AI법 과방위 통과안에 대한 시민사회 의견서

2024년 12월 3일

민변 디지털정보위원회, 정보인권연구소, 진보네트워크센터, 참여연대

지난 2024년 11월 26일 국회 과학기술정보방송통신위원회(이하 과방위)는 전체회의를 열고 <인공지능 발전과 신뢰 기반 조성 등에 관한 기본법안>(AI 기본법안)을 통과시켰다. 이 법안은 과방위에 발의된 19개 발의안을 병합한 것인데, 전반적으로 AI의 위험성을 실효성있게 규율하기에는 매우 미흡하다. 이에 과방위를 통과한 AI 기본법안의 문제점이 무엇인지 시민사회의 의견을 제시하고자 한다.

우리는 시민사회가 지적한 문제점이 법제사법위원회에서의 검토 과정에서 개선될 수 있기를 바란다. 여러 가지 문제가 있지만, 특히 아래와 같은 핵심적인 문제점은 반드시 이후 논의 절차에서 수정이 필요하다.

첫째, AI 기본법안은 사회적으로 용납할 수 없을 정도로 비윤리적인 AI의 개발과 활용을 금지하는 규정을 두어야 한다.
둘째, 국방 또는 국가안보 목적의 인공지능에 대한 포괄적 적용 배제 조항을 삭제해야 한다.
셋째, 고영향 AI 사업자의 책무 위반에 대해 실효성있는 제재 규정을 마련해야 한다.

주요 쟁점별 문제점은 아래와 같다.

1. 금지된 인공지능 규정 부재

결국 AI 기본법안은 과학기술정보통신부(이하 과기정통부)와 산업계의 반대를 수용하여 금지된 인공지능 규정을 배제하였다. 이는 지금까지 AI 윤리를 내세웠던 과기정통부와 산업계가 얼마나 기만적인지 보여준다. 그들이 AI 윤리를 강조했던 것은 법적 규제를 회피하기 위한 명분에 불과했을 뿐이다. 공공장소에서의 실시간 얼굴인식 시스템, 중국의 사회신용시스템, 인권침해 논란에도 미국에서 서비스를 하고 있는 클리어뷰와 같은 얼굴인식 시스템, 자율적인 AI 살상무기 등과 같은 비윤리적인 AI의 개발과 도입을 허용하겠다는 것인가. 그것이 아니라면 금지된 인공지능에 대한 최소한의 규정이라도 AI 기본법안에 포함할 것을 촉구한다.

2. 국방, 국가안보 목적의 AI 적용 배제

AI 기본법안은 “국방 또는 국가안보 목적으로만 개발・이용되는 인공지능으로서 대통령령으로 정하는 인공지능”에는 이 법의 적용을 배제하고 있다. 이는 국방부와 국가정보원의 요구가 반영된 것으로 보인다.

그러나 국방 또는 국가안보 목적의 AI라는 이유로 AI의 안전성, 신뢰성을 위한 기본적인 원칙과 사업자의 책무를 적용하지 않는 것은 매우 위험하다. AI 윤리원칙이나 AI의 안전성, 신뢰성을 담보하기 위한 여러 조치들에 구애받지 않고, 자율적인 AI 살상 무기나 정보수집을 명분으로 한 시민감시 AI를 만들겠다는 것인가? 만일 국방이나 국가안보 목적의 AI의 개발 및 활용을 위해 필요한 규정이 있다면, 특별법에서 규정하면 된다. AI 기본법안은 특정 분야에 대해 별도의 법률을 통해 규정하는 것을 막지 않기 때문이다.

지금까지 국방 또는 국가안보라는 목적으로 얼마나 많은 권한 남용과 인권 침해가 있었는지 기억해 보라. 특히, 국가정보원에 대한 민주적 통제는 여전히 요원한 상황이며, 오히려 정부여당과 국정원은 수사권 복원을 통해 과거의 권력을 되찾기 위해 혈안이 되고 있다. 법사위 심사 과정에서 국방 또는 국가안보 목적의 AI에 대한 적용 배제 조항을 반드시 삭제해야 한다. 오히려 국방 또는 국가안보 목적의 AI는 기본적으로 그 오남용에 대한 적절한 규제가 필요하기 때문에 고영향 인공지능으로서 정의될 필요가 있다.

3. 개인정보보호법과의 관계 명확화

인공지능 개발과 이용에 있어 데이터에 포함된 개인정보 처리 문제는 세계적으로 중요한 쟁점이다. 우리는 AI 기본법안이 인공지능 산업 육성을 명분으로 개인정보 규제를 완화하는 수단으로 사용되지 않을지 우려한다. 물론 현재의 조항으로도 인공지능 개발, 이용 과정에서 처리되는 개인정보에 대해서는 개정보보호법이 적용된다고 볼 수 있다. 그러나 「데이터기반행정 활성화에 관한 법률」 등 개인정보 보호법과의 관계를 명확히 규정한 예시처럼 개인정보보호법과의 관계를 명시하는 것이 바람직하다.

또한, 제15조(인공지능 학습용데이터 관련 시책의 수립 등)에서도 학습용데이터 시책을 수립・시행하거나 변경할 경우, 개인정보보호위원회의 심의를 거치도록 할 필요가 있다. 기본적으로

학습데이터는 개인정보의 대량 처리를 수반하기 때문에 개인정보의 보호와 관련된 부분이 관련 시책 마련 등에 반드시 기본사항으로 반영되어야 하기 때문이다.

4. 고영향 인공지능의 범위

AI 기본법안은 정부여당안(정점식 의원안)에서 '유아교육・초등교육 및 중등교육에서의 학생 평가'를 고영향 인공지능으로 새롭게 포함하는데 그쳤다. 우리가 앞서 제출한 의견서에서 고영향(고위험) 인공지능으로 포함해야 한다고 주장했던 많은 영역이 여전히 배제되어 있다. △범죄 수사나 체포 업무 외의 영역에서 생체인식정보를 분석・활용하는 데 사용되는 인공지능, △수사 및 기소 등 기본권을 침해할 수 있는 국가기관의 권한 행사에 이용되는 인공지능, △군 또는 정보기관에서 첩보, 방첩, 무기 운용에 사용되는 인공지능, △사람의 감정인식에 사용되는 인공지능, △사법부 또는 행정부에서 판결, 결정, 심판 등의 업무에 사용되는 인공지능, △정보통신망의 운영에 사용되는 인공지능, △선거 및 투표행위, 투표결과에 영향을 미치기 위하여 사용되는 인공지능, △제품 안전에 영향을 미칠 수 있는 인공지능 등이다. 금지된 인공지능에 대해서는 유럽연합 외에 다른 국가에서는 관련 규제가 없어서 도입하지 않았다고 하면서도, 유럽연합 뿐만 아니라 미국에서도 고영향 인공지능으로 규정하고 있는 여러 분야는 왜 배제했는지 의문이다.

5. 고영향 인공지능 사업자의 책무 및 벌칙

앞선 의견서에서 지적했다시피, 고영향 인공지능 사업자의 책무 규정은 여전히 구체성이 미흡한데, △개발 사업자의 책무와 이용 사업자의 책무를 구분하고 있지 않고, △ 최종결과, 주요기준, 학습데이터개요 등을 설명하도록 하고 있으면서도 '기술적으로 가능한 범위'로 한정하고 있으며, △이용자 보호 방안은 규정하고 있지만, 영향받는 자의 보호 방안은 배제하고 있다. 또한 '책무'가 사업자의 '의무'를 의미하는 것인지 모호하기 때문에 명확하게 '의무'라는 개념을 사용할 필요가 있다.

AI 기본법안에서 개선된 점은 과기정통부 장관으로 하여금 법 위반 사항을 발견하거나 혐의가 있음을 알게 된 경우, 또는 법 위반에 대한 신고를 받거나 민원이 접수된 경우 사업자에게 관련 자료를 제출하게 하거나, 필요한 조사를 할 수 있도록 한 점이다. 그리고 법 위반 사실이 인정되면 해당 위반행위의 중지나 시정을 위하여 필요한 조치를 명할 수 있다.(제40조)

그러나, 사업자의 책무 규정 위반에 대한 벌칙은 여전히 규정하고 있지 않다. 과기정통부 장관의 중지명령이나 시정명령을 이행하지 아니했을 경우에 3천만원 이하의 과태료를 부과하고 있을 뿐이다. 즉, 사업자 책무 규정 위반이 발생하고, 법 위반 사항에 대해서 과기정통부의 조사가 이루어지고 시정명령이 내려진 후, 시정명령을 이행하지 않았을 경우에만 비로소 고작 3천만원 이하의 과태료가 부과될 뿐이다. 이런 정도의 미약한 벌칙 수준으로 사업자들이 책무 규정을 이행하도록 어떻게 보장할 수 있을지 의문이다.

사업자의 책무 이행을 강제할 수단이 없다면 과연 사업자들이 AI 위험성 통제를 위한 조치들을 제대로 이행할 동기부여가 있을지 의문이다. AI 기본법안은 사업자의 책무 위반에 대해, 위반의 심각성에 상응하는 벌칙을 부과해야 한다. 과기정통부 장관의 시정명령을 이행하지 않는 사업자는 죄질이 심각하므로 과태료에 그칠 것이 아니라 훨씬 과중한 과징금을 부과하거나 형사처벌을 할 필요가 있다.

6. 범용 AI에 대한 규율

AI 기본법안은 생성형 AI에 대해 고지 및 표시 의무 등 투명성 의무를 부과하고 있는 한편, 학습에 사용된 누적 연산량이 대통령령으로 정하는 기준 이상인 AI 시스템에 대해서는 △ 수명주기 전반에 걸친 위험을 식별, 평가 및 완화하고, △ 관련 안전사고를 모니터링하고 대응하는 위험관리체계를 구축할 것을 의무화하고 있다.

그러나 범용 AI(혹은 최첨단 AI)에 대해서는 별다른 규율을 하고 있지 않다. 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. 또한, 범용 AI의 개발 및 운영 과정에서 사용되는 막대한 에너지 소비량에 대해서도 공개하도록 하여, 기후위기를 악화시키고 있는 것에 대해 적절한 책임을 지도록 할 필요가 있다.

7. AI 사업자에 대한 검인증

AI 기본법안은 AI 사업자 단체 등이 검증, 인증 활동을 자율적으로 수행하도록 하고, 과기정통부의 역할은 이를 '지원'하는 역할로 제한하고 있다. 그러나, 검증, 인증 활동 자체는 민간업체에 의해서 이루어질 수 있어도, 과기정통부는 이러한 검증, 인증 자체가 적절한 자격을 갖춘 업체에 의해서

제대로 수행될 수 있도록 보장할 필요가 있다. 그렇지 않으면, AI 사업자가 책무 이행을 회피하면서도 마치 책무 이행을 하는 것처럼 면죄부를 부여할 우려가 있다. 과기정통부는 검, 인증을 수행하는 사업자들이 적절한 자격을 갖추고 있는지 평가하고, 실제 검, 인증 활동이 제대로 수행되고 있는지 감독해야 할 책임이 있다.

8. 영향받는자의 권리

AI 기본법안이 정의 조항에서 '영향받는 자'의 개념을 두고, 제3조(기본원칙)에서 "인공지능이 사람의 생명・신체의 안전 및 기본권에 중대한 영향을 미치는 경우", 그 결과의 이유 및 원리 등에 대하여 기술적・합리적으로 가능한 범위에서 명확하고 의미 있는 설명을 제공받을 수 있는 '영향받는 자의 권리'를 규정한 것은 바람직하다. 또한, 제40조(사실조사 등)에서 '이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우' 과기정통부가 필요한 조사를 하도록 함으로써, 영향받는 자를 포함한 이해당사자에게 '신고' 및 '민원'을 제기할 수 있도록 한 것도 적절하다.

그런데, 제3조(기본원칙)에서 규정하고 있는, 영향받는 자의 설명 요구권을 실제 어떻게 행사할 수 있는지 규정하는 조항을 포함하고 있지 않다. 법사위 심사 과정에서 이러한 입법 미비가 해결될 필요가 있다.

영향받는 자의 권리와 피해구제 조항을 별도로 규정할 필요가 있을 뿐만 아니라, 법안 전반적으로 영향받는 자를 고려하도록 수정되어야 한다. 예를 들어, 인공지능 기본계획에도 '이용자 및 영향을 받는자의 권리보호 및 피해구제에 관한 사항'이 포함되어야 하며, 국가인공지능위원회의 위원으로 '이용자와 영향받는자를 대표할 수 있는 사람'이 위촉되어야 한다. (불행하게도 현재 구성된 국가인공지능위원회는 이용자, 영향받는 자, 인권 및 시민사회를 대표할 수 있는 사람들이 배제된 것으로 보인다)

9. 인공지능 감독기구

시민사회는 과기정통부가 AI 기본법안의 주무부처로서 안전성, 신뢰성 확보의 책임까지 담당하는 것에 대해 우려를 표명해왔다. 지금까지 과기정통부가 보여준 모습은 AI의 위험으로부터 시민의 안전과 인권을 보호하기보다는 AI 산업육성만을 강조하는 것이었기 때문이다. 과기정통부가 법

위반에 대한 사실조사를 하고 시정조치를 명령할 권한을 보유하고 있다고 한들, 제대로 사업자를 감독할 것인가 의구심이 드는 것도 사실이다.

AI 개발, 제공 사업자의 책임성 부재로 인해 안전이나 인권을 침해하는 사고가 발생할 경우, 관할부처인 과기정통부 역시 책임으로부터 자유로울 수 없음을 명심해야 한다. 국회는 과기정통부가 AI에 대한 규율을 제대로 하지 않을 경우, AI 감독을 위한 별도의 행정기관의 신설을 검토해야할 것이다.

10. 인공지능 영향평가

AI 기본법안에 인공지능 (인권)영향평가 조항이 포함된 것은 다행스러운 일이지만, 매우 한계가 많다. EU AI Act에서는 고위험 AI 운영자에게 인권영향평가 수행을 의무화하고 있으나, 우리나라의 AI 기본법안은 단지 영향평가를 위해 '노력'할 의무만을 부여할 뿐이다. 국가인권위원회가 권고한 바와 같이 최소한 고위험 AI의 운영자에게는 인공지능 (인권)영향평가를 의무화할 필요가 있다. 특히 공공기관이 고영향 AI 시스템을 운영할 경우 국민들은 선택의 여지없이 그 대상이 되어야 하므로, 영향평가를 의무화해야 한다.

11. 딥페이크 고지/표시 의무

AI 기본법안에서 "인공지능시스템을 이용하여 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상 등의 결과물", 즉 딥페이크를 제공하는 경우 해당 결과물이 "인공지능시스템에 의하여 생성되었다는 사실을 이용자가 명확하게 인식할 수 있는 방식으로 고지 또는 표시하여야 한다"는 내용이 포함된 것은 바람직하다. 예술 창작 영역의 딥페이크 사용에 대해서는 고지 또는 표시 의무를 유연하게 적용하도록 하였다.

시민사회의 요구에도 불구하고 이러한 규정이 포함되지 않다가, 최근 딥페이크 성착취물이 논란이 되면서 새롭게 포함되었다. 이처럼 심각한 문제가 발생한 이후에야 사후약방문식으로 AI 위험을 통제하기 위한 조치를 AI 기본법안에 포함시키겠다는 것인지 우려스럽다..

12. 데이터 센터

AI 기본법안은 정부로 하여금 “인공지능의 개발・활용 등에 이용되는 데이터센터의 구축 및 운영을 활성화하기 위하여 필요한 시책을 추진하”도록 하고 있다.(제25조) 이 조항만 보더라도 AI 기본법안이 AI 산업육성에만 치우져있을 뿐, AI의 개발 및 활용이 인간과 지구의 생태적 환경에 미치는 영향에 대해서는 얼마나 무관심한지 알 수 있다. AI 개발과 활용 과정에서 물과 전기 등 막대한 에너지가 사용되고, 이는 AI 데이터센터 인근 지역의 공동체에 부정적 영향을 미칠 뿐만 아니라, 기후위기를 심화할 것이라는 우려가 제기되고 있다. 게다가 AI 사업자들이 에너지 소비에 대한 데이터를 공개하지 않고 있기 때문에 기후위기에 미치는 영향에 대한 과학적 분석이 제대로 이루어지지도 않고 있다. 그럼에도 AI 기본법안은 과도한 에너지 사용에 대한 AI 사업자의 책임을 묻기는 커녕, 오히려 AI 데이터센터의 구축 및 운영을 활성화하기 위해 행정적, 재정적 지원을 하도록 하고 있다. 왜 AI 사업자들이 공동체에 부담을 지우는 것에 대해서는 책임을 묻지 않고, 공적 자원을 사기업의 이익을 위해 지원해야 하는가. 공동체와 사회에 대한 AI 사업자들의 책임과 기여를 전제로하지 않는 ‘묻지마식 지원’에 반대한다.