

NRC

POLICY BRIEF

 경제·인문사회연구회
NATIONAL RESEARCH COUNCIL FOR ECONOMIC, HUMANITIES AND SOCIAL SCIENCES

2024
ISSUE 78

발행년 2024년

발행처 경제·인문사회연구회

주소 세종특별자치시 시청대로 370

세종국책연구단지 연구지원동(A)

전화 044-211-1160

Homepage www.nrc.re.kr

인공지능 시대의 경쟁력 강화를 위한 AI 규제 연구

김정욱 한국개발연구원 선임연구위원 외

본 연구는 인공지능 기술이 확산되는 시대를 맞아 산업 발전과 경쟁력을 강화하기 위한 AI 규제 방향과 개선 과제를 모색하는 데에 목적이 있다. 이를 위해 글로벌 규제 현황과 금융, 제조업, 보건 의료 분야의 데이터, 안전과 신뢰, 윤리 문제를 분석하기 위해 연구기관 전문가와 협동 연구를 수행하였다.

※ 이 글은 경제·인문사회연구회(NRC) 협동연구과제 『인공지능 시대의 경쟁력 강화를 위한 AI 규제 연구』 보고서 제3장 제3절의 내용을 요약한 것입니다. 이 보고서는 국가정책연구포털 (nkis.re.kr)에서 볼 수 있습니다.

• • • Key Messages and Proposals • • •

- 인공지능 규제 방안을 모색함에 있어 AI 기술 발전 단계와 규제 쟁점의 변화를 중요하게 고려해야 하고, AI 위험과 쟁점, 해결 방안 관련 연구와 정보수집, 사례 축적을 통해 규제 역량을 강화해야 한다. AI 규제는 신중한 접근이 요구되고, AI 규제를 계속 보완하고 개선하는 거버넌스가 필요하다. AI 기술과 산업 육성에 필요한 정책 추진과 AI 안전과 신뢰 확보를 위한 다양한 규제 방안들을 종합적으로 고려해야 한다.
- 경쟁력 제고를 위한 AI 기술 활용과 규제 쟁점이 산업마다 다르며 산업별 규제 접근이 필요하다. 요컨대, 금융 분야는 오·남용을 방지하고 AI 의사결정의 신뢰성과 공정성 확보를 위해 알고리즘의 투명성과 설명가능성을 제고하며, 시스템 위험을 예방하는 방안이 중요하다. 제조 분야는 기업 간, 산업 간 데이터 공유와 연계를 활성화하고 방대한 데이터를 안전하게 수집, 저장, 처리할 수 있는 인프라 구축이 필요하고, 제조 프로세스 전반에 AI 기술을 접목하여 생산성과 품질 제고, 물류 관리, 운영비용 절감을 확대하는 정책이 강화되어야 한다. 의료·보건 AI 경쟁력을 위해서, 데이터의 민감성을 고려하고 보호하는 차원을 넘어, 양질의 보건 의료 데이터를 안정적으로 확보하고 활용할 수 있도록 하는 거버넌스 체계 구축이 선결 과제다.

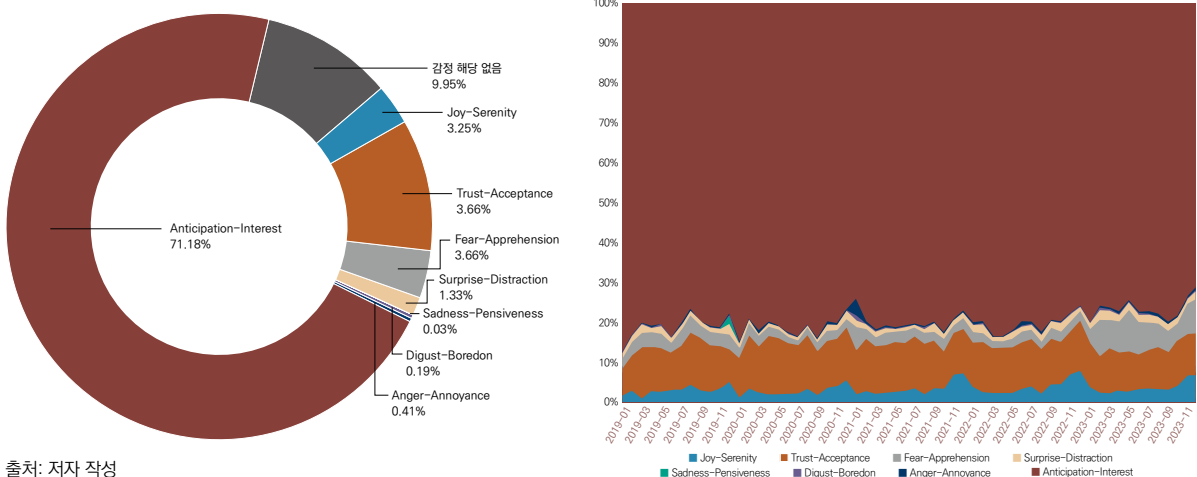
- AI 산업의 경쟁력 강화를 위해 규제실험 수단을 다양하게 활용하는 방안을 검토할 필요가 있다. EU 인공지능법의 경우도 AI 혁신과 발전을 위한 주요 규정으로 AI 규제 샌드박스, 실사용 테스트, 중소기업 및 스타트업 지원에 관한 규정을 포함하며, OECD는 AI 샌드박스를 다른 규제 및 제도적 메커니즘과 결합하여 시행함으로써 기술혁신을 촉진할 수 있음을 강조하고 있어 참고할 만하다.
- 국내 AI 산업 경쟁력을 강화하기 위해 규제실험 수단 활용을 고려해야 한다. 특히, AI 기술 활용 사업을 대상으로 AI 표준과 샌드박스를 결합하는 방향을 검토하고, 중소기업 지원에 중점을 둔 샌드박스 활용이 필요하며, 특정 AI 기술 분야를 대상으로 명확하게 정의된 테스트 환경을 제공하고, 공공 부문과 민간이 해당 규제를 함께 만드는 방안을 검토해야 한다. 그리고 사회적 영향이 클 것으로 예상되는 산업 분야를 특정하여 샌드박스를 운영하는 방안을 고려할 수 있다.

01

미디어 텍스트에 기반한 AI에 대한 감정분석

AI 확산에 따른 사회경제적 파급효과가 광범위한 분야에서 나타나고 AI 위협에 대한 인식이 고조되면서 AI 위협과 피해를 줄이는 규제 필요성에 관한 논의가 증가하고 있다. 2019년부터 2023년까지 우리나라 미디어에 게시된 AI 관련 기사에 담긴 국민의 감정을 분석한 결과, ‘기대감과 관심(붉은색)’의 감정이 71.18%로 가장 큰 비중을 차지했고 다음으로 ‘신뢰와 수용’이 10%, 환희와 평온이 3.25%로 나타났다. ‘공포와 불안’, ‘놀람과 산만’, ‘화남과 불쾌감’ 등 우려하고 불쾌해하는 5가지 항목의 부정적인 감정은 전체의 8% 미만이었다.

〈그림 1〉 감정별 기사 비중 분포 및 시계열 변화 추이



출처: 저자 작성

그러나 개인 정보 유출과 같은 사고가 잇따르고 생성형 AI가 개발되면서 AI에 대한 부정적 인식도 증가하는 추세다. 특히 ‘화남과 불쾌감(파란색)’과 ‘분노와 불쾌감(회색)’의 감정이 증가하는 상황이다. AI에 관한 올바른 이해 및 활용법 확산과 함께 앞으로 실제 나타날 수 있는 피해를 대비해야 한다.

02

AI 규제 쟁점의 세 가지 축: 데이터, 안전, 윤리

세계 주요국은 AI 활용을 확산하고 이를 바탕으로 기업과 산업의 효율성과 혁신, 경쟁력 제고를 달성하기 위해 노력하고 있다. AI 활용과 관련 산업을 육성하여 경제 성장과 발전에 새로운 동력을 확보하겠다는 기대가 확산되고, 이를 위한 진흥 정책이 강화되고 있다.

한편, AI 개발과 사용의 올바른 방향과 원칙을 제시하기 위한 논의도 활발하다. OECD, UN 등 국제기구와 주요국은 AI 원칙, 가이드라인, 권고 등 AI 개발과 사용의 방향성을 제시하고 규제하는 기준을 채택하고 있다. 국제적으로 채택된 주요 AI 원칙, 가이드라인, 권고 등을 종합적으로 분석하여 이러한 공식 문서가 필수적으로 다루고 있는 AI 규제 쟁점을 알아보았다.

〈표 1〉 AI 규제 쟁점의 세 가지 축(데이터, 안전, 윤리)과 영역별 특징

구 분		데이터 수집·처리	안전성 확보	윤리적 사용
		개인정보보호, 데이터 품질 및 편향	AI 시스템의 안정성, 신뢰성, 견고성, 보안	AI의 공정성, 투명성, 책임성, 편향 해소
주요 이슈		개인정보 유출, 보안 위협, 데이터 무단 수집	시스템 취약점, 사이버 공격, 데이터 손상 및 유실	AI 기술의 사회적 수용성, 인권, 다양성, 차별 문제
규제·관리 영역		개인정보보호, 데이터 관리 및 보안, 데이터 소유권과 접근권, 데이터 투명성	시스템 신뢰성, 예측가능성, 위험 평가와 관리, 표준 및 인증, 테스트와 검증	차별적 알고리즘과 편향적 데이터 처리, 개인 프라이버시 보호
중요 논의 기점 및 사건		GDPR(2018), CCPA(2020)	자율주행차 사고(2016), 금융 AI 시스템 오류 사례	채용 AI 시스템, 얼굴 인식 AI 등
적용 사례		개인정보보호, 데이터 최소화, 데이터 주권, 머신 언러닝(Machine Unlearning)	자율주행차, 의료 AI 시스템 안전성, 금융 AI 시스템 보안	채용 AI 시스템, 신용평가 AI의 공정성 및 투명성, 얼굴 인식 AI와 인권 보호
주요 규제안		법적 프레임워크, 규제 법안, 데이터 보호법 -사례: EU GDPR, 미국CCPA, 캐나다 PIPEDA	기술 표준, 안전 프레임워크, 규제 및 인증 체계 -사례: ISO/IEC 표준, NIST프레임워크, EU AI Act	윤리 가이드라인, 국제 원칙, 권고 사항 및 가이드라인 -사례: 아실로마 AI 원칙, EU 집행위원회 신뢰할 수 있는 AI 가이드라인, UNESCO AI 윤리 가이드라인, OECD AI 원칙
규제 고려 사항	기술적	데이터 품질, 적합성, 정확성, 개인 정보보호 보장	시스템의 보안성, 안정성, 신뢰성	알고리즘의 공정성, 편향 제거, 설명 가능성
	사회적	데이터 소유권, 투명성, 사용자 동의와 권리	시스템의 예측 가능성, 리스크 관리, 사용자 보호, 공공 안전	사회적 책임, 인권 보호, 차별 금지
	문화적	데이터 프라이버시와 보안에 대한 문화적 인식 차이	안전성에 대한 문화적 인식, 리스크 허용 수준의 차이	윤리에 대한 문화적 차이, 공정성과 정의에 대한 인식 차이

출처: 저자 작성

분석 결과, AI 규제 정책이 공통으로 다루는 세 가지 주요 쟁점은 데이터, 안전과 신뢰, 윤리적 문제와 관련 있었다. 각 쟁점의 축은 배타적인 구분이 아니고 서로 밀접하게 관련되고 상충하는 경우도 있다. 본 연구는 주요 국제기구와 국가들이 채택한 다양한 AI 규제 정책이 이 세 가지 축을 중심으로 대응 방안이 논의되고 관련 규제를 시행하기 위해 노력하고 있음을 확인하였다.

안전성 문제와 관련하여, 기술적 문제와 제도적 문제가 구분된다. AI 기술과 시스템이 갖는 자체적인 결함이나 오류, 기술적 한계와 관련된 위험이 중요한 사안으로 논의되고 있으며, AI 기술을 보완하고 개선할 수 있는 기술적 해결 방법을 찾는 노력이 계속되어야 한다. 또한 알고리즘 설계의 견고성을 확보하기 위해 AI 개발과 사용의 생애주기를 모니터링하고 문제를 보완, 개선하는 순환적 관리 체제가 필요하다. 실제로 이에 관한 대응 방안 모색이 활발하며 AI 규제 정책의 일부로 중요하게 고려되어야 한다.

AI 규제 필요성 논의의 또 다른 축은 데이터 문제에 관한 것이다. AI 데이터의 개인정보 유출을 방지하고 데이터 오남용 규제가 중요한 사안으로 논의된다. 이와 함께, AI 시스템의 편향성을 줄이고 AI 학습데이터의 질적 문제를 해소할 필요가 있다. 데이터의 질을 제고하고 양질의 데이터가 계속 공급되고 관리될 수 있어야 한다.

데이터, 안전과 신뢰, 편향성 문제를 해소하기 위해 다양한 표준이 개발되고 있다. AI 기술 개발과 사용 확산에 있어 AI 표준은 중요한 역할을 한다. 표준은 자발적 참여가 바탕이 되고 이행 강제성이 높지 않으나 산업 진흥과 경쟁력 강화 관점에서는 유연한 규제 방식이 될 수 있다. 그러나 AI 오용과 남용, 불법 사용 등 부적절한 AI 사용에 따른 위험 규제는 이행 강제성이 강화된 규제 방식을 고려할 필요가 있다.

AI 등장으로 새롭게 논의되는 규제 쟁점은 윤리 문제다. 글로벌 규제 논의 동향을 보면, AI 윤리에 관한 원칙과 상위 기준이 채택되고 있고 인권 보호와 연관되어 논의가 진행되고 있다. AI 윤리 논의는 보편적 가치와 연결되고 보편적 가치를 추구하며 꾸준한 장기적 접근이 필요하다. 규제 정책 측면에서는 윤리 문제와 관련된 사안을 명확하게 설명하고 검증하는 과정이 필요하다.

03

국내 AI 국가정책 동향

우리나라는 「AI R&D 전략」, 「AI 국가전략」, 「디지털 뉴딜 정책」 등 범정부 정책을 통해 AI 개발과 사용을 촉진하고 2023년 「AI 일상화 및 산업 고도화 계획」, 「초거대 인공지능 경쟁력 강화 방안」 수립하여 추진하고 있다. 국내 정책을 종합적으로 보면, 연구개발 촉진, 활용 확산, 인력 양성, 안전과 신뢰 구축 등 부처별 다양한 정책과 전략을 통해 사회경제 전반에 걸친 AI 진흥과 대응에 주력해 온 것을 확인할 수 있었다. 또한 AI 관련 일반적인 정책과 규제보다 특정 산업이나 분야를 대상으로 하는 경우가 더 많았고, AI 육성과 개발이 목적인 정책이 다수였다. 일반적 규제면서 AI의 사회적·윤리적 문제에 대응하기 위한 정책은 소수에 불과했다. AI 윤리 기준, 신뢰성 확보, 안전성과 같이 AI의 역기능을 방지하고 중요한 가치를 증진하기 위해 시행된 정책들은 현재

〈표 2〉 범정부 AI 전략의 중점과제 비교 (2024년 5월 현재)

정책명	발표시기	목 적	중점산업	윤 리	신뢰성	정보보안	데이터 활용	규 제
인공지능(AI) R&D 전략	2018. 5월	촉진	공공분야 (국방, 의료, 안전 등)	-	-	-	-	-
인공지능 국가전략	2019.12월	촉진 / 예방	전 산업 (제조, 바이오· 의료 등)	역기능방지 및 AI 윤리 체계 마련	신뢰성·안전성 등의 검증체계 구축	정보보호 지능화 혁신	데이터 개방· 유통 활성화/ 데이터 활용 지원	종합적 규제 혁신/포괄적 네거티브 규제로 전환
한국판 뉴딜 종합계획 (디지털뉴딜)	2020. 7월	촉진	교육, 비대면 산업 (의료· 근무·비즈니스)	-	-	사이버 방역 체계 구축	데이터 구축· 개방·활용	-
인공지능 일상화 및 산업 고도화 계획	2023. 1월	촉진 / 예방	전 산업	AI 윤리 선도 프로젝트	신뢰성 검·인 증 체계 마련	-	데이터 축적· 활용 기반 강화	법·제도· 규제 정비 2.0 프로젝트
초거대 인공 지능 경쟁력 강화방안	2023. 4월	촉진 / 예방	의료, 법률· 세무, 문화· 예술, 심리상담, 학술·연구	-	신뢰성·성능 평가	-	초거대AI 학 습용 데이터 구축 보강	초거대AI 규제 개선

출처: 저자 작성

까지 주로 민간의 자율적 선택을 바탕으로 시행되고 있고 표준의 역할이 강조되고 있음을 확인하였다.

AI 규제 접근 방식을 이행 강제성에 따라 나눈다면 자율적 참여 방식과 강제적 규제 방식으로 구분할 수 있다. 이에 따라 국내 정책을 구분하면, 지금까지 우리나라의 범분야 또는 수평적 AI 규제는 전자의 자율적 참여를 기반으로 하는 방식에 가까운 것으로 분석된다. 국제적 동향을 보면, 「EU 인공지능법」이 대표적인 후자의 강제적 규제 방식이라 할 수 있다. 그러나 「EU 인공지능법」을 제외하고, 미국, 영국, 싱가포르 등 주요국은 입법을 통한 수평적 AI 규제를 도입하지 않았다. 이들 국가는 표준화 정책을 중심으로 AI 규제 정책을 추진하고 있고 전자의 자율적 참여를 기반으로 하는 규제 방식을 유지하고 있다.

AI 관련 분야의 특허 현황 분석한 결과, 우리나라는 제조업과 정보통신 분야 특허 출원이 활발하고 세계 주요국과 비교할 때 ICT 분야의 특허 출원이 상대적으로 활발하다. 부처별 R&D 현황에 따르면, 우리나라 정부가 다양한 분야에서 AI 개발과 육성을 지원하는 것으로 분석된다. 그러나 일부 중복 지원이나 경계가 모호한 투자가 확인되며, AI 육성을 위해서는 기술 단계별 중점 지원이나 집중적인 투자가 필요하고 실질적인 기술 개발을 위해 R&D 투자의 지속성이 강화되어야 한다.

04

주요국 AI 규제와 표준 동향

「EU 인공지능법」은 모든 분야의 AI 위험을 강제적이고 수평적으로 규제하고 처벌하는 방식의 제도다. 글로벌 AI 규제 동향을 조사하면, 미국, 영국, 싱가포르 등 세계 주요국은 EU와 유사한 규제 도입에 대해 현재까지는 미온적이고 신중한 입장임이 확인된다. EU 외의 다른 국가들이 채택한 AI 규제 체제를 비교 분석하면 몇 가지 공통점이 있다. 요약하면, AI 혁신과 활용 확산에 초점을 두고 적극적인 진흥 정책을 추진하는 동시에 AI 안전과 신뢰를 확보하기 위해 국가 차원의 모니터링 체제를 구축하고 있다는 점이다.

구체적으로 살펴보면, 영국은 AI 규제에 있어 ‘혁신 친화적 접근(pro-innovation approach)’을 채택하고 AI 안전성 연구소를 설립하는 등 AI 규제와 거버넌스에 필요한 정보를 수집과 분석, 논의하는 국가 차원의 모니터링 체제를 운영하고 있다. 미국은 국립표준기술원(NIST)을 통해 「위험관리프레임워크 버전1」을 발표한 데 이어 인공지능안전성연구소(AISI)를 설립하고 인공지능 안전 분야의 관행과 과학 발전, 제도 발전을 위해 정보와 의견을 수렴하고 모니터링하는 체제를 강화하고 있다. 싱가포르는 AI 기술 발전에 발 빠르게 대응하는 국가로 분석된다. 생성형 AI 등장 이후 국가 AI 전략 2.0을 도입하고 글로벌 기업 유치, 인재 육성, 산업 전반의 AI 확산과 활용에 기치를 높이는 한편 안정성 검증과 규제에 필요한 실용적 방안 모색에 중점을 두고 있다.

규제 모델 측면에서 볼 때, 현재까지 추진된 EU 규제 방식과 미국 규제 방식은 대조적이다. EU는 AI 위험을 구분하고 ‘허용할 수 없는 위험’이 내재된 AI를 금지하는 동시에 일정한 법적 요건을 부여하여 금지하고 처벌하는 규제 방식을 채택하고 있다. 반면, 미국은 포괄적인 입법을 추진하기보다는 기업들이 스스로 AI 안전과 신뢰를 확보하도록 하고 자발적인 참여를 기반으로 하는 표준을 제정 및 확산하는 방식을 채택하고 있다. 미국과 EU의 AI 안전과 신뢰 확보를 위한 규제 접근 방식에는 근본적인 차이가 있으나, 양국 모두 AI 거버넌스에 있어 표준의 역할을 강조하고 있다는 점을 주지할 필요가 있다. 2024년 3월 통과한 EU 인공지능법(AIA)은 점진적으로 발효하여 2026년 시행될 예정이다. 현재 이행 기준을 만들기 위한 논의가 진행되고 있고 표준과 인증이 EU AI 제도의 핵심 요소가 될 것으로 예상된다. AI 개발과 혁신의 속도가 빠르고 규제가 유사한 속도로 변화하기 어려울 뿐 아니라 과도한 규제로 신기술 개발과 사용이 제한되지 않아야 한다는 점에서, 주요국 AI 규제 정책은 표준의 역할에 초점을 맞추고 있다.

표준은 국제협력 사안으로도 중요하게 논의되고 있다. 국가마다 AI 규제 방식이 다르므로 국가들이 상호 운영성과 연결성을 확보하기 위해 국제표준 개발에 참여하고 양자적, 지역적 표준 개발과 확산 협력을 강화하는 추세다. 국제표준화기구(ISO)는 AI 정의와 용어 표준부터 AI 시스템 운영과 관리 표준, 신뢰성 표준, 생애주기 대응 표준, 유스 케이스 공유 등 AI 생태계를 전반적으로 개선하고 확립하기 위한 표준을 개발하고 있다. 국제기구 차원에서 논의되는 원칙과 기준이 국가 AI 정책 방향 설정에 영향을 주는 것은 물론이고 상위 기구에서 결정된 원칙과 기준이 이행 실무에 중요한 이정표 역할을 하므로, 국제 동향에 촉각을 세우고 적극적으로 참여할 필요성을 확인하였다.

05

산업별 AI 활용 동향과 쟁점

산업마다 활용되는 AI 기술이 다르고 이에 따라 부각되는 AI 위험과 쟁점도 변화한다. AI 규제 정책은 산업별 특성을 반영하고 신속하게 대응할 수 있는 산업별 접근 방식을 유지 및 강화하는 것이 효과적임을 분석하였다. 이 보고서는 금융, 제조, 보건의로 산업의 AI 활용 동향과 규제 쟁점을 분석하고 해외 규제 정책 사례를 비교하여 시사점을 도출하였다.

5.1 금융 산업의 디지털화와 AI 활용

금융 분야 AI 기술은 금융서비스의 고도화와 운영 효율성 제고에 활용되고 있고, 향후 금융 산업 경쟁력을 강화하는 잠재적 핵심 동인이다. 그러나 AI가 금융혁신을 선도하고 지속가능한 발전을 뒷받침하기 위해서는 금융산업의 특수성을 감안한 신중하고 균형 잡힌 규제 접근이 요구된다.

금융 데이터는 개인의 자산정보, 신용정보 등 고도의 민감정보를 포함하고 있어, 데이터 관리와 활용에 있어 보안과 프라이버시 보호 장치가 필수적이다. 해킹, 유출 등으로 인한 금융사고는 개인과 기업에 막대한 경제적 피해를 초래할 수 있기 때문이다. 데이터 익명화, 암호화 등 첨단 보안기술을 적용하고 엄격한 데이터 거버넌스 체계를 구축하며 정보 주체의 권리를 강화하고 데이터 오남용을 방지하기 위한 법·제도적 기반을 공고히 할 필요가 있다.

다음으로 AI 기반 금융서비스의 신뢰성과 공정성 확보를 위해, 인공지능 알고리즘의 투명성과 설명 가능성 제고가 시급하다. 특히 대출심사, 신용평가, 보험인수 등 개인의 경제생활에 직접적 영향을 미치는 영역에서 AI 의사결정에 대한 설명책임은 강화하고, 차별과 편향을 방지하기 위한 공정성 검증 체계를 마련해야 한다. 아울러 AI 오작동, 사이버 공격 등에 따른 금융사고 발생 시 법적 책임소재를 명확히 하고 소비자 권익 구제 수단을 확충하는 등 이용자 보호에도 만전을 기해야 한다.

또한 AI를 활용한 자산운용, 투자자문, 트레이딩 등에서 초래될 수 있는 금융시장 교란과 시스템 리스크를 예방하고 관리하는 정책이 병행되어야 한다. 시장 모니터링 강화, 위기 대응 매뉴얼 정비, 스트레스 테스트 시행 등을 통해 잠재적 위험 요인을 선제적으로 식별하고 대응하는 한편, 과도한 투기와 불공정거래를 억제하는 시장 감독 체계 고도화가 필요하다.

그러나 이 같은 리스크 관리 노력이 혁신을 저해하는 과도한 규제로 귀결되어서는 곤란하다. 급변하는 AI 기술 특성상 경직된 규제 적용은 오히려 금융 혁신의 걸림돌로 작용할 수 있기 때문이다. 따라서 포괄적이고 탄력적인 규제 체계를 구축하되, 법령상 근거가 필요한 부분은 명확히 하고, 세부 내용은 감독 가이드라인 등 연성 규범(soft law)에 담아 유연성을 확보하는 것이 바람직하다.

특히 AI 기술을 활용한 혁신적 금융서비스의 개발과 사업화를 지원하기 위해서는 선제적 규제 완화와 인센티브 제공이 필수적이다. 규제 샌드박스, 임시 허가 등을 적극 활용하여 혁신적 아이디어가 시장에서 빠르게 테스트 되고 구현될 수 있도록 지원하고, 성공 사례에 대해서는 규제 정비와 함께 세제 혜택, 재정지원 등을 패키지로 제공하는 방안을 고려할 수 있다.

한편, 금융 AI 생태계 고도화를 위해서는 AI 기술에 대한 자체 역량 확보가 필요하다. 해외 대형 IT 기업에 의한 AI 금융서비스 독점화에 대응하여 국내 AI 솔루션의 개발과 활용을 확대할 필요가 있다. 이를 위해 금융권 공동의 AI 오픈 플랫폼 구축, 산학연 협력 R&D 확대, 전문인력 양성 등에 대한 정책적 지원을 강화해야 한다. 그리고 AI 기술의 글로벌 발전 동향을 면밀히 모니터링하여 선진 사례를 신속히 벤치마킹하는 개방적 혁신 전략도 필요하다.

5.2 제조 분야 디지털화와 AI 활용

제조 분야에서 AI 기술의 전략적 도입과 활용은 생산 효율성 제고, 품질 향상, 에너지 절감 등을 통해 제조 기업의 경쟁력 강화에 기여할 수 있는 핵심 동인이 될 수 있다. 그러나 AI가 제조업 혁신을 선도하고 지속가능한 발전을 뒷받침하기 위해서는 제조업의 특수성을 감안한 신중하고 균형 잡힌 접근이 요구된다.

무엇보다 제조 현장에서 생성되는 방대한 데이터를 안전하게 수집, 저장, 처리할 수 있는 스마트 팩토리 인프라 구축이 시급하다. 센서, 사물인터넷(IoT) 등을 활용한 실시간 데이터 모니터링 체계를 갖추고, 엣지 컴퓨팅, 클라우드 등 최신 IT 기술을 접목하여 데이터 처리의 효율성과 보안성을 제고해야 한다. 아울러 기업 간, 산업 간 데이터 공유와 연계를 활성화함으로써 제조데이터의 가치를 극대화하기 위한 협력적 거버넌스 체계도 마련해야 할 것이다.

다음으로 제품 기획, 설계, 생산, 유지보수 등 제조 프로세스 전반에 AI 기술을 접목하여 혁신을 추진해야 한다. 시장예측, 수요분석 등에 AI를 활용함으로써 고객 맞춤형 제품을 적시에 공급하고, 설계 최적화, 불량 예측, 공정 자동화 등을 통해 생산성과 품질을 제고할 수 있다. 또한, 산업용 로봇, 무인운반차(AGV) 등과 AI 기술을 융합하여 유연하고 효율적인 스마트 공장을 구현하는 한편, 예지보전, 원격 모니터링 등을 통해 설비 가동률을 높이고 운영비용을 절감할 수 있을 것이다.

또한 AI 기술 확산이 기능인력 대체, 일자리 소멸 등을 초래할 가능성에 선제적으로 대응하기 위한 종합적 노동정책도 요구된다. 근로자의 직무전환과 재교육을 지원하는 고용안전망 확충, 숙련도 향상과 창의성 계발을 위한 인재양성 체계 구축 등을 통해 인간 중심의 지속가능한 제조 생태계를 조성해 나가야 한다.

한편, AI 기반 제조혁신이 심화시킬 수도 있는 중소기업과 대기업 간, 수도권과 지방 간 불균형을 우려하고 경계해야 한다. 대기업과 선도기업 위주로 AI 기술이 도입되고 그 효과가 집중될 경우, 산업 양극화는 더욱 심해질 수 있기 때문이다. 따라서 중소제조기업의 AI·데이터 역량 확충을 위한 공적 지원체계를 강화하고, 권역별

제조혁신센터 등을 통해 지역 기반의 산학연 협력 활성화가 요구된다.

무엇보다 개별 기업 차원에서 AI에 대한 이해와 수용성 제고가 선행되어야 한다. 현장 맞춤형 사례 교육, 체험 프로그램 등을 통해 기업과 근로자의 AI 리터러시를 높이고, 일하는 방식의 변화를 유도해야 한다. 또한 AI 프로젝트의 성공 사례를 적극 발굴·확산함으로써 AI 기술 도입에 대한 심리적 장벽을 낮추고 혁신 분위기를 조성할 필요가 있다.

그러나 이 같은 AI 기반 제조혁신이 기업과 근로자에게 실질적 이익으로 귀결되기 위해서는 잠재적 위험요인에 대한 선제적 관리도 필요하다. 무엇보다 산업안전 분야에서의 AI 활용은 인간의 생명과 직결되는 만큼 엄격한 규제 적용이 불가피하다. 또한 AI 기반 설비의 공정성과 생산제품의 품질 역시 소비자 신뢰 확보를 위해 엄격한 규제가 요구된다. 완성차, 전자제품, 의약품 등 소비자 안전에 직결되거나 파급력이 큰 주요 품목에 대해서는 AI 품질관리 시스템의 적합성을 정부가 직접 평가·인증하고 지속적으로 관리·감독할 필요가 있다. 아울러 AI 기반 생산공정에서 발생할 수 있는 알고리즘 편향, 데이터 오류 등에 기인한 제품 하자에 대해 명확한 법적 책임을 부과함으로써, 기업의 자율적 품질 통제를 유도해야 할 것이다.

다만, 이 같은 정부 주도의 명령-통제형 규제가 기업 자율성과 창의성을 과도하게 제약하지 않도록 유의해야 한다. 기술 발전 속도에 맞춰 규제를 지속적으로 업데이트하고, 성과를 수시로 모니터링하며, 업계 피드백을 규제 개선에 신속히 반영하는 유연한 거버넌스가 필요하다.

5.3 보건 분야 디지털화와 AI 활용

보건 의료 분야에서도 AI 기술의 전략적 도입과 활용은 의료서비스의 질적 향상과 효율성 제고를 통해 국가 보건의료 경쟁력 강화에 기여할 수 있는 핵심 동인이 될 수 있다. 그러나 AI가 보건의료 혁신을 선도하고 지속 가능한 발전을 뒷받침하기 위해서는 보건의료 산업의 특수성을 고려한 신중한 접근이 요구된다.

보건의료 데이터는 개인의 건강정보, 유전정보 등 매우 민감한 정보를 포함하고 있어 다른 산업 대비 엄격한 프라이버시 보호와 보안이 필수적이다. 따라서 양질의 보건의료 데이터를 안정적으로 확보하고 안전하게 활용할 수 있는 거버넌스 체계를 구축하는 것이 선결과제라 할 수 있다. 특히, 가명처리, 암호화 등 최신 데이터 보안 기술을 적극 도입하고, 사회적 합의에 기반한 데이터 활용 원칙을 정립할 필요가 있다.

또한, 인공지능 기술을 활용한 의료행위는 생명과 직결되는 만큼 안전성 확보가 무엇보다 중요하다. 진단 및 치료에 적용되는 AI 모델에 대해서는 엄격한 임상시험과 평가를 통해 객관적으로 검증하고, 지속적인 모니터링을 통해 안전성과 유효성을 담보하는 관리체계가 마련되어야 한다. 아울러 오진, 부작용 등 AI 기반 의사결정의 부정적 결과에 대한 법적 책임 소재를 명확히 하고, 피해 구제 절차를 제도화하는 등 의료사고 예방과 환자 보호를 위한 안전장치도 함께 고려되어야 할 것이다.

한편, 보건의료 분야의 AI 활용은 기술적 문제를 넘어 윤리적, 사회적 합의가 매우 크므로, 인간 중심, 윤리

기반의 원칙을 정립하고 실천하는 것이 중요하다. AI 기반 의사결정의 투명성과 설명 가능성을 제고하여 환자와 의료진 간 신뢰를 구축하고, 데이터와 알고리즘의 편향성을 해소하여 의료접근성과 형평성을 개선해야 한다. 이를 위해 의료윤리 전문가, 시민사회 등 다양한 이해관계자가 참여하는 사회적 논의를 통해 보건의료 AI 윤리기준과 거버넌스 체계를 수립해 나가야 할 것이다.

아울러 AI 기술 발전의 속도와 파급력을 고려할 때, 과도한 규제보다는 산업 혁신과 기술 진보를 저해하지 않는 선에서의 유연한 규제 접근이 바람직하다. 최소한의 안전과 윤리 기준을 법제화하되, 세부 사항은 전문가 집단과 산업계의 자율 규제에 맡기는 공동규제(Co-regulation) 방식을 고려할 수 있다. 또한 글로벌 기술 추세와 해외 정책동향을 면밀히 분석하여, 우리 실정에 맞는 규제체계를 선제적으로 설계해야 할 것이다.

이러한 제도적 기반에서, 우리나라 보건의료 생태계 고도화를 위한 두 트랙 전략을 추진할 필요가 있다. 첫째, 최신 AI 기술을 적극 도입하여 정밀의료, 디지털치료제, 스마트병원 등 미래 보건의료 신산업을 육성하고, 글로벌 경쟁력을 확보해야 한다. 이를 위해 AI 헬스케어에 특화된 테스트베드 구축, 규제 샌드박스 운영, AI 의료기기 인허가 절차 개선 등 정부 차원의 전략적 지원이 요구된다.

둘째, 장기적 차원에서 우리 고유의 AI 보건의료 기술 역량을 지속적으로 축적해 나가야 한다. 국내 의료기관-대학-기업의 협력체계를 구축하여, 우리나라 국민 건강데이터에 기반한 한국형 AI 솔루션을 개발하고, 내수 시장에 공급함으로써 자생적 AI 보건의료 생태계의 토대를 다져야 할 것이다. 이를 통해 국내 AI 기술이 활용되는 비중을 점진적으로 높이고 해외 의존도를 낮춰나감으로써, 우리 의료체계의 독자적 디지털 능력을 제고할 수 있을 것으로 기대된다.

종합하면, 우리나라가 AI 보건의료 강국으로 도약하기 위해서는 제도와 윤리, 기술과 산업이 선순환하는 지속가능한 생태계 조성이 관건이다. 의료 당국의 적극적 규제개혁, 연구계와 산업계의 협력적 혁신, 시민사회의 주도적 참여가 긴밀히 연계될 때, AI의 힘으로 국민 건강 증진과 국가경쟁력 제고라는 두 마리 토끼를 잡을 수 있을 것이다.

06

결론 및 시사점

6.1 산업별 규제 전략과 AI 위험에 대한 수평적 규제 필요

산업별 상황과 필요에 대응할 수 있는 산업별 규제 전략이 유용하고 동시에 AI 시대에 대비한 국가적 AI 규제 체제 개선과 보완도 시급하다. 산업별 규제의 제도적 한계, 가령 산업 간 규제 중복, 규제 공백, 규제 회피 등 효과성과 비효율성 문제가 보완되어야 하고 이를 위해 국가적 차원에서 최소한의 AI 안전과 신뢰 기준을 마련하는 것이 중장기적 산업 경쟁력 제고에 이롭기 때문이다. 현재의 규제 모호성과 미래에 대한 불확실성이 민간의 AI

개발과 투자를 위축하는 요인이 된다는 우려의 목소리도 있다.

따라서, AI 위험에 대응하고 안전과 신뢰를 확보하기 위한 수평적 규제가 필요하고 이를 통합적으로 모니터링하고 지속적으로 개선 및 보완할 수 있는 이행 체계가 마련되어야 한다. 다만, 모니터링 대상, 규제 정책의 적용 범위와 규범 수준, 이행 강제성 여부는 신중한 검토를 바탕으로 해야 한다. 이를 위해, 논의 및 모니터링 체제를 강화하고 표준 및 인증체계를 활용, 규제샌드 박스 등 실험적 규제 수단을 적극 활용할 필요가 있다.

6.2 AI 안전과 신뢰 확보를 위한 모니터링 체제 필요

주요국이 추진하고 있는 AI 규제 체제를 비교하면, AI 혁신과 활용 확산에 초점을 두고 진흥 정책을 추진하는 동시에 AI 안전과 신뢰를 확보하기 위한 국가적 모니터링 체제를 구축하고 있다는 공통점이 있다. AI 원칙, 가이드라인, 윤리 및 거버넌스 지침, 권리장전과 같이 기본 방향을 제시하는 상위 기준을 두고 이를 기반으로 하는 느슨하면서도 유연한 규제 체제를 마련한 것으로 파악된다. 즉, 하위 이행 기준은 산업별, 분야별, 기관별 규칙, 지침서 등을 통해 구체적으로 마련하도록 하는 동시에, 기업과 민간 기관의 자발적인 참여를 근간으로 하는 규제 방식을 채택하고 있다.

한편, 실제로 대부분이 글로벌 빅테크 기업들이 내부적인 AI 윤리 기준과 검증 시스템을 갖추고 이를 통해 AI 신뢰, 품질 안전, 경쟁력 제고를 전략적으로 추진하고 있는 점도 주목된다. AI 산업이 확대됨에 따라 궁극적으로는 AI 활용 기업들이 자체적인 안전성 검증 제도를 운영하고 대외적으로는 위험 사례와 대응 방안을 공유하도록 하는 생태계가 필요하다. 다양한 분야에서, 그리고 기업 내, 산업 내, 그리고 국가적 차원에서 AI 원칙과 기준의 이행을 모니터링하는 체제를 확립해야 한다. 이를 통해 AI 원칙과 기준을 시의성 있게 보완하고, AI 위험과 대응 분석에 필요한 데이터를 구축하여 효과적인 방안을 모색해 볼 수 있을 것이다.

6.3 AI 위험과 신뢰 확보를 위한 표준화 및 표준 확산 필요

AI 표준을 통해 AI 거버넌스를 보완하고 강화해야 한다는 것이 기본적인 논의 동향이다. 그러나 실제로 표준을 개발하고 사용하도록 하는 데에는 몇 가지 어려움이 따른다. 첫째, 합의에 기초한 표준을 개발하려면 객관적인 증거가 뒷받침되어야 하나, 과학적인 근거를 확보하기가 어렵다는 문제가 있다. 현실적으로 AI의 사회경제적 영향과 위험 사례가 충분히 축적되지 못한 상황이고 기술은 빠르게 변하고 있어서 표준 및 규제를 위한 구체적인 기준을 결정하기에 어려움이 있다. 그러므로 표준 개발을 위해 기술적, 과학적 근거를 축적하는 것이 시급한 과제로 지적된다. AI 위험 사례, 유스케이스 취합 및 모니터링 표준 개발 등 주요국 표준 정책이 사례와 정보 수집을 중요하게 다루고 있음을 참고할 필요가 있다.

둘째, AI 활용과 위험이 전방위적으로 확산되고 앞으로 더욱 가속화 할 것으로 예상된다. 이에 따라 AI 거버넌스를

확립하기 위한 기술적 표준과 제도적 표준이 모두 중요하게 고려된다. 표준 개발에 있어, AI의 사회·윤리적 영향, AI 거버넌스, 프라이버시 보호 등의 문제를 다루는 정책과 원칙을 표준으로 제정하는 문제는 특히 어렵고 까다로운 과제다. 사회적 합의가 필요하고 제도적 표준 개발은 다양한 의견을 수렴 및 반영하는 과정이 필요하다.

문제는 논의 절차로 인해 규제 도입이 지연되지 않아야 한다는 점이다. AI 개발과 사용이 빠르게 확산하고 있으므로 AI 신뢰와 안전을 위한 규제 정책이 시의성 있게 추진되어야 한다. 기술, 제도, 산업 전문가 그룹의 표준 개발이 더욱 활발하게 논의되어야 한다.

셋째, 주요국은 국제표준화 동향에 발맞춰 국내 표준을 개발하고 있다. AI 기술과 규제의 국제적 흐름에서 뒤처지지 않고 글로벌 표준에 부합하는 산업경쟁력을 유지하기 위한 전략으로 이해할 수 있다. 국제표준화기구 활동에 참여하여 국제 표준과 국내 표준 및 규제를 일치시키기 위해 노력하는 한편 파트너십을 체결하고 AI를 포함한 신기술 분야 협력 관계를 강화하려는 노력도 요청된다.

끝으로, 앞서 분석한 미국과 EU 사례에서 볼 수 있듯이, 한국도 국가 차원에서 통일된 원칙과 통합된 거버넌스 체계가 필요하고 AI 안전과 신뢰를 확보하기 위한 규제 정책 수단으로서 AI 표준 및 인증제도를 활용해야 한다. 이를 위해 AI 관련 광범위한 분야의 표준 및 인증 제도를 정비하고 전문성과 역량을 강화해야 한다.

6.4 산업 경쟁력 강화를 위한 규제실험 수단 활용 방안 필요

「EU 인공지능법」의 경우, AI 혁신과 발전을 위한 주요 규정으로 AI 규제 샌드박스, 실사용 테스트, 중소기업 및 스타트업 지원에 관한 규정을 포함하며, OECD는 AI 샌드박스를 다른 규제 및 제도적 메커니즘과 결합하여 시행함으로써 기술혁신을 촉진할 수 있음을 강조하고 있어 참고할 만하다. 국내 AI 산업 경쟁력을 강화하기 위해 다음의 4가지 방안을 고려할 수 있다. 첫째, AI 기술을 활용한 사업을 대상으로 AI 표준과 샌드박스를 결합하는 방향을 검토할 수 있다. 둘째, 중소기업 지원을 중점으로 하는 샌드박스 활용 방안이 필요하다. 셋째, AI 기술과 관련성이 높은 특정 분야를 대상으로 명확하게 정의된 테스트 환경을 제공하고, 해당 분야에 대한 명확한 규제를 공공 영역과 민간 영역이 함께 만들어 가는 방안을 검토할 수 있다. 넷째, AI 기술과 결합해 사회적으로 영향이 클 것으로 예상되는 산업 분야를 특정하여 샌드박스를 운영하는 방안을 고려할 수 있다.

AI 산업의 경쟁력 제고를 위해 AI 규제실험을 추진할 경우, 기존 규제 샌드박스와는 다르게, 별개의 관리 및 운영 주체를 둘 필요가 있다. 이는 기존 규제 샌드박스가 소관 부처별로 운영됨에 따른 비효율성을 보완하고 AI 기술 분야와 관련성이 높거나 AI 산업 활성화를 촉진할 이니셔티브를 가진 특정 부처가 주도적으로 추진하도록 함으로써 AI 규제실험의 효과성을 높이기 위함이다. 또한, 특정 부처가 규제실험을 주도하더라도, 별도 기관이나 조직에 해당 업무를 위임함으로써 전문성을 확보하고 운영 및 참여기업 관리의 효율화를 추구할 수 있을 것이다. 끝으로, 이상에서 제안한 규제실험 방식은 AI 기술이 적용·응용되는 특정 산업분야에서 요구하는 최소한의 규제를 유지한 상태에서 추진해야 할 것이다.

AI 기술 진보가 빠르게 진행되고 있으므로 유연한 규제 체제를 마련하고 AI 안전과 신뢰를 확보하기 위한 노력이 필요하다. 특히 규제실험을 통해 규제준수 및 이행에 대한 모니터링, 피드백 과정을 병행하고 점진적으로 규제 준비를 해나가는 과정이 필요하다. 종합적이고 거시적인 관점에서 규제 환경을 조성하기 위한 많은 토론과 후속 연구가 진행되어야 한다. 🌈

연구기관		연구책임자	공동연구원	연구보조원
저자		김정욱, 김종립, 최유경, 김민정, 유성희, 최현이, 김승현, 진승화, 김윤경, 박정후, 추수진		
주관 연구기관	한국개발연구원	김정욱 선임연구위원 (Jungwook Kim)	김민정 전문위원 유성희 전문위원 최현이 전문연구위원	김윤경 연구원 박정후 연구원
협력 연구기관	과학기술정책연구원	김종립 부연구위원	김승현 연구위원 진승화 부연구위원	추수진 선임연구위원
	한국법제연구원	최유경 연구위원	최환용 선임연구위원 조용혁 연구위원	허세령 연구원 김현정 연구원



QR코드를 스캔하여 접속하면 국가정책연구포털(nkis.re.kr)에서 해당 보고서의 원문을 볼 수 있습니다.