【文件名称】：王毓莹：人脸识别中个人信息保护的思考

【发文机关】：《法律适用》2023 年第 2 期

【成文日期】：2023 年 02 月 10 日

【发布日期】：2023 年 02 月 10 日

【网络链接】：https://mp.weixin.qq.com/s/5VHL2tms1FuVTW9XNxllLw

【上传人】：数字经济委

【文件内容】：

王毓莹：人脸识别中个人信息保护的思考

原创 王毓莹 法律适用 2023-02-10 07:00 发表于北京

编者按

为落实中共中央宣传部、教育部、科技部印发《关于推动学术期刊繁荣发展的意见》精神，顺应媒体融合发展趋势，积极适应移动化、智能化发展方向，《法律适用》推出网络优先出版等新型出版模式。目前，已于“中国知网”上线最新一期《法律适用》知网全部首发文章，并于微信公众平台同步推出，敬请关注！

王毓莹　中国政法大学法律硕士学院教授　法学博士

摘　要

随着人脸信息技术的广泛应用，人脸信息领域的法律问题也层出不穷。本文从人脸识别技术出发，结合人脸信息法律属性，对人脸信息处理的行政、刑事、民事法律规范中的问题进行了分析探讨。针对当前人脸信息行政法规范不统一、民事同意原则失灵、刑事入罪标准过高的现实情况，提出行政、民事、刑事法律保护完善建议，并建议严格落实人脸信息处理备案制度、加强人脸信息的数据保护影响评估、推动人脸信息公益诉讼等配套制度。

关键词人脸识别技术　数据保护影响评估　算法备案　公益诉讼

人脸信息的重要用途之一便是人脸识别，人脸识别技术已被广泛应用于社会生活，大到智慧城市的建设，小到手机等 APP 应用的登录解锁，其在金融、电商、安保、娱乐等诸多领域都发挥着巨大作用。人脸识别因高效便捷且成本低廉而被作为密码使用，但是从网络安全角度看，其生物特征有悖用户可随时更改密码的基本原则，并不适合作为唯一安全验证方式。

实践中利用技术或规则漏洞的违法犯罪活动日益加剧，违规收集使用人脸信息的情形比比皆是。在“315”晚会上，央视曝光了多家企业未经告知私自通过监控摄像头搜集消费者人脸信息，涉事企业包含科勒卫浴、宝马、Max Mara 等多家知名企业。为利用好人脸识别这把双刃剑，有必要厘清其法律属性，溯及实践问题的根源，进而有针对性地加以规制和解决。

一、人脸信息的法律属性

（一）人脸信息属于敏感个人信息

“人脸识别是一种基于人的面部特征信息进行身份识别的生物特征识别技术。”人脸识别技术通过采集、存储、分析、识别人的面部特征信息，达到识别身份的目的。人脸识别信息通常包括两个部分，一是人脸原始图像，二是人脸数字特征信息。前者属于人脸识别技术处理人脸信息，获取原始图像，后者属于处理基于人脸识别技术生成的人脸信息，即通过技术将原始图像转化成的数字特征信息。二者均系“使用人脸识别技术处理个人信息相关民事案件”范围。首先，人脸信息系个人信息。其足以单独或者与其他信息结合，用以识别特定自然人的身份，故而属于《个人信息保护法》第 4 条所界定的个人信息。当然，若对人脸信息匿名化处理，如打马赛克等，则其不具有可识别性，不属于个人信息。其次，人脸信息属于个人生物识别信息。欧盟《通用数据条例》（GDPR）将个人生物识别数据定义为经由特定技术处理和获取的有关自然人身体、生理或行为特征的个人数据，并且该个人数据能够识别或确认特定自然人。人脸信息正是基于大数据、人工智能等特定技术处理和获取，与自然人脸部生理特征有关，可以确认自然人的独特身份的个人数据。最后，人脸信息系

敏感个人信息。人脸信息属于“数字人权”，具有唯一性、永久性和不可替代性，一旦被泄露或者非法使用，将引发无底线的算法歧视、无节制的追踪监视、无下限的不信任和提防等不良后果，损害人格尊严，且人脸识别广泛应用于金融支付，人脸信息被盗用，必然危害财产及金融安全，因此属于《个人信息保护法》第 28 条规定的敏感个人信息。

（二）人脸信息具有人格利益属性

人脸信息是否属于私密信息，进而依据《民法典》第 1034 条第 2 款适用人格权中的有关隐私权的规定，尚存争议。肯定说认为，个人生物识别信息包含身体、生理及行为特征，具有高度私密性，关乎人格尊严，包括人脸信息在内的个人生物识别信息属于私密信息。否定说认为，私密信息的标准在于客观上具有私密性、主观上不愿为他人知晓以及是否涉及隐私利益。人脸信息不具有客观私密性，且出于日常交往需要，人们常袒露面部，也不符合主观不愿为他人所知晓的要求，因此不属于私密信息。交叠关系说认为，个人信息与隐私权相互关联又有所区别，包括人脸信息在内的个人信息与隐私权之间存在交叠关系。无论采何种学说，问题的核心在于人脸信息保护适用何种法律规范。可以肯定的是，人脸信息包含人格利益，具有人格利益属性。人脸是社会交往不可或缺的生物表征，承载着社会身份、地位，甚至与传统观念中的“面子”挂钩。《民法典》人格权编具体条款中“等权利”“人格利益”之表述实质上确定了中国民法体系中人格权利保护的开放性。在此背景下，人脸信息的可识别利益，显而易见是《民法典》所确认的信息空间人格权益，因为该类信息直接影响自然人对识别自身身份可能性的控制能力。《人脸识别技术处理个人信息若干规定》第 2 条至第 9 条亦从人格权益和侵权责任角度，界定滥用人脸识别技术处理人脸信息行为的性质和责任。第 2 条以“列举+兜底”的方式明示几类典型行为，明确将非法使用人脸信息界定为侵害自然人人格权益的行为。

二、人脸信息的行政法律保护问题

（一）禁止性法律规范层级低导致区域执法问题

《人脸识别技术处理个人信息若干规定》第 2 条明确界定利用人脸识别技术处理个人信息的侵权行为，第 1 项和第 6 项均提及“违反法律、行政法规的规定”，实则系引致条款，须根据其他关于人脸信息的法律、行政法规判定侵权行为。

在行政法领域，目前并无专门针对人脸识别的法律、行政法规，仅有各地出台的地方性法规。2021 年《深圳经济特区公共安全视频图像信息系统管理条例（草案）》明确禁止在旅馆客房、医院病房、医院检查室、集体宿舍、公共浴室、卫生间、更衣室、哺乳室等可能泄露公民隐私的场所和区域安装系统。禁止利用采获信息非法进行基于人像、人体及车牌等敏感信息的个人身份识别，上述敏感信息用于公共传播时，除法律另有规定外，应当匿名化处理。该条例禁止公共场所采集的信息非法用于人脸识别，且公共传播时须匿名化处理，消除可识别性，本质上不属于传播人脸信息。2020 年《天津市社会信用条例》第 16 条规定，市场信用信息提供单位不得采集自然人的生物识别信息。该条禁止采集的生物识别信息包括人脸信息，市场信用信息是市场主体守法、履约状况的客观数据和资料，与生物识别信息关联不大，符合必要原则。2022 年修订的《杭州市物业管理条例》第 50 条第 2 款规定物业服务人不得强制以人脸识别等方式进入物业管理区域或者使用共有部分。随着老旧小区改造及物业现代化建设，“刷脸”进小区适用广泛，以人脸识别作为门禁方式便于小区物业管理。考虑到人脸信息泄露风险，实际生活不愿“刷脸”的居民很多，上述条例则为业主拒绝小区“刷脸”门禁提供法律支撑。

但是，纵观上述条例，存在以下问题：其一，均属地方性法规，位阶低于法律和行政法规，无法作为《人脸识别技术处理个人信息若干规定》中“违反法律、行政法规”的判断依据。其二，覆盖领域不同且狭小，《深圳经济特区公共安全视频图像信息系统管理条例（草案）》主要规范公共场所，《天津市社会信用条例》旨在构建社会信用信息，《杭州市物业管理条例》则着眼于小区物业管理和服务。其三，分散于深圳、天津、杭州各地，仅适用于各自行政区域内执法。如此种种，无疑导致法律规范对人脸信息保护力度不足、范围不广以及区域执法等深层次问题。

（二）处罚标准不明导致无法有效威慑违法行为

《个人信息保护法》第 66 条规定，违法处理个人信息的责任主体，视情节严重程度，可能会受到没收违法所得、罚款、暂停相关业务或者停业整顿、吊销相关业务许可或者吊销营业执照等相应处罚，直接负责的主管人员和其他责任人员也面临相应数额罚款。该法第 71 条规定，企业违反法律规定，可能受到治安管理处罚甚至承担刑事责任。根据《个人信息保护法》第 60 条、《网络安全法》第 8 条、《数据安全法》第 6 条的规定，国家网信部门、国务院有关部门以及县级以上地方人民政府有关部门为承担个人信息保护职责的部门，电信、公安、国安、交通、金融、自然资源、卫生健康、教育、科技部门等同样是网络安全、数据安全监管部门。极易导致多部门执法问题。

然而，各部法律中违法情节认定标准并不明确，交由行政执法机关自由裁量，导致各地行政机关执法不一。如上海小鹏汽车销售服务有限公司因向第三方公司购买 22 台人脸识别摄像设备于 2021 年 1 月至 2021 年 6 月期间非法采集、上传人脸照片 431623 张，被上海市徐汇区市场监管局处以罚款 10 万元。2021 年 4 月 18 日至 2021 年 10 月 14 日期间，禹州某售楼部共抓拍案例全量到访图片及录像数据 124200 条，客户认证记录 180 条，未明示收集、使用信息的目的、方式和范围，被处罚金 20 万元。前者非法采集、上传人脸照片 40 余万张，仅罚款 10 万元，后者抓拍图片、录像及非法认证记录 12 万余条，却罚款 20 万元，信息数量不足前者三分之一，罚金较前者翻一番，各地执法不一可见一斑。进而衍生出如何计量人脸信息价值问题，以及如何衡量非法采集人脸信息数量与罚款数额之间的关系，径行按比例细化，抑或综合考量其他因素，其他因素又为何种因素，何以具体综合考量，均有不明之处。当罚金与非法采集人脸信息所获利益不对等，甚至远低于利益时，巨大的套利空间将诱发相关主体的侥幸心理，难以有效遏制甚至助长人脸信息识别领域的违法行为。

（三）公权力约束规范不明诱发相关法律风险

为保障公共安全，公共机关早期仅使用身份证件识别公民个人身份，之后应用人脸识别技术，发挥其事后追踪、提供证据的功能，如通过比对人脸信息与犯罪信息数据库，快速锁定犯罪嫌疑人。该行为系在公共场所开展的基于安全的大规模执法或者侦查行为，须公众认知和配合，并不侵犯人脸信息。公权力借助无处不在的摄像头和人脸识别技术不断扩张，虽利于遏制不法行为，但是无形中也限缩私权利的空间，公权力与私权利处于此消彼长的矛盾状态。化解矛盾的关键在于合理界定公权力侵入私权利的范围，即规范公共机关收集人脸信息的适用情形。

当前我国关于公权力主体收集人脸信息的规范尚不明确，实践中人脸识别无差别地适用于刑事违法行为和普通违法行为，如追逃重犯嫌疑人、交通肇事乃至交通违章等，导致各类违法行为分级不明，在普通刑事违法以及普通其他违法行为中，公权力过度侵扰私权利。欧盟《人工智能监管提案》第 19 条规定，出于执法目的，在公共空间使用 AI 系统对自然人进行“实时”远程生物识别，被认为侵犯有关人员的权利和自由，因为它可能影响大部分人的私生活，引起被持续监控的感觉，并间接妨碍人们行使集会自由和其他基本权利。禁止将这些系统用于执法目的，除非这些系统的使用对于实现重大公共利益是绝对必要的，其重要性大于风险。这些情况包括：寻找犯罪的潜在受害者，包括失踪儿童；对自然人的生命或人身安全的特定威胁，或特定恐怖袭击威胁；如果理事会第 2002/584/JHA 号框架决定所述刑事犯罪在相关成员国可判处至少 3 年的最长监禁或拘留，并且根据该成员国的法律规定，可对这些刑事犯罪的犯罪人或嫌疑人进行侦查、定位、鉴定或起诉。根据国内法对监禁判决或拘留令设定门槛，有助于确保只有达到一定严重程度的犯罪才有可能允许使用“实时”远程生物识别系统。欧盟将公权力使用人脸识别的情形限于严重刑事犯罪，或许可结合我国实际情况，借鉴一二。

三、人脸信息的民事法律保护问题

（一）用户与平台地位不平等导致同意原则失灵

《个人信息保护法》第 14 条和《民法典》第 1035 条构建了以“告知—同意”为核心的个人信息处理规则。告知同意原则又称知情同意原则，指信息业者应当充分告知信息主体有关个人信息被收集、处理和利用的情况，并征得信息主体的明确同意。但是，实践中用户和平台地位不平等，平台方以提供免费服务而占据优势地位，用户为免费使用相关服务而处于劣势地位，导致处理人脸信息时知情同意原则失灵，主要表现为违背公开透明原则、单独同意规则以及禁止强迫规则。

告知是处理人脸信息的前提，遵循公开透明原则。根据《民法典》第 1035 条第 1 款第 2 项和第 3 项、《个人信息保护法》第 7 条和第 48 条、《人脸识别技术处理个人信息若干规定》第 2 条第 4 项，处理人脸信息应当严守公开透明原则，明示目的、方式和范围，且个人有权要求处理者解释说明个人信息处理规则。故而，明示处理人脸信息的方式，应当采用尽量简洁、清晰易懂的语言描述，便于个人查阅和保存，至于内容涉及重要事项的，应当采用显著的标识性方式提请个人注意。但是，从目前 APP 应用实践看，个人信息处理者普遍采取弹窗隐私政策或将隐私政策置于页面底端的方式，以概括同意结合特定例外的形式，明示个人信息处理规则。隐私政策的公开透明机制存在的问题较为集中，主要表现为内容冗长、专业性极强、未清晰详细说明处理规则、收集的用户个人信息发生变化时特别是收集内容已涉及个人敏感信息未及时将相应的隐私政策通知用户。如在手机应用市场里下载的 5 款下载量过亿次的 App，平均每款 App 需要用户“阅读并同意”的内容约 27 万字，且其中夹杂大量生涩难懂的法律术语，关涉用户权益的条款则语焉不详。2021 年，新京智库对 78 款在应用商店排名靠前的热门 APP 进行调研，其中 67 款 APP 具有人脸识别功能，而隐私政策条款中未提及人脸识别的应用数量高达百分之五十。但超过 70%的用户很少或从未阅读隐私协议且忽略协议内容的更新提示。相较于一般个人信息，人脸信息作为敏感个人信息，关乎个人人格尊严，应当予以严格保护，处理人脸信息遵循单独同意规则。《个人信息保护法》第 29 条在一般知情同意规则的基础上，要求人脸信息主体作出单独同意。《人脸识别技术处理个人信息若干规定》第 2 条第 3 项规定，未经单独同意处理人脸信息，属于侵害自然人人格权益的行为。信息处理者不得以一揽子告知的方式，将人脸信息与一般个人信息一并告知信息主体，而应当采取分别单

独告知方式。单独同意条款也应当特殊显示，采用足以引起用户注意的方式，例如加粗、变换颜色、字体等途径。同时，同意内容应当避免概括同意或者批量同意，用户接受单独同意的选项不应默认勾选，而交由信息主体主动勾选。但是，实践中同意的模式设计多种多样，单独同意和概括同意之间难以界定，如在同一界面显示多个告知文件，分别涉及人脸信息处理及一般信息处理，为优化用户体验和提高效率，用户可一键勾选或者单独勾选，究竟属于单独同意还是概括同意。多样的现实生活不存在标准模式，也导致实践中别有用心者规避单独同意规则。如某宝 APP 的登录验证和支付指令验证环节均开通了人脸识别，但其仅在隐私政策中通过字体加粗的形式告知用户“脸部图像或者视频属于您的个人敏感信息”，并未就该个人敏感信息的处理做任何单独同意处理。

同意保障个人信息自决权，处理人脸信息禁止强迫同意。《个人信息保护法》未规定同意瑕疵和非自愿同意的法律后果。根据《网络交易监督管理办法》第 13 条第 2 款和《人脸识别技术处理个人信息若干规定》第 4 条，信息处理者不得强迫或者变相强迫个人同意处理人脸信息，具体方式包括与其他授权捆绑、停止安装使用等。强迫或者变相强迫同意，有悖信息主体的真实意愿，其效果相当于未取得同意。但是，实践中 APP 运营商在用户协议中采用“要么同意要么不得使用”的“霸王条款”强迫用户同意处理人脸信息。南都记者抽取了十款金融类、人脸识别类、医疗健康类 App 进行测评，三成被测 App 存在强制授权处理人脸信息问题。

（二）民事救济损害难认定

民事私益诉讼是对人脸信息受侵害当事人最为直接的救济方式。民法典颁布后，《民事案件案由规定》新增个人信息保护纠纷案由，司法实践中涌现出大量案件。如郭长城与东方黑马资本管理（北京）有限公司个人信息保护纠纷一案，又如广州唯品会电子商务有限公司、周彦聪个人信息保护纠纷案。但司法实践对人脸信息的保护尚处于摸索阶段，人脸信息领域相关案例少，较为典型的有“人脸识别第一案”郭兵诉杭州野生动物世界有限公司服务合同纠纷案、人脸识别装置侵害邻居隐私权案。

民事私益诉讼对处理人脸信息不法行为的规制效果并不显著。一方面，基于侵权责任构成要件，救济当事人的前提是存有损害事实，对于损害采“实害说”还是“非实害说”存在争议。侵犯人脸信息很少产生实际损害，更多表现为信息泄露的外部风险和担心信息泄露的内部焦虑。如在郭兵诉杭州野生动物世界有限公司服务合同纠纷案中，园方将入园方式由指纹识别调整为人脸识别，难谓人脸识别侵害了郭兵何种权益，法院以收集人脸信息超出目的，违反正当性原则，判令删除信息。即使人脸信息侵权的风险转化为实际损害，也可能是“多因一果”，难以认定信息处理者的责任份额，导致私益诉讼成本和收益不均衡。另一方面，企业利用互联网技术以及平台商业模式加强对人脸信息数据的掌控力，企业与个人之间的不平等地位导致基于平等关系救济的民事责任难以充分发挥效用。人脸识别技术跨区域广、专业性强，作为信息主体的个人难以证明作为信息处理者的企业存在侵权行为。即使规定个人信息保护侵权采过错推定原则，但是普通自然人并未掌握相关专业技术且无法调查企业内部信息保护运行机制，针对企业利用优势地位主张未实施违法行为或已尽到合理注意义务，难以收集固定证据以提出反证。

（三）监护人同意规则有虚置风险

共青团中央发布的《2020 年全国未成年人互联网使用情况研究报告》显示，2020 年我国未成年网民规模达到 1.83 亿，个人信息未经允许在网上被公开的比例为 4.9%。未成年人心智尚未成熟，在纷繁复杂的网络空间极易受迷惑、欺骗，加之“触网”低龄化趋势明显，个人信息易被侵害，从而影响其身心健康，甚至严重威胁人格尊严和人身安全。为强化未成年人个人信息保护，相关法律法规作出相应规定。《儿童个人信息网络保护规定》第 2 条以 14 周岁为标准界定“儿童”范围，将 14 周岁以下未成年人归于儿童群体。第 8 条进而要求运营者设置专门规则，指定专人负责。《未成年人保护法》第 72 条第 1 款，以监护人同意的方式强化对 14 周岁以下未成年人个人信息保护。《个人信息保护法》第 31 条沿袭该规定，第 28 条将其信息纳入敏感个人信息以进一步强化保护。可见，14 周岁系强化未成年人个人信息保护的年龄标准，14 周岁以上的未成年人与成年

人信息保护一致，14 周岁以下未成年人的个人信息系敏感个人信息，处理其信息须经监护人同意。

问题在于，其一，监护人同意机制存在虚置风险。未成年人可借用他人身份注册账号，规避软件对年龄的强制要求。监护人对自身个人信息已自顾不暇，更疲于应对海量的未成年人个人信息授权确认，加之心理上的边际递减效应，对“同意”的谨慎程度越来越低。此外，个人信息处理者通过邮件、人工电话、人脸识别等验证监护人身份，耗费巨额人力物力成本，很多小型互联网企业无法承受。在这种情况下，监护人同意机制容易被虚置化，无法真正保障未成年人的个人信息安全。其二，以 14 周岁作为强化保护年龄标准是否妥当。尽管 14 周岁以上的未成年人对个人信息已有一定保护意识，但其容易不顾后果地暴露过多个人信息。若缺乏正确引导以及严格保护，极易成为个人信息泄露的重灾地。将年龄划定为 14 周岁的立法模式，能否在尊重未成年人自主权与个人信息保护之间达到巧妙平衡，尚待实践检验。

四、人脸信息的刑事法律保护问题

（一）入罪标准过高不利于打击人脸信息犯罪

《刑法》第 253 条规定侵犯公民个人信息罪，分别以情节严重和情节特别严重划分两档刑罚，但何为情节严重抑或特别严重有待司法适用解释。2017 年，最高人民法院会同有关部门发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号），全面、系统规定侵犯公民个人信息罪的定罪量刑标准。该解释第 5 条第 1 款规定侵犯公民个人信息罪“情节严重”的情形，但是未明确提及人脸信息。该款第 4 项规定住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息，“等”系“等外”，人脸信息作为敏感个人信息，可解释为“等其他可能影响人身、财产安全的公民个人信息”。依据该款，非法获取、出售或者提供人脸信息达到 500 条以上，才认定为侵犯公民个人信息罪基本刑的“情节严重”，方才构

成侵犯公民个人信息罪。该解释第 3 项规定非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上即认定为“情节严重”。

笔者认为，上述量刑标准有待进一步优化。其一，侵犯人脸信息入刑标准过高。从信息数量上看，人脸信息数量是行踪轨迹信息、通信内容、征信信息、财产信息数量的 10 倍，或可推定司法解释认为，人脸信息所蕴含的价值或者重要性远远不敌行踪轨迹等信息。然而，人脸信息系敏感个人信息，一旦泄露将损害人格尊严、人身及财产安全，其重要性即便不高于行踪轨迹等信息，但也可与之等量齐观。其二，概括性定量 500 条的基础何在。不同于其他个人信息，人脸信息具有专有性与不可变更性，于被害人而言，即便泄漏一条，也将造成终身不可挽回的损失，同时人脸信息的失范性传播极易会引发下游犯罪，概括限定失范性传播 500 条以上的人脸信息才被认定为侵犯公民个人信息罪，不利于打击人脸信息犯罪。

（二）人脸信息犯罪滋生下游黑灰产业犯罪行为

侵犯人脸信息而构成侵犯个人信息罪，往往是犯罪链条中的上游，极易滋生下游黑灰产业犯罪。首先，侵犯公民个人信息罪往往可能是电信诈骗犯罪链条中的一环。诈骗分子首先通过网络渠道非法获取公民个人信息，尤其是人脸信息，而后利用所获取的信息实施电信诈骗行为，侵犯个人信息与电信诈骗形成上下游犯罪关系。如徐玉玉案中，被告非法获取个人信息，进而实施电信诈骗，造成徐玉玉死亡。其次，侵犯公民个人信息罪可能是故意杀人罪等人身犯罪的开端。如在最高人民检察院发布的依法惩治侵犯公民个人信息犯罪典型案例“陈某甲、于某、陈某乙侵犯公民个人信息案”中，三名罪犯作为“私家侦探”受雇于闵某，提供闵某妻子郭某的行踪轨迹信息，该信息被闵某用于杀害妻子郭某。该案虽为侵犯行踪轨迹信息，人脸信息也意义非凡，侵犯人脸信息也必然引发此类犯罪。最后，构成侵犯公民个人信息罪的，也可能同时构成其他刑事犯罪。如同时构成《刑法》第 177 条之一所规定的窃取、收买、非法提供信用卡信息罪。

五、关于人脸信息保护完善建议

（一）行政、民事、刑事法律保护完善建议

“良法是善治的前提”，针对法律规范层级低、处罚标准和公权力约束规范不明等人脸信息行政法律保护问题，有必要完善相关法律法规、统一执法标准并且合理约束公权力。**首先**，加强顶层设计，构建关于人脸识别的法律、行政法规体系。在条件成熟时，吸纳地方性法规的有益经验，并结合实践需求，将人脸识别相关的地方性法规上升为法律或者行政法规，提高法律规范的位阶，增强适用效力。**其次**，统一执法标准，明确《个人信息保护法》《网络安全法》《数据安全法》等法律中违法情节认定标准。行政执法机关基于统一的标准，结合侵犯人脸信息不法行为的实际情况，作出相应处罚，防止各地执法畸轻畸重。**最后**，构建约束公权力的规范制度。区别人脸识别适用于严重刑事违法、普通刑事违法和普通其他违法行为等不同情形。当人脸识别适用于侦查刑事违法行为时，须做好刑事程序合规，如严格规范技术侦查措施事前审批程序、遵守保密制度、保障信息主体的事后知情权以及求偿权等权利救济等。

对于人脸信息的**民事**法律保护问题，**其一**，同意原则失灵的根源在于用户与平台地位不平等，主要表现在技术掌握、举证能力、免费使用等方面。用户大多不曾掌握人脸识别技术且举证能力弱，均可归于信息主体私益诉讼能力弱，对此可发展民事公益诉讼，由法律规定的机关和有关组织以及检察机关补足用户的诉讼能力，使得用户与平台处于平等地位，保障同意原则有效贯彻落实。具体制度将与行政公益诉讼制度一并于后文详述。用户为使用平台提供的免费服务不得不同意其处理人脸信息，实则反映用户作为“数字理性”主体的自我修养不足，享受服务不是无成本消费或者搭便车，提供包括人脸信息在内的个人信息是享受服务的对价，用户应当明确自身的权利义务，在真正知情同意的基础上使用服务。**其二**，为解决民事损害认定难问题，应当合理界定侵犯人脸信息的认定标准。“实害说”要求实际造成财产、人身、名誉或者其他损失，“非实害说”仅需存在侵犯权益的行为。采

“非实害说”更契合人脸信息作为敏感个人信息需强化保护的属性，因为侵犯人脸信息较少导致实际损害，更多系致害风险。并且《刑法》规定的侵犯个人信息罪是情节犯而非结果犯，刑法应是“不得已”情形下采取的最后手段，刑法尚且未规定结果犯，民事法律更无须采“实害说”。**其三**，针对监护人同意规则的虚置风险，一方面，顺应“触网”低龄化趋势，加大监护人责任，增强监护人以及未成年人对人脸信息的保护意识，另一方面，明确监护人同意的具体适用方式，并通过技术手段，严格规范监护人同意制度。

至于解决人脸信息**刑事**法律保护问题，可采取以下措施。**其一**，降低侵犯人脸信息入罪标准，建议将人脸信息纳入《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第 5 条第 1 款第 3 项，与行踪轨迹信息、通信内容、征信信息、财产信息并列，非法获取、出售或者提供 50 条以上即应认定为“情节严重”，构成侵犯个人信息罪。**其二**，完善犯罪线索移送制度，全链条打击侵犯人脸信息犯罪及其下游犯罪。横向上，在办理民事、行政等案件中，将发现可能涉及信息犯罪的案件线索移送刑事处理；纵向上，在办理侵犯个人信息犯罪案件中，发现其他犯罪线索的，移送相关部门处理。刑法是抑止不法行为、保护合法权益的兜底法律制度，唯有全链条、全环节严厉打击，方可有效遏制和威慑侵犯人脸信息犯罪行为。

（二）其他配套制度完善建议

1. 源头治理，落实人脸信息算法处理备案制度提高保护效率

现代社会的个人信息处理行为呈现大规模、系统化、持续性的特点。面对具有规模性和事前可规范性的人脸信息处理活动，相较于行政执法的事后性和随机性，事前规制在保护人脸信息方面显然具有更高效率。算法作为人脸信息处理者收集和处理数据、推送信息、调配资源的核心力量，一旦失范将会损害国家利益、社会公共利益和公民合法权益。2021 年 9 月，网信办等九部门印发《关于加强互联网信息服务算法综合治理的指导意见》，以 3 年为期规划了我国现阶段算法治理的基本蓝图，描绘了治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。算法备案作为算法治理机制之一，其性质属于行政备案。此前，网信办曾对非经营性互联网信息服务

和区块链信息服务实行备案管理。《互联网信息服务算法推荐管理规定》第24条规定算法备案制度，要求算法推荐服务提供者提供算法类型、算法自评估报告、拟公示内容等信息。监管部门通过对备案算法的风险评估，保证风险的源头控制；通过记录算法设计和检验，使监管机构能有效地评估、追溯和验证复杂算法。因此，企业应该严格遵守管理规定，落实人脸算法备案制度。

2. 强制规定，增加人脸信息数据保护影响评估强化风险防范能力

欧盟GDPR第35条规定，当数据处理活动可能对自然人权利和自由带来高风险时,应提前评估其对于个人数据保护的影响即欧盟GDPR合规工作中频繁出现的数据保护影响评估(Data Protection Impact Assessment)。关于影响评估机制，我国也有相关规定。《网络安全法》第53条规定网络安全风险评估和安全事件应急预案。在环境影响和食品安全领域也已构建相应的评估机制。无论网络安全、环境抑或食品安全领域，风险防范机制的宗旨一致，皆以提前评估风险的方式强化风险防范能力。从风险等级看，人脸信息领域面临的风险并不亚于网络安全、环境和食品安全领域；从立法技术看，上述领域的评估机制取得良好实施效果，可借鉴延伸至人脸信息保护领域。对人脸信息这一关系人格利益的个人敏感信息领域，建议必要时可要求数据控制者实施人脸信息的数据保护影响评估，从施加数据控制者强制性义务的角度，防范侵犯人脸信息的风险。

3. 补充救济，发展公益诉讼拓宽人脸信息的救济渠道

滥用人脸识别技术违规处理人脸信息，不仅危害个人人身及财产权益，还可能损害公共利益。且实践中被侵权人分散、举证能力弱，通过私益诉讼维权成本高，公益诉讼制度可有效弥补其不足之处。相较于私益诉讼，公益诉讼制度的核心区别在于涉及社会公共利益，其核心难点亦在于社会公共利益的认定。从主体看，“社会公共利益”涉及不特定多数人的利益。但是，人脸信息保护亦是价值权衡的过程，须平衡效率与安全、技术发展与利益保护之间的关系，若不特定多数人的利益严重阻碍技术发展，则需谨慎认定其是否属于公共利益。以公益诉讼保护人脸信息具备政策、法律和实践基础，值得积极稳妥拓展。

首先，发展公益诉讼保护人脸信息具备政策基础。《最高人民检察院关于积极稳妥拓展公益诉讼案件范围的指导意见》和《中共中央关于加强新时代检察机关法律监督工作的意见》强调，要积极稳妥拓展公益诉讼案件范围，探索办理个人信息保护领域公益损害案件。包括人脸信息在内的个人信息保护属于稳妥拓展公益诉讼案件的范围。**其次**，发展公益诉讼保护人脸信息具备法律基础。从案件范围看，侵犯人脸信息属于民事和行政公益诉讼范围。《个人信息保护法》明确侵犯个人信息属于民事公益诉讼案件范围，《人脸识别技术处理个人信息若干规定》进一步规定侵犯人脸信息属于民事公益诉讼案件范围。《行政诉讼法》第 25 条规定，行政公益诉讼的范围为生态环境和资源保护、食品药品安全、国有财产保护、国有土地使用权出让等领域。“等”应作“等外”解释，包括人脸信息领域。从具体制度看，公益诉讼制度已较为健全。《民事诉讼法》和《行政诉讼法》分别规定民事公益诉讼和行政公益诉讼。最高人民法院和最高人民检察院联合颁布《关于检察公益诉讼案件适用法律若干问题的解释》，进一步明确民事和行政公益诉讼案件的诉前程序、管辖、起诉、立案、出庭、裁判、上诉、执行等基本制度。《人民检察院公益诉讼办案规则》进一步细化检察机关公益诉讼制度。人脸信息公益诉讼案件可径行适用现有的成熟制度。**最后**，发展公益诉讼保护人脸信息具备实践基础。自《个人信息保护法》施行起来，2019 年、2020 年、2021 年个人信息公益诉讼的案件数量节节攀升。司法实践中，检察机关积极稳妥探索人脸信息保护公益诉讼。如广州市越秀区人民检察院办理的全省首例向互联网法院提起的涉“人脸识别”公民个人信息保护民事公益诉讼案；上海市奉贤区人民检察院办理的李开祥侵犯公民个人信息刑事附带民事公益诉讼案；苏州市相城区人民检察院办理的看房人被“无感抓拍”检察行政公益诉讼案；等等。司法实践为人脸信息公益诉讼的开展奠定坚实基础。

责任编辑：李国慧
文章来源：《法律适用》2023 年第 2 期