발간등록번호 31-9735044-001340-14

일 잘하는 실력 국회

국회입법조사처
NATIONAL ASSEMBLY RESEARCH SERVICE

이슈와 논점

국회입법조사처

이슈와 논점 ▌제1619호 ▌2019년 10월 15일 ▌발행처 국회입법조사처 ▌발행인 김하중 ▌www.nars.go.kr

딥페이크(Deepfake)의 발전과 해외 법제도 대응

김 유 향*

1. 들어가며

인공지능(AI) 기술의 진전에 힘입어 진짜같은 합성사진이나 가짜뉴스를 넘어 이제 딥페이크(deepfake) 영상이 새로운 사회문제로 떠오르고 있다. 딥페이크는 AI 기반의 인간이미지 합성기술로서 첨단 영화제작에 활용되는 등 산업 차원의 잠재력도 매우 큰 기술로 주목받고 있다.

그러나 최근 낸시 팰로시(Nancy Pelosi) 미 하원의장과 마크 저커버거(Mark Zuckerberg) 페이스북 최고경영자의 딥페이크 영상이 유포되면서 딥페이크가 가짜뉴스의 위협을 더욱 증가시킬 수 있음에 우려가 커지고 있다.

특히 미국은 2018년 중간선거 전부터 딥페이크의 정치적 영향에 대해 주목하였으며, 2020년 대선을 앞두고 대응방안 마련에 대한 요구도 확대되고 있다. 허위조작정보가 선거 및 정치에 미치는 영향을 막기 위해 노력하고 있는 유럽의 경우도 마찬가지이다. 아직 딥페이크에 대해 크게 주목하지 않고 있지만, 우리도 내년 총선을 앞두고 있고, 연예인과 일반인여성의 불법영상합성 등이 문제가 되고 있어 그 대응방안을 고민해야할 시점이다.

이 글에서는 딥페이크 기술의 최신 발전 동향 및 이를 둘러싼 쟁점, 그리고 해외의 법제도적 대응에 대해 분석하고 국내에의 시사점을 모색하고자 한다.

2. 딥페이크의 개념 및 기술동향

(1) 개념

딥페이크란 허위의 동영상 콘텐츠를 만들거나 변형하는데 사용되는 AI기반 기술, 또는 진짜처럼 보이는 가짜 동영상 등을 의미한다.[1] 즉 AI기술과 안면 매핑(facial mapping) 또는 안면 스와핑(face - swapping)기술을 이용해 만든 가짜 영상으로 특정 인물의 얼굴과 신체 부위를 전혀 다른 영상과 합성해 새로운 영상을 만들어 낸다. 신경망을 사용하는 딥러닝(심층 학습)의 '딥(Deep)'과 가짜라는 의미의 '페이크(Fake)'를 합친 신조어이다.[2]

(2) 기술동향

딥페이크는 AI기술 중 하나인 '생성적 적대 신경망(Generative Adversarial Networks)' 기술을

1) Tom Taulli, "Deepfake: What You Need To Know", *Forbes*, Jun 15, 2019.

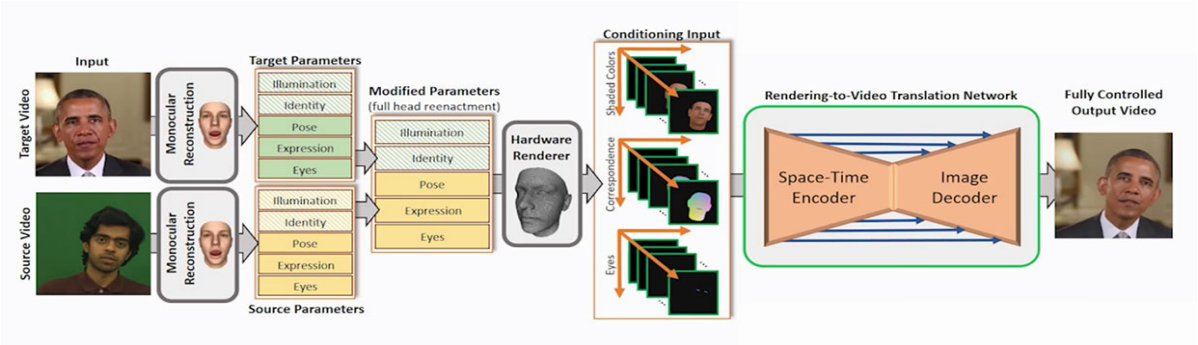
2) 용어는 2017년 12월 포르노비디오의 등장인물들을 유명인의 얼굴로 바꾼 합성 영상물을 처음으로 유통시킨 Reddit 이용자, '딥페이커즈(deepfakes)'에서 비롯된 것이다.

* 사회문화조사실 과학방송통신팀 팀장, 788-4710, ykim@assembly.go.kr

이용하며, 이 기술은 이미지의 진위 여부를 판단하는 '감별자' 알고리즘과 이미지를 만들어 내는 '생성자' 역할을 하는 알고리즘으로 구성되며, 두 알고리즘이 서로 대립하는 과정을 통해 원본과의 오차를 줄여, 진위를 판단하기 어려운 콘텐츠를 생성한다.

고 소셜미디어와 인터넷 상의 사진들이 딥페이크에 이용되지 못하도록 하는 기술들이 대표적이다.[4] 미국, EU 등 외국에서는 이와 같은 딥페이크 식별기술이 다양하게 발전하고 있다.

[그림 1] 딥페이크 영상 제작 과정



자료: https://arxiv.org/pdf/1805.11714.pdf

기존의 딥페이크 기술은 여러 장의 사진과 음성 데이터를 딥러닝 알고리즘으로 학습해 동영상을 만들어내기에 대상 인물의 사진이 대량으로 필요했다. 그러나 최근에는 단 1장의 얼굴 이미지 사진을 '말하는 얼굴 동영상(talking head videos)'으로 손쉽게 변환할 수 있는 새로운 기술까지 등장하였다.[3]

이처럼 딥페이크 기술이 급격히 발전하면서 딥페이크를 통한 허위조작 영상의 위험성도 그만큼 커지고 있다.

딥페이크는 진위 여부를 가려내기 어렵기 에 피해를 막기 위한 가장 최선의 대응은 또 다른 AI기반 딥페이크 식별기술의 발전이다. 즉 딥페이크를 만드는 과정에 이미지에 남긴 디지털 아티팩트(Artifact), 운영체제나 앱을 사용하면서 생성되는 흔적을 통해 식별하는 방법, 그리

3. 주요 딥페이크 사례와 영향

최근 다양한 딥페이크 영상이 등장하고 있지만, 아직은 유명인들을 통해 주목을 끌기 위한 목적의 영상들이 많다. 저커버거가 자신은 세상을 손에 넣었다고 거만하게 말하는 영상이나, 낸시 펠로시 하원의장이 혀가 꼬여 말이 잘 안 나오는 상태에 있는 듯한 동영상 등은 대표적으로 사람들의 관심을 끌기위해 제작되고, 유포된 것들이다.[5]

그러나 딥페이크가 정치적 공격의 도구로 실제 사용된 사례도 있다. 인도에서는 2018년 4월 현 모디 정권을 지속적으로 비판해온 여성 언론인, 라나 아윱(Rana Ayyub)의 얼굴을 포르노 동영상에 합성한 딥페이크가 유포되었는데, 정

3) "'사진 한 장으로 인터뷰 동영상 제작'…삼성, AI 신기술 개발", 연합뉴스, 2019. 5. 24.

4) 미국 국방부 방위고등연구계획국(DARPA)는 딥페이크 동영상 식별기술에서부터 동영상 확산 전 소셜미디어상에서 유포를 보류하는 방법, 워터마크 등 다양한 딥페이크 식별기술의 개발을 지원하고 있다.

5) "Politics WatchDog"이라고 Facebook 페이지가 5월 22일 게시한 동영상이다.

권 지지자들이 딥페이크를 활용해 정권의 비판자를 공격한 것이다.

또한 멕시코에서는 2018년 대통령 선거 캠페인 후반에 딥페이크 음성메시지가 크게 문제가 되었다. 메시지는 "대통령 후보인 안드레스 마누엘 로페스 오브라도르(Andrés Manuel López Obrador)의 캠페인 종료식인 AMLOFest 참가자들이 후보 캠프에서 받은 선불카드로 TV를 구입하려 가게 앞에 모여 있다"는 4분가량의 가짜음성이었다.

딥페이크의 부정적 파괴력은 아직 충분히 드러나지 않았다. 그러나 정치·경제·외교안보 등 다양한 분야에 큰 영향을 미칠 수 있다.

먼저 정치면에서, 딥페이크는 허위조작 정보와 결합하여 각국의 선거에 심대한 영향을 미칠 수 있다. 즉 대선 투개표 전날 후보자에게 불리한 허위조작 영상이 유포될 경우 이를 바로잡을 충분한 시간을 확보하지 못한 상태에서 돌이킬 수 없는 결과를 야기할 수 있다.

외교안보 측면에서는, 국가 간 정보전의 도구로서 활용될 수 있다. 실제로 미국과 유럽 국가들은 러시아와 중국이 딥페이크를 정보전에 이용하고 있음에 크게 우려하고 있다.

또한 경제면에서는, 기업의 신규 주식공개(IPO) 직전에 경영자의 범죄행위 관련 허위동영상이 확산되거나 주식이나 경제관련 허위정보를 결합한 영상들이 배포된다면 경제에 큰 타격을 줄 수 있다.

4. 해외의 법제도적 대응

(1) 미국

미국은 표현의 자유보호를 위해 콘텐츠에 대한 규제는 최소한으로 하지만, 딥페이크의 피해자는 프라이버시 보호 및 명예훼손의 차원에서 법적으로 보호받을 수 있다. 또한 주정부 차원에서는 「사이버스토킹법」 등에 근거해 제작자를 처벌할 수도 있다.[6]

미국은 딥페이크에 대해 기술적 해결책을 우선하지만, 입법 움직임이 없는 가짜뉴스와 달리 적극적 입법 시도가 진행되고 있다.[7]

올해 6월에는 상원 7인과 하원 4인이 「Deepfakes Report Act of 2019」를 제출하였다.[8] 법안은 국토안보부가 법안 발효 후 200일 이내 그리고 그 이후 18개월마다 딥페이크 기술의 상태와 활용현황을 평가하는 심층조사와 보고서 발표, 그리고 공청회를 개최할 것을 주요 내용으로 하고 있다. 같은 달 이벳 클락(Yvette Clarke) 하원의원(민주당)은 딥페이크의 발신에 레이블(label)을 의무화하는 규제 법안인 「Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019」(H.R.3230)을 발의하였다.[9]

또한 주정부 차원에서는 뉴욕 주 의회에 2018년 5월, 개인정보보호 등의 관점에서 딥페이크를 규제하는 법안인 「Act to Amend the Civil Rights Law」가 제출된 상태이다.[10]

그 외 딥페이크에 대한 미 의회의 관심을 잘 보여주는 것이 2019년 6월 13일 하원 정보특별

---

6) The Michigan Penal Code (Excerpt)Act 328 of 1931

7) 비록 정부기관 폐쇄로 폐지되었지만 2018년 12월에 이미 딥페이크 규제 법안인 「Malicious Deep Fake Prohibition Act of 2018」가 제출된 바 있다.

8) Mark Tapscott, "Senators Want DHS to Study Deepfake Videos", *The Epoch Times*, July 1, 2019

9) 〈https://www.congress.gov/bill/116th-congress/house-bill/3230〉

10) 뉴욕주 의회〈https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Summary=Y&Text=Y〉

위원회가 개최한 공청회 "AI, 허위미디어, 딥페이크의 국가안전보장상의 과제"이다. 공청회는 2020년 대선에서 러시아 등의 딥페이크를 이용한 개입시도에 대비하기 위한 것으로서 기술적 대처 이외에 법·정책적 대응에 대한 논의도 다양하게 진행되었다.

특히 위조 콘텐츠의 생성, 배포 자체를 금지하는 법률 제정에 대한 요구와 더불어 현재 플랫폼 기업의 포괄적인 면책을 정한 「통신품위법」 제230조[11]의 범위가 너무 광범위하여 딥페이크의 범람을 적절히 통제하고 있지 못하다는 지적도 제기되었다. 딥페이크에 대비하여 플랫폼 기업에 대한 무조건적 면책이 아니라 '적절한 대처'를 면책 조건으로 하는 법개정이 필요하다는 주장은 이 맥락에서 제기된 것이기에 향후 주목할 부분이다.

미국은 딥페이크 기술이 시장혁신을 가져올 수 있으므로 딥페이크 전체를 악으로 보기는 힘들다는 기술경제적 차원의 지적과 언론의 자유 보호 관점에서 규제에 신중한 의견들이 지배적이지만, 한편으로 국가안보차원의 문제로 인식하고 적극 대응을 모색하고 있다.

(2) EU

EU는 허위정보에 대해 적극적 입법으로 대응하고 있으므로, 딥페이크는 허위정보 관련법에 의해 규제된다. 유럽에서 딥페이크 피해자는 「개인정보보호규정(GDPR)」 제17조 '잊힐 권리(삭제할 권리, right to erasure)'에 따라 삭제를 요청할 권리가 있으며, 데이터 처리에 이의를 제기(제21조)할 수 있다. EU는 2018년 딥페이크를 비롯한 허위정보 전반에 대응하기 위한 전략 「Communication-Tackling online disinformation: a European Approach」를 발표하고, 모든 형태의 허위정보식별을 위해 정보의 출처 및 신뢰성 여부를 쉽게 알 수 있도록 조치하게 하였다.[12] 2019년에는 허위정보에 대한 대응을 보다 발전시킨 보고서, 'Report on the Implementation of the Action Plan Against Disinformation'을 발표하였다.[13] 개별국가의 경우 독일은 「네트워크법집행법(NetzDG)」, 프랑스는 「정보조작대처법」에 따라 처리될 수 있다.

5. 맺음말

딥페이크의 가장 큰 위험은 일반국민은 물론 정부도 무엇이 진짜 또는 가짜인지를 식별할 수 없는 상황이 될 수도 있다는 것이다. 우리국회에서도 약 20여건의 허위정보에 대한 법안이 제출되어 있지만, 딥페이크에 대한 대응은 부재한 상태이다.

딥페이크는 산업적 잠재력이 큰 기술이지만 기존의 허위정보와는 차원이 다른 위험성을 내포하고 있으므로 입법적 검토와 더불어 정부차원에서도 기업과 연계하여 콘텐츠의 서명기능 개발, 변경내용 표시, 사용자 활용 허위동영상 판정도구 배포 등 기술적·정책적 노력도 이루어져야 할 것이다.

❑ 「이슈와 논점」은 국회의원의 입법활동을 지원하기 위해 최신 국내외 동향 및 현안에 대해 수시로 발간하는 정보 소식지입니다.

11) 47 U.S. Code § 230. Protection for private blocking and screening of offensive material.

12) 〈https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach〉

13) 〈https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf〉