이슈페이퍼 2025-04호

STARTUP ALLIANCE

AI기본법의 발전적 시행을 위한 제언

AI기본법의 발전적 시행을 위한 제언

서울과기대 IT정책전문대학원 김현경 교수

2026년 1월 시행을 앞둔 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 (이하, “AI기본법”)의 시행령(초안)이 지난 9월 8일 공개되었다. 그러나 전문이 국민에게 전면 공개되지 않고 국가AI 전략위원회에 제정 방향만 보고된 점에서, 정부의 깊은 고민이 드러난다. AI기본법 제정 이후, 학계와 산업계는 모호한 규정과 규제 불확실성에 대한 우려를 지속적으로 제기해왔다. 특히, 복잡하고 불명확한 법률 규정의 실질적 집행이 결국 하위법령의 구체적 설계에 달려있는 만큼 시행령 내용에 대한 업계의 관심과 우려가 큰 상황이다. 이에, 본 이슈페이퍼는 AI기본법 시행에 따른 리스크를 최소화하고 실효성을 제고하기 위해 시행령에서 고려해야 할 핵심 사항들을 제안한다. 구체적으로 ▲고영향 AI의 예외 및 해제 기준 마련, ▲정부 주도의 고영향 판단 절차 전환, ▲AI 시스템 정의의 구체화, ▲스타트업 등 중소기업 친화적 준수체계 구축, ▲개발사업자와 이용사업자의 의무 구분, ▲이용자 개념의 명확화, ▲투명성 의무 예외 규정 마련 등을 검토하였다. 이러한 제안은 불필요한 규제 부담을 완화하고 산업 현실을 반영한 합리적 집행 방안을 모색하는 동시에, EU AI Act와의 정합성을 확보하여 국제적 규제 조화 속에서 국내 AI 산업의 경쟁력을 강화하는 것을 목표로 한다.

목차 Table of Contents

1

시작하며

1 시작하며

「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법안」(이하 "AI 기본법")이 2025년 1월 제정되었고, 이제 시행을 4개월 남짓 앞두고 있다.[01] 필자는 이 법이 통과한지 불과 한 달 남짓한 지난 2월 'AI기본법'이 가지고 있는 몇 가지 규제의 문제점과 시행 쟁점 등에 대하여 언급한 바 있다.[02] 이후 황정아 의원 대표 발의로 규제조항에 대한 3년 유예를 규정한 법안이 국회 제출된 바 있으며, 유관 학회에서 아직 시행되지도 않은 AI기본법 개정안을 제안하기도 하였고, 스타트업 등 업계에서는 시행령과 관련된 의문을 연일 제기하고 있는 형편이다.

우리 입법에 단초가 되었던 EU AI법(이하 "AI Act")[03]은 2025년 8월부터 범용인공지능(GPAI) 모델 제공자의 의무 사항을 시행한다. 단, 이 날짜 이전에 시장에 출시되거나 서비스를 시작한 GPAI 모델 제공자는 2027년 8월 2일까지 AI Act를 준수해야 하므로 실질적으로 대상 사업자는 2년여간의 유예기간을 확보한 것이라고 볼 수 있다. 그렇다면 2026년 2월 시행될 우리 AI기본법이 정말 실질적으로는 세계 최초의 시행이라고 볼 수 있다. 최근 EU 내 기업을 포함 40여 개 회사(ASML, 미스트랄, BNP파리바 등)가 2년의 시행 연기 주장하고 있으며, 메타는 AI Act에 따른 GPAI 행동강령에

01 시행 2026. 1. 22., 법률 제20676호, 2025. 1. 21., 제정

02 2025년 2월 19일 국회에서 개최된 "AX발전포럼 출범식 및 정책토론회"에서 "AI기본법 시행 현안"이라는 주제로 발표하였다.

03 European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

대한 서명을 거부한 상태다.[04] 독일 디지털부는 AI 혁신과 발전을 지원하기 위해 "경제적 부담을 완화하고 과도한 규제를 방지 및 줄이기 위한" 논의가 필요하다고 밝힌 바 있으며, 스웨덴의 울프 크리스테르손(Ulf Kristersson) 총리는 이전에 시행되지 않은 AI법 조항의 시행을 일시 중단할 것을 촉구한 바 있다.[05]

과학기술정보통신부(이하 "과기정통부")는 지난 2월 필자 발표 당시 시행령안을 2월에 공개, 의견수렴을 하겠다고 하였으나, 연일 초안 공개를 연일 미루더니, 지난 9월 8일 시행령안 전문을 공개하는 대신 대통령 직속 "국가AI전략위원회"에서 AI 기본법 하위법령 제정 방향을 보고하였다. 시행령안 전문을 일만 국민에게 공개하지 못하고 국가AI전략위원회에 방향성만 보고한 것으로 봐서 정부의 고민도 매우 큰 것으로 보인다.[06] 법은 국회에서 통과시켰으나, 결국 시행을 위한 하위법령을 마련하여 실질적 집행의 방안을 모색하는 것은 정부의 몫이기 때문이다. **'복잡'하고 '모호'하며 '불명확'하고 '민감'한 법은 시행령의 내용에 따라 법의 집행이 완전히 달라질 수 있다.** 다행히 정부는 "인공지능 안전·신뢰 확보를 위한 기본법상 최소한의 의무 규정의 범위와 내용을 구체화·명확화하여, 기업의 불확실성을 완화하였으며, 관계부처와의 협의를 통해 중복·유사 규제도 해소할 계획이다"라고 밝혔고, 덧붙여 "인공지능 기본법 시행 초기 제도의 현장 안착을 위하여 실질적으로 규제 유예와 동일한 효과 달성이 가능한 과태료 계도기간을 운영할 계획이며, 구체적인 운영 방식과 기간 등은 의견수렴을 통해 합리적으로 정할 예정이다. 계도기간 중에는 기업의 투명성·안전성 확보 의무 이행을 위한 자문(컨설팅)과 비용 지원도 해나갈 계획이다"라고 발표했다.[07]

이하에서는 이러한 정부의 움직임에 부응하기 위하여 AI기본법을 둘러싼 문제 상황과 발전방향을 제안하고자 한다.

---

04 GPAI 모델 제공자가 실행강령Code of Practice에 서명하는 것은 자율이나, 서명할 경우, AI법의 의무를 준수하고 있음을 입증하는 데 도움이 될 수 있다. AI위원회는 서명 기관의 규정 준수 여부를 모니터링하며, 비서명자는 자세한 설명이나 격차 분석을 포함하여 독립적으로 규정 준수를 입증해야 하며, 특히 수명 주기 변경 및 모델 수정과 관련하여 AI 사무국에서 더 많은 조사를 받게 된다.

05 https://www.ainet.link/22483 (2025.9.9. 최종 확인)

06 과학기술정보통신부(2025.9.8.) 보도참고자료. 본 자료에 따르면 인공 지능 기본법 하위법령은 9월 중 이해관계자를 대상으로 의견수렴을 거쳐 시행령 초안을 확정, 10월 초 입법예고를 진행하고, 고시·방침(가이드라인)도 시행령과 함께 공개·의견수렴하여 지속 고도화해 나갈 계획이다

07 과학기술정보통신부(2025.9.8.) 보도참고자료.

2

AI기본법 시행을 둘러싼 문제 상황

2 AI기본법 시행을 둘러싼 문제 상황[08]

2-1 사업자 스스로 묻기?, “나는 고영향 인공지능 사업자”인가!

AI기본법상 고영향 인공지능 사업자에 해당한다는 것은 엄중한 규제의 대상이 됨을 의미한다. 우선 고영향 인공지능의 안전성·신뢰성을 확보하기 위하여 위험관리방안의 수립·운영등 법 제34조 제1항 각호에서 정하는 사항(6가지)을 이행하여야 한다. 또한 AI에 기반한 제품 서비스라는 것을 고지하는등 투명성 의무가 부여된다(법 제31조제1항).

이렇듯 고영향 인공지능에 해당한다는 것은 사업의 기획, 개발, 마케팅 등에 큰 영향을 받으며, 투자 여부에도 중대한 요소가 된다. 그런데 이에 대하여 과기정통부장관이 전문위원회의 자문을 받아 확인할 수 있다고만 규정할 뿐, 고영향 인공지능에 해당되는 기준, 확인 방법, 절차 등은 모두 입법 미비이며 대통령령에 위임하고 있다. 즉 **사업자는 고영향 영역이라고 규정된 모호함 속에서 스스로 고영향 인공지능 사업자인지 확인하고, 잘 모르겠으면 과기정통부장관의 확인을 구하는 방식이다.**

08 김현경, “AI 규제 입법의 문제점에 대한 검토-EU AI Act와 한국의 AI기본법간 비교, 분석을 중심으로”, 성균관법학 제37권 제1호(2025.3) 참조

일례로 “범죄 수사나 체포 업무를 위한 생체인식정보(얼굴·지문·홍채 및 손바닥 정맥 등 개인을 식별할 수 있는 신체적·생리적·행동적 특징에 관한 개인정보를 말한다)의 분석·활용”(법 제2조제4호 바목)은 “고영향 인공지능” 영역이다. 그러나 생체인식정보는 엄격히 민감정보로써 이는 법령에 근거가 있는 경우에만 처리할 수 있으므로 이를 처리할 수 있는 자는 일반 사업자가 아니며 수사기관 등 공공기관이다. **수사기관 스스로 이러한 AI제품 서비스를 개발하지 않고 수사기관이 보유하고 있는 민감정보의 처리를 위탁하여 이러한 서비스 개발을 민간 사업자에게 의뢰한다고 가정할 때 이러한 AI서비스 개발을 위탁받은 사업자는 고영향 AI사업자라고 할 수 있는가?** 해당 서비스에서 오는 오류로 인한 국민에 대한 책임은 엄격히 국가기관이 부담하는 것이지 해당 업무를 위탁받아 수행한 사업자가 부담하는 것은 아니다. 이는 공공영역에서 AI제품 서비스를 조달하는 과정에서 해당 서비스의 위중함과 성격에 따라 “고영향”여부를 판단할 문제이며, 일률적으로 단일 법령을 통해 시행령에서 세부사항을 어떻게 규정할 수 있을지 의문이다. “채용, 대출 심사 등 개인의 권리·의무 관계에 중대한 영향을 미치는 판단 또는 평가”(법 제2조제4호 사목)를 제외하면 고영향 인공지능은 대부분 공공영역에서 정부 등이 수행하는 업무에 해당된다. 정부가 직접 개발하는 경우를 제외하면 공공기관 등이 AI 제품·서비스를 구매하기 위한 조달, 개발과정에서 동일 유사한 문제에 봉착하게 된다. 이는 공공영역에서 부담하여야 하는 책무를 정부 조달을 통해 사업자에게 전가할 수 있으므로, 오히려 **공공영역의 AI제품·서비스에 대한 규율은 민간 사업자에 대한 일반적 규제와 구분되어 규율되어야 할 것이다.**

한편 주로 민간 영역의 고영향에 해당될 “채용, 대출 심사 등 개인의 권리·의무 관계에 중대한 영향을 미치는 판단 또는 평가”(법 제2조제4호 사목) 역시 사업자 혼란은 여전하다. **은행이 대출심사 서비스를 직접 개발하여 스스로 사용하는 경우 해당 은행은 “고영향 인공지능 사업자”에 해당하는지, 만약, 이러한 서비스를 외부에 위탁하면 수탁 AI사업자가 고영향 사업자이고 제공받는 ‘은행’은 고영향에서 제외되는지,** 그렇다면 잘못된 대출심사로 인한 편향에 대한 책임은 은행이 아니라, 해당 AI서비스를 제공한 사업자가 부담하는지 등의 불명확성이 존재한다.

‘고영향AI 규정’, 현장은 이렇게 말한다

[고영향 AI 정의와 의무조항은 범용모델·오픈소스 모델의 개발·활용 현실을 반영 못해]

범용모델은 여러 산업·도메인에 사용되는데, 한 용례(예: 특정 산업 안전 매뉴얼 챗봇)라도 고영향에 해당되면 전체 범용모델 개발사가 고영향 관련 의무를 부담해야 하는 구조입니다.

‘학습데이터 개요 설명 의무’(제34조 제1항 제2호)는 현실적으로 이행이 어렵습니다. 범용모델은 공개된 대규모 데이터를 학습하기 때문에, 이를 전부 특정·설명하는 것은 사실상 불가능합니다.

오픈소스 모델 역시 마찬가지라 할 수 있습니다. 예컨대, 이를 의료기기에 적용하면, 고영향 AI에 해당할 가능성이 높지만, 실제 책무 주체가 누구인지 불명확합니다. 현재 법에서는 실제 활용처를 결정하는 ‘이용자’가 수범 대상에서 제외되어, 모델 개발사나 서비스 개발사에게만 책임이 집중되는 구조이기 때문에 규제 형평성 측면에서 심각한 문제가 될 것입니다.

※시행령(초안) 관련 [고영향 AI 기준의 모호성과 확인 절차는 현장에서 큰 부담으로 작용해]

사업자는 자사 서비스가 고영향에 해당하는지 명확히 판단하기 어려워 결국, 과기정통부 장관에게 확인을 요청할 수밖에 없게 됩니다(법 제33조)

그러나 최근 공개된 시행령 제24조에 따르면, 확인 기한은 ‘30일 이내’로 규정되어 있으나, 3일 연장이 가능하고(제4호), 경우에 따라 재확인까지 요구될 수 있는데요, 이 경우, 사업자는 소요기간을 예측할 수 없고, ‘최대 3개월 이상 지연될 가능성’이 있어 사업 일정 수립 및 추진에 중대한 차질이 발생할 우려가 있습니다.

더욱이, 사업자가 고영향 해당 여부를 스스로 확인하기 어려워 과기정통부에 확인을 요청하는 것임에도 불구하고, 시행령은 절차상 사전자율검토 결과 제출을 요구하고 있습니다. 이러한 규정은 제도의 취지와 배치되며, 기업에 불필요한 이중부담을 초래하는 모순으로 작동할 수 있습니다.

※ 본 박스의 내용은 편집자인 스타트업얼라이언스의 수집한 현장 의견으로, 기고자의 견해와 다를 수 있습니다.

2-2 광범위한 “인공지능의 범위”

“인공지능”이란 학습, 추론, 지각, 판단, 언어의 이해 등 인간이 가진 지적 능력을 전자적 방법으로 구현한 것을 말하며, “인공지능시스템”이란 다양한 수준의 자율성과 적응성을 가지고 주어진 목표를 위하여 실제 및 가상환경에 영향을 미치는 예측, 추천, 결정 등의 결과물을 추론하는 인공지능 기반 시스템을 말한다고 규정하고 있다(기본법 제2조제1호 및 제2호). 이 정의는 OECD가 업데이트한 AI 정의를 반영한 것으로 보이지만,[09] AI 시스템의 의미를 사실상 거의 모든 소프트웨어 시스템으로 확장하는 결과를 초래했다.[10] 이는 다음과 같은 이유 때문이다. i) 특정 수준 이상의 자율성이 필요하다는 기준이 없으며, ii) “may(할 수 있다)”라는 표현을 사용함으로써, AI로 간주되기 위해 반드시 배포 후 적응성을 나타낼 필요가 없기 때문이다. 따라서, EU AI Act는 기계 학습뿐만 아니라 논리 기반(logic-based) 및 지식 기반(knowledge-based) 접근 방식에도 적용된다(전문(12)).[11] 그 결과, 예측가능한 시스템인 결정론적 소프트웨어 시스템(deterministic software systems) 역시 고위험 분야에서 사용될 경우 엄격한 규제를 받게 된다. 이에 대해 “EU AI Act는 AI 시스템이 작동하는 방식을 구별하지 않음으로써, 오히려 더 안전하고 통제하기 쉬운 시스템 까지도 간접적으로 제재하고 있으며 이는 진정한 의미의 위험 기반 접근 방식과 정면으로 배치될 수 있다”는 지적도 가능하다.[12]

09 OECD (2024), “Explanatory memorandum on the updated OECD definition of an AI system”, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris. Available at https://doi.org/10.1787/623da898-en (2025.9.9 최종확인).

10 EU AIA Recital (12) AI Act, the only software systems that should not be regarded as AI are “systems that are based on the rules defined solely by natural persons to automatically execute operations”.

11 EU AIA Recital(12) ----enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved.

12 Thibault Schrepel, Decoding the AI Act: A Critical Guide for Competition Experts (ALTI Working Paper, Amsterdam Law & Technology Institute – Working Paper 3-2023, October 2023), p. 11, Available at https://ssrn.com/abstract=4609947 (2025.9.9 최종확인).

2-3 연산량 기반 안전성확보의무 대상자 규정의 문제점

AI기본법 제32조는 학습에 사용된 누적 연산량이 대통령령으로 정하는 기준 이상인 인공지능시스템의 인공지능사업자는 안전성을 확보의무를 이행하여야 한다. EU AI Act 역시 10^{25} FLOPs 이상을 사용한 모델은 자동으로 "시스템적 위험"을 초래하는 고위험 모델로 간주(제51조 제2항)되며, 추가적인 규제를 받는다. 그러나 이러한 기준은 여러 가지 이유에서 타당성이 부족하다.

우선 **연산량(FLOPs)만으로 위험성을 판단할 수 없다.** 모델의 위험성은 단순히 연산량뿐만 아니라 애플리케이션의 맥락, 모델 구조, 학습 데이터의 품질 등 다양한 요소에 의해 결정된다.[13] **다음으로 FLOPs 기준의 설정이 비과학적이다.** 연구에 따르면, 연산량이 적은 모델도 특정 조건에서는 대형 모델보다 더 높은 위험성을 가질 수 있으며, 성능에서도 우수할 수 있음이 밝혀졌다.[14] 무엇보다도 이러한 기준은 정치적 타협의 결과라는 비판이다. FLOPs 기준은 프랑스(미스트랄) 및 독일(Aleph Alpha) 스타트업을 보호하기 위한 정치적 타협의 결과로 설정되었다. 협상 과정에서 두 나라가 10^{25} FLOPs 이하 모델은 "시스템적 위험"으로 간주되지 않도록 로비를 벌였으며, 결과적으로 객관적인 기준 없이 특정 기업을 보호하기 위한 방식으로 규제가 결정되었다.[15] 연산량(FLOPs)만으로 위험성을 판단할 수 없으며 모델의 위험성은 단순히 연산량뿐만 아니라 애플리케이션의 맥락, 모델 구조, 학습 데이터의 품질 등 다양한 요소에 의해 결정된다. 그럼에도 불구하고 우리 AI기본법은 **그나마 연산량의 기준이라도 제시한 EU AIA와는 달리 아예 그러한 기준을 통째로 시행령에 위임한 바 이러한 법률에서 정할 규제적 사항을 대통령령에 포괄위임한 것으로 이 조문 자체는 포괄위임금지원칙 위반이다.**

---

13 Claudio Novelli and others, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' (2024). p.4 Available at https://ssrn.com/abstract=4821952, (2025.9.9 최종확인).

14 Cornelia Kutterer, 'Regulating Foundation Models in the AI Act: From "High" to "Systemic" Risk' (AI-Regulation Papers 24-01-1, 12 January 2024), p.6. Available at https://ai-regulation.com/wp-content/uploads/2024/01/C-Kutterer-Regulating-Foundation-Models-in-the-AI.pdf(2025.2.9 최종확인).; Nicolas Moës and Frank Ryan, "Heavy is the Head that Wears the Crown: A Risk-Based Tiered Approach to Governing General Purpose AI", The Future Society, (September 2023). Available at https://thefuturesociety.org/wp-content/uploads/2023/09/heavy-is-the-head-that-wears-the-crown.pdf (2025.9.9 최종확인).

15 그러나 프랑스는 여전히 현재의 임계값에 만족하지 않고 더 높은 임계값(10-26)을 주장하고 있는데, 미스트랄과 같은 회사들이 가까운 미래에 현재 임계값에 도달할 가능성이 높기 때문이다.

2-4 기타

의무대상이 되는 사업자와 보호 대상이 되는 이용자의 개념이 혼재되어 있으며, 투명성 의무 이행을 위한 기술적 조치 역시 불완전하다. 뿐만 아니라 스타트업 등 소규모 기업이 준수하기에는 지나치게 복잡하고 이행하기 어려운 기술문서나 템플릿등이 마련될 우려도 크다.

3

발전적 시행을 위한 제언

3 발전적 시행을 위한 제언

최근 황정아 의원이 인공지능 투명성 확보의무(제31조), 인공지능 안전성 확보 의무(제32조), 고영향 인공지능의 확인(제33조), 고영향 인공지능과 관련한 사업자의 책무(제34조), 고영향 인공지능 영향평가(제35조)의 시행을 3년 유예한 법안을 제안한 바 있다. AI기본법이 내년 2월 시행을 앞두고 있는 상황에서 이러한 유예법안의 통과는 쉽지 않을 것으로 보인다. 한편 (사)인공지능법학회 등 일각에서는 아직 시행도 되지 않은 AI기본법의 개정안을 발표하기도 한다. 이 역시 시행을 목전에 앞둔 법의 모호성을 해결할 수 있는 현실적 방안은 아닌 듯하다. 이 법은 앞서 언급한 몇 가지 중대한 규제 모호성은 존재하지만, AI정책 추진을 위한 거버넌스와 기반을 마련하였다는 측면에서는 적극 시행이 기대되는 측면도 있다.

그렇다면 이러한 법률의 유용성을 높이면서 리스크를 줄이는 **가장 현실적인 방안은 시행령을 통해 명확성을 제고하고, 시행의 범위를 조율하는 것이다.** EU AI Act 역시 중대한 지침 개발은 대부분 2026년 8월로 예정되어 있는바,[16] 우리 역시 시행령에는 다음과 같은 사정을 고려할 필요가 있다.

16 https://artificialintelligenceact.eu/implementation-timeline/ (2025.9.9.확인)

3-1 고영향 AI의 예외 및 해제 기준 마련

고영향 영역에 해당됨에도 불구하고 AI 시스템이 예외적으로 非고영향 AI 시스템으로 간주될 수 있는 조건에 대한 기준을 개발해야 한다. 일례로 **의도된 목적이 고영향(위험) 아님이 명확한 경우, 결과에 대한 수정이 가능한 경우, 업계에서 스스로 정한 자율적 기술/관리 기준을 준수한 경우, 단지 학문 예술적 표현을 위한 목적인 경우 등은 고영향 영역에 해당되더라도 고영향으로 간주되지 않도록 하는 방안**이다. EU역시 2026년 2월 2일까지 부속서 III(고위험)에 해당하는 AI 시스템이 예외적으로 비고위험 AI 시스템으로 간주될 수 있는 조건에 대한 지침을 개발할 것을 밝힌 바 있다. 한편 **고영향으로 분류되었다가 해제될 수 있는 요건도 구체화하여야 할 것**이다.

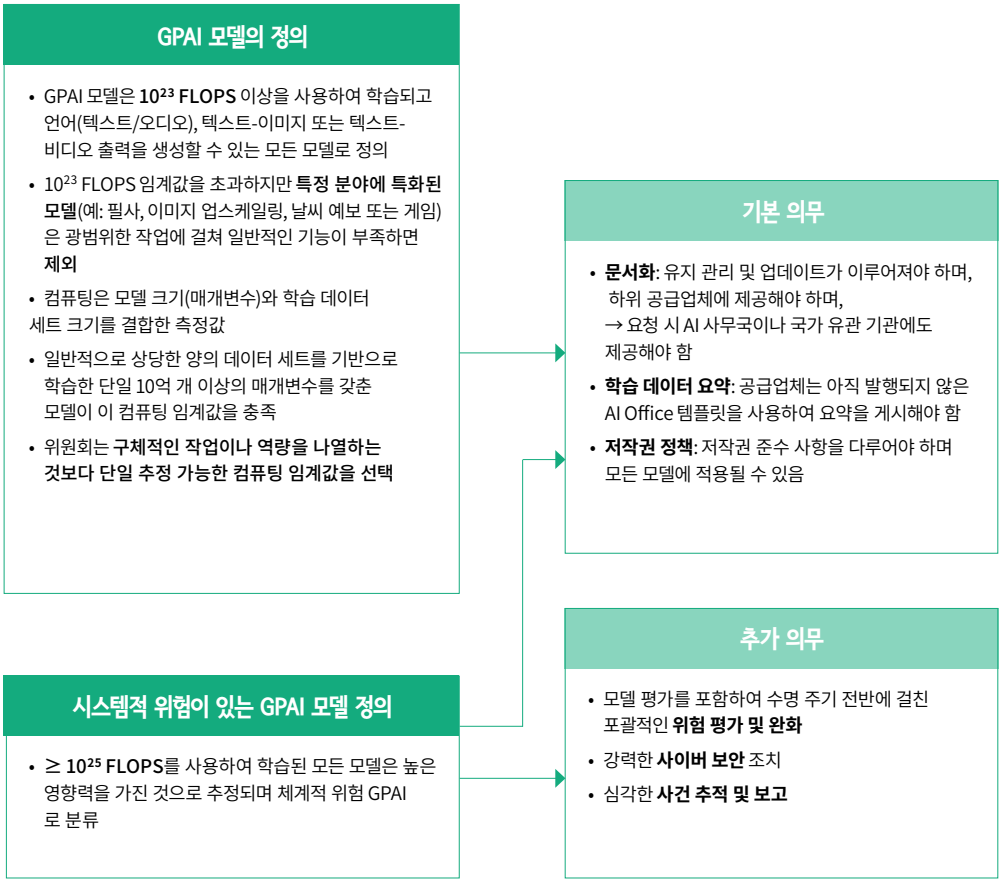
3-2 정부 주도의 고영향 판단 절차 전환

고영향 AI사업자 판단 절차의 구조적 전환이 필요하다. 현재는 스스로 고영향 사업자임을 입증하고 책임져야 하나, **정부는 해당 사업이 고영향에 해당되는지에 대한 사전 체크리스트를 공통기준과 영역별 추가기준으로 구분하여 구체적으로 제시해야 할 것**이다. 체크리스트를 통해 고영향인 경우가 모호한 경우, 고영향이 아닌 것으로 추정하는 방안이 고려될 수 있다. 특히 **모호한 경우 고영향에 해당되지 않기 위한 요건을 제시할 필요도 있다. 뿐만 아니라 고영향 확정에 대한 사업자의 이의제기 또는 재평가 요구권도 보장할 필요가 있다.** 사업자는 해당 제품·서비스가 고영향 AI로 확정된 경우 일정기간내에 재평가 요청할 수 있고 정부는 재평가 실시 및 고영향 여부 및 사유에 대한 구체적 통보 의무를 부담토록 하여야 할 것이다.

3-3 AI 시스템 정의의 구체화

시행령을 통해 AI시스템의 범위를 조정할 필요가 있다. 예측가능시스템인 결정론적 소프트웨어(deterministic software systems)를 제외하고, 특정 수준 이상의 자율성과 적응성으로 범위와 기준을 구체화하는 등 이 법이 적용되는 AI 시스템의 정의에 대한 세부 지침을 마련해야 할 것이다. EU에서 지난 7월 18일 발표한 GPAI모델의 정의 등이 참조될 수 있다.

그림1. EU의 Overview of Guidelines for GPAI Models (2025.7.18.)



3-4 스타트업 등 중소기업 친화적 준수체계 구축

소규모 기업의 요구 사항을 고려하여 간소화된 방식으로 준수할 수 있는 안전 시스템 요소에 대한 기준을 제시하여야 할 것이다. 이러한 기준은 기존 산업별 관련 법령 간의 상호 보완성을 고려하여 정기적으로 업데이트되어야 하고, 이러한 기준을 발표할 때에는 스타트업을 포함한 중소기업 등 이 규정의 영향을 가장 많이 받을 가능성이 있는 부문의 요구에 각별히 주의를 기울여야 할 것이다. 특히 각종 양식이나 기술문서 작성에 있어서 중소기업의 요구에 맞춰 간소화된 문서 양식을 마련해야 할 것이며, 단순화된 방식으로 수행할 수 있도록 템플릿을 개발하는 등 행정적 부담을 줄여야 할 것이다.

3-5 개별사업자와 이용사업자의 의무 구분

AI기본법은 개념정의에서 개발사업자와 이용사업자를 구분하되, 법문의 내용에 반영하지 않고 일률적으로 '인공지능 사업자'라는 용어만 사용하고 있다. 이는 입법의 실수로 오인될수 있으며 이는 법률의 신뢰성 흠결을 야기한다. 따라서 시행령에서는 **개발사업자와 이용사업자를 구분하여 해당 주체별 의무 사항을 구분할 필요가 있다.** 일례로 개발단계에서의 고영향이 이용단계까지 이어지는 경우 고영향 확인은 개발사업자만 부담하고 이용사업자는 면제하되, 개발단계에서 고영향이 아니나, 이용단계에서 고영향인 경우 이용사업자만 확인 주체가 되도록 하는 방안 등 개발사업자와 이용사업자의 범주를 구체화 하고 그 의무도 구분하여야 할 것이다. EU에서 지난 7월 18일 발표한 GPAI모델 제공자 결정 기준 및 책임 할당에 대한 사항을 참조하면 다음과 같다.

그림2. EU의 Overview of Guidelines for GPAI Models (2025.7.18.)

GPAI 모델 제공자 결정

단일 기업(Entity)이 개발

- 기업(Entity) A가 GPAI 모델을 개발하여 EU 시장에 출시하는 경우 A가 제공자.
- 기업(Entity) B가 기업(Entity) A를 위한 모델을 개발했지만 기업(Entity) A가 이를 시장에 출시한 경우 역시 A가 제공자.

저장소 호스팅

- 모델을 저장소(예: Entity C에서 호스팅)에 업로드해도 제공자 상태는 이전되지 않으며 Entity A가 제공자로 유지

컨소시엄 개발

- 컨소시엄이 개발하거나 컨소시엄을 위해 개발한 GPAI 모델의 경우, 사실 관계와 계약 조건에 따라 제공자는 일반적으로 코디네이터이거나 컨소시엄 자체

상류 및 하류 책임 할당
Upstream and downstream responsibility allocation

상류 제공자 (Upstream providers)

- 상류 행위자가 먼저 EU 시장의 하류 행위자에게 모델을 제공하는 경우, 해당 행위자가 제공자가 되며 GPAI 제공자 의무를 충족해야 함

다운스트림 시스템 통합자 (Downstream system integrators)

- 하류 행위자가 GPAI 모델을 AI 시스템에 통합하여 해당 시스템을 EU 시장에 출시하는 경우, 그들은 시스템 제공자가 되며 시스템과 관련된 의무를 충족해야 함

Non-EU origin models

- 모델이 EU 외부에서 공개되었지만 나중에 EU 시장에 배치된 시스템에 통합된 경우, 해당 모델은 그 시점에 배치된 것으로 간주
- 상류 행위자가 EU 사용을 명시적으로 배제하지 않은 한, 해당 행위자가 제공자가 됨. EU 사용을 명시적으로 배제한 경우, 하류 행위자가 제공자가 됨

Downstream modifier가 제공자가 되는 경우

수정에 사용된 학습 컴퓨팅이 원래 모델을 교육하는 데 사용된 컴퓨팅의 **1/3을 초과하는 경우** 다운스트림 액터가 새로운 GPAI 공급자가 됨.

- 모든 GPAI 모델에 대해 10^{23} FLOPS의 ≥ 1/3
- 시스템 위험이 있는 GPAI 모델의 경우 10^{25} FLOPS의 ≥ 1/3

의무 범위

- 수정과 관련된 의무만 적용. 즉, 문서, 학습 데이터 요약 및 저작권 정책은 추가 컴퓨팅 및 데이터에만 적용.
- 그러나 시스템 위험 GPAI 모델을 수정하는 경우, 하류 행위자는 위원회에 대한 통지를 포함하여 모든 체계적 위험 의무를 완전히 순수해야 함

3-6 이용자 개념의 명확화

사업자와 이용자를 구분하는 기준 역시 명확히 하여야 할 것이다. 이 법은 ’이용자‘를 인공지능 제품 또는 서비스를 ’제공받는 자‘를 말한다고 규정하여 “최종 이용자”와 “이용 사업자”의 개념을 혼동되게 규정하였다. 즉 워터마크 표시의무는 ‘사업자 ' 에게 부과되는데, 웹툰 제작사가 웹툰에 AI창작물을 사용하는 경우 이용자인지, AI제품 서비스를 이용한 '이용사업자'인지 모호하다. 또한 회사가 채용AI를 구매하여 내부적으로 사용하는 경우 이용자는 회사로 볼 수 있으나, 실제 보호필요성은 회사가 아니라 채용대상자가 더 클 수 있다. 이러한 의무대상자의 불명확성을 시행령에서 명확히 하여야 할 것이다.

3-7 투명성 의무 예외 규정 마련

투명성 의무 관련하여 인공지능사업자는 생성형 인공지능 또는 이를 이용한 제품 또는 서비스를 제공하는 경우, 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상 등의 결과물을 제공하는 경우 그 결과물이 생성형 인공지능에 의하여 생성되었다는 사실을 표시하도록 규정하고 있다. 그러나 머신러닝을 사용하여 AI 산출물 여부를 판단하는 기술적 수단(GPTzero, OpenAI AI Text Classifier, Copyleaks 등)에 많은 오류가 있는 상황이다. 투명성 의무를 준수하기 위해서는 AI생성물을 인간 생성과 식별하는 기술적 수단이 완비되어야 하나, 현재 상황에서 이러한 기술적 조치는 불완전하다. 따라서 **시행령에서 이러한 고지 또는 표시의 방법 및 그 예외의 범위를 폭넓게 규정할 필요가 있다.** 즉 학문, 예술적·창의적 표현물에 해당하거나 그 일부를 구성하는 경우에는 투명성 의무 예외 규정 마련하거나, 업계 스스로 정한 자율적 고지, 표시 방식을 준수한 경우 예외 사유 인정하는 등의 방안이 고려될 수 있다.

‘투명성 의무 규정’,
현장은 이렇게 말한다

[투명성 의무의 정의와 적용 범위가 모호하여 사업 현장에 혼란을 주고 있어]

‘생성형 AI’ 정의(제2조 제5항)가 지나치게 넓어, 새로운 결과물을 창작하지 않고 LLM 기반으로 단순 요약·번역만 하는 서비스까지 규제 대상이 될 수 있어 사업자는 어떤 서비스가 규제 대상인지, 각 기능에 어떤 의무를 부담해야 하는지 명확히 알기 어렵습니다.

‘의무 범위’ 역시, 불분명한데요, B2C 서비스는 End User에게 직접 고지·표시하면 되지만, B2B2C 모델에서는 비즈니스 고객만 대상으로 하면 되는지, 아니면 최종 End User까지 포함해야 하는지 기준이 명확하지 않습니다.

예를 들어, ‘AI 기반 광고문구 생성’ 기능이 있을 경우, 광고주에게만 AI 활용 사실을 알리면 되는지, 광고를 접하는 소비자까지 고지해야 하는지 불확실한 상황입니다. 이러한 불명확성은 사업자의 규제 대응에 불필요한 부담과 위축을 초래할 우려가 있습니다.

※ 본 박스의 내용은 편집자인 스타트업얼라이언스의 수집한 현장 의견으로, 기고자의 견해와 다를 수 있습니다.

참고문헌

참고문헌

과학기술정보통신부(2025.9.8.) 보도참고자료

김현경(2025.3.), “AI 규제 입법의 문제점에 대한 검토-EU AI Act와 한국의 AI기본법간 비교, 분석을 중심으로”, 성균관법학 제37권 제1호.

Claudio Novelli and others(2024), ‘Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity’ (2024)(Available at https://ssrn.com/abstract=4821952)

Cornelia Kutterer(2024), ‘Regulating Foundation Models in the AI Act: From “High” to “Systemic” Risk’ (AI-Regulation Papers 24-01-1, 12 January 2024), p.6.

EU AIA Recital

Nicolas Moës and Frank Ryan(2023), “Heavy is the Head that Wears the Crown: A Risk-Based Tiered Approach to Governing General Purpose AI”, The Future Society, (September 2023)(Available at https://thefuturesociety.org/wp-content/uploads/2023/09/heavy-is-the-head-that-wears-the-crown.pdf)

OECD (2024), “Explanatory memorandum on the updated OECD definition of an AI system”, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris(Available at https://doi.org/10.1787/623da898-en)

Thibault Schrepel(2023), Decoding the AI Act: A Critical Guide for Competition Experts (ALTI Working Paper, Amsterdam Law & Technology Institute – Working Paper 3-2023, October 2023), p. 11(Available at https://ssrn.com/abstract=4609947)

https://artificialintelligenceact.eu/implementation-timeline/

https://www.ainet.link/22483

발행인 스타트업얼라이언스

기획/제작 스타트업얼라이언스

발행처 스타트업얼라이언스

서울특별시 강남구 봉은사로 215,

11층(논현동, KTS 빌딩)

https://startupall.kr

발행일 2025.9.17

ISSN 2982-4834

STARTUP
ALLIANCE