这一层面解释权的核心。

（三）服务使用者的算法备案义务

作为一种高风险算法，人脸识别应用者应当履行相应的备案义务，即将应用者的名称、服务形式、应用领域、人脸识别算法类型、人脸识别自评估报告、拟公示内容等信息提供给监管机构。算法备案不是“行政许可”或“行政确认”，其目的不在于为应用者设定权利和义务，而是基于实现算法透明的目的，为后续政府政策制定、执法活动提供信息，属于“行政告知式备案”。当备案信息作为监管事实的基础时，备案则具有了监督功能，此时监管机构可在后续算法的实质审查过程中，具体判断应用者的行为是否符合备案内容，若不符合，则有权要求其改正。

《人脸识别管理规定》第十六条明确规定了备案义务。其规定：“在公共场所使用人脸识别技术，或者存储超过1万人人脸信息的人脸识别技术使用者，应当在30个工作日内向所属地市级以上网信部门备案。申请备案应当提交下列材料：（一）人脸识别技术使用者及其个人信息保护负责人

[38] 沈伟伟：《算法透明性的迷思》，《环球法律评论》2019年第6期。

的基本情况；（二）处理人脸信息的必要性说明；（三）人脸信息的处理目的、处理方式和安全保护措施；（四）人脸信息的处理规则和操作规程；（五）个人信息保护影响评估报告；（六）网信部门认为需要提供的其他材料。”

（四）服务使用者的守门人义务

当服务使用者是提供第三方 APP 的接入（包括分发、下载、更新等），或向第三方 APP 运营提供技术资源和信息收集渠道，以及提供市场和用户触达中介服务的操作系统、应用程序分发平台、大型平台型 APP 时，鉴于其控制了技术环境和运营环境，对人脸识别服务的技术设置和条款条件具有决定性作用，其还应承担“守门人”义务。为此，若第三方 APP 涉及人脸识别应用时，服务应用者（1） 应当制定符合法律法规要求的准入规范，不得为不达标的第三方 APP 使用其所管控的通道、空间和其所提供的服务；（2） 应利用必要的技术手段，对使用其所管控的通道、空间和使用其所提供的技术服务的第三方 APP 人脸识别行为进行监管，必要时提出警告和整改意见；（3） 建立相关的投诉受理和处置机制；（4） 配合监管机构对违反法律法规的第三方 APP 的调查处理。

五、人脸生成合成生态治理

（一）技术提供者的训练数据来源合法义务

训练数据是指用于训练 AI 模型，使其做出正确判断的

已标注数据/基准数据集，技术提供者对数据来源的合法性负责。训练数据的来源主要包括：从公开数据集获取、从第三方购买、自行收集、使用合成数据。

从训练数据来源维度，针对不同来源的训练数据，技术提供者的合法义务有不同侧重。**第一，从公开数据集获取。**技术提供者主要承担个人信息保护义务，需满足使用公开个人信息的要求，除非个人信息主体明确拒绝或处理该信息会侵害个人信息主体重大利益，原则上技术提供者收集、使用公开的个人信息无须征得个人信息主体的同意，但收集、使用应当在合理限度内。**第二，从第三方购买。**（1）技术提供者在购买第三方数据集前可查看开源数据集提供方的公开信息披露，重点核查其中是否包含敏感信息或隐私；（2）技术提供者可与第三方签订协议时明确责任风险，要求第三方对数据做无瑕疵或者不侵权保证、确保授权权利的完整合法；（3）涉及个人信息的相关数据，技术提供者要求第三方在传输前进行匿名化处理；（4）技术提供者应对第三方提供的数据权属文件进行抽查，核查数据的原始权利主体、授权链条、授权范围、是否留存违法违规和可能侵权内容；（5）技术提供者需遵循与第三方协议中目的限制的规定。**第三，自行收集。**不得窃取或者以其他非法方式收集数据，技术提供者使用爬虫、Open API 等技术手段爬取数据的：（1）应当遵守合理、正当的数据爬取协议；（2）在爬取对象上，

避免从已声明禁止第三方爬取数据的网站爬取数据；（3）在爬取方式上，不得强行绕过或破坏技术措施来爬取数据、应控制访问规模、访问频次，不得干扰网络服务的正常功能；（4）在爬取内容上，避免未经权利人授权，秘密爬取他人拥有著作权的作品、未合法公开的个人信息、他人受法律保护的商业秘密等数据。**第四，合成数据。**技术提供者使用合成数据，应验证合成数据的准确性，将其与人工注释的真实数据模型进行比较以确保结果的准确性。

从可能侵害权益的维度，技术提供者的训练数据来源合法义务主要包括个人信息保护义务、反不正当竞争法上的义务、不侵犯知识产权、肖像权等他人合法权益的义务等。（1）训练数据包含个人信息的，应当履行告知义务，并征得个人信息主体同意或者符合法律法规规定的其他情形。（2）训练数据去标识化义务。训练数据中包含个人信息的，技术提供者应主动删除标识符、采取匿名化措施。（3）保障个人信息主体查阅、更正和删除权等权利。向用户提供查阅、更正、删除个人数据的选项。（4）用以训练的数据不含有侵犯商业秘密的内容。（5）用以训练的数据不含有侵犯知识产权、肖像权、隐私权等他人合法权益的内容。

（二）技术提供者的训练数据质量保障义务

（1）使用高质量训练、验证和测试的数据集，技术提供者应对数据集规模、均衡性、准确性、与算法任务相关程

度等指标进行测试。（2）技术提供者应保证训练数据的真实性 、准确性、客观性、多样性。（3）标注规则。为保证训练的算法模型的准确性，技术提供者应确保对训练数据的人工标注标准一致、标注内容正确，应制定清晰、具体、可操作的标注规则，对标注人员进行必要培训，抽样核验标注内容的正确性。（4）防止歧视。在训练数据选择过程中，技术提供者应采取措施防止出现种族、民族、信仰、国别、地域、性别、年龄、职业等歧视。

（三）技术提供者的数据安全义务

技术提供者应加强训练数据管理，采取必要措施保障训练数据安全，防止训练数据污染、训练数据泄漏等安全问题。（1）技术提供者应具有数据安全保护机制，保障数据的保密性、完整性、可用性，可采用的方式包括但不限于：加密算法、完整性校验。（2）技术提供者应对所使用的数据进行安全检测，对检测到的被污染数据进行修复或过滤，并保留检测处置记录。

（四）技术提供者的算法义务

（1）算法伦理与算法公平。在算法设计、模型生成和优化的过程中，采取措施防止出现种族、民族、信仰、国别、地域、性别、年龄、职业等歧视。（2）模型优化训练义务。对于运行中发现、用户举报的不符合法律法规要求的生成内容，除采取内容过滤等措施外，技术提供者应通过模型优化

训练等方式防止再次生成。（3）信息安全管理义务。技术提供者应通过加强技术管理等方式，定期审核、评估、验证生成合成类算法机制的正当机理。（4）算法备案义务。技术提供者应对算法进行备案，并在其对外提供服务的网站、应用程序等的显著位置标明其备案编号、提供公示信息链接。（5）算法安全评估义务。技术提供者应依法自行或委托专业机构，对其提供的具有生成或编辑人脸功能的工具开展安全评估。（6）算法透明度义务。技术提供者应提供可以影响用户信任、选择的必要信息，包括预训练和优化训练数据的来源、规模、类型、质量等描述，人工标注规则，人工标注数据的规模和类型，基础算法和技术体系等。

（五）产品/服务提供者的内容安全义务

1.用户输入信息的审核义务

为从源头上降低人脸生成合成技术被滥用的可能性，产品/服务提供者应对用户使用产品/服务过程中输入的信息进行审核。一般而言，在人脸生成合成场景下，用户输入信息包含原始的人脸图像视频素材和生成指令两类内容，分别对应着不同的审查义务。

就人脸图像视频素材而言，产品/服务提供者应当通过显著提示，确保对该素材的使用已征得相应权利主体的同意。一方面，这包含图像视频著作权人的授权；另一方面，由于人脸图像视频素材中包含的人脸信息属于敏感个人信息，对

该信息的处理还应根据《个人信息保护法》的规定获得信息主体的单独同意。

就生成指令而言，其一般以文字形式呈现，产品/服务提供者应当通过技术或人工方式对用户的生成指令进行审查。例如，产品/服务提供者可以通过敏感词筛查机制，对用户生成指令中的违禁词汇进行识别及过滤，以此预防系统根据用户的不当指令生成不当内容。除此之外，鉴于实践中用户还可能通过暗示性表达引导系统生成不当内容，产品/服务提供者可尝试利用模型的推理判断机制对指令的实质含义进行审查。

2.用户输入信息的保护义务

产品/服务提供者应对用户使用产品/服务过程中输入的信息履行保护义务，包括但不限于：（1）仅可将用户输入信息用于提供该人脸生成合成产品/服务目的；（2）如将用户输入信息用于其他目的，特别是将其用于算法、模型训练，应额外获得用户的同意或具备其他合法性基础；（3）对用户输入信息承担保密义务，除却业务转让、法律要求等合理必要情形，不应将用户输入信息披露给第三方，同时，还应在服务条款中对信息披露范围及情形作出明确说明，并要求信息接收方承诺对用户输入信息采取同等水平的保护措施；（4）采取相应技术措施和其他必要措施，防止用户输入信息遭到篡改、破坏、泄漏或非法获取、非法利用。

3.用户生成合成结果的审核义务

产品/服务提供者应对用户使用产品/服务所生成合成的结果进行审核，过滤反动、色情、血腥、暴恐等不当内容。鉴于产品/服务提供过程中生成合成的人脸图像、视频数量较大，人工审核负担较重、成本较高，产品/服务提供者可采取“以技术审核为主，以人工审核为辅”的审核方式。即首先对生成合成的人脸图像、视频采用技术审核，分别就其中包含的文本、图像画面等内容进行审查。对此可建立“黑白名单”机制，由技术自动屏蔽属于不合规的黑名单中所包含的生成合成内容，自动通过属于合规的白名单中所包含的生成合成内容。在此基础之上，再将技术审核无法判断的内容交由人工审查，在节省审核成本的同时提高审核准确率。

（六）产品/服务提供者的内容标识义务

1.隐性标识义务

产品/服务提供者应当采取技术措施，在用户生成合成内容之上添加不影响用户使用的标识，并按照相关规定保存日志信息。添加隐性标识的主要目的在于确保日后实现对生成合成内容的识别和追溯，实践中的可行方案包含添加数字水印、在文件元数据中嵌入标识信息等。

2.显性标识义务

产品/服务生成合成内容可能导致公众混淆或者误认的，产品/服务提供者应当在生成合成内容的合理位置、区域进行

显著标识。添加显著标识的主要目的在于使得公众浏览信息时即知悉该内容为非真实内容，防止公众混淆误认。对于如何判断“可能导致公众混淆或误认”，应当根据风险等级对应用场景进行区分。例如，提供人脸美颜修饰功能的合成服务为低风险场景，如对其添加显著标识，反会令其用户体验显著下降，因而无需添加显著标识。又如，人脸生成、人脸替换、人脸操控等生成合成非真实人脸图像或视频的场景为高风险场景，可能会使公众对现实中的个人产生错误认知，或误认拟真人物为现实中真实存在的个人，因此应当在该生成合成内容之上添加显著标识。至于显著标识的形式，采用文字或图形等方式均可，尺寸和位置亦可根据个案定制化选择，达到常人可辨识的程度即可。

（七）产品/服务提供者的用户管理义务

鉴于人脸生成合成产品/服务被不当利用的风险较大，产品/服务提供者应当对用户实施一定的管理，包括但不限于：（1）基于移动电话号码等方式，对用户进行真实身份信息认证，以便后续在发生滥用事件时迅速实现追责；（2）发布产品/服务使用指引，引导用户正当使用产品/服务；（3）设置投诉反馈渠道，依法对平台上的侵权内容采取删除、屏蔽、断开链接等处置措施；（4）对违规使用产品/服务的用户账号采取警示、限制功能、暂停服务、关闭账号等措施，留存相关记录并依法向有关主管部门报告。

（八）服务应用者的正当使用义务

服务应用者应依法正当使用人脸生成合成产品/服务，包括但不限于：（1）确保其在使用产品/服务过程中输入的信息具备充分授权，不侵犯他人合法权益，不包含违法不良内容；同时应避免输入商业秘密、核心数据、重要数据等敏感内容；如前述输入信息中包含个人信息，应依法征得相关主体的同意或具备其他合法性基础；（2）不得将产品/服务用于非法目的，包括但不限于自行或帮助他人制作、复制、发布、传播法律法规所禁止的信息，或利用产品/服务从事危害国家安全和利益、侵害社会公共利益、侵犯他人合法权益等违法活动；（3）鉴于产品/服务本身可能会由于技术缺陷等原因生成合成包含歧视、色情、暴力等不良导向内容，用户应自行对生成合成内容进行审查，确保不包含违法不良内容后再进行传播利用；（4）不得采取技术手段删除、篡改、隐匿生成合成内容的相关标识；（5）不得通过网络漏洞、恶意软件或其他非法手段干扰产品/服务的正常运行。

第四章　人脸识别产业的最佳实践

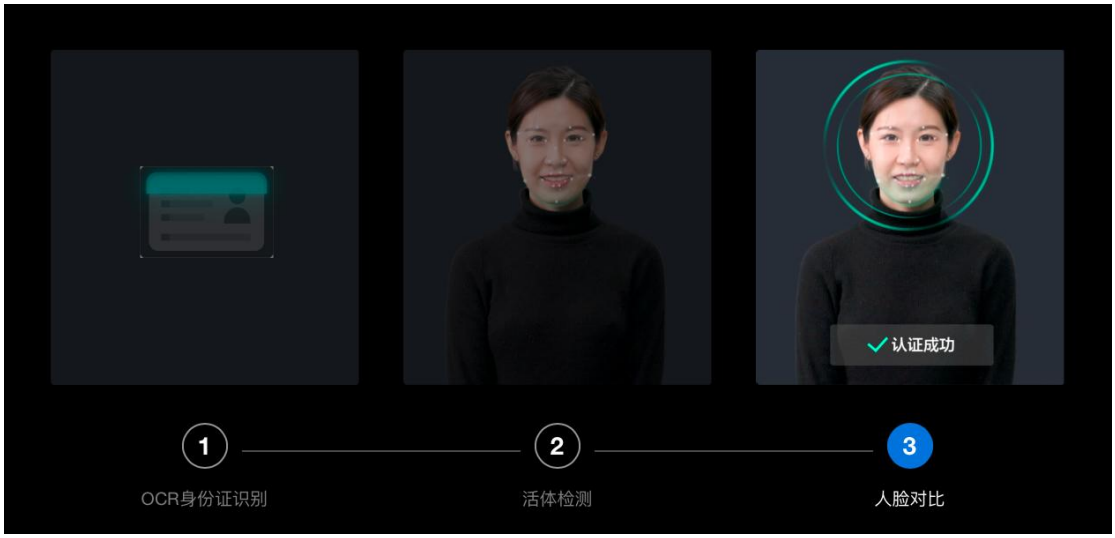
案例一：以权威数据源为基础进行人脸识别

百度智能云人脸实名认证提供活体检测、人脸比对、身份证 OCR 等功能，直连公安、运营商等权威数据源，提供整套集成及运维方案，满足金融、保险、医疗、政务等业务要求的远程人脸身份核验的安全性、通过率、易用性，保障上千家企业业务运转。

在银行、保险等高危金融场景中，为响应银保监会的要求，以及用户个人资金的安全性保障，授信、转账、投保、回访、保全等业务流程均需要验证操作者身份的真实性。黑产攻击手段日益进化，给业务风控也带来了诸多挑战。炫瞳活体这类最新基于光线的活体检测技术，用户体验优，同时兼顾了业务安全性；安全加密及大数据风控能够对 SDK 端传入的本地环境扫描设备指纹及安全信息进行设备风险识别，辨别是否为风险设备，有效防御黑产批量虚拟机、病毒侵入等攻击手段，降低第三方黑产攻破概率，符合机构检查要求。

在通信运营商场景，为响应工信部对手机用户实名制的规定，远程人脸实名认证广泛应用于用户办理入网开卡手续，防止用户在不知情的情况下被冒名开卡，保障用户权益，同时有效减少电信诈骗、垃圾骚扰电话、倒卖等情况出现。基

于百度实时检测活体和人脸对比，助力客户将线上、线下及物流环节打通，使顾客线上享受线下同等优惠，同时便于市场部进行客户管理。该方案在活体检测、人脸比对过程安全有保障，还提供附加能力，支持获取活体过程中的操作信息用于后审流程。



作为首批通过信通院可信人脸识别评估，并且荣获四级（优秀级）安全防护等级的产品，百度智能云人脸实名认证也提供了微信小程序、微信 H5、APP SDK，公有云及私有化等多种接入及部署方式。

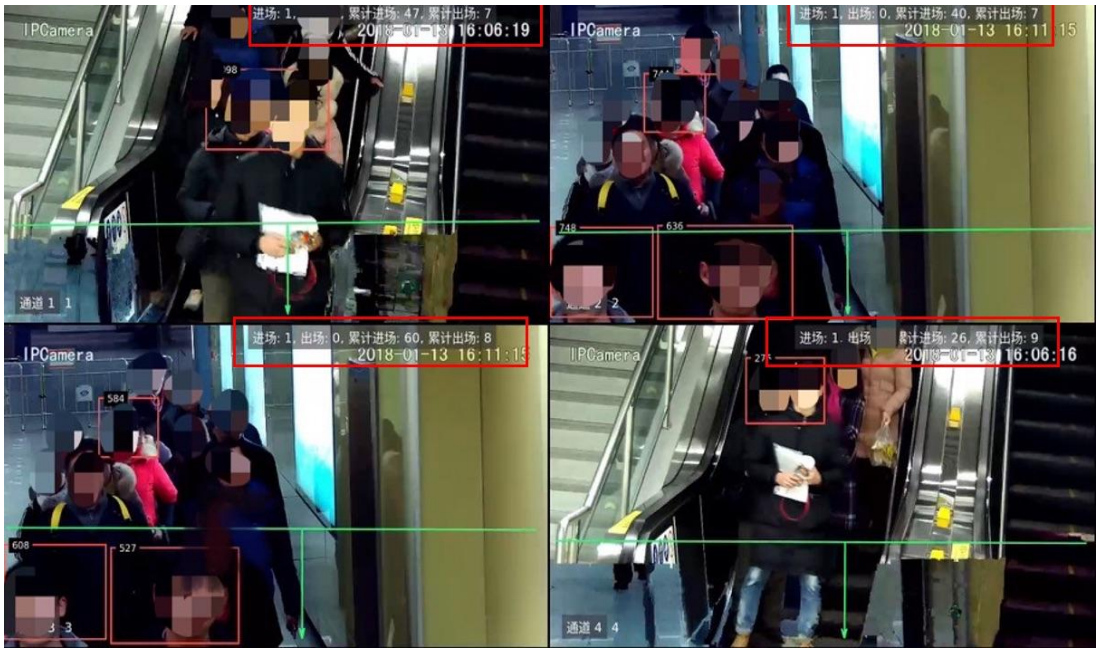
案例二：以最小必要原则为基础进行人脸识别

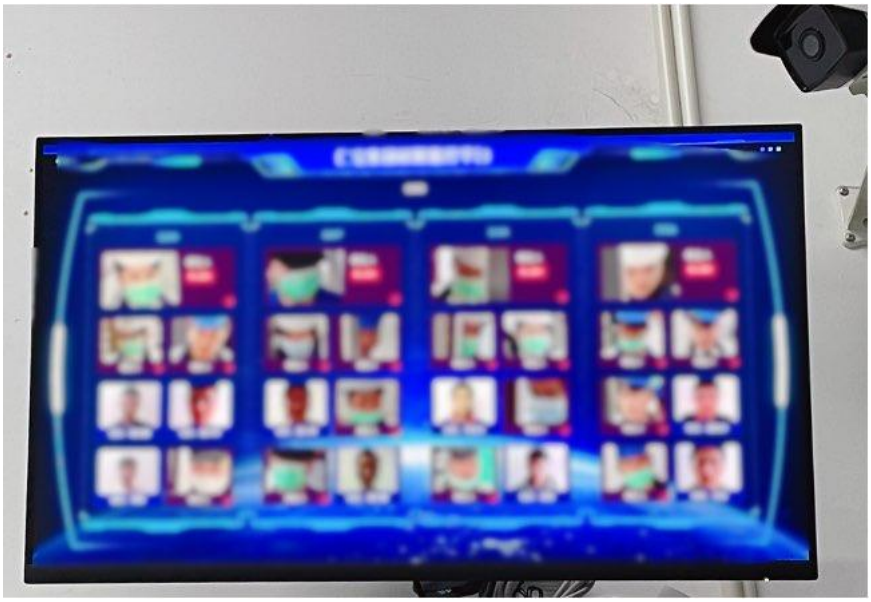
度目智能视频分析盒以 AI 视频分析为核心，轻量部署，即插即用，充分利用现有摄像头，帮助企业降低成本，提高监管效率。

如何科学、有效地对客流量进行时间、空间上的分析，并快速及时地做出经营决策，成为商业、零售业营销模式成

功与否的关键。由人工来统计客流量，极易出现漏数顾客人数，且无法不间断地统计，很难做到全面统计，只能作为某时间段的概数统计，缺乏全面性和有效性。利用度目智能视频分析盒实时统计进出场人数和累计人数，并将数据实时推送业务平台，支持自定义进出场方向，自主配置人员信息参数，支持吸顶和壁装监控角度。通过对不同时段客流量的统计，管理人员可以在客流高峰期增加工作人员，提高服务质量，进而增加销售；在空闲时减少工作人员，避免出现人员浪费。

无感通行是指用户在通过鉴权通道时自动校验，如果有权限则直接通过，没有阻拦；无权限用户会通过业务人员拦截。无感通行是未来出入口控制系统的发展趋势，无闸机、无需人员配合，即可便利通行，且能保障系统的安全性。无感通行利用前端人脸抓拍摄像机实时精准抓拍，依托边缘盒子实时辨识人员身份；人员信息与通行记录在平台上统一管理。该方案提高通行效率，解决通行拥堵问题，高峰期依然保持高精度毫秒级识别。


IPCamera
进场: 1, 累计进场: 47, 累计出场: 7
2018-01-13 16:06:19
通道 1 1
IPCamera
进场: 1, 出场: 0, 累计进场: 40, 累计出场: 7
2018-01-13 16:11
IPCamera
进场: 1, 出场: 0, 累计进场: 60, 累计出场: 8
2018-01-13 16:11:15
IPCamera
进场: 1, 出场
累计进场: 26, 累计出场: 9
2018-01-13 16:06:16
通道 4 4




设置区域ID: 2
ROI
设置
全屏
清除

案例三：回应反诈需求进行人脸识别

北京银行人脸识别系统是基于行业领域先进的人脸识别技术进行的改造部署，重点针对当下风险较高的黑产图像攻击，进行了全方位防护升级，实现了人脸比对、活体检测、环境安全检测等功能，可以根据不同的业务场景安全等级实现灵活调度，有效防范黑产攻击，为业务安全保驾护航。

北京银行“京彩生活”APP 是北京银行零售业务的重要渠道系统，具有客户交易量大，业务多样性等特点，在登录、转账、更换绑定设备等关键环节均使用了人脸识别功能。因此，北京银行尤其关注和重视人脸识别的安全性和稳定性，经过多次优化迭代，持续完善业务功能和技术能力，系统安全不断升级。

北京银行人脸识别技术的安全亮点主要在于人脸安全防护的组合应用，在提升了防成像攻击的活体检测基础上，持续加固了环境安全检测，从客户端到后端提供了业务全生命周期的防护机制，同时对于人脸识别场景，采用双算法切换的机制，结合反欺诈平台的安全认证反馈机制，及时对风险场景进行定位，有效打击人脸安全风险交易，保障客户财产安全。

案例四：以算法治理为基础进行人脸识别

中国电信人脸实名认证系统重点围绕活体检测安全、人脸质量判断、人脸识别精度提升等方面做了大量工作，可应

用于全面、安全、高效的用户身份信息真实性核验服务，满足用户多场景下的身份认证需求。与权威数据对接，支持多维度实名认证：身份证信息、手机号、人脸核验、活体检测等。该应用在行内已经得到了全面推广，目前承接了多项人脸实名认证业务。

中国电信人脸实名认证系统在电信线下营业厅、线上智能客服等多个产品中得到了应用。随着 AI 技术的不断发展与进步，人脸应用的安全问题也随之与日俱增。中国电信高度重视人脸安全问题带来的用户财产利益损失风险，研发人员将技术与业务紧密结合，在保证用户体验流畅性的前提下，技术不断探索迭代优化，以保障电信用户在线下及线上场景都能得到金融级的安全保障。

该技术提出了动态特征队列（DFQ）方案，采用度量学习的方法提升模型泛化性。可以实现有效抵御各类图片、屏幕翻拍及 3D 面具、头模的攻击，还针对活体注入、绕过行为增加防深伪功能，抵御如静态人像图片活化和 AI 换脸等各类常见深度伪造形式。

技术层面上，中国电信关注人脸识别领域的四个研究方向：精准，公平，可解释，隐私。首先，随着各类深度伪造人脸，对抗样本攻击等技术演进升级，可信人脸需要不断提高鉴伪能力，提高算法精度与鲁棒性。其次，技术需要服务全体人类，对各人群与个体都应更安全，更便捷。再次，神

经网络技术依旧是数据驱动的黑盒技术，尤其对需要防范各类攻击的可信人脸方案，需要进一步拓展可解释能力，减少攻击漏洞。最后，数据隐私，信息隐私都是电信集团关注的重点，在便利可信的同时需要兼顾使用者的隐私安全。

业务拓展方面，中国电信致力于 AI 技术赋能各行各业。公共安全领域，电信将积极应用可信人脸技术建设雪亮工程等，维护社会安全。社区生活领域，电信将基于可信人脸技术推出云边一体化解决方案，保护业主安全，提高生活便利性，为社区居住者提供归属感、舒适感和未来感。金融支付领域，电信综合多项可信人脸技术，为企业个人快速提供身份认证，信用评级等应用，让金融系统便捷与安全。

案例五：以个人信息保护为基础进行人脸识别

蚂蚁集团始终高度重视数据安全与隐私保护。在人脸识别治理领域，除了不断开拓刷脸支付等新型支付方式外，还持续提升金融级的人脸安全能力，探索多主体多维度的治理方式，致力于为消费者提供安全、便捷的交易体验，为不同业态的商家提供所需的支付解决方案。

蚂蚁的人脸识别技术具备金融级安全性，通过全链路安全防御体系来保障健康发展。结合云端活体算法、客户端安全、通信传输安全以及在此基础上的全链路人脸威胁对抗体系来做保障，具备及时的人脸威胁感知能力、处置能力、闭环的防御处置流程。同时配置风险治理专项强化人脸识别认

证服务的安全管控：确保线上线下高风险业务场景中人脸必须配合交易密码、短信验证码等认证手段组合的多因素认证方式；强化与人脸识别相关的业务逻辑测试、软件开发工具包 （SDK）代码检查、漏洞扫描等措施。

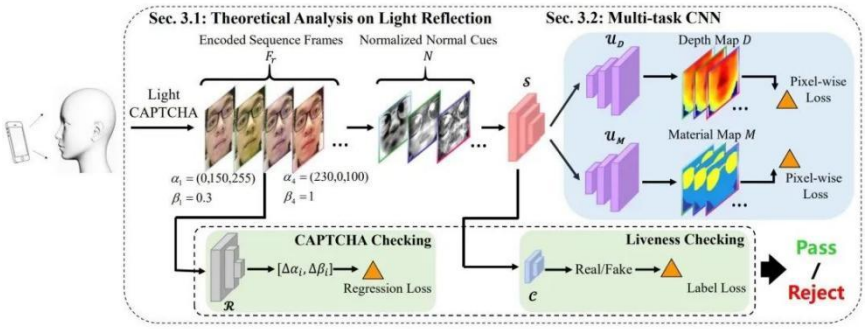
蚂蚁集团制定了《生物识别服务通用规则》，用于向用户说明在其使用基于生物识别信息的相关服务时，将如何收集、存储、保护、使用包括人脸在内的生物识别信息，并向用户说明所享有的访问、更新、管理和保护其生物识别信息的权利。蚂蚁通过确认协议、弹窗提示等形式征得用户的同意后进行数据处理，保障用户知情权、决定权。在使用人脸识别技术进行身份核验前，支付宝会通过标准的人脸引导页，向用户告知《生物识别服务通用规则》，仅在用户明确确认进行下一步操作后方才处理其信息。对于采集到的人脸信息，蚂蚁采用了行业领先的“一图一密”的加密技术进行保存，即为每一人脸信息单独创建密钥进行安全管理，保障安全强度。

案例六：以网络安全为基础进行人脸识别

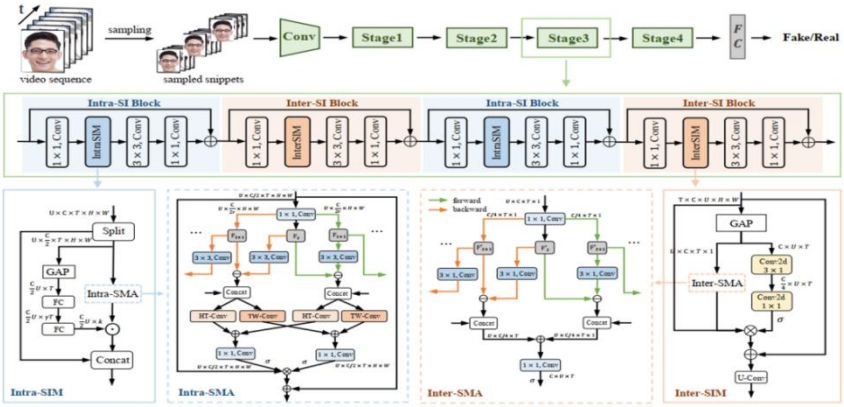
腾讯云慧眼是腾讯云和腾讯优图实验室共同打造的人脸核身产品，拥有证件 OCR 识别、活体检测、人脸对比等能力，可以满足行业内大量对用户身份信息核实的需求。腾讯云慧眼通过设备安全增强、活体安全增强、智能分级认证增强，全面升级核身安全能力，能够在刷脸核身的同时实时

检测环境风险，根据风险等级智能选择认证方式，精准拦截多种类型的刷脸攻击。产品适用于金融、保险、电商、直播、社交等行业的实名注册、密码修改、交易提现场景。特别是，腾讯云慧眼支持多地的惠民保项目，使用人脸核身进行在线投保，在基本医保参保人员罹患重病大病时，在现有医保之外，再增加一份大额自费医疗费用的补充保障。

腾讯可信人脸安全技术主要包含人脸活体检测、人脸内容取证和人脸对抗攻防三大关键技术。



针对物理呈现攻击风险，腾讯优图研发了完整的活体检测体系，覆盖线上和线下各类平台。针对 deepfake 等人脸内容生成攻击，腾讯优图研发了相应的内容取证技术框架。在人脸图像内容取证方向，从人脸图像生成的原理和本质出发，关注人脸空间特征的不一致性，提出通过局部关联学习来进行伪造检测的新方法，基于注意力机制同时提取 RGB-频域空间特征，并设计多尺度局部相似性建模网络来衡量局部区域特征间的相似性，最终构造泛化性强、鲁棒性高的相似模式，支持多种图像伪造方法的有效检测。



案例七：以本地部署为基础进行人脸识别

火山引擎结合 AI 技术，以用户为中心、以短视频为主要载体，面向“深度交互、重体验”短视频生产场景，通过智能硬件拍摄+云端剪辑，结合互动大屏、AR、XR 等技术生成“人+景/虚拟空间”Vlog 短视频；提供更具故事记录与拍摄角度、更身临其境的沉浸式体验场景产品，降低用户制作视频的门槛。

智能算法是整个 AI 智能剪辑里的核心部分，AI 算法主要包含多模态聚类算法和人物高光剪辑算法两个部分。本地的多模态聚类算法主要实现游客的身份识别以及跨摄像头的目标跟踪；高光剪辑算法则综合了动作、表情、手势以及人与物的关系等多种能力，分析当前游客的状态，能够自动剪辑出游客最值得留念的一瞬间。

系统架构：在数据安全上，除云端和边缘端相互认证，每个边缘集群都有独立 token，并保证人脸采集只在本地部署。数据安全方面：边缘端仅对局域网开放访问权限，不暴露公网入口；边缘端设备与云端管理平台通过 SDK 采集上

报，不直接暴露设备信息接口；云端与边缘端数据通过 AES 加/解密实现鉴权，且不同景区采用不同密钥，保证数据安全性；所有 OpenAPI 均严格校验请求账号的数据权限，保证不同租户数据完全隔离。同时，通过火山 IAM 鉴权机制，校验不同子用户的操作权限；用户人脸数据，仅保存提取后的特征数据，人脸图片使用完成后，会自动删除。

附：人脸识别产业治理倡议

近年来，人脸识别技术在安防、金融、医疗、支付、教育、文娱等诸多领域中相继落地，便利了人们日常生活并推动了数字经济与社会发展。但与此同时，人脸识别技术也引发了信息滥用、算法误差、数据泄露、人格歧视、秘密监控等风险。为维护用户权益，促进产业规范发展，特作出如下倡议：

1.坚持“以人为本的设计”

将保护用户权益置于人脸识别产业的中心，在人脸识别技术和产品研发、提供和具体应用的各阶段，均将“不伤害用户”设定为默认前提，并贯彻到企业内部运营、战略、业务流程和组织架构之中。

2.坚持“最小必要原则”

人脸识别技术应用者只有在特定的目的和充分的必要性、合理性的前提下，才允许应用该技术。

3.坚持“透明原则”

人脸识别技术应用者以显著方式、清晰易懂的语言，真实、准确、完整、及时地向用户披露人脸识别信息，包括是否使用人脸识别技术、用于何种场景及其目的、对用户权利的影响等。

4.坚持“用户选择权”

为用户提供及时、便捷的关闭和退出方式，让用户能对

不合法、不合理的人脸识别随时拒绝，并为其提供替代方法。

5.坚持“问责原则”

人脸识别技术的研发者、产品和服务提供者与应用者应各自建立明确、有效的问责机制，发生侵害后，应根据过错原则划分责任边界，承担与风险相适应的法律责任。

6.坚持“全面合规原则”

人脸识别技术的研发者、产品和服务提供者与应用者应建立全周期、全链路合规的理念，全面遵守个人信息和隐私保护、数据安全、算法治理、平台责任等与之相关的所有规制要求。

7.积极倡导协同共治

企业以尊重用户权益为理念，行业以尊重用户权益为设计原理，通过与政府、用户的良性互动，发掘、推广人脸识别技术落地的最佳实践，推动人脸识别产业向上向善。