

人脸信息泄露可能导致“被贷款”等问题！“刷脸”要守好安全防线

刷脸解锁、刷脸支付、刷脸进小区……当前人脸识别技术已被广泛应用于各种工作和生活场景，给人们生活带来诸多便利的同时，也极大提升了社会运行效率。然而，当“刷脸”成为生活常态，一些“强制刷脸”“无感抓拍”等不当使用乱象以及人脸识别数据滥用等安全风险也日益凸显，应当引起重视和警惕。

人脸识别数据被“强制”收集。日常生活中，部分场景强制要求人脸识别作为唯一验证方式，被“刷脸”或强制“刷脸”认证情况屡见不鲜。个别商家、机构违反个人信息必要原则，过度收集人脸识别数据，甚至通过强迫、捆绑方式收集人脸识别数据，明显超出正常使用需要，导致个人信息存在违法违规收集风险。

人脸图像被不当存储和传输。人脸图像包含丰富的信息，尤其是高精度图像可能包含虹膜、唇纹等相关信息。因此，非必要存储、传输人脸图像有较高安全风险。特别是如将人脸识别数据与个人身份等敏感个人信息关联存储，还可以关联个人行为 and 交往规律，重构特定目标的“关系网”，进而带来更大的安全风险。

人脸识别数据被非法使用。随着人脸识别技术的广泛应用，部分个人信息处理者所持人脸信息呈指数式增长，因人脸信息等身份信息泄露导致“被贷款”“被诈骗”等问题时有发生。例如一些不法分子通过窃取人脸信息，冒充用户身份进行账户注册、实名认证、刷脸支付以及网络贷款，导致受骗者财产损失；甚至还有一些不法分子将非法获取的人脸信息用于洗钱、涉黑等违法犯罪活动，导致用户被无辜卷入，给个人财产安全、公共安全甚至国家安全带来损失。

国家安全机关提示

人脸信息暗藏身份密码，非法使用触碰的是法律红线。人脸信息安全关系数据安全和广大人民群众切身利益，要构建全方位安全保障体系。

强化法治规范。我国《中华人民共和国数据安全法》《中华人民共和国网络安全法》《网络数据安全管理条例》等法律法规相继出台，为我国网络数据安全，以及包括人脸识别技术应用在内的网络应用提供了制度保障。《人脸识别技术应用安全管理办法》作为上述法律、行政法规的关键配套制度，明确了人脸识别技

术的应用边界、使用规则,是对上位法中关于个人信息处理原则的具体细化落实,增强了法律法规的可操作性和执行力,有利于保障新技术合规应用,提升个人信息保护水平。

强化技术防范。建立严格的访问控制机制,定期对人脸识别系统进行安防检查,采用防火墙、入侵测试系统、入侵防御系统等网络安全设备,保护人脸识别系统免受网络攻击。数据采集要遵循最小必要原则,仅采集实现特定目的所必需的人脸数据,避免过度采集,采用先进的加密算法对采集到的人脸数据进行加密存储,且对不再需要的人脸数据及时清理和删除,降低数据泄露风险。

强化自我防范。个人应提高对人脸识别技术安全风险的防范意识,谨记“非必要不提供”原则,除了必要人脸认证之外,在授权使用面部识别前应确保其用途、范围以及信息保护措施,核准正规网络平台和软件,减少个人人脸信息泄露风险。如发现个人人脸信息被非法使用,应寻求法律帮助,维护自身合法权益。

(来源:央视新闻客户端,转引自:新华网,网址:<https://www.news.cn/20250610/8c71774d80b34985b80a6e1005bae953/c.html>。时间:2025年6月10日。访问时间:2025年6月11日9:00。)