Advances in Social Sciences 社会科学前沿, 2024, 13(8), 72-77
Published Online August 2024 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2024.138675

Hans汉斯

人脸识别中个人信息的法律保护

——以“人脸识别第一案”为启示

王婷婷

西安交通大学法学院，陕西 西安

收稿日期：2024年6月3日；录用日期：2024年7月25日；发布日期：2024年8月5日

摘　要

“人脸识别第一案”提高了大家对人脸信息保护的重视。我国对人脸识别中个人信息的保护仍然存在着知情同意规则形式化、民事救济的损害难以确认、保护责任主体不明确、监管机构分散化，监管措施单一等问题。应做到保护个体的自由选择权，确保被有效告知、拓展公益诉讼为人脸信息的救济、强化各个主体的安全保护责任、完善监管机构与监管措施以促进我国个人信息保护的迅速发展。

关键词

人脸识别，个人信息保护，人脸识别第一案

Legal Protection of Personal Information in Face Recognition

—Taking the “First Face Recognition Case” as a Revelation

Tingting Wang

School of Law, Xi’an Jiaotong University, Xi’an Shaanxi

Received: Jun. 3rd, 2024; accepted: Jul. 25th, 2024; published: Aug. 5th, 2024

Abstract

“The first case of face recognition” has increased everyone’s attention to the protection of face information. In China, there are still some problems in the protection of personal information in face recognition, such as the formalization of informed consent rules, the difficulty to confirm the damage of civil relief, the unclear subject of protection responsibility, the decentralization of regulatory agencies, and the single regulatory measures. We should protect the individual’s free

文章引用: 王婷婷. 人脸识别中个人信息的法律保护[J]. 社会科学前沿, 2024, 13(8): 72-77.
DOI: 10.12677/ass.2024.138675

choice, ensure to be effectively informed, expand public interest litigation for face information relief, strengthen the security protection responsibility of each subject, and improve regulatory agencies and regulatory measures to promote the rapid development of personal information protection in our country.

Keywords

Face Recognition, Personal Information Protection, First Case of Face Recognition

1. 引言

信息技术迅猛发展，互联网充斥着每个人的日常生活，人脸识别作为一项提高生活便捷程度的利器，已经被大众接受。然而，其中个人信息的保护也面临着被滥用、泄露的危险，技术的双面性推动着个人信息法律规范的进步。

当前已有诸多学者对“人脸识别第一案”进行多角度研究。高仲劭指出，人脸识别第一案的判决对于我国的个人信息保护的司法实践提供了一定的参考，具有相应的积极意义[1]。罗斌、李卓雄则认为作为一种综合性民事权益，个人信息权益包含诸多权益因素，这也对于个人信息保护的相关法律法规提出了一定完善要求[2]。劳东燕更加注重从判决结果进行反思，指出要恰当利用科学技术，平衡收益与风险[3]。石佳友和刘思齐(2021)通过“人脸识别第一案”的个人信息保护所遇到的挑战，思考利用当前法律来保护个人信息的高效可行方式[4]。毕玉谦、洪霄认为以此案为切入点，民事诉讼要积极回应新兴权利的诉讼，并提出了对诉讼规制的思考[5]。本文在已有研究的基础之上，以“人脸识别第一案”为例，努力探究人脸识别中个人信息保护所存在的不足，以及提出相应法律保护的努力方向和进路。

2. 案情简述

我国人脸识别的第一案，是郭某诉杭州野生动物世界有限公司服务合同纠纷。2019 年 4 月，郭某购买该动物世界的双人年卡，合同确定以指纹识别方式入园，郭某留下姓名、联系方式、指纹信息等。后入园方式改为人脸识别，动物世界向郭某发送了两条短信，要求其激活人脸识别系统[6]。此后，双方就入园方式和退卡事宜协商，但未达成一致，郭某以违约且存在欺诈行为为由，要求野生动物世界赔偿相关费用，清除个人信息等。

本案三个争议焦点涉及了个人面部信息收集许可方式、单方面决定收集加工等处理信息的合法性、面部信息被侵害后的救济方式三个问题。法院认为个人面部信息的获取应当经过当事人的同意，野生动物园擅自更改合同履行方式侵害了消费者的信赖利益，其已经不符合必要原则，信息处理是不正当的。

在服务合同履行中尚有违约责任救济，但是对于广泛存在的“悄无声息”的场景下人脸识别信息的侵权，又该适用何种救济体系。此案件唤起人们对个人面部信息的重视，也是纳入法律保护框架的前奏。

3. 人脸信息保护的现行法律规制

《民法典》和《个人信息保护法》的出台，以及最高人民法院推出的《关于审理使用人脸识别技术

处理个人信息相关民事案件适用法律若干问题的规定》都是相关文件[7]。“第一案”发生时尚无法律规范，但是其蝴蝶效应推动了规则的完善，最高法院针对一个具体问题出台一个司法解释是不多见的，从具体的点解决民生问题，能够有效实现司法政策的目的。

人脸识别归在个人信息下，属于隐私权的一部分。民法典第六章人格权编规定了义务主体负有对他人隐私不可侵犯的义务，不得以任何方式进行侵扰、泄露、公开等行为，保护自然人的生活不被打扰，发生侵权行为时，侵权责任保护是常用方式之一[8]。当然，在我们享受信息红利时也要对个人面部信息的收集让渡一定部分，企业要正当、合法、合理地收集。

各类有关规定中，对于人脸信息处理要遵循合法、正当、必要、诚信原则，理论上违反原则的行为都是违法行为，但是原则性内容相对来说较为宽泛，需要去具体认定。“人脸识别第一案”反映的是相关主体对人脸识别信息是不成体系的。同时，民法典确定了知情处理规则，即处理个人信息应当经过当事人同意。“人脸识别第一案”中以在大堂张贴海报的方式进行，并未有效告知并获得当事人的同意。

同时，《刑法修正案(九)》，将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，并扩大了单位犯罪认定标准，解决了司法实践中相关犯罪的认定难。

2023 年 5 月 23 日，《网络安全标准实践指南——人脸识别支付场景个人信息保护安全要求(征求意见稿)》发布，该《实践指南》针对室内外各区域中的人脸识别支付场景，为人脸识别支付的服务提供方及相关场所管理方提出了具体的个人信息保护要求，相关内容亦能为企业合规处理人脸识别信息等与生物识别相关的敏感个人信息提供有益启发。

个人信息保护的法律规范从无到有，从一般到专门化，未来还将在提高效率和保护隐私方面寻求平衡和精细化。完善公检法部门之间的联合协作，推动形成个人信息保护多元共治的良好局面。

4. 人脸识别中个人信息保护的现存不足

4.1. 知情同意规则形式化

信息采集需要获得被采集者的同意，个人信息自主原则是基本原则之一，但是在实践中此原则常被架空或被变相地规避。在实践中，主要体现为强制或变相强制收集，信息网络下点击一下就已订立合同，认定过于“形式化”三大问题。

强制或变相强制是指在未经信息主体同意下，基于管理者同意而直接移用；或将人脸识别作为唯一一种方式获取服务。比如说部分高校系统中直接将掌握的学生信息录入，或部分销售场所或娱乐场所只允许刷脸进入而不提供其他进入方式。这都变相地剥夺了被采集者的知情同意权。

信息网络环境下，使用某个 APP 时，在注册页面下方有一行小字，往往只有点击同意才能够使用此软件，大部分人意识不到点击一下就已和软件拥有者订立了合同，也不会认真阅读其中的条款。民众的敏感度低，从众效应和自身信息处理能力的限制使个体做出选择并非理性，而司法实践中对于形式化文本的支持率也高达 96%以上。

信息时代格式条款规则僵化，对于在协议中已经划线或加粗的字体提示，只是达到了提示目的，但是并无勾选项，使用者并不能选择，然而基于使用某些 APP 的需求，尽管 APP 未必需要使用这些信息[9]，也必须同意。知情同意仍然是强制的。

4.2. 民事救济的损害难以确认

当事人个人面部信息被损害后一般会选择民事私益诉讼，但是司法实践对于人脸识别的相关案例数量较少，仍然处于探索阶段。对于损害事实难以确定，因为很难产生实际可计量的损害，更多是信息泄露的外部影响和担心信息泄露的内部焦虑。即使转换为实际上的损害，也难以具体确定侵权主体以及多

个主体之间需要承担的份额比例，导致当事人无法获得相匹配的民事救济；企业与个人之间在信息掌握方面的不平等地位，也使解决平等主体之间的民事诉讼机制难以发挥实效。信息泄露往往具有隐秘性且技术性较强，个人难以获取证明力较高的原始证据，难以提出反证证明企业未能尽到合理注意义务。实践中被侵权人较为分散，举证能力较弱，且维权成本较高，使当事人往往选择放弃维护自身利益。

4.3. 保护责任主体不明确

人脸识别技术被应用于娱乐、技术和考勤等多个领域。随着人脸识别技术的门槛较低，数据收集的主体和收集的种类也日益拓宽，但是小型企业可能并无相关的防范个人信息泄露的技术手段，加上数据安全保护的责任的主体也并不够明确，可能会出现一开始的数据被随意获取和交易的后果。

从线上路径来说，互联网平台提供一份服务协议，人脸信息会直接传输到云端的服务器，这样的话提供网络服务的主体、整理获取数据的主体和实际控制人是同一个人[10]，用户能够明确谁掌握着自己的身份信息，在发生纠纷时往往能够有明确的被告。但是协议中并未对具体的责任保障义务作出规定；从线下路径来说，设备的实际控制人和数据的处理人并不相同，难以确定具体主体。比如说门禁系统中，设备控制人是物业，但数据控制人是谁往往需要花费大量时间去追溯，涉及的多个主体之间又会相互推诿，难以具体确定保护责任的主体。

4.4. 监管机构分散化，监管措施单一

我国目前并没有个人信息方面的专门机构来监管，涉及网信、工信、邮政、人民银行等部门，部门分布较为分散，对于个人信息方面的监管能力有限。部分领域监管主体缺失，比如说旅游领域对于旅游经营者掌握的旅游者信息，并没有明确规定确认监管措施或程序的内容；部门权限模糊不清，多头监管仍然存在。在信息的收集和使用等环节，实行的部门化的监管方式，并未明确部门之间的权责划分[11]。比如通过三大服务商将信息出境贩卖，电信与公安部门之间都有责任会相互推诿；监管机构仅具有一般的知识，对于专业知识较强的技术性领域，很难实现有效监管。

监管措施较为简单，难以实现高效监管。信息监管机构大多采用事前咨询、行政许可等方式，也有趋势用行政约谈替代行政处罚等现象；监管措施较为落后，人脸信息的泄露等危险是复杂的不可确定的，是新时代科技手段发展的成果，但目前监管方式尚未实现从事后转为事前的目标，往往是在造成严重后果之后才能发现。

5. 人脸识别中个人信息保护的进路

5.1. 保护个体的自由选择权，确保被有效告知

首先，要确保信息主体免于被强制。信息处理者要采取多种方式作为选择项，不能增设不合理要求或者设置不合理的门槛条件；必须履行有意义的事前告知，采取消费者能够有效获取信息的方式，在作出行动前告知；赋予信息主体犹豫的期限，在合理的时间内允许消费者思考并做出选择。

其次，在告知的具体过程中，要更为精细化。告知具体内容，包括收集主体、收集类型和数量、使用目的、留存期限等；告知替代性措施，对于信息主体给予其选择权，同时信息处理者也要充分告知人脸识别的必要性；事前直接告知消费者风险所在，以及自身所采集的保障措施，让消费者有心理准备并自主做出选择，自主承担后果；删除的告知方式[12]。对于授权存储的期限已经届满时，单独告知用户将对信息进行处理，若用户对告知没有回应则默示同意；

最后，绝大多数双方之间都是以合同关系出现，比如说游乐园、健身房的人脸识别信息，需要我们对此做出权力授予的合理判断。在健康体检或医美服务类等私密性较强类型的合同时，可约定资料除本

人持身份证可以打开，其他人无权查阅，若其未能尽到应尽义务，则可以利用违约责任追究并索取赔偿。

5.2. 拓展公益诉讼为人脸信息的救济

相比于私益诉讼，公益诉讼能很好降低当事人的诉讼成本，难点在于确定何为“社会公共利益”。公益诉讼保护人脸信息具有政策支持，最高人民检察院强调要积极稳妥地拓展公益诉讼适用案件领域，探索解决个人信息保护领域的案件，人脸识别信息是其中一部分[13]；侵犯个人信息属于民事公益诉讼，《个人信息法》有明确规定；公益诉讼制度在《民事诉讼法》以及《人民检察院公益诉讼办案规则》中有一定的完善，在管辖、起诉、上诉、执行等各个程序阶段都有较为健全的制度保障；在 2019 年至今，有关个人信息的公益诉讼案件数量正在上升，包括广州市越秀区人民检察院的首例涉及人脸信息的公益诉讼案等，这些实践案例都为个人信息采用公益诉讼奠定了基础。

目前，我国已经明确适用举证责任倒置，这有利于当事人维护自身权益。用普通侵权责任的认定方式受害者无法获得有效救济，举证责任倒置可以警告人脸信息应用方，一定程度上减少侵权行为的发生。

5.3. 强化各个主体的安全保护责任

一方面，应进一步明确责任分配原则，应该由防范风险成本最低的主体承担相应责任。用户个人技术能力有限，获取信息的能力较弱，需要付出巨大的成本，和获益并不匹配。企业拥有较强的技术能力，更好地掌控信息处理方式和信息保护技术，因此应当由企业承担更多的责任；在涉及多个主体时，可以明确各个流转环节的权利义务，根据数据流转的具体情况来确定各环节的责任主体[14]。比如说欧盟将其分为数据的控制者和数据的处理者，为二者设定相应的权利和义务，从而明确责任主体的分配比例。这两者中数据控制者仍要承担主要责任，因为其具有更高的保障能力，数据处理者则在处理的范围内承担责任，出现复杂状况时两者要承担连带责任。另一方面，相关法律法规应为人脸信息流动全过程的主体设定权利义务。采集环节数据控制者应当评估自身保障能力，同时将敏感信息放入更安全的保障系统，分开特殊保护；流动环节要定期开展自我评估，当企业违反规定导致信息不安全时，要主动承担赔偿责任，弥补用户的损失。这样有助于推动企业自我完善，采取更为有效的安全保障措施保护人脸信息。

5.4. 完善监管机构与监管措施

建立独立的信息监管机构作为核心。该机构可以通过其代表性和权力，对不同利益主体进行协调，对各类场景下出现的空间不确定性、跨区域性的个人信息保护问题进行统一管理。比如说英国的人脸识别的应用监督和咨询委员会等；监管机构应当配备专业的监管人才，可以聘用专家、顾问等方式实现监管的专业化；可以给予内部机构健全，信息保护较好的企业一定的激励，推动企业严格遵守管理规定，通过行政委托、特许经营等模式加强政府和企业之间的合作[15]。

事前审查机制的确立。人脸信息属于敏感个人信息，各国都谨慎对待。设置一个门槛和责任底线，政府对其进行最低限度的检查，建立相关的行业标准，审查企业的信息安全保障程度、内部的操作指南、企业信用等内容，考量不同场景下风险的严重程度等，在保护个人信息同时不妨碍企业创新发展；建立完善的反馈机制，通过部门之间的沟通实现动态的良性监管，运用匿名、征求意见的形式实现社会监管，适应不断变化的整体环境，多元共治。

同时，也要提高监管措施的科技化。可以建立个人信息保护检测平台，实现精准监管。该检测平台将公开观测的数据，包括实际控制者等，但无法下载数据或向第三方发送；建立人工智能风险报警机制，发现不正常的漏洞或攻击状况立即作出风险提示；引入匿名机制和去识别化机制，将个人信息隐匿在表象之下，当然不可能是完美的机制，但是各项机制相互连通，将有助于个人信息保护措施的提升。

6. 结语

随着互联网和人工智能技术的推进，我们的日常生活中充斥着各类需要人脸识别信息的技术设备，在大众的风险意识仍然处于相对较低水平下，政府和企业应该担起自身的个人信息保护责任，民众也应增强自身的保护意识。

参考文献

[1] 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.

[2] 罗斌, 李卓雄. 个人生物识别信息民事法律保护比较研究——我国“人脸识别第一案”的启示[J]. 当代传播, 2021(1): 77-81.

[3] 劳东燕. “人脸识别第一案”判决的法理分析[J]. 环球法律评论, 2022, 44(1): 146-161.

[4] 石佳友, 刘思齐. 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[J]. 财经法学, 2021(2): 60-78.

[5] 毕玉谦, 洪霄. 民事诉讼生成权利规制探析——以“人脸识别第一案”为切入点[J]. 法学杂志, 2020, 41(3): 53-62.

[6] 余建华, 钟法. “人脸识别纠纷第一案”: 个人信息司法保护的典范[N]. 人民法院报, 2022-03-08(003).

[7] 石超, 张蓓洁. 人脸识别个人信息的倾斜保护[J]. 中国科技论坛, 2022(4): 146-156.

[8] 李昭熠, 卫承霏. 智能传播环境下隐私权关系构成要素的展开[J]. 当代传播, 2022(5): 109-112.

[9] 胡安琪, 李明发. 网络平台用户协议中格式条款司法规制之实证研究[J]. 北方法学, 2019, 13(1): 53-62.

[10] 刘军平, 杨芷晴. 人脸识别数据保护困境及其法律应对[J]. 科技与法律(中英文), 2021(6): 18-28.

[11] 于洋. 论个人生物识别信息应用风险的监管构造[J]. 行政法学研究, 2021(6): 101-114.

[12] 朱佶, 宋励, 张光. 人脸识别技术滥用问题及查处对策[J]. 信息网络安全, 2021(S1): 86-89.

[13] 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.

[14] 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.

[15] 王毓莹. 人脸识别中个人信息保护的思考[J]. 法律适用, 2023, 2023(2): 15-24.