딥페이크 범죄 1 탄
- 종류와 그 예방책 및 대응방법-

안녕하세요. 이승민 변호사입니다.

최근 딥페이크를 활용한 디지털 성범죄의 심각성이 전 사회적 문제로 대두되고 있습니다. 검찰은 '영리 목적, 조직적 범행, 아동청소년 대상 딥페이크 허위영상물 제작 및 유포 범행에 대하여는 원칙적으로 구속수사하는 등 엄정 대처하기로 하였다'고 공표한 바 있고, 2024. 9. 26. 국회에서는 딥페이크 범죄 법정형 상향 등을 위한 법 개정안이 통과되었습니다.

이번 연구자료에서는 **딥페이크 범죄의 종류, 예방책, 대응방법**에 대해 알아보겠습니다.

딥페이크의 개념

딥페이크(deepfake)란 딥 러닝(deep learning)과 가짜(fake)를 합친 말로 인공지능(AI)을 기반으로 한 인간 이미지 합성 기술입니다. 기계 학습 기술을 사용함으로써 사람의 얼굴, 목소리와 행동 등을 다른 사람의 사진이나 영상과 정밀히 합성하여 가상의 영상을 만들 수 있게 된 것입니다.

이를 통해 고인이 되어 다시는 만나볼 수 없었던 지인의 모습을 생생하게 접할 수 있고, 사망한 영화배우의 이미지를 이용한 영상 제작이 가능해지는 등 딥페이크는 매우 놀랍고 무궁무진한 활용성이 있는 기술로 받아들여지고 있습니다.

그러나 최근 이를 이용하는 다양한 신종 범죄들이 생겨나고 있는데, 딥페이크 기술이 범죄 목적으로 악용될 경우 우리 사회에 심각한 피해를 초래할 우려가 있습니다. 이하에서는 딥페이크 이용 범죄의 종류 및 그에 대한 예방책과 대응방법에 대해 알아보겠습니다.

딥페이크 범죄의 종류

가. 딥페이크 성범죄 – 음란물 합성/지인능욕

가장 흔한 딥페이크 범죄는 유명인, 정치인, 혹은 지인 등 일반인의 얼굴을 성적 영상에 합성하는 것입니다. 피해자는 자신이 동의하지 않은 성적 콘텐츠에 등장하게 되며, 이는 피해자에게 심각한

정신적 피해를 유발할 수 있습니다. 딥페이크 성범죄에 대해서는 다음 연구자료에서 더 자세히 알아볼 예정입니다.

나. 사기 및 보이스피싱

딥페이크로 음성이나 얼굴을 합성해 특정 인물(CEO, 유명인 등)의 목소리나 얼굴을 흉내 내어 사기 행위를 저지르는 사례도 발생하고 있습니다. 가짜 음성이나 영상 은 지인 사칭 사기 전화 내지 영상통화를 통한 보이스피싱 범죄 등에도 사용됩니다.

다. 허위사실 유포 및 명예훼손

정치적 또는 사회적 목적으로 딥페이크 기술을 사용하여 특정 인물이나 조직에 대한 허위 정보를 퍼뜨리는 행위도 딥페이크 범죄의 일종입니다. 이러한 영상이나 음성 자료는 진짜처럼 보이기 때문에, 대중을 속이거나 특정 인물의 명예를 훼손하는 데 이용될 수 있습니다.

라. 협박, 공갈 및 인질 범죄

딥페이크로 생성된 영상이나 음성을 이용해 피해자를 협박하거나, 특정인을 납치한 것처럼 꾸며 그 사람의 가족이나 지인에게 석방의 대가로 특정 행위나 금품을 요구하는 공갈 또는 인질강요 범행을 하는 경우도 있습니다.

마. 기타

정치적인 목적에서 딥페이크 영상을 제작해 특정 인물이 거짓으로 발언하거나 행동하는 모습을 만들고 이를 퍼뜨려 사회적 혼란이나 정치적 갈등을 일으키는 경우가 있습니다. 또한, 딥페이크 기술을 통해 특정 인물의 얼굴이나 음성을 도용하여 그 사람인 것처럼 행동함으로써 신분을 속이고 접근이 제한된 장소에 출입하거나 기밀 정보를 빼내는 행위도 가능합니다.

딥페이크 범죄 예방책

딥페이크 범죄는 기술의 발전과 함께 더 정교해지고 있으며, 지난 검찰 업무 경험에 비추어 봐도 고도로 지능화된 범죄를 기술적으로 전부 차단하는 것은 사실상 불가능에 가깝습니다. 따라서 이를 사전에 방지하는 것이 중요하며, 이를 위해 준비할 수 있는 예방책으로는 다음과 같은 것이 있습니다.

① **개인 정보 보호**: SNS 나 공개된 공간에 개인 사진 또는 영상을 최소한으로 게시하는 것이 중요합니다. 이를 통해 딥페이크 생성에 사용될 수 있는 재료를 줄일 수 있습니다.

② **저작권 보호 도구**: 온라인에서 자신의 이미지나 영상의 무단 사용을 방지하기 위해 워터마크 또는 디지털 인증 도구를 사용할 수 있습니다.

③ **계정 보안 강화**: 이중 인증을 통해 SNS 나 이메일 계정의 보안을 강화하고, 비밀번호를 주기적으로 변경하여 해킹에 대비하는 것이 좋습니다.

④ **기술적 대응**: 딥페이크 탐지 소프트웨어와 AI 기반 기술을 통해 딥페이크 영상을 식별할 수 있습니다. 정부는 물론 다수의 기업과 연구소들이 딥페이크 콘텐츠를 자동으로 감지하는 기술을 개발 중입니다.

영상 통화 등을 통해 상대가 돈을 요구하는 경우라면 상대를 무조건 신뢰하지 않고, 상대에게 얼굴 앞에 손을 놓고 흔들거나 고개를 옆으로 돌려보라는 등의 요청을 통해 딥페이크 영상에서 발생할 수 있는 영상 왜곡이나 떨림을 확인해 보는 것이 좋습니다. 가족이나 지인의 경우, 서로를 확인할 수 있는 암호를 정해놓거나 서로만 알 수 있는 내용을 물어보는 등의 방법을 이용하는 것이 가능합니다.

딥페이크 범죄 피해 대응방법

가장 먼저 딥페이크 범죄 피해를 입게 되었다면 **인근 경찰서나 검찰청, 경찰청의 사이버수사대, 디지털성범죄지원센터 등에 신속하게 신고**해야 합니다. 온라인 플랫폼에서도 신고 기능을 통해 딥페이크 콘텐츠를 삭제 요청할 수 있습니다.

또한, 딥페이크 범죄로 인해 심리적 피해를 겪는 경우 심리전문가를 만나보는 것이 좋습니다. 디지털 성범죄 피해자 지원센터 등 전문기관에서 도움을 받을 수 있습니다.

특히 딥페이크 범죄를 활용한 디지털 성범죄는 빠른 대응이 가장 중요하기 때문에, 디지털 성범죄 수사 대응에 경험이 많은 법률전문가를 통해 적극적으로 대처해야 피해를 최소화할 수 있을 것입니다.

이승민 변호사(형사 그룹장, 前 인천지검 여성아동범죄조사부 수석검사)
Partner
seungmin.lee@seumlaw.com