不在于技术本身　而是应用的问题

人脸识别时代该如何保护隐私？

如今，脸的用途越来越广泛了。人们刷脸支付、刷脸安检、刷脸入住酒店……几乎时时处处都要把脸推到前台，但是频繁刷脸背后是否存在安全隐患，我们的“脸”有没有被盗用或滥用，到底应该如何在享受便利的同时保护自己的“脸”。凡此种种，都成为生活在人脸识别时代的我们需要关注的问题。

“新技术总会有安全问题，人脸识别本身为生活提供了便利，而它最大的风险在于信息泄露。”在记者所做的 X?15 刷脸变形记调查访谈中，有专家如是表示。同时，还有专家指出，人脸识别安全问题不在于技术本身，而是应用的问题。

那么，人脸识别时代，我们该如何保护自己的隐私？在记者的采访中，多位专家告诉我们，有几个问题是我们必须要注意的，与此同时我们必须要了解某些机构滥用人脸识别有何法律风险，同时明确人脸信息采集的法律边界究竟在哪，这样就能在必要的时候采取法律的手段保护自己。

怎么辨别有害？关键在于如何使用

人脸技术一“出生”就带有原罪吗？答案恐怕是否定的。

“我比较反对在人脸识别上出了一件事，就觉得人脸识别技术敏感，碰不得。很多情况下人脸是公开数据，我们每天走在街上都能被人看到，不能说人脸就不能给别人看了。”中国人民大学法学院副教授丁晓东说。

在他看来，实际上，我们的人脸信息早就已经相互流通和流动了，“所以我认为不能因为 ZAO 事件就对这一技术采取禁止的态度，而是要在具体的场景中进行风险的防范，这可能是更为重要的，也是更需要保持的一个态度。”

丁晓东认为，就争议来说，重点不是换脸本身会不会存在问题，而是民众能不能对这一技术形成可靠的辨识，比如我们看漫画时，知道是假的。如果一些技术的使用，使得民众或一般人在短时间里难以辨识，就可能存在风险，例如对新闻联播主播进行换脸，然后制造假新闻。“人脸识别在有的领域可能会产生很大风险，包括新闻领域，通过深度伪造技术使得伪造的新闻图片传播。”

联合国网络安全与网络犯罪问题高级顾问吴沈括则表示，技术是中立的，但使用技术的人是有立场的。人脸识别技术的安全问题不在于该项技术本身，而是应用的问题。危险在于利用这项技术达到了不该达到的目的，实施了不该实施的行为。

令吴沈括担忧的是，人脸识别技术一旦被普及，它可以定位某人而该人却毫不知悉。该项技术用于侦查犯罪就是助力公共安全；当用于跟踪他人，就可能侵犯隐私，干涉他人自由；假如应用于冒充他人，就是在实施犯罪。因此，人脸识别技术是否有害关键在于如何使用。

滥用有何法律风险？可能涉嫌刑事犯罪

虽然某些 APP 及其背后运营机构获取大众的“脸”越来越方便了，但是它们若想滥用也是要注意风险的，所以这在一定程度上阻止了人脸被滥用。

“以换脸视频为例，若有人用其谋利，则涉嫌侵犯他人肖像权。同时，可能涉嫌侵犯相关影视作品的制片方的著作权。”中闻律师事务所合伙人赵虎举例称。

赵虎详细解释换脸视频背后可能面临的风险，根据我国著作权法的规定，电影和类电作品的著作权由其制片者享有，制片者对作品享有保护作品完整权，即保护作品不受歪曲、篡改的权利。不仅如此，换脸视频还涉嫌侵犯相关人物的名誉权问题；严重者也可能涉嫌刑事犯罪。

北京志霖律师事务所副主任赵占领指出，有关人脸数据的滥用，存在五种违规或犯罪的可能。一是未经用户同意的情况下收集用户个人信息；二是违反法律规定的必要原则，超范围收集用户个人信息；三是收集用户个人信息之后未按照事先约定的用途、方式使用或转让；四是未尽到网络安全管理义务，由于管理漏洞或技术漏洞导致用户的个人信息被泄露；五是经营者或其员工将用户的个人信息非法转让或倒卖给他人，这也是涉嫌刑事犯罪的行为。

陈立彤告诉记者，最高人民法院、最高人民检察院在今年 6 月 1 日正式实施的《关于办理侵害公民个人信息刑事案件适用法律若干问题的解释》中明确了侵害公民隐私犯罪行为的具体标准和类型，将公民个人信息安全置于法律保护的最高位阶，在刑事法律上对侵害公民数据权的行为标清了底线。

不过，陈立彤也指出，两高司法解释的重点在于打击侵害公民个人信息的“明偷”“明抢”，对于滥用格式条款非法“获取”用户授权，侵害公民隐私权的“暗偷”“暗抢”行为影响却不大。

陈立彤解释道，这是因为，隐私权作为民事权利，用户也有自我处分的权利，一旦网站搬出已经获得用户授权的“隐私条款”作为抗辩理由，刑事法律就很难认定其为犯罪行为。

信息采集的法律边界何在？保护难以落实

既然人脸识别技术越来越普及了，那么某些 APP 及其背后的运营机构是不是就可以大肆采集用户的“脸”了？当然，这个答案一定是否定的。有些信息可以采集，有些则不能，我们普通人也有必要知道如下的信息。

依据《信息安全技术个人信息安全规范》，个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息等。陈立彤提醒大家，“采集个人信息需取得个人信息主体的同意，未经同意，不得转让、共享、加工其个人信息。”

吴沈括则举了一些国外“抵制”人脸识别的例子。2019 年 5 月，旧金山成美国首个禁止面部识别监控的城市。2019 年 6 月，美国在国会听证会上讨论了对执法部门使用面部识别软件所带来的担忧。2019 年 7 月，萨默维尔市通过了禁止在公共场所使用面部识别软件的法令，成为继旧金山之后全美第二个禁止面部识别技术的城市。同时，瑞典数据保护局（DPA）曾表示面部识别技术违反了欧盟隐私法规“通用数据保护条例”（GDPR）的若干条款，因此会对非法收集数据的校方处以罚款。

吴沈括进一步告诉记者，围绕面部特征等个人信息的收集、利用，各国法律大多是以用户的“知情-同意”作为合法的基础。没有人否认个人信息数据应该受保护，但如何去保护却难以落实。部分企业会因为法律为数据保护设定的“过高”要求叫苦不迭，认为增加了合规成本。

吴沈括说，目前我国需要进一步推进法治化进程，建立相关法律法规，做到有法可依。这是确保技术不被滥用、限制技术的负面影响、真正发挥其促进社会发展作用的关键所在。

如何防范刷脸泄露隐私？弄懂 APP 的条款

现在要求识别人脸的 APP 越来越多了，我们是否要为了保护自己的“脸”而放弃使用它们呢？这样可能会在生活中遭遇一些不方便吧。那么，我们到底应该如何做呢？

“大众应当提高自我防范意识，认真阅读隐私政策，发现可疑条款或者隐私条款过于模糊不清、晦涩难懂的情况以及对 APP 或者其背后公司信任度不够时，应当拒绝使用该 APP。此外，在个人信息侵权事件发生后，应当及时向法院起诉、向政府有关部门举报。”大成律师事务所高级合伙人陈立彤建议。

“大众能注意的是不要给特别小的人脸识别机构提供照片。”

安恒信息安全研究院院长吴卓群表示，由于人脸识别的方式是先收集人脸数据，然后来匹配验证的，所以人脸识别机构其实已经搜集了很多面部特征、原始图片以及照片，这些都会保留在其服务器上，因此普通的民众很难去规避人脸识别的风险。

不过，吴卓群也提示目前不必太过担忧，毕竟从目前来看，人脸识别被曝光滥用的案例是比较少的。但是，他指出，换脸等攻击方式已经比较普遍了。

不过，吴卓群也表示，对于人脸识别，事实上每一家公司的算法都是有一些区别的，采用不同算法通过不同传感器传回来的人脸数据每一家也都不一样。因此，同一张照片在一家能识别成功，在另一家就不一定能识别成功。（程平 罗亦丹）

广告发行部电话：(0471) 4687563　广告经营许可证：呼工商广字 1501004000013　邮编：010010　本报激光照排印刷：呼和浩特日报社印刷厂　本报零售：每份 1.6 元