ISSUE BRIEF

이슈브리프 527호
(2024. 3.25)

EU ‘인공지능 규제법(AI Act)’ 통과의 의미와 시사점

제527호

윤정현 신안보연구실
조은정 안보전략연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

지난 3월 13일 EU는 세계 최초로 '인공지능 규제법(AI Act)'을 통과시켰다. 이번 법안에서 EU는 역내 AI 기술 개발을 지원하는 'AI 혁신 패키지(AI Innovation Package)'와 사용자와 개발자의 안전과 기본권을 보장하는 'AI 조정 계획(Coordination Plan on AI)'을 포함시킴으로써 AI의 '개발'과 '규제'를 위한 균형점을 찾고자 하였다. 법안은 AI의 위험도를 4단계 등급별로 분류함으로써 위험도에 따른 차등 규제안을 제시하고 있다. 이번 EU의 AI Act가 갖는 외교전략적 함의는 크게 두 가지라 할 수 있다. 첫째, EU가 AI와 디지털전환 등 첨단기술 분야에서 규범력을 앞세워 진영을 넘어선 실리 외교를 추구하는 제도적 발판을 마련했다는 점이다. 둘째, 미중 등 AI 기술 주도국들과 벌어진 하드파워의 격차를 AI 규제력이라는 소프트파워로 좁혀가는 전략을 구사했다는 점이다. 다만, 이번 법안은 세계 최초의 강제력을 갖는 AI 법안으로서 상징하는 바가 크지만, 정부의 실질적인 관리·감독 가능성, 산업·연구생태계의 다양성 측면, 군사적 활용과 같은 민감한 분야로의 확장성 측면에서 아직 미흡한 점도 사실이다. 우리 정부는 "AI 발전을 위축시키지 않는 범위에서 적절한 AI 신뢰성·안정성을 확보한다"는 방침을 결정한 바 있다. 따라서, 향후 EU AI Act가 미치게 될 글로벌 AI 규제 환경 변화에 적응하기 위한 민관의 노력이 시급한 상황이다. 특히, AI의 사회적 활용 위험성에 대한 기업과 연구 생태계 전반의 인식 전환과 책무성이 강화되어야 할 것이다. 나아가, 올해 9월 서울에서 개최될 제2차 'AI의 책임있는 군사적 이용에 관한 고위급회의(REIAM)' 의제에서 본 법안의 어떠한 측면을 반영할 수 있는지에 대해서도 고민이 필요하다. 즉, 이번 EU AI Act를 통해 확인한 핵심 원칙과 위험 기준들을 이견이 적은 분야부터 REAIM에 점진적으로 연계해가는 노력이 요구될 것으로 전망된다. 이를 통해 수용성을 확보하고 보편적 원칙을 구현해가는 민·관·군의 협력적 AI의 활용 관행을 만들어 나가야 한다.

핵심어 : 유럽연합(EU), 인공지능 규제법(AI Act), AI 위험, AI 혁신 패키지(AI Innovation Package)', 'AI 조정 계획(Coordination Plan on AI)'

세계 첫 '인공지능 규제법(AI Act)'의 도입

지난 3월 13일 유럽에서 세계 최초로 '인공지능 규제법(AI Act)'이 통과되었다. 이번 규제법은 2021년 유럽 집행위원회(European Commission)가 글로벌 빅테크 기업들이 무분별하게 생체정보를 수집하고 데이터화하여 상업적 용도로 사용하면서 개인의 인권을 침해할 수 있다는 위험성을 담은 법안을 제출하면서 비롯되었다. 이번 규제법에는 유럽 내 AI 기술 개발을 지원하는 'AI 혁신 패키지(AI Innovation Package)'와 사용자와 개발자에 안전하고 기본권을 보장하는 AI 생태계 조성을 위한 'AI 조정 계획(Coordination Plan on AI)'이 포함되어 있어 EU가 AI '개발'과 '규제'의 균형점을 찾기 위해 고심한 흔적을 엿볼 수 있다. 2023년 10월 미국 바이든 행정부가 AI 개발자가 정부와 주요 데이터를 공유하도록 행정명령을 발표한 바 있으나, 민관을 아울러 포괄적이고 법적 구속력을 갖춘 기술 규제법을 내놓은 것은 EU가 처음이다. 로베르타 메솔라 유럽의회 의장은 "혁신을 가능하게 하는 동시에 기본권을 보호해 줄 선구적인 법"이라 자평하였다. 이번 법안은 '제1차 AI의 책임있는 군사적 이용에 관한 고위급회의(REAIM)' 개최('23. 2), '제1차 AI 안전 정상회의(AI Safety Summit)' 개최('23. 11) 등, 그간 EU가 최초로 주최해왔던 AI의 통제에 관한 국제회의 의제들 상당수가 구체화된 결과이기도 하다. EU 회원국들의 최종 승인만을 남겨둔 이번 규제법은 향후 36개월 동안 단계적으로 확대 적용되어 2026년에 전면 시행될 예정이다.

EU AI Act의 주요 내용

이번 EU AI Act의 주요 골자는 크게 세 가지로 요약된다. 첫째,

신뢰할 수 있는 AI의 개발 지원이다. 해당 법안을 시행하기 위해 2024년 2월에 설립된 유럽 AI 사무소는 향후 개발자와 사업체들에게 자문과 지원을 제공할 예정이다. 이는 AI 기술 활용에 전제된 인간의 존엄성, 윤리, 투명성의 원칙 등이 보장되는 환경을 조성함으로써 주요 이해관계자들의 수용을 장려하고, 상호 협력과 혁신을 제도적으로 지원하기 위한 노력이다. 이를 위해 유럽 집행위원회는 AI Pact라는 이니셔티브를 도입하고, 개발자들이 AI Act의 주요 의무 사항을 준수하도록 장려하고 있다.

둘째, 자유롭고 안전한 AI 사용을 위해 위험도를 식별하고 그에 맞는 엄격한 규제를 마련하여 위험을 완화하고 관리한다. 이번 규제로 유럽에서 AI 서비스는 정보의 민감도와 중요성에 따라 4단계로 차등 규제된다. 가장 먼저 개인의 특성이나 행동을 데이터화하고 점수를 매기는 '소셜 스코어링'은 전면 금지된다(unacceptable risk). 의료, 교육, 고용, 금융 등 핵심적인 공공 서비스와 이민이나 국경 관리처럼 국가 시스템과 밀접한 AI는 고위험 등급(high risk)으로 분류되어 위험관리 시스템 구축 및 인간 관리자의 감독 아래 놓인다. 또한 앞으로는 AI로 생성된 컨텐츠라는 사실을 식별할 수 있는 정보를 제공하고 정보의 투명성을 제고함으로써 제한된 위험(limited risk)도 적극적으로 관리될 전망이다. 이에 비해 '스팸 필터'처럼 위험도가 낮은 AI 서비스나 혁신이나 비즈니스 운영과 관련하여 무해하다고 판단되는 경우 저위험 등급(minimal risk)으로 분류되어 저강도 규제에 놓인다. 기본적으로 AI 규제법에 따라 AI를 활용한 실시간 생체 정보 수집 및 식별 시스템은 금지되나 예외적으로 테러와 같이 중대 범죄 용의자 수색 등 불가피한 경우 법원으로부터 사전 허가를 득한 뒤 허용된다.

셋째, AI Act는 개인의 권리 보호와 기업의 투명성을 보장하고 글로벌 표준 설정을 목표로 한다. 이를 위해 실효적 이행 수단 역시 담보하고 있다. 규제법에 따르면 EU는 규정을 어기는 기업에 전 세계 매출액의 최대 7%의 벌금을 부과할 수 있게 되었다. 이미 지난 달 디지털 서비스법(DSA, '24. 2)을 시행한 바 있는 유럽 집행위원회는 AI 규제법 통과 하루 만인 3월 14일 전격적으로 미국 X, 중국 틱톡과 알리익스프레스에 대해 위반 여부 조사에 착수하였는데, 이를 우연이라고 보기 어려울 것이다. EU는 글로벌 온라인 플랫폼들에 AI로 조작한 딥페이크 예방 조치 정보를 요구함은 물론, 개인 맞춤형 광고를 위해 개인정보가 무분별하게 이용되고 있는지의 여부를 감독할 수 있게 되었기 때문이다. 이는 그간 선언적으로 그쳐왔던 AI의 기본 원칙들을 정부가 실효적으로 강제할 수 있는 제도적 기반을 갖추게 되었음을 시사한다. 나아가 EU는 이 같은 규제가 안전하고 신뢰할 수 있는 AI 생태계 조성을 위한 글로벌 표준으로 자리할 수 있기를 기대하고 있다.

그렇다면 이번 법 도입의 가장 큰 의의는 어디서 찾을 수 있는가? 무엇보다도 EU가 규범을 선도함으로써 AI 질서에 유의미한 영향을 미칠 수 있는 제도적 발판을 마련했다는데 있다. 또 다른 중요한 의의는 EU가 미중 등 AI 기술 주도국들과 벌어진 하드파워 격차를 AI 규제력이라는 소프트파워로 좁혀가려는 의지를 보여주고 있다는 점이다. EU는 냉전기에도 '유라톰(EURATOM)'이라는 역내 원자력공동체 발족을 통해 핵규범을 공동 개발하고 '국제원자력기구(IAEA)'나 '핵확산금지조약(NPT)'에 앞서 표준화해왔던 경험을 갖고 있다. 즉, 당시에도 핵 물질과 관련된 민감한 첨단기술 영역에서 미소 패권들의 견제를 극복하고 유의미한 행위자로서의 자신들의 입지를 공고히 다졌던 것이다. EU는 이 같은 노련한 규범

외교의 경험을 21세기의 최첨단 이중용도 기술인 AI 분야에서 재현하려 하고 있다.

한계 및 시사점

이번 법안은 세계 최초의 강제력을 갖는 AI 규제법으로서 상징하는 바가 크지만, 정부의 실질적인 관리·감독 가능성, 산업·연구생태계의 다양성 측면, 보다 민감한 분야로의 확장성 측면에서 아직 한계점을 보이는 것도 사실이다. 첫 번째는 기술독점주의에 따른 '개발자'와 '규제자'간 정보 불균형성이다. EU가 AI 규제법을 서두른 중요한 이유 중 하나는 오는 6월로 예정된 유럽의회 선거에서 AI 기술을 이용한 딥페이크와 가짜뉴스가 미칠 부작용을 최소화하기 위해서이다. 기술이 발전하면서 AI가 '환각(hallucination: 모델이 오류를 만들고 조작하는 경우)' 증상을 일으켜 딥페이크의 바이럴 확산 및 AI의 자동조작으로 선거에서 유권자를 호도할 우려가 높아지고 있다. 이에 따라 전문가들은 빅테크에 집중화된 기술독점주의로 인해 상대적으로 기술 개발 정보가 불충분한 규제기관이 과연 이들에 대한 규제가 가능할 것인지 의문을 제기한다. 이번 AI Act에 비판적인 전문가들은 이번 법이 현재 소수의 글로벌 빅테크들이 독점하고 있는 기술 권력을 견제하기에는 불충분하며 AI 생태계 교란을 막기위해서는 더욱 강력한 규제안 마련이 필요하다고 주장한다.

두 번째는 AI 윤리 강조에 따른 AI 개발 저해 가능성이다. 일각에서는 이번 유럽의 발빠른 AI 규제법 공표가 유럽에 양날의 검이 될 것이라 전망한다. AI 규제 분야에서 유럽이 선도적인 역할을 개척해 나가는 발판을 마련했다는 시각과 미국이나 중국과 비교하여 AI 기술의 후발주자인 유럽이 스스로

AI 기술 개발에 족쇄를 채웠다는 시각이 공존하기 때문이다. 프랑스 'AI 위원회'는 최근 AI 기술 발달은 국가 경쟁력과 밀접한 관련을 맺고 있으며 따라서 국가 규제안 마련 시 자국내 AI 기업 협력이 필요하다는 권고안을 내놓았다. 이는 유럽 내에서 EU의 과도한 AI 윤리의 강조로 AI 기술 개발을 저해할 수 있다는 위험성을 개별 국가들이 감지하고 있음을 방증한다. 실제로 유럽의 영세 스타트업과 중소기업들은 이번 AI 규제가 과도하게 부여된 의무로 실제 개발 업무에 부담을 지울까 우려하고 있다. 즉, 결국 선도국인 미국과 중국 경쟁 구도를 오히려 강화하는 결과를 낳을 수 있다는 비관론까지 제기되고 있는 것이다.

세 번째는 민간에 주어진 규제와 달리 안보와 가장 민감한 군사적 영역에서는 아직 적용이 요원한 점이다. AI 기술은 군사적 목적으로 사용될 때, 상업적 차원과는 또 다른 심각한 윤리적 후폭풍을 낳을 수 있다. 뿐만 아니라 AI가 고도화되어 사람의 판단을 넘어서는 능력을 갖추게 될 경우, 전통적인 군사 규칙과 윤리적 원칙을 무시하거나 방해하는 결과로 이어지기도 한다. 이 같은 위험성에도 불구하고 이번 법안은 상업적 활용 규제에 초점을 맞춤으로써, 향후 이를 보다 민감한 군사 부문으로 어떻게 확대·적용해 나가야 하는지에 대한 숙제를 남겨둔 셈이다.

그렇다면, 이번 법안 통과에 한국의 민간·국방 분야를 포함한 AI 생태계는 어떻게 대응해야 하는가? 우리 정부는 지난해 11월 AI 안전 정상회의 참가에 앞서 "AI 발전을 위축시키지 않는 범위에서 적절한 AI 신뢰성·안정성을 확보해야 한다"는 기본 방향을 강조한 바 있다. 이 같은 기조가 향후 EU AI Act가 미치게 될 글로벌 AI 규제 환경 변화에도 순조롭게 추진될 수

있을지는 확신하기 어려워진 상황이다. 규제와 혁신의 균형을 추구한다는 당위성은 공유하고는 있으나, AI 추격국으로서 국내는 아직 기술개발과 활용성의 제고가 우선적으로 고려되기 때문이다. 또한, 고위험 체계에 대한 인식이 EU의 AI Act와 다른 점도 향후 국내의 법·제도에서 시급히 보완해야 하는 부분이다. 무엇보다 우리는 자율살상무기나 자율주행시스템의 오작동 등 아직 일상과는 거리가 있는 상황에서 벌어지는 물리적 피해만을 AI 기술이 낳는 가장 큰 위협으로 생각해왔다. 그러나 이번 법안은 일상에서 직면할 수 있는 AI 남용의 위험성에 초점을 맞추고 있다. 예를 들어 정보 조작이나 생체 인식 데이터를 사용하여 개인정보를 유출하는 행위, 이들을 유형화하고 평가하는 행위 등은 가장 엄격한 규제가 적용되는 최고 위험군으로 간주 된다. 개인과 집단에 대한 편견을 조장하거나 사회 통합을 해칠 수 있는 결과로 이어질 수 있기 때문이다. 이는 향후 우리의 AI 기업과 개발자에게도 보다 무거운 책무성을 요구할 수밖에 없을 것이다. AI의 사회적 활용 위험성에 대한 기업과 연구생태계 전반의 인식 전환이 시급한 이유이다.

나아가, 올해 9월 서울에서 개최될 제2차 REIAM 회의에서 제시할 의제에서 본 법안의 어떠한 측면을 고려할 것인지에 대한 고민도 필요하다. 물론, 민간·상업 활동 규제에 초점을 둔 EU AI Act와 달리 REAIM은 군사 분야를 대상으로 하나, 이번 법안의 원칙과 AI 위험성에 대한 보편적 기준들을 완전히 배제한 채 논의하기는 어렵기 때문이다. 최근 UN에서 군사적인 목적으로 책임있는 AI를 활용하는 방안들을 지속적으로 검토 중이며, 국제법적 의무에 부합하면서 국제 안보, 안정 및 책임을 저해하지 않는 방안을 모색하고 있다. 제2회 REAIM 회의를 앞두고 있는 우리 정부로서는 EU가 던진 AI Act의 원칙들을

군사 분야에 접목할 경우 제기될 수 있는 쟁점과 보완 사항에 대해서도 신중히 검토하여 의제를 준비해야 하는 상황이다. 특히, 핵심 이해당사국 상당수가 불참하는 불완전한 합의에 머물지 않도록 활용 분야별 민감성을 고려하여 논의를 세부적으로 전개해야 한다. 즉, 이번 EU AI Act를 통해 확인한 핵심 원칙과 위험 기준들을 이견이 적은 분야부터 REAIM에 점진적으로 연계해가는 노력이 요구될 것으로 전망된다. 이를 통해 핵심 참여국들의 수용성을 확보하고 보편적 원칙을 구현해가는 민·관·군의 협력적 AI의 활용 관행을 만들어 나가야 한다.

//끝//