人脸识别技术的应用、规范与风险管控

作者：杨迅 | 夏雨薇

- 人脸识别的应用场景
- 涉及人脸识别的主要法律规范
- 人脸识别技术应用的主要条件
- 人脸识别的安全评估和 SDK 风险管控

人脸识别技术是指能够通过图像或视频中的主体的面部特征识别或验证其身份的技术。随着科技的发展，人工智能技术的不断发展，人脸识别技术也逐渐广泛应用在包括金融、商业、交通、安防、教育等各个行业。同时，由于人脸识别技术的使用必然涉及采集和处理作为敏感个人信息的人脸信息，引起了个人信息保护方面的顾虑。近日，铁路系统人脸识别案的判决更是引起热议。

本文拟以笔者在业务中经常处理的金融业和零售业为例，介绍人脸识别技术应用中的个人信息保护和风险防范。

一. 人脸识别的应用场景

近年来，人脸识别技术以其准确、高效和便捷的特点在各行各业得到广泛应用。人脸识别相对于人工辨认更加客观，不容易被化妆等外在因素干扰；同时，人脸识别技术实施时间相对较短，相对人工识别，效率较高；而且，人脸识别支持远程开展，因此相对便捷。因此，在实践中，我们看到人脸识别技术普遍应用于 APP 身份验证、门禁、安保、支付等场景的身份验证和识别。尤其是，我们处理的人脸识别有关项目涉及以下行业和应用场景:

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

(一) 金融服务

在我们法律服务过程中，金融机构是使用人脸识别的主力军。他们使用人脸识别的主要场景包括：金融类 APP 和门禁。

金融类 APP

金融业机构通过收集 APP 提供相关金融服务的情况较为常见。在登录 APP、完成实名认证和相关身份识别的环节，往往涉及人脸识别技术的运用。通过人脸识别验证用户身份的方式，通常能够满足客户身份识别和反洗钱的要求。尤其是，该种方式能够代替金融机构网点的人工验证，特别适用于门店较为稀缺的中型银行、理财公司和公募基金公司。

门禁

金融机构也经常使用人脸识别系统设置门禁。这是因为，金融机构往往储存着许多涉及投资者个人、普遍公众和国家金融安全的信息；尤其是，出于金融监管，金融机构内部也必须设立信息隔离，比如公募基金行业中，投研信息就必须隔离在一般办公环境外，内部不能不受控制地分享。这就需要安全有效地信息隔离措施——除计算机系统的隔离外，通过门禁的物理隔离也是有效隔离手段之一：而人脸识别技术能够提供更为安全可靠的解决方案，不会因为门禁卡丢失导致不便或安全隐患。

(二) 商业零售

在我们的法律服务中发现商业零售机构，比如超市等，也大量使用人脸识别技术。他们使用人脸识别的主要场景包括：市场调研和安保。

市场调研

在商业零售活动中，面对的是广大的不特定公众，需要对公众的行为、背景、偏好深入了解，从而制定相应的营销策略。因此，在商业零售机构的调研活动中，往往涉及识别路人、访客和最终购买者之间的关系。比如确定在广告投放一定范围内的个人或者某个特定地区的个人，进入商业零售场所和在商业零售场所购物的人员之间的关系。这时，人脸识别技术则成为一种有效便捷的技术手段。

安保

部分商业零售机构采用人脸识别技术加强安保。尤其是一些机动化程度比较高，员工较少的大型超市，为减少偷窃带来的损失，安装人脸识别系统：当有前科的个人进入超市时，可通过人脸识别确认并向超市安保员工提供警示，密切关注相关个人的行为。这种自动采集、自动识别的方式，能够便捷有效地减小超市等商业零售机构由于盗窃导致得损失。

二. 涉及人脸识别的主要法律规范

我国关于个人信息的法律法规以及有关判例已经从各个角度提出了使用人脸识别技术的规范要求。

(一) 《个保法》对处理人脸信息的规范

在现有法律体系中，《个人信息保护法》(“**《个保法》**”)和《信息安全技术 个人信息安全规范》(以下简称“**《个人信息安全规范》**”)都在一些方面规范了人脸识别的合规要求。

《个保法》对敏感个人信息做出定义，明确了生物识别信息属于敏感个人信息；进一步地，《个保法》原则性地规定了处理敏感个人信息的要求。该些具体包括: (1)处理敏感个人信息需要具有特定的目的和充分的必要性，采取严格的保护措施，并应取得个人的单独同意; (2)信息处理者应以显著方式、清晰易懂的语言真实、准确、完整地向个人告知其个人信息处理规则，处理相关识别信息的必要性，以及对个人权益的影响。人脸识别信息属于敏感个人信息，因此前述处理敏感个人信息的要求适用于处理人脸信息。

除了前述对处理敏感个人信息的原则性规定，《个保法》第 26 条针对公共场所开展的“人脸识别”活动提出了额外的要求，即置于公共场所的人脸识别设备应设置显著的提示标识。同时，除非取得个人单独同意，人脸识别采集信息的目的只能为维护公共安全。

(二) 《个人信息安全规范》以及其他标准文件对处理人脸信息的规范

《个人信息安全规范》就处理包括人脸信息在内的生物识别信息作出了相对明确、具体的标准和要求，包括:

- 收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意;
- 注销账户的过程需收集敏感个人信息核验身份时，应明确对收集敏感个人信息后的处理措施，如达成目的后立即删除或匿名化处理等;
- 原则上不应存储原始个人生物识别信息(如样本、图像等)，可采取的措施包括但不限于: (a)仅存储个人生物识别信息的摘要信息; (b)在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能; (c)在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像; (d)个人生物识别信息应与个人身份信息分开存储。
- 不应公开披露个人生物识别信息。

此外，《信息安全技术 人脸识别数据安全要求》(“**《人脸数据要求》**”)、《信息技术 生物特征识别人脸识别系统技术要求》等有关开展人脸识别的国家标准，规定了人脸信息处理活动的安全要求，人脸识别系统的架构\业务流程和内控要求。

2023 年 12 月生效的《信息安全技术 个人信息处理中告知和同意的实施指南》("**《告知同意指南》**")则针对"人脸识别"常见应用场景中提出了可供参考的合规措施，在商场等公共场所开展人脸识别的，需要在商场店铺入口或者在或者人脸识别购物柜台张贴或通过屏幕播放个人信息处理规则，并获得用户单独同意——例如引导个人通过扫描二维码的方式阅读相关规则并点击同意。

除了上述通用要求，针对金融行业涉及的人脸识别行为，全国金融标准化技术委员会在《个人金融信息保护技术规范》(JR/T 0171-2020)(以下简称"《个人金融信息规范》")中针对用于人脸识别信息作出特殊规定。具体而言，由于人脸信息属于《个人金融信息规范》规定的 C3 类个人金融信息(用于用户鉴别的个人生物识别信息)，在收集方面，相关金融机构应注意避免委托或授权无金融业相关资质的机构收集人脸信息，此外，在 APP 使用人脸识别技术收集人脸信息时，应采取一定加密技术措施保证数据的保密性，防止其被未授权的第三方获取。在传输、存储人脸信息时，也应使用加密措施，加强人脸信息在金融服务领域全生命周期技术管理与保护，保障个人金融信息主体合法权益。

(三) 《审理人脸识别案件规定》对人脸识别技术应用提出的要求

最高人民法院颁布的《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"**《审理人脸识别案件规定》**")主要从事后纠纷解决角度，对人脸识别活动中侵害自然人人格权益行为的认定、民事责任和免责事由做出规定。

根据《审理人脸识别案件规定》第 2 条，处理人脸信息是否为侵害人格权权益行为，主要从以下角度判断: (1)收集前是否公开个人信息的处理规则，是否征得自然人或者其监护人的单独同意; (2)收集后是否采取相应安全措施防止信息泄露、篡改或丢失，是否违反法律规定或合同约定向他人提供人脸信息，是否违反处理规则处理个人信息；以及(3)处理人脸信息是否违背公序良俗，是否违反合法、正当、必要的原则。

在民事责任承担方面，如涉及多个信息处理者处理人脸信息，侵害自然人人格权益的，需要根据被害人主张，根据其过错程度和造成损害结果的大小承担侵权责任；在满足《民法典》规定的连带责任要件的情况下，该等多个信息处理者可能需要承担连带责任。尤其是，如果共同决定处理人脸信息的范围、方式和目的，共同参与人脸信息的处理活动，无论在哪个环节出现对人脸信息的滥用和侵犯相关个人的个人信息权益，该共同的信息处理人都有可能需要承担连带责任。

此外，《审理人脸识别案件规定》第 5 条规定了信息处理者的免责情形，即: (1)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而处理人脸信息; (2)为维护公共安全，在公共场所依法使用人脸识别技术; (3)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人脸信息。此外，在自然人或者其监护人同意的范围内合理处理人脸信息的，也属于免责范围。

上述《审理人脸识别案件规定》从民事责任及其认定的角度，为企业开展人脸识别中可采取的内控措施提供了更为多元、全面的思路，该些合规措施一方面有助于企业更为安全地处理人脸识别信息；另一方面，当相关争议或纠纷发生，也可以作为企业合理抗辩的依据。

(四) 《人脸识别规定》拟对人脸识别技术应用作出进一步规范

2023 年 8 月 8 日，国家互联网信息办公室发布《人脸识别技术应用安全管理规定(试行)(征求意见稿)》(以下简称"**《人脸识别规定》**")。《人脸识别规定》对人脸识别的使用范围、使用原则、使用规则及相关主体的责任义务作出详细规定。

首先，《人脸识别规定》在呼应《个保法》对采集敏感个人信息的原则要求的基础上，对使用人脸识别技术的场景提出要求，强调旅馆客房、公共浴室、更衣室、卫生间及其他可能侵害他人隐私的场所不得安装图像采集、个人身份识别设备。就其他经营场所而言，《人脸识别规定》要求不得以办理业务、提升服务质量等为由强制、误导、欺诈、胁迫个人接受人脸识别技术验证个人身份，且对于个人自愿选择使用人脸识别技术验证身份的，也需保证其充分知情、主动参与，并在验证过程中保证其得到清晰易懂的、说明该等人脸识别用于身份验证的提示。对在公共场所、经营场所使用人脸识别技术远距离、无感式辨识特定自然人提出要求和限制，对相关服务提出"最小必要"的要求。

其次，《人脸识别规定》对使用人脸识别技术提出了安全性的要求。从管理上说《人脸识别规定》要求法定条件或者取得个人单独同意外，技术使用者不得保存人脸原始图像、图片、视频，除非经过匿名化处理。从技术上说，针对人脸识别技术设备设施，《人脸识别规定》也提出了一系列要求：比如，面向社会公众提供人脸识别技术服务的，相关技术系统应当符合网络安全等级保护第三级以上保护要求，并采取数据加密等一系列安全措施保护人脸信息安全；对所有人脸识别技术而言：应当每年对图像采集设备、个人身份识别设备的安全性和可能存在的风险进行检测评估，并根据检测评估情况改进安全策略，调整置信度阈值，采取有效措施保护图像采集设备、个人身份识别设备免受攻击、侵入、干扰和破坏。

最后，《人脸识别规定》对处理人脸信息的人脸识别技术使用者提出了事前评估及监管备案的要求。即，人脸识别技术使用者处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录，该等个人信息保护影响评估报告应当至少保存三年。如处理人脸信息的目的、方式发生变化，或者发生重大安全事件，人脸识别技术使用者应当重新进行个人信息保护影响评估。在公共场所使用人脸识别技术，或者存储超过 1 万人的人脸信息的人脸识别技术使用者，还应当在 30 个工作日内向所属地市级以上网信部门备案。

三. 人脸识别技术应用的基本条件

人脸识别技术，作为个人信息的处理方式，也需要满足《个保法》下的基本条件，即合法性、正当性和必要性。此外，人脸识别技术作为一种敏感个人信息的处理方式，还需要给予个人选择采取非人脸识别的方式，即满足"不唯一性"要求。

(一) 合法性

人脸识别技术，作为个人信息的一种处理技术，同样需要满足《个保法》规定的合法基础之一。就金融机构的 APP 和门禁场景，以及商业零售业的市场调查和安保场景而言，一般不涉及公共安全，也与履行法定义务无关，因此其合法基础一般在于相关个人的同意。更进一步，根据《个保法》第 29 条，处理敏感个人信息应当取得个人的单独同意；根据第 28 条，生物识别信息属于敏感个人信息；而人脸识别信息属于敏感个人信息。因此，处理人脸识别信息，用于个人身份识别的，应当获得个人的单独同意。

《个保法》没有进一步界定“单独同意”的实现方式。**《告知同意指南》**对单独同意的实施方式作出一些解释，即“特定业务功能涉及需单独同意的情形时，可采用单独的交互式界面或纸质页面向个人告知相关信息。”可见，单独同意要求(1)单独的交互方式；以及(2)告知相关信息。

比如，对于金融 APP 中通过人脸识别和验证用户身份的，可以考虑在注册页“隐私声明”之外，在人脸识别功能页同步弹出“人脸身份认证提示”弹窗，通过要求用户勾选的方式进一步单独确认同意基于身份验证的人脸信息处理。

尤其值得注意的是，基于同意处理个人信息的，法律要求处理者应当向个人完整告知人脸识别信息的处理情况。《审理人脸识别案件规定》第 4 条说明告知要求应具体包括: (1)处理人脸信息的规则、明示处理目的、方式和范围; (2)制定专门的处理规则的方式以增强告知，例如向个人通过弹窗提示专门处理规则。

近期个人诉成都铁路局的案件中，成都铁路局与其委托代理人认为自助实名制闸机运用广泛，且久经媒体宣传，根据日常生活经验，使用者应当清楚刷脸进站时存在收集人脸信息并比对的行为。虽然法院认为采用人脸识别技术并不违法，但其并未认可成都铁路局与其委托代理人对于“告知”的辩护，法院认为成都铁路局存在告知缺陷，现场广播并不是充分告知方式，并发出司法建议书。可见，采用人脸识别的，应当完整地告知相关具体的处理规则。对于金融 APP 而言，可以比较容易通过弹框中的链接转引到相关隐私政策；对于商业零售场景，一般可以考虑店堂告示加广播的方式，或如同国家铁路集团，根据法院出具的司法建议书对网站进行及时更新、对设备进行优化以便更好提供人脸信息采集告知义务。

(二) 正当性

根据《个保法》对正当性的相关要求，处理个人信息不得通过误导、欺诈、胁迫等方式处理。《审理人脸识别案件规定》也要求，不得通过授权捆绑的方式做出单独同意、不得强迫或变相强迫自然人进行单独同意。根据《APP 用户权益保护测评规范 - 个人信息获取行为》，APP 不得存在通过积分、奖励、优惠等方式欺骗误导用户提供人脸等个人信息的行为。通常而言，无论是金融业还是零售业机构，收集人脸信息的核心目的是基于风险控制与企业管理，极少存在欺骗误导行为。

信息处理者需要特别注意的是，为了保证用户能够自由且明确表达同意与否，人脸信息收集的同意机制在设置时不得存在“无法取消同意”、“不同意收集人脸信息 APP 即立刻闪退”等的情况，这种设置也会严重损害用户的自主选择权。

(三) 必要性

“必要性”是《个保法》下处理个人信息的基本要求之一。就收集人脸信息的必要性而言，根据《审理人脸识别案件规定》，人脸信息的收集应当基于提供产品或者服务所必需，信息处理者不得要求自然人同意处理其人脸信息才提供产品或者服务，除非处理人脸信息属于提供产品或者服务所必需。又，根据《人脸数据要求》个人信息处理者应仅在人脸识别方式比非人脸识别更具安全性或者便捷性时方采取人脸识别方式进行身份识别。

比如，就金融机构而言，用户在 APP 上操作金融投资的，金融机构需要验证用户身份，从而通过反洗钱审查以及保护用户账户安全。这种情况下，人脸识别比非人脸识别安全性更高，属于必要的。同样的，金融机构内部需要信息隔离的，通过人脸识别方式能够保障更高的安全性。这些都是人脸识别必要性的体现。

同时，“必要性”也体现在对个人信息的处理行为的限制。即以对个人信息，尤其是敏感个人信息的影响最小的方式和程度处理个人信息，比如保存最短期限，最少人的接触。比如在金融 APP 场景中，通过第三方 SDK 返回识别结果能够满足业务需求的，就不返回真实身份信息；在商场市场调研场景中，通过人脸识别实现广告受众、进店客户和消费客户匹配的，就不需要关联具体的身份；在成都铁路局的刷脸案中，人脸识别设备离线操作，不储存生物识别信息也是最低程度处理个人信息的体现。

(四) 不唯一性

《审理人脸识别案件规定》禁止物业企业或者其他建筑物管理人以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式。《人脸数据要求》进一步规定：个人信息处理者不得将人脸识别方式作为身份识别的首选方式或默认方式，不得设置障碍使得自然人难以选择使用非人脸识别方式。从监管角度，《证券期货业网络和信息安全管理办法》也规定人脸识别方式不得作为唯一的客户身份认证方式。换而言之，在目前的立法趋势下，即使存在必要性，人脸识别也不能作为唯一的识别方式，而必须同时提供非人脸识别的选项。

比如，就金融 APP 而言，如果涉及用户资产查询、修改电话号码等相对不敏感的功能的，一般使用手机号码验证或账号密码验证，人脸识别(或其他生物识别信息识别)可以作为备选项；如果涉及开户、银行卡变更等风险较高的操作的，可以考虑将人脸识别作为选择之一，同时提供线下人工验证等替代方式，从而满足“不唯一性”要求。

四. 人脸识别的安全评估和 SDK 风险管控

人脸识别技术的实施涉及处理个人敏感信息，因此特别考虑处理行为的安全性，实施法律要求的风险防范措施，包括管理措施和技术措施。从管理措施而言，最重要的就是实现的个人信息保护安全评估和人脸识别服务提供商管理。

(一) 个人信息保护影响评估

《个保法》要求在开展一些个人信息处理活动前需要开展个人信息保护影响评估，该些活动包括处理敏感个人信息，而人脸识别属于处理敏感个人信息，因此必须开展个人信息保护影响评估。

虽然，目前尚没有就人脸识别开展个人信息保护影响评估的具体指引，但是参照《个人信息安全规范》等，该评估应该包含以下两个环节: (1)开展人脸识别的合法性、正当性和必要性；和(2)实施人脸识别过程中可能产生的风险、给相关个人带来的影响，以及可以采取的减小风险的措施。而尚未生效的《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第 15 条规定个人信息保护影响评估的内容包括: (一)是否符合法律、行政法规的规定和国家标准的强制性要求，是否符合伦理道德; (二)处理人脸信息是否具有特定的目的和充分的必要性; (三)是否限于实现目的所必需的准度、精度及距离要求; (四)采取的保护措施是否合法有效并与风险程度相适应; (五)发生或者可能发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、非法利用的风险以及可能造成的危害; (六)可能对个人权益带来的损害和影响，以及降低不利影响的措施是否有效。

该影响评估应制成影响评估报告。这不仅仅是《个保法》下的合规要求，也是一旦发生个人信息的泄漏事件时，应对民事责任和行政处罚的重要抗辩依据。

(二) 第三方 SDK 风险管控

对于移动渠道端口而言，实施人脸识别的，一般采用接入第三方 SDK 的方式。这就需要信息提供者管控采用第三方 SDK 的风险。

采用第三方人脸识别 SDK 一般属于第三方 SDK 介入操作，应当遵守接入第三方 SDK 的管理义务。

根据《个人信息安全规范》的相关要求，当个人信息处理者在其提供的服务中接入具备收集个人信息功能的第三方产品或服务，且双方不属于委托处理关系时，个人信息处理者应当遵守第三方接入管理的要求。根据《网络安全标准实践指南——移动互联网应用程序 (App) 使用软件开发工具包(SDK)安全指引》(“**《SDK 指引》**”)中的认定，如果 App 和 SDK 提供者均以单独身份向 App 用户提供服务的，且均自行决定处理方式和目的的，App 提供者应当承担个人信息处理者和接入第三方管理的责任。

以各类 APP 通过人脸识别验证用户身份为例，APP 客户端仅向人脸识别 SDK 开放自身平台：触发人脸识别功能时，人脸识别 SDK 将在 APP 客户端启动并获取该页面的人脸信息，而 APP 客户端本身并不收集并使用人脸信息。当人脸识别 SDK 完成人脸识别后仅向 APP 传输验证结果，而非人脸识别信息本身。这种情况下，虽然从商业上说，SDK 开发者实现的是 APP 开发者委托的事项，但是由于其自身决定处理人脸识别的具体方式，是单独的个人信息处理者。

因此，通过接入 SDK 方式处理人脸识别信息的 APP 开发者需要参照《个保法》对提供个人信息的安全管理要求，对 SDK 的运作开展持续性的安全评估与监督。根据《SDK 指引》的规定，评估需要包括对 SDK 来源安全性、代码安全性与行为安全性的评估。重点包括审阅 SDK 开发者的主体资格、隐私政策、SDK 是否存在法律明确规定的恶意行为，SDK 是否具备足够的信息传输与存储安全能力、以及 SDK 处理个人信息的合规性等。一般而言，我们建议 APP 开发者对 SDK 开发者的技术文档、合规文档、接入协议等文件进行审阅和核查，并通过双方所签署的协议确定处理个人信息的目的、方式，双方责任和义务。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	**伦敦**	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野