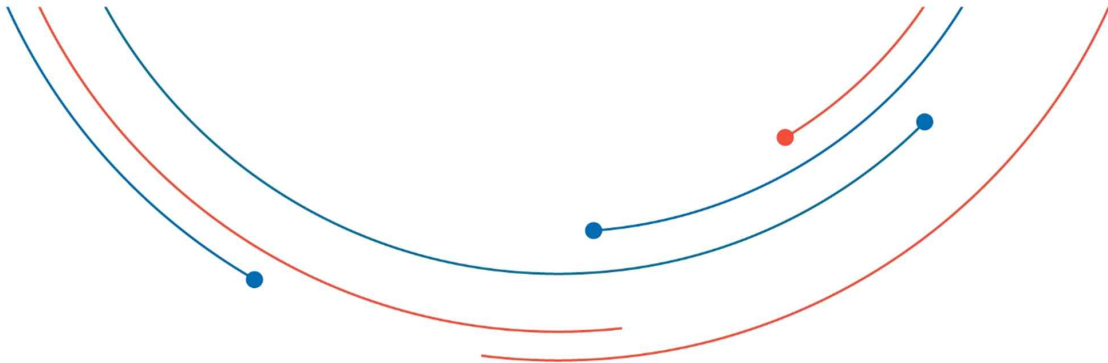




AI.GOV 이슈리포트 2025-4호

인공지능정부 전환을 위한 법제도 고려사항



NIA 한국지능정보원

일러두기 NOTE

「AI.GOV 이슈리포트」는 공공부문의 인공지능 전환 및 디지털정부와 관련된 다양한 이슈를 분석하고 향후 정책 방향을 모색하기 위해 한국지능정보사회진흥원에서 기획하여 발간하는 보고서입니다.

한국지능정보사회진흥원의 사전 승인 없이 본 보고서의 무단전재나 복제를 금하며, 가공·인용할 때는 반드시 출처를 명시하여 주시기 바랍니다.

본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있으며, 문의 및 제안은 아래 연락처로 문의해주시기 바랍니다.

- 발행처: 한국지능정보사회진흥원
- 발행인: 황종성
- 작성자: 한국지능정보사회진흥원 인공지능정부본부 AI정부기획팀
김미진 선임(mj123@nia.or.kr)
- 기 획: 한국지능정보사회진흥원 인공지능정부본부
정부만 본부장, 박선주 팀장, 김미진 선임
- 보고서 온라인 서비스: www.nia.or.kr

목 차 CONTENTS

I. 배경 및 필요성	4
II. 디지털정부와 인공지능정부의 구조적 차이	5
1. 개념 · 기술 · 행정 차이	5
2. 책임구조 · 위험에 대한 법제도 요구사항 차이	6
III. 기존 공공정보시스템 구축 절차	7
1. 현행 공공 정보시스템 구축 · 운영 절차	7
2. ISP 단계와 구조적 한계	7
3. 계약 · 검수 단계에서의 제도적 한계	8
4. 운영 단계에서의 책임 · 통제 공백	9
IV. 공공 AI서비스 도입 관련 법제도 현황 및 문제점	10
1. 기존 법제도의 적용 구조	10
2. 책임소재 · 공정성 · 설명가능성 관련 법제도 문제	11
3. 인공지능 기본법 주요내용 및 한계점	12
V. 해외 공공AI 도입 절차 · 법제도 사례	14
1. EU: 위험기반 규율과 생애주기 중심 공공 AI 관리 체계	14
2. 미국: 기관 거버넌스와 영향 중심의 공공 AI 관리	15
3. 영국 · 싱가포르: 원칙기반 규율과 실무형 프레임워크 중심	16
4. 캐나다: 자동화 의사결정 중심 영향평가(AIA)	17
5. 해외사례 비교결과	18
VI. 법제도 개선방안 및 정책적 제언	19
참고문헌	22

I 배경 및 필요성

□ 공공부문 AI 도입 가속화와 행정환경의 변화

- 초거대 AI와 생성형 AI 기술을 중심으로 공공부문 전반에 인공지능 활용 확산
 - 대규모 언어모델(LLM), 기계학습, 자연어 처리(NLP) 등 AI 기술은 기존 정보시스템이 처리하기 어려웠던 비정형 데이터까지 분석·활용할 수 있는 기반을 제공
- 대규모 언어모델 기반 AI 기술은 공공기관이 보유한 방대한 행정 자산을 즉시 활용 가능한 자원으로 전환시키는 역할을 수행
 - 법령, 지침, 내부 규정, 민원 데이터, 정책 보고서 등 축적된 행정 문서와 데이터는 LLM 기반 AI를 통해 검색·요약·분석·응답 등 다양한 방식으로 활용
- 공공 AI 활용은 단순 시범·실증 중심 단계를 넘어 정책분석, 의사결정 지원, 대국민 서비스 제공 등 행정 운영의 핵심 영역으로 확대
 - AI는 민원 분류·응답, 정책 시뮬레이션, 위험 예측, 행정 지원 도구 등 다양한 영역에서 공무원의 판단을 보조하거나 사전 대응을 가능하게 하는 수단으로 활용
- 이러한 변화는 행정 서비스의 처리 속도와 품질을 동시에 개선하고, 국민의 생활 문제를 선제적으로 해결하려는 현 정부의 국정 운영 방향과도 부합

□ 인공지능정부를 위한 디지털정부 법제도 개선 필요

- 공공부문 AI 활용이 빠르게 확대되고 있으나, 이를 규율하는 법·제도와 사업 절차는 여전히 전통적인 정보시스템 구축·운영을 전제로 설계
 - 현행 공공 정보시스템 구축 체계는 기능과 산출물이 사전에 명확히 정의되는 정형 시스템을 전제로 하고 있어, AI 서비스와 같이 학습·추론·성능 변화가 반복되는 동적 시스템을 충분히 미반영
- AI 시스템은 학습데이터 변경, 모델 업데이트, 성능 재조정이 지속적으로 이루어지는 특성을 가지나, 현행 제도는 완성형 납품과 단년도 계약을 기본 전제로 운영
 - 이로 인해 AI 모델의 성능 고도화나 환경 변화에 따른 재학습이 계약 범위를 벗어난 추가 과업으로 해석되거나, 운영 단계에서의 개선 활동이 제도적으로 제약

II

디지털정부와 인공지능정부의 구조적 차이

1 개념·기술·행정 차이

□ 전산화를 넘어 판단·대응의 지능화 정부로 확장

- 디지털정부는 행정 절차와 공공서비스를 정보기술 기반으로 전산화 연계하여 효율성과 접근성을 제고하는 정부 운영 방식
 - 전자문서, 온라인 민원, 행정정보 공동이용 등은 기존 행정 절차를 디지털 시스템으로 전환함으로써 업무 처리 속도를 개선
 - 디지털정부는 국민의 행정 접근성을 높이는 데 기여해 왔으며, 이는 규칙과 절차가 명확한 정형 업무를 중심으로 발전
- 인공지능정부는 행정 전반에 AI의 분석·추론·예측 기능을 내재화하여 행정 판단과 대응 방식 자체를 전환하는 정부 운영 모델
 - AI는 단순한 업무 자동화 도구가 아니라, 정책 설계, 민원 분류, 위험 예측, 의사결정 지원 등 공무원의 판단을 보조하거나, 사전 대응을 가능하게 하는 핵심 수단

□ 규칙 기반 시스템에서 학습·확률 기반 AI 시스템으로 발전

- 디지털정부는 사전에 정의된 규칙과 로직에 따라 작동하는 규칙 기반(rule-based) 시스템을 중심으로 구성
 - 규칙기반 시스템은 처리 결과가 예측 가능하고 일관성이 높지만 복잡하거나 비정형적인 상황에 대한 유연한 대응 한계
- 인공지능정부는 학습 데이터와 알고리즘에 따라 결과가 달라질 수 있는 학습 기반(model-based) AI 시스템을 핵심 기술로 활용
 - 이로 인해 AI 시스템은 동일한 입력에도 확률적으로 다른 결과를 도출할 수 있으며, 성능 또한 운영 환경과 데이터 변화에 따라 지속적으로 변동

□ 판단 지원 중심의 행정처리 방식으로 변화

- 디지털정부는 시스템이 정해진 절차를 수행하고 최종 판단은 공무원이 담당하는 '절차 수행 중심' 구조
- 인공지능정부는 AI가 분석·추천·예측을 통해 판단 과정에 직접 관여하며, 인간과 AI의 협업(Human-in-the-loop)이 행정 운영의 기본 구조

2 책임 구조·위험에 대한 법제도 요구사항 차이

□ 행정처리 결과에 대한 책임구조 불명확화

- 디지털정부 환경에서는 행정 처리 결과에 대한 책임 구조가 비교적 명확하게 설정
 - 규칙 기반 정보시스템은 사전에 정의된 절차와 로직에 따라 작동하며, 시스템은 행정 판단을 보조하는 도구로 기능
 - 이에따라, 최종 결정과 책임은 담당 공무원 또는 행정기관에 귀속되는 구조를 유지
- 인공지능정부 환경에서는 AI가 행정 판단 과정에 직접 관여하면서 책임 구조가 복잡적·불명확해질 가능성이 확대
 - AI가 민원 분류, 대상자 선별, 정책 효과 예측 등에서 판단 결과를 제시하거나 자동화된 결정을 수행할 경우,
 - 오류나 부당한 결과 발생 시 해당 책임이 개발자, 운영기관, 관리·감독 주체 중 누구에게 귀속되는지 명확히 구분하기 어려운 상황 발생 가능

□ 편향·불투명 등 새로운 위험에 대한 법제도적 대응 필요

- 학습 데이터의 편향, 알고리즘 설계의 불투명성, 운영 환경 변화에 따른 성능 저하(모델 드리프트) 등은 전통적 정보시스템에서는 상대적으로 제한적으로 발생
- AI 시스템은 기존 정보시스템과 다른 유형의 위험을 내포하며, 이러한 위험은 행정의 공정성·신뢰성에 직접적인 영향을 미칠 수 있어 제도적 대응 필요
 - AI 결과에 대한 설명 가능성 확보, 공정성 검증, 인간 개입 수준의 명확화, 운영 단계에서의 상시 모니터링 등 필수적인 행정 책임 요소로 인식

| 책임구조 및 편향 문제점 사례 |

사례	문제점
SyRI(네덜란드)	복지 부정수급 탐지를 위해 다양한 데이터를 결합한 불투명한 알고리즘이 특정 계층에 대한 편향적 선별과 과도한 감시를 초래했음에도 책임주체와 권리구제 절차 불명확
COMPAS(미국)	재범 위험 예측 알고리즘이 인종 편향 논란과 함께 판단 근거가 공개되지 않는 블랙박스 구조로 운영되면서, 결과의 공정성과 책임성 검증 불가

III

기존 공공 정보시스템 구축 절차

1 현행 공공 정보시스템 구축·운영 절차

- 공공부문 정보시스템 구축은 「행정기관 및 공공기관 정보시스템 구축·운영 지침」을 중심으로 단계적·표준화된 절차에 따라 추진
 - 해당 지침은 정보시스템 도입의 타당성을 검토하는 ISP 수립 단계부터, 사업 기획, 구축, 검수, 운영에 이르는 전 과정을 체계적으로 관리하기 위한 기준으로 활용
- 현행 절차는 ISP 단계에서 사업 필요성과 범위를 정의하고, 이후 단계별로 요구사항을 구체화하는 구조를 기본으로 함

| 현행 공공정보화사업 절차 |

단계	주요내용
ISP단계	대상 업무 분석, 시스템 구축 방향, 소요 예산, 추진 일정 등 종합적으로 검토하며 이를 토대로 이후 사업 기획과 예산 편성, 조달 절차 연계
구축 단계	사전에 정의된 요구사항을 충족하는 시스템 개발
검사 단계	기능 구현 여부, 성능 기준 충족 여부, 보안·안정성 확보 여부 등이 주요 검사 항목으로 활용되며, 검사 완료 시 시스템은 '완성형' 산출물로 인식
운영 단계	구축이 완료된 시스템을 안정적으로 유지·관리

- 정형화된 업무와 예측 가능한 운영 환경에서의 전통적인 디지털정부에서는 이러한 절차가 효과적으로 작동했으며, 이는 디지털정부 발전의 핵심 기반으로 기능

2 ISP 단계에서의 구조적 한계

- 현행 ISP 단계는 정보시스템 구축의 필요성과 타당성을 검토하는 핵심 단계이나, 전통적인 디지털 시스템을 전제로 설계되어 AI 서비스 특성을 충분히 반영하지 못함
 - ISP는 업무 분석과 시스템 구축 방향 설정에 초점을 두고 있으나, 학습·추론·확률적

결과를 전제로 하는 AI 시스템에 대해서는 적용 범위와 검토 항목이 제한적

- 현행 ISP에서는 해당 업무를 AI로 처리하는 것이 적절한지, 규칙 기반 시스템이나 업무 프로세스 개선으로 대체 가능한지에 대한 검토가 명시적으로 요구되지 않음
 - 이로 인해 'AI 도입'이 기술 트렌드나 정책적 기대에 따라 선제적으로 설정되고, 실제 행정 효과나 위험 요소에 대한 충분한 검토 없이 사업 기획
- AI 서비스의 성능과 공정성은 학습 데이터의 범위와 품질에 크게 좌우되나, 현행 ISP 체계에서는 데이터 활용과 알고리즘 영향에 대한 검토 미흡
 - 활용 데이터에 대한 출처, 개인정보 포함 여부, 편향 가능성, 재이용 가능 범위 등에 대한 체계적인 검토 미포함
 - 또한, AI 알고리즘이 행정 판단에 미치는 영향과 그 파급 효과에 대한 분석도 구조적으로 미흡
- 행정판단에서의 AI 개입 범위, 공무원의 개입이 필요한 지점, 오류 발생 시 책임 귀속 주체 등 책임구조와 인간 개입 수준에 대한 설계 부족
 - 이는, 이후 구축·운영 단계에서 법적 해석 문제와 책임 논쟁으로 이어지며, 공공 AI 서비스의 안정적 정착을 어렵게 만드는 요인으로 작용

3 계약·검수 단계에서의 제도적 한계

- 공공 정보시스템 구축 계약 구조는 단년도 예산과 완성형 납품을 기본 전제로 설계 되어 있어 AI 서비스 개발 방식과 구조적 충돌 발생
 - 현행 계약 방식은 사업 착수 시점에 요구사항을 최대한 구체화하고, 계약 기간 내 '완성된 시스템'을 납품하는 구조로 운영
 - 이는 반복적 개선과 실험을 전제로 하는 AI 개발 방식과 근본적으로 상이
- AI 서비스 개발 과정에서 필수적인 모델 학습·재학습·성능 고도화 활동이 계약 범위 외 과업으로 해석되는 문제 발생
 - AI 모델은 초기 구축 이후에도 데이터 추가, 환경 변화 등에 따라 지속적인 재학습과 성능 조정이 필요하나, 현행 계약 구조는 이러한 활동을 추가 개발로 간주
 - 이로 인해 운영 단계에서 AI 성능 개선이 지연되거나, 실질적인 고도화 없이 초기

수준에 머무르는 문제가 발생 가능

- 검수 단계는 요구사항 충족 여부, 기능 정상 작동 여부 등이 주요 기준 설계되어 AI 서비스의 품질과 위험을 충분히 평가하는 데 한계
 - AI 서비스에서 핵심적인 성능 안정성, 편향 발생 가능성, 설명 가능성 수준 등은 공식적인 검수 항목으로 다뤄지지 않음
 - 그 결과, 검수 시점에는 문제가 드러나지 않더라도 실제 운영 과정에서 공정성 논란이나 신뢰성 문제가 발생할 가능성 존재
- 이러한 계약·검수 구조는 공공 AI 서비스를 ‘일회성 구축 사업’으로 인식하게 만들며, 운영 중심의 관리·책임 체계 형성을 저해
 - 구축 완료 시점을 기준으로 사업 성과를 평가하는 구조는 공공 AI 서비스의 품질과 책임성을 장기적으로 담보하기 어렵게 만드는 요인으로 작용

4 운영 단계에서의 책임·통제 공백

- 공공 AI 서비스에서 운영 단계는 성능·공정성·신뢰성 관리의 핵심 단계이나, 현행 정보시스템 운영 체계는 이를 충분히 포괄하지 못함
 - 정보시스템 운영은 장애 대응, 보안 관리, 시스템 가용성 등을 중심으로 설계
 - AI 서비스에서 필수적인 모델 성능 변화, 데이터 편향 누적, 알고리즘 영향 확대 등은 공식적인 관리 대상에서 상대적으로 배제
- AI 시스템은 운영 환경과 데이터 변화에 따라 성능이 저하되거나 예측 결과가 달라질 수 있음에도, 이를 상시 점검·조정하는 제도적 장치가 미흡
 - 현행 운영·유지관리 체계에서는 학습 데이터의 분포 변화, 정책 기준 변경, 이용 행태 변화 등을 주기적으로 점검하거나 재학습을 수행하도록 하는 명확한 기준 부재
- AI가 행정 판단에 실질적으로 관여하는 경우, 결과 오류나 부당한 판단이 발생했을 때 이를 누가 인지·조정·중단할 수 있는지에 대한 권한과 책임이 불명확
 - 특히 공무원이 AI 결과를 참고하였을 뿐이라는 이유로 책임 주체가 모호해지거나, 반대로 AI 결과를 신뢰하지 않고 수작업으로 되돌리는 상황이 발생

IV

공공 AI 서비스 도입 관련 법제도 현황 및 문제점

1 기존 법제도의 적용 구조

□ 「개인정보 보호법」과 「전자정부법」이 기본적인 법적 근거로 적용

- AI 서비스를 개발·운영할 경우, 개인정보의 수집·이용·제공 처리에 대해서는 「개인정보 보호법」, 정보시스템의 구축·운영 등에 대해서는 「전자정부법」과 관련 하위 지침 적용
 - 그러나, 이러한 법제도는 AI 시스템을 전제로 설계되기보다는 전통적인 정보시스템과 데이터 처리 방식을 중심으로 구성
- 「전자정부법」은 전자적 행정 처리의 효율성과 연계를 목표로 하며, 시스템의 안정적 구축·운영을 중시하는 반면, AI 시스템의 학습·추론·모델 변경과 같은 특성에 대해서는 별도의 규율 체계를 두고 있지 않음
- 「개인정보 보호법」 역시 개인정보의 처리 행위를 중심으로 규율하고 있어, AI 학습 과정에서 발생하는 데이터 활용 방식과 완전히 정합적인 구조를 갖추지 못함
- AI 모델 학습 과정에서는 대량의 데이터가 반복적으로 활용·가공되며, 초기 수집 목적과 다른 형태의 분석·추론이 이루어질 수 있음
 - 그러나, 현행 법체계에서는 이러한 활용이 목적 제한 원칙과 어떻게 조화되어야 하는지에 대한 명확한 기준이 제시되지 않는 경우가 많음
 - 이로 인해 공공 AI 서비스 개발 현장에서는 법 적용 범위와 해석을 둘러싼 불확실성이 지속적으로 발생
- AI 학습 데이터의 재활용 가능 여부, 모델 고도화 과정에서의 개인정보 처리 범위, 운영 단계에서 발생하는 추가 데이터 수집의 적법성 등에 대해 명확한 판단 기준 부재
 - 이로 인해 기관별로 보수적인 해석 또는 상이한 대응이 이루어지고 있으며, 이는 공공 AI 서비스 도입과 확산을 제약하는 요인으로 작용

2 책임소재·공정성·설명 가능성 관련 법제도 문제

□ AI 판단 결과에 대한 책임소재 규정 한계

- AI가 판단 과정에 관여하는 경우 결과의 오류·부당성에 대해 개발자, 운영기관, 실제 의사결정권자 중 누구에게 책임이 귀속되는지 명확히 구분하기 어려움
- 현행 법제도는 AI를 행정 주체로 인정하지 않으며, AI 판단이 행정결정에 미치는 영향 수준에 따른 책임 분담 구조도 명시적으로 규정하고 있지 않음

□ 알고리즘의 공정성에 대한 규정 부재

- 현행 법체계에서는 알고리즘 설계나 학습 데이터의 편향 여부를 사전에 점검하거나 시정하도록 요구하는 절차가 명확히 규정되어 있지 않음
- 이로 인해 공공 AI 서비스는 차별 논란 발생 시 사후적으로 문제를 해명하는 데 그치는 경우가 많으며, 제도적으로 공정성을 사전에 담보하기 어려운 구조

□ AI 판단 결과에 대한 설명 가능성 요구 부재

- 행정절차법상 이유 제시 의무는 행정처분의 근거를 설명하도록 요구하고 있으나, AI 모델의 내부 작동 원리나 판단 과정까지 설명해야 하는지에 대해서는 명확한 기준 부재
- 특히 딥러닝 기반 모델의 경우 결과 도출 과정이 복잡하고 비가시적인 특성을 가지므로, 기존 제도만으로는 국민의 설명 요구에 체계적으로 대응하기 어려운 한계

□ 공공 AI 서비스의 신뢰성과 수용성을 저해

- 책임·공정성·설명 가능성 문제는 공공 AI 서비스의 신뢰성과 수용성을 저해하는 핵심 요인으로 작용
- 법적 기준과 절차가 명확하지 않은 상황에서는 공무원 역시 AI 활용에 소극적으로 대응할 수밖에 없음

- 이는 공공 AI 서비스가 실증 단계에 머물거나 제한적으로만 활용되는 결과로 이어질 가능성이 큼
- 이러한 문제를 구조적으로 해소하기 위해 인공지능 기본법을 포함한 법제도 정비의 방향성과 한계를 종합적으로 검토 필요

3 인공지능 기본법의 주요 내용 및 한계점

□ 인공지능 기술의 안전하고 신뢰 가능한 활용을 위한 기본 원칙

- 인공지능기본법은 인공지능 기술 발전을 저해하지 않으면서도 국민의 권리 보호와 사회적 신뢰 확보를 도모하는 것을 목적으로 함
- 또한 인공지능 정책의 기본 방향, 국가와 사업자의 책무, 안전·신뢰 확보를 위한 관리 체계 등을 포괄적으로 규정

□ 책임성·공정성·투명성 확보를 중요한 원칙으로 제시

- 인공지능 기본법은 AI 시스템이 사회적 영향을 미칠 수 있음을 전제로, 차별 방지, 안전성 확보, 설명 가능성 제고, 인간의 통제 가능성 보장 등을 주요 원칙으로 명시
- 이는 공공 AI 서비스 설계·운영 시 준수해야 할 기본 기준으로 작용할 수 있음

□ 기존 법제도의 한계를 보완하는 상위 규범

- 개인정보 보호법과 전자정부법이 개별 영역 중심의 규율을 제공하는 반면, 인공지능 기본법은 AI 시스템 전반에 공통적으로 적용되는 신뢰·안전 원칙을 제시
- 공공 AI 서비스 개발 시 고려해야 할 최소한의 기준을 제도적으로 명확히 하는 역할
- 다만, 인공지능 기본법은 ‘원칙법’ 성격이 강하여 공공 AI 서비스 도입 절차 전반을 직접 규율하는 데에는 한계가 존재
- 법률 차원에서 구체적인 사업 절차, 계약 방식, 검수 기준, 운영 관리 체계까지 상세히 규정하기보다는, 기본 방향과 원칙을 제시하는 데 중점

- 실제 공공 AI 사업 현장에서 적용 가능한 세부 기준과 절차는 하위 법령·지침 또는 별도의 운영 기준을 통해 보완될 필요가 있음

□ 구체적인 사업 절차와 직접적으로 연결되는 구조는 미완성

- 인공지능기본법은 AI 시스템의 신뢰성과 안전성을 확보하기 위한 방향성을 제시하는데 중점
- 개별 공공 AI 사업의 기획·조달·구축·검수·운영 단계에서 무엇을 어떻게 이행해야 하는지에 대한 구체적 절차까지는 규정하지 않고 있음
- 이로 인해 공공 AI 서비스 도입 현장에서는 인공지능 기본법과 기존 정보시스템 관련 법·지침 간의 역할 분담이 명확하지 않은 상황
- 정보시스템 구축·운영과 관련된 실무 절차는 여전히 「전자정부법」과 관련 지침에 따라 운영
- 인공지능 기본법에서 제시하는 책임성·공정성·투명성 원칙이 실제 사업 절차에 어떻게 반영되어야 하는지에 대한 해석은 기관별로 상이하게 이루어지고 있음

□ 계약·검수·운영 단계에서 인공지능 기본법의 원칙을 적용할 수 있는 기준 부재

- 공정성 확보나 설명 가능성 제고와 같은 법적 원칙이 계약서의 범위 설정, 검수 항목 구성, 운영 단계의 점검 기준으로 어떻게 구체화되어야 하는지에 대한 표준이 마련되어 있지 않음
- 결과적으로 인공지능 기본법은 공공 AI 서비스 도입을 위한 ‘방향타’ 역할은 수행하나, 실행력을 확보하기 위해서는 절차·지침과의 정합성 강화가 필수적
- 공공 AI 서비스가 법적 불확실성 없이 안정적으로 도입·운영되기 위해서는, 인공지능 기본법의 원칙을 기존 정보시스템 구축·운영 절차와 유기적으로 연결하는 제도적 보완이 필요

V

해외 공공AI 도입 절차·법제도 사례

1 EU: 위험기반 규율과 생애주기 중심 공공 AI 관리 체계

□ 위험 수준에 따른 차등 규율 체계 구축

- EU 인공지능법(AI Act)은 AI 시스템을 허용 불가(unacceptable risk), 고위험(high-risk), 제한적 위험, 최소 위험 등으로 구분
 - 특히 공공서비스 영역에서 활용되는 AI를 고위험 AI로 폭넓게 분류하여 엄격한 관리·통제 의무를 부과

□ 생애주기(lifecycle) 규율

- EU 공공 AI 제도의 핵심은 개발-배포-운영 전 과정을 포괄하는 ‘생애주기(lifecycle) 규율’에 있음
 - 고위험 AI에 대해서는 데이터 품질 관리, 기술 문서화, 위험 관리 체계 수립, 인간 감독(human oversight) 설계, 로그 기록, 사후 모니터링 등 개발 이후 운영 단계까지 포함하는 의무가 법률 차원에서 명확히 규정
 - 이는 AI를 ‘한 번 구축해 납품하는 시스템’이 아니라, 지속적으로 관리·점검해야 할 행정 수단으로 인식하고 있음을 시사

□ 공공 AI 도입 절차를 기존 정보시스템 구축 절차와 분리하여 재구성

- EU 사례는 공공 AI 도입 절차를 기존 정보시스템 구축 절차와 분리하여 재구성하고 있다는 점에서 시사점이 큼
 - 전통적인 기능 중심 검수나 일회성 성능 평가에 그치지 않고, 운영 과정에서의 성능 저하·편향 발생·위험 확대 가능성을 상시 관리하도록 제도화
 - 공공 AI 서비스의 책임성과 신뢰성을 구조적으로 담보하려는 접근
- 한국 공공 AI 도입 절차와 비교할 때, EU는 법률 차원에서 ‘운영 단계 관리’를 명시적으로 의무화하고 있다는 점에서 뚜렷한 차이를 보임

- 현행 우리나라 제도가 구축 완료 시점을 중심으로 사업 성과를 평가하는 구조라면, EU는 운영 단계에서의 준수 여부가 핵심적인 규제 대상
- 이는 한국형 공공 AI 도입 절차 개선 시 참고해야 할 중요한 제도적 시사점을 제공

2 미국: 기관 거버넌스와 영향(Impact) 중심의 공공 AI 관리

□ 기관별 거버넌스와 위험·영향 관리 중심

- 미국은 단일한 포괄적 AI 법률보다는, 기관별 거버넌스와 위험·영향 관리 중심으로 공공 AI 도입 체계를 구축
- 미국 연방정부는 공공부문 AI 활용에 대해 일괄적인 기술 규제보다는, 각 연방기관이 AI 사용에 따른 위험과 영향을 스스로 관리하도록 하는 거버넌스 중심 접근
- 이는 AI 기술의 빠른 변화에 유연하게 대응하기 위한 전략으로 평가됨

□ 권리·안전에 영향을 미치는 AI에 대한 관리 의무 명시

- OMB(행정관리예산국) 메모를 통해 ‘권리·안전에 영향을 미치는 AI’에 대한 관리 의무를 명확히 제시
- OMB는 연방기관이 AI를 도입·활용할 경우, 해당 AI가 국민의 권리, 안전, 기회 접근에 중대한 영향을 미치는지 여부를 사전에 식별하고,
- 이에 해당하는 경우 강화된 위험 관리, 내부 검토, 책임 체계를 적용하도록 요구
- 이는 AI 활용 자체를 제한하기보다는, 영향 수준에 따라 관리 강도를 차등화하는 방식

□ 기관 내부 책임성 강화

- 미국 공공 AI 관리 체계의 또 다른 특징은 ‘기관 내부 책임성 강화’에 있음
- 연방기관은 AI 활용 사례를 체계적으로 관리·공개하고, AI 사용에 대한 내부 승인 절차와 책임자를 지정하도록 요구받으며,
- 이를 통해 AI 활용의 투명성과 책임성을 기관 차원에서 확보하도록 설계

- 이러한 접근은 법률보다는 행정지침과 거버넌스를 통해 실질적인 통제력을 확보하려는 방식으로 이해할 수 있음

□ 도입절차를 기관 운영체계 흡수

- 한국과 비교할 때, 미국 사례는 공공 AI 도입 절차를 법률 중심이 아닌 ‘기관 운영 체계’로 흡수하고 있다는 점에서 차별성
- 한국은 공공 AI 도입 시 법적 근거와 절차 정합성 확보에 상대적으로 무게를 둬
 - 반면, 미국은 기관별 자율성과 책임을 전제로 AI 도입을 관리하고 있으며, 이는 향후 한국형 공공 AI 거버넌스 설계 시 참고할 수 있는 중요한 시사점을 제공

3 영국·싱가포르: 원칙 기반 규율과 실무형 프레임워크 중심

□ 영국 : 공공 AI 활용에 적용 가능한 공통 원칙을 제시

- 영국은 단일한 인공지능법을 제정하기보다는, 공공 AI 활용에 적용 가능한 공통 원칙을 제시하고 이를 기존 규제 체계에 연계하는 방식을 채택
- 영국 정부는 ‘AI Regulation White Paper’를 통해 안전성, 투명성, 공정성, 책임성, 이의제기 가능성 등 핵심 원칙을 제시하고,
 - 각 부문별 규제기관이 해당 원칙을 소관 영역의 공공 서비스와 정책에 적용하도록 하는 원칙 기반 규율 방식을 도입
- 이러한 접근은 기술 변화에 대한 규제의 유연성을 확보하는 장점이 있으나, 공공부문에서는 적용 편차가 발생할 수 있음
 - 공공 AI 서비스의 도입 절차와 관리 기준이 기관별로 다르게 해석·적용될 가능성이 존재하며, 특히 중앙정부와 지방정부, 대형 기관과 소규모 기관 간의 제도 이행 역량 차이가 공공 AI 품질 격차로 이어질 우려

□ 싱가포르 : AI거버넌스 프레임워크

- 싱가포르는 법률 중심 규율보다는 실무에 즉시 적용 가능한 ‘AI 거버넌스 프레임워크’를 통해 공공 AI 도입 절차를 구체화
- 싱가포르는 「Model AI Governance Framework」를 통해 데이터 관리, 인간 개입, 책임성, 투명성 확보 방안을 구체적으로 제시하고 있으며,
 - 공공부문에서도 해당 프레임워크를 활용해 AI 서비스 기획·개발·운영 전 과정에 적용 가능한 체크리스트와 가이드를 제공

□ ‘법률의 상세 규율’과 ‘현장 적용성’ 간 균형의 중요

- 영국과 싱가포르 사례는 공공 AI 도입 시 ‘법률의 상세 규율’과 ‘현장 적용성’ 간 균형의 중요성을 시사
- 영국이 원칙 중심 접근을 통해 제도적 유연성을 확보하고자 했다면, 싱가포르는 실무 프레임워크를 통해 공공기관이 실제 사업에서 활용할 수 있는 절차적 기준을 제공
 - 이는 한국형 공공 AI 도입 절차 설계 시 중요한 비교 기준으로 활용될 수 있음.

4 캐나다: 자동화 의사결정 중심 영향평가(AIA)

□ ‘알고리즘 영향평가(AIA)’를 의무적으로 수행

- 캐나다는 공공부문에서 자동화된 의사결정(Automated Decision-Making, ADM)을 활용하는 경우, ‘알고리즘 영향평가(AIA)’를 의무적으로 수행하도록 제도화
- 캐나다 정부는 「Directive on Automated Decision-Making」을 통해 공공 서비스에서 자동화된 의사결정 시스템을 도입할 경우, 사전에 AIA를 수행하여 해당 시스템이 국민의 권리, 공정성, 투명성, 책임성에 미치는 영향을 평가하도록 요구

□ 공공 AI 도입 절차에 직접적으로 결합된 실질적 관리 도구

- AIA는 질문지 기반 평가를 통해 AI 시스템의 영향 수준을 4단계로 분류하고, 영향 수준이 높을수록 강화된 검토, 설명 제공, 인간 개입, 감사 체계 등을 의무화하는 구조

- 이는 AI 도입 여부 자체를 제한하기보다는, 위험 수준에 따라 관리 강도를 조정하는 방식으로 공공 AI 서비스의 책임성과 수용성을 동시에 확보하려는 접근
- 앞서 살펴본 EU의 법률 중심 규율, 미국의 기관 거버넌스, 영국·싱가포르의 원칙·프레임워크 접근과 상이
- 캐나다는 AI 도입 전 단계에 구체적인 평가 도구를 삽입함으로써 공공 AI 도입 과정에서 발생할 수 있는 법적·윤리적 위험을 제도적으로 관리하고 있음

| 해외 공공AI 도입 절차·법제도 사례 |

구분	주요내용
EU	위험등급 기반으로 AI를 차등 규율하고 개발·운영 전 생애주기에 걸쳐 법적 의무를 부과하는 강한 규제 중심 체계를 구축
미국	법률 중심 규제 대신 기관별 거버넌스와 영향 기반 관리체계를 통해 자율성과 책임성을 동시에 확보하는 방식으로 운영
영국	공공 AI 활용에 대한 공통 원칙을 제시하고 이를 기존 규제 체계에 연계하는 원칙 기반 유연 규율 방식 적용
싱가포르	법률보다 실무 적용 가능한 거버넌스 프레임워크와 체크리스트를 통해 공공 AI 도입 전 과정의 실행력 확보
캐나다	자동화 의사결정에 대해 알고리즘 영향평가(AIA)를 의무화하여 도입 전 단계에서 위험 수준에 따라 관리 강도를 차등화하는 체계

5 해외사례 비교결과

□ ‘전 주기 관리’와 ‘위험 기반 절차 설계’ 필요

- 해외 사례 종합 시, 공공 AI 도입의 공통된 방향성은 ‘전 주기 관리’와 ‘위험 기반 절차 설계’로 수렴
- EU는 법률을 통해 운영 단계까지 관리 의무를 명확히 하고, 미국은 기관 책임 체계를 중심으로 영향 관리에 초점을 두며, 영국·싱가פור는 원칙과 실무 가이드를 통해 현장 적용성을 확보
- 이러한 해외 사례는 공공 AI 도입을 기존 정보시스템 구축 절차에 단순히 포함시키는 것이 아니라, AI의 위험과 특성을 반영한 별도의 절차적 장치를 마련해야 함 시사

VI

법제도 개선방안 및 정책적 제언

□ 기본 방향: '구축사업'에서 '전 주기 관리 체계'로의 전환

- 한국형 공공 AI 도입 절차 개선의 핵심은 공공 AI 서비스를 단일 구축사업이 아닌 '전 주기 관리 대상'으로 재정의하는 데 있음
- 기존 정보시스템 구축 절차는 완성형 시스템을 전제로 설계되어 AI 서비스의 반복적 학습·성능 변화·운영 중 위험 관리 특성을 충분히 반영하지 못하고 있음
 - 이에 따라 공공 AI 서비스는 기획-개발-검수-운영 전 과정을 하나의 연속된 관리 체계로 인식하는 절차 전환이 요구됨
- 인공지능 기본법은 공공 AI 도입의 '원칙 틀'을 제공하고, 정보시스템 구축·운영 지침은 이를 실행하는 '절차 도구'로 기능해야 함
 - 인공지능 기본법이 제시하는 신뢰성, 안전성, 책임성, 공정성 원칙은 공공 AI 서비스 전반에 적용되는 상위 기준으로 작동하되,
 - 실제 사업 추진 과정에서는 전자정부법 및 정보시스템 구축·운영 지침과 결합되어 구체적인 절차와 산출물로 구현될 필요
- 이를 위해 법률 간 역할 분담을 명확히 하고, 중복·공백 영역을 점차적으로 보완하는 접근이 필요
 - 개인정보 보호법은 데이터 처리의 적법성 기준을, 인공지능 기본법은 AI 시스템의 신뢰·안전 원칙 명확화
 - 전자정부법과 관련 지침은 사업 절차와 운영 관리 기준을 담당하도록 역할을 명확화

□ 'AI 사전검토-AI 전용 계약·검수·운영 단계 관리'

- 한국형 공공 AI 도입 절차는 'AI 사전검토-AI 전용 계약·검수·운영 단계 관리'로 이어지는 패키지 형태로 설계
 - 이는 해외 사례에서 확인된 위험 기반 관리와 전 주기 규율 흐름을 국내 제도 환경에 맞게 재구성

□ AI 사전검토(AI Gate) 도입 및 계약·검수 절차 개선

- 공공 AI 서비스 도입의 출발점으로서 ISP·기획 단계에 ‘AI 사전검토(AI Gate)’를 공식 절차로 도입할 필요
 - AI 사전검토는 해당 행정 과제가 AI로 해결하기에 적절한지, 규칙 기반 시스템이나 업무 프로세스 개선으로 대체 가능한지는 없는지 등을 사전에 판단하는 절차로, 무분별한 AI 도입을 방지하고 정책 효과성을 제고하는 역할을 수행
- AI 사전검토에서는 데이터·권리·책임·운영 관점의 최소 검토 항목을 표준화하여 적용 필요
 - 학습 데이터의 범위와 개인정보 포함 여부, 알고리즘이 행정 판단에 미치는 영향, 국민 권리 침해 가능성, 인간 개입 수준, 운영 단계에서의 모니터링·중단 기준 등을 기획 단계에서부터 검토
 - 이후 단계에서 발생할 수 있는 법적·제도적 리스크를 사전에 관리할 수 있음
- 계약 단계에서는 기존의 ‘완성형 납품’ 중심 구조에서 벗어나 AI 서비스 특성을 반영한 계약 모델로의 전환이 요구
 - AI 모델의 성능 고도화, 재학습, 운영 중 개선 활동을 계약 범위에 포함하고, 단순 구축 성과가 아닌 운영 단계의 품질 유지와 책임 이행을 계약 조건으로 설정
 - 이로써, AI 서비스가 실질적으로 기능할 수 있는 제도적 기반을 마련할 필요가 있음
- 검수 단계는 기능 구현 여부를 넘어 AI 품질과 위험을 점검하는 전용 체계로 개편
 - 정확도·안정성 등 기본 성능 지표뿐만 아니라, 편향 발생 가능성, 설명 가능성 수준, 운영 관리 체계의 적정성 등을 검수 항목에 포함
 - 이로써, 공공 AI 서비스가 운영 단계에서도 신뢰성을 유지할 수 있도록 하는 구조적 보완이 요구

□ 운영 단계 관리 강화 및 공공 AI 거버넌스 개선

- 공공 AI 서비스의 성과와 신뢰성은 구축 완료 시점이 아닌 운영 단계에서 결정되므로, 운영 관리 체계의 제도화가 필수적

- AI 서비스는 운영 환경과 데이터 변화에 따라 성능이 달라질 수 있으므로, 단순한 시스템 유지관리 중심의 운영 방식으로는 공공 AI 서비스의 품질과 책임성을 안정적으로 확보하기 어려움

○ 운영 단계에서는 인간 감독을 명확한 역할·권한·절차로 구체화 필요

- AI 판단 결과를 검토·조정·중단할 수 있는 담당자 지정, AI 결과에 대한 승인·보완 기준 설정, 과도한 AI 의존을 방지하기 위한 내부 통제 절차를 운영 기준으로 명확히 규정함으로써, AI와 공무원의 협업 구조를 제도적으로 정착

○ 상시 모니터링 체계를 통해 성능 저하·편향·오작동을 지속적으로 점검하는 구조 마련 필요

- 모델 성능 변화, 데이터 품질 저하, 민원·이의제기 발생 현황 등을 주기적으로 점검하고, 필요 시 재학습·개선 조치를 취할 수 있도록 운영 기준과 점검 주기를 명시함으로써, 공공 AI 서비스의 위험을 사전에 관리

○ 공공 AI 거버넌스는 기관 내부 책임 체계와 범정부 표준 제공이 병행되는 이원 구조로 설계

- 각 기관은 AI 서비스에 대한 실질적 책임과 운영 관리를 담당하고, 범정부 차원에서는 공통 기준·표준·가이드를 제공함으로써 기관 간 편차를 최소화하고 공공 AI 서비스 전반의 품질과 신뢰성을 제고

□ 공공 AI 서비스 도입을 위한 정책적 제언과 결론

○ 정책적으로는 인공지능 기본법의 원칙을 기존 정보시스템 구축·운영 절차에 실질적으로 결합하는 것이 핵심 과제

- AI 사전검토 도입, AI 전용 계약·검수 기준 마련, 운영 단계의 인간 감독 및 상시 모니터링 체계 구축은 공공 AI 서비스의 안정적 도입을 위한 제도적 장치로 기능해야 함

○ 단기적으로는 일부 공공 AI 사업을 대상으로 개선된 절차를 시범 적용하고, 이를 통해 표준화된 체크리스트·가이드·계약 모델을 정립 필요

○ 중·장기적으로는 정보시스템 구축·운영 지침 개정과 법제도 간 역할 분담 정비를 통해 공공 AI 도입 절차의 지속 가능성을 확보 필요

참고문헌

- 1) 대통령직속 디지털플랫폼정부, 「공공부문 초거대AI 도입·활용 가이드라인(2.0)」, (2025.4).
- 2) 디지털공간의 보안 및 규제에 관한 법률(LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique).
https://world.moleg.go.kr/web/wli/lgsllInfoReadPage.do?CTS_SEQ=54019&AST_SEQ=105, (2025.7.30).
- 3) 임영모·김리나·안성원, 2024년 공공부문 AI 도입현황 연구, 소프트웨어정책연구소, (2025.4).
https://spri.kr/posts/view/23866?code=data_all&study_type=&board_type=research.
- 4) Avi Perera, "AI Governance Frameworks: A Comparative Analysis", (November 2, 2024).
<https://aviperera.com/ai-governance-frameworks-a-comparative-analysis/>
- 5) Digital Gov Hub, "OMB M-25-22 Driving Efficient Acquisition of Artificial Intelligence in Government,"
<https://digitalgovernmenthub.org/examples/omb-m-25-22-driving-efficient-acquisition-of-artificial-intelligence-in-government/>
- 6) EU 「Artificial Intelligence Act」, EU Official Journal (12 July 2024).
- 7) European Commission, INSPIRE Directive
https://knowledge-base.inspire.ec.europa.eu/legislation/inspire-directive_en
- 8) FedRAMP, <https://www.fedramp.gov>, (2025.7.30. 방문).
- 9) G-Cloud 14, <https://www.crowncommercial.gov.uk/agreements/RM1557.14>, (2025.7.30. 방문).
- 10) Geoawesome, The INSPIRE Directive Explained: Simplifying Geospatial Data Sharing Across Europe,

- <https://geoawesome.com/the-inspire-directive-explained-simplifying-geo-spatial-data-sharing-across-europe/>, (2025.9.3.방문).
- 11) GOV.UK, National AI Strategy, (2021.9.22 공표, 2022.12.18. 최종 개정), <https://www.gov.uk/government/publications/national-ai-strategy>,(2025.9.6.방문).
 - 12) Govtrack.US, H.R. 353 (115th): Weather Research and Forecasting Innovation Act of 2017, <https://www.govtrack.us/congress/bills/115/hr353/summary>, (2025.9.3.방문).
 - 13) IMDA, "Singapore proposes framework to foster trusted Generative AI development," <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai>,(2025.9.6.방문).
 - 14) KEG Lawyers, "Revenge Porn Laws in California – Penal Code 647(J)(4) PC," <https://www.keglawyers.com/revenge-porn-penal-code-647j4>, (2025.9.3.방문).
 - 15) Legislation.gov.uk, Flood and Water Management Act 2010, <https://www.legislation.gov.uk/ukpga/2010/29/contents>, (2025.9.3.방문).
 - 16) Legislation.gov.uk, Voyeurism (Offences) Act 2019, <https://www.legislation.gov.uk/ukpga/2019/2>, (2025.9.3.방문).
 - 17) Niam Yaraghi, 'Transforming health care for older adults, Innovations, equity, and economics,'(August 2, 2023), <https://www.brookings.edu/articles/transforming-healthcare-for-older-adults/>, (2025.9.3.방문)
 - 18) Pair 공식 웹사이트, "Solutions for Public Good," <https://pair.gov.sg/pages/about>; GovTech, "Explore Pair, a government AI chatbot that helps public officers in Singapore conduct research, generate

- ideas, and compose messages.” (Last updated 8 July 2025),
<https://www.tech.gov.sg/products-and-services/for-government-agencies/productivity-and-marketing/pair>, (2025.7.29.방문).
- 19) Singapore Infocomm Media Development Authority & Personal Data Protection Commission, "AI Governance Framework 2nd Edition (PDPC)," <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>, (2025.9.6.방문).
- 20) The Ministry of Health and Prevention, France, "Digital Health Roadmap" (2023–2027), (May 2023),
https://extranet.who.int/countryplanningcycles/sites/default/files/public_file_rep/FRA_France_Digital-Health-Roadmap_2023-2027.Pdf, (2025.9.3.방문).
- 21) The White House, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", (2023.10.30.),
<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>, (2024.6.30.방문).
- 22) U.S. Department of Justice, The Fair Housing Act,
<https://www.justice.gov/crt/fair-housing-act-1>, (2025.9.3.방문).
- 23) US Congress.GOV, AI LEAD Act(S.2293),
<https://www.congress.gov/bill/118th-congress/senate-bill/2293/text>, (2025.9.6.방문).
- 24) US Office of Personnel Management, “The Artificial Intelligence Classification Policy and Talent Acquisition Guidance: The AI in Government Act of 2020,” (2024.4.29).