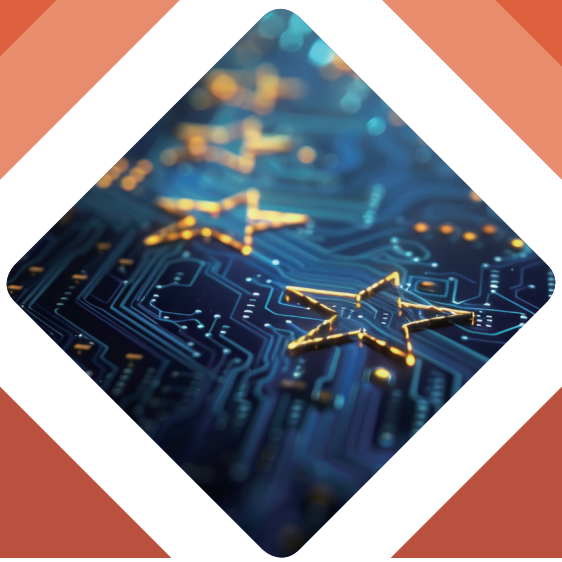
유럽연합 인공지능법(EU AI ACT)의 주요내용 및 시사점

Summary and Implications of EU AI Act



Executive Summary

유럽연합(EU)의 인공지능법(AI Act)은 AI 기술의 급속한 발전과 광범위한 적용에 따른 윤리적, 법적, 사회적 영향에 대응하기 위해 마련된 최초의 포괄적인 AI 규제 법안이다. 이 법은 2024년 3월 유럽의회(EP)에서 통과된 이후 5월 유럽이사회에서 최종 승인했으며, 6개월에서 36개월 후부터 단계적으로 시행될 예정이다.

EU AI법은 AI 시스템을 위험 수준에 따라 분류하는 것이 주요 특징이며, 이 보고서는 AI의 분류의 정의 및 예시와 이에 따르는 의무 사항들을 정리한다. '수용 불가 위험 AI 시스템'은 인간의 존엄성, 자유, 평등, 차별금지, 민주주의 및 법치와 같은 EU의 기본 가치를 위반하는 경우 사용이 전면 금지된다. '고위험 AI 시스템'은 생체인식, 중요 인프라, 교육, 필수 서비스 등 사회적으로 민감한 분야에 사용될 때 높은 수준의 규제를 받게 되며, '제한된 위험성을 갖는 AI 시스템'은 비교적 낮은 위험을 가지고 있지만, 사용자와의 상호작용 과정에서 일정한 투명성이 요구된다. 마지막으로, '저위험 AI 시스템'은 일상적인 상업적 또는 개인적 용도로 사용되며, 비교적 낮은 위험성을 지녀 규제 부담이 최소화된다.

이 법안은 AI 정책 표준을 설정하고, 기업들의 AI 개발 방식을 변화시키며, 윤리적이고 책임 있는 AI 발전에 영향을 미칠 것으로 예상된다. EU의 규제는 종종 글로벌 표준이 되는 경향이 있어, AI법이 전 세계 AI 정책에 미칠 영향이 클 것이다. 기업 차원에서는, EU 내에 법인이나 사무소를 두고 있지 않은 기업도 EU에서 AI 시스템이 이용될 경우 이 법 규제사항을 적용받게 되며, 공급자뿐만 아니라 배포자, 수입업자, 유통업자에게도 의무가 부과되어 광범위한 기업에 영향을 미칠 것으로 예상되므로 면밀한 검토와 대비책이 필요할 것이다.

소프트웨어정책연구소 AI정책연구실 안성원 실장 swahn@spri.kr
산업정책연구실 박강민 선임연구원 gangmin.park@spri.kr
AI정책연구실 장진철 선임연구원 jincheul@spri.kr

The European Union (EU) Artificial Intelligence Act is the first comprehensive AI regulatory bill designed to address the ethical, legal, and social impacts resulting from the rapid development and widespread application of AI technologies. Passed by the European Parliament in March 2024 and subsequently approved by the European Council in May 2024, the Act is set to be implemented in stages, starting between six and thirty-six months from its approval.

A key feature of the EU AI Act is the classification of AI systems based on their risk levels. This report outlines the definitions and examples of these classifications, along with the corresponding obligations. AI systems that pose an “unacceptable risk” are banned entirely if they violate fundamental EU values such as human dignity, freedom, equality, non-discrimination, democracy, and the rule of law. “high-risk AI systems” are subject to stringent regulations when used in socially sensitive areas such as biometric identification, critical infrastructure, education, and essential services. “limited-risk AI systems” carry relatively lower risk but require a certain level of transparency in their interaction with users. Finally, “low-risk AI systems” are used for everyday commercial or personal purposes, involve minimal regulatory burden, and are considered to have relatively low risk.

This Act is expected to set AI policy standards, alter corporate AI development practices, and influence the ethical and responsible advancement of AI. The EU’s regulations often become global benchmarks, meaning the AI Act could significantly impact AI policies worldwide. For corporations, even those without a physical presence in the EU, compliance with these regulations will be necessary if their AI systems are used within the EU. Obligations are not only imposed on providers but also on distributors, importers, and other entities, necessitating thorough review and proactive measures by a wide range of businesses.

I. 서론

■ 유럽연합(EU)의 인공지능법(AI Act)은 AI 기술의 급속한 발전과 광범위한 적용에 따른 윤리적, 법적, 사회적 영향에 대응하기 위한 최초의 포괄적인 AI 규제 법안

- EU는 2021년 4월 집행위원회(EC)의 AI 법안 제안을 시작으로, 2022년 12월 EU 이사회의 검토, 2023년 6월 유럽의회의 수정안 가결됨

- 2024년 6월 이후부터 단계적으로 시행될 예정으로 발효 6개월 후 금지 대상 AI 규정 시행, 12개월 후 범용 AI 모델에, 24개월 후 고위험 AI 시스템에 대한 규제가 시행될 예정

■ EU AI법은 AI 정책 표준을 설정하고, 기업들의 AI 개발 방식을 변화시키며, 윤리적이고 책임 있는 AI 발전에 영향을 미칠 것으로 예상되어 그 중요성이 큼

- (글로벌 표준 설정) EU의 규제는 종종 글로벌 표준이 되는 경향이 있어, AI Act가 전 세계 AI 정책에 미칠 영향이 클 것으로 예상됨
- (기업 활동에 미치는 영향) EU 시장에서 활동하는 기업은 이 법을 준수해야 하므로, 글로벌 기업들의 AI 개발 및 사용 방식에 큰 변화를 가져올 것
- (윤리적 AI 발전) 이 법은 AI의 윤리적 사용과 인권 보호를 강조하여, 더욱 책임있는 AI 기술 발전을 촉진할 것

■ EU AI Act의 주요 내용은 다음과 같음

- (위험 기반 접근법) AI 시스템을 위험 수준에 따라 분류하고, 고위험 AI 시스템에 대해 엄격한 규제를 적용
- (금지된 AI 규정) 기본권을 침해하는 특정 AI 사용을 명시적으로 금지
- (거버넌스 체계) AI 규제를 위한 EU 차원의 거버넌스 구조를 수립

■ 본 보고서에서는 EU AI법의 주요 내용을 살펴보고, 시사점을 도출하고자 함

Ⅱ. 법률 개요 및 추진 경과

1. 목적 및 특징

■ 입법 목적 및 법률체계

- (입법 목적) EU 내에서 사용되는 AI 시스템에 대한 EU의 가치가 일관되게 적용될 수 있는 원칙을 수립하기 위한 것으로, 인간중심의 신뢰할 수 있는 AI의 촉진과 AI 시스템으로부터의 안전, 환경 보호, 법치 등 기본권을 보호하고 혁신을 지원하는 것을 목적으로 함
- (법률 체계) AI법은 113개 규정과 13개의 부속서로 되어있는 방대한 규정

[표 1] 법률 체계

장	제목	
제1장	총칙	
제2장	AI 활용 관련 금지행위	
제3장	고위험 AI 시스템	제1절 고위험 AI 시스템 분류
		제2절 고위험 AI 시스템에 대한 요구사항
		제3절 고위험 AI 시스템 제공자, 배포자 및 기타 당사자의 의무
		제4절 관할 당국 및 신고 기관에 통지
		제5절 표준, 적합성 평가, 인증서 등록
제4장	특정 AI 시스템의 제공자 및 배포자에 대한 투명성 의무	
제5장	범용 AI 모델	제1절 분류 규칙
		제2절 범용 AI 모델 제공업체의 의무
		제3절 시스템적 위험이 있는 범용 AI 모델 제공업체의 의무
제6장	혁신 지원 방안	
제7장	거버넌스	제1절 EU 차원의 거버넌스
		제2절 국가관할 당국
제8장	고위험 AI 시스템을 위한 EU 데이터베이스	
제9장	사후 모니터링, 정보공유, 시장 감독	제1절 시판 후 모니터링
		제2절 심각한 사고에 대한 정보 공유
		제3절 시행
		제4절 구제책
		제5절 범용 AI 모델 제공업체에 대한 감독, 조사, 집행, 및 모니터링
제10장	행동 규약 및 지침	
제11장	권한 위임 및 위원회의 절차	
제12장	벌칙	
제13장	최종 조항	

■ 주요특징

- 27개 회원국 시장에서의 AI 관련 규정을 통일함으로써 AI 규범의 법적 확실성을 확보하는 포괄적 규범의 성격
  - 회원국이 개별적으로 AI 시스템에 대한 규제를 강화하는 것을 방지하여 AI 시스템의 개발, 수입, 또는 운영자에게 법적 확실성을 제공
  - GDPR과 마찬가지로 이 법률의 영토 관할권은 광범위하며, EU의 AI 사용자뿐만 아니라 EU에서 AI 시스템을 시장에 내놓거나 서비스하는 공급자도 관할

    * 일반 개인정보보호법(GDPR): 개인정보의 수집, 처리, 보관에 대한 규제를 강화하여 EU 시민의 데이터 권리를 보호하는 것이 목적이며, 개인정보 처리 동의 요건 강화, 데이터 이동권 보장, 기업의 책임성 강화 등을 내용으로 함

- AI 시스템을 위험성에 기반을 두어 규제를 차별화
  - 위험 개념의 통일성 도모, 위험성의 강도와 범위에 비례하여 규제의 유형을 분류
  - 수용할 수 없는 AI 시스템의 활용을 금지, 고위험 AI 시스템의 준수사항을 규정하고, 이 외에는 투명성 의무를 부과

- EU가 발표한 디지털 서비스법(DSA), 디지털 시장법(DMA), 디지털 거버넌스법(DGA)과 같은 다른 법률과 상호 보완적인 역할하고 있음
  * 디지털 서비스법(Digital Service Act, DSA): 온라인 플랫폼의 투명성과 책임을 강화하여 사용자를 보호하는 것이 목적, 콘텐츠 관리, 광고의 투명성, 사용자 권리 강화 등을 내용으로 함
  * 디지털 시장법(Digital Markets Act, DMA): 대형 기술 회사의 시장 지배력을 제한하고 공정한 경쟁을 촉진하는 것이 목적, 시장 지배적인 플랫폼에 대한 규제 강화, 경쟁 촉진 정책 실행 등을 내용으로 함
  * 디지털 거버넌스법(Digital Governance Act, DGA): 데이터의 접근성 및 공유를 개선하여 데이터 주도형 혁신을 지원하는 것이 목적, 데이터 접근 및 재사용을 위한 거버넌스 구조 확립, 데이터 보안과 개인정보 보호 강화 등을 내용으로 함

2. 정의 및 적용 대상

■ AI 법안은 AI 시스템과 범용 AI 모델을 다음과 같이 정의

[표 2] 관련 정의

용어	정의
AI 시스템	다양한 수준의 자율성을 가지고 작동하도록 설계되고 배포 후 적응력을 발휘할 수 있으며 명시적 또는 암묵적 목적을 위해 수신한 입력으로부터 물리적 또는 가상환경에 영향을 미칠 수 있는 예측, 콘텐츠, 추천 또는 결정과 같은 산출물을 생성하는 방법을 추론하는 기계 기반 시스템
범용 AI 모델	자기 감독을 사용하여 대규모 데이터로 학습된 경우를 포함하여 일반성을 가지며 다양한 고유의 작업을 유능하게 수행할 수 있고 다양한 시스템이나 어플리케이션에 통합될 수 있는 AI 모델 (단, 시장에 출시되기 전에 연구, 개발 및 프로토타이핑 활동에 사용되는 AI 모델은 제외)
범용 AI 시스템	범용 AI 모델을 기반으로 직접 사용하는 것은 물론 다른 AI 시스템과의 통합을 통하여 다양한 목적을 달성할 수 있는 기능을 갖춘 AI 시스템

■ 이 법은 AI 개발자, 공급자(수입 및 유통업체 포함), 배포자 모두에게 적용

- AI 시스템이 운영되는 장소와 AI 시스템이 생성하는 결과물이 EU에서 이용되는 경우 EU 역외의 사업자라 하더라도 EU 시민을 대상으로 제품이나 용역(서비스)을 제공하는 기업이라면 해당 규범이 적용
  * 고위험군의 경우 AI 구매 후 사용 시 배포자에게도 의무 사항 부과

- EU AI법은 EU 전역에 적용되는 법령(Regulation)이고 지침(Directive)이 아니기 때문에 각 회원국의 법령의 상위법으로 적용됨
  - 각 회원국의 국가 법령으로 EU AI법과 상반되는 내용을 담은 조항은 회원국 내에서 법적 구속력이 없게 됨

- 단 AI법은 군사, 국제협약, 연구개발 등 다음과 같은 경우에는 적용하지 않음

  * ① AI 시스템이 군사, 방위 또는 국가 안보 목적으로만 시장에 출시, 운용, 또는 사용되는 경우, ② 제3국의 공공당국 또는 국제기구, 제3국의 공공당국 또는 국제기구가 EU 또는 EU 회원국과 체결한 국제협약에 따라 법 집행 및 사법공조를 위하여 AI 시스템을 사용하는 경우, ③ 시장 출시나 서비스 제공 전 단계의 AI 시스템 또는 모델에 관한 연구, 테스트 및 개발 활동, ④ 과학적 연구개발 목적만을 위해 개발되고 서비스가 제공되는 AI 시스템, ⑤ 순수하게 사적이고 비전문적인 활동을 위하여 AI 시스템을 사용하는 배포자, ⑥ 무료 라이선스 혹은 오픈소스 라이선스로 출시된 AI 시스템 중 금지된 AI 시스템, 고위험 AI 시스템, 또는 범용 AI 시스템에 해당하는 경우를 제외한 AI 시스템

3. 추진 경과 및 향후 일정

■ (EC의 AI 법안 제안) 2021년 4월, EC는 유럽의회와 EU 이사회의 요구에 따라 AI 개발과 활용에 대한 신뢰 확보, 기본권 보장, 이용자 안전 강화 등을 목표로 하는 AI 법안(Artificial Intelligence Act)[1] 제안

- EC는 AI 이용에 따른 위험에 대처하기 위해, 위험 수준에 비례한 접근방식을 채택하여 위험 수준을 '수용 불가 위험', '고위험', '최소위험'으로 분류하여 규제 방향을 설정

■ (EU 이사회의 AI 법안 검토) 2022년 12월, EU 이사회는 EC가 제안한 AI 법안을 검토하고, 목표, 정의, 규제, 적용 대상 등에 관한 입장문[2,3]을 발표하면서 법안 목표를 제시

- AI법 제정의 목표는 유럽을 신뢰할 수 있는 글로벌 AI 허브로 만들고, AI를 사용할 때의 위험과 이점이 균형을 이루는데 초점을 둠

---

1 EC, Proposal for a regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence and amending certain Union legislative acts, 2021.4.21.

2 Council of European Union, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, 2022.11

3 Anna Pingen, Council's Common Position on Artificial Intelligence Act, 2023.1

■ (유럽의회의 AI 법안 검토 및 수정) 2023년 6월 14일, 유럽의회는 EC가 제안한 AI 법안을 검토하고, 생성형 AI 관련 사항을 추가한 AI 법안(수정안)[4]에 대해 본회의에서 투표를 진행하여 가결

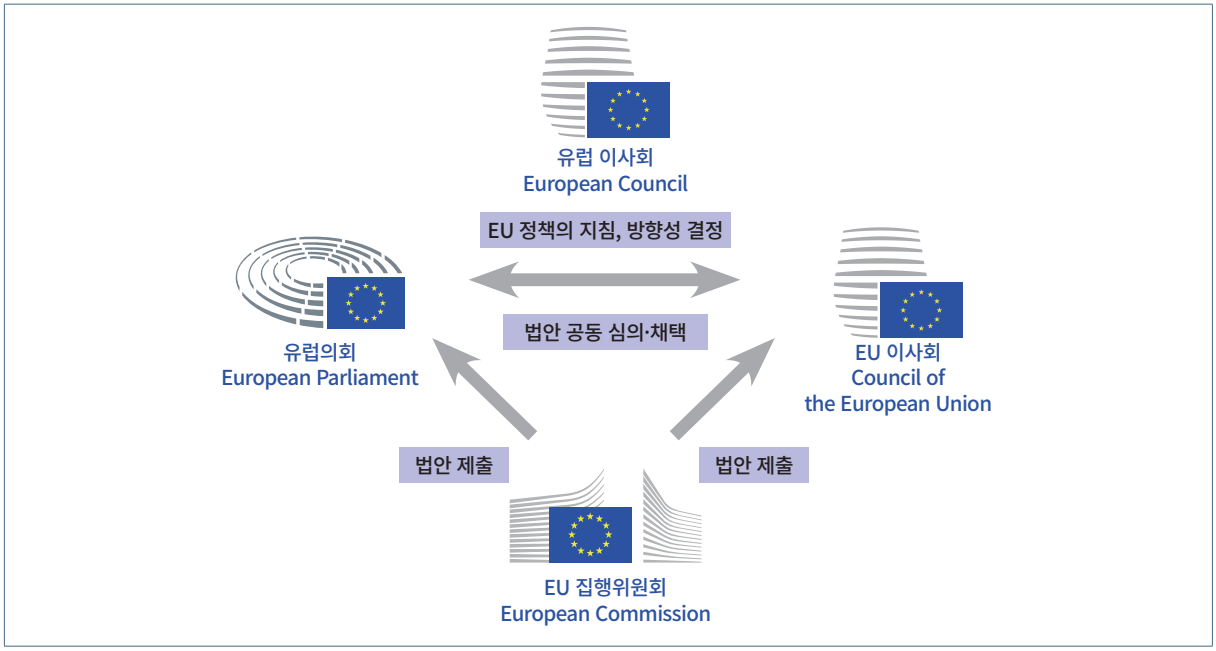
- 유럽의회는 1년 이상 AI 법안을 검토하는 상황에서 챗GPT에 관한 이슈가 긴급하게 대두되면서 AI 규제에 대한 사항을 담은 AI 법안을 본회의 투표에 부쳐 법안을 신속 가결

- 유럽의회에서 가결된 AI 법률 수정법안은 AI의 인간과 윤리적 영향에 대한 유럽 규제 접근방식을 제시

■ (협의) EC, 유럽의회, EU 이사회는 합의를 통해 법률 최종안을 마련하기 위해 약 6개월에 걸친 협의를 거쳐 2023년 12월에 이르러 정치적인 합의에 도달

- 일반적으로 EU는 주요 3개 조직(EC, EU 이사회, 유럽의회)이 3자 협상을 진행하여 새로운 법안에 대한 절충안을 마련하여 최종적으로 법률 제정

[그림 1] EU 주요 3개 조직의 법률 제정 관계도



4 EU Parliament, Amendments adopted by the European Parliament on 14 June 2023 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), 2023.6.14

■ (AI 법안 최종 승인) 2024년 3월 13일 유럽의회가 AI 법안을 최종 채택하고, 이어서 EU 이사회도 5월 21일 AI 법안을 최종 승인

- 유럽의회와 EU 이사회가 AI 법안을 승인함에 따라 EU AI법의 제정은 의장 서명과 관보 게재의 과정을 거쳐 2024년 6월 이후에 규정의 조항에 따라 순차적으로 시행

[표 3] AI법 추진 경과

일정	내용
2021년 4월	• EC, AI 법안 제안 및 공개 자문 개시
2021년 8월	• 유럽의회 시민권 및 헌법 정책국, 윤리적, 법적 관점에서 생체인식 기술 사용 분석 연구 발간
2021년 11월	• EC, 소셜 스코어, 생체인식 시스템, 고위험 앱 관련 변경사항이 반영된 초안을 이사회, 의회 제출
2022년 4월	• 유럽의회 내부시장위원회(IMCO)와 시민자유위원회(LIBE) 보고서 초안 발표
2022년 5월	• EU 이사회, 이미지 및 음성 이해, 오디오 및 비디오 생성 등에 관한 수정안 발표
2022년 9월	• 유럽의회 법제위원회가 검토, 마지막 위원회로서 AI 법안 채택
2022년 12월	• EU 이사회가 AI 법안에 대한 공통 입장 채택
2023년 6월	• 유럽의회, AI 법안에 대해 찬성 499표, 반대 28표, 기권 93표로 통과
2023년 12월	• 유럽의회와 EU이사회 잠정 합의
2024년 2월	• 유럽의회 내부시장위원회 및 시민자유위원회가 71대 8로 회원국과 법안 협성 결과 승인
2024년 3월	• 유럽의회 최종 채택(3월 13일)
2024년 5월	• EU 이사회 최종 승인(5월 21일)

■ 향후 시행 일정

- AI 시스템을 금지된 AI 시스템, 고위험 시스템, 제한된 위험성을 갖는 시스템, 저위험 시스템으로 분류하여 단계적으로 AI법을 적용
  - 총칙 및 AI 활용 관련 금지행위는 발효 후 6개월, 범용 AI 모델 관련 규정은 발효 후 12개월, 고위험 AI 시스템의 경우에는 12개월~24개월, 고위험 AI 시스템 중 부속서 II 관련 규정은 발효 후 36개월부터 시행

[표 4] 위험 등급별 순차적 AI법의 발효

일정	법 제정 과정
2024년 6월	• 유럽의회, EU 이사회 의장 서명 후 관보 게재 및 발효
2024년 발효 직후	• AI 법령 EU 감독기구인 AI 사무소설립을 위한 작업 시작 • 각 EU 회원국은 AI 규제 샌드박스를 제정
2024년부터 법 시행기간 동안	• EU 집행위원회는 법정 기한에 맞추어 AI 법령 의무를 이행하기 위해 집행위원회와 자발적으로 협력할 조직과 함께 AI 협정(Pact)을 개시할 것
법령 발효 이후 6개월: 2024년 4분기~2025년 1분기	• 금지된 AI 시스템 금지조항 발효 및 집행 (Title 1: General Provisions, Title II: Prohibited AI practices)
법령 발효 이후 12개월: 2025년 2분기~3분기	• 파운데이션 모델을 포함한 범용 AI 모델 관련 의무 사항 발효 (Title III, Chapter 4: Notified authorities and notified bodies, Title VI: EU AI Board/ National Regulators, Title VIIIA: GPAI, Title X: Penalties)
법령 발효 이후 24개월: 2025년 4분기~2026년 3분기	• 독립적으로 운영되는 고위험군 AI 관련 의무 사항 발효 + General Application (고위험군 중 36개월 이후로 미루어진 특정 고위험군은 부속서 Ⅰ 참조)
법령 발효 이후 36개월: 2026년 4분기~2027년 3분기	• AI 법령 모든 의무 사항 발효 - Annex II- High Risk AI system used as a safety component of a product covered by EU Harmonisation legislation

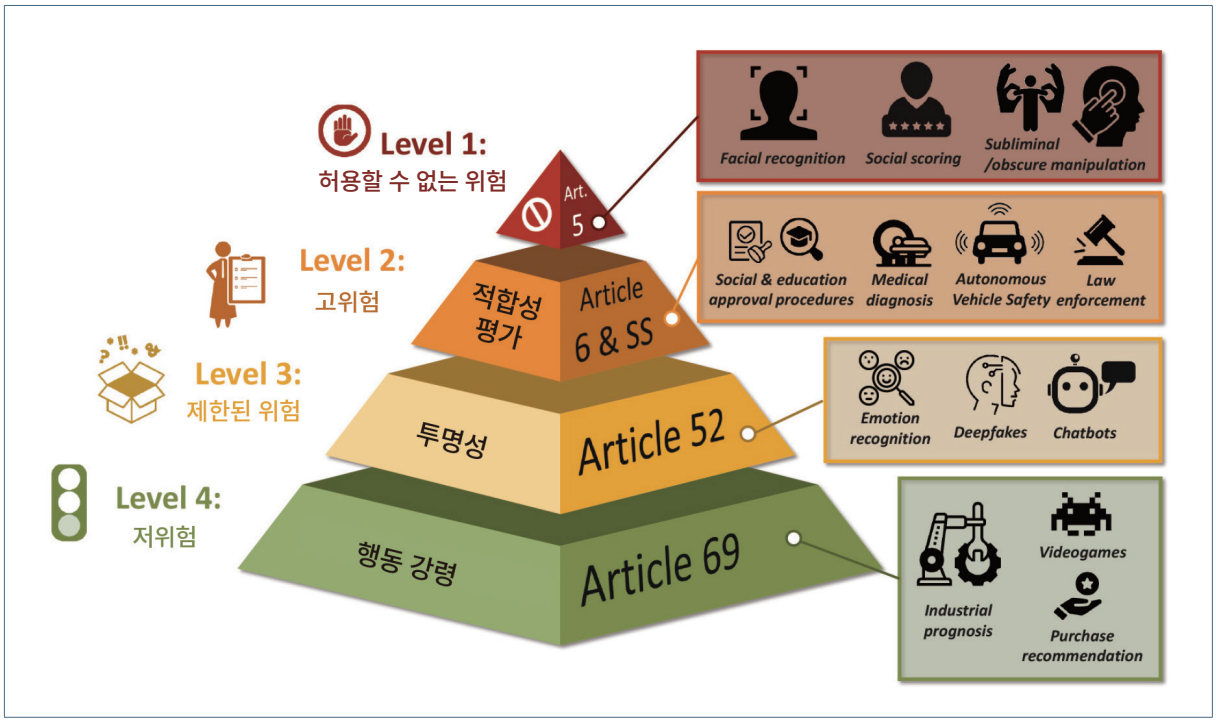
Ⅲ. AI 분류에 따른 주요내용

■ 위험 기반 규제 접근에 따른 수범 대상 별 규제 내용

- AI법은 위험 수준에 따라 AI 시스템에 대한 규제 수준을 차등화하는 위험 기반 접근법(Risk-based approach)을 취함

- 특정한 AI 시스템을 금지하거나 고위험 AI 시스템, 제한된 위험을 갖는 AI 시스템, 최소위험 AI 시스템 등으로 분류하여 차등적으로 규제함
  - AI법에 특정한 AI 시스템 사용례(Practice)는 인간의 건강, 안전, 기본권 등에 중대한 위험을 초래할 수 있어 절대적으로 금지함(이하에서 '수용 불가 AI 시스템'이라고 칭함)
  - 인간의 건강과 안전, 기본권에 미치는 위험 정도에 따라 특정한 시스템을 고위험(High-risk) AI 시스템으로 분류하여 이러한 AI 시스템을 규제함(이하에서 '고위험 AI 시스템'이라고 칭함)
  - 사람과 상호작용하는 AI 시스템 중에서 딥페이크 기술과 같이 비인격화, 기만, 조작 등의 문제를 일으킬 수 있는 기술은 제한된 위험성을 갖는 시스템으로 분류함(이하에서 '제한된 위험성을 갖는 AI 시스템'이라고 칭함)

[그림 2] 위험 기반 구분과 예시



출처: Díaz-Rodríguez et al., 2023

① 수용불가 AI 시스템

- 수용불가 AI 시스템은 의미하는 바와 같이 EU AI법에서 명문으로 규정된 특별한 예외가 없는 한 사용 자체가 금지됨
  - AI 시스템이 인간의 존엄성, 자유, 평등, 차별금지, 민주주의 및 법치 존중과 같은 EU의 기본 가치를 위배하는 경우 공공, 민간을 불문하고 그 사용을 금지함
  - AI법은 금지가 필요한 AI 시스템의 사용 예시(Prohibited Artificial Intelligence Practices)를 규정하고, 해당 AI 시스템이 시장에 출시되거나 서비스가 제공되는 것을 말 그대로 금지함

- 수용불가 AI 시스템 관련 규정을 위반한 경우 최대 3,500만 유로(약 518억 원)와 직전년 회계연도 기준 전 글로벌 연 매출액의 최대 7% 중 더 큰 금액에 대한 제재금이 부과됨

[표 5] 수용불가 AI 시스템 사용 예시

유형	주요 내용
잠재의식 또는 조작적, 속임수 기법으로 인간 의사결정 왜곡, 조작	AI 시스템이 인간의 잠재의식을 이용하거나 의도적으로 조작해 사람이 정보에 기반한 의사결정을 내릴 능력을 현저하게 저해하여 심각한 피해를 초래하거나 초래할 가능성이 있는 의사결정을 내리는데 사용되는 경우
인간의 취약성을 악용하여 인간 행동 왜곡	AI 시스템이 사람 혹은 특정 집단의 취약성(연령, 장애, 사회적 또는 경제적 상황 등)을 악용하여 사람의 행동을 심각하게 왜곡하여 심각한 피해를 초래하거나 초래할 가능성이 있는 경우
개인의 사회점수 (Social scoring) 시스템	AI 시스템이 일정 기간 사회적 행동이나 알려진, 추론된 또는 예측된 개인 또는 성격적 특성을 기반으로 자연인 또는 집단을 평가하거나 분류하는 경우
범죄 위험 평가, 예측	AI 시스템이 자연인이 범죄를 저지를 위험성을 평가 또는 예측하기 위해 사용되는 경우(단, 이 금지 사항은 범죄 활동에 대한 연루를 지원하는 데 사용되는 AI 시스템에는 적용되지 않음)
불특정 다수의 얼굴 이미지 처리	AI 시스템이 인터넷이나 CCTV 영상에서 얼굴 이미지를 비대상으로 스크래핑하여 얼굴 인식 데이터베이스를 생성하거나 확장하기 위해 사용되는 경우
생체인식 분류 시스템 사용	생체인식 분류 시스템을 사용하여 생체인식 데이터를 기반으로 개별 자연인을 분류하여 인종, 정치적 의견, 노조 가입, 종교 또는 철학적 신념, 성생활 또는 성적 지향을 추론하거나 유추하는 경우(단, 이 금지 사항은 생체인식 데이터를 기반으로 합법적으로 취득한 생체인식 데이터 세트에 대한 라벨링 또는 필터링이나 법 집행 분야에서 생체인식 데이터 분류에는 적용되지 않음)
근로자 또는 학생의 감정 자동 인식	직장과 교육기관에서 자연인의 감정을 추론하기 위해 AI 시스템을 사용하는 경우 (단, 이 금지 사항은 의료 또는 안전 목적을 위한 경우는 제외함)
'실시간' 원격 생체인식	법 집행 목적을 위해 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체인식 식별 시스템을 사용하는 경우(단, 이러한 사용이 다음 목적 등에 필요한 경우에는 예외) - 예외 1: 납치, 인신매매 또는 성착취 피해자에 대한 표적 수색 및 실종자 수색 - 예외 2: 사람의 생명 또는 신체적 안전에 대한 구체적이고 실질적이며 임박한 위협 예측 가능한 테러 공격 위협의 예방 - 예외 3: 부속서 II에 언급된 범죄에 대한 형사 수사나 기소 또는 형사 처벌을 집행하기 위한 목적으로 범죄를 저지른 것으로 의심되는 사람의 현지화 또는 식별

② 고위험 AI 시스템

- 부속서 III(Annex III)에서 AI법에 따라 AI 시스템을 '고위험'으로 분류할 수 있는 사례(Case)를 열거
  - 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[5]

5 - 고위험 AI 시스템 공급자는 AI 시스템의 시장 출시 전 △위험관리 시스템, △데이터 거버넌스, △기술 명세서, △로그의 기록/관리, △운용자에 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

- 고위험 AI 시스템 관련 규정을 위반한 경우 최대 1,500만 유로(약 222억 원)와 직전년 회계연도 기준 전 글로벌 연 매출액의 최대 3% 중 더 큰 금액에 대한 제재금이 부과됨

[표 6] 고위험 AI 시스템 사례

구분	주요 내용
생체인식	(a) 원격 생체인식 식별 시스템 (b) 생체인식 분류에 사용되도록 의도된 AI 시스템 (c) 감정 인식에 사용되도록 의도된 AI 시스템
중요 인프라	(a) 중요 디지털 인프라, 도로 교통의 관리 및 운영 또는 물, 가스, 난방 또는 전기 공급에서 안전 구성 요소로 사용되도록 의도된 AI 시스템
교육 및 직업 훈련	(a) 교육 및 직업 훈련 기관에 대한 접근 또는 입학을 결정하거나 사람을 배정하는 데 사용되도록 의도된 AI 시스템 (b) 학습 성과를 평가하는 데 사용되도록 의도된 AI 시스템 (c) 교육을 평가하는 목적으로 사용되도록 의도된 AI 시스템 (d) 학생의 금지된 행동을 모니터링하고 감지하는 데 사용되도록 의도된 AI 시스템
고용, 근로자 관리 및 자영업 접근	(a) 타깃 구인 광고를 게재하고, 구직 신청서를 분석 및 필터링하고, 후보자를 평가하기 위해 사람들을 모집 또는 선발하는 데 사용되도록 의도된 AI 시스템 (b) 사람들의 성과 및 행동을 모니터링하고 평가하는 데 사용되도록 의도된 AI 시스템
필수 개인 서비스 및 공공 서비스 및 혜택 접근	(a) 필수 공공 지원 혜택 및 서비스에 대한 자격을 평가하고 이러한 혜택 및 서비스를 부여, 감소, 취소 또는 회수하는 데 사용되도록 의도된 AI 시스템 (b) 신용도를 평가하거나 신용 점수를 확립하는 데 사용되도록 의도된 AI 시스템 (c) 생명 및 건강보험 대상자의 위험 평가 및 가격 책정에 사용되도록 의도된 AI 시스템 (d) 사람들의 긴급 전화를 평가하고 분류하거나 경찰, 소방관, 의료 지원 및 응급 의료 환자 분류 시스템을 포함한 응급 대응 서비스를 파견하거나 파견 우선순위를 설정하는 데 사용되는 AI 시스템
법 집행	(a) 법 집행기관 또는 관련 지원기관에서 범죄 희생자가 될 위험을 평가하기 위해 사용하거나 대신 사용하도록 의도된 AI 시스템 (b) 법 집행기관 또는 관련 지원기관에서 폴리그래프(거짓말탐지기) 또는 유사한 도구로 사용하도록 의도된 AI 시스템 (c) 법 집행기관 또는 관련 지원기관에서 범죄의 수사 또는 기소 과정에서 증거의 신뢰성을 평가하기 위해 사용하도록 의도된 AI 시스템 (d) 법 집행기관 또는 관련 지원기관에서 범죄 또는 재범 위험을 평가하기 위해 사용하도록 의도된 AI 시스템 (e) 법 집행기관 또는 관련 지원기관에서 범죄 또는 재범 위험을 평가하기 위해 사용하도록 의도된 AI 시스템
이주, 망명 및 국경 통제 관리	(a) 기관에서 폴리그래프 또는 이와 유사한 도구로 사용하도록 의도된 AI 시스템 (b) 기관에서 회원국의 영토에 입국하려는 또는 이미 입국한 사람이 초래하는 보안 위험, 불법 이주 위험 또는 건강 위험을 포함한 위험을 평가하도록 의도된 AI 시스템 (c) 기관이 망명, 비자 또는 거주 허가 신청을 검토하고 신분을 신청하는 사람의 자격과 관련된 불만을 처리하도록 지원하도록 의도된 AI 시스템 (d) 기관에서 이주, 망명 또는 국경 통제 관리의 맥락에서 사람을 탐지, 인식 또는 식별하는 목적으로 사용하도록 의도된 AI 시스템(단, 여행 서류 검증은 제외)
사법 행정 및 민주적 절차	(a) 사법기관에서 또는 사법기관을 대신하여 사실과 법률을 조사하고 해석하고 구체적 사실에 법률을 적용하는 데 사법 기관을 지원하거나 대체 분쟁 해결에서 유사한 방식으로 사용하도록 의도된 AI 시스템 (b) 선거 또는 국민투표의 결과 또는 선거 또는 국민투표에서 투표를 행사하는 사람의 투표 행동에 영향을 미치도록 의도된 AI 시스템

- 한편, 고위험 AI 시스템의 운용자의 경우 △적절한 감독자 지정, △입력 데이터의 관련성과 대표성이 있음을 보장, △모니터링, △최소 6개월간의 로그 기록 보관, △고위험 AI 시스템을 운용자의 사업장에서 사용할 경우 근로자 대표 및 근로자에게 AI 시스템의 사용을 알릴 의무를 부과
- 수입업자와 유통업자의 경우 △EU 적합성 선언 및 사용 지침의 제공 여부 확인 보장, CE마크 부착 여부, △관할 당국에 관련 세부 정보 제공 등의 의무를 부과

③ 제한된 위험성을 갖는 AI 시스템

- 사람과 상호작용하는 AI 시스템 중에서 딥페이크 기술과 같이 비인격화, 기만, 조작 등의 문제를 일으킬 수 있는 기술은 제한된 위험성을 갖는 시스템으로 분류

- 이러한 시스템에는 투명성 의무가 부과되며, 이를 통해 사용자는 AI와의 상호작용을 명확히 인지할 수 있게 되며, 잠재적인 위험으로부터 보호받을 수 있음
  - 투명성 의무란 시스템 제공자가 AI 사용 상황과 맥락을 고려하여, 상대방이 AI 시스템과 상호작용하고 있다는 사실을 인식할 수 있도록 고지해야 하는 의무
  - 합성 콘텐츠(오디오, 이미지, 동영상, 텍스트 등) 생성하는 AI 시스템의 공급자는 결과물을 기계판독이 가능한 형태로 표시하고, 인공적 생성이나 조작을 판별할 수 있도록 해야 함

- 인증기관, 관할 당국에 부정확, 불완전, 오해의 소지가 있는 정보를 제공한 경우 최대 750만 유로(약 112억 원) 또는 직전년 회계연도 기준 글로벌 연 매출액의 최대 1% 중 더 큰 금액의 제재금이 부과

④ 저위험 AI 시스템

- 저위험 AI 시스템의 경우에는 거버넌스 메커니즘을 포함한 명확한 목표와 성과지표에 기초한 자발적인 행동 강령(Code of Conduct) 작성
  - 행동 강령을 고위험 AI 시스템에 적용되는 의무의 일부 또는 전부를 자발적으로 적용하도록 장려

■ 범용 AI 모델에 관한 규제

- 범용 AI 모델(General Purpose AI Model)을 일반적인 AI 시스템과 구분하며, EU 내 대리인을 임명해 규제를 준수
  - 범용 AI 모델 공급자는 AI 개발 및 테스트에 대한 자세한 기록을 보관하고, 지적 재산을 보호하면서도 AI를 사용하려는 다른 회사에 관련 정보를 제공하고, EU 위원회 및 국가 당국과 협력해야 함

- 범용 AI 모델 중에서도 시스템적 위험(Systemic risk)이 존재하면 추가적인 규제 사항 적용
  * 시스템적 위험: 범용 AI 모델로 인하여 EU 시장에 중대한 영향을 미치며 공공 보건, 안전, 안보, 기본권 또는 EU 사회 전체에 실질적으로 또는 합리적으로 예측 가능한 부정적인 영향을 미칠 위험
  - 시스템적 위험이 있는 범용 AI 모델 제공자는 특정 규칙을 준수하고, 표준 프로토콜을 사용하여 모델을 평가하고, 시스템적 위험을 식별하여 줄이고, 심각한 사고가 발생하면 AI 사무소와 국가 당국에 보고하며, AI 모델과 인프라가 안전한지 확인해야 함

- 관련 규정을 위반한 경우 최대 1,500만 유로(약 222억 원)와 직전년 회계연도 기준 전 글로벌 연 매출액의 최대 3% 중 더 큰 금액에 대한 제재금이 부과될 수 있음

■ 규제 적합성 평가

- 고위험 AI 시스템 공급자는 고위험 AI 시스템을 시장에 출시하기 전, 그리고 출시한 후 다음과 같은 적합성 준수사항을 확인해야 함
  - (시장 출시 전) 공급자는 위험관리 시스템, 데이터 거버넌스, 기술 명세서 제작/보관, 결과 추적 로그의 기록과 관리, 배포자에 대한 정보 공개의 투명성, 사람에 의한 감독, AI 시스템의 정확성, 신뢰성, 보안 등
  - (시장 출시 후) 최소 6개월간의 로그 기록 보관, 품질관리시스템 운영, 관련 문서의 보관, AI 시스템이 AI법을 위배한다고 판단되면 조치하고 관련 정보를 배포자, 관련 당국에 통보

- 이러한 절차를 완료하면 CE 마크를 획득하여야 하며, 자체 인증을 통해 적합성을 인증하며, 고위험 시스템의 일부에는 외부 공인 기관의 적합성 검사가 필요
  * CE 마크: 제품이 안전, 건강, 환경 그리고 소비자 보호와 관련된 EU 규격의 조건들을 준수한다는 의미의 유럽 통합규격 인증마크
  - 표준이 제정되지 않은 생체인식 식별 또는 자연인 분류를 위한 AI 시스템과 타 법률에 외부 공인 기관의 적합성 인증이 필요한 경우 외부의 적합성 검사가 필요

- 고위험 AI 시스템에 대해 공급자뿐만 아니라 배포자에게 다양한 의무를 부과
  - 배포자는 감독자 지정, 지정할 의무, 고위험 AI 시스템의 동작을 모니터링하고 필요한 경우 공급자나 관련 당국에 통보, 최소 6개월간 로그 기록 보관 의무, 근로자에게 해당 AI 시스템의 사용 고지 등

Ⅳ. 정책적 지원 및 거버넌스

■ 정책적 지원

- AI법은 규제만을 규정한 법률은 아니며, AI 혁신과 발전에 관해 △규제 샌드박스, △실제 환경에서 테스트, △중소기업과 스타트업 지원의 세 가지 사항을 규정
  - (AI 규제 샌드박스) EU는 회원국이 국가 차원에서 시장에 출시되기 전에 AI 시스템을 개발, 테스트 및 검증할 수 있는 환경으로 AI 규제 샌드박스를 만들 것을 요구

- (실제 환경에서 테스트) 고위험 AI 시스템 공급자(잠재적 공급자 포함)는 AI 법안에 규정된 모든 조건을 충족한 경우에는 규제 샌드박스가 아닌 실제 환경에서도 테스트할 수 있음
- (중소기업과 스타트업 지원) EU 내에 설립된 중소기업/스타트업에 관하여 AI 규제 샌드박스에 대해 우선적인 이용 기회를 제공하는 등의 혜택을 부여

■ 거버넌스 : 집행기관 및 자문단 구성·설치

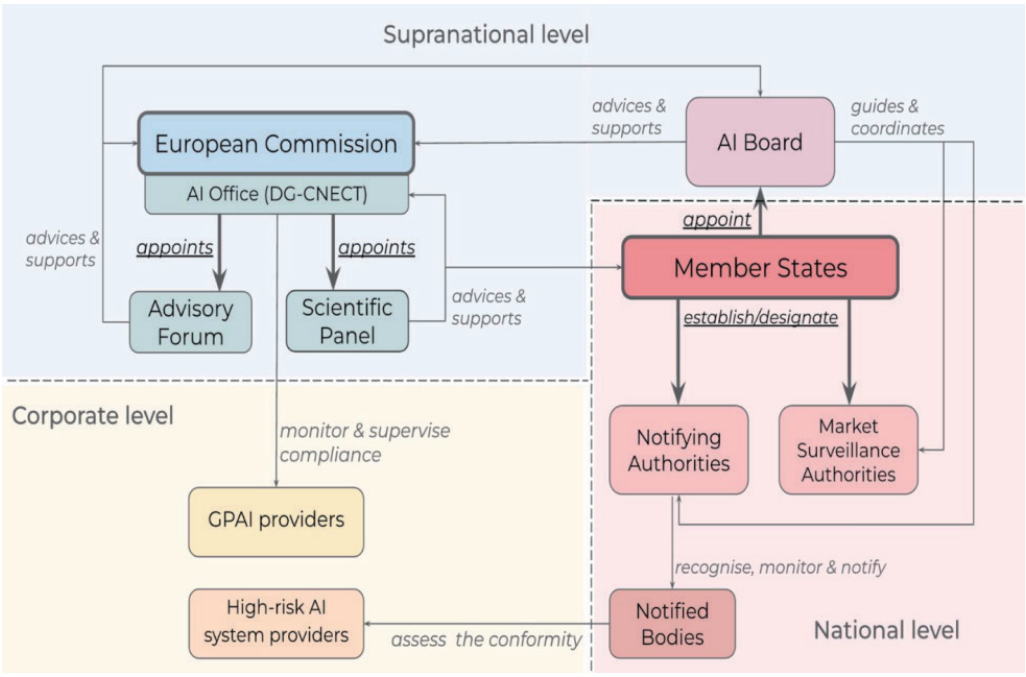
- (EU AI 이사회, EU AI Board) 회원국의 관련 기관 대표, 유럽 데이터 보호 감독관 및 EU 집행위원회의 고위급 대표로 구성

- (EU AI 사무국, EU AI Office) EU 집행위원회 내 기능적으로 독립된 기관으로 EU 역내 AI 전문지식과 역량을 보유한 전문가로 구성

- (독립적인 과학전문가패널, Scientific Panel) EU AI 사무소 활동을 지원하기 위한 독립적인 전문가로 구성된 과학 패널

- (자문단, Advisory Forum) 산업계(빅테크, 스타트업, 중소기업), 학계, 시민사회대표로 구성해 EU AI 이사회에 기술적 전문지식과 의견 제공

[그림 3] EU AI Act 구현 및 집행에 관여하는 기관



출처: Novelli et al., 2024

Ⅴ. 결론 및 시사점

■ EU AI법의 제정은 전 세계적으로 AI 시스템에 대한 법적 규제 강화와 표준화의 시작을 의미하며, 다양한 국가들이 EU의 규제를 참고하여 자국의 AI 규제 정책을 수립할 가능성이 높음

- EU AI법은 AI 시스템의 윤리적 사용과 안전성에 대한 글로벌 기준으로 설정되면서, 다른 국가들이 유사한 규제를 도입하거나 EU의 규제를 준수하도록 요구하는 압력으로 작용할 수 있음

■ 기업 차원에서는 EU AI법에서 명시하는 수용 불가 AI 시스템이나 고위험 AI 시스템에 대한 규제 사항에 대해 면밀한 검토 및 대비책 마련 필요

- 특히, EU 내 법인이나 사무소를 두고 있지 않은 기업도 EU에서 AI 시스템이 이용될 경우 법의 적용을 받게 되며, 공급자뿐만 아니라 배포자 모두에 대한 의무가 존재해 광범위한 기업에 영향을 미칠 것

- 이를 위해서는 향후 EU 시장 내에 점진적으로 안착되는 과정과 규제의 효과, 분쟁 양상을 면밀하게 추적할 필요가 있음
  * 글로벌 빅테크 기업들은 이미 EU의 디지털서비스법(DSA)과 디지털시장법(DMA) 시행에 대규모 자원을 투입하여 대응책을 마련한 바 있음(Mackrael & Schechner, 2023)
  * EU는 DMA에 의거 삼성전자와 구글의 협력이 다른 AI 개발사 접근을 차단했는지 검토하겠다는 계획을 밝힌 바 있음 (YTN, 2024.7.2.)

■ EU AI법에서 수용 불가 AI 시스템으로 분류된 경우, 이러한 시스템은 특별한 사정이 없는 한 EU 역내 시장에 출시 자체가 금지되며, 고위험 AI 시스템에 대해서는 개발자와 배포자에게 높은 수준의 의무 사항을 규정함

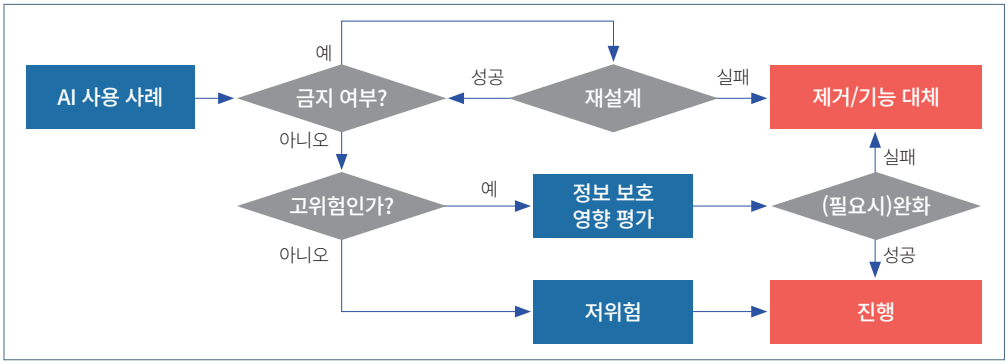
- 국내 고위험 AI 시스템의 개발자는 AI 시스템의 안전성과 신뢰성을 보장하기 위해 위험관리 시스템, 훈련 데이터의 품질 등 다양한 요건들에 대한 고려가 필요

- 국내 고위험 위험 AI 시스템의 배포자는 시스템의 안전한 사용을 보장하기 위한 지침을 준수해야 하며, 시스템의 성능과 안전성을 유지하고, 오작동에 대한 대비책 마련 필요

EU AI법 관련 기업의 대비 방안[6]

- AI 사용 사례를 평가할 때 고려해야 할 아래와 같은 질문에서 대답이 '예'인 경우가 있으면, 해당 AI 시스템은 수용불가 AI 시스템으로써 신중히 고려
  - 사용자의 감정을 인식하기 위해 AI 기능을 사용하는가? (예: 학생의 수업 집중도를 평가하기 위한 CCTV)
  - 안면 인식 데이터베이스를 구축하거나 보완할 목적으로 AI 기능을 사용하여 인터넷이나 CCTV 영상에서 안면 이미지를 무작위로 수집하는가?
  - 프로파일링이나 성격 특성 평가 등 AI 기능을 사용하여 개인이 범죄를 저지를 위험과 같이 개인을 판단하거나 예측하는가?
  - 사용자 개인 데이터에서 특정 분류를 예측하기 위해 생체인식 분류 목적의 AI 기능을 사용하고 있는가? (예: 통계 및 마케팅 목적으로 비디오에서 성별/인종 특성을 추출하여 활용)
  - 개인의 행동을 조작하고 해를 끼칠 수 있는 취약성(예: 연령, 장애 또는 기타 사회 경제적 특성)을 활용하는 AI 기능을 사용하고 있는가? (예: 이미지로 노인층을 식별하는 AI 모델)
  - 해롭거나 불리한 대우로 이어질 수 있는 점수를 할당하기 위해 AI 기능을 사용하여 개인의 사회적 행동이나 특성을 추적하고 있는가?

- 기업은 AI 사용 사례에 대해 금지 및 고위험 여부를 판단하여, 완화를 통한 제거 및 기능 대체 여부 혹은 그대로 진행해도 될지에 대해 판단할 필요가 있음
  - 고위험 AI일 경우, GDPR에 정의된 정보보호 영향 평가를 통해 기본 개인정보 보호 기준을 준수



- 기업의 정보책임자(CIO)는 법무 담당자와 협력하여 AI 규정 준수 및 책임 있는 AI를 위한 노력을 주도하여 고객과 직원의 신뢰를 구축해야 함
  - CIO는 고위험 범주에 속하는 AI 시스템을 식별하며, 사용된 데이터가 윤리적으로 확보되었는지, 개인정보 보호법을 준수하는지 확인해야 함
  - 수용 불가 AI 시스템 사용 사례에 대해서는 완화할 방안을 제시하며, 계획, 개발, 검증, 배포, 검토, 모니터링, 피드백 및 개선을 포함한 AI 모델의 개발과 운영 전 단계의 위험성을 확인
  - CIO는 EU AI법 준수를 보장하기 위해 직원을 포함한 모든 이해관계자와의 투명성과 참여를 촉진하는 임무를 수행하며, 개인정보 보호를 위한 기술을 이해하고 도입할 필요가 있음

6 Gartner (2024), "Getting Ready for the EU AI Act, Phase 2: Risk-Assess & Categorize." 및 Gartner (2024), "Quick Answer: How Bank CIOs Can Align Their AI Strategies With the EU AI Act." 저자 재구성.

참고 주요국 AI 법률 및 규제 현황

■ 미국

- (국가 AI 이니셔티브법 제정) 바이든 정부 출범 후 'AI 이니셔티브법(The National AI Initiative Act of 2020)'을 제정('21.1)해 AI 기술의 다차원적 영향에 대응
  - 백악관 과학기술정책실(Office of Science and Technology Policy, OSTP)은 이 법에 의거하여 '국가 AI 이니셔티브실(National Artificial Intelligence Initiative Office, NAIIO)'을 출범시켜 국가 AI 정책을 마련[7]
- (AI 권리장전에 대한 청사진 발표) 미 백악관은 AI 기술의 개발과 사용 과정에서 발생할 수 있는 부작용을 최소화하기 위해 'AI 권리장전에 대한 청사진(The Blueprint for an AI Bill of Rights)'을 발표('22.10)하여 AI 윤리 지침 정립[8]
  - ① 안전하고 효과적인 시스템, ② 알고리즘에 의한 차별로부터 보호, ③ 데이터 개인정보 보호, ④ 사전고지 및 설명 적시, ④ 인적 대안, 고려 및 대체를 기본 원칙으로 제시
- (AI 행정명령 공표) 바이든 대통령은 AI 기술의 투명성 향상과 새로운 기준 마련을 주요 목표로 하는 'AI 행정명령(Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence)'을 발표하고 이에 기반한 후속 이니셔티브 발표('23.10)[9]
  - 이 행정명령은 AI 권리장전(AI Bill of Rights)을 확장하여 구체적이고 실행 가능한 조치를 수립하는 데 중점
  - 행정명령에 따라 국가 안보, 경제 안보, 공공 안전 등에 영향을 미치는 AI 모델은 훈련 단계부터 정부에 고지해야 하며 정부 검증 전문가팀(AI 레드팀)의 안전성 평가를 거쳐 결과 보고[10]
    * 국립표준기술연구소(NIST)와 에너지부(DOE) 등을 대상으로 AI 시스템의 안정성, 보안, 신뢰성 확인을 위한 표준, 도구, 테스트 개발 권고
  - 행정명령에 기반한 신규 후속 이니셔티브로 NIST 내 미국 AI 안전연구소(The US AI Safety Institute, US AISI) 신설, 미국 정부의 AI 사용으로 인한 위험관리 방향을 제시한 AI 활용에 대한 정책 이행 가이드라인 초안 공개
    * 사람이 만든 콘텐츠 인증, AI 생성 콘텐츠에 대한 워터마크 표시, 유해 알고리즘 식별 등에 대한 규칙을 제정하고 시행에 필요한 기술 가이드라인 개발을 통해 적극적인 AI 규제 시행 의지 표명
  - 행정명령이행을 위해, 2024년 1월, 미국 국립과학재단(NSF)은 연구자들에게 책임감 있는 AI 연구를 위한 리소스를 제공하는 NAIRR 파일럿(National AI Research Resource Pilot)을 시작[11]
    * NAIRR 파일럿은 안전하고 신뢰할 수 있는 AI를 발전시키기 위한 AI 연구뿐만 아니라 의료, 환경 및 인프라 지속가능성 문제에 대한 AI 적용을 지원하며 교육자들에게 AI 기술과 책임 있는 접근방식에 대한 교육을 가능하게 하는 인프라 제공
- 2024년 2월 바이든 정부는 특정 민감한 개인 데이터 및 정부 관련 데이터를 중국을 포함한 관련 국가로 전송하는 것을 제한하는 행정명령을 발표하여 AI 관련 위험에 대응하고 민감한 데이터를 보호하기 위한 추가 조치 수행[12]
  * 해당 행정명령은 AI 기능과 알고리즘의 개발이 관련되지 않은 여러 데이터 세트의 패턴을 인식하고 잠재적으로 데이터 익명화를 해제하는 등 "관심 대상 국가"에 의한 대량의 민감한 데이터 수집과 관련된 위험을 악화시킨다는 점에 주목하여 AI와 관련된 위험을 관리하고 완화하려는 바이든 행정부의 조치로 해석됨

---

7 국립외교원 외교안보연구소, "바이든 행정부의 인공지능 국가정책: 평가와 함의", 2021.12

8 법률신문, "해외 디지털 기본권 추진 동향", 2024.02

9 FACT SHEET: VIce Presdient Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence, 2023

10 법률신문, "미국과 영국의 AI 규제 동향", 2024.02

11 NSF, "Democratizing the future of AI R&D: NSF to launch National AI Research Resource pilot", 2024.01

12 White & Case, "New Executive Order Seeks to Protect Americans' Sensitive Personal Data", 2024.03

- 입법적인 측면에서 미국은 아직 포괄적인 AI 규제 법안이 제정되지 않았으나, 현재는 연방 정부, 주 정부, 업계 자체, 법원이 혼합하여 관리 중

■ 중국

- (AI 입법 의지 공표) 2023년 6월, 중국 최고 통치기구인 국무원은 AI법을 입법 의제로 삼겠다고 발표
  - 이전의 중국은 AI를 전체적으로 규제하기보다는 새로운 AI 제품이 등장할 때마다 개별 법안을 발표하는 형태로 단편적이고 세분화된 규제 시행
    * 예컨대 "인터넷보안법", "데이터보안법", "개인정보보호법", "인터넷 정보 서비스 알고리즘 추천 관리 규정", "인터넷 정보 서비스 딥페이크 관리 규정" 등 산발적인 법률 제정을 통해 AI에 따른 리스크에 대응
- (생성형 AI 서비스 관리 잠정방법에 관한 법률 공포 및 시행) AI에 대한 감독을 강화하기 위해 생성형 AI에 대한 최초 규제인 '생성형 AI 서비스 관리 잠정방법' 시행('23.8)[13]
  - 해당 법률은 생성형 AI의 건전한 발전과 표준화된 적용 촉진, 국가 안보와 사회 공공 이익 수호 및 권익 보호를 위해 제정되었으며, 중국이 중시하는 가치에 반하거나 사생활, 개인정보 등 개인의 권리를 침해하는 콘텐츠를 규제하는 등 생성형 AI로 생산되는 콘텐츠의 규제를 그 주된 내용으로 함
  - 기술개발 촉진을 위한 지원사항을 제시하여 생성형 AI 혁신과 발전을 장려하는 한편, 보안평가, 데이터 훈련·라벨링, 콘텐츠 관리 및 표기, 개인정보 보호, 운영상 규제 등 생성형 AI 서비스 제공·이용 전반에 대한 의무 사항을 명확하게 제시
    * 중국은 앞서 발표되었던 초안에 명시된 처벌 규정을 삭제하는 등 완화된 규정을 발표하며 미·중 기술패권 경쟁 속 중국 산업 발전을 지원하는 방향으로 선회
    * 중국 AI 기업은 모든 기반모델에 대해 중국 대중에게 공개하기 전에 중국 정부에 등록하여야 하며, 외국 기업은 중국 내에서 제품 출시 승인을 받지 못함(중국은 자국 기업을 보호하고 경쟁을 억제)
- (글로벌 AI 거버넌스 이니셔티브 발표) 중국은 '글로벌 AI거버넌스 이니셔티브' 발표('23.10)를 통해 글로벌 규칙과 표준에 대한 리더십 구축 시도
  - AI 기술의 공정한 활용을 강조하여 상대적으로 개발도상국의 이해관계를 중시하는 경향을 보임[14]
    * 중국은 앞서 2021년 글로벌 발전 이니셔티브(GDI), 2022년 글로벌 안보 이니셔티브(GSI), 2023년 3월에는 글로벌 문명 이니셔티브(GCI)를 각각 제안했으며, 중국 외교부는 이번 '글로벌 AI 거버넌스 이니셔티브'가 앞서 제안한 3개의 이니셔티브와 함께 인류 운명 공동체의 비전을 발전시키려는 중국 노력의 일환이라고 밝힘
    * 기술 독점·AI 공급망 파괴 반대와 더불어 글로벌 발전·안보·문명 이니셔티브 제안을 통해 AI 부문의 서방 주도 리더십의 대안으로 중국의 리더십을 강조

■ 영국

- (AI 백서 발표) 과학혁신기술부(DSIT)는 'AI 규제에 대한 혁신적 접근(A pro-innovation approach to AI regulation)'이라는 AI 백서를 발표하고 EU의 강력한 규제와는 차별화되는 유연한 규제 프레임워크 제시('23.3)
  - 영국은 혁신을 억제할 수 있는 AI에 대한 고정 규칙이나 법안 도입은 최소화하고 새로운 단일 규제기관을 신설하여 전권을 부여하는 대신 기존 관련 기관이 부문별·상황별 지침을 채택하는 유연한 규제 방향 채택
    * 개별 규제 기관들은 안전·보안·견고성, 투명성·설명 가능성, 공정성, 책임·거버넌스, 이의제기·시정 등 5개 원칙에 따라 우선순위를 정해 규제를 적용하고, 성장과 혁신을 모두 지원할 수 있는 비례적 접근을 취할 것을 제안
  - 정부는 규제 기관의 프레임워크 이행 지원을 위해 관찰·평가·의견, 일관성 있는 원칙 이행 지원, 위험 평가, AI 혁신기업 지원, 교육 및 인식 제고, 국제 규제와의 상호운용성 보장 방안 마련 등 기능 수행

---

13 법률신문, "중국의 AI 관련 법률 규제 현황", 2024.06.

14 연합뉴스, "中, 美 제재 확대하자 "모든 나라 AI 개발 동등 권리·기회" 촉구", 2023.10

- (세계 최초 AI 안전성 정상회의 개최) 영국은 AI에 대한 최초의 글로벌 정상회담인 AI 안전성 정상회의(AI Safety Summit)를 개최('23.11)하여 주요국 사이에서 중개자로서 AI 규제논의를 주도
  - 영국은 글로벌 AI 산업에서 미국과 중국의 경쟁구도 등의 정세를 활용하여, 영국이 AI 국제표준에 중추적인 역할을 시도
    * 영국은 본 회의에서 AI 안전성 국제기구 설립을 제안하는 등 미국, EU 등 주요국 사이에서 중개자로서 AI 규제논의 주도
  - 본 회의에서 각국 정상은 정부와 주요 기업이 고급 AI 모델을 출시하기 전에 테스트를 선행하고, 최첨단 AI 모델이 가져올 수 있는 위험에 대응하기 위한 공유된 과학적 증거 기반 설명가능한 모델 개발을 수행하도록 합의
- (AI법 제정에 대한 논의) 2024년 3월 AI에 대한 규제 원칙을 법으로 제정하는 것을 목표로 법안이 제안되었으나 큰 진전 없이 폐기됨

■ 일본

- (AI 전략 회의 개최) 현재 AI 규제를 위한 특정 법률은 없으며 전문가 및 정부관계자들이 참여하는 'AI 전략 회의'를 통해 AI 규제·활용에 대한 정책방향 논의
  - 일본 정부는 'AI 전략 2022('22.5)'에 따른 주요 과제로 AI 정책 컨트롤타워 역할을 하는 'AI 전략 회의'를 설치하였으며, 이를 통해 민간·교육·공공분야에서의 이용 촉진, 허위 정보 및 개인정보 침해 등 리스크 대응, 국제 규제 검토, 국내 AI 개발지원 등 논의
    * 'AI 전략 회의' 제6차 회의에서는 생성형 AI 개발자와 제공자의 규칙 준수 촉구 조치, 생성형 AI 촉진을 위한 개발자 대상 정부 보유 데이터 제공 방안 등을 논의('23.11)
- (AI안전연구소 설립) 2024년 2월 14일 경제산업성 산하 정보처리추진기구(IPA)에 AI 안정성 확보 전담 조직인 'AI안전연구소'를 설립
  * 연구소는 국제 파트너와 협력하여 AI의 안전 표준, 평가 방법론 및 우수사례를 개발함으로써 AI의 책임있는 사용을 보장하기 위한 글로벌 노력에 기여함을 목적으로 함
- (AI 가이드라인 발표) 경제산업성과 총무성은 AI에 관한 잠정적 논점정리를 바탕으로 기존 가이드라인을 통합·업데이트한 「AI 사업자 가이드라인」을 발표('24.4)
  * <G7 히로시마 AI 프로세스>의 틀을 기반으로 기존 「AI 개발 가이드라인」, 「AI 이·활용 가이드라인」, 「AI 원칙의 실천을 위한 거버넌스·가이드라인」을 통합 정리
  - 해당 가이드라인은 <인간 중심의 AI 사회 원칙>에 따라 AI 개발자, AI 제공자, AI 이용자를 대상으로 한 10개 원칙을 제시
    * 「AI 사업자 가이드라인」에 대해 4,000여 건의 의견이 접수되었으며, 소프트뱅크, 구글 등은 법적 구속력이 없는 가이드라인 구성에 찬성 의견을 제시[15]
- (AI 법안 도입 추진) 일본 정부는 5월 AI 전략 회의에서 AI의 안전성 확보를 위한 규제법 마련을 검토하기 시작했다고 발표('24.5)
  - 일본은 지난 2024년 4월 법적 구속력이 없는 AI 가이드라인을 발표하는 등 애초 완만한 대응을 추진했으나 이번에 '법 규제'로 정책 방향을 전환
    * 기존 가이드라인이 AI 위험성에 대한 대응이 충분하지 않다는 비판에 더불어 미국·유럽 등 국제사회에서 규제 움직임이 강화됨에 따른 대응으로 해석됨
  - 일본 정부는 2024년 여름에 전문가 회의를 구성해 사업자 등의 의견을 청취할 예정이며, 법안은 내년 정기 국회에 제출을 목표로 하고 있음[16]
    * 법안은 허위 정보를 걸러내고, 저작권을 보호하며, AI의 윤리적 사용을 보장하는 데 중점을 둠. 일본은 AI에 대한 법적 틀을 마련함으로써 기술혁신을 촉진하고 사회적 가치와 개인의 권리를 보호하고자 함[17]

---

15 KOTRA, 일본의 AI 정책과 실제 사례, 2024.04

16 한겨레신문, "미국·유럽 규제 움직임에…일본도 'AI 규제법' 만든다,", 2024.05

17 NIPA, 글로벌 ICT 월간동향리포트, 2024.02

■ 캐나다

- (AI 및 데이터 법안 제정 추진) 캐나다 의회는 2022년 6월 AI 시스템 개발과 활용에 대한 적정한 규제 체계 마련을 위해 제안된 'AI 및 데이터법(AIDA: Artificial Intelligence and Data Act)'의 입법화를 추진('22.6)
  - 법안은 특히 고위험 시스템에 대한 규제와 강력한 처벌을 규정하고 있어, 자유로운 AI 시스템 개발·이용을 지향하면서도, 안전하고 신뢰할 수 있는 AI 시스템 개발·이용 환경 조성에 주안점을 둠[18]
  - AIDA는 고영향(High-impact) AI 시스템 사용에 대한 규칙을 마련하여 유럽연합(EU)에서 제안된 인공지능법(AI Act)과 같이 고위험 영역에 집중한 위험 기반 접근방식을 채택
    * 장관은 고위험 시스템으로 인해 '긴박한 피해가 발생한 심각한 위험'이 있다고 판단되는 경우 시스템 사용·제공의 중지 명령이 가능하며, 동 법의 관리 및 집행 지원을 위해 소관 부처의 고위 공무원을 'AI 및 데이터 위원'으로 지정 가능
  - 캐나다 의회는 2023년 4월 AIDA의 두 번째 검토 회의를 완료하였으며, AIDA 법률은 규제 협의, 규정 초안 개발 및 협의, 최초 규정 시행 등을 거쳐 새로운 법이 발효되기까지 최소 2년의 기간이 소요되어 2025년 이후에나 발효될 것으로 예상됨[19]

- (생성형 AI 이용에 관한 지침 발표) 캐나다 정부는 2023년 9월 선진적 생성형 AI 시스템의 개발 및 관리를 위한 자발적 행동 강령을 발표
  - 이 행동 강령은 캐나다 AI 산업에 공통 표준을 제공하고 공식 규정이 발효될 때까지 생성형 AI 시스템을 책임감 있게 개발하고 사용하고 있음을 자발적으로 입증할 수 있도록 하고 있음
    * 시스템 개발자의 책임, 안전, 공정성과 형평성, 투명성, 인간에 의한 감독 및 모니터링, 시스템의 유효성 및 견고성에 대한 내용을 담고 있으며, 생성형 AI 관련 도전과제와 우려 사항을 살펴보고, 책임감 있게 생성형 AI를 이용하기 위한 원칙, 잠재적 이슈 및 모범사례 등을 제시[20]

■ 종합

- 주요 국가들은 AI 기술 발전에 따른 위험과 부작용을 인식하고, 이를 최소화하기 위한 규제 도입의 필요성에 공감하고 있으나 포괄적인 AI 규제 법안 도입에 대한 태도와 접근방식에 대한 차이 존재
  - (미국) 미국은 포괄적인 AI 규제가 없는 상황에서, 행정부 내에서 효력이 발생하는 행정명령을 통해 AI의 긍정적인 잠재성은 극대화하고 국가 안보, 허위 정보 생성, 일자리 등에 미치는 영향은 최소화하는 규제 추진
  - (중국) 단편적이고 세분화된 규제 시행으로 강력한 규제와 정부 통제를 통한 AI 기술 관리
  - (영국) 강력한 규제 대신 유연한 접근을 취하며, 다양한 상황에 맞춘 규제 제시
  - (일본) 현재 구체적인 법률보다는 가이드라인과 AI 전략 회의를 통한 논의가 주를 이룸
  - (캐나다) AI 및 데이터법(AIDA)을 통해 고위험 AI 시스템에 대한 규제를 중점적으로 다루고 있으며, 법안 발효 전까지 자발적 행동 강령을 통해 산업 자율 규제를 추진

- 주요 국가들은 자국의 규제를 논의하는 동시에 글로벌 규제 기준 마련을 위한 국제 논의에도 적극적으로 참여
  - (미국) '국가 AI 이니셔티브법', 'AI 권리장전 청사진' 등을 발표하고, 중요한 AI 관련 이슈에 대한 의견 수렴, 교육 분야에서의 AI 위험과 기회에 관한 보고서 발표 등 AI 거버넌스 정책을 지속 추진
  - (중국) '글로벌 AI 거버넌스 이니셔티브' 발표('23.10)를 통해 글로벌 규칙과 표준에 대한 리더십 구축 시도
  - (영국) AI에 대한 최초의 글로벌 정상회담인 AI 안전성 정상회의(AI Safety Summit)를 개최('23.11)하여 주요국 사이에서 중개자로서 AI 규제논의를 주도
  - (일본) AI안전연구소를 설립하여 국제 파트너와 협력하여 AI의 안전 표준, 평가 방법론 및 우수사례를 개발함으로써 AI의 책임 있는 사용을 보장하기 위한 글로벌 노력에 기여

18 한국지능정보사회진흥원, [디지털 법제 Brief 제2022-3호] 캐나다, 인공지능 및 데이터 법안의 주요 내용 및 시사점, 2022.07

19 소프트웨어정책연구소, [AI브리프 스페셜] 미국, 영국, 캐나다의 인공지능(AI) 정책 동향, 2023.10

20 한국저작권위원회, [캐나다] 생성형 AI 시대의 저작권에 대한 의견수렴 진행, 2024.03

- 생성형 AI와 같은 최신 핵심 이슈에 대한 국가적 대응과 더불어 정부와 민간 부문 간의 협력 체계 강화 필요
  - (미국) 생성형 AI 규제 요구가 증가하고 규제에 대한 우려가 커지는 상황에서 백악관은 주요 IT 기업들과의 정책 협력을 통해 리더십을 발휘하고, AI 기업들이 자발적으로 안전하고 투명한 AI 개발을 약속하도록 유도
  - (중국) AI에 대한 감독을 강화하기 위해 생성형 AI에 대한 최초 규제인 '생성형 AI 서비스 관리 잠정방법' 제정 및 시행
  - (캐나다) 정부는 생성형 AI 시스템의 개발 및 관리를 위한 행동 강령을 발표('23.9)하여 캐나다 AI 산업에 공통 표준 제공, 생성형 AI를 책임감 있게 개발하고 사용하고 있음을 자발적으로 입증할 수 있도록 유도.

⊙ 참고문헌

1. 국외문헌

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion,* 99, 101896.

Edwards, L. (2022). Expert explainer: The EU AI Act proposal. *Ada Lovelace Institute*. Retrieved from: https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/

Gartner (2024). Getting Ready for the EU AI Act, Phase 2: Risk-Assess & Categorize.

Gartner (2024). Quick Answer: How Bank CIOs Can Align Their AI Strategies With the EU AI Act.

Mackrael, K., Schechner S. (2023) America's Tech Giants Rush to Comply With New Curbs in Europe. *The Wall Street Journal*.

Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2024). A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. *AI Board, Scientific Panel,and National Authorities* (May 5, 2024).

2. 국내문헌

국가안보전략연구원 (2024). EU '인공지능 규제법(AI Act)' 통과의 의미와 시사점.

국립외교원 외교안보연구소 (2021). "바이든 행정부의 인공지능 국가정책: 평가와 함의"

법률신문 (2024.2.29.). "미국과 영국의 AI 규제 동향"

법률신문 (2024.6.10.). "중국의 AI 관련 법률 규제 현황"

법률신문 (2024.2.15.). "해외 디지털 기본권 추진 동향"

소프트웨어정책연구소 (2023). 미국, 영국, 캐나다의 인공지능(AI) 정책 동향

심소연 (2024). 규제중심의 유럽연합 인공지능법(EU AI Act), 국회도서관.

연합뉴스 (2023.10.19.). "中 , 美 제재 확대하자 "모든 나라 AI개발 동등 권리·기회" 촉구"

이해원 (2024). 유럽연합 인공지능법: 주요 내용과 시사점, 스타트업 얼라이언스.

중앙일보 (2024.5.9.). "AI 법안 진행에 대한 우려 커져"

한겨레 (2024.5.23.). "미국·유럽 규제 움직임에…일본도 'AI 규제법' 만든다"

한국지능정보사회진흥원 (2022). 캐나다, 인공지능 및 데이터 법안의 주요 내용 및 시사점

KOTRA (2024). 일본의 AI 정책과 실제 사례.

KISTEP (2024). EU 인공지능(AI) 규제 현황과 시사점.

NIPA (2024.2.). 글로벌 ICT 월간동향리포트.

YTN (2024.7.2.). "EU, 빅테크에 천문학적 과징금 예고... 삼성전자 불똥?"