

「대한민국 인공지능 행동계획」(안)에 대한 의견서

제출 단체 : 디지털정의네트워크, 정보인권연구소

제출 일시 : 2026년 1월 4일(일)

1. 총론

지난 12월 16일, 대통령직속 국가인공지능전략위원회 공개한 「대한민국 인공지능 행동계획」(안)(이하 AI 행동계획)은 AI의 개발·활용에만 중점을 두고 있으며, AI의 위험성을 통제하고 사업자 책임성을 강화할 장치가 부재함. 또한, AI의 영향을 받는 사람들의 권리 보호 및 피해 구제 방안에 대한 계획도 미흡함.

'11) 전략분야 AI 기본 사회'에서 모두가 AI의 혜택을 누릴 수 있는 포용적 AI 정책을 다루고 있기는 하지만, 이 역시 사회적 취약계층도 배제되지 않고 AI에 접근할 수 있어야 한다면, 공익적 목적이나 사회 문제 해결을 위해 AI를 활용하는 등 'AI의 활용'에 초점을 맞추고 있을 뿐, AI가 시민의 인권과 안전을 침해하지 않도록 안전장치를 마련할 필요성이나 AI로 인해 영향을 받을 수 있는 노동자, 소비자, 여성, 장애인, 학생 등의 권리 보호 방안에 대해서는 제대로 다루고 있지 않음.

또한, AI 행동계획은 AI 개발 및 산업 발전을 명분으로 개인정보 보호원칙을 형해화하고 있는데, 이러한 정책 방향은 철회되어야 마땅함. 비단 특정 산업의 발전을 위해서 역사적으로 형성되어온 기본적인 원칙을 수정해야 할 근거가 부족할 뿐만 아니라, AI 개발 및 활용 과정에서 대량의 개인정보 처리와 프로파일링, 감시 기술의 고도화에 의해 개인정보 자기결정권에 대한 위협이 커진다는 점을 고려하면, 오히려 개인정보보호법이 강화될 필요가 있음.

AI 행동계획은 AI의 개발 및 도입이 시민들의 삶과 사회에 도움이 될 것이라고 막연하게 전제하고 있음. 그러나 챗지피티나 제미나이와 같이 시민들이 일상적으로 사용하고 있는 AI에 의해 청소년이 자살하거나, 사람과의 소통보다 기계와의 소통에 의존하거나, 학교에서 자신의 지적 역량을 훈련하는 과정을 대체하는 등 여러 우려가 제기되고 있는 등 단지 AI를 많이 사용한다고 그것이 우리의 삶에 도움이 된다고 단정할 수는 없음. 채용 AI나 부정수급탐지 AI 등 예측 AI의 경우, 예측의 정확성에 대한 의문이나 차별적 결정 등 다양한 문제가 제기되고 있음. 물론 우리에게 도움이 되는 AI 시스템도 존재할 수 있음. 분명한 것은 마치 자동차나 승강기와 같은 제품을 출시할 때 안전성 검사를 받는 것처럼, 복지 정책을 도입할 때 공정성에 대한 검토를 하는 것처럼, 국가는 AI 제품이나 서비스가 시민의 안전과 인권을 침해하지 않도록 보장해야 할 기본적인 책무가 있다는 것임. 그러나 AI 행동계획은 AI 제품이나 서비스가 어떠한 위험이 있는지, 그러한 위험을 어떻게 탐지, 제거, 완화할 것인지에 대해 충분히 다루고 있지 않음.

이 때문에 우리는 AI 행동계획에서 다루고 있는 정책의 문제점에 대한 의견을 제시하는 것과 동시에, AI 행동계획에서 다루고 있지 않은 의제들, 특히 AI의 위험성에 대해 어떻게 안전장치를 마련할 것인지, 위험한 AI를 제공하는 사업자와 AI를 활용하는 기관의 책임을 어떻게 물을 것인지, AI의 영향을 받는 시민의 권리를 어떻게 보호할 것인지에 대한 의제들을 제안하고자 함.

마지막으로 AI 행동계획이 이러한 의제를 미리 포함하지 못한 것은 국가인공지능전략위원회의 구성 자체가 편향되어 있기 때문이라는 점을 지적하고자 함. 즉, 편향적 데이터로 학습한 AI가 편향적인 결과물을 산출할 수 밖에 없듯이, 국가인공지능전략위원회의 구성 자체가 AI 개발 및 산업 발전을 요구하는 산업계 인사를 중심으로 편향적으로 구성되어 있기 때문에 이처럼 편향적인 정책이 나올 수밖에 없음. 지금이라도 국가인공지능전략위원회가 산업 발전뿐만 아니라 공공성과 시민권리 보호를 균형있게 고려한 AI 정책을 수립하고자 한다면, 위원회부터 재구성할 필요가 있음. 다양한 의견을 배제한 편향적인 정책이 지금은 효율적으로 보일 수는 있어도 공감대를 얻지 못한 정책은 추진 과정에서 저항에 부딪힐 수밖에 없다는 점을 강조하고자 함.

2. AI 행동계획에 대한 의견

(1) 개인정보 보호

가. 액션플랜 : 5. AI 데이터 공유 생태계 활성화

- 수정 요구
 - AI 학습·평가를 위한 데이터 공유 활성화를 명분으로 개인정보 또는 민감정보의 기부·공유를 장려하는 정책은 정보주체의 권리를 침해할 우려가 큼. 특히 세제 혜택, 가점 부여 등 경제적, 행정적 인센티브를 통해 개인정보 제공을 유도하는 방식은 지양해야 하며, 개인정보가 포함된 데이터의 경우 정보주체의 명시적 동의와 실효성있는 옵트아웃 권리가 전제되어야 함.
- 제안이유
 - 본 액션플랜은 개인정보를 기술 발전을 위한 수단적 자원으로만 간주하고 있음. 그러나 개인정보는 기술 발전을 이유로 자유롭게 도구화될 수 없는 헌법상 기본권이며, 정보주체의 실질적인 통제 하에 처리되어야 함. 특히 ‘기부’라는 표현은 정보주체의 자발적 의사에 따른 제공 형식을 취하고 있으나, 경제적 인센티브와 결합될 경우, 특히 사회적 취약계층에게 사실상의 압박으로 작동하여 개인정보 자기결정권을 침해할 소지가 큼. 데이터 공유 활성화 정책은 개인정보 보호 원칙을 최우선 가치로 설계되어야 함.

나. 액션플랜 : 6. 보건의료 AI 고도화와 AX 전환에 필요한 학습데이터 확충

- 수정 요구
 - 보건의료 데이터의 결합·활용을 통한 AI 학습데이터 확충 계획은 개인정보, 특히 민감정보 보호 측면에서 엄격히 제한해야 함. 다기관 의료데이터, 공공·민간 의료데이터, 개인 유래 건강 데이터의 결합 및 활용은 정보주체 동의, 목적 제한, 안전조치, 감독 체계 등 요건을 명확히 한 경우에 한해 공익적 목적에 한해 제한적으로 허용되어야 함.
- 제안이유
 - 보건의료 데이터는 개인의 신체·정신적 상태, 질병 이력, 치료 기록 등 인간의 존엄성과 내밀한 사적 영역에 밀접하게 연관된 민감정보에 해당함. 그럼에도 본 행동계획은 보건의료 AI 고도화라는 명분 하에 대규모 의료데이터 결합과 활용의 필요성만을 강조하고 개인정보 보호에 대한 요건은 충분히 제시하지 않고 있음. 특히

공공데이터와 민간 의료데이터, 개인의 건강 데이터를 결합해 활용하는 경우 재식별 위험과 목적 외 이용 가능성이 현저함에도 이에 대한 통제 방안은 추상적으로만 제시돼 있음. 보건의료 데이터 활용은 개인정보보호법 상 민감정보 보호 원칙에 부합하도록 보다 엄격한 기준이 마련될 필요가 있음.

다. 액션플랜 : 8. 국가 AI·데이터 거버넌스 정립

- 수정 요구
 - CTO-CAIO-CDO 통합 거버넌스 구축 과정에서 개인정보 보호 기능과 권한이 약화되지 않도록 명확한 제도적 장치가 마련돼야 함. 데이터 활용 촉진을 중심으로 한 거버넌스 개편은 개인정보 보호를 약화시킬 수 있음. 개별 부처의 개인정보보호책임자, 그리고 국가적 수준에서 개인정보보호위원회의 독립성과 권한이 보장되어야 함.
- 제안이유
 - 과연 ‘데이터’라는 이름을 붙인 기구들이 개인정보 보호 차원에서 거버넌스를 운영할 지 의문임. 국가 차원의 데이터·AI 거버넌스를 효율적으로 통합하겠다는 목표를 제시하고 있으나 데이터 활용 촉진에 중점을 둔 구조로 운영될 가능성이 높음. 개인정보 보호는 행정 절차나 산업 정책의 효율성보다 더욱 핵심적인, 헌법상 기본권의 영역임. 거버넌스 일원화가 데이터 활용 효율성의 관점에서 이루어질 경우 개인정보 감독·통제의 실효성이 약화될 수 있음. 따라서 국가 AI·데이터 거버넌스는 데이터 활용 확대·효율성 증대 등을 전제하기보다 개인정보 보호를 우선하는 방향으로 설계돼야 함. 데이터 관련 거버넌스의 통합이 개인정보 보호 책임자가 감독기관의 역할을 침해하지 않도록 주의할 필요가 있음.

라. 액션플랜 : 31. 개인정보·미개방 산업 데이터 활용

- 수정 요구
 - 인공지능 학습을 위해 개인정보 원본 활용이 가능하도록 하는 방향의 법제 추진은 중단돼야 하며 개인정보 보호 원칙을 완화하는 방향이 아니라 정보주체의 권리를 실질적으로 강화하는 방향으로 개인정보보호법 개정이 이루어져야 함. 인공지능 시대에 개인정보 정책의 최우선 과제는 데이터 활용 확대가 아니라 정보주체가 자신의 정보에 대해 통제할 수 있는 권리를 강화하는 것을 명확히 해야 함.
- 제안이유
 - 본 액션플랜은 인공지능 학습과 산업 경쟁력 강화를 명분으로 개인정보의 활용 확대를 추진하고 있으나, 이는 개인정보 보호의 기본 원칙을 도외시한 접근임. 헌법상 개인정보자기결정권은 정보주체가 자신에 관한 정보가 이용되는 범위와 대상을 스스로 결정하는 기본권으로서, 산업적 목표에 우선하여 보호되어야 함. 현행 개인정보보호법 역시 목적 적합성을 핵심 원칙으로 삼고 있고, 수집된 개인정보를 인공지능 학습 등 새로운 목적으로 이용할 경우 정보주체의 동의를 받는 것이 원칙임.
 - 그럼에도 불구하고 개인정보 원본 활용을 허용하려는 법제의 추진은 개인정보를 기본권이 아닌, 산업적 수단으로 간주하는 편향된 인식에 기반하고 있음. 특히 대량의 데이터가 실시간으로 수집·처리되고 고도화된 프로파일링이 가능해진 현재의 AI 환경에서, 원본 개인정보 활용 확대는 정보주체의 권리 침해로 직결될 위험이 더욱 커지고 있음. 지금 필요한 것은 개인정보 원본을 활용하도록 규제를 완화하는 것이 아니라, 무분별한 개인정보 활용에 대한 거부권 등 정보주체가 자신의 정보에 대한

통제권을 실질적으로 행사할 수 있도록 제도적 장치를 강화하는 것임. 따라서 인공지능 학습을 위한 개인정보 활용 정책은 개인정보 보호 원칙을 훼손하지 않는 방향으로 재검토되어야 하며, 오히려 정보주체의 권리를 강화하는 방향으로 개인정보보호법 개정이 추진되어야 함.

(2) 공공 AI

가. 액션플랜 : 50. AI-Native한 공무원 협업체계 구축

- 수정 요구
 - 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.
- 제안이유
 - 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. 최소한 AI 시스템을 업무에 활용하기 전에 해당 AI 시스템이 제대로 작동하는지, 편향이나 차별적인 결과를 야기하지 않는지에 대해 확인하는 절차를 두어야 함.

나. 액션플랜 : 51. 칸막이를 넘어 데이터와 맥락을 연결하는 AI 업무관리 플랫폼 구축

- 수정 요구
 - 지능형 업무관리 플랫폼, 범정부 AI 공통기반, AI 통합 워크스페이스 등의 구축 과정에서 부처별 개인정보 및 데이터의 책임기관이 명확하게 설정되어야 하며, AI 학습을 통해 개인정보나 기밀정보가 권한이 없는 타 기관에 노출되지 않도록 주의해야 함. 개인정보 및 데이터를 타 기관에 제공, 공유할 때에는 법적 근거나 정보주체의 동의가 있어야 함.
- 제안이유
 - 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.

다. 액션플랜 : 52. 공공 정보화 사업, 민간 클라우드로 전환

- 수정 요구
 - 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.

- 제안이유
- 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.

라. 액션플랜 : 54. 공공부문 AI 도입에 대한 국민 기본권 보장, 공공 AI 영향평가

- 수정 요구
- ▲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.
- 제안이유
- 공공기관의 업무는 투명성, 책무성을 기본적으로 담보해야 하며 AI를 활용한다고 예외가 될 수 없음. 따라서 AI가 산출한 결과물에 대해 영향을 받는 당사자에게 설명할 수 없는 경우, 이러한 AI를 도입해서는 안됨.
- 영향평가에는 영향받는 사람의 참여가 필수임. 이는 유엔 인권실사(인권영향평가를 포함한)의 기본적인 원칙이며, 또한 바이든 행정부의 인공지능 행정명령의 이행 지침에서도 공공부문 AI에 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.

마. 액션플랜 : 55. 안전한 AI이용 보장, 공공부문 AI 윤리기준 마련

- 수정 요구
- 「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.

- 제안이유
- "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.

바. 액션플랜 : 56. 공공 AI 대전환 가속화, 적극행정 인센티브와 감사 면책 마련

- 수정 요구
- 국민의 기본권에 큰 영향을 미치는 사업에는 면책을 배제하고, 면책 범위를 기술적 시범 서비스에 한정해야 함.
- 제안이유
- 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.

사. 액션플랜 : 60. 교사 지원형 AI 보조교사 및 교육행정 AI 확산

- 수정 요구
- ▲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.
- 제안이유
- 학교에서 AI의 활용이 항상 교사들을 지원하는 것은 아니며 오히려 교사들에게 부담이 될 수도 있음. 교사들이 과도한 업무에 시달리고 있다면 AI가 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.

아. 액션플랜 : 63. 공공AX 거버넌스 및 실행체계 구축

- 수정 요구
- 효율성 중심의 공공 거버넌스를 이해관계자의 민주적 참여에 기반한 거버넌스로 재편해야 함.
- 제안이유
- "갑을병정으로 이어지는 하청구조와 단기 계약직 중심의 개발, 일정 기간마다 교체되는 운영사 시스템"이 AI를 도입한다고 해결될리는 만무함. AI를 도입하면서 여전히 효율성 중심의 거버넌스를 유지한다면 근본적인 관료적 구조를 얼마나 개편할 수 있을지 의문임. 단지 CTO와 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.

(3) AI 핵심인재 확보 및 교육부문 AI

가. 액션플랜 : 17. 초중등 전학년에서 연속적인 디지털·AI 교육 필수 이수 / 18. 초중등 AI 실습 교육 플랫폼 구축

- 수정 요구
 - AI가 학생의 정신적, 지적 역량 강화에 미치는 영향에 대한 고민(AI가 교육에 어떤 영향을 미치는지에 대한 본질적인 질문)이 선행되어야 함.
- 제안이유
 - '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 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.

나. 액션플랜 : 19. 평가 제도 및 입시 제도 혁신

- 수정 요구
 - 서·논술형 평가에 AI를 도입하는 것은 설명가능성 및 편향성에 대한 충분한 검토가 이루어진 후에 이루어질 필요가 있음.
- 제안이유
 - '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.

나. 액션플랜 : 18. 초중등 AI 실습 교육 플랫폼 구축 / 60. 교사 지원형 AI 보조교사 및 교육행정 AI 확산

- 수정 요구
 - 교육 과정에 AI 시스템을 활용할 경우 학생 개인정보권리 침해 및 감시 우려를 최소화해야 함.
- 제안이유

- 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.

(4) AI 사이버보안과 국정원의 역할

가. 액션플랜 :

- 10. AI 기반의 사이버 보안 체계 구축, AI 보안 기술 경쟁력 강화 및 보안 전문 인재 양성
- 11. AI 시대, 넥스트 AI 안보 위협 대응 및 협력 강화
- 52. 공공 정보화 사업, 민간 클라우드로 전환
- 수정 요구
- AI 사이버보안에 대한 국가정보원의 권한을 배제하고, 궁극적으로 국정원의 사이버보안 권한을 삭제해야 함.
- 제안이유
- 그동안 시민사회의 지속없는 노력으로 국정원의 국내정보 수집 권한은 일부 제한되었지만, 국정원은 여전히 사이버안보정보와 공공 정보통신망에 대한 사이버보안 업무를 담당하고 있으며, 이를 매개로 국내 및 민간 영역에 끊임없이 개입하려고 시도하고 있음.
- 그러나 AI 행동계획은 국정원이 '사이버 AI 안보 플랫폼' 구축 등 AI 사이버보안의 컨트롤타워 역할을 맡도록 하고 있을 뿐만 아니라, K-사이버보안 LLM 구축 협력, 허위정보 판별 기술, 민간 클라우드 정책 방안에 대한 검토, 개인정보 불법정보 방지 대책에 협력 등 민간의 기술 생태계나 정보통신망에 관여할 수 있는 여지를 마련해놓고 있음. 이를 통해 기존에 국정원이 사이버보안 권한과 관련하여 갖고 있던 문제가 AI 시대에도 확대재생산될 위험이 있음. 국정원의 사이버보안 역할 만큼이나 AI 사이버보안을 왜 비밀 정보기관이 맡아야 하는지 의문임.
- 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 권한을 국정원에게 부여하겠다는 것이나 마찬가지임. 국정원이 위협 예측 기반의 능동적 방어라는 명분으로, 불법이 명확하지 않은 민간의 트래픽에 대해 선제적으로 탐지, 차단, 관여할 수 있다면, 민간 정보통신 공간에 대한 사이버 감시와 프라이버시 침해의 우려가 큼. 사이버보안을 위한 이러한 대응이 필요하다면, 권한 남용의 여지가 적고 정치 사회적 감독이 가능한 일반 행정기관에서 맡도록 해야 할 것임.

- 이는 비단 국정원이 시민감시와 정치 개입을 해왔던 암울한 과거를 갖고 있기 때문이 아니며, 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 AI 사이버전략에 대한 수립 권한을 통제받지 않는 정보기관에게 부여해야 하는지 의문임. 만일 국정원에게 이러한 역할을 맡겨야 한다면, 다른 정부부처 수준의 예산 및 국회의 통제를 받도록 해야 할 것임.

3. 신규 행동계획 제안

(1) 영향받는 노동자의 권리 보호

가. 검토 배경

노동자는 ‘산업AX’ 전략으로 인하여 고용불안과 감시 강화 등 그 권리에 중대한 영향을 받을 것으로 예상됨.

그러나 액션플랜은 AI로 인한 구조적 실업에 대한 대책을 포함하고 있지 않으며, ‘재교육’과 ‘직무전환’ 중심의 대책으로 AI 실업을 노동자 개인의 적응 문제로 치환하고 있음. 고용 안정 대책 없는 실업 급여 등 사후 대책은 기업의 쉬운 해고를 방치하고, AI 시대에 노동자 개인의 고통과 국가적 부담을 가중할 뿐임.

또한 액션플랜은 직장에 배치되는 AI가 인권침해적 감시를 강화하고 노동조건에 깊은 영향을 미치는 데 대한 대책을 포함하고 있지 않으며, 다만 “(가칭)노동분야 AI 윤리 가이드라인”으로 공정성과 투명성을 보완할 것을 요구하고 있을 뿐임.

액션플랜은 국가적으로 AI 전환을 전제로 할 뿐 아니라 이를 목표로 강하게 추진하면서 그 영향을 받는 노동자 또는 노동조합이 국가적으로나 개별 기업 단위에서 AI의 도입 여부, 또는 AI 도입의 속도와 규모에 대하여 참여하고 발언할 기회가 명시적으로 보장되어 있지 않음.

나. 정책 권고 사항

- AI로 인한 구조적 실업에 대한 대책을 포함하여야 함
 - 2023년 12월 AI 도입을 이유로 국민은행 콜센터에서 발생한 대량 해고 사건에서처럼, 개별 기업이 AI 전환을 이유로 노동자를 손쉽게 대량으로 해고하는 일을 규제하는 고용 안정 대책이 마련돼야 함.
- 고용관계와 노동조건에 영향을 미치는 AI시스템을 규제하는 입법을 추진하여야 함
 - ILO는 AI 모니터링과 알고리즘 기반 관리의 증가가 고용관계와 노동조건에 미치는 영향에 대하여 우려하는 보고서를 발간하며 입법적인 규제가 필요하다고 분석한 바 있음. EU AI Act 또한 직장에서의 감정인식 및 노동조합 가입여부를 추론하는 생체인식분류를 금지하고, 노동조건 및 근로 계약에 영향을 미치는 인공지능을 고위험으로 분류하여 규제하고 있음.
- 노동자 또는 노동조합이 국가적으로나 개별 기업 단위에서 AI의 도입 여부, 또는 AI 도입의 속도와 규모에 대하여 참여하고 발언할 기회를 보장해야 함.
 - AI로 인한 노동조건과 고용 관계 변화에 대한 노동자와 노동조합의 정당한 협상권을 보장하여야 함.

(2) 영향받는 여성의 권리 보호

가. 검토 배경

AI 전환이 여성에게 미치는 영향으로, 경력 단절과 돌봄 부담으로 인해 경제활동 참여와 AI 재교육 기회가 제한될 것이 예상됨.

그러나 액션플랜은 이에 대한 대책으로 AI 인재에 국한한 경력 단절 해소(26), "AI 시대 중장기 생애 경제 지원방안"을 "논의"(86)하는 데 그침.

특히 돌봄 대책은 AI를 기반으로 하는 정밀 예측과 선제적 개입, 지능형 인프라로 AI 기반 돌봄 경제를 창출하는 데 몰입할 뿐(88), 여성의 돌봄 부담을 사회적으로 분담하는 구조적 대책을 전혀 포함하고 있지 않음.

나. 정책 권고 사항

- AI 관련 국가 정책 결정 구조에 여성의 참여가 보장돼야 함
 - 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.
- 액션플랜에 성평등 대책이 포함돼야 함
 - 인공지능이 성차별을 비롯한 차별·혐오를 재생산할 수 있다는 우려가 계속 제기되었고, 다양한 사례로 실증되어왔음. 따라서 인공지능 정책을 수립할 때는 차별·혐오의 문제가 인공지능이 유발하는 주요한 위험이며, 평등권이 인공지능과 관련하여 보호하여야 할 가치임을 분명히 인지하고 대책을 마련할 필요가 있음.

(3) 영향받는 소비자의 권리 보호

가. 검토 배경

인공지능 기술은 생성형 AI, 추천·노출 알고리즘, 자동화된 고객 응대, 신용·보험·통신·플랫폼 거래 등 다양한 영역에서 이미 소비자의 일상적 선택과 계약, 가격 결정, 서비스 이용 과정에 깊이 관여하고 있음. 그러나 현재의 인공지능 정책 및 AI 행동계획은 산업 경쟁력 강화와 기술 개발에 주로 초점을 두고 있어, 인공지능을 실제로 이용·소비하는 시민의 권리 보호에 대한 체계적인 접근은 부재한 상황임.

적절한 정책적 개입이 없다면 인공지능의 개입 여부와 작동 방식이 소비자에게 충분히 고지되지 않거나, 자동화된 판단으로 인한 불리한 결과에 대해 설명받거나 이의를 제기하고 구제받기 어려운 구조가 고착화될 우려가 있음. 또한 인공지능 기반 추천, 가격 결정, 거래 조건 설정 과정에서 차별이나 기만, 불공정 거래가 발생할 가능성이 확대되고 있으나, 기존 소비자 보호 제도는 이러한 새로운 유형의 피해를 효과적으로 대응하는데 한계가 있음.

신뢰할 수 있는 인공지능 생태계 조성 and 인공지능 서비스의 사회적 수용성을 확보하기 위해서는, 기술 개발 및 산업 육성을 넘어 소비자의 알 권리, 공정한 거래, 차별로부터의 보호, 실효적인 피해 구제 수단을 보장하는 소비자 보호 정책이 AI 행동계획에 포함될 필요가 있음.

나. 정책 권고 사항

- 인공지능 기반 소비자 보호 정책의 체계적 추진
 - 공정거래위원회를 주관 부처로 하여, 과기정통부, 개인정보보호위, 금융위, 방미통위, 보건복지부 등 관계 부처와 협력하여 인공지능 이용 과정에서 발생할 수 있는 소비자 피해 유형을 체계적으로 분석하고, 인공지능 특성을 반영한 소비자 보호 정책 방향을 수립할 필요가 있음
- 인공지능 기반 차별로부터 소비자 보호
 - 인공지능에 기반하여 개인별 차등 가격, 플랫폼에서의 이용자의 성별·지역·인종 등에 따른 차별적 광고 등 차별적 서비스로부터 소비자를 보호할 수 있는 기준 및 절차를 마련할 필요가 있음.
- 소비자의 알 권리 및 선택권 강화
 - 인공지능이 가격 결정, 상품 추천 등 거래에 중대한 영향을 미치는 경우 해당 사실과 주요 특성을 소비자에게 명확히 고지하도록 할 필요가 있음. 또한 인공지능의 자동화된 결정이 소비자에게 중대한 영향을 미치는 경우, 소비자가 인간의 개입을 요청하거나 이의를 제기할 수 있는 절차를 도입할 필요가 있음.
- 인공지능 기반의 기만적인 불공정 거래 행위에 대한 규율 강화
 - 인공지능을 활용한 과장 광고, 허위 정보 제공, 다크 패턴 등 기만적인 행위를 불공정 거래 행위로 규정하고, 관련 가이드라인과 집행 기준을 마련할 필요가 있음.
- 효과적인 소비자 권리 구제 제도의 강화
 - 최근 개인정보 대량 유출사고에도 불구하고 소액·다수 피해가 발생할 경우 소비자의 권리를 구제할 수 있는 집단/단체 소송 제도가 마련되어 있지 않아, 효과적인 구제가 이루어지고 있지 않음. AI 개발·이용 과정에서도 대량의 개인정보가 처리되어 침해가 발생할 수 있고, 개인정보 외에도 이와 유사한 소액·다수 피해가 발생할 수 있음. 또한 개인정보 피해와 같이 AI의 불투명성으로 인해 소비자가 그 원인을 입증하는 것이 곤란할 수 있음. 이에 효과적인 소비자 피해 구제를 위해 집단/단체 소송 제도 및 증거개시 제도를 도입할 필요가 있음.
- 인공지능 거버넌스에 소비자 참여 확대
 - 인공지능 정책 수립 및 이행 점검 과정에서 소비자 단체와 시민사회의 참여를 확대하고, 소비자 관점의 문제 제기와 정책 제안이 제도적으로 반영될 수 있는 협의 구조를 마련할 필요가 있음.

(4) 국가안보 목적 AI 기본법 제정

가. 검토 배경

인공지능 기본법은 ‘국방 또는 국가안보 목적으로만 개발·이용되는 인공지능’을 적용 대상에서 제외하고 있고, 현재 입법예고된 시행령은 주로 국방부나 국정원이 지정하는 업무를 적용 배제 대상으로 규정하고 있음. 즉, 국방부나 국정원의 업무에는 인공지능 기본법이 적용되지 않는다는 것임.

그나마 AI 행동계획은 국방 분야의 경우 ‘(가칭) 국방 AI 기본법’을 ‘26년 2분기까지 제정하도록 하고 있음. 그러나 ‘국가안보 목적’ AI 분야로서 국정원이 담당하는 분야는 여전히 제외되어 있음. 다시 말하면, 국정원이 국가안보를 명분으로 개발, 활용하는 AI에 대해서는 아무런 법적인 규율이 적용되지 않는다는 것이고, 앞으로 이를 규율할 법제를 만들 계획도 없다는 것임.

AI는 과거 다른 감시 수단에 비해 훨씬 은밀하고 광범위한 감시가 가능하도록 하는 바, 국정원에게 아무런 규율도 없이 AI를 마음대로 개발, 활용하도록 하는 것은 너무나 위험함. 국가안보 AI를 규율할 수 있는 법제가 조속히 마련되어야 하며, 이 역시 행동계획에 포함되어야 함.

나. 정책 권고 사항

- 국가안보 목적 AI 기본법 제정
 - 국정원은 과기정통부와 협력하여 국가안보 목적 AI를 규율하기 위한 기본법을 제정해야 함.
 - 기본원칙은 인공지능 기본법에 두어야 하며, 국가안보 목적 AI 기본법은 기본법 규율에서 벗어나는 예외적인 사항만 규정하되, 국가안보 목적 AI 라고 하더라도 필요성 및 비례성 요건을 충족해야 하고, 사법적인 통제와 감독을 받을 것을 요건으로 해야 함.

(5) 금지된 AI 및 고영향 AI 분야 추가 지정

가. 검토 배경

현재 인공지능 기본법 및 하위 법령 논의 과정에서는 우리 사회에서 원칙적으로 금지되어야 할 인공지능의 유형이나, 고위험(고영향)으로 분류하여 특별히 관리해야 할 인공지능 분야에 대해 충분히 구체화되지 못한 상황임. 인공지능 기본법은 EU 인공지능법이나 미국 바이든 정부 행정명령에 비하여 고위험(고영향) 인공지능 분야를 지나치게 협소하게 규정하고 있고, 금지해야 할 인공지능에 대해서는 전혀 언급하고 있지 않음. 또한, 11월 12일 입법예고된 인공지능 기본법 시행령은 고영향 인공지능 분야를 추가적으로 규정할 수 있음에도 전혀 규정하지 않고 있음. 이는 한국 정부가 금지된 인공지능 및 고위험(고영향) 인공지능 분야에 대한 연구와 검토가 매우 미진한 상황임을 의미함. 인공지능 기본법이 2026년 1월 22일 시행되는 바, 이미 늦기는 했지만 조속히 금지된 인공지능 및 고위험(고영향) 인공지능 분야에 대한 연구 및 의견수렴을 통해 추가적으로 이를 지정할 필요가 있음.

그럼에도 불구하고 현행 인공지능 행동계획(안)은 이러한 핵심 쟁점에 대해 누가, 언제까지, 어떤 절차와 기준을 통해 검토하고 사회적 논의를 진행할 것인지에 대한 로드맵을 제시하지 않고 있음. 금지 인공지능 및 고위험(고영향) 인공지능의 범위 설정은 특정 부처나 기술 관점에 국한될 수 없는 사안으로, 전 부처의 협력과 함께 시민사회, 산업계, 학계 등 사회 각계의 의견을 폭넓게 수렴할 필요가 있음. 이에 인공지능 행동계획을 통해 향후 논의 구조와 일정, 책임 주체를 명확히 제시할 필요가 있음.

나. 정책 권고 사항

- 금지된 AI 및 고영향 AI 분야의 추가 지정

- 과기정통부는 다른 정부부처와 협의하여 금지 인공지능 및 고위험(고영향) 인공지능 분야의 추가 지정을 위한 일정 및 절차를 마련해야 함.

(6) 고영향 AI 사업자의 책임 구체화

가. 검토 배경

식품이든 자동차든 국민의 안전, 생명, 인권에 부정적 영향을 미칠 수 있는 상품은 시장에 출시되거나 서비스 제공 전에 그 안전성이 충분히 평가되어야 하며, 인공지능 역시 예외가 될 수 없음. 더구나 신기술로서 안전과 인권에 미치는 영향이 분명하지 않은 AI의 특성을 고려할 때, AI의 안전성을 보장할 수 있는 제도적 안전장치를 마련하는 것은 정부의 기본적인 책무임.

현재 인공지능 기본법 및 하위 법령 체계에서는 고영향 인공지능 사업자의 책무가 매우 부실하게 다루어져 있음. 또한, 인공지능 생태계에서 실제로 작동하는 다양한 행위자(기초모델 개발자, 하위스트림 개발자, 배치자, 유통·판매자, 이용·운영자 등)에 대한 구분 및 각 행위자의 역할과 책임도 명확하게 규정되어 있지 않음. 이로 인해 위험이 발생했을 때 책임 소재가 불명확해지고, 사업자가 'AI가 한 결정'이라는 이유로 설명 책임과 피해 구제를 회피할 가능성이 커지며, 소비자·노동자·시민 등 영향받는 자의 권리 보호가 실효적으로 보장되지 않을 우려가 있음.

따라서 인공지능 기본법이 실효성있게 작동할 수 있기 위해서는 인공지능의 개발 및 활용 과정에서 책임을 져야 할 주체들이 명확하게 구분되고, 각 행위자의 역할에 따라 합당한 책임을 부여할 수 있도록 할 필요가 있으며, 이러한 정책을 조속히 수립하여 인공지능 기본법에 반영해야 함.

나. 정책 권고 사항

- 인공지능 생태계 내 행위자의 역할과 책임 규정
 - 인공지능 생태계 내의 각 행위자를 역할과 책임에 따라 구분하고, 문제가 발생했을 때 각 행위자가 어떠한 책임을 지고, 이러한 책임 소재의 규명을 위해 사전에 어떠한 조치가 필요한지 등에 대한 정책을 조속히 수립하고 인공지능 기본법에 반영해야 함.
- 범용 AI 모델 위험성 평가 및 책임 규정
 - 고영향 AI 시스템과 구분하여, 범용 AI(또는 프론티어 AI) 모델에 대해서는 그 위험성과 안전조치를 평가할 수 있는 정책이 별도로 수립되어야 함.
- 오픈소스 모델이나 시스템에 대한 정책 수립
 - 이러한 정책을 수립할 때 오픈소스 모델이나 시스템에 어떻게 적용될 것인지에 대한 방안도 포함되어야 함.
- 영향받는 사람들의 권리 및 피해구제
 - 인공지능 시스템에 의해 부정적 영향을 받는 사람들의 권리의 보장과 피해구제 방안이 포함되어야 함.
- 기본권 영향평가 활성화 방안 수립
 - 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.

- 정책결정에 영향받는 사람들의 관점 반영
 - 이러한 정책 수립 과정에서 사회 각 부문에서 인공지능의 영향을 받는 사람들의 목소리가 충분히 반영될 수 있도록 해야 함
- 정책수립시 이해관계자 참여 보장
 - 과기정통부는 다른 정부부처 및 이해관계자와 협의하여, 이러한 정책 마련을 위한 행동계획을 수립해야 함.

(7) AI 시스템의 투명성 강화

가. 검토 배경

인공지능 시스템의 활용이 확대됨에 따라, 그리고 인공지능 시스템의 본질적인 불투명성을 고려할 때, 인공지능의 사용 여부와 개입 방식, 결과의 생성·추천·결정 구조를 이용자와 사회가 인지할 수 있도록 하는 투명성 확보는 신뢰 가능한 인공지능 생태계 구축의 핵심 요소임.

인공지능 기본법 및 하위 법령에서도 고영향 또는 생성형 인공지능 포함 여부, 생성형 인공지능의 결과물인지 여부, 딥페이크 여부 등의 표시에 대한 규정을 두고 있으나, 현재 규정은 의무의 주체와 방법에 있어서 매우 미흡한 상황임. 투명성 확보를 위해 필요한 기술적 수단과 표준, 검증 방식에 대한 연구·개발 역시 더 연구가 이루어져야 할 과제임.

투명성은 단순한 정보 공개를 넘어, 소비자·노동자·시민 등 영향받는 자가 인공지능의 개입을 인지하고 권리를 행사할 수 있도록 하는 전제 조건이라는 점에서, 인공지능 행동계획을 통해 중장기적 연구·검토 과제와 이행 로드맵을 제시할 필요가 있음.

나. 정책 권고 사항

- 인공지능 시스템 투명성에 대한 종합적 정책 수립 필요
 - 인공지능 시스템의 특성에 따라 누가, 어떻게 표시 의무를 이행할 것인지, 플랫폼 사업자의 책임은 무엇인지, 우회를 방지하기 위한 방법은 무엇인지, 이를 위해 개발이 필요한 기술은 무엇인지 등에 대한 정책 수립을 위한 행동계획이 제시되어야 함.
- 설명가능하지 않은 AI는 공공부문에 도입하지 말아야 함
 - 최소한 시민들의 인권이나 권익에 영향을 미치는 경우, 공공분야에서는 설명가능하지 않은 AI, 위험성이 검증되지 않은 AI는 도입하지 않겠다는 명확한 입장 표명이 필요함.
- 인공지능 투명성 및 설명가능성에 대한 연구
 - AI 시스템의 불투명성을 개선하기 위한 기술 개발, 설명가능성과 해석가능성 등 개념의 의미, 투명성의 이행 방안 등에 대한 연구와 검토가 필요함.

(8) 범죄 수사 및 예방 목적 AI의 남용 방지를 위한 정책

가. 검토 배경

경찰 등 수사, 치안 기관은 범죄 수사, 범죄 예방, 경호 및 공공 안전 확보를 목적으로 안면인식, 행동 분석, 위험 예측, 영상 분석 등 다양한 인공지능 기술의 도입을 확대하고 있음. 이러한 인공지능 기술은 시민에 대한 광범위한 정보 수집과 프로파일링, 은밀한 감시를 수반할 수 있어 사생활의 자유, 개인정보 자기결정권, 표현의 자유, 집회·결사의 자유 등 기본권에 중대한 영향을 미칠 수 있음. 그럼에도 불구하고 그 특성상 이 분야 인공지능 기술의 사용이 투명하게 드러나지 않을 가능성이 큼. 실제로 개인정보의 처리와 관련해서도 수사기관은 비례적이지 않은 예외를 인정받고 있음.

그러나, 현재 인공지능 기본법 및 하위 법령, 그리고 인공지능 행동계획(안)에서는 수사·치안 목적 인공지능의 도입과 활용에 대한 별도의 통제 기준이나 남용 방지 정책이 충분히 고려되지 않고 있음.

범죄 수사·예방이라는 목적이 시민의 기본권 침해로 정당화되지 않도록 하기 위해서는, 인공지능 행동계획을 통해 수사·치안 목적 인공지능의 위험성을 명시적으로 인식하고, 도입·활용 과정 전반에 대한 통제 원칙과 사회적 논의 구조를 마련할 필요가 있음.

나. 정책 권고 사항

- 범죄 수사 및 예방 목적 AI 관련 정책 수립
 - 범죄 수사 및 예방 목적 AI의 개발 및 도입에 적용되는 정책을 투명하고 충분한 공론화 과정을 거쳐서 수립해야 함.
- 적법성, 필요성, 비례성 요건 준수
 - 이러한 정책은 다음과 같은 원칙을 준수해야 함. 범죄 수사 및 예방 목적 AI의 도입은 언제나 법률에 근거해야 하며, 어떠한 AI가 사용되는지 투명하게 공개되어야 함. 또한 항상 필요성 및 비례성 요건을 갖추어야 하며, 국회 및 법원의 통제와 감독을 받아야 함. 누구나 접근할 수 있는 공간에서의 원격 생체인식 감시는 금지되어야 함