

单位代码	10476
学号	
分类号	D9

河南师范大学

硕士学位论文

(专业学位)

人脸识别技术应用中的个人信息保护问题研究

专业学位领域：法律（法学）

专业学位类别：法律硕士

申请人：

指导教师：

二〇二二年五月

RESEARCH ON PERSONAL INFORMATION
PROTECTION IN THE APPLICATION OF FACE
RECOGNITION TECHNOLOGY

A Dissertation Submitted to
the Graduate School of Henan Normal University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Law

By

Supervisor:

May, 2022

摘要

人脸识别技术是将采集的人脸与数据库现存面部信息进行比对来验证人们身份的技术。人脸识别技术具有独特性、易采集性、可识别性等特征，因而在各个领域得到广泛的应用。本文针对个人信息的概念及法律属性界定展开学术观点论述。通过分析关联说、隐私说及识别说三种学术观点得以确定我国采用“识别说”即个人信息是可识别的个人信息，并经过个人信息法律属性存在的三种学说（即隐私权学说、财产权学说及兼有人格权和财产权益两者学说）阐述说明以此得出“个人信息既有人格权性又有财产权益性”的结论。由人脸识别技术的使用及个人信息的法律属性可以看出人脸识别技术应用中的个人信息往往易面临各种法律风险：人们的人格尊严遭受侵犯、隐私权易受到损害、个人数据面临威胁、财产权益受损等。因此，人脸识别技术应用中个人信息保护已经成为法学界和司法实务界共同关注的问题。

当下，《最高人民法院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》仅对人脸识别技术以及人脸信息进行了概括和定义，着重强调形式上的告知同意和个别领域使用，缺乏具体操作的规范。即使颁布的《个人信息保护法》对“个人信息”进行了相对完整的规制，但关于人脸识别技术应用这一特殊、具体领域中个人信息如何保护的规范仍有缺失。譬如，实质上的告知同意如何实现，信息主体和信息使用者的权利义务如何界分，侵犯个人信息的损害事实及赔偿标准如何认定等，都不明确。同时，忽略了关于以政府为代表的公权力领域使用人脸识别技术进行收集、使用个人信息的行为规范。除此之外，还存在行政机关监管空白或重复、行业应用行为失范、个人法律意识淡薄等问题，都不利于人脸识别技术应用中的个人信息保护。

借鉴欧盟等域外国家的先进经验，应当在坚持已有的合法性、合理性、告知同意等原则基础上，遵循最小必要性原则、透明性原则、保护隐私原则、场景化使用原则、损害连带赔偿原则等，完善相关民事立法。通过细化非国家机关一般情况规则，落实人脸信息收集、使用、保存过程中实质上的告知同意，框定人脸识别技术使用的边界，明确人脸识别技术运用中的权利和义务，完善相关人脸信息损害认定标准和赔偿标准等具体路径，同时配之以诸如制定以事前规制为主的国家机关公权领域使用规范；设立专门行政监管机关并进行分类监管，以完善使用人脸识别技术企业的事前准入、事中审查评估、事后救济惩戒等环节；根据人脸信息的获取、使用、保存过程，企业加强自我监督管理

提高专业工作人员的工作能力和保密意识，行业自律组织制定统一行业自律规则和监督管理规范；针对人脸识别技术应用的每个阶段进行信息主体享有何种权利及事后将如何救济的普法工作等措施，为人脸识别技术应用中的个人信息保护提供良好的法治环境和社会基础。

关键词：人脸识别技术应用，个人信息，法律风险，保护

ABSTRACT

Face recognition technology is to verify people's identity by comparing the collected face with the existing facial information in the database. Face recognition technology is unique, easy to collect, recognizable and other characteristics, so it has been widely used in various fields. This paper discusses the concept of personal information and the definition of legal attributes. By analyzing the three academic viewpoints of relevance theory, privacy theory and identification theory, it is determined that China adopts "identification theory", that is, personal information is identifiable personal information. And through the existence of personal information legal attributes of the three theories (namely the theory of privacy, the theory of property rights and both the theory of personality rights and property rights) to illustrate the conclusion that "personal information has both personality rights and property rights". From the use of face recognition technology and the legal attributes of personal information can be seen that the application of face recognition technology in personal information is often vulnerable to all kinds of legal risks: people's personal dignity is violated, privacy is vulnerable to damage, personal data is threatened, property rights and interests. Therefore, the protection of personal information in the application of face recognition technology has become a common concern of law and judicial practice.

At present, the Provisions of the Supreme People's Court on several Issues concerning the application of law in the Trial of Civil cases involving the Use of face recognition Technology to process personal Information only summarize and define face recognition technology and face information, emphasizing formal consent and use in individual fields, and lacking specific operation standards. Even if the "Personal Information Protection Law" issued on the "personal information" relatively complete regulation, but on the application of face recognition technology in this special, specific field of personal information protection standards are still missing. For example, it is not clear how to realize the substantive consent, how to divide the rights and obligations of the information subject and the information user, and how to determine the damage facts and compensation standards of infringing personal information. At the same time, the government as the representative of the

public power field to use face recognition technology to collect, use personal information code of conduct. In addition, there are also blank or repeated administrative authority supervision, industry application behavior anomia, personal legal awareness and other problems, are not conducive to the application of face recognition technology in personal information protection.

Drawing lessons from the advanced experience of the EU and other countries outside the region, the relevant civil legislation should be improved by following the principles of least necessity, transparency, privacy protection, scenario-based use, and joint and several compensation for damage on the basis of adhering to the existing principles of legality, rationality and consent. By refining the general rules of non-state organs, the implementation of face information collection, use, preservation process essentially informed consent, framed the boundaries of the use of face recognition technology, clear face recognition technology in the use of rights and obligations, improve the relevant face information damage identification standards and compensation standards and other specific path, At the same time, it is necessary to formulate regulations for the use of state organs' public rights. The establishment of special administrative supervision organs and classified supervision, in order to improve the use of face recognition technology enterprises prior access, review and evaluation, afterwards relief and punishment links; According to the face information access, use, preservation process, enterprises to strengthen self-supervision and management to improve professional staff working ability and confidentiality awareness, industry self-discipline organization to develop unified industry self-discipline rules and supervision and management norms; For each stage of the application of face recognition technology, information subjects enjoy what rights and how to remedy the legal work and other measures to provide a good legal environment and social basis for the protection of personal information in the application of face recognition technology.

KEY WORDS : The application of face recognition technology, personal information, legal risk, protection

目 录

摘 要	I
ABSTRACT	III
目 录	V
绪 论	1
1.1 研究背景及意义	1
1.2 国内外研究现状	2
1.2.1 国内研究现状	2
1.2.2 国外研究现状	3
1.2.3 对国内外现状的评价	4
1.3 研究方法	5
1.3.1 案例分析法	5
1.3.2 文献分析法	5
1.3.3 比较分析法	5
1.4 本文的创新点与不足	6
第一章 人脸识别技术应用中个人信息保护概述	7
1.1 人脸识别技术概述	7
1.1.1 人脸识别技术的内涵	7
1.1.2 人脸识别技术的特点	7
1.1.3 人脸识别技术的应用	8
1.2 个人信息概述	9
1.2.1 个人信息的概念界定	9
1.2.2 个人信息的法律属性界定	9
第二章 人脸识别技术应用中个人信息面临的法律风险	11
2.1 人格尊严遭受侵犯	11
2.2 隐私易受损害	11
2.3 个人数据安全面临威胁	12

2.4 财产权益受损	13
第三章 人脸识别技术应用中个人信息保护的现状及缺陷	15
3.1 人脸识别技术应用中个人信息保护的现状	15
3.1.1 相关民事立法	15
3.1.2 行政监管现状	16
3.1.3 行业应用现状	16
3.1.4 个人意识呈现	17
3.2 人脸识别技术应用中个人信息保护的缺陷	17
3.2.1 相关法律法规内容制定单一	17
3.2.2 相关执法机构监管缺位	18
3.2.3 人脸识别技术行业应用失范	19
3.2.4 个人维权意识薄弱	19
第四章 人脸识别技术应用中个人信息保护的建议	21
4.1 完善相关民事立法	21
4.1.1 坚持相关基本原则	21
4.1.2 细化非国家机关一般情况规则	23
4.1.3 制定国家机关公权领域的使用规范	25
4.2 强化相关人脸识别技术运用的行政监管	26
4.2.1 建立专门的行政监管机关	26
4.2.2 设置行政监管机关分类管理制度	27
4.2.3 制定相关监管措施	27
4.3 建立行业自律机制	28
4.3.1 加强企业自律	28
4.3.2 制定并完善行业自律规则	29
4.4 增强个人的维权意识和能力	30
4.4.1 加强信息主体的维权意识	30
4.4.2 提升信息主体的事后救济能力	30
结 语	31
参考文献	33

绪论

1.1 研究背景及意义

2020 年杭州市基层人民法院审理的郭兵诉杭州野生动物园服务合同纠纷案被誉为中国“人脸识别技术应用中个人信息侵权纠纷的第一案”。杭州野生动物园改变原有的指纹验证入园方式，运用人脸识别技术识别顾客的面部信息进行入园。原告郭兵认为人脸信息属于敏感信息，杭州野生动物园未经顾客允许无权使用面部识别进行验证入园。其行为严重侵犯了自己的权利，动物园应当对自己的损失负责并删除已采集的信息。随后一审判决：杭州野生动物园须删除郭兵已存在的人脸信息，赔偿原告郭兵权益损失及交通费共计 1038 元。^①虽然本案被认定为是服务合同纠纷问题，但是我们可以看出该案件本质是人脸识别技术应用过程中关于个人信息方面的矛盾纠纷。差不多同一时间，美国脸书也遇到同样问题，其擅自收集和获取数百万用户人脸信息的行为遭到了集团诉讼。然而，美国法院对此作出与中国相差极大的判决。美国要求脸书不得使用人脸识别技术功能，要将已存的人脸信息清除，并赔偿伊利诺伊州用户 6.5 亿美元。

由此可见，我国对人脸识别技术应用中个人信息保护尚未得到高度重视，或是说相关个人信息保护意识仍处于萌芽阶段。甚至在我国已经进入全面发展人脸识别技术的时期，个人信息仍然没有得到最大限度的保护。例如：刷脸支付、考勤打卡、疫情刷脸查询行程、校园门禁等。其带给人们方便和利益的同时也催生了许多问题，如现阶段关于人脸识别技术的应用，没有详细、具体的法律依据进行明确限制或是个人信息权益受到侵害后无法得到有效救济。

故文章立足于人脸识别技术发展的大背景，思考个人信息的法律属性和相关的法律风险，探究人脸识别技术应用中个人信息保护的现状及缺陷，多角度、全方位地提出关于人脸识别技术应用中如何保护个人信息的合理建议，真正实现保护个人信息权益的目的。

^① 案件源自中国裁判文书网（2019）浙 0111 民初 6971 号判决书

1.2 国内外研究现状

1.2.1 国内研究现状

近几年来,相关人脸识别技术应用案例的频出导致关于人脸识别技术应用的讨论和研究开始丰富起来。我国主要从以下几个方面展开关于人脸识别技术应用中个人信息保护研究。

① 个人信息概念界定

关于个人信息概念的界定,我国学术界主要分为三种学说。第一种是关联说,该说法认为人们的全部信息都视为个人信息。第二种是隐私说。其提出个人信息是不为多数人所熟知并不愿意对外公开的信息。第三种是识别说。该学说认为个人信息是能够直接或间接方式将信息主体辨认出来的信息。

② 个人信息的法律属性界定

关于个人信息的法律属性界定,主要围绕着个人信息属于人格权还是财产权的争论。第一种,将个人信息纳入隐私权的人格权学说。学者王俊秀指出在传统隐私范围内为个人信息提供保护。^①第二种为财产权学说。刘德良教授直接将个人信息归属于财产权。他认为个人信息可以视为商品进行交换,信息主体可以以个人信息受到侵害为由主张经济赔偿来保障自身合法权益。^②第三种为兼顾人格权及财产权益两种属性的学说。王利明教授指出个人信息权是一种独立的具体人格权。该权利的主体是特定的,不能为他人所用。同时,该权利还具有财产属性。^③杨立新认为个人信息是具体人格权并且在个人信息受到侵害时信息主体具有人格请求权和侵权责任请求权。^④

③ 人脸识别技术应用的法律风险

只要利用人脸识别技术收集人们面部信息不加以合理限制,就可能导致其他个人信息被过度收集、获取。比如,姓名、年龄、兴趣爱好等。因此,不法者借此方法将人们个人信息用于其他地方来谋取利益,对人们的生活产生极大影响,在某种程度上会造成人们权益的损害。故在人脸识别技术应用中个人信息所面临的法律风险有以下几方面:第一是人格尊严。学者周行从人脸的社会文化、面部信息获取须知情同意以及政府对公

^① 王俊秀. 数字社会中的隐私重塑——以“人脸识别”为例[J]. 探索与争鸣, 2020(02): 86-90.

^② 刘德良. 《个人信息的财产权保护》[J]. 法学研究, 2017(03): 82.

^③ 王利明. 论个人信息权在人格权法中的地位[J]. 苏州大学学报(哲学社会科学版), 2012(06): 68-75+199-200.

^④ 杨立新. 个人信息: 法益抑或民事权利——对《民法总则》第111条规定的“个人信息”之解读[J]. 法学论坛, 2018(01): 34-35.

民生活管控三方面出发阐述了使用人脸识别技术对人格尊严究竟会产生什么样影响。^①第二是隐私权。学者陈荣新提出人脸识别信息与其他敏感个人信息有着密切联系。在进行收集获取人脸信息过程中可能会出现其他敏感个人信息的泄露、滥用，加大隐私受到侵犯的可能性。^②第三是财产权益。正如前面王利明教授与杨立新教授所言，会对个人信息财产权益产生侵害。

④ 人脸识别技术应用中个人信息保护的规制

我国关于人脸识别技术应用中个人信息保护的规制建议主要从以下两种角度展开。一方面是从法律原则出发，杨建军提出需要坚持必要性和保护隐私原则。^③另一方面从健全法律机制出发。学者周坤琳指出该技术使用过程中存在许多弊端，需要从立法、执法、司法等方面入手进行完善。^④学者孙楠依据人脸识别技术获取、保存、使用、救济等流程来逐步提出改善相关立法机制的建议。^⑤学者邢会强强调根据公私域应用不同来加强该技术应用过程中个人信息保护的力度。^⑥

1.2.2 国外研究现状

由于人脸识别技术发展时间和速度的差异，导致欧美国家与我国在关于人脸识别技术应用及个人信息保护的规制有较多区别。通过查阅相关国外文献，总结归纳欧美等国家的研究主要集中在以下几方面：

① 关于人脸识别技术应用的场景

学者Lander Karen认为公民自由等权利会因人脸识别技术的滥用受到侵犯。所以，他认为使用人脸识别技术应该依据场景的不同来进行标准划分，譬如，若涉及到社会公共利益方面，要以维护大众的基本权利为标准进行人脸识别技术的使用，并且不能越过此标准。

② 关于个人信息法律属性的界定

国外关于个人信息法律属性的界定主要分为两种观点，但这两种观点的本质都偏向将个人信息作为人格权进行保护。一种是以美国为代表的英美法系国家。他们主要将个人信息保护集中于隐私权。如颁布的《华盛顿隐私法案》对执法机关和企业如何使用人

^① 周行. 人脸信息立法保护的规范体系建构[J]. 中南民族大学学报, 2021(08): 129-135.

^② 陈荣新. 比较法视野下人脸识别信息保护的法律模式研究[J]. 国际经济法学刊, 2021(04): 10-23.

^③ 杨建军, 李童心. 人脸识别技术运用的法律原则[J]. 南宁师范大学学报, 2020(05): 37-47.

^④ 周坤琳, 李悦. 回应型理论下人脸数据运用法律规制研究[J]. 西南金融, 2019(12): 78-87.

^⑤ 孙楠. 人脸识别技术应用的法律规制研究[D]. 吉林大学, 2020.

^⑥ 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(05): 51-63.

脸技术进行限定。联邦参议院《商业面部识别隐私法案》也指出利用人脸识别技术的企业须经用户同意才能采集或使用用户的人脸信息。^①另一种是以德国为代表的大陆法系国家。他们认为个人信息和人格权的实质是一样的，都是通过保护自然人的人格尊严和人格利益来保证个人信息的安全。

③ 关于人脸识别技术应用中个人信息保护的立法模式

针对各州不同情况美国为保护人们个人信息进行分别立法。例如，伊利诺伊州《生物信息隐私法案》对“生物信息”进行准确定位，法律条文明确说明了个人信息包括面部信息。佛罗里达州《生物识别信息隐私法案》提出企业只有征得信息主体的同意才可以使用人脸识别信息。而欧盟则采取与之相反的统一立法模式。其颁布的《通用数据保护条例》强调“能辨认”的个人信息，要依据“禁止处理”“法定必需”“明示同意”原则进行相关信息的获取、使用。其中，信息主体同意是进行人脸识别技术的唯一标准。

②

1.2.3 对国内外现状的评价

结合国内外研究现状，可以了解到人脸识别技术应用中个人信息保护问题已有一定的研究基础，特别是关于人脸识别技术、个人信息、人脸识别技术应用中个人信息保护的合理规制等方面研究较为丰富。这些为本文研究人脸识别技术应用中个人信息保护问题奠定了坚实的理论基础。但是，关于人脸识别技术应用中个人信息保护仍有许多问题，还需进一步的探讨和研究。

第一，如今《民法典》《个人信息保护法》的出台已对“个人信息的识别说”有了相对明确的倾向性，其将个人信息分为一般个人信息和敏感个人信息且指出人脸信息属于敏感个人信息。但多数学者的研究仍聚焦于个人信息概念界定，对出台的《民法典》《个人信息保护法》关注还是较少。

第二，在对个人信息法律属性界定相关文献进行研究时，发现大多学者仅对个人信息的法律属性进行探讨，未从人脸识别技术应用与个人信息的法律属性具有关联性角度出发去探究在人脸识别技术应用过程中个人信息所面临的风险及在人脸识别技术应用中保护个人信息的必要性。

第三，在分析风险及成因时大多归结于法制的不完善，着重强调关于立法方面的构

^① 闫晓丽. 美国对人脸识别技术的法律规制及启示[J]. 信息安全与通信保密, 2020(11).

^② 刘晓春. 欧盟《通用数据保护条例》原则条款解析[N]. 中国市场监管报, 2019-04-16(006).

建,对于行政监管、行业自律及个人方面的关注度不高。相关学者研究虽有涉及行政监管行业自律等方面的探讨,但相较过少。并且,关于信息主体个人权利意识方面的研究也鲜有提及。众多学者大都按照以法律原则为基础和全方面构建法制机制两种角度单独展开讨论,没有将二者放在一起相互融合研究,导致提出的个人信息保护规制过于单一、缺乏全面性。同时,《最高人民法院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》(下文简称为《人脸识别技术规定》)和《个人信息保护法》的出台已经解决一些学者研究的问题也采纳了一些学者的有效建议,特别是关于法律原则方面的。而学者的研究与构想则大多还停留在《个人信息保护法》、《人脸识别技术规定》未颁布前,未能从新的研究角度或方向出发提出适合的建议措施。《人脸识别技术规定》《个人信息保护法》出台后仍有许多问题亟待解决,尤其是关于法律规制方面。

因此,在原有研究基础上,本文从个人信息的法律属性出发探寻人脸识别技术应用过程中个人信息所面临的风险,多角度分析我国关于个人信息保护现状及问题,进而提出具有针对性的建议,共同打造一个全面完备的人脸识别技术应用中个人信息保护机制,提高人脸识别技术使用过程中个人信息保护力,促进社会健康有序发展。

1.3 研究方法

1.3.1 案例分析法

本文不仅对人脸识别技术应用中个人信息保护问题进行理论研究,还针对人脸识别技术的特性结合国内杭州动物园人脸识别案件的分析,间接引出本文研究对象及研究目的。

1.3.2 文献分析法

利用互联网、图书馆及相关平台来获取关于人脸识别技术与个人信息保护的国内外文献资料,具体包括国内外的立法条文、学术研究、相关司法判例。在此基础上,进行细致研究分析,找出我国目前在使用人脸识别技术中个人信息保护仍存在的问题,进而提出适合我国个人信息保护发展的优质方案。

1.3.3 比较分析法

个人信息已有明确立法,但关于人脸识别技术应用中个人信息的保护立法并不完

善。经过国内外相关学者研究、相关立法和人脸识别技术应用中对个人信息侵权等实践的对比分析，结合我国现状，提出人脸识别技术应用过程中关于个人信息保护的可行性建议。

1.4 本文的创新点与不足

本文立足于实务，以理论为支撑，从人脸识别技术应用与个人信息法律属性出发，通过对《民法典》《个人信息保护法》、《人脸识别技术规定》立法内容的解读及对执法等多方面现状的分析，总结归纳关于人脸识别技术应用中个人信息保护存在的问题，提出“法律原则+法律机制”二合一保护模式，即以相关法律原则为基础同时也从立法完善、行政监督、行业自律、个人意识四个方面对人脸识别技术应用中个人信息保护进行全方位的合理规制。

本文的不足是：目前，关于人脸识别信息保护究竟是涉及人格权还是财产权的争论，学界尚无定论。并且笔者知识储备不够，分析研究能力还需不断加强。因此，本文对人脸识别技术应用中个人信息法律属性的分析和探讨较为浅显，还不够全面，今后的学习中还需不断努力充实自己。

第一章 人脸识别技术应用中个人信息保护概述

伴随着人脸识别技术不断升级提高,人们的个人信息被泄露、滥用事例也不断增多,人们由此产生的各种矛盾也不断激化。因此,需要给予个人信息更多关注,加大对个人信息保护的重视。那么,在探究人脸识别技术应用中个人信息保护问题之前,需要人脸识别技术和个人信息的概念、法律属性等相关内容进行明晰。

1.1 人脸识别技术概述

1.1.1 人脸识别技术的内涵

2019 年发布的《互联网技术司法应用白皮书》对人脸识别技术进行了阐述。人脸识别技术是以照片或影像为媒介获取收集面部信息数据,再利用已有的面部数据库进行对比分析,来进行身份认证的技术。目前应用最广泛的人脸识别技术系统由三部分组成。第一步是进行人脸的面部信息采集,主要使用相机等录像电子设备对面部拍照、扫描。第二步是对获取的人脸照片视频等进行研究。该系统利用算法、算力等高科技手段对获取的人脸信息进行细致剖析,进而得到人脸信息的主要特征。第三步是进行比较。其将具有主要特征的面部信息和已存入数据库的面部信息数据进行比照,由此来验证人们的身份。其实可以看出人脸识别技术应用中的面部信息与其他个人信息是相链接的,存在牵一发而动全身的关系。

1.1.2 人脸识别技术的特点

通过前面对人脸识别技术内涵的介绍,可以发现人脸识别技术具有以下几种特征:

第一,人脸识别技术运用的独特性。人脸是独一无二的,每个人都不一样。人脸信息是具有识别、区分信息主体特殊性能的个人信息。与其他类型的个人信息相比,面部信息的敏感性更强,对收集、使用、存储等的安全性要求更高。又因为人脸识别技术的运用就是人脸信息获取、使用和保存,那么一旦面部信息被泄露、盗用就意味着人脸识别技术应用过程出现问题。也就是说,人脸信息所具有的独特性也赋予了人脸识别技术运用的独特性。

第二,利用人脸识别技术获取的人脸信息具有易采集性。面部信息是一种一直暴露

在外界环境下的个人信息，无法进行隐藏或躲避。在日常生活中，人脸的易采集性为随时随地使用人脸识别技术创造了条件。当需要时，人们只须在摄影设备前方短暂停顿就可以完成信息采集。随之，开始上传、匹配的识别工作。从某种程度上来说，人脸识别技术完全不需要人工协助操作和被采集人的自愿配合。正是因为这种特性，导致获取人脸信息的同时也能为取得其他个人信息提供最便捷的途径。这种情况相当于将每个人脱光衣服放在大众视野之中，毫无私密性可言。美国的脸书就是最典型的案例。脸书通过用户的照片进行标记、获取其个人资料，将脸书平台形成一个融合通道，以此互相分享用户个人信息。

第三，人脸识别技术具有可破解性。虽然人脸识别技术已经进入飞速发展的阶段，但是对人脸识别技术使用的安全性，人们并没有给予高度的重视。近年来，关于人脸识别技术被破解的案例频发。例如，在取快递时只需拿着一张照片就可以打开快递箱，在他人不注意时扫描他人面部信息即可获取其他个人信息、财产账户进而骗取钱财。这些违法行为都在证明人脸识别技术本身存在技术弊端即可破解性。倘若发生人脸识别技术被攻击的情况，如何保障面部信息安全、如何解决由此产生的个人信息数据安全问题、财产安全问题以及后期救济工作如何进行都将成为我们值得思考和研究的问题。

第四，人脸识别技术的使用后果具有不可更改性。由于面部信息具有独特性，他人可以通过面部信息准确识别出信息主体、个人偏好等私密信息，可能会导致获取的面部信息出现泄露或不正当使用，与其关联的个人信息也会受到一定程度上的侵害并且无法进行更改，也就是说无法恢复到未使用人脸识别技术之前的原始状态。即使事后能够进行弥补，也只能在最小程度上降低损失。

1.1.3 人脸识别技术的应用

根据应用主体的不同，可以将人脸识别技术的应用分为以公共服务为目的的国家政府公权力领域和以商业为目的的金融、医疗等私人领域。

现如今的人脸识别技术在公权力机构中占据着重要位置，尤其是在公共安全和公共管理方面。我们可以看到国家政府等公权力机构经常将人脸识别技术应用到城市规划建设、治安防控、抓捕犯人、执法监督等方面。以追捕犯人为例，国内著名的北大弑母案凶手吴谢宇最终能被抓获，就是得益于利用人脸识别技术将多次被监控设备抓拍到的照片和数据库中吴谢宇资料进行分析、对比、识别。

随着人脸识别技术的普及,在其他社会领域中的应用也给人们的生活带来了巨大的改变。医疗、科技、金融等领域就成为人脸识别技术应用的主力军。就拿金融行业来说,在办理开户或银行卡业务时,人脸识别技术能够通过面部信息快速获取客户个人的相关身份信息,极大程度上提升了银行的工作效率,缓解了银行内部的运转压力,促进了防控安全目标的快速实现。银行 app 紧跟人脸识别技术的发展,开通了刷脸支付的功能。在 APP 采集完个人面部信息后就可以进行线上线下免密支付,使得人们的生活变得更加便捷、快节奏化。

1.2 个人信息概述

1.2.1 个人信息的概念界定

明晰个人信息的概念是探究人脸识别技术应用中个人信息保护问题的基础。关于个人信息概念界定,理论界有三种不同的声音。第一种,关联说指出人们的一切信息都属于个人信息。这种说法将个人信息的概念夸大化,看似表面上对人们的个人信息保护范围比较全面,但在实际操作中无法进行真正地落实。第二种,隐私说将个人信息与隐私权挂钩,提出个人信息是他人不知且不愿意让他人所熟知的信息。其将个人信息的范围缩小至敏感个人信息之中,着重强调个人信息的使用与隐私权易受侵害的关系,在一定程度上忽视了其他权益遭受损害的可能性。第三种,识别说是目前学界及大多数国家广泛认可和使用的学说。其提出个人信息是不管以直接方式还是间接方式均能够进行识别和辨认的信息。该学说不仅能够体现出个人信息的本质即可识别性,而且适用于当下人脸识别技术的应用。

目前,我国《民法典》《个人信息保护法》均采用“识别说”对个人信息作出了概念界定。其中《个人信息保护法》第 4 条明确指出个人信息是已识别或可识别的自然人有关的各种信息。同时,第 28 条也将生物识别信息纳入敏感个人信息之中。由此可见,可识别是个人信息的关键,也是人脸识别技术应用中个人信息的关键。

1.2.2 个人信息的法律属性界定

目前,我国关于人脸识别技术应用中个人信息的法律属性学界主要存在三种分歧。一种是将个人信息归入隐私权的人格权学说。该学说认为若个人信息遭到泄露、错用、非法利用就会给人们的隐私权带来损害。这种说法虽然有一定道理,但这些年来人脸识

别技术的迅速普及与发展,导致利用人脸识别技术对人们个人信息进行非法利用、泄露等行为时不仅仅会对人们的隐私权造成侵害,还会对其他权利产生一定威胁。因此,单纯地从隐私权对个人信息进行保护的理論早已过时。一种是财产权说。在视为具有财产权性质的个人信息受到侵害时人们可以将自己的个人信息作为商品来衡量物质上经济赔偿价值。这一学说具有较大局限性,仅将个人信息框定在财产权这一个小小的权利之中,不足以将个人信息法律属性完整体现,会造成与将个人信息归为《民法典》人格编的立法矛盾,完全无视了个人信息的人格权属性。最后一种是兼顾人格权与财产权益两种属性的学说。一方面,《民法典》人格权编以及《个人信息保护法》都已经对个人信息具有人格权属性的说法加以肯定。在处理个人信息时,其都与人们的各种人格权有着密不可分的关联。另一方面,如人脸识别技术广泛应用在金融等商业领域,会使个人信息在进行获取、使用、输送过程中具有一定的财产性。在利用人脸识别技术对个人信息非法获取、泄露、滥用的同时,就会使人们财产权益受损。那么,就可以依据个人信息具有财产性进行财产损害赔偿。

本文通过关于个人信息的法律属性界定分析,可知“个人信息既有人格权属性又有财产性属性”的学说最具有合理性。故笔者围绕个人信息既有人格权属性又有财产性属性展开关于人脸识别技术应用中个人信息保护将面临怎样风险等问题研究。

第二章 人脸识别技术应用中个人信息面临的法律风险

经过人脸识别技术的使用、整合和对比，个人信息的获取量和准确度显著提升，那么可能会产生个人信息泄露、非法使用等情况，导致人们人格权遭受侵犯进而引出人们隐私权易受损害，同时也会使人们的个人数据安全面临威胁，与之相关的财产权益受到侵害。所以，我们在人脸识别技术应用过程中理应加大对个人信息的保护力度。

2.1 人格尊严遭受侵犯

人格尊严是公民作为平等的人最基本的保证，是受到国家尊重和保护的一项公民人格权利，是人们价值中最重要的一项。我国《宪法》与《民法典》都对此进行了规定，体现了对人格尊严的认可和重视。人脸是一个人最直观的表现，是人与人之间进行区分的关键，也是人与人交往最直接的名片，并且人脸也是个人情绪表达和人格的展现，我们可以通过人脸获取对每个人的第一印象，进而产生是否要了解和认识该人的想法。因此，人脸与人格尊严有着千丝万缕的联系。

人脸识别技术主要是通过面部拍摄的资料与数据库中信息进行对比识别的。人脸成为人脸识别技术应用的主要媒介。现如今我们无形之中就会处于各种各样的拍摄环境，面部信息利用识别的门槛也因此降低，导致人们滥用、错用人脸识别技术的频率提高，也会使人脸识别技术应用中个人信息被侵害后的不可逆性尤为凸显。再加上人脸本身所具有的独特性和可破解性，在经过信息主体允许或知道同意的情况下，就会产生种种人脸信息被随便收集、获取并进行使用的非法行为。这样会使信息主体的人格尊严受到挑战，同时也将人脸信息背后所赋予的尊严转变为一组组没有生气的数据，远远背离了使用人脸识别技术的初衷，也会使人们丧失独立人格。就像前一段央视曝出大量人脸照片被兜售的案例。不法分子就是利用特殊的软件将识别的人脸制作成一段视频来形成相同的人脸识别图像以此来进行匹配和认证。这对信息主体的人格尊严极其不尊重，也严重侵犯了人们的人格权。

2.2 隐私易受损害

我们通过威斯汀“信息隐私权理论”的司法实践，得到了关于信息隐私权的完整阐释。信息隐私权的关键在于控制和决定，即公民有权自己决定他人是否能获取、识别和

使用个人信息。^①《民法典》的颁布赋予了隐私权民法意义上的定义。隐私权是在没有经过自然人允许的情况下拥有不能让他获取或知道信息、空间或活动的权利。由此可见,是否侵犯隐私的重点在于人们对于获取个人信息的行为是否知情和同意。并且隐私权是人格权编的一部分,个人信息具有人格权的法律属性。所以,人脸识别技术应用中个人信息也具有隐私权的法律属性。

虽然单单一张人脸并不能称之为隐私,但人脸识别技术是通过识别人脸进而获取面部信息等数据分析得出人们性别、年龄、健康状况等众多个人信息。这些个人信息是属于人们的隐私范畴。并且面部信息本身就属于个人信息的一种,可以用来进行身份验证,了解人们的文化水平、工作等相对隐私的个人信息。再加上其独特的易采集性,无须过多接触甚至不需接触就可以完成面部信息的采集和获取。这就意味着在平时日常生活中极易发生未经本人同意就被擅自获取面部信息的情况,而且信息主体还不能轻易或直观发现自己面部信息已被获取、被采集的事实,也会引起其他相关个人信息的泄露和被过度剖析。同时,人们的知情同意权也不可避免的遭到了忽视。所以,在未得到信息主体允许的前提下,信息使用者依靠人脸识别技术所特有的技术优势过度采集、分析和披露人们的个人信息,会导致信息主体的个人信息无法真正得到保护,也会给人们的隐私安全带来不可估量的侵害后果。譬如,平时生活中进出一些场所必须进行面部识别,下载手机上 APP 注册账号也需人脸识别,甚至进出自己家小区也要人脸识别。就拿近期江苏苏州张先生所在小区来说,张先生小区物业不经业主同意将人脸识别系统作为进出小区的唯一途径,要求业主办理面部信息录入,不然无法进入小区。这充分体现了经常出现未经信息主体同意过度滥用和非法使用人脸信息包括面部信息在内所有个人信息的情况,就导致面临隐私泄露的法律风险增大。

2.3 个人数据安全面临威胁

众所周知,产品需要时常进行更新换代,人脸识别技术也是如此。目前,我国人脸识别技术行业的发展还不够成熟,大多数使用人脸识别技术的企业之间存在多方面差距。如关于人脸识别技术的熟练程度和渗透度存在差异,关于个人信息数据安全认知参差不齐,关于个人信息数据保管能力良莠不齐。先进人脸识别技术的使用需要大量时间和金钱成本,而一些中小企业由于自身原因极少会选择升级提高人脸识别技术,那么就

^① 张民安. 信息性隐私权研究[M]. 广州: 中山大学出版社, 2014.

会造成人脸识别技术落后，给不法者破解人脸识别系统获取个人信息提供了可趁之机。人脸识别技术一旦遭到破解，就会导致人脸信息泄露、滥用并且被泄露的信息主体处于弱势地位，信息主体的个人信息数据也无法保证其安全性，会带来不可预知的风险。

从技术方面看，人脸识别技术是采取分析对比的计算机技术进行面部识别，并且可以长距离不分时间地点获取个人信息。这就意味着人脸识别技术可以不受控制，不需信息主体的同意进行自动信息识别，导致信息主体与信息使用者之间信息不对称，会激化信息主体与信息利用者之间的矛盾。同时，以谋取商业价值为目的信息使用者肯定会过于关注对人脸识别信息的利用和分析，忽视信息主体的感受，极易产生人脸识别技术滥用、错用、非法使用的情况，导致信息主体的个人信息数据安全性降低。消费时刷脸支付，其利用人脸识别技术获取消费者面部信息去分析识别具体个人信息（包括支付时间、金额、商品信息、消费者年龄、消费者购物偏好）。商家可以充分依据这些信息，制定对准不同年龄段的针对性营销策略。但其为商业用户更好制定针对性服务提供个人信息数据时，却大大忽略了消费者群体的个人信息数据安全问题。况且，现在深处于大数据时代，人脸识别技术使用过程中个人数据安全就显得更加突出。譬如，很多网络公司使用人脸识别功能对用户身份进行解析时，都会存在或多或少的隐患。再加上金融本身的不稳定性，进一步加剧了个人数据泄露的风险。

2.4 财产权益受损

人脸识别技术虽在我国已得到广泛的应用，但在使用过程中，面部信息的泄露易造成人们人格利益受损。人脸识别信息的泄露、滥用表面看似侵犯了肖像权，实则侵害了个人信息的财产性。由前面个人信息的法律属性分析可知，个人信息既有人格权属性又有财产权益属性。那么，人脸识别技术应用中的个人信息也具有这两种属性。并且，人脸信息等个人信息是与自然人的财产安全有关的信息数据。所以，当人脸识别技术和经济紧密接触时，财产权益是否会受到损害这一问题就显得尤为重要。若将在金融领域，企业通过该技术获得并提取面部信息，可以深度分析整合特定人的其他相关个人信息进而获取其个人资金账户的详细信息。就等于金融企业不经用户同意情况下就有可能擅自了解到用户是否开通银行账号或已办理哪些资金业务。那么，一旦非法采集或泄露，就会导致用户个人资金账户等相关信息的暴露，甚至也会由此产生财产失踪的潜在危险。前一段广州互联网法院通报一起因被刷脸引发王女士背上万余元贷款的纠纷就是活生

生的例子。不法分子冒用王女士身份，用拾取的王女士身份证为自己开通借记卡账户并以人脸识别核验身份的方式开通手机银行贷款功能。正是因为人脸自身无法避免的特性及人脸识别技术的不断优化，导致利用人脸识别技术获取个人信息的能力越来越强，金融领域个人信息数据被他人窃取冒用、财产权益易受侵害的法律风险越变越高，互联网金融交易安全也会受到威胁，使金融消费者长期处于一个不安全的交易环境。

根据个人信息既有人格权又有财产权益的法律属性及人脸识别技术对个人信息侵害方式分析可知在人脸识别技术应用过程中个人信息会面临着人格权、隐私权、个人数据安全、财产权益等法律风险。因此，对人脸识别技术应用中个人信息进行保护是有必要的。

第三章 人脸识别技术应用中个人信息保护的现状及缺陷

3.1 人脸识别技术应用中个人信息保护的现状

3.1.1 相关民事立法

①《民法典》关于个人信息保护的立法规定

《民法典》不仅新增设了人格权编这一编，还将个人信息和隐私权纳入了人格权编的内容。其中，《民法典》在明确自然人个人信息概念和范围的同时，还指出生物识别信息属于个人信息的一部分并给予个人信息保护充分的肯定。除此之外，《民法典》将个人信息与隐私权两者结合，规范了处理个人信息的基本原则，赋予了信息主体享有知情同意权、删除权、隐私权。譬如，信息使用者在处理个人信息时理应遵循合法性原则、合理性原则。在处理个人信息前，信息使用者须征得信息主体的同意才能对个人信息进行获取。又因为信息使用者处理个人信息是通过获取、收集、使用、保存等多个复杂程序进行的，不是一个简单行为能够完全解决的。故《民法典》规定信息主体可以对处理个人信息过程中信息使用者的各种行为行使删除权等权利。虽然《民法典》有所提及敏感个人信息，但仅仅是对一些如健康信息敏感个人信息的列举，并没有对敏感个人信息（包括人脸识别信息在内）的概念、处理等进行划分说明。

②《个人信息保护法》

《个人信息保护法》在《民法典》基础上对个人信息处理规则、分类及个人信息保护范围等具体内容进行了更加细致的规定。并且对个人敏感信息的获取、利用、保存作出更高要求。《个人信息保护法》主要集中在以下几方面：第一，强调了信息主体的知情同意权并对信息使用者遵循告知同意原则的方式进行了更具有实操性的规范。例如，信息使用者须用清楚易懂的语言或方式将个人信息的获取、使用等情况告知信息主体。信息主体关于信息使用者处理个人信息行为的同意要以自己充分知情并出于自愿为前提。第二，在《民法典》规定信息主体享有知情同意权、删除权的基础上对信息主体享有权利和信息使用者的义务进行更加详细的规范。譬如，对于各种app强制同意的条款，除获取信息主体个人信息的必要性外信息使用者不得擅自处理未经信息主体明确自愿同意的相关个人信息。第三，针对敏感个人信息问题进行专门探讨。如第28条提出敏

感个人信息的泄露或非法使用会导致人格尊严、人身财产安全受到侵害。第 31 条将未成年人的个人信息归为敏感个人信息并强调了在处理未成年人个人信息时须经其父母或其他监护人的同意。虽然《个人信息法》相对于《民法典》对敏感个人信息的着墨较多，但关于人脸识别技术应用中个人信息的保护问题仍未进行过多叙述和制约。

③《最高人民法院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》

在借鉴《民法典》《个人信息保护法》的基础上，我国发布了关于人脸识别技术应用中个人信息保护专门规定，即《人脸识别技术规定》。该规定针对民事领域中使用人脸识别技术处理个人信息进行了概括性说明。如第 1 条解释并使用了人脸信息这一概念。其将使用人脸识别技术处理个人信息的行为看作为处理人脸信息的行为，并且将人脸信息处理囊括为人脸信息的获取、保存、使用、加工等。同时，还从人格权、侵权责任、合同等具体角度对人脸识别技术应用中的个人信息保护进行规定。如第 2 条至第 9 条针对几种滥用人脸识别技术导致个人信息受到侵害的典型行为进行分析和性质认定。第 10 条至第 12 条从合同角度针对几种个人信息受到侵害的典型行为进行责任归属的制定。针对人脸识别技术的使用我国虽已经进行专门规制，但仅将焦点聚集在几种典型行为并没有将问题落到实处进行解决与探究。

3.1.2 行政监管现状

2019 年工信部对换脸软件“ZAO”进行约谈并要求该软件对涉及人脸信息方面的问题进行整改。2021 年针对上海市徐汇区检察院调查出关于八家企业长期非法收集消费者人脸识别信息的事实，相关行政机关对这八家企业进行了严厉的行政处罚，并扩大了对商业圈等使用人脸识别技术企业获取消费者人脸信息的监管力度和巡查力度。由这两个例子可以看出，相关行政机关对于人脸识别技术应用中个人信息保护方面还存在许多问题。

3.1.3 行业应用现状

我国人脸识别技术市场规模一直处于扩大阶段，并且广泛应用于多种多样的企业。如以腾讯、百度为代表的互联网企业方面，他们将人脸识别技术与自己 APP 绑定。在进行 APP 登录或下载时，可能会出现强制或是暗性要求人们同意人脸信息的获取。在安保方面，商场、超市利用人脸识别技术检查人们的进出。在金融方面，相关金融企业根据

获取的个人信息来判断人们的资产水平。在医疗方面，利用人脸识别技术研究遗传病史和遗传疾病的分布人群，医院通过使用人脸识别技术录入病人面部信息获取病人以往病史进而简化就医步骤。甚至在人们的日常生活学习和工作中，也充斥着人脸识别技术应用的身影。学校运用人脸识别技术收集学生的面部信息和调取学生个人信息用于学生进出管理，企业的员工们利用面部识别与系统存放的个人信息对比识别进行考勤打卡、小区物业购置人脸识别器材作为小区门禁。

3.1.4 个人意识呈现

对于人脸识别技术在人们生活中的广泛应用，人们大都选择坦然接受该技术带来的便捷。如，刷脸支付、刷脸考勤、刷脸接水等。但对于一些不必要采取人脸识别技术收集个人信息依旧强制使用人脸识别技术的情况，如小区刷脸门禁、商超刷脸识别进入、酒店人脸识别进行登记入住。虽有人对此颇有怨言，但大多数人还是选择了沉默或被迫接受。

3.2 人脸识别技术应用中个人信息保护的缺陷

3.2.1 相关法律法规内容制定单一

由前面相关立法可以看出《民法典》《个人信息保护法》《人脸识别技术规定》已经从多方面对个人信息保护作出了细致的规定，并且也将人脸信息纳入个人信息范畴。但又因人脸识别技术不同于其他传统个人信息收集处理技术，基于其专属的独特性，目前出台的法律法规并不足以解决人脸识别技术应用中个人信息保护实际存在的问题。这些法律法规主要包括以下几方面问题：一是仅将关于个人信息保护的一般法律原则照搬到关于人脸识别技术处理个人信息的规定中，并未从人脸识别技术自身的特性分析，添加具有人脸识别技术特性的法律原则。二是告知同意、单独同意仅从形式上规范并未提及实质上怎样落实的具体操作。三是对于人脸识别技术的使用范围、方式、场所没有一个明确的标准和划分，仅对几个特定场所如火车站、商场进行阐述说明。过于笼统的规定并不能真正做到对个人信息保护。四是关于人脸识别技术运用中信息主体和信息使用的权利义务并无详细阐述和规定。在人脸信息收集、利用和保存过程中，会发生许多信息主体与信息使用者之间利益碰撞。但该规定依旧按照《个人信息保护法》适用所有领域的信息主体与信息使用者权利义务来实行。五是没有明确的损害认定和赔偿标准。

单靠《民法典》中关于侵权责任规定进行个人信息的处理,远不能达到在人脸识别技术应用过程中个人信息事后救济的要求。

此外,《民法典》《个人信息保护法》《人脸识别技术规定》多侧重于非国家机关的规范,对以政府为代表的国家机关提及甚少,未能形成强劲的约束力。在公共安全和公共管理方面,政府等公权力机关可以使用人脸识别技术强制性获取、使用人脸信息及其他个人信息以此来达到保护国家和公共安全的目的。但也存在着许多不需要公权力机关强制使用人脸识别技术进行过度获取、分析、使用个人信息的地方,而相关国家机关仍旧强行使用人脸识别技术,侵害信息主体的个人信息。这样给人感觉政府等公权力机关都可以在任何地方随意使用该技术。可见,以政府为代表的国家机关使用人脸识别技术必须要有一个明确的标准划分。若没有一个合法、统一的标准或参照,会使相关国家机关在利用该技术获取个人信息时具有较强的主观能动性。毕竟人与人之间主观认知方面也会存在差异,导致使用人脸识别技术进行个人信息获取的标准或参照不一,容易加大以政府为代表的相关国家机关工作进展难度。同时,也会使相关国家机关和非国家机关使用该技术的权限不对等,也激化了公权力机关与信息主体、信息使用者之间关于个人信息保护的矛盾。比如说,《人脸识别技术规定》中的单独同意规则仅适用于自然人同意处理面部信息的情形。关于公权机关的使用是否需要征得个人同意并没有过多要求。

总而言之,我国相关民事立法存在三方面问题:一是未针对人脸别技术特殊领域进行专属性法律原则规定。二是关于人脸识别技术应用中个人信息的一般性规定多为原则性规范和特定领域的细化规定,缺少非国家机关一般规则的制定。三是未对以政府为代表的公权机关进行约束和规定,会产生一些相关国家机关与非国家机关之间使用不对等问题。

3.2.2 相关执法机构监管缺位

由于人脸识别技术自身的独特性和运用过程中可能产生种种问题,除了专门的法律的规范,还需要多个行政部门与之协助进行监管和治理。行政机关能否依法合理地行使自己的职权,履行自己的职责,是保障人脸识别技术使用中个人信息法律风险最小化、效益最大化的关键。

目前,我国没有一个专门统一的行政监管机构。如果信息使用者使用人脸识别技术不当,那么无法确定应当由哪个行政部门进行监督和治理。即便确定了某个行政机关对

此进行管理,也会出现各种监管过松或过严、监管重复的情况,不能真正做到适度监管。再加上立法中未对相关行政机关行使人脸识别技术方面的职权进行具体规定,就会导致出现因使用人脸识别技术造成人脸信息或是其他信息泄露、滥用时,多个行政机关可能采取不作为或推脱的方式以逃避职权的行使,造成监管空白、行政缺位。

由于人脸识别技术的独特性,需要一个专业对口的行政机关对信息使用者运用人脸识别技术的过程进行随时关注、预测和评估。就像我国一般行政机构及相关工作人员并不具备关于人脸识别技术的足够知识储备和危机意识,导致其无法准确判断、预测信息使用者是否具有使用人脸识别技术的能力、是否会给信息主体带来法律风险、能否及时解决人脸识别技术自身技术问题及个人信息受到损害的问题,极易出现多人治理越治越乱的现象,反而会加重使用人脸识别技术对个人信息的侵害,使信息主体的权益更加难以得到全面的保护。

3.2.3 人脸识别技术行业应用失范

单纯依靠现有法律法规和行政机关的监督管理,是明显不足以支撑人脸识别技术运用中个人信息的保护,还需要使用人脸识别技术行业的参与。

企业都是以获取经济利益为目的来使用人脸识别技术的,所以在获取、使用人脸信息过程中,企业为了利益多少会忽视信息主体的权益。故需要行业组织和行业规则进行约束。截止至今,我国加入使用人脸识别技术行业的企业不在少数,却没有统一的行业规则进行约束,也未设立行业组织进行管理。即便有了行业规则,没有自律的行业组织也是不行的。毕竟行业组织也是由一些使用人脸识别技术的核心企业构成,他们必定会偏向自身制定行业规则。那么,或多或少会影响信息主体的权利,扩大与信息主体之间的矛盾,极易造成个人信息的泄露。前段时间发生的小鹏汽车违法采集顾客的人脸照片被罚就是典型的例子。上海小鹏汽车公司利用人脸识别技术设备对顾客进行个人信息分析,并且不经顾客同意违法上传顾客照片。并且即便有了行业规则,但行业规则缺少法定强制力才是在人脸识别技术应用的企业中难以得到全面贯彻落地的关键。

3.2.4 个人维权意识薄弱

人脸识别技术运用的关键是信息主体提供自己的人脸信息,那么信息主体向信息使用者提供自己人脸信息时就会享有一些权利。虽然该技术已经在我国如火如荼地广泛应用,但是我国关于该技术的应用仍处于基础阶段,还不够成熟。加上人脸信息的易采集

性，会导致信息主体在很大程度上不知道自己的人脸信息在何时被采集、怎样使用，甚至早已被深度获取其他个人信息。即使信息主体对使用人脸识别技术知情，也会面临不知为何深陷个人信息被侵害的谜团之中。更不要提及信息主体能清楚明了地知道在使用人脸识别技术过程中自己所享有的个人信息权利。所以，就会出现在人脸信息等个人信息被侵犯后，信息主体未进行维权的情况。

第四章 人脸识别技术应用中个人信息保护的建议

4.1 完善相关民事立法

前面分析可得，我国虽有专门相关立法的保护，但还存在着一些问题并未得到真正的规范和解决。所以，下面就从民事立法方面提出一些改进建议。

4.1.1 坚持相关基本原则

在人脸识别技术应用的规制中，不管是公权力领域的合理使用还是其他领域的限制使用，都是通过对个人信息的保护来确保自然人权利的合法正当行使。为此，在人脸识别技术应用中个人信息的保护在遵循原有的合法性、合理性、告知同意原则的基础上，也要遵循以下几种原则：

① 最小必要性原则

必要性原则需要根据目标和目标实现过程、实施行为对权利人侵犯程度得出合理的结果。又因为人脸识别技术应用中个人信息属于个人特殊敏感信息范畴，而个人特殊敏感信息在进行使用、分析时需要遵守“法定必需”的特殊原则。^①所以，这就要求个人信息在人脸识别技术应用中必须遵守最小必要性原则。最小必要性原则要求在获取个人信息时必须与其所使用的领域或场景有直接联系。也就是说，只有利用人脸识别技术获取个人信息的行为与使用该个人信息的目的或用途是有直观的相关性，才能进行人脸识别技术的使用。

《人脸识别技术规定》的第2条第8款强调了必要性原则。但是仅仅强调必要性原则是不够的，还要更进一步坚持最小必要性原则。所以，使用者们在进行人脸识别技术运用时对个人信息的获取利用须要以最小必要性原则要求自己。这就要求，在使用人脸识别技术时，应当考虑个人信息是否与自己的产品或服务的运用有直接关联性。就是说，如果没有运用人脸识别技术来获取个人信息，则无法实现使用者的目标或目的。仅仅为了使用者自身便捷，方便管理等可有可无的理由，利用人脸识别技术来获取个人信息的行为就不符合最小必要性原则。

② 透明性原则

^① 付微明. 生物识别信息法律保护问题研究[D]. 中国政法大学, 2020.

透明性原则来源于《欧盟一般数据保护条例》，其主要针对信息利用者和监管机构进行管理和制约。透明性原则要求信息使用者对自己所使用的个人信息要有一个公开透明的说明，例如，在获取人脸信息时要告知人脸信息所有者其使用范围、使用目的以及后续使用后关于人脸信息处理的问题。参考欧盟规定的透明性原则，我国对人脸识别技术运用中收集、使用面部信息也应当作出相应的透明性原则保护解释。人脸信息的使用者要对其所有者积极主动、公开透明进行叙述，不能对相关用途、目的进行隐瞒或是危害信息所有者的个人权益。透明性原则是告知同意原则的前提和基础。只有落实透明性原则，才能使人脸信息所有者有效行使知情权和同意权。

③ 保护隐私原则

人脸识别技术应用获取收集的面部信息极易过度分析人们的个人信息，人们的隐私权也容易遭受到侵害。所以，在人脸识别技术应用中，理应告知被使用者相关人脸信息的获取用途、使用目的以及存放时间等，并且要获得相关被使用者实质上的知情同意，不得强迫被使用者同意。同时，对于获取人脸信息的使用目的等都要与其告知相关被使用者的情况相匹配，不能超越其界限，不能深度挖掘个人信息。没有经过被使用者的允许，不能将获取的人脸信息用于盈利或和其他未经授权的机构共享信息。除此之外，使用者也理应遵守与被使用者相承诺的使用时间。在超过期限后或被使用者取消同意，应当自觉将获取的相关面部信息及涉及的其他个人信息进行清理、消除。

④ 场景化使用原则

由于人脸信息具有独特性、易采集性、可识别性，所以根据场景的不同，利用人脸识别技术获取收集的面部信息深度也会有所不同。因此，应当对不同场景中获取面部信息的条件进行分别规制。例如，在金融、医疗等领域中，信息使用者若想收集被使用者的面部信息必须要告知被使用者相关使用目的、用途或者时间，并要征得被使用者的同意。在国家政府公权力领域，面部信息获取和使用的条件就存在较大的差别。若出现必要或特殊情况时，他们可以越过被使用者直接使用面部信息并深度获取其他相关个人信息。例如，公安机关将嫌疑犯照片和数据库现有的人脸信息进行分析对比、交警捕捉市民交通违规镜头来获取违规市民的个人资料。

⑤ 损害连带赔偿原则

人脸识别的不可更改性决定了信息使用者利用人脸识别技术获取被使用者的面部信息后，易出现被使用者的面部信息或相关个人信息泄露、滥用、非法盈利的情况。若

要造成严重的损失时，被使用者有权要求信息使用者承担相关损失的连带赔偿责任。一旦发生泄露、滥用情形人脸信息等其他个人信息都会受到无法恢复原状的损失，所以需要加强事后损害赔偿的救济。该原则的坚持能够在很大程度上监督信息使用者合理合法使用人脸信息减少面部信息非法售卖、滥用的情形，加强信息使用者对自身的约束，同时也能有效提高了对人脸识别技术应用中个人信息的保护力度。

4.1.2 细化非国家机关一般情况规则

如今，现行关于个人信息保护法律规范，都是以合法性原则、必要性原则、透明性原则和告知同意原则为基础，把个人信息是否收集和获取的权利交于人们自己手中。我国颁布的《人脸识别技术规定》反复强调了告知同意原则，并将其细化为单独同意，信息使用者必须在进行人脸信息活动单独征得人们自身明示同意，不然就属于侵权行为。同时，也从人格权和侵权责任、合同角度对个别领域信息使用者应用人脸识别技术中个人信息进行了规定。由此可以发现，对于使用人脸识别技术中个人信息受到侵害的普通行为没有一个准确的衡量标准，主要围绕针对个别特殊领域以合法性原则、必要性原则、透明性原则和告知同意原则为基础进行个人信息保护的规定。也正是因为缺少一般具体规则和标准，将合法性原则、合理性原则和告知同意原则凸显地毫无作用，我们对于侵害个人信息行为的判断也有大大折扣，不知究竟什么属于侵害个人信息的行为，什么不属于侵害个人信息的行为。即使判定为侵害个人信息的行为也没有一个能够通用的普遍救济手段和规定。所以，若要达到原则不停留于表面的目的，就要先解决一般规则具体化的问题。

① 落实人脸信息收集、使用、保存过程中实质上的告知同意

虽然《人脸识别技术规定》《个人信息保护法》已经规定了告知同意原则，但是在进行人脸信息获取、使用、保存时仅仅停留于形式上并没有落实到实质。人们往往出于从众、不知情或是外界压力情况下作出所谓形式上的“同意”，但从根本上并没有表达出人们本质的意愿，这也在一定程度上损害了人们的人格尊严。比如说，小区门禁强制要求使用人脸识别技术；在上网时经常出现只有允许使人脸识别功能才能进行APP使用。所以，我们需要对人脸信息获取、使用、保存过程中侧重落实实质上的告知同意。依据人脸识别技术使用情况的不同，被利用者有权要求使用者告知其人脸信息的使用、保存情况，做到双方信息对等。对于人脸信息的使用超越原有标准或是范围的特殊情况，理应告知被使用者相关具体情况并再次获取同意，不应强制或不告知实情要求被使用者必

须同意。通过对以上具体规范的适用使被利用者能够从实质上真正做到告知同意，进而使人格尊严得以体现。

② 框定人脸识别技术使用的边界

非国家机关使用人脸识别技术主要集中在两方面：一是以获取利益为目的的商业使用，二是为方便个人的私人使用。两者都需要一个明确的人脸识别技术使用边界划分标准来规范商业和个人使用时的行为。但目前我国出台的相关法律法规并没有对其使用边界进行一个详细的划分。例如，没有设定可以利用人脸识别技术场所、应用范围，没有相关具体处罚法律规定。这样导致商业或个人在利用人脸识别技术时毫无边界可言，个人信息混乱使用，难以进行管理。所以，以《民法典》和《人脸识别规定》为基础，框定人脸识别技术使用边界，让非国家机关关于人脸识别技术的使用处于一个合理合法的规制范围内。首先，不管是用于商业用途还是用于私人都要获取信息主体的同意和知情。其次，关于人脸信息获取范围的设定，可以限制对人脸信息获取分析的深度。若与使用目的没有任何关联性，则不能对人脸信息超出既定范围的获取、使用、分析。然后，人脸识别技术使用边界（如场所、范围）确定后，在实际应用时不能进行随意更改，不能超过信息主体原本同意的界限。

③ 明确人脸识别技术运用中信息主体的权利

在人脸识别技术应用中个人信息保护的规制中，要凸显保障提供人脸信息的信息主体权利的重要性。虽然《人脸识别技术规定》已将信息删除权、知情同意权纳入人脸识别技术运用中，但是其他涉及到人脸识别的个人信息权利并没有得到明确的规定。例如，信息自决权。信息自决权是德国的施泰姆勒在 1971 年个人信息保护法草案里提出来的，是人们按照法律法规掌握自身个人信息的主动权并有最终决定是否被获取或使用的权利。即利用人脸识别技术随意收集、使用、保存人脸信息时，信息主体都有权提出反对意见。同时，信息主体可以选择人脸信息利用者阐述其理由。如果其原因无法让人脸信息主体接受，那么人脸信息主体就可以依照自己的意愿处理问题。人脸信息访问权和更改权的确立。人脸信息的使用和保存是人脸识别技术应用的必经阶段。在其使用和保存中，难免会出现人脸信息使用者操作不当、过度分析滥用或删除人脸信息的情况。再加上人脸信息主体具有知情权，人脸信息主体就有权对人脸信息的使用、保存的过程进行了解访问，以确保自己的知情权、隐私权、财产权益不受侵犯。并且在了解过程中，人脸信息主体若发现人脸信息的使用目的、范围等发生改变，便有权行使信息自决权。信

息自决权的行使也从侧面可以看出任人脸信息在决定去留时也有更改权。

④ 明确人脸识别技术运用中信息利用者的义务

有了人脸识别技术运用中信息主体权利的明确，自然也要对人脸识别技术运用中信息利用者的义务进行规制。人脸信息是人脸识别技术运用的关键，信息主体是获取人脸信息的载体，所以在人脸信息收集使用、保存或删除的过程中，要积极回应人脸信息主体的要求，主动告知信息主体相关信息的使用情况。例如，人脸信息主体提出更改或删除人脸信息的要求，信息利用者理应积极配合，按照人脸信息主体的意愿履行自己的义务。由于人脸信息具有高度敏感性和不可逆性，在遭遇人脸信息泄露、滥用，也应当积极作出关于人脸识别技术使用的整改，甚至在必要的情况下可以停止人脸信息的获取并删除相关个人信息。否则，在没有立法的强制力约束下信息利用者将掌握大部分主权，人脸识别技术应用的信息主体将处于弱势地位。

⑤ 完善相关人脸信息损害认定标准和赔偿标准

《人脸识别技术规定》中仅指出关于人脸识别技术应用中个人信息保护问题要依据《民法典》相关损害认定标准和赔偿标准进行实施，并没有根据人脸识别技术的特性从根本上解决个人信息受到侵害的问题。由于人脸信息自身的特性，再加上人脸识别技术应用过程中涉及到多个参与者（如技术提供者、信息获取者、信息主体等），会导致多个参与者在程序上违法程度不同，损害认定标准不一以及赔偿标准不明的情况。所以，完善人脸信息损害认定标准和赔偿标准要多考虑人脸识别技术应用过程的参与者、人脸信息的特性等。并且，人脸识别技术的使用与隐私权、人格权、财产权益、个人信息数据安全有密切的联系，也要考虑财产损害和精神损害等相关问题。故参照人脸信息的特性，多个参与者的参与程度，坚持损害连带赔偿原则，因地制宜灵活进行损害认定标准和赔偿标准判别。如，无须等待出现损害结果就可以进行损坏认定，即不以实质损害结果作为损害认定的必备条件和标准。人脸信息的独特性和不可更改性决定了人脸信息在泄露的瞬间就开始制造无法恢复的损失，没有必要等到信息主体权益最终出现受损时再进行判断。相关人脸信息的赔偿标准可依照人脸识别技术使用过程中不同参与者制造损害程度的不同来进行不同额度的赔偿。

4.1.3 制定国家机关公权领域的使用规范

《人脸识别技术规定》第1条就对适用范围作出了明确的限制，其主要是用于平等民事主体之间引起的民事纠纷。这就说明了该规定是处理非国家机关关于人脸识别技术

应用中个人信息保护问题，与以政府为代表的国家机关毫无关系。人脸识别技术应用的信息使用者是由国家机关和非国家机关两者共同构成的，缺少任何一方的规制都会导致人脸识别技术应用中处理个人信息保护问题的不完整性。

为了弥补国家机关公权领域的空白，下一步应该制定相关国家机关使用规范。由于人脸信息的不可逆性，相关国家机关公权领域的规范制定主要以事前规制为主。在政府等国家机关的运用中，个人利益要让位于重大公共利益，人们没有对于人脸识别技术使用的拒绝权，很大程度上增加了人脸识别技术在政府等国家机关的滥用率或错用率。因此，就需要对政府等国家机关运用人脸识别技术进行合理规制。一方面，要加强人脸识别技术运用审查。制定一个利用人脸识别技术来收集个人信息的标准或参照，使以公共服务为目的的国家政府等国家机关在收集人脸信息前进行合理审核，以降低使用人脸识别技术获取面部信息的非必要性。一方面，规定除必要或特殊情况下政府等国家机关利用人脸信息理应主动提前告知信息主体关于人脸信息使用的具体去向和范围。另一方面，赋予国家机关使用人脸识别技术一定程度上的豁免权^①。也就是说在在面对一些法律规定危害国家安全或是重大犯罪等特殊情况下，以政府为国家机关可以不经信息主体的同意，通过人脸识别技术去深度获取这些信息主体的个人信息。并且事后不追究其违反相关法律规则的责任。同时，关于利用人脸识别技术获取个人信息的标准每个人有不同的见解和认知。并且人脸信息本身具有的敏感性，在政府等国家机关审查关于是否适用人脸识别技术来获取面部信息产生争议时，可以适当地开展内部会议或实施听证程序。通过内部会议讨论或听取广大群众的意见，再作出一个合理准确判断。

4.2 强化相关人脸识别技术运用的行政监管

执法与立法密不可分，相辅相成。立法为执法提供原则性的基础支撑，执法中的经验和教训为立法提供新思路和新对策。两者一并保护人们个人信息的权益，才能减少个人信息受到侵害，才能更好地促进人脸识别技术的长久发展。因此，很有必要对执法机构进行行政监管。

4.2.1 建立专门的行政监管机关

目前，我国没有相关人脸识别技术的行政监管机关。虽然设立有国家信息中心、网

^① 孙道锐. 人脸识别技术的社会风险及其法律规制[J]. 科学学研究, 2021(01): 12-20+32.

信办等数据保护机构，但是这些机构都没有明确的法律授权。凡是涉及到人脸识别技术运用时易出现监管主体不明、职责划分不清的问题，都会导致关于该技术的行政监管复杂混乱。比如说，利用人脸识别技术应用进行非法营业是属于工商管理行政机关的监督范畴；触及刑法方面的是属于公安机关审查范畴。可见，如此混乱交错的关系，很容易出现重复监管或空白管理的现象，造成国家资源的严重浪费和信息主体个人信息权益的受损。所以，可以借鉴欧洲集中统一管理的方式，设立一个专门且独立的行政监管机关对人脸信息获取、使用、保存或删除的整个过程进行监督和管理。

4.2.2 设置行政监管机关分类管理制度

单依靠一个专门行政监管机关是不够的，还需要在行政监管机关进行分类管理，对使用人脸识别技术的政府和企业适用不同的标准。人脸信息自身的极度敏感性、易采集性、可破解性，会在人脸识别技术利用过程中产生极多的不稳定因素。就拿企业来说，要事先向行政监管机关事先进行报备登记，只有在获得行政监管机关的许可后才可以使用人脸识别技术。政府也需要事前报备后才能利用人脸识别技术获取人脸信息。行政监管机关可以依据他们报备登记的收集方式、目的、用途及潜在风险进行一个理性分析，并给予他们可能出现不稳定因素的指导建议。因此，对人脸识别技术运用的行政监管需要针对企业和政府两个主体为代表的领域进行分类管理。

4.2.3 制定相关监管措施

第一，设置一定的准入制度。人脸识别技术是一个新兴技术，人脸信息属于高敏感、可识别的个人信息，易采集、易遭到泄露和滥用。所以，该技术的使用需要一个较高的入门门槛和标准。因此，行政监管机关需要根据人脸识别技术的特性，对申请使用该技术的企业进行审查。若企业能达到行政监管机构所规定的准入标准，那么该企业就可以使用人脸识别技术。

第二，设置定期审查评估制度。即使有了事前准入制度进行审查和企业报备登记，但在运用过程中，也存在行政机关无法避免的一些企业投机取巧行为。所以，行政监管机关需要对使用人脸识别技术的企业进行定期审查评估^①。在定期审查过程中，若发现侵害行为或存在泄露人脸信息的风险，可以及时制止危险的扩大。同时，通过定期的审查记录，可以对使用人脸识别技术的企业进行风险评估，总结归纳出更好的预警机制，

^① 崔建. 大数据时代个人信息保护问题研究——基于政府监管的分析视角[D]. 河北经贸大学, 2017.

从而避免更多人脸信息泄露问题的出现。

第三，设置事后救济的惩戒制度。虽然有专门的行政监管机关进行监管，但是总会有钻漏洞的情况发生。并且人脸信息自身的不可更改性、不可逆性，会导致在行政监管机关发现个人信息受损时已经无法进行挽救。所以行政监管机关只能做到在最大程度上减少信息主体个人信息的损害。比如，通过对人脸识别的侵害行为进行具体调查和详细分析，推断该行为是否违法、是否归于信息使用者的过错。如果属于违法行为或是归于信息使用者的过错，那么行政监管机关就应当对信息使用者进行处罚。若情况严重，可以对其进行高额处罚。目前，我国人民法院是大力支持和鼓励被侵权者主张民事权益的。若人脸识别行为造成公民知情权、隐私权、人格尊严、财产性权益受损，也可以参照侵权行为主张民事权益。

4.3 建立行业自律机制

正如前面所言，相关立法虽已进行规制，但人脸识别技术运用过程中个人信息保护仍有局限性。因此，加强行业自律能够有效填补立法和执法的空白，平衡人脸识别技术与个人信息保护之间的关系。但是行业自律机制的建立不仅需要企业的参与还需要行业组织自律规则的规范。故以下就针对企业和行业自律组织规则两方面提出一些建议。

4.3.1 加强企业自律

谋取利益是企业使用人脸识别技术的根本目的，这就导致在人脸信息获取、使用、保存过程中企业会首要考虑自身，很容易忽视人脸信息主体的权利。所以，人脸信息获取、使用、保存的整个过程就成为企业进行合理规范的基础。

第一，企业应当与信息主体达成相关信息告知、保密的约定。也就是说，企业在利用人脸识别技术获取人脸信息前，需要积极履行告知义务（即人脸信息使用去向、范围）。同时，也有义务告知信息主体在利用人脸信息过程中可能存在的风险。人脸识别技术的应用极易出现人脸信息泄露、非法使用的现象并产生侵犯隐私权、人格权、个人信息权的法律风险。这些问题之所以会出现，与随意使用该技术的企业有很大的关系。那么就需要企业自身与信息主体达成保密约定，若要出现侵害信息主体相关个人信息的情况，企业自身需要对人脸信息主体承担一定的责任。这在一定程度上能够制约企业泄露、不当使用等行为。

第二，企业理应对获取、使用人脸信息进行保密。一方面，企业自身要有完备的硬

件设施。应加强相关人脸识别技术的升级改造，增加个人信息数据的安全性，防止外来者的非法入侵和获取。另一方面，企业理应提高工作人员的技术能力和工作素养。毕竟人脸识别技术还是新兴技术，需要专业人员对此进行使用、检查，确保人脸信息使用的安全性。同时，也要加强相关技术人员的保密意识和对信息主体隐私的保护意识。企业保密义务的落实需要企业里工作人员的遵循。例如，签订保密协议，按期开展相关保密课程、隐私保护课程的学习。

第三，企业要严格把关人脸信息的输送。若有他方使用人脸信息的需要，获取人脸信息的企业要对需求者进行全面的审查评估，查看需求者能否达到合理使用、妥善保管人脸信息的保护标准。如果在审核时发现需求者无法达到标准，则企业不得进行输送。反之，可以进行输送。同时，在需求者使用的过程中，企业也不能放松对需求者的监督，按时进行查看审核。倘若发现需求者有操作不当行为，必须立即停止其使用并要求删除已经传输过去的人脸信息。

4.3.2 制定并完善行业自律规则

企业自律需要行业自律组织予以引导。行业自律组织在对企业进行监督管理时也需要行业自律规则与之相配合。行业自律规则的实施有利于加强对使用人脸信息行为的监管和治理，在一定程度上规范使用人脸识别技术企业的行用，能够为人脸识别技术的持续发展注入新鲜力量。

人脸识别技术的运用主要就是人脸信息获取、利用的过程，所以行业自律规则的制定就可以从这方面入手进行规制。基于对人脸识别获取、使用的标准不同，每个企业关于告知、保密等约定最终实施标准和落实程度也会有所不同，因此可以制定一些行业自律规则来作为行业的统一参照，为人脸信息的使用做最根本的保障。又因各行各业有所不同，行业自律规则的制定也需要因地制宜，全方位考虑，在做到规范使用人脸识别技术的同时能增强在各个行业的适配度。除此之外，行业自律规则也要加大关于行业自律组织监督管理规范的制定。行业自律组织在对利用人脸识别技术的企业进行监督管理时，可能会出现监管不当或监管过度的情况，则行业自律规则需要制定灵活变通的行业自律组织监管标准，以此来应对行业自律组织关于不同使用人脸识别技术行业的监督管理。

4.4 增强个人的维权意识和能力

通过前面分析可知,虽然《人脸识别技术规定》已经赋予了人脸信息主体知情同意权和信息删除权,但是由于我国人脸识别技术运用发展仍处于一个初期阶段,信息主体对于自己权利行使的关注度并不高。因此,主要需要从维权意识和事后救济能力入手提高信息主体个人信息的安全性。

4.4.1 加强信息主体的维权意识

信息主体有权要求信息使用者停止使用并删除自己相关个人信息。人脸识别技术技术的运用主要集中体现在人脸信息的获取、使用、保存。那么,就可以针对获取、使用、保存人脸信息几个不同阶段,逐一向信息主体普及其权利该如何行使及保护,以此加强信息主体的维权意识。例如,相关使用者必须要告知并取得信息主体关于人脸信息使用情况的同意。如果没有此举动,信息主体就可以以侵犯自身知情同意的权利进行个人信息保护。人脸识别信息进行使用时,若要出现与先前所说人脸信息使用目的、方式、范围不同的情形时,信息主体就可以要求其立即删除人脸信息和可能获取到的其他个人信息。如果信息利用者不进行删除,那么信息主体可以依据自身的信息删除权进行维权。由于利用人脸识别技术可能会使相关个人信息陷入隐私泄露、人格尊严受损、损害财产权益、个人数据安全系数较低的法律风险中,导致信息主体与之相关的隐私权、人格权、个人信息权受到侵犯,所以信息主体可以以此向信息使用者追究民事责任。

4.4.2 提升信息主体的事后救济能力

参考近些年发生相关人脸识别技术案件以及人脸识别技术的特性,会发现信息主体仅依靠事前的知情同意权来维护权益是万万不够的。很多情况下,信息主体都是在已经发生利用人脸识别技术侵害个人信息行为后才得知自身权利受损。因此,需要提升信息主体事后救济能力,及时进行止损。信息主体在发现人脸信息使用不当、泄露等情况时,可以立即停止信息使用者对人脸信息的获取和使用,并要求信息使用者删除已被记录的人脸信息。若造成一定财产损失,信息使用者要对此进行赔偿,以做到在最小程度上减少信息主体的损失,保障个人信息的安全。

结 语

人脸识别技术的应用推动了我国科技技术和经济的快速发展，对人类社会进步有着深远影响。虽然该技术应用在各种领域为人们提供了方便，但对人们个人信息安全也具有一定威胁，如人格尊严易受侵犯、隐私易受损害、个人数据安全降低、财产权益受损。所以，我们在鼓励发展使用人脸识别技术的同时，也要常持一颗防范之心，加强对个人信息的保护。

虽然我国《民法典》《个人信息保护法》《人脸识别技术规定》对人脸信息的归属给予了准确答复，从人格权、侵权责任和合同规则角度笼统解释了关于人脸识别技术如何处理个人信息的问题并厘清了一些滥用人脸识别技术侵害个人信息行为的性质和责任。但依旧未能彻底解决在使用人脸识别技术过程中出现的侵犯个人信息问题。通过对我国关于人脸识别技术应用中个人信息保护现状可知，我国仍面临着专门立法内容单一、行政监管缺位、人脸识别技术行业失范、个人维权意识薄弱等问题。

因此，针对个人信息可能会面临的风险及我国现存问题，提出“法律原则+法律机制”两合一模式，以相关法律原则为基础并且从立法、行政、行业、个人四个方面进行全方合理规制。一方面，遵循最小必要性原则、透明性原则、保护隐私原则、场景化使用原则、损害连带赔偿原则等，完善相关民事立法。另一方面，通过细化非国家机关一般情况规则，落实人脸信息收集、使用、保存过程中实质上的告知同意，框定人脸识别技术使用的边界，明确人脸识别技术运用中的权利和义务，完善相关人脸信息损害认定标准和赔偿标准等具体路径，同时配之以诸如制定国家机关公权领域的使用规范，强化相关人脸识别技术运用的行政监管，建立行业自律机制，增强个人的维权意识和能力等措施，为人脸识别技术应用中个人信息安全保驾护航。

参考文献

(1) 连续出版物

- [1] 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(01): 77-81.
- [2] 王俊秀. 数字社会中的隐私重塑——以“人脸识别”为例[J]. 探索与争鸣, 2020(02): 86-90.
- [3] 赵淑钰. 生物识别信息法律规制的国际经验与启示[J]. 中国信息安全, 2019(11): 37-39+43.
- [4] 闫晓丽. 美国对人脸识别技术的法律规制及启示[J]. 信息安全与通信保密, 2020(11): 94-101.
- [5] 银丹妮, 许定乾. 人脸识别技术应用及其法律规制[J]. 人工智能, 2020(04): 32-39.
- [6] 周坤琳, 李悦. 回应型理论下人脸数据运用法律规制研究[J]. 西南金融, 2019(12): 78-87.
- [7] 骆宏, 陈德俊, 孙晓等. 人脸识别技术在公安工作中的应用与推广——充分发挥人脸识别技术在侦查办案及民生服务中作用[J]. 中国公共安全, 2016(11): 129-132.
- [8] 周行. 人脸信息立法保护的规范体系建构[J]. 中南民族大学学报, 2021(08): 129-135.
- [9] 陈荣新. 比较法视野下人脸识别信息保护的法律模式研究[J]. 国际经济法学刊, 2021(04): 10-23.
- [10] 李朋, 王明达. “人脸识别”场景下个人面部信息保护问题初探——由“人脸识别第一案”展开[J]. 上海法学研究, 2021(14): 246-254.
- [11] 杨建军, 李童心. 人脸识别技术运用的法律原则[J]. 南宁师范大学学报, 2020(05): 37-47.
- [12] 刘德良. 《个人信息的财产权保护》[J]. 法学研究, 2017(03): 82.
- [13] 夏金莲. 人脸识别技术的应用风险及其法律规制——以《个人信息保护法》的制定为契机[J]. 西昌学院学报, 2021(03): 56-61.
- [14] 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[J]. 北京航空航天大学学报(社会科学版), 2020, 33(05): 21-29.
- [15] 王泽鉴. 人格权保护的课题与展望——人格权的性质及构造: 精神利益与财产利益的保护[J]. 人大法律评论, 2009(01): 51-103.
- [16] 张华韬. 我国人脸识别侵权责任制度的解释论[J]. 社会科学家, 2021(07): 97-103.
- [17] 蒋淑旭, 胡丹. 刷脸支付下消费者个人信息的法律保护[J]. 山西省政法管理干部学院学报, 2020, 33(04): 43-46.
- [18] 王利明. 人工智能时代对民法学的新挑战[J]. 东方法学, 2018(03): 4-9.
- [19] 王利明. 论民事权益位阶: 以《民法典》为中心[J]. 中国法学, 2022(01): 32-54.
- [20] 王利明. 敏感个人信息保护的基本问题——以《民法典》和《个人信息保护法》的解释为背景[J]. 当代法学, 2022(01): 3-14.
- [21] 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(02): 60-78.
- [22]张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(03): 38-59.
- [23]张新宝. 个人信息处理的基本原则[J]. 中国法律评论, 2021(05): 18-27.
- [24]张新宝. 论个人信息权益的构造[J]. 中外法学, 2021(05): 1144-1166.
- [25]Linders D. From e-government to we-government: Defining a typology for citizen coproduction in the age of social media[J]. Government information quarterly, 2012, 29(04): 446-454.
- [26]高富平. 个人信息使用的合法性基础——数据上利益分析视角[J]. 比较法究, 2019(02): 72-85.
- [27]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[J]. 中国政协, 2020(14): 32-33.
- [28]王洪亮. 《民法典》与信息社会——以个人信息为例[J]. 政法论丛, 2020(04): 3-14.
- [29]王利明. 《个人信息保护法》的亮点与创新[J]. 重庆邮电大学学报(社会科学版), 2021, 33(06): 1-13.
- [30]杨复卫, 白家焯. 人脸识别技术的法律风险及其场景化治理[J]. 重庆理工大学学报(社会科学), 2022, 36(01): 180-190.
- [31]孙道锐. 人脸识别技术的社会风险及其法律规制[J]. 科学学研究, 2021(01): 12-20+32.
- [32]王德政. 针对生物识别信息的刑法保护: 现实境遇与完善路径——以四川“人脸识别案”为切入点[J]. 重庆大学学报(社会科学版), 2021(05): 133-143.
- [33]黄岚文. 存在安全风险的人脸识别[J]. 科学大观园, 2017(08): 78-79.
- [34]杨立新. 个人信息: 法益抑或民事权利——对《民法总则》第111条规定的“个人信息”之解读[J]. 法学论坛, 2018(01): 34-35.
- [35]周汉华. 《个人信息保护法(草案)》: 立足国情与借鉴国际经验的有益探索[J]. 探索与争鸣, 2020(11): 9-11.
- [36]王利明. 论个人信息权在人格权法中的地位[J]. 苏州大学学报(哲学社会科学版), 2012(06): 68-75+199-200.
- [37]王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(04): 62-72.
- [38]周汉华. 个人信息保护的法律定位[J]. 法商研究, 2020(03): 44-56.
- [39]洪延青. 人脸识别技术的法律规制研究初探[J]. 中国信息安全, 2019(08): 85-87.
- [40]张新宝. 我国个人信息保护立法主要矛盾研讨[J]. 吉林大学社会科学学报, 2018, 58(05): 45-56+204-205.
- [41]叶名怡. 个人信息的侵权法保护[J]. 法学研究, 2018, 40(04): 83-102.
- [42]程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(03): 102-122+207-208.

- [43]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(04): 19-36.
- [44]王秀哲. 大数据时代个人信息法律保护制度之重构[J]. 法学论坛, 2018, 33(06): 115-125.
- [45]刘艳红. 民法编纂背景下侵犯公民个人信息罪的保护法益: 信息自决权——以刑民一体化及《民法总则》第 111 条为视角[J]. 浙江工商大学学报, 2019(06): 20-32.
- [46]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(03): 73-81.
- [47]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(06): 1-20.
- [48]刘越. 论生物识别信息的财产权保护[J]. 法商研究, 2016, 33(06): 73-82.
- [49]程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学, 2019(04): 26-43.
- [50]王晓锦. 人工智能对个人信息侵权法保护的挑战与应对[J]. 海南大学学报(人文社会科学版), 2019, 37(05): 126-134.
- [51]李庆峰. 人脸识别技术的法律规制: 价值、主体与抓手[J]. 人民论坛, 2020(11): 108-109.
- [52]邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(05): 51-63.
- [53]王成. 个人信息民法保护的 mode 选择[J]. 中国社会科学, 2019(06): 124-146+207.
- [54]张建文, 赵梓羽. 人脸识别技术应用的法律规制[J]. 西南石油大学学报(社会科学版), 2021, 23(05): 100-105.
- [55]张新宝, 葛鑫. 人脸识别法律规制的利益衡量与制度构建[J]. 湖湘法学评论, 2021, 01(01): 36-51.

(2) 专著

- [1]唐汇西. 网络信息政府监管法律制度研究[M]. 武汉: 武汉大学出版社, 2015.
- [2]邹毅, 黄玲. 信息网络与高新技术法律前沿(第八卷)[M]. 上海: 上海交通大学出版社, 2014.
- [3]京东法律研究院. 欧盟数据宪章: 《一般数据保护条例》GDPR 评述及实务指引[M]. 北京: 法律出版社, 2018.
- [4]程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021.
- [5]张民安. 信息性隐私权研究[M]. 广州: 中山大学出版社, 2014.
- [6]周汉华. 域外个人数据保护法汇编[M]. 北京: 法律出版社, 2006.
- [7]王利明. 侵权责任法研究(下)[M]. 北京: 中国人民大学出版社, 2011.
- [8]郭瑜. 个人数据保护法研究[M]. 北京: 北京大学出版社, 2011.
- [9]郭明龙. 个人信息权利的侵权法保护[M]. 北京: 中国法制出版社, 2012.
- [10]谢远扬. 个人信息的私法保护研究[M]. 北京: 中国法制出版社, 2016.
- [11]郎庆斌, 孙毅, 杨莉. 个人信息保护概论[M]. 北京: 人民出版社, 2008.
- [12]齐爱民, 贾淼, 朱炼等. 个人资料保护法原理及其跨国流通法律问题研究[M]. 武汉: 武汉大学出版社, 2004.

(3) 学位论文

- [1]王玉. 基于图像集合和视频序列的视频人脸识别算法研究[D]. 吉林大学, 2017.
- [2]杨智超. 人脸识别技术下的个人信息法律保护研究[D]. 西北民族大学, 2021.
- [3]赵爽. 人脸识别技术风险的法律规制研究[D]. 中国矿业大学, 2020.
- [4]崔建. 大数据时代个人信息保护问题研究——基于政府监管的分析视角[D]. 河北经贸大学, 2017.
- [5]付微明. 生物识别信息法律保护问题研究[D]. 中国政法大学, 2020.
- [6]宋平. 人工智能应用中个人信息保护研究[D]. 河北大学, 2019.
- [7]卢德利. 人工智能的安全风险及其法律规制[D]. 武汉大学, 2019.
- [8]牛海虹. 人脸识别运用中的个人信息保护[D]. 中国社会科学院大学, 2019.
- [9]孙楠. 人脸识别技术应用的法律规制研究[D]. 吉林大学, 2020.
- [10]王漪清. 我国人脸识别技术应用的法律规制——基于《个人信息保护法(草案)》[D]. 对外经济贸易大学, 2021.

(4) 报纸文章

- [1]刘晓春. 欧盟《通用数据保护条例》原则条款解析[N]. 中国市场监管报, 2019-04-16(006).
- [2]杨合庆. 论个人信息保护法十大亮点[N]. 法制日报, 2021-08-22.
- [3]崔爽. 人脸识别第一案: 用法律拦住“伸得太长的手”[N]. 科技日报, 2019-11-08(005).
- [4]朱巍. 人脸识别的法律性质认定[N]. 检察日报, 2019-11-06.

(5) 电子文献

- [1]黄驰波. 《北大学子弑母案嫌疑人落网机场: 刚升级人脸识别系统! 可对比报警》[EB]. <http://www.infzm.com/contents/148615>, 2020-01-20.
- [2]牛谷月. 小鹏汽车被罚: 7 家门店 22 台摄像设备 6 个月违法采集 43 万张顾客人脸照片[EB]. http://k.sina.com.cn/article_1683472727_6457c1570200186xo.html, 2021-12-14.