

刷脸：身份制度、个人信息与法律规制

胡 凌

【摘要】人脸识别(俗称“刷脸”)技术已经在越来越多的场景下得到应用,既涉及公共服务场所和设施,也涉及私人服务行为。有必要超越对刷脸行为本身就事论事的讨论,而是深入刷脸嵌套和应用的具体场景,为未来其他生物信息的应用提供问题意识和理论框架。首先,刷脸是一种身份法律制度,起到身份认证功能,能够开启一个通向赛博空间的账户,从而延续了人脸作为通用标识符的社会功能。其次,刷脸意味着认证权力过程从分布式转向集中化,认证信息与载体的分离。再次,需要关注刷脸可能的风险,特别是背后的个人信息的自动化整合以及可能的使用方式与歧视、异化的问题。最后,网格和网络作为治理之理想类型的二分,为理解刷脸提供了有益的视角,同时也是场景理论的一个具体应用和延伸。

【关键词】人脸识别;身份认证;赛博空间;隐私;个人信息保护

【作者简介】胡凌,法学博士,上海财经大学法学院副教授。

【原文出处】《法学家》(京),2021.2.41~55

【基金项目】本文系国家社科基金重大项目“大数据时代个人数据保护与数据权利体系研究”(18ZDA146)、教育部重大攻关项目“大数据时代个人信息保护边界与策略研究”(17JZD031)的阶段成果。

引言

人脸识别(俗称“刷脸”)技术已经在越来越多的场景下得到应用,既涉及公共服务场所和设施,也涉及私人服务行为。关于使用这一技术的法律、伦理与文化基础,迄今尚未在我国本土语境下得到充分讨论。^①从中央到地方,我国目前开始逐渐出台一些针对作为生物识别信息的人脸信息的立法,^②部分规则主要涉及这一行为过程中的某些环节,例如公共视频监控^③、人脸数据作为敏感个人信息的搜集与使用等。^④刷脸技术的大规模使用,在人类历史上是全新的事物,不仅涉及有关肖像、隐私、监视的传统观念与制度,而且涉及国家认证能力、安全预防问题,还涉及刷脸背后相关场景下法益的保护和平衡。^⑤和任何其他技术形态一样,刷脸作为一种较为进阶的技术,是嵌套在之前较不智能的技术环境下得到逐步使用和更新

的;^⑥从较不智能到更为智能的技术装置的演进,能够帮助使用主体在更大范围内降低成本、开拓应用场景,同时也开始面临人脸数据泄露风险等疑问和挑战。^⑦由此,从法律角度对这一技术进行研究的惯常思路是,将刷脸视为人工智能(AI)应用的一种,从而分割成算法规制、场景化的数据使用规制、事后损害救济等一般性问题分别加以讨论,特别是人脸数据文件作为敏感个人信息的使用监管与保护。事实上,仅仅看到刷脸的算法与数据面向,不足以理解这一技术在中国乃至世界范围内的迅速兴起以及应用场景的制度逻辑,从而难以辨识技术使用的应然维度。有必要看到,刷脸的特殊性在于,它被广泛应用于社会主体不同身份的认证(authentication)和行为识别(identification)场景,从而也涉及人脸数据作为不同身份信息标识符的相关问题,因此有必要将刷脸放在一个更

为开阔的数字身份认证与识别的路径下进行讨论,以辨明这一技术应用的不同层次、主体和用途,进而在不同的应用场景下,按照该行业/环境的使用目的与惯例,通过成本—收益分析判断该技术是否可以以及应如何得到使用。受到广为关注的人脸数据泄露和歧视风险,也可以从这一视角找到解决路径。

本文将详细讨论刷脸在身份认证与识别场景中的原理及其法律应对。第一节从宏观维度对比传统网格社会和现代网络社会中刷脸的不同功能,从而将刷脸定位为一种技术—法律制度过程,强调其是社会治理中身份制度的重要环节,而非简单的技术应用过程。第二节将讨论身份认证中的刷脸,认为认证的实现过程,从传统物理空间中的分布式(人们亲自持有各类证件到不同场景中的权威机构进行认证),开始转向虚拟空间中的数据集中化(数据库中已经储存相关信息,只需要远程确认)。人脸作为新型身份标识符,可能起到广泛的表面上去身份化的效果,嵌套在实名身份认证体系中的刷脸,实际上会促成社会中身份认证权力在横向与纵向上的集中,而这对于作为平台的政府和企业具有不同的意义。第三节将讨论行为识别和追踪中的刷脸,以及人脸数据能否作为基础身份信息加以使用的问题。刷脸事实上为数据主体在物理空间中开启了默认账户,这在事前和事后产生了不同的功能。人脸数据在不同领域具有不同的法律属性,需要进一步区分为公共安全进行的追踪和平台企业对个人行为的服务追踪,并提供不同的信息披露要求。第四节进一步讨论作为个人信息的面部数据在具体场景中的风险,认为表面上的去身份化仍然有可能在实质上掩盖并加强社会性身份歧视等不公平因素,而未经授权的刷脸也会促成合并更多场景的个人画像,从而为个体带来不可预知的风险。因此,有必要深入不同的具体场景辨识技术使用的特定社会规范,防止通过刷脸形成的数据主体异化。

一、作为身份法律制度的刷脸

(一)人脸是通用身份标识符

尽管刷脸在当下数字时代更多地是与技术相互关联,但从社会性角度来看,人脸从来都是一种互相识别和验证的通用身份标识符。在传统的熟人社会中,人们主要不是像其他动物那样通过声音和气味互相识别同类,而是认脸。^⑧通过认脸(“认人”),熟人社会中的成员得以识别相互之间的社会地位和差序社会网络中的相对地位,从而使得人类种群得以稳定交往、合作,维系血缘和信任。由此,认脸能力意味着在看到人脸的那一瞬间,同时在头脑中反映出对方的姓名、称谓、社会身份甚至过往与其打交道的经历,如果不能很快记起并按照相应规范进行回应,那么会被认为失礼。和指纹、虹膜、DNA信息这些纯粹静态的生物信息不同,人脸具有重要的社会性(因此更多具有公开的而非私密的属性)和动态性(表情和皱纹都反映了内心变化与沧桑经历),我们很难完全拒绝来自别人的人脸识别(蒙面的社会几乎不存在),除非彻底与世隔绝。从这个意义上说,人脸、辨识人脸的技术、对相貌表情和人类情感关联的发掘,一直都构成了人类社群社会规范和环境的重要组成部分,已经逐渐形成社会制度和法律制度。刷脸和社群身份、声誉机制、集体记忆/遗忘、合作交往等机制一起,共同构成了长久以来的社会生活。因人脸和身份各异,甚至刷脸一词在现代还被赋予某种特权色彩,反映了不经正当程序就享受某些服务的现象。这些都说明,为了理解数字时代的刷脸,需要回到线下社会运作过程本身。

随着现代社会朝向陌生化和高度流动性转变,人脸的社会性意义开始受到削弱,人脸代表的对稳定小规模社群成员的认证意义,也被国家和单位组织提供的大规模认证职能所替代。新的国族和社会身份取代了传统身份,并通过“证件”“证明”这类现代治理工具得以维系,最终通过法律加以确认,国家和社会的认证权力由此展开。^⑨在此

过程中,身份法律制度逐渐兴起。例如,以《居民身份证法》为代表的国家认证制度,规定了作为“每个公民唯一的、终身不变的身份代码”“由公安机关按照公民身份号码国家标准编制”的身份证号码(第3条),及其发放、使用与查验方式。通过这一制度,居民获得了有效公民身份,并能真正成为负责的法律主体。^⑩

刷脸也正是在这个意义上获得了新的价值,其技术层面逐渐凸显(带有机器色彩的“人脸识别”说法更为普遍)。机器算法取代了人脑,替代其他社会成员对特定个体的社会身份进行认证与识别,人与人的关系愈加生疏,隐私和个人信息保护逐渐成为社会问题。通过快速登入账户与认证,无处不在的刷脸能够帮助在线交易和公共服务提升效率,成为一种极端的选择/退出机制和默认设置,而且还可能意味着(在成本允许的条件下)我们在每一个场景中的任何举动都需要认证身份、识别行为,并可被追踪。机器认脸的计算过程在逻辑上和人脑类似,即在比对面部数据的同时,访问含有该个体姓名、生日、身份证号码甚至犯罪记录等的数据库,将相关信息关联在一起做出决策。人机交互伦理和社会规范逐渐成为数字时代无法回避的问题。

大规模刷脸的背后,也反映了新型数字基础设施的构建。从法律治理和服务角度来看,在公共领域布置的公共视频监控终端,已成为智慧城市设施的重要组成部分,延伸到城市管理的诸多方面;从私人服务角度来看,以第三方支付为代表的刷脸应用,将不同的单位和组织连在一起,提供统一的支付系统(连带一般性的信息管理系统)服务。人机社会规范、新型基础设施与社会网络机制(如声誉评分、同侪合作、网络记忆、表情识别等)共同运作,辅助作为正式制度的法律正常运行,帮助降低流动性社会的交易总成本,有效应对社会失范现象,使得整个数字环境的可信程度大大增加,从而顺利地将传统的线下成员身份资格之间

的了解和信任,转变为经由机器自动执行的线上信任,^⑪最终促成了人类社会性的架构变化和重塑。通过大规模刷脸实践,社会成员获得了继身份证之后新的可信身份证明和通用身份标识符(新冠肺炎疫情期间则增加了作为健康码的二维码)。因此,抛开技术应用的外壳,数字时代的刷脸仍持续体现出强烈的身份法律制度属性。刷脸技术的使用,首先需要服从于制度的目标,即流动性的社会和法律治理。

(二)刷脸如何嵌入国家治理:从区隔到联通

从社会治理和法律治理的模式来看,上文提及的从传统社会到现代流动性社会的转型,也部分体现了从封闭网格(grid)到开放网络(network)的变化。^⑫在网格化社会中,流动性程度较低,社会成员在每一个网格中具有可辨识的不同社会地位和相对固定的社会身份,社会通过官僚制组织和具有外在强制力的成文法律规范进行治理。为确保本网格的安全,且使社会成员享有相应的权利、履行义务,需要由外在组织赋予固定不变的身份,并给予具有法律效力的证明文件。于是,不同层次的身份认证就变得不可或缺,各类证件的使用成为常态。而从查验身份证件到人脸识别的转换,仅折射出通用身份标识符形态的变化,实质上没有区别。在这一阶段,个人信息的收集和使用,主要被用于网格内的区隔认证(若超出则无效,价值效用会降低),并可以动员群众参与治理,大规模个体的行为痕迹对网格化治理的意义不大,只是被用于个别情形中的事后证据收集与事实认定,从而通过法律和单位组织的次级成文规范进行惩罚,形成潜在威慑。^⑬

在网络化社会中,不同网格被吸纳进同一个流动性更强的高维网络之中,社会成员的身份变得多元,统一的跨越网格的数字身份认证替代了独立分散的验证措施。新的在线社会强调通过信息技术和社交网络的“连接”和“联通”,由此形成了“点赞文化”等声誉机制和社会机制。^⑭正如下

文将详细阐述的那样,此种社会连接是被互联网平台面对不特定用户不断通过身份认证和行为识别重新塑造出来的,这和表面上宣称的以通用身份标识符进行“去身份化”实践并不完全相符。当在线场景大量集中在一个平台上时,用户的数字身份就可以通过进一步挖掘数据得到塑造,在不同的传统场景下获取用户行为习惯偏好,向其有针对性地推荐广告和商品,从而更好地使多元社会身份为用户的消费者身份服务。在数字社会中,人与人之间的人脸直接识别仍然存在,并维系着不同的社会网络,但在更多情况下,通过无处不在的大规模机器间接识别作为中介,才能确保流动中的安全、秩序和信任。只有在这一阶段,大规模的个人信

息可以跨越场景使用,具有更多关联和挖掘价值,可被用来帮助预测个体行为,进行更多事前预防。也因此,对其的保护与风险防范,以及对数据分析的算法权力的警惕,才成为新问题。

下表将网络和网格中的刷脸及其特征进行了对比,能够进一步凸显不同场景技术—法律制度的治理意义:

理想类型 要素	网格	网络
场景特征	流动性低的区隔性	流动性高的联通性
人际关系	熟人	陌生人
信任感	具体信任	抽象信任
安全机制	通过成文规则事后惩罚威慑	通过信息预测评分,事前预防
主要用途	确认成员资质,前台展示	联通数据库追踪,后台分析
认证方式	认人或物理证件	数字化人脸数据文件
个人信息使用	非集中化储存使用,风险低	集中化储存使用,风险高

网络社会中无处不在的摄像头代表了“权力的眼睛”,可能会给社会主体带来压迫感,但问题不在于技术本身,而是由于大规模流动性导致稳定的社会秩序和社会关系难以短期形成均衡,从

而很难让传统熟人社会中的各种机制和不成文规范再次发生作用并降低风险。因此,刷脸不过是嵌入当代社会治理过程的技术—法律制度形态。它是为了应对流动性而存在的,是总体安全和信任的一部分,而不单纯是一种中立技术。只有深入理解这一技术—法律制度是如何在不同场景下得到内化和使用,才能更好地评估其成本和收益。

二、刷脸与认证权力的集中化

(一)当认证权力遇见刷脸

人脸识别技术的提升,首先是基于早期互联网时代数字化照片的流行,大量免费的在线人脸数据集,为人工智能机器学习能力的开发奠定了基础;^⑤其次,由于家用和公共摄像头的增多,以及智能手机和数码相机的普及,大众对到处充满镜头的社会环境的接受/容忍程度日益提高;^⑥最后,刷脸技术逐渐变得成熟,被更多地用于公共服务,成为一种身份认证的方式和数字基础设施服务,在打击犯罪、维护公共安全方面也起到了积极作用。人脸在法律上长期以来仅具有肖像权的私法意义,现在则能够被大规模数据化,成为一种认证口令、敏感的个人信息和数字经济的生产资料。人脸识别精确度是一个逐渐实现的过程,经过前期大量的人脸数据集训练,人工智能有能力精确区分人和其他事物(这对无人驾驶汽车和其他智能化产品非常关键),甚至每一个特定的个人;一旦连接到更多数据库,还能对该个体的身份和背景信息有更多掌握,且机器不会因人脸的些微变化而遗忘或误认。^⑦刷脸的大致技术过程是,首先需要被识别者提供本人较为清晰的照片录入数据库,然后利用计算机视觉技术,通过相关硬件上的摄像头/屏幕在经由扫描收集到的真实人脸图像上进行特征参数标记,形成虚拟3D模型,从而转化为一个实时的人脸数据文件,最终将这一文件与数据库照片进行对比,以判断是否为同一个体。^⑧识别精确度依赖于不断改进的人脸图像标注算法。例如,在新冠肺炎疫情期间,一些公司开

发出新型算法,甚至能基于有限人脸样本识别出佩戴口罩的小区居民。^⑩

认证制度是国家的核心法律制度之一,通过为公民创设唯一的权威身份、颁发身份证件,并通过这一证件对人口、税收、公共服务等方面的统计调查,国家能够实现有效治理。^⑪随着单位和社会组织的兴起,不同的组织、协会也会相应地对其成员围绕各自颁发的社会身份进行认证,认证权力也更加泛化。在互联网时代,作为生物特征识别之一的人脸识别技术逐渐推动一场“身份认证的革命”。^⑫公共服务场所(例如机场、火车站、宾馆)通过刷脸确认需要使用交通、住宿服务的旅客,某个企业用刷脸让员工打卡进入其办公区域,支付宝通过刷脸确定用户有权进行大额资金转账,它们的目标都在于确保享有特定资质的主体以真实的给定身份(公民、消费者、员工等)进行活动,享有权利,接受服务。人脸具有普遍性、真实性和唯一性的特点,可以作为成本较低的一种生物信息标识符。作为人的自然属性,人脸并非一种天然的社会身份信息,对于传统的社会组织来说,可以将其和代表身份资质的身份证件结合起来使用。^⑬而对于那些并不强调身份特征的、为大量流动性用户提供服务的组织而言(例如互联网平台),刷脸技术会更受欢迎。

传统身份证件在认证过程中的功能,包括:(1)对外展示特定身份信息,既可出示给第三人查验,也能体现颁发者的不同权力等级和效力差别(例如国家颁发的身份证不能等同于校园卡);(2)对内作为一种资质证明,在不同领域行使特定权利义务的凭证,很可能是一串数字编号,甚至可以机读。相应地,通过刷脸进行的身份认证,能够通过实时对比认证对象和后台数据库基础信息,无疑降低了认证主体和被认证对象的成本。对前者而言,省去了人力和传统证件的对比查验过程;对后者而言,免去了身份证件丢失补办的麻烦。这意味着刷脸使证件的对外展示部分消失了,人

脸从而成为一种替代各类证件的、能适用于各类不同场景的通用身份标识符,从外部看不出不同的社会身份(无论是公共关系还是私人关系),但成员的资质信息本身嵌入在背后的数据库和计算过程当中,从而实现了信息与物理载体的真正分离。从表面上看,此过程似乎是由数字系统取代了物理证件,即人(脸)+物理证件→人(脸)+数字系统,但实质上是数字系统背后的数据库比对过程替代了人和物理证件之间的匹配关系(持有身份证件、目测相貌比对),从而更加精准。

刷脸认证的逻辑过程涉及两类人脸数据,一类是基于在先法律关系所收集的人脸照片,另一类是实时生成的人脸数据文件。第一步是收集人像照片形成基础人脸数据库,这是由在先的特定法律关系决定的(由权威来证明你是谁,授予身份,是否做到知情同意),第二步是对已经收集到的图像进行使用(也需要告知),先是对真实人脸的实时拍照生成新的人脸数据文件,再用这个数据文件与事先收集的照片进行比对,即相当于使用一个基础人脸数据库,能否联通到更多数据库获取信息,还要看是否明确告知被认证的个体。

就通过信息系统的认证而言,通用身份标识符的出现,使得原来通过用户名和密码登录账户和身份认证这两个行为合二为一,变得更为简易。也就是说,刷脸事实上帮助用户开启登录了一个单独账户,以人脸更加方便地取代了账号信息,并开始积累行为数据。这意味着认证基础设施的升级,在一定程度上能降低传统身份证在认证过程中发生泄露的风险。此类风险在早期实名制的实践中较为突出,当时很多网站在登录后要求用户上传身份证件照片或号码而未采取加密措施,造成大量用户身份证信息失窃并流转于黑市,甚至可能被用来骗贷、虚假注册公司,结果影响到个人社会信用。而如果账号信息(现在是人脸)本身能够承担登录和认证的双重功能,那么避免使

用基础身份信息,就可以降低此类风险。

(二)刷脸认证的两种思路

然而,如果刷脸技术取代不同的账号信息,被相当广泛地在公共领域和私人领域当中使用,那么有可能会造成如下后果:公共和私人用于认证身份的基础信息标识符被混同。除非人脸数据文件因算法和技术水平不同而有差异,但就其表现在外的实际过程而言并没有差别,进而取消了一切票据和证书所代表的时空、法律和社会意义。^②早期的互联网治理实践也表明,基础身份信息(身份证仅表明公民的政治身份)不应当被广泛用于各类社会服务,而应当仅限于公共权力机关提供的公共服务或重大交易场景(例如参与交通、金融、医疗、教育、购置车房等),否则的话,如果连普通交易场景都要查验身份的话,那么一旦泄露,便可能直接影响当事人的重大人身和财产安全,也会淡化基础身份的价值。如果放在网格模式下,那么这种担忧更容易理解,它代表了一种“分散认证”思路,即不同身份证件应当被用于区隔领域单独使用,而不会发生混同,目的是确保符合资质的人有资格从事某些活动,并防止他人盗用资质和相应的资源。尽管证件化的社会生活一直在不断扩张,人们拥有的各种代表社会身份的证件/证明也越来越多,但分散认证思路及其实践在互联网产生之前的物理空间中一直运转良好。

在互联网上,这一趋势开始终结,很多网络服务提供者没有能力——向用户颁发带有成员身份性质的独一无二的证书,^③而是放任用户使用自己的用户名或邮箱进行注册,它们仅关心账户的使用行为(是否消费或付出了注意力)而非用户的各种社会身份及其真实性。看上去这意味着赛博空间的逻辑开始压倒物理空间,趋向一种“去身份化”逻辑,即主导赛博空间的平台企业向大量不特定用户通过创设账户的方式发放虚拟身份证明以推动数字经济生产。截至目前,人们在赛博空间中并不拥有真正稳定的法律意义上的普遍虚拟身

份,即使有实名制认证,也不过是线下基础身份的映射。如果说互联网用户仍然有某种普遍社会身份的话,那就是“消费者”,传统的社会身份只有统一在消费者这一标签下,才生出新的意义(例如生产相应的行为数据)。

虚拟身份的匿名性,无疑带来了非法信息传播、诈骗等诸多网络犯罪问题,因此国家计划推行统一的真实身份认证,以便于识别追踪,于是就产生了“集中认证”思路。集中认证的理念是,面对互联网大规模服务去身份化的服务能力,为降低基础身份信息混同的风险,仍然需要使用某种超越各类传统身份信息的统一标识符,要么是线下二代身份证的映射(例如公安部第一研究所开发的二代身份证数字版CTID,甚至通过“一网通办”平台自建APP),要么重新创设赛博空间中的新基础身份(例如公安部第三研究所开发的eID)。

由此可见,认证方式已经出现了分散认证(网格化)和集中认证(网络化)的明显路径区分,刷脸在这一背景下产生了截然不同的后果。对前者而言,任何物理空间以及设备都可能通过刷脸进行用户身份认证,因此可能产生不同的人脸数据文件,分散在不同的认证主体服务器上,监管起来成本较高。正是刷脸技术的普及,将赛博空间中的控制/生产逻辑扩展到物理空间中,完成了完美的空间分割与封闭。这对线下封闭组织的秩序管理和资源使用有一定的好处。对后者而言,依托于平台的特定APP都可以集中使用手机硬件或平台提供的人脸识别功能,平台作为认证代理人,既能够降低监管成本,也能降低中小APP的运营合规成本。类似地,大型平台的第三方账号登录机制起到同样的功能,将经过认证的本平台服务账号扩展到更多第三方服务上,从而成为一种基础设施服务。从这个意义上说,大型平台企业有能力率先提供较为安全的人脸识别服务,既方便了用户,又能够通过延伸至更多APP而获得流量,成为其竞争优势,此外还可以帮助降低监管成本和创

业成本。

刷脸技术在嵌入上述两种认证思路的过程中变相推动了集中认证。这主要是因为大量私人服务越来越多地使用刷脸帮助消费者登入账户,待技术成熟后,进一步将其推广至线下诸多场景乃至传统组织。这反映了赛博空间覆盖物理空间的另一条路径,即表面上帮助单位和社会组织维持既有身份认证体系,但通过技术系统渗透其中,不断增强对其成员进行的行为识别和追踪,以技术便利换取(传统组织无法处理的)行为数据。由此,刷脸客观上促成了社会中认证主体数量的减少和认证权力的集中,人脸作为一种自然生物信息不会取代各类社会身份,但开发人脸识别技术的服务提供商者试图将这一自然身份逐渐凌驾于多元社会身份之上,成为激活各类社会身份与活动的口令和钥匙。

三、行为识别与人脸数据的法律性质

(一)公共机关与人脸识别

当下引发较多争议的是通过刷脸进行的行为识别,这不仅进一步凸显公共机关和私人服务提供者的差别,而且也有助于厘清人脸数据在网格/网络不同语境下的法律性质。本节将分别讨论公共机关和私人服务中通过刷脸进行行为识别的法律问题。如前所述,对特定个体进行身份认证后,刷脸事实上自动开启了一个虚拟账户(取代手动账户登录),同一个账户可以继续用于积累数据和跟踪,识别出特定账户使用者的行为,从而持续定位同一个人。鉴于刷脸的成本较低,它更容易被使用在不同场景中的明示接受服务活动。刷脸开启账户的行为同时具有事后追踪和事前预测两种功能。从公共机关的角度来看,为确保公共安全需要,较早地使用身份证作为定位公民在公共场所活动(从酒店旅馆入住到公共视频监控)的唯一标识符,在应用刷脸技术后,相关账户积累了认证对象的相关活动,能够起到事后追踪、提供证据的功能。^⑤例如,多年以来的公共安全视频监控建

设,使城市中遍布摄像头和传感器,^⑥可以汇集到公共安全应急指挥中心或其他警务平台(最近升级为智慧城市的“城市大脑”之一部分),公共区域的摄像头也从单一的录像存储功能升级为可动态识别认证对象的刷脸功能,越来越成为一种信息基础设施和默认技术设置。在这一过程中,摄像头背后的算法会自动将获取的人脸数据与更多特定数据库(例如犯罪信息数据库)进行比对匹配,从而能很快锁定交通肇事者、犯罪嫌疑人或普通违法者。此为与仅仅访问基础身份数据库之认证过程的不同之处。

人脸数据的法律性质在识别阶段就成为一个问题,即在多大程度上被识别个体能够“同意”其人脸数据可以对接不同数据库中进行比对,这需要根据不同法律设定的场景进行辨别。例如,人脸数据文件是否是《居民身份证法》意义上的基础身份信息,或是《网络安全法》意义上的(敏感)个人信息。作为生物性的通用标识符,人脸数据文件未必天然能够成为基础标识符,而是需要国家的强制性认可。^⑦尽管现有规则将人脸界定为主要的个人信息或敏感信息,但其在性质上仍然是一种可采集的自然生物信息,在地位上不具备由国家授权发放或确认的条件,也不能对外展示证明身份,只能与身份证结合起来使用。在技术层面上,人脸数据文件也无法被看成是固定不变的基础身份信息,因为不同识别主体使用不同的技术和算法生成的人脸数据文件是不同的,这取决于算法、摄像的像素以及建模的颗粒度等因素。从这个意义上说,一张人脸可能对应着完全不同的人脸数据文件。^⑧就此而言,人脸数据并非一种认证意义上的单一基础信息和身份证明,而是必须依托权威的认证系统及其背后的官方数据库加以辅助说明,它本身只能是一个激发各类身份技术装置的口令(即用户名和密码),实质性的身份认证仍然需要在后台进行。鉴于人脸识别技术有能力对所有社会个体进行识别,远远超出了我国法律

规定的应当申领身份证的16周岁范围,则这一技术的使用将在身份证制度以外创设出一套新型的个体识别体制,并能够打通原来各种各样的身份证件数据库,例如居民身份证、护照、户口簿、机动车驾驶证、军官证等军(部)队身份证明、往来港澳通行证、大陆居民往来台湾通行证等。

因此,通过摄像头的针对不特定人的刷脸行为,就可以被视为一种以人脸为媒介的大规模实时身份信息查验(包含了认证与识别过程)。根据《居民身份证法》第15条的规定,在程序上核查实体身份证,需要查验主体(如警察)表明身份和意图,而通过公共摄像头的无人身份查验,只能以加强信息披露的方式增强合法性。例如,不能简单地说明特定位置安装的是公共安全摄像头(这只是表明安装主体和目的),还需要针对三种不同的功能分别标识,并以可视化的图像加以呈现:(1)单纯的录像和存储;(2)通过人脸进行认证;(3)收集人脸数据文件和其他数据库进行比对分析。^②这还能在事前起到提升执法威慑强度的功能,其效果会大大优于一一般性的警察安全巡查。如果按照这一逻辑开展公共安全视频制度建设,那么就需要对《居民身份证法》进行修改,授权“电子警察”为公共安全的需要在某些区域以不间断的方式通过刷脸进行身份证查验,并以合理方式(可见标识、短信等)告知进入该区域的公民正在被查验,从而和线下查验行为相匹配。

这一行为若涉及访问犯罪数据库或任何其他执法数据库,则可被解释为一种在公共场所开展的基于公共安全的大规模执法/侦察行为,需要公众更加有效的认知和配合,而非对个体肖像权的侵犯。^③基于公共安全而设置的刷脸,超越了私法意义上个人信息使用的“知情同意”原则,但仍需要在形式上告知展示,这里涉及的更多的是对公民在公共场所行为信息的收集和处理,已经进入了公共数据的范畴。^④一般性的人脸识别摄像头,对普通人在公共场所的行为尚不构成足够的压

力,缺乏针对性,而在机动车驾驶的特定场合以及行人过马路的十字路口,刷脸技术对特定违法行为的捕捉越来越容易,可以精准定位到个体,就会给当事人带来直接的压力与合规动力。^⑤

公共机关的刷脸识别行为,会改变传统技术装置下的公私权力关系。首先,它进一步延伸了自边沁(Jeremy Bentham)、福柯(Michel Foucault)以来的“全景敞视监狱”的监视逻辑,^⑥即通过无处不在的摄像头在社会中表明“权力眼睛”的存在,能够以有效提升发现违法行为之概率的方式,增加对潜在犯罪行为的威慑。在这种情况下,事后惩罚就开始变得没那么重要,普遍的事前威慑才是刷脸更加重要的社会功能。甚至身份识别本身不一定真实发生,只要大众相信有可能发生,就会有效地进行自我约束,从而遏制潜在的不法行为。

其次,人脸识别有能力无差别地适用于刑事违法行为和普通违法行为。原来因违法活动等级的差别而使得国家资源不得不投入到那些更重要的领域,而现在公共机关则可以无差别地监控在逃嫌疑人、交通肇事和普通的行人闯红灯行为,并自动分类实施处罚。如果从一般公共执法行为上升到刑事侦查行为,那么需要更进一步做好刑事程序合规,例如,(1)严格规范技术侦查措施事前审批程序;(2)特别是侦查过程中获得的人脸数据文件需要单独收集储存,获悉的秘密内容应当保密,获取的与案件无关的人脸数据应当及时销毁;(3)明确被识别个体对技术侦查措施的事后知情权以及求偿权等救济性权利;(4)完善通过技术侦查取得证据的使用规定,等等。^⑦

再次,刷脸背后的数据库接入与分析,无疑能扩大公共机关(特别是公安机关)的执法和取证能力,不仅可以迅速比对公共数据库,而且还能够将监控摄像头延伸设置在小区、商场、学校等组织,即它们拥有的录像或服务器在某些情况下能够连通至当地公安机关的监控平台,变成了公共空间(有争议的)延伸。这更需要做好程序上的知情展

示和民众沟通参与。

最后,由于人脸是个体表露在外的进行社会交往的公开媒介,个体仍然有足够多的选择和能力避免被识别,例如对头部和面部进行全部或部分遮掩。^⑤这也说明了即使是在非私人空间中,也存在一定程度的隐私期待,人们会对未经授权使用摄像头在公共场所以安全为名进行录像的做法感到反感。^⑥这种社会态度,不单纯是简单区分公共权力和私人权利的问题,而是摄像头(权力)的可见性,人们可以接受公共场所针对不特定人的监控,但却无法接受直接针对自己或私人空间的摄录行为。可以设想,大规模常规刷脸终端设备的出现,可能会变相推动遮掩面部社会规范的形成(新冠肺炎疫情期间已经形成了佩戴口罩的习惯和社会规范)。由此有必要规范公共安全视频安装的位置和数量,增强信息披露和公共空间内可见的威慑。

(二)私人服务与人脸识别

越来越多的私人服务提供者使用摄像头和刷脸技术,这主要体现在支付领域和安全防护领域,也出现了不经告知的违法偷拍直播。在私人主体使用刷脸的场合,应当执行知情同意原则作为约束,明确展示说明摄像头和终端的功能。这意味着在一些无法对摄像头及其功能进行展示披露的场合,刷脸将无法合理地被使用。和其他个人信息一样,如果人脸数据不是该项提供的服务必须收集的话,那么用户有权拒绝以刷脸方式开通一个账户并积累其活动数据。

私人服务提供者基于默认的用户协议生成、获取和使用人脸数据文件,并可能主张这一文件因为企业投入技术劳动而创设,有权排他性地使用这些作为生产资料的数据(例如训练人工智能)。只要使用过程能精确识别和还原到特定主体,对同一人的行为进行追踪,那么对人脸数据文件的使用就可被认定为使用个人信息,从而需要遵守一系列个人信息保护规范,法律提供的可能

救济包括知情权和删除权等。^⑦

私人服务提供者(特别是平台企业)通过刷脸帮助用户开启新账户以后,产生的行为数据就会在事前对用户未来的活动产生约束,这就回到了数字经济的生产过程。^⑧社会主体的在线身份不再是某个组织通过外在证件赋予的,而是使用服务的事前资质和事后活动的集合,数据集(及其不断挖掘的实践)构成了新的社会意义上的动态在线身份,为整个新经济的价值生产服务,人脸数据只是这一生产过程中的一环。^⑨应当看到,刷脸通过互联网应用大量普及,本身加速了数字经济的生产、交易和资源流动,即确保活动主体的唯一性和行为的连贯性,由此通过刷脸而积累活动数据,使得身份识别只有在网络在线场景下才具有更大价值。对网格化的传统组织机构而言,认证与识别过程相互分离,不会混合在一起;由于成员的社会身份是默认给定的,在必要时,单位或社会组织只需进一步追踪成员活动即可。但通过网络化平台和数字系统进行刷脸,认证和识别这两个环节就完全可以无缝融合在一起,以认证统摄识别,从而产生了诸如基础信息泄露等风险。下文将讨论此类风险大小和预防问题。

四、个人信息、刷脸风险与法律应对

(一)刷脸的风险与一般性规制

公众舆论和不少研究者往往会担心,一旦刷脸技术普及,则作为生物信息的人脸数据文件会遭到大规模泄露,使得作为通用标识符的身份信息被伪造和滥用,进而带来无法预估的损失。^⑩按照一般个人信息保护思路的讨论,人脸数据作为敏感个人信息,需要经过更为严格的程序处理,刷脸风险集中于采集、存储与数据分析三个环节。

在数据采集环节,实际上只要满足形式上的知情同意规范,说明采集的目的与用途,就很难完全阻止针对人脸或照片的数据采集。在数据存储环节,讨论者普遍认为可能会发生人脸数据泄露风险,考虑到人脸具有唯一性,一旦泄露,则会带

来难以弥补和想象的损失。^④按照这一说法,其主要的假想前提是:(1)在大量的重要场景中,刷脸认证设施十分普遍,这一点正在逐步成为现实;(2)非法获取者用他人面部数据制作3D模型或物理面具,^⑤进而伪造篡改其在线身份,^⑥或冒充刷脸。^⑦此类观点的问题在于:首先,泄露风险究竟有多高,仍然很模糊,而只是强调“无法预估的”风险难以进行成本—收益分析,至少目前人脸数据失窃不像银行卡账号密码或身份证失窃那样显著,概率也不比后者更高。^⑧其次,需要区分事先收集的人脸照片和实时生成的3D数据文件的不同风险,前者自互联网产生以来一直都存在,并且已经形成了大量数据集,但后者则更为关键。第三,至少是目前,伪造面部模型行动的成本太高,几乎难以大规模进行,对追求低成本获利的“黑灰产”团队而言得不偿失,^⑨只要认证主体采用多重因子认证或人工审核,就能解决大部分的安全问题。因此,尽管人脸数据失窃很耸人听闻,但这并非从真实的成本—收益分析加以测算,而更多地是由于人们对极具人身属性的面部在心理上十分敏感,经过大众媒体的宣传放大,变成了似乎不证自明的道理。从实际来看,对特定主体人脸数据文件的滥用,并不比未经许可传播或商用其照片所带来的人格权损害更多,甚至远远低于身份证和电话号码失窃的概率。易言之,大众之所以会内心中觉得脸被盗刷后引发的风险更大,不仅是因为它是一种生物性信息隐私(指纹更容易被收集,但没人在意),更是因为它的公共属性,即传统观念中将人脸作为进入社会网络的重要标识,代表了社会身份,一旦被盗刷,则可能意味着失去(虚拟)社会地位和信任,最终丧失社会行动和交往能力。当然,上述分析并不意味着就可以忽视大众舆论和态度,而是强调需要不断平衡使用刷脸技术的政策目标和风险,保持大众对这一技术使用的信任,防止过度恐慌。

除了极端情况下的人脸数据文件被伪造冒

用,刷脸的真实风险主要在于实质性知情同意的落空。人脸一直会暴露在社会生活和工作过程中,一旦人脸成为单纯的账户登入或支付口令,则就相当于将用户名和密码完全暴露在外,很容易通过远程刷脸被非法使用,造成不知情情况下的人身财产损失。在一些情况下,甚至还会造成所属单位和网格的相关潜在权益受损。^⑩人脸数据泄露的主要原因,恰好在于其易用性和有效率,一旦当通用标识符被大量认证主体和场景广泛收集采用时,它自然会成为“黑灰产”犯罪团体关注的对象,从而导致其失窃概率增大。人脸数据也可能与二维码等标识打通,与电话号码、身份证一样都指向唯一不变的个体,如果通用标识符的展现形态过多,那么其泄露风险就会增加,并冲淡其认证价值。此外,相关人脸数据文件或照片可能被自动化地上传至特定数据库进行实时比对和关联,导致没有经过认证对象的知情和授权而脱离场景地理解和使用人脸数据。对于此类人脸识别搜索引擎和自动化整合服务,有必要加以限制。

因此,在人脸数据的采集和储存环节可以进行如下制度性规制:首先,需要认识到,没有哪一种单一的认证方式是绝对安全的,双重或多重因子认证尽管成本较高,但却是提升安全概率的必由之路。在需要确保信息安全的领域,应当强制要求多重因子登录识别。其次,按照分类分级原则系统规划不同场景中认证的方式,防止基础身份和次级身份混同。例如,刷脸可被用于公共服务或需要基础身份认证的重要场景,但要限制普通私人服务通过人脸或身份证进行直接认证(除非采用eID加密技术)。再次,可以限制留存实时生成的人脸数据文件的时间,降低泄露概率。最后,强化对人脸识别软硬件的专业认证措施,采取类似网络安全分级制度进行分级管理。对于那些落入基础设施领域的刷脸服务,需要加强诸如牌照管制一类的特殊监管方式,这将有助于提升和统一技术标准与安全标准,使刷脸变成稀缺性资

源,从而避免向社会更大范围的服务提供者提供,激励后者转向开发其他安全的身份认证手段。^⑧

在数据分析环节,由于人脸的公开性和社会性,其作为自然属性的面部信息能够在一定程度上被赋予社会意义,即不可避免地肤色、表情、五官等因素放在一起,展示出某种统计意义上的社会评价(性别、阶级、肤色,甚至同性恋和成人视频演员等),由此只要拥有足够大的样本,就能够通过分析给特定主体贴上标签,进行精准差别对待(歧视)。目前出现的数字歧视行为表明,表面上的去身份化的刷脸服务,可能会在技术平等的意识形态下掩盖黑箱中持续的身份歧视,人脸识别只不过为服务商或认证主体提供了更加广泛和低成本的服务而已,发生的变化,只是客观上用统一的账户体系取代多元化账户体系。在中国语境下,在多大程度上能够产生社会性歧视行为尚有待观察,当下可能更值得关注的是消费者歧视问题(例如大数据杀熟)。

(二)场景化规制的方法论反思

场景理论作为数字隐私保护的新型路径已得到了诸多讨论,甚至也可以扩展到对一般性技术(例如算法)进行规制的讨论。本文将推进这一理论的积极意义,即探索如何具体地发现和界定场景,从而理解某种特定技术在嵌入既有制度环境之后应如何应用的问题。单纯的个人信息保护与算法规制研究的惯常思路是,将算法与个人信息看成是基本上在真空中就可以运行无误的制度,处于核心地位;即使进入具体场景展开讨论,也只是自上而下地阐释基本原则和规则,进而消解了场景的特殊性和自主性。^⑨这种思路不太符合现实实践,未能看到这些问题的发生实际上依赖于技术设计、从属于需要该种技术的在先制度逻辑,也遮蔽了作为一种制度的技术本身运行的真实状况,从而难以合理地评估个人信息保护的程度以及平衡效率导向的技术目标与场景中其他社会规范、大众认知与参与之间的关系。类似地,比例原

则要求对个人信息的使用和收集须与其应用的政策目标相匹配,而这也要求我们进一步讨论如何在理论上建构场景及其制度逻辑。

前文的讨论已经充分表明,刷脸技术是逐步嵌套进公共和私人的不同场景中得到应用的,不可能也没有必要凌驾于既有行为目标和规范之上,只有首先理解认证/识别中身份权力机制的演变,才能更好地界定场景,进而在问题集合中寻求个人信息/隐私问题的适当定位和解决方案。具体而言,第一步是要看到数字身份在社会转型中的重要意义,将其放置于网络/网格模式二分中进行讨论,这决定了不同场景中政策目标和实施效果的本质差异。第二步是将认证/识别设定为划分更为具体的场景的标准,鉴别出达成共识的某种法律关系,进而区分出公共机关与私人服务提供者的不同制度性约束,包括该行业/环境的使用目的与惯例等,理解技术如何进入既有制度设计,并成为制度的一部分。最后一步则是,在需要强化个体权利时,进一步讨论具体个人信息保护与算法监管的规则细节,根据成本—收益分析评估风险,形成解决方案和政策建议。

按照上述这一方法论思路,还可以稍作延伸,讨论刷脸在上文未涉及的其他热点领域的应用及其法律问题。它们都超出了单纯个人信息和算法的范畴,而是需要回溯至该场景的基本法律关系和原则共识。例如:

其一,教育与情感计算。在诸如学校课堂的教育领域,摄像头和人工智能可以帮助教师记录和分析学生的表现,潜在地提升考试分数,但这会把教育和学习过程完全变成像富士康工厂那样的机械生产流程,成为分数教育的一个缩影。^⑩问题还在于,人工智能无法精准判断人在特定场合的表情和行为(一些学生们之所以没有专注听老师讲课,很可能是因为已经学会了),故而总是存在着(机器性)权力无法深入和理解的特定社会空间。学生们自主学习的潜在能力可能会因此受到

干扰和侵犯,所以应当对学校的类似活动进行法律限制。

其二,雇主监视。雇主会通过刷脸加强对雇员的监视,特别是在远程办公或灵活用工的情况下。这可能会造成劳动者在工作场所中进一步丧失隐私,强化了雇主对劳动过程的控制权力。在开放的灵活用工平台上,平台所有者通过刷脸对平台上数字劳动者加强控制力,其行为可以被解释为人身/经济从属性的一种司法标准,从而为数字劳动者争取权益。^⑤

其三,社会规范。违法行为(例如闯红灯)监控往往通过头像展示和嵌入社会信用的方式加以约束。^⑥这降低了公共机关的行政总成本,但必将增加个体合规成本,即对人机规范和机器执法方式的认知成本。例如,现有的道路规则及其标识变得越来越繁复,需要司机完全集中精力进行驾驶,稍有疏忽,就可能会被无处不在的刷脸捕捉到,进而被判定为违规,最终被扣分。现在这种认知负担已经从驾驶活动扩展到日常活动的许多方面。从这个意义上说,不能仅因为实施成本低就盲目使用刷脸技术和扩张权力对个体行为的约束空间,而是应看到个体认知成本的约束,将一部分底层社会行动空间继续交由个体熟悉的社会规范,否则普通人将会因无法认知大量规范而持续违规,威慑也难以起到作用。

结语

刷脸是赛博空间不断扩展的必然阶段,但很可能只是伴随新技术开发的生物信息认证的诸阶段之一。有必要超越讨论单纯的刷脸行为本身,而是深入刷脸嵌套和应用的具体场景,为未来其他生物信息的应用提供问题意识和理论框架。从经验来看,刷脸技术服务于一个设定空间中的两种不同层次目的:(1)外层的身份认证,即确定某个个体是否有资质和权利使用某种服务(无论是公共的还是私人的服务),验证“你是谁”;(2)内层的识别与追踪,即在确定资格之基础上通过同一账

户对成员/用户的行为数据进行积累和分析,证明“你是你”,同时在各场景内进一步获知和间接影响数据主体的行为,使其按照不同的政策目标行动。上述两个层次会涉及个人信息保护及算法规制,但更多是涉及制度性原理,比如说为何需要认证/识别、围绕此行为构建出来的主要法律关系,以及这一技术如何嵌入、推进、解决或改变已有的问题意识。即使需要在特定场景中讨论,这一路径也和流行的“场景化隐私”研究有所不同。场景理论声称需要寻找不同场景的具体规范,但并未展示如何在特定场景中应用该理论,因此就自我消解了。只有首先理解认证/识别中身份权力机制、法律关系的演变,才能更好地界定场景,进而在问题集合中寻求个人信息/隐私问题的适当定位和解决方案。例如,在认证层面,收集人脸作为认证信息越来越成为无须选择的默认设置,只能根据不同行业需要加以分类限制;而在识别层面,则需要加强程序性的明示告知,尊重人们的选择。

刷脸在名义上代表了一种普世的效率导向的技术应用,伴随着后台更多数据库的联通,公权力机关在公共安全方面能够无缝切换地在不同场所持续追踪违法者或嫌疑人,而提供私人服务的平台企业则可以推动更为高效的支付、交易和其他服务。^⑦特别是后者在某种程度上率先推动了认证权力在赛博空间中的泛化和集中,在帮助诸多线下主体加强认证过程的同时,表面上推进了一种打破既有传统组织边界的“去身份化”社会过程,但实质上是通过普及刷脸来获取更多传统场景下无法获得的行为数据,并重新界定和塑造流动的多元社会身份。由此,刷脸不单纯是一个社会身份查验过程,它也意味着身份认证和行为识别系统在社会范围内的重塑。中国的社会治理正经历着从网格模式(grid)向网络模式(network)转变的过程,认证/识别在这一过程中的功能有较大差异,从而带动作为个人信息的人脸在不同场景下产生不同的意义。

本文的初步研究结论是,首先,刷脸是一种身份法律制度,起到身份认证功能,能够开启一个通向赛博空间的账户,从而延续了人脸作为通用标识符的社会功能,这意味着认证权力的极大增强。其次,刷脸意味着认证权力过程从分布式转向集中化,认证信息与载体的分离。在实践中,法律对公共机构和私人机构的刷脸实践之要求是不同的,但通用标识符可能进一步模糊了公共服务和私人服务的界线,导致不同身份与权限的混同,形成了从(社会身份)认证到识别的转换。在法律上仍然需要区分对为公共安全目的和为私人目的进行的刷脸监控的不同约束。再次,尽管无须恐慌,但我们仍需要关注刷脸的可能风险,特别是其背后的个人信息的自动化整合以及可能的使用方式与歧视、异化的问题。最后,网格和网络作为治理之理想类型的二分,为理解刷脸提供了有益的视角,也是场景理论的一个具体应用和延伸。

*感谢赵晓力、沈伟伟、戴昕、岳林提出的建议。

注释:

①国内目前讨论较多的是一般性的人工智能伦理,而直接针对刷脸的研究较少,例如李延舜:“公共视频监控中的公民隐私权保护研究”,《法律科学》2019年第3期,第54-63页;王秀哲:“公共安全视频监控地方立法中的个人信息保护研究”,《东北师大学报》2019年第5期,第57-68页。国外研究通常将刷脸归结至监视研究(surveillance studies)或隐私研究的领域,例如Sara M. Smyth, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, New York: Routledge, 2019, pp.7-10。

②关于欧美国家此方面立法的介绍,参见洪延青:“人脸识别技术的法律规制研究初探”,《中国信息安全》2019年第8期,第85页;邢会强:“人脸识别的法律规制”,《比较法研究》2020年第5期,第51-54页。最近我国的《个人信息保护法(草案)》《天津市社会信用条例》《杭州市物业管理条例(修订草案)》都对生物识别信息的收集作出了限制。

③例如《公共安全视频图像信息系统管理条例(征求意见稿)》《公共安全人脸识别应用图像技术要求》《安全防范视频监控人脸识别系统技术要求》。

④此方面的一般性讨论,参见赵精武:“《民法典》视野下人脸识别信息的权益归属与保护路径”,《北京航空航天大学学报(社会科学版)》2020年第5期,第21-29页;林凌、贺小石:“人脸识别的法律规制”,《法学杂志》2020年第7期,第68-75页;郭春镇:“数字人权时代人脸识别技术应用的治理”,《现代法学》2020年第4期,第19-36页。

⑤此方面的一般性综述,参见Jake Goldenfein, *Monitoring Laws: Profiling and Identity in the World State*, Cambridge: Cambridge University Press, 2019, pp.14-20。

⑥例如,手机从手动输入密码到指纹、人脸识别;公共摄像头从简单的录像存储到识别身份;火车站从人工查验票证到旅客刷脸进站,等等。

⑦参见杨智杰:“人脸识别十字路口:脸的恐慌”,《中国新闻周刊》2019年第37期,第22-25页。

⑧“认脸”经过长期演化,已经内化为人类的一种通用能力,用以区分辨识曾打过交道的人们和陌生人,甚至能根据社会态度区分好人和坏人。另外,我们容易辨识出人类双胞胎的些许差异,但有时却难以区分哪怕是相貌差异较大的同一类动物。

⑨See Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World*, Princeton: Princeton University Press, 2001, pp.47-49。

⑩参见朱体正、崔晓:“身份证制度初探”,《中国司法》2005年第2期,第105页。

⑪参见[德]尼克拉斯·卢曼:《信任:一个社会复杂性的简化机制》,瞿铁鹏译,上海人民出版社2005年版,第20-25页。

⑫此处仅仅是就理想类型而言,现实中的网格和网络往往是混合交织在一起的。

⑬颇能反映网格治理模式的文件,例如2015年中共中央办公厅、国务院办公厅印发的《关于加强社会治安防控体系建设的意见》。

⑭参见[荷]何塞·范·戴克:《互联文化:社交媒体批判史》,赵文丹译,中国传媒大学出版社2018年版,第6-9页。

⑮和其他类型的信息内容服务(甚至包括可以独立创作作品的人工智能)的兴起一样,能够识别人脸的人工智能需要以低成本获取人脸样本进行训练,因此适用“责任规则”(选择退出)而非“财产规则”(选择加入)。

⑯参见马静华:《公共视频监控:运行机制、刑事司法与警

民态度》，法律出版社2017年版，第36-38页。关于人脸识别实践在美国的历史演进，参见 Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York: New York University Press, 2011, pp.37-45。

①⑦机器在跨年龄识别的能力方面远超人类(人类会遗忘，且无法辨识相貌的改变)。例如，公安部的打拐行动内部软件“团圆”系统在识别丢失儿童方面，远超后者父母的识别水平，哪怕儿童的相貌发生了改变；在张学友演唱会上识别出在逃犯的天网系统，也胜过一般民警的识别能力。

①⑧参见王文峰：《人脸识别原理与实战》，电子工业出版社2018年版，第11-14页。

①⑨参见“助力安全复工复产 京东数科戴口罩人脸检测准确率超99.8%”，载央广网 http://tech.cnr.cn/techgd/20200225/t20200225_524991462.shtml，2020年11月1日访问。

②⑩参见欧树军：“权利的另一个成本：国家认证及其西方经验”，《法学家》2012年第4期，第1-13页；欧树军：《国家基础能力的基础》，中国社会科学出版社2013年版，第18-24页。

②⑪参见邱建华等：《生物特征识别：身份认证的革命》，清华大学出版社2016年版，第1-3页。

②⑫国内很多火车站都已经可以直接刷脸进站，不需要旅客出示车票和身份证。在安全性要求更高的金融行业，远程身份认证还需要人工辅助，例如要求眨眼、发声等，国家基于此已经允许远程开户，参见中国人民银行2015年发布的《关于银行业金融机构远程开立人民币银行账户的指导意见(征求意见稿)》。

②⑬例如已购的火车票可以通过刷脸获取，进火车站时也可以通过刷脸进入，如果全部整合在一起，就可以在前端取消掉任何环节，人脸就是享有一切服务的天然凭证。

②⑭诸如QQ号之类的账号体系一度存在，但被证明是没有太大必要的，且还会带来账号继承、黑市买卖等问题。参见岳林：“网络账号与财产规则”，《法律和社会科学》(第15卷第1辑)，法律出版社2016年版，第45-46页。

②⑮参见何文波等：“我国身份证件使用法律制度研究——以‘住宿’‘出行’活动为考察对象”，《北京警察学院学报》2017年第6期，第15-20页。

②⑯2015年国家发展改革委等九部委联合发布的《关于加强公共安全视频监控建设联网应用工作的若干意见》(发改高技[2015]996号)提出，到2020年，基本实现“全域覆盖、全网共享、全时可用、全程可控”的公共安全视频监控建设联网应用，在加强治安防控、优化交通出行、服务城市管理、创新社会治理等方面取得显著成效。

②⑰例如印度就颁发了基于生物特征的唯一身份标识符，参见 Charles Assisi and N.S. Ramnath, *The Aadhaar Effect: Why the World's Largest Identity Project Matters*, New York: Oxford University Press, 2019, pp.25-18。我国的二代身份证虽然嵌入了指纹，但单独的指纹信息不构成表明公民身份的标识符。

②⑱身份证件的拍摄是按照专门技术标准进行的，但也很难说就代表了最为清晰的像素和颗粒度。

②⑲各地的公共安全视频管理规定基本都没有区分一般摄像头和具备人脸识别功能的摄像头。《广州市公共安全视频系统管理规定》和《个人信息保护法(草案)》对公共场所摄像标识作了规定。

③⑩《居民身份证法》第6条仅规定，居民身份证具备视读与机读两种功能，视读、机读的内容限于该法第3条第1款规定的项目(即姓名、性别、民族、出生日期、常住户口所在地住址、公民身份号码、本人相片、指纹信息、证件的有效期和签发机关)；公安机关及其人民警察对因制作、发放、查验、扣押居民身份证而知悉的公民的个人信息，应当予以保密。但并未就此类信息与其他数据相互关联的行为作出规定。

③⑪参见《上海市公共数据和一网通办管理办法》(2018年11月1日起实施)第3条。

③⑫驾驶员会使用导航服务提示安装摄像头的大致位置，从而增强注意力；行人一旦得知在十字路口闯红灯会被计入个人的社会信用账户，则也会减少闯红灯的概率。这些举措都能起到告知提示的功能。

③⑬参见[法]米歇尔·福柯：《规训与惩罚》，刘北成、杨远婴译，生活·读书·新知三联书店2014年版，第42-44页。

③⑭参见裴炜：“数据侦查的程序法规制——基于侦查行为相关性的考察”，《法律科学》2019年第6期，第43-54页。

③⑮一般情况下，国家缺乏正当理由要求在一般区域去除头部和面部的遮盖，除非是在公共游行期间或重大交易场景。很多西方国家都有反蒙面法，2019年的两个最近例子是，法国在“黄马甲”事件中通过立法，要求参加游行的人们不得对自己面部进行遮掩，否则警察无法通过摄像头捕捉进行严重暴力犯罪的嫌疑人的影像；我国香港地区也针对当时广泛的街头暴力行为出台了《反蒙面规例》。

③⑯在一些公寓中的相邻关系纠纷中，原告认为被告(同一层楼对门的邻居)以安全问题为由在共用楼道里安装摄像头的行为侵犯了其隐私，法院往往支持这种观点。

③⑰参见《中华人民共和国网络安全法》第43条。

③⑱See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New

York: Public Affairs, 2019, pp.38-43.

③ See John Cheney-Lippold, *We Are Data: Algorithms and the Making of Our Digital Selves*, New York: New York University Press, 2017, pp.24-28.

④例如备受关注的2019年人脸识别第一案,尽管本质上是一个合同纠纷,但被大众媒体纷纷包装成为对刷脸技术合法性的挑战。参见浙江省杭州市富阳区人民法院(2019)浙0111民初6971号民事判决书。

⑤普遍观点认为,人脸数据因其不可更换的原因,一旦泄露,便会造成严重后果。但笔者尚未看到对其可能后果的详细描述或预测。

⑥现实中也出现过通过一张具有足够高精度的照片就能攻破人脸识别系统的案例,参见“不可思议!一个3D面具就能破解刷脸支付,还能进火车站?微信:盗刷,我赔!”,载网易<https://www.163.com/dy/article/F18ORQF305199NPP.html>, 2020年11月1日访问。

⑦像DeepFake那样的换脸软件,也可以轻易做到这点。但这是另一个问题。

⑧在张富、余杭飞、史良浩等侵犯公民个人信息罪一案中,被告以牟利为目的,利用已非法获取的公民个人信息,通过使用软件将相关公民头像照片制作成公民3D头像,从而通过了支付宝人脸识别认证,并使用上述公民个人信息注册支付宝账户。参见浙江省衢州市中级人民法院(2019)浙08刑终333号刑事裁定书。

⑨近年来发生的个人信息泄露事件表明,很少有单独针对人脸数据信息进行的攻击和非法买卖,遭到攻击和非法买卖的更多是文字和符号性信息。

⑩所谓“黑灰产”团队,是指有一些不法人员利用电商平台,批量倒卖非法获取的人脸等身份信息和“照片活化”网络工具及教程,形成了一条完整的黑色产业链。

⑪这类类似于黑客“撞库”,亦即通过解析出一个账户的密码,就可以猜测其他账户的密码。

⑫其逻辑类似于第三方支付的发展过程,最终只有获得牌照的少数支付巨头可以将其支付方式变成一种基础设施,并取得市场优势地位。特别是在金融交易等涉及重大财产安全的领域,需要在法律上对人脸识别系统的效力进行独立确认,即用户的刷脸行为在严格情况下等同于电子签名。黄奇帆近期在一次演讲中提到了这种监管模式,参见“黄奇帆:指纹、人脸、虹膜等特征识别技术公司应‘先证后照’”,载《南方都市报》2019年8月15日。

⑬参见王秀哲:“身份证明与个人信息保护——我国居民身份证法律规制问题研究”,《河北法学》2010年第5期,第2-11页;Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press, 2009, pp.5-9.

⑭参见寓扬、茜茜:“开学季摄像头潜入课堂,人工智能商业化后的隐私黑盒能关得住吗?”,载澎湃网https://www.thepaper.cn/newsDetail_forward_4324561, 2020年11月1日访问。

⑮关于控制力标准,参见胡凌:“分享经济中的数字劳动:从生产到分配”,《经贸法律评论》2019年第3期,第33-51页。

⑯参见“多地启动人脸识别抓拍整治闯红灯行人闯红灯该不该上镜”,载央视网<http://news.cctv.com/2017/06/13/ARTI2joiRYad-FeG4deE7wKUZ170613.shtml>, 2020年11月1日访问。

⑰支付宝2019年发布了《生物识别用户隐私与安全保护倡议》,中国支付清算协会2020年则发布了《人脸识别线下支付行业自律公约(试行)》,积极推动行业自律。

参考文献:

[1]王秀哲:“身份证明与个人信息保护——我国居民身份证法律规制问题研究”,《河北法学》2010年第5期。

[2]欧树军:“权利的另一个成本:国家认证及其西方经验”,《法学家》2012年第4期。

[3]胡凌:“分享经济中的数字劳动:从生产到分配”,《经贸法律评论》2019年第3期。

[4]李延舜:“公共视频监控中的公民隐私权保护研究”,《法律科学》2019年第3期。

[5]林凌、贺小石:“人脸识别的法律规制”,《法学杂志》2020年第7期。

[6]郭春镇:“数字人权时代人脸识别技术应用的治理”,《现代法学》2020年第4期。

[7]邢会强:“人脸识别的法律规制”,《比较法研究》2020年第5期。

[8]Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York: New York University Press, 2011.

[9]Sara M. Smyth, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, New York: Routledge, 2019.

[10]Jake Goldenfein, *Monitoring Laws: Profiling and Identity in the World State*, Cambridge: Cambridge University Press, 2019.