Dispute Settlement 争议解决, 2024, 10(6), 14-22
Published Online June 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.106298

Hans汉斯

深度伪造人工智能的刑事风险应对

张发慧

青岛大学法学院，山东 青岛

收稿日期：2024年4月26日；录用日期：2024年5月9日；发布日期：2024年6月19日

摘　要

深度伪造技术是被称作“生成式对抗网络”(GAN)的人工智能深度学习人类样本，将个人的外貌、声音等生物识别信息伪造合成虚假内容的人工智能技术。目前我国刑法对于深度伪造技术的规制主要存在两种模式。一是对非法获取、出售、提供个人生物信息的上游犯罪进行风险预防的前置性保护模式，二是对利用深度伪造的虚假信息实施诈骗、诽谤等下游犯罪进行事后评价的后端处置模式。但上述两种规制模式都未对非法利用深度伪造技术的行为进行刑事规范，难以规制“合法获取 + 不法利用”生物识别信息的行为，无法实现刑法的规范保护目的。因此，应当对非法利用深度伪造技术行为进行定性分析，加强对个人生物识别信息的刑法保护，将非法利用行为纳入侵犯公民个人信息罪的行为类型，弥补非法利用深度伪造技术的刑法规制空白。

关键词

深度伪造技术，生物识别信息，侵犯公民个人信息罪

Addressing the Criminal Risks of Deepfake Artificial Intelligence

Fahui Zhang

Faculty of Law, Qingdao University, Qingdao Shandong

Received: Apr. 26th, 2024; accepted: May 9th, 2024; published: Jun. 19th, 2024

Abstract

Deepfake technology is artificial intelligence technology called “generative adversarial networks” (GANs) that learn from human samples and forge biometric information such as an individual’s appearance and voice into fake content. At present, there are two main modes of regulation of deepfake technology in China’s criminal law. The first is a pre-protection model for risk prevention for upstream crimes that illegally obtain, sell, and provide personal biological information,

文章引用: 张发慧. 深度伪造人工智能的刑事风险应对[J]. 争议解决, 2024, 10(6): 14-22.
DOI: 10.12677/ds.2024.106298

and the second is a back-end disposal model for post-event evaluation of downstream crimes such as fraud and defamation using deepfake false information. However, neither of the above two regulatory models criminally regulates the illegal use of deepfake technology, and it is difficult to regulate the behavior of "lawful acquisition + illegal use" of biometric information, and it is impossible to achieve the purpose of normative protection of the criminal law. Therefore, it is necessary to conduct a qualitative analysis of the illegal use of deepfake technology, strengthen the criminal law protection of personal biometric information, include illegal use in the type of crime of infringing on citizens' personal information, and fill the gap in the criminal law system for illegal use of deepfake technology.

Keywords

Deepfake Technology, Biometric Information, Crimes of Infringing on Citizens' Personal Information

1. 引言

随着人工智能技术的纵深发展，AI 对于人类的学习模仿已经进入“深水区”。习近平主席高度关注人工智能技术发展，强调“建立健全保障人工智能健康发展的法律法规、制度体系、伦理道德”。深度伪造技术、AI 换脸技术的兴起，使得人们在享受大数据时代带来的信息红利的同时，也承担着个人信息隐私泄露的风险。“科技是把双刃剑”，深度伪造技术隐含法律风险，造成生物识别信息的非法传播使用，危及公民权利、社会秩序与国家安全。为规制深度伪造技术的滥用行为，现行刑法应当聚焦新型网络犯罪研究，把握深度伪造技术等生成式人工智能的技术特征，对深度伪造技术产生的刑事风险类型化处理。因此，如何勘定新兴技术滥用行为的刑法定性，积极弥合刑法规制的缺漏，构筑具有针对性与严密性的刑法应对体系，是当前大数据时代亟需解决的议题。

2. 深度伪造技术：元宇宙时代的机遇与风险

元宇宙时代的到来标志着人工智能发展迈向新阶段，人工智能在为数字网民带来福祉的同时也产生了技术失控与滥用的风险，“数字利维坦”成为人们不得不警惕的风险。深度伪造技术作为人工智能技术的一个分支，其初衷是增强人机交互和社交的娱乐性。但是，深度伪造技术的滥用也带来了诸多数据治理风险。面对新兴技术的“两面性”，明确深度伪造技术的技术特征，将深度伪造产生的犯罪风险类型化处理，是刑法规制深度伪造技术滥用行为的基本前提。

2.1. 深度伪造的技术解构

深度伪造(Deepfake)是计算机的“深度学习”(Deep learning)和“伪造”(Fake)的组合，顾名思义，其出现于人工智能和机器学习技术时代，属于深度合成技术。Deepfake 目前在国际上并没有公认的统一定义，美国在其发布的《2018 年恶意伪造禁令法案》中将“Deepfake”定义为“以某种方式使合理的观察者错误地将其视为个人真实言语或行为的真实记录的方式创建或更改的视听记录”，其中“视听记录”即指图像、视频和语音等数字内容。

深度伪造的技术原理是利用生成式对抗网络(GAN)或者卷积神经网络等算法实现人脸的“嫁接”。

运用深度伪造技术可以让一个“真实的人”做从未做过之事情，说从未说过的话，并且让一般民众无法察觉伪造的违和感。科技的进步在给我们带来充满科技感的视听盛宴的同时，也让我们迷失在人工智能伪造的虚幻迷障中，分不清现实与虚幻。正因此，深度伪造技术伴生着严重的虚假信息传播风险和个人生物信息的非法利用行为。深度伪造的技术内核和类型特征意味着其不可避免地会收集使用自然人的生物识别信息，个人生物识别信息面临被非法利用的风险，亟需现行刑法对非法利用生物识别信息的行为作出回应。

2.2. 深度伪造技术的犯罪行为类型化

深度伪造技术在代码开源后进入公众的娱乐生活领域，进而引发了诸多信息数据风险，网民在利用“Aatarify”“Zao”等软件进行一键换脸娱乐狂欢的同时，一些不法分子借机非法利用深度伪造技术进行违法犯罪活动，涉及伪造色情视频、传播虚假信息或广告，危及个人和企业的合法权益、社会秩序甚至国家安全。具体案例见表 1。

Table 1. Classification of crimes involving deepfake artificial intelligence
表 1. 深度伪造技术犯罪行为涉及的罪名分类

时间	事件	性质	可能构成的罪名
2017	黑客攻击卡塔尔通讯社发布卡塔尔元首的虚假讲话	国家安全	危害国家安全罪
2018	印度记者 Rana Ayyub 遭到伪造色情视频报复	名誉权、肖像权	侮辱罪、传播淫秽物品罪
2019	AI 换脸软件 ZAO 在中国发布	肖像权	侵犯公民个人信息罪
2020	上海某公司高管因对方伪装成公司领导被诈骗 150 万元	财产权	诈骗罪
2021	杭州市陈某被女友伪造不雅视频敲诈勒索	财产权、肖像权	敲诈勒索罪
2023	福州市某科技公司法人代表被犯罪分子利用 AI 换脸技术冒充其好友诈骗 430 万	财产权	诈骗罪

由上表可知，深度伪造技术的非法利用行为引发的刑事风险主要集中在侵犯公民个人信息的上游犯罪和利用伪造虚假信息破坏国家安全、社会秩序以及侵犯公民人身权利和财产权利的下游犯罪。深度伪造技术主要涉及以下三类犯罪类型。

第一，利用深度伪造技术侵犯公民个人信息。例如，在张富、余杭飞、史良浩等侵犯公民个人信息罪 [1] 一案中，被告人张富、余杭飞等人以牟利为目的，利用已非法获取的公民个人信息，通过使用软件将相关公民头像照片制作成公民 3D 头像，从而通过支付宝人脸识别认证，并使用上述公民个人信息注册支付宝账户，此案中，被告人利用深度伪造技术生成人脸识别动态图的行为构成侵犯公民个人信息罪。在人脸识别关联银行账户、交通出行的数据时代，生物识别信息具有唯一性、独特性，非法获取个人生物识别信息的行为具有严重的社会危害性，情节严重，刑法应当予以严厉规制。

第二，利用伪造的虚假信息破坏国家安全与社会秩序。美国国会研究服务处发布《深度伪造与国家安全》报告指出，深度伪造已成为国家信息战的技术手段，对手可以通过利用深度伪造技术，生成虚假新闻报告，破坏公开披露的信息，瓦解公众对公开信息的信任等。2022 年，乌克兰总统泽连斯基宣布投降的深度伪造视频于 3 月 16 日出现在社交媒体平台。深度伪造的虚假新闻借助互联网飞速广泛传播，对国家安全与社会秩序具有极强的破坏性。

[1] 张富、余杭飞、史良浩等侵犯公民个人信息罪案，浙江省衢州市中级人民法院(2019)浙 08 刑终 333 号刑事判决书。

第三，利用伪造的视频侵犯公民的人格权和财产权。未经同意的色情内容是迄今为止 Deepfake 技术的最大用途。这种趋势几年前首次出现在 Reddit 上。用户会拍摄现有的成人视频，并用名人的脸替换表演者的脸，严重侵害了个人的名誉、肖像等人身权利。此外，利用伪造的色情视频对被害人实施敲诈勒索的犯罪行为也呈现泛化趋势，使得公民的人格权和财产权都遭受着巨大的风险。另外，深度伪造技术为电信网络诈骗提供了新型的诈骗手段，行为人通过盗用个人生物识别信息合成视频、语音冒充信息权利主体，对第三人实施电信诈骗。

3. 深度伪造技术的刑法既有规制模式及困境

目前，涉及深度伪造技术的刑法规制呈现双重维度：一是指向深度伪造行为侵害公民个人信息的风险预防模式。二是指向法益侵害后果的事后规制模式。但上述规制体系编织的刑事法网存在“空隙”，为倒卖个人信息的黑灰产业链提供了可趁之机。

3.1. 前置保护模式：保护个人信息法益

我国现行刑法对于公民个人信息采用前置保护方式。2009 年，《刑法修正案(七)》增设了非法获取公民个人信息罪和非法出售、提供公民个人信息罪，2015 年《刑法修正案(九)》将《刑法修正案(七)》增设的两个罪名整合为一。深度伪造技术指向的生物识别信息较一般的个人信息具有人身专属性和唯一性，规制深度伪造技术的滥用行为符合《刑法》保护公民个人信息的当然旨趣。

司法实践中，深度伪造技术侵犯公民个人信息、隐私权的案例屡见不鲜。杭州野生动物世界案作为人脸识别的第一案，敲响了公众对于个人信息保护的警钟。此后，对深度伪造技术滥用行为予以刑法规制的案件屡见不鲜。诸如，在王小明、周思寒侵犯公民个人信息罪[2]一案中，被告人王小明利用被告人周思寒提供的人脸识别视频制作软件和方法，将非法获取的公民个人信息制作成人脸识别视频后，以 60 元至 90 元不等一条的价格出售给游戏玩家完成人脸认证。两被告人利用深度伪造技术牟利，侵犯不特定多数人的个人生物识别信息，达到“情节严重”的数量标准，均构成侵犯公民个人信息罪。

在 Web3.0 时代，个人信息、隐私数字化，呈现高度融合性和开放性。例如新冠疫情期间的健康码，就是公民个人的姓名、身份证号、行踪轨迹、身体健康状况等信息的集合体。公民个人信息的泛数据化，使得深度伪造技术的数据样本更易获得，深度伪造技术在大数据时代异化，严重侵害公民信息和隐私。“在预防型刑法理论的影响下，对于非法获取、出售或者提供生物识别信息的行为，应予以适度的前置规制防止下游黑灰产业链犯罪行为的突变。”[1]因此，规制深度伪造技术的滥用行为关键要从源头管控，保护公民的个人信息安全。

3.2. 事后规制模式：基于法益侵害后果

随着元宇宙时代的到来，网络空间成为承载和传播公民个人信息的场域，为深度伪造技术等生成式人工智能的发展提供了大量的数据样本。每个公民都是大数据时代的“透明人”，个人信息成为“数字金矿”，不仅滋生出非法利用生物识别信息的网络犯罪，也使得传统犯罪手段异化，并形成上下游配合的链条结构，严重危及国家安全、社会秩序以及公民的人格尊严与财产权等传统法益。

深度伪造技术直指公民的生物识别信息，并通过对生物识别信息的加工改造以达到下游犯罪的目的。“生物识别信息传播的时间维度强调历程性，由初始阶段演变为发展阶段后，又异化至失范阶段。”[1]深度伪造技术的滥用行为使得生物识别信息的传播进入失范阶段，为实施下游犯罪提供便利。司法实践中，鉴于侵犯公民个人信息罪“情节严重”的数量标准难以认定，且行为人多以深度伪造的生物识别信

[2]王小明、周思寒侵犯公民个人信息罪案，湖南省宁乡市人民法院(2022)湘 0182 刑初 127 号刑事判决书。

息为工具进行下游犯罪，所以刑法规制侧重于将深度伪造技术作为异化的传统犯罪手段，基于下游犯罪行为侵犯的不同法益对深度伪造技术予以规制。诸如，行为人利用合成的面部动图突破微信、支付宝等平台的人脸认证系统转移被害人财产的犯罪行为被认定为盗窃罪，在林广龙、邓庆材盗窃案[3]中，被告人邓庆材骗取被害人的生物识别信息后，利用深度伪造技术将图片活化，破解微信的身份认证措施，将被害人账户内的财产占为己有。由此观之，在法律适用过程中，上游的侵犯公民个人信息行为被下游的犯罪行为所吸收，刑法对深度伪造技术的规制运用基于侵犯法益后果的事后规制模式。

3.3. 现实难题：生物识别信息的滥用现象

有学者主张，“深度伪造技术所蕴含的技术风险在于对虚假信息造成社会危害的‘加成’效果，其不当利用可能会加剧法益侵害的程度或者使法益侵害复合化。”[2]该观点对于深度伪造技术的风险评价值得商榷。笔者认为，深度伪造技术的滥用行为实质上是对公民个人生物识别信息的滥用，而无论是前置保护模式还是事后规制模式都未对生物识别信息予以特殊保护，现行刑法体系难以规制“合法获取 + 非法利用”生物识别信息的犯罪行为。

其一，前置保护模式并未突出生物识别信息非法利用行为的社会危害性。现行刑法对个人信息“合法获取 + 非法利用”行为的规制存在法律缺位。《刑法》第 253 条规定了出售、提供和非法获取三种行为类型，并未对合法获取后的非法利用行为予以评价。但深度伪造技术的数据库大部分来源于网络上的公开信息。诸如，网络用户发布在互联网上的照片和个人信息，以及政治领导和公众人物的公开数据信息。此外，“深度伪造行为与后端行为可能是割裂的，例如制作视频并转让给他人的行为，对制作视频者就难以按照后续的行为处罚。”[3]深度伪造的非法利用行为是对信息权利主体的进一步侵害，其行为具有更严重的社会危害性。

其二，事后规制模式难以实现法益保护目的。“某些深度伪造技术滥用行为根据现有刑法规定却无法定罪论处。”[4]诸如，利用 AI 换脸进行恋爱欺骗的行为，以及冒用明星形象欺骗粉丝刷礼物的行为。此外，对深度伪造技术的事后规制基于已然发生的法益侵害后果，是对犯罪行为的后端评价，难以应对大数据时代生物识别信息非法传播迅速的风险。

综上所述，现行的刑法规制模式无法抵御实践中个人生物识别信息的非法利用风险，亟需弥补对合法获取后非法利用深度伪造技术伪造生物识别信息的行为进行规制的法律空白。

4. 深度伪造技术的刑法规制完善路径

新兴技术的快速发展与法律的滞后性之间的冲突必然会产生法律风险，深度伪造技术的超越性致使现行刑法体系无法规制深度伪造技术滥用行为。因此，应当从深度伪造技术滥用生物识别信息的本位思维观念出发，与《个人信息保护法》等前置法相衔接，明确生物识别信息在个人信息分类分级制度中的定位，厘清深度伪造技术滥用行为的刑法定性，重塑深度伪造技术滥用行为的刑事治理样态，将生物识别信息滥用现象纳入教义学体系之内，并对其进行适当的规制，实现风险的预防[5]。

4.1. 厘清深度伪造技术滥用行为的刑法定性

“生成式人工智能在刑事犯罪领域的风险可以分为外源性技术滥用风险和内因性数据安全风险两部分。”[6]应当明确的是，深度伪造具有两层面向：一是深度伪造技术，即 Web3.0 时代的生成式人工智能技术；二是深度伪造信息，属于涉生物识别信息的敏感个人信息。深度伪造技术具有技术中立性，秉持刑法谦抑性的应然立场，刑法规制的应当是深度伪造技术的滥用行为。有学者认为，“滥用‘深度伪

[3]林广龙、邓庆材盗窃案，湖北省巴东县人民法(2021)鄂 2823 刑初 48 号刑事判决书。

造’技术行为的本质是借助于他人的生物识别信息实现身份冒用”[7]，主张增设“身份盗窃罪”来规制深度伪造非法利用行为。与之持相反观点的学者认为，“伪造信息的行为本身不具有独立的违法性，因为伪造行为的目的会被后续其他行为的目的所吸收，所以深度伪造的行为本身不应成为我国刑法的归责对象。”[8]笔者认为，上述两种观点都具有理论缺陷。

4.1.1. 身份盗窃观点之批驳

其一，深度伪造技术非法利用行为的法益侵害后果并未突破传统的公民个人信息犯罪的框架。深度伪造滥用行为的本质是对生物识别信息的侵害，而在《民法典》《个人信息保护法》等前置法规范体系下，生物识别信息仍属于公民个人信息范围。“刑法上的犯罪不可能仅按照行为手段进行分类，而是要按行为所侵害的具体法益来分类。”[9]深度伪造滥用行为并未侵害新型法益，增设身份盗窃罪这一新罪缺乏新型法益立场。

其二，身份盗窃的目的性评价不足，难以涵摄利用深度伪造技术侵害一般主体权益的行为。身份盗窃犯罪窃取的是特定主体在法律上的主体地位和资格，而深度伪造的目的是利用个人生物识别信息合成虚假信息，其犯罪对象既可以是国家领导、公众人物等特定主体，也可以是普通公众等一般主体。例如，典型的身份盗窃罪名——冒名顶替罪、招摇撞骗罪侵害的是国家工作人员等特殊的身份资格所享有的权益。而深度伪造技术通过对收集的个人生物识别信息进行数据处理合成虚假信息，侵害的法益可能具有复合性，其针对的不是特定人的身份资格，而是一般人的人格权和财产权或是他人对信息权利主体的信赖利益。

其三，以身份盗窃入罪规制深度伪造技术违背刑法谦抑性立场。在现行刑法体系对公民个人信息已有规范的情况下，对于深度伪造技术的滥用行为应当通过解释论路径进行刑法适用，合理控制刑法介入的限度。此外，对深度伪造技术进行“一刀切”式的刑事治理模式扼杀了人工智能等高新技术发展的可能性，与“科技是第一生产力”的时代发展理念相悖。

4.1.2. 后续行为吸收说之弊端

“互联网+”时代使得数据具有高度的关联性和粘合性，大数据分析让个人信息“无处躲藏”。深度伪造的非法利用行为具有严重的社会危害性，加剧了生物识别信息泄露传播的风险，后续行为吸收说难以规制深度伪造技术的非法利用行为。

其一，后续行为吸收说难以实现对个人信息全周期的保护。作为个人信息的一种，生物识别信息的生命周期包括收集、存储、使用、共享、转让、公开披露与删除等环节[4]。其中的共享、转让、公开披露和删除环节，本质上都是提供、使用生物识别信息的一种方式。因此，现有刑法框架保护了生物识别信息生命周期中获取、提供与使用阶段，但除此以外的其他中间环节并未得到相应的保护。

其二，后续行为吸收说的规制效力受“明知”要件的约束。基于共犯理论，将深度伪造技术的非法利用行为认定为其他犯罪行为的帮助行为并不可取。帮助犯要求行为人的犯罪行为符合“明知”要件，但是由于互联网的虚拟性和隐匿性，在司法实践中往往难以证明信息提供者、出售者的共同犯罪故意。例如，在杨超、孙芳柱、万兴健破坏计算机信息系统案[5]中，被告人杨超利用在网上向被告人万兴健等人购买或由被告人孙芳柱、微信昵称“不能把”(身份不清)等人非法提供的他人身份信息、高清人像图、支付宝账号等，制作成人像验证动态图像，利用 OPPO_IMEI 软件等工具破坏计算机信息系统，冒用他人身份进行支付宝账户信息修改或实名认证。本案中，被告人杨超辩称他对万兴健等人非法提供行为并不知情，且不知道万兴健利用深度伪造信息实施下游犯罪。根据裁判结果，审理法院仅对被告人杨超突

[4]参见国家标准化管理委员会《信息安全技术个人信息安全规范》，GB /T 35273-2020。
[5]杨超、孙芳柱、万兴健破坏计算机信息系统案，浙江省温岭市人民法院(2020)浙 1081 刑初 1116 号刑事判决书。

破支付宝身份认证系统的行为进行评价，认定其构成破坏计算机信息系统罪，但杨超滥用深度伪造技术对下游犯罪的帮助行为并未受到刑法规制，后行为吸收说对于深度伪造的目的性评价不足。

4.1.3. 深度伪造技术滥用行为之定性

本文认为，对于“合法获取 + 非法利用”的深度伪造技术的滥用行为，应当通过对生物识别信息的特殊保护予以刑法规制。

首先，规制深度伪造技术非法利用行为的域外经验借鉴。目前，针对深度伪造技术带来的数据安全风险，美国与欧盟采取了两种不同的规制路径。美国对深度伪造进行专门性立法，将深度伪造的侵害性定位为制造虚假信息，侧重于防范虚假信息对于国家安全和传播色情视频的危害；欧盟则是将深度伪造认定为对生物识别信息的滥用，沿袭了传统的个人信息保护路径。基于我国刑法的现有体系，对于深度伪造的刑法规制应当借鉴欧盟模式。原因在于，我国对于深度伪造的虚假信息，可由危害国家安全罪和妨害社会管理秩序罪的罪名体系所评价，无需进行专门立法予以规制。而我国《个人信息保护法》的出台，为深度伪造的信息——数据治理路径提供了部门法基础。此外，美国对于深度伪造的专门立法略显仓促，与鼓励技术发展相悖。部分影视公司认为，《深度伪造责任法案》强制制作者承担显著标识义务的做法违背宪法第一修正案，美国的立法推进过程遭受批判。相较之下，欧盟基于完善的个人信息保护制度，通过特别保护个人生物识别信息防范深度伪造风险的规制路径更为从容。

其次，深度伪造滥用行为本质上是对生物识别信息的滥用。滥用深度伪造技术最为直接地侵害了个人生物识别信息，其技术实质决定深度伪造技术需要收集大量的个人生物识别信息样本。而深度伪造滥用行为非法使用生物识别信息是非法获取生物识别信息的衍生行为，同样侵犯了个人信息安全，应当以侵犯公民个人信息罪予以规制。如前所述，深度伪造技术的非法利用行为具有独立的社会危害性，但现行刑法尚未将非法利用行为纳入规制范围。鉴于信息网络“一对多”的传播方式，生物识别信息一旦泄漏将会产生难以弥补的后果，而深度伪造技术的滥用行为导致生物识别信息呈现非法传播不断扩散的态势，亟需刑法作出回应。

4.2. 增加侵犯公民个人信息罪的行为类型

深度伪造技术的非法利用行为加剧了个人生物识别信息非法传播的风险，其实质是对公民个人信息的侵害。而现行刑法将“侵犯”的语义限定为“非法出售、非法提供和非法获取”三种行为方式，规制范围过于狭窄，难以应对数字信息时代个人信息面临的多样化侵害风险。笔者认为，现行刑法应当在保持立法稳定性的基础上，适当调整侵犯公民个人信息罪的行为类型，以规制滥用深度伪造技术行为产生的算法黑箱问题。

4.2.1. 必要性：非法利用行为具有更为严重的社会危害性

大数据时代，在互联网上传播的信息爆炸式增长，个人信息泄漏风险与日俱增。目前，网络平台和社交软件的普及与发展，使得线上存在大量的人脸图片、通讯住址等公开的个人敏感信息。从现实情况可以看出，深度伪造技术的滥用行为大多通过爬取公开的个人生物识别信息进行非法利用。非法获取公民个人信息行为的侵害后果是静态的，其对个人信息权益的危害程度较为轻微。而非法利用生物识别信息行为的侵害后果是动态的，危及公民个人权益、社会秩序与国家安全。

此外，深度伪造技术等生成式人工智能的发展使得个人信息的侵害主体多元化，逐渐形成侵害个人信息的黑灰产业链，侵害手段日益复杂化和专业化[10]。非法利用深度伪造技术侵害个人生物识别信息的行为具有独立的危害性，深度伪造技术实质上是对个人生物识别信息的加工利用，行为人未经信息权利主体同意加工生物识别信息，侵犯了被害人的肖像权和个人信息权益[11]。因此，应当基于前文

所述预防风险为核心的事前规制模式的必要性，将“非法利用”行为类型纳入侵犯公民个人信息罪的规制范围。

再次，深度伪造技术的滥用将会消解社会公众的信任，人类社会将会步入“一切所见皆为虚妄”的“后真相时代”。在“后真相时代”，由于深度伪造的信息泛滥，视频形式的鉴真方式将不再被信任，社会公众会把摆在眼前的一切信息视为欺骗，“人们只相信自己愿意相信的东西”。鉴于此，深度伪造技术的非法利用行为具有造成信息无序社会的潜在风险，消解社会公众对于“真相”的认知。因此，非法利用深度伪造技术具有严重的社会危害性，现行刑法应当对深度伪造技术滥用行为予以规制。

4.2.2. 可行性：部门法为刑法规制非法利用行为提供依据

我国刑法对于个人信息保护的法律规范出台较早，导致“先刑后民”特殊情况的出现，刑法基于先行立法的审慎原则，对个人信息的保护随着信息时代发展逐渐“力不从心”，大量具有严重社会危害性的侵害个人信息的行为无法得到有效制裁[12]。

随着社会对于个人信息保护的呼声不断增加，此后的立法过程对个人信息保护作出了回应。2020 年出台的《民法典》第 111 条规定：“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”随后，针对个人信息问题，2021 年颁布了专门的《个人信息保护法》，该部门法进一步细化了《民法典》构建的个人信息保护框架。《个人信息保护法》第 10 条规定：“任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。”上述法律规范实质上规制了深度伪造技术滥用行为对个人生物识别信息的非法使用、加工和传输的行为，作为刑法的前置法，为刑法规制深度伪造技术非法利用行为奠定了基础。

综上所述，笔者认为，应当将合法获取后非法利用生物识别信息的行为作为侵犯公民个人信息罪的第 4 款规定的犯罪行为予以规制。为突出对生物识别信息的特殊保护，其“情节严重”的认定应当依照高度敏感信息的入罪标准，规定非法利用生物识别信息行为的起刑点为 50 条。由此，在保持刑法稳定性的基础上形成对个人信息全方位、多层次保护的刑法规制模式。

5. 结语

深度伪造技术等生成式人工智能将在信息数据世界的不断扩张和信息数据安全保护之间造成难以弥合的间隙[13]。来自深度伪造技术等生成式人工智能的知识欺诈，以及深度伪造技术非法利用个人生物识别信息的现象，加剧了人们对于个人信息泄漏的忧虑。应当明确的是，深度伪造具有技术中立性，其技术风险本质上是使用者恶意利用的风险。人工智能的进步已然进入“波兰尼时刻”，对于深度伪造技术带来的信息数据的风险，应当秉持刑法谦抑性的原则审慎规制，以风险预防为导向，构建适用范围相宜的事前规制模式，实现个人生物识别信息保护的源头治理。技术进步永无止境，刑法应当在保持立法稳定性的基础上充分发挥法律解释的能动性，将深度伪造等技术进步带来的刑事风险容纳在体系规制范围内，体现法律对现实问题的回应。

参考文献

[1] 王文娟. 生物识别信息传播风险的刑事规制向度——基于 525 份刑事裁判文书的内容分析[J]. 新闻与传播研究, 2022, 29(7): 75-88+127-128.

[2] 姜瀛. 人工智能“深度伪造”技术风险刑法规制的向度与限度[J]. 南京社会科学, 2021(9): 101-109. https://doi.org/10.15937/j.cnki.issn1001-8263.2021.09.012

[3] 李怀胜. 滥用个人生物识别信息的刑事制裁思路——以人工智能“深度伪造”为例[J]. 政法论坛, 2020, 38(4): 144-154.

[4] 李明鲁. “深度伪造”的刑法治理路径[J]. 科技与法律(中英文), 2021(6): 40-47+73. https://doi.org/10.19685/j.cnki.cn11-2922/n.2021.06.005

[5] 劳东燕. 风险社会中的刑法: 社会转型与刑法理论的变迁[M]. 北京: 北京大学出版社, 2015: 71.

[6] 单勇, 王熠. 来自“世界 3”的知识欺诈: 生成式人工智能的刑事风险应对[J]. 西南政法大学学报, 2023, 25(4): 70-85.

[7] 李腾. “深度伪造”技术的刑法规制体系构建[J]. 中州学刊, 2020(10): 53-62.

[8] 敬力嘉. 作为行为不法类型的犯罪参与——兼论非法发布深度伪造信息的行为不法[J]. 华东政法大学学报, 2020, 23(6): 73-87.

[9] 张明楷. 网络时代的刑事立法[J]. 法律科学(西北政法大学学报), 2017, 35(3): 69-82. https://doi.org/10.16290/j.cnki.1674-5205.2017.03.007

[10] 黄丽勤, 宋骏男. 未成年人数据权的二元保护研究[J]. 青少年犯罪问题, 2020(4): 64-73.

[11] 周光权. 涉人脸识别犯罪的关键问题[J]. 比较法研究, 2021(6): 13-29.

[12] 于冲. 侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界[J]. 政治与法律, 2018(4): 15-25. https://doi.org/10.15984/j.cnki.1005-9512.2018.04.002

[13] 盛浩. 生成式人工智能的犯罪风险及刑法规制[J]. 西南政法大学学报, 2023, 25(4): 122-136.