

个人信息保护法律热点问题

人脸识别司法解释下的企业合规要点

前言

从社区门禁、刷脸通勤，到人脸登录 App、刷脸支付以及高铁安检，人脸识别给人们生活带来便利的同时，也面临被滥用危害个人安全的风险。3.15 晚会曝光了企业私自采集消费者人脸信息用于客流分析的现象后，各地行政机关加大处罚力度，2021 年 4 月宁波市对 3 家房地产公司分别处以罚款 25 万元¹，2021 年 7 月上海市对某跨国公司中国子公司处以 50 万罚款²。

在围绕人脸信息处理产生的民事侵权、违约纠纷的解决方面，最高人民法院公布了《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》（下称“**司法解释**”）自 2021 年 8 月 1 日起开始实施。本文拟以司法解释为基础，从民事责任角度梳理人脸信息处理的规制框架及企业最新合规要点。

一、“人脸信息处理”的规制概况

1、“人脸信息”的属性

司法解释并未对“人脸信息”做出定义，但明确将“人脸信息”归属于《民法典》规定的“生物识别信息”。结合个人信息相关法律法规及国家标准，人脸信息可以理解作为一种人脸识别特征或者人脸识别数据。根据《信息安全技术 人脸识别数据

安全要求》，人脸识别数据是指，人脸图像³及其处理得到的，可单独或其他信息结合识别特定自然人或特定自然人身份的数据。

同时，结合《民法典》、《个人信息保护法（二审稿）》、《信息安全技术 个人信息安全规范》（GB/T 35273—2020，以下简称“**《信安规范》**”），如下图所示，人脸信息不仅属于生物识别信息，还属于敏感个人信息（是指一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息），需要按照敏感个人信息、生物识别信息的特殊规则进行保护、处理。

个人信息	•个人身份、住址、财产健康等信息
敏感个人信息	•个人财产信息 •个人健康信息
生物识别信息	•人脸、指纹等

2、覆盖人脸信息处理全链条的规制框架

根据最高人民法院副院长杨万明在新闻发布会的说明，司法解释依照《民法典》、《网络安全法》、《消费者权益保护法》制定，同时吸收了个人信息保护立法的经验成果。我们认为，主要体现在以下两个方面：

¹ https://zine.zjol.com.cn/zine/nbnews/202104/t20210421_22421654.shtml

² <http://finance.china.com.cn/news/20210804/5623454.shtml>

³人脸图像（face image）是指，自然人脸部信息的模拟或数字表示。人脸图像可通过设备收集，也可对视频、数字照片等进行处理后获得，主要包括可见光图像、非可见光图像（如红外图像）、三维图像等。

(1) 司法解释依照《民法典》关于“个人信息的处理”的定义，将人脸信息的处理界定为“人脸信息的收集、存储、使用、加工、传输、提供、公开等各个环节，从而将企业的人脸信息处理行为的全链条纳入了适用范围；

(2) 司法解释关于人脸信息处理的规定，实质上整合、反映了《民法典》、《网络安全法》、《消费者权益保护法》、《个人信息保护法（二审稿）》、《信安规范》、《信息安全技术 个人信息告知同意指南（征求意见稿）》（2020年1月20日发布）关于敏

感个人信息、生物识别信息的处理规则（关于敏感个人信息、生物识别信息的具体处理规则、告知同意原则的详细内容，可以参考[《“摇钱树”还是“烫手山芋”——企业应如何处理个人敏感信息》](#)、[《App合规系列一企业收集使用个人信息时如何取得同意（上）》](#)）。

具体而言，司法解释第二条、第十二条的规定涵盖了收集人脸信息之前的告知、单独同意原则，以及不得违约提供人脸信息、信息的安全存储、依法删除等各环节的要求（如下表梳理）。

人脸信息处理流程		违法行为表现
收集/处理前	告知、明示原则	1) 未公开处理人脸信息的规则 2) 未明示处理的目的、方式、范围
	单独同意原则	1) 未征得自然人或者其监护人的单独同意 2) 未按照法律、行政法规的规定征得自然人或者其监护人的书面同意
处理环节	提供	违反法律、行政法规的规定或者双方的约定，向他人提供人脸信息
	安全存储	未采取应有的技术措施或者其他必要措施确保其收集、存储的人脸信息安全，致使人脸信息泄露、篡改、丢失。
	处理	1) 违反企业明示或者双方约定的处理人脸信息的目的、方式、范围等 2) 违背公序良俗处理人脸信息 3) 违反合法、正当、必要原则处理人脸信息的其他情形
消费者权利	删除	消费者请求企业承担违约责任时，请求删除人脸信息的，人民法院依法予以支持。

二、特殊行业人脸识别合规热点

1、合规热点一：物业、建筑物管理人不得仅以人脸识别作为唯一门禁方式

2019年以来，部分城市的小区、写字楼的物业服务企业要求将人脸识别作为出入小区、写字楼等的唯一验证方式，相关人员不刷脸不得进入小区或者写字楼。

根据司法解释第十条，物业服务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，不同意的业主或者物业使用人有权向法院请求为其提供其他合理验证方式。

2、合规热点二：宾馆、商场、体育场馆、娱乐场所等经营场所门店不得违法开展人脸识别

一些商场、娱乐场所等经营场所的线下门店存在较多“无感知收集”人脸分析、识别情况。即一些门店通过私自安装摄像头及后台分析软件，在消费者进入人脸识别区域后，在未向其明示处理规则及采集目的等、也未取得消费者同意的情况下，直接通过拍照录像等形式摄取人脸信息，用于对消费者的年龄、性别、喜好等进行分析。

对此，司法解释第二条第（一）项规定，在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规

定使用人脸识别技术进行人脸验证、辨识或者分析，法院应当认定属于侵害自然人人格权益的行为。

上述司法解释没有对经营者违反何种法律、行政法规做出明确规定，但是根据《消费者权益保护法》第 29 条的规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。由于商场等经营场所的经营者通过抓取人脸信息进行年龄、性别分析的过程涉及到人脸信息的收集，如果经营者没有按照第 29 条的要求履行明示告知及取得同意的手续，该类行为将构成司法解释第二条第（一）项的违法使用人脸识别技术，很可能被法院认定人脸信息权益侵权而被要求赔偿。

3、 合规热点三：企业通过 App 等以捆绑、强迫形式获得消费者同意人脸信息处理构成侵权

部分企业、商家在 App 安装使用过程中，存在强迫收集人脸信息、通过一揽子收集不同意即无法使用、概括授权或者与其他功能捆绑等不合理手段处理人脸信息的现象。

(1) 强迫收集、不同意则不让使用：在人脸信息并非提供产品或者服务所必需的情况下，要求用户同意处理其人脸信息才提供产品或者服务。

(2) 一揽子收集、捆绑授权：在 App 安装规则、用户协议中，将人脸信息的收集、使用规则与其他个人信息的收集、处理规则一起记载，通过同意按钮等一次性征得用户同意，实际上剥夺用户对人脸信息处理的选择权、同意权。

根据司法解释第四条，对于违反单独同意，或者强迫、变相强迫消费者同意处理其人脸信息的，构成侵害自然人人格权益的行为。需要注意的是，第四条的规定不仅适用于线上应用，对于需要告知同意的线下场景也同样适用。

4、 合规热点四：互联网公司 etc 以格式合同排除用户人脸信息主要权利的，相应条款将被认定无效

我们注意到，一些大型互联网公司、新型科技平台公司在日常的业务模式下，出于节省沟通成本、提高业务效率的考虑，往往与大量消费者订立单方

事先拟定的用户协议、服务协议，并在该协议中以格式条款的形式规定关于收集、使用人脸信息的内容。

根据司法解释第十一条⁴，如果企业借助用户协议、服务协议的格式条款，要求消费者授予关于处理人脸信息的“无期限限制、不可撤销、可任意转授权”等权利，消费者有权向法院请求确认格式条款无效。此外，除了以上情形之外，企业应当注意《民法典》规定的格式条款无效的其他情形，如果存在免除或者减轻企业责任、加重消费者责任、限制消费者关于人脸信息主要权利的其他条款，也有可能在判决中被法院认定为无效。

5、 合规热点五：严格的举证责任规定之下，企业在处理人脸信息时应注意“留痕”

基于消费者与企业之间信息不对称等客观情况，关于人脸信息处理时的违约、侵权责任举证机制，司法解释第六条并没有简单在消费者、企业之间平等分配举证责任，尽管第六条第一款列举了一般的“谁主张谁举证”规则，但第六条第二款、第三款从实质上对企业提出了更高的举证责任要求。具体而言：

(1) 根据第二款，企业主张其行为符合《民法典》第 1035 条第一款⁵规定的“合法、正当、必要原则”以及处理个人信息的条件时，应当就相关事实承担举证责任；

(2) 如果企业希望援引司法解释第五条的免责事由⁶主张对于处理人脸信息不承担民事责任的，应

⁴司法解释第十一条 企业采用格式条款与自然人订立合同，要求自然人授予其无期限限制、不可撤销、可任意转授权等处理人脸信息的权利，该自然人依据民法典请求确认格式条款无效的，人民法院依法予以支持。

⁵民法典第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：

（一）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；

（二）公开处理信息的规则；

（三）明示处理信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

⁶第五条 有下列情形之一的，信息处理者主张其不承担民事责任的，人民法院依法予以支持：

（一）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的；

（二）为维护公共安全，依据国家有关规定在公共场所使用人脸识别技术的；

（三）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的；

（四）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；

（五）符合法律、行政法规规定的其他情形。

当就其情形符合司法解释第五条的规定承担责任。

结合《个人信息保护法（二审稿）》第 68 条关于企业过错推定责任的规定⁷，可以发现司法解释延续了个人信息保护法（二审稿）第 68 条对企业处理个人信息时的严格责任要求，如果企业无法举证证明其对个人信息的处理满足上述（1）、（2）情形，很有可能被法院要求承担违约责任或者侵权责任。因此，企业在必需处理人脸信息时，应当就已经向消费者公开处理信息的规则，明示处理信息的目的、方式、范围，以及实际获得消费者的单独同意或者书面同意等事项留存足够的书面证据，防止发生诉讼时被法院要求承担举证责任。

结语

人脸识别司法解释的实施，从门禁管理、门店经营、App 运用等诸多环节强化了对企业处理个人信息的合规要求，为了避免因违法处理人脸信息受到消费者的侵权/违约等民事诉讼及相关赔偿请求，企业应当对照司法解释对收集、处理人脸信息的相关规则进行自查修改。此外，根据最新消息，全国人大常委会将于 8 月 17 日至 20 日开会《个人信息保护法草案》进行第三次审议，《个人信息保护法》近期可能颁布实施。最高人民法院副院长杨万明在 7 月 28 日答记者问时也表示，将及时制定完善其他个人信息保护民事司法解释。企业应持续关注相关立法、司法解释的制定动向，完善个人信息合规要求。

⁷ 个人信息权益因个人信息处理活动受到侵害，个人信息处理者（企业）不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

杨锦文 合伙人 电话：86 10 8553 7608 邮箱地址：yangjw@junhe.com
高 健 律 师 电话：86 10 8519 1359 邮箱地址：gaojian@junhe.com
李圆圆 律 师 电话：86 10 8540 8665 邮箱地址：liyanyuan@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”或君合微信公众号“君合法律评论”/微信号“JUNHE_LegalUpdates”。