인공지능 법안에 대한 시민사회 의견서

일시 : 2024년 10월 31일
민변 디지털정보위원회, 정보인권연구소, 진보네트워크센터, 참여연대

지난 2024년 7월 1일, 우리는 22대 인공지능법 제정에 대한 시민사회 의견서를 발표한 바 있다. 이 의견서는 국민의힘 정점식 의원이 대표발의한 「인공지능 발전과 신뢰 기반 조성 등에 관한 법률안」(의안번호: 2200543)을 중심으로 인공지능 법안의 주요 쟁점에 대한 비판 및 시민사회의 입장을 표명한 것이다. 그런데 당시 의견서는 제22대 국회에서 논의할 인공지능 법안의 입법 방향을 중심으로 의견을 제시한 것이고, 이후 여러 인공지능 법안이 발의되었기 때문에, 현 국회에 계류 중인 11개 법안의 주요 쟁점 및 조항별로 세부적인 시민사회의 입장을 다시 한번 밝히고자 한다. 본 의견서는 아래 법안들을 대상으로 한다.

인공지능 산업 육성 및 신뢰 확보에 관한 법률안 (안철수 의원 대표발의, 의안번호 2200053)
인공지능 발전과 신뢰 기반 조성 등에 관한 법률안 (정점식 의원 대표발의, 의안번호 2200543)
인공지능산업 육성 및 신뢰 확보에 관한 법률안 (조인철 의원 대표발의, 의안번호 2200673)
인공지능산업 육성 및 신뢰 확보에 관한 법률안 (김성원 의원 대표발의, 의안번호 2200675)
인공지능기술 기본법안 (민형배 의원 대표발의, 의안번호 2201158)
인공지능 개발 및 이용 등에 관한 법률안 (권칠승 의원 대표발의, 의안번호 2201399)
인공지능 기본법안 (한민수 의원 대표발의, 의안번호 2203072)
인공지능책임법안 (황희 의원 대표발의, 의안번호 2203235)
인공지능 발전 진흥과 사회적 책임에 관한 법률안 (배준영 의원 대표발의, 의안번호 2203297)
인공지능의 발전과 안전성 확보 등에 관한 법률안 (이훈기 의원 대표발의, 의안번호 2203960)
인공지능산업 진흥 및 신뢰 확보 등에 관한 특별법안 (김우영 의원 대표발의, 의안번호 2204250)

1. 인공지능 관련 개념 정의

해당 법률의 규제 대상 및 수범 주체를 규정한다는 점에서 정의 조항을 어떻게 규정해야 하는지는 매우 중요하다. 그러나 대부분의 발의안에서 인공지능 및 수범 주체의 범위를 모호하게 규정하고 있다.

(1) 인공지능 정의

정점식 의원안을 비롯하여 대부분의 발의안들이 인공지능을 ""인공지능"이란 학습, 추론, 지각, 판단, 언어의 이해 등 인간이 가진 지적 능력을 전자적 방법으로 구현한 것을 말한다"(제2조 제1호)라고 정의하고 있는데, 인공지능 이전의 소프트웨어 기능 역시 인간의 지적 능력의 일부를 구현하려고 했다는 점에서 이 정의는 지나치게 폭이 넓다. 예를 들어, 번역의 경우, 최근 인공신경망을 통해 성능이 고도화된 번역 서비스가 제공되기 이전에도 전통적인 소프트웨어를 활용한 번역 서비스가 제공되었던 바 있다.

유럽연합 인공지능법, 미국 인공지능 행정명령, 유럽평의회의 인공지능 국제협약 등에서는 OECD의 인공지능 개념을 사용하고 있는데, 국제적인 상호운용성을 고려할 때 우리나라에서도 OECD의 인공지능 개념과 호환가능한 방식으로 규정할 필요가 있다.

(OECD의 인공지능 개념, 2023년 버젼)
An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

AI 시스템은 명시적 또는 암묵적 목표를 위해, 수신된 입력으로부터 물리적 또는 가상 환경에 영향을 줄 수 있는 예측, 콘텐츠, 추천 또는 결정과 같은 출력을 생성하는 방법을 추론하는 기계 기반 시스템이다. AI 시스템마다 배포 후 자율성 및 적응성 수준이 다르다.

(2) 인공지능사업자 및 이용자

대부분의 발의안들이 '인공지능사업자' 및 '이용자' 정의를 두고 있다. 참고로 정점식 의원안의 경우 다음과 같다.

- "인공지능사업자"란 인공지능산업과 관련된 경제활동을 영위하는 자를 말한다. (제2조 제7호)
- "이용자"란 인공지능제품 또는 인공지능서비스를 제공받는 자를 말한다.(제2조 제7호)

안철수, 권칠승, 황희 의원안의 경우에는 인공지능사업자를 인공지능개발사업자와 인공지능이용사업자로 세부적으로 규정하고 있다. (아래는 권칠승 의원안의 경우)

- 가. 인공지능개발사업자: 인공지능의 구현 등 개발과 관련된 경제활동을 영위하는 자
- 나. 인공지능이용사업자: 인공지능을 이용하여 제품 또는 서비스를 제공하는 자

인공지능 제품 및 서비스에는 다양한 주체들이 관여하는데, 위의 정의들이 이러한 주체들을 명확하게 구분하고 있는지 의문이다. 예를 들어, 환자들의 질병 진단을 위한 인공지능의 경우, 이를 개발하는 사업자, 의료 인공지능을 사용하여 환자들을 진단하는 병원, 실제 진단을 받는 환자 등이 관여될 것이다. 이때 병원이 인공지능사업자(좁게는 인공지능이용사업자)인지, 또는 이용자인지 명확하지 않다.

이용자가 누구인지도 명확하지 않다. 번역 서비스와 같이 인공지능 서비스를 이용하는 주체가 최종 소비자인 경우도 있고, 의료 인공지능과 같이 또 다른 사람들에게 '인공지능을 이용하여 서비스를 제공하는 자'일 수도 있다. 만일 공공기관에서 인공지능을 활용하여 복지 서비스 수급 대상자 여부를 결정할 경우, 공공기관이 이용자인가 아니면 인공지능의 결정으로 영향을 받는 사람들이 이용자인가. 수사기관에서 인공지능을 활용하여 용의자를 프로파일링할 경우 그 영향을 받는 사람은 자신이 인공지능의 이용 대상이 되었다는 사실 자체를 인지하지 못할 수도 있다.

이처럼 인공지능 관련 주체들의 개념 구분이 모호할 경우, 책임을 부담하는 주체는 누구인지, 반대로 누구에게 어떠한 권리를 부여해야 하는지 모호해질 수 밖에 없다.

김우영 의원안만이 '인공지능제품 또는 인공지능서비스를 개발하여 제공하는 자'를 '제공자'로, '자신의 업무 또는 서비스 제공을 위하여 인공지능제품 또는 인공지능서비스를 이용하여 인공지능시스템을 운영하는 자'를 '운영자'로 명확하게 구분하여 정의하고 있으며, 이러한 정의 규정에 찬성한다. 다만, 김우영 의원안 역시 이용자를 '인공지능제품 또는 인공지능서비스를 제공받는 자'로 규정하고 있는데, 이 개념은 앞서 언급한 바와 같이 (인공지능제품 또는 서비스를 제공자로부터 제공받는다는 점에서) 운영자 개념과 겹치거나 인공지능 서비스를 직접 이용하지는 않지만 그 결정의 영향을 받는 사람들을 배제할 위험이 있다는 점에서 좀 더 검토가 필요하다.

2. 금지되는 인공지능

권칠승 의원안을 제외하고는 금지되는 인공지능 관련 조항을 포함하고 있지 않다. 유럽연합 AI ACT의 경우, 용인할 수 없는 인공지능을 금지하고 이를 위반하는 경우 전세계 연간 매출액의 최대 7%의 과징금을 부과하고 있다. 여기에는 중국에서 일부 도입하고 있는 사회신용점수 시스템, 미국 업체 Clearview AI가 시행하고 있는 인터넷 스크랩을 통한 얼굴인식 데이터베이스 생성, 일부 국가에서 도입하고 있는 실시간 원격 생체인식 및 예측치안 시스템 등이 포함되어 있다. 우리나라에서 이를 금지하지 않는 것은 거꾸로 이런 비윤리적인 인공지능 시스템도 허용하겠다는 의도인지 의문이다. 아직 인공지능의 발전 단계가 초기이기 때문에 관련 규정을 도입할 필요가 없다는 의견도 있으나, 이러한 인공지능의 개발이 이미 이루어진 이후에 금지하는 것은 해당 기업의 저항에 부딪힐 수 있을 뿐만 아니라, 향후에 금지될 수 있는 인공지능의 개발을 방치하는 것은 오히려 산업발전에 역행하는 것이 될 수 있다.

그나마 권칠승 의원안에서 금지된 인공지능(제21조) 조항을 포함한 것은 다행스러운 일이나, 어떠한 인공지능을 금지할 것인지 여부를 전적으로 시행령에 위임한 것은 적절하지 못하다. 금지된 인공지능의 유형을 법에서 명시하지 않은 반면, 이에 대한 예외는 법에서 규정하고 있고(제21조 제2항), 유럽연합과 달리 예외도 매우 폭넓게 규정하고 있다. 금지된 인공지능 규정 위반에 대한 벌칙 규정도 포함하고 있는 만큼,

금지되는 인공지능의 유형에 대해 법에서 명확히 규정하는 것이 바람직하며, 예외는 포괄적으로 규정하기보다는 (유럽연합 인공지능법과 같이) 금지된 인공지능의 유형마다 필요한 만큼만 규정할 필요가 있다.

3. 고위험 인공지능의 유형

안철수 의원안	정점식 의원안	조인철 의원안	김성원 의원안	민형배 의원안	권칠승 의원안	한민수 의원안	황희 의원안	배준영 의원안	이훈기 의원안	김우영 의원안	추가 제안
「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급		「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급		「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급	「에너지법」에 따른 에너지, 「먹는물관리법」에 따른 먹는 물 공급
「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계		「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	인간의 생명과 관련된 인공지능	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계	「보건의료기본법」에 따른 보건의료의 제공 및 이용체계
「의료기기법」에 따른 의료기기 + 디지털 의료기기	「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기		「의료기기법」에 따른 의료기기		「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기	「의료기기법」에 따른 의료기기 + 장애인 보조기구
원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법		원자력시설 등의 방호 및 방사능 방재 대책법		원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법	원자력시설 등의 방호 및 방사능 방재 대책법

생체정보 처리	범죄수사나 체포업무에 있어 생체정보 처리	범죄수사나 체포업무에 있어 (행정기관보유)생체정보 처리	범죄수사나 체포업무에 있어 (행정기관보유)생체정보 처리	범죄수사나 체포업무에 있어 생체정보 처리		범죄수사나 체포업무에 있어 생체정보 처리	생체인식과 관련된 인공지능	범죄수사나 체포업무에 있어 생체정보 처리	범죄수사나 체포업무에 있어 생체정보 처리	범죄수사나 체포업무에 있어 생체정보 처리	원격으로 생체인식정보를 식별, 분류
채용, 신용등급평가, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가		채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용 등 인사평가 또는 직무 배치의 결정에 이용되는 인공지능 / 응급서비스, 대출 신용평가 등 필수 공공・민간 서비스 관련 인공지능	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가	금융 분야에서 사람의 신용도 평가 또는 신용평점 설정에 사용 / 보험 분야에서 사람의 위험 평가 및 가격 결정에 사용 / 채용 과정에서의 지원자 평가, 승진과 해고의 결정, 인사평가, 직무 배치, 업무 할당의 결정 등에 사용
「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영		「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영		「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	교통, 수도, 가스, 난방, 전기 등 주요 사회기반시설의 관리・운용과 관련된 인공지능	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영	「교통안전법」에 따른 교통수단, 교통시설, 교통체계 작동.운영
공공기관 등이	공공기관 등이	공공기관 등이		공공기관 등이		공공기관 등이		공공기관 등이	공공기관 등이	공공기관 등이	사회보험, 공공부조,

공공서비스 제공에 필요한 자격 확인, 결정 또는 비용징수 등에 사용하는 인공지능으로서 국민에게 영향을 미치는 의사결정을 위하여 사용	공공서비스 제공에 필요한 자격 확인, 결정 또는 비용징수 등에 사용하는 인공지능으로서 국민에게 영향을 미치는 의사결정을 위하여 사용	국민에게 영향을 미치는 의사결정을 위하여 사용		국민에게 영향을 미치는 의사결정을 위하여 사용		국민에게 영향을 미치는 의사결정을 위하여 사용		국민에게 영향을 미치는 의사결정을 위하여 사용	국민에게 영향을 미치는 의사결정을 위하여 사용	국민에게 영향을 미치는 의사결정을 위하여 사용	사회서비스 등 혜택의 수급 자격의 평가, 부여 등에 사용되는 인공지능 /
그밖의 대통령령	그밖의 대통령령	그밖의 대통령령	그밖의 대통령령	그밖의 대통령령		그밖의 대통령령		그밖의 대통령령	그밖의 대통령령	그밖의 대통령령	그밖의 대통령령
							수사 및 기소 등 기본권을 침해할 수 있는 국가기관의 권한 행사에 이용되는 인공지능				범죄예방, 수사, 기소, 형집행 업무에 사용되는 인공지능
							문서의 진위 확인, 위험평가 등 이민, 망명 및 출입국관리와 관련된 인공지능				이민, 망명, 출입국 관리 등 분야에서 법적 지위 부여, 적격성, 위험 평가 등에 사용
					대통령령에 종류 및 유형 모두 위임						

우선 권칠승, 황희 의원안을 제외하고 다른 발의안들은 모두 '고위험영역 인공지능' 개념을 사용하고 있는데, 권칠승, 황희 의원안에서 규정하고 있는 바와 같이 '고위험 인공지능' 개념이 더 적절하다. 왜냐하면, 고위험영역 인공지능이라고 모두 고위험 인공지능인 것은 아니며, 궁극적인 규제 대상은 고위험영역의 인공지능이 아니라 실제 고위험인 인공지능이기 때문이다.

안철수, 정점식, 조인철, 민형배, 한민수, 배준영, 이훈기, 김우영 의원안은 유사하게 고위험영역 인공지능을 규정하고 있다. 대표적으로 정점식 의원안의 경우 다음과 같이 열거하고 있다. (제2조 제3호)

가.「에너지법」 제2조제1호에 따른 에너지,「먹는물관리법」 제3조제1호에 따른 먹는물 등의 공급을 위하여 사용되는 인공지능

나.「보건의료기본법」 제3조제1호에 따른 보건의료의 제공 및 이용체계 등에 사용되는 인공지능

다.「의료기기법」 제2조제1항에 따른 의료기기에 사용되는 인공지능

라.「원자력시설 등의 방호 및 방사능 방재 대책법」 제2조제1항 제1호 및 제2호에 따른 핵물질과 원자력시설의 안전한 관리 및 운영을 위하여 사용되는 인공지능

마. 범죄 수사나 체포 업무에 있어 생체정보(얼굴・지문・홍채 및 손바닥 정맥 등 개인을 식별할 수 있는 신체적・생리적・행동적 특징에 관한 개인정보를 말한다)를 분석・활용하는 데 사용되는 인공지능

바. 채용, 대출 심사 등 개인의 권리・의무 관계에 중대한 영향을 미치는 판단 또는 평가 목적의 인공지능

사.「교통안전법」 제2조제1호부터 제3호까지에 따른 교통수단, 교통시설, 교통체계의 주요한 작동 및 운영에 사용되는 인공지능

아. 국가, 지방자치단체,「공공기관의 운영에 관한 법률」에 따른 공공기관 등(이하 "국가기관등"이라 한다)이 공공서비스 제공에 필요한 자격 확인, 결정 또는 비용징수 등에 사용하는 인공지능으로서 국민에게 영향을 미치는 의사결정을 위하여 사용되는 인공지능

자. 그 밖에 국민의 안전・건강 및 기본권 보호에 중대한 영향을 미치는 인공지능으로서 대통령령으로 정하는 인공지능

그러나 고위험(영역) 인공지능을 이렇게만 규정하는 것은 너무 제한적이다. 고위험(영역) 인공지능 사업자의 경우 그 위험에 비례하는 책임을 부과받아야 하는만큼 가능한 구체적으로 고위험(영역) 인공지능 유형을 법률에 규정할 필요가 있다. 예를 들어, 위의 유형에는 다음과 같은 고위험 분야가 제외되어 있다.

- 안철수, 황희 의원안과 같이 범죄 수사나 체포 업무 외의 영역에서 셍체인식정보를 분석・활용하는 데 사용되는 인공지능

- 황희 의원안에서 규정한 바와 같이, 교통 인프라 외에 수도, 가스, 난방, 전기 등 주요 사회기반시설의 관리・운용과 관련된 인공지능, 수사 및 기소 등 기본권을 침해할 수 있는 국가기관의 권한 행사에 이용되는 인공지능, 문서의 진위 확인, 위험평가 등 이민, 망명 및 출입국관리와 관련된 인공지능

이 외에도 유럽연합 인공지능법 및 미국 행정명령에서 위험성이 높다고 판단하고 있는 분야/유형들이 제외되어 있다.
- 안전검사대상 기계, 안전관리대상 제품, 어린이 제품 등 안전에 큰 영향을 미치는 제품
- 군 또는 정보기관에서 첩보, 방첩, 무기 운용에 사용되는 인공지능
- 사람의 감정인식에 사용되는 인공지능
- 교육 및 직업훈련과 관련한 평가, 기회제공, 자원 할당업무, 부정행위 감시에 사용되는 인공지능
- 정보통신망의 운영에 사용되는 인공지능
- 사법부 또는 행정부에서 판결, 결정, 심판 등의 업무에 사용되는 인공지능
- 선거 및 투표행위, 투표결과에 영향을 미치기 위하여 사용되는 인공지능

위의 분야 역시 고위험영역에 해당하지 않는지, 아니라면 그 근거는 무엇인지 꼼꼼하게 따져볼 필요가 있다. 권칠승 의원안의 경우에는 고위험 인공지능의 종류 및 유형을 모두 시행령에 위임하고 있는데, 고위험 인공지능 사업자에게 상당한 책임을 부여해야 하는만큼 법에서 규율하는 것이 적절하다.

4. 고위험(영역) 인공지능 사업자의 책무 및 벌칙 규정

(1) 발의안의 신뢰성 확보조치 의무 규정의 문제점

안철수, 정점식, 조인철, 민형배, 한민수, 배준영, 이훈기, 김우영 의원안의 경우 '고위험영역 인공지능과 관련한 사업자'의 신뢰성 확보조치를 유사하게 규정하고 있다. 대표적으로 정점식 의원안은 다음과 같은 신뢰성 확보조치 의무를 부여하고 있다. (제28조)

1. 위험관리방안의 수립・운영
2. 신뢰성 확보를 위한 조치의 내용을 확인할 수 있는 문서의 작성과 보관
3. 기술적으로 가능한 범위 내에서의 인공지능이 도출한 최종결과, 인공지능의 최종결과 도출에 활용된 주요 기준, 인공지능의 개발・활용에 사용된 학습용데이터의 개요 등에 대한 설명 방안의 수립・시행
4. 이용자 보호 방안의 수립・운영
5. 고위험영역 인공지능에 대한 사람의 관리・감독
6. 그 밖에 고위험영역 인공지능의 신뢰성과 안전성 확보를 위해 위원회에서 심의·의결된 사항

우선 이 조항은 사업자에 대한 의무 형식으로 규정되어 있지만, 의무의 구체적인 내용도 빈약하고 처벌 규정도 없어 사실상 거의 아무런 실효성이 없는 것으로 보인다. 또한, 이것이 인공지능을 개발하는 사업자의 의무인지, 제3자가 개발한 인공지능을 이용하여 서비스를 제공하는 사업자의 의무인지도 모호하다.

또한 최종결과, 주요기준, 학습데이터개요 등을 설명하도록 하고 있으면서도 '기술적으로 가능한 범위'로 한정하고 있다. 그럼, 설명가능하지 않은 인공지능을 중요한 의사결정에 사용할 경우 누구에게 어떻게 책임을 물을 것인가. 이용자 개념이 모호한만큼 '이용자 보호 방안'이 무엇을 의미하는지도 모호하다. 유럽연합 인공지능법은 인공지능 제공자(provider)로 하여금 배치자(deployer)에게 해당 인공지능에 대한 상세한 설명을 제공하도록 하고 있는데, 이처럼 인공지능을 이용하여 서비스를 제공하는 배치자를 보호하기 위한 조항인 것인지, 아니면 인공지능의 영향을 받는 사람들(그런데 이들은 인공지능의 직접적인 이용자는 아니다)을 보호하기 위한 방안을 의미하는 것인지 모호하다.

(2) 추가적으로 규정해야 할 의무 규정

고위험 인공지능 사업자에게 여러 의무를 부과하는 것은 인공지능의 위험성을 식별, 완화하고 이용 과정에서 위험을 통제하며, 문제가 발생할 경우 그 책임을 지우고, 인공지능의 영향을 받는 사람들의 권리를 보호하기 위한 것이다. 그런데 위의 신뢰성 확보조치에는 이를 위한 여러 의무들이 빠져있다. 고위험 인공지능의 신뢰성 확보를 위해 다음과 같은 추가적인 의무를 포함할 필요가 있다.

인공지능을 개발하고 해당 제품을 제공하는 사업자의 경우, 다음과 같은 추가적 의무가 있을 수 있다.
- 기술 문서 및 로그기록 등 사후에 문제를 추적할 수 있는 문서의 작성 의무
- 인공지능 훈련에 사용되는 데이터의 적정성에 대한 평가 의무
- 인공지능을 운영하는 자에 대한 적절한 정보제공 의무
- 사이버보안 등 안전성 확보를 위한 조치 의무
- 장애인접근성 보장 의무

인공지능을 자신의 업무나 서비스 제공을 위해 이용하는 사업자의 경우, 다음과 같은 의무가 있을 수 있다.
- 개발자가 제공한 설명서에 따라 해당 인공지능을 사용할 의무
- 지속적인 모니터링 의무
- 입력 데이터를 사용할 경우 입력 데이터를 적절하게 관리할 의무
- 사고발생시 관련 이해관계자(개발자 및 감독기관 등)에게 통지할 의무
- 인공지능의 결정 대상이 되거나 영향을 받는 사람들에게 고지하거나 설명할 의무

그나마 황희 의원안에서 개발사업자의 의무와 이용사업자의 의무를 구분하여 규정하고 있어 바람직하다. 황희 의원안은 개발사업자에게 다음과 같은 의무(제19조 제1항) 및 알고리즘의 동작원리를 알릴 의무(제2항)를 부과하고 있다.

1. 고위험 인공지능 개발과 관련하여 국민의 생명이나 신체적 안전에 중대한 위험성이 있는지에 대한 위험 평가
2. 고위험 인공지능 개발 단계별 문서의 전자화
3. 고위험 인공지능의 개발 결과의 추적을 위한 기록
4. 고위험 인공지능의 이용자에 대한 정보 제공
5. 사람에 의한 고위험 인공지능의 관리・감독
6. 고위험 인공지능 개발 과정에서의 사이버 보안 강화

이용사업자에게는 지속적인 모니터링 의무, 이용자에게 고위험 인공지능을 이용한 서비스가 제공되고 있음을 고지할 의무, 중대한 위험성에 대해 설명할 의무 등을 부여하고 있다. 다만, 여기서 이용자가 인공지능 서비스를 직접 이용하는 사람이 아니라, 인공지능의 영향을 받는 모든 사람을 포괄하는 것인지 의문이다.

이훈기 의원안에서 인공지능 영향평가 조항을 포함한 것은 환영한다. 그러나 단지 영향평가를 위해 노력할 의무만을 부여할 뿐이고, 구체적인 내용 및 방법은 시행령에 위임한 것은 아쉬운 부분이다. 국가인권위원회가 권고한 바와 같이 최소한 고위험 인공지능을 이용하는 사업자에게는 인공지능 (인권)영향평가를 의무화할 필요가 있다.

(3) 처벌 규정

대부분의 발의안에서 벌칙 적용의 공무원 의제 조항 및 직무상 비밀누설에 대한 처벌 조항만을 포함하고 있다. 그 외에는 배준영, 이훈기 의원안에서 인공지능정책센터 명칭 사용 위반에 대한 벌칙을, 권칠승 의원안에서 금지된 인공지능 위반에 대한 벌칙을 포함하고 있을 뿐이다. 무엇보다 고위험 인공지능 사업자의 책무 규정 위반에 대한 벌칙 규정을 두고 있지 않기 때문에, 이 법안의 실효성이 의심된다. 벌칙 조항이 없다면 사업자들은 신뢰성 있는 인공지능을 위한 자신의 책무를 이행할 아무런 부담도 느끼지 못할 것이다. 그나마 조인철, 한민수, 김우영 의원안에서 과기정통부장관으로 하여금 사업자에게 책무의 준수를 권고할 수 있도록 한 것은 긍정적이지만, 처벌 규정이 없는 권고는 한계가 있을 수 밖에 없다.

벌칙 규정을 두기에 사업자에 대한 책무 조항의 구체성이 떨어지는 것이 문제일 수 있는데, 이는 시민사회가 비판하는 지점이기도 하다. 즉, 처벌 규정은 고위험 인공지능 사업자의 의무를 보다 구체적으로 규정하는 것과 병행되어야 한다. 필요하다면 보다 현실적이고 구체적인 책무 규정을 도입하기 위해 좀 더 사회적인 논의를 할 필요가 있다. 고위험 인공지능 규율에 별다른 실효성도 없는 법안을 서둘러 만들 필요는 없지 않은가. 과학기술정보통신부는 처벌 규정을 두기 위해서는 사회적 합의가 필요하다는 하나마나한 얘기만 하고 있다. 다른 규정은 사회적 합의가 필요없는가? 인공지능법은 고위험 인공지능의 위험으로부터 사람들의 안전과 인권을 보호하고, 이를 위해 사업자에게 책임을 부과하는데 있어서 어떻게 실효성을 가질 수 있는지 설명할 수 있어야 한다.

5. 기본원칙

안철수 의원안	정점식 의원안	조인철 의원안	김성원 의원안	민형배 의원안	권칠승 의원안	한민수 의원안	황희 의원안	배준영 의원안	이훈기 의원안	김우영 의원안
안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상	인간의존엄과 가치, 인류의 공동이익	안전성과 신뢰성, 국민의 삶 향상	인류의 발전과 편의	안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상	안전성과 신뢰성, 국민의 삶 향상
창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경		창의정신의 존중, 안전한 이용환경		창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경	창의정신의 존중, 안전한 이용환경
	인공지능・인공지능기술에 따른 변화에의 적응	인공지능・인공지능기술에 따른 변화에의 적응	인공지능・인공지능기술에 따른 변화에의 적응	인공지능・인공지능기술에 따른 변화에의 적응		인공지능・인공지능기술에 따른 변화에의 적응		인공지능・인공지능기술에 따른 변화에의 적응	인공지능・인공지능기술에 따른 변화에의 적응	인공지능・인공지능기술에 따른 변화에의 적응
개발・이용에서의 차별 금지					개발・이용에서의 차별 금지		개발・이용에서의 차별 금지			
개인의 자기정보결정권 보장, 신뢰성・투명성					투명성, 위험관리		개인의 자기정보결정권 보장, 신뢰성・투명성			

대부분의 발의안이 1) 안전성과 신뢰성, 국민의 삶 향상, 2) 창의정신의 존중, 안전한 이용환경 조성, 3) 변화에 적응할 수 있는 시책 강구 등의 원칙을 규정하고 있고, 안철수, 권칠승, 황희 의원안만이 차별금지 원칙 및 투명성 원칙을 규정하고 있다. 현재 인공지능과 관련하여 가장 큰 위협의 하나로 거론되고 있는 것이 인공지능의 차별적 결정의 문제와 불투명성(또는 인공지능의 결정에 대한 설명 불가능성) 문제인데, 이러한 위험 해결의 지향을 원칙에 담지 않는 것은 문제이다. 안철수, 권칠승, 황희 의원안을 수렴하여, 차별금지 및 기본권 보호, 투명성 및 설명가능성 보장을 원칙으로 포함해야 한다.

6. 범용 인공지능 (생성형 인공지능)

안철수 의원안	정점식 의원안	조인철 의원안	김성원 의원안	민형배 의원안	권칠승 의원안	한민수 의원안	황희 의원안	배준영 의원안	이훈기 의원안	김우영 의원안
생성형 인공지능 고지 및 표시	생성형 인공지능 고지 및 표시			생성형 인공지능 고지 및 표시		생성형 인공지능 고지 및 표시		생성형 인공지능 고지 및 표시	생성형 인공지능 고지 및 표시	
	생성형 인공지능 안전 확보 의무									고위험 범용 기초모형과 관련한 사업자의 책무

대부분의 인공지능이 범용 인공지능(General Purpose AI)이 아니라 '생성형 인공지능'에 대해 규정하고 있는데, 이는 매우 제한적인 규정이다. 챗GPT 등 범용 인공지능 모델의 실제 활용 분야가 생성형 인공지능 서비스이기는 하지만, '생성형 인공지능' 개념은 텍스트, 이미지, 영상 등의 '생성'에 초점을 둔 규정이다. 범용 인공지능 모델은 생성형 인공지능이 아닌 다른 예측 및 의사결정 분야에서 활용될 가능성이 크기 때문에, 생성형 인공지능이 아닌 '범용 인공지능' 개념을 사용하고 범용 인공지능 모델 개발자나 범용 인공지능 사업자에 대한 의무 규정을 두는 것이 바람직하다. 유럽연합 인공지능법 및 미국 인공지능 행정명령 역시 위험이 큰 범용 인공지능(또는 파운데이션 모델)에 대해서 적대적 테스트와 국가적 관리를 의무화하고 있다. 그나마 대부분의 안들이 생성형 인공지능의 고지 및 표시 의무만을 규정하고 있고, 정점식 의원안이 '안전확보 의무'를 규정하고 있다. 다만, '범용 인공지능'으로 확대 적용할 필요가 있다.

범용 인공지능 모델(범용 기초모형)의 개념을 규정하고 있는 것은 김우영 의원안 뿐이다. 그런데 김우영 의원안은 '고위험 범용 기초모형과 관련한 사업자'에게 '학습 데이터에 대한 정보와 안전평가 실시 결과 및 사이버 보안 조치내역을 보고'할 의무만을 규정하고 있을 뿐이며, 다른 의원안과 같이 생성형으로 활용될 경우의 투명성 의무에 대해서는 규정하지 않고 있다.

생성형 인공지능으로 사용될 경우의 투명성 의무와 함께, 사회적 위험성이 큰 (특정 기준 이상의) 범용 인공지능 사업자에 대한 안전 확보 의무를 모두 규정할 필요가 있다. 특히, 학습 데이터의 경우 저작권 및 개인정보 침해 논란이 제기되고 있는 바, 이러한 문제를 사업자들이

어떻게 해결하고 있는지 학습에 사용된 데이터의 개요와 함께 공개하도록 할 필요가 있다. 그렇지 않다면, 저작권 및 개인정보 침해에 대해 잠재적인 피해자들이 대응할 수 없게 될 것이기 때문이다.

7. 인공지능 사업자에 대한 검인증

황희 의원안을 제외한 대부분의 발의안이 민간에서 자율적으로 검증, 인증 활동을 하고, 정부(과학기술정보통신부)는 이를 지원하는 역할로 제한하고 있다. 검인증은 사업자들이 자신이 법을 준수하고 있다는 것을 입증할 수 있는 방법이다. 발의안에서 자율적인 검인증으로 제한하고 있는 것은 그만큼 법에서 고위험 인공지능 관련 사업자들의 책무를 모호하게 규정하고 있는 것과 연결된다.

검인증이 의미가 있기 위해서는 우선 법령에서 고위험 인공지능 사업자의 책무를 구체적이고 명확하게 규정할 필요가 있다. 둘째는 이러한 규제 준수를 평가할 수 있는 역량이 있는 검인증 기관을 감독당국이 지정해야 한다. 셋째, 검인증 기관이 검인증 활동을 제대로 수행하는지 지속적으로 모니터링 해야 한다. 이러한 시스템은 새로운 것이 아니며, 이미 정보 보안이나 개인정보 보호 분야 등에서 인증 체계가 마련되어 있다.

8. 영향을 받는 사람들의 권리 및 구제

기존 발의안들의 가장 큰 문제 중 하나는 인공지능의 영향을 받는 사람들의 권리에 대해 무관심하다는 것에 있다. 단지 황희 의원안(제21조)만이 고위험 인공지능 이용자의 권리를 규정하고 있다.

- 고위험 인공지능을 이용한 제품 또는 서비스에 대한 설명요구권
- 고위험 인공지능을 이용한 제품 또는 서비스에 대한 이의제기권 또는 거부권
- 고위험 인공지능 여부 및 이용자의 권리에 대해 고지받을 권리 (이용자에게 고지할 사업자의 책무)
- 관련 자료에 대한 요청권, 사업자가 거부할 경우 자료 제공을 명령해줄 것을 청구할 권리

물론 황희 의원안 역시 '이용자의 권리'로 규정하고 있어, 해당 인공지능 서비스를 직접 이용하지는 않지만 그 결정의 영향을 받는 사람들의 권리에까지 이 규정이 적용되는지는 명확하지 않다. 예를 들어, 자신의 의사와 무관하게 사회복지 서비스를 받을 권한이 있는지 인공지능의 판단 대상이 된 사람은 이용자인가 아닌가. 또한 인공지능으로부터 피해를 입은 사람은 자신의 피해에 대해 관할 당국에 진정할 수 있는 권리를 가져야 한다.

2020. 3. 유엔 사무총장(A/HRC/43/29)은 인공지능 사용에 대한 책임성을 완전하게 보장하는 법률체계와 절차 방법을 마련하고, 감독 체제를 수립하며, 인공지능의 피해에 대한 구제 수단을 구비할 것을 권고한 바 있다. 우리나라 국가인권위원회도 인공지능 개발·활용 과정에서 이용자와 정보주체가 보장받아야 할 권리를 명시하고 피해 발생에 대한 구제 절차를 마련할 것을 요구하였다. 유럽연합 AI ACT의 경우, '구제'(제4절) 절을 별도로 두고, 이 법 위반 사항에 대하여 시장감독기관에 진정하여 처리하도록 하고(제85조), 고위험 인공지능의 의사결정으로 영향을 받은 사람이 설명을 받을 권리(제86조) 등을 보장받도록 규정하였다. 미국 AI 행정명령에 따라 마련된 OMB 규칙의 경우, 연방정부 조달 AI에 대하여 인적검토와 구제절차를 보장하였다. 영향을 받은 개인이 자신에게 미친 인공지능의 부정적인 영향에 대하여 항고하거나 이의를 제기할 수 있고, 가능한한 거부(opt-out)권도 행사할 수 있도록 하였다.
이러한 점을 고려하여 인공지능법인 그 영향을 받는 사람들의 권리를 반드시 포함해야 한다.

9. 인공지능 국가거버넌스

안철수 의원안	정점식 의원안	조인철 의원안	김성원 의원안	민형배 의원안	권칠승 의원안	한민수 의원안	황희 의원안	배준영 의원안	이훈기 의원안	김우영 의원안
대통령 소속	대통령 소속	대통령 소속	국무총리소속	국무총리소속	국무총리소속	국무총리소속		국무총리소속	대통령 소속	대통령 소속
국가인공지능위원회	국가인공지능위원회	국가인공지능위원회	인공지능위원회	국가인공지능위원회	국가인공지능위원회	인공지능위원회		인공지능위원회	인공지능위원회	인공지능위원회
주무부처 : 과학기술정보통신부										
국가인공지능	국가인공지능		국가인공지능	국가인공지능	국가인공지능	국가인공지능				국가인공지능

센터	센터		센터	센터	센터	센터				센터
인공지능안전연구소	인공지능안전연구소									
한국인공지능진흥협회		대한인공지능진흥협회	대한인공지능진흥협회							
민간자율인공지능위원회	민간자율인공지능위원회	민간자율인공지능위원회		민간자율인공지능위원회		민간자율인공지능위원회		민간자율인공지능위원회	민간자율인공지능위원회	민간자율인공지능위원회
							인공지능분쟁조정위원회			

지난 시민사회 의견서에서 지적한 바와 같이 인공지능법을 집행하고 그 준수를 감독하며 피해를 구제하기 위한 관할 당국은 독립적인 기관이어야 한다. 그러나 모든 발의안이 이 법안의 주무부처로 과학기술정보통신부를 전제로 하고 있다. 비록 상위에 대통령 또는 국무총리 산하 심의의결 기구가 있더라도 실질적인 역할은 과기정통부가 담당할 것이다. 문제는 지금까지 과기정통부가 인공지능 산업육성에 치우쳐있으며, 안전과 인권 보호에는 전문성과 관심을 보이고 있지 않다는 점이다.

안철수, 정점식 의원안은 인공지능안전연구소 규정을 포함하고 있는데, 시민사회 역시 안전연구소의 설립에는 찬성한다. 그러나 안철수, 조인철, 김성원 의원안이 규정하고 있는 '인공지능진흥협회' 및 여러 의원안에 포함된 '민간자율인공지능위원회'는 사업자 중심의 로비 단체가 될 위험성이 크다. 사업자 단체 자율적으로 이를 설립하는 것을 막을 수는 없겠지만, 굳이 법에 규정하고 이에 대한 지원 근거를 마련할 필요가 있을지 의문이다. 오히려 예산을 통해 지원을 해야 한다면, 인공지능에 의해 부정적인 영향을 받는 사람들(사실상 대부분의 국민들)이 인공지능과 자신의 권리에 대해 인식할 수 있도록 돕는 리터러시 사업을 지원해야 할 것이다.

10. 기타 의견

(1) 실증 규제특례 조항 폐지

조인철 의원안 제14조에서 인공지능 실증 규제특례 규정을 두고 있는데, 이미 「정보통신융합법」에 정보통신기술에 대한 실증 규제특례를 규정하고 있는 상황에서 중복적으로 규정할 필요가 있을지 의문이다.

(2) 우선허용, 사후규제 조항 폐지

김성원 의원안 제11조, 김우영 의원안 제14조는 여전히 우선허용, 사후규제 조항을 포함하고 있는데, 이는 이미 21대 국회에서 시민사회의 문제제기로 삭제된 조항으로 이를 포함하는 것에 대해서 적극 반대한다.

(3) 인공지능제품의 비상정지 기능

조인철 의원안 제28조는 인공지능제품의 비상정지 규정을 포함하고 있는데, 이러한 규정의 필요성에 대해서는 공감하며, 다만 비상정지 기능이 필요한 것은 고위험 인공지능일 것인 바, 고위험 인공지능 사업자에 대한 의무의 하나로 규정할 필요가 있다.

11. 결론

과학기술정보통신부는 아직 인공지능 도입 초기이기 때문에 규제를 최소화해야 한다고 주장한다. 그러나 이미 자율주행차가 운행을 시작한 가운데 산업 현장과 돌봄 가정에 인공지능의 도입이 빠른 속도로 증가하고 있으며, 그로 인한 위험이 현실화되고 있다. 2023년 12월 KB 국민은행은 인공지능 상담 서비스를 도입한 뒤 상담원 240명을 한꺼번에 해고하여 사회적으로 큰 충격을 주었고, 금융 업종을 비롯한 콜센터 노동자의 인력 감축이 빠른 속도로 확산되고 있다. 2023년 11월에는 산업로봇이 사람을 박스로 잘못 인식하여 노동자가 압착사망하는 사고가 발생하였고, 인공지능 산업로봇으로 인한 사고가 국내외에서 점점더 많이 발생하고 있다. 대통령이 공무원에게 챗GPT 사용을 지시한 이후로 각급 공공기관이 앞다투어 생성형 인공지능을 도입하기 시작한 것은 물론 사회복지 돌봄, 검찰과 경찰 등 갈수록 더 많은 공공영역에서 인공지능을 도입하고 있다. 그러나 인공지능으로 인한 안전, 인권, 차별 위험은 제대로 다루어지고 있지 않으며, 인공지능을 제공하거나 운영하는 기업 또는 기관이 갖추어야 할 책무는 어디에도 명확히 규정되어 있지 않은 현실이다.

전반적으로 대부분의 발의안들은 인공지능 산업 육성에 치우져있다. 그러나 인공지능을 포함한 신기술의 육성을 위한 근거는 이미 기존 지능정보화기본법에 마련되어 있다. 과기정통부는 이미 2025년 AI 및 디지털 혁신 예산으로 9000억원에 달하는 예산을 편성했으며, 지난 9월 26일 국가인공지능위원회가 출범하였으며, 11월 중 인공지능 안전연구소도 출범할 예정이라고 한다.

그러나 문제는 이미 지금도 사람들의 안전과 인권을 위협하는 인공지능이 아무런 규제없이 도입되고 있다는 점이다. 인공지능의 불투명성 때문에 드러나지 않은 피해를 어떻게 파악할 것인지, 피해자의 권리는 어떻게 구제할 것인지, 자료를 보관할 아무런 의무 규정도 없이 사고가 났을 때 원인은 어떻게 규명하고 누구에게 책임을 물을 것인지 당장 최소한의 대책을 마련해야 한다. 시민사회의 요구는 불필요한 규제를 도입하라는 것이 아니라, 지금 도입되고 있는 인공지능에 의해 발생할 수 있는 위험을 완화하고 적절한 책임을 부과하며, 피해를 구제하는데 필요한 대책을 내놓으라는 것이다. 인공지능 법안은 이를 위한 대책을 마련하는 것이 핵심이 되어야 하며, 과기정통부를 포함한 정부와 국회는 이러한 요구에 응답할 수 있어야 한다.