

人脸识别技术法律规制研究

何世新

广西大学法学院, 广西 南宁

收稿日期: 2024年5月17日; 录用日期: 2024年5月29日; 发布日期: 2024年7月4日

摘要

郭兵诉杭州动物世界采集游客人脸信息一案的判决存在对人脸生物识别信息获取和处理的必要性论证不足的问题, 必要性应是比例原则在个人信息处理领域的展开, 知情同意原则是意思自治在个人信息处理领域的体现。使用人脸识别技术在符合合法、正当、必要原则的前提下, 还要严格遵守知情同意原则, 不得以不同意为由拒绝提供服务。面对人脸识别技术运用扩大化趋势, 应当严守上述两原则, 并通过严格把控技术准入、增加公众参与、扩展救济渠道等加以规范。

关键词

人脸识别, 个人信息处理, 必要原则, 法律规制

Research on Legal Regulation of Face Recognition

Shixin He

School of Law, Guangxi University, Nanning Guangxi

Received: May 17th, 2024; accepted: May 29th, 2024; published: Jul. 4th, 2024

Abstract

The judgment of Guo Bing v. Hangzhou Wildlife World on collecting tourists' face information is insufficient to demonstrate the necessity of obtaining and processing facial information. The principle of necessity should be the expansion of proportional principle in the field of personal information processing, and the informed consent principle is the embodiment of autonomy of meaning in the field of personal information processing. The use of face recognition in accordance with the legal, legitimate and necessary principles of the premise, but also strictly abide by the informed consent principle, do not refuse service on the grounds of non-consent. In view of the trend of the expansion of face recognition technology, the above two principles should be strictly

observed and regulated by strictly controlling technology access, increasing public participation, and expanding relief channels.

Keywords

Face Recognition, Personal Information Processing, Necessity Principle, Legal Regulation

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

备受关注的郭兵诉杭州动物世界有限公司(以下简称动物世界)这一“中国人脸识别第一案”以法院判令动物世界删除原告人脸面部信息和赔偿合同利益损失落下帷幕,[1]但消费者并未迎来“真正的胜利”。景区以人脸识别更换原指纹识别的行为究竟是否符合必要原则?“同意否则拒绝服务”的行为如何规制?以及面对人脸识别技术广泛使用现象如何构建合适的法律规制路径,都是目前需要探讨的问题。

2. 人脸识别技术及其应用中的问题

2.1. 人脸识别技术及其安全隐患

人脸识别技术是能将自然人的照片、视频等形式的面部探测图像转化成数字模板,具有检测、识别和验证功能的技术,与指纹识别、虹膜识别等技术相比,人脸识别技术具有非接触式、交互性强和高效便捷等优势[2]。自然人的人脸信息是个人信息中的生物识别信息之一,受法律保护。《个人信息保护法》已将其从民法典里笼统归属个人信息范畴提入敏感个人信息之列,采取更为严格的保护措施。随着我国信息和人工智能产业的发展,人脸识别技术已经运用到越来越多的场景中,如支付、安防、医疗、金融等领域,但其快速发展运用也带来一系列风险挑战,如隐私泄露之忧、财产安全之虞和歧视对待之隐患等。人脸识别技术使用根据行为主体不同分为公权力机关使用和私主体民用,本文主要讨论后者。

2.2. “人脸识别第一案”案情与判决分析

2019年4月,郭兵向动物世界购买了以指纹识别技术入园的景区年卡。合同履行期间,动物世界决定将入园方式变更为为人脸识别,向郭兵在内的所有年卡用户发送短信告知办理人脸识别系统激活,否则无法正常入园,并于同年10月单方停止使用指纹系统。郭兵不同意改用人脸识别,诉至法院,请求判令动物世界关于改用人脸识别技术的告知短信和对新用户告知办理人脸入园年卡的店堂告示无效并赔偿年卡费用。最终,两审法院均判令动物世界主动删除郭兵的人脸面部照片信息并赔偿合同损失,但在判决的论证途径中存在一定问题。

一审法院在判决中认为动物世界为了提高年卡用户进入景区的效率,放弃指纹识别而改用人脸识别技术的行为符合必要原则。二审法院则认为改用人脸识别的短信是对郭兵发出的新要约,因郭兵的拒绝未达成合意而不成为双方的合同内容,对短信内容无评判必要。而采用人脸识别的店堂告示是对新办卡用户的要约,与郭兵无关,亦未评论其是否符合必要原则。

本案中的核心问题是动物世界以人脸识别替换指纹识别是否符合必要原则,而法院对这一问题有所回避。人脸识别技术或许能提高游客入园的效率,但是也要考虑到人脸相对于指纹的特殊性,如前所述

提到该技术非接触性的特点会带来不易察觉的隐私泄露和歧视对待的风险。例如媒体报道过某地售楼部采用人脸识别技术暗中歧视区别对待购房者以至于客户不得不带上头盔看房,这是指纹等接触式、需要被采集者配合的识别技术难以做到的。人脸识别技术过度延伸的后果非指纹、虹膜等技术可比,效率的背后还应有安全的考虑,人脸面部信息泄露及滥用的后果需予以谨慎考虑。一审法院仅仅以采用人脸识别技术能提高景区入园效率为由就判定动物世界改用人脸识别符合必要原则,这是难以具有说服力的。

即便假设动物世界改用指纹识别的行为符合必要性,其还要遵循知情同意原则,要明示收集和使用人脸信息的目的、方式,并征得用户同意。本案中动物世界试图将年卡用户在办卡时留存的个人面部照片激活升级为人脸识别信息,向用户发送了告知短信,但短信中“请激活人脸识别否则将无法入园”的通知实际上是以“不同意则拒绝服务”的方式限制消费者选择权并侵害自然人的个人信息权益。二审法院也据此以动物世界在合同履行中违约为由作出判决,围绕合同有效性进行论证,不评判改用人脸识别是否必要,未对人脸信息保护做深入讨论。

3. 收集、处理人脸信息的原则及存在的问题

3.1. 合法、正当、必要原则与比例原则

合法、正当、必要原则可见于中国《消费者权益保护法》《网络安全法》和本案发生后实行的《民法典》与《个人信息保护法》等相关条文,是我国处理个人信息所需遵循的基本准则。合法原则是该原则中的形式性、程序性要求,即主体处理个人信息应当符合法律和行政法规的规定,遵循法定程序。正当、必要原则是实质性要求,是对主体处理个人信息行为手段方式、目的的合理性评价。正当原则包含“目的正当”,要求处理个人信息的使用目的需要特定、明确与合理,还包含“业务正当”,即个人信息的收集应出于业务需要,不得超出业务能力范围收集[3]。对于必要原则,“必要”一词仍属于模糊不确定有待论证的法律概念,要准确评价动物世界的行为,乃至从中找到完善对人脸识别技术法律规制的思路,就要对必要原则做出合理的解释。有学者认为,必要原则是个人信息处理者负有的一种相对有限和审慎的注意义务,强调对“直接相关”“最低频率”和“最少数量”个人信息的最小化处理[4]。另有学者主张必要原则包含禁止过度损害和禁止保障不足两方面[5]。还有学者考虑动态利益平衡,低位阶法益不能对抗高位阶法益,力求实现自然人和个人信息处理产业与国家利益的平衡[6]。

笔者同意必要原则是比例原则在个人信息处理领域的展开,是公法的私法化。国家机关对个人信息的处理无疑要符合比例原则,如欧盟《一般数据保护条例》序言第四项“……必须根据比例原则……”,我国《个人信息保护法》中对于国家机关采集个人信息规定的“不得超出履行法定职责所必需的范围和限度”等。而私主体采集个人信息也要受到比例原则的限制,比例原则的精神在于“禁止过度”,该精神可对整个法律体系发挥作用。传统三阶比例原则由三个子项组成:适当性、必要性和衡量性,个人信息处理的必要原则即是其子原则之体现。必要性里面包含两层含义:一,为实现某一目的存在多种行为方式选择,否则必要原则也无适用的余地;二,在能够实现这一目的的诸多待选方式中,选择其中最小损害公民权利的方式,也即“最温和手段”。行为人收集、处理人脸信息前,应当进行事前评估,即是否存在其他方式实现其业务目的,其意欲采取的行为方式是否合法、正当尤且必要,是否是对自然人个人信息权益侵害程度最小的方式。

本案中动物世界辩称由于用户指纹存在破损、污染,指纹识别机器准确率低等原因,为了提高用户入园效率,不得不改用人脸识别系统。而在提高入园效率的方式选择上,景区有扩大园区入口、增加指纹识别机器以分散、缩短排队长度、更新升级原指纹识别系统以提高准确率、增加工作人员用人工审核无法正常指纹识别的用户等方案。然而景区没有与年卡用户讨论协商,而是单纯告知“同意人脸识别否

则拒绝服务”并单方拆除指纹识别设备,把园区可能本应承担的经营成本直接转移到用户身上,获取比指纹更为敏感的人脸生物识别信息,增加消费者对人脸信息泄露风险的担忧,也无法证明是“最小损害”,这种行为是不符合必要原则的。而且,动物世界单方告知用户需激活人脸识别否则无法正常入园的行为,也严重违背了知情同意原则。

3.2. 知情同意原则与“不同意则拒绝服务”

知情同意原则其在法律条文表述中一般紧跟在合法、正当、必要原则之后,是个人信息收集领域中的传统“帝王条款”。知情同意原则要求个人信息收集者向被收集者明示收集、使用信息的目的、方式和范围,核心要求是征得被收集者同意。该原则下的理想场景是:每个自然人都能完全地了解他人收集自己个人信息的目的和可能带来的后果,并基于充分的理性做出抉择,意思自由和私权自治得到圆满的维护。然而,这对自然人的理性要求极为苛刻,且数字信息产业的飞速发展已经极大超越了该原则的立法背景。随着人类社会进入“大数据时代”,个人信息收集和处理已经成为不可逆转的经济浪潮,知情同意原则既给个人信息收集、处理者增加获取被收集者同意的成本,成为收集方眼中阻碍产业发展的绊脚石,同时自然人面对繁多纷乱的告知事项,往往忽略大部分条款,又或者因能力不足无法意识到行为风险,从而使同意沦为形式主义,保护理性和意思自由的知情同意原则效果大打折扣,学界因此产生知情同意原则存废之争,有学者鲜明提出,同意不应是个人信息处理的正当性基础[7]。

笔者认为,知情同意原则由来已久,是私法中意思自治原则在人脸信息收集处理领域的体现,其法律价值根植于自由。伯林的消极自由说认为:一般说,就没有人或者人的群体干涉我的活动而言,我是自由的,在这个意义上,自由简单地说,就是一个人能够不被别人阻碍地行动的领域[8]。自然人享有自由,拥有对处理人脸面部信息等个人信息的自决权。个人没有谨慎阅告知事项,授予他人获取个人生物识别信息权限,也是基于主体的意志自由并自甘承担风险后果,他人无权干涉。对于自然人缺乏判断能力以致遭受权益损害的情形,可以采取改良知情同意原则、加强程序规制和完善事后救济等措施,而非直接摒弃该原则,从他人外部视角主观臆断自然人抉择能力本身就是存在法理缺陷的。况且即便否定该原则,其他的如“场景理论”和“社会控制”等理论亦有不足,当下国内外均没有更优的路径选择[9]。难以想象本案中若动物世界直接将年卡用户办卡时存留的照片信息升级为人脸识别信息而不向用户发送告知短信会引起何种纠纷,园方选择发告知短信既是在形式上遵守知情同意原则,或许也有避免事后纠纷之意。而我国涉及人脸识别的最新立法《个人信息保护法》也继续肯定了知情同意原则。

在肯定知情同意原则存在的必要后,实践中对该原则的遵守却存在一系列问题。正如动物世界向年卡用户告知需激活人脸识别否则将无法正常运转一样,个人在面对告知事项时,实际上没有真正选择的自由,因为不同意条款以授予面部信息就无法获得相对方的产品和服务。除了本案的景区入园外,各地还存在进入小区的门禁、高校课堂签到和部分APP注册强制使用人脸识别的现象。对于“不同意则拒绝服务”的行为,我国法律法规早已作出规制:《电信和互联网用户个人信息保护规定》就规定:“……不得以欺骗、误导或者强迫等方式……收集、使用信息”。然而其后的《消费者权益保护法》和《网络安全法》将相关表述改为“不得违反法律、法规的规定和双方的约定收集、使用信息”,表义反而略显含糊。2021年11月生效的《个人信息保护法》针对近年来的强制同意行为,再次明确表述为:“个人信息处理者不得以个人不同意处理其个人信息为由,拒绝提供产品或者服务”,并将该内容列为独立的第十七条,而非之前的法律法规中跟在合法、正当、必要原则后的附款,可见该行为已经引起了明显的社会关注。《个人信息保护法》出台后,近四成受访者认为人脸识别滥用技术情况有所好转[10]。然而,出于收益和风险的掂量,仍可能有部分信息处理者铤而走险,人脸识别第一案并非最后一案。对于“不同意则拒绝服务”的行为,还需通过加强事前准入审查和完善事后救济两大方向予以规制。

4. 完善人脸识别技术法律规制的建议

面对人脸识别技术的使用扩大化趋势，防止从第一案向无限案迸发，需尽快完善相关法律制度。笔者无意在此文中给出完整的制度框架和具体判断是否可采用人脸识别的科学评估体系，因为这一是需要强大的团队花费大量时间才能完成，二是人脸识别技术是随互联网和大数据产业发展而日新月异的，制度设计的滞后性无法避免。但是至少可以通过本案引出的两大原则及其实施中存在的问题进行思考。

4.1. 完善事前审查制度

对于人脸识别，域外大致形成了“原则禁止，特殊允许例外”的处理原则趋势，^[11]且欧美民众对全面禁止人脸识别技术的呼声较高，美国部分州市甚至立法禁止政府使用人脸识别技术^[12]。然而全面禁止人脸识别技术过于极端，会影响技术创新和信息产业发展，加之欧美和我国国情差异较大，欧美民众对人脸识别的恐慌多出于对政府的不信任和对自由价值的差异化理解等因素，我国应辩证看待，采取特别允许制度，即事前审查准入以规范人脸识别技术运用才是平衡公民信息安全和产业经济效益的最优选。

我国《个人信息保护法》新增了关于收集、处理人脸识别信息的行政许可规范，然而主要针对的是个人信息处理者向境外提供个人信息的行为。如第三十八条要求向境外提供信息的，要通过国家网信部门组织的安全评估或者通过专业机构的个人信息保护认证。而对于在我国境内收集、处理人脸信息的行为，该法律只要求个人信息处理者事前进行个人信息保护影响评估并保存报告至少三年，然而这是处理者内部的自我评估，而非行政机关组织的安全评估即事前审查，这对处理者的自我评估能力和诚信品质要求较高。后续立法修改可以参照向境外提供个人信息所需的审查手续，要求行为人收集人脸信息前也要通过网信部门的安全评估。因此，符合条件有必要进行事前审批的行为人在境内采集、处理人脸信息之前，应自行或向专业机构进行技术资质评估并向行政部门提交人脸识别技术许可申请，由行政机关综合其使用目的和范围、技术算法的安全性、用户告知协议的规范性、人脸信息的储存安全状况等因素考量，严格把控人脸识别技术运用准入，并可对获得使用人脸识别资质的单位进行备案登记，定期抽查检测。

4.2. 民众参与必要性论证

无论是网信部门的安全评估还是行为人自我做出的影响评估，核心是对是否符合合法、正当、必要原则的评判，尤其是必要原则。《网络数据安全条例(征求意见稿)》中只初步要求数据处理者公开展示处理规则，而在规则制定时缺少外界参与。笔者建议参考其中第四十三条“互联网平台运营者制定规则时要向社会公开征求意见”，人脸数据收集、处理者也应公开征求、听取公众的意见。社会公众、团体有广泛的代表性，具有专业、高效和务实的优势，能补充人脸识别信息治理的空白、增加治理机制的灵活性等^[13]。信息收集处理者罗列所有能实现业务目的的方式后，其选择“最温和手段”时应交换立场、听取相对方意见而非单方决断，要站在被收集方的角度考量，是否必须采用人脸识别技术。通过公布具体方案、召开座谈会等方式，听取公民意见，寻求对其个人信息权益损害最小的方式。如在动物世界一案中，园方应将所有能实现业务目的的入园方式选择告知年卡用户，可采用网络线上投票选择、在线下入园点对年卡用户做抽样调查、召开座谈会等方式，充分吸取相对方的意见，而不应单方决定采用人脸识别技术。

4.3. 妥善解释说明但书条款

“不同意则拒绝服务”的行为已经被《个人信息保护法》所禁止，且该法再次申明必须遵守知情同意原则，若再发生类似于郭兵诉杭州野生动物世界的案件，法院就不用围绕合同有效性进行论证而可以

直接适用该法。虽然该法第十六条明确表述收集、处理一方不能以自然人不同意为由拒绝提供服务或产品，但其后也加了但书条款“属于提供服务或产品所必需的除外”。此但书条款主要是为了部分必要场景所设，如由政府机关主导的政务 APP、机关内部办公、曾经的防疫政策等都可见人脸识别技术的使用。除此之外，私主体在民商事领域如互联网在线支付涉及到账户本人身份确认等也会强制使用人脸识别，该但书条款为这些行为给予肯定。但其也不可避免地为未来人脸识别技术扩大化运用趋势埋下纠纷伏笔，这是由其法律概念“必需”的不准确性所造成的。举证与反证某产品或服务是否必需采用人脸识别技术会是一个复杂问题。虽然目前看来举证难度较大，毕竟在民商事领域中，人脸识别不是唯一的途径，指纹、声音、字符图形数字密码和虹膜等都是替代之选，且能防止产生人脸识别非接触式难以察觉所带来的一系列问题。但人脸识别是同互联网和大数据产业相随发展的，现在社会接受程度较高的线上支付领域也不过是近十年的新兴产物。知情同意原则未来一定会继续受到挑战，这一但书条款会是争议点乃至突破口之一。在“场景理论”和“社会控制”等理论挑战下，我国立法仍坚持知情同意原则，就要在立法或司法解释中提前对该但书条款加以阐释、限缩以稳定该原则。

4.4. 完善对侵权行为的规制

4.4.1. 拓宽权利救济渠道

对于人脸信息权益纠纷，我国仍主要以消费者提起民事诉讼的途径解决，如本案郭兵起诉动物世界。但行为人往往是大规模集群收集人脸面部信息，而自然人又受制于其对人脸信息重要性的认知和法律维权意识等因素而难以集体提起诉讼，一方面这导致未提起诉讼的其他当事人权益得不到救济，另一方面若相关当事人均独立提起诉讼，也会增加司法机关的负担。美国相关法案就把人脸识别信息保护权定义为“集体性权利”，可由州检察长提起诉讼以维护个体利益^[14]。为此我国可以考虑授予检察机关对大规模集群侵犯自然人人脸面部信息行为的起诉权。在 2021 年 3 月，江苏镇江市京口区检察院就曾向该区市场监督管理局等相关单位发出公益诉讼诉前检察建议，督促行政机关依法充分履行监管处理该区多处房产售楼部采集自然人人脸信息行为的职责，对此或许可以考虑将人脸信息侵权之诉明确规定纳入公益诉讼之列^[15]。除检察机关，团体组织如消费者协会也可提起维权之诉。

此外还可以考虑非诉手段，探讨自然人与企业协商以及第三方协调的可能。为此可以引入行业自律，中国支付清算协会于 2020 年初发布的《人脸识别线下支付行业自律公约(试行)》就对人脸识别技术在金融支付领域的运用对会员单位提出包括用户权益保障在内的五大管理要求，是一项有益探索^[16]。更多的行业也应行动起来，未来可通过所属行业协会介入自然人与会员单位的协商、提供投诉渠道并公开回应、对违规会员予以行业惩戒等方式，拓展救济渠道，保障公民人脸信息权益。

4.4.2. 加大惩罚力度

明确行为人法律责任后，要考量侵权损害赔偿的补足性和警示效果。笔者通过威科先行法律信息库，以“人脸识别”为检索关键词，检索浙江省内 2021 年 1 月至 10 月因违规采集人脸信息而作出行政处罚的案件共 56 起，多发生在房产销售领域，罚款金额最低 1.5 万元，最高 25 万元。这样的处罚额度所能带来的威慑力值得思考。2021 年 11 月生效的《个人信息保护法》提高了对行为人的处罚力度，对违法收集、处理人脸信息者予以一百万元以下的罚款，情节严重的处以五千万元以下罚款、停业整顿甚至吊销营业执照等。这一处罚力度相比原主要依据《消费者权益保护法》相关规定作出的处罚更重。该法生效后，通过前述方式检索得到相关案件呈减少趋势。初步看来，该惩罚力度似是有效遏制违规收集人脸信息现象，但仍需等待更长的时间予以同期比对、证明。总之，提高惩罚力度是一项可行的规制路径，未来仍可考虑增加相应措施，如前述的行业协会惩戒、更高比例的营业额罚款、禁止行为人一定年限内

再次从事人脸信息收集处理等。此外,在相关侵权案件中自然人的实际损失一般难以计算,为此可以参考美国、欧盟设置最低赔偿额度标准,[17]甚至设立惩罚性赔偿制度等。

参考文献

- [1] 中国法院网. 人脸识别第一案[EB/OL].
<https://www.chinacourt.org/article/detail/2022/03/id/6563642.shtml>, 2024-01-10.
- [2] 景晨凯, 宋涛, 庄雷, 等. 基于深度卷积神经网络的人脸识别技术综述[J]. 计算机应用与软件, 2018, 35(1): 223-231.
- [3] 梁泽宇. 个人信息保护中目的限制原则的解释与适用[J]. 比较法研究, 2018(5): 16-30.
- [4] 卢家银. 网络个人信息处理中必要原则的涵义、法理与适用[J]. 南京社会科学, 2021(12): 118-125.
- [5] 刘权. 论个人信息处理的合法、正当、必要原则[J]. 法学家, 2021(5): 1-15.
- [6] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [7] 任龙龙. 论同意不是个人信息处理的正当性基础[J]. 政治与法律, 2016(1): 126-134.
- [8] 以赛亚·伯林. 自由论[M]. 胡传胜, 译. 南京: 译林出版社, 2003: 189.
- [9] 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[J]. 法制与社会发展, 2018, 24(6): 111-136.
- [10] 新京报. 环球人物网: 近4成受调查者认为人脸识别技术滥用情况有所好转[EB/OL].
http://epaper.bjnews.com.cn/html/2022-02/22/content_815037.htm?div=-1, 2024-02-10.
- [11] 高仲劭. 人脸识别信息处理行为的法律规制[J]. 学习论坛, 2022(1): 130-136.
- [12] 石佳友. 人脸识别治理的国际经验与中国模式[J]. 人民论坛, 2022(4): 48-53.
- [13] 洪延青. 人脸识别技术应用的分层治理理论与制度进路[J]. 法律科学(西北政法大学学报), 2024, 42(1): 89-99.
- [14] 林凌. 人脸识别信息保护中的“告知同意”与“数据利用”规则[J]. 当代传播, 2022(1): 108-112.
- [15] 杨华. 人脸识别信息保护的规范建构[J]. 华东政法大学学报, 2023, 26(2): 68-79.
- [16] 宋丁博男, 张家豪. 新安全格局下人脸识别技术应用的法律规制[J]. 科学决策, 2024(2): 143-154.
- [17] 付微明. 个人生物识别信息民事权利诉讼救济问题研究[J]. 法学杂志, 2020, 41(3): 73-81.