JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 1, pp. 205-214, January 2025
https://doi.org/10.9708/jksci.2025.30.01.205

Research on Improvement Measures to Prevent Digital Crimes

Kwang-Hyun Park*

*Professor, Dept. of Police & Law, Kwangju Women's University, Gwangju, Korea

[Abstract]

Recently, digital crimes abusing artificial intelligence (AI) technology have been raised as a social problem. Advances in technology are changing the nature of crime. In particular, in order to deal with this phenomenon as deepfake crimes become rampant, the Special Act on the Punishment of Sexual Violence Crimes, etc. on October 16, 2024, requires the purpose of distributing, etc., in the punishment provisions for synthesis, editing, processing, etc. By deleting the purpose crime provision, the punishment for editing deepfake pornography for the purpose of distribution, etc. has been expanded to include punishment even in cases where there is no purpose such as distribution. New regulations have been established to punish not only creators of deepfake pornography, but also those who possess, purchase, store, and view the content. The scope of application has been expanded in that possession is also punished, and punishment for producers of deepfake pornography has been significantly strengthened. Additionally, the Act on Sexual Protection of Children and Adolescents is actively responding to deepfake crimes. In addition, deepfake election crimes, defake copyright infringement, and criminal legal issues are problematic. In this study, we examine the functions and social risks of deepfake and seek countermeasures according to the reality of digital crimes using deepfake technology.

▸ **Key words**: Digital sex crime, Deepfake, Artificial intelligence, Pornography, Criminal liability, Ability to take responsibility, Election crime, Defamation

[요 약]

최근 인공지능(AI) 기술을 악용한 디지털 범죄가 사회적 문제로 제기되고 있다. 기술의 발전이 범죄 양상을 바꿔놓고 있다. 특히 딥페이크 범죄가 사회적 문제로 제기됨에 따라 이러한 현상을 적극적으로 대처하기 위해 2024년 10월 성폭력범죄의 처벌 등에 관한 특례법을 개정하였다. 성적인 허위영상물 등의 합성·편집·가공 등에 대한 처벌 규정에서 반포 등을 할 목적을 요하는 목적범 규정을 삭제함으로써 반포 등 목적으로 한 딥페이크 음란물 편집 등을 처벌하던 것을 반포 등 목적이 없는 경우에도 처벌대상으로 확대하였고 딥페이크 음란물을 제작한 자뿐만 아니라 단순 소지·구입·저장·시청자도 처벌하는 규정을 신설하였는데, 소지한 경우에도 처벌한다는 점에서 처벌범위가 확장되고, 딥페이크 음란물 제작자 등에 대한 처벌도 대폭 강화하였다. 또한 아동·청소년의 성보호에 관한 법률에서도 딥페이크 범죄에 적극적으로 대응하고 있다. 이 외에도 딥페이크 선거범죄, 딥페이크 저작권 침해 등 형사법적 쟁점 등이 문제된다. 본 연구에서는 딥페이크의 기능 및 사회적 위험성을 살펴보고, 딥페이크 기술을 활용한 디지털 범죄의 실태에 따른 대응방안을 모색하고자 한다.

▸ **주제어**: 디지털 성범죄, 딥페이크, 인공지능, 음란물, 형사책임, 책임능력, 선거범죄, 명예훼손죄

• First Author: Kwang-Hyun Park, Corresponding Author: Kwang-Hyun Park
*Kwang-Hyun Park (sanaigo@naver.com), Dept. of Police & Law, Kwangju Women's University
• Received: 2024. 11. 25, Revised: 2024. 12. 23, Accepted: 2024. 12. 27.

Copyright © 2025 The Korea Society of Computer and Information
http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945
www.kci.go.kr

I. Introduction

인공지능의 발달로 디지털 범죄 중 딥페이크 범죄와 같은 신종범죄가 최근 사회적 문제로 제기되고 있다. 딥페이크(Deep Fake)란 컴퓨터가 인간처럼 생각하고 학습할 수 있는 인공지능 기술인 딥러닝(deep learning)과 가짜라는 영어 뜻의 페이크(fake)를 결합한 합성어로 AI기술을 활용하여 실제와 비슷한 가짜 사진이나 영상 및 음성 등을 제작하는 기술이다. 딥페이크는 기술의 양면성을 지닌다. 딥페이크는 가상 인물 캐릭터를 이용하여 역사적 인물의 모습을 재현할 수 있고 교육 콘텐츠 제작에 활용하는 등 순기능적으로 사용되는 반면 이를 악용하여 가짜 뉴스를 전파하거나 타인의 얼굴 또는 음성 등을 무단으로 도용하여 헌법상 보호되는 사생활의 자유을 침해하거나 범죄로 악용하는 경우도 있다. 즉, 인공지능 기술은 비디오, 오디오 등의 딥페이크를 이용하여 실제로 부존하거나 가상의 사건 등을 재현하여, 창의적이고 현실감 있는 콘텐츠 문화를 만들어 낼 수 있다는 긍정적인 측면과 함께, 딥페이크 성범죄, 여론조작을 통한 딥페이크 허위사실 유포 등은 민주주의를 위협하는 등 사회 여러 분야에서 위험성을 내포하고 있다. 딥페이크는 단순히 이미지 짜깁기를 의미하는 것이 아니라 인공지능의 학습 기술을 사용해 단순하게 사진을 합성해 주는 것부터 입 모양에 맞쳐 원본과 동일한 음성을 자연스럽게 구현함으로써 악용될 소지가 크다. 특히, 10대 딥페이크 범죄가 만연하고 있는데, 이는 스마트폰의 폐해 및 유해 콘텐츠 접근 용이성 등에서 기인한다. 이를 위해 미국, 프랑스에서는 등교 후 스마트폰 사용금지라는 규제를 시행하고 있다.

Table 1. Age Status of Arrested Suspects in Korea

연도	10대 피의자 수	전체 피의자 수	10대 피의자 비율
'21년	51	78	65.4%
'22년	52	85	61.2%
'23년	91	120	75.8%
'24년 1월~7월	131	178	73.6%

이러한 디지털 범죄의 딥페이크 역기능을 방지하기 위해 2024년 10월 16일 '성폭력특별법'과 '아동·청소년의 성보호에 관한 법률'을 개정하였다. 또한 딥페이크 선거범죄에 대응하기 위해 공직선거법 제82조 8에서 딥페이크 영상 등을 이용한 선거운동 제한조항을 신설하였으며, 형법상 제309조 명예훼손죄, 동법 제311조 모욕죄의 성립이 적극적으로 검토되고 있다.

그리고 딥페이크는 지식재산권 중 저작권에서도 문제된다. 저작권에는 저작재산권과 저작인격권으로 구성되는데, 동의없이 무단으로 사용한 경우 저작재산권이 문제되며, 저작인격권으로는 동일성유지권, 복제권, 2차적저작물작성권 등의 침해가 문제된다. 다만, 일부 법적으로 허용되는 '패러디(Parody)'로서 인정되는 경우에는 동일성유지권 또는 2차적저작물작성권 침해로부터 비교적 자유로울 수 있지만 헌법상 표현의 자유도 헌법 제37조 제2항에 의해 한계를 가진다.

기존의 선행연구들은 주로 딥페이크 기술의 활용에 관한 다수의 논문이 존재하고, 딥페이크 관련 범죄에 관한 융합연구는 미미하므로 딥페이크에 따른 범죄를 구체적으로 살펴보는 것이 본 연구의 목적이다.

이하에서는 딥페이크 국내·외 동향을 살펴보고 딥페이크 범죄를 유형화한 후 문제점을 파악하여 기술적, 법적, 교육정책적 개선방안을 모색하고자 한다.

II. Preliminaries

1. International trends

1.1 USA

미국은 딥페이크 범죄에 대해 빅테크에 대한 법적 의무를 강화하고 있다. 빅테크 기업들은 고의 또는 과실로 성착취물을 방치하여 광고 수익을 올리고 있다는 점에서 불법 콘텐츠 유통에 책임을 묻고 있는데, 50개주 중 27개 주정부에서 딥페이크를 규제하는 법안을 마련하였고 캘리포니아 주가 대표적이다.[1][2]

미국은 딥페이크에 관한 일반적 규제를 위해 2018년 Sasse 상원의원은 처음으로 「악의적 딥페이크 금지법」(Malicious Deepfake Prohibition Act of 2018)법안을 발의하였지만 의회를 통과하지 못하였다. 이후 2019년 「딥페이크 책임법」(DEEP FAKES Accountability Act)으로 명명되는 법안도 통과되지 못하였다. 그러나 2023년에 Clarke 의원은 재차 수정 보완한 「딥페이크 책임법」을 발의하여 2024년 현재 위원회에 회부되어 심의 중에 있다. 이 법안은 딥페이크에 의해 변경된 요소에 대해 표시의무를 부과하고 동일성을 벗어난 변화된 범위를 간략히 설명할 것을 의무화하고 있다. 또한 생성형 인공지능 등에 의해 만들어 졌으며 콘텐츠 출처를 밝힐 것 등의 의무를 부과하고 있다. 우리나라의 경우 공직선거법에서 시행하고 있다.[3] 이러한 공개 준수의무를 이행하지 않거나, 공개내용을 제거·변경하는 경우 기록당 최대 150,000달러의 민사벌금(civil penalty) 및 가처분 조치를 받을 수 있다

www.kci.go.kr

[Sec. 2(a) - §1041(f)(2)]. 그리고 의무 미준수 시 타인에 대한 명예훼손의 의도가 있었거나 성적 행위를 하는 것처럼 보이게 하는 경우 등에는 벌금 또는 5년 이하 징역형의 형사처벌이 가능하다. 이 밖에 온라인 플랫폼 제공자에게 배포된 콘텐츠가 딥페이크여부를 식별하는 감지하는 시스템을 갖출 것을 요구하고 있으며, 국토안보부 과학기술국 산하에 딥페이크 전담팀을 설치하도록 하고 있다. 바이든 정부는 2023년 AI 행정명령에서 AI 생성 합성 콘텐츠에 대한 출처 및 표시 의무, 인증 등의 도구로써 평가 프로그램을 개발하도록 하였다. 개별적인 케이스로써 캘리포니아, 텍사스 주에는 선거 관련 딥페이크에 전문화된 법률도 있다. 디지털 성범죄의 경우 버지니아 주는 2019년부터 딥페이크 형태로 생성한 보복형 성적촬영물에 대하여 1년 이하의 징역 과 2,500달러 이하의 벌금을 과하는 법률을 시행하고 있고, 캘리포니아 주는 디지털 성범죄와 관련한 딥페이크 합성물의 배포를 민사적인 규제를 통해 해결하고 있다.[4]

1.2 EU etc.

2024년 5월 EU 이사회는 EU 인공지능법(Artficial Intelligence Act: AI Act)을 최종 승인하였고 8월에 공식 발효되어 인공지능의 위험성에 따라 순차적으로 AI시스템의 투명성과 책임성을 강화할 계획이다.[5] 유럽연합은 이 법을 제정해 플랫폼에 불법, 유해한 콘텐츠의 삭제, 감시, 감독 의무를 부과했다. 특히 AI 규제법으로 딥페이크 워터마크 표시, 디지털서비스법으로 플래폼에 대한 유해 콘텐츠 검열 의무화를 명시하였다. EU 인공지능법은 약한 인공지능시스템의 경우도 특정 인공지능 시스템의 경우 제공자와 배포자에게 의무를 부과한다. 딥페이크에 관해 EU 인공지능법특별규정이 존재한다. 딥페이크의 정보표시와 공개 시기는 최대한 자연인과의 첫 번째 상호작용 또는 자연인에게 처음으로 노출되는 시점까지를 요하고, 정보에 관련된 제공 방식은 명확하고 식별가능한 방식이어야 한다. 인공지능시스템 투명성에 대한 제공자 및 배포자 의무 미준수 시에는 과태료가 부과된다. 더욱이 사업체가 위반한 때에는 직전 회계연도 전 세계 연간 총 매출액의 최대 3% 금액의 과태료를 부과한다.

1.3 Other countries

영국도 딥페이크 성착취물 제작 및 유통시 형사처벌을 강화하고 있고, 프랑스는 비(非)동의 딥페이크 제작 및 유통을 금지하고 있는데, 세계 각국은 딥페이크 범죄에 대해 형사법적 개입을 통해 적극적으로 대응하고 있다. [5]

2. Domestic trends

딥페이크 성범죄는 2024년 10월 16일 '성폭력범죄의 처벌 등에 관한 특례법'를 개정하여 시행하고 있다. 이전 법에서는 성적인 허위영상물 등의 편집·합성·가공 등에 대한 처벌 규정을 목적범으로 규정하였다. 그러나 개정법에서는 '반포 등을 할 목적' 규정을 삭제하였는데, 이러한 목적을 증명하기 난이했기 때문이다. 그리고 딥페이크 음란물 제작자뿐만 아니라 소지·구입·저장·시청자도 처벌하는 규정을 신설하였다. 최근 물의를 일으킨 미국 국적의 외국인이 딥페이크 성관련 영상물 소지 등의 혐으로 수사 중에 있다. 개정법은 종전에 비해 딥페이크 음란물 제작자 등에 대한 처벌을 대폭 강화하였다. 또한 아동·청소년의 성보호에 관한 법률에서는 아동·청소년성착취물을 이용한 협박의 및 강요행위에 대해 형벌을 강화하였으며 긴급을 요하는 등 일정한 경우 사법경찰관리가 신분비공개수사를 할 수 있고, 사법경찰관리은 방송통신심의위원회에 대한 삭제 또는 접속차단 조치를 요청할 의무를 부과하는 규정을 신설하였다.[6]

그리고 딥페이크 선거범죄에 대응하기 위해 공직선거법 제82조8는 딥페이크 영상 등을 이용한 선거운동 제한 조항을 신설하였다. 제1항은 '누구든지 인공지능 기술 등을 이용하여 만든 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상 등을 선거일 전 90일부터 선거일까지 선거운동을 위하여 제작ㆍ편집ㆍ유포ㆍ상영 또는 게시하는 행위를 하여서는 아니되고', 제2항에서는 '누구든지 제1항의 기간이 아닌 때에 선거운동을 위하여 가상의 정보라는 사실을 명확히 인식할 수 있도록 중앙선거관리위원회 규칙으로 정하는 바에 따라 해당 사항을 딥페이크영상 등에 표시하여야 한다'고 규정하였다.[6] 이를 위반한 경우에는 공직선거법 제250조 허위사실공표죄가 성립하고, 제4항에서 제82조의8제2항을 위반하여 중앙선거관리위원회규칙으로 정하는 사항을 딥페이크영상등에 표시하지 아니한 경우5년 이하의 징역 또는 5천만원 이하의 벌금이나 7년 이하의 징역 또는 1천만원 이상 5천만원 이하의 벌금에 처하게 된다.[7] 이 밖에 형법상 309조 명예훼손죄, 동법 제311조 모욕죄가 성립된다.

3. Usefulness of deepfakes

딥페이크는 적대관계생성신경망(GAN)을 이용하여 원본 이미지 위에 다른 이미지를 결합해 새로운 이미지를 생성하는 기술을 말한다. 적대관계생성신경망 기술은 생성모델과 분류모델로 나뉠 수 있다. 생성모델은 원본과 차이가 없는 데이터를 만들려는 것이고 분류보델은 원본과 다른 점

www.kci.go.kr

을 찾아내는 것인데 무한 반복실행을 통해 원본과 흡사한 데이터를 만들어내는 알고리즘이다. 큰 틀에서 보면 AI기술, 그 안에서도 딥러닝 기술의 하나이다.[8] AI프로그램이 가짜 이미지나 동영상을 만들기 위해 이미지를 조작하여 실제처럼 보이는 는 것을 전반적으로 딥페이크라 부르지만 드라마·영화 상에서 배우가 직접 촬영하기 어려운 부분에 대역을 사용한 후 대역의 얼굴을 배우의 얼굴로 변환하는 '페이스에디팅(face-editing)'기술, 배우의 주름, 나이대 등 얼굴을 보정하는 '페이스에이징/디에이징' 기술 등 여러 가지가 존재한다.[9] 적대관계생성신경망을 이용한 기술들은 이미지를 생성해 낸다는 특성 때문에 영화,드라마 등 미디어 산업에서 활용되고 있다. 기존 VFX(visual effects) 는 수작업으로 행해졌지만 AI 기술을 활용하여 인간의 작업부분을 최소한으로 하고, 콘텐츠에서 구현해 내야할 난이한 영상도 효과적으로 제작함으로써 시간, 비용 및 제작환경 등에 효율적이고 완성도 높은 결과물을 창출하게 되었다. 예를 들어 딥페이크 기술을 이용하면 영상속 인물이 현재 한국어를 사용하지만, 중국어, 영어, 프랑스어, 독일어 등을 말하는 것처럼 자연스럽게 입 모양을 변경하여 영상을 만들어낼 수 있다.[10] 실제로 2024년 광복적에 독립투사의 얼굴과 음성을 자연스럽게 만들어 세계 각지에 홍보하며 캠페인의 효과를 높이기도 하였다.

딥페이크 기술은 얼마든지 유용한 목적으로 다양하게 사용될 수 있다. 특히 표현의 자유에 더 큰 날개를 달아주는 혁신적인 기술이다. 존재하지도 않는 인간, 즉 버추얼 휴먼(virtual human)을 만들어줘 인플루언서·가수·아나운서·연예인 등으로 광고계와 방송 및 영화계에서 활동할 수 있게 해준다. 또한 딥페이크는 특정인에 대해 시간 여행을 가능하게 해준다. 즉 나이를 더 들게 할 수도 있고, 덜 들게 할 수도 있다. 이처럼 나이를 조정하는 딥페이크 기술을 특별히 '디에이징'(de-aging)이라고 부른다. 딥페이크는 현행 헌법상 표현의 자유를 통한 행복추구권 측면에서 유용성을 가진다. 다만 사생활의 자유와 기본권 충돌이 발생할 수 있다. 이하에서는 딥페이크 범죄를 유형화하여 살펴보고자 한다.[11]

III. Deepfake-related crimes

1. Deepfake sex crime

1.1 Reality of deepfake sex crimes

성과 관련된 규제법률은 기본법이자 일반법인 형법 이외에도 성폭력특별법, 아동청소년 성 보호에 관한 법률, 성매매방지법과 같은 특별형법, 그리고 절차법인 형사소송절차나 형 집행상 특례 등 다수의 법률들이 마련되어 있다. 성범죄의 경우 보호법익이 문제되는데, 보호법익(Rechtsgut)이란 법으로써 보호할 가치가 있는 이익을 말하며, 일반적으로 성적자기결정권을 보호법익으로 한다. 보호법익은 처벌규정의 법적근거를 제공하기 때문에 그 기능 및 역할이 매우 중요하다. 성적 자기결정권은 성적결정에 대해 자유로운 성 선택의 자유를 부여한 헌법의 인간의 존엄성과 행복추구권에서 파생된 권리이다. [12][13] 이와 더불어 사회적 법익에 관한 범죄 중 공연음란죄와 같은 성 풍속에 관한 범죄유형도 존재한다. 성폭력특별법상 딥페이크 기술을 이용성범죄를 종전 비범죄화 유형에서 현재 범죄화 하여 처벌하는 이유는 성적자기결정권 및 사생활의 자유를 보호하기 위한 것이다.[14] 전체가 아닌 일부의 이미지로부터 추출한 데이터를 전혀 관계없는 포르노나 성착취물에 삽입한 후 이를 유포하겠다는 협박 또는 금전을 요구하는 범죄가 발생하고 있다. 게다가 딥페이크 기술을 통해 성폭력 피해자의 얼굴을 합성하여 가짜 영상을 만들고, 기존에 법적심판을 받은 성폭력 사건을 사실이 아닌 것처럼 조작할 수도 있다. 즉, 성폭력 가해자는 책임을 회피하기위해 딥페이크 기술을 악용할 수 있고. 최근 미성년자들이 친구가 SNS에 올려진 사진을 동의없이 딥페이크 음란 콘텐츠에 조작한 사건이 발생하였다.

이러한 콘텐츠는 인터넷상에 유포되면 완전히 삭제하기 어렵다. 현행 성폭력특별법상 카메라등 이용 촬용죄는 판례에 의하면 피해자의 신체를 직접 촬영한 영상이나 이러한 영상의 복사본에 국한되므로 법적용에 사각지대가 발생하고 있다. 이로 인해 성범죄 증거를 위조하거나 허위사실을 제작해 형사체계에 혼란을 초래할 수 있으므로, 적극적으로 디지털성범죄에 사전예방에 초점을 두어야 한다.[15]

Table 2. Status of Deepfake Sex Crimes

딥페이크 성범죄 접수 건수	812건
집중 단속 기간 접수 건수 (8월 28일 이후)	일평균 12.66건
딥페이크 성범죄 피의자 수	387명

1.2 Deepfake sex crime problem

딥페이크 기술을 악용한 디지털성범죄를 예방하기 위해 정부는 다양한 노력을 기울이고 있다. 그럼에도 딥페이크 기술을 이용한 디지털 성범죄는 여전히 우리 사회를 불안

www.kci.go.kr

하게 만드는 요소로 여겨지고 있다. 종전에는 연예인을 대상으로 한 허위 영상물이 대다수였지만, 최근에는 남녀노소를 불문하고 일반인들이 SNS에 올려진 일상 사진이나 영상을 사용하여 성적자기결정권을 침해하는 성관계 영상과 합성 및 제작, 유포하는 '지인능욕'이라는 새로운 범죄 행태가 발생하고 있다.[16][17] 영상 속의 인물은 존재하지 않는 가상의 인물이므로 특정될 수 없고, 이로 인해 아동·청소년에 대한 인권침해 등에 해당하는지 판단하기 난이하다. 만약 실존하지않는 인물이 영상에 출연하는 것이라면 이를 두고 성폭력처벌법에서 정의하는 아동·청소년 및 특정인물이 출연하는 음란물의 요건에 해당하지 않게 된다. 실제로 존재하지 않는 인물을 가공하여 제작한 딥페이크 영상이라면 성폭력처벌법상 불법촬영물의 제작뿐만 아니라 소지죄 처벌조항에도 포섭되지 않아 구성요건에 해당되지 않을 수 있다. 만약, 이러한 불법 구매자 또는 이용자 다운로더는 형법총칙상 형법상 공범 또는 불법 판매자의 종범으로서 처벌하는 경우 저작권법에 위반될 수 있다.[18]

1.3 Trends in precedents

딥페이크 성범죄가 일상적인 일터를 넘어 전국 초·중·고등학교까지 확산하고 있다.[19] 최근 주요 외신들은 한국이 몰카범죄에 대응하기 위해 딥페이크와 전투를 벌이고 있다며 보도하였고, 한국이 세계적 딥페이크 성착취물 문제의 원천이라고도 말하고 있다. 최근에 발생한 '서울대 N번방' 사건에서 허위 음란물을 제작하고 배포한 혐의 등으로 공소제기된 주범이 1심에서 징역 10년을 선고받았다. 서울중앙지법 형사31부(2024.10.30. 2024고합465)는 아동·청소년의 성보호에 관한 법률 위반(성착취물제작·배포 등) 등 혐의가 적용되었다. 1심 재판부는 피고인이 제작한 허위 음란물은 그 자체로 혐오감을 느끼게 하고, 피고인들의 대화도 경악스러울 정도이며, 마치 사냥감을 선택하듯이 피해자를 무작위로 선정해 졸업, 결혼, 가족사진 등을 이용해 오랜기간 성적으로 모욕하고 인격을 말살시켜 비난가능성이 크다는 입장을 표했다.[19] 이어 피고인들의 심신미약주장을 받아들이지 않았으며, 범죄의 피해 회복이 사실상 불가능하고, 법의 엄중한 심판을 통해 법과 도덕을 무시 형벌이라는 엄격한 사회적 제재가 부과된다고 강조했다.[19]

2. Deepfake election crime

2.1 Reality of deepfake election crimes

2024년은 '슈퍼 선거의 해'라고 부른다. 전 세계 76개국이 미래 방향을 바꿀 수 있는 중요한 선거를 치렀거나 치를 예정이다. 선거에 참여하는 유권자만 42억 명에 이른다.[20] 그런데 세계 각국은 각종 선거에서 딥페이크를 악용한 가짜뉴스 등으로 혼란을 겪고 있다. 한국도 지난해 총선을 앞두고 딥페이크를 악용한 선거법 위반 사례가 증가하자 공직선거법을 개정해 선거운동 목적의 딥페이크 영상을 제작, 편집, 유포, 상영, 게시를 금지했다. IT전문가들은 기술적인 접근만으로는 딥페이크 범죄를 효과적이고 원천적으로 차단할 수 없기 때문에 이와 병행하여 교육 등의 제도적 보완 조치가 선행될 것을 주장한다. 아동 성범죄뿐만 아니라 디지털 위장 수사 범위를 일반 성범죄까지 확대하여 실효성 있는 대책이 필요하다. 딥페이크 불법생성물 탐지 기술은 이미 피해 및 침해가 발생된 후 개입하는 사후 조치로 사전점죄 예방에 신속하게 대응하지 못한다. 이에 더해 딥페이크 탐지 기술을 우회하는 새로운 기술이 계속 발전하고 있으므로 적극적 대응이 요구된다.[21]

2.2 Problems with deepfake election crimes

주지하듯이 선거는 시민들이 자신을 대리할 대표를 선택하고 앞으로의 정책을 결정하며 사회적 합의를 이루는 민주주의의 출발 지점이다. 따라서 올바른 선택이 이루어지려면 모든 후보와 정책에 대해 사실에 근거한 정확하며 공정한 정보를 유권자들에게 제공해야 한다. 공정한 선거를 위한 기본적인 거버넌스로서 우리나라의 경우, 공직선거법을제정했고, 중앙선거관리위원회를 운영하고 있다.[22] 그럼에도 선거의 공정성을 해치는 행위는 언제나 발생했고, 그에 따른 조사와 재판, 처벌도 꾸준히 이루어졌다. 예를 들어 금품수수 행위, 허위사실 유포와 비방 등은 법률상 선거범죄로 명시돼 있는데, 이 때문에 징역 또는 100만 원 이상의 벌금형을 받으면 선거 결과 당선이 됐더라도 무효 처리가 된다(공직선거법 제264조). 그런데, 최근 '딥페이크'(deepfake)라는 인공지능 기반의 신기술이 사회 전반에 보급되면서 다루기 힘든 새로운 선거범죄가 갈수록 증가하고 있다. 2023년 8월과 9월에 유네스코(UNESCO)가 선거를 앞둔 미국·멕시코·인도 등 16개국 출신 성인 8,000명을 대상으로 조사한 결과, 응답자의 85%가 딥페이크 등 온라인 가짜뉴스가 선거에 매우 나쁜 영향을 미칠 것이라고 대답했다. 빌 게이츠 마이크로소프트(MS) 창업자는 인공지능이 생성한 딥페이크에 의해 퍼진 허위 정보는 선거 및 민주주의를 훼손한다는 우려를 표했다. 딥페이크가 선거에 미치는 영향에 대한 걱정이 갈수록 커지고 있다. 2020년 미국 대선을 앞둔 하원 의회는 딥페이크가 대선에 큰 영향을 줄것으로 우려해 "착취에 대한

책임 소재를 명확하게 하며 모든 사람을 거짓된 모습으로부터 보호하는 '딥페이크 책임법'(HR.3230-2019)을 2019년 6월 발의했다. 이 딥페이크 책임법은 딥페이크 기술 자체를 전적으로 나쁜 기술로 보지 않고 중립적인 기술로 보면서도 악용과 남용에 대비하는 규정을 제시하고 있다. 특히 딥페이크를사용할 경우, 이에 대한 사용 정보를 기록한 기술적 조치인 워터마크(watermark)를 남기도록 할 뿐만 아니라 "딥페이크 기술로 제작했다"는 라벨(label)을 다는 등 '디스클로저'(disclosure, 자발적 폭로) 조치도 같이 시행하도록 해 '투명성'(transparency)을 강하게 요구한다.[23] 이를 무시하거나 의도적으로 표식을 제거한 경우, 민·형사상 책임을 묻는다. 이 법안이 발의된 후 4년이 지나도록 특별한 진전이 없이 여전히 의회에계류 중이지만, 이후에 다른 법안과 정책에 적지 않은 영향을 줬다. 예를 들어 2023년 10월 30일 조 바이든 미국 대통령이 발표한 'AI 행정명령'에도이 규제가 그대로 인용됐다. 인공지능 기반 사기와 속임수로부터 미국 시민을 보호하기 위해 "인공지능이 생성한 콘텐츠에 명확하게 라벨을 붙일수 있는 콘텐츠 인증 및 워터마킹에 대한 지침을 개발"하라는 상무부를 향한 지시가 AI 행정명령 안에 포함돼 있다. 2024년 3월 유럽의회의 인준을받은 유럽연합의 인공지능 법(AIA, AI Act) 역시 딥페이크와 같이 인공지능이 생성한 콘텐츠로 인한 피해를 예방하기 위한 조치로 워터마크와 디스클로저를 요구한다.딥페이크의 이러한 악용에 따른 부작용은 '선거'라는 특별한 상황에 들어서면 더 심각해진다. 일반인을 대상으로 한 딥페이크 사건은 인지되는 순간부터 이를 추적해 범인을 찾아내 처벌하는 과정에서 시간제한을 받지 않는다. 그런데 선거의 경우 '선거기간'과 '선거일'이라는 특정한 시간적 조건을 가지고 있다. 예를 들어 선거일에 임박해 상대 후보에 대한 악의성딥페이크 영상을 만들어 배포하면, 이에 대해 반박할 시간적 여지가 거의없다. 누가 그 딥페이크 영상을 열람했는지도 파악하기 힘들고, 이에 대한 해명 자료를 추가로 배포한다고 해도 선거일에 이르면 변명 활동도 중단해야 한다. 결국 딥페이크를 이용해 유권자에게 잘못된 정보를 제공하고 나면, 이를 시정할 틈도 없이 선거가 마감될 수 있다. 선거가 끝난 후 딥페이크 영상을 누가 만들어 배포했느냐를 따질 때, 이로 인해 이익을 얻은 입후보자나 소속 선거본부에서 책임질 만한 증거를찾아내지 못할 경우, 법률에 명기된 당선무효 조치도 취하기 어렵다. 특히최근 선거 운동에는 특정 후보의 지지층들이 열정적이며 자발적으로 선거운동을 하는 경향이 강해져서 유튜브 활동은 물론 딥페이크를 이용한 홍보물 제작과 배포도 직접 당당할 만큼 전문성도 가지고 있다. 더구나 딥페이크 기술 역시 작은 비용으로도 쉽게 활용할 수 있고, 조금만 지식을 가지게되면 공개된 도구를 가져다가 직접 제작할 수도 있다. 최근에는 정보화가진행된 베트남이나 말레이시아 등에서 적은 비용을 받고 고품질의 딥페이크 콘텐츠를 제작해 주겠다는 광고를 텔레그램이나 다크웹을 통해서 쉽게만날 수 있다.[23]

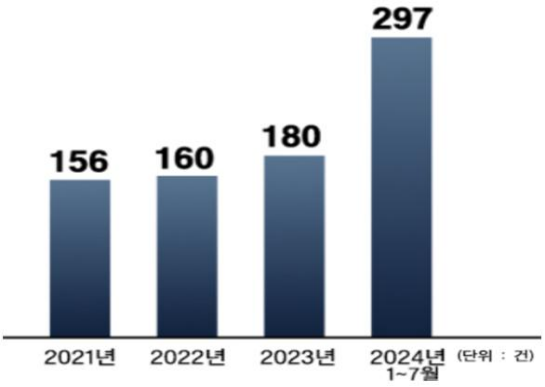


Fig. 1. Current Status of False Video Crimes

3. Crimes of intellectual property infringement, including copyright

3.1 Copyright infringement

딥페이크 저작권 침해는 생성형AI를 이용한 창작물이 저작권법의 보호대상인 저작물에 해당하는지 아니면 생성형 AI를 이용한 '인간 이용자'의 아이디어 제공 또는 명령어 입력이 저작권의 보호 대상인 '창작적인 표현형식에 어느 정도 기여하는 행위'로 볼 수 있는지 여부에 따라 결정된다. 우리 판례는 현행 저작권법상 법률에 의해 원칙적으로 자연인에게 인정되고, 법인에게도 확장해서 인정하고 있다. 그런데 현재의 생성형 AI는 '인간 이용자'의 아이디어 제공 또는 명령어 입력에 의해서만 새로운 데이터를 만들어내고, '인간 이용자'의 관여 없이 오직 생성형 AI가 독자적으로 새로운 데이터를 발생 또는 생성하지 않는다.

그리고 생성형AI 프로그램 제작자 또는 제공자는 이러한 프로그램을 제작하거나 제공한 자일뿐이지, 생성형AI를 이용한 창작물에 창작적 기여를 한 자는 아닌 점에서 '생성형 AI를 저작자로 인정하는 법개정'이 이루어지지 않는 한, '인간 이용자'가 저작권자가 된다. 단지 아이디어 제공 또는 명령어 입력을 통해 생성형AI를 이용하여 창작활동을 한 경우일지라도 아이디어 제공 또는 명령어 입력이 '인간 이용자'의 사유의 산물로 평가될 수 있다면, 현행법상 인간 이용자만을 작재산권 및 저작인격권의 귀속주체로볼 수 있다.(대법원 2021. 7. 8. 선고 2018도525 판결 등).[24]

또한 생성형 AI를 이용하여 창작활동을 한 자는 저작자

www.kci.go.kr

및 저작권 귀속주체 표시의 경우 해당 저작물을 생성형 AI를 이용하여 저작하였다는 사실까지 은닉하며 자신의 저작물이라고 할 수 있지만, 해당 저작물을 생성형AI를 이용하여 저작하였다는 것을 공지하고 해당 저작물은 '자신의 저작물'이라고 표현할 수도 있다. 생성형AI를 이용한 저작물의 경우, 인간이 해당 저작물의 저작자인 경우, 현행법상 적법한 저작자 표시이므로 사기죄 성립요소인 기망행위에 해당한다고 볼 수는 없어 성립여부에 대해 소극적이다.[25]

3.2 Types of Copyright Infringement

제4차 산업혁명 시대의 도구를 활용하여 누구나 쉽게 딥페이크 영상제작이 가능해짐에 따라 다양한 콘텐츠에 얼굴, 음성 등을 합성하여 무단으로 배포하는 새로운 저작권 침해유형이 새롭게 문제되고 있다. 이러한 저작물 콘텐츠를 활용하여 무단으로 영상을 제작하거나 배포하는 행위는 저작권법상 동일성 유지권이라는 저작인격권과, 저작재산권으로서의 복제권, 2차적저작물작성권, 저작물 이용과정에서의 일시적 복제 등을 침해할 소지가 있다. 이에 대해 한국저작권보호원은 저작권 침해 사례로 한 유형으로 딥페이크 기술을 이용한 침해를 조사하였는데, 이 보고서에 따르면, 유튜브 등에 게시된 딥페이크 영상의 상대수가 저작권법을 위반한 사실을 확인하였다.[26]

IV. Improvement plan

정부는 새로운 디지털 질서 정립 추진계획에서 8대 핵심과제를 제시했다. 이 중 AI 기술의 안전성과 신뢰, 윤리 확보 및 딥페이크 활용 범죄 등에 대응하기 위해 AI기본법 제정, AI생성물에 워터마크 표시 의무화, 디지털 안전 통합법 제정, 디지털 포용법 제정 등을 목표로 하고 있는데, 이하에서는 디지털 범죄 예방을 위한 개선방안을 기술적, 법적, 교육정책적 대응방안을 모색하고자 한다.



Fig. 2. The Government's Eight key Wigital Issues

1. Technical countermeasures

인공지능은 이미지 생성모델, 음성생성모델을 포함한 생성 AI의 대중적이고 보편적으로 활용되고 있다. 이에 따라 생성 AI가 사진, 영상, 음성 등을 합성하여 딥페이크를 제작함으로써 오용되고 있는데, 기술적 대응방안이 요구된다.

1.1 Generative AI prompt filtering

특정 단어나 위법한 의도를 가진 프롬프트를 필터링을 통해 예방하는 것이다. 대부분의 생성형 AI 이미지나 영상은 텍스트 기반의 프롬프트(명령어)로 만들어지는데, 진다. 최근에는 디자인 회사에서 프롬프트 디자이너라고 해서 명령어를 잘 '디자인'하고 실행하는 인력을 채용하기도 한다. 오픈AI(OpenAI)나 어도비(Adobe)와 같은 기업은 특정 키워드나 주제에 대한 생성을 제한하는 시스템을 강화하고 있다. 기술적 필터링은 특정 키워드나 명백히 부적절한 표현에 대해서는 효과적이지만, 문맥적으로 애매한 프롬프트에 대해서는 부정확하게 작동할 수 있다. 은유적 표현이나 우회적 언어를 쓸 경우 필터링 시스템이 제대로 인식하지 못할 수 있다.필터링이 지나치게 엄격해질 경우, 예술가가 인공지능을 이용해 실험적이거나 비판적인 예술을 창작하는 데 제약이 생길 수 있다. 예술적 표현의 자유와 사회적 책임 사이의 균형을 맞추는 것이 기술적으로나 윤리적으로 매우 어려운 과제다.

1.2 Development of detection technology for AI products

오픈AI, 구글에 이어 국내의 네이버와 카카오 및 과학기술정보통신부와 정보통신기획평가원(IITP)도 AI 생성물 여부를 탐지·검증하는 기술연구를 개발 중이다. 기본적으로 딥페이크 탐지 기술은 AI 모델에 원본 데이터와 변조 데이터를 함께 넣고 미세한 차이점을 학습시키는 것이다.

물론 인공지능을 이용한 딥페이크의 기술이 정교해지고 발전속도가 탐지 기술을 앞지르고 있어 실효성 측면에서 회의적인 시각이 많다. 또한 선행조건으로 조작 여부를 탐지하기 위해서는 원본과 변조 데이터가 모두 필요하며, 원본과 변조 데이터를 AI 모델에 학습시킬 때는 이 모델을 이해할 수 있는 형태로 가공해야 하는 문제가 남아있다.

intel	페이크 캐처	얼굴의 혈류 신호 분석
Microsoft	비디오 어센티케이터	육안으로 식별 불가한 프레임 분석
Google	신스ID	육안으로 식별 불가한 워터마크 부착
DEEPBRAIN AI	딥러닝 기반 딥보이스 탐지	음성 정보 추출과 위변조 판별 모델 통합
BRAINDECK	아이리스5	음성 합성시 주파수 손실 흔적 감지

Fig. 3. AI detection technology and content

www.kci.go.kr

그러므로 딥페이크 생성과 탐지 기술의 격차의 해결은 학습 데이터의 충분한 확보가 선행과제이다

마이크로소프트(MS)의 탐지 도구 '비디오 어센티케이터(Video Authenticator)'는 육안으로 보이지 않는 프레임을 분석 후 신체 경계선에서 흐릿함의 정도 등으로 진위를 파악하고 인텔의 딥페이크 영상 탐지 기술인 '페이크캐처(FakeCatcher)'는 혈류 변화처럼 세부적인 특징을 이용하고 있다. 이것은 사람의 심장이 뛸 때 정맥의 색이 미세하게 바뀌는데 딥페이크는 이런 변화가 없다는 점에 착안한 기술이다. 딥브레인AI는 딥러닝 기반 딥보이스 탐지 기술 특허를 출원했다. 구글의 딥마인드 신스ID는 육안으로 식별할 수 없는 가짜 표식을 남기는 방식으로 딥페이크를 만드는 데 사용한 AI 모델의 흔적을 찾거나 딥페이크 파일에 담긴 정보를 분석한다. 국내의 아이리스5(Iris-5)'는 음성 합성 과정에서 발생하는 주파수 손실의 흔적을 감지하는 기술을 개발하고 있다.

1.3 Watermarking Insertion and Blockchain

딥페이크 탐지기술은 딥페이크 기술발전의 속도를 따라가지 못하고 있는 실정이고, 비교대상인 원본 데티터가 부재한 경우 한계점에 다다른다. 그러므로 생성 AI를 통해 생성한 이미지나 토큰에 워터마킹을 하자는 논의가 제기된다. 워터마킹은 디지털 컨텐츠에 지각적으로 인지되지 않는 특정마크를 은닉하는 기술로, 인터넷 확산에 따른 불법행위에 효과적으로 대응할 수 있는 기술이다. 워터마킹은 필터링, 압축 등에 의해 워터마크가 변형되지 않고, 원 신호의 품질 열화가 없어 불법사용자에 의해 검출, 삭제, 수정이 불가하다. 워터마크 삽입방법은 텍스트, 오디오, 이미지, 그리고 비디오 등 디지털 컨텐츠 종류에 따라 다르지만 이미지 화소 자체를 조작하는 공간영역 기반 워터마크 삽입과, 이미지를 주파수 영역으로 변환한 후에 워터마크를 삽입하는 주파수 영역기반 상입의 2가지로 구분된다.

워터마킹은 악의적 공격에 취약하다는 비판이 있지만, 미세 조정도 식별할 수 있는 특정 패턴과 데이터의 하류부분에 고유의 지문을 부여하는 등 이를 극복할 수 있는 지속적인 연구와 개발이 요구된다.[27]

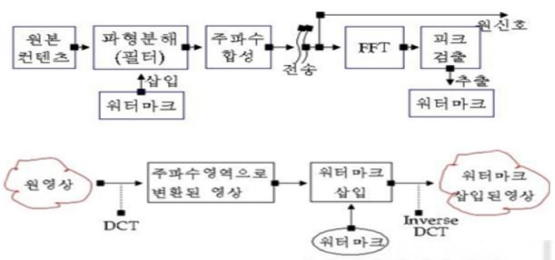


Fig. 4. Watermark insertion/extraction configuration diagram

이 밖에 블록체인 기술을 활용하는 것이다. 블록체인은 P2P 방식을 기반으로 하여 소규모 데이터들이 사슬 형태로 무수히 연결되어 형성된 '블록'이라는 분산 데이터 저장 환경에 관리 대상 데이터를 저장함으로써 누구도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있게 만든 것인데, 기존에 전자화폐로 거래할 때 중앙 서버에 거래 기록을 보관하는 것과는 달리, 블록체인은 모든 사용자에게 수많은 기록을 하나의 묶음으로 만들어 거래 기록을 보여주며 서로 비교해 위조를 막을 수 있다는 장점이 있다.

2. Legal countermeasures

딥페이크을 악용행위는 기술의 긍정적 측면에도 불구하고 타인의 사생활 및 인권을 침해하는 허위 미디어를 생성한다. 이 허구적 생성물을 이용하여 디지털 성범죄 관련 영역, 사기, 허위정보유포 등 신종범죄로 구체적인 다양한 유형으로 현출되고 있다. 따라서 딥페이크 범죄 문제에 대해 학제간 연구를 통한 접근이 필요하다. 신종기술의 발전은 긍정적인 측면과 부정적인 측면이 상존하므로 이에 대한 입법적 개입이 요구된다. 그러므로 스토킹처벌법과 같이 구체적인 행위태양을 열거하여 각 행위에 따른 불법의 정도를 평가한 후 양형기준을 개별적으로 마련할 필요가 있다. 구체적이고 세분화 된 구성요건을 명확히 규정하고, 불법에 비례한 법정형의 규정 및 형사소송법 상 특수한 수사방법 도입을 통해 일반인들의 범죄인식 강화를 통한 심리적 강제가 필요하다.[25] 범죄에 해당하는 딥페이크는 언제라도 금지되어야 한다. 그러나 그 이외의 딥페이크는 자유롭게 사용하도록 하여 기술의 순기능을 활용하고 표현의 자유를 보장하도록 조화롭게 운용되어야 한다.[26] 그러나 이때에도 생성자와 유포자가 딥페이크 저작물임을 표시하도록 강제할 필요가 있다. 기존의 딥페이크 저작물 표시를 제거하는 것 역시 금지하여야 한다. 이미 텍스트를 생성하는 유형의 생성형 인공지능을 이용하는 경우 이를 밝히는 내용의 적절한 인용방식이 필요하다는 가이드라인이 국내·외 학계에서 제시되고 있는 상황이다. 딥페이크 생성물인 미디어가 텍스트보다 더 큰 파급효과를 미친다는 점을 고려할 때, 딥페이크 생성물은 딥페이크 기술을 통해 만들어진 것이라는 점 및 실재하지 않는 '허위'의 것이라는 점을 미디어 자체 내에서 명백하게 명시할 필요가 있다. 딥페이크 생성물 이용자 및 온라인 서비스 제공자에게 표시강제의무를 부과하고 표시강제의무 위반시 징벌적 손해배상제도를 도입하든지 딥페이크 생성물을 온라인상에 게시하는 사람이 인공지능 생성 콘텐츠 또는 합성 컨텐츠임을 스스로 라벨링하여야 한다. 또한 사전고지제도를

통해 개별적으로 민사법적 책임을 지거나 형사법적으로 범죄에 해당할 수 있음을 입법화할 필요가 있다. 이를 통해 디지털범죄에 대한 사회적 위험성을 이용자들에게 정보를 제공하고 일반예방효과 및 규범 내면화에 기여할 수 있다. 딥페이크 생성 프로그램 사용의 유의점에 대한 가이드라인을 제공하고 딥페이크 탐지기능 강화 및 딥페이크 영상 표시의무 등 일반예방효과로써 형사처벌 가능성을 주의시킬 필요가 있다.[25]

3. Education policy countermeasures

새로운 기술은 우리에게 새로운 가능성을 제시한다. 인공지능과 이를 기반으로 한 딥페이크 기술도 마찬가지다. 그러나 이러한 기술 자체에는 도덕과 양심이 없다. 그래서 이 기술을 활용하는 인간이 양심을 따라 행동해야 한다.[26] 기술에 수많은 문제가 존재한다면 법으로 강력하게 규제하면 된다고 말하지만, 미란다 원칙을 만들었던 미국 연방대법관 얼 워런의 말을 상기할 필요가 있다. “윤리는 바다(sea)이고, 법은 이 바다 위를 떠다니는 배(ship)다. 바닷물이 많을수록 배는 잘 떠다닌다. 바다라는 윤리가 성숙하지 않은 상태에서 무작정 법을 들이밀면 당연히 무리가 발생하고 구성원 간에 갈등이 심해진다. 그리고 신기술은 잠재된 유용성을 펼치기도 전에 이내 사회에서 사라질 수 있다. 그래서 예를 들면 선거에 있어서 딥페이크 악용을 막기 위한 최초의 수단이 법이 되면 안 된다. 딥페이크가 왜 선거에 악영향을 주며, 유권자로서의 권리를 어떻게 왜곡하는지를 유권자인 시민들이 충분히 깨닫고 공감하는 윤리의식 성숙이 먼저 필요하다. 새로운 기술이 나올 때마다 이에 따른 윤리 의식과 시민역량을 비례되도록 하여 문화지체현상이 발생하지 않도록 하는 노력이 요구된다. 인공지능 윤리 강화의 방법론으로 가이드라인은 법적구속력을 없으므로 실정법에 도입하는 것도 고려할 수 있다. 즉,법률 측면에서 인공지능 윤리원칙 등을 제시하는 기본법이 부재하므로 이에 대한 입법이 필요하다. 그러므로 첫째, 인공지능 윤리에 관한 포괄적인 기본법 제정이 요구된다. 둘째, 서비스 업체 및 제작자들의 평가 및 인증 제도의 확립을 통해 인센티브 지원이 필요하다. 셋째, 기업의자율적인 인공지능 윤리 확립을 위해 가이드라인을 마련하고, 새롭게 부각되는 디지털범죄에 적극 대응해야 한다.

V. Conclusions

인공지능을 통한 기술의 발전은 뉴미디어 발전에 이바지하는 등 우리에게 많은 긍정적인 변화를 가져다 준다. 최근 독일 온라인 플랫폼 마이헤리티지는 18세의 나이로 ‘대한 독립만세’를 외치다 순국한 유관순 열사와 도시락 폭탄 의거를 앞두고 촬영한 사진 속 윤봉길 의사를 딥페이크 기술을 통해 생생한 영상으로 되살려 큰 화제를 불러왔다. 범인 몽타주에 딥페이크 활용 및 이미 사망한 사람의 얼굴을 재현해 고인을 잊지 못하는 가족들을 위로하고, 과거의 추억을 소환해 새로운 감동을 만드는 등 선한 취지로만 사용된다면 긍정적인 부분이 많은 기술이다. 하지만 기술의 진보가 언제나 우리에게 장점만 가지고 오는 것은 아니다. 딥페이크 기술을 이용하여 유명인의 얼굴을 음란물에 합성 및 배포하고, 허위사실을 유포하고 협박하는 등 범죄에 악용하는 사례가 지속해서 발생하고 있다. 전문가들은 딥페이크가 위 사례처럼 범죄에 악용될 경우, 진위여부를 구별하는 데에 문제가 되고, 나비효과로 인해 사회적 혼란으로 이어질 것이라고 경고한다. 이런 악용 사례가 지속해서 증가한다면 진보된 기술은 오히려 우리에게 큰 혼란을 일으키는 양날의 검이 될 것이다. 딥페이크 기술이 일반인들에게 보급되어 사용된 지 얼마 되지 않은 시점에 이러한 문제점이 지적된다는 것은 딥페이크 기술의 발전에 따라 더 많은 문제점이 발생할 것이라는 점을 시사한다. 최근 정부는 AI 강국 실현과 디지털 뉴딜 성과를 위해 법· 제도 정비를 세계 각국과 발맞춰 추진하고 있다. 이러한 법·제도의 정비를 비롯하여 인공지능 기술이 인류 사회에 올바르게 사용될 수 있도록 다방면의 노력이 지속해서 필요하다.

ACKNOWLEDGEMENT

This paper was supported by Research Funds of Kwangju Women's University in 2024(KWU24-005)

REFERENCES

[1] A. A. Maksutov, V.O. Morozov, A.A. Lavrenov, and A. S. Smirnov, “Methods of deepfake detection based on machine learning,” In 2020 IEEE conference of russian young researchers in electrical and electronic engineering (EIConRus) pp. 408-411, March 2020.

[2] M. H. Maras,. “Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos”, The International Journal of Evidence & Proof, Vol. 3, No. 3, pp. 255-262, October 2019.

www.kci.go.kr

[3] S. W. Kang. The singer who was restored to AI. How did it become realistic? [Internet]. Available: https://www.sedaily.com/NewsVIew/22HDOPL0Z9.

[4] H. G. Shin. Beckham speaks nine languages? Deepfakechanges the shape of your mouth [Internet]. Available: https://www.mk.co.kr/news/it/view/2020/12/1339733/.

[5] S. H. Lee, Big data analysis for Deepfake: The war against fakes, Software Policy & Research Institue, Seongnam: Gyeonggi, SPRI Report IS-090, 2020.

[6] T. D. Fikse, Imaging Deceptive Deepfakes An ethnographic exploration of fake videos, Masters thesis, University of Oslo, Oslo, Norway, October 2018.

[7] J. Wakefield. Deepfake presidents used in Russia-Ukraine war Internet]. Available: bbc.com/news/technology-60780142

[8] T. J. Pinch, & W. E. Bijker, “The social construction of facts and artefacts: Vol. 14, No. 3, pp. 399-441, August 1984.

[9] D. G. Douglas, The Social Construction of Technological Systems, anniversary edition: New Directions in the Sociology and History of Technology. MIT press, 2012.

[10] J. Park & Y. H. Cho, “Technology Trends Related to Deepfake Video Detection”, Korea Software Congress 2019, Pyeongchang, pp.724-726, December 2019.

[11] L. Guarnera, O. Giudice & S. Battiato, “Deepfake detection by analyzing convolutional trace”, Conference on Computer ision and Pattern Recognition Workshops, pp. 666-667, 2020.

[12] T. Karras, S. Laine, M. Aittala, J. Hellsten,, J. Lehtinen &, T. Aila, “Analyzing and improving the image quality of stylegan”, Conference on Computer Vision and Pattern Recognition, pp. 8110-8119, 2020

[13] H. N. Lee. The world must actively discuss AI ethics and deepfake technology [Internet]. Available: http://www.aitimes.com/news/articleView.html?idxno=140468

[14] M. J. Kim. AI Music Project, once again, "Using the voice of the late Turtle Man, let's see the entire turtle performance [Internet]. Available: https://www.gukjenews.com/news/articleView.html?idxno=2123459

[15] H. J. Lee. Face editing skills to revive a dead singer...Change the Drama Production Environment with AI [Internet].Available: https://magazine.hankyung.com/business/article/202103049965b

[16] CJ OLIVENETWORKS AI lab. AI and contents [STEP 1] AI BM, planning [Internet]. Available: https://youtu.be/_2vLNMsPfyw

[17] S. Li. How Hollywood Became Obsessed With De-aging Its Stars [Internet].

[18] K. Howard. Avengers: Endgame Deepfake Casts Nicolas Cage as Captain America. <DEN OF GEEK> [Internet]. Available: https://www.denofgeek.com/movies/avengers-endgame-deepfake-nicolas-cage-captain-america/

[19] Alanazi, S., Asif, S., & Moulitsas, I, “Examining the societal impact and legislative requirements of deepfake technology: a comprehensive study”, 14(4) Int. J. Social. Scienc. Humanit., 58 (2024).

[20] Delfino, “Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act”, 88 Fordham L. Rev. 887 (2019).

[21] EPRS(European ParliamentaryResearch Service), Tackling Deepfakes in European Policy, Parl. Eur. Doc. No. PE 690.039 (2021).

[22] Kumkar, L. & Rapp, J., “Deepfakes”, ZfDR 2022, 199, 202.

[23] Shirish, A. & Komal, S., “A Socio-legal enquiry on deepfakes”, 54(2) Cal. W. Int'l L.J. 1 (2024).

[24] Thiel, M., “„Deepfakes“ – Sehen heißt glauben? Gefahren, gesetzgeberischer Handlungsbedarf, Konsequenzen für die biometrische Gesichtserkennung”, ZRP 2021, 202.

[25] Vasist, P. & Krishnan, S., “Deepfakes: An Integrative Review of the Literature and an Agenda for Future Research”, 51 CAIS, 590, 593 (2022)

[26] Wittmer, S. & Steinebach, M., “Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet”, MMR 2019, 650, 653.

[27] Kllee, Jwkim, "A study on the technical and criminal countermeasures for deep fake pornography crime," 4th Industrial Revolution Law and Policy Vol.2 , pp160-162

Authors



Kwang-Hyun Park received the M.S. and Ph.D. degrees in Law from Chonnam National University, Korea, in 2008 and 2011, respectively. Dr. Park is currently a professor of criminal law at Kwangju Women's University. He is interested in criminal law as well as criminal psychology and intellectual property rights.

www.kci.go.kr