대한민국 인공지능법 시행령안에 대한 CCIA 의 견해

1 월 21 일, 대한민국은 인공지능 기본법(이하 '법')을 통과시켰습니다.[1] 법의 조항은 2026 년 1 월 22 일부터 발효되며, 2025 년 9 월 과학기술정보통신부(과기부)는 법 시행을 위한 하위 규정 초안(이하 '시행령')을 발표했습니다. 과학기술정보통신부는 시행령을 최종화함에 있어, 투명성 의무, 고영향 AI 시스템의 범위 설정 및 추가 의무 부과 절차, 영향 평가 요구사항, 그리고 더 광범위한 절차적 고려사항과 관련된 초안 텍스트의 심각한 우려사항을 해결해야 합니다.

상세한 의견은 아래에 제시됩니다.

정의

일반적으로 과학기술정보통신부는 개발자와 배포자 각각의 책임을 더 정확하게 정의해야 합니다. 법[2]과 초안 시행령에서 "AI 사업체"라는 용어가 과도하게 광범위하고 일관되지 않게 적용되어 AI 생태계의 다양한 행위자들에게 법적 불확실성을 초래하기 때문입니다. AI 기술의 복잡하고 층위화된 성격을 고려할 때, 시행령은 시스템을 구축하고 제공하는 개발자의 의무와 이를 최종 사용자에게 제공되는 서비스에 통합하는 배포자의 의무를 명확히 구분해야 합니다.

또한, 시행령은 "사용자"를 AI 를 자체 서비스에 통합하는 주체를 포함하는 대신 최종 AI 제품 또는 서비스를 궁극적으로 받는 최종 사용자로 명시적으로 정의해야 합니다. 정부의 "AI 기본법 주요 개념 설명"은 현행 접근 방식으로 인해 발생하는 혼란을 강조하며, 이는 법적 책임을 잘못 배분할 위험을 초래합니다.

시행령은 또한 배포자가 개발자의 의도된 목적을 넘어 큰 영향을 미치는 용도로 범용 AI 시스템을 실질적으로 수정하는 경우의 책임 관계를 명확히 해야 합니다. 이러한 경우, 최초개발자가 아닌 배포자가 "고(高)영향 AI 개발자"로 간주되야 하며, 그에 상응하는 의무를 져야 합니다. 이 접근은 최종 애플리케이션을 통제하는 주체가 위험을 평가하고 관리하는 데 가장 적합하다는 기본 원칙을 반영합니다. 이러한 명확한 설명이 없다면, 최초 개발자는 자신이 의도하거나 통제하지 않은 후속 수정에 대해 광범위하고 예측 불가능한 책임을 지게 될 수 있으며, 이는 상당한 법적 불확실성을 야기하고 범용 AI 시스템의 개발 및 배포를 저해할 수 있습니다.

---

[1] https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2V4H1W1T2K5M1O6E4Q9T0V7Q9S0U0.

[2] 법 제 2 조 제 7 항은 "인공지능 사업체"를 다음과 같이 정의합니다. "2.7. '인공지능 사업체'란 인공지능 산업 관련 사업에 종사하는 다음 각 호의 법인, 단체, 개인, 국가기관 등을 말한다: (a) 인공지능 개발자: 인공지능을 개발하고 제공하는 사람; (b) 인공지능 배포자: (a)호 사업체가 제공한 인공지능을 이용하여 인공지능 제품 또는 인공지능 서비스를 제공하는 사람."

부록: 발효일

인공지능법은 2026 년 1 월 22 일에 발효될 예정입니다. 그러나 시행령과 400 쪽 분량의 지침은 올해 12 월 이전에는 확정되지 않을 것으로 예상됩니다. AI 개발자와 배포자가 이 법을 준수하기 위해 절차를 개발하고, 인력을 훈련하며, 제품에 기술적 기능을 통합해야 하는데, 이러한 짧은 기간은 합리적인 준비 시간을 제공하지 못할 것입니다. 따라서 과학기술정보통신부는 이러한 조항의 집행을 최소 6 개월, 바람직하게는 1 년 동안 유예해야 합니다.

제 22 조: AI 의 투명성 보장 의무

시행령 제 22 조는 AI 사업자가 고영향 또는 생성적 AI 를 사용하는 제품 또는 서비스를 제공하기 전에 사용자에게 사전 고지하도록 규정하고 있습니다. 사전 고지는 계약서 또는 이용 약관에 정보를 포함하여 제품에 라벨을 붙이거나, 사용자 화면에 표시하거나, 서비스가 제공되는 장소에 게시하거나, 기타 승인된 방법을 사용하는 방식으로 이루어질 수 있습니다. 제공자는 또한 AI 가 생성한 출력물에 사람이나 기계가 읽을 수 있는 형식으로 라벨을 붙일 수 있습니다. 이러한 고지는 사용자가 정보를 어떻게 인식하는지와 연령, 신체적 또는 사회적 조건을 고려하여 명확하고 쉽게 인식할 수 있어야 합니다. AI 가 사용되고 있음이 이미 명백한 경우, 시스템이 내부 사업 목적으로만 사용되는 경우, 또는 제품 또는 기술의 특성 및 용도에 따라 장관이 정하는 기타 경우에는 이 의무가 적용되지 않습니다.

과학기술정보통신부는 투명성 의무가 개발자가 아닌 AI 배포자에게 적용되도록 제 22 조를 개정해야 합니다. 배포자는 AI 시스템이 소비자 대상 환경에서 어떻게, 어디에, 어떤 목적으로 배포되는지를 결정하기 때문입니다. 특히 관할권 외부에 있는 개발자는 모델이 어떻게 통합, 맞춤화되거나 최종 사용자에게 제공되는지에 대한 통제력이나 가시성이 없는 경우가 많기 때문에 배포와 관련된 공개 및 라벨링 의무에 대해 책임을 지는 것은 비현실적이고 불공평합니다. 많은 경우 배포자는 가중치 미세 조정, 독점 애플리케이션에 통합, 출력이 제공되는 사용자 인터페이스 설계 등 모델의 동작을 크게 변경합니다. 이는 배포자만이 의미 있고 상황에 적합한 공개를 구현하는 데 필요한 운영 지식을 가지고 있음을 의미합니다. 이러한 요구 사항을 배포자에게만 국한하면 사용자 경험과 준수 역량을 직접 제어하는 당사자에게 가장 효과적인 책임을 부여할 수 있습니다.

또한, 해당 지침은 특히 실제 음향과 구분이 어려운 오디오 출력물에 대해 “명확하고 눈에 띄는” 공개가 무엇인지에 관해, 기관들이 원본 법 제 31 조 제 3 항에 따른 의무를 어떻게 이행할 수 있는지에 대해 거의 명확성을 제공하지 않습니다. 현재 구조는 중복된 의무를 부과할 위험이 있으며, 이는 사용자 이해도를 높이지 못한 채 불필요한 부담을 초래할 것입니다. 이를 해결하기 위해 과학기술정보통신부는 사용자에게 해당 제품 또는 서비스가 생성형 AI 를 활용한다는

사실을 법 제 31 조 제 1 항에 따라 통지하는 조건 하에, 단일하고 명확한 표시 방법으로 두 조항을 모두 충족할 수 있도록 이러한 요건을 간소화해야 합니다.

또한, 제 22 조에는 동등한 외국 규제 제도를 준수하는 것이 국내 정보 공개 및 신고 요건을 충족하는 것으로 인정하는 상호 인정 조항이 포함되어야 합니다. 많은 AI 배포업체가 여러 관할권에 걸쳐 운영되고 있으며, 각 규제 시스템에 대해 동일한 투명성 메커니즘을 개별적으로 마련하도록 요구하는 것은 불필요한 비용을 발생시키고, 사용자 경험의 일관성을 해치며, 규정 준수 방식을 분산시킬 위험이 있습니다. 상호 인정 메커니즘을 통해 규제 기관은 실질적인 성과에 집중하고 국제 규제 수렴을 장려할 수 있습니다.

과학기술정보통신부는 제 22 조 (1)항을 다음과 같이 개정하는 것을 검토해야 합니다:

> *"(1) 고위험 AI 또는 생성 AI(이하 "제품 등")를 사용한 제품 등을 제공하기 전에 AI 사업체배포자는 법 제 31 조 (1)항에 따라 다음 각 호의 방법 중 어느 하나로 사전 통지를 제공해야 합니다:*
>
> *1. 제품 등에 직접 표시하거나 계약서, 매뉴얼, 이용약관 등에 명시.*
>
> *2. 사용자 화면, 터미널 등에 표시.*
>
> *3. 제품 등이 제공되는 장소(관련 장소와 합리적으로 관련된 범위 내 장소 포함)에 쉽게 인식할 수 있는 방식으로 게시.*
>
> *4. 기타 과학기술정보통신부장관이 제품의 특성을 고려하여 인정하는 방법**(이와 동등한 수준의 사용자 보호를 규정하는 외국의 법령에 따른 동등한 공개 또는 고지 요건을 준수하는 것 포함)**으로서 이 조에 따른 의무를 충족하는 것으로 간주되는 방법*
>
> ***(2) 법 제(1)항 및 제 31 조 (2)항과 제 31 조 (3)항의 목적을 위해, 단일하고 명확하며 눈에 띄는 표시 또는 통지 방법은 사용자에게 제품 또는 서비스가 제 31 조 (1)항에 25 매사추세츠 가 노스웨스트 스위트 300C 워싱턴 디씨 20001 페이지 4 따라 요구되는 생성 AI 를 활용한다는 사실을 알린 경우 다중 공개 요건을 충족하기에 충분한 것으로 간주한다."***

제 23 조: AI 시스템의 안전성 보장 의무

제 23 조는 최소 10^{26} FLOPs 의 누적 연산 용량을 사용하여 훈련받은 AI 시스템에 대해 과학기술정보통신부(MSIT)에 위험 완화 및 관리 계획을 의무적으로 제출하도록 하는 등 추가

안전 요건이 적용되는 AI 시스템의 범위를 정의합니다. 누적 연산 용량 계산 방법론은 과학기술정보통신부의 추가 지침을 따릅니다.

이러한 시스템에 대한 요건 자체는 엄격하지 않으며 업계에서 채택한 자발적 관행과 일치하지만, 컴퓨팅 학습을 위험의 대리 지표로 사용하는 것은 효과적이지 않으며 특히 미국 등 해외 AI 개발자들의 범위 설정에 불균형적인 위험을 초래합니다. 규제 임계값을 컴퓨팅 용량에 기반하는 것은 결함이 있고 점점 더 시대에 뒤떨어진 위험 대용 지표입니다. 모델이 더욱 효율적이고 전문화됨에 따라 훨씬 적은 컴퓨팅 성능으로 고급 기능을 구현하게 되어 이러한 임계값은 더 이상 유효하지 않게 됩니다. 예를 들어, 한국이 고위험으로 분류할 모델과 성능이 비슷한 중국의 DeepSeek-V3 는 컴퓨팅 사용량이 적다는 이유만으로 이러한 의무 범위에서 제외될 것입니다. 더욱이, 제 23 조는 컴퓨팅 임계값을 기반 모델이 아닌 AI 시스템에 적용함으로써 이러한 문제를 더욱 악화시킵니다. 이러한 접근 방식은 학습, 배포 및 컴퓨팅 미세 조정을 혼동할 뿐만 아니라 동일한 모델을 기반으로 구축된 여러 시스템에 대해 중복된 위험 평가를 수행하도록 강요합니다. 마지막으로, 계산 임계값에 대한 의무 강화는 미국 기업에 불균형적으로 영향을 미치는 동시에 국내 및 중국 경쟁사를 배제하는 차별적 제도를 조성할 위험이 있습니다. 이는 차별적 대우를 피하겠다는 한국의 WTO 및 한미 FTA 약속과 상충될 수 있습니다. 이러한 결과를 방지하기 위해 시행령은 계산 임계값을 완전히 폐지하고 대신 AI 시스템의 성능을 기반으로 위험을 평가해야 합니다.

그러나 시행령이 고영향 시스템 지정 기준으로 컴퓨팅 임계값을 유지한다면, 과학기술정보통신부는 최소한 특정 원칙을 채택해야 합니다. 첫째, 위에서 설명한 바와 같이 임계값를 시스템이 아닌 AI 모델에 적용되도록 해야 합니다. 둘째, 업계와 긴밀히 협력하여 설계 및 적용이 기술적 현실과 국제적 모범 사례를 반영하도록 해야 합니다. 여기에는 광범위한 업계 합의와 지지를 받는 접근 방식을 활용하여 컴퓨팅 기반 프레임워크의 적법성, 예측 가능성 및 효과를 개선하는 것이 포함됩니다.3 셋째, 이 의무는 컴퓨팅 임계값을 초과하는 기본 모델에만 적용되어야 하며, 해당 기본 모델에서 파생된 미세 조정 모델은 범위에서 명시적으로 제외되어야 합니다.이는 규제 과잉으로 인한 혁신 위축 및 기초 모델 기반의 하위 응용 프로그램 개발 저해를 방지하는 핵심 안전장치입니다. 또한, 시행령 제 23 조를 개정하여 AI 시스템의 안전 의무 적용 여부를 판단하는 세 가지 정의 기준을 명시적으로 명문화하고, 이러한 핵심 요소들을 하위 지침에서 법적 구속력이 있는 조항으로 재배치하여 명확성과 법적 확실성을 강화해야 합니다. 넷째, 과학기술정보통신부는 급속한 기술 발전과 진화하는 모델 역량을 고려하여 컴퓨팅 임계값을 주기적으로 검토하도록 하는 조항을 포함해야 합니다.

과학기술정보통신부는 제 23 조를 다음과 같이 개정하는 것을 검토해야 합니다:

(1) 법 제 32 조 (1) 항의 "학습에 사용된 누적 컴퓨팅이 대통령령으로 정하는 기준 이상인 인공지능 ***모델*** ~~*시스템*~~*" 이란 인공지능 기술 발전 수준, 위험 수준 등을 고려하여 과학기술정보통신부 장관이 공고한 기준을 충족하는 인공지능* ***기본 모델*** ~~*시스템*~~*으로, 계산이 26 부동소수점 이상인 것을 의미하며,* ***이러한 기본 모델에서 파생된 미세 조정 모델은 이 규정의 적용에서 제외한다****.*

(2) 제 1 항의 고시에서는 학습에 사용되는 누적 연산량의 구체적인 계산 방법을 포함해야 하며, ***모델의 안전의무 적용 여부를 판단하는 세 가지 정의 기준을 명시해야 한다.***

(3) 과학기술정보통신부장관은 인공지능 기술의 발전과 변화하는 위험 프로파일을 반영하기 위해 업계 전문가와 협의하여 제(1) 항에 따라 규정된 연산 임계값을 주기적으로 검토하고 필요한 경우 개정하여야 한다.

제 24 조: 고영향 AI 검증 절차

제 24 조는 법에 따라 시스템이 "고영향 AI"에 해당하는지 공식 검증을 요청하는 AI 사업체를 위한 절차를 규정합니다. 사업체는 과학기술정보통신부에 공식 요청을 제출해야 하며, 과학기술정보통신부는 사용 부문, 인간 안전과 기본권에 대한 잠재적 위험의 심각성과 빈도, 사전 평가, 전문 위원회 의견, 기타 관련 데이터를 기반으로 신청을 평가합니다. 장관은 30 일 이내에 결정을 내려야 하며, 복잡한 사안의 경우 30 일 더 연장될 수 있습니다. 사업체가 결정에 동의하지 않을 경우, 10 일 이내에 재검증을 요청할 수 있으며, 이 경우 사유와 증빙 자료를 제출해야 합니다. 이러한 요청이 있을 경우, 장관은 전문가의 자문을 받아 재평가를 실시하고 30 일 이내에 답변해야 합니다.

고영향 AI 에 대한 제 24 조의 정의 및 검증 기준은 고영향 환경에서 사용하도록 의도된 시스템만 규제 범위에 포함되도록 축소되어야 합니다. 이러한 명확한 규정이 없다면, 다양한 무해하거나 저위험 애플리케이션에 배포될 수 있는 기초 또는 범용 AI 시스템조차도 의도치 않게 고영향 AI 로 분류되어 과도한 규정 준수 부담을 야기하고 혁신을 저해할 수 있습니다.

더욱이, 최대 60 일, 제한적인 경우 최대 90 일까지 검증 기간을 허용하는 제 24 조에 따른 현행 절차적 일정은 선의로 규정을 준수하려는 기업에게 법적 불확실성과 운영 지연을 초래할 위험이 있습니다. 이 문제를 해결하기 위해 본 조항은 (i) 고영향 AI 시스템으로 분류될 가능성이 낮은 시스템에 대해 신속한 확인 절차를 도입하고, 더 짧은 기간(예: 15 일) 내에 대응을 요구하거나, (ii) 검증 기간 동안 합리적인 사업 판단에 따라 진행한 후 고영향 AI 시스템을 운영한 것으로 판명될 경우 기업의 책임을 면제하는 안전항구 조항을 도입해야 합니다.

과학기술정보통신부는 제 24 조를 다음과 같이 개정하는 것을 검토하여야 합니다:

(1) AI 사업자가 법 제 33 조 (1) 항에 따라 고영향 AI 에 해당하는지 여부에 대한 검증을 요청하고자 하는 경우, 별지 제 2 호 서식의 검증 요청서를 과학기술정보통신부장관에게 제출하여야 한다.

(2) 과학기술정보통신부장관은 다음 각 호의 사항을 고려하여 고영향 AI 에 해당하는지 여부를 판단하여야 한다.

1. 인공지능이 법 제 2 조 제 4 호 각 목의 어느 하나에 해당하는 분야에 사용될 ***목적으로 제공되는지*** *여부*

2. 사람의 생명·신체 안전 및 기본권에 미칠 수 있는 위험의 영향, 심각성 및 빈도와 각 사용 분야의 구체성

3. AI 가 법 제 33 조 (1) 항에 따른 고영향 AI 에 해당하는지 여부에 대한 사전 검토 결과

4. 법 제 33 조 (2) 항에 따라 전문위원회의 자문을 받은 경우 자문 결과

5. 그 밖에 AI 가 고영향 AI 에 해당하는지 여부를 확인하기 위하여 필요한 자료로서 과학기술정보통신부장관이 정하는 자료

(3) 과학기술정보통신부장관은 (1) 항에 따른 요청을 받은 날로부터 30 일 이내에 답변하여야 한다. 이 경우 제품 등의 복잡성, 중요성 등을 고려하여 30 일의 범위에서 그 기간을 연장할 수 있다. ***다만, 고영향 AI 로 분류될 가능성이 명백히 낮은 서비스에 대해서는 과학기술정보통신부장관이 답변기간을 30 일 미만으로 하는 신속확인 절차를 마련하여야 한다.***

(4) (3) 항에 따른 회신을 받은 인공지능사업자는 회신을 받은 날로부터 10 일 이내에 재확인 요청의 목적 및 사유를 기재한 문서(전자문서를 포함한다. 이하 같다)와 필요한 자료를 과학기술정보통신부장관에게 제출하여 재확인을 요청할 수 있다.

(5) (4) 항에 따른 재확인 요청을 받은 과학기술정보통신부장관은 법 제 33 조 제 2 항에 따른 전문위원회(이하 "전문위원회"라 한다)의 자문을 받아 해당 제품이 고영향 인공지능에 해당하는지 여부를 재확인하고, 재확인 요청을 받은 날로부터 30 일 이내에 회신하여야 한다.

(6) 사업자가 검증 결과를 받기 전 기간 동안 자사 시스템이 고영향 AI 가 아니라는 합리적인 판단에 따라 배포 또는 서비스 제공을 진행한 경우, 해당 사업자는 추후 해당 시스템이 고영향 AI 로 판명되는 경우 고영향 AI 의무 불이행에 대한 책임을 지지 않는다.

제 26 조: 고영향 AI 사업 의무

제 26 조는 AI 기업이 관련 법률에 따라 영업비밀로 간주되는 정보를 제외하고, 영향력이 큰 AI 시스템과 관련된 위험 관리 관행의 핵심 요소를 웹사이트에 공개하도록 규정하고 있습니다. 이러한 공개에는 위험 관리 정책 및 구조, 표준 및 설명 조치, 사용자 보호 조치, 그리고 AI 시스템 감독 책임자의 연락처 정보 등 핵심 정보가 포함되어야 합니다. 배포자가 개발자가 이미 이러한 의무를 이행했고 시스템 기능을 크게 변경하지 않는 AI 시스템을 사용하는 경우, 해당 AI 기업은 제 26 조에 따라 규정을 준수하는 것으로 간주됩니다. 배포자는 개발자에게 필요한 정보를 요청할 수 있으며, 개발자는 협조해야 합니다. 또한 AI 기업은 이러한 조치를 최소 5 년 동안 이행하고 문서화해야 합니다.

제 26 조는 위험 관리 의무 이행 및 공개에 대한 주요 책임이 개발자가 아닌 AI 배포자에게 있음을 명확히 하기 위해 개정되어야 합니다. 배포자는 AI 시스템의 사용 방식과 장소를 결정하는 당사자이므로 배포의 맥락, 위험 프로필 및 잠재적 영향을 가장 잘 알고 있기 때문에 적절한 위험 관리를 수행하고 제 26 조 (1)항에 따른 의무를 이행할 수 있는 더 나은 위치에 있습니다. 이러한 책임을 배포자에게 부여하면, 관련 위험이 아직 명확하지 않을 수 있는 개발 단계가 아닌 실제 사용 사례에 기반한 준수를 보장할 수 있습니다.

내부 위험 관리 조치를 공개해야 하는 현행 요건은 철폐되거나 상당히 축소되어야 합니다. 이러한 의무는 내부 위험 정책이나 조직 구조의 공개를 요구하지 않는 모법의 범위를 초과합니다. 공개 의무는 기업이 보안이나 경쟁 우위를 저해할 수 있는 민감한 내부 프로세스를 공개하도록 강요하지 않으면서 투명성과 책임성을 보장하는 데 필요한 범위로 제한되어야 합니다. 규제 당국은 규정 준수 점검의 일환으로 위험 관리 문서를 기밀로 검토할 권한을 보유할 수 있지만, 공개 게시에 대한 포괄적인 요건은 없어야 합니다.

"영업 비밀"만 공개 대상에서 제외하는 현행 조항의 보호 범위는 너무 제한적입니다. 기업은 개인 정보, 상업적으로 민감한 운영 정보, 보안 관련 세부 정보 등 노출되어서는 안 되는 다른 범주의 매우 민감한 정보를 일상적으로 처리합니다. 이 조항은 기밀 유지 보호를 이러한 범주까지 명시적으로 확대하여 규제 당국에 제출되거나 규정 준수 문서에 포함된 민감한 데이터가 공개되지 않도록 보호해야 합니다.

과학기술정보통신부는 제 26 조를 다음과 같이 개정하는 것을 검토해야 합니다:

> *(1) AI ~~사업체~~ **배포자**는 법 제 34 조 (1) 항에 따라 취한 다음 각 호의 조치를 ~~홈페이지 등에 게시하고~~ **필요한 경우 공시하여야 한다**.*

*다만, **정보공개는 투명성과 책임성을 확보하기 위하여 필요한 정보에 한하며,** 부정경쟁방지 및 영업비밀보호에 관한 법률 제 2 조제 2 호에 따른 **영업비밀에 해당하는 사항, 개인정보, 영업상 민감한 운영정보, 보안 관련 사항 등 기타 민감정보**는 제외할 수 있다.*

*1. 법 제 34 조(1)항 제 1 호에 따른 위험관리계획의 주요 내용에 대한 **요약 정보**(위험관리 정책 및 조직체계에 대한 간략한 설명 등)*

2. 법 제 34 조(1)항 제 2 호에 따른 기준 및 설명 조치의 주요 내용

3. 이용자 보호 조치

4. 해당 고영향 인공지능을 관리·감독하는 자의 성명 및 연락처

(2) 법 제 34 조(1)항 제 1 호부터 제 3 호까지의 조치를 전부 또는 일부 이행한 인공지능 시스템을 제공받은 AI 배포자가 해당 인공지능 시스템의 기능에 중대한 변경을 초래하지 아니하는 경우에는 법 제 34 조(1)항의 조치를 이행한 것으로 본다.

(3) AI 도입자는 AI 개발업체에 필요한 자료의 제공을 요청할 수 있으며, AI 개발업체는 이에 협조하도록 노력하여야 한다.

*(4) 인공지능~~사업체~~ **배포자는** 법 제 34 조(1)항 각 호의 조치를 이행하고, 그 근거를 서면으로 5 년간 보관하여야 한다.*

(5) 법 제 34 조(3)항에서 "대통령령으로 정하는 바에 따라 별표 1 의 조치를 이행한 경우"란 별표 1 의 조치를 해당 법에 따라 이행한 경우를 말한다.

제 27 조: 고영향 AI 영향 평가

제 27 조는 고영향 AI 시스템에 대한 법 제 35 조 (3)항에 따른 AI 영향평가 수행 요건을 명시하고 있습니다. 해당 평가는 기본권이 침해될 수 있는 개인 또는 집단을 식별하고, 침해될 수 있는 권리를 명시하며, 그러한 영향의 사회적 및 경제적 결과를 평가해야 합니다. 또한 AI 의 사용 방식을 검토하고, 평가에 사용된 정량적 또는 정성적 지표와 계산 방법을 상세히 기술하며, 위험 예방, 손실 완화 및 복구 전략을 포함해야 합니다. 평가 결과 개선 필요성이 발견되는 경우, 결과와 실행 계획을 제시해야 합니다. AI 기업은 직접 평가를 수행하거나 제 3 자에게 위탁할 수 있으며, 과학기술정보통신부는 평가 방법 및 절차에 관한 보다 상세한 지침을 발행할 수 있습니다.

현재 제 27 조 초안은 개발자 또는 배포자가 영향평가 수행에 대한 주요 책임을 지는지 여부를 명시하지 않습니다. 배포자는 영향력이 큰 AI 시스템이 어떻게 그리고 어떤 맥락에서 사용되는지를 결정하기 때문에 기본권, 사회적 영향 및 사용 행태에 미치는 잠재적 영향을 평가하는 데 가장 적합한 위치에 있습니다. 따라서 제 27 조는 배포자에게 주요 책임을 명확히 부여하는 동시에, 필요한 경우 개발자가 제공하는 정보에 의존할 수 있도록 허용해야 합니다.

배포 담당자가 영향 평가 과정을 주도해야 하지만, 종종 개발자만이 제공할 수 있는 시스템의 기술적 세부 사항이 필요합니다. 본 조항은 개발자가 평가 완료에 필요한 관련 문서, 데이터 및 기술적 설명을 제공함으로써 배포 담당자와 협력하기 위해 합리적인 노력을 기울여야 함을 명시해야 합니다. 이러한 접근 방식은 책임성과 실질적 실행 사이의 균형을 맞춥니다.

중복되는 준수 부담을 줄이고 규제 상호운용성을 증진하기 위해, 본 조항은 배포자가 국제적으로 인정된 표준 또는 프레임워크(예: OECD, ISO/IEC 또는 기타 신뢰할 수 있는 관할권 절차)에 따라 이미 수행된 영향 평가를 활용할 수 있도록 허용해야 합니다. 단, 해당 평가가 실질적으로 동등해야 합니다. 이러한 인정은 글로벌 모범 사례와 부합하고 국경 간 혁신을 지원하는 동시에 기본권의 강력한 보호를 보장할 것입니다.

과학기술정보통신부는 제 27 조를 다음과 같이 개정하는 것을 검토해야 합니다:

> *(1) AI **배포자는** 법 제 35 조 (3) 항에 따른 AI 영향평가(이하 "영향평가"라 한다) **의 주요 책임을 지며, 영향평가는** 다음 각 호의 사항을 포함해야 한다.*
>
> *1. 해당 고영향 AI 를 사용하는 제품 또는 서비스로 인해 기본권에 영향을 미칠 가능성이 있는 대상의 파악(특정 특성을 가진 개인 또는 집단의 파악을 말한다).*
>
> *2. 고영향 AI 로 인해 영향을 받을 수 있는 기본권의 유형 파악*
>
> *3. 고영향 AI 로 인해 개인의 기본권에 발생할 수 있는 사회·경제적 영향의 세부 내용 및 범위*
>
> *4. 해당 고영향 AI 의 사용 행태*
>
> *5. 영향평가에 사용된 정량적 또는 정성적 평가 지표 및 결과 산출 방법*
>
> *6. 고영향 AI 로 인한 위험 예방 및 손실 회복 등*
>
> *7. 개선이 필요한 경우 영향평가 결과 및 시행 계획에 관한 사항*

*(2) 인공지능~~사업체~~ **배포자**는 직접 또는 제 3 자에게 위탁하여 영향평가를 실시할 수 있으며, **국제적으로 인정된 표준 또는 프레임워크에 따라 이전에 실시된 평가에 의존할 수 있다. 다만, 그 평가가 이 조의 요건과 실질적으로 동등한 경우에는 그러하다.***

(3) AI 개발자는 시행자가 영향평가를 완료하는 데 필요한 관련 기술 정보, 문서 및 협력을 제공하기 위해 합리적인 노력을 기울여야 한다.

*(~~3~~**4**) 법 및 이 영에 달리 규정된 경우를 제외하고 과학기술정보통신부장관은 영향평가의 구체적인 내용 및 방법을 수립하여 보급할 수 있다.*

결론

과학기술정보통신부가 AI 기본법 시행령을 확정함에 따라, 시행령이 규제 의무를 그 의무를 이행하기에 가장 적합한 기관에 맞게 조정하는 것이 중요합니다. 투명성 요건(제 22 조), 고영향 AI 검증 절차(제 24 조), 위험 관리 및 정보 공개 의무(제 26 조), 영향 평가(제 27 조) 등 주요 조항 전반에 걸쳐, AI 시스템의 사용 방식과 맥락을 결정하는 주요 책임은 배포자에게 있으며, 개발자는 필요한 기술 정보를 제공하여 협력할 명확한 의무를 가져야 합니다. 또한, 이 프레임워크는 상호 인정 메커니즘과 국제적으로 인정되는 평가의 수용을 통합하여 중복된 준수 부담을 줄이고 국경 간 규제 상호운용성을 지원해야 합니다. 또한, "고영향 AI"의 범위는 진정으로 고위험 상황을 대상으로 좁고 명확하게 정의되어야 하며, 정보 공개 요건은 책임 소재 규명에 꼭 필요한 정보로 제한되어야 하며, 민감 정보 보호는 영업비밀을 넘어 개인, 운영 및 보안 관련 데이터까지 확대되어야 합니다.

성공적인 시행을 위해 과학기술정보통신부는 기업이 새로운 요건에 적응할 수 있도록 준비 기간을 더 길게 제공하고, 절차 초기에 명확하고 상세한 규제 지침을 발표해야 합니다. 이 기간 동안 과학기술정보통신부는 이러한 요건의 시행에 대한 유예를 약속해야 합니다.

한국의 인공지능 기본법 시행령은 적절하게 개발된다면 글로벌 AI 거버넌스 분야의 선도 기업으로서 한국의 입지를 강화할 수 있는 기회를 제공합니다. 한국의 탄탄한 국내 AI 생태계와 확대되고 있는 국제 시장 입지를 고려할 때, 지나치게 제한적인 규제는 외국인 투자를 위축시키고, 연구개발을 저해하며, 한국 기업과 스타트업의 경쟁력을 약화시킬 수 있습니다. 균형 잡히고 국제적으로 상호운용 가능한 접근 방식은 기본권을 보호하면서도 혁신, 투자 및 장기적 경제 성장을 촉진시킬 것입니다.