

# 君合专题研究报告



2019年9月5日

## “变脸”软件的三条法律红线

近日，一款“换脸”APP(下称“**换脸APP**”)使整个朋友圈都“ZAO”了起来。一时间，朋友圈集体沦陷，好友们纷纷依靠AI“换脸”技术轻松实现明星梦，上传一张清晰的个人正面照，并完成人脸认证后，即可摇身成为热门影视剧的男女主角。

朋友圈陷入换脸狂欢的同时，换脸APP用户协议中的“霸王条款”也被公众热议，该软件的运营安全性、用户个人信息保护及版权授权问题纷纷受到挑战。然而，万般刁难，仍有勇夫。根据相关报道显示<sup>1</sup>，截至8月31日早上8点半，换脸APP在iOS应用商店排到免费榜下载量第9位，娱乐榜第2位。不过，笔者注意到，对于公众广泛诟病的相关用户协议条款，换脸APP的团队在本文发出前已经相应修改了用户协议，发表了致歉声明，承诺会保护用户个人信息安全。

变脸APP引发的纷争随着该APP的改进已告一段落。作为法律从业人员，我们思考的是，类似APP的运营，应有以下几条法律红线不能逾越：(1)个人信息保护；(2)著作权保护；以及(3)《合同法》公平原则的约束。本文中，笔者将着重围绕以上三条法律红线，结合换脸APP运营实例予以浅议。

### 红线之一：个人信息保护

#### (1) 人脸-个人生物识别信息

从广义的范围来理解，精确的人脸画像、人脸照片由于包含人脸面部特征，属于个人生物识别信息。做此项归类的法律意义在于：个人生物识别信息广泛用于身份认证、交易及支付环节，该等信息一旦泄露，势必给用户带来难以消除的影响，其对个人生活及交易安全的重大影响决定了该等信息必须被法律严格保护。任何主体对于他人个人生物识别信息的收集及使用，均应当遵循法定规则，而不得自行随意创设规则。

个人面部肖像应作为个人生物识别信息予以严格保护，早已成为业内共识：

1) 2017年6月1日施行的《中华人民共和国网络安全法》(下称“《**网络安全法**》”)将个人生物识别信息纳入个人信息范畴，予以保护。但《网络安全法》并未对个人生物识别信息的外延予以明确；

2) 2018年5月1日起施行的推荐性国家标准《信息安全技术个人信息安全规范》(GB/T 35273-2017，下称“《**个人信息规范**》”)附录的“个人信息示例”部分将“个人生物识别信息”界定为“个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等”，明确将个人面部特征纳入个人生物识别信息的范畴。尽管该等国家标准为推荐性国家标准，但其对于个人生物识别信息外延的界定，符合行业共识；

<sup>1</sup> 21世纪经济报道8月31日文章，链接：<https://mp.weixin.qq.com/s/qlhVDwv36C714y-f3hhnAQ>。

3) 2018年5月25日正式生效的欧盟《通用数据保护条例》(下称“GDPR”)第四条也明确将个人面部图像(facial images)纳入生物数据(biometric data)的范畴。

事实上,关于换脸APP运营合法性的讨论中,公众讨论的焦点也集中于AI换脸技术是否会对使用刷脸技术进行支付的支付方式带来安全隐患。尽管支付宝平台已经公开发布声明表示该等AI换脸技术并不会对支付安全产生威胁,然而,公众仍然广泛缺乏安全感。毕竟,技术操作已经脱离了公众能够控制的范畴而全部交由APP运营者控制,一旦APP运营者超越法律及道德的边界,或者网络安全本身出现问题,都可能造成不可逆转的负面后果。

## (2) 采集及使用规则

人工智能的时代,数据是核心基础,正所谓“无数据不AI”,个人信息数据也已然成为AI行业运营主体争夺的对象。例如,2017年6月顺丰菜鸟关于数据的争议<sup>2</sup>,以及2017年8月的华为腾讯数据纷争<sup>3</sup>。

数据采集及使用规则如未被重视,倒霉的永远是用户。中国目前尚未爆发互联网运营者大规模侵犯用户隐私的新闻,但是,在世界范围内已经发生不少案例。例如,2018年1月,Facebook因面部识别系统涉嫌侵犯用户隐私而在美国伊利诺伊州被提起集体诉讼<sup>4</sup>;此外,Facebook还因涉嫌数据收集违规而遭受英国<sup>5</sup>、法国<sup>6</sup>、西班牙<sup>7</sup>、意大利<sup>8</sup>监管部门

罚款/调查。除Facebook外,Google的数据收集也遭受投诉及调查<sup>9</sup>。以上案例说明,个人信息保护面临的挑战任重道远。

中国的《网络安全法》对于个人信息保护提出一些法定规则。例如,第四十一条规定的严格保密要求,合法、正当、必要原则,同意规则,目的限定原则,不得泄露、篡改、毁损要求,不得向他人提供要求。《个人信息规范》进一步明确了“七大原则”:权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则。

相较于欧盟的GDPR,《个人信息规范》与其在基本原则相似,但GDPR在上述原则之外还提出准确、必要、及时的数据处理要求<sup>10</sup>。此外,GDPR对于个人生物识别信息还提出更为严格的要求。GDPR明确,个人生物识别信息属于特殊信息,不同于一般的个人信息,使用个人生物识别信息原则上都是被禁止的<sup>11</sup>,仅有在特殊情形下例外,例如用户明示同意例外、公共利益例外等。<sup>12</sup>

《网络安全法》、《个人信息规范》及GDPR规定的相关使用原则/规则中,以下几个原则/规则应尤为得到重视,我们相应整理如下:

---

2 新浪财经 2017年6月2日报道, <https://finance.sina.com.cn/roll/2017-06-02/doc-ifyfuzny2084327.shtml>。

3 新浪科技 2017年8月10日报道, <http://tech.sina.com.cn/i/2017-08-10/doc-ifyixhyw6480463.shtml>。

4 腾讯科技 2018年4月7日报道, <https://tech.qq.com/a/20180407/007521.htm>。

5 新浪科技 2018年7月11日报道, <https://tech.sina.com.cn/i/2018-07-11/doc-ihfefkqp9787190.shtml>。

6 新浪科技 2017年5月16日报道, <https://tech.sina.com.cn/i/2017-05-16/doc-ifyfeivp5784995.shtml>。

---

7 新浪科技 2017年9月12日报道, <https://tech.sina.com.cn/i/2017-09-12/doc-ifykuffc5245138.shtml>。

8 新浪科技 2018年12月8日报道, <https://tech.sina.com.cn/i/2018-12-08/doc-ihprknvt6985856.shtml>。

9 新浪财经 2019年5月23日报道, <https://finance.sina.com.cn/stock/relnews/us/2019-05-23/doc-ihvhiew3924142.shtml>。

10 GDPR第5条第1款(d)项。

11 GDPR第9条第1款。

12 GDPR第9条第2款,共计规定10项例外。

序号	使用原则	含义	《网络安全法》	GDPR
1	同意原则	网络运营者收集、使用个人信息必须得到被收集者同意	第四十一条第一款 <sup>13</sup>	第 9 条第 2 款(a)项, 要求对于“特定目的”使用予以“明示同意”
2	特定目的原则	网络运营者不能收集与其提供服务无关的信息	第四十一条第二款 <sup>14</sup>	第 5 条(b)款
3	匿名化要求	指将个人数据移除可识别个人信息的部分, 确保数据主体不会再被识别	第四十二条 <sup>15</sup>	已匿名化的数据(anonymous information)不属于个人数据, 不受 GDPR 约束

13 “网络运营者收集、使用个人信息, 应当遵循合法、正当、必要的原则, 公开收集、使用规则, 明示收集、使用信息的目的、方式和范围, 并经被收集者同意。”

14 “网络运营者不得收集与其提供的服务无关的个人信息, 不得违反法律、行政法规的规定和双方的约定收集、使用个人信息, 并应当依照法律、行政法规的规定和与用户的约定, 处理其保存的个人信息。”

15 “网络运营者不得泄露、篡改、毁损其收集的个人信息; 未经被收集者同意, 不得向他人提供个人信息。但是, 经过处理无法识别特定个人且不能复原的除外。”

对于互联网运营者而言，应当对于《网络安全法》、《个人信息规范》及 GDPR 确定的上述保护原则予以重视。尽管 GDPR 为欧盟法规，但鉴于其“长臂管辖”<sup>16</sup>，所有收集欧盟公民信息的企业，无论是否为欧盟企业，均会受到 GDPR 的约束，违反 GDPR 相关规定将面临巨额罚款。我们建议相关互联网企业对于个人信息收集及使用予以高度重视，特别是对于个人生物识别信息的收集及使用，均应当以用户同意为前提，以特定目的使用为边界，以不挪作他用为约束标尺。

### (3) 保护客体-肖像权及隐私权

换脸技术其实已经不是什么新鲜事。早在 2017 年 12 月，美国社交网站“Reditt”上一个名为“DeepFake”的用户发布了一个视频，其将成人电影中一位演员的脸更换为某个明星的脸，可以达到以假乱真的效果。DeepFake 实际上是一种人工智能集成的人物图像合成技术（俗称，人脸交换技术），即将图像或视频中的脸替换为另一张人脸。上述视频发布后，公众对于该等技术可能产生的负面影响纷纷表示担忧，原因是，基于 DeepFake 的功能，其很有可能被用来制作虚假的名人色情视频或报复色情内容、假新闻或恶意恶作剧。此后，Reddit 迫于压力封杀了“DeepFake”的账号，结果却导致“DeepFake”用户直接开源了 DeepFake 的代码。DeepFake 技术甚至还有相应的中文站点 (<https://deepfakes.com.cn/>)。

DeepFake 被逼下架，是公众对于换脸技术担忧的结果，用户的担忧，实则是对于个人肖像及隐私保护的担忧。在用户生产内容（UGC）的时代，大量的信息及数据是用户自行上传，例如用户在微博等社交网站上传自己的肖像照片，该等上传内容属于用户自发上传内容，严格来讲，并非《网络安全

法》规制的网络运营者向用户收集的信息范畴。当前的网络环境下，对于个人生物识别信息的保护，我们认为应当区分为用户主动上传及被动上传两个层面来考虑：

1) 对于用户主动上传并自行选择公开的个人肖像内容，应当属于肖像权的保护范畴。中国法律对于肖像权保护的判断标准是：是否发生以营利目的的使用，非营利目的使用且未对肖像予以丑化毁损的使用，一般情况下不构成肖像权侵权。而对于用户自行上传的信息，由于已经由用户主动公开，可能已经不再属于隐私权的范畴，因此可能无法再给予隐私权的保护，但仍然能够得到肖像权的保护；

2) 对于被动上传的个人生物识别信息，应当给予肖像权（如适用）及隐私权的双重保护。用户被动上传的信息，即用户基于网络运营者的要求而提供的相关信息，属于《网络安全法》规范的网络运营者向用户收集的信息。根据民法理论，个人肖像同样属于隐私权的范畴，未经许可不得擅自向第三方提供。因此，对于网络运营者向客户收集的信息中的个人面部信息内容，网络运营者应当同时给予肖像权及隐私权保护。在未经用户同意情形下，不得以任何方式（匿名化除外）对外提供或使用，而仅能在网络运营者提供服务的限定目的范围内使用。相比而言，《网络安全法》下对于用户个人肖像的保护，要比肖像权制度的保护更为严格，即并不区分是否以营利为目的使用，未经用户同意或超越限定目的而对外提供或使用都是被禁止的。

事实上，《网络安全法》并未明确其对于用户个人信息，特别是个人生物识别信息给予的保护是何等权益的保护。我们倾向于认为，个人生物识别信息的核心内容是个人隐私，总体而言应给予隐私权的保护；对于个人肖像、画像等体现用户整体面部特征的内容则属于用户肖像权的范畴，应给予肖像权的保护。因此，对于个人生物识别信息的保护应

<sup>16</sup> GDPR 第三条的规定，GDPR 适用于设立在欧盟之外，但依据国际公法欧盟成员国法律可适用地的控制者对个人数据的处理。

当区分情形，适当情形下应给予肖像权及隐私权的双重保护。

## 红线之二：著作权法边界

### (1) 视频变脸-修改权还是改编权

在探讨影视片段合理使用边界的问题之前，我们希望对于换脸 APP 运营方式涉及的著作权权利进行探讨。目前网络上大量文章的主流观点是，换脸视频是对原视频的改编。其理由在于，如换脸的内容产生喜剧/恶搞效果，则可能形成新的作品而构成改编作品。

对此，我们持有不同观点：

1) 改编权，是指改变作品、创作出具有独创性的新作品的权利。然而，换脸视频中，除了角色的脸换了，其他内容并未发生改编，新的内容并不存在独创性可言。即使产生所谓的喜剧/恶搞效果，也无法与影视作品对于独创性要求的高度等同；

2) 相反，我们倾向于认为，通过后续技术对于视频中人脸进行更换，实际上是对作品的修改，属于修改权的范畴。当然，除修改权外，还涉及保护作品完整权。根据《著作权法》的规定，著作权人享有保护作品不受歪曲、篡改的权利。因此，如果相应的歪曲、修改并未得到著作权人的同意，则用户及变脸 APP 运营者均面临很高的侵权风险。

退一步而言，无论是修改还是改编，对于原作品的使用，以及对于修改/改编完成内容的使用，显然都应当得到原作品著作权人的同意。因此，未经授权而对视频进行“变脸”，其合法性值得商榷。

### (2) 非商业使用不完全等于合理使用

实践中，影视行业内的同仁对于合理使用存在一定程度的误解，误以为非商业目的使用就等同于合理使用。例如，换脸 APP 现有版权说明中仍然表述为，换脸 APP 利用技术对于换脸 APP 上的短视频

进行修改编辑后形成的短视频和动图，仅可在法律法规允许的范围内“以社交为目的进行非商业性的信息网络传播”。

似乎通过“非商业性使用”的声明就可以摆脱侵权风险，实则不然。《著作权法》禁止一切未经许可的使用，而并不考察涉嫌侵权主体的主观状态。因此，被诉侵权后一切装无辜卖萌的行为、表明所谓不知构成侵权、没有利用著作权内容盈利等抗辩，在《著作权法》面前都是苍白无力的。

至于合理使用，《著作权法》仅规定了 8 种情形，其中被公众广为引用的条款为第一款，即“为个人学习、研究或欣赏，使用他人已经发表的作品”。那么问题来了，为个人娱乐所用，是否属于合理使用的范围？以变脸 APP 为例，公众使用换脸 APP 变脸并上传的心态，显然是处于猎奇心理，觉得有趣、好玩儿，而并非单纯的学习、研究或欣赏目的；视频上传到 APP 后，激发公众的好奇心，用户逐一利用相同视频变脸，显然并不具有学习、研究、欣赏价值，而仅具有娱乐价值。并且，将换脸视频公开，显然也突破了“为个人”欣赏的范围。

并且，换脸 APP 所声称的非商业性目的使用，显然也是值得商榷的。在换脸 APP 运营初期阶段，似乎暂无可见的商业利益。然而，随着换脸 APP 业务开展，换脸 APP 中将来很可能取得广告等的商业收入，很难不会改写换脸 APP 的商业运营目的，由此也可能导致“非商业性目的”使用缺少说服力。

从谨慎的角度来看，较好的做法，是由换脸 APP 与热门视频的著作权权利主体达成合作，获得相应的授权后供用户使用，否则，无论是换脸 APP 的运营者，还是其用户，均很难摆脱侵权风险。

## 红线之三：《合同法》的公平原则

### (1) 民事活动均应遵守公平原则

换脸 APP 原有用户协议<sup>17</sup>中有一条内容，其要求用户同意：换脸 APP 在用户上传“变脸视频”后即视为同意换脸 APP 运营者及其关联方享有“全球范围内免费、不可撤销、永久、可转授权和再许可的权利，包括但不限于：人脸照片、图片、视频资料等肖像资料中所含的您或肖像权利人的肖像权，以及利用技术对您（用户）或肖像权利人的肖像进行形式改动。”如果用户同意上述条款，则意味着，不仅用户上传的个人肖像可以为换脸 APP 运营者随意使用且改动，而且同一视频内容中用户上传的其他角色的肖像也可以为换脸 APP 运营者随意使用。

如此霸道的授权条款，着实让公众吓了一跳。根据《合同法》规定，民事活动应当遵守公平原则，当事人均应当遵循公平原则确定各方的权利和义务，当事人之间的权利义务应当具有对等性。上述用户协议条款，显然有些过分，用户凭什么要同意他人对自己的肖像随意改动呢？

## (2) 违反公平原则的格式条款无效

基于公平原则，《合同法》第三十九条要求提供格式条款的一方应当遵循公平原则确定当事人之间的权利和义务。同时，《合同法》第四十条规定，提供格式条款一方免除其责任、加重对方责任、排除对方主要权利的，相应的格式条款无效。

换脸 APP 的用户协议，属于典型的格式条款，其中对于换脸 APP 运营主体责任的排除，对于用户责任的加重，很可能被认定为无效。换脸 APP 的运营者在广受公众诟病后，也意识到格式条款中存在

的问题，从而相应调整了用户协议中的许多不当表述。换脸 APP 在 9 月 1 日后连续两次紧急修改了用户协议，现有的用户协议内容，将换脸 APP 对用户信息的使用方式限定为“仅为通过后期技术将您（用户）提交的照片叠加到您选定的短视频中…生成新的短视频并实现“换脸效果”，同时增加“将根据《隐私政策》仅最大努力在合理、必要且明示的范围内使用您授予的内容”。

换脸 APP 原有长篇大论将自己责任全部摘除的用户协议和版权声明，显然是“吃力不讨好”。修改后的用户协议，似乎符合《网络安全法》的要求，但后续执行效果如何，只能拭目以待了。换脸 APP 引发的用户协议争议，提醒广大网络运营者，起草用户协议等格式条款时，千万不能“赶尽杀绝”，否则很可能面临相同的困窘局面。

## 结语

人工智能领跑的时代，无论是用户个人、互联网运营者还是监管机关，均应对于个人信息保护问题予以重视。我们认为，类似 APP 的运营，应当具备充分的法律支撑，不能突破个人信息保护、著作权保护及合同法《公平原则》的约束，严格遵守以上三条红线设定的边界，才能合法、合规、合理运营，才可能得到用户的支持及监管部门的认可。

我们建议，相关互联网运营主体在确定运营方式、考量个人信息的收集及使用方案、设置用户协议及隐私条款时，充分征询律师的意见，确保运营合法合规性。

<sup>17</sup> 原用户协议中该等表述已经为换脸 APP 运营者于 2019 年 9 月 1 日及 9 月 2 日相继修改。

黄荣楠 合伙人 电话：86 21 2208 6280 邮箱地址：huangrn@junhe.com  
刘佳迪 律 师 电话：86 21 2208 6399 邮箱地址：liujd@junhe.com  
马钦奕 律 师 电话：86 21 2283 8324 邮箱地址：maqy@junhe.com

---

本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息, 敬请关注君合官方网站“[www.junhe.com](http://www.junhe.com)”或君合微信公众号“君合法律评论”/微信号“JUNHE\_LegalUpdates”。

