2025 년 10 월 2 일

「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 하위법령 및 가이드라인(안)

BUSINESS SOFTWARE ALLIANCE (BSA) 의견서

과학기술정보통신부 귀하

BSA 비즈니스 소프트웨어연합 (Business Software Alliance, BSA)[1] 은 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 '인공지능 기본법') 및 해당 법률의 시행령(안)을 포함하는 하위법령 및 가이드라인 [2] (이하 '하위법령(안)')와 관련하여 의견을 제출할 기회가 주어져 기쁘게 생각합니다.

BSA 는 각국 정부와 세계시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있는 연합체로 BSA 회원사는 AI 제품 및 서비스 제공 뿐만 아니라 제 3 자가 AI 시스템 및 애플리케이션 개발에 활용할 수 있는 도구를 제공하는 데 앞장서고 있습니다.

인공지능 기본법 제정은 매우 중요한 정책적 진전이었습니다. 이 법은 AI 발전을 지원하기 위한 진흥 규정과 신뢰 기반을 조성하기 위한 규제 조항을 모두 포함하고 있습니다. 다만 하위법령(안)이 발표되기 전 산업계에서는 우려가 있었습니다. 특히, 2026 년 1 월부터 발효 예정인 "인공지능사업자"에게 부과되는 의무 조항[3]들이 혁신을 저해하고, 투자를 위축시키며, 궁극적으로 한국의 AI 정책 목표를 약화시킬 수 있다는 점이 그 원인으로 지목되었습니다[4].

---

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] 인공지능기본법에 대한 하위법령(안)은 다음과 같이 구성됨:
- a) 인공지능기본법 시행령(안)
- b) 인공지능기본법에 관한 고시(안): 1) 사업자 책무 고시(안); 2)안전성 확보 고시(안).
- c) 가이드라인(안) 1)고영향 AI 판단 가이드라인(안); 2) 고영향 AI 사업자 책무 가이드라인(안); 3) AI 안전성 확보 가이드라인(안); 4) AI 투명성 확보 가드라인(안); 과 5) AI 영향평가 가이드라인(안).

[3] 인공지능사업자는 인공지능기본법 제 2 조 제 7 호에 따라 "인공지능 산업과 관련된 사업에 종사하는 법인, 단체, 개인 및 국가기관 등"으로 정의되며, 인공지능개발사업자와 인공지능이용사업자를 포괄함. 관련 의무사항은 인공지능기본법 제 31 조(인공지능 투명성 확보 의무), 제 32 조(인공지능 안전성 확보 의무), 제 33 조(고영향 인공지능의 확인), 제 34 조(고영향 인공지능과 관련한 사업자의 책무), 제 35 조(고영향 인공지능 영향평가), 제 36 조(국내 대리인 지정)에 규정되어 있음.

[4] 산업계의 주요 우려 사항 참조: 1."Korea considers grace period for AI Basic Act amid industry concerns and delays", Chosun Biz, August 2025, https://biz.chosun.com/en/en-it/2025/08/05/WOZ7AGFKDRDLVDZWJG6TN6NWZM/, 2 "South Korea AI law under renewed pressure for revision over regulation, trade concerns", MLex, July 2025, https://www.mlex.com/mlex/articles/2370338/south-korea-ai-law-under-pressure-for-revision-amid-growing-concernsj

이러한 배경에서, BSA 는 하위법령(안)이 해당 규제 의무들이 어떻게 해석되고 이행될지에 대한 체계적이고 필수적인 세부사항을 제시하고 있다는 점에서 높이 평가합니다. 특히 하위법령(안)이 고영향 AI 의 정의 및 범위, 그리고 인공지능개발사업자와 인공지능이용사업자 각각에게 귀속되는 의무 등[5] 중요한 기본 쟁점들에 대한 구체적인 지침을 제공하고 있음에 주목합니다. 이를 위한 과기정통부의 노고에 깊이 감사드립니다.

BSA 는 하위 법령(안)에서 다루어지지 않았거나 추가 검토가 필요한 사안에 대한 정책 제언을 드리고자 합니다. 또한 기업들이 효율적이고 예측 가능하게 법을 준수할 수 있도록 추가적인 지침과 세부 지침이 필요한 영역에 대한 의견을 제언 드리고자 합니다.

요약

다음과 같은 내용을 제언드립니다.

1. **외부 기관을 통한 인증 및 검증 의무 부과 지양**

   인공지능사업자가 엄격한 자체 평가 절차와 독립적인 내부 테스트 팀을 통해 자체적으로 점검할 수 있도록 허용되어야 합니다. 더 나아가, 미국 국립표준기술연구소(NIST)의 AI 위험관리 프레임워크와[6] 등 국제적으로 공인된 프레임워크와 표준을 활용할 수 있는 유연성을 보장해야 합니다.

2. **AI 를 사용한 경미한 수정의 투명성 의무 적용 제외**

   법 제 31 조의 투명성 의무는 콘텐츠의 의미나 본질적 내용을 변경하지 않는 경미한 수정이나 개선에는 적용되지 않음을 명시적으로 규정해야 합니다.

3. **위험 평가 요소 정합성 확보 및 이행 조치 결과 제출 의무 간소화**

   1) 시행령(안) 제 23 조의 안전 기준은 다양한 애플리케이션에 활용될 수 있는 기반 기술인 AI 모델에 적용되도록 하고, 특정 용도를 위해 하나 이상의 AI 모델과 기타 요소가 결합된 AI 시스템에는 적용되지 않도록 규정해야 합니다.

   2) 단순 누적 연산량 기반의 임계값 설정은 지양해야 합니다.

   3) 법 제 32 조의 "중대한 영향" 평가 기준은 제 35 조에 따른 인공지능 영향평가 기준과 정합성을 이루도록 마련해야 합니다.

   4) 기업이 안전조치 관련 문서를 내부에 보관하도록 하고, 실제 피해에 대한 조사가 개시될 때에만 과기정통부에 제출하도록 규정해야 합니다.

[5] 고영향 인공지능 판단 가이드라인 (안) 및 고영향 AI 사업자 책무 가이드라인 (안)에 규정

[6] NIST AI Risk Management Framework, January 2023, https://doi.org/10.6028/NIST.AI.100-1.

4. **'고영향 AI' 의무는 AI 모델이 아닌 AI 시스템에 적용**

   시행령(안) 제 26 조에 이러한 구분을 반영하여, 법 상 고영향 AI 에 대한 의무가 AI 모델이 아니라 AI 시스템에 부과됨을 명확히 규정해야 합니다. 이를 통해 해당 의무들이 실제 위험을 초래하는 구체적 사용 사례에 부과되도록 해야 하며, 고영향 AI 과 저영향 AI 응용분야를 모두 지원하는 범용 기술에는 불필요한 규제가 적용되지 않도록 해야 합니다. 이를 통해 감독의 초점이 가장 효과적인 영역, 즉 고영향 AI 에 집중될 수 있습니다.

5. **인공지능개발사업자와 이용사업자 간 책임 분담 해소를 위한 시행령(안) 제 26 조 제 2 항 삭제**

   법 제 34 조 제 1 항의 의무는 고영향 AI 사업자 책무에 관한 가이드라인에서 규정한 책임 배분에 따라 엄격히 이행되도록 해야 합니다.

6. **법 제 40 조에 따른 조사 권한 운영 방식에 대한 추가 지침 마련**

   시행령(안) 제 31 조는 조사 권한 발동을 위한 법적 절차, 기준, 요건을 명확히 규정하고, 특히 '부당한 목적'에 따른 민원 제기 여부의 판단 기준을 명확하게 정의해야 합니다. 조사는 실제 위반에 대한 합리적 근거가 있는 경우에만 개시되어야 하며, 단순한 민원 제기만으로는 그 권한이 발동되어서는 안 됩니다. 특히 현장조사 등은 사전에 법원의 허가를 받은 경우에만 행사될 수 있어야 합니다.

외부 기관을 통한 인증 및 검증 의무 부과 지양

법 제 30 조 제 3 항은 고영향 AI 를 제공하려는 인공지능사업자가[7] "사전에 검・인증 등을 받도록 노력하여야 한다"고 규정하고 있습니다. 또한 시행령(안) 제 21 조는 과학기술정보통신부가 "검증 및 인증 활동에 관한 기준, 방법 및 절차"를 마련·배포할 수 있도록 규정하고 있습니다.

BSA 는 제 3 자(외부)에 의한 검 인증 의무화에 우려를 표하며, 인공지능사업자가 철저한 자체 평가와 내부의 독립적인 테스트 팀을 통해 검증할 수 있도록 시행령(안)에서 규정해주시기를 제언드립니다. AI 에 대한 철저한 검증과 평가는 중요합니다. 그러나 외부기관 등 제 3 자가 이를 수행할 경우 기업의 지식재산권, 개인정보보호 및 사이버 보안에 중대한 위험을 초래할 수 있습니다. 따라서 인공지능사업자가 엄격한 자체 평가 절차와 독립적인 내부 테스트 팀을 통해 자체적으로 점검할 수 있도록 허용되어야 하며, 미국 국립표준기술연구소(NIST)의 AI 위험관리 프레임워크[8]등 국제적으로 공인된 프레임워크 및 표준을 유연하게 활용할 수 있도록 해야 합니다.

외부기관을 통한 검・인증 의무화에 따른 주요 위험은 다음과 같습니다.

- 외부 검・인증 과정에서 기업은 기밀 및 민감 정보를 제 3 자와 불가피하게 공유해야 합니다. 이는 기업의 지식재산권 뿐만 아니라 개인정보와 사이버 보안을 위협할 수 있습니다. 예를 들어, AI 시스템의 개발자가 외부 감사기관과 개인정보를 공유해야 할 경우

[7] 인공지능사업자는 인공지능기본법 제 2 조 제 7 호에 따라 "인공지능 산업과 관련된 사업에 종사하는 법인, 단체, 개인 및 국가기관 등"으로 정의되며, 인공지능개발사업자와 인공지능이용사업자를 포괄함.

[8] NIST AI Risk Management Framework, January 2023, https://doi.org/10.6028/NIST.AI.100-1.

대량의 개인정보를 이전해야 하는 상황이 발생할 수 있습니다. 감사기관이 충분한 수준의 개인정보 보호조치를 구현하지 않은 경우 AI 기업이 해당 정보를 보호하기 위해 적용하는 기존의 보호 조치를 약화시킬 수 있습니다. 마찬가지로 감사기관에 데이터를 이전하는 과정이나 감사기관에서 데이터를 보관하는 중에 악의적인 공격에 노출될 가능성이 있습니다.

- 특히 AI 감사기관에 대한 국제 공인 표준이 아직 개발 중이라는 점에서 완전하지 않은 것이 현실입니다. AI 감사의 표준, 인증된 시험 절차나 명확한 책임 메커니즘 또한 부재한 상황에서 현재 AI 감사 분야는 다른 산업의 감사 기관에 적용되는 것과 같은 견고한 보호장치가 부족할 수 있습니다. 또한 전문성과 역량을 갖춘 AI 감사기관의 수 또한 제한적입니다. AI 감사의 보호 장치 및 품질 보증 부족은 기업이 선택하는 감사기관과 해당 감사기관이 적용하는 기준에 따라 일관성 없는 결과를 초래할 위험이 있습니다. .
- 이는 불필요한 비용과 절차가 추가되어 AI 개발 및 도입이 지연되고, 사회적 편익은 제한적인 반면 기업 부담은 가중됩니다. 이는 궁극적으로 한국이 책임 있는 AI 기술 도입에서 국제 경쟁력을 약화시키는 결과로 이어질 수 있습니다.

이와 대조적으로, 독립적인 내부팀이 수행하는 자체 시험과 인증은 이러한 문제없이 위험을 관리할 수 있으며, 비용과 절차 부담도 적습니다. 이는 정부가 강조하는 "책임 있는 AI 혁신 촉진" 기조와도 부합합니다.

제언: 외부 인증 및 검증 의무 부과를 지양해야 합니다. 대신, AI 사업자에게 엄격한 자체 평가 프로세스와 독립적인 테스팅 팀을 통한 내부 점검을 허용하고, 국제 표준(예: NIST AI 위험 관리 프레임워크)을 활용할 수 있는 유연성을 제공해야 합니다.

AI 를 사용한 경미한 수정의 투명성 의무 적용 제외

법 제 31 조는 고영향 AI 또는 생성형 AI 를 제공하는 인공지능사업자에게 AI 가 생성한 출력물이 현실과 구별하기 어려운 경우 사용자에게 이를 고지하고 '표시'하도록 규정하고 있습니다. 하위법령(안)은 이러한 고지 및 표시가 사용자가 "소프트웨어를 이용하여 쉽게 내용을 확인할 수 있는 방법으로"[9] 제공될 수 있으며 "소프트웨어를 통해 확인 가능한 비가시적 표시"[10] 를 포함한 방법이 허용된다고 명시하고 있습니다. 특히, [Coalition for Content Provenance and Authenticity(C2PA)] 표준을 활용한 비가시적 메타데이터 삽입이 법 제 31 조[11]요건을 충족하는 방안의 하나로 제시하고 있습니다. 또한 이러한 의무가 "이용자에게 최종적으로 AI 제품 및 서비스를 제공하는 사업자"에게[12] 귀속됨을 명확히 규정합니다.

이와 같이 기반 모델 개발자가 다른 기업이 해당 모델을 활용하여 제품·서비스를 제공하는 경우에는 투명성 의무를 부담하지 않는다는 점이 명확해진 것은 매우 중요한 진전입니다. 인공지능개발사업자 및 그 외 주체(이용사업자, 배포자 등) 의 구분이 분명해져야 하며, 투명성 의무가 실제로 AI 도구를 사용하여 콘텐츠를 생성하는 주체에게 부과되도록 유지해야 합니다.

[9] 시행령(안) 제 22 조 3 항, 하위법령(안) 내 27pg
[10] 인공지능 투명성 확보 가이드라인(안), 하위법령(안) 내 68p
[11] 인공지능 투명성 확보 가이드라인(안), 하위법령(안) 내 70p.
[12] 인공지능 투명성 확보 가이드라인(안), 하위법령(안) 내 65p.

이러한 주체만이 맥락과 잠재적 위험성을 가장 잘 파악할 수 있으며, 이에 따라 필요한 투명성 조치를 적절히 이행할 수 있습니다.

아울러 투명성 의무는 국제적으로 형성되고 있는 모범 규범과 정합성을 이루도록 하고, 인공지능사업자에게 불필요한 규제 부담을 지우지 않으면서, 책임을 가장 적절히 이행할 수 있는 주체에게 명확히 귀속되도록 해야 합니다.

끝으로, 비례성 확보를 위해 법 제 31 조의 투명성 의무는 단순히 밝기·대비·확대/축소와 같이 콘텐츠의 의미나 본질을 실질적으로 변경하지 않는 경미한 수정[13]에는 적용되지 않아야 합니다. 이는 EU AI 법의 경미한 수정 예외[14] 와도 일치하며, 국제 규제 정합성 확보에 기여할 것입니다.

제언: 법 제 31 조상의 투명성 의무가 콘텐츠의 의미나 실질을 중대하게 변경하지 않는 경미한 수정이나 개선에는 적용되지 않음을 명시해주시길 제언드립니다. 이를 통해 한국의 규제 프레임워크가 비례성을 확보하고, 저위험 활동에 대한 과도한 규제를 방지하며 국제적 규제 정합성을 촉진하는데 기여할 것입니다.

위험 평가 요소의 정합성 확보 및 이행 조치 결과 제출 의무의 간소화

법 제 32 조는 시행령(안) 제 23 조는 AI 시스템이 누적 연산량 기준(10 의 26 제곱 FLOPs, 초당 부동소수점 연산)을 초과하는 경우 다양한 안전 및 위험 관리 조치를 이행하도록 규정하고 있습니다. 하위법령(안)은 누적 연산량 기준 외에도 해당 AI 시스템이 "현재 AI 시스템에 활용되는 AI 기술 중 최첨단의 기술을 적용하여 구성·운영"되고, "사람의 생명, 신체의 안전 및 기본권에 광범위하고 중대한 영향을 초래할 위험"이[15] 있는 경우에 해당함을 규정합니다.

BSA 는 시행령(안) 제 23 조에 대해 다음 네 가지 수정을 제언드립니다.

- 첫째, 제 23 조의 안전 기준은 AI 시스템이 아닌 AI 모델에 적용됨을 명확히 해야 합니다. AI 모델은 광범위한 응용 분야에 활용될 수 있는 기반 기술이며, AI 시스템은 하나 이상의 AI 모델을 다른 요소와 결합하여 특정 목적을 위한 AI 응용 프로그램을 생성 것으로 명확히 구분됩니다. 이러한 구분이 하위법령(안)에 명확히 규정되는 것을 제언드립니다. 예를 들어, 하나의 거대 언어 AI 모델 (LLM)은 번역, 챗봇, 소프트웨어 코드 생성 등 수백 개의 AI 시스템에 통합될 수 있습니다. 즉, 모델은 기반 기술이고 시스템은 이를 특정 목적에 사용하는 것입니다.
- 둘째, 누적 연산량을 기준으로 규제하는 방식을 재고해주시길 제언드립니다. 연산량을 기준으로 규제하는 것은 고부하 모델이 자동적으로 고영향 AI 로 간주된다는 전제를 두고 있으나, 실제로는 그렇지 않습니다. 훈련 연산량은 모델이 사전 훈련 단계에서나 후속 수정

[13] 기타 경미한 수정에는 선명도 조정, 채도 조정, 필터 적용, 크기 변경, 비율 조정, 자르기, 형식 변환, 리샘플링, 노이즈 제거, 그리고 오디오에서의 배경 잡음 제거가 포함됩니다.

[14] EU AI Act, Article 50(2). This article states that providers of AI systems that generate synthetic audio, image, video or text content must ensure outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Importantly, Article 50 includes an exception: the obligation does not apply where the AI system "performs an assistive function for standard editing or does not substantially alter the input data provided by the deployer or the semantics thereof."

[15] 안전성 확보 고시(안), 하위법령(안) 내 49p.

과정에서 초래할 수 있는 위험과 직접적인 상관관계가 없습니다. 또한 기술이 급격히 발전함에 따라 연산 임계값 기반의 규제는 빠른 시일 내 뒤처질 가능성이 크며, 정부가 임계값을 반복적으로 갱신해야 하는 문제가 발생할 수 있습니다. 이러한 불확실하고 유동적인 임계값 설정은 산업계, 특히 중소기업이 투자와 기술적 의사결정을 내리는 과정에서 상당한 예측 불가능성과 부담을 초래할 수 있습니다.

- 셋째, 법의 다른 조항들을 토대로 "중대한 영향" 여부를 판단하기 위한 보다 구체적인 기준이 마련되어야 합니다. 시행령(안)이 인공지능사업자에게 AI 가 초래할 수 있는 위험과 영향을 고려하도록 요구하고 있다는 점은 주목할 만합니다. 그러나 "중대한 영향"의 존재를 판단하기 위한 기준은 보다 구체적으로 마련되어 기업들에게 더 명확한 지침을 제공할 수 있어야 합니다. 구체적으로, 하위법령(안)은 인공지능사업자가 "시스템의 사용 목적, 적용 분야, 합리적으로 예측 가능한 수준의 오용 가능성, 다른 산업 및 기존 AI 시스템의 유사 사례, 잠재적 피해 범위 및 심각도"[16] 등을 종합적으로 고려하여 생명, 신체 안전, 기본권에 미칠 잠재적 영향을 평가해야 한다고만 규정하고 있습니다. 그러나 이러한 평가가 구체적으로 어떻게 수행되어야 하는지에 대한 지침은 부재하며, 특히 "시스템의 사용 목적"과 같이 모호한 표현은 다양한 응용 가능성을 지닌 AI 모델의 맥락에서 기업들에게 상당한 불확실성을 초래할 수 있습니다.
- 넷째, 보고 의무에 대한 재검토를 제언드립니다. 법 제 32 조는 인공지능사업자가 이행 조치 결과를 과학기술정보통신부에 제출하도록 규정하고 있습니다. 더 나아가 하위법령(안)은 이를 매년, 특정 사안이 발생할 때마다(예: 새롭게 식별된 위험이 발생한 경우, 위험의 발생을 인지한 날로부터 1 개월 이내) 제출하도록 규정하고 있습니다.[17] 그러나 이러한 보고 의무는 기업에의 과도한 문서 작업 부담을 초래하고, 실제 위험관리 보다는 형식적인 보고에 자원을 소모하게 할 우려가 있습니다. 이러한 맥락에서 인공지능사업자가 이행 조치에 관한 문서를 내부적으로 보관하도록 규정하되, 실제로 인공지능으로 인해 피해가 발생하여 과학기술정보통신부의 조사가 진행될 경우에만 제출하도록 할 수 있도록 재고해주시기를 제언드립니다. 이는 민감정보의 노출을 줄이고, 보안 위험을 최소화하면서도, 실제 피해가 발생한 경우 규제 당국이 필요한 정보를 적시에 확보할 수 있도록 보장할 것입니다.

(1) 시행령(안) 제 23 조를 AI 시스템이 아닌 AI 모델에 초점을 맞추도록 개정해야 합니다.

(2) 연산 능력에 기반한 임계값 설정 방식에서 벗어나는 방안에 대한 재고가 필요합니다.

(3) 법 제 32 조의 "중대한 영향" 평가 기준을 법 제 35 조의 고영향 인공지능 영향평가 요소와 정합적으로 일치시켜야 합니다.

(4) 안전 조치 이행 결과 제출 의무를 간소화하여, 기업이 문서를 내부적으로 보관하되 실제 피해가 발생하여 과학기술정보통신부가 조사를 진행하는 경우에만 제출하도록 합리화해야합니다.

[16] AI 안전성 확보 가이드라인(안), 하위법령(안) 내 98p

[17] AI 안전성 확보 가이드라인(안), 하위법령(안) 내 135p

고영향 의무는 AI 모델이 아닌 AI 시스템에만 적용

법은 고영향 인공지능 시스템에 의무를 부과함으로써 고영향 시스템을 개발 및 활용하는 기업이 적절한 조치를 취하도록 규정하고 있습니다. 하위법령(안)이 "고영향"의 의미를 정의하는 데 초점을 맞춘 점에 깊이 공감하며, 나아가 의무의 적용 범위를 보다 명확히 할 것을 제언드립니다.

우선적으로 고영향 AI 에 관한 의무가 AI 모델이 아닌 AI 시스템에 부과되도록 명시해야 합니다. 고영향 AI 의무는 수천 가지의 다양한 활용 가능성을 지원하는 기반 기술인 AI 모델에는 적용될 수 없습니다. 이러한 의무는 AI 시스템에 적용될 때 의미가 있습니다. AI 시스템은 하나 이상의 모델과 다른 요소들을 결합하여 특정 환경에서 사용되며, 그 환경은 고영향 시나리오일 수도 있고 비고영향 시나리오리 수도 있기 때문입니다. 예컨대, 시행령(안) 제 26 조는 제 34 조의 의무가 AI 모델이 아니라 특정 목적, 즉 고영향 시나리오에서 활용되는 AI 시스템에 적용됨을 명확히 규정해야 합니다.

제언: 고영향 의무가 기반 기술인 AI 모델이 아니라, 특정 목적을 위해 배포되는 AI 시스템에만 적용됨을 명확히 해 실 것을 제언드립니다. 이러한 구분은 의무가 실제로 위험을 발생시키는 사용 사례에 집중되도록 하는 데 핵심적이며, 고영향과 저영향 응용 분야 모두를 지원할 수 있는 범용 기술에 불필요한 규제가 부과되는 것을 방지합니다. 특히 시행령(안) 제 26 조와 같은 조항에서 이를 명확히 규정하는 것은 불확실성을 줄이고, 과도한 규제를 피하며, 감독의 초점을 고영향 시나리오에서의 AI 활용에 맞추도록 하는 데 기여할 것입니다.

인공지능개발사업자와 이용사업자 간 책임 분담 해소를 위한 시행령(안) 제 26 조 제 2 항 삭제

법 제 34 조와 시행령(안) 제 26 조는 고위험 인공지능 사업자의 일반적인 책임 (위험 관리, 인력에 의한 감독 보장, 안전 및 신뢰성 조치)를 규정하고 있습니다. 그러나 시행령(안) 제 26 조 제 2 항은 특정 상황에서 인공지능이용사업자를 이러한 책임에서 면제하는 것으로 해석할 수 있습니다. 제 26 조 제 2 항에 따르면, 인공지능이용사업자는 "법 제 34 조 제 1 항 제 1 호부터 제 3 호까지의 사항의 조치를 모두 또는 일부 이행한 인공지능시스템을 제공받은 인공지능이용사업자가 인공지능시스템의 중대한 기능 변경을 초래하지 않은 경우에는 법 제 34 조제 1 항에 따른 조치를 이행한 것으로 본다[18]."고 명시되어 있습니다.

하위법령(안)은 제 26 조 제 2 항의 의도는 "인공지능개발사업자가 법에 따른 고영향 인공지능사업자의 책임을 이행하여 인공지능시스템을 인공지능이용사업자에게 제공하는 경우, 이용사업자가 일부 책무를 중복해서 부담하지 않도록 하기 위함[19]"으로 설명합니다. 또한 하위법령(안)은 범용 AI 모델을 자체 시스템에 통합하는 인공지능사업자의 사례를 들어, 이에 해당하는 경우 해당 인공지능사업자는 기존 AI 의 목적·용도·기능을 "중대하게 변경한 것"으로 간주되어 "고영향 인공지능개발사업자의 지위를 갖는다[20]"고 명시하고 있습니다.

[18] 시행령(안) 제 26 조 제 2 항, 하위법령(안) 31p.

[19] 고영향 인공지능 판단 가이드라인 (안), 하위법령(안) 174p.

[20] 고영향 인공지능 판단 가이드라인 (안), 하위법령(안) 174p.

이를 통해 시행령(안) 제 26 조 제 2 항의 운영 방식에 대한 맥락을 어느 정도 제공하지만, 제 26 조 제 2 항이 인공지능개발사업자와 인공지능이용사업자 간의 책임 배분에 상당한 혼선을 초래한다는 점에서 해당 조항을 전면적으로 삭제할 것을 검토해주시길 제언드립니다. 이러한 혼선은 최소 두 가지 이유에서 발생합니다.

- 첫째, 제 26 조 제 2 항은 이용사업자가 AI 시스템을 어느 정도까지 변경해야 개발사업자로 간주되는지에 대해 상당한 불확실성을 야기합니다. 제 26 조 제 2 항은 이용사업자가 아무런 수정 없이 "기성" AI 시스템을 사용하는 상황을 상정하는 것으로 해석될 수 있습니다. 그러나 실제로는 인공지능이용사업자들이 자사의 필요에 맞게 AI 시스템을 구성하거나 미세조정(fine-tuning) 하는 것은 불가피합니다. 이러한 미세조정이 시행령(안) 제 26 조 제 2 항이 상정한 "중대한 기능적 변경"에 해당하는지 여부는 명확하지 않습니다. 따라서 제 26 조 제 2 항은 인공지능이용사업자가 언제 개발사업자 수준의 의무를 지게 되는지를 불명확하게 합니다. 이로 인해 책임이 중복되거나 잘못 배분되는 결과가 발생할 수 있으며 이는 바로 제 26 조 제 2 항을 통해 해소하고자 하는 우려 사항입니다.
- 둘째, 시행령(안) 제 26 조 제 2 항은 인공지능이용사업자를 법 제 34 조에 따른 의무, 즉 AI 시스템이 책임감 있게 배포되도록 보장하는 의무(예: 인력에 의한 감독 보장, 안전 및 신뢰성 확보 조치에 대한 문서화 등)에서 면제될 수 있음을 시사합니다. 그러나 이러한 의무는 실제 사용 환경을 아는 이용사업자만이 수행할 수 있는 의무입니다. 이러한 의무를 인공지능개발사업자가 이용사업자를 대신하여 수행하는 것은 불가능합니다. 실제로 "고영향 AI 사업자 책무 가이드라인(안)"에서도 해당 조치는 인공지능이용사업자가 이행해야 한다고 명확히 규정하고 있습니다.[21]

제언: 인공지능개발사업자와 인공지능이용사업자 간의 책임 분담에 대한 혼란을 해소하기 위해 시행령(안) 제 26 조 제 2 항의 삭제를 검토해주시길 제언드립니다. 법 제 34 조 제 1 항상의 의무는 "고영향 AI 사업자 책무 가이드라인(안)"에서 명시된 책임 분담에 따라 엄격하게 이행되어야 합니다.

국내대리인 지정 요건의 비례성 확보 및 역할 명확화

법 제 36 조와 시행령(안) 제 28 조[22]는 한국 내 주소지나 영업소가 없는 인공지능사업자가 특정 기준(그 중 일부는 글로벌 매출을 기준으로 함)을 초과하는 경우 국내 대리인을 지정하도록 요구하고 있습니다. 합리적인 기준을 마련하기 위해서는 매출 기준을 글로벌 매출 기준이 아니라 한국 내 이용자로부터 발생한 매출을 기준으로 수정되어야 합니다. 이는 의무가 사업자의 실제 한국 시장 내 경제적 존재를 반영하도록 하면서, 한국 내 사업이 미비하거나 없는 기업들에게 불필요한 부담을 부과하는 것을 방지할 수 있습니다.

이러한 배경에서 국내대리인은 규제 당국과의 연락창구로 기능해야 하며, 인공지능사업자의 행위에 대해 법적 책임을 지는 주체가 아님을 명시할 수 있도록 재고해주시길 제언드립니다. 이는

[21] 고영향 AI 사업자 책무 가이드라인 (안), 하위법령(안) 337pg. '위험 식별' 아래 "이용사업자는 개발사업자로부터 제공받은 정보를 바탕으로, 실제 서비스 환경에서 인공지능 시스템이 이용될 때 발생할 수 있는 사람의 생명, 신체의 안전 및 기본권에 대한 위험을 식별하고, 관련 데이터(사고 신고, 불만 사항, 수리 내역 등)를 통해 지속적으로 갱신하기 위해 노력해야 함." 이라 명시하고 있음

[22] 시행령(안) 제 28 조 제 2 항, 하위법령(안) 33p.

"국내 대리인이 법을 위반한 경우에는 해당 국내대리인을 지정한 인공지능사업자가 그 행위를 한 것으로 본다"고 규정한 인공지능 기본법 제 36 조 제 3 항과도 일치합니다. 국내 대리인에게 법적 책임을 직접 부과할 경우, 해당 역할을 수행하는 개인이나 기관에 불합리한 위험을 발생시키며, 자격 있는 기관들이 이 역할을 맡는 것을 기피할 수 있습니다.

제언: 시행령(안) 제 28 조의 국내대리인 지정 요건을 개정하여, 매출 기준이 글로벌 매출이 아니라 한국 이용자로부터 발생한 매출을 기반으로 하도록 하여 국내 시장과의 명확한 연계를 보장해야 합니다. 또한 국내대리인은 인공지능사업자의 행위에 대한 법적 책임을 지는 주체가 아닌 연락 창구로서만 기능한다는 점을 분명히 할 것을 제언드립니다.

'조사권한 운영 방식에 대한 추가 지침 마련

법 제 40 조는 과학기술정보통신부에 특정 조항(제 31 조 제 2 항 및 제 3 항, 제 32 조 제 1 항 및 제 2 항, 제 34 조 제 1 항) 위반 또는 위반이 의심되는 경우 관련 자료를 요청하거나 사실 조사를 수행할 수 있는 권한을 부여합니다. 조사는 신고나 민원 제기로 시작될 수 있으며, 공무원이 인공지능사업자의 사무실에 직접 방문하여 관련 자료를 조사할 수 있습니다. 시행령(안) 제 31 조는 "위반 사항 또는 혐의에 대하여 충분한 자료나 증거가 이미 확보되어 있는 경우"와 "신고나 민원이 민원인의 사적이익을 위하여 제기된 경우나 공무를 방해하기 위하여 제기된 경우 등 목적이 정당하지 않은 것으로 판단되는 경우"에는 조사를 실시하지 않을 수 있다고 규정하고 있습니다.[23]

이러한 권한이 단순히 위반에 대한 "의심"이나 인공지능사업자에 대한 "민원"만으로도 발동될 수 있어 그 범위가 지나치게 광범위하게 적용될 수 있다는 점에 대하여 우려를 표합니다. 실질적인 위반이나 피해의 입증 없이 단순한 의심이나 민원에 근거하여 조사가 이루어질 수 있다는 점은 기업에게 불확실성과 규제 리스크를 부과합니다. 이는 특히 데이터 센터, 연구소, 사무소 등 한국 내 핵심 인프라를 보유한 기업들에게 더욱 큰 부담을 초래할 수 있으며, 해당 인프라와 그 안에 포함된 모든 정보가 단순한 민원만으로 조사 대상이 될 가능성이 있습니다. 결론적으로 이러한 불확실성과 규제 리스크는 한국 시장에 대한 투자 의욕을 크게 위축시킬 우려가 있습니다

또한 시행령(안)은 "부당한 목적"으로 제기된 민원의 경우 조사를 개시할 수 없다고 규정하고 있으나, 판단기준은 불명확합니다. 다른 하위법령의 지침들과 달리, 민원이 적법한지 여부를 판단하기 위한 구체적인 기준, 요건, 절차가 부재한 점은 결과적으로 조사 권한 발동 여부에도 영향을 미치게 될 수 있습니다.

이에 시행령(안)을 통해 법 제 40 조의 조사권한을 발동하기 위한 법적 절차, 기준, 요건을 명확히 규정할 것을 제언드립니다. 또한 민원이 "부당한 목적"으로 제기되었는지 판단하는 방법과 불복 절차가 포함되어야 하며 절차적 공정성과 투명성을 보장해야 합니다. 무엇보다 위반이 발생했다는 합리적인 근거가 존재할 때만 조사를 개시해야 하며, 단순히 민원이 제기되었다는 사실만으로는 권한이 발동되어서는 안 됩니다. 더불어 공무원이 사무소에 출입하여 관련 자료를 열람하는 등의 권한은 반드시 법원이 발부한 영장 등 사법부의 사전 허가를 거쳐 행사되어야 합니다.

[23] 시행령(안) 제 31 조, 하위법령(안) 35p.

제언: 시행령(안) 제 31 조는 법 제 40 조의 조사 권한을 발동하기 위한 법적 절차, 기준, 및 요건을 명확히 규정해야 하며, 민원이 "부당한 목적"으로 제기되었는지에 대한 판단 기준도 구체적으로 명시해주시길 제언드립니다. 또한, 조사는 실제 위반이 발생하였다는 합리적인 근거가 존재할 경우에만 개시되어야 하며, 단순한 민원 제기만으로는 조사 권한이 발동되지 않도록 하는 방안을 고려해주시길 제언드립니다. 특히, 현장 점검 등의 권한은 과학기술정보통신부가 사전에 법원의 허가를 받은 경우에 한해 행사되어야 합니다.

마치며

하위법령(안) 마련을 위한 과기정통부의 노고에 다시 한번 감사드리며, 저희의 정책 제언이 도움이 되었기를 바랍니다. 관련한 논의에 있어 BSA 가 기여할 수 있는 부분이 있다면 기쁘게 참여하도록 하겠습니다. 본 의견서와 관련하여 문의 사항이 있으시거나 추가 필요하신 부분이 있으면 언제든지 연락 부탁드립니다.

감사합니다.

Tham Shen Hong

아태지역 정책 매니저