

chapter 2

EU 인공지능(AI) 백서 주요 내용 및 시사점



김지윤 Ⅵ 한국인터넷진흥원 주임연구원
윤재석 Ⅵ 한국인터넷진흥원 팀장

I. 서론

2020년 2월 19일, 유럽연합 집행위원회(European Commission: EC)는 디지털 변화에 대응하기 위한 경쟁력 강화방안과 미래전략을 담은 정책을 발표했다. 이 정책은 유럽 데이터 공동체(데이터 단일시장) 구축을 목적으로 하는 “유럽 데이터 전략(A European Strategy for Data)”과 인공지능(AI) 기술의 안전한 활용과 도입을 촉진하기 위한 “인공지능 백서(White Paper on Artificial Intelligence)”로 구성되어 있다.

AI 기술은 EC 집행위원장인 Ursula von der Leyen이 주력하고 있는 집행위의 6대 정책과제 중 하나로, EC는 2014년 이후로 꾸준히 디지털 중심의 경제 활성화와 비(非)개인 데이터의 이동 규정(Regulation on the Free Flow of Non-personal Data), 사이버보안법(Cybersecurity Act), 오픈데이터 지침(Open Data Directive), 유럽연합 일반 데이터 보호 규칙(General Data Protection Regulation: GDPR), 신뢰할 수 있는 AI 윤리 가이드라인(Ethics Guidelines for Trustworthy AI) 마련 등 윤리적 기반 마련을 위한 노력을 기울여 왔다.

* 본 내용은 김지윤 주임연구원(☎ 061-820-1945, jkim141@kisa.or.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

EC는 인공지능 백서에서 AI 기술 도입 촉진과 안전하고 윤리적인 AI 활용을 위해 “우수성의 생태계(Ecosystem of Excellence)”와 “신뢰성의 생태계(Ecosystem of Trust)” 구축이라는 접근법을 제시했다. 백서는 AI 산업 활성화를 위한 공동 투자 기금 확보(예; Horizon Europe과 InvestEU 등) 및 기술 개발 전략(예; Digital Europe Programme) 등 회원국 공동의 노력을 강조함과 더불어, AI 시스템 관련 사용자의 불안과 불신을 없애기 위한 기술·정책적 노력을 제시하며 “4차 산업혁명” 시대에 AI 시장을 선도하려는 EU의 움직임을 보여주고 있다.

우리나라 정부 또한 2019년 12월, 관계부처 합동으로 “인공지능(AI) 국가전략”을 발표했다. 이는 같은 해 10월 28일 문재인 대통령이 직접 발표한 “대통령 인공지능 기본구상”을 바탕으로 하여 민간 전문가 및 전 부처가 참여해 제시한 전략을 담고 있다. 정부는 “IT 강국을 넘어 AI 강국으로(AI for Everyone, AI for Everything)”라는 국가 비전 달성을 위해 “AI 경쟁력 혁신”, “AI 활용 전면화”, “AI 조화·공존”이라는 3대 분야를 제시하고 이에 따른 9개의 전략과 부처별 100대 세부 과제를 정했다. 정부는 2030년까지 AI 산업 활성화를 통해 경제적 이익 창출과 삶의 질을 높이는 것을 목표로 하고 있다[1].

본 고에서는 최근 세계가 주목하는 AI 기술에 있어 EU의 전략·정책·규제를 살펴봄으로써, 국내 AI 전략 정책 수립에 참고할만한 시사점을 도출해보고자 한다.

II. EU 인공지능 백서 주요 내용

EC는 인공지능 백서와 함께 EU 내 국민의 기본권 및 주권 향상, 향후 5년간 데이터 경제 활성화를 위한 정책과 전략을 제시한 “유럽 데이터 전략(A European Strategy for Data)”과 “인공지능, IoT 및 로봇 공학의 안전과 책임에 대한 보고서(Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics)”를 발표했다.

이 보고서들은 AI 기술 도입 촉진과 산업 활성화를 위한 전략과 더불어 현행 규제에 대한 진단 및 목표 논의, 잠재적 위험의 해결과 예방 방안에 대해 다룬다. 특히, 인공지능 백서에서는 AI 도입 촉진과 안전한 활용을 위해 AI 기술 적용 제품·서비스 생애주기 전반에 윤리적 측면을 강조한 정책 방안을 제시한 것이 특징이다.



〈자료〉 European Commission, “Excellence and Trust in Artificial Intelligence,” 2020. 2, p.2.

〈그림 1〉 EU 인공지능 우수성과 신뢰도 제고 방안

EC는 회원국의 일반 대중과 AI 관련 이해관계자, 유럽의회 등의 의견 수렴을 통해 EU 내 AI 기술 도입과 발전 방향을 설정하기 위한 기반으로 “우수성의 생태계(Ecosystem of Excellence)”와 “신뢰성의 생태계(Ecosystem of Trust)”를 제시했다[5].

“우수성의 생태계” 구축 부분에서는 AI 활성화를 위한 기반 마련을 강조하며 EU 회원국 간 그리고 민·관 협력체계를 촉진하는 정책과 전략을 제시한다. “신뢰성의 생태계” 구축 부분에서는 AI 도입과 활성화에 있어 대중의 신뢰를 얻는 것을 목적으로 윤리적 측면을 고려한 AI 시스템 설계 방식과 전략을 제시한다.

1. 우수성의 생태계

EC는 AI 활성화를 위한 기술 및 산업 기반 마련을 주요 과제 중 하나로 꼽고 있다. 이를 위한 “우수성의 생태계” 형성은 민간-공공 파트너십 형성을 통한 연구 활성화와 인프

[표 1] 우수성의 생태계(Ecosystem of Excellence) 구축을 위한 EU 집행위 주요 과제

번호	주요 과제	주요 내용
1	회원국과 협력	인공지능백서에 대한 공개협의 결과를 고려하여 2020년 말까지 채택될 조정 계획의 개정 내용을 회원국에 제안
2	연구 및 혁신 조직에 역량 집중	유럽-국가-민간 차원의 투자를 결합하는 테스트센터 구축
3	기술 역량 강화	디지털 유럽 프로그램(Digital Europe Program) 네트워크를 활용하여 주요 대학과 고등 교육기관에 최고 수준의 교수와 과학자를 유치하고, 우수한 AI 대학원 프로그램을 제공
4	중소기업 육성	EU 회원국 당 하나 이상의 디지털 혁신 허브를 구축하여 AI 연구지원
5	민간 파트너십 형성	Horizon Europe을 통해 AI 관련 민간 파트너십 형성, AI 연구 및 혁신 부문의 협업 보장, 테스트 센터 및 디지털 혁신 허브와의 협력 추진
6	공공부문 AI 기술 우선 도입을 통한 도입 촉진	의료, 농촌 행정, 교통, 공공 서비스 부문에 AI 우선 도입 추진
7	데이터 접근 및 연산 시스템 안전성 강화	AI 알고리즘, 연산 시스템 등의 보안 강화 및 연산 능력 강화
8	국제기구를 통한 논의와 협력	WTO, OECD, UNESCO 등 국제기구와 협력하여 윤리 지침 마련 및 국가 간 데이터 흐름 원활화

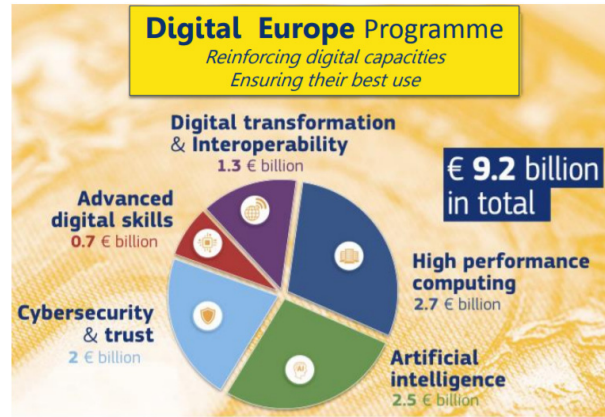
〈자료〉 European Commission, “White Paper on Artificial Intelligence,” 2020. 2. 19., 재구성

라 확충을 목표로 하며, ① 회원국과 협력, ② 연구 및 혁신 조직에 역량 집중, ③ 기술 역량 강화, ④ 중소기업 육성, ⑤ 민간 파트너십 형성, ⑥ 공공부문 AI 기술 우선 도입을 통한 도입촉진, ⑦ 데이터 접근 및 연산 시스템 안전성 강화, ⑧ 국제기구를 통한 논의와 협력의 여덟 과제를 제시한다([표 1] 참조).

① 회원국과 협력

EC는 2018년 채택한 「유럽 인공지능 전략(Artificial Intelligence for Europe)」과 관련하여 EU 내 AI 개발과 이용 장려를 위해 회원국과 공동으로 조정 계획(Coordinated Plan)을 제시했다. 이 계획을 통해, AI 관련 연구·투자·시장 활성화, 인재 활용 등의 분야에서 EU 내 70여 개 회원국과 집행위 사이의 효과적 협력을 위한 공동 조치를 제안하고, 2027년까지 정기적 모니터링과 점검을 통해 조정 계획을 확대할 예정이다.

EC는 2020년 말까지 AI 백서 내용에 대한 회원국과의 공개협의 결과를 통해 채택할 조정 계획의 개정 내용을 회원국에 제안할 방침이다. 이를 통해, 향후 10년 동안 EU 공동 연구 프로그램과 기금을 통해 투자를 극대화할 것을 목표로 하고 있다. 그 예로는, EU 내 전문 인력 양성과 최첨단 연구 투자를 통한 과학 및 기술 신장 연구개발 프로그램인



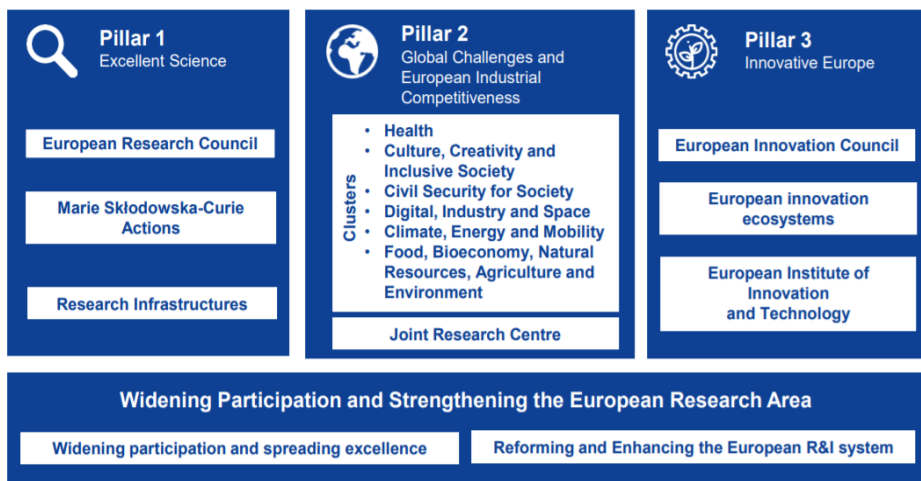
〈자료〉 European Commission, "Digital in the Next MFF," 2018. 6.25, p.8.

[그림 2] Digital Europe Programme 예산 활용 분야

Horizon Europe과 EU 내 슈퍼컴퓨터, AI, 사이버 보안 등 디지털 기술을 양성하는 계획인 Digital Europe Programme이 있으며, EU는 Digital Europe Programme을 통해 2021년부터 2027년까지 약 92억 유로를 투자할 예정이다.

② 연구 및 혁신 조직에 역량 집중

EC는 우수성의 생태계 형성에 필요한 연구 활성화를 위해 EU 각지에 퍼져 있는 AI



〈자료〉 European Commission, "Horizon Europe – Investing to shape our future," 2019. 5, p.10.

[그림 3] Horizon Europe 기본 구조

연구센터 사이의 협력체제를 형성하고 최고의 연구 인력을 확보하는 것을 세부 목표 중 하나로 내세웠다. 이는 유럽이 전통적으로 강세를 보이던 제조업 관련 AI 기술 강화와 더불어 상대적으로 약세를 보이는 소비자 관련 AI 애플리케이션 개발에 투자하여 세계를 선도하는 AI 기술력을 확보하겠다는 것이다.

EU는 회원국이 기존에 보유한 연구센터 간 네트워크 강화뿐만 아니라 새로운 연구센터를 설립하여 적어도 회원국 당 하나의 주력 연구센터를 보유하고 네트워크를 확대하여 AI 관련 연구의 시너지 창출에 주력할 예정이다[3]. 이는 앞서, 언급한 Digital Europe Programme과 Horizon Europe의 투자와 관련 연구 및 혁신 조치를 통해 진행될 것이다.

③ 기술 역량 강화

유럽의 AI 관련 역량 강화와 모든 EU 국민이 디지털 혁신의 혜택을 받을 수 있도록 EC는 “기술 역량 강화 아젠다(Skills Agenda)”를 강화할 방침이다. “디지털 교육 행동 계획(Digital Education Action Plan)”의 개선을 통해 AI 및 디지털 관련 교육과 훈련 시스템의 개편, AI 개발자를 위한 커리큘럼 개발, 여성 AI 전문가 육성 확대, Digital Europe Programme을 통한 세계 최고 수준의 교수와 과학자를 유치하여 수준 높은 AI 석사 프로그램 개발 등을 목표로 하고 있다[4].

④ 중소기업 육성

중소기업의 AI 활용 지원을 위해 EU는 “디지털 혁신 허브(Digital Innovation Hub)”를 강화하여 중소기업 간 협력을 촉진하고, 공동 투자 기금인 InvestEU를 통해 이를 지원할 예정이다. InvestEU는 “유럽 전략 투자 기금”과 13개 EU 금융기구를 통해 중소기업에 자금 지원, 기술 조언 및 정보를 제공하고 기술 혁신과 일자리 창출을 목적으로 하는 프로그램이다. EC는 이러한 지원을 통해 회원국 당 적어도 하나 이상의 디지털 혁신 허브를 구축하고 이를 바탕으로 회원국마다 AI 관련 전문성을 강화할 것을 목표로 하고 있다.

⑤ 민간 파트너십 형성

EC는 민간 부문의 참여를 통한 AI 관련 혁신 및 의제 설정, 공동 투자를 끌어내기 위해 민간-공공부문 파트너십 형성을 목표로 제시했다. 민간 부문 최고경영진은 협력에 긍정적인 의사를 내비쳤으며, 이러한 민간-공공부문 파트너십은 Horizon Europe와 더불어 디지털

텔 혁신 허브를 통한 중소기업 육성 계획 등 백서에서 제시하는 세부 전략과 유기적으로 결합하여 진행될 예정이다.

⑥ 공공부문 AI 기술 우선 도입을 통한 도입 촉진

EC는 공공부문에 AI 기술을 우선 도입하여 관련 제품 및 서비스의 확산을 촉진하고 EU 내 모든 국민이 디지털 혁신을 통한 혜택을 누릴 수 있는 기반을 마련할 계획이다. 지방 공공행정, 의료, 운송 서비스, 재무 및 기타 공공 분야에 AI 제품 및 서비스를 도입할 예정이며, 특히 삶의 질 개선에 크게 영향을 미치는 의료와 운송 서비스에 우선 도입할 계획이다.

⑦ 데이터 접근 및 연산 시스템 안전성 강화

데이터의 보관과 생성 장소가 사용자 중심으로 이동해가면서 EU는 엣지 컴퓨팅, 클라우드 인프라, AI, 양자 컴퓨팅 등에 투자하고 있으며, Digital Europe Programme을 통해 40억 유로의 지원을 할 예정이다. EU는 이러한 투자가 안전하고 효율적인 데이터 수집과 관리 관행 형성에 도움을 주고 데이터의 재사용성과 정보주체 신뢰를 획득하여 AI 도입을 촉진할 것으로 기대하고 있다.

⑧ 국제기구를 통한 논의와 협력

EC는 데이터 활용을 포함하는 EU 외 국가와의 경제 활동에서 데이터 흐름을 방해할 가능성이 있는 과도한 규제에 대응하기 위해 세계무역기구(WTO), OECD, UNESCO와 같은 국제기구와 협력하여 정책적 대안을 논의할 예정이다. 이를 통해, 경제 활성화뿐만 아니라 인간의 존엄성과 다원주의적 가치를 존중하는 AI 개발 및 활용과 개인정보 보호 등 인간의 권리 보호를 위한 기반을 마련하고 있다.

2. 신뢰성의 생태계

EC가 AI 기술 도입 촉진과 확산을 위해 중요하게 생각하는 다른 과제는 EU 내 정보주체의 신뢰 확보이다. 데이터 관련 기술의 안전성 강화와 더불어 문제 예방과 피해 구제 등 AI 기술에 대한 정보주체의 신뢰를 높여 AI 도입을 촉진하겠다는 목적이다.

EC는 신뢰성의 생태계 형성을 위해 ① 문제 정의, ② AI 관련 법제 프레임워크 조정,

③ 미래 AI 관련 EU 법제 범위 규정, ④ 요구사항 유형 구분, ⑤ 법적 요건 대상 명확화, ⑥ 법규 준수와 집행, ⑦ 위험성에 대한 자발적 라벨링 체계(Voluntary Labelling Scheme) 마련, ⑧ 거버넌스 체계의 정비 여덟 과제를 제시하고 있다.

① 문제 정의

AI 기술은 제품과 서비스에 도입되면서 책임 소재와 문제 양상이 다양해지게 된다. 예로 자율주행 자동차의 경우, 제품의 설계와 시연 단계에서는 문제가 되지 않았으나 실제 운행 중에 주변 지형과 보행자를 구분하지 못해 사고가 발생한 경우가 발생하여 법적 책임 소재를 밝히는 데 문제가 발생하기도 한다[7].

EC는 AI 기술이 적용된 제품 및 서비스로 인해 육체적, 경제적 피해와 같은 물적 손실 뿐만 아니라 인종·성차별 등 편향된 AI 훈련 데이터로 인한 정보주체의 기본 권리 침해로 위험의 정의를 세분화하여 피해 발생 시의 책임 소재 명확화와 정보주체를 위한 안전장치(safeguard)를 마련할 계획이다.

② AI 관련 법제 프레임워크 조정

EC는 정보주체 기본 권리를 침해하는 인종·성차별을 방지하고 데이터 보호 규칙의 적용 범위를 AI까지 확대하여 관련 법제를 정비하는 것을 세부 과제로 설정했다. 또한, 제품 및 서비스의 사용 과정에서 발생하는 새로운 문제를 법적 대상으로 고려하는 등 AI 관련 문제 예방을 위한 ‘위험’의 정의를 확대할 예정이다. 특히, AI가 수집하는 대규모 데이터의 분석이 정보주체의 개인정보 재추적 및 익명성 해제로 인한 개인정보 침해 우려가 있어, 안전한 개인정보 활용을 위한 대책 마련이 중요시된다.

EC는 다음과 같은 상황에서 발생하는 위험과 문제 해결을 위해 법제 프레임워크를 개선할 수 있다는 견해다.

- 첫째, AI 적용 제품뿐만 아니라 서비스로 규제 대상 확대가 필요한 경우
- 둘째, AI 적용 제품 및 기술이 새로운 법적 문제를 일으켜 기존 법률 조정이 필요한 경우
- 셋째, 기존 제품 출시 후 AI 기술을 도입하여 기존 공급망 체계의 이해관계자 간 법적 책임 소재가 불분명해질 경우

EC는 새롭게 변화하는 환경에 대응하기 위한 법제 정비와 EU 회원국 모두가 참여하는

공동 정책 마련을 목표로 하고 있다.

③ 미래 AI 관련 EU 법제 범위 규정

EC는 미래 AI 관련 규제 범위 결정을 위해 AI의 정의와 그 구성요소인 ‘데이터’ 및 ‘알고리즘’ 개념의 명확화를 우선하고 있다. 또한, 급변하는 환경에 맞춰 발전하는 정책이 될 수 있도록 유연한 AI 개념 정의를 강조하고 있다.

합리적인 규제 개입을 위해서 EU는 “위험 기반 접근 방식(Risk-based approach)”을 채택하여 ‘고위험(High-risk)’으로 간주하는 AI 시스템에 대한 규제에 차등을 둔다.

EU는 AI 제품이나 서비스 이용이 일반적 업무 특성상 상당한 위험이 발생할 가능성이 큰 경우(예; 의료, 운송, 에너지 등)나 AI 제품이나 서비스 세부 분야별 적용이 추가적 위험을 일으킬 수 있는 경우(예; 사법 시스템)를 ‘고위험’으로 분류한다.

④ 요구사항 유형 구분

EC는 AI 상위 전문가 그룹의 윤리 가이드라인(Ethics Guidelines for Trustworthy Artificial Intelligence)을 고려하여 추후 AI 관련 법규에 포함될 수 있는 여러 요구사항 유형을 제시하고 있다[2].

- 편향되지 않고, 위험 상황에 대한 광범위한 시나리오를 포함한 AI 훈련용 데이터
- AI 시스템 활용 데이터 및 알고리즘 공개와 데이터의 안전한 기록과 보관
- AI 시스템의 전체 수명주기를 고려한 위험 예방 설계 및 합리적 대처 방안 마련
- AI 제품·서비스 전체 수명주기에 개입하는 인적 감독을 통한 이중 안전장치 마련
- 원격 생체인식 기술 등에 대한 생체 데이터 처리 원칙 준수 및 정교화

⑤ 법적 요건 대상 명확화

AI 관련 법적 요구 사항 적용 대상과 관련하여 EC는 두 가지 큰 틀을 제시하고 있다. 첫째, 법적 책임 대상에 있어 EU는 AI 시스템 전체 수명주기에 관여하는 개발자, 생산자, 배포자, 최종 사용자 등 각 수명주기에 따른 관여도를 고려한 책임의 차등 배분을 제시했다. 둘째, 법적 책임 대상의 지리적 요건과 관련하여 GDPR과 같이 EU 국민을 대상으로 AI 제품이나 서비스를 제공하는 모든 조직과 기업을 법적 책임 대상으로 하고 있다.

⑥ 법규 준수와 집행

EC는 AI 제품 및 서비스의 잠재적 예방을 위해 고위험 AI 시스템으로 분류된 제품 및 서비스에 대한 사전 적합성 검사(Prior Conformity Assessment) 시행을 요구한다. 이는 앞서 “④ 요구 사항 유형 구분”의 분류를 통해 고위험으로 분류된 AI 시스템에 적용되며, AI 시스템 전체 수명주기를 고려한 반복적이고 다면적 검사를 요구한다. 부적합 판정 시, EU가 주도하여 AI 시스템을 재교육하며, 중소기업 부담을 덜기 위한 온라인 검사 도구 제공 등의 방안을 마련하여 사전 적합성 검사 시행을 지원할 예정이다.

⑦ 위험성에 대한 자발적 라벨링 체계

고위험으로 분류되지 않는 AI 시스템에 대한 규제책을 마련하고자 EC는 자발적 라벨링 체계의 도입을 제안한다. 자발적 라벨링은 앞서 설명한 요구 사항을 자발적으로 준수하는 경우, EC가 검토 후 시스템 안정성을 인증하는 라벨을 부여하는 인증 체계이다. 인증체계 가입은 의무가 아니나 준수할 경우 법적 의무 요건이 적용되며 법의 사각지대에 있는 AI 시스템까지 법 적용 대상으로 포함하게 된다. 이 체계는 정보주체 보호와 사업자의 AI 관련 규제 준수를 위한 인증 비용 등의 감소를 목표로 한다.

⑧ 거버넌스 체계의 정비

EU는 각 회원국의 관계 당국 간 협력체계를 강화하기 위해 유럽 차원의 거버넌스 구조를 개편하고, 정보 교환 및 모범 사례 공유, 트렌드 분석, 공동 법제 마련을 위한 의견 조정, 전문 지식의 공유 등을 목표로 한다.

III. 주요 시사점

EU 디지털 개발 전략의 특이점 중 하나는 시스템 개발자 등 제공자에 대한 법적·윤리적 규범 마련과 준수에 집중한다는 점이다. 특히, EU는 “사전 적합성 검사(Prior Conformity Assessment)”와 “자발적 라벨링 체계(Voluntary Labelling Scheme)”를 통해 AI 적용 제품·서비스의 개발 및 활용과 관련해 법적인 규제책뿐만 아니라 윤리적 규범을 만들어 이들의 효과적 관리에서 나아가 경제적 실효성 제고를 추구한다.

1. 사전 적합성 검사

사전 적합성 검사는 EU 권역 내 AI 관련 공동 규제책 마련 및 효과적 시행을 위해 AI 적용 제품 및 서비스의 위험도 분류 기준에 따라 시행된다.

사전 적합성 검사는 ‘고위험’ AI 시스템 적용 제품 및 서비스에 적용되며, 이 경우 [표 2]에서처럼 EU가 백서에 제시한 요구사항에 대한 준수 여부를 확인한다. EU는 AI 기술 관련 위험을 “훈련 데이터 편향성으로 인한 기본권 침해 위험”과 “제도적 안전장치 부재로 인한 물적 손실의 위험”으로 정의한다. “훈련 데이터 편향성으로 인한 기본권 침해 위험”은 인종차별이나 성차별과 같은 정보주체 기본권에 대한 위험을 의미하며, “제도적 안전장치 부재로 인한 물적 손실 위험”은 AI 기술 적용 제품 및 서비스 사용 시 발생 가능한 신체·재산상의 피해 위험을 의미한다.

AI 제품 및 서비스는 학습을 통해 발전하므로 시스템 수 생애주기를 다면적이고 반복적으로 평가하며, 생애주기 상 이해관계자의 참여도를 평가하여 참여 수준에 따라 법적 책임을 차등 부여한다. 사전 적합성 검사 부적합 판정 시, EU 주도로 AI 시스템을 재교육하도록 하며, EU는 중소기업에 대해 온라인 검사 도구 제공 등의 지원과 더불어 피해 발생 시의 정보주체의 피해 구제책을 마련한다.

한편, 우리나라 정부는 “先 허용, 後 규제”의 견해를 밝히고 있으며, “규제 샌드박스”를

[표 2] 사전 적합성 검사(Prior Conformity Assessment) 요구사항 유형

분류	내용
훈련 데이터	데이터 편향성 제거, 정보주체 사생활 보호, AI 기술 이용 관련 위험 시나리오 고려 여부
데이터와 기록 보관 방식	AI 알고리즘 문제 발생 시 추적을 위한 훈련 데이터의 기록 보관 및 보안 수준 검토
정보제공 투명성	AI 시스템/알고리즘의 정확성 및 작동 원리에 대한 공개
시스템 견고성 및 정확성	AI 시스템의 동일 결과 재현 가능성과 오류 불일치 처리 요건 점검
인적 감독	인간의 검토/감시를 통한 이중 안전장치 마련 ※ AI 제품·서비스 설계 단계의 적절성 검토 ※ 인적 개입을 통한 시스템의 조정과 중단
원격 생체 인증* 관련 상세 요건	민감정보 처리 요건 준수 여부와 예외 상황의 고려 ※ 정보주체의 명시적 동의, 공익을 위한 법의 집행 등 AI 사용의 정당성 및 비례성이 보장되는 경우에만 생체정보를 통한 인증 가능

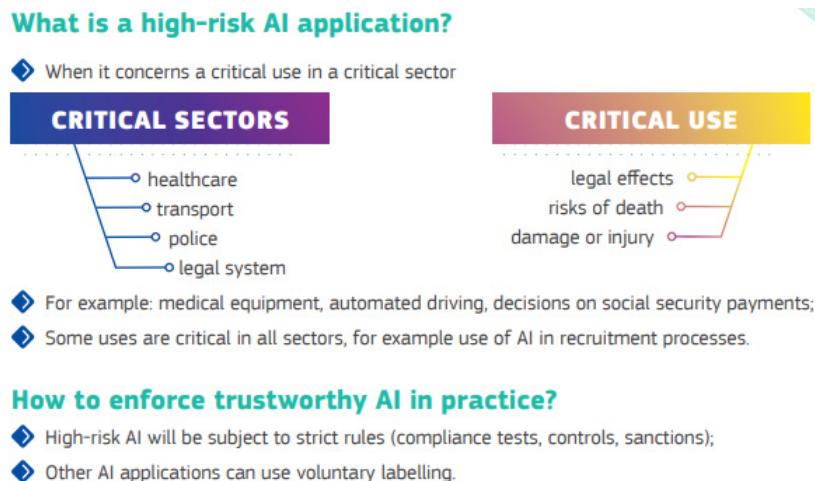
*DB 내 생체정보와 정보주체의 생체정보 간 인증(authentication) 및 식별(verification)

〈자료〉 European Commission, “White Paper on Artificial Intelligence,” 2020. 2. 19., 재구성

통해 이를 실천하고 있다. “규제 샌드박스”는 신기술에 대한 규제 존재 및 허가 여부에 대해 30일 이내 회신하는 “신속 확인”, 모호하거나 불합리한 규정을 우회할 수 있도록 일정 조건을 부여해 우선 테스트를 허용하는 ‘실증특례’와 기존 불합리하거나 모호한 규정에 제한받지 않고 시장 출시를 허락하는 ‘임시허가’로 이루어져 있다. 다만, 무분별한 기술의 난립을 막기 위해 “안전장치 3종 세트”라는 이름으로 생명·안전·환경 분야 저해 여부를 고려하고, 테스트 도중 잠재적 위험 발생 가능성을 확인한 경우 특례 취소, 손해 발생 시의 입증 책임을 사업자에게 부과하는 등의 장치를 마련하고 있다.

2. 자발적 라벨링 체계

자발적 라벨링 체계는 ‘고위험’으로 분류되지 않는 AI 제품 및 서비스 제공자의 자율 규제를 촉진하고 이를 법적으로 관리하기 위한 체계이다. EU 권역 내 혹은 거주민을 대상으로 하는 사업자가 전술한 사전 적합성 검사 요구사항[표 2]의 준수 여부를 자발적으로 신고하면, EC가 이를 검토하여 시스템 안정성을 인증하는 라벨을 부여하는 방식이다. 자발적 라벨링 체계의 가입은 의무가 아니나 가입 후 법적 요건이 적용되며, 법의 사각지대에 있는 AI 제품과 서비스도 법 적용 대상으로 포함하여 정보주체 보호를 주된 목적으로 한다.



〈자료〉 European Commission, “Excellence and Trust in Artificial Intelligence,” 2020. 2, p.3.

[그림 4] 고위험 AI 애플리케이션 분류

EC는 2021년까지 피드백을 바탕으로 자발적 라벨링 체계의 세부 요건을 확립하여 AI 관련 사업자 관리의 효율성을 제고하고자 한다. EC는 자발적 라벨링 또한 기타 인증체계와 마찬가지로 충분한 기반이 마련되면 시스템 안정성을 입증하는 상징으로서 정보주체의 신뢰도를 높여 AI 도입을 촉진할 것으로 기대하고 있다.

우리나라도 AI 시스템의 안정성 평가를 위한 인증제도 마련의 중요성을 인지하고 있다. 국가기술표준원에서는 지난 2018년 “범부처 인증제도 실효성 검토 제도”를 통해 불합리한 정부인증 7개를 폐지하고, 21개를 개선하는 등 인증제도 실효성 검토와 개선에 노력을 기울이고 있다.

IV. 결론

EU AI 전략의 독자적 측면은 기술 구축과 확산에 있어 윤리성의 강조와 이를 뒷받침하는 법제 및 체계를 마련하는 것이다. 이는 개발자나 설계자 등 제공자 측면에 집중한 규제책을 통해 확인할 수 있다. 위험도 분류를 통해 사전 적합성 검사와 자발적 라벨링 체계의 두 가지 방식으로 법적 책임 대상인 AI 시스템과 법의 사각지대에 있을 수 있는 이의 시스템 또한 법의 테두리에 포함함으로써 효과적인 AI 시스템 관리와 정보주체 신뢰 확보를 도모한다. 이러한 제공자 집중 규제 방안은 정보주체의 신뢰를 높여 AI 기술을 확산하는데 다양한 도움을 줄 수 있을 뿐 아니라 EU 시장 내 경쟁국 사업자의 무분별한 난입을 막아 시장을 보호하며, 안정성이 입증된 EU 내 AI 제품 및 서비스가 세계 시장에서 활약하는 데 도움을 줄 것이다.

반면, 우리나라 정부는 사전 규제보다 사후 규제, 개발자 규제보다는 이용자 보호에 치중하는 양상을 보인다. 우리나라 AI 기술 경쟁력을 강화하고, 이를 통한 디지털 경쟁력 세계 3위(現 10위, IMD)[6] 달성을 위해 AI 인프라 확충, 기술 경쟁력 확보, 글로벌 지향 AI 스타트업 육성 등 EU의 “우수성의 생태계” 형성과 비슷한 전략적 흐름을 보이고 있으며, 법제 마련에는 “규제 샌드박스”를 통한 AI 기술 우선 개발과 도입에 힘쓰며, 선두효과가 강하게 작용하는 현대의 기술 싸움에서 우위를 점하기 위해 혁신을 장려하면서 역기능을 억제할 수 있는 방향으로 규제 패러다임의 변화를 꾀하고 있다.

그러나 이러한 접근 방식은 정보주체 보호에 있어 보완적·예방적 조치가 필요할 것이다.

[표 3] 한-EU AI 활성화 전략 비교

전략	EU	한국
AI 기술 강화	<ul style="list-style-type: none"> - 데이터 접근 및 연산 시스템 안전성 강화 - 연구 및 혁신 조직에 집중 지원 	<ul style="list-style-type: none"> - 고성능 컴퓨팅 이용 환경 구축 - AI 분야 R&D 혁신 - 전문 인재양성 프로그램 확충 - AI 관련 기초 연구 지원 확대
AI 인프라 확충	<ul style="list-style-type: none"> - 민간 파트너십을 통한 공공 투자와 안전 논의 - 중소기업 육성을 위한 투자 펀드 구축 - 공공부문 AI 도입촉진과 확산 - AI 관련 이해관계자 참여 독려와 법제 이행 촉진을 위한 규제 당국 및 당국 네트워크 강화 	<ul style="list-style-type: none"> - 공공-민간 데이터 지도 연계 강화 - AI 거점화 전략 수립 및 집적단지 설립 - 표준 산업 AI 모델 개발 등 프로젝트 추진 - AI 스타트업 지원 확대 - 중소기업-소상공인 지원 - AI 투자 펀드 조성 및 미래기술 육성자금 신설 - 산업 전반의 AI 활용 전면화(23개 전략) - AI 역기능 대응 기술 개발 및 범부처 협업체계 마련
법제 정비	<ul style="list-style-type: none"> - AI 관련 문제 정의 확립과 대응책 마련 - AI 관련 인권 및 정보주체 권리 보장을 위한 법제 정비 - AI 관련 발생 가능 문제 예측과 법적 대응책 마련 - AI 제품 및 서비스 관련 담당자 법적 의무 정립 - AI 제품 및 서비스 관련 사전 적합성 검사와 사후 처리 - 법 의무사항 준수와 자발적 라벨링 정책 	<ul style="list-style-type: none"> - AI 기본 법제 마련 및 분야별 제도 정비 - 이용자 보호 정책 수립 지원체계 마련 - AI 기본 법제 마련 및 분야별 제도 정비
국제협력	<ul style="list-style-type: none"> - EU 내 AI 산업 활성화를 위한 공동 투자와 공동 계획 - 국제기구 규제 대응을 위한 논의와 협력 	<ul style="list-style-type: none"> - 글로벌 규범에 정합하는 AI 윤리기준 확립

〈자료〉 한국인터넷진흥원 작성

이는 전문가들과 논의를 통해 AI 시스템 안전성 확보를 위한 기준을 확립하고, 사전 안전성 검사와 같이 시스템 위험도에 따라 생애주기를 고려한 주기적 검토, 자발적 라벨링 체계와 같은 자율 규제 방안 도입 등을 통해 기존 정책을 보강해나갈 수 있을 것으로 예상된다.

한-EU 간 환경적인 차이로 인한 세부 전략에는 차이가 있으나, EU와 우리나라 모두 국민 삶의 질을 높이고 국민이 체감할 수 있는 공공부문에서 AI를 우선 도입하려는 움직임을 확인할 수 있다. 특히, 우리나라는 스마트시티, 5G 코어 네트워크 강화 등 도전적이며 우리나라의 강점을 살린 전략을 통해 AI 활용 기반 마련뿐만 아니라 국민 생활의 질을 높이고 이를 통한 신뢰 획득을 목표로 한다. 이렇듯 일상생활에 시나브로 녹아드는 AI 기술은 편리함과 안정성을 바탕으로 AI 기술 도입에 대한 국민의 우려를 해소하고 나아가 신뢰를 심어주어 성공적 AI 도입 활성화를 위한 초석이 될 것이다.

[참고문헌]

- [1] 관계부처 합동, “인공지능(AI) 국가전략,” 2019. 12. 17.
- [2] European Commission, “AI Alliance Consultation,” 2019.
- [3] European Commission, “Digital in the Next MFF,” 2018. 6.25, p.8.
- [4] European Commission, “Excellence and Trust in Artificial Intelligence,” 2020. 2, p.3.
- [5] European Commission, “White Paper on Artificial Intelligence,” 2020. 2. 19.
- [6] IMD World Competitiveness Center, “IMD World Digital Competitiveness Ranking 2019,” 2019.
- [7] NBCNews, “Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk,” 2019. 11. 9.