

人脸识别技术应用中的隐私权保护

王宏杰

(河北经贸大学, 河北 石家庄 050061)

【摘要】随着人工智能的快速发展,人脸识别技术被应用在门禁、考勤、身份核验等各种场景中。但人脸识别技术的运用在便利人们生活、提高工作效率的同时,带来的风险同样不容忽视。人脸识别技术的滥用使公民的人身安全和财产安全都受到了巨大的威胁。因此,通过对我国人脸识别技术应用中的隐私权保护立法现状进行分析,尝试通过完善隐私权保护的相关立法、加强行业自律、并且完善监督机制和提高公民隐私权保护意识等途径,保护公民隐私权,并促进人脸识别技术进一步发展。

【关键词】人脸识别; 个人信息; 隐私权

一、人脸识别技术应用中的隐私权概述

(一) 人脸识别技术与隐私权的概念

1. 人脸识别技术的概念

人脸识别技术就是利用计算机分析人脸图像,检测图像的频域空间滑动检测图像块,判别是否是人脸区域,提取有效的特征信息,用来识别人身份的一种技术。^[1]人脸识别于1965年首次提出,上个世纪90年代发展迅速,出现了许多知名的人脸识别商业公司。进入新世纪以来,这一技术得到进一步发展,在金融、安保、公安等各个领域逐渐被广泛应用。

2. 隐私权的概念

1890年,美国学者沃伦和布伦代斯在发表的《论隐私权》一文中,首次将隐私权作为一种独立的权利提出,提出“独处权说”,将隐私权描述为一种“免受外界干扰的、独处的权利”。^[2]在法国,隐私权被称为“忘却权”,指个人为了自由发展其人格而要求所必需的安宁与平静的权利。^[3]我国学者林喆认为:“隐私应该是指个人的私生活信息,隐私权就是指个人所享有的与公共利益无关的私密信息的支配和控制权。”^[4]从以上观点可以看出,隐私权的中心内容是信息主体控制自身隐私的权利,可以独立决定是否对外披露,以及如何对外披露,不受他人非法干涉。也就是说,公民可以管理和控制个人信息,按照个人意愿自由决定如何使用个人信息,以及保护个人信息不受他人的非法侵犯和干涉,以维护个人的基本尊严。

(二) 人脸识别信息的特殊性

个人生物识别信息,也称人体生物信息、个人生物信息、个人生物特征信息,是指采集于人体的指纹、虹膜、面容、声音等信息,具有唯一性和不可变更的特质。^[5]人脸信息是生物识别信息的一个分支,同时也是个人核心隐私,是隐私权的客体。

具体而言,人脸信息具有独特性、方便性和易采

集性等特征,与声纹、指纹、虹膜等一般生物识别信息相比具有强烈的敏感性和特殊性。不同于指纹、声纹等一般生物识别信息需要信息主体配合才能完成采集,人脸信息的采集具有非接触性,许多应用软件的操作过程具有隐蔽性,在没有与使用者签署用户协议,使用者并不知情的情况下随意收集用户人脸信息,严重侵犯用户隐私权。另外,和其他生物识别信息相比,人脸信息具有更强的人格属性。人脸信息即肖像,属于人格权的调整范围,不仅关系到使用者的人格利益,更包含着更大的商业价值。每个人的脸部特征都是独一无二,不可更改的。人脸信息一旦丢失,将会对信息主体造成极大的损失。因此,我国应将人脸信息等敏感信息与一般生物识别信息区别对待,加强对人脸信息的保护。

二、我国人脸识别技术应用中隐私权保护的司法与立法现状

(一) 我国人脸识别第一案评析

2020年11月20日,杭州市民郭兵诉杭州野生动物世界有限公司一案,在杭州市富阳人民法院一审判决。^[6]因杭州野生动物有限公司升级入园方式,以短信通知游客采用人脸识别方式入园,原告郭兵认为人脸信息属于个人敏感信息,一旦外泄,会对信息主体产生重大影响。野生动物公司未经消费者同意,直接以短信通知消费者的方式无效。这种强制收集用户人脸信息的方式,严重侵犯了消费者的个人隐私,欲办理退卡却遭到野生动物公司的拒绝,遂将其诉至法院。最终法院判定支持原告诉讼请求。郭兵与动物园之间就购买年卡成立合同关系,在履行合同过程中,动物园变更入园方式为“刷脸进入”,属于单方变更合同内容,若郭兵不同意变更内容,则应当履行原来的约定,否则构成违约。^[7]

从侵权的角度来看,可以基于《消费者权益保护法》的规定,以动物园未经原告同意,变相强制收集

原告人脸信息为由,要求其承担违约之诉。也可以根据《民法典》第1035条“不得过度处理”的规定,要求其承担侵权责任。但基于《消费者权益保护法》提起的侵权之诉中,以消费者购买商品或接受服务等约定为前提,对个人信息的确认并不完整。以《民法典》为基础的侵权之诉中,虽然规定了自然人有个人信息权,但却没有明确相关民事责任,在司法救济方面存在较大缺陷。基于此,我国有必要厘清人脸识别技术的发展和公众个人信息保护的边界,深入研究人脸识别技术的法律规制,探寻我国人脸识别技术中隐私权保护的适宜路径。

(二)我国人脸识别技术中隐私权保护相关立法现状

我国《民法典》、《网络安全法》和《信息安全技术个人信息安全规范》等均对个人信息作出了规定。《民法典》第1034条延续了《网络安全法》对个人信息的定义,将生物识别信息纳入个人信息的保护类别,通过具体人格权的方式进行保护;《网络安全法》规范了个人信息的收集和利用行为;《消费者权益保护法》规定信息收集应当依照“合法、正当、必要”原则,并强调消费者在收集信息时的知情同意权;《信息安全技术个人信息安全规范》更是对生物识别信息进行了明确的定义和权威的规定,个人生物识别信息被列为个人敏感信息,采取更全面、更完善的保护措施。

在我国《民法典》的规定中,对个人信息和隐私有所不同,对隐私的保护多于对个人信息的保护。《民法典》第1032条和第1033条明确规定自然人享有隐私权,将隐私划分为四大部分,并以罗列的方式禁止各种可能出现的侵犯公民隐私权的行为。而人脸信息既属于隐私,又属于个人信息,因此,受到隐私权和个人信息的双重保护。

(三)我国人脸识别技术应用中隐私权保护存在的问题

当前,人脸识别技术被广泛应用,而相关立法却并不完善。许多开发商未经用户同意随意收集用户人脸信息,或未采取防止信息泄露的完备系统,导致用户信息泄露,被不法利用。使得人脸识别技术受到越来越多的非议,人脸识别技术的发展寸步难行。

1. 监管及救济机制不完善

首先,在科技快速发展的时代,行政监管对风险防控、保障公民权益起着重要作用。然而,在立法缺失的情况下,行政监管不能及时落实,未能建立人脸识别技术的监控体系,以及不能及时、有效的管控技术发展对社会的影响。并且,没有专门的监督机构,当人脸识别技术出现不同问题时,网络问题由网信办负责,刑事问题由公安机关负责,而违法经营问题又

由工商部门负责,这种混乱局面就是因为人脸识别技术缺乏专门监管机构造成的。

其次,缺乏侵权救济机制。受害者在人脸信息遭到侵犯时,常常不知道以何种方式,向何种部门求助。使得信息主体无法有效保护人脸信息,人脸信息被滥用的情况屡见不鲜。我国现行法律没有赋予权利主体以诉权资格,没有明确举证责任的分配和可以提出的合理诉求等。这就使得个人信息主体出现维权困境,不能保护个人信息,在信息处理活动中处于弱势地位。

2. 现行法律体制不健全,未成体系化

首先,《民法典》将生物识别信息与自然人的一般个人信息放在一起罗列,不能体现出生物识别信息的特殊性。其次,《民法典》对于生物识别信息保护的的规定零星分布在不同条文中,呈现出分散性,以原则性规范为主,因此在涉及生物识别信息的保护时,需要将其归入到个人信息的保护范畴中,针对性不强。其他法律对生物识别信息的功能、作用也均没有明确规定,法律没有规定谁有权收集公民的人脸信息以及收集后的相关权利义务规定,就导致出现随意收集公民人脸信息的乱象,对收集到的人脸信息更是缺乏相应保护措施,使得公民的个人隐私陷入危险境地。因此,我国对生物识别信息的法律保护亟待完善。

3. 行业自律缺失

面对人脸识别技术日新月异的发展,其带来的风险也不断增多。在国家法律法规尚未完善的前提下,行业自律应率先采取行动,规制风险。企业作为技术的开发者或使用者,理应承担应有的责任。然而,目前我国人脸识别技术中的行业自律却没能起到相应的作用。就人脸识别技术的总体企业数量而言,加入行业协会并且严格遵守协会标准的企业数量较少,而且行业标准不具有法律强制力,难以得到落实。其次,企业在制定行业规范时,往往以维护企业利益为主要目的,难免掺杂自身私利,难以完全成为行业发展的指引。

三、完善我国人脸识别技术应用中隐私权保护的对策和建议

(一)完善立法保护

目前,我国仅在《信息安全技术个人信息安全规范》中有对个人生物识别信息以及个人敏感信息的定义和相关规范。规定须有本人明确同意的意思表示,才能进行个人敏感信息的收集;个人敏感信息的传输储存应采取相应的安全举措等。但是《信息安全技术个人信息安全规范》不属于法律规范,位阶较低。所以我国应及时加强生物识别信息法律层面的规范。具体而言,应当明确规定生物识别信息的权责条款、禁止性规定、限制条件和特定的救济措施等。对信息主体的知情权和更正权等权利加

以保障。明确数据处理者应采取加密等安全保障措施,以及违法处理信息后的惩处制度。最后,还应建立刑事法律保护机制,刑法是维护信息主体合法权益的最后一道防线,及时解决非法伪造、获取和占用人脸信息的定罪量刑问题,为生物识别信息的法律保护提供坚强的后盾,以保障我国生物识别技术应用在法制轨道上顺利运行。

（二）加强行业自律

由于个人信息隐私权保护规制的主体主要是各类软件或社会机构等网络服务提供者,法律不适宜直接为网络服务提供者规定具体的权利义务。所以,法律可以通过规定具体原则的方式为行业自律提供指导。具体包括用户知情同意原则、数据合理使用原则、数据安全保护原则和用户权利保障原则等。

1. 用户知情同意原则

现今,我国许多软件默认同意、被动同意现象普遍,有的软件将知情同意条款设置为概括授权,用户只能选择同意或不同意,若不同意将不能使用该软件,不能充分体现用户的个人意愿。其次,有的条款内容隐蔽、意思隐晦,经常被折叠或包含在相关协议中。更有甚者,在用户拒绝协议后仍然继续收集用户个人信息,严重侵犯用户隐私权。所以,在立法中应明确用户知情同意原则,软件在采集、使用用户个人信息时,应通过用户协议等方式通知用户,并在重要内容处,用足以引起用户注意的标红或下划线等方式标注。随后,用户协议禁止默认同意、被动同意等情形,均应采用明示同意。

2. 数据合理使用原则

数据合理使用原则也称必要原则,即应用人脸识别技术的服务提供者在收集和使用人脸信息时应考虑是否必要。^[8]在应用数据时,应在隐私侵权风险与为消费者带来的便利间取得平衡。还应针对特殊群体做出特殊规定,例如:儿童、明星等,为该群体提供更多的保护和更高的透明性。

3. 用户权利保障原则

用户权利保障原则分为透明原则和侵权救济原则,透明原则即服务提供者应将用户信息的收集、使用、储存情况明确告知用户,保持对用户个人的透明性,才能保障用户的权利。侵权救济原则是指,当用户的个人信息遭到侵犯时,能够及时得到帮助。专门法应就用户的救济方式作出具体规定,对服务提供者处以民事赔偿、行政处罚或刑事处罚。

（三）完善监督机制

目前,我国已在各部门法内设立了公民隐私权保护的条款,但是因为没有专门的监管主体和完善的监督机构,导致无法有效地保护公民的个人隐私权。因此,我国应该设立专门的监督机构,由精通人脸识别

的专业人员和法律人士来监督和管理公民的个人信息。并设立投诉举报的渠道,当公民发现其人脸信息被非法采集时,可通过该渠道向监督机构反映情况,以维护自身合法权益。

（四）提升公民隐私权保护意识

公民在使用应用人脸技术的软件或接受应用人脸技术的服务时,关注隐私权保护条例,阅读应用手册,加深对人脸识别技术的认识,以及了解面部信息的用处和储存安全等相关情况后再录入面部信息。并且,当面部信息受到侵犯后,向相关监管部门请求保护,及时冻结人脸信息,避免受到更大的损害。

近年来,人脸识别技术作为网络发展的新生领域,逐渐走进大众的视线,受到公众的广泛关注。这一技术在金融、安保、通行和机场安检等各个领域极大地提高了工作效率,无疑为人们的生活提供了巨大的便利。但其侵犯个人隐私和信息滥用等问题也随之暴露出来,引起了公众的担忧。但是,随着我国网络领域的不断革新和进步,人脸识别技术会朝着安全、高效的方向发展。总而言之,相信随着我国立法体系的逐渐发展、监督机制的完善和公民隐私权保护意识的不断提高,人脸识别技术必然不断向智能化、科技化、安全化高速发展,个人信息得到高效、合法、全面保护指日可待。

参考文献:

- [1] 霍妍,李长明.基于人脸识别考勤系统的设计与实现[J].通化师范学院学报,2016,37(12):1-3.
- [2] 吕玥媛.智能化公共视频监控下公民隐私权保护研究[D].北京:中国政法大学,2020.
- [3] 王利明.《人格权法研究》[M].北京:中国人民大学出版社,2005.599.
- [4] 林喆.《公民基本人权法律制度研究》[M].北京:北京大学出版社,2006:371.
- [5] 胡鹏鹏.大数据背景下个人生物识别信息的立法保护研究[J].信息安全研究,2020,6(09):798-806.
- [6] 毛亚楠.人脸识别第一案:告的是什么[J].方圆,2019(24):14-17.
- [7] 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,2020(5):21-29.
- [8] 刘啸宇.人脸识别技术的应用与隐私权保护[D].青岛:青岛大学,2020.

作者简介:

王宏杰(1999.5-),女,蒙古族,内蒙古自治区通辽市,硕士研究生,研究方向:行政法方向。