

人脸识别的法律风险和规制

高富平

人类时常使用人脸来辨识个人，而计算机技术出现和应用后，使人具有自动识别个人的能力，这便是今天引人注目的人脸识别技术。这是一项伴随计算机应用，在上世纪 60 年代就出现的技术，只是这几年才日益瞩目。它现在面向移动设备为创新解决方案提供支持（例如，个人照片应用程序和辅助身份验证）。尤其是最近名为 ZAO 的 AI 换脸软件在社交媒体疯狂刷屏，人们只需要一张正脸照就可以对视频中人物的脸进行替换，既可以换成自己的脸，也可以换成别人的脸，能够达到以假乱真的效果。这个软件带来的法律问题已超过迄今为止所有相关的软件和技术，将人工智能“人脸识别”问题推上了风口浪尖。

人脸识别带来的隐忧

人脸识别也称为面部识别，是一种旨在识别图像或视频中人的方法。它通过人的面部特征来识别或验证某个人身份，包括获取、分析和比对三个过程：

（1）人脸探测（face detection），即探测和定位图像和视频人脸；

（2）人脸抓取(face capture)，基于个人面部特征，将面部信息（模拟信息）转变为数字信息（数据）；

（3）人脸匹配，验证两张人脸属于同一个人。人脸识别属于生物测定学（Bio-metrics）范畴，本质上是使用一组关联某人的唯一性识别和验证数据来识别和验证个人身份。识别回答，“你是谁？”验证回答“你是否真的是你所说的你”。随着多维传感器抓取人面部特征技术的进步，人脸识别成为继指纹、虹膜扫描、语音识别等之后识别或验证人身份的便捷生物识别技术。

人脸识别早已经进入我们的日常生活，这项技术逐渐地替代用户名＋密码打开计算机、手机或某个信息系统，我们逐渐享受刷脸支付、进入机场或车站，使用含有人脸

□ 人脸识别带来的安全隐患不是该项技术本身问题，而是应用问题，是用于了不该用于的目的，实施了不该实施的行为。人脸识别本身是一项核验身份，确保个人安全的技术，但是存在技术被不法利用、信息泄露和生物信息滥用三重风险。

□ 从规制内容的角度，人脸识别需要从两个方面加以规制，一是从个人信息保护角度，解决信息泄露和滥用问题；二是从使用行为方式角度，不仅要建立智能化的人脸识别的伦理规范，而且要将以欺诈为目的“换脸”纳入冒充身份违法犯罪行为。

识别的管理软件管理个人照片或在社交网络识别朋友等。人脸识别也正在被广泛应用于当事人身份验证、送达等法律实施和判决执行领域，应用于检测潜在客户特征（如年龄、性别等）以更精准投放广告等商业领域。如此等等的应用，似乎正预示着人脸即身份时代的来临。

与此同时，人脸识别也带来人们对隐私和安全方面的担忧。人脸识别技术本是用来验证“你是否真的是你所说的你”，确保在未亲临现场的情形下，一个行为是由本人亲自实施的，是解决电子支付、网络交易、网络申请公共服务等身份安全问题最有效的技术措施。但是，一旦我们自己的“生物密码”丢失或者被人换来换去，或者他人可以真实地冒充自己，那么验证人身份真实性的最后一道屏障将会崩塌。人脸特征具有终身唯一且无法改变的特点，人们可以频繁更换密码，但很难通过频繁“换脸”来保证账户的安全性。一旦发生“盗脸”，不仅是隐私泄露问题，更是会给自己人身和财产带来安全风险。一旦他人有了跟你面部特征相同的数据，他戴上高清 3D 面具，配合系统指令做出相应动作，就可以实施各种欺詐，演绎现实版的电影《变脸》，具有较大的社会危害性。

安全隐患的关键是应用

但是，上述的安全问题不是该项技术本身问题，而是应用问题，是用于了不该用于的目的，实施了不该实施的行为。人脸识别技术广泛普及使用，使人们可以在公众中识别出某个人，甚至跟踪某个人的位置、运动和跟随等，而该人却不知悉。当该项技术用于侦查犯罪分子就是为了公共安全；当用于跟踪他人，就可能侵犯隐私，干涉他人自由；而冒充他人，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。

正因为该项技术有被人利用于“坏事”的可能，因而就对利用该项技术的主体的信息安全水平提出了更高的要求。人脸被数字化处理后构成了一个人的“活体数据”，一旦泄露或被不法利用，其风险远高于其他识别性信息。我们身份认证所依赖的身份证系统是通过权威的身份登记系统来维系的，对于掌握和利用我们生物身份信息的主体，我们有理由苛以严格的程序和安全义务，以确保生物识别信息的安全，防范无可挽回的风险。

除了生物信息安全问题，还有个人生物信息保护问题。既然个人生物信息是个人信息中最具唯一性的识别信息，那么个人应当控制该

信息的利用，以防范人脸识别所需要的信息或数据在个人不知悉、未参与或未同意的情形下被使用、分享甚至销售。个人信息保护原则是：人生物信息利用的最起码规则。2018 年 12 月 17 日，微软副总裁 Brad Smith 在布鲁金斯学会的会议演讲指出微软在人脸识别技术应用的六项原则：公正（公正地对待所有的人）、透明（记录和清晰指出人脸识别技术能力和限制）、负责（确保该项技术使用可控）、非歧视（禁止用于不法歧视）、告知和同意（使用时告知并获得同意）和合法监控（为实施法律的监控应当确保公民民主自由）。亚马逊公司也主张应负责任地应用面部识别，面部识别不应该以侵犯个人权利（包括隐私权）的方式使用，或者对需要人为分析的场景做出自主决策。所有这些均体现了个人信息保护的基本精神——对人的尊重。因此，人脸识别本身是一项核验身份，确保个人安全的技术，但是存在技术被不法利用、信息泄露和生物信息滥用三重风险。

人脸识别的法律规制

针对上述三种风险我们需要采取相应的规制措施。从规制内容的角度，人脸识别需要从两个方面加以规制，一是从个人信息保护角度，解决信息泄露和滥用问题；二是从使用行为方式角度，不仅要建立智能化的人脸识别的伦理规范，而且要将以欺詐为目的“换脸”纳入冒充身份违法犯罪行为。

从规制方式的角度，仍然是自治与法治相结合。法律的主要功能是明确禁止使用的领域、方法，并规定相应法律责任，树立人脸识别技术应用边界；而在允许的领域或行为应当鼓励行业自治，形成各种商业使用人脸识别技术的最佳准则，建立人脸识别技术应用的行业规范。

在法律不明确的情形下，除了不触碰法律禁止底线外，更要以对人的尊重作为行为准则。不让客户“丢脸”，才能赢得客户“芳心”。

（作者系华东政法大学教授、数据法律研究中心主任）

恶势力犯罪中“纠集者”的刑事责任如何认定

葛立刚

根据 2019 年 4 月 9 日“两高两部”发布的《关于办理恶势力刑事案件若干问题的意见》（以下简称 2019 年《意见》），恶势力一般为 3 人以上，纠集者相对固定。毫无疑问，纠集者是恶势力违法犯罪组织架构中的核心人物，依法严惩“纠集者”也是在“扫黑除恶”刑事司法活动过程中贯彻宽严相济刑事政策的应有之义。那么，涉恶犯罪中哪些恶势力人员应当被认定为“纠集者”？如何确定纠集者的刑事责任范围，以及如何在个案中确定纠集者的具体刑事责任？下面逐一分析：

“纠集者”的认定

2009 年“两高一部”《办理黑社会性质组织犯罪案件座谈会纪要》（以下简称 2009 年《座谈会纪要》）首次对“恶势力”的组织特征做出相对详尽规范的表述，即“一般为 3 人以上，纠集者、骨干成员相对固定”，2018 年“两高两部”《关于办理黑恶势力犯罪案件若干问题的指导意见》（以下简称 2018 年《指导意见》）对此进行了修正，除了人数要求外，其仅规定“纠集者相对固定”，对骨干成员是否固定则未予明确。但对此处“纠集者”的涵义，司法认定中曾出现分歧，一种意见认为其意同 2009 年《座谈会纪要》中“纠集者”的字面含义，仅指召集其他成员实施违法犯罪活动的人员，另一种意见则认为，其应指纠集在一起实施违法犯罪活动的所有成员。

2019 年《意见》基本采纳了前一种意见，指出，纠集者是指“在恶势力实施的违法犯罪活动中起组织、策划、指挥作用的违

法犯罪分子”。也即，在涉恶违法犯罪活动中，只有聚集其他成员、制定违法犯罪计划、指挥违法犯罪活动具体实施的违法犯罪分子，才应当被认定为纠集者。

同时，2019 年《意见》虽然重申了恶势力“纠集者相对固定”的组织特征，但又指出，组织成员较为固定，但多次实施的违法犯罪活动由不同成员组织、策划、指挥，对有前述行为的成员也可认定为纠集者。由此，恶势力中的“纠集者”的固定性要求亦被一定程度弱化。进言之，在恶势力违法犯罪活动中，“纠集者”应包括两种情形：一是恶势力组织中惯常负责组织、策划、指挥的违法犯罪分子；二是在单次违法犯罪中实施上述行为的恶势力组织中较为固定的成员。

纠集者的刑事责任范围

从 2019 年《意见》对“纠集者”的定义看，纠集者在恶势力违法犯罪组织中所起的作用，类似于刑法对“首要分子”的界定，即刑法第 97 条规定，“本法所称首要分子，是指在犯罪集团或者聚众犯罪中起组织、策划、指挥作用的犯罪分子。”而根据刑法第 26 条的规定，对组织、领导犯罪集团的首要分子，按照集团所犯的全部罪行处罚。

那么，是否意味着，恶势力违法犯罪组织中的纠集者是否也应对该组织所犯的全部罪行负责？答案显然是否定的。

首先，恶势力在成员的固定性、组织的稳定性及行为的违法性程度方面均有别于犯罪集团，2018 年《指导意见》及 2019 年《意见》也均对恶势力和恶势力犯罪集团进

行了区分，根据犯罪集团首要分子处罚范围的立法规定，并不能当然推导出恶势力违法犯罪组织中纠集者的应然处罚范围，否则就陷入了类推解释的错误；

其次，首要分子所组织、领导的犯罪集团本就以实施相关犯罪为设立宗旨，将该集团计划内实施的所有犯罪归责于其，亦能体现罪责刑一致，而恶势力组织中的纠集者所实施的纠集行为的效力，并不必然施于整个恶势力组织，正如上文所述，恶势力组织中可能并没有固定的纠集者，纠集者组织、策划、指挥的作用也主要体现在具体的违法犯罪活动中，故在刑事责任的承担范围上应有别于犯罪集团；

最后，恶势力与黑社会性质组织也不同，其本身并不是刑法直接规制的对象，刑法所要打击的是恶势力组织实施的犯罪而不是恶势力本身，或者说，刑法对恶势力的遏制是通过打击其实施的犯罪活动来实现的，所以恶势力违法犯罪活动中纠集者的刑事责任，只有放在具体的犯罪活动中才具有进行规范评价的意义。也即，在恶势力组织实施的犯罪活动中，纠集者只应对其实施了组织、策划、指挥的具体犯罪承担其作为纠集者的刑事责任，而不必然对该组织实施的所有犯罪承担责任。

如何确定纠集者的具体刑事责任

2019 年《意见》要求，对于恶势力的纠集者，“要正确运用法律规定加大惩处力度”。实际上，恶势力犯罪属于一种特殊的共同犯罪形态，对包括纠集者在内的所有恶势力成员的定罪量刑，都应遵循刑法关于共同犯罪的处罚规定。具体而言，在涉恶势力的犯罪活动中，可以通过刑

法关于主犯的规定实现对纠集者的从严惩处。同时由于纠集者的犯罪授意内容通常具有模糊性和概括性，在何种程度上追究纠集者的刑事责任，也是个案认定中亟需厘清的问题。

比如被告人朱某等寻衅滋事一案中，朱某在赌博期间通知其他成员共十余人，携带器械对参赌人员实施殴打，被害人马某被划伤腹部，构成重伤，被害人岳某被殴打致轻伤。该案因证据原因，无法查清重伤是由谁所直接实施伤害行为所致，故对朱某以外的所有人员均以寻衅滋事罪定罪判处，但对朱某则定故意伤害罪。理由即在于，对寻衅滋事的纠集者即朱某而言，其不仅要对自己直接实施的犯罪行为负责，还要对被纠集者在其授意范围内实施的犯罪活动承担刑事责任。朱某主观上明知被纠集者的殴打行为可能导致他人重伤以上结果而仍然纠集人员实施上述行为，客观上也确实发生了致人重伤的结果，其行为完全符合故意伤害罪（重伤）的构成要件。按照罪责刑相适应原则，寻衅滋事罪不足以涵盖上述主客观内容，而应以更重的罪故意伤害罪定罪论处。故在恶势力犯罪案件的司法认定中，应当根据个案具体情况准确认定纠集者的授意范围，纠集者应对被纠集者实施的在其授意范围内的所有犯罪行为承担相应刑事责任，当然，对于超出授意范围的行为，也不能将其归责于纠集者，以真正做到在责任认定中的主客观相统一。

综上，恶势力中“纠集者”的身份认定应放在具体的违法犯罪活动中，并以其实施纠集行为的具体犯罪活动作为确定其刑事责任范围的依据。在个案认定中，还应明确纠集者的授意范围，以准确判定其承担刑事责任的程度。

（作者单位：上海市虹口区人民法院）