누구나 'AI 딥페이크' 범죄 대상 피해자 보호 중심 제도보완 시급

생성형 AI, 보편화·고도화 추세
성적 콘텐츠 제작 등 악용사례 증가
법적 안전장치 사업자·이용자 집중

생성형 인공지능(AI)의 이미지 편집·합성 기능이 고도화되면서 이를 악용한 딥페이크 성착취물 제작이 일상적인 위협으로 확산되고 있다.

12일 〈메트로경제신문〉 취재와 업계 분석을 종합하면, 최근 '누디피케이션(nudification)'이나 '디클로싱(De-Clothing)'으로 불리는 앱과 도구들이 딥페이크 성착취 범죄를 대량으로 만들어내고 있다. 이들 툴은 AI를 활용해 실제 인물의 사진을 나체 이미지로 합성하거나 조작하는 방식이다.

제작 문턱도 낮다. 다량의 나체 이미지를 AI에 학습시킨 뒤 얼굴 인식 알고리즘을 활용해 각도와 방향에 맞춰 합성하는 구조로, 일정 수준의 코딩 지식만 있으면 구현이 가능하다. 개발 과정에서 발생하는 기술적 문제는 깃허브(GitHub)에 공개된 오픈소스나 생성형 AI 도구를 참고해 해결할 수 있다. 이렇게 만들어진 봇 수백 개가 텔레그램 채널 등을 통해 유통되고 있으며, 일부 고도화된 툴은 유료로 거래되기도 한다.

이 같은 문제를 단적으로 드러낸 사례가 일론 머스크의 xAI가 개발한 생성형 AI '그록(Grok)' 논란이다. 그록은 본래 누디피케이션을 목적으로 한 서비스는 아니지만, 최근 업데이트 이후 이용자들이 단순한 명령어만으로 여성과 아동을 대상으로 한 딥페이크 성착취물을 생성할 수 있었던 것으로 드러났다.

전문가들은 이번 사태의 원인으로 그록의 윤리 설계와 안전장치 부족을 지목한다. 오픈AI의 챗GPT나 구글의 제미나이가 비교적 엄격한 콘텐츠 필터링 체계를 갖춘 것과 달리, 그록은 '덜 검열하는 AI'를 표방하며 성적 콘텐츠에 대한 관리·감시 시스템을 충분히 구축하지 않았다는 지적이다.

논란이 확산되자 엑스(X)는 이미지 생성 기능 제한과 유료화 전환에 나섰지만, 유럽연합(EU)과 영국 등 규제 당국은 이를 근본적인 해결책으로 보기 어렵다며 압박 수위를 높이고 있다. 영국 정부는 접속 차단 가능성까지 언급했으며, EU는 알고리즘을 포함한 불법 콘텐츠 관련 자료 보존 명령을 내렸다.

이러한 국제적 흐름 속에서 우리 정부도 오는 22일 시행되는 'AI 기본법'을 통해 대응에 나선다. AI 기본법은 생성형 AI 기반 제품과 서비스에 대해 사전 고지를 의무화하고, 생성 결과물에 워터마크 등 표시를 부착하도록 규정하고 있다.

다만, 이 같은 의무는 AI 사업자에게만 적용되며, 결과물을 활용하는 일반 이용자에게는 투명성 확보 책임이 부과되지 않는다. 해외에서도 미국 캘리포니아주는 표시 훼손에 대비한 탐지 도구 제공을 규정하고, 중국은 플랫폼 사업자의 관리 책임을 강화하는 등 AI 생성물 표시 의무를 확대하는 추세다.

그러나 현행 AI 기본법만으로는 딥페이크 피해자를 충분히 보호하기 어렵다는 지적이 나온다. 정보통신정책연구원(KISDI) 보고서에 따르면 정준화 국회입법조사처 입법조사관은 현행 법 체계가 '이용자 중심'으로 설계돼 있어, 생성물로 인해 직접적인 피해를 입는 당사자 보호가 상대적으로 취약하다고 분석했다. 딥페이크 범죄가 타인을 대상으로 피해를 발생시키는 구조임에도, 법적 안전장치는 사업자와 이용자 간 투명성 확보에 집중돼 있다는 것이다.

보고서는 보호 대상의 범위 재검토 필요성도 제기했다. 현행법은 생명이나 신체 안전에 중대한 영향을 받는 경우를 중심으로 위험을 정의하고 있지만, 실제 딥페이크 피해는 사기·기만에 따른 재산적 손실이나 명예훼손 등으로 나타나는 경우가 적지 않다. 특히 디지털 환경에 취약한 계층이 서비스 이용자보다 더 큰 위험에 노출될 수 있다는 점에서, 피해자 보호를 중심에 둔 추가적인 제도 보완이 필요하다는 지적이다.

IT업계 관계자는 "현재의 기술력으로는 워터마크를 삭제하거나 AI 생성물 탐지를 우회하는 기술적 편법이 얼마든지 가능하다"며 "정부의 제도 정비와 병행하여, 개발 단계에서부터 윤리적 가이드라인을 강제하는 '세이프티 바이 디자인(Safety by Design)'이 업계의 생존 전략이 되어야 한다"고 강조했다. 이어 "결국 기술을 만드는 기업이 상업적 자유도보다 사회적 책임을 우선시하지 않는다면, 법과 제도는 언제나 기술의 악용 속도를 뒤쫓는 데 그칠 것"이라고 덧붙였다.

/김서현 기자 seoh@metroseoul.co.kr

지난해 K-푸드 플러스 수출 136억달러 '신기록' 12일 오후 서울시내 한 대형마트에서 외국인 관광객이 라면을 고르고 있다. 농림축산식품부는 지난해 K-푸드 플러스(+) 수출액이 한류 콘텐츠의 글로벌 인기와 'K-매운맛' 열풍 확산으로 라면·소스·아이스크림 등 가공식품을 주도로 역대 최고인 136억 달러를 돌파했다고 밝혔다. /뉴시스

기획예산처, 과기부 상설 협의체 신설

예산 편성 시 사전협의·협력 강화

기획예산처와 과학기술정보통신부가 국가 연구개발(R&D) 투자의 효율성·일관성을 높일 목적으로 상설 협의체를 신설한다. 또 예산 편성 시 사전 협의 및 협력을 강화해 나갈 방침이다.

12일 기획처에 따르면 올해 기준 전체 R&D 예산은 35조5000억 원이다. 이 중 85.3%를 차지하는 주요 R&D 예산 30조5000억 원은 과기부 과학기술혁신본부에서 배분·조정안을 우선 마련한다. 이를 바탕으로 기획처가 최종 예산안을 편성하는 게 그간의 운영 방식이었다.

이 같은 구조는 R&D 사업의 특수성을 고려한 기술적 검토와 재정적 관점에서의 분석을 동시에 반영할 수 있다는 장점이 있는 반면, 부처 간 칸막이로 소통이 원활하지 못 했다는 일부 지적이 제기된다.

이에 기획처와 과기부 과학기술혁신본부는 R&D 예산편성 과정에서 사전 협의 및 공동 검토를 강화하는 방향으로 부처 간 협업 방식을 발전시켜 나가기로 했다.

개편의 핵심은 기술적 전문성 검토와 재정 운용 원칙을 조화롭게 반영할 수 있도록, 양 부처가 초기 단계부터 충분히 논의하고 책임을 공유하는 협력체계를 구축하는 것이다.

양 부처는 협력, 소통 채널을 제도화하기 위해 'R&D 예산 협의회'를 신설한다. 그동안 부처 간 소통이 실무 차원의 비공식 논의에 주로 의존해 왔다는 지적에 따라 앞으로는 국장급 상설 협의체를 매월 1회 정례적으로 운영한다.

상설 협의체에서는 정부 R&D 중점투자 방향, 지출 효율화 방안, 신규사업 검토 등 의제를 시기별로 폭넓게 논의할 계획이다.

예산편성 과정에 상호 참여도 확대한다. 그간 부처 간 역할 분담이 오히려 칸막이로 작용해 왔다는 지적에 따라 과학기술혁신본부가 주요 R&D 예산 배분·조정안을 마련하는 과정에 기획처가 참여할 수 있도록 개선한다.

또 기획처 예산편성 과정에서도 과학기술혁신본부 의견이 반영될 수 있도록 개선한다. 기획처는 R&D 배분·조정안을 조정하는 경우, 신설되는 상설 협의체 등을 통해 과학기술혁신본부와 사전에 충분히 논의하고 의견을 반영할 계획이다.

기획처 관계자는 "이번에 마련된 개선방안은 2027년 예산안 편성 과정부터 즉시 적용된다"며 양 부처는 앞으로도 확대되는 R&D 투자가 더욱 효율적으로 이루어지도록 예산편성 과정에서 상호 역할을 존중하며 긴밀히 협력해 나갈 계획"이라고 말했다./세종=김연세 기자 kys@

한화, 미국향 조선 전략 속도… '설비·인증' 변수

美 현지 도크 부족 등 물리적 제약
종합 자격체계 아직 완비하지 못해

한화그룹이 무인군함까지 영역을 넓히며 미국향 조선 전략에 속도를 내고 있지만 미국 필라델피아조선소의 현실은 도크 부족과 인증 미완이라는 구조적 병목에 직면해 있다. 상선 수주만으로도 건조 여력이 빠듯한 가운데 해벅AI 협력을 통한 무인함정 개발 구상이 더해지며 추가 설비 확보 필요성이 한층 커졌다는 분석이 나온다.

12일 업계에 따르면 한화디펜스USA는 필라델피아조선소 도크 2기만으로는 향후 수요를 감당하기 어렵다고 보고, 유휴 도크 확보·타 조선소 도크 활용(분산 건조) 등을 검토 중이다.

한화는 지난 2024년 필라델피아조선소 인수(약 1억 달러)에 이어 추가 50억 달러 투자로 연간 건조능력을 최대 20척까지 확대하겠다는 계획을 밝혔지만, 증설이 완료되기까지는 수년이 소요될 전망이다. 현재 필라델피아조선소는 대형 상선과 미 해사청(MARAD) 관련 정부 선박 등 약 19척의 수주잔량을 보유한 것으로 알려졌고, 현 도크 체계 기준 연간 건조능력은 상선 1~2척 수준에 그친다. 업계는 적정 수주잔량을 3~4년치로 보는 만큼 대규모 증설이 현실화되기 전까지는 외부 협력이나 추가 설비 확보 없이는 병목이 불가피하다는 관측이다.


한화오션이 지난해 8월 미 해군 함정 유지·정비·보수(MRO) 사업을 처음 수주해 6개월 간 정비를 마친 군수지원함 '월리 쉬라'호가 출항하는 모습. /한화오션

여기에 최근 한화는 미국 자율선박 스타트업 해벅AI와 중형 무인수상정(ASV) 협업을 추진 중이다. 미 해양 전문매체 더 마리타임 이그제큐티브는 지난 8일 양사가 약 200피트급 자율 수상함 공동 개발을 검토하고 있으며, 생산 거점으로 필라델피아조선소가 거론된다고 전했다.

또 한화가 핵추진잠수함 건조 참여 가능성까지 공개적으로 언급한 만큼, 향후 군함·잠수함 신규 물량 확대 여지가 거론된다. 인력도 확충에 나선 것으로 보인다. 한화는 전문 인력 확보를 위해 미국 현지 인력을 한국 조선소로 초청해 실무 교육을 진행하는 '한·미 순환 교육' 구상을 필라델피아에서 기획 중인 것으로 알려졌다.

다만 필라델피아조선소는 도크 부족 외에도 미 해군 전투함을 직접 건조하기 위한 종합 자격 체계를 아직 완비하지 못한 상태다. 미 해군 함정 건조에는 시설보안인가(FCL), 미 해군 해상시스템사령부(NAVSEA) 및 함정건조감독단(SUPSHIP) 감독 체계 편입, 군사규격 품질 인증 등 복수 요건 충족이 필요하다. 특히 FCL은 미 국방방첩보안국(DCSA) 심사를 거치며 통상 12~18개월이 소요되는 것으로 알려졌다. 업계에서는 상선 위주로 설계된 도크 체계에서 군함·잠수함 생산을 병행할 경우 보안 통제 등 추가적인 공정 제약이 불가피하다는 지적도 나온다.

윤현규 국립창원대 조선해양공학과 교수는 "추가 도크 확보나 타 조선소 활용 없이 미 해군 군함·무인함정·잠수함 사업까지 동시 대응하기에는 물리적 제약이 분명하다"며 "한화의 미국 조선 전략은 미 정부 발주 정책에 맞춰 단계적으로 설비와 생산 거점을 확장하는 방식으로 전개될 가능성이 크다"고 말했다.

/유혜온 기자 dhaledhale@

"서울 경제 데이터, 한눈에 확인하세요"

서울시 '경제관' 구축·서비스
지도·그래프 중심 시각화 초점

창업을 계획하기 전에 원하는 지역의 사업체 분포와 밀집 업종, 지역 거주자의 평균소득과 소비 규모, 지난 10여 년간 어떤 산업이 성장하거나 쇠퇴했는지 등을 '한 곳에서 한눈에' 시각 데이터로 확인할 수 있는 서비스가 제공된다.

서울시는 서울데이터허브에 여러 기관에 흩어져 있던 경제 관련 데이터를 한데 모아 서울의 경제 상황을 파악할 수 있는 '경제관'을 구축, 13일부터 서비스에 들어간다고 12일 밝혔다. 경제관은 서울데이터허브 누리집에서 확인할 수 있다.

시는 경기 흐름, 산업 구조 변화, 창업 환경 등 기존에 통계 보고서나 전문 자료를 통해서만 접할 수 있던 경제 지표 및 정보를 전문가가 아닌 일반 시민도 쉽게 이해할 수 있도록 지도·그래프를 중심으로 시각화하는 데 초점을 맞췄다.

'경제관'은 ▲경제구조·성장 ▲경기지수 ▲산업 ▲창업·자영업 ▲고용·소득 ▲물가 ▲소비 ▲가계금융 ▲부동산, 총 9개 분야 핵심 경제 지표를 다루며 40개 화면을 통해 서울의 경제 흐름을 단계적으로 살펴볼 수 있는 점이 특징이다. 자치구별 지역내총생산(GRDP), 취업자수, 창업률, 부동산 거래량 등 주요 지표를 지도 기반 시각화, 시계열 그래프, 전년 대비 증감 비교 기능 등을 한 화면에서 확인할 수 있어 특정 지역이나 시점 변화를 직관적으로 확인할 수 있다.

특히 426개 행정동 단위로 세분화한 데이터를 제공, 자치구 평균이 아닌 실제 생활권 수준 경제 여건도 살펴볼 수 있도록 설계됐다.

/이현진 기자 lhj@