

《民法典》视域下人脸识别信息的法律保护研究

——从杭州“人脸识别第一案”谈起

范艳如

华东政法大学国际法学院, 上海

收稿日期: 2022年3月21日; 录用日期: 2022年6月2日; 发布日期: 2022年6月10日

摘要

大数据时代改变了人们的生活方式, 人脸识别技术已经广泛应用于安检、移动支付等重要场景中。“人脸识别第一案”是人脸识别技术进入诉讼领域的首例。目前, 人脸识别技术仍然处于发展阶段, 技术存在争议的同时, 对于人脸识别信息的保护也受到广泛关注。人脸识别信息属于“私密信息”, 应当采取严格保护措施。完善对人脸识别等个人信息的法律保护, 可以在现有规范的框架下, 借鉴国外立法经验, 进一步细化保护标准。

关键词

人脸识别, 技术争议, 信息保护

Research on Legal Protection of Facial Recognition Information under Civil Code

—Talking from the First Case of Facial Recognition in Hangzhou

Yanru Fan

School of International Law, East China University of Political Science and Law, Shanghai

Received: Mar. 21st, 2022; accepted: Jun. 2nd, 2022; published: Jun. 10th, 2022

Abstract

The era of data has changed people's way of life. Facial recognition technology has been widely used in important scenarios such as security check and mobile payment. The First Case of Facial

Recognition is the first time in which facial recognition technology has entered the field of litigation. At present, facial recognition technology is still in the development stage. While the technology is controversial, the protection of face recognition information has also received extensive attention. Facial recognition information is “private information” and therefore strict protection measures should be taken. To improve the legal protection of personal information including facial recognition, under the framework of existing norms, we can learn from foreign legislative experience and further refine the protection standards.

Keywords

Face Recognition, Technical Disputes, Information Protection

Copyright © 2022 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

在信息科技高速发展的大数据时代，人脸识别技术正在不断地改变我们的生活，现在已经被大规模地应用于入站安检、移动支付等重要场景中。但是关于人脸识别信息的保护，仍存在较大的争议。如何防止人脸识别技术被滥用，保证人脸识别信息的安全是人们普遍关心的话题。《民法典》在人格权编第六章专章规定了隐私权和个人信息保护，第 1034 条第 2 款规定了生物识别信息属于个人信息，第 1034 条至 1039 条对于个人信息的保护搭建了较为宏观的法律框架，但现有框架在实践时存在难以量化，执法难以操作的隐忧。基于谨慎衡量新兴技术的利益和风险的前提，以《民法典》所确立的“合法、正当、必要”原则为基础，可以在司法解释或者下位法层面对于保护路径进行详述。

2. 杭州“人脸识别第一案”及其判决结果

人脸识别技术进入诉讼领域的首例当属杭州“人脸识别第一案”，即浙江省富阳区人民法院原告郭兵与被告杭州野生动物世界有限公司(以下简称野生动物世界)服务合同纠纷一案。

该案基本案情如下：2019 年 4 月，郭兵购买野生动物世界双人年卡，确定指纹识别入园方式。郭兵与其妻子留存了姓名、身份证号码、电话号码等，并录入指纹、拍照。后野生动物世界将年卡客户入园方式从指纹识别调整为人脸识别，并更换了店堂告示。2019 年 7 月、10 月，野生动物世界两次向郭兵发送短信，通知年卡入园识别系统更换事宜，要求激活人脸识别系统，否则将无法正常入园。此后，双方就入园方式、退卡等相关事宜协商未果，郭兵遂提起诉讼，要求确认野生动物世界店堂告示、短信通知中相关内容无效，并以野生动物世界违约且存在欺诈行为为由要求赔偿年卡卡费、交通费，删除个人信息等。

法院经审理认为，本案双方因购买游园年卡而形成服务合同关系，后因入园方式变更引发纠纷，其争议焦点实为对经营者处理消费者个人信息，尤其是指纹和人脸等个人生物识别信息行为的评价和规范问题。法院在判决中对于个人信息的法律规定作出分析：我国法律对于个人信息在消费领域的收集、使用虽未予禁止，但强调对个人信息处理过程中的监督和管理，即个人信息的收集要遵循“合法、正当、必要”的原则和征得当事人同意；个人信息的利用要遵循确保安全原则，不得泄露、出售或者非法向他人提供；个人信息被侵害时，经营者需承担相应的侵权责任。法院认为，原告在办理年卡时，野生动物

世界以店堂告示的形式告知持卡人需提供部分个人信息，未对消费者作出不公平、不合理的其他规定，客户的消费知情权和对个人信息的自主决定权未受到侵害。郭兵系自行决定提供指纹等个人信息而成为年卡客户。野生动物世界在经营活动中使用指纹识别、人脸识别等生物识别技术，其行为本身并未违反前述法律规定的原则要求。

3. 人脸识别引发的争议与信息保护问题

上述案件主要是个案化解决郭兵本人的诉求，就大数据时代人们所关心的人脸识别技术的使用情景限制问题，法院囿于诉讼争点没有也无法展开更为详细的阐述。在本案特定情况下，法院判决中并没有否认野生动物世界要求刷脸的正当性，判决中还明确了“野生动物世界在经营活动中使用指纹识别、人脸识别等生物识别技术，其行为本身并未违反前述法律规定的原则要求”。

实际上，早在人脸识别案件之前，人脸识别技术的应用争议进入公众视野已有较长一段时间。2019年10月29日，在“2019年城市轨道交通运营发展论坛”上，北京市轨道交通指挥中心官员就北京地铁大客流应准备的应对措施做了主题演讲。演讲指出，人物同检效率低，与轨道交通海量乘客出行的矛盾十分突出，为此，北京地铁要应用人脸识别技术实现乘客分类安检，研究建立人员分类标准，并形成对应的人脸库，依托人脸识别系统对乘客进行判别，安检人员据此采取不同的安检措施。此消息一出，舆论哗然，继而引发了更广泛的在日常生活中有关使用人脸识别技术的讨论与争议。梳理有关人脸识别技术的争议，可以发现讨论主要集中在两方面。

一是技术本身存在缺陷的争议，使用这项技术时的风险仍不容小觑。^[1]尽管人脸识别技术已经较为普遍地出现在人们的日常生活中，但技术本身仍有较大的优化空间，在实际应用过程中仍有较大的出错率，并非所有的识别算法都能达到立项效果。此外，很多人脸识别机器的内置算法并非三维识别，无法区别真人与照片。早在2019年，浙江嘉兴上海外国语大学秀洲外国语学校402班科学小队的同学曾在一次课外科学实验中发现，只要用一张打印照片就能代替真人刷脸，骗过小区里的丰巢智能柜，取出父母们的货件。人脸识别技术发展到今天，仍在致力于攻克诸多技术难关，监管在活体识别与二维照片区分上取得了一定进展，但是并非所有的人脸识别技术都优化到这一地步。这项技术的成熟情况与应用反馈仍然有待观察。

二是在人脸识别信息的保护规范方面应当如何完善的争议。《民法典》第1035条规定，处理个人信息的，应当遵循合法、正当、必要原则。合法是绝对前提，如何明确“正当性、必要性”的合理边界则是当下人脸识别信息保护的难点。个人信息的保护主要涉及个人隐私与公共安全之争，有观点认为，为公共安全考虑可以牺牲个人隐私。这种观点值得怀疑。公共安全和个人隐私的分野难以出台具体的量化标准，政府机构出于便民和公共安全考虑，在机场、车站等可能发生较大公共安全事件的场合采用人脸识别入关，尚且符合正当性和必要性的要求。但是非政府机构在诸如居民小区、写字楼和高级商场等场所，以效率和安全防护为由，推行人脸识别技术的落地实施，是否满足正当性和必要性的要求，则有待考量。

4. 《民法典》视野下人脸识别信息的法律定性

现行立法并未对“人脸识别技术”的内涵和外延作出界定，但学界普遍认同该项技术属于身份核验的生物识别技术。人脸识别信息作为生物识别信息的一种，在当下数据时代具有重要的应用。例如，个人重要信息的电子记录可以通过人脸识别获得，尤其是个人财产可以通过人脸识别解锁密钥并进行财产处分，已经成为常见惯例。

《民法典》第四编为“人格权”，在该编第六章，条文明确区分了隐私权与个人信息的保护。第1032条

规定自然人的隐私权。第 1034 条规定自然人的个人信息受法律保护，该条第三款明确对于个人信息的保护程度也有不同，个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。对于个人信息在民法典下的法律定性，学界存在争议。有学者认为，前述规定从实定法层面明确了个人信息属于民事权益，是一种独立的人格权益。^[2]有学者指出，作为信息时代的一项全新挑战，个人信息保护的本质应当是一项需要通过个人信息保护法确立的一项新型公法权利。^[3]有学者认为，个人信息权利保护只能适用于特定的信息关系，只能针对商业性或专业性收集个人信息的主体，由此需要区别于侵权隐私保护与执法隐私保护。个人信息权利保护不能像隐私权保护那样，可以针对不特定的第三人。^[4]本文认为，在民法典视域下，通过私法权利体系和隐私权给予个人信息保护具有可行性，下文将从人脸识别信息的基本特征出发，试论将个人信息保护归于个人权利。在第 1034 条规定之下，人脸识别信息作为一种特殊的个人信息，应当使用何种保护标准，对此仍待商榷。人脸识别信息是否可归于该条第三款所说的“私密信息”，将影响对于人脸识别信息的保护程度。

在法律规范层面梳理人脸识别信息的法律属性，应当以人脸识别信息的独特性为规范起点，^[5]基于其特征和在生活场景中的使用频率与重要程度，应当将其定位为“私密信息”，可归于隐私权的范畴。人脸识别技术的实质是收集、积累、分析生物数据，以此勾勒个人画像。眼下人脸识别技术的使用目的有三，一是身份认证，二是识别与追踪，三是影响主体的行为选择。所以，人脸识别技术所涉及的，不仅是隐私权保护问题，更关乎社会对包含人脸识别信息在内的个人信息收集与利用方式的基本走向。人脸识别信息的特征主要可以归纳为以下两点：（一）具有敏感性。人脸识别技术与指纹等其他生物识别技术相比，在使用中具有无意识性、非接触性、侵入性强的特点。（二）几乎无法更换性。不同于传统字符密码在风险潜在阶段可以进行更改，人脸识别信息一旦录入系统，几乎很难再发生颠覆性的变化，尽管可能随着时间的推移，部分面部特征发生改变，识别机器仍可能在一定程度内通过智能算法进行匹配。因此人脸识别信息一旦这些信息被泄露或者被非法窃取，它对个人的人身和财产安全会造成重大的伤害。

综上，基于人脸识别信息的基本特征，其法律定位应当归属于《民法典》第 1034 条第三款的“私密信息”，可以适用隐私权保护的规定。个人信息保护的本质应当是一项新型权利，而对人脸识别信息的保护程度要高于对一般的个人信息的保护程度。

5. 人脸识别信息的保护路径分析

（一）使用人脸识别技术的风险与现有法律规定

研究人脸识别信息的保护路径，首先要厘清人脸识别技术在使用中存在的风险。人脸识别技术至少存在以下几种主要的潜在风险。一是存在导致公民成为“透明人”的可能。人脸识别不仅是收集数据，更重要的是通过人脸数据迅速锁定自然人身份。二是存在数据泄露的风险。有些银行账户和人脸信息进行绑定、关联。一旦人脸信息被泄露，或被不法分子违法共享、转让，将对公民的人身和财产安全产生巨大隐患。三是数据被滥用的风险。数据滥用的主体除了违法犯罪分子，还包括公权力。^[6]四是无法有效救济的风险。寻查泄露数据者在实践上存在极大困难，在这种情况下，民事诉讼在救济受害者方面能发挥的作用受到极大限制。

现行《民法典》对于人脸识别信息的保护方式主要规定在第 1035 至 1039 条，覆盖信息的收集、存储、使用、加工、传输、提供和保密等全阶段。根据《民法典》第 1035 条，处理个人信息时，首先应征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；其次应公开处理信息的规则；再次应明示处理信息的目的、方式和范围；最后对于个人信息的处理，不得违反法律、行政法规的规定和双方的约定。就人格权单独成编的争议按下不表，《民法典》专章设立人格权编，并单列个人信息保护，体现出对大数据时代公民人格权保护面临挑战的回应。传统民法的人格权与侵权责任制度已难以满足有

效保护个人信息、维护自然人人身财产安全的需要，将个人信息单列表明了信息时代对个人信息加强私法保护的基调，在涉及个人信息保护的立法中应当关注自然人的民事权益保护与信息自由这两个法律价值之间的权衡与协调，彰显了法律对人格尊严和人格自由的尊重。^[7]

目前我国如何规范各种应用场景下的人脸识别技术应用与信息保护，还有很长的路要走。我国关于个人信息保护的法律法规仍在不断完善中。2021年11月1日，《个人信息保护法》开始施行，该法第28条规定了敏感个人信息的种类和保护原则。其中，包含人脸识别信息在内的生物识别信息属于敏感个人信息，一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。此外，还规定了只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。2020年2月，全国金融标准化技术委员会审查通过的《个人金融信息保护技术规范》(JR/T 0171-2020) (以下简称《规范》)将生物识别信息列为敏感性最高的C3类信息，并要求金融机构不应委托或授权无金融业相关资质的机构收集C3类信息，金融机构及其受托人收集、通过公共网络传输、存储C3类信息时，应使用加密措施；不得公开披露用于用户鉴别的个人生物识别信息。2020年3月新修订的我国国家标准GB/T 35273-2020《信息安全技术个人信息安全规范》明确规定个人生物识别信息属于个人敏感信息，并对个人敏感信息进行了特殊保护：传输和存储个人敏感信息时，应采用加密等安全措施；共享、转让个人敏感信息前，除向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；不应公开披露个人生物识别信息；等等。2020年10月，杭州市人民代表大会常务委员会发布了关于《杭州市物业管理条例(修订草案)》的说明。条例新增了“不得强制业主通过指纹、人脸识别等生物信息方式使用共用设施设备，保障业主对共用设施设备的正常使用权”等内容，有望成为中国首部明确写入人脸识别禁止性条款的地方性法规。

(二) 个人信息法律保护可参考借鉴国外立法

就“人脸识别第一案”来讲，包括人脸识别信息在内的个人信息作为人格权的一部分，是受到法律保护的。物业公司、动物园等公共场所不能说要就要。收集个人信息必须符合“必要原则”和“最小够用”的原则。从个案来讲，“人脸识别第一案”原告胜诉，有着标志性意义，但本文并不认同法院在判决书中写到“野生动物世界在经营活动中使用指纹识别、人脸识别等生物识别技术，其行为本身并未违反前述法律规定的原则要求。”

有关人脸识别信息等数据保护方面的立法，放眼其他国家，寻求可行的借鉴做法，也有重要意义。欧盟《通用数据保护条例》(GDPR)中被称为“全球最严数据管理条例”，其对于生物识别信息采取了“禁止收集使用”的原则。而对于原则外的使用，GDPR也详细列举了多达10条的细则。应当认识到，在当今信息科技高速发展的情况下，人脸识别或许成为无法避免的趋势，法律法规如何在人脸识别信息的利用与保护之间进行平衡，应当视人脸识别技术的收益与风险关系而定。收益大于风险，则应当注重信息利用；风险大于收益，应当注重保护。如果收益与风险的关系不确定，则法律应该谨慎，而不能盲目放开其利用。因此，本文并不赞同“禁止收集使用”的刚性原则，相反，应该对个人信息的保护搭建严密的框架中，保护公民的人格权免遭侵害，也同时为信息技术的良好发展保驾护航。

(三) 对人脸识别信息进行从严保护

《民法典》的规定奠定了对于私密信息应当从严保护的基调，《个人信息保护法》明确了对生物识别在内的敏感个人信息要严格保护，在下一步的法律法规完善过程中，可以从以下三个方面进一步完善人脸识别技术的法律规制。第一是在信息保护规范方面做出程度区分。对采集的人脸信息施加保护要比对一般个人信息的保护更严格，并联合技术部门共同制定相应的保护标准。正如前文所述，人脸识别信息，也就是《个人信息保护法》中的敏感个人信息，应当高于对一般个人信息的保护程度。^[8]本文认为，

在民法典视野下其法律定性为“私密信息”，应当归属于隐私权的范畴，其保护应适用隐私权的相关规定。第二是设置不同的启用阈值。区分政府机构与商业等非政府机构配置不同的信息收集的限制标准。人脸信息属于私密信息，必须权利人“明确同意”才能进行采集，如果权利人没有明确同意，则必须要基于公共利益的需要才能收集。虽然公共利益的解释可能会比较宽泛，但还是有特定内涵，比如为了公共安全、保护个人生命财产安全等，都属于公共利益的范围；而出于商业目的或盈利目的，则不属于公共利益范围。在“人脸识别第一案”中，动物园属于商业机构，收集用户的人脸识别信息很难说是为了公共利益。第三是明确并建立统一的责任规范。可以参考欧盟 GDPR 的做法，建立健全一体适用的安全与责任底线，有助于明确责任分配，并给实践确立统一的标准。GDPR 是对公私部门一体适用的，这就意味着，无论是政府部门还是非政府部门，只要使用人脸识别技术，就必须遵守相同的责任规范。

综上，《民法典》对大数据时代人格权所面临的挑战给予了充分重视，显示出对人脸识别信息应当从严保护的态度，未进一步就保护路径做出更为细致的规定，但随后的立法都契合对人脸识别信息进行特别保护的立法精神。新兴技术的发展与在生活场景中的应用趋势无法阻挡，为回应技术隐患和使用争议，建设制度保护的笼子应是信息保护立法的出发点。“人脸识别第一案”中，法院对于动物园可以生物识别方式入园的经营方式予以肯定，这个观点值得商榷。本文认为，应当谨慎衡量人脸识别这一新兴技术的利益和风险，以《民法典》所确立的“合法、正当、必要”原则为基础，在司法解释或者下位法层面逐渐完善对于人脸识别等信息数据的保护方式，为实践和司法确立明确可行的保护标准。

参考文献

- [1] 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(5): 51-63.
- [2] 程啸. 论我国民法典中个人信息权益的性质[J]. 政治与法律, 2020(8): 2-14.
- [3] 周汉华. 个人信息保护的法律定位[J]. 法商研究, 2020, 37(3): 44-56.
- [4] 丁晓东. 个人信息权利的反思与重塑 论个人信息保护的适用前提与法益基础[J]. 中外法学, 2020, 32(2): 339-356.
- [5] 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(5): 21-29.
- [6] 劳东燕. 人脸识别技术的潜在风险与法律保护框架的构建[EB/OL]. <https://mp.weixin.qq.com/s/SpWd6CBOti9sstMt1Odn5w>, 2021-11-30.
- [7] 程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学, 2019(4): 26-43.
- [8] 王利明. 人脸信息是敏感信息和核心隐私应该强化保护[EB/OL]. https://mp.weixin.qq.com/s/J6nfcX_aNU3TpRYrHtIrA, 2021-11-30.