법무법인 린

Tech Legal Insights

AID (Artificial Intelligence Decoding) Vol. 1

2025. 01

2024년 12월 26일 "인공지능 발전과 신뢰기반 조성 등에 관한 기본법"(이하 "인공지능기본법")이 국회를 통과했습니다. EU AI법을 모델로 사람의 생명, 신체의 안전 및 기본권에 중대한 영향을 미치거나 위험을 초래할 우려가 있는 고영향 인공지능시스템 영역을 규제하면서 한편으로는 우리 나름의 인공지능기술과 산업 발전, 안전성 확보 의지도 담고 있습니다. AI 관련 포괄적 법 제정은 앞서가고 있는 EU AI법에 의해 영향을 받기는 했지만 단일 국가로서는 세계 최초인 셈입니다. 이하에서는 우리 인공지능기본법의 특징과 향후 입법적 과제, 기업에 대한 시사점 등을 외국 사례와 비교하면서 살펴보고자 합니다.

1. 인공지능기본법의 규제 체계

인공지능기본법은 EU AI법과 같이 인공지능 활용이 가져올 위험(영향)에 대한 평가를 통해 10가지 '고영향' 규제영역을 열거했고, 대통령령으로 세부 종류를 추가할 수 있으며, 관련 '위험'은 인공지능안전연구소가 정의 및 분석을 하도록 위임하고 있습니다. 또한, 제품 및 서비스가 초래할 고영향 여부에 대한 판정 권한을 과학기술정보통신부(이하 "과기정통부") 장관에게 부여하고 있습니다.

반면, EU AI법이 채택한 '위험기반(risk-based)' 차별적 규제방식은 AI법 뿐만 아니라 2018년에 발효시킨 EU 개인정보보호법, 2024년 12월부터 발효되고 있는 일반제품안전법 등에서도 공통적으로 발견되는 일종의 글로벌 스탠다드라고 할 수 있습니다. 따라서 향후 인공지능기본법 운영을 통해 어떤 관련 데이터와 기준으로 인공지능이 초래할 영향(위험)을 판정하고 대처할 것인지, 또한 EU에 수출하려는 우리 사업자가 지켜야 하는 고영향 기준은 고위험과 어떻게 다르고, 어떤 절차를 거쳐 추가 규제의 위험 없이 수출할 수 있는지 등은 추가 분석이 필요해 보입니다.

Related Areas

TMT

인공지능

Contact

구태언 변호사

T. 02-3477-8695

E. tekoo@law-lin.com

방석호 미국변호사

T. 02-3477-8695

E. shbang@law-lin.com

1-1. 인공지능기본법의 시행 체계

인공지능기본법은 기본 계획 등 범정부적 추진계획을 수립하고 실행함에 있어 기존 '지능정보화기본법'의 종합계획 및 실행계획을 고려하도록 하고 있고 기본 계획은 '지능정보화기본법'의 부문별 추진계획으로 본다고 명시함으로써 인공지능기본법상의 정부 기본계획은 논리적으로 '지능정보화기본법'의 종합계획과 실행계획 수립이 선행되어야만 비로소 가능하게 되는 구조입니다. 더욱이 인공지능기본법은 최고 정책 심의, 의결기관으로 대통령 소속의 국가인공지능위원회를 설치하도록 하고 있지만 이미 지능정보화기본법상 최고 심의, 의결기관으로 정보통신전략위원회가 인공지능 영역을 관할할 수 있기 때문에 운영상 거버넌스에 대한 조율도 필요해 보입니다. 부칙은 공포 후 1년이 경과한 때로부터 시행한다고 명시하고 있는데 이는 지능정보화기본법과의 관계상 불가피한 시간 계산으로 보입니다.

왜냐하면, 지능정보화기본법 시행령 제5조가 "중앙행정기관의 장과 지방자치단체의 장은 매년 12월 31일까지 다음 해의 실행계획을 확정한 후 다음 해 1월 31일까지 과기정통부 장관과 행정안전부 장관에게 제출"하도록 규정하고 있기 때문에 인공지능기본법상 정부의 기본계획은 2026년에야 비로소 수립될 수 있다는 계산이 나오기 때문입니다.

1-2. 생체인식정보 활용에 대한 규제

인공지능기본법은 '고영향'의 예로 '범죄 수사나 체포 업무를 위한 생체인식정보의 분석·활용'을 들고 있지만, EU AI법은 생체인식정보를 어떻게 활용하는지에 따라 '허용되지 않은' 위험이 되기도 하고, 또는 '고위험'으로 분류되기도 합니다. '생체정보'는 현 개인정보보호법 시행령 제18조에 규정된 '민감정보'로서 실생활에서 사용되고 있는 안면인식정보를 포함하며, 사이버보안, 자율주행, 스마트폰 인증, 건강진료 등 다양한 분야에서 안면인식기술의 핵심 데이터로 활용되고 있을 뿐만 아니라, 최근 코로나 팬데믹 시기에는 공공장소에서 열 스캐너를 활용한 안면인식시스템 설치 등을 통해 그 활용이 더욱 일반화되었습니다.

따라서 국가인권위원회도 개인정보보호 차원에서 이미 우려를 표명했고, EU AI법에서 '금지'되는 AI 활용 영역은 AI가 들어간 지능형 CCTV('AI CCTV'로 불리기도 함)를 이용해 군중 속에서 특정인을 실시간으로 식별(identification)하는 용도를 말합니다.

즉 EU AI법상 AI기반의 생체정보를 통한 본인확인(verification) 작업은 '고위험'으로도 분류되지 않으며, 설사 '금지'되는 실시간 AI CCTV 활용의 경우에도 납치, 인신매매 등의 피해자를 식별하거나 테러용의자를 추적하는 등의 예외적인 경우에는 허용되도록 하고 있습니다. 또한 EU AI법은 '생체정보'를 활용하고자 하는 사법집행기관이 사전에 '기본권 영향평가'를 받고 그 결과를 관할 기관에 통보하도록 규정하고 있습니다. 그러나 '생체정보'도 개인정보이기 때문에 EU AI법은 2016년 EU 개인정보보호법에 따른 정보보호영향평가를 받은 경우 이에 갈음하도록 규정하고 있습니다. 우리의 인공지능기본법은 그러한 인공지능 영향평가 세부 규정을 대통령령에 위임하고 있지만 이미 개인정보보호법은 관련 규정을 두고 있다는 점도 참고할 필요가 있습니다.

1-3. 교육분야의 AI 활용에 대한 규제

인공지능기본법은 고영향 영역 중 하나로 '교육기본법 제9조제1항에 따른 유아교육·초등교육 및 중등교육에서의 학생 평가'를 적시하고 있고, EU AI법도 모든 등급의 교육, 훈련 기관에서 AI 활용에 따른 접근, 학습결과평가, 등급평가 등에 대해 단계별 세부 규제를 하고 있습니다. 이런 점에서 최근 논란이 된 디지털 AI교과서의 경우, 개인별 눈높이 맞춤학습을 통한 학습효과 제고라는 긍정적인 측면도 있지만 개인정보침해 등의 부정적인 측면도 있는 AI 활용 영역입니다.

특히 EU AI 법은 이용자 개인 응답에 따른 학습결과물을 AI가 평가하고 이에 맞춘 맞춤 학습과정을 제공하는 것은 일단 고위험으로 분류되는 위험요소가 있는 것으로 보되, 최종 판단을 위해서는 고위험 분류 예외 사유로 언급된 "인간의 의사결정에 중요한 영향을 미치지 않는 경우를 포함, 건강, 안전, 기본권에 심각한 위험을 초래하지 않는 경우"에 해당되는 지의 여부 까지 검토하도록 하고 있습니다. 결국 디지털 AI 교과서를 어떻게 규제할 것인가의 문제는 인공지능기본법의 성격상 일단 사업자의 자율적 조치에 맡기되 일정 기간 관련 데이터의 처리, 축적 등에 대한 기술적 분석 작업이 선행되어야만 고영향 영역으로 별도로 분류하고 지속적으로 관리를 해야 할 정도의 고영향 영역인지에 대한 최종 판단이 가능할 것으로 보여집니다.

2. 인공지능기본법의 법제도적 보완 과제

인공지능기본법 제정의 패러다임을 2020년에 탄생된 지능정보화기본법의 모체인 정보화촉진기본법

서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

(1995년 제정), 이를 전면개정한 국가정보화기본법(2009년 전면 개정)의 연장선에서 접근했기에, 즉 인공지능사회, 인공지능윤리라는 법률용어의 사용에서도 드러나듯이 국가 전체의 지능정보화라는 매크로 차원에서 인공지능의 발전과 안전성 확보라는 두 마리 토끼를 모두 붙잡고자 하였기에 법 운영에 따른 조정문제는 불가피할 것으로 보입니다.

물론 주무 부처는 두 법 모두 과기정통부이지만 공공정보화를 담당하는 주무 부처인 행정안전부도 지능정보화기본법상 실행계획을 수립할 때는 한 축으로 참여를 하도록 되어 있기 때문에 인공지능기본법을 제대로 운영하기에는 현 법체계상 행정안전부의 협조가 필요할 수밖에 없으며, 현 인공지능기본법상의 주요 정책수단 또한 지능정보화기본법상의 그것들과 '동기화'될 수밖에 없어 보입니다. 따라서 향후 인공지능기본법만의 고유한 특성, 특히 관련 기술과 산업의 국가경쟁력의 확보 및 발전이라는 시급한 과제를 반영한 입법 보완작업을 통해 독자적 의의와 시대적 중요성을 더 부각시킬 필요가 있어 보입니다.

2-1. EU AI법과 인공지능기본법의 규제 체계 비교

2026년 8월2일부터 본격적으로 시행될 EU AI법은 EU 설립조약에 담긴 공동체 가치, 즉 인권과 자유의 보장에 합치하도록 AI가 건강, 안전, 기본권에 관한 공공의 이익을 보호하기 위해 인간 중심적인 기술이 되어야만 함을 선언하면서 특히 개인의 권리, 안전, 행복에 지대한 영향을 미치는 고위험 영역을 8가지로 열거, 2027년 8월2일부터 법 규정이 전면 적용되도록 하고 있습니다. 또한 고위험 AI 시스템 활용 영역은 위험관리시스템의 설치, 데이터 거버넌스와 편향 방지, 투명성 확보 및 감독 그리고 적합성 평가를 통한 인증 및 EU 데이터베이스 등록 등의 사전적 절차 요건을 충족시켜야만 하도록 규정하고 있습니다.

우리의 인공지능기본법도 이와 비슷하게 생명, 신체의 안전 및 기본권에 중요한 영향을 미치거나 위험을 초래할 우려가 있는 고영향 영역을 10개로 정의함으로써 인간 중심적인 AI 기술 개발과 보급, 신뢰할 수 있는 안전조치 등을 강조하고 있지만, AI 활용과 혁신이 저해되지 않도록 사업자의 자율규제를 기조로 하고 있습니다. 구체적으로 고영향 AI 활용 서비스나 제품을 제공하는 사업자가 먼저 자율적으로 안전성과 신뢰성을 보장하는 조치를 취하게끔 하되 과기정통부 장관의 사후 감독을 부가하는 틀을 제시하고 있습니다.

3. 시사점

인공지능기본법은 말 그대로 '기본법'이기 때문에 특히 고영향 관련 법들이 순차적으로 정비되어 져야만 합니다. EU는 AI법외에 디지털기술의 확산에 따른 변화를 수용하기 위해 2024년 12월 발효된 일반제품안전법과 제조물책임법, 그리고 2021년 5월부터 시행되고는 있지만 2028년 12월까지 의료기기가 초래할 위험 등을 고려해 단계적으로 적용되어지는 의료기기법과 같이 입법 정비작업을 계속하고 있습니다. 특히 AI를 포함한 SW의 활용이 제조업에 확산되면서 EU는 1985년 제조물책임법을 전면 개정한 새로운 법 (Product Liability Directive)을 2024년 12월 9일부터 시행하고 있고 국내법으로의 전환시기는 2026년 12월까지로 설정했습니다.

또한 새로운 EU 제조물책임법은 피해자의 손쉬운 구제에 더 역점을 두고 입증책임을 완화하는 등 기존의 법을 보완하는 동시에 제조업자에게 과중한 부담을 주지 않으려는 배려도 하고 있다는 점을 참조해, AI 활용 열풍이 불고 있는 제조업 분야에 불필요한 추가 갈등과 분쟁이 야기되지 않도록 2000년 1월에 만들어진 우리의 현 제조물책임법을 정비할 필요가 있습니다. 더욱이 이번에 통과된 인공지능기본법이 인공지능사업자, 이용자 외에 '영향받는 자'라는 용어를 새롭게 정의하고 있고, EU가 일반적으로 사용하여 온 '고위험' 대신 '고영향'이라는 용어를 쓰고 있기 때문에(EU AI법에서는 범용 AI의 학습데이터가 일정 한도를 초과할 경우 '고영향' AI로 분류, 시스템적 위험에 대비한 추가 규제를 하고 있음) 국경 없는 글로벌 통상 환경에서 향후 제조물책임 분쟁에 대비해 사업자의 자율규제를 보장하면서도 AI를 활용하는 기업의 혁신적 활동이 위축되지 않도록 피해 범위 및 원고적격의 확대 등으로 인한 추가 피해를 사전에 예방할 수 있는 정부의 산업별 가이드라인, 관련 고시 제정도 시급해 보입니다.

실리콘밸리에서는 2025년을 AI, 양자기술과 비즈니스의 수퍼사이클이 만들어지기 시작하는 원년으로 보고 있습니다.
법무법인 린의 AI 산업센터는 이러한 기술혁신의 대전환기에 국내외 주요 이슈를 분석하고,
관련 입법과 정책, 그리고 기업활동의 등대 역할을 할 AID를 월간으로 발행합니다.
내용에 대한 질문 등은 **구태언 TMT 전문그룹장**(tekoo@law-lin.com),
방석호 AI산업센터장(shbang@law-lin.com)에게 보내주십시오.

서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com