Dispute Settlement 争议解决, 2024, 10(2), 829-835
Published Online February 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.102113

Hans汉斯

“人脸信息”的法律保护探究

陈　玲，王恒倩

上海政法学院，刑事司法学院，上海

收稿日期：2023年10月9日；录用日期：2024年1月30日；发布日期：2024年2月19日

摘　要

近年来，人脸识别技术迅速发展，在交通、刑事侦查等诸多领域都有所运用，这一技术在带来诸多社会便利的同时也引发了各种各样的风险，使得个人的信息安全受到威胁，为解决当前出现的困境，应当加强对人脸识别运用中个人信息的法律保护。本文基于中国处理人脸信息的行政、刑事、民事法律规范中的问题进行分析探讨并提出相应的建议，以期在新兴技术下个人信息的保护更加周到，相关法律更加严谨。

关键词

人脸识别，个人信息，法律保护

Exploration of the Legal Protection of “Face Information”

Ling Chen, Hengqian Wang

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: Oct. 9th, 2023; accepted: Jan. 30th, 2024; published: Feb. 19th, 2024

Abstract

In recent years, the rapid development of face recognition technology, in transportation, criminal investigation and many other fields have been used, this technology brings a lot of social convenience but also triggered a variety of risks, so that personal information security is threatened, in order to solve the current dilemma, the use of face recognition should be strengthened in the personal information of the legal protection. This paper analyzes and discusses the problems in China’s administrative, criminal, and civil legal norms for dealing with face information and puts forward corresponding suggestions, with the hope that the protection of personal information will be more considerate and the relevant laws will be more rigorous under the emerging technology.

文章引用: 陈玲, 王恒倩. “人脸信息”的法律保护探究[J]. 争议解决, 2024, 10(2): 829-835.
DOI: 10.12677/ds.2024.102113

Keywords

Face Recognition, Personal Information, Legal Protection

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. 问题的提出

伴随着技术进步和行业发展，人脸识别技术在各领域得到广泛应用，如交通出行、门禁考勤、支付等，为人们提供了更智能的服务，增强了安全保障，也维护了社会的和谐与稳定。然而，人脸识别技术是一把双刃剑。尽管它带来了便利，但也伴随着个人信息安全等问题，可能导致个人信息泄露、隐私权受损，甚至财产损失。刷脸认证和支付已经无处不在，不言而喻地强调了人脸信息的重要性。值得注意的是，人脸识别技术在不断应用和发展的同时，“人脸信息”的保护也从理论走向了现实。对此，我国在法律层面已经开展针对性探索，并逐渐形成较为系统的人脸信息保护规则。但人脸识别技术应用过程中会产生诸多问题，目前的法律法规对其规制有限。《中华人民共和国民法典》首次提到“生物识别信息”，并将其置于人格权编框架之下的个人信息保护范畴，出台了规制人脸信息的《中华人民共和国个人信息保护法》(以下简称《个保法》)等法律法规，但平台和用户地位的不平等造成告知同意原则的失灵，举证能力有限等对保护公民人脸信息有所欠缺。有关人脸信息的法律规定十分零散，从人脸识别法律规范层级上看，位阶越高的规范，对人脸识别的规制越笼统，位阶越低的规范对人脸识别越关注，但这些低位阶的规范效力有限，无法完全发挥对人脸信息的保护作用。刑法具有谦抑性，但不意味着能够缺位，尤其是当前个人信息肆意泄露和滥用的情况下，理应发挥刑法的保护机能。侵犯公民个人信息罪是《刑法修正案(九)》予以修改的，早于《民法典》《个保法》，那么对于人脸识别信息所对应本罪的“情节严重”之标准应如何适用，以及对于“合法获取公民个人信息后非法使用”行为又该如何有效规制，这些问题都值得深入研究，急需提出相应措施来切实保障人脸识别信息主体的合法权益。

2. 民事法律保护问题

随着信息技术自我敏感度的提升，“刷脸”行为几乎可以瞬间完成，政府和企业利用人脸信息作为个人 ID 密匙中“独特码”进行公共管理和商业服务。然而“人脸信息”与隐私信息存在较大差异，机构对人脸信息的收集也不同于隐私侵权，因此，这对构建以隐私为基础的“人脸信息”保护原则带来了一系列的挑战。

第一，造成告知同意原则的失灵。《个保法》第 14 条和《民法典》第 1035 条构建了以“告知－同意”为核心的个人信息处理规则。告知同意原则是指信息业者应当充分告知信息主体有关个人信息被收集、处理和利用的情况，并征得信息主体的明确同意[1]。然而，在实际操作中用户与平台之间的地位并不平等，平台方以提供免费服务而占有优势地位，而用户为了免费使用相关服务却处于弱势地位，这就造成了在处理人脸信息时告知同意原则的失效。

《个保法》第 29 条在一般知情同意规则的基础上，要求人脸信息主体单独同意，未经单独同意处理人脸信息，属于侵害自然人人格权益的行为[1]。信息处理者不能采用“一揽子”通知，而应采用个别通知

[1]参见《人脸识别技术处理个人信息若干规定》第 2 条规定。

的方法，且单独约定条款的使用方法应该足够吸引使用者的注意力，如使用粗体，改变颜色等。对人脸信息进行明示处理时，也应使用尽可能简洁、清晰易懂的语言进行描述，以方便个人查阅和保存，对于重要内容，应该采用标识性方式引起个人的注意。然而从当前 APP 应用实践来看，一般情况下，个人信息处理者采用的是弹窗隐私策略，或者将隐私策略放在页面底部，以概括同意结合特定例外的形式，对个人信息处理规则进行明确。相较于一般个人信息，人脸信息作为敏感个人信息，关乎个人人格尊严，应当予以严格保护[2]，处理人脸信息遵循单独同意规则。同时，同意内容应该避免概括同意或者批量同意，不应该在默认情况下进行勾选，而应该将同意权交给信息主体。但实际操作过程中同意的方式有很多种，比如，在同一个界面上会显示多个告知文件，它们分别与人脸信息处理及一般信息处理有关，为了优化体验，提高工作效率，用户可以一键勾选，也可以单独勾选。判断这两种方式到底属于单独同意还是概括同意，现实生活中的多元化并没有形成统一的规范，这也造成了实践中利用单独同意规则来规避越轨行为。且《个保法》未规定同意瑕疵和非自愿同意的法律后果。根据规定，信息处理者不得强迫或者变相强迫个人同意处理人脸信息。强制或变相强制的同意，违背了信息主体的本意，其结果等同于没有取得对方的同意，但实际应用中，APP 运营商往往通过“霸王条款”强制用户对人脸信息进行加工，“同意”流于形式。大部分用户并没有掌握人脸识别技术，他们的举证能力较弱，归根到底是用户与平台地位不平等，这些都是信息主体私益诉讼能力较弱的主要原因。

美国和欧盟对侵犯人脸信息的行为都规定了严厉的处罚措施，并且公民享有起诉的权利。瑞典就曾经对违反 GDPR 的行为予以高额的行政处罚，GDPR 规定所有信息主体都有权向监管机关投诉、向司法机关提起诉讼，以救济被侵害的人脸信息。美国伊利诺伊州《生物信息隐私法案》(简称“BIPA”)规定，机构有违反 BIPA 侵害信息主体行为的，信息主体可以申请民事诉讼，该机构过失或者故意都要赔偿受害人[2]。2018 年，美国就发生过一起关于 Facebook 违法储存人脸信息的集体诉讼案件，并且得到法院支持。这些都是对人脸信息进行法律保护的具体体现，对中国有一定的借鉴意义。

滥用人脸识别技术非法处理人脸信息，不仅危害个人权益， 还可能损害公共利益。针对实践中被侵权人分散、举证能力弱、通过私益诉讼维权成本高等问题，公益诉讼制度可有效弥补其不足之处[3]。首先，中国发展公益诉讼保护人脸信息具有政策基础。最高人民检察院《关于积极稳妥拓展公益诉讼案件范围的指导意见》强调，要积极稳妥拓展公益诉讼案件范围，探索办理个人信息保护领域公益损害案件。人脸信息在内的个人信息保护的案件理应在内。其次，发展公益诉讼保护人脸信息具有法律基础。从案件范围看，侵犯人脸信息属于民事和行政公益诉讼范围。《个保法》明确侵犯个人信息属于民事公益诉讼案件范围。《行政诉讼法》规定行政公益诉讼的范围[3]：“等”应包括人脸信息领域在内。公益诉讼制度已较为健全，人脸信息公益诉讼案件可径行适用现有的成熟制度。最后，发展公益诉讼保护人脸信息具备实践基础。自《个保法》施行以来，个人信息公益诉讼的案件数量日益增多，实践中也在积极探索人脸信息保护公益诉讼。如湖南省长沙市望城区人民法院审理的个人生物识别信息行政公益诉讼案[4]；李某某侵犯公民个人信息刑事附带民事公益诉讼案等[5]。司法实践为人脸信息公益诉讼的开展奠定坚实基础，故可以进一步发展民事公益诉讼，由法律规定的有关组织以及检察机关来补足用户的诉讼能力，让用户与平台处于平等的地位，从而确保同意原则能够贯彻落实。用户为了获得平台的免费服务必须同意其对人脸信息进行加工，这实际上体现了平台或者用户作为一个“数字理性”的主体缺乏足够的自律能

[2]BIPA 认为：“任何因违反本法而受损害的人，有权向州巡回法院提起诉讼，或向联邦地区法院提起补充诉讼，胜诉一方可就每项违规行为获得赔偿。”
[3]参见《行政诉讼法》第 25 条。
[4]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之二，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——北大法宝 V6 官网(https://pkulaw.com/)，最后访问时间：2023 年 5 月 26 日。
[5]参见上海市奉贤区人民法院(2021)沪 0120 刑初 828 号刑事判决书。

力。享受服务不是无成本消费或者搭便车，提供包括人脸信息在内的个人信息是享受服务的对价，其应当明确自身的权利义务，在真正知情同意的基础上提供、使用服务[4]。

第二，过错推定原则保护力度不强。《个保法》第 69 条规定了发生侵权行为时人脸信息处理者的过错推定原则，相关法律法规没有规定具体的举证责任和其他特殊举证责任。因此，按照民事诉讼程序中原则上“谁主张谁举证”的规定，由信息主体自己对侵权责任中过错之外的构成要件承担举证责任。首先，侵权行为举证困难。信息主体无从获取信息处理者处理信息的痕迹，难以证明信息处理者实施了不当收集、泄露了自己的人脸信息等侵犯了人格权的行为。其次，损害举证困难。根据《人脸识别解释》第 8 条，对侵害信息主体人身权益的财产损失按照其受到的损失或人脸信息处理者因此获得的利益赔偿。但实践中信息主体受到的损害往往难以认定。一方面，人脸信息主体难以在最开始就察觉到有侵权行为，也难以认定发生了多大损失。信息主体相对于信息处理者来看处于弱势地位，量化侵害人脸识别造成的损失较困难。另一方面，如有第三方原因使得人脸信息被泄露，信息处理者以事前做了风险评估主张减免责任时，信息主体向第三方请求赔偿则可能更困难。

信息主体处于弱势地位，在人脸信息受侵犯时因举证不足有限或证据收集渠道有限而维权困难。因此，应对信息主体实行倾斜性法律保护，除上文提到的借助国家机关力量提起诉讼外，还应审时度势地减轻信息主体的举证责任。人脸信息兼具人格利益与财产利益，但侵害人脸信息往往无法直观地判断有无损害以及损害程度，量化评估损害较困难，故应适当降低人脸信息侵权中损害的认定标准。一方面，对损害的认定采取较开放的解释，将风险性损害纳入损害范围，如将预防风险的成本归入损害范围。另一方面，对《人脸识别解释》规定的损害认定标准予以明确化、具体化。当行为对信息主体有造成损害的可能性即可认为达到了相应的认定标准。另外，对精神损失是否纳入《个保法》第 69 条规定的“损失”，学界有不同的声音，本文认为这里的“损失”应当包括精神损失。理由如下：损失包括财产损失与精神损失，第 69 条没有特意规定财产损失，也没有将精神损失排除在外，则应当做文义解释，将精神损失含括在内；《民法典》规定只有造成一定严重的精神损害才可申请精神损害赔偿，“严重”本身就要求损害程度高，将精神损失纳入损失范围，有利于保障信息主体受到侵害后能得到应有的救济。实践中可由法官充分考虑人脸信息侵权各因素之后公平认定、自由裁量。

3. 行政法律保护问题

中国现有的有关个人信息保护的行政法律有近 40 部，法规 30 余部，部门规章 200 多部较为分散，且有关个人信息保护的规定不够统一，无法准确界定行政法领域对个人信息的保护范围，甚至有些条款的规定欠缺可行性，致使“人脸信息”的法律保护未能达到预期效果。

第一，处罚标准不明导致未能有效遏制违法行为。《个保法》规定，违法处理个人信息的责任主体，视情节可能会受到没收违法所得、罚款、暂停相关业务等相应处罚，主管人员和其他责任人员也面临相应数额罚款[6]。根据《个保法》及《网络安全法》的规定，很容易造成跨部门执行的问题。然而在不同的立法中，对违法情形的判断标准却没有一个清晰的界定，往往是由各行政执法部门自行裁量，从而造成不同的执法结果。

第二，禁止性法律规范层级低导致区域性执法问题。《人脸识别技术处理个人信息若干规定》提及“违反法律、行政法规的规定”，实则系引致条款，然在行政法领域，目前只有一些地方性法规来规制人脸识别侵权行为问题。2021 年《深圳经济特区公共安全视频图像信息系统管理条例(草案)》明令禁止在旅馆客房、集体宿舍等可能泄露公民隐私的场所和区域安装人脸识别系统。禁止利用采获信息非法进

[6]参见《中华人民共和国个人信息保护法》第 66 条、71 条；参见《中华人民共和国个人信息保护法》第 60 条、《网络安全法》第 8 条。

行基于敏感信息的个人身份识别，敏感信息用于公共传播时应当匿名化处理，除法律另有规定的除外[7]。2022 年修订的《杭州市物业管理条例》规定物业服务人员不得强制以人脸识别等方式进入物业管理区域或者使用共有部分[8]。以上条例，其一，均属地方性法规，位阶低于法律和行政法规，不能成为《人脸识别技术处理个人信息若干规定》中“违反法律、行政法规”的判定依据。其二，覆盖领域不同且狭小，深圳条例主要规范公共场所，而杭州条例则着眼于小区物业管理和服务。其三，只在本地区的行政执法中使用，这无疑造成人脸信息保护力度不足、区域执法等问题。

第三，公权力约束规范不明引发私权保护风险。早期公共机关利用身份证件来识别公民个人身份，随后，将人脸识别技术用于其事后追踪、提供证据等[5]。例如，将人脸信息与犯罪资料库进行比对，便可迅速锁定嫌疑人。该行为系基于公共利益在公共场所进行的，并不侵犯人脸信息[6]。公权力利用无所不在的摄像头以及人脸识别技术不断扩张，虽然它对遏制违法行为起到了很大的作用，但它同时也限制了私权的发展，私权利与公权力处于“此消彼长”的矛盾状态。

“良法是善治的前提”，针对处罚标准、法律规范层级低等人脸信息行政法律保护问题，首先，统一执法标准。厘清《个保法》《网络安全法》等法律中违法情节判断标准，行政执法机关基于统一的标准，结合不法行为的实际情况，作出相应的处罚，避免各地执法畸轻畸重。其次，完善人脸识别相关法律和行政法规体系。当条件达到一定程度时，可以吸收地方性法规中的有益经验，并与实践需求相结合，将与人脸识别有关的地方性法规上升为法律或者行政法规，从而提升法律规范的位阶，强化其适用效力。最后，构建规范制度，对公权力进行制约，区别人脸识别适用于刑事违法和其他违法行为等不同情形。当人脸识别应用于刑事侦查时，必须做好刑事程序的合规性工作，比如对技术侦查措施的事前审批程序进行严格规范，遵守保密制度，保障信息主体等。

4. 刑事法律保护问题

一旦人脸信息被泄露或冒用，将会给被害人带来不可逆的伤害，此时需要形成完备的法律体系，并结合其他行业规范，对“人脸信息”实行周密的保护。但现实中，中国司法机关对公民个人信息的普遍认识仍停留在信息的隐私特性上，司法资源过度倾注于隐私性较强的个人信息，比如公民身份信息和活动信息，从而忽视了外在社会属性较强的人脸信息。我国现行刑法及司法解释对于人脸信息保护的规定较为模糊，主要有以下两点。

第一，入罪门槛过高不利于打击犯罪。《刑法》第 253 条规定侵犯公民个人信息罪有“情节严重”和“情节特别严重”两档。但何为情节严重或特别严重需要司法解释进一步说明。最高人民法院在 2017 年联合相关部委颁布《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》，该解释第 5 条第 1 款对“情节严重”的犯罪行为进行了界定，但是并没有直接提到人脸信息。人脸信息系敏感个人信息，可解释为该款第 4 项中的“等其他可能影响人身、财产安全的公民个人信息”。依据该款只有非法获取、出售或者提供人脸信息达到 500 条以上，才认定为侵犯公民个人信息罪的基本刑的“情节严重”，否则不构成该罪。如若如此，侵犯人脸信息入刑标准过高。人脸信息数量是行踪轨迹信息、通信内容等信息数量的 10 倍，信息所包含的价值或者说重要性比行踪轨迹等信息低得多。但“人脸信息”本质上系敏感信息，一旦泄露，将可能对人身及财产安全造成损害，因此，人脸信息的重要性即便不高于行踪轨迹等信息，但也可与之相提并论。此外，人脸信息的专有性和不可更改性，对于受害者来说，哪怕是泄露了一条都可能会给他们带来终生无法弥补的伤害，同时人脸信息的失范性传播很容易导致下游犯罪的发生，失范性传播超过 500 人脸信息的才能被认定为侵犯公民个人信息罪，这不利于打击侵犯人脸信息犯罪[7]。

[7]参见《深圳经济特区公共安全视频图像信息系统管理条例(草案)》第 10 条、第 30 条、第 31 条。
[8]参见《杭州市物业管理条例》(2022 年修订)第 50 条第 2 款。

第二，对非法使用人脸信息的行为规制不足。《刑法》规定侵犯公民个人信息罪的行为模式包括非法获取、出售、提供以及窃取四种，对非法使用的行为并未纳入该罪的构成要件中。但相较于其他行为，非法使用人脸信息直接和个人联系起来，具有更为直接的侵害性。有学者认为，合法获取后非法使用的行为，现行刑法足以进行规制，无单独规定之必要。即获取人脸识别信息的行为很多都是下游犯罪的上游行为，而获取后的使用行为可能与下游犯罪的实行行为发生重合，直接将其规定为下游犯罪的罪名即可[8]。虽然非法使用人脸信息行为通常属于其他犯罪的上游，往往被当作其他犯罪的犯罪手段方式之一，按照牵连犯处理。但若前后两个行为侵犯的法益不同，而刑法只评价一个行为，即使犯罪分子最终也依法承担相应的刑事责任，但这有违数罪并罚之嫌，即无法充分反映案件事实，又遗漏评价，造成法益保护的不周延。如果当后继行为尚未造成严重的法益侵害结果，或者非法使用与后继行为分属于犯罪“产业链”上的不同环节时，此时对于非法使用者就存在处罚上的漏洞[9]。

针对上述刑事法律保护的现状，有学者认为，可以将“非法使用”作扩大解释，即只要行为人是带着非法使用目的来获取公民个人信息，不论获取行为是否符合形式规范，都直接在实质上将其评价为“非法获取”，虽然此种解释不存在合法获取后非法使用的行为类型，其直接归属到非法获取后非法使用当中，弥补法条的不足[10]。但该解释有类推解释之嫌，相当于把“非法”评价的重点由客观的获取行为转向主观的“利用目的”，行为人获取行为是否合法完全取决于行为人的主观，即行为人在没有非法使用目的时，获取行为是合法的，反之则是非法的，在逻辑上不能自洽。本文认为，可以考虑以刑法修正案的方式增设侵犯公民个人信息罪的行为模式，即在《刑法》第 253 条之一第 2 款的基础上增加“使用”一词。《个保法》已对非法使用个人信息作出相关规定，也为刑法将非法使用行为入罪提供了理论依据和完善路径。而对于入罪门槛的问题，可以降低侵犯人脸信息入罪门槛，将人脸信息纳入该解释第 5 条与行踪轨迹信息、财产信息并列。

5. 结语

随着科技的发展，人们的生活方式发生了巨大的变化。过去，我们需要提供“我就是我”的相关身份信息，而如今，人们只需要一张人脸就能验证自己的身份，不需要再经过人工验证，大大节约了人力成本。

我们在让渡部分个人信息的基础上获得便利，个人信息的价值得以体现[11]。但随着人们对个人信息的广泛使用，过度滥用和泄露的现象日益增多，个人信息安全受到了严重的威胁，人脸信息作为一种高度敏感的个人信息，其采集和使用的不规范现象引起了对其进行保护的迫切需求。在中国的法律框架下，我们已经看到了一系列规范人脸信息保护的法律法规的出台，包括《民法典》和《个人信息保护法》等，然而人脸识别技术的不断发展，需要进一步完善法律规范进行监管和保护人脸信息。民事法律规范可以为信息主体提供有效的救济途径；行政法规可以强化对信息处理者的约束，确保其合规操作；刑事法律规范可以惩处侵犯公民人脸识别信息的行为。多方并举、共同发力，形成完备的“人脸信息”法律规范体系，为人脸识别信息提供强而有效的法律保护，以使包含人脸信息在内的个人信息得到更好的保护和利用。

为了实现对人信息的全面保护，我们需要政府、企业和个人的共同努力，只有通过多方合作，形成完备的法律规范体系，才能在技术发展和个人信息保护之间找到平衡，确保人脸识别技术的应用既能够为社会带来便利，又能够保障个人信息的安全和隐私，从而构建更加和谐、安全的社会。在这个信息时代，保护个人信息安全，特别是人脸信息的安全，已经成为我们必须共同关注和努力的重要课题。

参考文献

[1] 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.

[2] 潘林青. 面部特征信息法律保护的技术诱因、理论基础及其规范构造[J]. 西北民族大学学报(哲学社会科学版), 2020(6): 75-85.

[3] 朱秋晨. 人脸信息民事司法保护的路径选择[C]//上海市法学会. 《上海法学研究》集刊 2022 年第 5 卷——2022 世界人工智能大会法治论坛文集. 2022: 178-188.

[4] 郭春镇. 数字人权时代人脸识别技术应用的治理[J]. 现代法学, 2020, 42(4): 19-36.

[5] 何文波, 金晓伟, 高争志, 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[J]. 北京警察学院学报, 2017(6): 15-20.

[6] 胡凌. 刷脸: 身份制度、个人信息与法律规制[J]. 法学家, 2021(2): 41-55+192.

[7] 王文娟. 生物特征识别信息失范性传播的刑事治理困境及其出路[J]. 科技与法律(中英文), 2021(5): 55-64.

[8] 李玉萍. 侵犯公民个人信息罪的实践与思考[J]. 法律适用, 2016(9): 11-16.

[9] 刘宪权, 陆一敏. 生物识别信息刑法保护的构建与完善[J]. 苏州大学学报(哲学社会科学版), 2022, 43(1): 60-71.

[10] 陈文昊. 侵犯公民个人信息罪中的“外围”立法与解释进路[J]. 重庆邮电大学学报(社会科学版), 2018, 30(3): 36-43.

[11] 张勇. APP 个人信息的刑法保护: 以知情同意为视角[J]. 法学, 2020(8): 113-126.