AI 개발자와 이용사업자: 명확한 구분의 중요성

인공지능(AI)은 모든 경제 분야에서 디지털 혁신을 촉진합니다. 제조업체는 AI를 사용하여 안전하고 지속 가능한 제품을 설계하고, 스타트업들은 AI 기반 번역 프로그램의 도움을 받아 세계 시장에 진출합니다. 보건 연구원은 AI를 사용하여 환자에게 더 나은 치료를 제공하고 새로운 의료 혁신을 주도합니다. 또한 산업 분야를 불문하고, 모든 기업들은 AI 시스템을 통해 장애인을 위한 제품의 접근성을 개선할 수 있습니다. 이렇듯 수많은 분야에서 AI는 복잡한 문제를 해결할 수 있는 새로운 기회를 창출합니다.

AI 제품 및 서비스의 성공은 기술에 대한 대중의 신뢰를 기반으로 합니다. 이러한 신뢰를 얻기 위해 AI를 개발하고 사용하는 조직은 AI 기술이 주는 특수한 기회와 위험성을 함께 고려해야 합니다. 또한 정책결정권자는 책임 있는 혁신을 지원하는 법적 및 정책 환경을 구축함으로써 AI에 대한 대중의 신뢰와 확신을 고양할 수 있습니다. 법적 및 정책 환경을 조성할 시, (1) AI의 고위험 사용과 (2) AI 시스템의 개발자와 이용사업자의 서로 다른 역할과 책임을 인식해야 합니다.

개발자
AI 시스템 설계, 코딩 및 생산

예

AI 시스템을 설계, 코딩 또는 생산하는 회사를 개발자라고 정의하며, 음성 인식을 위한 AI 시스템을 개발하는 소프트웨어 회사를 예로 들 수 있습니다.

이용사업자
AI 시스템 사용

예

AI 시스템을 사용하는 회사를 이용사업자라고 정의하며, 내부에서 또는 제3자가 개발한 AI 시스템을 사용하여 대출을 심사하는 은행을 예로 들 수 있습니다.

한 조직이 개발자와 이용사업자의 역할을 모두 수행할 수 있습니다.

예

특정 사이버 보안 회사가 네트워크 트래픽과 객단가를 모니터링하는 AI 소프트웨어를 개발하고, 그 소프트웨어를 자체 플랫폼에서 사용할 경우, 해당 회사는 개발자이면서 동시에 이용사업자로 정의됩니다.

개발자와 이용사업자의 다른 역할을 인식함으로써 정책결정권자는 AI 시장에서 조직의 역할에 따른 의무를 조정할 수 있습니다. 예를 들어, AI 시스템의 이용사업자는 일반적으로 AI 시스템 개발 회사에서 결정한 설계를 제어할 수 없습니다. 마찬가지로, AI 시스템 개발자는 일반적으로 시스템을 이용하는 회사의 AI 시스템 사용 방식을 제어할 수 없습니다.

예

개발자는 은행이 대출신청을 분류하는 데 도움이 되는 AI 시스템을 설계합니다. 이 AI 시스템의 개발자는 일반적인 응답과 특정 기능이 작동하는 방식을 인식하도록 AI 시스템을 교육하기 위해 사용되는 데이터에 대한 정보를 갖게 됩니다. 그러나 개발자는 대출을 신청하는 소비자와 상호 작용하지 않으며 어떤 대출 신청을 승인할지 선택하지 않습니다. 이에 반해, 은행은 소비자와 상호 작용하여 어떤 신청을 승인하거나 거부할지 결정합니다. 이용사업자로서 은행은 분류 과정의 결과를 사용할 주체이며, 대출 실행의 공정성을 평가할 수 있는 가장 적절한 위치에 있으며, 잠재적 위험을 경감시키기 위한 안전 조치를 이행할 수 있습니다.

개발자와 이용사업자를 구분하는 것이 중요한 이유는 무엇입니까?

개인정보보호법이 소비자의 데이터를 처리하는 다양한 유형의 회사를 구분하는 것처럼, 개발자와 이용사업자를 구분하는 것을 통하여 법적 체계로 AI 생태계에서의 역할에 따라 회사에 의무를 정확하게 할당할 수 있습니다. 결과적으로 기업은 이러한 의무를 더욱 잘 이행하고 소비자를 더욱 안전하게 보호할 수 있습니다. 예를 들어, 개발자는 AI 시스템을 훈련하는 데 사용되는 데이터의 특징을 설명할 수 있지만, 일반적으로 다른 회사가 AI 시스템을 구매하고 시행한 후에는 AI 시스템이 어떻게 사용되는지 이해하지 못할 것입니다. 하지만, 시스템을 사용하는 이용사업자는 일반적으로 AI 시스템이 어떻게 사용되고 있는지, 사용이 의도된 용도와 일치하는지, 감독이 잘 이루어지고 있는지, AI 시스템의 결과물은 어떠한 지, 접수된 불만 사항이 있는지, 그리고 시스템 성능에 영향을 미치는 실제 요인을 이해하는 데 가장 적합한 위치에 있습니다.

AI 시스템을 설계하고 사용하는 회사에 의무를 부과하는 모든 법률은 이러한 다양한 역할을 반영하고 그에 따른 책무를 할당해야 합니다. 이를 통해 실제 다변화된 AI 공급망 내에서 보다 적합한 기업이 리스크를 식별하고 완화할 수 있습니다. 이러한 이유로 전세계의 개인정보보호법은 역할에 따른 책임을 구분하는 것을 가장 중요시하고 있습니다. 예를 들어, 미국, 유럽, 아시아 및 남미의 개인정보보호법은 데이터 처리 방법 및 이유를 결정하는 관리자와, 관리자를 대신하여 지침에 따라 데이터를 취급하는 수탁하는 자의 서로 다른 역할을 구분합니다. 마찬가지로, 다양한 국가의 사이버보안 법률에서도 일반적으로 회사와 보안 서비스를 수탁하는 회사를 구분하고 있습니다.

고위험 AI 시스템의 개발자와 이용사업자는 어떤 의무를 져야 할까요?

기업이 고위험 영역에서 활용되는 AI에 대한 영향평가를 수행하도록 할 필요가 있습니다. 인공지능 영향평가는 기업이 AI로 인한 위험을 식별하고, 문서로 기록하고, 완화하는 데 도움을 주는 중요한 책임 도구입니다. 특히, 불법적인 차별을 초래할 수 있는 잠재적 편견을 감지하고 완화하는 데 유용한 도구입니다.

영향 평가를 관장하는 법률은 영향평가가 고위험 AI 사용에 적용되어야 하며, 개발자와 이용사업자에 대한 의무사항을 명확하게 구분해야 합니다.

개발자
AI 시스템 설계, 코딩 및 생산

고위험 AI 시스템의 설계 평가를 수행하는 개발자는 다음과 같은 정보를 적절히 문서화해야 합니다.

» AI 시스템의 의도된 목적

» AI 시스템의 한계성

» 발생 가능한 높은 수준의 리스크 및 완화 방안

» AI 시스템 교육에 사용된 데이터에 대한 설명

» 시판 전 AI 시스템의 평가 방법 요약

이용사업자
AI 시스템의 사용

고위험 AI 시스템의 영향 평가를 수행하는 이용사업자는 다음과 같은 정보를 적절하게 문서화해야 합니다.

» 이용사업자가 AI 시스템을 사용하려는 목적

» AI 시스템 사용으로 영향을 받는 개인에게 시스템 사용과 관련하여 공지하는 것을 포함한 투명성 조치

» 해당되는 경우 AI 시스템 평가 방법의 요약

» 발생 가능한 높은 수준의 리스크 및 완화 방안

» 해당되는 경우, 배포 후 모니터링 및 사용자 보호 장치