

论人脸信息删除权

周雨婷

烟台大学法学院, 山东 烟台

收稿日期: 2023年9月8日; 录用日期: 2023年10月7日; 发布日期: 2023年11月23日

摘要

人脸信息的收集有面向公众的收集和面向个体的收集, 但人脸信息收集的“告知-知情-同意”模式有其固有缺陷, 信息主体缺乏对重要情事的知悉, 也缺乏表意自由, 删除权的规定可以对其进行补正, 以真正保护个人信息权益。处理人脸信息欠缺合法性、正当性、必要性时, 信息处理者应当主动履行其删除义务, 对于面向个人的收集, 应当在人脸识别系统中嵌入自动删除设计或设计可让信息主体自行删除的选项, 人脸信息的删除应当和收集一样容易。对于面向公众收集的人脸信息, 在比对完成目的实现之后应当立即删除, 但也可基于社会管理需要留存一定期限, 在期限过后无其他事由的, 应当立即删除。通过诉讼方式行使人脸信息删除权有前置条件, 即已经向人脸信息处理者提出过删除申请。对于人脸信息, 其删除的方式首先应当是物理删除, 逻辑删除不应成为与物理删除的并列选项。

关键词

人脸信息, 删除权, 个人信息, 生物识别信息

On the Right to Delete Facial Information

Yuting Zhou

School of Law, Yantai University, Yantai Shandong

Received: Sep. 8th, 2023; accepted: Oct. 7th, 2023; published: Nov. 23rd, 2023

Abstract

The collection of facial information has public-facing collection and individual-oriented collection, but the “inform-know-consent” model of facial information collection has its inherent defects, the information subject lacks knowledge of important events, and lacks freedom of expression, and the provisions on the right to delete can be corrected to truly protect the rights and interests of personal information. When the processing of facial information lacks legality, legitimacy, or necessity, the information processor shall actively perform its obligation to delete, and for individu-

al-oriented collection, an automatic deletion design or option designed to allow the information subject to delete it on its own shall be embedded in the facial recognition system, and the deletion of facial information shall be as easy as collection. Facial information collected from the public shall be deleted immediately after the purpose of comparison is achieved, but it may also be retained for a certain period of time based on social management needs, and where there is no other reason after the time limit, it shall be deleted immediately. There are prerequisites for exercising the right to delete facial information through litigation, that is, an application for deletion has been submitted to the facial information processor. For face information, the first way to delete it should be physical deletion, and tombstone should not be a side-by-side option with physical deletion.

Keywords

Face Information, Right to Erasure, Personal Information, Biometric Information

Copyright © 2023 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

江苏省无锡市新吴区某健身房使用有人脸识别、指纹识别等功能的信息管理系统，强制要求会员刷脸或录入指纹进入。由于该系统采用分级分层、前后端分离等技术，消费者在前端平台仅能看到被采集的个人身份信息，未被告知个人信息收集清单及权限。在部分会员明确拒绝人脸采集识别后，该健身房擅自将会员办卡时提供的照片录入系统作为刷脸进出凭证，且在会员要求删除照片等信息时，以无管理权限为由拒绝删除¹。数字时代，人脸信息已经成为数字身份的主要识别方式，《个人信息保护法》第4条第2款与《民法典》第1035条第2款相比，关于个人信息处理范围的规定明显增加了“删除”这一处理方式，《个人信息保护法》第47条对个人信息删除权做出了更加具体的规定。但对于人脸信息的删除，其实现存在技术和实践上的困境，对于人脸信息删除权的性质与行使方式亦存在争议。从案例中可以看出，人脸信息收集的“告知-知情-同意”模式有其固有缺陷，信息主体缺乏对重要情事的知悉，也缺乏表意自由。删除权的规定可以对人脸信息“告知-知情-同意”收集规则的缺陷进行补正，以真正保护个人信息权益。对于人脸信息的删除规则，首先需要明确的是其权利义务主体，其次需要明确删除权的适用情形、行使方式及技术实现方式，个人信息删除权的构建可以在合理保护信息主体权益的基础上最大程度利用个人信息，推动经济的发展和社会的进步。

2. 人脸信息删除权的权利义务主体

“权利保护个人的某些利益，不同个体有自己的个人利益，如果他们希望，那这些个人有保护这些利益的权利。”随着记忆与遗忘的反转，大数据人工智能时代，人们愈发的需要被遗忘，以打破在时间和空间上的“数字化全景式监狱”[1]，法律应当赋予用户删除信息的权利，权利主体有权要求人脸信息处理者删除相关人脸信息，删除权为人们控制数据提供了一种新的方式。同时，为确保删除的彻底性，数据控制者还应当将包括在云计算上的一切后台数据一并删除。

¹ 最高人民法院：《最高检发布个人信息保护检察公益诉讼典型案例》之江苏省无锡市新吴区人民检察院督促保护服务场所消费者个人信息行政公益诉讼案，详见最高人民法院微信公众号：https://mp.weixin.qq.com/s/Q6W3JLuxB0K_o8CFfs1uQQ，最后访问日期：2023年4月6日。

2.1. 人脸信息删除权的权利主体

2.1.1. 一般主体

人脸信息删除权的权利主体是指作为自然人的具有身份可识别性²的信息主体。人脸信息属于个人生物识别信息,其不仅具有更高程度的可识别性,而且与自然人的身份不可分割,属于高度敏感的个人信息,由于其具有不可变更性且与身体属性不可分离、不可替代,其已经成为数字身份的主要识别方式[2],这也决定了人脸信息删除权的权利主体不可能是法人或其他组织³。

计算机、大数据和交互式数字媒体日渐普及,获取公民人脸识别信息的渠道和方式大大增加,致使“脆弱的个人”被置于受威胁的处境当中。人脸信息一旦被信息控制者泄露、非法提供或者滥用,对其个人名誉、财产与人身安全都影响甚巨。不仅会使受害人的人格尊严遭受严重的侵害,数据化的个人生物特征还可被永久性使用,造成不可逆的损害[3]。人脸信息属于肖像的类型之一,通过电子数据的方式使肖像再现自然人的相貌特征,并且具有极高的准确性。如果行为人利用信息技术伪造并非法使用他人的人脸信息,既侵害受害人的肖像权,又侵害了受害人的生物识别信息权益,而且还有可能侵害他人的名誉权。例如通过AI换脸技术将人脸信息剪辑接入淫秽视频,降低受害人的社会评价,侵害其名誉权。被窃取的面部信息与被侵权人的其他信息相结合,则将会对被侵权人造成更大的困扰,如在互联网上的身份被盗窃。因此,规范人脸识别技术,让人脸信息合法合规使用,是大数据时代背景下保障个人信息安全和隐私安全的重要方面。为了保护信息主体的人脸信息,应当赋予其可以随时行使更正、删除和注销的权利,并且无需任何前置条件即可当场实现并即时生效,以保障个人生物识别信息安全。诚如欧盟委员会(European Commission)前副主席雷丁女士所表示的,“人们必须在他们不想要使用他们的个人数据时,能够轻易地把这些数据转移给另一个网络或服务提供者或者删除这些数据……我想明确澄清,人们是有这么做的‘权利’,而不是有这么做的‘可能性’”。存储成本的低廉化、信息蕴含的分析价值的上涨,信息控制者在看到其背后的价值潜力的同时,也助长了他们进一步对个人信息的采集、存储和利用的野心,而删除权正是个人对抗强大信息控制者的法律手段。

相较于防御属性的隐私权,个人信息致力于实现信息主体对其个人信息的积极控制,个人信息是一种控制权,并且随着信息技术、新型判例和立法的与时俱进,其控制方式不断增多⁴。《德国联邦数据保护法》第20条规定了删除权,《通用数据保护条例》GDPR第17条规定了被遗忘权[4]。《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》(以下简称“解释”)于2021年8月1日正式生效,在借鉴国外相关立法的基础上,“解释”第十二条作出了与欧盟GDPR类似的规定,赋予自然人对人脸信息的“删除权”,自然人在信息处理者违反约定处理人脸信息时可行使。信息主体删除权是基于个人信息权益的一项法定权利,信息主体行使删除权不以信息主体与信息处理者是否就删除权进行约定为前提。只要信息处理者违反约定处理个人信息的,信息主体即有权要求其删除个人信息。当然,若信息处理者同时存在个人信息保护法规定的其他应当删除个人信息的情形,信

²可通过“姓名、性别、身份证号、定位地址、专属标识符”等信息主体进行准确识别。

³2013年7月修改后的《俄罗斯联邦民法典》在其第1521条第3款关于保护公民肖像的条款中,规定了肖像权人的删除权,原文为“如果违反本条第一款取得或者使用的公民的肖像在互联网上被传播,则公民有权要求删除该肖像,以及制止或者禁止进一步传播”。参见张建文:《俄罗斯民法典现代化中的非物质利益制度变革》,载《学术交流》2016年第9期,第71页。

⁴典型案例有“德国人口普查案”:德国1983年实施的《联邦人口普查法》规定政府可以对公民进行信息调查,其内容包括人口、住址、职业、教育经历、工作场所等15个方面的信息需要全面登记,德国依据《基本法》第2条第1款和第1条第1款关于一般人格权包含的现代化数据处理情况下,对个人信息不能无限制地调查、收集、处理和传递,据此创设了“信息自主权”,个人应该有权决定其私人生活是否公开、公开到何种程度以及公开的时间与方式。参见陈戈、柳建龙等:《德国联邦宪法法院典型判例研究:基础权利篇》,法律出版社2015年版,第44~46页。“雷巴赫士兵案”:三名士兵因抢劫德国雷巴赫镇的弹药库被捕入狱,某电视台推出《雷巴赫士兵谋杀案》的记录片,详细介绍了犯罪全过程,以及侦查、审查、起诉、审判全过程,还包含三名士兵的同性恋情、姓名、肖像。其中一名士兵出狱后向法院提起诉讼,主张电视台侵犯其一般人格权并要求禁播该记录片,宪法法院认为电视台在披露他人信息时没有遵循“最少够用原则”,毫无限制的报道、持续性的曝光不利于服刑完毕的士兵回归正常生活。参见前书第76页。另外还有“谷歌诉网萨雷斯案”以及我国的被遗忘权第一案“任某与百度公司人格权纠纷案”等。

息处理者亦应删除个人信息，信息主体也有权要求其删除人脸信息。对于人脸信息删除权，其仅为信息主体所享有，不得转让。

2.1.2. 特殊主体：未成年人的人脸信息删除权

未成年人，明确规定为不满十八周岁的我国公民，对于不满十四周岁的未成年人的个人信息要给予重点保护。对于未成年人，由于其心智不成熟，出于对其人脸信息的保护，原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别，收集未成年人的人脸信息。当下大量的手机 App (如短视频、直播及游戏类)的主要用户群体为未成年人，而不少应用软件以身份认证为由要求进行人脸识别。但未成年人由于其身心发育特点，对人脸识别的风险缺乏必要的认知和警惕性，甚至由于好奇心驱使而轻易向平台提供其人脸信息，这些信息如被擅自分析、泄漏或被盗用，可能对其未来一生的成长产生不利影响，导致其成为一些犯罪行为(如绑架拐骗)的受害对象。因此，对未成年人的个人信息特别是敏感信息给予特别保护，这是全世界的普遍做法。就我国而言，《个人信息保护法》第 28 条规定“不满十四周岁未成年人的个人信息属于敏感个人信息”；《个人信息保护法》第 31 条和《未成年人保护法》第 72 条规定“个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意”⁵。

“解释”第 3 条也特别规定：人民法院认定信息处理者承担侵害自然人人格权益的民事责任，应考虑受害人是否为未成年人这一重要因素。基于这些立法精神和法律规则，原则上应禁止对不满十四周岁的未成年人进行人脸识别。如基于公共安全(如校园安全)等原因确需对未成年人进行人脸识别，应征得未成年人的父母或者其他监护人的明确同意，经公安部门及履行个人信息保护职责的主管部门批准，并应采取严格的信息安全保护措施[5]。当未成人的父母或监护人提出人脸信息的删除申请时，应当立即删除。

2.2. 人脸信息删除权的义务主体

2.2.1. 私人机构

江苏省无锡市新吴区某健身房使用有人脸识别、指纹识别等功能的信息管理系统，强制要求会员刷脸或录入指纹进入。由于该系统采用分级分层、前后端分离等技术，消费者在前端平台仅能看到被采集的个人身份信息，未被告知个人信息收集清单及权限。在部分会员明确拒绝人脸采集识别后，该健身房擅自将会员办卡时提供的照片录入系统作为刷脸进出凭证，且在会员要求删除照片等信息时，以无管理权限为由拒绝删除。数字时代，人脸信息已经成为数字身份的主要识别方式，《个人信息保护法》第 4 条第 2 款与《民法典》第 1035 条第 2 款相比，关于个人信息处理范围的规定明显增加了“删除”这一处理方式，《个人信息保护法》第 47 条对个人信息删除权做出了更加具体的规定。但对于人脸信息的删除，其实现存在技术和实践上的困境，对于人脸信息删除权的性质与行使方式亦存在争议。从案例中可以看出，人脸信息收集的“告知-知情-同意”模式有其固有缺陷，信息主体缺乏对重要情事的知悉，也缺乏表意自由。删除权的规定可以对人脸信息“告知-知情-同意”收集规则的缺陷进行补正，以真正保护个人信息权益。对于人脸信息的删除规则，首先需要明确的是其权利义务主体，其次需要明确删除权的适用情形、行使方式及技术实现方式，个人信息删除权的构建可以在合理保护信息主体权益的基础上最大程度利用个人信息，推动经济的发展和社会的进步。

a) 人脸信息处理者

人脸信息删除的义务主体之一为人脸信息处理者，即自主决定处理目的、处理方式的组织、个人⁶。

⁵美国的《儿童网上隐私保护法》中规定，运营者必须做出“合理的努力”确保父母收到网站或在线服务提供商发出的采集其孩子个人信息的通知，同时相对地规定了父母授予同意和撤回同意的方式。

⁶欧盟于 1995 年出台的《欧盟数据保护指令》第 2 条明确规定：“信息控制者，是指能够单独或与他人共同决定处理个人信息的方法和目的，并对保管和使用这些信息负责的自然人、法人或公共机构；信息处理者，是指代表控制者处理数据的自然人、法人或公共机构。” See Directive 95/46/EC at Art 2.

一般情况下,信息收集者和信息处理者是同一主体,当信息收集者和信息处理者并非同一主体时,信息主体可以向信息收集者提出删除人脸信息的要求,此时信息收集者应当向信息处理者转达删除意愿。信息收集者在收集时也应明确告知信息处理方相关具体信息,其不得以未控制使用信息为由拒绝删除。

如果信息处理者是共同处理者,即两个或两个以上的个人信息处理者共同决定处理目的、方式的组织或个人,那么其中任意一个处理者都有删除义务;如果存在合并、分离等情形,负责接受并控制该信息的信息处理者负有删除的义务。

b) 第三方运营商

2022年6月,美国发布首次获得两党两院支持的《美国数据隐私和保护法案》(American Data Privacy and Protection Act, ADPPA)草案。该草案弥补了美国缺少联邦立法规制数据保护的空白。草案在“个人数据所有权和控制权”部分规定了有关数据的删除权为“一对多”模式,区别于传统删除权“一对一”模式,信息控制主体在收到个人删除的请求时,应当在验证之后向信息主体提供删除的权利,且该权利及于第三方服务商[6]。为实现产品和服务的核心功能,满足客户需求,平台与其相关联的公司或者合作第三方存在广泛的数据共享,除一般个人信息之外,还包括面部识别信息等敏感个人信息。平台将信息共享第三方的内容放置隐私政策文本中,经用户同意后,将其个人信息共享给第三方运营商。当人脸信息主体向原收集主体请求删除人脸信息时,第三方处理人脸信息的合法性基础亦不存在,因此,应当将第三方运营商纳入人脸信息删除的义务主体。在“已获得个人独立授权”的情形下,人脸信息主体在向原平台提出删除请求时,无须负有通知第三方删除的义务。原收集主体应当进行通知并采取相应措施,或者在共享人脸信息等敏感个人信息时只提供使用接口,第三方运营商并不能实际获取人脸信息相关数据,只能通过接口进行使用,获得相应的比对结果。此时原收集主体收到删除人脸信息的申请后,第三方运营商才无相关删除义务。

2.2.2. 公共机构

只要公共机构是以自动化方式收集和存储、处理个人信息的,就应当受到个人信息保护法的约束。由于其在收集和處理个人信息方面比一般私人机构更具权威性,信息主体面对公共机构时通常也愿意提供更全面、具体和隐私程度更高的个人信息,在责任追究上也应比私人机构更为严格。公共机构在提供服务过程中应审慎收集自然人的人脸信息,当服务目的已实现或不再必要时,应当主动删除收集的相关人脸信息,此应为数字政府建设的应有之义。

3. 人脸信息删除权的适用情形

当出现《个人信息保护法》第47条规定的内容时,处理人脸信息欠缺合法性、正当性、必要性时,信息处理者应当主动履行其删除义务,这表明我国对个人信息处理采取的是客观决定说,即只要人脸信息的处理不再“合法、正当、必要”时,就应当删除人脸信息,但判定标准需要以个案平衡为基础进行协调[7]。一项权利,要防止其被滥用或者误用,就需要对其适用范围进行界定,人脸信息的删除权不是一项绝对的权利,在若干特定情形下才能行使删除权。

3.1. 人脸信息处理不再合法

当对人脸信息的处理不再合法的时候,信息处理者应当删除人脸信息。判断人脸信息处理行为是否符合法律规定时,主要是从目的、行为、事由三个层面进行考察判断。

目的合法是信息处理的前提,不得为了诈骗、非法交易等目的收集、处理人脸信息,或是用他人面部数据制作3D模型或面具,伪造篡改他人在线身份,基于非法目的处理人脸信息危及到现实的人身或财产权利的时候,甚至已经跳出个人信息保护法保障信息流通与利用的范围,归入刑法的调整范围了。

行为合法是对人脸信息从收集环节的告知义务的履行、安全保障措施的实施、重要情势的报告等全生命周期中处理行为合法性的判断,处理行为不合法合规的,应当立即停止非法处理活动,并删除人脸信息[8]。

在事由合法性上,《个人信息保护法》第13条⁷列举了7类合法性事由,针对人脸信息具体而言,可以分为三大类,其中第一条第一项可以概括为取得信息主体同意类合法事由,第一条第六项概括为处理自行公开或合法公开个人信息类合法事由,其余剩下五类归为其他类合法事由。如果信息处理者未取得人脸信息主体的同意,也不存在其他类合法事由的,其构成“违反法律、行政法规处理个人信息”,此时应当删除人脸信息。此处的其他类合法事由应当将处理自行公开和合法公开类个人信息的合法事由排除在外,因为进入大数据互联网时代,人们在社交媒体上自主公开含有人脸图像的照片或者视频变得极为普遍,人脸信息属于敏感个人信息,即使其自行公开了人脸图像或视频,不能够当然的认为任何人都可以使用人脸识别技术收集、处理其人脸信息。获得信息主体同意处理人脸信息的,个人有权撤回同意。GDPR第7条第3款规定了信息主体有权随时撤回同意,但同意之撤回并不影响信息处理者在撤回同意之前相关处理行为的合法性。同意撤回的做出应当和做出同意一样简单⁸。当撤回同意又不具有其他类合法事由时,信息处理者丧失处理权,无继续处理的合法性事由。对于其他普通类个人信息,信息主体撤回同意的同时可以要求一同删除相关个人信息,也可以不删除只撤回同意,意味着其不能再继续收集相关个人信息,对于之前的个人信息,可以视情况决定删除或是停止除存储和采取必要安全保护措施之外的处理。对于人脸信息而言,通常情况下应当认为人脸信息主体撤回同意的,信息处理者应当删除存储的人脸信息。

对于人脸信息处理不合法的,信息处理者除停止非法处理活动、删除人脸信息外,还需要承担相应的法律责任(行政责任或刑事责任),其责任承担不因其已经删除人脸信息而豁免。

3.2. 人脸信息处理不再正当

人脸信息处理的正当性分为行使目的的正当性和手段的正当性。在人脸信息收集阶段,其收集原则之一就为目的正当性,目的应当在不迟于收集人脸信息时确定下来,应当禁止为满足商业目的通过搜集公开的人脸图像或者视频的方式间接获取人脸信息。目的正当性都需要结合具体情形进行分析,在“人脸识别第一案”中,动物园将收集的人脸照片用于辅助“指纹识别入园”变更为“人脸识别入园”,属于典型的处理目的和处理范围违约,除收集时指明的目的外,人脸信息处理者不具有继续保存信息的理由,此时,动物园应当删除之前收集的人脸信息。

手段的正当性则是指人脸信息收集时的方式,是否完整履行告知义务、人脸识别摄像头的安置是否清晰可见并设置显著提示标语、人脸识别过程中是否存在其实与不公平现象。

GDPR第17条第3款规定了被遗忘权适用的例外情形:如基于信息表达自由或诸如健康问题、科学研究、司法程序、法律规定等社会公共利益或因历史重要意义上升而具有社会关注价值,这些具有目的正当性而需要保留相关数据时,数据控制者可无须删除这些数据。放眼世界,欧美在对待删除权时选择了不同的价值路径,这也是数字环境治理语境下数据保守主义与激进主义的对抗,欧盟以人格尊严为核

⁷《个人信息保护法》第十三条:“符合下列情形之一的,个人信息处理者方可处理个人信息:(一)取得个人同意的;(二)为订立、履行个人作为一方当事人的合同所必需,或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;(三)为履行法定职责所必需;(四)为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;(五)为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息;(六)依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;(七)法律、行政法规规定的其它情形。依照本法其他有关规定,处理个人信息应当取得个人同意,但是有前款第二项至第七项规定情形的,不需取得个人同意。”

⁸GDPR Article 7(3): “The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.”

心价值取向,对删除权行使不断深入细化以打破“数字圆形监狱”的桎梏[9],但因此也加大了企业合规成本,与公众知情权出现矛盾冲突。而美国对言论自由的追求与行业自律,反对数据过度限制以影响自由贸易,因此对删除权普遍持质疑态度。但这也很容易使许多大型企业演变成“数据巨型机器”,逐步消解人权[10]。为此,我们应当在借鉴欧美立法的基础上探索一种温和的行使路径,实现数据开发利用与数据主体权益的平衡。对于人脸信息,其主要删除权例外情形主要在人脸识别算法训练权上。在众多权利中,权利能否受限制、应否被其他的权益所压倒,首先取决于有没有高于权利的价值,以及能否援引那些可能高于权利的价值来压倒权利。我国互联网、人工智能等新技术发展势头正猛,已经成为提升中国国家话语权、文化软实力的重要传播途径,对互联网信息技术行业也有许多鼓励支持政策,删除权在某种程度上阻碍数据流通,不利于互联网发展,我国在删除权的设计上不应照搬照抄国外经验,而是应当结合我国大数据时代经济发展水平进行设计。针对人脸识别系统存在的识别精度不够,可能在识别时出现混淆等问题⁹,解决的方法之一就是通过对大量的人脸信息进行算法训练,以不断提升人脸识别的准确度。而这其中,就需要人脸信息作为人脸识别算法训练的素材。对于人脸信息删除权,人脸识别系统开发者可否以算法训练为理由,在删除个人身份识别信息的前提下,保留相关脸纹数据以供算法训练。本文对此持否定意见,并认为人脸识别系统开发者应当向人脸信息识别数据库购买相关数据库使用权限,以进行算法训练。

3.3. 人脸信息处理不再必要

当人脸信息处理不再必要时,信息处理者应当主动删除人脸信息。必要性要求人脸信息的处理是最少且必要的,最少包括人脸信息提取的内容少和人脸信息的存储期限少,保存期限控制在为实现处理目的所必须的最少时间即可。必要性要求离开人脸信息的处理,就无法实现相关处理目的或服务。

《个人信息保护法》第47条第1款第1项规定:“处理目的已实现、无法实现或为实现处理目的不再必要的”,信息处理者应当删除人脸信息。比如消费者在购买健身服务的时候,双方约定通过人脸识别方式进行健身打卡,但是在合同履行过程中,双方取消打卡制度或者变更打卡方式,此时个人信息处理者就应当删除之前收集的人脸信息。又比如人民法院通过法院官网或者微信公众号披露失信人员名单时,会附上失信人员的人脸图像,在失信人员主动履行生效法律文书所确定的义务后,人民法院应当主动删除相关案件信息和人脸图像,因为此时督促失信人员自动履行生效法律文书确定的义务的目的已经完成¹⁰。但本条依然存在模糊性,目的的实现怎么判断?有赖于学理上进一步的研究和立法、司法实践上的探索,依据人脸信息处理的具体场景进行判断。第47条第1款第2项前半句规定当停止提供产品或服务的,应当删除人脸信息。比如疫情期间由于管控需要小区安装了人脸识别入门装置,在后疫情时代人脸识别装置已停止运营时,之前收集的人脸信息就应当删除。但实践中停止提供产品或服务的,尽管法律或者相关隐私政策中有相关删除条款,信息处理者也未必能真正落实,以睿视App为例,其隐私政策提到停止运营后将通知用户,将对其用户个人信息进行删除或匿名化处理,但在小区停止人脸识别后,用户从睿视App上仍然可以看到最初因疫情防控录入的人脸图像。

对于存储期限,应为实现处理目的所必需的最少时间。法律、行政法规有规定的,以法定保存期限为准,不得通过另行约定延长保存期限。保存期限的长短与泄露和滥用的风险成正比,没有规定的按照约定,但不得长于实现处理目的所需的最短期限。对于公共场所的视频监控,如果没有理由保留录像(如没有犯罪发生时),视频监控设备通常会将以前的录像在一段时间后删除;在使用人脸识别技术时,一旦

⁹ 比如面部特征之间的间隔距离会随着相机到拍摄对象的距离而变化。See Eilidh Noyes *et al.* Camera-to-subject distance affects face configuration and perceived identity, *Cognition* (2017). <https://techxplore.com/news/2020-02-huge-flaw-anthropometry-facial-features.html>

¹⁰ 重庆市永川区人民法院:《“失信曝光”失信寸步难行,请立即履行!》,详见重庆市永川区人民法院微信公众号:<https://mp.weixin.qq.com/s/FClnkqUpog09ZXZYaxvcsQ>,最后访问日期:2023年5月25日。

确定某个人的面部数据特征与数据库中的任何特征不匹配,就会被立即删除,其存储期限在结果出来之时为最长期限。

4. 人脸信息删除权的行使方式

在删除权的行使方式上,各地法院没有形成一致的司法适用思路。当信息主体的人脸信息被收集后,存储在企业内部的数据库中时,企业对数据的修改、删除具有隐蔽性,信息所有者和信息保存者处于不平等地位,企业对人脸信息的后续处理很难被外界知晓。因此,要保障人脸信息主体的删除权,其查阅权是删除权得以行使的前提。个人信息删除权的性质将影响其行使方式,对于个人信息删除权的性质,有学者认为其属于个人信息的一项权能,是人格权请求权的体现,其是基于人格权益产生的权利[11];有学者认为删除权应当被纳入个人信息权之中,不以定性为人格权[12];有学者持完全不同的观点,其认为删除权不是人格权请求权的组成成分,也并非救济性、防御性的权利,而是一种依附于个人信息处理行为,随之产生的附触发条件的程序性权利,其以信息处理者未主动履行其删除义务为触发要件[13]。本文对删除权为程序性权利持赞同意见,人脸信息删除权的行使方式可以分为三类,即信息处理者主动删除,信息主体申请删除和诉讼删除,其中,诉讼删除又可分为民事诉讼和公益诉讼两类诉讼方式。

4.1. 主动删除

当人脸信息处理行为不再合法、正当、必要时,人脸信息处理者应当主动删除满足删除条件的人脸信息。主动删除可以通过两种方式实现,一是人脸信息处理者设置了专门的审查机构,对相关信息进行审查后发现需要删除的进行删除;一种是经过系统设计的自动保护程序,在人脸信息处理系统设计之初,就在系统中嵌入删除的触发要件,如在收集人脸信息一定期限之后,或者人脸信息主体于系统界面提交删除申请时等,在满足删除触发要件时将自动删除。经过设计的隐私保护可以从源头解决人脸信息处理者信息删除不及时的问题,避免信息的泄露。舍恩伯格在其书中建议系统设置信息的有效期限,在信息存储期限到期后自动删除系统所存储的信息,一次保证信息主体可以在事前采取措施来行使他们的被遗忘权:在收集、存储或者分享之前,不用再担心没有他们的同意这些信息将会永远留存[14],这样的设置也可以减少删除权操作时的管理压力。但是,如何执行这些强制设备、需要投入的成本、具体执行的监管情况都需要信息控制者、系统设计者和政府进行协商、合作。

阿根廷议会 2000 年 10 月通过的《综合数据保护法》,对公共和私人的数据库如何收集、处理个人信息进行了规范。其认为当数据满足删除条件的时候属于“应当”删除而非“可以”,采取的是强制遗忘的态度,以删除为原则,以保留为例外。阿根廷该通过《知识产权法》来保护公民的肖像权,以当事人狭义上的同意为前提,未经同意授权的前提下,个人有权要求删除在网页上不当展示的肖像,除非是基于公共利益。

4.2. 申请删除

在申请删除的实现方式上,主要论述的为人脸信息处理者在面对信息主体行使删除权的过程中应当履行的保障义务。

其一,建立删除权申请通道的义务,设置“橡皮擦按钮”。人脸识别技术中应当着重强调保障用户利益,以用户的利益为出发点,为保障信息主体删除权的实现,人脸识别应用系统应在设计初期将上述的用户权利写入系统中,通过调整移动端应用的功能设置,建立长效、畅通的删除权申请通道,为个人信息主体提供更明确、更好操作的信息删除或注销方式。信息主体通过点击、上传等步骤与信息处理者良好沟通,避免人脸信息主体删除无门的情况出现。例如谷歌公司在“谷歌西班牙公司案”尘埃落定后

出台了在线申请程序，正式接受欧盟用户的被遗忘权申请。

其二，解释说明义务。人脸信息处理者应当清楚地解释说明信息主体如何删除相关人脸信息，标识详细步骤与流程。

其三，对删除申请的审查义务。对于人脸信息的删除请求，是否需要审查？需要。一是要看申请删除的主体是否为人脸信息主体，而是看是否符合删除权的适用情形，比如通过合同约定对人脸信息的收集，还不满足删除的条件下。三是未成年人的人脸信息的识别¹¹。人脸信息处理者应当通过程序设置或者设置专门负责人对删除权进行审查，以确保删除目的高效、及时的实现[15]。

其四，删除、披露与通知义务。删除义务是指在收到人脸信息主体提出删除申请后，通过审查具体条件和相关证据，最终作出删除人脸信息的决定。披露义务具体指对人脸信息主体删除权的申请进行审查并作出肯定或否定的评价，并将决定内容及理由一并披露给信息主体的行为。简言之，披露义务的对象为信息主体，内容是审查决定及理由，在此披露的内容可以作为之后起诉的依据。通知义务是指人脸信息处理者在接到删除的申请时，应当将此申请同步告知第三方运营者，在“已获得个人独立授权”的情形下，人脸信息主体在向原平台提出删除请求时，才无须负有通知第三方删除的义务¹²。

4.3. 诉讼删除

4.3.1. 民事诉讼

在个人信息保护纠纷案件中的请求权有两类，分别是《个人信息保护法》第 50 条第 2 款、第 69 条，针对侵害个人信息权益造成损害和侵害个人在个人信息处理活动中的权利的两种不同情形，分别构建两种不同的请求权基础。其中，第 69 条规定的请求权基础是个人信息处理者的信息处理行为侵害当事人的个人信息本权(或原权)权益且造成损害的情况下，当事人可基于侵权责任的请求权基础，向个人信息处理者请求损害赔偿等侵权责任。第 50 条规定¹³，侵害当事人在信息处理活动中的程序性权利、保护性权利，当事人提起诉讼的，人民法院应予救济的构成要件为：其一为当事人行使程序性、保护性权利具有法定或者约定的事由；其二，当事人向个人信息处理者提出了有效的程序性、保护性权利的请求；其三，个人信息处理者无正当理由拒绝当事人行使程序性、保护性权利，或对当事人提出的请求不予理睬。

何为当事人向个人信息处理者提出了有效的删除申请？此时需要区分不同情形予以细化。一是个人信息处理者未建立便捷的个人行使权利的请求受理和处理机制的，可视为个人信息处理者对当事人提出的请求不予理睬；二是个人信息处理者建立有便捷的个人行使权利的请求受理和处理机制，当事人未按请求受理方式提交申请，不应当认定当事人向个人信息处理者提出了有效的权利请求，但个人信息处理者接收并明确表示拒绝的除外。那何又为便捷的个人行使权利的请求受理机制？首先，受理个人行使权利的请求机制，是指个人信息处理者在个人信息处理活动中，对外建立的接收个人行使权利的渠道、通道、途径；其次，便捷的请求受理机制，是指个人信息处理者建立的接收申请的渠道应当位置显著、易于查找，且使用方便、快捷，没有设置不合理的障碍。一般而言，对于采用交互式页面提供产品或服务的，宜直接设置操作简单的交互式页面接受申请。同时，也鼓励并行采用人工客服电话、电子邮箱等多种途径接受申请。当事人向个人信息处理者提出了有效的删除申请但遭到拒绝或不被理睬时，人脸信息主体可以向原告所在地提起民事诉讼[16]。

¹¹关于未成年人的识别标准，应以时间发生节点为准，而非提交删除请求的时间。这也是《第 29 条信息保护工作组指引》关于未成年人倾斜保护的精神体现。

¹²GDPR 第 17 条第 2 款规定，数据控制者不仅要删除他们网站上所控制的这些信息，而且还必须采取“一切合理措施，包括技术性手段，通知正在处理这些数据的第三方，数据主体要求其删除关于这些数据的任何链接、副本或复制。”

¹³《个人信息保护法》第 50 条：“个人信息处理者应当建立便捷的个人行使权利的请求受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。”

4.3.2. 公益诉讼

虽然人脸信息删除权的行使以《个人信息保护法》为核心,但是并不意味可以忽视公法领域中对个人信息保护的机关的作用。2021年11月1日个人信息保护法正式实施,明确规定检察机关可以提起个人信息保护领域公益诉讼¹⁴。在2023年3月最高人民检察院发布的八件个人信息保护检察公益诉讼典型案例中,其中三件均是检察机关通过公益诉讼的形式行使人脸信息删权,覆盖领域分别涉及健身房、超市等公共服务场所、医疗卫生机构等公益事业单位及旅游景区等营运企业。用户(信息主体)与平台(人脸信息处理者)地位不平等导致信息收集的知情同意原则失灵,其体现在对相关技术的掌握与了解、举证能力、免费使用等方面,人脸信息主体的私益诉讼能力弱,因此可通过民事公益诉讼,由法律规定的机关和有关组织以及检察机关补足人脸信息主体的诉讼能力,使其与平台处于平等地位,以保障知情同意原则有效贯彻落实。

对于公共服务场所面向不特定多数人采集人脸信息的,其采集信息量大、面广、敏感度高,个人也很难提起申请要求删除人脸信息,如果监管不到位,将危害众多消费者人身、财产安全。则需要检察机关发挥公益诉讼检察职能,推动公共服务场所规范收集、处理、删除人脸信息,加强数据安全管控。

对于公益事业单位,例如在湖南省长沙市望城区人民检察院督促保护个人生物识别信息案中,为推进数字化门诊建设,疫苗受种人或监护人在点击疫苗接种告知书的“同意”时系统会自动收集人脸识别信息,检察机关在接群众举报并充分调研后发出行政公益诉讼诉前检察建议,督促行政机关对过度收集的人脸信息数据采取“备份封存+本地彻底删除+到期彻底删除”的方式消除安全风险。

对于旅游景区等营运企业,单个游客消费者提起申请删除人脸信息并不能解决普遍问题,检察机关可通过一体化办案优势,督促行政机关加强监管,促使信息处理者依法整改,建立合规体系,实现办案效果最优化。

4.4. 适用顺位

对于信息主体对其人脸信息的删除权的主张程序,一直存有争议。有观点认为权利主体可以直接向法院提起诉讼,以实现删除权的司法保护;部分观点认为如果赋予信息主体直接诉讼的权利,会导致法院涌入大量诉讼,造成司法资源更加紧缺。《民法典》中对此问题并无明确表述,《个人信息保护法》第47条规定了信息处理者应该主动删除符合删除条件的信息;信息处理者未删除的,个人有权请求删除,对是否以向信息处理者主张删除或其他程序作为诉讼前置条件仍未明确,需要在实践中进一步总结经验^[17],本文对此持赞同意见,即人脸信息删除权的行使有适用顺位,人脸信息主体提起民事诉讼的前提是向信息处理者提出了有效的申请删除,且删除请求被无理由拒绝或在合理期限内未予以回应时。卢西亚诺·弗洛里迪教授认为,对于被遗忘权,主体必须首先向出版者提起申请,只有申请失败了才能向搜索引擎提请删除链接;若仍然失败,才能向国家数据保护局或司法机关请求帮助;最后才可以向欧盟法院请求。俄罗斯于2015年修改2016年1月1日正式生效的《信息、信息技术和信息保护法》第103条第7款规定,申请人在删除的请求被拒绝的情况下有权诉至法院¹⁵。

清华法学院《〈最高人民法院关于审理个人信息纠纷民事案件适用法律若干问题的解释〉学者建议稿》第十八条关于删除权的行使方式,其建议内容为对于个人信息处理者违反法律、行政法规的规定或者违反约定处理人脸信息的,个人信息主体有权直接向人民法院提起诉讼。对于其他应当删除,而个人

¹⁴2022年,全国检察机关共办理个人信息保护公益诉讼案件6000余件。最高人民检察院:《最高检发布个人信息保护检察公益诉讼典型案例》,详见最高人民检察院微信公众号:https://mp.weixin.qq.com/s/Q6W3JLuxB0K_o8CFfs1uQQ,最后访问日期:2023年7月16日。

¹⁵俄罗斯《信息、信息技术和信息保护法》第103条第7款:“认为搜索系统管理者的拒绝缺乏理由的申请人,有权向法院起诉要求终止提供对申请人请求中指明的信息的链接。”

信息处理者未主动删除的,人脸信息主体应当先向信息处理者提出请求,被拒绝后才能提起诉讼¹⁶。

5. 人脸信息删除权的技术实现方式

在大数据时代的被遗忘权的构建的基础内容就是删除。要实现删除人脸信息的目的,首先需要明确人脸信息删除权的范围,其次应明确人脸信息的删除存在技术上的难题的时候,逻辑删除的技术实现方式是否可以应用与人脸信息此类高度敏感的个人信息中。

5.1. 人脸信息删除权的范围

在“人脸信息”的具体定义方面,“解释”并未进一步给出说明。也就是说,如自然人要求信息处理者删除个人人脸信息,究竟那些人脸信息属于需要被删除的范围?是否自然人提供的人脸信息和人脸识别技术生成的人脸信息都要删除?我们可以从人脸识别技术的角度出发,对人脸信息进行分类。

人脸识别技术的主要原理就是通过扫描原始人脸信息(可以是真实人脸或清晰的人脸照片),人脸识别软件能够探测并分离出被摄像头捕捉到的人脸信息,并使用算法分析和提取可识别的人脸特征点[18]。将其中 20~40 或者更多个人脸特征信息(如鼻子到嘴唇之间的距离等)转化为脸纹集合数据并作为样本存储起来。人脸测算法提取人脸特征数据,并将这些数据转化为计算机可识别数据,最终存储在数据库中的脸纹数据被称为“脸纹数据”。通俗来说,通过算法对人脸图像的提取和转化,脸纹数据已经是可供计算机直接读取和计算的几何向量以及字符串了。因此,我们可以对人脸信息进行如下分类:①“原始人脸数据”:由特定自然人单独同意提供给个人信息处理者的“原始人脸数据”,主要包括人脸图像和视频;②“脸纹数据”:个人信息处理者利用人脸识别技术加工原始人脸数据产生的脸纹数据,主要包括供计算机进行运算的向量和字符串;③“身份识别信息”:通常是指提供原始人脸数据的特定自然人的身份识别信息,例如自然人姓名等能够直接识别特定自然人身份的信息。

对于原始人脸数据和身份识别信息属于删除的范围并无多大争议,但是对于只能由计算机才能识别的“脸纹数据”是否属于删除权涵盖的范围存在疑虑。因为其可能与人工智能算法的算法训练的权利之间存在一定冲突。人脸识别技术要提升精确度就需要大量的人脸信息进行算法训练,或者出于一些科学研究的需要可以不删除脸纹数据。对于身份识别信息,如果录入人脸信息属于附加功能,在行使人脸信息删除权的时候可以不对身份识别信息进行删除。否则应当一同删除,因为单纯的人脸图像或视频或“脸纹数据”如果没有姓名等其他身份识别信息,其对自然人的人身、财产权利很难造成实质影响[19]。对于原始人脸数据,处于信息安全保障的需求,在存储时就不应当进行存储,如果收集了原始人脸数据未删除的,应当删除。

5.2. 逻辑删除(相对删除)

逻辑删除,是指使用状态符对该电子信息进行不可用标记,使标记后的电子信息不被前端系统检索到,当该信息仍然存在于后端数据库当中,在一定权限下仍可直接识别和使用。对于“删除”的界定法律上未有定论,鉴于当前技术水平的限制与删除成本的考量,应当从解释论上对“删除”进行扩张解释,将逻辑删除纳入“删除”的含义之中,以实现成本和效益的均衡。除非信息主体愿意支付删除的成本。

《信息安全技术-个人信息安全规范》(GB/T35273-2020) 3.10 将“删除”定义为在实现日常业务功能所涉及的系统中去除个人信息的行为,“使其保持不可被检索、访问的状态”。《信息安全技术、公共及商用服务信息系统个人信息保护指南》中 5.1(d)中将“删除”规定为“在信息系统中不可再用”,该款定

¹⁶ 参见中国法律评论:清华法学院《〈最高人民法院关于审理个人信息纠纷民事案件适用法律若干问题的解释〉学者建议稿》第十八条关于删除权的内容。详见中国法律评论微信公众号:<https://mp.weixin.qq.com/s/k4mVJy4OaRjqVs9GO6LCA>。最后访问日期:2023年7月19日。

义更符合删除权的立法目的。

当面对人脸信息此类敏感个人信息时,匿名化处理¹⁷是否可以作为“删除”的替代履行有待验证。可识别性是个人信息发挥分析价值的关键点,当经过匿名化处理的人脸信息无法指向特定对象或者不与特定对象相联结时,其分析价值则会大大减弱。人脸信息的分析利用价值与其可识别性成正相关,但匿名化处理过程中仍会保留部分识别因子,以保留匿名化处理后个人信息的价值。因此,匿名化处理后的数据仍有被再次识别的风险,匿名化只是相对的。若想让匿名化处理成为“删除”的替代方案之一,则需要再添加相关处理限制。

5.3. 物理删除

物理删除,是指当符合人脸信息删除条件时,信息控制者应当主动删除相关原始人脸数据、脸纹数据以及身份识别信息。查理德·福肯瑞思指出,有意义的删除应当规定具有一定的彻底性,企业不仅要清除相关内容和照片,还应清除与信息主体有关的所有元信息[20]。物理删除是指从文件系统中清除或数据库中执行删除(delete)等语句,使其无法直接被识别和使用。但物理删除并不是最终的状态,在计算机的存储介质中对电子信息执行物理删除只是将其从目录列表中除名,如日常在计算机上执行“清空回收站”命令。在执行“删除”命令后,该电子信息仍然可以被恢复,就如同硬盘恢复一样,可以恢复一定比例的原电子信息,要想达到彻底性的删除,最有效的方式就是重复多次的文件覆盖,但这种方式也是成本最高的。相较于匿名化处理与逻辑删除,匿名化处理对于义务主体而言负担很少,若将匿名化处理径直认定为删除的替代方案之一,可能会使其变相逃避履行删除义务。因此,匿名化不应当成为与删除并列的选项,对于电子化的人脸信息而言,无须追求重复覆盖的极端删除方式,但是也不能采用仍然可以识别和使用的逻辑删除,而应当采用物理删除的方式。只有当技术无法实现或为其他合理目的需要时,逻辑删除才能成为次优选项。

6. 结论

个人信息删除权对于保障信息的完整性与自决性具有十分重要的意义,收集行为的正当性与合法性并不能保证其后处理行为的合法性,后续处理行为仍然可能造成损害,在信息处理过程中一旦出现应删除个人信息的合理情形,信息主体就有权反对相关个人信息处理行为并提出删除要求,信息处理者应认真审查并采取相应措施[2]。但我国国内互联网、人工智能等新技术发展势头正猛,已经成为提升中国国家话语权、文化软实力的重要传播途径,对互联网信息技术行业也有许多鼓励支持政策,删除权在某种程度上阻碍数据流通,不利于互联网发展,我国在删除权的设计上不应照搬照抄国外经验,而是应当结合我国大数据时代经济发展水平进行设计,谨慎对待,有选择性的借鉴,以应对大数据时代下个人信息数据化带来的新挑战。

参考文献

- [1] 维克托·迈尔-舍恩伯格. 删除: 大数据取舍之道[M]. 袁杰, 译. 杭州: 浙江人民出版社, 2013.
- [2] 冉克平. 论个人生物识别信息及其法律保护[J]. 社会科学辑刊, 2020(6): 111-120.
- [3] 高富平. 论个人信息保护的目的一—以个人信息保护法益区分为核心[J]. 法商研究, 2019, 36(1): 93-104.
- [4] [英] IT Governance 隐私小组. 欧盟通用数据保护——GDPR 合规实践[M]. 刘合翔, 译. 北京: 清华大学出版社, 2021.
- [5] 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.

¹⁷《信息安全技术、公共及商用服务信息系统个人信息保护指南》5.5.2:“收集阶段告知的个人信息使用目的达到后,立即删除个人信息;如需继续处理,要消除其中能够识别具体个人的内容,如需继续处理个人敏感信息,要活的个人信息主体的明示同意。”

-
- [6] 宋丁博男, 张家豪. 中外数据被遗忘权制度比较研究[J]. 情报理论与实践, 2023, 46(3): 98-105.
- [7] 丁晓东. 被遗忘权的基本原理与场景化界定[J]. 清华法学, 2018, 12(6): 94-107.
- [8] 张建文, 等. 被遗忘权的法教义学钩沉[M]. 北京: 商务印书馆出版社, 2020.
- [9] Richards, N.M. (2013) The Dangers of Surveillance. *Harvard Law Review*, 126, 1934-1952.
- [10] 于靓. 论被遗忘权的法律保护[M]. 北京: 中国社会科学出版社, 2020.
- [11] 王利明. 论个人信息删除权[J]. 东方法学, 2022(1): 38-52.
- [12] 郑志峰. 网络社会的被遗忘权研究[J]. 法商研究, 2015, 32(6): 50-60.
- [13] 郭春镇, 王海洋. 个人信息保护中删除权的规范构造[J]. 学术月刊, 2022, 54(10): 92-106.
- [14] 维克托·迈尔-舍恩伯格, 肯尼斯·库克耶. 大数据时代[M]. 盛杨燕, 周涛, 译. 杭州: 浙江人民出版社, 2013.
- [15] James, B. (2010) Rule and Graham Greenleaf, *Global Privacy Protection*. Edward Elgar Publishing, Cheltenham, 81.
- [16] 李媛. 大数据时代个人信息保护研究[D]: [博士学位论文]. 重庆: 西南政法大学, 2016.
- [17] 杨万明, 最高人民法院研究室. 最高人民法院审理识别人脸识别技术处理个人信息案件司法解释理解与适用[M]. 北京: 人民法院出版社, 2021.
- [18] 邵国松. “被遗忘的权利”: 个人信息保护的新问题及对策[J]. 南京社会科学, 2013(2): 104-109+125.
- [19] 罗翔. 论人脸识别刑法规制的限度与适用——以侵犯公民个人信息罪指导案例为切入[J]. 比较法研究, 2023(2): 17-30.
- [20] 吴飞, 傅正科. 大数据与“被遗忘权”[J]. 浙江大学学报(人文社会科学版), 2015, 45(2): 68-78.