

AI 딥페이크 기술의 법적 위험과 관리

순판치(孙繁旗, Sun Fanqi) 연구원, 변호사
서남정법대학교 중동법률연구센터



생성형 AI의 발전과 DeepSeek를 통한 도약

최근 몇 년 동안 생성형 AI기술이 급속히 발전하면서 업무생산성과 산업분야의 기술혁신에도 새로운 변화를 맞았다. 미국의 Open AI팀이 ChatGPT를 통해 세계적 생성형 AI기술을 선도하면서 진정한 디지털 사회 전환과 새로운 기술혁명 시대를 견인하고 있다. 이에 중국은 인터넷 선도기업들이 이 분야를 이끌고 있으며, 대표적으로는 바이두의 ‘文心一言’, 알리바바 클라우드의 ‘通义千问’, ByteDance(字节跳动公司)의 ‘豆包’, iFLYTEK(科大讯飞)의 ‘星火大模型’, 그리고 텐센트의 ‘腾讯元宝’ 등이 있다. 이러한 생성형 AI 모델은 대부분 스마트 채팅 모드를 매개체로 하여 문자, 이미지, 동

영상 생성 기능을 갖추고 있다.

한편, 2024년 12월 중국은 오픈소스 모델인 DeepSeek-V3를 출시하면서 세계적으로 큰 이슈가 되었다. 또 머신러닝 및 추론비용이 낮으면서 더 효율성이 높은 DeepSeek-R1 모델을 연이어 출시했다. 이는 디지털 추론 및 코드 생성 등의 작업을 지원하면서 미중 애플리케이션 다운로드 순위에서 빠르게 1위를 차지하기도 했다. 현재까지 알리바바와 텐센트를 포함한 중국 대기업들은 자체 클라우드 플랫폼과 앱에 DeepSeek-R1 모델을 도입하여 인공지능의 새로운 작업 효율을 극대화했다.

딥페이크(Deepfake) 범죄와 유형

이처럼 중국은 생성형 AI인 DeepSeek의 성공으로 생성형 AI기술의 발전을 가속하고 있다. 하지만, 이를 활용한 새로운 사물의 생성 및 개발에 대한 법적 규제의 미비 등으로 다양한 부정적 문제들이 사회적 이슈가 되었다. 주로 생성형 AI인 DeepSeek를 활용한 문서위조, 딥페이크(Deepfake)를 통한 인권침해 및 사기, 지식재산권 침해 등 법적 문제를 낳았다. 특히, 생성형 AI를 기반으로 개발된 딥페이크 기술은 인터넷 음란물 산업에서 처음 등장했으며, 현재는 짧은 동영상(쇼츠) 제조, 영상 창작, 가짜 뉴스 생성, 문서위조, 비디오 채팅 등으로 확장되고 있다. 이 기술은 얼굴인식 알고리즘과 인공신경망(artificial neural network, ANN)을 포함한 기계학습 및 인공지능 도구와 기술을 활용한다.¹⁾

중국의 딥페이크와 관련한 침해사례는 사회적 문제가 된 이른바 ‘AI 얼굴 바꾸기(AI换脸)’ 사건으로, 저장성(浙江省) 항저우(杭州)에서 발생하였다.²⁾ 요약하면, 우(虞) 모 씨는 2020년부터 ‘AI 얼굴 바꾸기’ 소프트웨어를 사용하면서 처음에는 온라인에서 이 기술과 관련 소프트웨어를 홍보하여 이익을 얻다가 차츰 이를 사용하여 음란 사진과 동영상을 만드는 것이 더 큰 이익을 얻는다는 것을 알게 되었다. 그는 2년 동안 이른바 ‘여신 합성 동영상·사진 보기 단체방(女神合成视频图试看群)’ 등 6개의 소셜 그룹을 만들고, 대량의 음란물을 단체방에 게시했다. 공범은

전문가가 바라본 글로벌 핵심 이슈와 시사점



2,000여 명에 달했으며, 이들은 동의 없이 일부 영상과 사진을 ‘AI 얼굴 바꾸기’ 소프트웨어를 사용하여 인터넷에서 범죄에 사용할 대상의 정보를 수집했다. 얼굴합성 피해자는 약 100명에 달하며, 이를 통해 얻은 범죄수익은 약 6만 위안이 넘었다.

이 사건으로 사회적 파장이 커지자 항저우시(杭州市) 샤오산구(萧山区) 인민검찰원과 법원은 공정·공평의 사법 대응을 통해 피의자들에게 형사책임과 피해자에 대한 민사 구제를 약속하였다. 또 현재 AI를 활용한 딥페이크 기술에 대해 법적 규제가 없고, 사진 몇 장만으로 비디오와 결합하여 새로운 영상을 쉽게 제작할 수 있으며, 비용이 거의 들지 않을 뿐더러, 피해자도 알기 어렵기 때문에 주의를 당부하기도 하였다.

온라인 사기의 급증과 딥페이크(Deepfake) 범죄의 위험성

최근 3년 동안 인민법원이 심리한 전기통신 네트워크 사기 사건의 수가 매년 증가하는 추세를 보이며, 2024년에는 이와 관련한 사건이 1만여 건 심리되어

1) 张新生、王润周、马玉龙, “AIGC背景下虚假信息治理挑战、机会与策略研究”, 情报科学, 2024, pp.1-2.

2) 사례인 ‘浙江省杭州市萧山区人民检察院诉虞某某个人信息保护民事公益诉讼案’는 최고인민검찰원과 법원에 의해 ‘전형판례’로 분류되어 있으며, 중국에서으로 간주되어 우리나라의 ‘AI 얼굴 바꾸기’ 첫 번째 사건이라고도 불립니다.

피고인 수가 8만 2천여 명에 달한다. 또 사건 수와 피고인 수는 전년 대비 각각 29.4%와 26.7% 증가했다.³⁾ 그 중 전략적 신흥 산업과 관련된 사건 수와 비율은 매년 증가하여, 2024년에는 1,233건에 달하며, 이는 32.3%를 차지한다.

현재 딥페이크와 관련한 입법이 없고, 분쟁이 이미 발생한 상황에서 최고인민법원이 인공지능과 관련된 특허권, 저작권 등의 분쟁에 대해 피해자를 법으로 보호하기란 매우 어렵다. 또한, 딥페이크 기술을 통한 원클릭 얼굴 변경 등 인공지능 남용 침해행위에 대해서는 법에 따라 단호히 엄중히 처벌할 필요가 있음에도 법률적용의 한계로 인하여 어려움이 있는 것이 사실이다.⁴⁾

현재 이러한 사건 수는 지속적으로 증가하고 있을 뿐만 아니라, 범죄가 조직화, 규모화, 집단화의 경향을 보이고 있다. 일부 해외 전기통신 네트워크 사기 조직은 대형 범죄조직으로 발전했으며, 사기 조직 내 인원의 역할이 명확하고, 생산라인 방식을 통하여 체계적으로 운영되고 있다.⁵⁾ 딥페이크 기술은 이러한 범죄 조직에 의해 악용될 가능성이 매우 높다. 특히,

사기의 은밀성과 혼란성으로 인해 예방과 단속이 어려워 일반 대중이 더 높은 사기 위험에 처하게 된다.⁶⁾

생성형 AI의 악용 우려와 중국정부의 대응

한편, 앞서 언급한 바와 같이, AI를 활용한 딥페이크 기술은 음란 동영상 유포에 따른 법적 위험 외에도 사기나 지식재산권 침해의 위험성도 매우 높다. 올해 3월 초 개최된 전국인민대표대회에서 최고인민법원 형사재판 제3부 재판장인 천홍상(陈鸿翔)은 “인공지능이 빠르게 응용되는 디지털 공간에서 AI 얼굴변환과 음성합성 등의 기술은 콘텐츠 생산의 경계를 넓힐 뿐만 아니라, 사기 범죄의 온상이 되었다.”라고 했다. 사기범들이 AI 얼굴인식과 암호화 통신 등의 기술을 이용해 정밀하고 고도화된 사기를 저지르고 있어, 예방과 단속이 점점 더 어려워지고 있다는 취지이다. 또 전국정협 위원인 진동(靳东)과 레이쥔(雷军)은 양회에서 현재 ‘AI 얼굴인식 및 음성화’ 기술이 주로 인터넷을 통한 온라인에서 이루어지고, 본인도 피해자 중 한 명이라고 그 우려를 표명하면서 이를 규제하기 위한 입법이 조속히 이루어져야 한다고 주장하였다.⁷⁾ 이 외에도, 지식재산권 보호 측면에서 최고인민법원은 ‘원클릭 얼굴변경’ 등 AI기술 남용과 관련

3) “专访最高法刑三庭庭长陈鸿翔：加强AI深度伪造等研究 适时出台规范性法律文件”，最高人民法院，2025-03-08，<https://www.court.gov.cn/zixun/xiangqing/458031.html>(검색일: 2025.03.27.).

4) 참고로 2025년 3월 8일 오전, 제14기 전국인민대표대회 제3차 회의에서 최고인민법원 원장 장쥔(张军)의 업무보고에서 2013년부터 2024년까지 인민법원이 접수한 지식재산권 사건 수는 10만 건에서 49.4만 건으로 증가하였고, 최근 몇 년 동안 지식재산권 분야에서 새로운 유형의 분쟁이 나타나고 있으며, 지식재산권법원이 설립된 6년 간 기술 관련 지식재산권 및 독점 항소 사건이 약 2만 건에 달한다고 한다. “最高人民法院工作报告”，最高人民法院，2025-03-08，<https://www.court.gov.cn/zixun/xiangqing/457991.html>(검색일: 2025.03.27.).

5) 이는 사기수법이 지능화되어 성공률이 매우 높다. 또 이러한 범죄조직은 종종 ‘해외 고액연봉’을 미끼로 사람들을 유인하여, 해외에서 사기행위를 하도록 하며, 해외 사기범죄조직에 끊임없이 인력을 공급하고 일련의 관련 범죄를 파생시킨다.

6) “专访最高法刑三庭庭长陈鸿翔：加强AI深度伪造等研究 适时出台规范性法律文件”，最高人民法院，2025-03-08，<https://www.court.gov.cn/zixun/xiangqing/458031.html>(검색일: 2025.03.27.).

7) “两会大家谈：靳东、雷军深受其害——AI深度伪造风险如何治理”，新京报，2025-03-07，<https://baijiahao.baidu.com/s?id=1825943624199733325&wfr=spider&for=pc>(검색일: 2025.03.27.).

된 침해행위에 대해 엄중히 처벌할 것을 명확히 요구하고 있다.

이처럼 최근 몇 년 동안 중국정부는 딥페이크 기술로 인한 법적 위험을 면밀히 주시하고 있으며, 이를 관련부서의 대응지침의 제정과 법률 규정에 신속히 반영하도록 하고 있다. 관련부서의 대응지침 제정 측면에서 시진핑 총서기는 당의 제18차 전국대표대회 이후 여러 차례 차세대 인공지능 발전 가속화의 중요성을 강조하며, 인공지능은 과학기술 혁명과 산업 변혁

을 이끄는 전략적 기술로서 중요성을 가진다고 지적했다. 또 그는 인공지능의 응용과 관련한 잠재적 위험을 방지하고, 국민의 이익과 국가안보를 수호해야 한다고 강조했다. 중국공산당 제19차 전국대표대회와 제20차 전국대표대회 보고서에서도 인공지능과 실물경제의 융합을 촉진하고, 이를 전략적 신흥산업으로 지정하는 등의 중요한 조치를 잇따라 제안했다. 이러한 시진핑 주석의 메시지는 앞으로 딥페이크 남용 및 악용 방지를 위한 정책 및 입법에 동력이 될 것이다.

〈표 1〉 중국의 딥페이크 관련 정책 현황

정책 및 법제	부처/시기	주요 내용
법치사회건설 실시강요 (法治社会建设实施纲要)(2020 - 2025)	국무원 2020.12.7.	인터넷 생방송, 1인 미디어, 지식 커뮤니티 질의응답 등 뉴미디어 업태와 알고리즘 추천, 딥페이크 등 신기술 응용에 대한 규범적 관리방법 제정 및 완비
중국식 현대화의 전면적 심화 개혁 및 추진에 관한 결정(中共中央关于进一步全面深化改革、推进中国式现代化的决定)	국무원 2024.7.21.	인공지능 안전 감독관리제도 수립
국민경제 및 사회발전 제14차 5개년 계획과 2035년 장기목표 강요(国民经济和社会发展的第十四个五年规划和2035年远景目标纲要)	국가발전개혁위 2021.3.11.	<ul style="list-style-type: none"> - 네트워크 보안 핵심기술 연구개발 강화 - 인공지능 보안 기술혁신 가속화 - 네트워크 보안산업의 종합 경쟁력 제고 - 네트워크 보안 홍보·교육·인재양성 강화
인공지능 안전 거버넌스 구성(人工智能安全治理框架)	전국 인터넷 안전표준화 기술위원회 2024.9.9.	<ul style="list-style-type: none"> - 인공지능이 콘텐츠를 생성하거나 합성 시 허위정보 유포, 차별·편견, 개인정보 유출, 침해 등의 문제 제거 - 사실의 혼동과 사용자 오도 및 감정 우회 위험 제거
생산형 AI서비스 관리 임시방법(生成式人工智能服务管理暂行办法)	국가발전개혁위 등 2023.8.15.	<ul style="list-style-type: none"> - 해당 분류 및 등급에 따른 감독규칙 공식화

자료 : 관련 정책을 참고하여 저자 정리

AI 딥페이크 기술 보안 등의 강화와 전망

중국은 인공지능기술의 광범위한 응용에 따라 딥페이크 방지 등을 위해 개인의 ‘정보보호’와 ‘보안’ 등이 새로운 당면과제라고 보고 있다. 「법치사회 건설 시행 강요(法治社会建设实施纲要)(2020 - 2025)」와 「‘14.5’ 계획」 및 중국공산당 제20기 3중전회에서 인공지능 안전관리에 대한 사항을 공통으로 제시하였다.

〈표 1〉에서 알 수 있듯이, 중국의 AI를 활용한 딥페이크 관련 정책의 주요 취지는, (1) 관련 규범관리방법 제정, (2) 기술연구 개발 및 혁신 강화, (3) 안전 감독제도 구축 등으로 요약할 수 있다. 중국은 인공지능 발전과 안전을 조화롭게 추진하는 데 있어 그동안의 경험을 활용한 ‘사람 중심의 선량한 스마트 지향(以人为本、智能向善)’을 발전 방향의 원칙으로 하고 있다. 이를 통해 안전관리를 중시하며, 국제협력을 적극적으로 추진한다는 것이다. 특히, 전국 네트워크 안전표준화기술위원회(全国网络安全标准化技术委员会)가 제정한 「인공지능 안전관리 거버넌스 구성(人工智能安全治理框架)」은 딥페이크의 위험성을 응용보안분야에 집중시켜 허위정보 유포나 개인정보 유출 등과 같은 네트워크 영역에서의 보안 문제를 집중적으로 규정하고 있다.

2025년에 와서 생성형 AI 기술은 미국은 ChatGPT가, 중국은 DeepSeek가 이끌고 있다. 양국은 기술 분쟁과 보안 상의 문제, 정치적 요소 등으로 인해 서로 상대방에서 개발한 생성형 AI인 ChatGPT와 DeepSeek의 사용을 금지하고 있다. 하지만, 오히려

양국의 이러한 분쟁요소가 중국의 DeepSeek 등 생성형 AI기술 발전의 원동력으로 작용하고 있다. 하지만, 앞서 언급한 바와 같이, 중국 내에서 AI 딥페이크 등을 활용한 범죄가 증가함에 따라 사회문제가 되고 있는 것이 사실이다. 이에 대해 중국정부는 생성형 AI의 발전과정에서 발생하는 해결해야 할 과제로 인식하고, 다양한 정책과 입법을 준비하고 있다. 또 생성형 AI 기술의 발전을 위해서는 국제적 협력도 매우 중요하다. 이러한 점에서 중국정부는 어떠한 정책을 펼칠지에 대해서도 관심을 가지게 한다.

〈참고 자료〉

- 张新生、王润周、马玉龙, “AIGC背景下虚假信息治理挑战、机会与策略研究”, 情报科学, 2024.
- “专访最高法刑三庭庭长陈鸿翔: 加强AI深度伪造等研究 适时出台规范性法律文件”, 最高人民法院, 2025-03-08, <https://www.court.gov.cn/zixun/xiangqing/458031.html>(검색일: 2025.03.27.).
- “最高人民法院工作报告”, 最高人民法院, 2025-03-08, <https://www.court.gov.cn/zixun/xiangqing/457991.html>(검색일: 2025.03.27.).
- “两会大家谈: 靳东、雷军深受其害——AI深度伪造风险如何治理”, 新京报, 2025-03-07, <https://baijiahao.baidu.com/s?id=1825943624199733325&wfr=spider&for=pc>(검색일: 2025.03.27.).

CSF 이슈분석은 대외경제정책연구원(KIEP)에서 발간하고 있으며,

저작권 정책은 '공공저작물 자유이용허락 표시기준 제 4유형'에 따릅니다.

해당 원고에 대해 사전 동의 없이 상업 상 또는 다른 목적으로 무단 전재·변경·제 3자 배포 등을 금합니다.

또한 본 원고를 인용하시거나 활용하실 경우 △출처 표기 △원본 변경 불가 등의 이용 규칙을 지켜셔야 합니다.

본 원고에 대한 글, 그림, 사진 등 저작권자가 표시되어 있지 않은 모든 자료에 대한 저작권 책임은 저자 본인에게 있으며,

해당 원고의 의견은 KIEP 및 CSF의 공식적인 입장을 대변하고 있지 않습니다.