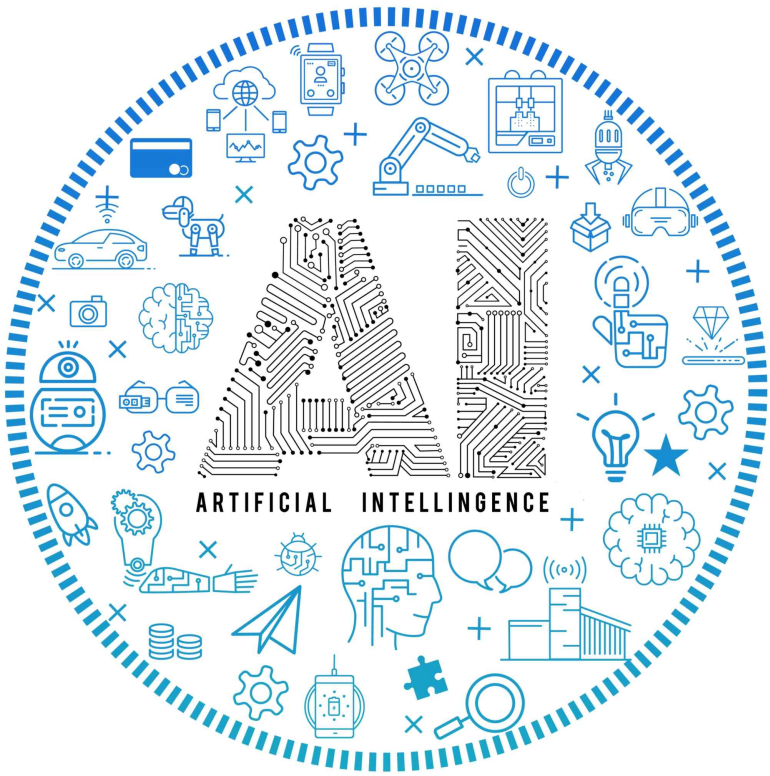
무 역 기 술 장 벽 [T B T] 이 슈 리 포 트 [2 0 2 4 - 0 3 - 0 4]

AI(인공지능) 분야

- EU AI Act -

고위험 (High Risk) 중심으로



산업통상자원부
국가기술표준원

TBT 종합지원센터
R&I Center

이슈 요약

– 가천대학교 조영임 교수–

규제 개요

규제 목적

유럽연합은 주요 국가 중 최초로 인공지능(AI)에 대한 포괄적이고 구속력 있는 규제를 공개하여, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지하고자 함

> **2021년 EU AI Act 초안 발표 배경**
>
> 2021년 4월 21일, 유럽 집행위원회(European Commission, EC)는 EU의 가치, 기본권, 원칙을 존중하고 법적 불확실성을 제거하기 위해 인공지능 사용이 가져올 고위험 요인을 명시하는 한편, 규제로 인해 기술 개발의 과도한 제약요건이 되지 않게 최소 필요조건으로 EU AI Act를 제안함

규제 요지

– 유럽 집행위원회(EC)는 2018년 4월 '유럽을 위한 인공지능'에 대한 커뮤니케이션을 발표한 이후 산업 부문의 디지털 전환정책을 추진

– '미래세대 보호를 위한 법적 과제 4'에 따르면, 유럽연합은 중장기적 정책 기조와 인공지능에 대한 안전 및 책임 문제에 대한 분석 의견을 제시

– 동 법안은 '유럽의 디지털 미래 구상전략' 의견서에서 발표된 정책 방향에 따라 제안

> **유럽의 디지털 미래 구상전략의 3가지 축**
>
> ① **(사람을 위한 기술 전략)** 인간에게 궁극적으로 이로운 방식의 AI 개발 및 사이버 위협으로부터의 보호 등
> ② **(공정하고 경쟁력 있는 디지털 경제)** 온라인 서비스/플랫폼의 규범 확립, 책임 강화 및 유럽 내 기업 간 공정경쟁, 데이터 접근성 보장 등
> ③ **(개방적이고 민주적이고 지속 가능한 사회)** 시민들의 데이터 리터러시를 배양하고 '유럽 건강 데이터 공간'을 구축

적용범위

– 유럽연합 내에서 AI 시스템을 출시하거나 서비스를 도입하는 모든 제공자

– 유럽연합 내에 위치하는 AI 시스템의 사용자

– AI 시스템이 생성한 결과물이 유럽연합 내에서 사용될 시, 제3국에 위치한 AI 시스템의 제공자 및 사용자도 규제 대상

시행일

법안은 2024년 8월 1일 발효되었으나, 실제 적용은 발효일로부터 2년 후인 2026년 8월부터 적용

규제동향 및 현안

주요 내용

- 고위험 AI : 인간의 건강과 안전, 기본권에 미치는 위험 정도에 따라 특정한 시스템을 고위험(high risk) AI 시스템 으로 분류하여 이러한 AI 시스템을 규제함(이하에서 '고위험 AI 시스템'이라고 칭함)
- 부속서(Annex) I과 III에서 고위험 AI 시스템의 종류를 열거하고 있는데, 부속서 I은 주로 그 자체 위험성을 가진 제품들을 규정하는 데 반해, 부속서 III은 자립형 인공지능이 수행하는 기능이 지닌 위험성을 고려하여 규정하고 있음

개념

- AI가 인간의 의사를 조작·착취·사회통제 등에 악용되어 인간의 존엄성, 자유, 평등, 차별금지, 민주주의 및 법치 존중이라는 EU 기본 가치에 위배되는 경우

기준

- ①잠재의식 조작, 기술을 통해 인간의 행동을 조종하는 시스템 ②취약성을 악용하여 인간 행동 왜곡 ③공적인 범용 사회적 점수화 시스템 ④생체 데이터 민감 정보 유추 ⑤법 집행 목적으로 공중에 개방된 장소에서 실시간 원격 생체인식 ⑥범죄 위험 평가 및 예측 ⑦표적화되지 않은 불특정 다수의 얼굴 이미지 처리 ⑧근로자 또는 학생의 감정 자동 인식

시사점 및 대응방안

시사점

- AI 기술의 윤리적인 측면이 강조되면서, 유럽을 포함한 전 세계의 AI 기술 개발이 저해될 수 있다는 우려가 제기되고 있음
- AI 규제 필요성이 증대하는 시점에서 동 법률의 상징성도 크지만, 내용이 방대하고 모호한 부분이 많아 해석 및 실제 이행 방법을 예측하기 어려운 측면이 존재함

대응 방안

- 제조업에서 AI는 예측 유지보수, 품질관리, 공정 자동화 등에 사용됨. 제조 공정에서 수집되는 데이터의 정확성과 신뢰성을 보장하고, 이를 기반으로 한 AI 모델을 개발해야 함.
- 헬스케어 산업에서 AI 기술은 진단, 치료, 환자 관리 등 다양한 분야에서 활용되기 때문에 고위험(High Risk) AI 시스템으로 분류되므로, 데이터 보호, 설명 가능성, 투명성, 안전성 등의 요구사항을 충족해야 함.
- 금융 산업에서는 AI가 리스크 관리, 사기 탐지, 고객 서비스 등에 활용되고 있음. 금융 서비스는 투명성을 강화해 사용자가 AI 시스템을 이해할 수 있도록 설명문을 준비해야 하며, 특히 금융 데이터의 민감성을 고려해 GDPR을 철저히 준수하고, AI 시스템의 리스크 평가 및 관리 체계를 함께 구축해야 함
- 챗봇은 고위험 AI군에 속하지는 않으나 최근 광범위하게 도입되어 사용되므로 투명성을 준수하는 것이 무엇보다 필요함. 특히 사용자가 챗봇과 상호작용하고 있다는 사실을 알 수 있도록 알려야 하고 사용자의 개인정보를 수집하고 처리할 때 GDPR을 준수해야 함

목차

1 규제 개요

규제 개요

규제명

EU 인공지능 법(EU AI Act)*

도입 배경

유럽연합(European Union, EU)은 주요 국가 중 최초로 인공지능에 대한 포괄적이고 구속력 있는 규제안을 공개하였으며, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지

- 유럽 집행위원회(European Commission, EC)는 2018년 4월 '유럽을 위한 인공지능'에 대한 커뮤니케이션을 발표한 이후 산업 부문의 디지털 전환정책을 추진
- '미래세대 보호를 위한 법적 과제 4*'에 따르면, EU는 중장기적 정책 기조와 인공지능에 대한 안전 및 책임 문제에 대한 분석 의견을 제시
  * 미래세대 보호를 위한 법적 과제 4 – 인공지능에 대한 유럽연합의 규제체계와 대응 전략을 중심으로
- 동 법안은 '유럽의 디지털 미래 구상전략' 의견서에서 발표된 정책 방향에 따라 제안됨

> **2021년 EU AI Act 초안 발표 배경**
>
> 2021년 4월 21일, EC는 EU의 가치, 기본권, 원칙을 존중하고 법적 불확실성을 제거하기 위해 인공지능 사용이 가져올 고위험 요인을 명시하는 한편, 규제로 인해 기술 개발의 과도한 제약요건이 되지 않게 최소 필요조건으로 EU AI Act를 제안함

규제목적

유럽연합은 주요 국가 중 최초로 인공지능(AI)에 대한 포괄적이고 구속력 있는 규제를 공개하여, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지하고자 함

- AI 솔루션을 시장에 출시하는 데에 드는 비용을 줄이고, 관련 기술의 개발을 과도하게 방해·제한하는 것을 방지하고, AI와 관련된 위험설 및 문제를 해결하기 위한 최소 요건을 명시함

- 위험 기반 접근방식에 따라 위험성이 높은 인공지능 시스템에 더욱 엄격한 요건 적용
- 위험성이 낮은 AI 시스템에는 가벼운 수준의 의무를, 고위험 AI 시스템에는 영향평가 등 추가적인 의무사항을 적용, 용인할 수 없는 위험성이 있는 인공지능 시스템은 EU 내 사용 금지
- 인지 행동 조작, 소셜 스코어링, 프로파일링 기반 치안 예측, 생체인식정보를 사용하여 인종·종교·성적 취향 등 특정 범주로 사람을 분류하는 시스템 등은 EU에서 사용할 수 없음
- 범용 AI(General Purpose AI, GPAI) 시스템의 경우 시스템적 위험을 내포하지 않은 AI 시스템은 가벼운 수준의 의무를 부과하나, 시스템적 위험을 내포할 경우 추가적인 요건을 준수하도록 의무화

시행일

동 법안은 2024년 8월 1일 발효되었으나, 실제 적용은 발효일로부터 2년 후인 2026년 8월부터 적용

2 규제 경과

EU AI Act 제정 추진 경과

법안 제정 경과

- EU 집행위원회가 2021년 4월 법안 초안을 발의, 2023년 12월 EU 입법 절차상 가장 중요한 관문인 EU 집행위원회, 유럽의회, 이사회 간 3자 협상에서 37시간이 넘는 마라톤 회의 끝에 최종 합의가 이루어짐

- 초안 발의 이후 Chat GPT 등 범용 AI의 등장에 따라 규제가 개정, 범용 AI와 관련된 조항 추가

[표 1] AI Act 제정 경과

일자	주요 내용
2021. 4. 21.	• EC에서 AI Act 법안 발표
2023. 6. 14.	• EC에서 AI 수정 법안 발표
2023. 12. 9.	• 유럽 27개국 정책입안자들 합의(Council of the EU)
2024. 2. 2.	• 유럽의회(European Parliament)에서 AI Act 법안 채택
2024. 3. 13.	• 유럽의회에서 AI Act 법안 제정

규제 목적

EU는 동 법안을 통해 다음과 같은 4가지 핵심 취지에 대해 명시하고 있으며, 이를 규제의 목적과 가치로 삼고있음

① 기술 개발을 과도하게 제한하거나 방해하거나 AI 솔루션을 시장에 출시하는데 드는 비용을 줄이고, AI와 관련된 위험성 및 문제를 해결하는 데 필요한 최소 요건을 명시하기 위함
* 위험 기반 접근방식에 따라 위험성이 높은 인공지능 시스템에 더욱 엄격한 요건 적용

② 위험성이 낮은 AI 시스템에는 가벼운 수준의 의무를 부과하고, 고위험 AI 시스템에는 영향평가 등 추가적인 의무사항을 적용하고 있으며 용인할 수 없는 위험성이 있는 인공지능 시스템은 EU 내 사용 금지

③ 인지 행동 조작, 소셜 스코어링*, 프로파일링 기반 치안 예측**, 생체인식정보를 사용하여 인종·종교·성적 취향 등 특정 범주로 사람을 분류하는 시스템 등은 EU에서 사용할 수 없음
* 소셜 스코어링(social scoring) : 개인의 특성, 행동과 관련한 데이터로 사회적 점수 평가 및 측정
** 프로파일링 기반 치안 예측(predictive policing) : 법 집행 시 잠재적인 범죄 활동을 식별하기 위해 수학적, 예측적, 분석 기법을 사용하여 범죄 예측, 범죄자 예측, 가해자의 개인정보 예측, 범죄 피해자 예측 등에 활용

④ 범용 AI (GPAI) 시스템의 경우 시스템적 위험을 내포하지 않은 AI 시스템은 가벼운 수준의 의무를 부과하나, 시스템적 위험을 내포할 경우 추가적인 요건을 준수하도록 의무화

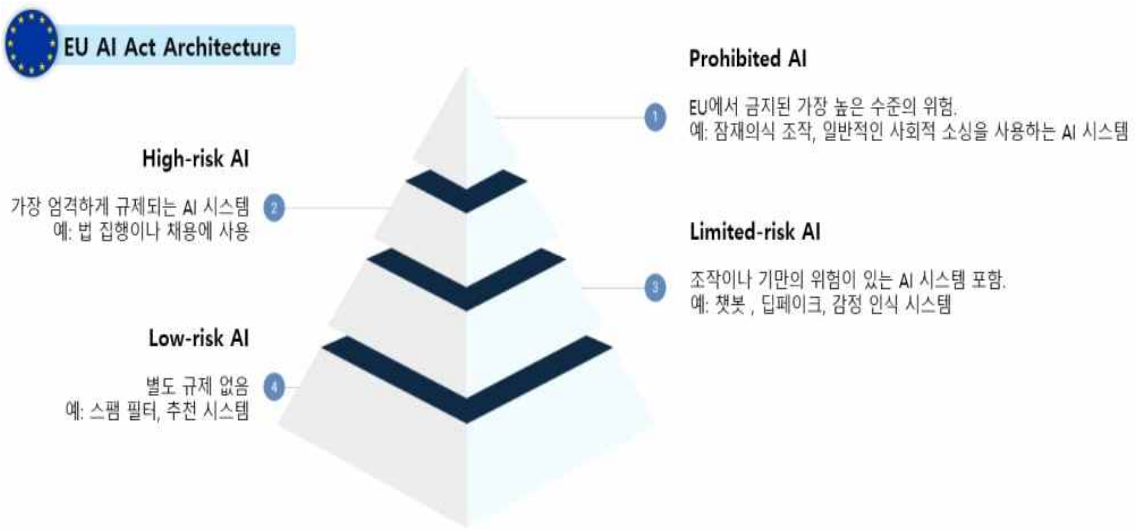
[그림 1] EU AI Act 향후 일정

3 규제 동향 및 현안

EU AI Act 위험 등급 구분

4단계 위험 등급

- EU AI Act는 AI를 사용 목적에 따라 '금지된 AI(prohibited AI)', '고위험 AI(high risk AI)', '제한된 위험을 갖는 AI(limited risk AI)', '최소 위험 AI(low risk AI)' 등 4단계로 구분하며, 위험 수준에 따라 제재 수준도 달리함
- AI 활용 분야에 따라 4단계 위험 등급으로 구분, 그중 '고위험 AI(high risk AI)' 규제가 시장에 가장 큰 영향을 끼칠 것으로 예상됨
- '금지된 AI'는 사회적 차별을 심화하거나 개인의 민감한 정보를 추론하는 AI, 국가의 사회 구성원 감시에 영향을 미쳐 자유나 권리가 침해될 수 있는 유형들로, 원칙적으로 사용이 금지되고 테러리즘 수색 등에만 예외적으로 허용됨
- 따라서 법 집행기관에서 예외적으로 이러한 시스템을 사용할 때, 납치 등 범죄 피해자 수색, 안전을 위협하는 테러 예방 등 그 사용 목적과 경우를 구체적으로 명시하는 것이 필요함



[그림 2] 위험도에 따른 AI 시스템의 분류 및 차등 규제

EU AI Act 고위험 AI

- 현실적으로 시장에 가장 큰 영향을 미치는 것은 '고위험 AI' 분야로서, 미국의 싱크탱크 데이터 혁신센터(center for data innovation)가 발표한 「유럽 AI 규제안에 따른 비용 보고서」는 EU GDP의 35%인 3조 4천억 유로 규모가 고위험 AI 범주에 들어갈 것으로 추정하였음
- 여기에는 중요 인프라 운영, 채용 프로세스나 직원 평가에 사용되는 시스템, 신용평가 시스템, 자동화된 보험 청구 처리 또는 고객을 위한 위험 보험료 설정과 관련된 시스템이 포함됨
- 고위험 AI 시스템을 사용하려면 시장에 출시하기 전 기본권 영향평가(fundamental rights impact assessment)와 적합성 평가(conformity assessment) 등의 평가를 받아야 하며 고위험 AI 시스템들은 EU의 AI 데이터베이스에 등록되어야 하고, 적절한 AI 위험 관리 시스템 운영, 결과 추적을 위한 로그 활동의 기록·관리, 인간에 의한 감독·소유 등 여러 요구사항을 준수해야 함

고위험 AI 관련 조항

- EU AI Act는 제6조에서 제49조까지 고위험(High Risk) AI 시스템의 종류(제6조~제7조), 준수사항(제8조~제15조), 제공자 및 사용자의 의무(제16조~제27조), 통보기관(notifying authorities)과 인증기관(notified bodies)(제28조~제39조), 기준(standards), 적합성 평가(conformity assessment), 인증서(certificates), 등록(registration(제40조~제47조) 등을 규정

- 고위험 AI 시스템에 대한 규제 내용으로는, 위험 관리 시스템 구축(제9조), 데이터 및 데이터 거버넌스(제10조), 기술 문서 작성(제11조), 로그 기록 보존(제12조), 투명성 및 정보 제공(제13조), 인간의 감독(제14조), 정확성, 견고성(robustness), 사이버보안(제15조), 품질관리 시스템(제17조) 등이 있음

- 부속서(Annex) I과 III에서 고위험 AI 시스템의 종류를 열거하고 있는데, 부속서 I은 주로 그 자체 위험성을 가진 제품들을 규정하는 데 반해, 부속서 III은 자립형 인공지능이 수행하는 기능이 지닌 위험성을 고려하여 규정하고 있음. 즉, 부속서 I는 설치형 인공지능, 부속서 III은 자립형 인공지능을 열거하고 있음

범위	의무
제품 안전성 관련 (부속서 II) • AI 시스템 자체가 부속서 II에 열거된 제품(안전 문제로 시장 출시 전 제3자의 적합성 평가를 받아야 하는 대상)에 해당하거나, AI 시스템이 그러한 제품의 안전요소로서 사용되는 경우 • 기계, 장난감, 의료기기, 교통수단 및 설비(차량, 항공기, 선박, 철도 시스템), 농업용 장비 등	시장 출시 전 의무 • 기본권 영향평가: 사용 목적, 사용 지역 및 시간적 범위, 사용으로 인해 영향을 받을 가능성이 있는 개인 및 집단, EU 및 회원국 기본권 관련 법률 부합 여부 및 기본권에 미칠 영향, 소외계층 및 환경에 미칠 수 있는 구체적 위험 등 평가 • 적합성 평가: 자체평가 허용, 제3자 적합성 평가 의무화
보건, 안전, 기본권, 환경 관련 (부속서 III) • 생체인식 범주화 • 핵심 기반시설(전기, 수도, 가스, 교통 등에 사용되는 안전요소)의 관리 및 운영 • 입학사정, 교육, 직업훈련 • 채용, 인사관리, 본질적으로 중요한 공공 및 민간 서비스에 대한 접근·수혜 가능성 판단 • 법률 집행(증거 분석, 금융사기 탐지 등) • 이민, 난민, 출입국 관리	시장 출시 후 의무 • 생성로그 최고 6개월 이상 유지 • 「AI법」 미준수사항 발생 시 즉시 시정조치 및 공급망 내 타 관계자들에게 통지 • AI 오피스와 협력해 법 준수가 입증 가능한 모든 정보와 문서 공유 • 전 수명주기 동안 성능과 안전성을 모니터링하고 지속적인 「AI법」 준수 평가 수행 • 기본권 침해를 유발하는 중대한 사건 및 시스템 장애 발생 시 규제 당국에 보고 • 중대한 변경사항 발생 시 적합성 평가 재실시

[그림 2] 고위험 AI 시스템의 범위와 의무

- EU AI Act는 기술적 요구사항으로 데이터 거버넌스, 프라이버시 거버넌스, 사이버보안을 규정하고 있음

- 이러한 규정을 계기로 기업들은 자사의 각 거버넌스 체계를 종합적으로 재검토해야 함. 기존에는 각 영역별로 부분적인 최적화에 그치기 쉬웠으나, 이제는 이들을 통합적으로 관리하고 고도화해야 할 필요가 있어, 중소기업들에 다소 부담으로 작용할 수도 있음

EU AI Act 부속서 Ⅰ 주요내용

- 부속서 I은 Section A와 Section B로 구성되며, Section A는 주로 현실 세계에서 위험을 일으킬 수 있는 제품에 관한 규정과 지침을 열거하고 있고, Section B는 모빌리티(mobility)를 규정하고 있음

- 부속서 I에서 열거하고 있는 제품들은 고위험과 연결되어 있어서 이러한 제품들에 설치되어 사용되는 AI 시스템도 고위험과 연결되어 있다고 보고 있는데, 이러한 접근은 인간의 생명이나 신체의 안전에 직접적인 영향을 미칠 수 있는 영역에 대한 규제를 강화하려는 의도로 해석할 수 있음

- Section A는 기계류, 완구, 레저용 선박 및 개인용 선박, 승강기, 폭발성 기체 장치와 보호 시스템, 전파기기, 고압기기, 케이블카 설비, 기체연료 연소장치, 의료기기(medical devices), 체외 진단 의료기기 등을 열거하고 있음

- Section B는 민간 항공기, 2륜 및 4륜 차량, 농업 또는 임업용 차량, 철도 시스템, 원동기 차량과 트레일러 및 관련 시스템과 구성 요소, 무인 항공기 및 그 엔진과 프로펠러 및 원격 제어 부품 및 장비 등을 열거하고 있음

  * 고위험 AI 시스템으로 분류될 가능성이 높은 주요 산업으로는 AI 산업 전체의 66%를 차지하는 헬스케어, 금융 서비스, 자동차 및 수송, 제조업 등이 있음

EU AI Act 부속서 Ⅲ 주요내용

- 생체(biometrics) (부속서 III 제1조): EU AI Act에서는 생체 데이터(biometric data)는 특별한 개인 데이터를 구성하므로, 관련 EU법 및 국내법에 따라 허용되는 한도 내에서 생체 시스템(biometric systems)의 사용 사례를 고위험으로 분류됨

- 고위험 AI 시스템에는 생체인식, 중요 인프라, 교육, 필수 서비스, 법 집행, 이주 및 사법에 사용되는 AI 등을 포함(단, 생체인식, 금융사기 탐지 등에 사용되는 AI에는 몇 가지 예외가 적용됨)

  * 고위험 AI 시스템 공급자와 운영자, 수입업자, 유통업자에게 의무가 부과되며 공공 서비스에 활용하거나 자연인의 신용도를 평가하는 경우에는 '기본권 영향평가'를 수행해야 함

  * 고위험 AI 시스템 공급자는 AI 시스템의 시장 출시 전 △위험관리 시스템, △데이터 거버넌스, △기술 명세서, △로그의 기록/관리, △운용 자에 대한 정보 공개의 투명성, △사람에 의한 감독, △그 외 정확성, 신뢰성, 보안 등에 대한 사항을 갖추고 적합성 평가를 받아야 하며, 이에 통과하면 EU 데이터 베이스에 등록해야 함

- 고위험 AI 시스템 공급자는 AI 시스템의 시장 출시 후 △최소 6개월간의 로그 기록 보관, △품질 관리 시스템 운영, △관련 문서의 보관, △시장 출시 후 법에 위배되거나 그렇다고 볼 이유가 있는 경우 필요한 조치를 취하고 당국에 통보해야 함

  * EU AI Act 및 국내법에 따라 사용이 허용되는 원격 생체 인식 시스템(remote biometric identification systems)은 고위험 AI 시스템으로 분류되나(부속서III 제1조 제a항), 특정 자연인이 본인임을 확인하는 것이 유일한 목적인 생체 인증(biometric verification)은 고위험 AI 시스템으로 분류되지 않음

  * 원격 생체 인식 시스템의 경우, 법 집행 목적으로 공공장소에서 '실시간'('real-time')으로 사용하는 것은 원칙적으로 금지되고, 그 밖의 '사후' 원격 생체 인식 시스템은 고위험 AI 시스템으로 분류되어 기록보존 및 인적 감시와 관련된 추가적인 의무가 부가됨

* 민감하거나 보호되는 속성 또는 특성에 따라 생체 분류(biometric categorisation)를 위해 사용되거나, 이러한 속성이나 특성을 추론하는 데 사용되는 AI 시스템은 고위험 AI 시스템으로 분류됨(부속서 III 제1조 제b항)

* 감정 인식(emotion recognition)에 사용되는 AI 시스템은 고위험 AI 시스템으로 분류됨(부속서 III 제1조 제c항). 생체(biometrics) 분야의 고위험 AI 시스템에 대한 시장 감시 당국(market surveillance authority)은 해당 생체(biometrics, 생체정보란 얼굴・지문・홍채 및 손바닥 정맥 등 개인을 식별할 수 있는 신체적 특징에 관한 개인정보를 말함) 분야의 AI 시스템이 법 집행, 이민, 망명 및 국경 통제 관리, 또는 사법 및 민주적 절차의 행정을 위해 사용되는 경우에 효과적인 조사 및 시정 권한을 가져야 함. 즉, 처리 중인 모든 개인 데이터와 업무 수행에 필요한 모든 정보에 접근할 수 있는 권한을 가져야 함. 시장 감시 당국은 완전한 독립성을 가지고 그들의 권한을 행사할 수 있어야 함

해외 규제 동향

미국의 대응 동향

미국은 인공지능 분야에서 글로벌 리더십을 가진 국가지만, 현재 연방정부 차원에서의 인공지능법은 아직 없는 국가임

- 2023년 10월 30일 조 바이든 미국대통령은 AI 행정명령(Executive Order 14110: Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)을 서명함. 바이든 행정부의 126번째 행정명령으로 미국정부가 만든 가장 종합적인 인공지능 거버넌스라고 평가됨. 행정명령은 8개 원칙(①안전과 보안 ②책임감 있는 혁신, 경쟁, 공동작업 ③근로자 지원 ④형평성과 시민권 향상 ⑤소비자 보호 및 보호장치 ⑥개인정보 및 시민권 보호 ⑦연방기관의 AI 위험관리 ⑧효과적인 글로벌 리더십)을 강조함

- 미국의 AI 행정명령에는 크게 두 가지 특징이 있음

* 첫째, 행정명령의 특성상 행정부처에만 적용되는데, 인공지능 개발지원을 위한 업무를 행정부처별로 세부적으로 분담하고 구체적인 지시사항을 명시하고, 가장 중요한 역할은 국가표준기술연구소(NIST)의 인공지능 기술표준의 설정이라고 강조함. 또한 안보, 국가경제, 공중보건, 안전에 3가지 심각한 위험(①생화학, 핵무기 제조, 사용 ②강력한 사이버 공격 ③인간 통제·감독 회피)을 초래할 수 있는 이중용도 파운데이션 모델 개발자는 미국정부에 납품할 경우 훈련 단계부터 고지하고, 정부 전문가팀(AI red-team)의 안전성 평가를 받고, 안전검사 결과 및 기타 중요정보를 미국정부에 보고할 의무가 부과됨

* 둘째, 미국 국무부는 AI 행정명령을 토대로 국제연합(UN) 등의 국제기구에서 미국의 글로벌 리더십 강화에 노력중임

- UN 총회 역사상 최초로 인공지능 분야를 규제하는 결의안이며, 핵심은 인공지능 설계, 개발, 배포 및 이용을 통한 인권 보호 및 17개 지속가능발전목표(SDGs)의 달성임. 미국 국무부가 주도한 결의안을 123개국이 지지했고, 회원국 전체(193개국)의 컨센서스(전원동의)로 투표 절차 없이 채택되었음

- UN 총회 결의는 국제법상 구속력은 없지만 전체 회원국이 만장일치로 찬성했다는 점에서 향후 AI 규제나 거버넌스 체계의 국제표준화 경쟁에서 미국이 주도권을 차지할 것임

국내 정책 동향

○ 한국의 AI 기본법 제정

– 한국의 「AI 기본법」은 EU AI Act보다 규제면에서는 약하지만 미국의 규제 완화 정책과는 반대되는 움직임을 보이고 있음

– 한국의 「AI 기본법」은 '고위험 AI'라는 용어 대신 '고영향 AI'라는 개념을 도입하였는데, '고위험'이라는 부정적 인식을 피하면서도 책임 있는 사용을 요구하려는 의도로 해석됨. 또한 EU AI 규제법처럼 사전 금지된 AI를 명시하지 않고, 정부 가이드라인을 통해 규제를 유연하게 운영하려 한다는 점에서 차이가 있으며, AI 연구개발에 쓰인 비용과 AI 기술 개발 기업에 투자 시 세액 공제를 해주는 내용을 담고 있음

○ 한국의 「AI 기본법」과 EU AI Act 비교

– 한국의 「AI 기본법」과 EU AI Act를 비교하면 다음 표와 같음

– 주요 차이점

* 한국은 산업 육성과 윤리적 활용에 초점을 맞추는 반면, EU는 위험 관리와 안전성 확보를 우선시 하였고, EU는 위험 기반 접근법을 통해 AI 시스템을 세분화하여 각기 다른 규제를 적용하지만, 한국은 포괄적 규제와 가이드라인 중심으로 규제를 설계하는 점이 다름

* 투명성 요구 수준도 EU는 AI 투명성 요건을 명확히 규정하며 사용자에게 AI 사용 사실을 반드시 알릴 것을 요구하지만 한국은 투명성을 권장하나 의무화 수준은 낮음

* 위험 분류 관점에서 보면, EU는 위험에 따라 금지(prohibited risk)에서 규제 제외(minimal risk)까지 세분화하지만, 한국은 아직 구체적 위험 분류 체계가 도입되지 않음

* 산업 육성 지원 관점에서 보면, 한국은 AI 산업 육성을 위한 지원 정책(R&D, 데이터 공유)을 강조하며, EU는 규제 준수를 강조함

– 공통점

* AI 윤리 원칙: 공정성, 투명성, 책임성을 강조

* 국제표준과의 연계: 국제 AI 표준에 부합하도록 국내 정책 설계

* AI 안전성과 신뢰성 확보: AI 시스템의 안전성을 보장하고, 위험을 최소화하려는 목표

구분	한국「AI 기본법」	EU AI Act
제정시기	• 2024년 12월 26일 제정 • 2026년 1월 1일부터 발효	• 2023년 6월 14일 제정 • 2024년 8월 1일 발효
접근방식	• 자율 규제 중심	• 위험 기반 접근법 (risk-based approach)
목적	• AI 기술의 윤리적 사용 및 안전한 개발 보장 • 국가 차원의 AI 산업 육성 및 국제 경쟁력 강화	• AI의 안전성 확보 및 윤리적 사용 보장 • EU 단일 시장 내에서 통합 규제 적용
주요 특징	• 윤리 원칙 제시: 공정성, 투명성, 책임성 등을 기반으로 AI 개발 및 활용 규범 제정 • 자율 규제 중심: 민간의 자율성을 강조하며 AI 기술 발전을 저해하지 않는 방향으로 설계	• 위험 기반 접근법: AI 시스템을 4개의 위험 군으로 분류 - Prohibited risk: 금지 - High risk: 엄격한 규제

	• 산업 지원: AI 스타트업 및 기업에 대한 지원 정책 포함 (R&D 투자, 데이터 인프라 지원 등) • 국내 표준화 연계: 국제표준과 조화를 이루는 국내 AI 표준 제정	- Limited risk: 정보 제공 요구 - Minimal risk: 규제 제외 • 투명성 요건: 사용자에게 AI의 사용 사실과 작동 원리를 명시적으로 알릴 것 요구 • 엄격한 규제: 특히 high risk AI는 데이터 관리, 알고리즘 검증, 사용 환경 평가를 포함한 다중 규제를 적용 • 강력한 감독: 각국의 독립적 감독 기관이 시행을 모니터링
규제적용 대상	• 모든 AI 시스템, 특히 국민 안전 및 복지에 영향을 미치는 서비스	• 위험 군별로 구분하여 차등 적용 • EU 내에서 제공, 사용되는 모든 AI 시스템
위험 분류	• 명시적 위험 분류 없음	• 4개 군 (prohibited, high, limited, minimal risk)으로 위험 분류
규제 초점	• 윤리 원칙 준수, 산업 육성 지원	• 안전성 보장, 데이터 및 알고리즘 검증
투명성 요건	• 일반적 투명성 권장	• 사용자에게 사용 사실 및 작동 원리 공개 의무
감독체계	• 정부 주도, 민간 협력	• EU 차원 감독 + 각국 독립적 기관
표준화노력	• 국내 표준화 우선, 국제 표준 연계	• 국제 표준과 완전한 통합
산업지원	• R&D 투자, 데이터 인프라 지원 포함	• 산업 지원보다는 규제에 중점
운영방식	• 정부 주도, 민간 협력 기반	• EU 차원의 규제 집행 및 개별 국가의 감독 기관 협력

4 시사점 및 대응 방안

시사점

고위험 AI 시스템에 대한 EU AI Act의 요구사항

- 고위험 AI 시스템의 배포자(개인적 비전문 활동 과정에서 시스템을 사용하는 경우를 제외하고 자신의 권한 하에 AI 시스템을 사용하는 사람으로 정의)는 주로 적절한 사용 및 감독에 관한 의무만이 규정되어 있어, 부담하는 의무가 크지는 않음
- 수입업체와 유통업체에도 고유한 의무가 있는데, 예를 들어, 제품 또는 소프트웨어에 AI 시스템이 AI법 및 기타 해당 EU 법률을 준수함을 나타내는 필수 CE 마크가 부착되어 있는지 확인해야 함
- 수입업자, 배포업자 또는 유통업자가 AI 시스템에 자신의 상표를 부착하거나, 이를 실질적으로 수정하거나, 제공자가 예상하지 못한 고위험 용도로 사용하는 경우, 이들은 제공자로 분류되어 법에 따라 고위험 시스템 제공자에게 적용되는 모든 의무를 부담하게 됨
- EU AI Act를 위반한 기업은 최대 3,500만 유로 또는 전 세계 연간 매출의 7% 중 더 큰 금액의 벌금을 부과받을 수 있으며, 위반의 유형과 심각성에 따라 벌금의 크기는 달라질 수 있음

* 규제를 심각하게 위반하는 경우, 해당 AI 시스템의 사용을 중단하라는 명령을 받을 수 있으며, 특히 위험성이 높은 AI 시스템에 적용될 것으로 보임

* 부적절하게 수집된 데이터나 불법적으로 처리된 데이터는 삭제해야 하고, 처리 과정에서도 사용자 동의를 받아야 하며, 그렇지 못할 경우 데이터 삭제 명령을 받을 수 있음

대응방안

EU에 진출하려는 국내 기업들의 대응방안

- EU 시장에 진출하려는 기업은 각 산업별로 필요한 준비 사항을 철저히 준비하거나 현지 기업과 협력을 통한 규제 샌드박스를 활용하는 것이 필요함
- 헬스케어 산업에서 AI 기술은 진단, 치료, 환자 관리 등 다양한 분야에서 활용되기 때문에 고위험(High Risk) AI 시스템으로 분류되므로, 데이터 보호, 설명 가능성, 투명성, 안전성 등의 요구사항을 충족해야 함
- 금융 산업에서는 AI가 리스크 관리, 사기 탐지, 고객 서비스 등에 활용되고 있음. 금융 서비스는 투명성을 강화해 사용자가 AI 시스템을 이해할 수 있도록 설명문을 준비해야 하며, 특히 금융 데이터의 민감성을 고려해 GDPR을 철저히 준수하고, AI 시스템의 리스크 평가 및 관리 체계를 함께 구축해야 함
- 제조업에서 AI는 예측 유지보수, 품질관리, 공정 자동화 등에 사용됨. 제조 공정에서 수집되는 데이터의 정확성과 신뢰성을 보장하고, 이를 기반으로 한 AI 모델을 개발해야 함
- AI 시스템의 성능을 지속적으로 모니터링하고 필요한 경우 즉시 수정할 수 있는 체계를 마련해야 함. 자율주행은 제조업 중에서도 리스크가 큰 업종에 속하는데, 자율주행 시스템이 수집하는 방대한 양의 데이터를 합리적이고 문제없이 처리하고 저장함은 물론 사이버 공격에 대비할 수 있도록 보안 체계를 강화하는 것이 중요할 것임

5 모니터링 출처

기관	내용
유럽표준위원회 (CEN-CENELEC)	CEN-CENELEC JTC 21 '인공 지능' https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/
영국 AI안전 연구원	고급 AI 거버넌스를 가능하게 하는 엄격한 AI 연구 https://www.aisi.gov.uk/
미국의회	인공지능 보안법 발의 https://www.congress.gov/bill/118th-congress/senate-bill/4230?q=%7B%22search%22%3A%22
세계법제정보센터	유럽연합_AI법_영문본(2024.03.13.가결)
KDI 경제교육・정보센터	세계 최초로 통과된 EU「AI법」, 우리 기업의 대응 방향은?, 2024-06
SCMP	홍콩, 최초의 AI 데이터 보호 지침 발표, 더 많은 규정 준수 확인 약속, 2024-06-11
전자신문인터넷 (ETNEWS)	산업부 주도 'AI활용 진흥법' 만든다...6대 분야별 전략 마련, 2024-05-09
한국과학기술 기획평가원	기술동향브리프(2024-150호, 2024 사이버보안: 주요 전략 및 중점 분야)
대통령실 국가안보실	국가 사이버안보전략(2024년 2월, 대통령실 국가안보실)

주 의

○ 본 보고서는 산업통상자원부 국가기술표준원의 무역기술장벽(Technical Barriers to Trade, TBT) 대응 활동의 일환으로 최신 규제 정보를 제공하기 위해 작성되었습니다.

○ 본 보고서는 TBT종합지원센터의 동의 없이 무단 배포 및 변경할 수 없으며, 상업·법률적 판단 근거로 활용될 수 없습니다.

○ TBT종합지원센터에서 운영 중인 KnowTBT 포털을 통해 더 많은 해외 기술규제 정보를 제공 받을 수 있습니다(www.knowtbt.kr).

Tel. : 02-3487-7758 **Fax** : 02-571-0003 **E-mail** : tbt@kotica.or.kr