Open Journal of Legal Science 法学, 2023, 11(6), 5206-5212
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.116744

Hans汉斯

AI诈骗面临的刑法问题及其干预限度

——以“福州市 AI 换脸诈骗”为例

吴　晓

贵州大学法学院，贵州　贵阳

收稿日期：2023年8月21日；录用日期：2023年9月4日；发布日期：2023年11月13日

摘　要

人工智能技术发展的同时带来了一系列的法律风险问题，许多不法分子利用AI技术进行诈骗的犯罪行为屡见不鲜，并且以假乱真，让人防不胜防。本文以“福州市AI换脸诈骗案”为例，否定人工智能的刑事主体地位，分析出AI诈骗除涉及诈骗罪外，还面临侵犯公民信息罪、帮助信息网络犯罪活动罪、伪造身份证件罪等刑事法律问题。此外，为促进AI行业有序发展及信息数据的创新发展，本文对刑法干预限度进行分析，提出刑法在规制此类新型犯罪时，可以对利用AI犯罪的行为分类型按不同程度进行规制，即慎重认定数据获取、收集过程中的犯罪，从严打击数据利用过程中的犯罪。此外，刑法对于这类中立技术的规制应持审慎态度，以维持刑法的谦抑性，应充分发挥其他部门法的规制作用。

关键词

人工智能，AI诈骗，刑法干预限度

Criminal Law Problems and Intervention Limits Faced by AI Fraud

—Taking “Fuzhou AI Face-Changing Fraud” as an Example

Xiao Wu

College of Law, Guizhou University, Guiyang Guizhou

Received: Aug. 21st, 2023; accepted: Sep. 4th, 2023; published: Nov. 13th, 2023

Abstract

The development of artificial intelligence technology has brought about a series of legal risk problems, and many criminals that use AI technology to commit fraud crimes are common, and fake and

real, so that people are impossible to prevent. This paper takes the case of "Fuzhou AI face-changing fraud" as an example, denies the criminal subject status of artificial intelligence, and analyzes that AI fraud involves not only the crime of fraud, but also the crime of violating citizens' information, the crime of helping information network criminal activities, and the crime of forging identity documents. In addition, in order to promote the orderly development of the AI industry and the innovative development of information data, this paper analyzes the intervention limits of criminal law and proposes that criminal law, when regulating such new crimes, can regulate the use of AI crimes by types and according to different degrees, that is, carefully identify crimes in the process of data acquisition and collection, and strictly crack down on crimes in the process of data utilization. In addition, the regulation of this kind of neutral technology should be prudent in criminal law to maintain the modesty of criminal law and give full play to the regulation role of other departments of law.

Keywords

Artificial Intelligence, AI Fraud, Intervention Limits of Criminal Law

1. 问题的提出

随着人工智能技术的发展，AI 模型从只专注于完成一类特定的任务到如今已经发展成为可以解决多个问题的智能综合体，但发展的同时也带来了一系列的法律风险问题。近日福州市一起利用 AI“偷脸”技术在十分钟内骗走被害人 430 万的电信诈骗案件引发网友热议。以致“AI 诈骗正在全国爆发”、“AI 诈骗成功率接近 100%”等话题冲上微博热搜。诈骗分子的诈骗手段越来越科技化，他们竟然用上了 AI 换脸技术，逼真程度足以使人以假乱真，轻松骗取被害人信任，让人防不胜防。5 月 8 日，包头市公安局电信网络犯罪侦查局发布一起利用智能 AI 技术进行的电信网络诈骗案。福州市一公司法人代表郭先生突然接到朋友的微信视频电话，好友告诉郭先生其需要一笔 430 万的保证金，想借用郭先生的账户过一下账，并称其已将 430 万转入郭先生账户中。基于对好友的信任，郭先生没有核实钱款是否到账，就将 430 万转给对方。后来与好友确认后才得知是诈骗分子利用智能 AI 换脸技术，佯装成好友对郭先生进行了诈骗。此过程仅十分钟不到，诈骗分子便得手，令人唏嘘[1]。

骗子使用 AI 程序筛选被害人，在社交平台如微信朋友圈，短视频平台，通过骚扰电话等方式获取人们的声音信息和面部信息。再利用声音合成、AI 换脸，佯装亲友或同事骗取财物，数额较大的，无疑构成诈骗罪。AI 诈骗严重侵犯了人们的财产利益，必然要受到刑法规制，但是，此类案例中存在的疑问是，是否应当否定人工智能的刑事主体地位？此外，除了构成诈骗罪外，行为人是否还面临其他刑事法律问题？刑法在规制这类新型犯罪时应保持何种干预限度？本文将对以上问题逐一展开论述。

2. 人工智能技术的概述

2.1. 人工智能技术

人工智能(Artificial Intelligence)，简称 AI。人工智能是一门源于计算机科学控制论、哲学、信息论、

[1]参见包头市公安局官方网站中警方发布“10 分钟，挽回 336 万元！福建企业家为包头点赞！”一文。网址：http://gaj.baotou.gov.cn/jffb/article/detail?articleId=852244673606062080，2023 年 8 月 10 日访问。

心理学、语言学等多门学科的边缘新学科。最早在 1956 年 Dartmouth 大学的会议上，由“人工智能之父”麦卡锡(McCarthy)及一批心理学家、数学家等首次提出[2]。明斯基(Marvin Minsky)是人工智能的创始人之一，他以“让机器从事需要人的智能的工作的科学”一句话概括了人工智能研究的实质。人工智能一般被分为强人工智能与弱人工智能，强人工智能具有更为深度的学习能力，能够实现甚至超越人类的智力范围产生成果。弱人工智能则只能在有限范围复制和超越人类的能力[1]。从以往的技术来看，强人工智能的实现只是一种主观的想象，但 2022 年 Chat GPT 的研发让人们对人工智能的想象更加深入，人工智能的潜力似乎是极大的。互联网技术的发展极大地推动了人工智能技术的创新发展，如今的人工智能技术已经显现出高智能化、自主操纵、深度学习、深度拟人、跨界融合等特征。

2.2. “深度伪造”技术

伴随人工智能的创新发展，作为其主要功能之一的“深度伪造”(Deep Fake)[3]技术也备受关注。该项技术是于 2014 年，苹果公司发明的，该发明小组的核心成员是伊恩·古德费洛(Ian Goodfello) [2]。他们利用丰富的样本和充实的数据，将这些模型与数据相互检验，并利用匡纠模型，把两个不同人的面孔替换。这种技术是信息组构和验证其真假度的两种数据程序的产物，难以发现其造假的痕迹[3]。正如我们所熟知的 AI 换脸技术，其应用程序“ZAO”、“Fake App”、“Deep Face Lab”等，一经上线便得到极大的社会关注和流量支持。AI 换脸技术主要是通过人脸检测算法(常见如 Haar 特征级联分类器、HOG 特征 + SVM 分类器等)进行人脸识别，提取人脸特征、完成关键点定位后进行交换矩阵计算，最后进行合成渲染完成换脸。该换脸技术冒充特定人物后面部表情自然流畅，由于视频电话存在网络问题，使得该“换脸”技术的瑕疵更不易被发现，足以以假乱真，骗取被害人信任。除 AI 换脸外，“深度伪造”技术还包含声音模拟、文本生成和微表情合成等[4]。AI 拟声技术，是利用 AI 模型学习特定的人的声音特征，比如其声音音色、音调、语速等特征，通过语音深度合成技术，重新生成新的与特定人极相似的声音，足以使人以假乱真。

“深度伪造”技术的研发一直备受公众关注。尤其是今年以来，Chat GPT 和 GPT-4 等技术的应用，成为了计算机科技领域的热点，激起了公众对 AI 技术的广泛关注和热情。如今伴随着深度合成技术的开放开源，利用深度合成技术的产品和服务日益增多，人们在家利用一台电脑便可以制作 AI 换声、AI 换脸的虚假音视频。因此，该技术常常被犯罪分子利用，进而侵犯公民合法权益。

3. 人工智能刑事主体地位之否定

从法理的角度明确人工智能的法律地位，是解决与人工智能技术发展相关的法律问题的关键。关于人工智能机器人刑事责任主体地位的赋予与否学界存在较大争议，肯定派的主要理由是如今的强 AI 机器人会在人类设定的程序、安排的计划外依照其自主的、不被操控的意志选择性地实施危害社会的行为，其具有辨认和控制能力，具有刑事责任主体地位，应承担刑事责任[5]。持该观点的主要代表人是华东政法大学的刘宪权教授，在知网上以“人工智能”为关键词搜索，刘教授的研究成果较多，核心观点均为肯定强人工智能机器人的刑事责任主体地位。刘宪权教授首先提出 ATM 机为机器人，ATM 机也可能被骗[6]。他认为 ATM 机具有识别功能，也可能产生认识错误。此外，学者吴允峰也指出，强人工智能可以独立思考和决策，是独立的主体，可以承担刑事责任。他也提出“机器人可能被骗”的观点，他认为利用 ATM 机侵犯财产权的行为既不符合盗窃罪的基本特征，也不具备诈骗罪中的“处分意识”要素，属于立法空白[7]。

[2]参见《谭铁牛：人工智能的历史、现状和未来》，https://www.cas.cn/zjs/201902/t20190218_4679625.shtml，2023 年 8 月 3 日访问。
[3]“深度伪造”(Deep Fake)一词源于 2017 年美国红迪网发布伪造视频的作者的昵称，后发展为此项技术的名称。其含义为深度学习与伪造。

笔者支持否定论的观点，目前为止，强人工智能仅为一种主观臆想，是学者们对于强人工智能的发展预测，并没有充实的数据支撑，当然结论也难以成立。此外，“机器人”是研究者赋予人工智能的一种拟人化称谓，现实中并不存在所谓机器人，因为机器人既不是人也不是机器。“机器”没有处分意识，“机器不能被骗”是公认的事实。上述所谓不符合盗窃罪构成要件的观点，仅是先验地认为“盗窃只能秘密窃取”而得出的结论。

关于人工智能的刑事法律地位，我们应明晰以下几点：

1) 明确利用缺乏“自由意志”的 AI 实施诈骗行为的责任主体。

责任能力的核心要素是自由意志，自由意志包括辨认能力和控制能力两方面。一个人拥有自由意志，意味着他的行为是“他自身”的产物，他是他行为的主人，并且对自己的行为有正确的社会意义的认识。目前 AI 的智能仅是一系列算法逻辑堆砌和运算的结果，其行为是在算法程序的驱动下实施的，它对自己的行为也无法作出理性甚至伦理价值的判断，缺少社会意义上的理解力。因此，它不具有自在自为的自由意志。不存在人格，更无法对其“行为”负责，故在法律地位上它仍旧是法律关系的客体。缺乏“自由意志”的责任主体并非法律惩罚的对象，故应当追究研发者、使用者的责任。

2) 当 AI 具有行为控制能力但不具备责任承担能力时，实施诈骗行为的责任主体仍为研发者、使用者。

即便在未来人工智能也可以拥有自由意志，能够达到辨认和控制自己的行为的程度。它们也难以具备责任能力。因为责任能力不仅与自由意志因素有关，还与道德情感因素紧密联系。如果 AI 无法与人类一样具有道德情感，它们就不具有承担刑事责任的能力。因为没有道德情感的人工智能仍然是机器，对其施行刑罚是没有意义的，它们没有羞耻心与社会责任感，故无法理解刑罚的道德谴责意义，也不能感受到刑罚带来的情感谴责与痛苦。故此时的责任主体仍为研发者、使用者。

3) 将来 AI 同时具备行为能力与责任能力时，实施诈骗行为应持“承认和限制”的立场。

目前的 AI 只是在人类编程和控制之内作出行为。现阶段还需要在法理上对人工智能体的“法律人格”、“自由意志”等问题作出合理的解释，在未来才能考虑在法律上赋予 AI 主体资格。由于 AI 技术是一把双刃剑，既可以造福人类，也会给人类带来风险，法律要去规制 AI 技术带来的犯罪问题，只需去追究 AI 研发者、使用者的责任，明确真正的犯罪主体。需要强调的是，未来 AI 同时具备行为能力与责任能力时，法律规范、法律制度所应体现的对于 AI 所可能具有的法律人格、权利、责任等的基本立场，应被总结为“承认和限制”，即承认 AI 在某些情形下可以被作为法律主体看待，享有相应的权利并承担相应的责任，但同时 AI 的法律主体资格，与自然人并不完全等同，当二者利益产生冲突的时候，应始终优先保障自然人的利益。

4. AI 诈骗面临的刑事法律问题

在明确人工智能刑事主体地位之后，我们应该顺势思考 AI 诈骗可能涉及哪些犯罪。在 AI 诈骗案件中，行为人利用 AI 技术筛选被害人，利用换脸、拟声等技术冒充其亲友，获取被害人信任。行为人主观上以非法占有为目的，故意诈骗他人财物，客观上以假扮亲友、虚构事实的方法，骗取被害人数额较大的财物，使被害人产生认识错误并基于认识错误处分财产，造成被害人财产的损失，符合刑法典第 266 条之诈骗罪的构成要件。因此，利用 AI 技术进行诈骗无疑构成诈骗罪，除构成诈骗罪外，其手段行为与目的行为还涉及其他犯罪。

4.1. 手段行为触犯侵犯公民个人信息罪、伪造身份证件罪

行为人利用 AI 大量爬取或深度伪造公民脸部、声音信息涉及刑法第 253 条之一第三款规定：“窃取或者以其他方法非法获取公民个人信息的，构成侵犯公民个人信息罪”。根据最高人民法院与最高人民

检察院颁布的司法解释[4]，公民个人信息是指能够识别或反映特定自然人身份以及活动情况的各种信息。脸部、声音信息具有人身专属性，可以成为识别特定人物身份信息的重要依据，无疑在此范围中。此外，使用 AI 技术处理的人脸、声音信息，以及基于 AI 技术生成的人脸、声音信息与特定人物的真实信息具有高度相似性，能够单独或者结合其他信息来识别特定人物身份或者反映特定人物活动情况，仍应该纳入刑法保护的公民个人信息范畴[8]。故行为人利用 AI 深度伪造或者大量爬取公民个人信息可能构成侵犯公民个人信息罪。“福州市 AI 换脸诈骗”一案中，行为人利用 AI 筛选被害人，在社交平台爬取或窃取被害人亲友的面部、声音信息，以及其之后基于 AI 技术生成的人脸、声音信息均可用以识别特定人物身份，属于公民个人信息。行为人利用 AI 换脸技术伪装好友与被害人进行微信视频电话，骗取郭先生的信任，使郭先生基于认识错误处分财产，导致财产损失。这一过程中，行为人除构成诈骗罪以外，其获取公民个人信息的手段行为还触犯了刑法第 253 条之一规定的侵犯公民个人信息罪。

此外，伴随互联网的发展，当前网上的各种应用软件，如银行 APP、支付宝、微信等均要求通过网上实名注册开通，身份证件的网络实名认证也成为了其中必要的环节。许多软件都需要进行实名认证或刷脸认证才能继续使用。故不法分子利用认证过程中的漏洞进行冒充注册或登录，登录成功后与亲友发微信进行诈骗活动。他们收集他人真实的姓名、身份证号码等信息，采用 AI 换脸等“深度伪造”(Deep Fake)技术替换他人身份证件的相片，通过网络验证。以此规避平台实名制管理，如将他人相片替换为自己相片以通过人脸验证。这类行为伪造了含有虚假内容的身份证件，使得该证件具有真实身份证件的功能，不仅妨害了国家对身份证件的管理秩序，而且侵犯了刑法保护的法益。因此，最高人民法院、最高人民检察院以及公安部联合发布的《意见二》第 6 条认为该行为符合刑法第二百八十条第三款之伪造身份证件罪的构成要件，并规定实践中对此行为可以按照伪造身份证件罪追究刑事责任[5]。

4.2. 目的行为涉及帮助信息网络犯罪活动罪

行为人在获取面部、声音等信息后，如何利用这些信息与是否成立犯罪有很大关联。行为人将信息提供给他人这一行为，由于具有帮助属性，容易触犯帮助信息网络犯罪活动罪与诈骗罪之帮助犯。需要做好此罪与彼罪的区分。其中关键在于行为人“明知”的范围。如果行为人明知他人实施电信网络诈骗犯罪，仍然将获取的信息提供给其用于诈骗犯罪，主观上对于被帮助人所实施诈骗行为的性质、手段、后果具有确切认识，客观行为与正犯行为具有紧密关联，应认定为刑法第 266 条之诈骗罪的帮助犯。因为根据刑法总则共同犯罪理论，共同犯罪为共同故意犯罪，包括主观上的共同故意与客观上共同实施了相关行为。电信网络诈骗犯罪属于帮助信息网络犯罪活动罪的特别法条，当行为人明知被帮助人实施诈骗犯罪，仍然为其提供帮助，应该认定为诈骗罪的帮助犯而不再认定为帮信罪。如果行为人仅明知被帮助者实施网络违法犯罪活动，积极为其提供帮助，应认定为一般法条即刑法第 287 条之帮助信息网络犯罪活动罪[9]。

5. 人工智能时代 AI 诈骗的刑法干预限度

刑法面对人工智能犯罪这类新型犯罪，在利用刑法对其进行处罚的同时，也要注意干预的限度，过度干预可能会产生适得其反的效果。人工智能时代利用 AI 进行诈骗的社会危害性虽不容小觑，但刑法对于新类型犯罪应当保持一定的谦抑性，不能一味进行严厉打击。刘宪权等人也指出，人工智能时代数据信息的发展创新与价值创造本身就离不开对数据的获取与流通，如果刑法过多地干预数据的获取、收集过程，可能会阻碍数据创新与发展[10]。故笔者认为刑法可以分类型处理不同的 AI 诈骗犯罪。如上所述，

[4]参见2017年5月最高人民法院与最高人民检察院所颁布的《关于办理侵犯公民个人信息刑事案件适用法律的若干问题司法解释》。
[5]参见 2021 年 6 月 22 日最高人民法院、最高人民检察院、公安部联合发布的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(二)》第 6 条。

AI 诈骗一般因其手段行为与目的行为触犯刑法，手段行为一般为数据的获取、收集、存储过程，目的行为一般为数据的利用过程。刑法对于这两种不同类型的犯罪行为的应当采不同程度的规制。

5.1. 谨慎认定数据获取、收集、存储过程中的犯罪

AI 诈骗的手段行为一般为数据的获取、收集、存储过程，而信息数据的发展离不开数据的制作与传播。当今的数据共享时代，大多信息数据都可以通过网络合法获取，当然也有不少不法分子非法获取受保护的个人信息，但是刑法不能轻易将新兴技术所带来的弊端全部归于刑事犯罪领域，对于非法获取、收集、存储的行为应当慎重认定。如果刑法过度干预这一过程，必然会限制信息数据的创新与发展，与我国大力推动人工智能技术发展的政策相违背。但如果刑法适度对数据获取过程进行规制还有利于鼓励数据创新，维护网络运行秩序，推动社会信息数据的发展进步。大部分人获取数据只是为了资源共享以及日常学习或娱乐需要，这一过程也很难产生危害社会的后果。因此，为保护信息时代数据的获取与流通、促进信息数据的创新与发展、兼顾社会安全保障与数据发展进步[11]，刑法应当谨慎认定数据获取过程中的犯罪。

5.2. 从严惩处数据利用过程中的犯罪

AI 诈骗的目的行为一般为数据信息的利用过程，一般来说，对网络上获取的数据信息，在进行个人利用时一般应当进行加工或标明出处。如果仅仅是日常学习或娱乐需要对数据信息进行获取、存储，一般不会涉及刑法问题。但由于信息时代的发展，网络上公开的个人数据信息越来越容易获取，于是总有不法分子会利用这些数据进行不法活动，非法利用或者非法提供给他人。为了保障社会安全与行业发展秩序，刑法需要对此进行规制。而利用数据的这一过程一般不会影响到信息数据的流通，但这一过程又极易涉及数据的不法利用，故基于对技术使用环节中具有的社会危害性的考量，为打击利用非法利用数据危害社会的行为，应当从严惩处数据利用过程中的犯罪。

5.3. 刑法面对中立技术应保持其谦抑性

AI 换脸和拟声技术属于中立技术，本身存在着技术发展与安全保障的冲突，我们不能仅关注其法益侵害的危害性、严峻性而限制或禁止这类行为，还应看到技术本身于社会发展的积极意义。中立性信息技术不应被轻易犯罪化，刑法应秉持优先保障技术发展自由的立场，响应国家大力推动技术发展的政策，慎用刑法，只有对个人信息的侵犯足以危及人身、财产权利，才可发动刑罚权[12]。在此之前应当充分发挥其他部门法的规制作用。人工智能这类新兴技术的滥用并不天然具有刑事违法性，许多技术滥用行为仅仅涉及民事纠纷或行政违法，应当优先考虑辅以较宽缓的民法或行政法等规制。如利用《民法典》第 111 条规定的“自然人的个人信息受法律保护，任何组织或个人不得非法买卖、提供或者公开他人个人信息”、民法典人格权编之公民肖像权、隐私权以及民法典人格权编第 1023 条对自然人声音的特别保护等。此外，可以加强行政法中对相关部门的监管，责令有关部门和平台加强监督，严格把控个人信息的控制主体，公开个人信息的控制主体应当是社会组织或政府机构。同时，做好法治宣传工作，提醒公民提高警惕。总之，在利用严厉的刑法规制此类中立技术时，应当思考是否还有其他更为经济、更为宽缓、更为有效的方法可以达到同样的规制目的。

6. 结束语

伴随着大数据时代与信息社会的发展，人工智能的发展只会更加迅速。利用人工智能的诈骗行为只增不减。AI“换脸”与“拟声”技术的成熟度已经很高，极易获得被害人信任，让人防不胜防。刑法必须采取有效的措施规制此类犯罪。由于此类犯罪手段行为与目的行为均可能涉及多种罪名，因此在规制

过程中，应当做好此罪与彼罪的区分。刑法对于 AI 诈骗的规制应当遵循分类型处理的方式，以便在实现打击犯罪的目的的同时，不阻碍社会发展，兼顾社会安全保障与 AI 发展进步。面对这类新兴技术，应当坚持刑法、民法、行政法一体打击的原则，避免刑法的垄断治理。如前所述，看待任何事物都应当持辩证思维，人工智能的发展有利有弊。我们在获得新体验的同时，还要时刻防范着不法分子利用人工智能侵犯公民的人身与财产安全。因此，在生活中面对如此以假换真、让人防不胜防的 AI 诈骗，我们应该注意：保护个人信息，不随意透露个人信息或资产情况，防范信息泄露；不轻易透露自己的身份证、银行卡、验证码等重要信息，不过度公开或分享动图、视频等；不贪图小便宜，遇扫码送礼等活动要拒绝；不随意下载陌生软件或点击网络链接；不轻信视频或语音，提高警惕，特别是涉及隐私信息、转账时，应当进行多方式验证确认身份。

参考文献

[1] 陈洪兵. 人工智能刑事主体地位的否定及实践展开——兼评“反智化批判”与“伪批判”之争[J]. 社会科学辑刊, 2021(6): 92-98.

[2] Libby, K. (2020) Deepfakes Are Amazing. They’re Also Terrifying for Our Future. Popular Mechanics. https://www.popularmechanics.com/technology/security/a28691128/deepfake-technology/

[3] 刘建明. 深度伪造对媒体与人类的致命威胁[J]. 新闻爱好者, 2021(4): 8-13.

[4] 尚海涛. “深度伪造”法律规制的新范式与新体系[J]. 河北法学, 2023, 41(1): 23-42.

[5] 刘宪权. 人工智能时代的“内忧” “外患”与刑事责任[J]. 东方法学, 2018(1): 134-142.

[6] 刘宪权. 人工智能时代的刑事责任演变: 昨天、今天、明天[J]. 法学, 2019(1): 79-93.

[7] 吴允锋. 人工智能时代侵财犯罪刑法适用的困境与出路[J]. 法学, 2018(5): 165-179.

[8] 彭辅顺. 非法使用公民个人信息行为的刑法规制[J]. 中国刑事法杂志, 2023(1): 107-124.

[9] 任俊. “明知他人利用信息网络实施犯罪”的认定[D]: [硕士学位论文]. 重庆: 西南大学, 2021.

[10] 刘宪权, 汤君. 人工智能时代数据犯罪的刑法规制[J]. 人民检察, 2019(13): 31-34.

[11] 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.

[12] 罗翔. 论人脸识别刑法规制的限度与适用——以侵犯公民个人信息罪指导案例为切入[J]. 比较法研究, 2023(2): 17-30.