财经法学 No. 2，2021
pp. 60 - 78

人脸识别技术中的个人信息保护
——兼论动态同意模式的建构

石佳友　刘思齐*

内容提要：人脸识别技术在现有应用场景中已经被证明了其便捷性和高效性，但是，围绕该技术自身准确性、安全性、伦理性和合法性等问题的争议也从未停息。2020 年我国“人脸识别第一案”引发公众及学界关注与讨论，急需在快速扩散的技术应用中，寻找信息法益保护模式。完善人脸识别技术中个人信息保护模式的可能性如下：第一，坚持“合法、正当、必要”原则，引入“特殊审查许可”对技术适用和信息处理行为进行限制，以此作为第一道保护屏障；第二，基于准入限制，在必要技术实践中严格限制概括同意的适用范围并辅助以监管审查和退出权保障；第三，在技术日趋成熟的前提条件下，科学甄别并引入动态同意模式，以实现明确、清晰、特定且有效的同意授权，保障信息主体的合法权益。

关键词：人脸识别　生物识别信息　知情同意权　动态同意

一、引　言

2020 年 6 月 15 日，杭州市富阳区人民法院公开审理郭兵诉杭州市野生动物园服务合同纠纷案。该案是由 2019 年杭州市野生动物园入园系统升级导致的纠纷。入园方式升级后，原告之前购买的年卡所采用的入园方式由指纹验证变更为人脸识别。原告诉称人脸信息作为敏感个人信息，对信息主体影响重大，被告就改变入园方式进行的短信、公告通知无效，且变相强制收集人脸信息，违反《消费者权益保护法》，要求动物园退还购卡费用，赔偿相关交通费用并且删除已

* 石佳友，中国人民大学法学院教授；刘思齐，吉尼斯世界纪录咨询（北京）有限公司高级经理。
本文为国家社科基金重大课题“健全以公平为原则的产权保护制度研究”（20ZDA049）的阶段性成果。

采集的信息。〔1〕被告则辩称其进行的个人信息收集符合知情同意原则，因此双方服务合同依然合法有效。一审法院判决支持原告请求。〔2〕虽然此案被定性为服务合同纠纷，但有观点认为这是围绕敏感个人信息处理中“告知与选择”“最小必要”和“风险评估”三大原则的争议。〔3〕该案并非我国首次因人脸技术而产生争议。早在2017年，城市公共交通路口设置人脸识别查处违反交通规则人员的做法就引发了关于公共安全和公民个人隐私权如何进行价值平衡的热烈讨论。〔4〕2020年底，天津市人民代表大会表决通过了《天津市社会信用条例》，其第16条禁止社会信用信息提供单位采集生物识别等信息。〔5〕

国际范围内，人脸识别技术也同样争议不断。2019年5月英国南威尔士公民爱德华·布里斯奇（Edward Bridges）在英国知名人权组织的支持下，以午餐时间被人脸识别摄像头拍摄并被侵犯人格权利为由，将南威尔士警方告上法庭。2020年8月，上诉法院最终支持原告诉求，认为公共监控中使用人脸识别侵犯公民隐私权，违反《人权和基本自由欧洲公约》第8条、英国2018年《数据保护法案》第64条以及2010年《平等法案》（The Equality Act 2010）第149条。〔6〕随后，当地人权组织将人脸识别技术称为“具有威胁性的危险技术”，〔7〕并呼吁禁止在公共领域使用该技术。在美国，脸书公司则因未经用户同意而收集、存储个人生物识别信息面临集体诉讼。〔8〕在最新的动议中，脸书公司将赔偿6.5亿美金，同时应在动议获批后的180天内关闭当地人脸识别“照片标签”功能，同时删除数据库中存储的人脸图像及人脸生物识别符模板信息。在政策层面，美国多个城市政府也相继表现出对于人脸识别的犹疑和抵制态度。基于技术歧视、叠加算法偏见、隐私与自由的压迫和公权力过度的多重顾虑，2020年9月，美国伊利诺伊州斯普林菲尔德市发布市政令，暂停人脸识别在公开政务中的使用。另外，加利福尼亚州、马萨诸塞州、俄勒冈州等州所属的10个城市亦相继发布市政令，直接禁止包括警察部门在内的政府机构在辖区内公共场合使用人脸识别技术。

20世纪50年代至今，生物识别技术迅速发展。有预测数据指出人脸识别行业未来年均增速可能高达25%，其市场规模在2022年将达到约67亿元。〔9〕人脸识别技术前景可观，但其风险

〔1〕 参见《国内“人脸识别第一案”在富阳法院开庭》，载微信公众号“富阳日报”，2020年6月16日。

〔2〕 参见《富法发布：原告郭兵与被告杭州野生动物世界有限公司服务合同纠纷案一审宣判》，载微信公众号“富阳法院”，2020年11月20日。

〔3〕 参见毛亚楠：《人脸识别第一案：告的是什么》，载《方圆》2019年第24期。

〔4〕 参见《人脸识别曝光闯红灯者是否涉及隐私，专家：把握尺度》，2017年6月17日，载https://www.sohu.com/a/149740580_400941，最后访问时间：2019年5月25日。

〔5〕 参见《天津市社会信用条例》，2020年12月1日，载http://app.myzaker.com/news/article.php?pk=5fc607d08e9f0960b129247c&f=huangli，最后访问时间：2021年1月30日。

〔6〕 该案首次审理时，原告诉称公共场合使用人脸识别技术侵犯隐私权，违反数据保护条例。被告辩称该技术类似公共场合拍摄或监视手段，该行为在法律框架下依然合法。最终威尔士行政高等法院女王审判庭虽然认可人脸识别技术“干扰”个体隐私权，但认为警方将该技术用于公共安全符合法律框架规定，并未支持原告诉求。

〔7〕 See Liberty, Liberty wins Ground-breaking Victory against Facial Recognition Tech, Aug. 11, 2020, available at https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/, last visited on Oct. 12, 2020.

〔8〕 诉讼起因为脸书公司2010年推出的照片标签功能，该功能通过识别用户上传照片中的人脸“标记朋友”，未经许可为当地年满18周岁的用户开启服务，该行为被认为违反《伊利诺伊州生物隐私保护法》相关数据处理规定。

〔9〕 参见杨智杰：《人脸识别十字路口：脸的恐慌》，载《中国新闻周刊》2019年第11期。

与收益比例关系依然存疑。〔10〕人脸识别技术自身和所涉及的个人信息均具有特殊性，而这些特殊性则导致在技术应用过程中产生新的个人信息风险与威胁。因此，行业引领者和制度设计者应在技术发展和公民权利保护之间把握边界，〔11〕在技术应用与发展中，同时构建相对应的隐私和个人信息权益保护模式。本文将从人脸识别技术的特殊性切入，结合我国社会经济体制和技术发展环境，顺应现有的立法趋势，对比甄别域外实践经验，探寻我国人脸识别技术实践中个人信息保护的适宜路径。

二、人脸识别对个人信息保护的特殊挑战

欧盟《互联网及移动设备人脸识别技术的意见书》（2012 年）中将人脸识别技术定义为“通过自动处理包含人类面部图像的数字照片来识别、验证以及鉴别个体的技术”。美国司法部司法援助局定义该技术为“通过生物识别算法来检查和匹配自然人人脸的区别性特征的技术”，并称这项技术有助于快速识别无身份人和死者，在调查和预防犯罪活动上是“有价值的调查工具”。从技术应用场景划分，人脸识别目前主要应用于两大场景：一是政府机构进行公共管理和维护公共安全的场景；二是涉及身份认定和定制服务的多样化商业场景，包括照片分类与标签、安全访问、精准营销以及消费者服务等等。在上述场景中，人脸识别技术所带来的便利性被日渐认可，但其背后的风险和隐患也逐步进入各界视野，带来重重顾虑。

第一，人脸识别技术的实践须基于拉网式的人脸信息收集，因此在收集过程中可能严重威胁个人隐私。美国学者经调查研究认为隐私权风险是人脸识别技术发展中最为核心的问题，同时在伦理、政策、安全、公平公正性方面都存在技术衍生问题。〔12〕人脸识别技术与公共监控摄像头的融合，导致公民个人“随时随地活在镜头之下”，个人行动路径和习惯偏好都可能在拉网式的人脸图像捕捉中被分析、提取和窥探。斯坦福大学有研究者曾称可通过面部特征的智能分析，判断主体的性取向，〔13〕触及个人隐私。

第二，人脸识别技术造成人身、财产以及心理上的安全隐忧。在某媒体发起的覆盖两万多人的人脸识别调查中，30.86％的受访者表示已经因为人脸信息泄露蒙受财产损失，而在“最担忧的安全隐患”中，个人行踪持续记录（54.4％）和账户盗刷导致财产受损（53.72％）仅次于“人脸信息泄露”被列为第二和第三。〔14〕通过人脸识别，被系统判断为“本人”的用户可以远程

〔10〕 参见邢会强：《人脸识别的法律规制》，载《比较法研究》2020 年第 5 期。

〔11〕 参见王梓辉：《人脸识别第一案：技术滥用下的隐私之殇》，载《三联生活周刊》2019 年第 46 期。

〔12〕 See Lucas D. Introna，Helen Nissenbaum，Facial Recognition Technology：A survey of Policy and Implementation Issues，working paper，Center for Catastrophe Preparedness and Response，New York University，available at SSRN：https://ssrn.com/abstract=1437730，last visited on Feb. 17，2021.

〔13〕 See Lisa Ryan，Artificial Intelligence Can Tell if You're Gay or Straight from a Pic of Your Face，Scientists Say，The Cut，Sept. 8，2017，available at https://www.thecut.com/2017/09/artificial-intelligence-gay-straight-stanford-study.html，last visited on May 25，2020.

〔14〕 参见南方都市报个人信息保护研究中心人工智能伦理课题组：《人脸识别应用公众调研报告 2020》第 8－9 页，载 http://www.chuangze.cn/attached/file/20201020/20201020205632833283.pdf，最后访问时间：2021 年 2 月 17 日。

行使访问权或者决定权，例如进出某特定空间，或进行远程金融交易等。除此之外，有学者将人脸信息称为“生物密码”，〔15〕并且指出人们一旦丢失该密码，将无法通过更换来保障安全，也因此让“冒充者”有可乘之机。除了物理性的财产损失，有学者认为人的社会存在表征就是生物和哲学双重意义下的“脸”，因此脸的存在与否和人的社会存在直接相关，〔16〕若人脸信息泄露并遭遇侵权，则可能造成其精神上的社会存在受到压迫。

第三，人脸识别技术为肖像权保护带来新的忧虑。有学者指出人脸识别技术在人工智能发展的推动下在各领域进入实质性应用，也将对肖像权产生新的威胁。〔17〕首先，人脸识别依托于光学摄影技术，通过终端摄像头拍摄人脸照片并进行快速识别。随着技术的发展，不同拍摄环境对于镜头精确度的影响日益降低，对人脸肖像的提取和利用的门槛也随之降低。其次，人脸识别需要存储大量人脸图像或人脸生物识别符作为数据库进行后续识别比对，因此若人脸数据库遭遇泄露并用于技术深度伪造，其所造成的安全危害将无法预估。

第四，人脸识别算法可能造成自由危机。现如今，自动化技术和人工智能依然无法完全去除人工干预的痕迹，且在智能算法自动累积学习中，人的主观选择效应将被无限次叠加，从而引发“标签化”的歧视问题。从法理学视角出发，有学者认为“技术挤压自由”，技术便利性的强化将提高人类对技术判断的依赖性，从而潜移默化地逐步挤压自由，导致人性中的模糊状态异化为“好”与“坏”的两种极端选择。〔18〕基于我国公众普遍对公权力更为信任、对权威更为认可的这一社会心理特点，当技术结合公权力之后，这种挤压将更加明显。

为了进一步探寻人脸识别技术中的个人信息保护路径，做到有的放矢，应明确技术应用中个人信息风险的特殊性：

第一，人脸信息具有特殊属性。人脸信息属于活体数据，〔19〕来源于自然人身体，具有直接识别性、独特性、唯一性，极难变更或替代。相较于指纹或声纹等需要主体配合才能够采集的其他生物识别信息，人脸不可藏匿，“随身携带”且极易采集。〔20〕同时，人脸信息一定程度上可以关联到特定自然人的既往社会评价、名誉等人格利益，若遭遇泄露或冒用，则可能影响其在社会生活中的自由，且该影响在互联网时代犹如现代“刺黥”〔21〕，极难褪色消逝。2018 年人工智能报告〔22〕显示出在广泛的人脸识别应用中，若是将数据主体根据“兴趣”进行分类，衍生出特定

〔15〕 参见高富平：《人脸识别的法律风险和规制》，2019 年 9 月 18 日，载 https://www.sohu.com/a/341722243_289260，最后访问时间：2020 年 8 月 9 日。

〔16〕 参见袁治杰：《网络时代〈民法典〉对脸的保护》，2020 年 7 月 1 日，载 https://www.thepaper.cn/newsDetail_forward_8070851，最后访问时间：2020 年 8 月 9 日。

〔17〕 参见王利明：《人工智能时代对民法学的新挑战》，载 http://iolaw.cssn.cn/fxyjdt/201805/t20180516_4659264.shtml，最后访问时间：2020 年 8 月 29 日。

〔18〕 参见《“人脸识别的运用与滥用——比较法上的回应”学术沙龙顺利举行》，载微信公众号“大数据和人工智能法律研究院”，2019 年 10 月 31 日。

〔19〕 参见刘权：《警惕人脸识别技术的风险》，载《学习时报》2019 年 10 月 16 日，第 A2 版。

〔20〕 参见前引〔10〕，邢会强文。

〔21〕 参见《别把人脸识别技术搞成现代“刺黥”》，2019 年 10 月 30 日，载 https://m.thepaper.cn/baijiahao_4816253，最后访问时间：2019 年 10 月 30 日。

〔22〕 See AI Now Report 2018，also see online archive of AI Now Institute，available at https://ainowinstitute.org/AI_Now_2018_Report.pdf，last visited on Oct. 30，2019.

个体标签，将直接导致背负标签的主体面临特殊对待或过度监控的问题。

第二，无接触信息采集中的知情同意障碍。人脸识别技术中的信息采集以摄像头自动拍摄为手段，不需要信息主体主动接触采集设备。因此，在整个采集过程中，被采集对象往往毫无察觉，从而错失判断风险并明确表达同意或拒绝的机会。同时，现有人脸识别服务存在“使用即同意”的乱象，例如某公共查询平台将人脸识别设置为“唯一”的识别方式，导致信息主体因需要选择服务而不得不同意。

第三，“同意”边界模糊且范围不明，导致人脸信息泄露后溯源无门。在现有人脸识别用户服务协议文本调查中，不少人脸识别服务协议中均约定了向“相关第三方”传输人脸图像用于比对识别。但是，该第三方身份通常无从知晓，仅仅以“相关性”进行约束，极可能导致人脸图像经过多次传输后无迹可查，无从溯源。以新型冠状病毒肺炎疫情防控初期实践为例，基层管控多处应用了人脸识别技术采集公民人脸，而后网络人脸“黑市”就随之出现，数千张戴口罩和不带口罩的人脸照片被廉价出售，但是，这些人脸图像的源头却不得而知。

第四，技术滥用导致管制缺席。新技术如同“诱人的魔盒”，诱使各领域跃跃欲试：从校园管理到公共洗手间的厕纸取用，从线上账户登录查询到线下垃圾分类，包裹着“黑科技”或者“智慧”外衣的人脸识别技术，无限制地在各种场景下被推广使用，而这些使用场景是否符合信息处理的合法性、正当性和必要性，是否存在合理监管路径，依然存在巨大疑问。

第五，事后救济效力存在局限性。万物互联以及技术仿冒导致人脸信息的侵权结果扩散极快，极难恢复如初。同时，由于技术和信息的不对等地位，公民个人极易因为缺乏专业技术知识而维权困难。〔23〕另外，现有侵权赔偿救济模式的震慑效力仍然有待检验。值得注意的是，立法机关于 2020 年 10 月公布的《个人信息保护法（草案）》中规定了违法处理个人信息的法律责任，除勒令整改之外，还规定了违法处理者 100 万以下以及主管人员 1 万到 10 万人民币的处罚额度，情节严重时处罚额度最高可达非法所得的 5%。同时，信息主体可根据实际损失或信息处理者违法营业额百分比请求赔偿，并允许在无法计算时由法院行使自由裁量权。〔24〕虽然现有草案通过提高违法成本对违法信息处理行为予以威慑，但是，从人脸识别行业现有规模来说，100 万处罚额度是否具备足量的威慑力，是否能够有效阻止处理者因利益而“铤而走险”，尚且存疑。

三、人脸信息保护的现行法律框架

在 2021 年起正式施行的《民法典》中，“个人信息保护”与“隐私权”并列作为第四编第六章的主要内容，其通过固定的法律条款明确了个人信息定义、保护原则以及相关主体权利。2020 年 10 月公开征求意见的《个人信息保护法（草案）》进一步区分一般个人信息和敏感个人信息，并分别对两类信息处理过程中涉及的处理者义务、主体权利以及责任部门都作出了具有针对性的

〔23〕 参见张延来：《“人脸识别第一案”一审宣判，听听原告代理律师谈人脸识别技术与法律的细节》，载微信公众号“网络法实务圈”，2020 年 11 月 20 日。

〔24〕《个人信息保护法（草案）》第 62 条规定了违法处理个人信息或未采取必要安全措施的法律责任，以及情节严重的责任；第 65 条规定了信息主体因个人信息被非法处理而产生的求偿权。

规定。同时，草案顺应时代需求，体现出对于个人信息流动必要性的认可，并以尊重信息流通需求、实现信息价值和保障合理合法利用为立法目的，充分体现了我国在个人信息保护领域的积极主动态度和未来立法趋势。

（一）人脸信息保护具备明确的法律基础

《民法典》第1034条第2款从信息记录形式、可识别属性两个角度定义个人信息，且明确罗列出“生物识别信息”属于个人信息，肯定其受保护的法律地位。但是，《民法典》并未进一步细化“生物识别信息”的定义。其他现行法律包括《消费者权益保护法》和《网络安全法》，对于生物识别信息均未做出明确的定义。从文义解释来看，生物识别信息应解释为生物活体上足以识别特定主体的信息。全国信息安全标准化技术委员会在2019年6月公开发布的《信息技术安全技术生物特征识别信息的保护要求》征求意见稿中，将生物识别信息定义为“生物特征样本、特性、特征模型、性质以及原始描述数据的识别特征，或上述数据的聚合”〔25〕。人脸信息来自活体，且作为原始生物特征具有识别性，符合该生物识别信息定义。

《民法典》第1034条第2款强调个人信息的“特定自然人的可识别性”。根据现有规定，具备“可识别性”的生物信息才符合保护对象的界定，反之，倘若人脸图像在经过模糊或遮挡处理，抑或是图像数字编码处理之后，则因丧失可识别性可能无法受到保护。这其中依然存在隐患：一是技术的流动性和发展变迁将导致当下无法被识别的人脸在未来有可能被新技术破译，恢复其可识别性；二是大数据共连的环境下，原本丧失识别性的信息，再次结合位置、行踪或者其他信息之后，可能重新具备整体识别性，足以指向特定自然人。

相较之下，欧盟和美国对于生物识别信息的定义则更为具体，且人脸信息均被明确纳入生物识别信息范畴。欧盟《通用数据保护条例》（英文简称“GDPR”）第4条第14款将“生物识别数据”定义为“对自然人的物理、生物或行为特征进行特定技术处理后所得到的具备识别性的个人数据”，例如人脸图像或指纹数据。美国《加利福尼亚州消费者隐私保护法案》（英文简称“CCPA”）将“生物识别信息”定义为个人“生理、生物或行为上的特征”，包括脱氧核糖核酸序列等一切可以单独或结合其他信息识别特定个体的信息。〔26〕美国《伊利诺伊州生物信息隐私法案》（英文简称“BIPA”）将“生物识别信息”直接概括定义为具有“个人生物识别标识符”的任何信息，〔27〕并以反例形式列举出不包含在“生物识别信息”里的信息种类。由此可见，美国从生物识别信息的定义上趋于囊括尽可能多的生物特征及相关数据，在实践中可以帮助执法者快速判断涉案数据是否属于生物识别数据，从而援引相关的保护性规定。

（二）人脸信息作为敏感信息进行特别保护的立法趋势

《民法典》对私密信息进行了“隐私权＋个人信息”的双重保护，这被认为是“权利＋利益”的二元保护模式。《民法典》第1034条第3款规定：“个人信息中的私密信息，适用有关隐私权

〔25〕《信息技术安全技术生物特征识别信息的保护要求》征求意见稿第3.1.4条采用了“生物特征识别数据”这一说法，并在第3.1.3条定义“生物特征”为可检测到的个体生理或行为特征，并可以从中提取可识别、可重复的特征，以便自动识别个体。

〔26〕 See SB－1121 California Consumer Privacy Act of 2018，SEC. 9. Section 1798. 140（b）.

〔27〕 See 740 ILCS 14/Biometric Information Privacy Act，Sec. 10.

的规定；没有规定的，适用有关个人信息保护的规定。”按照这一规定，私密信息首先适用隐私权保护的规定。这些规定包括：第 1032 条第 2 款规定的“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”；第 1033 条规定的“除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为……（五）处理他人的私密信息……”。根据《民法典》前引条款，仅在上述隐私权规定无法适用的时候，方可适用个人信息保护的有关规定。这一做法可以理解成，对于私密信息应优先适用隐私权的规定，类似于特别法，因为隐私权是《民法典》明确承认的“民事权利”类型，而个人信息保护由于未明确使用“权利”措辞，属于法律所保护的“利益”范畴，所以其规则属于普通法。这一做法正好与比较法上以隐私权涵盖个人信息的通例相反，具有独特性。〔28〕第 1034 条第 3 款在解释上的困惑在于，“没有规定”究竟是指隐私权保护范围未能涵盖（即可能存在隐私权范围以外的私密信息），还是指隐私权保护手段方面没有规定（即存在隐私权保护方式无法保护的私密信息）。但不难理解的是，此种保护模式可能并非最适宜的方式。〔29〕就信息特性而言，人脸信息并非不愿为人所知的信息，对周围的人来说也不具备足以比肩隐私的私密性（当然，对于陌生人具有一定的私密性）。在实际社会生活中“人脸”作为公民社会交往的“活体名片”，具备生理和心理的双重属性，蕴含丰富的非语言情感信息，〔30〕承载了对应主体的既往社会评价、信用评分，以及人格尊严。因此，人脸信息应属于“并不私密但却敏感”〔31〕的信息，如果简单适用一般类型的个人信息保护规则，则可能导致保护不力，致使信息主体权益遭受侵害。

值得注意的是，《个人信息保护法（草案）》摒弃了“私密信息”这一外延高度不确定的概念，转而采取了“一般信息—敏感信息”的分类方式，其第 2 章第 2 节明确以“敏感个人信息的处理规则”为标题，并且在第 29 条中明确列举个人生物特征属于敏感信息。相较而言，“敏感信息”的概念内涵更为明确具体（如种族、政治与宗教信仰、生物识别信息、健康信息、性取向等）；而“私密信息”在边界上则较为模糊，可涵盖所有未公开的个人信息，包括在特定范围内（如家庭成员、朋友间）分享的所有信息。从客体范围的确定性角度来看，《个人信息保护法（草案）》的做法似更可取。另外草案中第 27 条针对公共场所的图像采集、身份识别设备的规定，可以直接关联到人脸识别技术，足见草案对于这一特殊信息处理技术的关注和区别性规制。

对比国外现有规则，生物识别数据由于其特殊性，一致地被作为特殊数据予以单独保护。GDPR 第 9 条第 1 款将生物识别数据列为特殊类别的个人数据之一，规定在通常情况下禁止处理。美国在人脸信息保护领域制定专项规范，例如 BIPA 中针对私人实体进行人脸数据处理提出特殊要求，同时美国信息技术与创新基金会在针对联邦数据隐私法案的建议中也明确将生物识别数据列为敏感数据。〔32〕

---

〔28〕 参见石佳友：《〈民法典〉：网络安全制度创新的新里程碑》，载《中国信息安全》2020 年第 10 期。

〔29〕 参见潘林青：《我国个人敏感信息的界分基础及其立法表达——兼评民法典（草案）第一千零三十四条》，载《北京邮电大学学报》（社会科学版）2020 年第 2 期。

〔30〕 参见郭春镇：《数字人权时代人脸识别技术应用的治理》，载《现代法学》2020 年第 4 期。

〔31〕 前引〔29〕，潘林青文，第 37 页。

〔32〕 See Alan McQuinn，Daniel Castro，A Grand Bargain on Data Privacy Legislation for America，ITIF，Jan. 14，2019，available at https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america，last visited on May 25，2020.

（三）人脸识别中个人信息处理原则的从严适用

《民法典》第1035条规定了个人信息处理的原则和条件，而《个人信息保护法（草案）》沿袭相关原则，并在第29条针对个人生物特征等敏感信息提出了更高要求，即“特定目的”和“充分必要性”，以及更严格的“知情同意”，并在第30条和第32条两次提及从严规定，〔33〕体现出对于该类型信息更坚定的保护态度。

其一，人脸识别技术中个人信息处理应具备严格的合法性前提。知情同意是个人信息处理的合法性基础，而《民法典》中则体现出不同程度的“同意”层级：第1035条规定个人信息处理的“同意”可以来自“自然人或其监护人”，或者是“法律、行政法规另有规定”；第1033条中处理隐私或私密信息可根据“法律另有规定”或“权利人明确同意”。有学者认为这一差异体现了《民法典》在私密信息和一般个人信息保护的三点不同：一是法定授权情形不同，即对于处理私密信息的法定授权，仅限于我国正式施行的法律，并不包含行政法规；二是作出同意的主体不同，在隐私权保护的框架下对于私密信息仅有信息主体本人有决定权，而在个人信息保护框架下允许监护人代为决定；三是“明示同意”是以书面或其他形式做出清晰的许可，而同意则可能包含了不反对、默认等被动暗示。〔34〕基于生物识别信息具备更高敏感度这一共识，如果直接适用一般个人信息的要求，是无法充分保障主体的权益的。《个人信息保护法（草案）》第30条规定个人生物特征等敏感信息的同意授权应该是本人单独、书面同意。对于“单独”一词，在文义上应解释为“独立的，不和其他一起的”，即该同意应该是独立且明确的“专项同意”，不能与其他信息混同或随意扩增其原有同意范围。在同意形式上，要求主体基于“完全知情”做出书面“具体、清晰、明确的”同意，这基本与域外做法一致。GDPR第9条规定在常规情况下禁止处理包含生物识别数据等的特殊数据，只允许在数据主体明确同意，且该同意具备对抗禁止处理规定效力的前提下才可以处理。BIPA中则明确要求处理生物识别数据必须基于书面同意，包括纸质或电子的形式，以保障信息主体通过“主动行为”，在形式上更为明确地表达对个人信息的决定。不难看出，各国对生物识别信息属于特殊数据已经达成共识，且认可一般性的同意会导致主体对于信息掌控和自决的效果有所折损，无法满足主体权益保护需求。

其二，人脸识别技术处理个人信息时应严格遵循“明确特定目的”及必要性要求。目的正当性的含义不仅仅是合法合规，还应同时符合目的限制、诚实信用和公开透明的要求，〔35〕即“相关、特定、明确且合法”，这也与第1035条规定的四条件中“公开处理规则”和“明示目的、方式和范围”相呼应。从这个角度来看，《个人信息保护法（草案）》第29条第1款规定仍有值得完善的地方。该款规定：“个人信息处理者具有特定的目的和充分的必要性，方可处理敏感个人信息。”此处“具有特定的目的和充分的必要性”，措辞过于宽泛，建议在“具有”之前增加“基于维护公共利益或个人的重大利益”。以GDPR第9条为参考，尽管该条第1款也使用了“特定

〔33〕《个人信息保护法（草案）》第30条提及若法律、行政法规要求书面同意则从其规定；第32条提及法律、行政法规上规定应当取得行政许可或做出更严格限制的，则从其规定。

〔34〕 参见王春晖、程乐：《解读民法典“隐私权和个人信息保护”》，载《南京邮电大学学报》（社会科学版）2020年第3期。

〔35〕 参见王洪亮：《民法典与信息社会——以个人信息为例》，载《政法论丛》2020年第4期。

目的”（specific purposes）这一说法，但该词语结合随后其他几项条款，可以被明确解读为个人的重大利益或者在健康、劳动、社会保险等领域的公共利益，具体包括：对信息数据主体的基本权利和利益是必要的、非营利机构的正当性活动中所进行的处理、处理是为了实现公共利益所必要的、科学或历史研究目的或统计目的是必要的并采取了合理的保护措施等。

人脸识别技术的实际应用，目前大致分为政府机构基于公共服务或社会管理目的的使用和企业基于商业目的的使用。政府部门应用人脸识别处理信息往往基于法定授权〔36〕而无需个人的单独同意，且通常覆盖面极广，因此应依法明确划定“警戒线”，寻求个人利益和公共利益的平衡。《个人信息保护法（草案）》第 27 条对公共场所设置图像采集以及身份识别设备有所规定，为这一场景下的人脸识别技术应用设置了三层约束：第一，以“维护公共安全”为目的，而“必需”则限制了政府机构在存在替代方案能够达成同一目的时对人脸信息等生物特征信息的使用；第二，设置明显标识保障个体知情权的有效落实；第三，禁止目的之外的对外公布和传输，即将生物识别信息限制在目的框架之中。但是，公共安全范畴伸缩性较强，〔37〕包含了信息、食品、卫生、交通、建筑物、环境等广泛领域，因此草案应考虑细化公共安全目的、技术使用主体以及批准审核程序等，确保个人法益的折损程度和所保护的法益符合比例原则，例如进一步明确列举出人脸识别等生物识别可以适用的具体公共安全场景，包括重大公共卫生健康所需、追踪调查重大违法犯罪嫌疑人，或为维护个人宪法性基本权利和公共安全所必需等。

在商业应用领域，人脸识别技术作为当下不断发展的新型技术，其技术的专业性和普通人的认知水平存在较大的落差，信息处理目的也更为动态，在处理过程中是否一直符合初始目的，对于个人来说难以充分监督。我国现有个人信息安全规范将审核监督的责任分配到信息控制者，要求信息控制者成立个人信息安全负责人和个人信息保护机构，履行隐私政策的制定签发，安全影响评估和审计等职责。〔38〕但是，作为信息控制者组建的下属机构，其并不独立，角色更趋近“责任人”而无法充分履行独立监管的责任。《个人信息保护法（草案）》第 32 条体现出在行政监管上的从严趋势，即在处理生物识别信息时，如果法律法规要求必须获得特殊许可或有更为严格的要求，应从严适用。这一规定体现出我国未来在敏感个人信息处理上从严治理的大方向，也为未来细分信息类型、“量身”制定行政法规提供可能性和空间。

其三，人脸信息处理应严守“最小必要”的限度。《民法典》第 1035 条强调“不得过度处理”，要求必须采取对权利人最小侵害的方式处理信息。〔39〕“过度”一词，文义上应该理解为超越常度或者超过制度规定，但是《民法典》第四编第六章中除了第 1033 条规定未经法律许可或主体明示同意时禁止处理私密信息之外，其他条款并没有明确“常度”的标准线。所以，生物识别信息处理的限制“常度”在现行法规下依然相对模糊。《个人信息保护法（草案）》第 29 条尝

〔36〕《民法典》第 1036 条规定处理个人信息而无需承担责任的情形之三：维护公共利益或该自然人合法权益的合理处理；《个人信息保护法（草案）》第 13 条规定的允许处理情形之三、四、五，包括为履行法定职责或义务、应对突发公共卫生或保护更高位阶的法益以及公共利益和监督的目的，且依然设定了“合理范围”限制。

〔37〕 参见冯群星、蒋琳、潘颖新、周姝祺：《个人信息保护法草案公布，拟进一步规范公共场所人脸识别应用》，载微信公众号“AI 前哨站”，2020 年 10 月 21 日。

〔38〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020）第 11.4、11.7 条。

〔39〕 参见何鹏、刘新宇：《民法典：大数据时代下个人信息保护的民法基础》，载《中国政协》2020 年第 14 期。

试进一步定义“必要性”，将“特定目的”和“充分必要性”作为两个更为严苛的信息处理条件，并在第54条明确要求个人信息处理者在处理敏感信息前须进行事前风险评估，并全程受监管部门的监督管理。

就比较法的规定来看，考虑到生物识别信息敏感度的定性，欧盟和美国在生物识别信息处理领域采用更为保守的做法，即采取概括性“禁止”结合“例外情形”来反向明确允许处理的“必要场景”，即“原则禁止、例外允许”。GDPR第9条第1款规定生物识别信息等特殊数据禁止处理，而第2款列举十种允许处理的例外情形，并且没有包含“等”作为兜底，就意味着有且仅有这十种情形允许处理生物识别信息。与之相比，美国似乎趋向更为保守的做法，趋于以禁用的方式限缩技术应用的范围，且民间技术反对者们已经自发创建网络社群，呼吁抵制人脸识别技术的应用，〔40〕充分规避技术风险以及技术可能造成的个人权利侵害。《人脸识别道德使用法案》要求政府机构在没有形成技术应用准则和条件之前，禁止使用或投资购买人脸识别技术处理生物识别信息。同时，美国国会针对执法目的下的技术使用，出台《人脸识别技术保证法案》规定执法过程中的技术审批流程、期限和信息最小化原则，限制联邦政府的执法机构在执法过程中使用人脸识别。〔41〕旧金山市《通知秘密监视条例》中禁止政府和执法机构使用人脸识别技术进行拉网式的公共监控，并严格监督政府对于监控技术的购买和使用。纽约州立法机关也通过了禁止学校使用人脸识别以及其他生物识别技术的法令；波特兰市则禁止一切政府及商业私营机构在公开场合中应用人脸识别技术。反对者认为，全面禁止人脸识别技术会剥夺社会革新的可能性，降低犯罪调查等合法目的实现效率，应关注“预防滥用”或小范围试点，〔42〕至少无须全面禁止，〔43〕为技术发展保留必要空间；而支持者则呼吁全面禁止这项“危险的侵入性”〔44〕技术，这也符合美国宪法第四修正案中对于联邦公民隐私权和平等自由等基本权利的保护理念。

就人脸识别技术存废之争，笔者认为，人脸识别技术作为信息时代的产物，在一定范围内有助于提高社会管理效率，为公众带来便利，一刀切式的禁止可能会严重制约社会发展。不过，鉴于人脸识别技术可能对人的基本权利造成严重的影响，必须借助合法、正当、必要等原则来加以严格规制，而这也是抑制技术泛滥、保护个人权利的必要“防护盾”。

（四）初具雏形的行业自律机制

人脸识别技术区别于传统个人信息处理手段，在其技术保护中，行业自治组织基于专业知识，结合法律规范，以行业自律形式规范技术的设计、开发以及应用，可以有效填充法律规范和技术专业性中间的留白。2019中国刷脸支付市场调查数据显示，截至2018年刷脸支付用户达到

〔40〕 参见禁用人脸识别网站 htt://www.banfacialrecognition.com/的具体描述。

〔41〕 See S. 2878 Facial Recognition Technology Warrant Act of 2019, SEC. 3 (a).

〔42〕 See Kate Kaye, In Portland Debate, Facial Recognition Giants Hide Behind Tech Lobby Think Tank, Redtailmedia, Jan. 20, 2020, available at https://redtailmedia. org/2020/01/20/in-portland-debate-facial-recognition-giants-hide-behind-tech-lobby-think-tank/, last visited on Aug. 17, 2020.

〔43〕 See Ashley Johnson, Opinion: Portland Can Address Facial-recognition Technology Concerns Without Banning It, Oregonlive, Jan. 15, 2020, available at https://www. oregonlive. com/opinion/2020/01/opinion-portland-can-address-facial-recognition-technology-concerns-without-banning-it. html, last visited on Aug. 17, 2020.

〔44〕 Evan Selinger, Woodrow Hartzog, The Incondensability of Facial Recognition, 66 *Loyola Law Review*, 101 - 122 (2019).

0.61 亿人，而在支付平台的推动下，未来预计可增长到 7.6 亿人。〔45〕 中国支付清算协会发布的《人脸识别线下支付行业自律公约（试行）》对其会员单位提出安全管理、终端管理、风险管理和用户权利保护的要求，呼吁应在遵循国家法律法规的前提下，保障用户信息和财产安全。另外，目前已有互联网企业发起《生物识别用户隐私与安全保护倡议》，从隐私、安全、防止信息滥用、责任与监督、公平性五个方向发起行业倡议，结合我国法律规范，提出“最小、够用”这一基本原则，并建议企业内部设置风险小组，保护用户信息安全。〔46〕 但目前此类行业公约覆盖范围仅限于互联网服务领域，对于线下其他领域的人脸识别应用，例如人脸识别门禁等更为普遍的现象，依然缺乏行业指引。

四、人脸识别中个人信息保护路径探析

人脸识别技术的便捷性和效率性无可否认，一定程度上符合当代构建智能社会的需求，但其技术实现所依托的人脸信息，一旦遭到泄露或侵权后将可能严重影响信息主体的其他民事权益，甚至人格尊严、平等、自由等宪法性基本权利。因此，既要充分利用技术革新的便利，也要避免技术泛滥的弊端，理性评估并规制技术适用和个人法益间的平衡才是未来的趋势。有学者建议根据实际国情，在人脸识别规制中有甄别地借鉴域外的特别许可制度，即经由授权机构评估审核和许可，允许技术适用，同时辅助以定期技术准确性测试和技术应用审计，并设置惩罚性赔偿的制度。〔47〕 另有观点也提出人脸识别信息的保护在于事前保护，包括必要性审查，确保信息处理和目的实现符合价值比例要求，以及细化技术适用标准以及知情同意的实际操作制度。〔48〕 因此，人脸识别中的个人信息保护路径应从特别许可的准入审查以及更为合理的知情同意模式入手。

（一）基于合法、正当、必要原则的技术准入审查制度

无论是合法、正当、必要这些基础原则还是其他具体原则，都应在生物识别信息处理中结合适用，而知情同意原则的适用应以基础原则适用为限制。〔49〕 在人脸识别技术适用前，应经由法定授权机构根据理性设计的审查标准和步骤，对技术准确性、算法非歧视性设置、安全加密设置和主体权利保障路径等进行评估。

英美和欧盟等国家和地区均选择借助法案或规范强制要求在处理生物识别信息之前进行风险评估，其差别在于评估导向。英国深受欧盟 GDPR 影响，以数据保护为导向，明确针对生物识别数据等特殊数据强制适用评估制度。美国则以隐私保护为导向，对任何足以识别个体的信息的处

〔45〕 参见《2019 中国刷脸支付技术应用社会价值专题研究报告》，2019 年 11 月 21 日，载 https://www.iimedia.cn/c400/66866.html，最后访问时间：2020 年 5 月 10 日。

〔46〕 以阿里巴巴支付宝为例，其发起的行业隐私安全保护倡议的原则在人脸识别用户授权协议条款中已有体现，且影响其他从业者复制相似规范和模式。

〔47〕 参见前引〔10〕，邢会强文。

〔48〕 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》，载《北京航空航天大学学报》（社会科学版）2020 年第 5 期。

〔49〕 参见张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019 年第 6 期。

理均进行评估，并要求在四种情形下必须进行隐私影响评估，即：开发或采购任何处理或采集个人识别信息的新技术时，创建涉及隐私的程序、系统、技术或信息收集方式时，涉及新的隐私风险的系统升级时，发布全新或升级的个人识别信息收集规则时。其核心目的在于保障个人信息收集的合法合规，提前识别风险和影响，同时评估保护措施的有效性。〔50〕

目前，《个人信息保护法（草案）》第六章拟指定国家网信部门进行统筹协调，结合国务院下辖部门和各地人民政府部门，在各自管辖领域内进行个人信息保护监管，但尚未细分到具体职能部门。全国信息安全标准化技术委员会发布的2020年《信息安全技术个人信息安全影响评估指南》旨在指导行业基于个人权益影响和安全措施设置情况，以访谈、检查、测试的方法对待评估的个人信息处理技术进行风险评估。无论是现有法律规定，还是现行行业规范，对于我国后续信息处理的安全影响评估模式，均有借鉴作用，但前者在其适用范围、后者在其强制力上都存在缺陷，仅能作为目前生物识别信息处理的参考性或国家推荐性评估制度予以参考。因此，未来人脸识别技术准入审查应考虑从以下三方面进行构建：

1. 借助国家强制力，以专项法律或行政法规的形式强制要求在技术适用前进行全面的技术检测和信息安全影响评估，并禁止豁免评估的例外情形。与设置公正、权威、独立保护机构的学者建议〔51〕和欧盟集中监管体制不同，《个人信息保护法（草案）》第56条所确立的监管体制依然是多机构混合且分散监管的模式：由国家网信部门负责统筹协调个人信息保护工作，而国务院其他有关部门在各自职责范围内负责个人信息处理活动的监管。在这一监管模式下，建议网信部门针对不同类型的个人信息（例如生物识别信息）设置单项评估机构，只有通过评估的技术才能获得应用许可，并对该技术应用进行定期回访、追踪与监督，〔52〕实现动态评估。《个人信息保护法（草案）》第54条具体规定了事前评估的实施主体、适用场景和评估内容。在评估内容上，草案提议的内容覆盖基本需求，但实践中如何评估其原则的适用程度、以何种标准和参考系进行评估，还需要更细致、更具可操作性的规定。

2. 设立合法、正当、必要三重审查维度。人脸识别技术应用中的个人信息处理应从严贯彻“合法、正当、必要”原则。根据比较法经验，生物特征信息作为敏感个人信息，原则上应禁止处理，〔53〕若出现“法定必需”情境，例如出于国家安全、公共安全、司法鉴定的目的，允许有限的法定授权机构进行处理，〔54〕但依然不允许豁免“合法、正当、必要”原则的适用。

就此而言，欧盟GDPR可以作为借鉴，其第35条规定数据保护影响评估的最少内容范畴，包括：数据处理目的和具体操作的系统性描述，数据控制者希望实现的具体合法利益描述（适用情形下）；数据处理与目的是否相称和必要；评估数据处理对个体权利和自由所产生的风险；为

〔50〕 See U. S. Department of Homeland Security Website，available at https://www.dhs.gov/privacy-impact-assessments，last visited on Feb. 17，2021.

〔51〕 参见李慧琪：《个人信息保护法草案稿已形成，专家建议未来机构设置要明确独立性》，载《南方都市报》2020年7月27日，第A12版。

〔52〕 参见前引〔10〕，邢会强文。

〔53〕 GDPR第9条第1款规定：“对于那些显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、足以识别特定自然人的生物性识别数据以及和自然人健康、个人性生活或性取向相关的数据，应当禁止处理。”

〔54〕 参见石佳友：《人格权立法的进步与局限——评民法典人格权编草案（三审稿）》，载《清华法学》2019年第5期。

应对风险而设置的保障措施、安全措施以及个人数据保护机制；技术处理过程中如何将数据主体合法权利和法案相关规定纳入考量并适用的证明。以上规定分别与 GDPR 第 5 条第 1 款“合法性、合理性和透明性”、第 2 款“具体、清晰和正当的目的”以及第 3 款“为达到目的而适当的、相关的、必要的处理”相对应。

3. 人脸信息存储安全应作为准入审查重点。人脸识别技术的实践无可避免地需要筛选捕捉人脸图像进行数据库比对。因此，人脸识别数据库势必包含大量人脸信息样本。面对海量人脸信息存储需求，人脸识别技术中的存储安全设置必须作为事前准入评估重点，应从三方面予以审核：首先，信息存储的时限和分区。基于人脸信息的特性，若结合其他个人信息将导致信息主体面临急切的隐私、尊严及自由威胁，有学者认为人脸识别技术实践中应在原则上禁止存储原始人脸信息，或在必要时和其他个人信息分开存储。〔55〕其次，人脸信息的匿名化存储设置。现有个人信息的规制中均要求信息应进行技术处理使其丧失指向特定自然人的识别性，且在当下技术条件下无法恢复，比如通过加密、假名、随机化处理，去除其标识性。但有学者提出信息匿名化程度的提高将降低其可用性，〔56〕且不存在绝对不可技术复原的信息。因此，应借助法律规则，明确匿名化处理并非对外传输或共享信息的前提条件，二者并不具备充分条件关系。若须共享传输，则应再次审核第三方传输及二次处理设置是否合规合法、是否足以保障主体法益。最后，第三方介入情境下的存储服务审查。实践中人脸识别技术使用方可能向第三方采购技术或设备，或接入第三方人脸数据库，例如全国居民身份证系统等，实现其技术应用，因此，在涉及第三方服务时，应对第三方技术提供者协议里涉及信息采集和存储的条款进行审查。

（二）人脸识别技术应用中的知情同意实践建议

1. 人脸识别中的知情同意应以告知义务的充分履行为前提

国外法中以“Informed Consent”作为一般个人信息处理的前提，其中 Informed 从文义上解释为“信息充分、知悉情况”，因此整体应被理解为“充分了解情况后的同意”。在处理生物识别信息时，则进一步提升其同意的要求：GDPR 第 9 条第 2 款要求在不违背禁止处理的条件下，由信息主体做出明确同意；BIPA 则升级为清晰严格的书面告知同意形式，从而固定信息传递的明确性和稳定性。〔57〕在目前我国人脸识别的技术实践中，生物识别信息处理者存在未能充分履行告知义务的情形，包括告知“缺席”或者告知“失灵”。究其原因，一方面是由于生物识别信息处理者藏匿于终端设备之后，用户面对提供服务的终端机器无从查询，或者告知冗长造成阅读不便；另一方面，生物识别服务涉及专业技术领域，技术知识不对等可能导致信息主体难以理解告知内容。基于此，建议在生物识别信息处理的告知义务上给予两个维度的规范：

第一，针对生物识别信息等敏感个人信息的处理行为均统一要求履行告知义务，不得免除，

〔55〕 参见陈道英：《〈个人信息保护法（草案）〉之“得”与“失”》，载微信公众号“大数据和人工智能法律研究院”，2020 年 11 月 5 日。

〔56〕 参见王春晖、程乐：《完善个人信息保护法（草案）的建议》，载《人民邮电报》2020 年 11 月 6 日，第 3 版。

〔57〕 参见林凌、贺小石：《人脸识别的法律规制路径》，载《法学杂志》2020 年第 7 期。

即任何组织或机构，无论出于何种目的（不违反禁止规定）处理生物识别信息之前，都应向所涉信息主体进行告知，且告知内容至少包括其处理的个人信息类型、收集方式、信息处理目的、存储方式与时限、安全设置以及信息处理者身份和联络方式等基本信息。〔58〕

第二，应采用清晰、通俗、易懂且明确的语言进行书面告知，同时对不易理解的部分或重点内容进行单独告知。〔59〕在处理人脸信息等敏感信息时，可能面临处理信息规模巨大或远程采集等情况，应考虑结合现代技术手段，通过移动端推送或服务内弹窗等形式进行单独告知。若告知中存在预设格式条款或系统预设模式，应由国家相关监管机构进行预先审查，在生物识别信息的处理周期开始之前保障信息主体的知情权。

2. 从严限制概括同意的适用

根据前文所述，人脸识别技术存在两种适用情形：第一，法律法规允许的、为实现重大的利益所需的情形，例如公共安全、公共健康所需等；第二，法律法规不禁止，且获得主体明示同意授权的情形。在知情同意领域，同意的模式不断发展演变。传统的知情同意要求明确、具体且详实，被称为特别同意，但特别同意在以往生物特征信息处理（基因研究或生物资料库等）的实践中，被证明存在效率较低无法满足实践所需的问题。〔60〕无论是法定许可还是基于主体知情同意的情形，人脸识别势必需要采集海量人脸图像，并和数据库中存储的人脸识别符进行比对，因此完全适用特别同意的难度和成本之大将超乎想象。作为同属于生物识别信息的基因，在其处理实践中，概括同意模式允许将信息主体的同意从当下处理目的延伸扩充至固定框架下的未来处理目的，凭借其灵活性和自由度受到推崇。〔61〕

我国个人信息的同意模式也普遍采用概括同意结合特定例外的形式，它给予信息处理者一定的自由，在设定的处理范围框架内合理处理信息，提高信息处理效率，以应对技术升级或场景变更的需求。但是，作为特别同意的矫正提案，反对观点认为概括同意在未加限制的情况下，可能导致告知程度下降，〔62〕造成同意虚化。因此，在人脸信息处理中，应甄别现有知情同意模式，适当采用附带严格限制条件的概括同意，保障信息价值实现，同时保持个人法益保护的应有水准。另外，可以仿效基因研究领域的医学伦理审查机制，设立科技伦理委员会，对人脸识别等可能引发伦理风险的科技应用，设置科技伦理审查机制，〔63〕规范同意模式的适用。

首先，人脸识别中概括同意的适用条件应予限制。由于概括同意涉及限制框架下一定程度的

---

〔58〕《个人信息保护法（草案）》第 18 条规定处理个人信息前应向个人告知信息处理者身份和联系方式，个人信息的处理目的、方式、种类和保存期限，以及个人行使权利的方式和程序，同时若发生变更，应将变更部分告知个人。若通过制定个人信息处理规则的方式告知，其处理规则应当公开，便于查阅和保存。

〔59〕《个人信息保护法（草案）》第 31 条规定处理敏感个人信息的，除第 18 条规定的告知事项，还应告知处理敏感个人信息的必要性以及对个人的影响。

〔60〕 See Christine Grady et al.，The Changing Face of Informed Consent，376（9）*The New England Journal of Medicine*，856－867（2017）.

〔61〕 参见田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018 年第 6 期。

〔62〕 See Björn Hofmann，Broadening Consent and Diluting Ethics，35（2）*Journal of Medical Ethics*，125－129（2009）.

〔63〕 参见石佳友、庞伟伟：《人体基因编辑活动的民法规制——以〈民法典〉第 1009 条的适用为例》，载《西北大学学报》（哲学社会科学版）2020 年第 6 期。

信息处理自由，在人脸信息等敏感信息处理前，必须经由严格的适用审查。生物资料库研究适用概括同意的探讨中，有学者建议伦理委员会对这种同意模式的采用进行提前审查，并允许主体自由选择是否愿意适用概括同意；也有观点建议根据信息对主体的重要性，将个人信息处理划分为四个层级，〔64〕并基于情境理论，考量并选择匹配的同意模式；另有观点认为针对生物识别信息等敏感性更高的信息，“以一概全”的同意模式无法有效避免风险，而应根据情境酌定。〔65〕无论是伦理审查，还是情境酌定，应由具备专业技术和法律知识的法定授权机构就人脸识别服务中的同意模式进行审查，或将其囊括在事前技术准入审查程序之中，以判断技术应用场景下概括同意模式是否足以有效规避风险、是否存在超额让渡主体权益的情形，〔66〕信息处理情形是否具备采用该同意模式的条件以及信息安全保障是否匹配和有效。

其次，人脸识别中概括同意的范围应予限制。其一，概括同意的框架范围必须合法且正当，符合目的限制。概括同意允许信息处理者在约定框架内处理信息，而无需再次取得信息主体的授权。但是，在人脸信息处理中，对该授权延展长度应做出明确的限制，例如规定仅允许在实现同一目的且情境一致的范围内，概括同意有效，若超越情境或变更目的，则需要二次评估并获得新的同意。其二，概括同意范围应以必要性为限度。“最小、够用”除了作为生物识别信息收集的实践标尺之外，也应作为主体概括同意范围的边界。其三，人脸信息加工后的跨境存储、共享或处理不应纳入概括同意范围。有学者针对我国网络服务隐私条款进行了文本调查，发现存在“当服务器位于境外时，主体同意其数据在境外存储”〔67〕的表述，这种情形下的概括同意可能导致人脸信息在未经确认的境外不特定区域存储、流转，信息风险急剧升高。

最后，人脸识别中采用概括同意应设有严格的监督审查机制，并设置个人选择权、退出权等保障机制。知情同意源自信息主体对于个人信息处理的自决权，这意味着主体不仅有作出同意的自由，也享有撤回同意的自由。为避免技术不对等造成主体难以监督的困境，国家法定授权机构应定期进行信息处理监督和审查，以确保概括授权框架持续符合“合法、正当、必要”原则，并将其审查结果及时披露和公示，使得信息主体能够充分了解风险，有机会更新或撤回同意。信息处理者还应设置人脸识别之外的替代选项，例如动态验证码识别或密码识别，保障用户的自由选择权。

3. 利用技术发展和超级平台创新引入动态知情同意模式

面对刷脸支付终端或者人脸识别门禁，个人难以真正理解其中的安全风险，并且可能无法做出出于真实意愿的同意的意思表示。另外，人脸识别技术的实现过程存在不确定性，例如，约定“必要时”需要将人脸图像与“法律法规允许的或政府机关授权的机构所保存的人脸图像”〔68〕进行比

〔64〕 参见邹晓玫、杜静：《大数据环境下个人信息利用之授权模式研究——重要性基础上的风险评估路径探索》，载《情报理论与实践》2020 年第 3 期。

〔65〕 参见前引〔60〕，Christine Grady 等文，第 856 - 867 页。

〔66〕《瑞士民法典》第 27 条禁止就人格权作出“过度承诺”，原文为 Contre des engagements excessifs，防止民事主体过分地让渡或限制其人格权或自由（如婚姻自由）。

〔67〕 参见李延舜：《我国移动应用软件隐私政策的合规审查及完善——基于 49 例隐私政策的文本考察》，载《法商研究》2019 年第 5 期。

〔68〕 参见淘宝网《生物识别服务通用规则》第 1.4 条，载 https://render.alipay.com/p/f/fd-jm0izzjs/index.html，最后访问时间：2021 年 2 月 17 日。

对核验，或者人脸图像处理所对应的服务可能因为适用场景和功能存续情况而发生未知的调整，〔69〕但具体是哪些法律规定或哪个政府授权的机构，所提供服务（即信息处理目的）与人脸信息采集的持续相适性，对于信息主体而言均无从判断，无法给出符合期待的同意授权。就此而言，美国学者提出的动态情境理论佐证这一现实问题。该理论要求信息保护应考虑情境关联因素，以及信息主体在当下情境中做出的同意和合理预期。〔70〕如今美国 CCPA 也已经认可且采纳了情境风险这一理论，要求信息处理应符合信息主体在其同意情境下的合理预期。〔71〕

其实，涉及人体基因、健康状况的生物医学领域也曾面临类似的情境困境——高敏感度的信息特性、技术门槛和不对等地位，以及快速迭代的技术手段和处理目的，导致知情同意原则遭遇前所未有的挑战。围绕这一困境，学者们进行了激烈的批判、反思甚至重构，最终在传统特别同意、概括同意、分段分层同意、附条件同意等众多理论中，提出了动态同意模式，〔72〕允许个人选择其偏好的知情方式、频率以及内容，并自由决定授予同意或退出同意，〔73〕以提高信息主体在信息处理过程中的参与度。动态同意模式的核心在于参与感和撤回权，〔74〕这一授权模式对于人脸识别技术应用中的人脸信息知情同意具备参考借鉴意义。

首先，动态同意模式下信息主体享有中心地位，能够提高同意授权的有效性，实现充分意思自治。在原有基因生物研究的背景下，动态同意要求在生物资料库和提供基因的参与者之间搭建沟通平台，参与者可以进行偏好设置，自由选择在何时、以何种方式和频率、告知何种内容，进而做出同意选择。在现有人脸识别协议的文本调查中，发现几乎所有服务提供者都选择了加粗或使用着重符号提示用户注意阅读重点信息，但依然存在条款冗长的阅读负担，可能由于能力限制或时间紧迫而无法充分知情。动态同意模式下，个人将可以根据个人偏好，对国家法定人脸数据库中的人脸信息进行管理，定制告知的时间、频率、形式和内容等，提高知情效率。

其次，动态同意模式下信息披露程度和透明程度较高，满足生物识别信息等高敏感度信息处理的知情权要求。譬如，英国牛津大学研究者和部分产业界代表联合提出的同意确保和撤销研究项目（Ensuring Consent and Revocation，2008－2012）是动态同意模式在生物资料研究中的实践探索。该项目中，研究者可以通过技术平台动态地、开放地、及时地披露研究进度和生物资料及信息的处理细节。人脸识别技术正在快速革新，从二维平面识别到三维景深识别，再到活体检测技术。在快速迭代的技术发展中，信息处理的透明性将成为人脸识别中个人信息保护的

〔69〕 实地调查中某便利商店线下微信刷脸支付终端在确认使用服务前可通过点击屏幕小字提示阅读《微信刷脸支付服务协议》。其中第 1.3 条提及对于人脸图像的处理“可能因适用场景和功能存续情况而发生调整，具体以实际提供服务为准”，但该协议尚未发布于其他平台或渠道。

〔70〕 See Helen Nissenbaum，Privacy as Contextual Integrity，79 *Washington Law Review*，119（2004）.

〔71〕 See SB－1121 California Consumer Privacy Act of 2018，SEC 2，Section 1798. 105（d）.

〔72〕 参见前引〔61〕，田野文。

〔73〕 See Richman Wee，Dynamic Consent in the Digital Age of Biology，5（3）*Journal of Primary Health Care*，259－263（2013）.

〔74〕 See Arianna Schuler Scott et al.，Why We Trust Dynamic Consent to Deliver on Privacy，PhD thesis：Investigating Dynamic Consent as a Privacy Control，available at https://ora.ox.ac.uk/objects/uuid:b006cbc2-11b1-42fd-8528-9ca036672b4a/download_file?safe_filename=Camera_ready_IFIPTM_2019_paper_32.pdf&file_format=application%2Fpdf&type_of_work=Conference+item，last visited on Feb. 17，2021.

基础之一，〔75〕能够实时、有效地向个人传达其人脸信息正在由何种技术采集、如何处理、如何进行安全保障，以及实现了何种目的等信息处理细节，从而帮助个人做出判断。

再次，动态同意模式可以保障信息主体享有同意撤回权，将信息主体置于中心地位，允许其根据所了解到的事实决定选择进入和退出，打破既往“同意即终身”的弊端，符合情境理论中合理预期的需求。若将动态同意模式引入人脸识别应用，信息主体将有机会选择让自己的“人脸”消失于互联网络和信息世界之中，从而重获被大数据忘却的片刻自由。以新型冠状病毒肺炎疫情基层防控的场景为例，部分社区管理委员会执行严格的出入政策，采用人脸识别门禁，以限制非本社区人员的流动并追踪社区内人员的进出记录。在疫情防控的场景下，社区居民对于其人脸信息处理的预期是保护个人和社区健康安全，但在疫情逐渐缓解乃至有效控制之后，该期待即发生变化，此时作为信息主体，个人应有权根据更新后的处理目的（社区日常进出管理等），自由选择继续给予或撤回同意。

最后，动态同意在当今技术发展水平下具备实现可能性，且难度可控。万物互联时代的到来和 5G 网络技术的发展，使得轻便、快速、及时的移动小程序更加普及，搭建一个高效动态同意平台不再是难以克服的技术难题。与此同时，依托于现有极具实力的超级平台，人脸识别行业从业者将可能在控制成本的同时，实现高速有效的动态同意。例如，通过手机系统设置、统一用户中心或者加载在社交软件中的程序动态，及时披露公告附近人脸识别技术的细节，包括采集方式、处理目的、安全设置、存储时限、脱敏处理方式等等主体应当获知的信息。

动态同意模式也存在其制约因素，包括主体反复给予或撤回同意而影响信息处理效率，从而造成资源浪费和成本增加，而且信息主体是否能够从相关的、不相关的披露中有效识别潜藏风险也有待商榷。〔76〕但我们需要结合实践，结合其他同意模式，逐步构建我国高效科学的知情同意模式。

4. 人脸识别中的未成年人信息处理限制

由于无差异无接触信息采集的形式，人脸识别适用过程中无法区分被采集者的年龄，因此不可避免地涉及大量未成年人人脸信息。同时，根据我国近年来发布的移动社交用户报告，用户日益年轻已成为趋势，未成年人使用人脸识别服务（例如游戏登录、AI 图片编辑等）十分普遍。如果未成年人的人脸信息泄露或被侵权，其侵权影响将可能伴随一生，特别是技术歧视或算法偏见导致的不公平待遇，会直接严重影响未成年人步入正常社会生活。

未成年人的个人信息通常作为特殊类型的信息被予以特殊规定，且采用监护人代为同意的授权模式。GDPR 规定未成年人生物识别信息处理，除了满足第 9 条关于特殊数据的规定之外，还应同时获得其监护人的同意。同时，处理涉及儿童的个人数据应该更谨慎的考虑数据处理的必要性，保障其目的实现不以过度侵犯基本权利为代价。英国教育部曾根据《自由保护法案》和 1998

〔75〕 See Facial Recognition Policy Principles, uschamber.com, available at https://www.uschamber.com/sites/default/files/ctec_facial_recognition_policy_principles_002.pdf, last visited on Feb. 17, 2021.

〔76〕 See Kristin Solum Steinsbekk, Bjørn Kåre Myskja, Berge Solberg, Broad Consent Versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?, 21 (9) *European Journal of Human Genetics*, 897 - 902 (2013).

年《数据保护法案》发布针对教育机构的生物识别信息保护指导文件，规定学校在使用、计划安装生物识别系统之前，必须根据法律规定获得至少一位监护人的书面同意授权，并且提供了书面告知文件内容模板。〔77〕英国2018年《数据保护法案》中则提出“适龄设计规范”，要求如果某社会信息服务涉及儿童访问者或用户，应在其服务设计时，体现不同年龄差别适用的理念。

实践中，我国对于未成年人个人信息保护的年龄界限设定为14周岁。《民法典》第1036条第1款规定的行为人不承担责任的个人信息处理行为中包括“监护人同意的范围内”的“合理实施”。但是，结合第1034条个人信息定义和范围条款〔78〕来解读这一限制，可以理解为该限制仅适用于非私密信息的个人信息，而人脸信息由于其敏感特性，虽不私密但影响巨大，还应予以明确规范。笔者认为未成年人的人脸信息保护应在普遍保护标准之上予以更为严格的保护：第一，应普遍禁止处理未成年人的人脸信息；第二，在法定必要处理的例外情形下，借助识别系统的适龄设计保障和监护人同意授权模式对信息处理进行约束；第三，严格以“最小必要”为限。这里将衍生出一个问题：监护人同意的核实，包括个人年龄核实和监护人同意真实性核实两个方面。在主体年龄核实层面，随着网络用户的低龄化和普及化，实践中如果由服务提供者或信息处理者全权承担核查义务存在实际困难。因此，《个人信息保护法（草案）》第15条关于未成年人信息处理的规定，提出该条款的适用场景是信息处理者“知道”或“应当知道”，即要求处理者在其能力范围和注意义务内进行年龄核查，而非强加给处理者无限的义务。在一般个人信息处理过程中，有三种常见的年龄验证方式：第一，主体自查，即使用特定服务时个人在资料中心填写出生日期，但这种方式无法规避随意填写而导致误差率极高；第二，实名身份验证，即使用服务时需要提供身份证照文件进行验证，通过身份证照登记的年龄进行核对；第三，自动评审，即通过技术手段，结合个人提供的其他信息综合考评并预估用户年龄段。在人脸识别技术应用中，笔者建议首先应在技术中增加适龄设计，当检测到可能是未成年人用户时，提示应在获得其监护人书面同意后才可以继续使用服务；其次，限缩同意范围，严格禁止对于未成年人人脸信息的对外传输，并最小化其存储时限。

五、结　语

当今技术发展日新月异，“刷脸”已经日渐向更为广泛的领域蔓延。在可预测的未来，人脸识别技术在深度和广度上都将进一步延展，例如将识别技术扩展至毛细血管识别，以及基于主体内在情绪和心理变化等的情感识别，〔79〕或者基于数字孪生技术全方位捕捉复原生物的一切表征。同时，人脸识别的应用场景在未来也将日益广泛，而人脸信息也将逐步成为部分行业的核

〔77〕 See Protection of Biometric Information of Children in Schools and Colleges, Advice for Proprietors, Governing Bodies, Head Teachers, Principals and School and College Staff, March 2018, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf, last visited on Feb. 17, 2021.

〔78〕《民法典》第1034条规定私密信息适用隐私权规定，没有规定的适用个人信息保护，由此可以推断第1036条作为个人信息处理行为的规范，应适用于非私密信息的一般个人信息。

〔79〕 参见前引〔22〕。

心生产要素，那么，基于人脸信息所产生的商业利益，信息主体是否享有相应的报酬请求权，都可能成为值得探讨的议题。但是，在享受技术所带来的便捷红利时，人脸识别的法律风险不容忽视：人脸识别技术的泛滥可能会严重威胁个人的隐私权、平等权、人身自由、人身及财产安全等。当前由于监管执法的真空，人脸识别应用已有失控的苗头，亟待出台相关具体法律法规和监管措施。

我国《民法典》对个人信息保护制度已经作出了重要的完善，对个人信息的处理设定了基础性的法律框架，其所约束的义务主体“信息处理者”涵盖了从事个人信息处理活动的所有机构和个人，突破了《网络安全法》在适用对象上的限制，具有一般性意义。此外，立法机关当前也在紧锣密鼓地推进《个人信息保护法》的制定。在未来，相信与之相配套的行政法规、规章等规范性文件、实施准则也将陆续颁行。这些配套法律规则的实施，对人脸识别的法律规制而言，无疑是十分必要和大有助益的。

Abstract: Facial recognition technology demonstrated its promising efficiency in current applications, but it is always accompanied with massive concerns on its accuracy, safety, ethicality, and legitimacy. The first legal case upon the application of facial recognition in China acted as a signal to show the attention and discussion of the personal information protection in this area. There are three possible steps for improving the information protection mode in the application of facial recognition. First, the three core principles must be strictly followed as the front shied of information safety, and the technology should be prohibited unless there is special cautious authorization. Second, broad consent must be strictly regulated and the freedom of opt-in and opt-out must be guaranteed. Third, innovation on the format of informed consent could be given by getting proper experiences from dynamic informed consent based on the proven technologies, to secure the personal rights in information protection.

Key Words: facial recognition, biometric data, informed consent, dynamic informed consent

（责任编辑：武　腾　赵建蕊）