2025년 3월 21일

한국 인공지능 기본법
BUSINESS SOFTWARE ALLIANCE (BSA) 의견서

과학기술정보통신부 귀하

BSA 비즈니스 소프트웨어연합 (Business Software Alliance, BSA)[1]은 인공지능의 개발 및 신뢰 기반 조성에 관한 법률(이하 인공지능 기본법)과 관련하여 과학기술정보통신부에 의견을 제출할 기회가 주어져 기쁘게 생각합니다. BSA는 각국 정부와 세계시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있는 연합체로 BSA 회원사는 AI 제품 및 서비스 제공 뿐만 아니라 제3자가 AI 시스템 및 애플리케이션 개발에 활용할 수 있는 도구를 제공하는 데 앞장서고 있습니다.

2024년 국가인공지능위원회 출범 시, 대한민국 정부는 2027년까지 한국을 "세계 AI 강국 G3"[2]로 도약시키겠다는 계획을 발표하였습니다.

AI 산업 진흥과 신뢰 구축을 위한 인공지능 기본법의 제정은 이를 위한 중요한 초석이 될 것입니다.

현재 과학기술정보통신부는 현재 인공지능 기본법의 세부 조항 및 의무 사항을 규정하는 시행령을 마련 중인 것으로 알고 있습니다. 이에 인공지능 기본법이 정책 목표를 효과적으로 달성할 수 있도록 시행령을 마련하는 과정에서 아래의 의견을 고려해 주실 것을 제언드립니다.

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

2 "S. Korea vows all-out efforts to become global AI powerhouse", Yonhap News Agency, September 2024, https://en.yna.co.kr/view/AEN20240926002600315.

요약

다음과 같은 내용을 제언드립니다.

1. **"고영향 AI"의 정의 및 범위.** 1) 고영향 인공지능을 정의하는데 있어서 위험 기반 접근 방식을 채택하여 AI 시스템이 배포되는 산업이 아닌, 고위험 AI 시스템의 사용 사례에 초점을 맞춰야 합니다. 2) 중대한 의사결정을 수행하도록 개발된 AI 시스템을 중심으로 고영향 AI로 분류될 수 있는 구체적인 사용 사례를 식별해야 합니다. 3) 범용 AI(General Purpose AI, GPAI) 모델이 기본적으로 고영향 AI로 분류되지 않도록 명확히 규정해야 합니다. 이를 통해, GPAI 모델이 설계되지 않았거나 실질적으로 통제할 수 없는 고영향 시나리오에 대한 의무가 부과되는 상황을 방지할 것을 제언드립니다.

2. **인공지능 개발사업자와 인공지능 이용사업자의 구분.** 인공지능 기본법에서 인공지능 개발사업자와 이용사업자의 역할을 명확히 구분하고, 시행령에서 각 역할에 따른 의무 사항을 구체적으로 규정할 것을 제언드립니다.

3. **사전 인증 요구 사항.** 외부 테스트 및 인증 요구 사항을 부과하는 것을 지양해 주시기를 제언드립니다. 이는 지식재산권, 개인정보 보호, 사이버 보안 측면에서 위험을 초래할 수 있으며, 나아가 한국에서 AI의 개발 및 도입을 상당히 저해할 가능성이 있습니다. 특히, 사전 인증 요구 사항을 부과하는 것은 이러한 부정적인 영향과 예기치 않은 결과를 더욱 심화시킬 가능성이 있습니다. 이에, 내부 테스트 및 자체 인증을 장려하여 산업의 혁신을 지원해 주실 것을 제언드립니다.

4. **라벨링 및 워터마킹 요구 사항.** C2PA (Coalition for Content Provenance and Authenticity)와 같은 새롭게 국제적으로 인정받고 있는 글로벌 표준과의 정합성을 고려해 콘텐츠 인증 요구 사항을 마련해 주시기를 제언드립니다. 또한, 한국 고유의 인증 표준을 새롭게 도입하는 것과 AI 생성 콘텐츠에 대한 가시적 워터마크 적용을 의무화하는 것은 신중하게 재고해 주실 것을 제언드립니다.

5. **누적 연산량 (Computational Threshold).** 인공지능 기본법 제32조(인공지능 안전성 확보의무)의 의무 사항이 적절히 높은 누적 연산량에 다다르는 AI 시스템에만 적용됨을 명확히 규정해 주실 것을 제언드립니다. 또한, 설정된 누적 연상량 기준과 관계없이, 해당 의무는 진정한 고영향 AI 시스템에만 적용되어야 합니다. 아울러, 인공지능 기본법 제32조의 적용에 있어 원칙 기반 접근 방식을 채택하여, 인공지능사업자가 위험 관리 의무를 준수하는 데 있어 유연성을 가질 수 있도록 보장해 주실 것을 제언드립니다. 이를 통해, 실제 피해에 대한 조사가 이루어지는 경우에만 정보 제출을 요구함으로써, 민감한 데이터의 불필요한 노출 및 보안 위험이 발생하는 것을 방지할 수 있도록 고려해 주시기를 제언드립니다.

6. **국내 대리인 지정 요건.** 해외 인공지능사업자가 국내 대리인을 지정하도록 하는 광범위한 요구 사항을 부과하는 것을 지양해 주시기를 제언드립니다. 대신, 해당 요건을 한국에서 실질적으로 운영하는 고영향 인공지능 이용사업자에 한정해야 하며, 규제가 AI 생태계 내 개별 기업의 위험 특성 및 역할과 정합성을 이루도록

해야 합니다.

7. **조사 권한.** 인공지능 기본법 제40조에 따른 조사 권한의 법적 절차 및 요건을 명확히 규정하여, 적법 절차가 준수될 수 있도록 해 주실 것을 제언드립니다. 최소한, 과학기술정보통신부가 명확한 위반 증거를 확보하고 법원의 허가를 받은 경우에만 해당 권한이 행사될 수 있도록 해야 합니다.

고영향 AI의 정의 및 범위

인공지능 기본법은 AI가 고영향 AI로 간주될 수 있는 다양한 분야를 규정하고 있으며, 이에는 에너지 공급, 의료기기 개발 및 사용, 핵물질[3] 관리 등이 포함됩니다.

BSA는 특정 산업에서 사용된다는 이유만으로 AI 활용 사례를 고영향 AI로 분류하는 것에 대해 우려를 표합니다. 고영향 AI를 분류함에 있어서 산업이 아니라 높은 위험을 초래하는 사용 사례에 초점을 맞춘 위험 기반 접근 방식을 고려하는 것이 필요합니다. 이 접근 방식은 AI 시스템이 배포되는 산업이 아니라, 해당 시스템의 적용 방식과 의도된 사용 사례를 기준으로 위험을 평가하는 방식입니다. BSA는 정책 입안자들에게 개인의 자격을 결정하고 이에 따라 주거, 고용, 신용, 교육, 공공장소 접근, 의료 서비스, 보험의 제공 또는 거부를 결정하는 AI 시스템에 초점을 맞추는 정책을 제언해왔습니다. 이러한 접근 방식은 스팸 필터, 피싱 탐지 시스템과 같은 저위험 AI 시스템이 단순히 특정 산업(예: 의료 분야)에서 사용된다는 이유만으로 고영향 AI로 자동 분류되는 문제를 방지할 수 있습니다.

더불어 시행령은 고영향 AI로 간주될 수 있는 구체적이고 명확한 사용 사례를 규정하는 것이 필요합니다. 특히 중대한 의사결정을 수행하도록 개발된 AI 시스템을 중심으로 규정하는 것을 제언드립니다. 명확한 기준을 마련함으로써 기업들이 어떤 경우에 특정 AI 시스템이 고영향으로 간주되는지에 대해 명확히 이해할 수 있고 이를 통해 불확실성과 모호성을 줄일 수 있습니다.

또한 시행령에서 범용 AI (General Purpose AI, GPAI) 모델이 일괄적으로 고영향 AI로 정의되지 않도록 고려해 주실 것을 권장드립니다. 다른 AI 시스템과 마찬가지로, 특정 GPAI 모델이 고영향 AI인지 여부는 해당 모델의 사용 목적에 따라 결정되어야 합니다. 많은 GPAI 모델은 이메일 작성이나 번역과 같이 중대한 의사결정을 수반하지 않는 용도로 사용되므로, 불필요한 규제 부담을 받아서는 안 됩니다. 따라서, GPAI 모델의 분류는 철저히 해당 모델이 고영향 활용 사례를 위해 특별히 설계되고 의도된 경우에 한하여 결정되어야 합니다. 명확한 규정을 통해 GPAI 분야의 혁신을 지속할 수 있고, 실제 위험이 존재하는 분야에 대한 규제 및 감시를 집중할 수 있습니다이러한 명확한 규정이 마련되지 않을 경우, GPAI 시스템 제공업체는 의도하지 않은 고위험 시나리오에 대한 규제 의무(예: AI 기본법 제34조)를 부당하게 적용받을 위험이 있습니다

[3] 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 제2조 제4호

권장사항:

1) AI 시스템이 배포되는 산업이 아니라 고위험 활용 사례에 초점을 맞춘 위험 기반 접근 방식을 채택해야 합니다.
2) 중대한 의사결정을 수행하도록 개발된 AI 시스템을 중심으로 고영향 AI로 간주될 수 있는 구체적인 사용 사례를 식별해야 합니다.
3) GPAI 모델이 일괄적으로 고영향 AI로 분류되지 않음을 명확히 규정해야 합니다. 이를 통해, GPAI 모델이 본래 고영향 시나리오를 해결하도록 설계되지 않았거나 실질적으로 통제할 수 없는 경우에도 의무가 부과되는 상황을 방지할 수 있도록 검토해주시기를 바랍니다.

인공지능 개발사업자와 인공지능 이용사업자의 구분

인공지능 기본법은 인공지능개발사업자와[4] 인공지능이용사업자[5]를 구분하여 정의하지만, 포괄적으로 지칭하는 용어로 인공지능사업자를 도입하고 있습니다. 인공지능 기본법에서 규정하는 준수 의무는 인공지능사업자에게 일괄적으로 적용되며, 인공지능 개발사업자와 이용사업자를 구하지 않고 동일한 책임을 부여하고 있습니다. 예를 들어 제34조에서는 모든 인공지능사업자가 위험 관리, 사람의의 감독 보장, 안전 및 신뢰성 조치를 수행해야 하는 일반적인 책임을 규정하고 있습니다.

이에 대해 AI 생태계 내에서 각 주체가 맡고 있는 역할의 차이를 고려하여, 각 유형의 주체에게 부과될 의무를 명확히 구분해 주실 것을 제언드립니다. AI 시스템은 개발과 배포 과정에서 다양한 주체가 관여하는 복잡한 네트워크를 형성합니다. AI 공급망의 모든 참여자는 자신의 제품이 신뢰성과 안전성을 갖추도록 할 책임이 있지만, 인공지능 개발사업자와 인공지능 이용사업자의 역할 및 책임은 서로 다르게 정의될 필요가 있습니다. 현재, 인공지능 기본법상의 모든 의무가 인공지능 개발사업자와 인공지능 이용사업자에게 일괄적으로 적용되는 상황에서, 각 주체의 역할과 책임이 명확하게 구분되지 않을 경우 상당한 규제적 혼란이 발생할 우려가 있습니다.

따라서 AI 생태계 내 개별 주체의 역할을 기준으로 의무를 부과하고, 시행령을 통해 인공지능 개발사업자와 인공지능 이용사업자에게 각각 부과되는 의무를 명확히 규정해 주실 것을 제언드립니다.

- 인공지능 개발사업자는 AI 시스템을 설계하는 과정에서 해당 AI 시스템을 학습시키는 데 사용된 데이터의 유형, 시스템의 알려진 한계점, 그리고 의도된 사용 사례에 대한 정보를 보유하고 있습니다. 따라서, 인공지능 개발사업자는 AI 시스템의 의도된 목적, 기능, 개발 당시의 알려진 한계점 및 위험 요소, 학습 데이터, 그리고 판매 전 평가 방식에 대한 세부 정보를 제공할 수 있습니다.
- 반면, 인공지능 이용사업자는 AI 시스템을 특정 방식으로 사용하며, 그 결과 소

[4] 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 제2조 7호 가목
[5] 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 제2조 7호 나목

> 비자에게 미치는 영향을 보다 직접적으로 이해하고 있습니다. 따라서, 인공지능 이용사업자는 AI 시스템의 배포 목적, 영향을 받는 개인 또는 최종 사용자와 관련된 투명성 조치(예: 고객의 개인정보 활용 계획에 대한 고지), 배포 후 모니터링, 사용자 보호 조치, 그리고 AI 시스템 배포로 인해 발생할 수 있는 위험을 완화하기 위한 조치에 대한 세부 정보를 제공할 수 있습니다. 또한, 인공지능 이용사업자는 AI 시스템의 사용 중 입력되는 데이터와 그에 따른 출력 결과, 그리고 시스템의 성능에 영향을 미치는 실제 환경적 요인에 대해 더 높은 수준의 이해를 갖고 있습니다..[6]

향후 AI 책임성을 강화하는 정책을 마련할 경우, 인공지능 개발사업자와 인공지능 이용사업자의 역할 차이를 반영하고, 이에 따라 의무를 적절히 배분하는 것이 중요합니다. 또한, 일부 주체는 기존 AI 모델을 자사의 제품 및 서비스에 통합하는 역할을 수행할 수도 있습니다. 따라서 이러한 주체에게 부과되는 의무 또한 AI 시스템을 제품 및 서비스에 통합하는 역할을 고려하여 규정될 필요가 있습니다.

권장 사항: 인공지능 기본법의 준수 의무를 인공지능 개발사업자와 인공지능 이용사업자의 역할을 명확히 구분하고, 시행령에서 각 주체별 적용 의무를 명확히 규정해 주시기를 제언드립니다

사전 인증 요구 사항

인공지능 기본법 제30조 3항에서는 고영향 AI를 제공하려는 인공지능사업자는 "사전에 검증 및 인증을 받도록 노력해야 한다"고 규정합니다.

안전성과 보안을 강화하는 조치를 장려되어야 하는 사안이며, AI 시스템의 안전성, 보안, 정확성, 공정성을 평가하는 철저한 테스트와 검증이 필수적입니다. 이러한 원칙은 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 AI 리스크 관리 프레임워크에서도[7] 우선순위로 두고 있습니다. 그러나 외부 테스트(즉, 제3자 검증)를 통한 인증을 필수로 하는 요구 사항은 지양해야 합니다.

외부 테스트 인증은 기업의 기밀 및 민감한 정보를 제3자와 공유하도록 요구합니다. 이는 기업의 지식재산권 및 기타 민감한 독점 정보 뿐만 아니라, 개인정보 보호 및 사이버 보안과 관련된 위험을 초래할 수 있습니다. 예를 들어, AI 시스템의 개발자가 제3자 감사인과 개인정보를 공유해야 할 경우, 해당 기업은 대량의 개인정보를 감사인에게 이전해야 하는 상황에 놓일 수 있습니다. 이 경우, 감사인이 강력한 개인정보 보호 조치를 구현하지 않는다면 기업이 해당 정보를 보호하기 위해 적용하는 기존의 보호 조치를 약화시킬 수 있습니다.

---

6 예를 들어, 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 제34조 제1항 제2-4호 의무는 인공지능 개발사업자에게 부과하는 것이 가장 적절합니다. 이는 AI 시스템이 제품이나 서비스로 맞춤화 되고 배포되는 방식에 따라 설명 조치, 사람의 감독 및 사용자 보호 조치가 적절히 구현될 수 있도록 보장할 수 있는 주체가 인공지능 개발자이기 때문입니다.

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

마찬가지로 제3자 감사인에게 데이터를 이전하는 과정에서 또는 제3자가 데이터를 보관하는 동안 해당 데이터가 악의적인 사이버 공격에 노출될 가능성이 있습니다. 특히 제3자가 기업과 동일한 수준의 보안 조치를 적용하지 않은 경우, 이러한 위험은 더욱 심화될 수 있습니다. AI 감사를 위한 국제적으로 인정된 표준이 아직 개발 단계에 있어, AI 감사 시스템은 생태계는 아직 충분한 수준으로 구축되지 않았습니다 . 현재 AI 감사 분야는 다른 산업의 감사 기관에 적용되는 강력한 보호 조치를 갖추지 못했을 가능성이 있으며, 전문성과 역량을 갖춘 AI 감사인의 수 또한 제한적입니다.

사전 외부 테스트 및 인증 요구 사항이 AI와 관련된 식별된 위험을 효과적으로 완화하지 못하고, 한국에서 AI의 개발, 도입, 및 활용을 상당히 저해할 수 있다는 점이 우려됩니다. 이러한 요구 사항은 기업에 과도한 부담과 비용을 초래할 뿐 아니라 사회에 실질적인 혜택을 제공하지 못하는 불필요한 규제 체계를 형성할 수 있습니다. 또한, AI 관련 혁신 측면에서 한국이 다른 시장과 비교해 경쟁력을 약화시키는 결과를 초래할 수 있습니다.

나아가, AI 테스트를 위한 기존의기술 표준은 초기 단계에 있는데 오랜 기간 유지되어 온 자발적이고 시장 주도적인 합의 기반의 표준 개발 접근 방식과 일관되게 이루어져야 합니다. AI 시스템의 관리 기준을 평가할 적절한 표준에 대한 업계의 합의는 외부 감사 및 인증 프로세스의 필수 요소이며, 이를 기반으로 표준이 마련되어야 합니다.

반면, 내부 테스트 및 자체 인증은 AI 시스템을 개발하는 팀과 독립된 직원들로 구성된 팀이 수행할 수 있고 이러한 방식은 위에서 언급된 문제를 발생시키지 않으면서도 위험을 효과적으로 식별하고 완화할 수 있습니다. 또한, 외부 인증보다 부담이 적고 유연성이 높아 한국 정부가 추구하는 AI 혁신 정책 목표와도 부합합니다.

권장 사항: 외부 테스트 및 인증 요구 사항을 부과하는 것을 지양해 주시기를 제언드립니다. 이러한 요구 사항은 지식재산권, 개인정보 보호, 사이버 보안 측면에서 위험을 초래할 수 있으며, 나아가 한국의 AI 개발 및 도입을 상당히 저해할 우려가 있습니다. 특히, 사전 인증 요구 사항을 부과하는 것은 이러한 부정적인 영향과 예기치 않은 결과를 더욱 심화시킬 가능성이 있습니다. 이에 따라, 과학기술정보통신부는 내부 테스트 및 자체 인증을 장려하여 AI 혁신을 지원해 주시기를 요청드립니다.

라벨링 및 워터마킹 의무

인공지능 기본법 제31조는 고영향 AI 또는 생성형 AI를 제공하는 인공지능사업자에게 생성형 AI의 출력을 라벨링하고, AI가 생성한 가상 출력물이 현실과 구별하기 어려운 경우 이를 명확하게 표시할 의무를 부과하고 있습니다. 또한, 구체적인 통지 및 라벨링 방법은 시행령에서 정하도록 규정하고 있습니다.

BSA는 AI 생성 콘텐츠의 이력과 출처를 사용자가 식별할 수 있도록 지원하는 신뢰할 수 있는 콘텐츠 인증 및 출처 확인 메커니즘의 개발 및 도입을 지지합니다. 동시에 BSA는

Content Authenticity Initiative (CAI)의[8] 개방형 C2PA 표준을[9] 촉진하기 위한 노력을 지지합니다. C2PA 표준은 올해 국제표준화기구(ISO)의 승인을 앞두고 있으며, 정부를 포함한 누구나 디지털 출처 정보를 제품 및 프로세스에 통합할 수 있도록 개방된 표준입니다. 콘텐츠 제작자는 작업 과정에서 AI가 사용되었는지 여부와 그 사용 방식에 대한 정보를 제공할 수 있으며, 콘텐츠 자격증명을 통해 해당 작업이 어떻게 생성되었는지, 제작 날짜, 그리고 편집 내역 등을 표시할 수 있습니다. 해당 표준은 소비자가 신뢰할 수 있는 콘텐츠를 판단하는 데 도움을 주고, AI 활용의 투명성을 높이는 데 기여할 것입니다. 또한, 워터마킹과 함께 CAI의 접근 방식은 보안성이 높고 변조할 수 없는 출처 정보를 제공합니다. [붙임 1]은 이러한 접근 방식이 실무적으로 어떻게 적용되는지 설명하고 있으니 참고 부탁드립니다.

일본, 호주, 싱가포르, 유럽연합(EU) 등 많은 국가들은 콘텐츠 출처 검증을 위한 국제 표준을 채택 및 검토 중에 있습니다. C2PA와 같은 개방형 표준을 채택하는 것은 국제적 상호운용성을 촉진하고, 디지털 콘텐츠 생태계의 신뢰성과 무결성을 강화하는 데 기여할 것입니다. 을 높일 수 있을 것입니다. 콘텐츠 출처 확인을 위한 기술이 시간이 지나면서 발전할 것입니다. 따라서 어떠한 거버넌스 체계도 이러한 변화를 수용할 수 있도록 설계될 필요가 있다고 생각합니다. 따라서 어떤 인증 및 검증 솔루션이 가장 적절한지 조직별로 평가할 수 있는 유연한 규제 프레임워크를 설계하는 것이 중요합니다.

이러한 맥락에서 한국 고유의 독자적 콘텐츠 인증 표준을 개발하는 것에 대해 신중해야 합니다. 이는 기업이 C2PA와 같은 국제적으로 널리 인정된 표준을 활용하는 능력을 제한할 수 있으며, 다국적 기업에게 추가적인 규제 부담을 초래할 수 있기 때문입니다.

또한, 인공지능 기본법 제31조 제3항은 AI 시스템이 생성한 출력물임을 사용자가 "명확하게 인식할 수 있도록" 표시 또는 워터마크를 부착해야 한다고 규정하고 있습니다. 가시적 워터마크 부착을 의무화하는 것에 대해 우려를 표합니다. 가시적 워터마크는 콘텐츠 감상 및 감상의 질을 저하시켜, 워터마크 의무가 없는 다른 국가의 콘텐츠에 비해 국내 콘텐츠의 경쟁력을 약화시킬 수 있습니다. 또한, 가시적 워터마크는 쉽게 제거될 수 있어, 콘텐츠 인증 메커니즘으로서의 효과를 저해할 수 있으며, 소비자에게 잘못된 보안 인식을 줄 우려가 있습니다. 반면, C2PA기반의 콘텐츠 인증 방식은 콘텐츠의 출처와 변조 여부를 검증할 수 있는 보다 강력한 수단으로서 워터마킹보다 더욱 신뢰할 수 있는 대안을 제공할 수 있습니다.

권장 사항: 콘텐츠 인증 요구 사항이 C2PA와 같이 국제적으로 인정받고 있는 표준과 정합성을 이루도록 해 주시고 다음을 지양해 주실 것을 제언드립니다.

1) 한국만의 독자적인 인증 표준을 도입하는 것을 지양 해주시기를 권장드립니다.

2) AI 생성 콘텐츠에 대한 가시적 워터마크 적용을 의무화하는 것을 지양 해주시기를 권장드립니다.

8 Content Authenticity Initiative, https://contentauthenticity.org/.

9 C2PA Specifications at https://c2pa.org/specifications/specifications/2.1/index.html.

누적 연산량(Computational Threshold)

인공지능 기본법 제32조는 시행령에서 규정하는 누적 연산량 기준을 초과하는 경우, 인공지능사업자가 다양한 안전 및 위험 관리 조치를 구현해야 한다고 규정하고 있습니다.

일부 국가에서는 연산 누적 연산량 기준을 지나치게 낮게 설정하는 문제가 발생하고 있습니다. 예를 들어, EU AI 법은 시스템적 위험을 가진 GPAI의 기준을 10^{25} FLOPS(초당 부동소수점 연산)로 규정하고 있습니다.[10] 하드웨어 성능 향상과 소프트웨어 최적화로 인해 연산 능력은 빠르게 증가할 것으로 예상되는 상황에서 지나치게 낮은 누적 연산량 기준을 설정하면 실질적인 위험을 초래하지 않는 다양한 AI 시스템까지 규제 대상에 포함될 수 있습니다. 이는 개발자들에게 불필요한 규제 부담을 가중시키고, AI 혁신을 저해하는 결과를 초래할 수 있습니다. 신형 AI 모델들은 점점 EU AI 법의 기준에 근접하거나 이를 초과하는 경우가 많습니다. 빠르게 발전하는 기술 환경을 반영하기 위해 더 높은 기준을 설정할 필요성이 커지고 있습니다.

누적연산량 기준 적용 대상이 "진정한 고영향 AI" 시스템에 한정됨을 명확히 규정해 주실 것을 강력히 권장드립니다. 단순히 컴퓨팅 성능이 높다고 해서 AI 시스템이 자동으로 고영향 AI로 분류되어서는 안 되며, AI 시스템이 고영향인지 여부는 해당 시스템의 적용 방식과 사용 목적에 따라 결정되어야 합니다. 예를 들어, 고성능 연산을 수행하는 AI 모델이 기상 예측과 같은 저위험 활동에 사용될 경우, 고영향 AI로 간주될 필요는 없습니다. 반대로, 연산 성능이 낮은 AI 시스템이라도 개인의 대출 승인 여부나 주거 지원 자격을 결정하는 등 중요한 결정을 내리는 경우에는 더 큰 위험을 초래할 수 있으므로 고위험 AI로 간주될 수 있습니다. 따라서, AI 기본법 제32조에서 정하는 규제 의무는 계산 임계값을 초과하는 AI 시스템 중에서도 '실제 고영향 AI'에만 적용되어야 합니다.

또한 32조에 따른 인공지능사업자의 위험 관리 시스템 구축과 관련하여 지나치게 세부적인 요구 사항을 부과하지 않도록 검토해 주실 것을 권장드립니다. 이에 따라, 인공지능사업자가 자율적으로 의무를 이행할 수 있도록 보다 유연한 원칙 기반 접근 방식을 채택해 주실 것을 권장드립니다. 또한, 인공지능사업자는 고영향 AI 시스템이 실제로 피해를 초래한 경우에 한하여, 과학기술정보통신부의 조사가 진행될 때만 위험 관리 시스템에 대한 정보를 제출하도록 규정하는 것이 바람직합니다. 이러한 접근 방식은 기업의 민감한 정보 또는 독점적 사업 정보를 불필요하게 노출하는 위험을 줄이는 동시에, 보안 취약점이 발생할 가능성을 최소화하는 데 기여할 것입니다.

권장 사항: 인공지능 기본법 제32조의 의무 사항이 적절히 높은 누적 연산량 기준을 충족하는 AI 시스템에만 적용됨을 명확히 규정해 주시기를 권장드립니다. 또한, 설정된 누적 연산량 기준과 관계없이, 해당 의무는 진정한 고영향 AI 시스템에만 적용되어야 합니다. 아울러, 과학기술정보통신부는 제32조의 적용에 있어 원칙 기반 접근 방식을 채택하여, 인공지능사업자가 위험 관리 의무를 준수하는 데 있어 보다 유연성을 가질 수 있도록 보장해 주시기를 바랍니다. 이를 통해, 실제 피해에 대한 조사가 이루어지는 경우에만

10 Article 51(2) of the EU AI Act.

정보 제출을 요구함으로써, 민감한 데이터의 불필요한 노출 및 보안 취약점 발생을 방지할 수 있도록 검토해 주시기를 권장드립니다.

국내 대리인 지정 요건

인공지능 기본법 제36조는, 한국 내 사무소 또는 주소지를 두고 있지 않은 해외 인공지능사업자가 시행령에서 규정하는 이용자 수 또는 매출 기준을 충족할 경우, 국내 대리인을 서면으로 지정하고 과학기술정보통신부에 통지하도록 규정하고 있습니다. 그러나 이러한 요건은 해당 해외 인공지능사업자가 개발하거나 배포하는 AI 시스템이 고영향 AI인지 여부와 관계없이 적용되는 것으로 이해하고 있습니다.

위험 기반 접근 방식에 따라, 국내 대리인 지정 의무는 AI 시스템이 초래하는 위험 수준과 인공지능사업자의 역할(인공지능 개발사업자 또는 인공지능 이용사업자)에 따라 결정되어야 합니다. 따라서 해당 의무는 한국에서 고영향 AI를 배포하는 해외 인공지능 이용사업자에 한하여 적용되어야 합니다. 일반적으로 인공지능 이용사업자는 AI 시스템을 사용하는 주체로서 해당 시스템이 어떻게 활용되는지, AI 시스템의 출력 결과, 고객 불만 사항의 특성, 그리고 AI 시스템의 성능에 영향을 미치는 실제 운영 요소들에 대한 정보를 가장 잘 파악하고 있습니다. 즉 인공지능 이용사업자는 AI 시스템이 개인에게 미칠 위험을 이해하는 데 가장 적합한 위치에 있습니다.

현재와 같이 해외 인공지능사업자의 영향력 수준이나 AI 생태계 내 역할과 무관하게 일괄적으로 국내 대리인 지정 의무를 부과하는 것은 과도한 규제 부담을 초래할 수 있습니다. 이러한 접근 방식은 한국 내 AI 혁신과 투자를 저해할 뿐만 아니라, 고영향 AI 시스템을 운영하지 않는 해외 인공지능사업자에게 불합리한 불이익을 초래할 수 있습니다. 따라서, 한국에서 실질적인 운영을 수행하는 고영향 인공지능 이용사업자를 중심으로 보다 정밀한 규제 적용 방안을 마련하는 것이 과학기술정보통신부의 정책 목표에 더욱 부합할 것으로 보입니다.

권장 사항: 해외 인공지능사업자에게 광범위한 국내 대리인 지정 의무를 부과하는 것을 지양할 해주시기를 제언드립니다. 대신 한국에서 실질적인 운영을 하는 고영향 AI 인공지능 이용사업자에 한정하여 해당 요건을 적용함으로써, AI 생태계 내 기업의 역할과 위험 수준에 맞는 규제가 이루어지도록 검토 해주시기를 권장드립니다.

조사 권한

인공지능 기본법 제40조는 과학기술정보통신부에 특정 조항(제31조 제2항 및 제3항, 제32조 제1항 및 제2항, 제34조 제1항) 위반 또는 위반이 의심되는 경우 관련 자료를 요청하거나 사실 조사를 수행할 수 있는 권한을 부여하고 있습니다. 이러한 조사는 신고나 민원 제기로 시작될 수 있으며, 공무원이 인공지능사업자의 사무실에 직접 방문하여 관련 자료를 조사할 수 있습니다.

그러나 이러한 권한의 범위가 지나치게 광범위하게 적용될 수 있다는 점에 대하여 우려

를 표합니다. 특히, 단순한 의혹 제기나 민원 접수만으로도 조사가 개시될 수 있기 때문입니다. 실질적인 위반이 확인되지 않은 상태에서 조사 권한이 행사될 경우, 기업들이 불확실성과 규제 준수 리스크에 직면할 가능성이 큽니다. 이는 특히 데이터 센터, 연구소, 사무실 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. 이러한 규제 불확실성과 리스크는 한국 시장에 대한 투자 의욕을 크게 위축시킬 우려가 있습니다.

이에 시행령에서 제40조의 권한을 발동할 수 있는 법적 절차와 요건을 명확히 규정하고, 적법 절차가 준수되도록 보장할 것을 권장드립니다. 최소한, 조사가 개시되기 위해서는 명확한 법 위반 증거가 존재해야 하며, 과학기술정보통신부가 이를 확인하는 법원의 명령을 사전에 확보하도록 규정해야 합니다. 단순한 신고만으로 인공지능사업자에 대한 조사가 개시되는 것은 지양해야 합니다.

권장 사항: 인공지능 기본법 제40조의 권한 행사와 관련하여, 절차적 공정성과 투명성을 보장할 수 있도록 법적 절차와 요건을 명확히 규정해 주시기를 권장드립니다. 최소한, 해당 권한은 명확한 위반 증거가 확인된 경우에 한하여 행사되어야 하며, 과학기술정보통신부는 법원의 명령을 사전에 확보하도록 규정해 주시기를 권장드립니다.

마치며

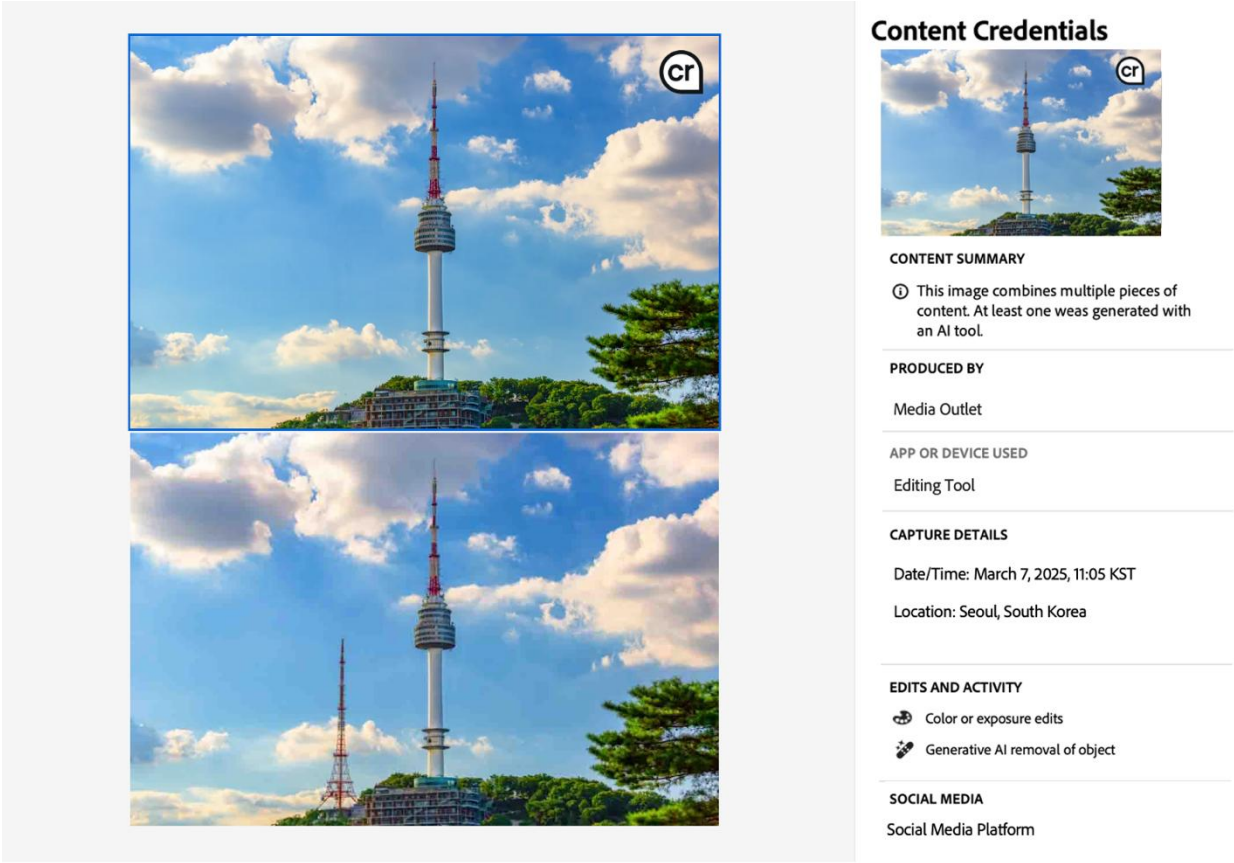
과학기술정보통신부가 시행령을 마련하는 과정에서 본 의견이 정책 논의에 도움이 되기를 바랍니다. 본 의견서와 관련하여 문의 사항이 있으시거나 추가로 도움이 필요하시다면 언제든지 말씀 부탁드립니다

감사합니다.

Tham Shen Hong

아태지역 정책 매니저

[붙임 1]



위 사진은 한 사진작가가 서울타워의 사진을 공유하기 위해 AI 도구를 활용하여 배경에 포함된 작은 타워를 제거한 사례를 보여주는 예시임.

콘텐츠 인증 정보(Content Credentials)를 통해 해당 이미지의 편집 이력이 기록되며, 최종적으로 수정된 버전이 공개될 경우, 사진이 촬영된 장소와 시간, 그리고 편집에 사용된 AI 도구에 대한 정보를 확인할 수 있도록 제공됨.