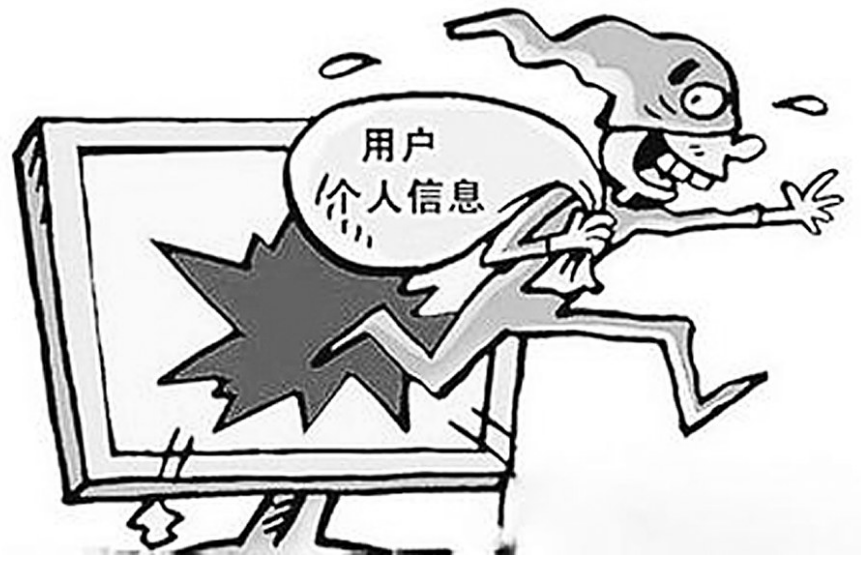
人脸信息灰色产业链引发关注，信息泄露或导致财产重大损失——

隐私信息频遭泄露该如何预防

近日，媒体报道的批量倒卖非法获取人脸等身份信息和“照片活化”网络工具及教程的黑产引起广泛关注。据报道，这些信息在淘宝、闲鱼等网络交易平台上大肆售卖，而且售卖的人脸信息并非单纯的人脸照片，还包含身份证号、银行卡号、手机号等公民个人身份信息。

出售公民信息等隐私数据应该承担怎样的法律责任？公民如何才能更好地保护自己的隐私？《法治日报》记者对此进行了采访。



网上售卖个人信息 肆意侵犯公民隐私

人脸特征信息作为高敏感性信息，与个人身份、金融、行为、位置、偏好等信息相关联。该信息被泄露时，或将导致人们个人财产等造成重大损失。

采访中，中国传媒大学文化产业管理学院法律系主任郑宁认为，出售公民隐私信息对公民日常生活产生的威胁主要有以下三个方面：一是垃圾信息源源不断，当人脸信息被某些刷单类App非法利用时，可能会收到垃圾邮件、垃圾短信、骚扰电话，甚至可能导致被迫网贷、金融账户被用于非法的用途；二是个人财产受到损失，非法中介常利用人脸信息和银行卡、身份证等证件进行贷款、借债或者冒名办卡透支消费；三是公民可能会遭遇裸聊、裸贷、私密信息泄露的危害。

出售公民隐私信息的行为为何屡禁不止？郑宁认为，这是因为售卖者的逐利心理，购买人脸信息的成本极低，被售卖的人脸数据可以用来“撞库”，也就是在不同网站尝试使用相同的帐号、密码获取该用户其他的账户信息，从而达到精准投放广告、精准营销或精准诈骗的目的，以此获得高昂利润。此外，犯罪成本低也是导致公民隐私信息一再被倒卖的原因。

在中国政法大学传播法研究中心副主任朱巍看来，售卖隐私信息是因为有市场需求。从技术角度来讲，这种需求来源于以下几方面：第一是为了“撞库”，“撞库”是指凭借用户的身份信息、人脸识别信息和其他相关信息破解用户账号；第二是为了精准营销，了解个人的运动轨迹，通过人脸比对可以掌握到此人上过什么网站、用过哪些类似的服务等，拿到此人的相关信息后可通过大数据等技术与此人真实身份相结合，实行精准营销；第三是为了精准诈骗，诈骗者通过搜集个人相关信息，了解个人购买的物品，以退票、退钱、更换货物为由，使公民上当，点击诈骗者所提供的二维码，从而进行精准诈骗。此外，还有一些个人目的，比如窥探个人隐私等。

法律助力信息保护 售卖平台难辞其责

关于倒卖公民隐私信息的行为将会受到何种处罚，朱巍说，对于倒卖公民隐私信息，刑法规定了侵犯公民个人信息罪，即将施行的《民法典》在人格权编中围绕“隐私权和个人信息保护”单独设了一章进行规范，可见国家对个人信息保护非常重视。

郑宁介绍，倒卖个人信息涉嫌构成非法获取公民个人信息罪。《刑法》第二百五十三条之一规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。同时，《网络安全法》第四十一条规定了收集、使用个人信息的基本原则：网络运营者收集、使用个人信息应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。《民法典》第一千零三十五条规定，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。消费者权益保护法第五十条规定，经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。

倒卖公民隐私信息的平台是否需要承担相关法律责任？对此，朱巍表示，这涉嫌违法违规销售，按照《电子商务法》的规定，平台应知或明知平台内经营者从事非法业务，平台方有制止的义务，如果不履行此义务，平台方将会承担责任。同时，平台要设立举报渠道，售卖个人隐私涉及刑事犯罪，平台应移交由公安机关处理，若没有举报渠道，平台方也要承担连带责任。

此外，还要看售卖主体是谁，若售卖主体为平台方，则毫无疑问，平台方为违法者；如果平台内经营者是售卖主体，则主要看平台对经营者的行为是否知情。除此之外，还要看经营者是否留下真实的身份信息，如果没有，则按照《电子商务法》的规定，平台方也要承担连带责任。平台承担的责任一方面是基于《电子商务法》中规定的电子商务平台经营者责任，包括对平台内经营者进行资质审核、身份信息的留存、违法违规情况的上报、对应知明知情况的负责等。基于《网络安全法》，平台方有网络安全保障的责任；若平台没有履行网络安全义务，明知道经营者在售卖个人信息而放任不管，则在一定程度上可认定为帮助犯罪。

郑宁说，《侵权责任法》第三十六条第二款规定，网络用户利用网络服务实施侵权行为的，被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。网络服务提供者接到通知后未及时采取必要措施的，对损害的扩大部分与该网络用户承担连带责任。《侵权责任法》第三款规定，网络服务提供者知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。《民法典》也规定，网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。《电子商务法》规定，电子商务平台经营者发现平台内销售或者提供法律、行政法规禁止交易的商品或者服务，应当依法采取必要的处置措施，并向有关主管部门报告。各电商平台应认真履行监督义务，运用大数据技术进行监控，及时发现和下架不合规商品，斩断出卖人脸信息的利益链条。

健全信息保护制度 树立信息保护意识

对于隐私泄露售卖的问题如何根除，郑宁认为，应从国家政府、企业和个人三方面抓起，国家应尽快完善公民生物信息保护的法律体系，加快“个人信息保护法”的立法进程，构建健全的个人信息权利救济和保护制度，明确收集、利用个人信息的范围；在执法方面，加大对企业非法收集和使用公民个人信息的行政处罚力度，提高侵犯公民个人信息的违法成本；在政府自身成为人脸信息搜集主体时，政府要有明确的法律依据并遵循合理必要原则，并限制公权力的过度扩张，尽可能减少对公民个人信息权益的侵犯。企业在采集和使用人脸数据时，应该遵守以下几个原则：用户同意、数据合规使用、透明性、数据安全保护措施、隐私设计、准确性和用户权利、问责制度。公民个人应树立强烈的个人信息保护意识，不随便扫码、注册等。

在朱巍看来，想要解决隐私信息售卖问题，首先要加大处罚力度，其次要将精准诈骗拔出萝卜带出泥，即除了诈骗罪之外，还要看诈骗者是从哪里获取的公民个人信息，要顺藤摸瓜，考虑诈骗背后的问题。除此之外，还要引入新的技术，比如区块链技术。区块链技术可相互验证，每个信息谁阅读了、谁拿走了都是可以留痕的，最好用技术手段解决技术问题。另外，个人信息，互联网实名制等可以构建统一的网站去储存，而不应该把个人信息放在各个商业网站上，通过统一的网站储存，变成EID，由国家统一管理则更好一些。

隐私信息保护对公民自己来说至关重要，对于公民如何更好地保护自己的隐私信息，郑宁给出以下几条具体建议：第一，树立强烈的个人信息保护意识。在个人信息有可能要被采集的时候，要尽可能询问采集的原因和用途、是否有合法依据，以及数据搜集方对数据安全的保护措施。第二，不要随便扫描二维码，不要随便把自己的验证码发给别人。第三，不要随便加微信和点链接，不要在非正规的网站上注册。

朱巍认为，一方面，公民不要随便在“三无”网站上注册信息，不要随便扫描二维码，不要轻易点开他人给的链接；另一方面，一旦发现自己的个人信息出现错误、受到更改、发生遗漏或者超出网站平台使用个人信息的范围等情况，公民可按照法律规定举报或向平台提起诉讼。

朱巍提醒，对于个人来说，公民要学会行使注销权和安宁权。注销权是指公民不再使用某App时，不仅要卸载还要注销，以此消除App中的个人信息；安宁权则指拒收广告等权利。

据新华网