



MINBYUN-Lawyers for a Democratic Society
민주사회를 위한 변호사모임

서울 서초구 서초대로 46길 74
전화 02)522-7284, 팩스 02)522-7285
웹페이지 <http://minbyun.or.kr>
전자우편 admin@minbyun.or.kr

문서번호 : 26-10-디정위-01

수 신 : 각 언론사

발 신 : 민변 디지털정보위원회

제 목 : [디지털정보위][성명]AI 속도전의 경고음, 금융권 개인정보 유출은 서막에 불과하다 정부는 데이터 집중·연계 정책을 기본권의 관점에서 전면 재검토 하라.

전송일자 : 2026. 10. 6.(화)

전송매수 : 총 3매

[디지털정보위][성명]

AI 속도전의 경고음, 금융권 개인정보 유출은 서막에 불과하다 정부는 데이터 집중·연계 정책을 기본권의 관점에서 전면 재검토 하라.

최근 주요 금융기관에서 고객의 개인정보가 잇따라 유출되는 사건이 발생하였다. 특히 이번 해킹 사건에서는 공격자가 인공지능 도구(ARTEXT AI)를 활용해 다수 금융사를 대상으로 대량의 자동화된 공격을 한 것으로 전해지고 있다.

정부는 3대 메가프로젝트 정책 등을 내세 인공지능 시대의 국가경쟁력을 강조하며 인공지능 기술 개발과 도입에 속도를 내고 있다. 행정·금융·의료·교육 등 사회 전 영역에 인공지능을 확산하고, 이를 뒷받침하기 위하여 방대한 데이터를 수집·연계·활용할 수 있는 국가적 인프라 구축을 추진하고 있다. 국민의 개인정보는 이러한 인공지능 인프라를 구성하는 핵심 자원으로 다루어지고 있다.

그러나 우리는 이러한 인공지능 속도전에 제대로 대비하고 있는가?

이번 개인정보 유출 사고는 위험에 대응하기 위한 제도적·구조적 안전장치를 충분히 마련하지 않은 채 기술 적용 확대와 데이터 인프라 구축만을 앞세울 경우 발생할 일의 서막이다.

특히 AI 에이전트 기술이 정부와 기업을 비롯한 사회 각 영역에서 실제 업무를 수행하고, 다른 시스템과 연결되어 스스로 판단하고 행동하는 단계로 발전하면서 새로운 위험이 나타나고 있다. 인공지능이 단순한 정보 제공 도구를 넘어 데이터베이스에 접근하고, 명령을 실행하며, 다른 시스템을 제어할 수 있게 될수록 취약점 하나가 초래하는 피해의 범위는 급격하게 확대될 수 있다.

그럼에도 국민의 기본권과 사회 전체의 안전을 보호하기 위한 제도적 대비는 기술 발전의 속도를 충분히 따라가지 못하고 있고, 정부는 ‘속도전’에만 집중하고 있다.

현행 인공지능기본법은 일정한 영역의 ‘고영향 인공지능’과 일정한 기준에 해당하는 ‘고성능 인공지능’에 대하여 일부 규제체계를 마련하고 있을 뿐이다. 막대한 연산능력과 범용성을 바탕으로 다양한 시스템과 서비스에 적용될 수 있는 인공지능 모델, 그리고 이를 기반으로 실제 행위를 수반하는 AI 에이전트 등이 가져올 수 있는 위험을 사회적 차원에서 어떻게 통제할 것인지에 대해서는 여전히 충분한 제도적 장치가 마련되어 있지 않다.

인공지능의 활용 범위가 넓어지고 그 능력이 강력해질수록 그에 상응하는 안전장치와 책임체계 역시 함께 강화되어야 한다. 고성능·범용 인공지능에 대한 위험평가, 보안성 검증, 독립적인 외부 평가, 사고 보고 체계, 개인정보 접근권한 통제, 로그와 추적가능성 확보, AI 에이전트의 권한 제한과 비상정지 매뉴얼 등 구체적인 안전장치를 기술의 확산과 동시에 제도화 해야 한다.

국민의 개인정보를 한 곳에 집중하거나 여러 데이터베이스를 상호 연계하는 정책은 편의성과 인공지능 활용 가능성만을 기준으로 평가해서는 안 된다. 정보가 집중될수록 침해사고가 발생했을 때의 피해 역시 집중되고 확대된다. 국가적 데이터 인프라는 단순한 산업 기반이 아니라 국민의 기본권과 사회 전체의 안전에 직결되는 핵심 정보라는 관점에서 판단되어야 한다.

지금 필요한 것은 무조건적인 ‘속도전’이 아니다.

기술의 속도가 빠를수록 사회는 오히려 위험을 점검하고 대비할 수 있는 제도적인
멈춤의 장치가 필요하다. 위험성이 확인되면 적용을 중단하거나 제한할 수 있어야
하고, 충분한 안전성이 검증된 이후에야 그 기술이 사회로 나올 수 있어야 한다.

인공지능 시대의 진정한 경쟁력은 얼마나 빨리 기술을 도입하느냐만으로 결정되지
않는다. 강력한 기술을 얼마나 사회가 안전하게 통제하고, 국민이 신뢰할 수 있는
방식으로 사용할 수 있는지가 결국 그 사회의 인공지능 역량을 결정하게 될 것이다.

속도전이 아니라, 안전성과 신뢰성을 확보하기 위한 멈춤과 대비 체계를 함께 만들어
가야할 때다.

2026. 10. 6.

민주사회를 위한 변호사모임 디지털정보위원회