딥보이스와 선거 : AI 음성 합성 기술이 민주주의에 던지는 질문

오세욱 선문대학교 미디어커뮤니케이션학부 교수

1. 들어가며: '딥페이크'보다 우려되는 '딥보이스'

지난 2018년 4월 미국의 온라인 매체 버즈피드(BuzzFeed)가 유튜브에 게재한 한 영상[1]이 많은 사람들을 놀라게 했다. 해당 영상 내용이 버락 오바마 전 미국 대통령이 도널드 트럼프 현 미국 대통령에게 욕하는 것이었기 때문이다. 이 영상 속에서 오바마 전 대통령은 "트럼프 대통령은 진짜 머저리(dipshit)입니다"라고 말했는데, 이는 버즈피드가 딥페이크(DeepFake) 기술의 위험성에 대해 경

1) BuzzFeedVideo. (2018, 4, 17). You Won't Believe What Obama Says In This Video! [Video]. Youtube. https://www.youtube.com/watch?v=cQ54GDm1eL0

고하기 위해 영화감독 조던 필(Jordan Peele)과 함께 만든 조작 영상이었다. 이 영상은 교묘하게 조작돼 일반인들이 봤을 때 조작 여부의 판단이 어려웠기 때문에 버즈피드가 이 사실을 공개하지 않았다면 큰 파장을 불러올 수 있었다. 딥페이크 기술은 인공지능의 바탕이 되는 기계학습(machine learning) 기법인 딥러닝(deep learning)을 사용해 원본 이미지나 동영상 위에 다른 이미지를 중첩(superimpose)하거나 결합(combine)해서 원본과는 다른 이미지와 영상을 만들어 주는 이미지 및 동영상 조작(manipulation) 기술을 말한다.[2] 딥페이크는 사람의 특별한 지시가 없어도 자동으로 최적의 결과물을 산출할 수 있는 기계학습이 적용돼 식별이 굉장히 어려운 허위정보 생성 기술로 활용될 수 있으며, 미디어를 통해 전달되는 것이 실재와는 동떨어진 것일 수 있다는 인식을 심어줄 수 있다. 게다가 최근 생성형 AI 기술의 발전으로 이러한 딥페이크 영상은 기술 전문가가 아니더라도 비교적 쉽게 만들어낼 수 있게 됐다.

이에 따라 선거 국면에서 딥페이크가 실제로 활용된 사례들도 국내외를 막론하고 빈번하게 나타나고 있다. 우리나라에서는 지난 2022년 제20대 대통령 선거 당시, 후보자의 외형과 목소리를 그대로 복제한 'AI 윤석열'[3]이 등장해 화제를 모으기도 했다. 당시에는 후보자가 직접 허락한 '공식 캠페인 도구'로서 긍정적인 기술 활용 사례로 평가받기도 했으나, 동시에 "만약 반대 진영에서 악의적인 내용을 담아 유포했다면 어떻게 대응했을 것인가"라는 질문을 우리 사회에 남겼다. 이러한 상황을 감안하여 지난 2023년 말, 우리나라 국회는 인공지능 기술을 악용한 선거 조작의 위험성을 선제적으로 차단하기 위해 「공직선거법」 제82조의8[4]을 신설하였다. 해당 조항은 선거일 전 90일부터 인공지능 기술로 만든 실제와 구분하기 어려운 가상의 음향, 이미지, 영상을 선거운동에 사용하는 것을 엄격히 제한하고 있다.

이 신설 조항에서 주목해 볼 부분은 '음향'이다. 법 조문에 명시된 '음향'이라는

---

2) 최순욱·오세욱·이소은. (2019). 딥페이크의 이미지 조작: 심층적 자동화에 따른 사실의 위기와 푼크툼의 생성. 미디어, 젠더 & 문화, 34(3), 339–380.

3) 국민의힘TV. (2022. 1. 13). [AI 윤석열] 더 나은 변화? ㅇ? [동영상]. Youtube. https://www.youtube.com/watch?v=c9HGMqUvIJA

4) **제82조의8(딥페이크영상등을 이용한 선거운동)** ① 누구든지 선거일 전 90일부터 선거일까지 선거운동을 위하여 인공지능 기술 등을 이용하여 만든 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상 등(이하 "딥페이크영상등"이라 한다)을 제작·편집·유포·상영 또는 게시하는 행위를 하여서는 아니 된다.
② 누구든지 제1항의 기간이 아닌 때에 선거운동을 위하여 딥페이크영상등을 제작·편집·유포·상영 또는 게시하는 경우에는 해당 정보가 인공지능 기술 등을 이용하여 만든 가상의 정보라는 사실을 명확하게 인식할 수 있도록 중앙선거관리위원회규칙으로 정하는 바에 따라 해당 사항을 딥페이크영상등에 표시하여야 한다.

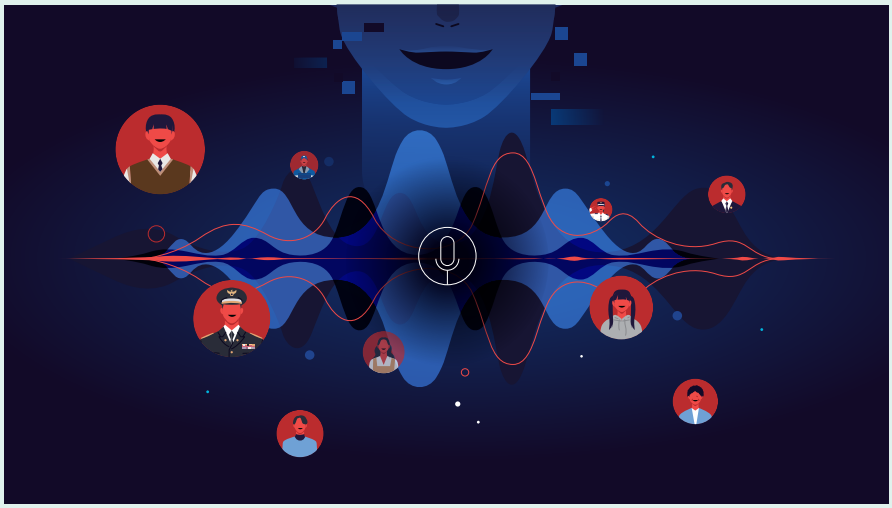
규제 대상은, 그동안 '영상' 조작에 쏠린 관심으로 인해 비교적 덜 주목받았다. 언론과 규제 당국이 딥페이크 영상의 시각적 부자연스러움을 식별하는 데 집중하는 사이, 인공지능 음성 합성 기술, 즉 '딥보이스(Deep Voice)'는 선거의 공정성을 위협할 수 있는 또 하나의 축으로 조용히 성장해 왔다.[5] 딥보이스가 딥페이크 영상보다 선거 국면에서 오히려 더 큰 위협이 될 수 있는 이유는, 역설적으로 그 기술적 단순함에 있다. 영상 조작물은 고도의 그래픽 처리와 방대한 연산 자원을 필요로 하며, 시각 데이터의 특성상 기술적 결함이 노출될 가능성이 상대적으로 높다. 반면 딥보이스는 수 초 분량의 음성 샘플만으로도 특정 인물의 음색, 억양, 호흡 패턴을 정밀하게 재현할 수 있다. 이러한 낮은 기술적 진입장벽은 악의적 의도를 가진 개인이나 조직이 조작 음성을 대량으로 생산·유포할 수 있는 환경을 조성한다.

선거가 진행될 때 '음성'이 갖는 의미는 시각 정보와는 또 다르다. 지난 우리나라의 선거 사례들을 돌이켜보면, 선거의 향방에 결정적 영향을 미친 사건들은 정교하게 편집된 영상보다 녹취록이나 통화 내용 공개와 같은 음성 기반 정보인 경우가 적지 않았다. 유권자들은 공식 연설보다 사적 맥락에서 유출된 것으로 보이는 음성 자료에 더 높은 진정성을 부여하는 경향이 있으며, 이는 딥보이스 기술이 유권자의 확증 편향을 자극하고 여론 형성 과정을 왜곡할 수 있는 구조적 조건이 된다. 2026년 6·3 지방선거를 앞둔 현시점에서 이러한 우려는 더욱 커진다. 지방선거는 후보자 수가 많고, 카카오톡이나 텔레그램 등 지역 기반의 폐쇄적 커뮤니티를 통해 정보가 유통되는 특성이 있어, 공적 감시망이 미치지 못하는 경로로 조작 음성이 확산될 가능성이 상대적으로 높기 때문이다.

2. 딥보이스 기술의 현황과 선거에서의 위험성

인공지능 기반 음성 합성 기술은 인공지능 기술의 발전에 따라 자연스럽게 발전하고 있다. 초기 TTS(Text-to-Speech) 기술이 기계적 낭독 수준에 머물렀다면, 최근의 생성형 AI 모델은 특정 인물의 음색, 억양, 호흡 패턴까지 정밀하게 재현하는 단계에 도달했다. 마이크로소프트의 연구팀이 개발한 'VALL-E'는 기존 학습 과정에서 접하지 못한 발화자의 3초 분량 녹음만으로도 고품질의 개인

5) Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753-1820.



화된 음성을 합성해낼 수 있다.[6] 'GLM-TTS'[7]와 같은 오픈소스 모델은 3~10초의 참조 음성만으로 파인튜닝(Fine-tuning) 없이 임의의 음성을 복제할 수 있는 기능을 제공한다. 원래 음악 창작을 위해 개발된 'SVC(So-VITS-SVC)'[8] 기술 역시 특정인의 음성 데이터를 학습시킨 뒤 제3자의 발화에 해당 음색을 입히는 방식으로 작동하면서도 원본의 음높이와 억양을 보존한다. 이 역시 오픈소스 모델로 개발되어 누구나 활용이 가능하다. 이러한 기술들은 감정이 섞인 떨림이나 격앙된 어조까지 구현할 수 있어, 단순한 텍스트 낭독과는 질적으로 구별된다. 과거 대규모 자본과 인력이 투입되어야 가능했던 음성 위조가 이제는 개인용 PC 한 대와 공개된 유튜브 영상 속 후보자의 짧은 발언만으로도 실행 가능한 시대가 된 것이다.

딥보이스가 딥페이크 영상보다 더 큰 위험성을 지니는 또 다른 이유는 유통 경로의 은밀성과 탐지의 기술적 난이도에 있다. 영상 조작물의 경우 시각적 부자연스러움을 포착하기 위한 탐지 도구가 비교적 활발히 개발되어 왔다.[9] 반면 딥보이스 탐지는 현재까지도 상당한 기술적 한계에 직면해 있다. 노스웨스턴대학교의 '노스웨스턴 보안 및 AI 연구소(Northwestern Security & AI Lab)' 소장인 서

6) Wang, C. et al. (2023). Neural codec language models are zero-shot text to speech synthesizers (arXiv:2301.02111). arXiv. https://doi.org/10.48550/arXiv.2301.02111

7) https://github.com/zai-org/GLM-TTS

8) https://github.com/svc-develop-team/so-vits-svc

9) SOCRadar. (2025, October 21). Top 10 AI deepfake detection tools to combat digital deception in 2025. https://socradar.io/blog/top-10-ai-deepfake-detection-tools-2025/

브라마니안(V.S. Subrahmanian) 교수는 독자적인 AI 음성 탐지 실험을 수행했다. 서브라마니안 교수의 연구팀은 시중에서 판매되거나 무료로 공개된 14종의 오디오 딥페이크 탐지 도구를 검증했다. 그는 테스트 결과가 매우 실망스러운 수준(discouraging)이었다고 밝혔다. 서브라마니안 교수는 "현재로서는 오디오 딥페이크 탐지기를 신뢰할 수 없으며, 실제 사용을 권장할 만한 도구도 없다"고 포인터(Poynter)와의 인터뷰에서 밝힌 바 있다.[10)]

음성 데이터는 영상에 비해 파일 용량이 작고 압축률이 높아 유통이 용이하다는 구조적 특성도 갖는다. 특히 2026년 지방선거와 같은 다층적 선거 국면에서는 공식 캠페인 채널보다 폐쇄형 SNS나 숏폼 플랫폼을 통한 유포가 주된 경로가 될 것으로 예상된다. 유튜브 쇼츠, 틱톡, 인스타그램 릴스 등 1분 내외의 짧은 콘텐츠는 정보의 맥락보다 강렬한 한 마디에 수용자의 주의를 집중시키며, 이러한 환경에서 후보자의 목소리로 생성된 짧은 발언은 사실 확인이 이루어지기 전에 확산될 수 있다. 더욱 주목해야 할 유통 경로는 카카오톡이나 텔레그램 같은 폐쇄형 메신저이다. 지인 간 공유를 통해 전달되는 파일 형태의 '녹취록'은 공적 언론 보도와는 다른 차원의 사적 신뢰를 기반으로 유통된다. 이러한 음성 파일은 검색 엔진의 수집 대상이 아니며, 중앙선거관리위원회 등의 실시간 모니터링 체계가 미치기 어려운 영역이다. 한 번 유포된 음성은 디지털 공간의 사적 네트워크 속에 잠복하다가, 선거 직전 결정적 시점에 재확산되며 표심에 영향을 미칠 수 있다.

딥보이스가 선거 과정에서 발휘할 수 있는 가장 심각한 영향력은, 유권자의 심리적 취약점과 결합하는 방식에서 비롯된다. 정치적 맥락에서 '녹취'는 단순한 정보 전달을 넘어 '은폐된 진실'이라는 강력한 상징성을 갖는다. 유권자들은 공식 연설보다 사적 공간에서 유출된 것으로 보이는 음성 자료에 더 높은 진정성을 부여하는 경향이 있으며, 이러한 경향은 확증 편향과 결합할 때 증폭된다. 자신이 지지하지 않는 후보에 대한 부정적 선입견을 가진 유권자에게, 해당 후보의 목소리로 합성된 부정적 내용의 음성은 기존 신념을 확인해 주는 강력한 근거로 작용한다. 이 문제와 관련해 우려스러운 점은 심리학에서 말하는 '수면자 효과(sleeper effect)'[11)]다. '수면자 효과'는 신뢰도가 낮은 출처에서 전달된 메시지라

10) Mahadevan, A. (2024, March 21). AI detection tools for audio deepfakes fall short. How to spot them. Poynter Institute. https://www.poynter.org/fact-checking/2024/deepfake-detector-tool-artificial-intelligence-how-to-spot/

11) Hovland, C. I., Lumsdaine, A. A., & Sheffield, F. D. (1949). Experiments on Mass Communication. Princeton University Press.

하더라도 시간이 경과하면 출처에 대한 기억이 약화되면서 메시지의 설득력이 오히려 증가하는 현상을 의미한다. 이를 딥보이스의 맥락에 적용하면, 설령 선관위나 언론이 특정 음성이 AI로 합성된 위조물임을 밝히더라도, 이미 해당 음성을 접하고 감정적으로 반응한 유권자의 인식에는 부정적 잔상이 오랫동안 남을 수 있음을 의미한다.

결국 딥보이스의 위협은 단순한 기술적 조작의 차원을 넘어, 민주적 의사결정의 전제인 합리적 토론과 사실 기반 판단을 구조적으로 침식할 수 있다는 데 있다. 2026년 지방선거를 앞둔 시점에서 딥보이스를 딥페이크 영상 못지않은 시급한 위협으로 인식해야 하는 이유는, 그것이 우리 사회의 구조적 취약점인 정치적 불신의 심리와 폐쇄적·사적 네트워크를 동시에 관통하고 있기 때문이다.

3. 현행 규제 체계의 한계와 보완 방향

「공직선거법」 제82조의8에 법문상 '음향'이 포함되어 있으나, 이 조항의 약칭이 '딥페이크영상 등'으로 정의되어 있다는 사실은 입법 과정에서의 관심이 주로 영상 조작물에 집중되었음을 보여준다. 중앙선거관리위원회의 운용기준 역시 '딥페이크영상 등'이라는 용어를 사용하고 있어 규제 당국과 현장 단속 인력이 음성 단독 조작물을 영상의 부수적 요소로 취급하게 만들 가능성이 있다. 음성만을 단독으로 활용한 조작물, 즉 딥보이스는 법이 규정한 '실제와 구분하기 어려운' 상태에 대한 입증이 영상보다 기술적으로 더 어렵다. 앞서 언급했듯이 현재 공개된 음성 위조 탐지 도구들의 신뢰성이 충분하지 않은 상황에서, 음성 조작물의 진위 판별은 영상에 비해 훨씬 모호하다. 이는 다가오는 2026년 지방선거에서 음성 조작물이 법적 규제를 실질적으로 회피할 수 있는 통로가 될 수 있는 위험성을 시사한다.

해외 몇몇 나라에서는 이미 AI 음성 조작의 실질적 위협을 경험하고 구체적 대응에 나서고 있다. 가장 대표적인 사례는 2024년 1월 미국 뉴햄프셔주 대통령 프라이머리 직전에 발생한 'AI 로보콜(robocall)' 사건이다. 프라이머리를 이틀 앞둔 시점에서 유권자들에게 바이든 당시 미국 대통령의 목소리를 모방한 자동전화가 발송되었다. 이 음성은 바이든 특유의 표현인 "What a bunch of malarkey!(이건 완전히 헛소리야!)"로 시작하며, "여러분의 투표는 이번 화요일이 아니라 11월에 의미가 있습니다"라고 말해 민주당 유권자들의 프라이머리 투표를 만류하는 내용이었다. 해당 전화의 발신자 번호는 뉴햄프셔 민주당 전 의

장인 캐슬린 설리번의 개인 휴대전화 번호로 위장되어 있었으며, 설리번 본인은 이와 무관한 것으로 확인되었다. 바이든 대선캠프는 대통령이 이 전화를 녹음한 사실이 없음을 즉각 확인했고, 뉴햄프셔주 법무장관실은 이 음성이 인공적으로 생성된 것으로 판단된다며 수사에 착수했다. 법무장관실은 이 전화가 "뉴햄프셔의 대통령 프라이머리를 방해하고 유권자 투표를 억압하려는 불법적 시도로 보인다"고 밝혔다.[12] 이 사건은 AI 음성 복제 기술이 실제 선거 과정에서 유권자 억압의 도구로 활용된 최초의 주요 사례로 기록되었으며, 이후 미국 연방통신위원회(Federal Communications Commission, FCC)의 AI 로보콜 전면 금지 결정과 관련자에 대한 600만 달러 과징금 부과 및 형사 기소로 이어졌다. 미국은 특정 매체 형태에 국한하지 않고 '음성 사칭' 행위 자체를 직접 규제 대상으로 삼았다. 한편, 유럽연합(EU)의 「AI 규제법(AI Act)」은 위험도에 따른 차등 규제를 적용하며, 정치적 목적의 AI 생성물에 대해 투명성 의무와 출처 표시를 강제하는 접근법을 취하고 있다.[13] 한국의 「공직선거법」이 '금지 기간' 설정을 중심으로 규제하고 있다면, 유럽연합의 「AI 규제법」은 생성물의 출처를 투명하게 밝히는 '과정의 규제'에 비중을 두고 있다는 점에서 향후 우리나라 법제의 보완 방향에 참고할 만한 시사점을 제공한다.

12) Sherman, A. (2024, January 22). Fake Joe Biden robocall in New Hampshire tells Democrats not to vote in the primary election. PolitiFact. https://www.politifact.com/factchecks/2024/jan/22/robocaller/fake-joe-biden-robocall-in-new-hampshire-tells-dem/

13) European Parliament. (2024). Regulation (EU) 2024/1689 (AI Act).

우리나라 현행 심의 체계에는 AI 기술이 결합된 음성 조작물에 특화된 별도의 기준이 마련되어 있지 않다. 특히 언론이 제보받은 음성 파일을 보도할 때 준수해야 할 기술적 검증 절차가 부재한 상황에서 속보 경쟁 상황까지 더해지면서 조작 음성이 검증 없이 기정사실화될 위험이 존재한다. 플랫폼 차원의 대응 역시 충분하지 않다. 플랫폼 기업들이 자율 규제에 나서고는 있지만, 국내 선거에서 실질적 유통 경로가 되는 카카오톡, 텔레그램 등 폐쇄형 메신저에서의 음성 파일 유포에 대해서는 실효성 있는 대응 체계를 갖추기 어렵다. 국내 포털 역시 딥페이크 영상에 대해서는 필터링 기술을 강화하고 있으나, 단순 음성 파일 공유에 대해서는 실시간 검증 시스템을 갖추기가 현실적으로 어려운 실정이다.

속이는 기술의 발전 속도는 그것을 적발하는 기술의 발전 속도보다 항상 빠르다. 완벽한 방안은 없겠지만, 다가오는 2026년 지방선거의 원활한 진행을 위해 다음의 세 가지 방향에서 보완 방향을 생각해 볼 수 있을 듯하다.

첫째, 언론의 음성 보도 원칙이 재설계될 필요가 있다. 익명으로 제보된 후보자 음성 파일에 대해서는 전문 기관의 기술적 검증 결과를 보도에 병기하도록 가이드라인을 강화할 필요가 있다. 단순히 "진위가 확인되지 않았다"는 면피성 문구는 앞서 언급한 수면자 효과를 차단할 수 없다. 검증이 완료되기 전까지 보도를 유예하거나 조작 가능성에 대한 명시적 경고를 삽입하는 구체적 절차도 논의해 볼 필요가 있어 보인다.

둘째, 기술적 표준화가 법적 규제와 병행될 필요가 있다. 'C2PA(Coalition for Content Provenance and Authenticity)'[14] 표준은 콘텐츠 제작자가 디지털 자산에 출처 정보를 암호화 서명된 메타데이터 형태로 부착할 수 있도록 해, 디지털 워터마크와 결합하여 메타데이터가 제거되더라도 자산과 출처 정보 사이의 연결을 유지할 수 있게 한다.[15] 이러한 글로벌 표준을 참고하여, 선거운동용으로 제작되는 AI 음성 콘텐츠에 기계적으로 식별 가능한 오디오 워터마크 삽입을 의무화하는 방안을 검토할 필요가 있다. 이는 사후 탐지에 의존하는 것이 아니라 생성 단계에서부터 디지털 출처 정보를 기록하게 함으로써, 조작 주체의 추적 가능성을 높이고 무분별한 유포를 억제하는 예방적 접근이 될 수 있다.

셋째, 유권자의 디지털 리터러시 강화와 비판적 수용 태도의 확립이 무엇보다 중요하다. 법적 규제와 기술적 방어선이 아무리 정교해지더라도, '속이는 기술'의

14) https://c2pa.org/

15) 오세욱. (2025). '그럴 듯한 가짜' 속 '진짜'를 확인하기 위한 새로운 표준 'C2PA'. KPF 미디어브리프. 2025년 4호.

진화 속도를 완벽히 앞지르는 것은 불가능에 가깝기 때문이다. 결국 허위 정보의 최종 도달점인 유권자 스스로 '방화벽' 역할을 수행해야 한다. 유권자들은 자극적인 폭로성 음성 정보를 접했을 때, 그것이 자신의 정치적 신념과 일치하여 즉각적인 감정적 동요를 일으킬수록 더욱 냉정하게 출처를 의심해 보아야 한다. 특히 카카오톡, 텔레그램 등과 같은 폐쇄형 메신저를 통해 공유되는 '출처 불분명한 녹취 파일'은 딥보이스 조작의 주된 타깃이 된다는 점을 인지할 필요가 있다.

4. 나가며: 귀는 열어두되, 무조건 믿지는 말아야

지금까지 인공지능 음성 합성 기술, 즉 딥보이스가 선거 과정에서 초래할 수 있는 위험성을 살펴봤다. 그 과정에서 드러난 핵심적인 문제의식은, 우리 사회의 규제 역량과 대중의 경계심이 '눈에 보이는' 위협에 편중되어 있는 사이 '귀로 파고드는' 위협에 대해서는 크게 비중이 높지 않았다는 점이다. 딥보이스의 위협은 단순한 문제가 아니다. 기술적 측면에서 최신 음성 합성 기술은 3초 내외의 샘플만으로 특정 인물의 목소리를 정밀하게 복제할 수 있는 수준에 이르렀으며, 이 기술들은 오픈소스로 공개되어 누구나 접근할 수 있다. 유통 구조의 측면에서 음성 파일은 영상에 비해 용량이 작고 폐쇄형 메신저를 통해 은밀하게 확산되며, 현존하는 탐지 기술로는 그 진위를 신뢰성 있게 판별하기 어렵다. 심리적 측면에서 '녹취'가 갖는 고유한 상징성은 유권자의 확증 편향을 자극하고, 수면자 효과를 통해 사후 정정의 실효성마저 약화시킨다. 이 세 가지 요인이 중첩되는 지점에서 딥보이스는 딥페이크 영상과는 질적으로 구별되며, 어쩌면 선거 국면에서 더 심각한 위협으로 다가올 수 있다.

2024년 미국 뉴햄프셔주 AI 로보콜 사건은 이러한 위협이 이론적 가능성이 아닌 현실임을 입증한 주요 사례다. 단돈 150달러의 제작비로 현직 대통령의 음성을 복제하여 수천 명의 유권자에게 투표 포기를 종용한 이 사건은, 민주주의의 기반을 흔드는 데 정교한 기술도 막대한 자본도 더 이상 필요하지 않다는 불편한 사실을 보여주었다. 우리나라의 「공직선거법」 제82조의8은 '음향'을 규제 대상에 포함시킴으로써 최소한의 법적 근거를 마련해 두었다. 그러나 '딥페이크영상 등'이라는 약칭에서 드러나듯 규제의 실질적 무게중심은 여전히 영상에 쏠려 있으며, 음성 단독 조작물에 대한 탐지·입증·단속의 구체적 체계는 미비한 상태라고 할 수 있다. 2026년 6·3 지방선거는 후보자 수가 많고 정보 유통이 지역 기반의 폐쇄적 네트워크에 의존하는 특성이 있어, 이러한 제도적 공백이 가장 먼저

시험대에 오를 수 있다.

이 글에서는 언론 보도 원칙의 재설계, C2PA 등 기술적 표준의 도입, 유권자 디지털 리터러시의 강화라는 세 가지 보완 방향을 제시하였는데, 어느 하나만으로는 완전한 해법이 될 수 없다. 속이는 기술의 진화 속도는 언제나 그것을 적발하는 기술보다 한발 앞서기 마련이며, 법과 제도는 태생적으로 기술 변화를 뒤쫓을 수밖에 없다. 그렇기에 이 세 가지 접근은 상호 보완적으로 작동해야 하며, 궁극적으로는 허위 정보의 최종 도달점인 유권자 스스로가 마지막 방화벽 역할을 수행할 수 있어야 한다. 민주주의는 시민의 합리적 판단에 기초한다. 그 판단의 전제가 되는 정보 환경이 기술적으로 오염될 수 있다는 사실은, 단순한 기술 규제의 문제가 아니라 민주주의의 작동 조건 자체에 대한 질문이다.