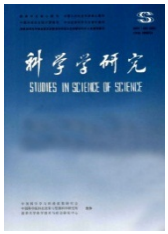


科学学研究
Studies in Science of Science
ISSN 1003-2053,CN 11-1805/G3

《科学学研究》网络首发论文

题目：人脸识别技术的社会风险及其法律规制
作者：孙道锐
DOI：10.16192/j.cnki.1003-2053.20200729.001
收稿日期：2020-02-09
网络首发日期：2020-07-29
引用格式：孙道锐．人脸识别技术的社会风险及其法律规制．科学学研究.
https://doi.org/10.16192/j.cnki.1003-2053.20200729.001

网络首发：在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

出版确认：纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

DOI：10.16192/j.cnki.1003-2053.20200729.001　网络首发时间：2020-07-29 15:03:28
网络首发地址：https://kns.cnki.net/kcms/detail/11.1805.G3.20200729.1457.005.html

人脸识别技术的社会风险及其法律规制

孙道锐

（大连海事大学法学院，辽宁大连 116026）

摘　要：人脸识别技术是以人工智能算法为技术支持，以大数据分析为手段，进而实现人脸识别的目的。根据算法的不同，有基于 2D 识别算法和 3D 识别算法的人脸识别技术系统。但不管基于何种算法，均面临欺骗攻击、技术利维坦及责任风险等社会风险。欺骗攻击包括 2D 欺骗攻击和 3D 欺骗攻击；人脸识别技术利维坦是集人工智能“赛维坦”和大数据“数字利维坦”于一身的复合型技术利维坦；责任风险表现为现有的过错责任原则无法有效地对人脸识别技术带来的责任规则进行划分。为防范人脸识别技术的社会风险，除需对该技术进行深度研发外，更需要从该技术系统的应用端出发，对该技术使用的范围、手段和目的进行规制。

关键词：人脸识别技术；面部识别信息；社会风险；法律规制；算法

中图分类号：DF522　文献标识码：A

Social risks and legal regulation of face recognition technology

Sun Daorui

（Law School, Dalian Maritime University, Dalian Liaoning 116026）

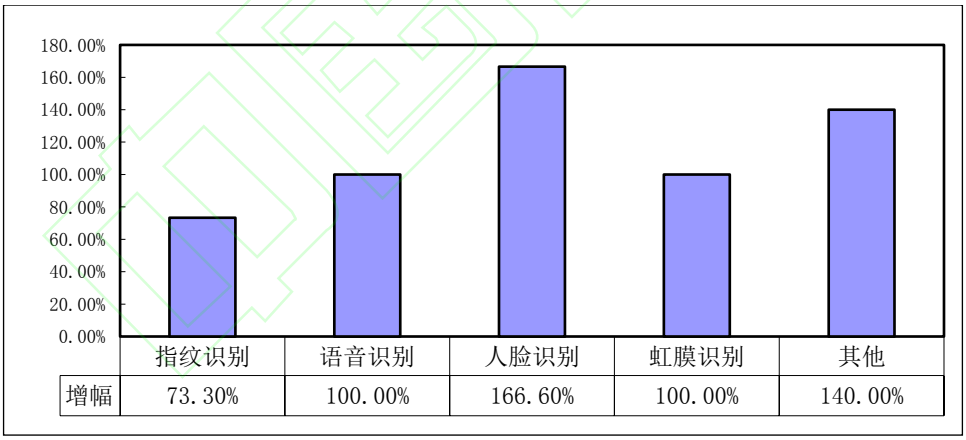
Abstract: Face recognition technology is based on artificial intelligence algorithm and big data analysis to realize the purpose of face recognition. According to different algorithms, there are face recognition technology systems based on 2D recognition algorithm and 3D recognition algorithm. However, no matter what algorithm is based on, there are social risks such as deception attack, technical Leviathan and responsibility risk. Deception attack includes 2D deception attack and 3D deception attack; Leviathan, a face recognition technology, is a composite technology Leviathan which integrates artificial intelligence "Leviathan" and big data "digital Leviathan"; liability risk shows that the existing fault liability principle can not effectively divide the liability rules brought by face recognition technology. In order to prevent the social risks of face recognition technology, in addition to in-depth research and development of the technology, it is

收稿日期：2020-02-09；修回日期：2020-07-22
基金项目：国家社科基金重大项目“民法精神与建设社会主义法治文化民本模式研究”（项目号：14ZDC022）
作者简介：孙道锐（1988-），男，云南宣威人，大连海事大学法学院博士研究生，研究方向为科技法学。第一作者，E-mail：evergreen_suen@sina.com。

also necessary to regulate the scope, means and purpose of the technology from the application end of the technology system.
Key words:face recognition technology; facial recognition information; social risks; legal regulation; algorithm

不论任何时期，信息安全一直都是人类关注的重点，而保障信息安全的核心问题之一就是准确高效地识别用户的身份信息。传统上，身份信息识别的方法包括基于身份标识物品（如证件）的方法和基于身份识别知识（如用户名、密码）的方法[1]。但传统的身份识别方法存在易伪造、易丢失、易遗忘、效率低下等不足。20 世纪 70 年代以来，随着人工智能技术和大数据的兴起，以及人类视觉研究的发展。加之因人的生物特征具有普遍性、唯一性、稳定性等优势，生物特征识别成为了身份信息识别的进阶方式。而在众多生物特征识别中，人脸识别又具有其独特的自然性优势，符合人类视觉认识习惯的原理，并可通过远距离非接触性的方式获取。因此，较指纹识别和虹膜识别等众多生物特征识别而言，人脸识别具备了更为广阔的应用前景。据分析统计，自 2015 年到 2020 年，人脸识别市场份额的涨幅达 166.6%，位居众多生物特征识别的首位（见图表 1）。

图表 1：2015—2020 年间生物特征识别市场份额增幅[2]



	指纹识别	语音识别	人脸识别	虹膜识别	其他
增幅	73.30%	100.00%	166.60%	100.00%	140.00%

随着人脸识别市场份额的快速增长，人脸识别技术系统得到了更为广泛的应用。但随之而来的是该技术社会风险发生的概率亦将呈比例增长。是故，对人脸识别技术社会风险的法律规制这一议题进行研究已极具现实意义。然而，我国迄今对人脸识别技术的研究基本上限于与该技术相关的自然科学理论与技术问题，鲜有涉猎于该技术的社会风险，亦未对此提出相应的法律规制策略。鉴于此，有必要对该议题进行研究，这既是规范人脸识别技术使用的应然举措；也是对个人

信息，尤其是面部识别信息保护的现实需要；更是推进人脸识别技术国家治理体系和治理能力现代化的中国探索，贡献中国方案。

1 人脸识别技术：从 2D 到 3D

1.1 2D 人脸识别技术

1964 年，布莱索（Bledsoe）提出了世界上首个人脸识别算法，该算法以链码为特征进行人脸识别，开启了首个真正意义上的自动人脸识别技术研究[3]。20 世纪 70 年代以后，随着计算机技术、图像处理技术、人工智能和大数据等诸多学科的快速发展，产生了 2D 人脸识别算法。比较有代表性的算法有几何结构特征分析（geometry feature analysis）算法、特征脸（Eigenface）算法和费舍尔脸（Fisherface）算法。

几何结构特征分析算法围绕人的眼睛、鼻子、嘴巴、下巴等面部轮廓之间的几何结构特征进行研究，通过分析各类面部剪影曲线以及提取人的面部结构图像达到人脸识别的目标[4]。该算法处于 2D 人脸识别技术的初级探索阶段，未能转化为实际应用。特征脸算法由马修·特克（Matthew Turk）和亚历克斯·彭特兰（Alex Pentland）于 1991 年首创，该算法将人脸识别问题视为一个本质上的二维识别问题。特克和彭特兰二氏把基于统计学的主成分分析方法引入人脸识别中，通过将人脸图像投射到一个特征空间中，将特征脸的特征权重与已知个体的权重进行比较来识别一个人脸[5]。时至今日，特征脸算法仍具一定的实用价值，一些人脸识别技术将特征脸算法作为特征提取的一个重要预处理步骤。费舍尔脸算法由彼得•N•贝尔胡默（Peter N. Belhumeur）等人于 1997 年提出，该算法结合了统计学的主成分分析方法和线性判断分析方法，是一种可不受光照方向和面部表情变化影响的人脸识别算法[6]。该算法利用了训练样本的类别标签信息，因此性能优于特征脸算法。综上，2D 人脸识别算法孕育出了 2D 人脸识别技术系统，该类技术系统的基本识别流程为图像数据采集、人脸检测、特征提取、信息比对等四个大步骤。

1.2 3D 人脸识别技术

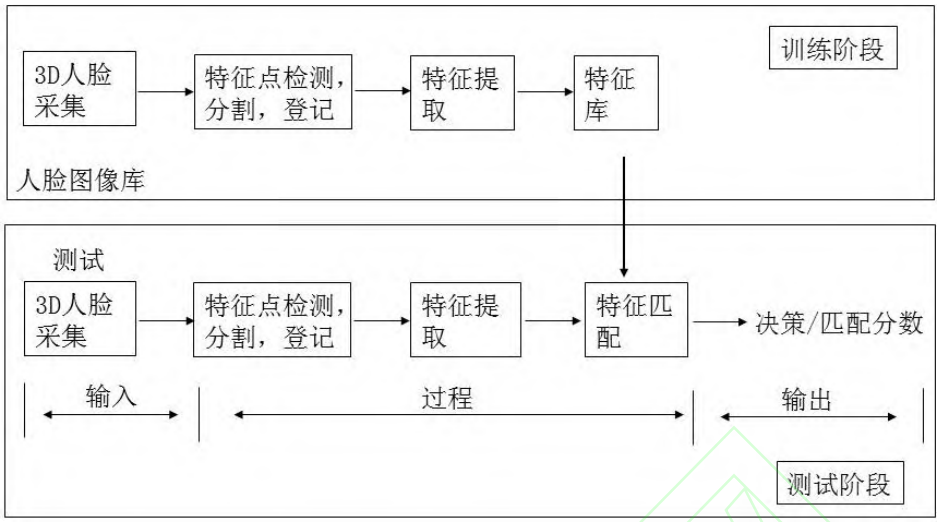
进入二十一世纪之后，随着人工智能算法和大数据分析取得了丰硕的研究成果，以及更为高清的图像处理设备的应用，诞生了 3D 人脸识别算法。比较有代表性的算法有 3D 变形模型（3D morphable model）算法、基于流形学习理论

（manifold learning theory）的算法、稀疏表示分类（sparse representation classification，SRC）算法和基于深度学习（deep learning）的算法。

沃尔克·布兰兹（Volker Blanz）和托马斯·维特（Thomas Vetter）于 2002 年提出了基于 3D 变形模型的人脸识别算法，解决了人脸检测与识别难以解决的多姿态问题[7]。该算法基于人脸的空间向量表示，形成一组示例的形状和纹理矢量 Si 和 Ti 的任何凸组合都呈现为一张逼真的人脸[8]。流形学习理论由约书亚·B·特南鲍姆[9]（Joshua B. Tenenbaum）于 2000 年提出。此后，该理论被引入人脸识别技术系统中，用以提取人脸图像的低维特征[10]。基于流形学习理论的算法所得到的子空间是一个非线性空间并且保持了原始样本空间的全局或局部拓扑结构，接近于人类的视觉感知系统，对人脸特征具有更好的表达[1]。稀疏表示分类算法由约翰·赖特（John Wright）等人于 2008 年提出，该算法将压缩感知理论（compressive sensing）引入人脸识别技术领域[11]。经验证，该算法是一种基于 L1 范数最小化问题，对图像被腐蚀、遮挡及噪声具有较强的鲁棒性，在很多应用场合都取得了很好的分类效果，是目前备受关注的一类人脸识别技术算法[12]。近年来，为解决因大姿势和照明变化的面部识别困难，诞生了一种基于深度学习的算法。该算法在具备面部身份保留（FIP）功能的同时，尽可能地减少个体自身差异，扩大不同个体间的区别性特征[13]。通过深度学习以及使用面部识别和验证信号作为监督可以很好地开发有效的特征表示，显著增强个体的面部特征，达到准确且高效的人脸识别目的[14]。

3D 识别算法使人脸识别技术取得了巨大的发展，同时具备了高效率与高识别正确率。在识别流程上，一个通用的 3D 人脸识别技术系统包括训练和测试两个阶段。训练阶段的主要任务是利用现有的人脸数据库进行人脸图像学习分类模型，测试阶段则是根据训练阶段所得到的分类模型对待检测人脸进行识别（见图表 2）。

图表 2：通用 3D 人脸识别技术系统[15]



1.3 小结

2D 人脸识别算法由于受姿态、光照、表情、老化、妆容变化和遮挡等原因，导致正确识别率较低[15]。并且，即使是同一张人脸在成像后也可能有较大的差别，或者是不同的人脸在一定的角度下，有时也极其相似，使得 2D 人脸识别技术系统存在较高的识别错误率。但不可否认，2D 人脸识别算法的研究为 3D 人脸识别算法的发展奠定了理论基础。此外，3D 人脸识别技术继承了 2D 人脸识别技术自然识别的过程和广泛的应用前景等优点，并具备了在光线较暗、面部位置和表情变化多样的情况下也能准确识别人脸的能力[16]。以下为 3D 人脸识别与 2D 人脸识别的数据对比（见图表 3）。

图表 3：3D 人脸识别与 2D 人脸识别的数据对比[17]

对比项	3D人脸识别	2D人脸识别
FAR（错误接受率越低，识别安全性越高）	0.0047%	0.1200%
FRR（错误识别率越低，使用就越方便）	0.1030%	9.7900%
姿态变化	100%识别率	23%识别率
头发遮挡	87%识别率	50%识别率
头部遮挡	95%识别率	低于5%成功率
弱光线	100%识别率	0%识别率

2 人脸识别技术的社会风险

2.1 欺骗攻击

2.1.1 欺骗攻击的类型

欺骗攻击（spoofing attack）也称为演示攻击（presentation attack），是指攻击者通过向人脸识别技术系统演示假识别信息，实现智胜人脸识别技术系统的行为[18]。此类假识别信息包括图片、视频和面具等工具。其中，图片欺骗攻击和视频欺骗攻击属于 2D 欺骗攻击，面具欺骗攻击属于 3D 欺骗攻击[19]。

图片欺骗攻击是通过向人脸识别技术系统展示真实的人脸照片来进行攻击，或者使用裁去眼睛和嘴巴等部分的高质量和高分辨率的打印照片，然后攻击者站在该类照片的背后，在人脸识别时重现眨眼和唇部运动进行欺骗攻击。视频欺骗攻击是图片欺骗攻击的高级版本，攻击者在人脸识别时通过回放人脸视频达到获取访问权限的目的。面具欺骗攻击是攻击者通过制作一个真实用户的面部 3D 蒙版，在这个蒙版中，3D 结构是根据面部的深度信息复制的，具有比图片和视频更高的真实度和欺骗性。典型的 3D 面具有 Thatsmyface 面具和 REAL-f 面具，Thatsmyface 面具可以轻易地欺骗许多现有的人脸识别技术系统，在由 Thatsmyface 面具构成的 3D 面具攻击数据集（3DMAD）数据库中，会话间变异性（ISV）建模方法的欺骗假接受率（SFAR）约为 30%。而 REAL-f 面具采用 3D 扫描和 3D 照片形式（3DPF）技术对 3D 结构进行建模并打印面部纹理，可以达到比 Thatsmyface 面具更高的外观质量和 3D 建模精度。通过观察 REAL-f 面具的头发、皱纹甚至眼球血管等细节，在缺少提示信息的情况下，肉眼很难辨别出这是否是一张真正的脸[20]。

2.1.2 反欺骗攻击的不足

当前，针对人脸识别技术的欺骗攻击，提出了纹理分析、运动分析、活性检测等三种反欺骗攻击的方法。第一，纹理分析，该方法基于人脸图像在多次采集后在纹理上存在模糊的特性，通过检查和分析捕获到的人脸图像的纹理来检测是否是一张真实的人脸。近来，基于纹理分析衍生出了微纹理分析的方法，该方法使用多尺度局部二进制模式，但该方法取决于人脸图像和视频的质量[21]。第二，运动分析，该方法通过对待测对象运动的情形来检测欺骗攻击，与真实的脸相比，

手机或纸等平面物体在移动方式上是明显不同的。第三，活性检测，该方法根据待识别对象呈现唇动、眨眼等运动姿势来判断是否具有活性[22]。

值得注意的是，包括活性检测、运动检测和纹理分析在内的反欺骗攻击检测方法在面对 3D 面具的欺骗攻击时基本失效。基于纹理分析的方法在 2D 欺骗攻击中使用面部的重捕效果可能无法识别 3D 面具攻击。根据相关评估实验显示，在只使用 2D 人脸识别算法时，3DMAD 数据库中有 65.7%的 3D 面具攻击被识别为合法用户[23]。基于眨眼和嘴唇动作的面部识别技术系统也可以被去除眼睛和嘴巴区域的面具击败[24]。并且，随着 3D 打印技术的发展，可以快速打印出高度精细化和高度仿真化的人脸面具，这对人脸识别技术系统提出了更高的反欺骗攻击的要求。

2.1.3 欺骗攻击的实例

人脸识别技术的滥用使得该技术系统很容易成为欺骗攻击的目标，特别是在基于 2D 算法的人脸识别技术系统中，这些问题通常更为突出，仅使用人脸的图片或视频就可以进行欺骗攻击。例如用打印的照片就能“破解”自助取件设备[25]。而具有 3D 结构的超真实感的人脸面具使得区分真实人脸和欺骗人脸变得更加困难，即使是那些已经具备欺骗攻击检测的人脸识别技术系统来说也是如此。2017 年发布的苹果 iPhone X 被 Bkav 的研究人员证实，当花 200 美元左右定制一个人脸面具时，面部 ID 可以被解锁[26]。2019 年 12 月 12 日，美国《财富》杂志报道 Kneron 公司使用高质量的 3D 面具成功欺骗了包括支付宝和微信在内的诸多人脸识别支付系统，完成了购物支付程序[27]。

2.2 异化为复合型技术利维坦

人脸识别技术集人工智能算法和大数据于一身，是以人工智能算法为技术支持，以大数据分析为手段，进而实现人脸识别的目的。一旦人脸识别技术被滥用，人工智能算法将异化为“赛维坦”（Seviathan），大数据将异化为“数字利维坦”（digital Leviathan）。由此，人脸识别技术将异化为集“赛维坦”和“数字利维坦”于一身的复合型技术利维坦。具体而言，人脸识别技术在内核上是人工智能算法，该技术的滥用将导致“科学从原本温文尔雅、带领人民走出黑暗时代的‘赛先生’，变成带领人们急速驶入未来世界、力量极其庞大却又找不到方向的巨型怪兽——赛维坦[28]。”此外，人工智能算法的赛维坦风险将直接导致人脸识别算法可能误判数据，不去审查数据反映的是否是假象，最终作出背离实际状况的决

策[29]。在大数据的领域，数据如同脱缰之马，手执缰绳和马鞭的人类无力操控之势逐渐显现，开始其异化过程，有演化成一种新的利维坦——“数字利维坦”之势[30]。当人脸识别技术异化为集“赛维坦”和“数字利维坦”于一身的复合型技术利维坦时，将有可能导致个人、社会和国家遭受到不同程度的侵害。

2.2.1个人人格权益遭到侵害

随着具备高清人脸识别功能的拍照设备和摄影器材的广泛应用，具备了远程捕获他人面部识别信息的能力。加之，人脸识别技术又以大数据分析作为手段，而大数据对隐私的窥探与暴露与生俱来，个人面部信息有可能在大数据的侵蚀下被有意或无意地公之于众，使公民的个人信息遭受到严重威胁，甚至成为了买卖的商品。据央视财经报道，在互联网平台“转转”上，10元就能买到5000多张人脸照片[31]。而人脸是一个人的名片，是与他人相区分的重要的生物性标志，与人终生不会分离。可以说，正是由于个人面部识别信息具有唯一性的特征，天然地与特定的人联系在一起，人们可以容易地做到观其脸，知其人。由此，人们越来越容易根据照片或视频中出现的面部识别信息准确地指向某一人，在一些特殊情形下将导致该个人社会评价的降低，人格权益的受损。例如，在孟倩诉光明网传媒有限公司人格权纠纷案件中，审判法院通过比对孟倩本人的身份证照片和百度相关图片得出光明网公司涉案网站上所使用的照片为孟倩本人，确定其为被侵权人，光明网的行为对孟倩的形象产生一定的影响，造成其精神上的损害①。

2.2.2加剧社会碎裂化的风险

当前，科学技术与社会的关系已经由“社会中的科学”向“科学伴随社会”的新范式转变[32]。这一范式意味着科学与社会已形成了深度交融、影响的关系，这一关系表现为：在科学技术得到良好的使用时，会起到促进社会发展进步的效果；当科学技术被滥用时，则会阻碍社会的发展。人脸识别技术与社会之间亦具有此种交互影响的关系。当该技术被滥用时，对社会的反作用亦表现出阻碍社会发展的效应，会不断制造和助推社会隔离的过程。掌握该技术系统的主体一旦肆意地滥用该技术，则会侵蚀他人最为私密的空间，加剧社会碎裂化的风险。并且，在数字利维坦的环境中，极端主义观念更容易兴起和广泛扩散，个人面部信息将被赤裸裸地暴露在任意第三人的镜头之下，经社交媒体的发酵，将对社会分裂不

①光明网传媒有限公司与孟倩人格权纠纷案，北京市第三中级人民法院，(2017)京 03 民终 8213 号民事判决书。

断地推波助澜，诱导群体极化，并不断侵蚀个体化社会的存在基石，使支撑个体化社会的一些理论概念和行为边界受到冲击[30]。

2.2.3 引发技术独裁和国家信息安全问题

国家技术利维坦将导致国家利用人脸识别技术以更加隐秘、牢固的方式体现国家的控制能力，编织新型的国家权力网络。国家意志通过制定人脸识别算法得以展现，以此加强国家在各个方面的监控能力和社会管理能力，进而压缩公民私权利的空间，导致技术权威和独裁，加剧寡头统治的危险[33]。近来，英国的埃德•布里奇斯（Ed Bridges）发起了一项众筹行动，旨在控诉南威尔士警方滥用人脸识别技术导致其隐私遭到非法侵犯[34]。无独有偶，人脸识别技术发源地的旧金山市于 2019 年 5 月通过了一项旨在禁止警察等执法部门使用人脸识别技术的规定[35]。

此外，人脸识别技术利维坦可能引发国家信息安全问题。在数字利维坦的背景下，域外恐怖势力和敌对势力一旦对国家人脸识别技术系统发起攻击，将使得国家存储公民面部识别信息的基础设施和重要机构成为被攻击的目标。这不仅会侵入到人们生活的各个方面，使个人丧失得以独处和静谧生活的权利，而且会引发国家信息安全问题[36]。我国作为人脸识别技术的使用大国，由此引发的信息安全问题不容忽视，将导致治理成本逐年增加。据 IDC 预测，2019 年中国网络安全市场总体支出达到 73.5 亿美元，2019 年至 2023 年预测期内的年复合年均增长率（CAGR）为 25.1%，增速继续领跑全球网络安全市场[37]。

2.3 责任风险

传统的责任伦理为过失责任追究原则，即行为人无过错则无责任，该原则的有效性在于实现对责任后果相对性主体的伦理绑定[38]。而这一机械式责任伦理在高度智能化、数据化的人脸识别技术里显得格格不入。因为现有的过错责任原则无法有效地对人脸识别技术带来的责任规则进行划分。人脸识别技术的核心即为人工智能算法，而这一算法是由人脸识别技术的开发者和设计者掌握。对设计者而言，存在知识责任失衡风险。在人脸识别技术领域，设计者是单一的原子责任主体，因人脸识别技术存在 2D 人脸识别算法和 3D 人脸识别算法之分，具有复杂性、系统性。该技术系统的设计者在对人脸识别技术系统进行设计时若囿于价值偏差、利益追求以及错误认识等因素时，极有可能会处于自如的状态，此时会削弱其承担责任的意愿，游走于法外灰色空间，背离应然价值责任，甚至是恶

意地藐视和否定社会伦理规范，引致责任失衡[38]。对决策使用者而言，存在滥用人脸识别技术系统，引发权力责任失当风险。一般而言，该技术的使用者利用自我认知实现对该技术系统使用的伦理判断与监督，是使用者的责任所在。但该技术系统的使用者若只是依据其权力权威，滥用该技术系统，容易造成使用者逾越现有伦理责任规范，将人脸识别技术的不完备性带入现实社会，侵犯公民的私有利益，引发权力责任失当的风险。例如，安徽省宿州市城市管理局滥用人脸识别技术，在其社交媒体公众号上公开市民穿睡衣出行的面部图像及身份证，错把手段当成了目的，造成权力责任失当[39]。

3 人脸识别技术社会风险的法律规制

正确认识风险是防范风险的第一道防线。为防范人脸识别技术的社会风险，既需要对该技术进行深度研发，更需要对该技术的使用加以规制。换言之，人脸识别技术若没有实际的使用，相关的科学技术理论便如茶壶风暴，影响不大。而一旦该科学技术应用于人类社会，便会对我们的生活造成巨大影响。此种情况下，为防范人脸识别技术的社会风险，更需要从该技术系统的应用端出发，对使用的范围、手段和目的等三个层次进行规制。

之所以依据这样的层次进行法律规制，是因为人脸识别技术的使用一般出现于如下三种情形：①应当使用、②可用可不用、③不需要使用。首先，在第①种情形下使用人脸识别技术自无疑问，第②种情形亦属于可使用人脸识别技术的范围，而第③种情形则不属于合理使用的范围。在人脸识别技术社会风险发生概率特定的情况之下，通过控制该技术的使用范围，可极大地降低社会风险的发生。其次，在第①和第②种应当或可以使用人脸识别技术的范围内，若使用人脸识别技术的手段被滥用或者不规范，将可能导致和扩大该技术的社会风险。最后，在第①和第②种情形下，虽基于规范的使用手段，但如果使用的目的不正当，同样会引起和扩大人脸识别技术的社会风险。

3.1 对人脸识别技术的使用范围进行规制

当前，人脸识别技术使用范围的不断扩大，使得在许多原本不需要使用人脸识别技术的范围内使用了该技术，这不仅挤压了人脸识别技术合理使用的空间，并且引发民众对人脸识别技术的不信任和抵触，谈“刷脸”而色变。因此，为避免人脸识别技术使用范围的不当扩大，防止该技术的社会风险，亟需对该技术的

使用范围加以规制。而要对人脸识别技术使用范围加以规制，需要确立该技术在特定范围内使用与否的标准。本文认为，人脸识别技术的使用涉及对他人面部识别信息的收集，根据《中华人民共和国民法典》（以下简称《民法典》）第 1035 条第 1 款之规定，处理个人信息应当遵循合法、正当、必要的原则。因此，人脸识别技术在特定范围内地使用需符合合法性、必要性、正当性三原则。之所以限于特定使用范围去讨论人脸识别技术使用与否，是因为该技术的使用范围极为广泛，只有通过具体问题具体分析，才不会犯以偏概全的错误，更具有现实意义。

首先，具有合法性。人脸识别技术根据使用范围的不同，可分为公私二元领域。在公领域范围内，个人信息自主权虽必须忍受重大公共利益的限制，但人脸识别技术的使用者仍须遵守合法性的原则，以宪法和法律作为行为依据，不得逾越法律规定的使用范围。在私领域范围内，人脸识别技术的使用不得违反法律规定，应充分尊重他人的个人信息自主权，不得损害他人合法权益。其次，具有必要性。必要性原则要求实施手段的最小损害性，即既能有效保障公民权利不被过度侵犯，又能有效兼顾公共利益，增进社会整体福利的客观要求[40]。最后，具有正当性。正当性一词是伦理学上的概念，用以判断某种行为是否具有适度性、合宜性与中道性[41]。人脸识别技术的使用亦要遵循此准则，不可盲目使用和过度使用，而应当是以人性尊严作为该技术系统使用正当性的根基。凡是人脸识别技术的使用会致使人性尊严受侵害的，皆属不正当使用的范围。例如，在学校教室内使用人脸识别技术系统，虽然并未违反法律规定，该技术系统的使用者亦认为具有必要性，但却不具有正当性。究其根源在于学校教室是立德树人的场所，非流水车间，在这样的领域范围使用人脸识别技术将侵害师生的人性尊严[42]。

3.2 对人脸识别技术的使用手段进行规制

在确定人脸识别技术的使用范围之后，为防范该技术的社会风险，需进一步规范该技术的使用手段。本文认为，人脸识别技术的使用手段应遵循形式上及实质上的合法性与正当性要求。

一方面，遵循形式上的合法性与正当性要求。根据《民法典》第 1035 条之规定，个人信息的处理应当符合下列条件：（1）征得该自然人或者监护人同意；（2）公开处理信息的规则；（3）明示处理信息的目的、方式和范围；（4）不违反法律、行政法规的规定和双方约定。根据该条规定之要义，就人脸识别技术的使用手段而言，在第①种情形下，人脸识别技术的使用者应当采取看得见的方式

收集他人面部识别信息，使面部识别信息的被收集者知晓其面部识别信息被采集。就此点而言，我国《海关监管作业场所（场地）监控摄像头设置规范》（以下简称《规范》）的规定比较有示范意义。《规范》规定，在人脸识别技术设备的使用上，海关监管作业场所（场地）应在监控摄像头安装地点附近的明显位置设置提示标识，标识尺寸可根据场地空间大小选择不同型号，表明该区域属于海关监控范围。在第②种情形下，使用人脸识别技术收集他人面部识别信息的，应当依法获得他人的知情同意，依照规范的协议获取他人的面部识别信息。需要注意的是，第一，作出同意的意思表示主体须为提供其面部识别信息的个人，在其缺乏意思表示能力的情况下，可由其监护人代为作出采集其面部识别信息的意思表示。第二，同意的模式宜采用选择进入模式，此种模式更有利于保护自然人对其面部识别信息的控制[43]。不得采取选择退出模式，因个人面部识别信息属于人格紧密型信息的范畴[44]，人脸与自然人终生永不分离，同意要件应为积极同意。第三，同意的形式可以是书面形式，也可以是口头形式。

另一方面，遵循实质上的合法性与正当性要求。根据《民法典》第 1035 条、第 1038 条和第 1039 条之规定，个人信息不得过度处理，信息处理者负有安全保障义务，国家机关及其工作人员负有保密义务。这就意味着，人脸识别技术的使用者及面部识别信息控制者应当遵循准确性原则、传输限制原则、完整性和保密性原则。首先，遵循准确性原则。就个人面部识别信息而言，随着个人年龄的增长或发生面部手术、整容或整形等情形，个人容貌会发生较大的变化。是故，为确保个人面部识别信息的准确，应及时更新。其次，遵循传输限制原则。该原则要求不得任意向第三方传输个人面部识别信息，只有作为接收者的第三方具备对他人面部识别信息同等程度的保护能力时，才具有传输的条件。并且，还需要根据人脸识别技术的使用者、控制者和接收者的不同，具体分析，才能对他人面部识别信息进行实际传输。具体而言，若公权力机关为人脸识别技术的使用者和控制者，可以向另一个具有同等程度保护能力的公权力机关进行数据传输；向私权利民事组织进行传输则应严格遵守法律规定，以必要性作为考量，审慎传输。若私权利民事组织作为人脸识别技术的使用者和控制者时，可以依法向另一个具有同等程度保护能力的公权力机关进行数据传输；向私权利民事组织进行传输时，非经用户主体同意，不得向第三方传输其个人面部识别信息。最后，遵循完整性和保密性原则。该原则是指在对个人面部识别信息的收集和控制过程中应确保个

人面部识别信息的完整和安全。通过采取合理的技术手段、组织措施，保护信息的完整和免受风险，避免面部识别信息未经授权即被处理或遭到非法处理，避免面部识别信息发生意外毁损或灭失，避免面部识别信息发生不法泄露。就技术手段而言，可对个人面部识别信息的保护设置一道“防火墙”，这有利于防止科技和商业的非理性发展[45]。就组织措施而言，我国目前并未有相关法律规定。笔者认为，可借鉴欧盟《通用数据保护条例》（GDPR）规定的数据保护官制度，该制度规定于该法第四章第四部分第 37 条至第 39 条。根据 GDPR 第 39 条的规定，数据保护官承担以下职责：第一，对信息数据的控制者和处理者进行告知和提供建议；第二，培训和指导负责信息控制和处理的工作人员；第三，与监管机关进行合作并充当监管机构的联系人；第四，审慎处理信息数据，将可能发生的风险纳入考虑范围。欧盟数据保护官制度具有一定的借鉴价值，通过构建起强有力的组织制度，有助于确保人脸识别技术的使用手段遵循实质上合法性与正当性的要求。

3.3 对人脸识别技术的使用目的进行规制

凡获取他人的面部识别信息，必是基于特定的初始目的，该目的或是由法律规范加以规定，或是由协议进行约定。人脸识别技术的使用者应当严格按照法定或约定的初始目的，谨慎控制和管理，不泄露他人的面部识别信息，更不以此作为谋取私利的手段。具体而言：第一，初始目的是由法律规定或协议约定，面部识别信息的处理者不得违反法律规定或协议约定的目的。第二，若收集到的面部识别信息违反初始目的，应当及时删除或更正。第三，面部识别信息的控制者向第三方传输信息数据后，该第三方对信息数据的处理亦不得违反原初始目的。需要指出的是，人脸识别技术的使用者依法或依照协议采集他人面部识别信息时，应当依照《民法典》第 1035 条之规定，明示处理信息的目的。即对法律规定的目的或协议约定的目的进行说明，承诺在法定或约定的目的范围内使用，使面部识别信息的被收集者知悉，谨慎控制和处理，并承当相应的风险责任。

值得注意的是，不违反初始目的存有例外情形。根据《民法典》第 1036 条之规定，以下三种处理个人信息的行为免责：（1）该自然人或其监护人同意的范围内合理实施的行为；（2）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；（3）为维护公共利益或者该自然人的合法权益，合理实施的行为。本文认为，对人脸识

别信息的处理不违反初始目的的例外情形可不限于上述行为。域外，GDPR 第 5 条第 1 段（b）规定了三种数据处理的例外情形，即基于公共利益、科学或历史研究或统计目的所作的进一步信息数据处理，不视为对初始目的的违反。本文认为，GDPR 规定的出于学术研究或统计目的亦不违反初始目的的规定颇值得借鉴。

4 结语

从 2D 识别算法到 3D 识别算法，人脸识别技术的发展已历经半个多世纪，但仍未臻于完善，存在一定的社会风险。为更好地预防和控制该技术在实际使用中可能引起的社会风险，不仅需要增加相应的研发投入力度，更需要从该技术的应用端出发，对该技术使用的范围、手段和目的进行规制。未来，随着我们负责任地运用我们的智慧和发明创造能力，在人脸识别技术领域取得巨大科技进步的同时，加上对该技术的使用越发科学化、规范化、合理化及合法化，我们应用该技术系统来识别和保障个人身份信息也将更安全和更高效。

参考文献：

[1] 孔俊，易玉根，王建中.基于全部与局部信息的人脸识别[M].北京：科学出版社.2016.
[2] 中国人脸识别市场发展迅速，预计到 2021 年市场规模将突破 50 亿元[EB/OL]. (2019-4-4) [2019-11-2]. https://www.chyxx.com/industry/201904/727180.html.
[3] Bledsoe W W. The model method in facial recognition, Tech Rep PRI:15[R].Palo Alto，CA，Panoramic Research Inc, 1966.
[4]Kaufman G J , Breeding K J . The Automatic Recognition of Human Faces from Profile Silhouettes[J]. IEEE Transactions on Systems, Man, & Cybernetics, 1976, SMC-6(2):113-121.
[5] Matthew Turk，Alex Pentland . Eigenfaces for recognition[J].Journal of Cognitive Neuroscience, 1991, 3(1):71-86.
[6]Belhumeur P N , João P Hespanha, Kriegman D J . Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, 19(7):711-720.
[7]Blanz V, Vetter T , Rockwood A . A Morphable Model for the Synthesis of 3D Faces[J]. Acm Siggraph, 2002,(7):187-194.
[8]Blanz V, Vetter T.Face Recognition Based on Fitting a 3D Morphable Model[J].IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(9):1063-1074.
[9]Tenenbaum, J. B. A Global Geometric Framework for Nonlinear Dimensionality Reduction[J]. Science, 2000, 290(5500):2319-2323.
[10]Ma Y, Fu Y. Manifold Learning Theory and Applications[M]. Boca Raton: CRC Press, 2012.
[11]Wright J, Ganesh A, Zhou Z , et al. Demo: Robust face recognition via sparse representation.[C]// Demo: Robust face recognition via sparse representation. IEEE, 2008.
[12]范自柱.快速稀疏表示分类的人脸识别算法[J].计算机工程与应用.2017,53(9):1-4.
[13]Zhu Z , Luo P , Wang X , et al. Deep learning identity-preserving face space[C]// 2013 IEEE International Conference on Computer Vision. IEEE, 2014.
[14]Chen Y, Chen Y, Wang X, et al. Deep learning face representation by joint identification-verification[C]// International Conference on Neural Information Processing Systems. Boston:MIT Press, 2014.
[15]Patil H, Kothari A, Bhurchandi K. 3-D face recognition: features, databases, algorithms and challenges[J]. Artificial Intelligence Review, 2015, 44(3):393-441.

[16]Zhou S, Xiao S. 3D face recognition: a survey[J]. Human-centric Computing and Information Sciences, 2018, 8(1):35.
[17] 中国人脸识别技术发展情况及 2019 年人脸识别技术发展趋势分析[EB/OL]. (2019-1-22) [2019-12-5].https://www.chyxx.com/industry/201901/709171.html.
[18]Erdogmus N, Marcel S. Spoofing Face Recognition With 3D Masks[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(7):1084-1097.
[19]Bagga M, Singh B. Spoofing detection in face recognition: A review[C]// International Conference on Computing for Sustainable Global Development. IEEE, 2016.
[20] Liu SQ., Yuen P.C., Li X., Zhao G. Recent Progress on Face Presentation Attack Detection of 3D Mask Attacks. In: Marcel S., Nixon M., Fierrez J., Evans N. (eds) Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition[C].New Delhi: Springer, Cham. 02 January 2019.
[21] Jukka Määttä, Hadid A, Matti Pietikäinen. Face spoofing detection from single images using micro-texture analysis[C]// International Joint Conference on Biometrics (IJCB). IEEE, 2011.
[22] Junied Khalid Khan, Divya Upadhyay. Security issues in face recognition[C]// 2014 5th International Conference- Confluence The Next Generation Information Technology Summit (Confluence), 2014.
[23] 陆经纬，陈鹤天，马肖攀，陈继民.基于多特征融合的 3D 打印面具攻击检测[J].激光与光电子学进展.2019(3):86-96.
[24] Shan Jia, Guodong Guo, Zhengquan Xu. A survey on 3D mask presentation attack detection and countermeasures[J]. Elsevier, 2019(9):1-13.
[25] 辛文.小学生破解刷脸取件刷脸支付躺枪，用脸支付到底安不安全？[EB/OL]. (2019-11-7) [2019-12-20]. http://zjnews.china.com.cn/yuanchuan/2019-11-07/196796.html.
[26] Iain Thomson. iPhone X Face ID fooled again by 'evil twin' mask[EB/OL]. (2017-11-28) [2019-12-21].
https://www.theregister.co.uk/2017/11/28/iphone_x_face_id_system_cracked_again/.
[27] Jeff John Roberts. Airport and Payment Facial Recognition Systems Fooled by Masks and Photos, Raising Security Concerns. [EB/OL]. (2019-12-12) [2019-12-29].
https://fortune.com/2019/12/12/airport-bank-facial-recognition-systems-fooled/.
[28] 高奇琦.人工智能：驯服赛维坦[M].上海：上海交通大学出版社，2018.
[29]孙保学.人工智能算法伦理及其风险[J].哲学动态,2019(10) :93-99.
[30]郧彦辉.数字利维坦：信息社会的新型危机[J].中共中央党校学报,2015(3):46-51.
[31] 央视财经.5000 多张人脸照标价 10 元，你的脸可能正被贱卖[EB/OL]. (2019-11-29) [2019-12-31]. http://tech.china.com.cn/ai/20191129/361337.shtml.
[32] 梅亮，陈劲，吴欣桐.责任式创新范式下的新兴技术创新治理解析——以人工智能为例[J].技术经济,2018(1):1-7.
[33]王小芳, 王磊. “技术利维坦”：人工智能嵌入社会治理的潜在风险与政府应对[J].电子政务, 2019(5) :86-93.
[34] New Scientist staff and Press Association. UK's controversial use of face recognition to be challenged in court[EB/OL]. (2019-5-21) [2020-1-5].
https://www.newscientist.com/article/2203953-uks-controversial-use-of-face-recognition-to-be-challenged-in-court/?from=singlemessage&isappinstalled=0.
[35] ERIC LUTZ. San Francisco, ground zero for surveillance capitalism, bans facial-recognition technology[EB/OL]. (2019-5-15) [2020-1-5].
https://www.vanityfair.com/news/2019/05/san-francisco-ground-zero-for-surveillance-capitalism-bans-facial-recognition-technology.
[36] 唐皇凤.数字利维坦的内在风险与数据治理[J].探索与争鸣,2018(5):42-45.
[37]IDC 发布最新版全球网络安全支出指南，中国增速领跑全球[EB/OL]. (2019-9-2) [2020-1-7]. https://www.idc.com/getdoc.jsp?containerId=prCHC45475719.
[38]谭九生，杨建武.人工智能技术的伦理风险及其协同治理[J].中国行政管理，2019(10)：44-50.
[39] 曝光市民睡衣照的人何以脑里少根弦[EB/OL]. (2020-1-21) [2020-1-21].https://guancha.gmw.cn/2020-01/21/content_33500426.htm.

[40]刘权.论必要性原则的客观化[J].中国法学,2016(5):178-195.
[41]闫世东.正当性：社会权力运行的基本原则[J].社会科学家，2013(3):39-41.
[42] 杨智杰.人脸识别十字路口：脸的恐慌[EB/OL].
(2019-10-21)[2019-12-11].http://www.inewsweek.cn/life/2019-10-21/7329.shtml.
[43]杜换涛.论个人信息的合法收集[J].河北法学，2018(10):34-44.
[44]项定宜，申建平.个人信息商业利用同意要件研究[J].北方法学，2017(5):30-39.
[45]王成.个人信息民法保护的模式选择[J].中国社会科学,2019(6):124-146.