

미국·영국 AI 규제 동향과 시사점

미래전략개발부 경제조사팀
범 형 원 (beomhw123@kdb.co.kr)

- ◆ AI 통제 이탈 우려가 제기되는 가운데, 美·英 일부 의원은 AI 중단 기능 의무화와 초지능 인공지능 개발 금지 등 법적 통제 방안을 제안
- ◆ 국내에서는 美·英 법안 등 해외 사례를 참고해 AI 입법 논의 시 사고 대응 절차와 국가 간 협력 방안을 검토할 필요

□ AI 성능 향상 속도 대비 안전성 검증 지연에 따른 AI 통제 필요성 대두

- 엔트로픽 CEO 아모데이는 재귀적 자기개선(RSI)*과 AI 통제 이탈 사례를 들어 안전성 검증이 성능 향상에 뒤쳐질 가능성을 제기
 - * RSI(Recursive Self-Improvement) : AI시스템이 스스로 AI성능을 업그레이드하며 진화하는 방식
 - 재귀적 자기개선으로 개발이 가속되면 위험 파악과 안전조치 마련에 필요한 시간이 부족해질 수 있다는 문제 인식
 - OpenAI 평가용 AI가 부여된 과업의 범위를 벗어나 외부 시스템을 공격하는 등 AI 통제 이탈 사고* 발생
 - * '26.7월, 오픈 AI의 최신형 모델이 보안 취약점을 이용해 AI 커뮤니티인 '허깅페이스'를 해킹
- 마이크로소프트 빌 게이츠는 기업의 자율규제만으로는 AI 위험 대응에 한계가 있어 정부의 입법 필요성을 강조
 - AI 악용에 따른 대규모 피해 가능성을 우려하며, 안전장치와 감시 의무 마련에 범정부 차원의 참여를 촉구
- 미국·영국 의원들은 AI의 작동을 중단하거나 개발을 금지하는 법안을 제출해 정부의 통제 권한을 논의
 - 미국은 '26.7.23일 AI Kill Switch Act와 '26.9.23일 Ban Artificial Super intelligence Act를, 영국은 '26.9.8일 Artificial Super intelligence Bill을 발의
 - 세 발의안은 AI 통제 범위와 정부 개입 방식 등을 중심으로 논의

□ 미국·영국의 법안은 AI 서비스 중단 기능 확보와 초지능(ASI)* 개발 금지를 제안하며 정부의 개입 범위를 구체화

* ASI(Artificial Superintelligence) : 인간의 지능을 뛰어넘는 지적 범위를 가진 인공지능 시스템으로 인간 수준인 범용인공지능(AGI)과 구분

- 미국 AI Kill Switch Act는 대규모 AI 서비스 사업자에게 서비스 중단 기능 확보와 사고 보고 의무를 부과하는 방안을 제시
 - AI 관련 기술*의 전년 매출이 5억달러 이상인 사업자 등을 대상으로 설정하고, 지정 사고 인지 후 15일 이내 보고를 요구
 - * AI 관련 기술은 미국 클라우드 시장가격 기준으로 AI 개발 연산자원의 비용이 1억달러를 초과하는 AI시스템을 의미
 - 동 발의안은 통제 이탈 등 지정 사고 발생 시 국토안보부(DHS)*가 기업에 AI 접근 제한 및 중단을 명령하고 이행 여부를 확인할 수 있는 권한을 부여
 - * DHS(Department of Homeland Security) : 테러 방지, 국경 통제 등을 담당하는 행정기관
 - 적법한 중단 명령의 방해, 감시 기능으로부터의 행동 은폐, 개발자가 의도하지 않은 목표 추구 등을 사고 범주에 포함
 - 개발자·운영자가 의도하지 않은 행동으로 10명 이상 사망 또는 1억달러 이상 경제적 피해를 초래한 경우도 포함
- 미국 Ban Artificial Superintelligence Act는 ASI 금지와 첨단 AI 개발의 일시 중단을 제안
 - ASI로 이어질 수 있는 특성*을 하나 이상 갖춘 AI도 금지 대상에 포함
 - * AI 연구 자동화, 무단 접근, 작동 중단 저항, 대량살상무기 개발 지원, 감독 회피
 - 학습 연산량 10^{25} 회 이상인 첨단 AI는 감독부처의 규칙 마련 전까지 학습·수정 등을 중단하고 미출시 시스템의 배포도 제한
 - AI 담당 장관이 국무장관과 협력해 국제협약·동맹국 공조를 추진하도록 하며, AI 연산 기반시설에 대한 수출통제도 정책 수단으로 제시
- 영국 Artificial Superintelligence Bill은 사후 통제의 한계를 이유로 ASI의 개발·배포·운영 금지를 제안
 - ASI가 자기개선과 중단 명령에 대한 저항 능력을 갖출 수 있어 사전에 제약이 필요하다고 주장
 - ASI로 이어질 수 있는 기술에 대한 정부의 감시·통제 권한과 국제적인 금지 협약 추진도 제안
 - '26.11.13일에 발의안의 취지와 기본 방향을 하원에서 논의 예정

미국·영국 AI 통제 발의안의 주요내용

구분	美 AI Kill Switch Act	美 Ban Artificial Superintelligence Act	英 Artificial Superintelligence Bill
발의 시점	'26.7.23일	'26.9.23일	'26.9.8일
규제 대상	연산비용·사업자 매출 등 일정 요건을 충족하는 AI서비스	ASI 관련 위험 특성 보유 AI, 일정 연산량 이상의 첨단 AI	초지능 인공지능(ASI)
핵심 수단	AI 중단 기능 확보 및 사고 보고, 정부의 제한·중단 명령 권한	ASI 금지, 첨단 AI 개발 일시 중단	ASI 개발·배포·운영 금지, 정부의 감시·통제 권한
진행 단계	하원 발의, 국토안보위원회 회부	상원 발의, 상업·과학·교통위원회 회부	'26.11.13일 발의안 심의 대기

자료 : 영국 의회, 미국 정부출판국

□ 국내는 AI 개발 역량 확충을 우선시하되, 미국·영국 입법 사례를 참고해 AI에 대한 안전관리 체계와 국가 간 협력 방안을 검토할 필요

- 미국·영국의 발의안은 사고 대응과 개발 금지라는 접근을 제시한 만큼, 향후 규제 범위와 집행 방식의 구체화 여부에 주목
 - 세 발의안은 의회 심사 중이므로 입법 논의의 진전과 실제 기업에 적용되는 내용을 지속적으로 검토 필요
- 국내는 AI 산업의 경쟁력 확보가 중요한 만큼, 광범위한 개발 제한보다는 기술개발과 안전관리의 균형을 고려할 필요
 - 해외의 입법 결과뿐만 아니라 국내 AI 기업의 개발 역량과 서비스 제공 형태 등을 고려
- 국제 공조는 ASI 개발 금지에 관한 국가 간 합의와 사고 대응을 위한 실무 협력으로 구분해 접근할 필요
 - 美·中 양국은 '26.9.24일 정상회담에서 ASI 협의 채널* 신설과 사고 관련 소통 채널 구축에 합의, 후속 협의와 구체적인 운영 방식에 주목할 필요

* US-China Super Intelligence Dialogue