ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION
CENTER FOR KOREAN INNOVATION AND COMPETITIVENESS

통합적 접근의 명암: 한국 AI 기본법의 전략·진흥·규제 구조와 규제 리스크

김세진, 호단 오마르 | 2025년 9월

한국은 하나의 인공지능(AI) 법에 전략, 진흥, 규제를 통합함으로써 AI 산업을 구축할 수 있는 강력한 제도적 수단을 마련하였다. 그러나 그중 규제 부문은 법이 지닌 다른 강점들을 잠식 또는 약화시킬 수 있는 위험을 내포하고 있다.

주요 내용

- 한국의 AI 기본법은 세계 최초로 AI 전략, 산업 진흥, 규제를 하나로 결합한 사례로, 장점과 단점을 동시에 증폭하는 구조적 특성을 지닌다.
- 데이터 인프라, 집적단지 조성, 인재 양성, 국제화 전략에 이르는 산업 진흥 조항은 체계적이고 미래지향적으로 설계되어 있으며, 향후 다른 국가들이 참고할 수 있는 정책적 모범이 될 잠재력이 있다.
- 규제 파트의 문제 진단 오류: 그러나 규제 부문은 AI 위험성에 대한 진단이 부정확하게 이루어져 있어, 전략 및 산업 진흥 파트의 정책적 효과를 훼손할 수 있다. 지나치게 광범위한 AI 정의, 경직된 연구개발(R&D) 의무, 중소기업 우선 규칙 등은 한국이 글로벌 경쟁력을 확보하는 데 필수적인 규모와 유연성을 저해할 위험을 안고 있다.
- 컴퓨팅 임계값, 투명성 라벨링 요건, '고영향 AI' 지정과 같은 프로세스 중심 보고 의무는 기업에 실질적인 책임성을 부과하기보다 행정적 부담을 가중시키며, 자원 낭비로 이어질 가능성이 크다.
- 이러한 문제를 보완하기 위해서는 두 단계의 조정이 요구된다. 첫째, 국회 차원에서 구조적 개정을 통해 법적 틀을 정비해야 하며, 둘째, 과학기술정보통신부(MSIT)는 시행령 단계에서 균형 잡힌 규제 설계를 마련하여 법의 산업 진흥 기능이 약화되지 않도록 해야 한다.

목차

소개

2024년 12월, 한국 국회는 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」(이하 "AI 기본법")을 통과시켰다.[1] 본 법안은 정부 정책 방향을 조율하기 위한 전략, 인공지능(AI)의 개발 및 채택을 촉진하기 위한 산업 정책, 그리고 위험 관리를 위한 규제 프레임워크를 포괄한다. 이를 통해 한국은 AI 정책의 세 가지 핵심 지렛대—전략, 진흥, 규제—를 하나의 법률로 통합한 세계 최초의 국가가 되었다.

시행 국가를 불문하고 AI 정책에서 전략, 진흥, 규제는 상호 의존적인 관계를 형성한다. 어느 한 부분의 결함은 다른 요소들의 효과를 약화시킬 수밖에 없다. 한국은 이 세 가지를 단일 법안에 결합함으로써 제도적 통합의 강점을 확보하였으나, 동시에 설계 오류의 대가가 커질 수 있는 구조적 위험을 내재하고 있다. 다시 말해, 본 법의 이점은 배가될 수 있으나, 설계상의 실수는 전체 체계의 효율성을 저해할 수 있다.

AI 기본법은 전략적 차원에서 국가적 비전을 제시하고, AI를 전략산업으로 규정하여 체계적 투자의 기반을 마련하는 데 성공하였다. 또한 데이터 인프라, 집적단지(클러스터) 조성, 인재 양성, 국제화를 지원하는 산업 진흥 정책을 법의 목적에 부합하도록 설계하였다. 그러나 산업 진흥 파트 내에서 중소기업(SME)에 대한 과도한 편향은 한국이 글로벌 경쟁력 확보를 위해 필요로 하는 규모 확대와 자원 배분의 유연성을 저해할 가능성이 존재한다.

무엇보다 규제 파트는 AI 위험성에 대한 진단이 부정확하게 이루어져 있으며, 지나치게 광범위한 정의, 경직된 연구개발(R&D) 의무, 그리고 투명성 라벨링·컴퓨팅 임계값과 같은 비효율적 규제 수단을 포함하고 있다. 이러한 규제 조항은 성과 기반 감독을 보장하기보다 행정적 부담을 가중시키고, 기업 자원의 낭비로 이어질 위험이 크다.

본 법은 2026년 1월 시행을 예정하고 있으며, 현재 과학기술정보통신부(MSIT)가 구체적 이행을 규정할 시행령을 마련 중이다.[2] 2025년 9월 8일 발표된 시행령 초안은 2025년 말까지 확정·공포될 것으로 예상된다.

이 법의 단일 설계 구조를 고려할 때, 한국은 법의 결함을 지금 수정하지 않을 경우 한국은 효과적인 조항과 비효율적인 조항을 동시에 고착화할 위험에 직면할 수 있다. 법의 기본 목표인

인권과 존엄성의 보호, 삶의 질 향상, 국가 경쟁력 강화라는 비전을 실현하기 위해서는 국회와 정부 모두에서 구조적 조정이 요구된다.

우선, 국회는 광범위한 정의, 규범적 연구개발 의무, 중소기업 편향, 비효율적 규제 메커니즘 등 혁신을 저해할 수 있는 구조적 결함을 개정해야 한다. 동시에 MSIT는 최종 시행령을 통해 과도한 행정 부담이나 경쟁 왜곡을 최소화하면서, AI 생태계를 실질적으로 지원하는 균형 잡힌 규제를 제시해야 한다.

국회는 AI 기본법에 다음과 같은 개정안을 제출해야 한다.

- **AI 정의의 정교화 (제2조 개정): AI 기본법 제2조(정의) 내 "AI 시스템" 정의는 지나치게 광범위하여, 단순한 계산 도구나 기존의 자동화된 소프트웨어까지 포함할 소지가 있다. 따라서 본 조항의 정의를 새로운 거버넌스 과제를 발생시키는 시스템에 한정되도록 축소해야 한다.** 이를 통해 규제 범위를 명확히 하고, 불필요한 행정적 부담을 최소화할 수 있다. 보다 정밀한 정의는 다음과 같이 논의할 수 있다; "인공지능 시스템(AI 시스템)"이란, 제공자 또는 사용자가 알 수 없는 매개변수를 기반으로 머신러닝을 통해 주어진 목표 집합을 달성하는 방법을 추론하고, 콘텐츠(생성형 AI 시스템), 예측, 권고, 의사결정과 같은 시스템 산출물을 생성하여 그것이 상호작용하는 실제 또는 가상 환경에 영향을 미치는 시스템을 의미한다.
- **국가 AI 전략위원회 권한의 전략 중심 재편 및 위험별 규제 권한을 부처별 전문성에 따라 배분(제7조~제9조 개정): 국가 AI 전략위원회와 그 기능을 다루는 제7조부터 제9조까지의 조항 역시 개정이 필요하다.** 위원회가 AI 기본계획을 통해 국가 AI 전략을 수립하고 정부 AI 프로그램 전반에 자원을 배분할 수 있는 권한은 유지하되, 규제 변경을 지시할 권한은 삭제해야 한다. 규제의 설계와 시행은 각 분야의 전문성을 보유한 부처에 위임하는 것이 타당하다. 이를 통해 전략적 통합의 이점은 최상위 수준에서 유지되면서도, 의료 AI, 금융 AI, 자율주행차와 같이 분야별 특수성이 요구되는 영역에서는 해당 위험을 가장 잘 관리할 수 있는 기관이 규칙을 수립할 수 있게 된다.
- **MSIT에 의한 유연한 R&D 로드맵 설계 (제13조 개정): 제13조(인공지능기술 개발 및 안전한 이용 지원)는 규범적 연구개발 우선순위를 삭제하고, 과학기술정보통신부(MSIT)가 유연한 국가 AI 연구개발 로드맵을 수립하고 주기적으로 갱신할 수 있도록 권한을 부여해야 한다.** 이러한 개정은 한국의 투자가 시대에 뒤떨어진 의무에 구속되지 않고, 글로벌 혁신의 흐름을 추적할 수 있도록 보장할 것이다.
- **중소기업 우선 조항 삭제 (제17조 개정): 제17조(중소기업등을 위한 특별지원)는 중소기업을 "우선 고려"해야 한다는 법적 요건을 삭제하는 방향으로 개정되어야 한다.** 법은 규모에 구애받지 않는 언어를 채택해 정부가 모든 규모의 기업을 각자의 강점에 따라 지원할 수 있도록 해야 한다. 이를 통해 스타트업과 중소기업은 실험과 확산에 집중할 수 있으며, 대기업은 자본 집약적인 연구개발, 규모 확장, 글로벌 시장 진출에 필요한 지원을 받을 수 있다.
- **투명성 요건 조정 (제31조 개정): 제31조(인공지능 투명성 확보 의무)는 의무적인 정보 공개 요건을 삭제하는 것이 바람직하다.** 워터마크와 AI 라벨은 기술적으로 취약하고 관할권마다 일관성이 부족하며, 허위 정보, 지식재산권 침해, 딥페이크 등 정책

입안자들이 우려하는 구체적 피해를 해결하지 못하기 때문에 오히려 잘못된 안전 의식을 심을 수 있다. 대신 법은 과학기술정보통신부와 관계 부처가 콘텐츠 출처 및 진위성 연합(C2PA)과 같은 자발적 출처 기준을 장려하고, 디지털 및 AI 리터러시 프로그램에 투자하며, 지식재산권 침해, 선거 캠페인 투명성, 온라인 괴롭힘과 같은 특정 피해에 대해 맞춤형 규칙을 채택하도록 규정해야 한다.[3]

- **컴퓨팅 기준 삭제 (제32조 개정): 제32조(인공지능 안전 확보 의무)는 현재 컴퓨팅 임계값 이상으로 훈련된 시스템에 대해 감독을 발동하는 구조를 취하고 있으나, 컴퓨팅 사용량은 위험을 예측하는 신뢰할 수 있는 지표가 아니므로 기준에서 제외되어야 한다.** 대신 제12조를 개정하여 AI 안전연구소(AISI)가 AI 시스템의 배포 후 평가를 수행할 수 있도록 권한을 부여하는 것이 바람직하다. AISI는 고영향 분야에 구축된 모델을 테스트하고, 실패 및 사고를 모니터링하며, 결과를 발표함으로써 감독이 임의적인 훈련 입력이 아닌 실제 성과에 근거하도록 해야 한다.
- **성과 기반 감독 도입 (제33조~제35조 개정): 고영향 AI에 대해 광범위한 자체 평가, 문서화, 위험 보고를 의무화하는 제33조부터 제35조까지의 조항은 프로세스 중심의 의무를 성과 기반 요건으로 대체해야 한다.** 법은 각 부처가 해당 분야의 AI 시스템에 대해 측정 가능한 성과를 설정하도록 지시하고, 한국표준과학연구원(KRISS)은 AI 시스템이 이러한 성과를 충족하는지를 평가할 수 있는 프로토콜을 설계하도록 해야 한다. 이를 통해 감독은 단순한 서류 작업에서 의미 있는 성과 기준으로 전환될 수 있다.
- **외국 기업 차별 규정 삭제 (제36조 개정): 제36조(국내 대리인 지정)는 외국 기업에 대한 더욱 엄격한 감독을 유발하는 매출 및 사용자 기준을 삭제하는 방향으로 개정되어야 한다.** 감독은 제공자가 국내 기업인지 여부와 관계없이, 해당 시스템이 고영향 시스템으로 지정된 경우에만 발동되어야 한다. 이를 통해 동등한 대우가 보장되고, 임의적인 기준이 제거되며, 기업 규모나 소재지가 아닌 실제 위험에 근거한 규제가 확립될 수 있다.

과학기술정보통신부는 AI 기본법에 따른 최종 시행령을 활용하여 시행의 명확성과 균형을 제공해야 한다. 특히,

- **표준화(제14조): 제14조(인공지능 기술의 표준화)의 경우, 표준은 산업계 주도로 수립되고 정부는 의장 및 조정자의 역할에 국한된다는 점을 명확히 할 필요가 있다.** 정부는 기술 표준의 개발을 산업 컨소시엄에 맡기되, 기업 간 협력, 국제 포럼 참여 지원, 기관 간 협력에 집중함으로써 한국의 접근 방식이 국제적 관행과 일치하고 국내 기업이 관련 시장에서 경쟁력을 유지할 수 있도록 해야 한다.
- **지원 정책(제18조·제19조): 제18조(AI 스타트업 지원)와 제19조(AI 융합 정책)의 경우, 정책 시행이 기업 규모와 무관하게 이루어져야 한다는 점을 명확히 해야 한다.** 스타트업과 중소기업은 교육, 사업화 지원, 도입 프로그램을 통해 계속 지원을 받을 수 있어야 하며, 동시에 대기업 역시 핵심 산업에서 AI 활용을 확대하고 글로벌 경쟁력을 강화하기 위한 자원을 확보할 수 있어야 한다. 자금 지원, 교육 제도, 도입 인센티브는 특정 규모에만 국한되지 않고 AI 생태계 전체를 강화하는 방향으로 설계되어야 한다.
- **데이터 요청(제40조): 제40조(사실조사 등)는 어떠한 데이터를 누구에게, 어떤 목적으로 요청할 수 있는지에 대한 명확한 지침을 마련해야 한다.** 요청은 위험 관리 조치나

사용자 보호 관행의 문서화와 같이 법 준수 여부를 확인하는 데 엄격히 필요한 정보로 제한되어야 하며, 관련 없는 사업 데이터에는 적용되어서는 안 된다. 또한 법령은 기업의 독점 정보를 보호하기 위해 강력한 기밀 유지 조치를 포함해야 하며, 이를 통해 불필요한 준수 비용을 최소화하면서도 책임성을 유지해야 한다.

- **벌칙(제42조): 제42조(벌칙)는 위반의 심각성과 영향에 비례하여 제재 규모를 조정할 필요가 있다.** 체계적이거나 반복적인 위반에 대해서는 제재를 강화하되, 경미하거나 초범인 경우에는 비례적 수준에서 적용하는 것이 바람직하다. 시행령에 명확한 지침을 마련함으로써 과도하게 가혹한 처벌이 법 준수 또는 협력을 저해하는 것을 방지하면서도 책임성을 보장할 수 있다.
- **과태료(제43조): 제43조(과태료)의 경우, 과태료 부과 전 유예 기간을 설정해야 한다.** 이 전환 기간 동안 새로운 의무를 이행하지 못한 기업은 즉시 과징금을 부과받기보다는 경고나 시정 지침을 받아야 한다. 이를 통해 국내외 사업자가 효과적인 준수 체계를 구축할 시간을 확보하는 동시에, 제도가 완전히 정착된 이후에는 강력한 집행력이 유지될 수 있을 것이다.

법률 개요

AI 기본법은 6개 장으로 구성되어 있다. (각 장별 조항 요약은 부록 참조) 각 장은 다음과 같다.

1. **총칙:** "AI 시스템", "고영향 AI", "생성 AI"와 같은 목적, 범위 및 주요 정의를 제시한다.
2. **인공지능의 건전한 발전과 신뢰 기반 조성을 위한 추진체계:** 국가 AI 전략의 체계를 구축한다. 대통령 직속 국가인공지능위원회, 정기 마스터플랜, 그리고 인공지능정책센터, 인공지능안전연구소(AISI)와 같은 지원 기관을 중심으로 구성된다.
3. **인공지능기술 개발 및 산업 육성:** R&D, 데이터 인프라, 표준에 중점을 둔 혁신 정책과 중소기업 및 스타트업을 육성하고, 집적단지(클러스터) 및 데이터센터를 육성하며, 기업의 해외 진출을 지원하는 산업 개발 조치를 결합한다.
4. **AI 윤리 및 신뢰성 확보:** AI 윤리 원칙 및 자발적 윤리 위원회와 같은 연성법(soft-law) 조치와 생성적이고 영향력이 큰 AI에 대한 투명성, 안전, 감독 및 영향 평가에 대한 경성법(hard-law) 의무를 결합한다.
5. **보칙:** 본법의 프로그램에 대한 자금 조달 및 운영 규칙을 정한다.
6. **벌칙:** AI 사용 공개, 국내 대리인 지정, 시정 명령 준수 등 주요 준수 의무를 위반할 경우 부과되는 벌칙과 행정 벌금을 규정한다.

본 보고서는 본 법의 구조를 따른다. 1장에서는 법의 범위를 형성하는 기본 정의를 검토한다. 2장, 3장, 4장에서는 각각 국가 AI 전략 수립, 산업 정책 발전, 위험 관리를 위한 규제 접근 방식 제시라는 세 가지 핵심 목표를 다룬다. 5장과 6장에서는 운영 프레임워크와 벌칙을 다룬다. 다음 섹션에서는 각 장을 차례로 평가하여 무엇이 잘 구성됐고, 무엇이 부족한지, 그리고 정책 입안자가 프레임워크를 더 효과적으로 만들기 위해 무엇을 수정해야 하는지 강조한다.

제1장 총칙

제1조부터 제5조까지로 구성된 이 법의 제1장은 이 법 전체의 법적 토대를 마련하는 기본 원칙과 정의를 정립합니다. 아래 표 1은 이 법 제2조의 주요 정의를 요약한 것입니다.

표 1: 대한민국 AI 기본법의 주요 정의 요약

용어	법의 정의	기사에서 호출됨
인공지능	학습, 추론, 지각, 판단, 언어 이해 등 인간의 지적 능력을 전자적으로 구현한 것입니다.	이는 핵심 기술을 진흥하는 데 사용되는 기본 용어로, 전체 법안에서 사용됩니다.
인공지능시스템	다양한 수준의 자율성과 적응성을 갖추고 예측, 권장 사항, 의사 결정 등의 결과를 추론하는 AI 기반 시스템입니다.	주로 제32조(대규모 AI 시스템에 대한 안전 조치)에서 언급되며, 고영향 AI에 대한 제33~35조의 근거가 됩니다.
인공지능기술	AI 구현에 필요한 하드웨어, 소프트웨어 또는 응용 프로그램 기술.	제6조(연구개발에 대한 정부지원) 제13조(AI기술 및 데이터 인프라)
고영향 인공지능	인간의 생명, 안전 또는 기본권에 중대한 영향을 미칠 수 있는 AI 시스템입니다.	제33조(영향력이 큰 AI의 식별) 제34조(영향력이 큰 AI사업자의 책임) 제35조(AI 영향평가)
생성형 인공지능)	입력 데이터의 구조와 특성을 모방하여 새로운 텍스트, 사운드, 이미지 또는 기타 출력을 생성하는 AI 시스템입니다.	제31조(생성AI에 대한 투명성 의무)
인공지능산업	AI 또는 AI 기술을 사용하여 제품이나 서비스를 개발, 제조, 생산 또는 유통하는 산업입니다.	제6조(AI산업 진흥을 위한 정부 지원)
인공지능사업자	AI 산업과 관련된 사업을 수행하는 법인, 조직, 개인 또는 정부 기관입니다. "AI 개발 사업자"와 "AI 활용 사업자"라는 두 가지 하위 범주로 구분됩니다.	제31조~제36조(이것은 모든 "경성법" 조항에 대한 주요 규제 주제입니다.)
이용자	AI 제품이나 서비스를 받는 사람.	제32조(안전조치) 제34조(설명청구권) 제35조(영향평가)
영향을 받는 자	AI 제품이나 서비스로 인해 생명, 신체적 안전 또는 기본적 권리에 상당한 영향을 받는 사람입니다.	제34조(피해자의 보호 및 설명) 제35조(기본권에 대한 영향평가)

용어	법의 정의	기사에서 호출됨
인공지능사회	AI를 통해 모든 분야(산업, 경제, 사회, 문화, 행정 등)에서 가치를 창출하고 진보를 촉진하는 사회입니다.	
인공 지능윤리	인간 존엄성을 존중하는 것을 바탕으로 AI의 모든 영역(개발, 제공, 활용 등)에서 사회 구성원 모두가 준수해야 할 윤리 기준을 정하고, 국민의 권리, 생명, 재산을 보호하는 안전하고 신뢰할 수 있는 AI 사회를 실현합니다.	제27조~제30조(이것은 모든 "연성법(Soft law)" 규정의 주요 주제입니다.)

분석: AI 시스템의 정의가 너무 광범위하다

이 법이 세 가지 서로 다른 목표를 동시에 달성하는 데 있어 한 가지 과제는 "AI"를 매우 다른 의미로 사용해야 한다는 것입니다. 때로는 AI를 광범위한 기술로, 때로는 산업으로서, 때로는 사람들이 실제로 사용하는 특정 시스템으로 지칭하기도 합니다. 즉, 법은 모든 면에서 정확해야 합니다. 규제 조항에서는 광범위한 기술 자체가 아니라 실제 AI 시스템과 도구가 관장된다는 점을 명확히 해야 합니다. 반면, 전략 및 산업 정책 조항에서는 연구 및 기술 개발 분야로서 AI를 지원하는 것에 대해 더 광범위하게 언급하는 것이 타당합니다.

AI를 정확하고 적절하게 정의하고, 진정으로 새로운 위험을 야기하는 시스템에 대한 효과적인 규제를 마련하기 위해, 법은 일반 소프트웨어에까지 확대 적용되지 않을 만큼 좁은 경계를 설정하고, 개발자와 사용자에게 확실성을 제공할 만큼 명확하며, 기술이 발전함에 따라 관련성을 유지할 만큼 안정적인 경계를 설정해야 합니다. 예측이나 권고와 같은 일반적인 기능이 아닌, 새로운 거버넌스 문제를 야기하는 기술적 속성만을 포괄해야 합니다.[4]

한국의 정의는 "다양한 수준의 자율성과 적응성을 바탕으로 예측, 제안, 의사결정 등의 결과를 추론하는 AI 기반 시스템"이지만, 세 가지 측면 모두에서 부족합니다. 첫째, 너무 광범위합니다. 많은 기존 소프트웨어 프로그램이 예측이나 제안을 생성하지만, 규제를 정당화하는 새로운 위험을 야기하지 않습니다. 둘째, 모호합니다. "AI 기반", "자율성", "적응성"과 같은 용어는 명확한 기술적 의미가 없어 해석과 지속적인 확장에 따라 그 범위가 제한됩니다. 셋째, 불안정합니다. 규제를 일반적인 기능에 묶음으로써 과거의 도구(예: 스프레드시트의 통계 모델)와 미래의 혁신을 모두 포괄하여 지속 가능하고 기술 중립적인 기반을 제공하기보다는 끝없는 수정을 강요할 위험이 있습니다.

제안

- 국회는 AI 기본법 제2조(정의)를 개정하여 'AI 시스템'의 정의를 좁혀 야 한다. 그래야 이후 법에서 이 용어가 사용되는 것은 새로운 거버넌스 과제를 야기하는 시스템에만 적용될 수 있다. 더 정확하게 표현하면 “인공지능 시스템(AI 시스템)”이란, 제공자 또는 사용자가 알 수 없는 매개변수를 기반으로 머신러닝을 통해 주어진 목표 집합을 달성하는 방법을 추론하고, 콘텐츠(생성형 AI 시스템), 예측, 권고, 의사결정과 같은 시스템 산출물을 생성하여 그것이 상호작용하는 실제 또는 가상 환경에 영향을 미치는 시스템을 의미합니다.

제2장: 인공지능의 건전한 발전과 신뢰 기반 조성을 위한 추진체계

제6조에서 제12조까지에 해당하는 이 법의 제2장은 국가 AI 전략을 수립하고 이를 강제할 제도적 장치를 구축합니다.

3 년 마다 모든 정부 부문의 AI 정책에 대한 국가 차원의 전략적 로드맵 역할을 하는 포괄적인 AI 기본계획을 수립하고 시행하도록 규정합니다. [5]이 계획은 인재 육성, AI 윤리, 투자 우선순위, 그리고 AI로 인한 사회 변화에 대한 국가 차원의 대응 전략을 제시함으로써 국가적 방향을 제시합니다.

계획에 정치적 영향력과 권한을 부여하기 위해 제7조부터 제9조까지는 대통령 직속으로 국가AI위원회를 설립하여 마스터플랜 승인, 연구개발 전략, 투자, AI 규제의 파악 및 개선 등 중요한 사안에 대해 심의하고 결정할 권한을 부여합니다. 이 법은 다른 정부 기관이 위원회의 결정에 따라 행동할 수 있는 명확한 권한을 부여합니다. 제8조에 따르면 위원회가 법률이나 제도의 변경을 권고하거나 의견을 표명할 경우 관련 국가기관(예: 부처)은 개선 사항을 이행하기 위한 계획을 수립해야 합니다. 정부는 2025년 9월 대통령령을 통해 국가AI위원회(국가인공지능위원회)를 국가AI전략위원회(국가AI전략위원회)로 확대 개칭했습니다.[6] AI 관련 최고 범부처 의사결정기구 로 승격되었고, 새로운 사무국이 신설되었습니다. 전략위원회는 2025년 9월 창립 회의에서 4개 안건을 채택했습니다. 정부의 총괄 마스터플랜인 '한국형 AI 실행 계획'(위원회 주도), 국가 AI 컴퓨팅 센터 설립 로드맵(과기정통부 주도), AI 기본법 시행령 지침 초안(부처 주도), 그리고 위원회 세부 운영 규정 (위원회 주도)입니다.

제10조는 위원회가 소위원회, 특별위원회, 전문가 자문단을 설치할 수 있도록 허용합니다. 이러한 메커니즘은 전문적인 사안을 다룰 수 있는 유연성을 제공합니다. 2025년 9월 현재 기술혁신 및 인프라, 데이터, 글로벌 협력, 사회, 과학 및 인재, 국방 및 안보, 산업 응용 및 생태계, 공공 부문 응용 등 8개 [7]분과위원회 가 있습니다. 각 분과위원회는 2026년 10조 1,000억 원에 달하는 정부의 AI 예산을 검토하고 조정하는 역할을 할 것입니다. 이는 2025년 3조 3,000억 원에서 3배 이상 증가한 수치입니다.[8]

제11조는 기본계획 및 관련 정책에 대한 기술 지원, AI의 사회·경제·문화적 영향 분석, 미래 동향 및 법적 수요 예측, 그리고 법률 또는 국가기관이 지정하는 사업 수행 등을 담당하는 AI정책센터를 지정할 수 있도록 규정하고 있습니다. 센터의 지정 및 운영에 관한 세부 사항은 대통령령으로 정합니다.

마지막으로, 제12조는 과학기술정보통신부 산하 AISI를 설립합니다. AISI는 위험 분석, 안전성 평가 기준 및 기술 개발, 그리고 AI 안전에 대한 국제 협력을 담당하며, 국민 보호와 신뢰가 대한민국 AI 생태계의 핵심 축으로 자리매김하도록 보장합니다.

분석: 마스터 플랜은 유지하고 마스터 규제 기관은 없애라

한국 모델은 AI처럼 혁신적인 기술에 있어 통일된 국가 비전이 필수적임을 정확하게 파악하고 있습니다. 이 법은 효과적인 AI 전략의 두 가지 핵심 요소, 즉 비전과 자원 배분을 현명하게 중앙집중화합니다. 단일하고 야심 찬 비전을 설정할 권한을 가진 대통령 직속 위원회를 설립함으로써, 정부는 R&D부터 공공 부문 응용에 이르기까지 모든 AI 관련 활동이 혁신 촉진, 경쟁력 강화, 그리고 AI를 이용하는 사람들의 삶 개선이라는 공동의 목표를 향해 나아가도록 할

수 있습니다. 또한 이러한 중앙집중화된 접근 방식을 통해 정부는 목표 달성에 가장 중요하다고 판단되는 분야에 자본과 인재를 효율적으로 투입하여, 조정되지 않은 프로젝트에 자원이 분산되는 것을 방지할 수 있습니다. 이러한 수준의 중앙집중화는 전략적 이점입니다.

그러나 이 법은 위원회 산하 규제 권한을 통합함으로써 지나친 잣대를 들이밀었습니다. 특정 부문을 지칭하지 않는 이 단일 기관에 각 부처의 규제 변경을 지시할 권한을 부여함으로써, 제8조는 사실상 최고 규제 기관을 만들어냅니다. 그러나 전문가 소위원회 의 지원을 받는 단일 기관이라 하더라도 개별 부처의 심층적이고 전문적인 전문성을 따라잡을 수는 없습니다. 보건부는 의료 AI의 고유한 위험을 이해하고, 금융위원회는 알고리즘 거래의 복잡성을 파악하며, 국토부는 자율주행차 문제를 해결하는 데 가장 적합한 위치에 있습니다. 전문성은 폭넓지만 피상적인 중앙 규제 기관이 이처럼 다양한 부문에 걸쳐 규칙을 지시할 경우, 그 결과는 필연적으로 실패로 끝날 것입니다. 안전한 혁신을 추구하기에는 너무 경직되어 있고, 고위험 안전 필수 애플리케이션에는 위험할 정도로 부적합하기 때문입니다.

제안

- 국회는 국가 AI 전략위원회가 AI 기본계획을 통해 국가 AI 전략을 수립하고 정부 AI 프로그램 전반에 걸쳐 자원을 배분할 수 있는 권한을 유지하되, 규제 변경을 지시할 권한은 삭제하도록 7조부터 9조까지 개정 해야 합니다. 규제 설계 및 집행은 필요한 전문성을 갖춘 각 부처가 담당해야 합니다. 이를 통해 전략적 통합의 이점을 극대화하는 동시에 의료 AI, 금융 AI, 자율주행차 관련 규정은 각 기관의 특정 위험을 가장 잘 관리할 수 있는 기관에서 제정될 수 있도록 할 것입니다.

제3장 인공지능기술 개발 및 산업 육성

이 법 제3장은 AI 산업의 투입과 산출 모두에 초점을 맞춘 두 부분으로 구성되어 있습니다. 첫 번째 부분은 산업의 기반을 구성하는 요소들을 다루고, 두 번째 부분은 이러한 요소들의 상용화 및 활성화를 목표로 합니다.

한국의 AI 산업을 지원하는 혁신 정책

15 조를 다루는 본 장의 첫 번째 부분인 “인공지능 산업 기반 구축”은 혁신 정책으로 가장 잘 설명될 수 있습니다. 강력한 AI 산업의 출현에 필요한 기본 요소와 인프라에 초점을 맞춥니다.

제13조는 정부가 AI 산업 발전에 도움이 될 것으로 판단되는 프로젝트에 자금을 지원할 수 있는 권한을 부여합니다. 여기에는 국제 기술 동향을 추적하고 협력 및 상용화를 지원하는 이니셔티브와 안전 기능, 개인정보 보호, 사회영향평가 및 기타 권리와 존엄성 보호에 중점을 둔 일련의 R&D 프로젝트가 포함됩니다. 시행령 은 이러한 프로젝트 에 대한 기준을 제시하는데, 여기에는 국가 AI 정책 준수, 교육 데이터 구축 및 활용 지원, 산업 성장 및 일자리 창출 지원, 경제적 이익 창출, 그리고 실용적이고 기술적으로 실현 가능해야 한다는 요건이 포함됩니다.

제14조는 정부가 AI 기술 표준 개발을 촉진하기 위해 표준을 직접 제정, 개정, 보급하고, 민간 부문의 표준화 추진 노력을 지원할 수 있도록 규정하고 있습니다. 또한, 정부는 국제 표준 제정 기관과의 협력을 강화해야 합니다.

제15조는 MSIT가 AI 학습 데이터의 생산, 수집 및 활용을 확대하는 정책을 주도하도록 요구합니다. 이 법안은 정부가 데이터 세트를 구축하고 공급하는 프로젝트에 자금을 지원할 수 있도록 권한을 부여하고, 특히 MSIT가 이러한 데이터 세트를 한곳에서 관리하는 "통합 제공 시스템"이라는 중앙 집중식 플랫폼을 운영하도록 요구합니다. 이 법안은 이 시스템이 민간 부문에서 무료로 사용할 수 있도록 제공되어야 하지만, 정부가 특정한 경우에 수수료를 징수할 수 있도록 권한을 부여하며, 자세한 내용은 나중에 대통령령으로 정할 예정입니다. 시행령은 제15조에 세부 내용을 추가하여 플랫폼이 사용자가 한곳에서 데이터 세트를 검색하고, 이를 명확하게 구성 및 추적하고, 다른 시스템과 연결하고, 품질 검사를 포함할 수 있도록 제안합니다. 시행령은 또한 수수료 징수를 위한 법적 근거를 제시하여 MSIT가 데이터의 유형과 용도에 따라 다른 요금을 부과할 수 있도록 허용하면서, 공공, 비영리 및 교육 사용자에 대한 면제를 요구하며, 전체 규칙은 부령으로 정합니다.

분석: 한국의 처방적 혁신 정책이 AI를 저해할 위험이 있다

한국은 정부가 AI 혁신 정책에 적극적인 역할을 해야 한다는 점을 올바르게 인식하고 있습니다. 강력한 AI 부문을 구축하는 데 필요한 투자(연구 개발, 데이터 인프라, 표준, 기술)는 그 혜택이 단일 기업을 넘어 훨씬 더 광범위하게 확산되기 때문에 시장의 투자가 저조한 전형적인 사례입니다. 민간 부문만으로는 산업의 번영을 위한 공동 기반을 구축할 수 없습니다. 한국이 AI 분야에서 경쟁력을 유지하려면 우선순위 설정, 초기 단계 연구 자금 지원, 데이터 세트와 같은 공동 자원의 확보에 있어 강력한 공공의 참여가 필수적입니다. 이러한 조항들의 의도는 이미 인프라를 포함하고 있는 이 대통령의 "AI 하이웨이" 구상을 기반으로, 한국이 AI 리더로서 부상하는 데 필요한 핵심적인 투자들을 추가하는 것으로 보입니다.[9]

하지만 이 법이 이러한 역할을 수행하는 방식은 혁신을 촉진하고자 하는 바로 그 자체를 저해할 위험이 있기 때문에 수정이 필요합니다. 과학기술정보통신부는 이미 2020년 제정된 국가연구개발혁신법에 따라 국가연구개발의 법적·관리적 틀을 담당하고 있지만, 연구개발 자체의 지침 전략은 이제 새로운 AI 기본법 제13조에 따라 결정되고 있습니다.[10] 윤리 및 안전과 관련된 특정 R&D 우선순위를 고정함으로써, 이 법은 정부 지원 연구가 어떤 분야에 집중해야 하는지 사실상 미리 정해 놓고 있습니다. 이러한 접근 방식은 한국 혁신 생태계에 가장 시급하거나 유망하지 않을 수 있는 분야에 투자를 집중시킬 뿐만 아니라, 한국이 글로벌 AI 개발 동향에 뒤떨어지는 결과를 초래할 위험이 있습니다.

표준과 관련하여 유사한 문제가 발생합니다. 제14조는 표준화의 중요성을 올바르게 강조하고 민간 부문의 노력을 인정하는 동시에 국제 표준 제정 참여를 확대하는 것을 목표로 합니다. 이는 한국 기업이 세계 시장에서 경쟁력을 유지하는 데 도움이 되는 중요한 조치입니다. 그러나 이 조항은 정부가 직접 표준을 제정해야 한다는 혼란스러운 암시를 던지고 있습니다. 기술 표준의 실제 개발은 공인된 표준 기구를 통해 업계에 맡기는 것이 가장 좋으며, 정부는 한국 기업의 적극적이고 영향력 있는 활동을 지원하기 위해 협력하고, 조정하며, 확보하는 역할을 해야 합니다. 정부가 표준을 지원하는 것에서 직접 제정하는 것으로 전환한다면, 업계 관행에 뒤처지는 규칙을 만들어내고 국제적으로 지지를 얻지 못할 위험이 있습니다.[11]

제안

- 국회는 제13조를 개정해야 한다. AI 기본법(AI 기술 개발 및 안전한 이용 지원)을 통해 규범적인 연구개발 우선순위를 폐지하고, 과학기술정보통신부가 유연한 국가 AI

연구개발 로드맵을 설계하고 업데이트할 수 있도록 권한을 부여합니다. 이러한 변화를 통해 한국의 투자는 시대에 뒤떨어진 의무 조항에 얽매이지 않고 세계적인 혁신을 따라갈 수 있게 될 것입니다.

- MSIT는 AI 기술 표준화에 관한 시행령 제14조에 따라 표준이 산업계에 지속적으로 적용되어야 함을 명확히 해야 합니다. 정부가 의장 및 조정자 역할을 하는 가운데, 산업통상자원부는 기업 간 협력, 국제 포럼 참여 지원, 기관 간 협력에 집중하는 동시에 기술 표준 개발을 산업 컨소시엄에 맡겨 한국의 접근 방식이 국제 관행과 일치하고, 기업들이 관련 시장에서 경쟁력을 유지할 수 있도록 해야 합니다.

한국의 AI 산업을 지원하는 산업 정책

두 번째 부분인 "AI 기술 개발 및 AI 산업 활성화"는 제 16 조 부터 제26조 까지를 다루며, 산업 정책으로 더 잘 설명될 수 있습니다. 이 부분은 기초적인 투입을 넘어 AI 기반 산업의 적극적인 사업화 및 성장에 초점을 맞춥니다.

제16조는 국가 및 지방자치단체가 기업 및 공공기관의 AI 도입 및 활용을 지원할 수 있도록 규정하고 있습니다. 지원에는 AI 제품 및 서비스 개발 및 보급 지원, 컨설팅 및 교육 제공(특히 중소기업, 벤처기업, 소기업 대상), 도입 비용 지원 등이 포함될 수 있습니다. 시행령에서는 구체적인 지원 방안을 제시하고 있습니다.

제17조와 제18조는 한국 AI 생태계에서 중소기업을 우선적으로 지원합니다. 제17조는 정부가 AI 관련 지원 정책을 시행할 때 중소기업을 우선적으로 지원하도록 규정하고 있으며, 제18조는 스타트업 창업자 지원, 교육 제공, 사업화 및 자금 조달 지원, 그리고 AI 기업가를 지원하는 기관 육성 사업을 허가합니다.

제19조는 정부가 경제의 다양한 부문이 AI 기술을 도입하고 운영에 통합하도록 장려하는 정책을 수립하도록 규정하고 있습니다. 또한, 정부는 국가 연구개발 체계 내에서 이러한 "AI 융합"과 관련된 연구개발(R&D) 프로젝트를 우선순위로 선정할 수 있도록 권한을 부여합니다. 즉, 정부는 어떤 연구 프로젝트에 자금을 지원할지 결정할 때 AI 기술을 특정 산업 과 결합하는 프로젝트를 구체적으로 선택할 수 있습니다.

제20조는 정부가 한국의 AI 산업 발전을 지원하기 위해 기존 시스템과 법률 및 규제 프레임워크를 개선하도록 요구하고, 이러한 개혁을 위한 연구 및 공개 협의에 대한 지원을 승인합니다.

제21조는 과학기술정보통신부(MSIT)에 국내 AI 전문 인력 양성 책임을 부여하고, 해외 인재 유치 정책을 승인합니다. 여기에는 글로벌 AI 전문 지식 모니터링, 국제 네트워크 구축, 외국인 전문가 의 국내 취업 지원, 해외 기관 및 국제기구와의 협력 촉진 등이 포함됩니다.

제22조는 정부가 글로벌 AI 동향을 추적하고 협력을 증진할 것을 의무화합니다. 정보 공유, 공동 연구개발, 국제 표준 참여, 외국인 투자 유치, 해외 마케팅, 윤리 관련 협력 등을 통해 해외 진출을 모색하는 기업에 대한 지원을 허용합니다. 공공기관이나 민간기관이 이러한 지원을 담당할 수 있으며, 정부 보조금이 지원됩니다.

제21조와 제22조는 인재 육성과 국제화를 다룹니다. 제21조는 과학기술정보통신부에 국내 AI 전문 인력 양성 및 해외 전문가 유치를 의무화하고, 제22조는 정부가 글로벌 AI 동향을

파악하고 국제 협력을 증진하도록 요구합니다. 여기에는 공동 연구개발(R&D)을 통한 기업의 해외 시장 진출 지원, 표준 제정 참여, 투자 유치, 마케팅 지원 등이 포함됩니다.

제23조부터 제25조까지는 산업 클러스터링, 공동 테스트베드, 컴퓨팅 용량 확대에 중점을 두고 있습니다. 제23조는 국가 및 지방자치단체가 기업과 기관을 연결하는 AI 클러스터를 지정하고 재정, 행정 및 기술 지원을 제공할 수 있도록 허용합니다. 제24조는 기업이 신기술을 시험, 인증 및 검증할 수 있는 실증 기지를 구축할 수 있도록 권한을 부여합니다. 제25조는 정부가 AI 데이터센터를 육성하고, 특히 중소기업과 연구기관의 AI 데이터센터 설립 및 활용을 지원하며, 지역 균형 발전을 촉진하도록 규정합니다. 시행령은 AI 클러스터 지정, 운영 기관 선정, 기업 테스트베드 개방 조건 등에 대한 세부 규정을 제시합니다.

마지막으로, 제26조는 인공지능 개발을 촉진하고, 조사 및 통계를 수행하고, 공동이용시설을 운영하고, 국제적 진출을 지원하고, 교육 및 인식 제고 캠페인을 실시하는 비영리 법인인 한국인공지능진흥협회를 설립하며, 정부의 보조금을 지원받습니다. 시행령은 협회 설립에 필요한 요건과 정관의 기준을 제시하고 있습니다.

분석: 산업 정책 조치는 규모에 구애받지 않아야 한다

한국의 접근 방식은 AI를 단순한 지원이 아닌 적극적인 산업 정책을 요구하는 전략 산업으로 간주하기 때문에 많은 부분에서 옳습니다. AI법은 경제 전반에 AI를 통합하고, 인재에 투자하고, 클러스터, 테스트베드, 데이터 센터를 구축함으로써 경쟁력을 여러 정책 영역에 접목합니다. 이는 글로벌 경쟁에 직면한 국가들이 필요로 하는 광범위하고 포괄적인 전략입니다. 시장만으로는 성과를 낼 수 없다고 가정하는 것이 아니라, 장기적인 산업적 우위를 뒷받침하는 주체, 인프라, 그리고 생태계를 의도적으로 강화하는 전략입니다.[12]

그러나 이 섹션의 여러 조항은 중소기업과 스타트업에 과도한 특혜를 주고 있습니다. 경제협력개발기구(OECD)가 2023년 한국의 혁신 정책 검토에서 지적했듯이, 중소기업은 일자리 창출의 핵심 동력이자 경제 전반에 디지털 기술을 확산하는 핵심 통로 역할을 하기 때문에, 한국이 중소기업과 스타트업에게 AI 경제에서 기회를 제공하는 것은 타당합니다.[13]그러나 이 법은 산업 정책 조치 전반에 걸쳐 중소기업에 우선권을 부여함으로써 지나친 과세를 하고 있습니다.

좋은 혁신 및 산업 전략은 규모에 구애받지 않고, 중소기업이 강점을 보이는 분야(민첩성, 실험성)를 지원하는 동시에 대기업이 가장 잘하는 분야 (자본 집약적 R&D, 규모 확장, 글로벌 시장 진출)에 집중할 수 있도록 지원해야 합니다. 중소기업을 "우선순위 고려"에 가두는 한국은 AI 투자와 글로벌 경쟁력의 대부분을 실질적으로 담당 하는 대기업으로부터 자원을 잘못 배분할 위험이 있습니다. 스타트업은 새로운 혁신을 개발할 수 있지만, 대기업의 규모와 수출 역량이 없다면 혁신이 세계 시장에 진출하기 어려울 수 있습니다. 다시 말해, 중소기업에 특혜를 주는 것은 겉보기에는 지원적인 것처럼 보일 수 있지만, 글로벌 경쟁력을 갖춘 AI 기업을 육성하는 한국의 장기적인 역량을 저해할 수 있습니다.[14]

제안

- 국회는 AI 기본법 제17조(AI 지원 정책에서 중소기업 우선 고려)를 개정하여 중소기업에 대한 "우선 고려" 의무를 삭제해야 합니다. 이 법은 규모에 구애받지 않는 내용을 채택하여 정부가 모든 규모의 기업을 각 기업의 강점에 따라 지원할 수 있도록

해야 합니다. 이를 통해 스타트업과 중소기업은 실험과 확산에 집중할 수 있고, 대기업은 자본 집약적인 R&D, 규모 확장, 그리고 글로벌 시장 진출에 필요한 지원을 받을 수 있습니다.

- 과학기술정보통신부는 중소기업과 대기업 간 지원이 균형을 이루도록 제18조(AI 스타트업 지원)와 제19조(AI 융합 정책)를 시행해야 합니다. 즉, 스타트업과 중소기업을 위한 교육, 사업화 지원, 조기 도입 프로그램을 지속적으로 제공하는 동시에, 대기업 이 핵심 산업에서 AI 활용을 확대하고 한국의 국제 경쟁력을 선도할 수 있도록 자원을 지원받을 수 있도록 해야 합니다. 과학기술정보통신부는 중소기업에만 유리하게 작용하는 것이 아니라 전체 AI 생태계를 강화하는 방향으로 자금 지원 프로그램, 교육 제도, 도입 인센티브를 설계해야 합니다.

제4장 인공지능윤리 및 신뢰성 확보

이 법 제4장(제27조~제36조)은 AI 관련 위험 관리의 초석입니다. 이 장은 연성법(soft law) 차원의 윤리적 조치(제27조~제30조)를 규정하고, 경성법(hard law) 차원의 규제 의무(제31조~제36조)를 부과하는 이중적 접근 방식을 통해 이를 실현합니다.

연성법(Soft law), AI 안전 중심 조치

이 법은 윤리를 최우선으로 하는 접근 방식을 취하며, 구속력 없는 원칙과 자발적 준수를 결합하여 AI 개발을 안내합니다. 제27조는 과학기술정보통신부(MSIT)가 안전성, 신뢰성, 접근성을 포괄하는 광범위한 윤리 원칙을 수립하고 공표할 수 있도록 권한을 부여합니다. 이러한 원칙은 법적 구속력은 없지만, 전체 AI 생태계의 기반이 될 것입니다. 이 프레임워크 준수를 촉진하기 위해 제28조는 기업, 대학, 연구기관이 자발적으로 민간 자율 AI 윤리위원회를 설립할 수 있도록 허용합니다. 자율 AI 윤리위원회는 준수 여부를 검증하고, 인권 문제를 조사하며, 내부 윤리 교육을 제공할 수 있습니다. 또한 제29조는 과학기술정보통신부가 AI로 인한 잠재적 위험으로부터 국민을 보호하기 위한 연구 개발을 수행하는 AISI를 설립할 수 있는 법적 근거를 제공 합니다. 마지막으로 제30조는 장관이 중소기업이 이러한 기준을 충족할 수 있도록 관련 정보, 행정 지원, 심지어 재정 지원까지 제공하도록 지시함으로써 자발적 검증 및 인증 제도를 지원합니다.

AI에 대한 엄격한 법률 및 규제 의무

이 법의 엄격한 규정은 제31조부터 제36조까지에 명시되어 있으며, AI 사업자에 대한 일련의 법적 구속력이 있는 의무를 규정하고 있습니다.

- 제31조는 AI 사업자에 대하여 (1) AI가 제품 또는 서비스를 운영하는 경우 이용자에게 통지하고, (2) 생성형 AI가 산출물을 생성하는 경우 이를 표시하며, (3) 음성, 이미지, 영상 등 합성 콘텐츠가 AI에 의해 생성된 경우 이용자가 이를 인지할 수 있도록 명확하게 공개하도록 규정하고 있습니다. 시행령 은 사업자가 이러한 의무를 유연한 통지 방식을 통해 이행하도록 [15]규정 하고 있습니다.
- 제32조는 대통령령으로 정하는 연산 한계값 이상으로 훈련된 인공지능(AI) 시스템을 개발하거나 제공하는 AI 사업자에 대해 수명주기 위험 관리 계획을 수립하고 이를 문서화하여 과학기술정보 통신부 에 제출하도록 규정하고 있습니다. 시행령은 이 연산 한계값을 10^{26} 개의 부동소수점 연산(FLOP)으로 제안하고 있습니다.

- 제33조는 AI 사업자가 자사 시스템이 고영향 시스템에 해당하는지 여부를 판단하기 위해 자체 평가를 실시하도록 규정하고 있습니다. 시행령 초안은 사업자가 과학기술정보통신부에 확인을 요청할 수 있는 공식 절차를 마련하고 있으며, 30일의 답변 기한(복잡한 경우 연장 가능)과 재확인 요청을 통한 이의신청 가능성을 명시하고 있습니다. 그러나 해당 법과 시행령은 이러한 검토를 정기적으로(예: 매년), 주요 시스템 업데이트 후, 또는 최초 배포 시에만 실시해야 하는지 명시하지 않아 검토 빈도 와 시점이 거의 정의되지 않았습니다.
- 제34조는 고영향 AI 시스템의 AI 사업자(이하 AI 사업자)가 위험 관리 계획을 수립하고, 사용자 보호 및 가능한 경우 결과에 대한 설명을 제공하며, 인적 감독을 시행하고, 이러한 조치에 대한 철저한 문서화를 유지함으로써 안전성과 신뢰성을 확보하도록 규정하고 있습니다. 시행령 은 사업자가 위험 관리 및 사용자 보호 조치의 핵심 요소(영업비밀 제외)를 공개하고 5년간 문서를 보관하도록 규정하고 있습니다.
- 제35조는 고영향 AI 시스템 운영자가 기본적 인권에 대한 잠재적 영향을 평가하기 위한 영향평가를 실시하도록 규정하고 있습니다. 시행령 은 영향평가의 적용 범위를 영향 집단, 위험에 처한 권리, 영향 및 완화 계획으로 제한하고 있으며, 사내 또는 제3자에 의한 영향평가를 허용하고 있습니다.
- 시행령 은 해당 기업 의 지정 기준을 연매출 1조 원 이상, 인공지능(AI) 서비스 단독 매출 100억 원 이상, 최근 3개월 동안 국내 이용자가 하루 평균 100만 명 이상, 또는 중대한 안전 사고 발생 후 시정 조치를 받은 기업으로 규정하고 있습니다.[16]

분석: AI 거버넌스를 위한 가벼운 비전이 엄격한 규칙으로 무너지다

한국 정책 입안자들의 의도는 자발적이고 윤리적인 조치와 업계의 자율 규제를 주도하는 것임이 분명해 보입니다. 그러나 제31조부터 제36조까지에 명시된 규제 의무 조항은 이러한 접근 방식을 약화시킵니다. 이러한 조항들은 유연성과 혁신에 대한 법의 강조점을 강화하는 대신, 의무적인 라벨링, 연산 임계값, 프로세스 중심 보고와 같은 단순하고 일률적인 규정에 의존하여 AI의 위험을 오진하고 감독을 왜곡합니다. 결과적으로 법의 가장 유망한 요소들은 형식적으로는 엄격해 보이지만 실제로는 효과가 없는 규제 도구에 의해 무산됩니다.

첫째, 데이터 혁신 센터(Center for Data Innovation)가 보고서 "AI 생성 콘텐츠 라벨링 의무가 부족한 이유"에서 설명했듯이, 제31조에서 요구하는 것과 같은 의무적인 AI 라벨링은 여러 가지 이유로 부족합니다.[17] 워터마크와 기타 마크는 기술적으로 취약하고 쉽게 제거될 수 있기 때문에 악의적인 행위자는 라벨링되지 않은 콘텐츠를 여전히 유포할 수 있습니다. 한국의 법은 영외 적용되기 때문에 한국에서 AI 서비스를 제공하는 해외 제공업체는 이를 준수해야 하지만, 한국 사용자가 관할권의 한계를 벗어나는 순간 해외 호스팅 플랫폼에서 라벨링되지 않은 콘텐츠를 접하게 됩니다. 이 법은 혼란을 줄이는 대신, "여기서는 AI 라벨링, 저기서는 안 됨"과 같은 혼란스러운 상황을 만들어 사용자들이 라벨링이 신뢰성의 확실한 지표라고 생각하게 만들 위험이 있습니다. 가장 중요한 것은 라벨링이 허위 정보, 지적 재산권 도용, 유해한 딥페이크와 같은 근본적인 우려를 해결하지 못한다는 것입니다. 이러한 우려는 획일적인 공개 규칙보다는 특정 문제에 대한 맞춤형 해결책을 요구합니다.

시행령은 보이지 않는 워터마킹 및 다양한 통지 방식 허용 등 공개 요건에 유연성을 더할 것을 제안하지만, 규제 기관은 핵심 규정 준수 도구로서 라벨링에 지나치게 의존해서는 안 됩니다.

대신, 정책 입안자들은 디지털 콘텐츠에 대한 신뢰를 더욱 광범위하게 구축하는 방향으로 전환해야 합니다. 즉, 사용자가 AI 및 인간 생성 콘텐츠의 출처와 이력을 확인할 수 있도록 암호화된 메타데이터를 내장하는 도구를 장려하여 모든 콘텐츠에 자발적인 출처 기준을 도입해야 합니다. 또한, 사용자가 오해의 소지가 있거나 불완전할 수 있는 라벨에 의존하기보다는 콘텐츠의 신뢰성을 직접 판단할 수 있도록 디지털, AI 및 미디어 리터러시에 투자해야 합니다. 마지막으로, 규제 기관은 광범위한 라벨링 요건보다는 허위 정보, 지적 재산권 침해, 딥페이크 등 특정 피해에 대한 구체적인 규칙을 수립하고, 문제별 해결책(예: 캠페인 공개 규칙, 지적 재산권 집행, 괴롭힘 방지법)을 제시해야 합니다.

둘째, 제32조처럼 어떤 AI 시스템을 엄격한 감시의 대상으로 삼아야 하는지 결정하기 위해 컴퓨팅 임계값을 사용하는 것은 심각한 문제가 있습니다. 컴퓨팅은 모델 학습에 사용된 리소스의 양만 측정 할 뿐, 모델 배포 방식의 후속 영향은 측정하지 않습니다. 스탠퍼드 대학교 연구자들이 설명했듯이, 컴퓨팅은 실제 기능, 새로운 행동 또는 위험에 대한 신뢰할 수 있는 예측으로 변환되지 않습니다.[18] 컴퓨팅 임계값은 실제로는 서투릅니다. 다양한 유형의 AI는 매우 다른 양의 컴퓨팅을 사용합니다. 대규모 언어 모델을 포착하는 수준은 강력한 비전 모델을 놓칠 수 있는 반면, 더 낮은 수준은 많은 무해한 시스템을 휩쓸 것입니다. 그리고 중요한 것은 미세 조정이나 인간 피드백을 통한 학습 중 작은 조정과 같이 추가 컴퓨팅 없이도 영향을 크게 증가시키는 방식으로 모델을 변경할 수 있다는 것입니다. 마지막으로, 칩이 더 빨라지고 알고리즘이 더 효율적이 됨에 따라 오늘날의 컴퓨팅 임계값은 빠르게 구식이 됩니다. 간단히 말해, 컴퓨팅은 쉬운 지름길처럼 보이지만 AI 규제의 주요 테스트로 사용하기에는 너무 둔하고 신뢰할 수 없습니다.

한국은 단순한 컴퓨팅 임계값에 의존하는 대신, 배포 후 평가 시스템을 도입해야 합니다.[19] 이는 AI 시스템이 배포된 후에 이루어지는 평가로, 학습에 사용된 컴퓨팅 용량이 아닌 실제 환경에서 시스템이 어떻게 작동하는지 에 중점을 둡니다. AI의 동작은 사용 환경에 따라 달라지기 때문에 배포 전 테스트에서 놓치는 위험과 실패를 파악할 수 있습니다. 예를 들어, 실험실에서는 안전해 보이는 모델이 의료, 금융 또는 교육 분야에 적용되면 매우 다른 성능을 보일 수 있습니다.

한국은 이미 AISI(AI 정보시스템연구원)를 설립했으며, 이 업무를 주도할 적임 기관입니다. AISI는 영향이 큰 지역에 배치된 모델을 테스트하고, 발생하는 사고나 장애를 수집 및 추적하며, 모델이 실제로 어떻게 기능하는지에 대한 명확한 결과를 발표해야 합니다.[20] 이러한 평가는 단순한 기술적 정확성을 넘어, 결과물이 사용자에게 이해 가능한지, 의도치 않은 위험을 야기하는지, 심지어 에너지 비용까지 고려해야 합니다. 이를 통해 정책 입안자와 대중은 AI가 현장에서 실제로 어떻게 작동하는지 확인할 수 있고, 한국의 감독은 유연하고 집중적인 관리를 유지할 수 있습니다. 이는 정적인 컴퓨팅 기준치로는 결코 달성할 수 없는 것입니다.

셋째, 제33조, 제34조, 제35조는 철저한 보고서, 위험 문서화, 그리고 평가가 의미 있는 책임으로 이어질 것이라는 전제 하에 절차의 투명성에 의존합니다. 그러나 서류 작업만으로는 진전이 보장되지 않습니다. 이는 포괄적인 것처럼 보이지만, 실제로는 단순한 체크리스트에 불과할 위험이 있습니다. 절차 규칙은 올바른 단계가 준수되었는지 여부를 측정하는 것이지, 시스템이 현실 세계에서 공정하고, 안전하며, 신뢰성 있게 작동하는지 여부를 측정하는 것이 아닙니다. 맥락과 사용 방식에서 위험이 발생하는 AI의 경우, 서류 작업만으로는 성과를 대체할

수 없습니다. 기업들이 성과 개선 없이 보고서와 규정 준수 파일을 작성하게 되고, 규제 기관이 기반 시스템을 테스트할 자원이나 전문 지식이 부족할 수 있다는 위험이 있습니다.

한국은 프로세스가 아닌 성과를 규제해야 합니다. 즉, 정책 입안자들은 절차적 체크리스트를 의무화하는 대신 성과 기반 요건을 설정해야 합니다.[21] 규제 기관은 AI 시스템이 구축 후 안전성, 공정성, 신뢰성이라는 측정 가능한 기준을 충족하는지 여부에 집중해야 합니다. 성과 기반 규제는 기업이 단순히 규정 준수 기준을 충족하는 것이 아니라 실질적인 성과를 달성하도록 보장합니다.

특정 하여 규제 함으로써 잘못된 방향으로 나아가고 있습니다. AI의 특정 활용이 사용자나 사회에 위험을 초래한다면, 누가 서비스를 제공하든 그러한 위험은 감독의 대상이 되어야 합니다. 외국 기업에만 더 엄격한 규칙을 적용하는 것은 국내 기업에 허점을 만들고, 공정성을 훼손하며, 보호 체계를 약화시킵니다. 기업의 소재지가 아니라 위험이 그 원인이 되어야 합니다.

제안

제4장의 규제 조항은 법의 나머지 부분을 훼손할 위험이 있습니다. 혁신 촉진, 경쟁력 강화, 시민 보호라는 법의 더 넓은 비전에 부합하도록 이러한 조항들을 입법 개정을 통해 재검토해야 합니다.

국회는 AI 기본법 에 다음과 같은 개정안을 제출 해야 합니다.

- 제31조(AI 투명성 확보 의무)를 개정하여 의무적 공개 요건을 삭제해야 합니다. 워터마크와 AI 라벨은 기술적으로 취약 하고 관할권 마다 일관성이 없으며, 정책 입안자들이 우려하는 허위 정보, 지식재산권 침해, 딥페이크 등 구체적인 피해를 해결하지 못하기 때문에 잘못된 안전감을 제공 합니다. 따라서 법은 과학기술정보통신부(MSIT)와 기타 부처가 C2PA(개인정보보호법)와 같은 자발적 출처 기준을 장려하고, 디지털 및 AI 리터러시 프로그램에 투자하며, 지식재산권 침해, 캠페인 투명성, 온라인 괴롭힘 등 특정 피해 에 대한 맞춤형 규칙을 채택하도록 지시해야 합니다.[22]
- 컴퓨팅 임계값 이상으로 훈련된 시스템에 대한 감독을 발동하는 제32조(AI 안전 보장 의무)를 개정하여 컴퓨팅 을 기준으로 삼는 것을 삭제합니다. 계산하다 사용 자체가 위험을 예측하는 신뢰할 수 있는 지표는 아닙니다. 대신, 법률은 AISI가 AI 시스템에 대한 배포 후 평가를 수행할 수 있도록 제12조를 개정해야 합니다. AISI는 영향이 큰 분야에 배포된 모델을 테스트하고, 장애 및 사고를 모니터링하며, 결과를 발표하여 감독이 임의적인 교육 입력이 아닌 실제 성능에 기반하도록 해야 합니다.
- 고영향 AI에 대한 광범위한 자체 평가, 문서화 및 위험 보고를 부과하는 제33~35조를 개정하여 프로세스 중심의 이러한 의무를 성과 기반 요구 사항으로 대체합니다. 이 법은 각 부처가 해당 분야의 AI 시스템에 대해 측정 가능한 성과를 설정 하도록 지시해야 하며, 한국표준과학연구원(KRISS)은 AI 시스템이 이러한 성과를 충족하는지 평가하는 평가 프로토콜을 설계하도록 지시해야 합니다. 이를 통해 감독 업무가 단순한 서류 작업에서 유의미한 성과 기준으로 전환될 것입니다.
- 제36조(국내대리인의 지정) 개정 외국 기업에 대한 엄격한 감독을 위한 기준인 수익 및 사용자 임계값을 제거합니다. 감독은 제공자가 국내든 해외든 관계없이 시스템이 고위험군 으로 지정된 경우에만 시행되어야 합니다. 이를 통해 동등한 대우를 보장하고,

임의적인 기준선을 없애며, 회사 규모나 위치 보다는 실제 위험에 대한 규제를 확립할 수 있습니다.

제5장 보칙

이 법의 제5장에서는 정부가 이 법의 조항을 어떻게 자금 지원하고, 모니터링하고, 집행할 것인지에 대한 운영 세부 사항을 제공합니다.

제37조는 정부가 AI 산업을 지원하기 위한 재정 자원을 확보하고, 연구개발, 인프라 및 기타 계획에 적절한 자금이 지원되도록 요구합니다.

제38조는 정책이 증거로 남도록 정기적인 조사와 통계 보고를 의무화합니다. 시행령 초안(제29조)은 이러한 조사의 범위를 더욱 구체적 으로 명시하여 산업 규모, 기업 매출, 인력 수급, 시설, 기술 동향, 글로벌 정책 동향, 투자 흐름 등을 포괄하도록 규정하고 있습니다. 또한 현장 조사, 문헌 조사, 설문조사 및 전자적 방법을 통한 데이터 수집도 허용합니다.

제39조는 업무의 효율적인 집행을 위해 전문기관에 업무를 위임할 수 있도록 규정하고 있습니다. 제30조 초안은 이 권한을 확대하여 과학기술정보통신부가 공공기관이나 협회에 AI 융합사업 지원, 데이터센터 활용, 산업조사 및 통계, 심지어 전문위원회 운영 등의 업무를 위탁할 수 있도록 규정하고 있습니다.

제40조는 과학기술정보통신부(MSIT)가 위반 사항이 의심되는 경우 자료를 요구하고, 조사 및 현장 검사를 실시하며, 위반 사항이 확인되는 경우 시정 명령을 내릴 수 있도록 허용합니다. 제31조 초안은 제한된 예외 조항을 규정하여, 충분한 증거가 이미 확보되었거나 민원이 경솔하거나 공무 방해 의도가 있다고 판단되는 경우 과학 기술정보통신부가 조사를 개시하지 않을 수 있도록 허용합니다.

마지막으로, 제 41조는 모든 위원과 위임받은 행위자에게 공직자 책임 기준을 적용하여 투명성과 집행의 성실성을 강화 합니다.

분석: 광범위한 데이터 수요는 규제 과잉의 위험을 초래합니다.

및 검사 수행에 대한 광범위한 권한 부여 위험 의 과도한 확대. 명확한 한계가 없다면 기업에 큰 부담을 주고, 혁신을 저해하며, 민감한 비즈니스 데이터 처리 방식에 대한 우려를 불러일으킬 수 있습니다.

제안

- 는 AI 기본법 제40조(데이터 요구 및 검사 권한) 시행령을 활용하여 AI 사업자로부터 어떤 데이터를 요청할 수 있는지, 어떤 감독 목적으로, 어떤 조건에서 요청할 수 있는지에 대한 명확한 지침을 마련해야 합니다. 요청 은 위험 관리 조치 또는 사용자 보호 관행 문서화 와 같이 법 준수 여부를 확인하는 데 꼭 필요한 정보로 제한되어야 하며, 관련 없는 사업 데이터에는 절대 적용되어서는 안 됩니다. 또한, 시행령은 민감한 상업 정보의 보호를 위해 강력한 기밀 유지 조치를 요구해야 합니다. 이러한 접근 방식은 불필요한 규정 준수 비용을 피하고 기업 의 독점 데이터를 보호하는 동시에 책임성을 유지할 수 있습니다.

제6장: 벌칙

제6장은 법 준수 의무 이행을 위한 처벌 규정을 규정하고 있습니다. 제42조는 이 법에 따른 업무 수행 중 취득한 사업자의 비밀정보를 유출한 자에게 3년 이하의 징역 또는 3천만 원 이하의 벌금을 부과합니다. 제43조는 외국 기업이 국내 대리인을 지정하지 아니한 경우, 기업이 생성형 또는 고영향 AI 시스템과 상호 작용하고 있음을 사용자에게 알리지 아니한 경우, 또는 정부의 시정명령을 이행하지 아니한 경우 등 세 가지 위반 행위에 대해 3천만 원 이하의 과태료를 부과합니다.

분석: 처벌은 위험과 피해에 비례해야 한다.

42조와 43조는 경미한 위반과 체계적인 피해를 구분하지 않습니다. 모든 위반 사항을 동일한 수준의 위험을 초래하는 것으로 간주하는 것은 실험을 저해하고, 규제 기관을 경미한 사례로 압박하며, 시민이나 AI 생태계를 진정으로 위협하는 심각한 위반에 대한 관심을 분산시킬 수 있습니다. 효과적인 운영 체계는 피해의 규모와 성격에 따라 처벌을 조정하여 혁신을 저해하지 않으면서 책임을 보장해야 합니다.

제안

- 는 AI 기본법 제42조(벌칙) 시행령을 활용하여 위반의 심각성과 영향에 따라 제재를 조정해야 합니다. 체계적 이거나 반복적인 위반에 대해서는 처벌을 강화하되, 경미하거나 초범인 위반에 대해서는 비례성을 유지해야 합니다. 시행령에 명확한 지침을 마련하면 책임 소재를 명확히 하는 동시에, 법에 따른 참여나 협조를 저해할 수 있는 지나치게 가혹한 처벌을 피할 수 있을 것입니다.
- 과학기술정보통신부(MSIT)는 시행령 제43조(행정 과징금)를 활용하여 과징금 부과 전 유예 기간을 설정해야 합니다. 이 전환 기간 동안 새로운 의무를 이행하지 않는 기업은 즉시 처벌보다는 경고 또는 시정 지침을 받아야 합니다. 이를 통해 국내외 사업자는 효과적인 규정 준수 시스템을 구축할 시간을 확보하는 동시에, 제도가 완전히 정착된 후에도 강력한 집행이 이루어질 수 있도록 보장할 수 있습니다.

결론

AI 기본법은 향후 10년간 한국의 AI 발전 방향을 제시할 것입니다. 이미 전략 및 산업 발전에 탄탄한 기반을 마련했지만, 무딘 획일적인 규칙은 이러한 성과를 무디게 만들 위험이 있습니다. 앞으로 나아갈 길은 결정적이고 실용적입니다. 구조적 결함을 해결하기 위해 법령을 강화 하고, 최종 시행령을 활용하여 위험 기반, 성과 중심의 균형 잡힌 규칙을 시행하는 것입니다. 한국이 이를 실천한다면, 이 법은 권리를 보호하고, 일상생활을 개선하는 혁신을 촉진하며, 글로벌 경쟁력에서 지속적인 우위를 확보할 것입니다.

부록: AI법 요약

제 1장 총칙

- 제1조(목적) 이 법은 인공지능(AI)의 건전한 발전을 도모하고 신뢰기반을 구축함으로써 국민의 권리와 존엄을 보호하고 삶의 질을 향상시키며 국가경쟁력을 강화함을 목적으로 한다.
- 제2조(정의) 주요 정의는 표 1 에 정리되어 있다.

- 제3조(국가의 기본 원칙 및 책임) : 안전, 신뢰성, 이해관계자의 설명권, 사업자의 창의성 존중, 사회적 적응을 위한 정책의 원칙
- 제4조(적용범위) : 영토외 적용 및 국방·안보에 관한 예외를 포함한 적용범위
- 제5조(다른 법률과의 관계) 다른 법률을 제정 또는 개정할 때의 법률의 우선권 및 법률과의 정합성의 요건

2장: AI의 건전한 발전과 신뢰 기반 기반을 위한 추진 시스템

- 제6조(AI 기본계획의 수립) 과학기술정보통신부 가 기본계획을 수립하는 목적, 수립해야 할 내용 및 다른 법률과의 관계
- 제7조(국가AI위원회) 국가AI위원회의 구성, 목적, 구성, 위원장의 역할, 위원의 임기, 비밀유지 의무 및 임기 제한 등에 관한 사항
- 제8조(위원회의 기능) 위원회의 구체적인 기능은 다음과 같습니다. 기본계획, 정책, 연구개발 전략 및 규정 심의. 위원회의 권고 기능
- 제9조(회원의 제척, 회피 및 기피) 이해상충 방지를 위한 규정
- 제10조(소위원회 등) 소위원회, 전문위원회 및 자문단의 설치에 관한 규정
- 제11조(AI정책센터) AI정책센터의 AI정책 및 국제규범 개발에 대한 역할
- 제12조(AI안전연구소) AISI의 설립 및 기능 “AI안전” 확보 및 국민보호

제3장 : AI 기술 개발 및 산업 진흥(인공지능 기술 개발 및 산업 발전)

1부: AI 산업 기반 구축(인공지능산업 기반 동의)

- 제13조(AI 기술 개발 및 안전 이용 지원) AI 기술의 연구개발, 사업화 및 안전 이용을 위한 정부 지원
- 제14조(AI 기술 표준화) 정부의 AI 기술 표준화, 학습 데이터 표준화, 안전 확보 노력
- 제15조(AI 학습데이터 관련 정책 수립) AI 학습데이터의 생산·수집·관리·유통을 위한 정책 및 제도의 수립

2부: AI 기술 개발 및 AI 산업 활성화(인공지능기술 개발 및 인공지능산업 활성화)

- 제16조(AI 기술 도입 및 활용 지원) 기업 및 공공기관의 AI 도입 및 활용 지원
- 제17조(중소기업 등에 대한 특별지원) 중소기업 우선지원 원칙
- 제18조(창업활성화) 인공 지능(AI) 관련 창업기업 지원
- 제19조(AI 융합 촉진) AI와 타산업의 융합을 촉진하는 정책
- 제20조(제도 개선 등) : 정부의 법령 개선 의무
- 제21조(전문인력 확보) 국내외 AI 인재 육성 및 확보 정책
- 제22조(국제협력 및 해외시장 진출 지원) 국제협력 및 기업의 해외시장 진출 지원
- 제23조(AI 클러스터 지정 등) AI 클러스터의 구축 및 지원
- 제24조(AI 검증 인프라 구축 등) AI 기술 검증 및 시험을 위한 시설·장비 구축

- 제25조(AI 데이터센터 관련 정책 추진 등) AI 데이터센터의 설립 및 운영을 위한 정책
- 제26조(한국AI진흥협회의 설립) 인공지능진흥을 위한 민간협회의 설립에 관한 사항

4장: AI 윤리 및 신뢰성(인공지능윤리 및 신뢰성 보장)

- 제27조(AI 윤리원칙 등) AI 윤리원칙 및 실행방안의 수립·보급
- 제28조(민간자율인공지능윤리위원회 설치) 민간윤리위원회의 설치 및 그 기능의 임의성
- 제29조(AI 신뢰도 제고 정책 수립) : 위험 최소화 및 신뢰기반 구축을 위한 정부 정책
- 제30조(AI 안전성 및 신뢰성 검증·인증 등 지원): 중소기업을 중심으로 자발적 검증·인증 활동을 지원합니다. 특히, 고부가가치 AI에 대한 의무를 강조합니다.
- 제31조(AI 투명성 확보 의무) AI 운영자의 투명성 의무에는 고영향·생성형 AI에 대한 사전 공지, AI 생성 콘텐츠에 대한 명확한 라벨링 등이 포함된다.
- 제32조(AI 안전성 확보 의무) 일정 계산 임계값을 충족하는 AI 시스템에 대한 안전 의무
- 제33조(고영향 AI 검증) AI 사업자가 자사의 AI가 고영향 AI인지 검증하도록 하는 의무 및 정부 확인 요청 절차
- 제34조(고영향 AI 관련 사업자의 의무) 고영향 AI에 대한 사업자의 구체적인 조치(위험 관리, 설명 가능성, 사용자 보호, 인적 감독 등)
- 제35조(고영향 AI 영향평가) 사업자의 인권영향평가 실시에 대한 노력기반 의무화
- 제36조(국내대리인 지정) 외국 AI사업자의 국내대리인 지정 의무

5 장 보칙

- 제37조(AI 산업 진흥을 위한 재원 확충 등) 정부의 AI 진흥 재원 확보 의무
- 제38조(실태조사·통계 및 지표) 정부의 조사 및 통계작성의무
- 제39조(권한의 위임 및 업무의 위탁) 다른 국가기관 또는 단체에 대한 권한의 위임 및 위탁에 관한 규정
- 제40조(사실조사 등) 정부의 AI 운영자 위반행위 조사권
- 제41조(벌칙 적용 시 공무원으로 간주되는 경우) 비공개위원 및 위탁받은 직원을 벌칙 적용 시 공무원으로 간주하는 규정

제6장 벌칙

- 제42조(벌칙) 비밀누설죄의 처벌
- 제43조(과태료) 특정 위반행위(신고하지 아니함, 국내대리인 지정하지 아니함, 시정명령 불이행 등)에 대한 과태료

부록(부칙)

- 발효일, 준비 행위 및 기존 법인에 대한 특별 조항

감사의 글

저자들은 로버트 D. 앳킨슨(Robert D. Atkinson) ITIF 회장, 에리카 샤퍼 ITIF 수석 디지털 커뮤니케이션 매니저에게 감사의 뜻을 전합니다.

저자들은 또한 편집에 도움을 준 랜돌프 코트 ITIF 최고 커뮤니케이션 책임자(CCO) 및 매니징 에디터에게 감사를 표하고 싶습니다.

모든 오류나 누락은 저자의 책임입니다.

저자 소개

김세진은 ITIF 산하 한국 혁신경쟁력센터의 부소장(Associate Director)으로 한·미 AI, 블록체인, 우주, 로보틱스 등 신흥 기술 분야와 국가경쟁력 정책을 연구하고 있습니다. 주요 저서로는 "중앙은행 디지털 화폐(CBDC)의 최근 발전 방향"(2020년 12월, Reuters Refinitiv 등재), "WeMix, Web3 Gaming and Ethics"(2023년 1월), "2025 글로벌 기술 트렌드: 17가지 트렌드 혁명이 온다"(2024년 11월) 등이 있습니다.

호단 오마르는 ITIF 산하 데이터혁신센터(Center for Data Innovation)의 수석 정책 관리자로 AI 정책 등을 연구하고 있습니다. 이전에는 런던에서 기술 및 위험 관리 부문 수석 컨설턴트로, 베를린에서 암호경제학자로 근무했습니다. 에든버러대학교에서 경제학 및 수학 석사 학위를 취득했습니다.

ITIF 소개

정보기술혁신재단(Information Technology and Innovation Foundation, ITIF)은 미국 워싱턴 DC에 본부를 둔 독립적인 501(c)(3) 비영리·초당적 연구 및 교육 기관으로, 과학기술 정책 분야에서 세계 최고 싱크탱크로 수 차례 인정받았습니다. ITIF의 사명은 혁신을 가속화하고 생산성을 높여 경제 성장, 기회 창출, 사회적 진보를 실현할 수 있는 정책 해법을 도출하고 평가하며 확산하는 것입니다. 자세한 내용은 itif.org/about에서 확인할 수 있습니다.

한국혁신경쟁력강화센터(CKIC) 소개

워싱턴 DC에 위치한 ITIF 산하 기관인 한국혁신경쟁력센터(Center for Korean Innovation and Competitiveness, CKIC)는 한국이 다음 경제 단계로 나아갈 수 있도록 실현 가능한 정책 해법을 제시하는 데 주력하고 있습니다. 본 센터는 신기술 산업, 산업의 스케일업, 노동시장 개혁을 토대로 한 혁신 주도형 경제로의 전환을 지원함으로써 한국의 장기 경쟁력을 강화하는 것을 사명으로 삼고 있습니다. 본 센터는 한국과 미국의 정부, 산업계, 학계와 긴밀히 협력하고 있으며, 자세한 내용은 itif.org/centers/korea에서 확인할 수 있습니다.

각주

1. 법제처 국가법령정보센터, 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 (약칭: 인공지능기본법), 2025년 1월 21일, https://www.law.go.kr/LSW//lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%9D%B8%EA%B3%B5%EC%A7%80%EB%8A%A5#undefined.
2. 과학기술정보통신부(MSIT), [국가인공지능전략위 보도참고] 국가 최상위 AI 전략 논의기구, 대통령 직속 「국가인공지능전략위원회」 출범, 2025년 9월 8일, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&pageIndex=8&bbsSeqNo=94&nttSeqNo=3186222&searchOpt=ALL&searchTxt=.
3. 콘텐츠 출처 및 진위성 연합(C2PA), "콘텐츠 출처 및 진위성을 위한 기술 표준", 2025년 9월 15일 접속, https://c2pa.org .
4. 패트릭 그레이디, "AI 법은 기술 중립적이어야 한다", 2023년 2월 1일, https://www2.datainnovation.org/2023-ai-act-technology-neutral.pdf .
5. 제6조(인공지능 기본 계획의이므로) ① 과학기술정보통신부 장관은 중앙행정기관의 장 및 지방자치단체의 장의 대기를 수신 3년마다 인공지능 기술 및 인공 지능산업의 진흥과 국가경쟁력을 위해 인공지능 기본계획(이하 “ 기본계획 ” 이라 해야 합니다)을 제7조에 따라인공지능위원회의 심의 · 증거의 관계를 맺어두고 변경 및 저장해야 합니다. 법제처 국가법령정보센터, 인공지능 발전과 신뢰 기반을 이해하는 기본법(약칭: 인공지능기본법), 2025년 1월 21일, https://www.law.go.kr/LSW//lsSc.do…
6. 과학기술정보통신부(MSIT), 「국가위원회 AI 전략 논의기구, 트럼프 직속 ' 국가인공지능 전략위원회 '' 보도자료, 2025년 9월 8일, https://www.msit.go.kr/bbs/view.do;jsessionid=Q8c56HbMdJ25UAapjE_TRv2pnofxRLT_D4knAwt0.AP_msit_1?sCode=user&mPid=208&mId=307&bbsSeqNo=94&nttSeqNo=3186222 .
7. 과학기술정보통신부, 「한국형 ' 과학기술×인공지능 ' 본격 추진」 보도자료, 2025년 9월 10일, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3186242 .
8. 과학기술정보통신부(MSIT), 「혁신경제의 두 엔진, 지능과 과학기술로 미래 성장을 견인하겠습니다」 인공 보도자료, 2025년 9월 3일, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3186192 .
9. 과학기술정통부(MSIT), “ 배경훈 등록, ' 회원가입 등록식 및 간담회 ' 개최 ” , 2025년 08월 29일. https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3186186 ; 대한민국 AI고속도로를 통해 AI 3대 강국 도약, 2025년 6월 23일, https://www.korea.kr/multi/visualNewsView.do?newsId=148944771 .
10. 국가연구개발혁신법(2020): 국가연구개발 프로그램 및 투자의 계획, 조정 및 관리에 있어 과학기술정보통신부의 역할을 확립 , https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62484&lang=ENG ; 과학기술정보통신부, 중장기 국가연구개발투자전략(2023-2027): 연구개발 우선순위 설정에 있어 과학기술정보통신부의 중심적 역할을 확인. 과학기술정보통신부 보도자료 ; AI 기본법 제13조(2024): 국제 동향 추적, 협력 및 사업화, 안전, 개인정보 보호, 사회적 영향 및 권리 보호에 중점을 둔 연구개발 등의 분야에서 정부 자금 지원 승인. 영문 번역 , https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf .

11. Nigel Cory, “Biden 행정부의 기술 표준 전략 분석: 좋은 점, 나쁜 점, 그리고 개선 아이디어”(ITIF, 2023년 10월 10일), https://itif.org/publications/2023/10/10/unpacking-the-biden-administrations-strategy-for-technical-standards-the-good-the-bad-and-ideas-for-improvement/ .
12. 로버트 D. 앳킨슨, "미국 경제 정책의 구조에 전략적 산업 경쟁력을 통합하다"(ITIF, 2022년 2월 7일), https://itif.org/publications/2022/02/07/weaving-strategic-industry-competitiveness-fabric-us-economic-policy/ .
13. OECD, OECD 혁신 정책 검토: 한국 2023, OECD 출판, 2023, https://www.oecd.org/en/publications/oecd-reviews-of-innovation-policy-korea-2023_bdcf9685-en.html .
14. Robert D. Atkinson 및 Eric Kang, "미국 혁신에서 대기업과 중소기업의 역할에 대한 국가경제위원회의 잘못된 이해" (ITIF , 2023년 7월 20일), https://itif.org/publications/2023/07/20/nec-gets-it-wrong-on-roles-of-big-and-small-firms-in-us-innovation/ .
15. 시행령 초안 제22조는 이러한 고지가 계약서, 매뉴얼 또는 서비스 약관, 화면 또는 장치 표시, 제공 장소의 물리적 게시 또는 과학기술정보통신부 (MSIT) 가 승인한 기타 방법 등 여러 채널을 통해 제공될 수 있다고 명시하고 있습니다. 생성 AI의 경우, 출력물은 사람이나 기계가 읽을 수 있는 형태로 레이블을 지정할 수 있으며, 보이지 않는 워터마킹(예: 출처 표준)은 허용되는 옵션으로 인정됩니다. 또한 이 시행령은 공개 내용이 주요 사용자 그룹에 쉽게 인식되고 적절해야 한다고 규정하고 있습니다. AI 기반이 이미 자명한 경우, 시스템이 내부 업무 목적으로만 사용되는 경우 또는 장관이 고시로 추가 사례를 지정하는 경우에는 예외가 적용됩니다. 과학기술정보통신부(MSIT), AI기본법 하위법령 제정방향, 2025년 9월 8일.
16. 시행령 초안 제28조에서는 제1항 제1호 및 제2호에 따른 수입기준액을 전년도(법인의 경우 전년도) 평균환율을 기준으로 대한민국 원화로 산정하도록 명시하고 있습니다. 과학기술정보통신부(MSIT), AI기본법 하위법령 연결방향, 2025년 9월 8일.
17, “AI 생성 콘텐츠 라벨링 의무가 부족한 이유”(Center for Data Innovation, 2024년 12월 16일), https://datainnovation.org/2024/12/why-ai-generated-content-labeling-mandates-fall-short/ .
18. Rishi Bommasani, "Drawing Lines: Tiers for Foundation Models", 스탠포드 기초 모델 연구 센터, 2023년 11월 18일, https://crfm.stanford.edu/2023/11/18/tiers.html .
19. Hodan Omaar, “미국은 캘리포니아에서 글로벌 AI 무대를 장악하여 배포 후 안전으로 전환해야 한다”(Center for Data Innovation, 2024년 10월 28일), https://datainnovation.org/2024/10/the-us-should-seize-global-ai-stage-in-california-to-shift-gears-to-post-deployment-safety/ .
20. Daniel Castro, “AI 사고 및 취약성 추적”(Center for Data Innovation, 2024년 4월 4일), https://datainnovation.org/2024/04/tracking-ai-incidents-and-vulnerabilities/ .
21. Daniel Castro, “AI 혁신에 해를 끼치지 않는 규제를 위한 10가지 원칙”(ITIF, 2023년 2월 8일), https://itif.org/publications/2023/02/08/ten-principles-for-regulation-that-does-not-harm-ai-innovation/ .
22. 콘텐츠 출처 및 진위성 연합(C2PA), "콘텐츠 출처 및 진위성을 위한 기술 표준", 2025년 9월 15일 접속, https://c2pa.org .