

공공운수노조·국민건강보험노동조합·디지털정의네트워크·문화연대·미디어기독연대·민주사회
를 위한
변호사모임디지털정보위원회·서울YMCA시민중계실·울산시민연대·인권교육온다·정보인권연구
소·참여연대·투명사회를위한정보공개센터·표현의자유와언론탄압공동대책위원회·한국사이버
성폭력대응센터·한국소비자연맹·한국여성단체연합·한국여성민우회

수 신 국가인공지능전략위원회
발 신 17개 단체(참여연대 담당 이지는 선임간사 02-723-0666, 디지털정의네트워크 담당 오병일
대표 02-774-4551, 민변디정위 담당 최새안 변호사 02-522-7284)
제 목 [공문]「대한민국 인공지능 행동계획」(안)에 대한 17개 단체 의견서
날 짜 2026. 1. 4. (별첨 포함 총 41 쪽)

「대한민국 인공지능 행동계획」(안)에 대한 17개 단체 의견서 제출의 건

AI 위험성 통제 장치·개인정보 보호원칙·민주적 거버넌스 체제 등
미흡

사업자 책임성 강화, AI 영향을 받는 사람들의 권리,구제방안
마련해야

1. 안녕하십니까.
2. 귀 위원회가 지난 2025년 12월 16일 공고하고 2026년 1월 4일까지 의견수렴 중인「대한민국 인공지능 행동계획(안)」은 전반적으로 AI의 개발·활용에만 중심을 두고 AI 위험성을 통제하거나 사업자의 책임성을 제고할 방안이 미흡합니다. 또한 AI의 영향을 받는 시민 등의 권리 및 구제 방안이 부재하고 AI의 개발 및 활용을 지나치게 강조한 나머지, 개인정보 보호원칙조차 무시하거나 헌법상 기본권인 개인정보자기결정권을 형해화하고 있습니다. 무엇보다 국가 전반을 아우르는 AI 정책을 수립하면서 시민사회와 영향을 받는 사람들의 참여를 보장하고 있지 못합니다. 이번 국가인공지능 행동계획(안)은 대폭 수정되고 미흡한 부분은 보완되어야 할 것입니다.
3. 이에 17개 시민사회단체는 98개 행동계획 전반에 대한 의견서를 별첨과 같이 제출하오니, 정책 수립 과정에 적극 반영하여 주시기 바랍니다. 특히 이번 의견서 제출이 형식적 절차로 끝나지 않고 실질적인 정책 수정 내지 보완으로 이어져 실효성 있는 결과로 이어지기를 기대합니다. 끝.

▣ 별첨자료. [「대한민국 인공지능 행동계획」\(안\)에 대한 17개 단체 의견서\(총 40쪽\)](#)

각 단체 직인 생략

시민사회 의견서

발행일 2026. 1. 4.

「대한민국 인공지능 행동계획」(안)에 대한 시민사회 의견서

AI 위험성 통제 장치 · 개인정보 보호원칙
· 민주적 거버넌스 체제 등 미흡

사업자 책임성 강화, AI의 영향을 받는
사람들의 권리 및 구제 방안 마련해야

목차

목차	3
총론	4
‘규제완화’ 분야 - 정보인권 강화해야	11
‘공공 AX ’ 분야 - 공공성·책임성 강화해야	17
‘문화·예술’ 분야 - 문화생태계 전반 아우르는 비전 제시해야	21
‘ AI 기본사회’ 분야 - 사회적 합의부터 도출해야	23
인공지능 ‘영향받는 자’ 관련 - 액션플랜의 중심돼야	30
I. 학생·학부모·교사 등 교육 부문	30
II. 환자·의료인·수급자 등 보건복지 부문	33
III. 국방·평화 부문	36
IV. 노동자	39
V. 여성	41

지난 12월 16일, 대통령직속 국가인공지능전략위원회는「대한민국 인공지능 행동계획」(안)(이하 초안)에 대한 의견을 수렴한다고 공지함. 이에 시민사회는 초안에 대해 아래와 같은 총론적 의견을 제시함.

1) AI의 개발·활용에만 중심을 두고 AI의 위험성을 통제하고 사업자 책임성을 강화할 장치 미흡

- 초안은 전반적으로 AI의 개발·활용에만 중점을 두고 있음. 심지어 '전략분야 AI 기본사회'마저도 취약계층도 어떻게 AI를 활용할 수 있을지, 사회적 문제 해결을 위해서 어떻게 AI를 활용할지에 초점을 두고 있음. 시스템이 가진 모순에는 눈 감은 채 AI를 개발하고 활용하는 것만으로 문제가 해결될 것이라고 믿는 건 그저 기술해결주의에 불과함.
- 초안은 "규제 패러다임을 '사전 통제'에서 '자율과 책임 기반의 사후 지원'으로 전면 전환해야 한다. 특히, 기업 활동을 저해하는 관료적 절차와 중복 규제를 철폐하기 위해, 원칙적으로 허용하고 예외적으로 금지하는 '네거티브 규제' 체계를 AI 분야에 우선 도입"한다고 함.(p55) 이는 시민의 안전과 인권을 위협하는 AI 시스템도 일단 도입하겠다는 것이나 다름없으며, 인공지능 기본법 제정 과정에서 시민사회의 반대로 삭제되었던 '우선도입-사후규제' 원칙을 되살리는 것임. 그마저도 초안은 사업자들이 자율적으로 어떻게 책임을 질 것인지, 예외적으로라도 무엇을 금지할 것인지에 대해서는 거의 언급하고 있지 않음.
- 초안은 현재와 근미래의 AI 성과와 발전이 마치 모든 것을 해결해줄 수 있으므로 공무원에서부터 학생까지 전 국민이 AI 활용 역량을 가져야 하는 것으로 전제함. 그러나 '알고리즘의 오류·편향·불투명성'은 기술적으로 완전히 해결된 것도 아니고 근미래에 그러한 전망이 보이는 것도 아님. 또한, AI가 인간의 정신과 역량에 어떠한 영향을 미칠지, 가령 AI를 사용하는 것이 사람들의 인지 역량, 직무 역량 등에 부정적인 영향을 미치는 것은 아닌지, 조직 차원에서 AI에 과의존했을 때 발생할 수 있는 문제는 무엇인지 등에 대해 아직 충분한 연구가 진행되지 않은 상황임. 초안에서도 "교육AI는 기술 변화 속도가 빠르고, 사회적 파급력이 큰 분야임에도 불구하고 새로운 기술의 교육적 타당성, 학습효과, 안전성을 지속적으로 관찰·검증하는 체계가 마련되어 있지 않다"(p150)고 하는데 이는 비단 교육 AI에 국한된 것은 아님. 그럼에도 초안은 마치 AI 시스템이 인간에 미치는 영향, 효과, 안전성이 검증된 것처럼 전제하고 있음.
- 반면, AI의 위험성을 통제하고 AI 제공/배치 사업자의 책임성을 강화할 장치는 거의 초안에서 다뤄지고 있지 않음. 예를 들어, 초안은 공공부문 AI 도입과 관련해서는 "민원 처리, 복지 선정, 규제 집행, 채용·심사 등 국민 생활과 직결된 영역에서 AI가 판단

과정에 개입할 경우, 알고리즘의 오류·편향·불투명성이 기본권 침해로 이어질 수 있다는 우려가 제기된다"며 공공 AI 영향평가를 언급하고 있지만, 이러한 위험성은 단지 공공부문 AI에만 발생하는 것이 아니며, 민간 분야에서도 수많은 고위험 AI 분야가 있을 수 있음. 또한, '알고리즘의 오류·편향·불투명성'은 악의적인 사용이 아니라 AI 시스템에 내재한 본질적인 문제인데 이를 어떻게 통제하고, 사업자는 어떠한 책임을 지는 것인지에 대해서 어떠한 행동계획도 제시하고 있지 않음. 단지 교육 AI와 관련해서만 "혁신을 장려하면서도 공공이 품질과 안전을 책임지는 실증-안전-평가-확산의 통합 거버넌스 구축이 필요하다"(p153)고 언급하고 있는데, 이는 모든 AI에 대해 기본이 되어야 함.

- 아직 인공지능 기본법과 하위법령에서 충분히 다루지 못했음에도 불구하고, 초안은 우리 사회에서 금지해야 할 AI, 또는 고위험(고영향)으로 관리해야 할 AI 분야에 대해, 누가 언제까지 어떻게 검토하고 사회적인 논의를 해나갈지에 대해 전혀 언급하고 있지 않음. 이는 과기정통부 뿐만 아니라 전 부처에서 검토하고, 사회 각계의 의견을 수렴하여 시급히 규정해나가야 할 사항이므로, 행동계획을 통해 향후 로드맵이 제시되어야 함. (행동계획은 인공지능 기본법과 밀접한 관계에 있으며, 실제 초안은 일부 분야에선 인공지능 기본법에의 반영을 언급하고 있음)
- 고영향 AI 사업자의 책무 역시 인공지능 기본법 및 하위법령에서 매우 부실하게 다루어졌고 추가적인 연구와 검토가 필요한 부분인데 행동계획에서 전혀 고려되지 않고 있음. 고영향 AI 개발자(모델 개발자, 하위스트림 개발자 등), 배치자, 유통업자 등 행위자별로 어떻게 다른 책임을 부과해야 하는지 엄밀하게 규정할 필요가 있으며, 이는 신속하게 추진되어야 할 과제로 행동계획에 포함되어야 함.
- 인공지능 기본법은 '노력할 의무'만을 부여하고 있고, 초안에서는 공공 AI에 대해서만 언급하고 있지만, 고위험(고영향) AI의 위험성을 식별, 완화, 제거할 수 있는 AI 기본권 영향평가를 누가(가령 국가인권위원회 및 과기정통부 등), 언제까지, 어떻게 활성화시킬 것인지에 대해 행동계획을 통해 로드맵이 제시되어야 함.
- 투명성 보장 방안 역시 인공지능 기본법 및 하위법령에서 규정하고 있으나 아직 미흡한 수준임. 특히, AI 시스템의 특성에 따라 누가, 어떻게 표시 의무를 이행할 것인지, 플랫폼 사업자의 책임은 무엇인지, 우회를 방지하기 위한 방법은 무엇인지, 이를 위해 개발이 필요한 기술은 무엇인지 등 행동계획을 통해 연구, 검토되어야 할 사항이 매우 많음에도 불구하고 초안에서는 고려되지 않고 있음. 투명성 보장 방안에 대한 행동계획이 필요함.
- 이미 초안도 인지하고 있듯이 AI 시스템의 불투명성은 근본적인 특성이며, AI 시스템의 설명가능성, 해석가능성 등에 대한 연구가 진행되고 있지만 아직 미진한 상황임. 특히 불투명한 AI 시스템은 투명성과 책무성을 핵심으로 하는 공공분야에서는 치명적인 문제가 될 수 있음. 공공분야에서는 설명가능하지 않은 AI, 위험성이 검증되지 않은 AI는 도입하지 않겠다는 명확한 입장 표명과 함께, AI 시스템의 불투명성을 개선하기

위한 기술 개발, 설명가능성과 해석가능성 등 개념의 의미, 투명성의 이행 방안 등에 대한 연구와 검토가 필요하며, 이 역시 행동계획에 포함되어야 함.

2) AI의 영향을 받는 사람들의 권리 및 구제 방안 부재

- 초안은 '12) 전략분야 글로벌 AI이니셔티브 구현' 부분에서 국제규범 형성에서의 '민주적 가치와 인권 존중의 원칙'을 간단히 언급한 것을 제외하면, 초안 전반적으로 '인권 원칙'보다는 '윤리'를 강조하고 있음. 나아가 초안 전반적으로 AI의 영향을 받는 사람들의 권리 및 구제방안에 대한 계획이 부재함.
- 초안은 "윤리기준의 국제적 정합성을 재점검하고, 개발·이용 전 과정에서 사업자가 스스로 점검할 수 있는 체계적 기준을 마련할 필요가 있다"(p133)고 하지만, 전 세계적으로 합의된 윤리기준은 없음. 반면, 전 세계적으로 합의된 인권 기준은 있으며, 유엔 사무총장과 인권최고대표는 일관되게 AI에 있어서 '인권기반접근'을 강조해왔음. 2024년 통과한 유엔 최초의 AI 결의안(A/78/L.49) 역시 "AI의 설계, 개발, 배포, 이용 전 과정에서 인권의 존중·보호·증진을 핵심 원칙으로 삼을 것"을 강조하고 있음. 유엔 표현의자유 특별보고관이 2018년 보고서(A/73/348)에서 언급한 바와 같이 AI 윤리는 인권을 보완할 수는 있지만 대체할 수는 없음. 모든 행위자가 스스로 윤리적인 행위를 하는 것은 중요하지만 사람들이 중요하게 생각하는 윤리는 다를 수 있음. 그러나 모든 사람은 권리가 있고 국가와 기업은 권리를 보장하고 침해를 구제해야 할 책임이 있음. 사람들이 자신의 권리를 인식하고 필요할 경우 국가와 기업에 권리의 보장을 요구할 수 있으며, 이를 보장하는 사회적인 체계를 수립하는 것이 AI 시대에도 특히 중요함. 따라서 초안의 '윤리 기반 접근'은 '인권 기반 접근'으로 수정되어야 함. 예를 들어, '55 안전한 AI이용 보장, 공공부문 AI 윤리기준 마련'의 경우, 공공부문 AI 윤리기준의 마련에 그쳐서는 안되며, 공공부문이 시민의 권리를 보장할 책임을 질 수 있도록 법제가 마련되어야 함. '82. 모두의 AI를 위한 AI 윤리 확산·고도화' 역시 모두를 위한 권리 보장 체제의 마련으로 수정되어야 함.
- 이와 함께, AI 시대에 특히 위험에 처할 수 있는 사람들의 권리를 보장할 수 있는 구체적인 행동계획이 필요함.
- 초안은 행동계획에 디지털 성착취물의 단속만을 포함하고 있을 뿐, 한국의 AI 정책에서 어떻게 성인지적 관점을 반영할 것인지에 대한 인식과 계획이 전무함. AI 시스템의 편향과 차별이 내재적인 문제라고 했을 때, 우리 사회의 가장 큰 편향인 성별 편향, 고정관념, 배제 등이 확대재생산되지 않도록 총체적인 고려가 필요함. 디지털 성착취물의 단속과 같은 AI 시스템의 '악용'에 대응하는 것도 필요하지만, AI 거버넌스에 성별 다양성이 고려될 수 있도록 구성하고, 실질적인 참여를 보장할 필요가 있음. 또한, AI 개발 및 활용 전 과정에서, 데이터와 알고리즘에서, 성별 편향이 나타나지 않도록 보장할 수 있는 시스템을 마련할 필요가 있음.

- AI는 비단 노동시장에 영향을 미칠 뿐만 아니라, 고용 및 노동 과정에서의 AI 시스템으로 인한 차별, 노동자 개인정보 프로파일링 및 알고리즘 기반 관리 확산에 따른 근로자 통제 강화 등 다양한 문제를 포함하고 있음. 그러나 초안은 주로 노동시장에 미치는 영향에 대해서만 초점을 맞추고 있으며, 노동환경이나 공정한 알고리즘과 관련해서는 간단히 언급하고 있을 뿐임. 특히, 이 부분은 개인정보위와 노동부 모두 제대로 규율하지 않는 규제 사각지대에 해당함. AI가 노동자의 고용 및 노동 과정에 미치는 전반적인 영향과 이에 대한 규제 방안이 행동계획에 좀 더 구체적으로 포함되어야 함.
- AI 전환은 소비자의 권리에도 큰 영향을 미치게 될 것임. 소비자는 생성형 AI 이용자일수도, 소셜미디어 이용자일수도, 환자일수도, 은행 고객일 수도 있음. AI는 소비자가 AI로 무엇을 생산할 수 있는지, 어떤 콘텐츠를 접할지, 어떤 치료를 받을지, 대출을 받을 수 있는지 영향을 미치게 될 것임. 자신에게 영향을 미치는 결정이 AI에 의해 이루어졌다는 것을 모를 수도 있고, 다크 패턴과 같이 현혹될 수도 있으며, 가격 차별이나 사기를 당할 수도 있음. 그러나 초안은 AI에 의해 소비자가 어떤 영향을 받게 될 것이고, 소비자 권리를 보호하기 위해 어떠한 조치가 필요한지, 어떤 부처들이 무엇을 준비할지 전혀 언급하지 않고 있음. AI 시대 소비자 보호를 위한 대책이 행동계획에 포함되어야 함.
- 초안은 AI 정밀복지 체계 구축(p141)에서 장애인을 포함한 것 외에는 AI 시대 장애인의 권리에 대해서는 전혀 언급하지 않고 있음. 그러나 AI는 장애인에게 기회를 제공할 수도, 오히려 차별을 심화할 수도 있음. AI가 장애인의 삶과 노동에 어떠한 영향을 미치게 될 것인지, 장애인의 권리를 어떻게 보호, 규제할 것인지에 대한 로드맵을 행동계획으로 포함해야 함.
- 공공 AI는 단지 시민들의 서비스를 위해서만 사용되는 것이 아니라, (의도와 무관하게) 시민들을 감시, 차별, 배제하기 위한 목적으로 사용될 수도 있음. 예를 들어, 경찰, 출입국, 사회보장 등에서 사용되는 AI가 그럴 수 있음. 특히, 초안에서 강조하는 바와 같이 공공 AI를 위해 "모든 관련 데이터는 표준화되고, 통합되며, 현재화"된다면, 시민에 대한 감시 역시 더욱 용이해질 것임. 이 경우 시민들은 자신이 AI의 대상이 되었다는 사실 자체를 인지하지 못할 수도 있음. 따라서 공공 AI에 의해 시민의 권리가 어떻게 영향을 받고, 시민의 권리를 보호, 규제할 수 있는 종합적인 방안이 행동계획으로 포함되어야 함. 또한, 시민의 권리를 보호하기 위한 공공기관의 책임성도 규정되어야 함.

3) 개인정보 보호원칙과 자기결정권 무시

- 초안은 AI의 개발 및 활용을 지나치게 강조한 나머지, 개인정보 보호원칙 조차 형해화하고 시민들의 개인정보 자기결정권을 침해하고 있음. 특히, "가명처리하지 않은 개인정보를 안전하게 AI학습에 활용할 수 있도록 '26년 1분기 내로 개인정보

보호법 개정을 추진"(p50)한다고 하는데, 이에 대해 시민사회는 일관되게 반대하는 입장을 표명해왔음. 단지 AI 개발에 도움이 된다는 이유로 역사적으로 형성되어온 기본적인 원칙을 손쉽게 무시하는 것은 정당성을 얻기 어려움.

- 심지어 초안은 "의료데이터 연계·구축 계획"(p46), "여러 병원들에 흩어져 있는 개인의 의료 정보를 개인단위로 정확히 연계"(주46)할 계획까지 추진하고 있음. 그러나 의료 AI가 막연하게 국민의 건강을 증진시킬 것이라는 희망만 있을 뿐, 실제로 이것이 어떤 기업에게 이익이 되는지, 민간 보험회사나 데이터 분석 회사의 이익을 위해 남용될 우려는 없는지, 책임성(responsibility), 안전성(safety), 형평성(fairness) 등의 가치(p48)가 어떻게 보장될 수 있는지 등에 대해서는 구체적으로 언급하지 않고 있음. 의료 AI의 오진으로 환자가 피해를 입거나 차별을 받을 가능성 등 의료 AI 추진 과정의 문제에 대해서도 고려되고 있지 않음.
- 공공 AI를 위해 "모든 관련 데이터는 표준화되고, 통합되며, 현재화"하고, "AI가 업무 맥락을 이해하고 요약·추천·예측을 수행하는 지능형 업무관리 플랫폼"의 구현에 대해서도 우려하지 않을 수 없음. 공공기관 내에서도 업무에 따라 개인정보나 기밀 데이터에 대한 접근은 통제되어야 하는데, 이와 같은 방식으로 데이터를 통합하고 AI 학습에 이용할 경우, 서로 다른 기관 사이에 개인정보나 기밀 데이터가 권한을 넘어 공유될 가능성은 이전보다 높아지고 통제는 더욱 어려워질 수밖에 없음. 또한, "AI가 업무 맥락을 이해하고 요약·추천·예측을 수행하는 지능형 업무관리 플랫폼"이 시민감시 목적으로 사용될 경우 인권 침해 우려는 더욱 커질 수밖에 없음. 이러한 시민감시의 문제는 현 정부의 '의도'가 중요한 것이 아니라, 정부가 데이터를 관리하고 처리하는 시스템에 내재한 문제임을 인식할 필요가 있음.
- 초안은 개인정보 활용에 대해서는 다각도의 행동계획을 구체화하고 있지만, 보호대책은 그 내용을 알 수 없는 「AI 시대 개인정보 보호 및 불법 유통 방지 종합 대책」을 수립하도록 하는 것에 불과함. 최근 대량 개인정보 유출 사고가 연이어 발생하고 있는 바, 정보주체의 권리 보호를 위한 집단소송제 도입 등 소비자 보호대책도 행동계획에서 함께 논의될 필요가 있음.

4) 민주적 거버넌스 체제 부재

- 지난 2024년 개최된 AI 서울 정상회의는 선언문에서 “안전이 책임있는 AI 혁신을 진전시키는 핵심 요소”임을 확인하였으며, "안전하고, 혁신적이고, 포용적인 AI 생태계 육성을 위해 정부·민간·학계·시민사회를 포함하는 다중이해관계자간 적극적 협력"의 중요성을 강조하기도 했음. 그러나 정부의 행태를 보면 이는 모두 번드르르한 말 뿐임. 정부는 인공지능 기본법 및 하위법령의 제정 과정에서 뿐만 아니라, 본 초안의 작성 과정에서도 시민사회의 참여를 일관되게 배제해왔음.
- 앞서 지금까지 본 초안에서 다루지 않은 많은 의제들(이조차 매우 일부분이지만)을 제기하였음. 이 많은 의제들이 공백인 이유는, 이에 대해 문제제기를 할 수 있는

사람들, 시민사회와 영향받는 당사자들이 AI 정책 결정 과정에 참여하지 못하고 배제되었기 때문임. 이런 식으로 계속 시민사회 및 영향받는 사람들을 배제한다면, 본 행동계획을 포함한 한국의 AI 정책 이행 과정에서 커다란 반발과 저항에 직면하게 될 것임.

- 본 초안의 또 하나의 커다란 공백은 AI에 대한 효과적인 감독을 위한 국가적인 거버넌스 계획이 부재하다는 것임. 관련하여 유엔 인권최고대표는 디지털 시대 프라이버시권 보고서(A/HRC/48/31)에서 AI에 대한 독립적이고 공정한 감독 체계의 필요성을 강조하면서, 개인정보보호 감독기구, 소비자 보호 기관, 차별 방지 기구, 국가 인권 기구 등 다양한 기관의 복합적 감독 구조를 제안한 바 있음.
- 본 초안의 공개 전에 국가 AI 전략위원회 분과위원조차 초안을 검토한 적이 없다고 함. 이 초안은 200페이지에 달하는 방대한 분량을 갖고 있으면서도 2025년 12월 16일에 공개되어 2026년 1월 4일까지, 주말을 포함해도 고작 20일 정도밖에 의견 수렴 기간을 주지 않았음. 모두가 한해를 정리하고 휴식을 취해야할 연말, 연시임을 고려하면, 전략위원회가 진정으로 의견을 수렴할 의지가 있는지 의문임.

5) 국가정보원의 역할 확대 및 시민 감시 우려

- 기존의 잘못된 구조를 그대로 둔 채 AI를 도입하게 되면, 문제 상황을 확대 재생산할 수 있음. 국가정보원의 권한 역시 마찬가지임. 국정원은 정보기관으로서의 역할에 맞지 않게 공공 정보통신망에 대한 사이버보안 권한을 갖고 있으며, 초안은 이를 그대로 인정한 채 개인정보 보안이나 사이버안보 분야의 AI와 관련하여 국정원에 역할을 부여하고 있음. 예를 들어, '10. AI 기반의 사이버 보안 체계 구축, AI 보안 기술 경쟁력 강화 및 보안 전문 인재 양성'(p15)이 국정원의 역할로 되어 있고, "AI를 활용한 사이버 위협 (딥페이크, 악성코드 생성 등)에 대해 기술적으로 선제적 탐지·차단하는 독자적인 '사이버 AI 안보 플랫폼' 구축을 위한 정보화 전략 계획"(p17)을 수립하는 역할도 국정원에 맡겨져있음. 국정원의 사이버보안 역할 만큼이나 AI 사이버보안을 왜 정보기관이 맡아야 하는지 의문임.
- 이에 대한 의구심은 비단 국정원이 시민감시와 정치 개입을 해왔던 암울한 과거를 갖고 있기 때문이 아님. 문제는 현재도 국정원은 예산 및 국회 감시를 제대로 받지 않는 초법적인 기관이라는 것임. 해외 정보 수집이라는 극히 제한적인 역할이 아니라, 왜 민간 네트워크와 연결될 수밖에 없는 공공 정보통신망에 대한 사이버보안, 나아가 국가 사이버전략에 대한 수립 권한을 통제받지 않는 정보기관에게 부여해야 하는지 알 수 없음. 만일 국정원에게 이러한 역할을 맡겨야 한다면, 다른 정부부처 수준의 예산 및 국회의 통제를 받도록 해야할 것임.
- 심지어 국정원은 공공 정보통신망에 대한 사이버보안 권한을 민간의 정보통신망으로 확대하기 위해 호시탐탐 노리고 있던 바, "AI를 활용한 사이버 위협 (딥페이크, 악성코드 생성 등)에 대해 기술적으로 선제적 탐지·차단하는 독자적인 '사이버 AI 안보

플랫폼' 구축"이야말로 공공의 정보통신망에만 국한하지 않으며, 민간 정보통신망에 대한 감시와 개입(선제적 탐지·차단!) 권한을 국정원에게 부여하겠다는 것이나 마찬가지임. 이는 시민들의 온라인 활동에 대한 감시로 남용될 우려가 큼.

- 정부는 행동계획에서 국정원의 역할을 정보기관의 역할로 제한하고, 국정원의 권한에서 사이버 보안 권한을 삭제해야 함.
- 초안은 국방 분야의 경우 '(가칭) 국방 AI 기본법'을 '26년 2분기까지 제정한다고 하고 있으나, '국가안보 목적' AI 분야는 여전히 제외되어 있음. 행동계획에 포함되어 있지 않다는 것은 아무런 법적 근거도 없이 국가안보 목적 AI의 개발과 활용을 하겠다는 것인지 의문임. 국가안보 AI를 규율할 수 있는 법제가 조속히 마련되어야 하며, 이 역시 행동계획에 포함되어야 함.

‘규제완화’ 분야 - 정보인권 강화해야

1. 액션플랜 번호

- 04. 국가데이터 통합플랫폼을 통한 민간·공공 데이터 자산화
- 05. AI 데이터 공유 생태계 활성화
- 10. AI기반의 사이버 보안 체계 구축, AI 보안 기술 경쟁력 강화 및 보안 전문 인재 양성
- 31. 개인정보·미개방 산업 데이터 활용 규제 과감한 정비
- 32. AI 학습·평가 목적의 저작물 활용 및 유통 생태계 활성화
- 33. 규제 합리화를 통해 혁신을 촉진하는 AI 산업생태계 조성
- 34. 국가 AI 대전환을 뒷받침하는 AI 법제 환경 조성

2. 수정 요구 및 제안 이유

- **【수정 요구】** ‘국가데이터 통합플랫폼’ 구축은 사전 위험 대비 분석, 방안 마련 후 신중히 추진해야 함. (액션플랜 4)

【제안 이유】

- 각 정부 부처가 고유한 공익적 목적에서 수집, 보유, 생산하고 있는 데이터를 민간데이터와 통합, 하나로 연계하는 것은 물리적 통합, 연계 이상의 의미를 지니는 것임. 우선 각각의 정부 부처가 고유의 목적에 맞는 행정 데이터를 수집, 보유하고 있는데 이를 서로 자유롭게 이동하고 공유한다는 것이 갖는 의미와 위험에 대해 제대로 파악할 필요가 있음. 다양한 기능과 목적에 따라 보유하고 있는 데이터를 자유롭게 이동하고 공유하면 할수록 유출 위험과 프라이버시 침해 가능성이 높아진다는 점도 고려해야 함. 결국 정부 부처를 비롯 공공기관이 각각의 고유한 공익 목적으로 수집 보유해 온 개인정보를 민간정보와 통합, AI학습 등에 활용하기 위한 목적인데 이는 개인정보의 목적 외 이용에 해당함. 국민의 개인정보를 인공지능산업 활성화를 위해 통합하고 이를 활용하도록 하겠다는 것은 개인정보보호의 기본원칙인 목적 구속성, 최소수집의 원칙에 반하는 등 개인정보자기결정권을 침해하는 것임. 2021년 법무부 과기부의 인공지능 얼굴인식 출입국 관리 시스템을 개발한다며 내외국인의 얼굴정보 등 민감정보를 정보주체 모르게 민간기업의 인공지능 학습 등에 활용하도록 해서 충격을 안겨주었던 사건은 현재 헌법재판소에서 그 위험 여부를 심리 중이기도 함.
- 표준화된 ‘국가데이터 통합플랫폼’은 모든 민간·공공데이터의 소재 정보가 한 곳에 연계될 수 있도록 함으로써 해킹 등 사이버공격의 표적이 될 가능성이 높고, 사고 발생시 그 피해 규모도 엄청날 것임. 지난 2023년 11월 17일 발생한 국가 행정 전산망 마비 사태, 2025년 9월 국가정보자원관리원 화재로 인한 정부 전산망 마비 사태 등

예상하지 못한 전산망 마비가 발생했을 시 자칫 국가기능 자체가 전면 중단될 수도 있음.

- 무엇보다 국가가 공익 목적으로 수집, 보유 및 생산한 데이터는 그 각각의 기밀성, 안전성, 책임성 등의 층위가 다양할 수밖에 없으며 이를 민간데이터와 연계 및 공유하겠다는 것은, AI기업에 국가의 기밀까지 조건없이 넘기겠다는 것과 다르지 않음.
- 정부 부처 등 공공기관과 민간 데이터를 연계 하나로 통합하는 국가데이터 통합플랫폼 구축은 원칙적 반대, 만약 추진한다면 사전 위험 대비 분석, 방안 마련 후 신중히 추진해야 할 것임.

- **[수정 요구]** 개인정보보호를 위한 방안은 **2026년 1분기** 내 수립해야 할 가장 시급한 과제임. (액션플랜 31)

[제안 이유]

- 빠르게 상용화하고 있는 AI 에이전트 활용으로 인한 오작동·권한 오남용·정책 우회, AI 에이전트로 인한 개인정보 유출 등의 위험을 차단하기 위한 기술적·관리적 대응 방안 마련은 이미 늦은 감이 있음. 따라서 이는 26년 최우선 과제로 추진해야 할 것임.
- 개인정보를 학습하는 고영향 AI의 내·외부 취약점 점검 등 개인정보 유출을 방지하기 위한 안전성 확보 방안 역시 액션 플랜대로 27년 4분기까지 마련하는 것은 AI활용을 위한 법제들은 26년 1분기 정비하겠다고 하면서 안전성 확보 방안은 그보다 한참 뒤로 미루는 것은 비례적이지도 않음. 안전성 확보가 마련되고 나서야 국민들도 AI정책에 신뢰를 보낼 수 있을 것임.

- **[수정 요구]** 개인정보 원본을 마치 공유재처럼 특정 기술의 발전을 위해 마음대로 쓸 수 있도록 하는 법개정에 반대함. (액션플랜 31, 33)

[제안 이유]

- 기본적으로 여러 법에 다양한 규제 특례 조항이 있어 혼란을 주고 있기 때문에, 개인정보에 관한 기본법인 개인정보 보호법과 관련법률에 대한 명확한 해석 기준 제시 내지 개정을 통하여 신속하고 안전한 개인정보의 AI 학습 방안에 대한 개선책을 제시한다는 방향은 기본 전제가 잘못된 것임. 헌법상 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지 정보주체 스스로 결정할 권리임 (2014헌마463). 이를 구체화한 개인정보보호법은 기본법으로서 “개인의 정보 보호”를 기본 원칙으로 하여, 개인정보 처리자에게 목적 명확화, 필요 최소한 범위내에서 적법, 정당한 수집 및 처리, 목적 외 활용 금지 등을 명시하고 있음(개인정보 보호법 제3조 제1항 내지 제2항). 또한 개인정보처리자는 적법하게 수집한 개인정보라고 하더라도 목적을 넘어 이용하기 위해서는 원칙적으로

정보주체에게서 별도 동의를 받아야만 함. 단 2020년 신설된 가명정보 처리에 관한 특례 규정에 따라 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 활용할 수 있도록 예외를 인정하고 있음. 현행 개인정보보호법에 따르면 개인정보처리자는 정보주체로부터 적법하게 수집한 개인정보라고 하더라도 정보주체의 동의 없이는 인공지능 학습데이터로 사용할 수 없음.

- 그럼에도 규제완화 또는 규제혁신이란 이름으로 개인정보 원본을 마치 공유재처럼 특정 기술의 발전을 위해 마음대로 쓸 수 있도록 법개정을 하겠다는 것은 헌법으로 보호받는 개인정보자기결정권을 침해하는 것이며, 개인정보보호법의 기본원칙을 무너뜨리는 것임. 무엇보다 인간의 존엄성이나 인격의 내적 핵심, 내밀한 사적 영역에 근접하는 민감한 개인정보를 포함하여 개인정보는 한 인간의 프라이버시를 구성하는 주요 요소이고 “프라이버시는 인간에게 필수적이며 세상과 관계 맺는 방식을 통제하는 인간 능력의 중심요소”라는 사실을 무시한 것임.
- 정보주체 동의 없이 원본 데이터의 활용을 명시적으로 허용하는 법규를 두고 있는 국가는 세계적으로 거의 없음. 인공지능 개발과 활용에서도 개인정보보호라는 기본적인 인권 보호가 중요하다는 원칙이 중요하다는 사실에 공감하기 때문일 것임. 2023년 54차 유엔 인권이사회 정기회기에서 만장일치로 채택한 <디지털 시대의 프라이버시권(Right to privacy in the digital age)>(A/HRC/RES/54/21 (2023년 10월 16일))에 따르면 회원국인 각국 정부가 프라이버시에 대한 간섭을 할 경우 합법성, 필요성, 비례성의 원칙에 부합하여야 함을 천명함. 따라서 인공지능기술 발전을 위해 원본 개인정보를 활용하기 위해서는 고도의 합법성, 필요성이 입증되어야 하며 또한 침해되는 권리와 목적을 통해 얻고자 하는 바가 비례적이어야 함.
- 인공지능 기술발전을 위한 학습을 위해 개인의 인격권 등을 포기하라는 것은 60,70년대 산업성장을 위해 인권을 희생시키던 권위주의 정부에서나 가능한 발상임.
- 2025년 한해에만 SKT 2300만명,롯데카드 297만명, 쿠팡 3370만명, 신한은행 19만 가맹점주 정보유출 등 내로라하는 대기업들조차 대규모 개인정보유출사고가 끊이지 않고 일어났음. 해킹에 의한 유출뿐 아니라 내부관련자 등에 의한 유출로 밝혀진 경우도 많음. 이런 상황에서 안전조치인 가명처리조치 하지 않은 개인정보 원본을 AI 학습 등에 활용하도록 하는 내용을 개인정보보호법에 담겠다는 것이야말로 개인정보보호위원회의 역할에 대한 주객전도가 아닐 수 없음.
- 이재명 대통령도 대규모 개인정보 유출에 대해 강력한 재발 방지 대책을 주문하고 있고 개인정보보호위도 이번 쿠팡을 비롯한 SKT, KT, 롯데카드 등의 대규모 개인정보 유출 사고의 재발을 방지하겠다고 천명하고 있음. 그런데도 오히려 개인정보 원본을 기업들에게 이용할 수 있도록 하는 법개정에 나서는 것은 앞뒤가 맞지 않음. 쿠팡과 같이 거대 플랫폼 기업들이 보유하고 있는 고객 개인정보는 수천만 건에 달하고 개인정보보호위가 전력 추진하고 있는 개인정보 원본활용을 법에서 허용한다면 가명처리조치 되지 않은 구매정보, 병원·약국 이력 등 건강 정보, 얼굴·음성·걸음걸이·지문 등의 생체인식정보 등 민감정보까지 원본 그대로 원래 수집 목적 외로

정보주체의 동의도 받지 않고 인공지능기술개발 등을 위해 이용될 것임. 오히려 인공지능 기술의 발전으로 대량의 데이터를 실시간으로 수집하여 처리할 수 있고, 이를 바탕으로 개인의 위치, 취향, 행동 패턴 등을 분석하는 등 프로파일링이 쉽게 이루어지고 있는 지금 정작 필요한 것은 정보주체가 자신의 정보가 인공지능산업을 위해 무분별하게 활용되는 것을 거부할 수 있도록 하고, 자신에 관한 정보를 스스로 통제할 수 있는 권리를 강화하는 것임.

- **[수정 요구] AI 학습·평가 목적의 저작물 활용 및 유통 생태계 활성화 위한 저작권법** 개정에서 실질적인 의견수렴과 사회적 합의과정이 반드시 필요함. (액션플랜 32)

[제안 이유]

- AI 학습·평가 목적의 유통을 진행하려고 할 때 이와 관련한 기존 저작물 제작·유통 과정의 권리관계의 불명확성 해소를 위해 정부 차원의 지원이 필요하다는 데는 공감함. 단, 주요 이해관계자들의 실질적인 의견수렴과 사회적 합의과정이 반드시 필요함.
- 과기정통부는 독자 AI 파운데이션 모델, 오픈소스를 지향하는 민간 주도의 AI 파운데이션 모델 등 AI 생태계 확산 및 사회적 이익 증진 등을 위한 AI 서비스 개발의 경우 법적 불확실성 없이 AI 학습 목적으로 저작물을 활용할 수 있도록 하는 내용을 담은「AI기본법」개정안 혹은「AI특별법」제정안을 '26년 2분기까지 마련할 계획은 또한 매우 신중해야 함. 당연히 문체부의「저작권법」개정 상황을 고려하여 추진하여야 하지만 사회적 이익증진이라는 포괄적이고 추상적 개념을 이유로 저작물 활용을 허용하는 것은 면밀한 검토와 이해 관계자의 폭넓은 의견 수렴과 토론을 거쳐 이루어져야 할 것임.

- **[수정 요구] AI 법제 환경 조성, AI기본법 하위법령 및 가이드라인 보완은 이용자, 이용사업자, 영향받는 자의 정의를 명확히 하고 관련 의무와 권리를 명확히 명시해야 함. (액션플랜 34)**

[제안 이유]

- 인공지능을 “업무 목적으로” 이용하여 영향받는 자에 대하여 직접적인 영향을 미치는 병원, 채용회사, 금융기관 등 사업자를 ‘이용사업자’에 포섭하여 합당한 책무를 지도록 시행령에 명확히 규정할 것을 포함하여야 할 것임. 지난 11. 16. 입법예고된 시행령안에는 이에 대한 규정이 없으나 가이드라인에는 전체적으로 병원, 채용회사, 금융기관 등 인공지능 제품이나 서비스를 업무에 사용하는 사업자를 모두 ‘이용자’로 보고 일체의 책무를 배제함.
- 참고로 유럽연합 인공지능기본법의 ‘배치자(deployer)’에 해당하는 개념이 우리 인공지능법에서는 ‘이용사업자’와 ‘이용자’로 나뉘며, 고위험 인공지능의 경우

이용사업자에게는 책무가 부과되지만, 이용자에게는 책무가 부과되지 않는 차이가 있음. 우리 인공지능법 제2조(정의)에서는 이용사업자는 제공사업자가 “제공한 인공지능을 이용하여 인공지능제품 또는 인공지능서비스를 제공하는 자(법 제2조 제7호)”이며, 이용자는 “인공지능제품 또는 인공지능서비스를 제공받는 자(법 제2조 제8호)”임. 이에 따라 자칫 병원, 채용회사, 금융기관 등 인공지능을 업무 목적으로 이용하여 영향받는 자에게 영향을 미치는 경우는 합당한 책무를 지도록 명확화 하여야 할 것임.

- 또한 인공지능법 제3조 제2항에서 영향받는 자의 설명요구권을 규정하면서 이에 대한 구체적인 조항을 규정하지 않고 있음. 법에서 권리는 명확하게 규정하고 있으므로, 시행령을 통해서라도 이를 이행할 수 있는 방안을 구체화하는 방향으로 보완되어야 할 것임

- **[수정 요구]** 각주에서 밝힌 ③ 이용사업자의 (특히 운용 과정의)의무 완화, ④ 서류 작성 의무 간소화는 반대함. (액션플랜 34)

[제안 이유]

- 인공지능법의 유일한 책무규정은 법 제34조 고영향 인공지능사업자의 책무임. 그런데 법 제2조(정의)에서 인공지능사업자는 인공지능개발사업자와 인공지능이용사업자로 구분되지만, 법 제34조는 이를 구분하지 않고 있음. 또한 지난 12. 16. 입법예고된 시행령(안)에서 조치 이행의 방법을 규정한 제1항 역시 조치의 내용에 따른 주체의 구분없이 인공지능사업자로만 규정하고 있음. 따라서 법에서 규정한 책무를 인공지능 개발사업자와 이용사업자 중 누가 이행을 해야하는지 명확하게 규정하여 수범자를 명확히 해주어야 함.
- 또한 인공지능사업자가 취해야 할 6가지 조치의 구체적인 ‘이행 방법과 절차’를 대통령령으로 위임하고 있으나 11.16. 입법예고된 시행령안에 구체적인 내용이 없음. 오히려 이용사업자가 조치의무를 이행한 것으로 간주되는 경우를 폭넓게 규정하여 법의 위임 범위를 벗어나고 있음. 시행령안은 개발사업자로부터 조치의 모두 또는 일부를 이행한 인공지능시스템을 제공받는 이용사업자가 ‘중대한 기능 변경을 초래하지 않은 경우’ 이용사업자의 조치의무를 면제하고 있음. 인공지능기술을 이용한 제품·서비스를 제공할 때 개발사업자와 이용사업자의 역할과 개별 단계에서 요구되는 조치의 내용은 다름. 따라서 원칙적으로 모든 인공지능사업자가 개별 단계별로 법 제34조의 내용을 준수하여야 함에도 시행령(안)은 일방적으로 이용사업자의 조치의무를 면제하고 있고, 그 요건조차 일부 이행으로 축소하고 있으며 심지어 ‘중대한 기능 변경을 초래하지 않은 경우’라고 추상적인 개념을 사용하여 조치의무 면제 범위를 더 넓힘. 이는 사실상 이용사업자의 조치의무를 전부 면제하는 내용임. 따라서 시행령안 조치의무 면제 요건은 모두 삭제하여야 함. 만약 이용사업자의 책무 면제 요건을 둔다면, 법에서 정한 모든 조치를 이행한 인공지능시스템을 제공받은

이용사업자로 하고, 기능변경을 초래하지 않는 경우에 한해서로 조건을 강화하는
방향이어야 할 것임.

- 문서는 안전사고나 인권침해 발생시 사실조사를 하거나 피해구제를 위하여 매우
중요한 사항이므로 반드시 작성하고 최대한 자세히 작성, 보관 의무를 두어야 함.
채무불이행에 따른 손해배상책임의 소멸시효가 10년을 감안 보관의무 기간은
10년으로 하는 것이 적정함.
- **[수정 요구]** 업무목적으로 AI 활용하는 이용자는 이용사업자로서 투명성 의무
명확화해야 함. (액션플랜 34)

[제안 이유]

- 인공지능법 제31조는 인공지능기본법에 대한 국회 법안심사과정에서 딥페이크
성폭력물에 대한 사회적 우려와 대책을 반영하는 취지에서 마련된 바 있음. 특히 법
제31조 제2항과 관련이 있는 생성형인공지능의 결과물로 인하여 “실제하지 않는”
허위조작정보, 소비자기만 마케팅, 보이스피싱으로 인한 이용자 오인이나 사기 피해가
발생하고 있음. 인공지능법 제31조 제3항은 “실제”와 구분하기 어려운 딥페이크
생성물을 특별하게 규제하는 것임.
- 무엇보다 큰 문제는 인공지능법 제31조 제3항은 딥페이크 영상과 같이
"인공지능시스템을 이용하여 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상
등의 결과물을 제공하는 경우 해당 결과물이 인공지능시스템에 의하여 생성되었다는
사실을 이용자가 명확하게 인식할 수 있는 방식으로 고지 또는 표시"하도록 하고
있는데, 지난 11/16. 입법예고된 시행령안에는 실제 AI 시스템을 이용하는 당사자를
이용자로 규정하여 이러한 고지 또는 표시를 해야 하는 주체가 없음. 즉, AI 시스템을
제공하는 인공지능사업자는 영상을 제작하는 주체가 아니므로 이러한 의무를
부담하지 않고, 실제 딥페이크 영상을 제작하는 사람은 이용자로 규정하여 의무
대상에서 배제하고 있는 것임. 따라서 법상 의무를 이행해야 할 주체가 모호해지는
상황이 발생함. 이런 측면에서도 AI 시스템을 이용하여 영상 등을 제작하는 주체를
이용사업자로 규정하여 의무를 부여하는 것이 타당함. 따라서 실제 AI 시스템을
이용하여 딥페이크물을 제작하는 주체가 이용사업자로서 투명성 확보 의무를 지도록
하위법령 등에 명확히 규정하여야 할 것임.

‘공공AX’ 분야 - 공공성·책임성 강화해야

1. 액션플랜 번호

50. AI-Native한 공무원 협업체계 구축
51. 칸막이를 넘어 데이터와 맥락을 연결하는 AI 업무관리 플랫폼 구축
52. 공공 정보화 사업, 민간 클라우드로 전환
53. 세계 1위 AI정부 도약 견인, 공공분야 AI챔피언 양성
54. 공공부문 AI 도입에 대한 국민 기본권 보장, 공공 AI 영향평가
55. 안전한 AI이용 보장, 공공부문 AI 윤리기준 마련
56. 공공 AI 대전환 가속화, 적극행정 인센티브와 감사 면책 마련
57. 공공AX 정책의 성공적인 실행을 위한 성과 평가 시행
58. AI를 활용한 최고의 대국민 서비스 제공
59. 행정/사법 투명성 증대를 위한 공공데이터 공개
60. 교사 지원형 AI 보조교사 및 교육행정 AI 확산
61. 국내 AI실증·고도화의 마중물, 공공시장의 AI 테스트베드화
62. K-Gov AX 모델의 글로벌 확산, K-AI 얼라이언스 구성
63. 공공AX 거버넌스 및 실행체계 구축

2. 수정 요구 및 제안 이유

- **[수정 요구]** AI-Native한 공무원 협업체계 구축 / 지능형 업무관리 플랫폼 활용 전에 해당 AI 시스템이 의도한 기능을 제대로 수행하는지, 편향이나 차별적 결과를 드러내지 않는지, AI를 활용하는 공무원의 직무와 업무 역량에 어떠한 변화를 야기하는지 충분한 검토를 하기 위하여 시행 대상 및 기간에 있어서 시범시행을 하도록 해야 하며, AI 시스템에 전적으로 의존하는 것은 자제해야 함. (액션플랜 50)

[제안 이유]

- 과연 현재의 기술 수준에서 AI에 업무를 전적으로 의존하는 것이 합당한지 의문임. AI의 요약이나 추천이 적절한지, AI에 의존하고 원문을 검토하지 않았을 때 문제가 생길 가능성은 없는지, 담당자의 업무 역량을 오히려 약화시키는 것은 아닌지 등에 대해 충분한 연구가 이루어지지 않았음. 업무에 대한 지적, 경험적 역량의 강화없이 AI 활용 역량도 강화될 수 없는데, AI에 대한 의존은 사람의 지적, 경험적 판단 역량을 저해할 수 있다는 점에 대한 고려도 필요함.
- **[수정 요구]** 칸막이를 넘어 데이터와 맥락을 연결하는 AI 업무관리 플랫폼 구축 / 지능형 업무관리 플랫폼, 범정부 AI 공통기반, AI 통합 워크스페이스 등의 구축 과정에서 부처별 개인정보 및 데이터의 책임기관이 명확하게 설정되어야 하며, AI 학습을 통해 권한이 없는 타 기관에 노출되지 않도록 주의해야 함. 개인정보 및

데이터를 타 기관에 제공, 공유할 때에는 법적 근거나 정보주체의 동의가 있어야 함.
(액션플랜 51)

【제안 이유】

- 부처간 연계는 단순히 기술적인 문제일 수는 없음. 데이터의 접근 및 통합 범위 등이 엄격하게 정의되어야 함. 자칫하면 통합이라는 명분하에 특정 데이터가 권한 범위를 넘어서 공유되어서는 안됨. 특히, AI를 사용할 경우 AI 학습 과정에서 서로 다른 부서의 데이터가 섞일 수 있고, 의도하지 않게 권한 범위를 넘어서 타 부처의 활용 과정에서 노출될 수 있기 때문에, 이러한 문제는 더욱 복잡해질 수 있음.
- **【수정 요구】** 공공 정보화 사업, 민간 클라우드로 전환 / 정부·공공기관에서 정보화 사업 추진 시 민간 클라우드 이용 검토를 의무화하는 것은 과도하며, 오히려 민간 클라우드를 사용할 경우 국가 안보, 정보 보안, 특정 기업 종속, 효과적 감독을 위한 요건 등을 엄격하게 규정해야 함. (액션플랜 52)

【제안 이유】

- 민간 클라우드 이용의 장점만을 언급하는 것은 부적절함. 오히려 정부 시스템을 민간 클라우드로 전환할 경우 다양한 문제에 봉착할 수 있음. 예를 들어, 민간 클라우드를 사용하면 계약상 통제장치를 마련하더라도 민간의 당사자가 기술적으로는 얼마든지 데이터에 접근할 수 있으므로 보안에 허점이 발생할 수 있음. 따라서 엄격한 정부 시스템을 보안 필요성에 따라 구분하고 보안이 필요한 시스템일수록 민간 클라우드 사용을 지양해야 함. 또한, 정부 시스템은 감독기관의 감사가 가능해야 하는데, 민간의 영업비밀이 투명한 감사에 방해되지 않을 수 있는 요건을 갖추어야 하며, 기존의 감독기관이 민간 클라우드를 감독할 수 있는 기술적 역량을 갖추었는지 등도 확인이 필요함. 정부 시스템이 특정 기업의 서비스에 종속될 우려가 없도록 고려가 필요함.
- **【수정 요구】** 공공부문 AI 도입에 대한 국민 기본권 보장, 공공 AI 영향평가에 대해 ▲국민 기본권 보장을 위해 AI의 결과물이 설명 또는 해석가능하지 않는 경우 해당 AI 시스템을 도입하지 않는다는 원칙을 분명히 해야 함, ▲공공 AI 영향평가를 할 때에는 영향을 받는 당사자의 의견을 반드시 수렴하도록 하며, 영향평가의 결과는 공개되어야 함, ▲영향평가 뿐만 아니라, 공공부문 AI 등록제를 시행하고 주요 내용을 공개해야 함, ▲AI 시스템을 조달할 때 공공 AI 영향평가를 시행하는 등 위험성 평가를 의무적으로 수행할 것을 규정해야 함.▲ 정부·공공기관에서 정보화 사업 추진 시 민간 클라우드 이용 검토를 의무화하는 것은 과도하며, 오히려 민간 클라우드를 사용할 경우 국가 안보, 정보 보안, 특정 기업 종속, 효과적 감독을 위한 요건 등을 엄격하게 규정해야 함. (액션플랜 54)

[제안 이유]

- 공공기관의 업무는 투명성, 책무성을 기본적으로 담보해야 하며 **AI**를 활용한다고 예외가 될 수 없음. 따라서 **AI**가 산출한 결과물에 대해 영향을 받는 당사자에게 설명할 수 없는 경우, 이러한 **AI**를 도입해서는 안됨.
- 영향평가에는 영향받는 사람의 참여가 필수임. 이는 유엔 인권실사(인권영향평가를 포함한)의 기본적인 원칙이며, 또한 바이든 행정부의 인공지능 행정명령의 이행 지침에서도 공공부문 **AI**에 대한 영향평가를 할 때 영향받는 자와의 협의를 강조하고 있음. 또한 영향평가가 형식화되지 않고 실질적인 의미를 지니기 위해서는 그 결과가 투명하게 공개되어야 함.
- 공공부문 **AI** 등록제는 공공부문 **AI** 시스템 현황 파악을 통해 중복 투자를 방지하고, 그 내용을 국민에게 공개함으로써 기관의 투명성을 강화할 수 있음.
- 공공 **AI** 영향평가를 조달 과정에서 필수적으로 수행하도록 조달 절차 및 정책에 반영할 필요가 있음.

- [수정 요구] 안전한 **AI**이용 보장, 공공부문 **AI** 윤리기준 마련 / 「인공지능기본법」과 그 시행령을 반영한 **AI** 윤리기준이 아니라, 공공부문의 안전성, 투명성, 설명 가능성, 책임성을 보장하기 위한 법제 개선이 필요하며, 그에 따른 공공부문 **AI** 도입 지침이 마련되어야 함. (액션플랜 55)

[제안 이유]

- "정부는 공공 **AI** 시스템의 설계부터 운영·평가에 이르는 전 과정에서 안전성, 투명성, 설명 가능성, 책임성을 보장하는 체계를 구축해야 한다"는 것에 공감함. 다만, 그것은 자율적으로 준수하는 윤리 지침이 되어서는 안되며, 법에 근거한 의무 규정이 되어야 함. 또한, 현행 인공지능 기본법 및 시행령은 공공부문의 안전성, 투명성, 설명 가능성, 책임성을 보장하는데 미흡하므로, 상위법 자체가 '54. 공공부문 **AI** 도입에 대한 국민 기본권 보장, 공공 **AI** 영향평가'의 제안 내용까지 포함하여 개정되어야 함.

- [수정 요구] 공공 **AI** 大 전환 가속화, 적극행정 인센티브와 감사 면책 마련 / 국민의 기본권에 큰 영향을 미치는 사업에는 면책을 배제하고, 면책 범위를 기술적 시범 서비스에 한정해야 함. (액션플랜 56)

[제안 이유]

- 감사 면책이 행정 책임성을 회피하는 수단이 될 수도 있음. 따라서 일괄적으로 면책을 하는 것이 아니라 기본권에 영향이 큰 사업은 면책을 배제하고, 기술적 시범 서비스 도입 등에 한정할 필요가 있음.

- **[수정 요구]** 교사 지원형 **AI** 보조교사 및 교육행정 **AI** 확산 관련해 ▲**AI** 보조교사(튜터) 서비스 도입 전에 학교에 충분한 인력을 제공하고 있는지 검토 필요하며, ▲학생 데이터를 활용한 민간 기업의 영리 행위를 엄격히 금지하고, 교육용 **AI** 도입 시 학부모와 학생의 '명시적 동의'를 필수 절차로 포함해야 함. (액션플랜 60)

[제안 이유]

- 학교에서 **AI**의 활용이 항상 교사들을 지원하는 것은 아니며 오히려 교사들에게 부담이 될 수도 있음. 교사들이 과도한 업무에 시달리고 있다면 **AI**가 아니라 충분한 교사 인력을 지원하는 것이 먼저임.
- 학생 개인정보가 민간 에듀테크 기업 활성화를 위한 먹잇감이 되어서는 안되며, 교육부문 **AI** 도입 전에 학생 개인정보보호를 위한 엄격한 체계 마련이 필요함.

- **[수정 요구]** 공공**AX** 거버넌스 및 실행체계 구축 / 효율성 중심의 공공 거버넌스를 이해관계자의 민주적 참여에 기반한 거버넌스로 재편해야 함. (액션플랜 63)

[제안 이유]

- "갑을병정으로 이어지는 하청구조와 단기 계약직 중심의 개발, 일정 기간마다 교체되는 운영사 시스템"이 **AI**를 도입한다고 해결될리는 만무함. **AI**를 도입하면서 여전히 효율성 중심의 거버넌스를 유지한다면 근본적인 관료적 구조를 얼마나 개편할 수 있을지 의문임. 단지 **CTO**와 같은 기술전문가가 중요한 것이 아니라, 공무원 노동조합 및 인권시민사회를 포함한 외부의 이해관계자를 비롯하여, 개인정보위, 인권위 등 공공기관의 감독기관도 거버넌스에 참여할 수 있도록 하는 것이 필요함.

‘문화·예술’ 분야 - 문화생태계 전반 아우르는 비전제시해야

1. 액션플랜 번호

- 69. AI 기반 콘텐츠 창작 지원체계 구축 및 창작자 생태계 활성화
- 70. K-컬처 산업의 AX 활성화 지원을 통한 콘텐츠 사업자 육성
- 71. AI 선도 적용으로 K-문화콘텐츠 산업의 지속적 성장 가능성 확보
- 72. K-콘텐츠와 K-AI의 동반 해외 진출을 통한 글로벌 시장 확대

2. 수정 및 제안

- **[수정 요구]** AI 기술 도입에 따른 창작생태계의 변화와 예술노동 종사자의 창작권, 노동권 보장을 위한 실태조사와 거버넌스 필요 (액션플랜 69)

[제안 이유]

- 초안에서 지적한 바와 같이 AI 기술의 도입은 창작생태계는 물론 콘텐츠 산업과 향유 환경에 지대한 영향을 미치고 있으며, 이는 예술 본연의 가치와 시민의 문화적 권리 전반을 뒤흔드는 중요한 변화를 예고하고 있음. 그러나 본 계획은 이러한 우려의 지점을 짚어내고는 있지만 이를 위한 정책적 과제는 창작도구 바우처 사업, 제작지원, 기술지원 등 AI를 ‘활용’하는 것에만 집중하고 있으며 변화 하는 기술 환경이 가져올 창작 생태계 내 주요 주체들의 권리 침해와 사회적 갈등에 대해서는 구체적인 대안을 제시하고 있지 못함.
- 최근 창작생태계 내에서 AI의 활용이 확대되면서 창작자의 창작물로부터의 소외 현상을 비롯해 창작노동에서의 생성물의 질이 점차 저하되는 ‘워크슬롭’ 현상과 AI 작업을 보완하는 과정에서의 창작자의 번아웃 문제까지 다양한 형태의 부작용들이 드러나고 있으며, 산업의 외형적 성장과는 달리 창작생태계 자체는 미래를 낙관하기 어려운 상황. 하지만 이러한 예술창작 현장의 예술노동 환경의 악화 등에 대한 정부 차원의 실태조사나 현장 이슈 파악은 전혀 이뤄지지 않고 있으며 이러한 논의를 진행할 수 있는 거버넌스 구조조치 만들어져 있지 못한 상황.
- AI 기술 도입을 통해 안전하고 지속가능한, 보다 창의적인 창작생태계를 만들기 위해서는 창작자 권리 보호를 위한 가이드라인 마련, 정기적인 실태조사를 통한 정책 조율, 현장 창작자의 참여가 보장되는 거버넌스의 구축이 필요.

- **[수정 요구]** 콘텐츠 사업자 중심의 성장 모델이 아닌 **AI** 기술 기반의 문화산업 생태계에 대한 통합적인 계획과 미래 비전의 필요 (액션플랜 70,71)

[제안 이유]

- 초안에서 제시하고 있는 70,71번 과제는 사실상 사업자 중심에서의 공급형 산업 촉진 정책에 가까운 내용으로 AI 기술에 따른 사회변화와 기술적 특징을 충분히 고려하지 못한 채 기존의 산업진흥 정책의 AI 버전이라고밖에 평가할 수 없음. 이러한 계획은 오히려 AI 문화산업 생태계를 닫힌 구조로 만들어 변화와 혁신 없는 K-컬처, K-콘텐츠라는 갈라파고스형 정책으로 귀결될 가능성이 큼.
- 지속가능한 AI 문화산업 생태계는 창의력의 원천으로서의 예술생태계와 창작자, 이를 기술적으로 지원할 수 있는 R&D 구조, 다양한 형태의 혁신적 실험들을 가능케하는 재정지원 구조와 마지막으로 기존의 소비자, 향유자가 아닌 이용자이면서 동시에 창조자의 역할을 하는 대중과의 소통과 교감의 구조를 한데 아우르는 통합적인 산업 생태계에 대한 비전이 필요. 정부 정책의 역할을 이러한 생태계 안에서의 선순환을 만들어내기 위한 조율과 통화, 연결과 촉진의 구조를 만들어내는 것이며 이는 사업자 중심의 기술, 재정 지원만으로는 이뤄지기 어려움.
- 특히 이 과정에서 AI 기술 도입을 통해 발생 할 수 있는 창작자, 산업 분야 노동자, 수용자에게 미칠 수 있는 부정적 영향들에 대한 평가와 준비가 과소 평가되어 있는데 특히 산업분야 노동자들의 경우 AI 기술 도입으로 인한 실직에 대한 위기 의식이 높아진 상황이며, 딥페이크 류의 AI 콘텐츠 범람으로 인한 수용자의 혼란과 사회적 갈등에 대해서도 그 위험성이 과소평가 되어 있는 상황.
- 지원과 증진이나 규제나 하는 이분법적인 정책 구도에서 벗어나 전체 생태계를 통합적으로 아우르며 건강하게 지속가능한 문화산업 생태계가 형성될 수 있도록 정책의 방향을 수정할 필요가 있으며, 특히 AI 기술도입이 가져올 전체 사회변화와 연동하여 문화, 예술 분야에 국한된 정책 계획의 수립이 아닌 보다 통합적이며 전체 사회 과제와 연결되는 정책적 시야를 확보할 필요가 있음.

‘AI기본사회’ 분야 - 사회적 합의부터 도출해야

1. 액션플랜 번호

80. 「모두를 위한 AI 기본 사회 추진계획」 수립
81. AI 기본 사회 추진 거버넌스 마련
82. 모두의 AI를 위한 AI 윤리 확산·고도화
83. AI 공론장 설계 및 운영
84. AI를 활용한 사회문제 해결을 위해 ‘모두의 AI 실험실’ 구축
85. AI 기본 사회 글로벌 얼라이언스 구성
86. AI 시대 생애 경제 통합 전략 마련
87. AI 전환 대응 일자리 혁신 및 현장 역량 강화
88. AI 시대 정밀복지·돌봄의 접근성 확대
89. AI 기본 의료의 구현
90. AI 범죄 근절 및 대응 역량 강화
91. 국민 금융 안전 제고 및 AI 기반 포용적 금융안전망 구축
92. 전 국민 AI 역량 대전환 프로젝트
93. 지역·계층 간 AI 교육격차 해소를 위한 지원체계 강화
94. 민관 협력형 AI 교육정책 연구체계 구축
95. 교육 AI서비스의 품질과 안전성을 위한 실증·평가·확산체계 구축

2. 수정 요구 및 제안 이유

- **【수정 요구】** 국제인권규범 및 헌법상 기본권을 기준으로 한 ‘인권 기반’ 원칙(예: 차별금지, 데이터 권리, 절차적 권리)를 명시하고, 고위험 AI 규제·인권영향평가·취약계층 보호에 관한 구체성을 보완할 필요가 있음. 또한 실질적인 시민참여형 거버넌스 구축을 위하여 인공지능에 영향을 받는 노동자, 금융취약계층, 장애인, 이주민 등이 정책 설계·평가 단계에 구조적으로 참여하도록 보장해야 함(액션플랜80)

【제안 이유】

- 이 추진계획은 AI 기술 발전의 혜택을 모두에게 분배하겠다는 방향성 자체는 긍정적이지만, 인권 기반 관점에서 통제·참여·구제 장치가 매우 추상적인 문제가 있음. 국가인권위와 시민사회는 이미 인공지능 정책에 인권영향평가와 권리구제 체계를 결합해야 한다고 반복해서 권고해왔음.
- 또 시민참여형 거버넌스 구축이 언급되지만, 실제로는 AI 정책이 전문가·정부 중심으로 설계되고 당사자·취약계층은 절차적 참여를 충분히 보장받지 못한다는 비판이 계속 제기되어왔던 점을 고려하여 실질적으로 인공지능의 영향을 받는자가 참여하는 구조를 설계할 필요가 있음.

- **[수정 요구]** 공익데이터 및 공익**AI**의 법적 지위는, 민주적 정당성을 부여받은 국회 입법을 통하여 국민의 여론 수렴 과정을 거쳐 명확화·제도화 할 필요가 있음. 인권영향평가의 제도화·권리구제 절차의 내재화·당사자 참여형 거버넌스 설계가 필수적으로 이루어지도록 보완이 필요함. 시민사회는 기술 진흥 부처인 과기정통부 외에 국가인권위, 개인정보보호위, 공정위 등 인권·데이터·시장 감시 기관이 함께 참여하는 **AI** 규제·감독 협의체 및 독립적 감독기구를 설치할 필요 있음 (**액션플랜 81번**)

[제안 이유]

- 국가인권위는 인공지능 정책·사업에 인권영향평가와 피해구제 체계를 결합할 것을 공식적으로 권고했으나, 현재 계획 문구에는 ‘어떤 위험을 어떤 기준으로 통제하고, 침해 시 어떤 절차로 구제할 것인지’가 구체화되어 있지 않음.
- 영향받는 자 및 인권침해 위험에 직접 노출되는 집단이 정책·사업 전 과정에서 구조적으로 참여하도록 설계할 필요가 있으며, **AI** 관련 다기관 협의체와 참여하는 독립적 감독기구 설치를 고려하는 것이 바람직함.

- **[수정 요구]** 윤리기준을 인권기준으로 재정의하여, 헌법상 기본권·국제인권 규범 (**UNESCO 권고, OECD AI 원칙 등**)을 명시적 해석 기준으로 삼는 ‘(인권)권리기반 **AI** 기본원칙’을 추가해야 함. 자율점검표를 ‘선언적 체크리스트’가 아니라, 공적 감독·책임과 연동되는 의무적 평가도구로 재설계할 필요 있음(**액션플랜 82번**)

[제안 이유]

- 현행 「인공지능 윤리기준」은 인간 존엄성, 인권보장, 프라이버시 보호, 다양성 존중 등을 3대 원칙·10대 요건 형태의 ‘윤리 선언’으로 제시하지만, 구속력 있는 권리·의무 규범은 아님. 따라서 윤리기준을 인권 권리 기준으로 재정의하고 ‘권리기반 **AI** 기본원칙’을 강조할 필요 있음
- 개발·이용 사업자가 **AI** 개발 생애주기 전반을 스스로 점검하는 자율 점검표 고도화를 핵심 수단으로 상정하고 있으나 인권침해 문제에는 위험축소와 비용·이윤 사이의 이해상충이 존재하기 때문에, 기업 내부의 자율 점검만으로는 프라이버시 침해, 차별, 감시, 노동권 침해 등 고위험을 통제하기 어렵고, 피해자에게 실질적 보호 수단도 제공하지 못함.

- **[수정 요구]** 공론장 참여 구조, 의제 설정, 권한 배분, 책임·구제 장치에 **AI** 영향을 받는 집단과 인권 시민단체의 실질적 참여권을 구체화하여야 함. 공론화 결과를 정책에 우선 반영한다는 추상적인 내용이 아니라, **AI** 활용 전·중·후 단계의 인권영향평가, 독립적

감독, 정보 접근권, 이의제기·중단 요구·손해배상 등 효과적 구제수단 등 정책 반영 내용을 구체화할 필요있음(액션플랜 83번)

[제안 이유]

- ‘국민 모두의 공론장’이라는 수사는 있으나, 실제 설계·운영 권한은 과기정통부·국가AI전략위·기업·전문가 등에게 집중될 가능성이 높고, 구조적 약자·인권 단체는 들러리로 소외될 위험이 큼.
- 또 제안된 구상은 참여의 깊이(의사결정 권한·비토권·동의권 등)를 전혀 구체화하지 않고 있어 문제가 있음.

- **[수정 요구]** 모두의 실험실 구축을 위한 공익데이터 개방에 대하여 공개대상정보의 범위와 공개 방식을 구체화하고, 데이터 처리시에 위험 관리 및 안전 조치를 충실히 할 것을 정책 권고 사항에 포함하여야 함(액션플랜 84번)

[제안 이유]

- 국민이 직접 AI를 활용해 시도하고 실패하고 개선해보는 사회적 실험의 장을 마련하고, 그 과정에서 축적한 경험과 데이터를 공유자산화하는 ‘모두의 실험실’을 2026년 3분기까지 구축한다고 하며, 공익데이터 개방을 정책권고사항에 포함시키고 있으나, ‘공익데이터’라는 용어만으로 그 대상과 범위가 불분명함. 정보의 집적은 재식별위험을 높임. 개인정보자기결정권이 부당하게 침해되지 않도록 위험관리 및 안전조치를 충실히 할 것을 정책권고 사항에 포함시킬 필요가 있음.

- **[수정 요구]** 원스톱 AI고용 서비스 체계의 일부로, 구인광고작성 - 채용확률·분석 - 인재추천 - 채용관리까지 원스톱 AI채용지원서비스를 2026년 4분기까지 완성한다는 계획은 전면 재검토가 필요하며, 수정되거나, 철회되어야 할 것으로 보임(액션플랜 87번)

[제안 이유]

- 인사, 고용 분야에서의 AI 도입은 투명성, 공정성, 차별 가능성 등의 측면에서 직업선택의 자유, 근로의 권리와 관련한 기본권에 미치는 영향이 크므로, 차별 위험 및 부정적인 영향을 초래할 가능성을 고려하여 도입 여부를 재검토하여야 할 것임
- 유럽연합 인공지능법에서도 채용, 승진, 해고, 성과평가, 모니터링 분야에 활용되는 인공지능시스템은 고위험으로 분류하고 있음, 아마존의 이력서 자동평가 시스템이 여성지원자의 이력서를 불리하게 평가한 사례, 페이스북이 채용공고를 성별고정관념을 강화하는 방식으로 노출한 사례 등 고용 분야에서 AI가 도입되어 문제된 사례가 존재함

- 투명성, 공정성을 확보하고, 데이터의 품질 관리, 인간의 감독 등 안전장치가 충실히 마련되기 이전에는 도입되어선 안될 것임.
- **[수정 요구]** 검토배경 중 ‘AI 기반 정밀 예측’에 대한 그 분석 방법 및 방향성 등에 대한 검토가 필요하며, 사회위험 조기 감지 및 자살·고립·정신건강 문제 예방에 대한 구체적인 방안 제시할 필요함. ‘AI와의 상호작용 확대에 따른 정서적·심리적 부작용 예방과 국민 정신건강 보호체계 마련’ 구체화가 필요함. 고령층 및 장애인 등 AI·디지털 리터러시에서 소외된 계층에 대한 접근성 강화 방안이 마련되어야 함(액션플랜 88번)

[제안 이유]

- 정신건강·돌봄 데이터는 민감성이 높은 개인정보로, AI 시스템이 이를 수집·분석·저장하는 과정에서 프라이버시 침해 가능성이 높으며, 수집된 개인정보를 토대로 특정 집단에 대한 편향적·차별적 판단을 할 위험성이 상당함. 따라서 원안과 같이 AI를 활용하여 ‘선제적 개입’을 통해 ‘사회위험을 조기 감지’하고자 하는 목표는 그 자체로 매우 위험하며, 최소한의 가이드라인이라도 제시되어야 함
- 최근 청소년 자살 사건에서 생성형 AI와의 대화가 결정적인 영향을 미쳤다는 이유로 소송까지 제기되고 있음¹. 이러한 사례를 고려할 때 AI를 활용해 자살과 사회적 고립을 예방하고자 하는 체계를 구축함에 있어서는, AI와의 상호작용 과정에서 발생할 수 있는 부정적 영향을 예방·차단하기 위한 방안 역시 그에 못지않게 중요한 과제로 다루어져야 함.
- 초안은 AI 복지·돌봄 혁신 로드맵 수립을 통해 예방형 복지 모델을 구축하고자 하나, 이를 위해서는 먼저 AI 접근에 취약한 고령·장애인 등 소외계층에 대한 체계적인 리터러시 교육이 선행되어야 함. AI 로드맵을 통해 어떤 개인정보가 활용되는지, 개인정보 활용으로써 발생하는 효과는 무엇인지, 그 위험성은 무엇인지 전체적인 정보 제공이 반드시 필요함.
- **[수정 요구]** 편중된 데이터 및 모델에 기반한 진단 오류 가능성 명시 및 책임소재에 대한 대안을 마련하여야 함. 대량의 건강정보를 수집·활용하는 과정에서 데이터 유출, 국가기관에서의 악용, 사이버 공격 등을 사전에 예방할 수 있는 체계를 구축하여야 함. 팬데믹을 대비하기 위한 ‘AI 건강 정보 제공 체계’에는 편향된 데이터 수집으로 인해 감염병에 특히 취약한 계층(의료 접근성 낮은 지역, 미등록 이주민, 노숙인, 시설수용자 등) 배제 가능성에 대한 대안을 마련하고, 개인정보 수집에 따른 추적 가능성을 예방하기 위한 방향성을 제시해야 함(액션플랜 89)

¹ BBC(2025. 8. 27.) Parents of teenager who took his own life sue OpenAI
<https://www.bbc.com/news/articles/cgerwp7rdlvo>

【제안 이유】

- 의료AI는 주류 집단의 데이터를 편향적으로 수집함으로써 규범 바깥에 존재하는 사회적 소수자에 대한 왜곡된 진단을 할 가능성이 존재하며, 건강에 중대한 영향을 미칠 수 있으므로 이에 대한 대안 마련은 필수적임². AI 제공자 및 이용자간 책임소재가 사전에 명확히 규정되지 않는다면 AI 기본 의료 체계 추진에 대한 전면 재검토가 필요함
- 건강 정보에는 생체정보, 병력, 유전체 정보 등 민감성이 매우 높은 정보를 포함하고 있는 바, 개인의 생명과 존엄에 직결되는 정보이므로 AI 기본 의료 체계에 앞서 선행적으로 강력한 보호체계를 마련해야 함
- 팬데믹 예방체계와 같이 감염병에 대한 전수조사 및 데이터 수집 활용이 이루어지는 경우 그 대상에서 배제되는 계층과의 의료서비스 격차는 더욱 확대되므로 이를 예방하기 위한 방안을 미리 마련해야 함. 뿐만 아니라 코로나19 팬데믹에서도 경험하였듯 개인정보 수집에 따른 동선 추적 및 공개, 이로 인한 사회적 낙인과 차별에 대비해야 함
- 【수정 요구】 근본적 예방을 위한 성평등 관점에서의 체계적인 교육 체계가 마련되어야 함. 통신사, 금융회사, 플랫폼 사업자가 참여하는 AI 범죄 실시간 차단망 구축 뿐만 아니라 딥페이크 성범죄를 방지하고 조장하는 플랫폼 사업자에 대한 강력한 제재도 포함되어야 함(액션플랜90)

【제안 이유】

- 딥페이크 성범죄는 성차별적 권력 구조에서 발생하는 수많은 성범죄중 하나일 뿐이므로, 성차별 구조를 철폐해야만 근본적으로 해결될 수 있는 범죄임. 따라서 범죄 발생에 대한 예방, 사후 조치, 피해회복 뿐만 아니라 여성혐오적인 시각을 변화시킬 수 있는 교육체계가 마련되어야 함
- 웹하드 카르텔 등 이미 우리 사회는 디지털 성범죄 ‘산업’에 플랫폼 사업자가 적극적으로 개입하여 막대한 부를 축적하고, 성범죄를 방지 및 조장한 사실이 드러났음. 이에 초안과 같이 플랫폼 사업자가 AI 범죄를 차단하는 주체에만 국한되어서는 안되고, 강력한 제재 대상이 되어야 함
- AI 범죄 대책을 위하여국가와 민간사업자인 통신사·금융회사·플랫폼 사업자가 협업하는 “AI 범죄 실시간 차단망”의 필요성을 인정할 수 있으나 운용과정에서 통신의 비밀 등 국민의 기본권을 침해할 우려가 있으므로 권한 남용 방지를 위하여 시스템의 투명성과 통제 가능성이 확보될 수 있는 조치가 선제되어야 할 것임

² 조선일보(2025. 11. 27.), 백인 남성 데이터로 공부한 AI... 아동·희소병 환자는 잘 못본다
https://www.chosun.com/economy/tech_it/2025/11/27/R27R5FCDDDBBAGUHC4CGOQ25E/

- **[수정 요구]** AI기반 보이스피싱 및 스미싱으로 인한 피해가 막대한 상황에서 ‘AI 기반 금융 안전·포용 인프라 로드맵’ 조성시 금융정보 유출 및 활용에 대한 국민적 불안감이 증폭될 것으로 예상됨. 금융정보는 특히 유출 및 활용에 있어 가장 민감한 정보이므로 구체적인 방안이 마련되지 않는 이상 해당 액션 플랜은 추진이 유보되거나 철회되어야 함. (액션플랜91)

[제안 이유]

- 초안만으로는 AI를 활용해 보이스피싱 범죄를 어떻게 예방하고, 민생범죄를 어떠한 방식으로 탐지하여 금융안전망을 강화하겠다는 것인지 구체적으로 파악하기 어려움. 또한 대량의 금융정보를 처리·활용하는 과정에서 이를 어떻게 보호하고 통제할 것인지에 대한 대안도 전혀 제시되어 있지 않아, 전반적으로 위험성이 큰 계획임

- **[수정 요구]** 중·고등학교 뿐만 아니라 평생교육 차원에서 AI 기본역량 교육에 단순한 도구 활용이 아닌 기술에서의 인권 보호 및 권리 행사 등에 관한 내용이 AI 기본역량 교육의 내용 및 방안에 반드시 포함될 수 있도록 정책 권고안에 명시되어야 할 것임. (액션플랜92)

[제안 이유]

- 전 국민 AI 기본역량 교육의 확대에서 시민들이 AI윤리를 이해하여 AI 이용자로서 올바른 활용을 할 수 있도록 하는 것은 긍정적인 방향이라고 할 것임
- 그러나, 정책 권고사항의 내용에는 기본 역량 교육의 방향이 기본적인 기술 이해와 활용에 치우쳐 있음(예 : AI·디지털 학습 공간 운영 등)
- 따라서, 중·고등학교 뿐만 아니라 평생교육 차원에서 AI 기본역량 교육에 단순한 도구 활용이 아닌 기술에서의 인권 보호 및 권리 행사 등에 관한 내용이 AI 기본역량 교육의 내용 및 방안에 반드시 포함될 수 있도록 정책 권고안에 명시되어야 할 것임

- **[수정 요구]** 민관 협력형 AI 교육정책 연구에 교육당사자들의 실질적 참여와 사회적 공론화 반영의 거버넌스 구성이 보강되어야 할 것임(액션플랜94)

[제안 이유]

- 정책 권고안에서는 ‘국가 AI 교육 연구센터’를 설립하여 민간 에듀테크 기업과의 협력 모델을 구축하고 교육 AI 연구 생태계를 운영하도록 하고 있음
- 이러한 행동계획에 있어서 교육당사자의 의견과 사회적 공론화보다 사기업의 이익이 더 우선적으로 반영될 우려가 있음

- 따라서, 민관 협력형 AI 교육정책 연구에 교육당사자들의 실질적 참여와 사회적 공론화 반영의 거버넌스 구성이 보강 되어야 할 것임
- **[수정 요구]** 교육당사자들의 실질적 참여와 공론화 없이 교육 AI서비스 도입을 전제하여 충분한 사회적 논의와 준비없이 1년~2년 내 실질적 도입을 계획하는 것은 재검토가 필요하다고 할 것임(액션플랜95)

[제안 이유]

- 지난 번 AI교과서 도입 논란에서도 이야기 되었듯이 교육적 효과에 대한 검증이 부족한 상황에서 교육 AI서비스를 전면적으로 학교 현장 도입하는 것에 대하여 신중을 기할 필요가 있음
- 교육 AI서비스의 개념과 내용도 불분명하고 현재까지 어느 범위까지의 활용을 의미하는 것인지 사회적 합의가 이루어 지지 않은 상태임
- 현 행동계획안에서는 '27년 전까지 교육 AI서비스 시행을 계획하고 있음(교육 AI 규제샌드박스 시범운용 등)
- 교육당사자들의 실질적 참여와 공론화 없이 교육 AI서비스 도입을 전제하여 충분한 사회적 논의와 준비없이 1년~2년 내 실질적 도입을 계획하는 것은 재검토가 필요하다고 할 것임

인공지능 ‘영향받는 자’ 관련 - 액션플랜의 중심돼야

I. 학생·학부모·교사 등 교육 부문

1. 액션플랜 번호

- 17. 초·중·고 전학년에 걸쳐 연속적인 디지털·AI 교육 필수 이수
- 18. 초·중·고 AI 실습 교육 플랫폼 구축
- 19. 평가 제도 및 입시 제도 혁신
- 60. 교사 지원형 AI 보조교사 및 교육행정 AI 확산

2. 수정 및 제안

- **[수정요구]** 초·중·고교 공교육 시스템을 혁신하는 방향이 AI 핵심인재를 확충하는 생태계를 구현하는 것이 될 수는 없음 (전략분야 AI 핵심인재 확보)

[제안 이유]

- 초·중·고교 공교육 시스템을 혁신하는 방향이 AI 핵심인재를 확충하는 생태계를 구현하는 것이 될 수는 없음. 인간의 총체적인 발달을 위한 관점에서 인간이 자신의 잠재력을 펼칠 수 있는 기회를 보장하고 이를 실현하는 과정으로 공교육 시스템은 운영되어야 함. 단지 한 산업의 성패를 위해 공교육 시스템이 동원되어야 한다는 발상은 위험함.

- **[수정 요구]** 입시경쟁 교육을 철폐하고 자신의 가치를 스스로 발견하고 자신을 실현할 수 있는 교육으로 전환되어야 함. (액션플랜 15)

[제안 이유]

- 학생들이 스스로 지식을 탐색하고, 비판적으로 사고하며, 창의적으로 융합하여 새로운 가치를 창출하도록 하기 위해서는 학교 교육이 정상화되어야 함. 입시경쟁 교육을 철폐하고 자신의 가치를 스스로 발견하고 자신을 실현할 수 있는 교육으로 전환되어야 함. 하지만 교육이 AI 산업에 머무를 수는 없음. 좀 더 통합적인 인류의 발전 과정 속에서 고민되어야 함.

- **[수정 요구]** 국가교육과정의 개정은 충분한 검증과 숙의 과정이 필요함 (액션플랜 16)

[제안 이유]

- 국가교육과정은 여전히 약 7년 주기의 일괄 개정 체계를 유지하고 있어, 변화를 반영하기 어렵다는 것에 동의하지만 국가교육과정이 충분한 검증과 숙의 과정 없이

변경된다면 돌이킬 수 없는 문제를 발생시킬 수 있음. 적절한 속도와 방향을 가지고 진행될 필요가 있음.

- **[수정 요구]** AI가 학생의 정신적, 지적 역량 강화에 미치는 영향에 대한 고민(AI가 교육에 어떤 영향을 미치는지에 대한 본질적인 질문)이 선행되어야 함. (액션플랜 17, 18)

[제안 이유]

- '17. 초중고 전학년에서 연속적인 디지털·AI 교육 필수 이수'에서는 학생에게 디지털·AI 교육을 필수적으로 이수하도록 하고, '18. 초중등 AI 실습 교육 플랫폼 구축'에서는 실제 실습까지 할 수 있도록 하고 있음. 그런데 현재 대학에서도 AI 교육 때문에 교육 현장이 혼란에 휩싸여 있음. AI를 많이 사용하는 것이 실제 학생들에게 이로운 영향을 주는지, 오히려 정신 건강이나 지적 역량 강화에 부정적인 영향을 미치는 것은 아닌지, 또는 교육 현장에서 올바르게 사용하기 위한 방법은 무엇인지에 대해서는 아직 아무것도 정립되어 있지 않은 상황임. 따라서 무조건 학교 내에서 AI에 대한 교육을 강화할 것이 아니라, 학생들에게 미치는 영향에 대한 연구를 기반으로 신중하게 접근할 필요가 있음.
- AI 교육을 할 때에도 단지 'AI 윤리'가 아니라 AI 시대의 시민의 권리는 무엇이고, 누가 책임 주체이며, 권리가 침해되었을 때 어떻게 구제받을 수 있는가를 중심으로 교육할 필요가 있음.
- 초등부터 고등까지 모든 학년에서 연속적이고 일관된 디지털·AI 교육체계를 운영하는 것은 AI를 별도의 교과로 운영하는 방안으로 교원의 양성 및 교과 편성과 관련하여 충분한 논의가 이뤄져야 할 사항이며 현재는 통합교과 성격으로 접근해야 하는 상황임.
- 국가 단위 AI·데이터 실습 플랫폼 구축은 AI와 데이터 교육에 대한 방향이 결정된 후에 구축할 수 있어 성급하게 추진될 수 있는 상황이 아니며, 기존의 정보실을 활용하는 방안이 현실적임.

- **[수정 요구]** 서·논술형 평가에 AI 도입은 신중할 필요가 있음. (액션플랜 19)

[제안 이유]

- '19 평가 제도 및 입시 제도 혁신'은 AI를 활용해 서·논술형 평가를 하겠다는 계획을 포함하고 있음. 그러나 AI의 편향성 문제 때문에 특정 배경을 가진 학생 또는 특정한 서술 방식에 유리/불리한 결과가 도출될 수 있으며, 불투명성에 의해 제대로 평가 결과를 설명할 수 없는 경우 많은 논란이 발생할 우려가 있음. 따라서 시행 전에 이러한 논란이 발생할 우려가 없을지 철저한 검증이 필요함.
- 정답 중심 평가 체계를 역량 중심·과정 중심 평가 체계로 전환하기 위해서는 다양한 노력이 필요하며 현재까지 학습자의 성장을 중심에 두고 추진되었던 교육개혁이 실패한 이유는 불평등한 노동시장 구조와 학벌중심의 사회 구조에 기인한 부분이

크므로 이 부분에 대한 대응 전략이 구체적으로 제시될 필요가 있음.

- **[수정 요구] 학생 개인정보권리 침해 및 감시 우려를 최소화해야 함. (액션플랜 18, 60)**

[제안 이유]

- 행동계획 '60 교사 지원형 AI 보조교사 및 교육행정 AI 확산', '18. 초중등 AI 실습 교육 플랫폼 구축' 등을 보면, 윤석열 정부의 AI 교과서와 마찬가지로 수업에 AI를 활용하려는 계획을 가지고 있음. 이렇게 될 경우 학생들의 학습 이력이 모두 데이터화되고 축적되어, 방대한 학생 데이터를 기반으로 한 프로파일링이 가능해짐. 더구나 이 행동계획도 민간 에듀테크 기업들이 서비스 개발에 참여할 수 있도록 허용하고 있음.
- 이 경우 학생들은 수업시간이 아니라도 언제 자신이 과제를 수행했고, 학업 역량은 어떠한지 언제든지 모니터링되는 상황에 놓이며, 이에 학생 개인정보의 침해 및 감시 위험이 높아짐. 또한 민간 에듀테크 업체의 AI 학습 목적으로 남용될 수도 있음.

II. 환자·의료인·수급자 등 보건복지 부문

1. 액션플랜 번호

06. 보건의료 AI 고도화와 AX 전환에 필요한 학습데이터 확충
30. 보건의료 특화 AI파운데이션 모델 확보
31. 개인정보·미개방 산업 데이터 활용 규제 과감한 정비
39. '30년 AI 기반 글로벌 바이오·헬스 5대 강국 도약
88. AI 시대 정밀복지·돌봄의 접근성 확대
89. AI 기본 의료의 구현

2. 수정 및 제안

- **[수정 요구]** 데이터 활용에 따른 '이익 공유제(Profit Sharing)' 명문화가 국가AI전략 논의의 전제가 되어야 하며, 데이터 결합 과정에서 정보 주체의 실질적 거부권(Opt-out)이 보장되어야 함. (액션플랜 6)

[제안 이유]

- 본 정책은 민간 병원과 공공 기관의 데이터를 통합하여 AI 학습용 데이터셋을 구축하는데 초점을 맞추고 있으나, 그 과정에서 데이터의 '소유 및 권리관계'를 기업편향적으로 해석하고 있음. 복합 시계열 진료 데이터는 재식별 위험이 매우 높은 민감 정보임에도 불구하고, 이를 '국가 자산'이라는 명분으로 결합하여 기업의 AI 파운데이션 모델 학습에 제공하는 것은 사실상 국민의 정보를 원재료로 삼아 기업의 이익을 창출하는 '데이터 약탈'적 구조를 고착화하는 것임. 공적 자원인 데이터를 활용해 발생한 수익의 일정 부분이 공공의료 기금이나 건강보험 재정으로 환수되는 기전을 반드시 마련해야 하며, 데이터 결합 과정에서 정보 주체의 실질적 거부권(Opt-out)이 보장되어야 함.

- **[수정 요구]** 지역 간 의료격차 해소라는 명분이 민간 플랫폼의 시장 독점 수단으로 변질되지 않도록 공공 거버넌스의 실질적 통제력을 확보해야 함. (액션플랜 30)

[제안 이유]

- 정부는 '독자 파운데이션 모델'을 통한 의료격차 해소와 공공의료 구현을 주장하지만, 실제 개발 주체인 민간 대기업의 모델에 보건의료 시스템이 종속되는 결과를 초래할 가능성이 적지 않음. 국가 보건의료 시스템의 안정적 운영을 기업의 영업 정책이나 서비스 종료 여부에 맡기는 것은 국가적 위험을 자초하는 행위이며, 이는 공공 인프라의 운영권을 사기업에 양도하는 '기술적 사사화'임. 민간기업에의 종속을 방지하기 위해, 국가 예산이 투입된 모델은 그 소스코드를 공개하거나 국가가 직접 개발·관리하는 '공공 오픈소스 파운데이션 모델' 형태로 개발되어야 함.

- **[수정 요구]** 의료 데이터의 가명처리 원칙을 엄격히, 보수적으로 해석하고, ‘사후심사’가 아닌 더욱 강화된 ‘사전 영향평가 및 실시간 모니터링’ 체계를 도입해야 함. (액션플랜 31)

[제안 이유]

- ‘가명 처리 없는 개인정보 활용’을 허용하고 ‘사후 적정성 심사’로 전환하겠다는 계획은 정보 보호의 근간을 뒤흔드는 초법적 발상임. 특히, 최근 여러 기업에서 개인정보가 매일 같이 유출되고 있는 상황에서 그에 대한 사회적으로 수용가능한 정책적 개선 없이 ‘사전적 적법성 추정’을 기반으로 정책을 추진하는 것은 기업의 과실이나 남용에 대해 국가가 면죄부를 주는 행위임. 이는 국가가 기업의 개발 편의를 위해 국민의 기본권 보호 의무를 포기하는 것이며, 기술 주권이라는 이름 아래 개인의 정보인권을 희생시키는 권위주의적-개발주의적 행정임. 규제 완화에 앞서 개인정보 침해 사고 발생 시 기업의 존립이 불가능할 정도의 징벌적 손해배상제 도입과 집행이 선결과제로 다루어져야 함.

- **[수정 요구]** 계획 수립 단계부터 산업계 위주의 거버넌스를 해체하고, 의료소비자단체와 시민사회가 실질적 거부권을 가질 수 있는 민관 협력 공공 거버넌스를 구축하여 의사결정의 공공성을 담보해야 함. (액션플랜 39)

[제안 이유]

- 보건의료 공공성과 산업 육성 사이의 구조적 방화벽(Insulation)을 제도화할 필요가 있음. 산업적 수익 논리가 건강보험 재정 운용과 공공 의료 데이터 관리 원칙을 침범하지 못하도록 법적·제도적 절연 장치를 마련하는 것이 최우선 과제로 논의되어야 함. 또한 ‘바이오·헬스 강국’의 평가지표를 산업적 성과 중심에서 ‘의료 접근성 개선율’, ‘가계 의료비 부담 절감 기여도’, ‘AI 도입에 따른 안전 사고율’ 등 공익적 지표로 재편할 필요가 있음.

- **[수정 요구]** AI는 의료인의 판단과 행위를 돕는 ‘보조 도구’임을 명확히 하고, 대면 진료 우선의 원칙을 확립해야 함. (액션플랜 89)

[제안 이유]

- 지방 의료인력 부족 문제를 AI와 원격 협진을 통해 부분적으로 극복할 수 있겠지만, 이를 통해 문제를 해결하겠다는 발상은 국가가 마땅히 수행해야 할 공공 의료 인력 확충 의무를 회피하고 문제 해결의 의지를 의심하게 만드는 오만한 발상임. 의료인이 직접 제공하는 서비스를 AI 등 기술을 통해 강화할 수 있으나, 이를 기술로 대체하겠다는 것은 문제를 적극적으로 방기함으로써 의료의 질적양극화를 부추기고,

고착하는 차별적 정책임. AI 솔루션 도입 예산에 상응하는 자원을 지역의료서비스 강화에 우선 배정하여, ‘기술’이 아닌 ‘사람’ 중심의 의료 안전망을 먼저 구축해야 함.

- [수정 요구] AI 시대 복지·돌봄의 접근성 확대를 위해 AI와 관련 기술들이 보완적 역할을 할 수 있으나 근본적인 해결책이 될 수 없음을 이해하고 이를 검토 배경 및 정책 권고사항에 반영할 필요가 있음. (액션플랜 88)

[제안 이유]

- AI 기반 예측 모형이 복지·돌봄에 대한 사람들의 접근성 확대에 보완적인 기능을 할 수는 있겠으나, 현재 한국 복지·돌봄의 문제가 정밀한 예측의 부재로 인한 문제라기보다는 전반적인 복지·돌봄 제도적 인프라와 공공책임성의 부재로 인한 결과임을 고려했을 때 근본적 문제해결의 방안이 될 수 없음을 고려해야 함. 여기서도 역시 기한을 정하고 돌봄 로봇 등에 대한 상용화 추진을 권고하고 있는데 사전에 안전성과 효능에 대한 철저한 검증을 전제로 추진해야 할 것으로 보임. 한국 사회 복지·돌봄 문제의 해결을 위해서는 복지와 돌봄 전반에 걸쳐 제도적 인프라와 공공책임성의 강화가 우선이며, 이를 보완하기 위한 장치로써 AI를 포함한 혁신 기술적 요소가 활용되어야 함을 강조할 필요가 있음.

III. 국방·평화 부문

1. 액션플랜 번호

73. 국방 AI 거버넌스 혁신으로 국방 AI 추진체계 재설계
79. 방산 AI 육성을 통한 방산수출 4대 강국 진입

2. 수정 및 제안

- **[수정 요구]** 국방AI 거버넌스에 국제법, 인권 및 인도법, 평화학 등 다양한 전문가와 시민사회 의견 수렴 보장해야 함 (액션플랜 73)

[제안 이유]

- 국방부 내 전담조직 및 관리체계를 수립하기로 하고 국방분야 국방AI위원회, 국방AI자문위원회 두기로 함. 이들이 국방 AI 거버넌스 혁신 로드맵을 제시하는 등 관련 정책의 절대적 주도력을 갖게 될 것이므로, 그 구성을 사업의 추진력에만 맞추는 것보다 다양한 관점과 검토가 반영되도록 거버넌스를 갖추는 것이 중요함. 특히 국방AI위원회는 강력한 의사결정기구를 지향하는 만큼 결정의 위험성이 클 수밖에 없음. 국방분야 AI의 파급력과 위험성을 고려할 때, 이에 대한 비판적 검토 의견을 줄 수 있는 전문가, 시민사회 인사를 국방AI 거버넌스에 반드시 참여토록 해야 함.

- **[수정 요구]** 국방AI기본법 제정 시한을 두지 말고 충분한 논의 거쳐야 함 (액션플랜 73)

[제안 이유]

- AI 기반 의사결정 지원, 지휘통제, 무기체계 운용 등 생명이나 신체 등에 영향을 끼치는 고영향 AI로서의 국방 AI 특성상 그 영향력은 한 국가를 넘는 차원의 문제임. 따라서 관련 기본법을 제정한다면 국제사회에서 진행되고 있는 관련 논의를 신중히 검토하고 이를 국내법에 반영토록 하는 과정이 반드시 수반되어야 함. 특히 남북 대치 상황에서 우리 헌법에서 국군에 부여하고 있는 안전보장과 국토방위, 국제평화 유지 노력과 침략적 전쟁 부인 등의 의무를 고려할 때 관련 법제도가 적절한지 논의가 반드시 사전에 이뤄져야 함. 따라서 이러한 충분한 논의를 전제할 때 2026년 2분기까지 법 제정을 권고한 것은 숙의의 과정에 소요되는 시간을 고려하지 않은 것이라 할 수 있음.

- **[수정 요구]** 방산AI 육성을 통한 방산수출 4대 강국 진입 목표 삭제해야 함 (액션플랜 79)

[제안 이유]

- 자율살상무기 및 AI 기반 의사결정지원체계는 인간의 생사 여부를 기계가 결정하거나 또는 의도하지 않은 피해를 줄 수 있다는 위험이 존재함. 또한 AI 무기에 의한 오폭이나 민간인 피해 발생 시, 그 법적, 윤리적 책임이 누구에게 귀속되는지 명확하지 않는 등 책임 공백으로 인한 전쟁 범죄에 대한 처벌을 어렵게 만드는 문제가 있음. 또한 AI 체계가 복잡하고 기술이 발달할수록 더욱 예측할 수 없게 되거나 인간 통제를 벗어날 위험이 있는 문제가 존재함. 이러한 문제들이 제기되고 있고 이에 대한 국제사회의 우려가 명백함에도 불구하고 방산AI를 수출품으로 평가하고 방산AI 확대를 국가 목표로 삼는 것은 적절치 않음. 따라서 해당 행동계획 및 권고를 삭제하고 대신 AI 기반 신무기 체계 발전 계획에 대해 국내외 AI 윤리 기준 등을 기반으로 한 검증 체계를 마련해야 함. 군관계자 및 기술자들만이 알 수 있는 방식이 아닌, AI 신무기 체계가 실제 전장에서 어떠한 변화를 가져올 수 있고 어떤 위험성이 있는지 공개적으로 밝히고 이러한 위험에 대해 사회적 검증이 충분히 이뤄지도록 해야 함.

● **[수정 요구] 군사용 AI 활용에 대한 윤리 기준 마련 계획을 추가해야 함 (신규 추가)**

[제안 이유]

- 이번 대한민국 인공지능 행동계획(안)에는 ‘안전한 AI이용 보장, 공공부문 AI 윤리기준 마련’ 과제, ‘모두의 AI를 위한 AI 윤리 확산 고도화’ 과제, 각 분야별(노동, 의료, 교육) AI 윤리 가이드라인 계획 수립 등이 포함되어 있음. 그러나 군사 분야 AI 윤리 기준 마련은 행동계획에 포함되어 있지 않음.
- AI의 군사적 활용, 특히 자율살상무기시스템(Lethal Autonomous Weapons Systems, LAWS) 개발은 기술적 한계, 윤리적 문제, 책임성 문제, 민간인 피해 증가, 오남용 가능성, 분쟁 확대 위험 등 여러 위험을 내포하고 있음. 군사용 AI 규제에 대해 국제적으로 합의된 가이드라인이 부재한 가운데, 유엔 사무총장은 2026년까지 인간의 통제 없이 작동하며 국제인도법에 부합할 수 없는 치명적 자율무기를 금지하고, 그외 모든 자율무기를 규제할 수 있는 법적 구속력이 있는 조약을 채택하라고 촉구했음. 한국 정부 역시 범부처 차원에서 자율무기를 비롯한 군사 분야 AI의 위험성을 통제할 방안을 수립해야 함.
- 외교부는 REAIM(Responsible AI in the Military Domain, 인공지능의 책임있는 군사적 이용에 관한 고위급회의) 논의에 주도적으로 참여해왔음. 행동계획에서 “글로벌 도전 과제 해결을 위한 국제협력”과 “글로벌 AI 기본사회 모범사례 확산” 등 AI 글로벌 거버넌스 의제를 선도하고 과기정통부, 산업부와 협조하여 범부처 협의체를 설치하겠다고 밝히고 있으나 여기에 국방부와 협력하겠다는 내용은 담기지 않음.

● **[수정 요구] 국방 AI 기반 의사결정 지원 체계 검증 단계 마련해야 함 (신규 추가)**

【제안 이유】

- AI 기반 의사결정 지원 체계는 일반적으로 알고리즘 편향성, 의사결정 과정의 불투명성(블랙박스 문제), 결과에 대한 책임 소재 불분명, 데이터 품질 문제 및 기술적 한계 등의 지적을 받고 있음. 국방 AI 기반 의사결정 지원 체계 역시 이러한 한계를 극복하기 어려움. 무엇보다 국방 AI의 특성 상 생명과 안전을 다룬다는 점에서 그 파급력과 영향력은 막대하다 할 수 있으므로 국방 AI 기반 의사결정 지원 체계는 엄격한 검증 절차가 필요함.

IV. 노동자

1. 액션플랜 번호

87. AI 전환 대응 일자리 혁신 및 현장 역량 강화

2. 수정 및 제안

- **[수정 요구]** ‘산업**AX**’ 전략으로 인하여 노동자에게 미치는 고용 불안과 감시 강화에 대한 대책을 포함하여야 함. 노동자 또는 노동조합이 국가적으로나 개별 기업 단위에서 **AI**의 도입 여부, 또는 **AI** 도입의 속도와 규모에 대하여 참여하고 발언할 기회를 보장해야 함. 특히 고용관계와 노동조건에 영향을 미치는 **AI**시스템을 규제하는 입법을 추진하여야 함(신규 추가)

[제안 이유]

- 노동 정책은 (87) AI 전환 대응 일자리 혁신 및 현장 역량 강화에 집중적으로 논의되고 있음.
- 우선 "중소기업과 플랫폼 기반 산업에서는 AI 도입 속도와 근로자 역량 간 격차가 커지고 있으며, 재직자 재교육·전환 프로그램의 미비, 프리랜서·긱워커의 사회안전망 부재, 알고리즘 기반 인사 평가 불투명성 등이 주요 리스크로 지적된다."고 진단하고 ‘AI 전환 대응 일자리 혁신 계획’을 수립하여 재직자·비정형 노동자·전환 대상자 등 실제 노동자 정책으로 AI 시대의 고용안정과 공정한 노동환경을 구축하도록 하였음.
- 특히 노동부에는 ‘26년 2분기까지 「AI시대 일자리 변화 대응 및 고용안정 종합계획」을 수립하고 ①중소기업 AI 도입 연계 훈련을 포함한 노동시장의 구직자, 재직자 등의 AI 역량강화, ② 플랫폼 노동자·프리랜서 등 초단기 노동자 대상 사회안전망 및 공정 알고리즘 기준 마련, ③ AI 대체 고위험군 직종별 맞춤형 전환 지원제도와 실업 안전망 확충을 핵심 축으로 포함하도록 하였음.
- 또한 노동부는 ‘26년 4분기까지 노동조건 결정에 있어 AI활용의 공정성과 투명성을 확보하기 위한 「(가칭)노동분야 AI 윤리 가이드라인」을 마련하고, 더불어 ‘27년 2분기까지 AI 도입에 따른 사회·산업 차원의 기술 변화로 인해 발생한 소득 및 기회 상실에 대한 적절한 보상 체계를 포함하는 「포용적 노동 전환 국가 전략」을 수립하여야 함.
- 그러나 AI 재교육과 전환 중심의 정책들로는 기존 고용의 안정률을 제고하기에 충분한 방안이라고 보기 어려움. 기술 실업은 구조적인 문제임에도 '재교육'과 '직무전환' 중심으로 대책을 제시하는 것은 노동자 개인의 적응 문제로 치환하는 것임. 개별 기업이 AI 전환을 이유로 노동자를 손쉽게 해고하고 국가가 사후에 일부 소득을 실업 급여 등으로 보전하는 것은 고용 안정 대책이 될 수 없음.

- 전반적으로 ‘산업**AI**’전략은 노동현장에 **AI**를 도입하여 생산성을 높이겠다는 목표를 가지고 있으나, 노동자에게 미치는 고용불안과 감시 강화에 대한 대책은 포함하고 있지 않음. 2023년 12월 **AI** 도입을 이유로 국민은행 콜센터에서 240명 일괄 해고 사건이 발생하였듯이, 노동자에 대한 손쉬운 대량 해고를 규제하여야 함. 또한 직장의 감정인식 및 노동조합 가입여부를 추론하는 생체인식분류를 금지하고, 노동 조건 및 근로 계약에 영향을 미치는 인공지능을 고위험으로 분류하여 규제하는 대책이 포함되어야 함
- 무엇보다 국가적으로 **AI** 전환을 전제로 할 뿐 아니라 이를 목표로 강하게 추진하면서 그 영향을 받는 노동자 또는 노동조합이 국가적으로나 개별 기업 단위에서 **AI**의 도입 여부, 또는 **AI** 도입의 속도와 규모에 대하여 참여하고 발언할 기회가 명시적으로 보장되어 있지 않음.
- 노동조건에 영향을 미치는 기업 **AI**의 공정성과 투명성을 확보하는 것이 중요함. 그러나 국가적으로 **AI** 산업전환과 인공지능기본법이 강력하게 시행되는 상황에서 이에 대한 대책으로 노동부의 ‘윤리 가이드라인’은 매우 미력할 수밖에 없음. **AI**로 인한 노동조건 변화에 대한 노동자와 노동조합의 정당한 협상권을 보장하고, 노동조건에 영향을 미치는 **AI**의 개발과 도입을 규제하고 노동자와 노동조합의 권리를 보호하는 입법적 대책이 시급하게 마련되어야 함.

V. 여성

1. 액션플랜 번호

26. AI 인재 경력 단절 해소
80. 「모두를 위한 AI 기본 사회 추진계획」 수립
86. AI 시대 생애 경제 통합 전략 마련
88. AI 시대 정밀복지·돌봄의 접근성 확대

2. 수정 및 제안

- **[수정 요구] AI 관련 국가 정책 결정 구조에 성평등 대책과 여성의 참여가 포함되어 함 (신규 추가)**

[제안 이유]

- 여성 정책과 성평등부의 역할은 여러 항목에 걸쳐 분산되어 있음. △출산 및 육아로 인한 석·박사급 AI 및 AI 융합연구 인력의 경력 단절을 해소하는 (26) AI 인재 경력 단절 해소, △과기정통부가 노동부, 성평등부 등과 함께 (80) 「모두를 위한 AI 기본 사회 추진계획」 수립하도록 하고, △여성·시니어·비정형 노동자 등이 경력 단절과 돌봄 부담으로 인해 경제활동 참여와 AI 재교육 기회가 제한되고 있다는 진단 하에, (86) AI 시대 생애 경제 통합 전략 마련을 위해 「AI 시대 중장기 생애 경제 지원방안」을 논의하도록 함. △특히 (88) AI 시대 정밀복지·돌봄의 접근성 확대를 위하여 '돌봄 경제' 부담을 완화하는 AI 기반으로 정밀 예측과 선제적 개입을 도입하는 한편, 로봇·센서·웨어러블 등 피지컬 AI를 활용한 지능형 돌봄 인프라로 돌봄노동 과부하 완화와 고령층의 자율·안전성 제고, 돌봄 경제의 지속가능성을 확보하고자 함
- 그러나 돌봄 노동자 등 대다수 여성에게 중대한 영향을 미치는 국가 정책에서 AI 전환과 AI 도입을 이미 전제하면서 사후 대책 위주로 정책을 마련하는 것은 그 영향을 받는 여성 당사자의 민주적 참여와 성평등한 관점 통합을 제한할 우려가 있음.
- 특히 인공지능이 성차별을 비롯한 차별·혐오를 재생산할 수 있다는 우려는 계속 제기되었고, 다양한 사례로 실증되어왔음. 따라서 인공지능 정책을 수립할 때는 차별·혐오의 문제가 인공지능이 유발하는 주요한 위험이며, 평등권이 인공지능과 관련하여 보호하여야 할 가치임을 분명히 인지할 필요가 있음. AI 관련 국가적인 정책 거버넌스에서 이러한 인공지능 위험에 대한 성평등 대책을 포함하고 여성의 참여를 보장하여야 함.