网络存储环节人脸识别信息的刑法保护

宋行健
(湖南师范大学 法学院,湖南 长沙 410000)

摘　要:人脸识别信息系个人数字身份的具体反映,具有多样化的社会功能。在元宇宙、云存储等新兴应用场景中,人脸识别信息刑法保护的必要性日益凸显。网络存储包括人脸识别仿真在内的海量信息,为后续信息共享和处理环节提供了重要的支持。如果网络服务提供者非法存储用户的人脸识别信息,拒不履行信息网络安全管理义务,经监管部门责令改正而拒不改正,并且致使用户信息泄露,造成严重后果的,应以拒不履行信息网络安全管理义务罪论处。在司法适用中,可以从信息网络安全管理义务的具体内容、"致使用户信息泄露,造成严重后果"的认定标准这两个角度入手,界定网络存储环节人脸识别信息的刑法保护范围。在界定信息网络安全管理义务的内容时,应考察信息存储的安全管理制度是否健全以及网络服务提供者处理用户请求的常态化措施是否有效运作。涉案信息数量应适用高度敏感个人信息的保护标准。

关键词:人脸识别信息;刑法保护;信息泄露;信息网络安全;管理义务

中图分类号:D924.3　　**文献标识码**:A　　**文章编号**:1008-7699(2024)06-0035-09

一、问题的提出

在数字时代,人脸识别信息的应用领域及功能日益广泛、多样。人脸识别信息,是指与特定自然人的面部特征相关联的、能够用于识别特定自然人的个人信息。[1]近年来,人脸识别信息的刑法保护引起了我国司法实践的关注,例如在 2023 年的"涉黄 AI 换脸案"中,被告人虞某利用 AI 换脸软件生成大量淫秽视频并传播,被换脸的有不少女明星等公众人物,虞某还提供换脸定制服务,根据 AI 换脸视频的长度、清晰度及视频生成的难易等条件,按照 5 分钟 300 元、10 分钟 500 元等标准来收取定制费用,2023 年 11 月,杭州市萧山区人民法院认定被告人虞某构成制作、传播淫秽物品牟利罪,判处虞某有期徒刑 7 年零 3 个月,并处罚金 6 万元。①

人脸识别信息处理涉及信息获取、提供、网络存储、删除等多个环节,网络存储环节保存人脸识别信息,保障了其他处理环节的有序推进。如果人脸识别信息在网络存储环节保护不当,出现信息泄露,被不法分子用于 AI 换脸等犯罪,将产生刑事风险。因此,学界对网络存储环节的刑法保护展开了初步探讨。一种观点认为,信息处理者不应存储而非法存储信息的,属于对人脸识别信息的非法持有行为,由于"持有"型行为与非法获取行为具有同等的社会危害性,因此可以通过立法上的完善,将"持有"型行为纳入侵犯公民个人信息罪的规制范围。[2]另一种观点认为,行为人合法获取人脸识别信息后,非法存储且拒不履行删除义务,可以被认定为不作为的"非法获取"行为,应按照侵犯公民个人信息罪处罚。[3]然而,前述两种观点或是围绕刑事立法的进一步完善来展开探讨,未能结合现有的刑事立法,提出刑法规制的具体路径,或是在解释过程中超出了"获取"一词的语义范围。本文认为,由合法存储转变为非法存储的情形,不

收稿日期:2024-06-13
基金项目:湖南省教育厅 2023 年度优秀青年项目(23B0101)
作者简介:宋行健(1995—),男,湖南衡阳人,湖南师范大学法学院讲师,法学博士.

① 侯甜.因"AI 换脸"技术被判!案件大量细节曝光[EB/OL].[2024-06-08].https://m.gmw.cn/2024-03/24/content_1303694276.htm.

宜认定为不作为的“非法获取”。可以将《民法典》及《个人信息保护法》所规定的存储、使用、加工、传输这四项公民个人信息的处理环节概括为使用公民个人信息。[4]由于《刑法修正案(九)》未将非法使用公民个人信息的行为入罪,因此,对于实践中的非法存储公民个人信息案件,难以直接适用侵犯公民个人信息罪。[5]

如果网络服务提供者非法存储了用户的人脸识别信息,并且导致其泄露,被他人用于实施盗窃、诈骗、制作淫秽物品等犯罪,那么,能否对网络服务提供者适用拒不履行信息网络安全管理义务罪?这里涉及两个问题:一是,人脸识别信息涉及收集、使用、删除等多个处理环节,以网络存储环节为视角探讨刑法保护问题的依据何在?二是,在拒不履行信息网络安全管理义务罪的适用过程中,应如何从信息网络安全管理义务的具体内容、用户信息泄露所引发的后果等角度,界定网络存储环节中的人脸识别信息的刑法保护范围?

二、网络存储环节人脸识别信息刑法保护的背景

(一)网络存储环节人脸识别信息涉及的新兴应用场景与风险

人脸识别信息与特定的自然人之间具有密切关联,不仅是个人数字身份的具体反映,也发挥着多样化的社会功能。[6]在数字时代,人脸识别信息的网络存储环节涉及一些新兴的应用场景,也面临着一些新的风险。例如,元宇宙能够提供一个持续性的、模拟的、沉浸式的环境,在计算机技术的支持下与用户实时互动。用户能够凭借自己的人脸信息构建数字化身份,在虚拟世界中开展体验与探索,获得一种不同于现实世界的空间体验。[7]从功能角度而言,虚拟世界在与现实社会交互的过程中,用户能够通过对虚拟世界的探索,更充分地认知现实社会中的事物。[8]

元宇宙依托于虚拟现实、增强现实、混合现实等沉浸式系统,为用户营造“沉浸性”或者“临场感”。[9]服务提供者为了提高用户登录的效率,需要存储用户的人脸信息用于验证身份。此外,在用户使用体感交互设备的过程中,服务提供者能够在用户不知情的情况下,记录用户的面部表情变化,进而分析用户的行为偏好,据此对虚拟场景作出个性化设计。然而,服务提供者收集、存储的人脸信息一旦泄露,用户的人身、财产安全将随之面临威胁。

此外,存储载体的多元化、存储形式的云端化,既增强了存储者管理人脸识别信息的能力,拓展了人脸识别信息存储的空间,也对人脸识别信息的刑法保护提出了更高的要求。云存储作为一种新兴的信息存储形式,能够利用网络整合不同类型的存储设备、应用软件。[10]然而,在云存储的过程中,如果信息存储的安全管理不到位,则将导致人脸识别信息泄露。[11]尽管零碎的信息泄露不会对用户权益造成严重损害,但是,如果不法分子将不同类型的个人信息组合、汇集成为一个信息组合体,并且对这些个人信息进行深度挖掘,则将导致用户的个人敏感信息泄露。

(二)网络存储环节人脸识别信息与其他处理环节的关联

德国社会学家尼克拉斯·卢曼提出了社会系统论,认为当代社会已经高度分化、专业化、自律化,社会系统关系日趋复杂化,社会各个系统本质上是各自独立又相互依存的整体。[12]人脸识别信息在社会系统中具有双重价值构造:从信息主体的角度而言,人脸识别信息呈现为个体价值;从社会系统环境的角度而言,人脸识别信息呈现为社会价值。这两种价值之间,体现出相互依存的共生关系,个体价值需要通过社会价值予以反映,而社会价值以个体价值为基础,受到个体价值的限制,需要在保障个体价值的基础上实现。[13]个体价值反映了信息主体在社会交往中的个人身份与尊严,与人身权益、财产权益密切关联。社会价值则体现为人脸识别信息在社会化利用过程中所呈现的工具价值,例如,金融机构通过人脸识别认证,能够保障用户的财产安全。

随着人脸识别信息在社会各领域得到广泛运用,不同的处理环节也分化出不同的应用场景。此时,各项处理环节相当于不同的系统,各类应用场景相当于不同的系统所处的环境,人脸识别信息的各项处理环节之间,呈现出相互依存的共生关系。因此,有必要立足人脸识别信息的全生命周期,对网络存储环

节与其他处理环节的关系展开探讨。

首先，从网络存储环节与收集、使用、加工等处理环节的关系而言，网络存储环节不仅起到了保存人脸信息的作用，而且为人脸识别信息的后续利用提供了重要的支持。以身份识别为例，信息处理者获取人脸识别信息后，要经过数据转换、比对匹配，才能将其用于识别信息主体的身份。其中，比对匹配是实现身份识别的关键，在比对的过程中，需要调取存储在数据库中的人脸识别信息。此外，人脸识别信息的功能从“身份识别”逐渐发展至“识别分析”，也就是在识别信息主体身份的基础上，进一步开展自动化决策。信息处理者调取存储的人脸识别信息后，评估信息主体的健康状况，归纳信息主体的行为习惯，再将所得出的结论用于新的分析，从而形成技术上的闭环。[14]在这一过程中，信息处理者存储的人脸识别信息的数量决定分析结论的准确性。与此同时，如果人脸识别信息因非法存储而遭到泄露，则不法分子在对人脸识别信息识别分析之后，能够将其用于“精准诈骗”等犯罪活动。

其次，从网络存储环节与传输、提供、公开、删除等处理环节的关系而言，网络存储环节要保证人脸识别信息在一定时段内存储状态的安全性，而且达到法定期限之后，信息处理者需要采取妥当措施，终止存储。传输、提供、公开这三项处理环节以人脸识别信息的安全存储为基础，删除则与网络存储环节的终止具有紧密的联系。如果存储、删除环节的衔接出现问题，导致人脸识别信息泄露，则不仅会给信息主体的日常生活带来不便，还会使信息主体的人身、财产权益面临刑事风险，这些危害后果是持续的、长久的、不可逆的。

（三）人脸识别信息“非法存储”的表现形式

在非法存储人脸识别信息的刑法规制过程中，由于存储、获取、提供均属于人脸识别信息的处理环节，因此，可以参考侵犯公民个人信息罪对于“非法获取”与“非法提供”的界定方式。“非法”意味着违反国家有关保护公民个人信息的法律、行政法规、部门规章。[15]在对侵犯公民个人信息罪“窃取或者以其他方法非法获取公民个人信息”中的“非法”一词的理解上，有学者指出，除了应考察行为人获取个人信息的方式是否属于非法外，还应当考察行为人是否具有获取个人信息的法律依据或资格。[16]这表明，对“非法存储”的界定，也可以从存储的方式和依据两个角度探讨。

第一，存储的方式不合法，体现为存储者对人脸识别信息的相关安全管理制度不健全，所遵循的处理规则、操作规程不规范，导致人脸识别信息泄露。《个人信息保护法》《个人信息保护技术指引》《信息安全技术个人信息安全规范》等已行规则和规程，要求妥善选择并安全保管存储介质、根据不同的信息类型采取不同的安全存储方案、建立健全信息访问的控制措施等，以从内外两个方面保障人脸识别信息的安全存储：一方面，对存储介质的选取与管理，应能够从内部保障存储环境的稳定，避免人脸识别信息因存储环境的变化而发生损坏或泄露；另一方面，对不同重要程度的个人信息分别存储，并且通过访问控制来设置不同的访问者权限，从外部保障存储状态的安全，防止未经授权的访问者擅自获取人脸识别信息。

第二，存储的依据不合法，体现为存储人脸识别信息缺乏特定目的和充分的必要性。存储者获取人脸识别信息后，为了更便捷地实现用户身份认证等功能，可以在实现处理目的的必要范围内存储人脸识别信息，并且将存储期限告知信息主体，征得信息主体的同意。但根据《个人信息保护法》第四十七条的规定，在已实现或无法实现个人信息处理目的、信息处理者停止提供产品或服务、个人信息的保存期限已满、个人撤回同意等情况下，信息处理者应当主动删除个人信息。如果存储者在存储期限届满后，没有主动删除人脸识别信息，或是在收到信息主体的请求后，未及时按要求删除人脸识别信息，均属于非法存储。

三、网络存储环节人脸识别信息刑法保护的依据

《最高人民法院、最高人民检察院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》（以下简称《个人信息刑案解释》）第九条规定，网络服务提供者拒不履行法律、行政法规规定的信息网络

安全管理义务,经监管部门责令改正而拒不改正,致使用户的公民个人信息泄露,造成严重后果的,应当依照刑法二百八十六条第一款的规定,以拒不履行信息网络安全管理义务罪定罪处罚。这表明,网络存储环节人脸识别信息的刑法保护,涉及拒不履行信息网络安全管理义务罪的适用。

(一)网络服务提供者的范围界定

由于拒不履行信息网络安全管理义务罪的犯罪主体限于网络服务提供者,那么,网络服务提供者是否包括人脸识别信息的存储者?《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》(以下简称《非法利用信息网络刑案解释》)第一条指出,网络服务提供者包括三种类型,第一种是技术支持类,提供信息网络的接入、计算、存储、传输服务;第二种是信息网络应用服务类,通过应用程序向用户提供网络购物、网络支付、网络直播等服务;第三种是公共服务类,例如电子政务平台可以实现在线审批、在线咨询等功能。网络服务提供者的第一种类型属于网络空间的“开辟者”和“维护者”,第二种、第三种类型则属于网络空间的“运行者”。[17]

从服务内容的角度而言,网络服务提供者的三种类型都涉及人脸识别信息的存储,因为用户需要借助人脸识别信息,向网络服务提供者证明自己的身份,第二种、第三种类型的网络服务提供者,除了在自身的服务器中存储人脸识别信息,还能委托第三方提供技术支持,从而涉及第一种类型的信息网络存储服务。例如,在提供网络金融服务的应用程序中,用户可以在注册账号时录入自己的人脸识别信息,此后就可以采用“刷脸”的方式登录,如果用户需要长期使用这些应用程序,则他们的人脸识别信息将持续存储在服务器中;网络服务提供者则能够根据服务器中存储的人脸识别信息,结合用户的财产信息等其他个人信息,有针对性地向他们推荐不同的理财产品。

(二)“用户信息”与“用户的人脸识别信息”的关联性

拒不履行信息网络安全管理义务罪的入罪情形之一为“致使用户信息泄露,造成严重后果”,而《个人信息刑案解释》将非法存储人脸识别信息的刑法规制范围限定为“致使用户的个人信息泄露,造成严重后果”,那么,“用户信息”与“用户的个人信息”以及“用户的人脸识别信息”具备怎样的关联性?

首先,“用户信息”具有广泛的外延,既包括用户的个人信息,又包括用户在网络上留下的活动轨迹、信息痕迹等。后者虽然反映了用户在访问时的偏好,但由于这些活动轨迹、信息痕迹不能用于识别特定自然人的身份,因此需要与用户的个人信息作出区分。[18]

其次,“用户的个人信息”包含“用户的人脸识别信息”。如前所述,《个人信息保护法》将人脸识别信息列入了“敏感个人信息”的范畴,敏感个人信息在遭受泄露或者被非法利用的情况下,不仅会侵犯信息主体的人格尊严,还将使信息主体面临社会歧视,这是对敏感个人信息专门保护的根本原因。[19]从整体上而言,“用户信息”“用户的个人信息”“用户的人脸识别信息”范围呈现出由大到小的包含关系,当用户在网络环境下使用人脸识别的方式核验身份时,人脸识别信息可归入拒不履行信息网络安全管理义务罪中的“用户信息”的范畴。

(三)人脸识别信息的存储者承担刑事责任的可行性

拒不履行信息网络安全管理义务罪属于纯正不作为犯罪,根据德国刑法理论对于纯正不作为犯罪客观构成要件的界定,值得重点探讨的有“需要性”与“可能性”这两个方面。[20]首先,“需要性”用于判断行为实施的必要性,存储者对人脸识别信息负有保密义务,应根据存储过程中所面临的风险,采取合法有效的保护措施,设立明确的处理规则和操作规程。如果以一般人的标准进行事前判断,存储者在建立并实施相关安全管理制度的情况下,能够降低人脸识别信息泄露的风险,减少人脸识别信息泄露对用户个人权益造成的不良影响,因此,存储者有必要加强对人脸识别信息的安全管理。其次,“可能性”用于判断实施行为的能力。人脸识别信息的存储者管理、支配着人脸识别信息,在这些信息遭到泄露的情况下,存储者不仅具备知悉犯罪发生的可能性,而且具备遏制犯罪发展的可能性。

由于人脸识别信息的存储者属于《非法利用信息网络刑案解释》第一条所规定的“网络服务提供者”,

因此，可以适用网络服务提供者信息控制能力的有关理论。控制力理论在欧盟信息保护领域得到普遍应用，该理论认为，可以根据网络服务提供者在不同情形下对用户信息的控制力，判断网络服务提供者的义务范围与责任轻重。网络服务提供者与用户信息的距离越近，控制用户信息的能力就越强，因此，需要保障用户信息存储状态的安全性；反之，如果网络服务提供者仅临时缓存用户信息，或者仅提供用户信息传输服务，则对用户信息的控制力相对较弱。[21]在持续存储用户信息的情况下，网络服务提供者对用户信息具备最强的控制力，需要健全信息存储的安全管理制度，防止用户信息泄露，而且一旦发现信息存储的安全管理制度存在漏洞，需要及时采取有效措施予以修复。

（四）适用拒不履行信息网络安全管理义务罪的必要性

拒不履行信息网络安全管理义务罪的法益，可以根据其在刑法中的位置来确定。立法者将该罪设置在刑法分则第六章第一节“扰乱公共秩序罪”之中，因此，该罪的法益是社会管理秩序中的信息网络安全管理秩序，具体是指对信息网络安全、合法、稳定运行的监管责任。[22]对于网络存储环节的人脸识别信息而言，由于人脸识别信息具备多样化的社会功能，对人脸识别信息的侵害也将影响信息网络的运行，进而对身份验证、金融交易、安全检查等功能造成干扰。因此，保障网络存储环节的人脸识别信息安全，是保护本罪法益的应有之义。为了有效实现法益保护的目的，在不断完善网络治理法律规范体系的基础上，还需要网络服务提供者有效履行信息网络安全管理义务。

一方面，从网络服务提供者履行信息网络安全管理义务的能力而言，随着互联网技术的发展，人脸识别信息的收集、存储、使用等环节，都由网络服务提供者控制，他们占据着技术主导优势。因此，在人脸识别信息的风险防范过程中，网络服务提供者实际扮演着“守门人”的关键角色。[23]另一方面，从履行信息网络安全管理义务的方式而言，由于网络服务提供者应保障人脸识别信息安全，切断违法关联行为。因此，网络服务提供者具备一定的公共职能，承担着类似于“替代式监管”的职责，其作为市场参与主体之一，按照国家网络监管部门的要求，应采取必要的技术措施保证数据安全。[24]

拒不履行信息网络安全管理义务罪的立法构造，是通过规定网络服务提供者履行信息网络安全管理义务，从而在刑事法和行政法领域内，实现对网络服务提供者不法行为的分层规制，进而促进人权保障机能、法益保护机能的协同实现。[25]首先，适用拒不履行信息网络安全管理义务罪来保护网络存储环节的人脸识别信息，符合我国当前信息网络的治理现状。信息网络将国家、社会、网络服务提供者、公众这四方主体紧密联系在一起，治理主体具备多元聚合的特征，治理规则呈现多元复合的趋势，[26]涉及人脸识别信息的制度、法律、技术之间需要相互配合，才能兼顾科技进步与网络安全。其次，这有利于实现预防性的刑法治理。随着法律制度的预防性功能越发明显，预防已逐渐从新兴法律原则演变为新型法治形态。[27]刑法规制作为社会治理的有机组成部分，也需要根据网络存储环节的人脸识别信息保护需求，对非法侵害人脸识别信息的新型犯罪进行前瞻性的治理。

四、网络存储环节人脸识别信息刑法保护的实现方式

如果网络服务提供者拒不履行信息网络安全管理义务，经监管部门责令改正而拒不改正，导致用户的人脸识别信息泄露，造成严重后果的，则构成拒不履行信息网络安全管理义务罪。在该罪的适用中，需要考察信息网络安全管理义务的具体内容、“致使用户信息泄露，造成严重后果”的认定方式。

（一）对信息网络安全管理义务具体内容的界定

拒不履行信息网络安全管理义务罪作为典型的不作为犯罪，具备双重义务构造，即“履行信息网络安全管理义务”与“责令改正后的改正义务”，履行特定的作为义务是避免法益侵害的逻辑前提。[28]对于信息网络安全管理义务的范围，有学者主张以“信息的传播、治理”为核心，认为不应将信息网络安全管理义务理解为对信息内容的管理。[29]有学者主张将主动审查的义务排除在外，将信息网络安全管理义务限定为“对用户和主管部门报告相关犯罪风险的配合义务”。[30]本文认为，拒不履行信息网络安全管理义务罪

属于采用空白条款的法定犯,以“不履行法律、行政法规规定的信息网络安全管理义务”为前提,需要关注《网络安全法》规定的义务内容。《网络安全法》第七十六条指出,“网络运营者”包括网络的所有者、管理者、网络服务提供者。这表明,“网络服务提供者”属于“网络运营者”的下位概念,需要遵守《网络安全法》第四十条至四十三条的网络运营者义务。

《网络安全法》要求网络运营者对收集的信息严格保密,并且建立、健全信息存储的安全管理制度,具体体现在三个方面。其一,对存储事由的限制。网络服务提供者存储人脸识别信息,应当遵循合法、正当、必要的原则,根据提供服务的内容、时限来确定人脸识别信息的存储范围、存储期限。其二,对存储方式的限制。在存储过程中,网络服务提供者不得篡改、毁损人脸识别信息,应健全安全管理制度,防止人脸识别信息泄露或遗失。与安全管理制度对应的是安全保护义务,《网络安全法》第二十一条规定,网络运营者需要制定安全管理制度和操作规程,采取防范网络攻击、监测网络运行状态与网络安全事件的技术措施,对数据进行分类保护。其三,充分尊重用户的个人信息自决权。网络服务提供者在对人脸识别信息进行网络存储时,需要经过用户的同意,而且当用户发现人脸识别信息的存储方式违反法律法规或双方的约定时,有权要求网络服务提供者删除或更正信息。

由于不同的部门法具有不同的价值追求与规范目的,因此,需要进一步根据拒不履行信息网络安全管理义务罪的规范保护目的,对《网络安全法》规定的义务予以筛选,总结出那些体现刑法价值的作为义务。[31]拒不履行信息网络安全管理义务罪将“致使用户信息泄露,造成严重后果”作为入罪条件之一,因此需要考察两个方面的因素。第一,人脸识别信息存储过程的安全管理制度是否健全,以及当用户报告技术漏洞时,网络服务提供者是否及时处理。这些因素与用户信息泄露之间具有较近的因果关系。第二,当存储期限届满时,网络服务提供者是否已经对人脸识别信息予以删除或做匿名化处理。人脸识别信息表现为原始信息或者仅存储摘要信息。如果网络服务提供者没有遵循前述要求,则人脸识别信息一旦泄露,将引发严重的损害后果。但由于这一后果并非由超期存储独立地引发,根本原因在于存在导致人脸识别信息泄露的技术漏洞,因此,超期存储只能成为附随性的判断标准。

在此基础上,还应继续围绕《网络安全法》与《个人信息保护法》有关“存储方式”与“用户意愿”的规定,进一步细化前述第一项考察因素。首先,在“存储方式”所涉及的义务内容中,应以《网络安全法》第二十一条、《个人信息保护法》第五十一条规定的安全保护义务为依据,认定安全保护义务的履行情况与人脸识别信息泄露之间的关联性。例如,制定内部安全管理制度和操作规程,确定网络安全负责人,采取防范网络攻击、监测网络运行状态的技术措施,将人脸识别信息与其他个人信息进行分类管理,对人脸识别信息做好备份和加密。其次,在“用户意愿”所涉及的义务内容中,根据《网络安全法》第四十三条、《个人信息保护法》第四十六条的规定,当用户发现网络服务提供者违反法律、行政法规的规定或者双方的约定,收集、使用个人信息,或者收集、存储的个人信息与实际情况不符的,有权要求网络服务提供者删除或者更正相应信息。为了及时回应用户的前述请求,网络服务提供者在存储人脸识别信息的过程中,需要设置一种常态化机制,及时地接收、审查用户提出的要求,[32]并且按照这些要求,调整人脸识别信息的存储状态。

(二)对“致使用户信息泄露,造成严重后果”的认定

对于“致使用户信息泄露,造成严重后果”的认定,《非法利用信息网络刑案解释》提出了多项标准,例如泄露的用户信息数量、对被害人人身安全造成的后果、对经济运行与社会秩序造成的危害。该司法解释在第四条第(一)至第(三)项,针对不同类型的用户信息,采取了三种不同的保护标准。第一,“高度敏感信息”适用最严格的标准,该司法解释列举了四种信息,即行踪轨迹信息、通信内容、征信信息、财产信息,泄露达到 500 条以上就属于“造成严重后果”。第二,“可能影响人身、财产安全的用户信息”,包括住宿信息、通信记录、健康生理信息、交易信息等。这些信息允许通过等外解释的方式不断扩张外延,但需要与已经明文列举的这几种信息在重要程度上相当,如果致使信息泄露,造成严重后果,应适用 5 000 条以上的认定标准。第三,对于前述两类信息之外的用户信息,《非法利用信息网络刑案解释》将“造成严重

后果”的认定标准规定为 50 000 条以上。

值得注意的是，该司法解释与《个人信息刑案解释》采取的分类标准相同。《个人信息刑案解释》在第四条的第（三）至第（五）项，将公民个人信息也分为三类，各个类型中的信息内容与《非法利用信息网络刑案解释》完全一致。二者区别在于，《个人信息刑案解释》将“非法获取、出售或者提供公民个人信息，情节严重”的认定标准，按照公民个人信息的三种类型，分别规定为 50 条以上、500 条以上、5 000 条以上。这表明，《非法利用信息网络刑案解释》第四条第（一）至第（三）项有关“用户信息”的界定，与《个人信息刑案解释》第五条第（三）至第（五）项有关“公民个人信息”的界定，具有密切的联系，在适用这两个司法解释时，都需要在现有的三种信息分类标准之下，进一步明确人脸识别信息的刑法保护依据。《非法利用信息网络刑案解释》涉及人脸识别信息在网络存储环节的刑法保护问题，《个人信息刑案解释》则主要围绕侵犯公民个人信息罪的适用来展开，因此涉及人脸识别信息在获取、提供环节的刑法保护问题。

那么，能否将人脸识别信息归入《非法利用信息网络刑案解释》对于用户信息的第二种分类，（“可能影响人身、财产安全的用户信息”）之中？这能否实现信息重要程度与保护强度相适应？首先，以“通信内容”与“通信记录”的关系为例，按照《非法利用信息网络刑案解释》的分类，“通信内容”属于“高度敏感信息”，而“通信记录”属于“可能影响人身、财产安全的用户信息”。二者都反映了信息主体在一定时段内的通信情况。区别在于，“通信内容”对信息的呈现形式更为具体，不仅能够体现通信的对象、持续时间，而且能够独立地反映通信的起因、经过、结果等关键信息；“通信记录”只能反映通信的次数、对象、持续时间，展现的仅是一种概括性的信息。其次，以“财产信息”与“交易信息”的关系为例，按照《非法利用信息网络刑案解释》的分类，“财产信息”属于“高度敏感信息”，而“交易信息”属于“可能影响人身、财产安全的用户信息”。从二者的逻辑关系而言，公民拥有一定数量的财产是其参与市场交易的基础，即使信息主体的一些交易信息遭到泄露，这些信息也只能从局部反映信息主体的交易习惯与消费倾向，而财产信息则更为全面地展现了信息主体的经济实力，一旦泄露，造成的后果也将更为严重。

这表明，人脸识别信息的重要程度与《非法利用信息网络刑案解释》中的“高度敏感信息”更为接近。一方面，从人脸识别信息的功能出发，它与“高度敏感信息”存在密切的关联。以“高度敏感信息”中的“财产信息”为例，它既包括表明财产数量的信息，又包括用于登录银行账户、金融产品账户的身份认证信息，这些信息能够用于确认登录者身份，授予登录者处分账户内财产的权限。[15]当登录者采取人脸识别的方式验证身份时，人脸识别信息就发挥着身份认证信息的功能。再以“高度敏感信息”中的“行踪轨迹信息”为例，通过比对多个采集设备上的人脸识别信息，能够分析出信息主体的行踪轨迹信息。例如，志愿者在照顾独居老人时，通过在独居老人的住所附近设置多个人脸识别信息采集设备，就能够根据每位老人被不同地点的采集设备识别的时间，判断出他们的行踪轨迹，从而有效发现并防范异常状况。另一方面，人脸识别信息具有特殊保护的必要性。《个人信息保护法》在界定“敏感个人信息”的概念时，采取了列举的方式，而且将生物识别信息置于首要位置，足以说明生物识别信息的重要性。由于人脸识别信息与特定自然人之间形成了唯一对应关系，而且具备鲜明的人身属性，因此它的保护不应等同于一般的个人信息。

根据《非法利用信息网络刑案解释》第四条，“致使用户信息泄露，造成严重后果”在认定的过程中，除了根据该司法解释中已经明确列举的几种情形，还可以根据第（八）款，即“造成其他严重后果”这一兜底条款。据此，可以根据人脸识别信息的重要程度，参考“高度敏感信息”的保护标准，将致使人脸识别信息泄露 500 条以上认定为“造成其他严重后果”。在具体认定过程中，可以先计算涉案人脸识别信息的总体数量，再剔除其中重复或者没有实际内容的部分。

五、结语

网络存储环节中人脸识别信息的刑法保护，需要在利用与保护之间寻求平衡，发挥法律与技术的双重保护优势。人脸识别信息能够实现身份辨识、状态分析、属性判断等功能，如果网络服务提供者拒不履

行信息网络安全管理义务,经监管部门责令改正而拒不改正,并导致用户的人脸识别信息泄露,造成严重后果的,应通过明确拒不履行信息网络安全管理义务罪的适用依据与标准,加强人脸识别信息的刑法保护力度。对于人脸识别信息除网络存储以外的其他处理环节应如何加强刑法保护,仍有待在今后的司法适用中进一步探讨。

参考文献:

[1] 孙哲南,赫然.生物特征识别学科发展报告[J].中国图象图形学报,2021(6):1254-1329.
[2] 刘宪权,陆一敏.人脸识别信息刑法保护的构建与完善[J].苏州大学学报(哲学社会科学版),2022(1):60-71.
[3] 李振林.非法取得或利用人脸识别信息行为刑法规制论[J].苏州大学学报(哲学社会科学版),2022(1):72-83.
[4] 喻海松.《民法典》视域下侵犯公民个人信息罪的司法适用[J].北京航空航天大学学报(社会科学版),2020(6):1-8.
[5] 喻海松.刑法的扩张——《刑法修正案(九)》及新近刑法立法解释司法适用解读[M].北京:人民法院出版社,2015:87.
[6] 付微明.个人人脸识别信息的法律保护模式与中国选择[J].华东政法大学学报,2019(6):78-88.
[7] 胡泳,刘纯懿."元宇宙社会":话语之外的内在潜能与变革影响[J].南京社会科学,2022(1):106-116.
[8] 黄欣荣,曹贤平.元宇宙的技术本质与哲学意义[J].新疆师范大学学报(哲学社会科学版),2022(3):119-126.
[9] 张晨原.元宇宙发展对个人信息保护的挑战及应对——兼论个人人脸识别信息的概念重构[J].法学论坛,2023(2):132-141.
[10] 张艺.个人信息存储问题的法律思考[J].贸大法学,2021(1):9-12.
[11] 程慧平,彭琦.个人云存储服务安全风险及治理策略[J].图书馆理论与实践,2018(1):54-60.
[12] 尼克拉斯·卢曼.法社会学[M].上海:上海人民出版社,2013:64.
[13] 欧阳本祺,史雯.社会系统论视域下生物识别信息的刑法平衡保护[J].法治现代化研究,2022(4):37-49.
[14] 韩旭至.刷脸的法律治理:由身份识别到识别分析[J].东方法学,2021(5):69-79.
[15] 周加海,邹涛.《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》的理解与适用[J].人民司法(应用),2017(19):31-37.
[16] 赵秉志.公民个人信息刑法保护问题研究[J].华东政法大学学报,2014(1):117-127.
[17] 李世阳.拒不履行网络安全管理义务罪的适用困境与解释出路[J].当代法学,2018(5):67-76.
[18] 杨楠.个人数位足迹刑法规制的功能性偏误与修正[J].安徽大学学报(哲学社会科学版),2019(4):100-110.
[19] 胡文涛.我国个人敏感信息界定之构想[J].中国法学,2018(5):235-254.
[20] 乌尔斯·金德霍伊泽尔.刑法总论教科书[M].北京:北京大学出版社,2015:376.
[21] 陈奕屹.电子商务平台拒不履行信息网络安全管理义务罪认定的困境与出路[J].法律适用,2020(13):111-123.
[22] 谢望原.论拒不履行信息网络安全管理义务罪[J].中国法学,2017(2):238-255.
[23] 喻浩东.网络空间中信息安全守门人的刑法义务[J].财经法学,2023(4):118-133.
[24] 周光权.拒不履行信息网络安全管理义务罪的司法适用[J].人民检察,2018(9):16-22.
[25] 杜小丽.社会治理视角下拒不履行信息网络安全管理义务罪再审视[J].中国法律评论,2024(3):86-95.
[26] 罗威丽.论违反信息网络安全管理义务的递进式规制模式:从行政命令到刑法惩罚[J].中国人民公安大学学报(社会科学版),2024(2):77-86.
[27] 黄文艺.论预防型法治[J].法学研究,2024(2):20-38.
[28] 姜涛.法定犯中行政前置性要件的法理基础与制度构造[J].行政法学研究,2022(1):63-76.
[29] 敬力嘉.论拒不履行网络安全管理义务罪——以网络中介服务者的刑事责任为中心展开[J].政治与法律,2017(1):50-65.
[30] 涂龙科.网络内容管理义务与网络服务提供者的刑事责任[J].法学评论,2016(3):66-73.
[31] 邹玉祥.论网络服务提供者的信息网络安全管理义务——以刑事不法判断的相对独立性为中心[J].东北大学学报(社会科学版),2020(5):73-80.
[32] 孙禹.论网络服务提供者的合规规则——以德国《网络执行法》为借鉴[J].政治与法律,2018(11):45-60.

Protection of Facial Recognition Information in Network Storage Under the Criminal Law

SONG Xingjian

(*Law School*, *Hunan Normal University*, *Changsha* 410000, *China*)

Abstract: Facial recognition information serves as a tangible manifestation of one's digital identity and fulfills a multitude of social functions. In emerging application scenarios such as the metaverse and cloud storage, the necessity of strengthening protection of facial recognition information is becoming increasingly prominent. The network storage plays a pivotal role in fixing and saving facial recognition information, providing important support for subsequent processing stages. If a network service provider illegally stores facial recognition information of users, neglects its obligations in information network security management, and refuses to take corrective measures as ordered by regulatory authorities, resulting in user information leakage and serious consequences, it may face penalties for failing to uphold its obligations in information network security management. In judicial application, the scope of protection for facial recognition information in network storage can be delineated from two angles: the precise obligations in information network security management and the criteria for determining "causing user information leakage and serious consequences". When defining the content of obligations in information network security management, it is advisable to scrutinize the robustness of the information storage security management system and whether network service providers have effectively implemented standardized procedures for addressing user requests. The volume of information involved in such cases should adhere to the protection standards stipulated for highly sensitive personal information.

Key words: facial recognition information; protection under the criminal law; information leakage; obligation to manage information network security

(责任编辑:董兴佩)