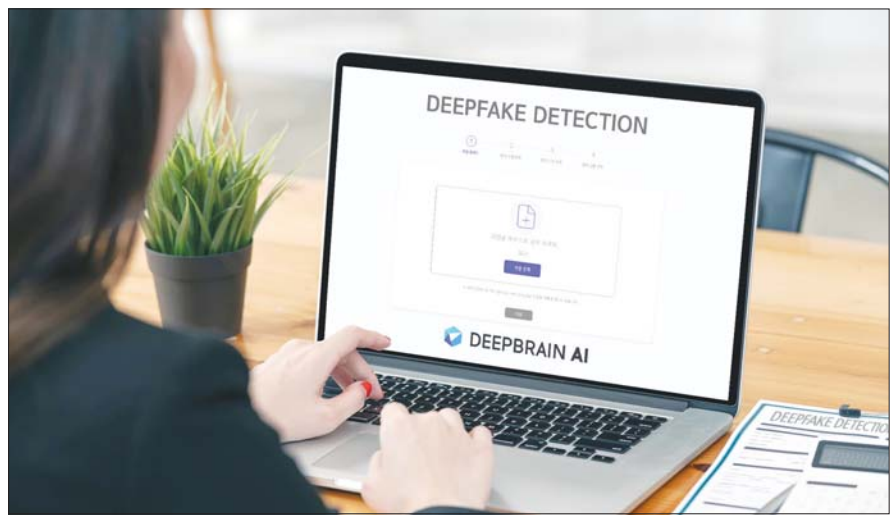
딥페이크 성착취물 AI교란 한계… 해답은 '플랫폼 책임 강화'

워터마크·독풀기 등 한계 드러나
'플랫폼 AI 모니터링' 강화 필요
텔레그램·카카오톡, 상반된 대응
美 캘리포니아주 AI 법안 발의



딥브레인AI의 딥페이크 이미지 탐지 솔루션을 이용하는 모습. 딥페이크 기술을 이용한 범죄가 기승을 부리고 있다. /딥브레인AI

딥페이크(Deepfake) 성착취물 제작 사건이 큰 파장을 일으키면서 플랫폼 책임 강화가 필요하다는 주장이 제시되고 있다. 딥페이크 제작을 막는 데에는 픽셀 단위에서 이미지와 동영상에 변형을 가해 인공지능(AI)을 교란하는 워터마크 삽입 기술(독풀기) 등이 있지만 현실적 한계가 크다는 이유다.

2일 IT업계 관계자들에 따르면 딥페이크 성착취물 제작을 막기 위한 해결책으로 AI 교란 기술이 주목 받고 있지만 일반인의 활용이 어렵고 한계가 있는 것으로 드러났다.

AI 교란 기술은 ▲워터마크 삽입 기법 ▲독풀기(Poisoning Attacks) 등으로 나뉜다. 워터마크 삽입 기법은 이미지나 데이터에 보이지 않는 표식을 추가해 AI가 이를 잘못 인식하거나 오작동하도록 유도하는 방법이다. 저작권물의 무단 학습을 막거나 AI 생성물이라는 사실을 표기하기 위해 고안 됐다. 독풀기는 워터마크 삽입 기법과 달리 이미지에 특화한 AI 교란 기술로, 올해 1월 시카고 대학교 연구팀이 발표한 나이트쉐이드(Nightshade) 이후 큰 관심을 받고 있다. 이미지에 픽셀 단위의 변형을 가해 AI의 이미지 인식을 막는 것으로, 나이트쉐이드를 이용해 변형한 이미지를 AI에 입력하면 소 그림을 쥐 그림으로 인식하는 등 문제를 일으킨다.

문제는 이들 기법을 일반인이 현실적으로 이용하기 어렵다는 점과 기술 발전에 따른 무력화 가능성이 있다는 점이다.

현재 무료 기술로 공개 된 유일한 '독풀기' 소프트웨어인 나이트쉐이드는 2.48GB(기가바이트)에 달하는 것은 물론 윈도우와 맥 OS에서 제한적인 GPU 조건 내에서만 구동한다. 딥페이크 성착취물 제작이 일반적으로 개인이 간단히 모바일 기기로 촬영해 SNS에 올린 사진들로 이뤄졌다는 점을 고려할 때, 현실적인 활용도가 극히 떨어진다.

콘텐츠 AI 솔루션 기업 포바이포 관계자는 "나이트쉐이트 모델의 원리가 원본 데이터를 대척점에 있는 이미지가 연상되도록 전혀 다른 이미지로 오염시킨다는 데 있는데, 이는 독풀기에 패턴이 생길 수밖에 없다는 이야기"라며 "오염 과정 데이터가 쌓이면 이를 반대로 돌려 놓는 패턴도 금세 찾을 수 있을 것"이라고 설명했다.

독풀기가 현실적 어려움이 있다는 점에서 제시되는 방안은 플랫폼의 AI 모니터링 강화를 의무화 하는 등 책임 강화다.

이번 집단적 딥페이크 성착취물 제작 사건은 웹사이트나 딥웹이 아닌 SNS 메신저 텔레그램을 통해 발생했다. 텔레그램은 강력한 보안성과 각국 정부와 타협하지 않는 이용자 보호, 전면 무료 서비스 제공을 장담하며 출발한 SNS 메신저다. 이러한 점이 결국 딥페이크 제작 범죄가 이뤄지는 모태가 됐다. 텔레그램 측은 지난달 CEO 파벨 두로프가 프랑스 쩡부에 검거 된 후 "아동 성착취물 등 범죄 모니터링을 강화 중"이며 "EU의 법률을 준수한다"고 밝히기도 했지만 실질적인 모니터링 효과는 없었다는 평가다.

반면 국내 메신저 프로그램인 카카오톡 등은 강력한 AI 모니터링을 통해 허위조작정보 및 불법 콘텐츠 유통을 막고 있다. 카카오는 지난 1월 딥페이크 관련 검색어를 청소년 보호 검색어로 지정한 데 이어 오픈채팅, 다음을 비롯 카카오 내 공개 게시판 서비스에 딥페이크 유통을 감시하는 모니터링을 진행하고 있다. 특히 카카오톡은 허위영상물 배포 및 제공 행위에 대해서는 카카오톡 전체 서비스 영구 제한이라는 강력한 제재까지 하고 있다.

해외에서도 플랫폼에 책임소지를 강화하는 내용의 법안이 발의되기도 했다. 외신 보도에 따르면 미 캘리포니아주 하원 의회는 AI 안전 대책 법안 투표를 완료해 오는 9월 말 주지사의 승인을 기다리고 있다. 해당 법안은 미성년자 딥페이크 성착취물을 성범죄로 규정하고, 플랫폼에 딥페이크 모니터링과 삭제를 명령할 수 있는 내용을 골자로 한다. 또 딥페이크 AI 기술을 제공하는 회사는 이용자에게 AI 탐지 프로그램을 함께 제공하도록 했다.

생성형 AI 및 딥페이크 탐지 전문 기업인 딥브레인AI 또한 플랫폼의 책임에 대해 강조했다. 장세영 딥브레인AI 대표는 "AI 기술을 악용한 딥페이크 범죄가 기승을 부리는 가운데, 관련 피해 확산을 최소화하고자 진위 여부 판별이 필요한 기업과 관공서 등을 대상으로 자사의 딥페이크 탐지 솔루션을 무료로 지원할 예정"이라고 덧붙였다.

/김서현 기자 seoh@metroseoul.co.kr

두산, 원전시장 경쟁력 강화… '밥캣 분리' 성공여부에 관심 집중

주주 반대 속 원전시장 공략 재편 가속
자금력 확보 후 생산설비 증설 전망
2029년까지 원자로 62기 수주 목표

두산그룹이 주주와 금감원의 반대로 두산로보틱스와 두밥캣의 합병안을 철회했지만 원전 경쟁력 강화에 속도를 낸다.

두산에너빌리티가 자회사 두산밥캣을 분리해 두산로보틱스의 자회사로 편입해 자금력을 확보한 다음 원전 수주를 위해 생산설비 증설에 나설 것으로 업계는 전망했다. 두산밥캣의 부채를 털어내면서 신규 투자 여력을 확보해 원전 시장에서의 경쟁력을 확보할 수 있기 때문이다.

2일 업계에 따르면 두산로보틱스와 두산밥캣은 지난달 29일 각각 이사회를 열고 양사 간 포괄적 주식교환 계약을 해제하기로 경의했다. 양사는 대표이사명의 주주서한을 발표하며 "사업구조 개편 방향이 긍정적일 것으로 예상되더라도 주주와 시장의 지지를 충분히 얻지 못하면 추진하기 어렵다고 생각한다"는 입장을 내놨다. 당초 두산에너빌리티에서 두산밥캣을 떼어내 두산로보틱스와 합병하려 했지만, 금융당국과 소액주주 반대에 한발 물러선 것이다.

다만 두산그룹은 두산에너빌리티에서 두산밥캣을 분할하는 1단계 개편안은 유지하며 오는 2029년까지 5년간 원자로 62기 이상 수주 목표를 달성하기 위한 투자 자본 마련에 나선다. 두산에너빌리티는 두산밥캣의 분할이 성사되면 차입금 7000억원 감소로 재무 지표 개선 효과를 보며 이후 비영업용자산 두산큐벡스·D20캐피탈 지분 등 비영업용자산 처분으로 5000억원의 현금을 확보하면 1조원가량의 투자금을 확보할 수 있다.

지난달 24조원 규모의 체코 원전 사업 수주를 이끈 두산에너빌리티가 폴란드, 아랍에미리트(UAE) 등의 추가 원전 수주에 나설적으로 전망된다. 이를 위해 두산에너빌리티는 노후화된 설비 개선 등을 위한 자금 마련이 어느때보다 절실한 시점이다.

다만 두산밥캣을 떼어내기 위해서는 해결해야할 숙제가 산적해있다. 인적분할로 탄생할 신설회사의 가치 책정 등이 논란의 중심에 선 만큼 분할합병 비율 조정 가능성이 거론되고 있다. 두산로보틱스가 8월 29일까지 정정 신고서를 제출하지 못하면서 이달 25일 주주총회도 개최할 수 없게 되면서 전체적인 일정을 새롭게 준비해야 한다.

또 두산에너빌리티의 인적분할에 대한 기존 주주들의 동의도 필요하다. 두산에너빌리티가 주식매수청구권용으로 설정한 예산 6000억원보다 청구 액수가 많으면 이번 합병 계획은 무산될 수 있다.

업계 관계자는 "체코를 비롯해 폴란드 등 글로벌 시장에서 원전에 대한 수요가 높아지고 있다"며 "두산에너빌리티가 수주 시장 경쟁에서 우위를 점하기 위해서는 이번 사업재편을 통한 투자금을 확보하는게 어느때보다 중요하다"고 말했다.

/양성운 기자 ysw@

전력기기 수요 급증… 피크아웃 우려에도 '맑음'

전력기기 업계, 변압기 초호황 지속
슈퍼사이클 대비 대규모 투자 가속
반덤핑 리스크 최소화 현지 생산 확대


HD현대일렉트릭의 전력 변압기. /HD현대일렉트릭

전력기기 업계가 호황을 맞이한 가운데 피크아웃(하락 전환) 우려를 제기할 만한 요인은 제한적이라는 평가가 나오고 있다. 생성형 AI 시장에 따른 전력 수요 증가와 중동의 친환경 혁신도시 건설 붐 등 여전히 전력기기 산업의 호황을 이끄는 요인이 다수라는 분석이다.

2일 업계에 따르면 올해 들어 7월까지 변압기 누적 수출액은 10억 3200만 달러로 지난해 연간 수출액의 87%에 달한다. 매월 수출액이 전년 동기 대비 증가하며 올해 실적은 지난 2010년 수출액(11억8600만달러)을 넘어 사상 최대치를 기록할 전망이다.

계속되는 호황에 피크아웃 시기에 대한 의문점이 제기되고 있으나, 업계에서는 아직 이와 관련된 우려는 이르다는 의견이 지배적이다. 특히 미국 내 노후 설비의 교체 주기가 도래했단 점이 글로벌 전력기기 시장에서 긍정적인 성과를 이어가는 데 중요한 요인으로 작용하고 있다.

통상 30년으로 여겨지는 노후 전력망 교체 수기가 찾아와 미국 정부는 고용량 전력망 설치, 시스템 현대화에 속도를 내는 중이다. 미국 에너지부에 따르면 미국 변압기의 70%는 교체 시점인 25~30여년 전에 설치됐다.

일각에서는 반덤핑 리스크에 대한 우려도 제기되고 있다. 한국 전력기기 업체는 지난 2011년 미국 반덤핑 조사를 받은 바 있다. 이에 국내 기업들은 미국 내 생산시설 확보를 통해 변압기 초호황기에 선제적으로 대응하고 있으며, 15~60%에 이르는 관세를 피하기 위해 미국 현지 공장의 생산량을 늘리는 전략을 채택하고 있다.

업계는 반덤핑 리스크의 영향을 적게 받을 것으로 내다보고 있다. 미국은 전력기기 부족 현상을 겪고 있는 만큼 자국의 이익을 위해 전력기기 수입을 제한할 가능성이 낮다는 분석이다.

더욱이 반덤핑이 성립하려면 국내 전력기기 업체가 미국으로 수출하는 제품의 단가가 내수 판가 대비 낮아야 한다. 그러나 국내 업체들에게 수익성이 가장 우수한 시장은 미국이며, 반대로 수요와 가격이 부진한 지역은 내수 시장이다. 이는 국내 전력기기 업체들의 미국 수출가격이 내수 판가보다 높은 수준임을 의미한다.

전력기기 업체들은 슈퍼사이클 진입에 대한 기대감에 대응하기 위해 대규모 증설 투자도 망설이지 않는 모습을 보이고 있다.

HD현대일렉트릭은 울산과 미국 앨라배마 변압기 공장에 각각 272억원과 180억원 투자를 통해 생산능력을 약 20% 확대할 방침이다. 또한 지난 2월부터 충북 청주에 대규모 중저압차단기 공장 건립을 추진 중이다. 증설을 통해 HD현대일렉트릭의 생산 능력은 2030년 기준 약 1300만대 수준으로 늘어날 전망이다.

LS일렉트릭은 약 2000억원 규모의 부산사업장 초고압 변압기 생산 능력을 2024년 9월까지 4000억원 수준으로 확대할 계획이다. KOC전기 증설이 완료되면 오는 2026년 5000억원 규모에 달하는 초고압 변압기 생산능력을 보유할 수 있을 전망이다. 앞서 LS일렉트릭은 국내 중소 변압기 업체 KCO전기 지분 51%를 매입한 바 있다.

/차현정 기자 hyeon@