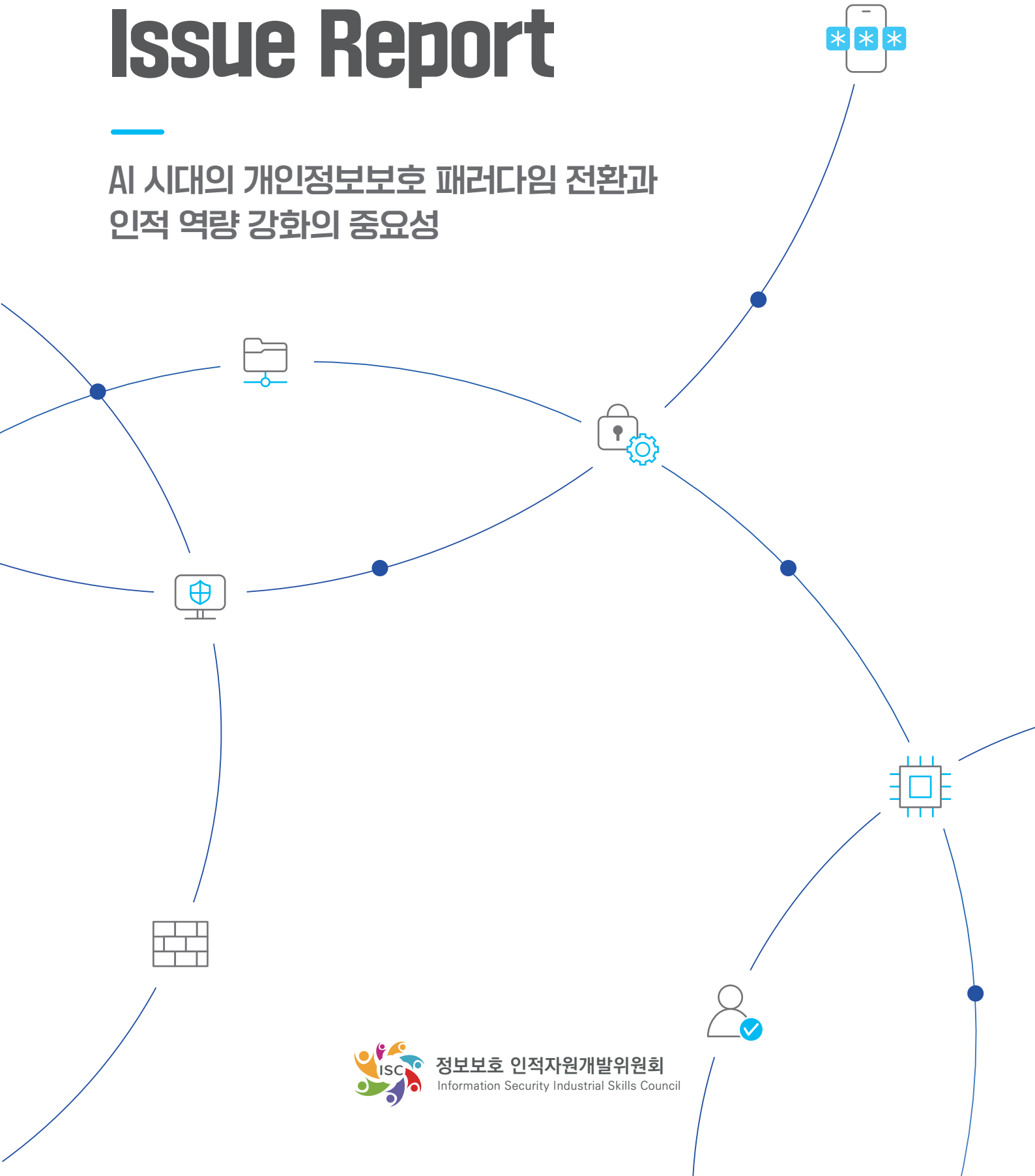
| 2025년 하반기

정보보호 인적자원개발위원회

Issue Report

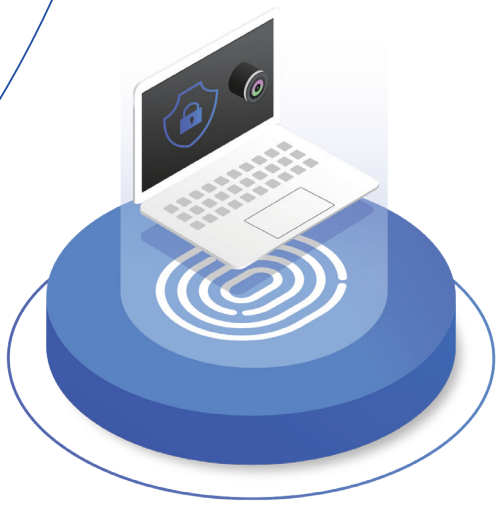
AI 시대의 개인정보보호 패러다임 전환과 인적 역량 강화의 중요성



정보보호 인적자원개발위원회
Information Security Industrial Skills Council

정보보호 인적자원개발위원회

Issue Report



CONTENTS

목 차

보고서 내용에 대한 문의는 아래의 연락처로 주시기 바랍니다.

정보보호 인적자원개발위원회 사무국 TEL. 02-6748-2011, 2039 E-MAIL. mhr0327@kisia.or.kr

본 이슈리포트는 가천대학교 법과대학 최경진 교수(인공지능·빅데이터 정책연구센터장)가 작성하였습니다.

01 머리말

인공지능(AI)은 4차 산업혁명의 핵심 동력으로서 사회 전반에 급속히 확산되고 있다. 특히 생성형 AI (Generative AI)와 대규모언어모델(LLM)의 등장은 단순한 기술적 진보를 넘어, 인간의 사고·의사결정·창작 활동은 물론 제조·운송·서비스 등 다양한 영역으로 확장되며 사회 구조와 가치체계 전반에 근본적인 변화를 일으키고 있다. 이러한 변화 속에서 개인정보는 AI 발전의 원천이자 동시에 가장 취약한 지점으로 부상하고 있다.

AI 시스템은 방대한 데이터를 학습하고 이를 기반으로 예측·분석·생성 기능을 수행한다. 이 과정에서 개인의 신상정보, 행동 패턴, 생체정보, 영상정보 등 민감한 데이터가 활용될 가능성이 높으며, AI 기술이 재식별(re-identification)이나 프로파일링(profiling) 기법을 통해 데이터 조각을 결합함으로써 개인을 간접적으로 식별하거나 차별적 결정을 내릴 위험성도 커지고 있다. 다시 말해, AI의 발전은 데이터 기반 사회로의 전환을 가속화하는 동시에 개인정보의 개념과 보호 방식에 대한 근본적 재정립을 요구하고 있다.

과거 개인정보보호의 초점이 '개별 데이터의 식별 가능성 여부'에 맞추어져 있었다면, 이제는 '데이터의 조합·추론을 통한 간접적 식별 가능성'과 'AI 의사결정 과정에서의 영향력'이 새로운 쟁점으로 떠오르고 있다. 특히 생성형 AI 서비스가 대중화되면서, 개인이 생성한 문서·이미지·음성 등의 콘텐츠가 학습 데이터로 활용되거나, 모델의 출력 과정에서 원저작자 혹은 특정 개인의 정보가 노출될 위험이 커지고 있다. 또한 AI가 방대한 비정형 데이터를 처리하는 과정에서 프라이버시 침해가 발생하더라도, 그 원인이나 책임 주체를 명확히 규명하기 어려운 점은 기존 법적 책임 구조의 한계를 드러내고 있다.

한편 전 세계는 미래 산업 경쟁력의 핵심을 AI에 두고 'AI 패권 경쟁'에 돌입하였다. 우리나라 역시 'AI G3'라는 국가 목표 아래, 인공지능 개발과 활용을 위한 범국가적 노력을 기울이고 있다. 이 과정에서 개인정보와 같은 가치 있는 데이터의 안전한 활용 기반을 마련하는 일은 AI 경쟁력 확보의 전제조건이라 할 수 있다. 실제로 각국은 AI 시대의 개인정보 침해 위험을 완화하는 동시에, AI 산업 발전을 위한 데이터 활용 촉진 정책과 법제 정비를 병행하고 있다.

결국 AI 시대에는 개인정보보호와 데이터 활용의 균형을 이루는 것이 핵심 과제이다. 개인정보보호와 AI 규제의 연계성과 조화를 어떻게 확보하느냐는 국가의 기술·법제 경쟁력을 좌우하는 문제로 부상하고 있다. AI 시대의 개인정보보호 패러다임을 정립하기 위해서는 기술혁신과 권리보호를 동시에 달성할 수 있는 균형 잡힌 시각이 필요하다. 개인정보보호는 단순한 권리 보호의 차원을 넘어, AI 신뢰성(trustworthiness) 확보의 핵심 전제이자 사회적 수용성의 기반이 된다. 개인정보가 안전하게 관리되지 않으면 사회 전반의 데이터 신뢰 체계가 흔들리고, 이는 곧 AI 경제와 산업 발전에도 부정적 영향을 미친다. 따라서 개인정보보호는 기술혁신의 제약이 아니라, 지속 가능한 AI 생태계를 위한 인프라이자 거버넌스의 핵심 기반으로 인식되어야 한다.

02 현재까지의 AI 및 개인정보보호 관련 정부 정책 추진 현황

1. AI기본법의 제정과 정책 추진체계

한국은 2025년 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」(이하 "AI기본법") 제정을 통해 국가 AI 정책의 방향성과 정부의 책무를 법률적으로 명확히 하였다. 동 법은 윤리성·안전성·신뢰성을 핵심 가치로 규정하고, 국가 차원의 거버넌스 체계인 국가AI전략위원회 설치, 투명성 의무 및 신뢰성 검·인증 제도, 고영향 AI 중심의 안전성 관리 등 다양한 규제·지원 장치를 도입하였다.

현재 정부는 AI기본법의 시행을 위한 하위법령을 마련 중이며, 과학기술정보통신부는 2025년 9월 「AI 기본법 하위법령집(안)」을 공개하였다. 여기에는 시행령(안), 시행규칙(안), 주요 가이드라인(안)이 포함되어 있으며, 산업 전반의 의견수렴이 진행 중이다.

또한 정부는 'AI G3' 실현을 위한 핵심 기반으로 데이터 혁신을 제시하고, 산업통상부·과학기술정보통신부·문화체육관광부·개인정보보호위원회 등 관계부처 간 협업을 통해 개인정보를 포함한 데이터의 안전한 활용 체계 구축을 추진하고 있다.

2. 개인정보 보호법 개정 및 신기술 연계 제도

2023년 개정된 「개인정보 보호법」은 정보주체의 통제권을 실질적으로 강화하고, AI 등 신기술 환경에 대응하기 위한 제도적 장치를 도입하였다. 개정법의 주요 내용은 다음과 같다.

- **개인정보 이동권(전송요구권) 도입:** 정보주체가 자신의 개인정보를 본인, 개인정보관리 전문기관, 또는 안전조치 의무를 이행하고 대통령령상 기준을 충족한 자에게 전송하도록 요구할 수 있는 권리 신설.
- **자동화된 의사결정 대응권 도입:** 인공지능 등 자동화된 결정이 개인의 권리나 의무에 중대한 영향을 미치는 경우, 정보주체가 이를 거부하거나 설명을 요구할 수 있도록 보장.
- **온·오프라인 규제체계의 일원화:** 종전 「정보통신망법」에서 분리되어 있던 온라인 사업자 특례 규정을 통합하여, 동일 행위에 대해 사업자 유형별로 상이하게 적용되던 불균형을 해소.
- **국외 이전 규제 정비:** 개인정보 국외 이전 허용 범위를 확대하고, 국제 기준(GDPR 등)에 부합하도록 제도를 개선.

아울러 정부는 AI 데이터 규제특례제 도입, 「데이터산업법」 개정, 공공데이터 품질관리 고도화 등 다양한 정책을 추진하고 있으며 AI 학습 및 활용의 전 단계에서 개인정보의 안전한 이용을 보장하기 위한 방안을 모색하고 있다. 그럼에도 불구하고, 법체계 간 중복과 공백, 개인정보 개념의 불명확성, 기술적 발전에 신속히 대응하는 역량의 부족 등은 향후 보완이 필요한 핵심 과제로 지적된다.

3. AI 혁신 지원을 위한 제도적 노력

개인정보보호위원회는 AI 학습 단계에서의 개인정보 활용을 지원하기 위해 2025년 「생성형 인공지능(AI) 개발·활용을 위한 개인정보 처리 안내서」를 발표하였다. 이 안내서는 '인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서'와 'AI 프라이버시 리스크 관리 모델' 등을 바탕으로, 사전실태점검·규제샌드박스·사전적정성 검토 등 정책 경험을 체계화한 것이다. 이 안내서는 AI의 수명주기(lifecycle)를 ① 목적 설정, ② 전략 수립, ③ 학습 및 개발, ④ 시스템 적용 및 관리의 4단계로 구분하고, 각 단계별로 사업자가 준수해야 할 개인정보보호 고려사항을 구체적으로 제시하였다. 또한 조사·처분 사례 및 혁신지원제도 사례를 함께 수록하여, 사업자들의 실무적 이해를 높이고 자율적 준수 문화를 확산하고자 하였다.

더불어 2025년 9월 발표된 「가명정보 제도·운영 혁신방안」에서는 평균 310일이 소요되던 가명정보 결합 절차를 100일 이내로 단축하고, 클라우드 기반 개인정보 이노베이션존을 구축하여 지역적 한계를 극복하는 데이터 결합·분석 환경을 조성하려는 정책 개선 방향을 제시하였다. 정부는 AI 학습용 데이터셋 공급을 확대하고, 개인정보 특화 인재 양성 프로그램도 병행 추진할 계획이다.

4. 종합 평가 및 향후 과제

이상의 정책적 노력은 AI 시대의 개인정보보호와 데이터 활용 간 조화를 도모하기 위한 중요한 진전으로 평가된다. 그러나 AI 혁신과 개인정보보호의 실질적 병행을 위해서는 이상의 다양한 제도 개선 노력과 함께 신뢰 기반의 자율규제 모델 구축이 필요하다. 특히 다음 세 가지 과제가 핵심으로 제시된다.

- AI기본법과 개인정보 보호법을 축으로 한 통합 거버넌스 설계
- 글로벌 호환성이 확보된 AI 인증·평가제도의 실효적 운영 및 감독 체계 정립
- 개인정보보호위원회의 전문적·기술적 역량 강화

이러한 체계적 접근을 통해서만 AI 혁신과 개인정보보호가 상호 대립이 아닌 상호 신뢰와 상생의 축으로 자리를 잡을 수 있을 것이다.

03 AI 악용과 개인정보 침해 사고 동향 및 효과적인 대응의 필요성

1. 주요 악용 유형

(1) 생성형 AI를 통한 개인정보 재식별 및 유출

최근 대규모언어모델(LLM) 기반의 생성형 AI 서비스가 폭발적으로 확산하면서, 이용자 대화기록·입력데이터·학습데이터에 포함된 개인정보가 비의도적으로 노출되는 사례가 발생할 수 있다. AI의 일시적 시스템 오류로 인해 일부 이용자의 이름·결제내역·대화내용이 다른 사용자에게 노출되는 경우에 AI 서비스의 학습 및 출력 단계에서 개인정보 통제 불능 위험이 발생할 수 있다. 이러한 문제는 단순한 보안사고가 아니라, AI 모델의 구조적 특성에서 기인한다. 생성형 AI는 학습 데이터의 통계적 패턴을 기반으로 결과를 산출하므로, 학습 과정에서 포함된 개인정보가 완전히 삭제되거나 익명화되지 않으면, '모델 기억(model memorization)' 형태로 남아 추후 재출력될 가능성이 있다. 즉, 데이터 삭제권(right to be forgotten)이 실질적으로 보장되지 않는다면 기존 개인정보보호 법제가 전제한 '데이터 주체의 통제권' 개념이 도전에 직면할 수 있다.

(2) AI 모델 학습데이터의 불법 수집 및 무단 이용

AI 개발기업이 모델 성능을 높이기 위해 웹상의 공개 데이터를 대량 수집하는 과정에서, 저작권과 개인정보보호 규정을 동시에 위반하는 사례가 발생할 수 있다. 예를 들어, 세계 최대의 시각콘텐츠 데이터베이스를 보유한 Getty Images는 Stability AI가 학습데이터에 포함된 이미지 무단 이용했다고 주장하며 2023년 1월 영국, 2월 미국에서 각각 저작권 침해 및 상표권 침해 소송을 제기하였다. 국내에서도 유사한 문제가 확인되고 있다. 한국방송협회는 네이버와 네이버 클라우드를 상대로 올해 초 AI 저작권 침해에 대해 공중파 3사에 2억 원씩, 총 6억 원을 배상하도록 하는 소송을 제기했다.

이처럼 AI 학습데이터의 불법 수집 문제는 데이터 활용 촉진정책과 개인정보보호정책의 경계를 재조정할 필요성을 제기한다. 데이터가 혁신의 원천이면서도 기본적 권리에 대한 침해의 근원이 될 수 있다는 이중적 속성은 향후 정책 설계 시 가장 신중한 고려를 요한다.

(3) AI 기반 딥페이크, 음성합성 등 위장·사기형 침해사례

AI 기술이 고도화되면서, 시각·음성 합성 기술을 이용한 사회공학적 범죄(social engineering)가 급증하고 있다. '딥페이크(Deepfake)' 기술은 인물의 얼굴, 음성, 행동을 실시간으로 합성하여 허위정보를 유포하거나, 사기·성착취 등 범죄에 악용되고 있다. 2024년 2월 홍콩에서는 글로벌 대기업 직원이 최고재무책임자

(CFO)가 개설한 영상회의에 참석하던 중 상사의 얼굴과 목소리를 딥페이크로 위조한 공격자에게 속아 2억 홍콩달러를 송금하는 사건이 발생했으며, 이는 AI 사기의 실질적 피해가 심각하게 증가할 수 있다고 경고하는 사건으로 평가할 수 있다. 국내에서도 유명 연예인이나 일반인의 얼굴을 합성한 불법 촬영물 제작·유포 사례가 급증하고 있으며, 이러한 범죄는 「정보통신망법」, 「성폭력처벌법」 등 기존 형사법 체계로는 완전한 예방이 어렵다.

이와 같은 AI 위장형 사기는 개인정보보호의 관점에서도 심각한 위협이다. 합성된 영상이나 음성이 실제 개인의 신원을 모방함으로써 '본인확인제도', '인증체계', '디지털 신뢰 인프라'를 근본적으로 훼손할 수 있기 때문이다. 따라서 AI 신원보호(identity protection)와 진위확인(authenticity verification) 기술의 고도화가 시급한 과제로 부상하고 있다.

(4) 알고리즘 편향 및 차별로 인한 개인정보 침해

AI 알고리즘은 학습데이터의 통계적 특성을 반영하므로, 데이터 내 편향(bias)이 존재할 경우 결과적으로 특정 집단이나 개인에 대한 차별을 야기할 수 있다. 이는 개인정보의 부당한 프로파일링, 자동화된 의사결정, 신용평가 차별 등으로 이어질 수 있으며, 결과적으로 개인의 정보자기결정권을 침해한다.

예컨대 미국의 아마존 채용 알고리즘은 과거 남성 중심의 인사데이터를 학습한 결과, 여성 지원자의 이력서를 자동으로 낮게 평가하는 편향을 보여 폐기된 바 있다. 국내에서도 일부 금융기관의 신용평가 AI가 연령·주소·학력 등 비민감정보를 조합해 간접적 차별 효과를 발생시킨 사례가 보고되고 있다.

이러한 문제는 단순한 기술적 오류가 아니라, 데이터 설계 및 거버넌스 부재의 결과로서, 향후 AI 규제체계 내에 개인정보보호와 공정성 평가를 동시에 반영하는 통합적 평가모델의 구축이 요구된다.

2. 최근 잇달아 발생한 개인정보 유출 사고

최근 국내에서는 개인정보 유출 사고가 다시 빈번히 발생하고 있으며, 특히 대기업 및 공공기관을 대상으로 한 해킹·크리덴셜 스터핑(Credential Stuffing) 등 고도화된 공격이 두드러지고 있다. 예를 들면, 홈쇼핑·편의점 계열 기업의 웹사이트 해킹 사건에서는 2024년 6월 21일 ~ 2025년 2월 13일 기간 동안 약 158만 건의 개인정보 유출 정황이 확인되었다. 유출 정보에 다행히 금융정보는 포함되지 않은 것으로 확인되었지만, 이름·성별·생년월일 등 다양한 주요 개인정보가 포함되었다. 공격 유형은 크리덴셜 스터핑 기법으로, 다수의 계정·비밀번호 조합을 무작위 대입해 로그인에 성공하는 방식이었다. 이에 대해 비정상 로그인 차단, 비밀번호 변경 권고, 보안위원회 신설, 정보보호 투자 확대 등의 대응이 이루어졌다. 생활뷰티 유통 기업의 해킹 사건에서는 2025년 3월 11일 밤 ~ 3월 12일 새벽 동안 약 6만여 개 IP에서 로그인 시도가 있었고, 이 중 약 4,900건이 실제 로그인에 성공한 것으로 분석되었다. 유출 가능성이 있는 정보로는 이름·수령인 정보(휴대전화번호·주소·현관출입방법)·프로필 사진·닉네임·피부타입·피부고민 정보 등이 포함되었으며, 비정상 계정 잠금, 자동입력 방지 기술 적용, 시스템 모니터링 강화 등의 대응이 이루어졌다. 대형 통신사의 해킹

사건에서는 상당기간 서버가 해킹에 노출되었는데, 해커가 28대 서버에 33개의 악성코드를 설치한 뒤 가입자 식별번호(IMSI) 등 약 2,696만 건의 개인정보 유출 가능성이 제기되었다. 전 국민적인 관심으로 전국 매장에서 무료 SIM 교체, 향후 5년간 보안 투자 7,000억 원 계획, 신규 가입·번호 이동 일시 중단 등이 대응책으로 시행되었다. 정보유출은 민간에만 머무르지 않는다. 민간 보안업체에 따르면 다크웹 상 유출된 한국인의 개인정보 규모가 4억 6천만 건으로 추산되고 있다. 공공 취업정보포털에서도 23만 명 이상 구직자의 개인정보 및 일부 금융정보가 외부로 유출된 바 있다.

가장 최근에는 또 다른 대형 통신회사에서 개인정보 유출 사건이 발생했다. 최초로 개인정보 유출 정황이 감지된 시점은 2024년 10월경인데, 이후 불법 펨토셀 ID가 20개로 확인되는 등 범위가 확대되었다. 피해자 규모 및 피해액은 조사 확대에 따라 증가하고 있으며, 불법 기지국 접속 이력이 있는 이용자 수가 수천 명 이상으로 파악된 바 있다. 언론을 통해서 "펨토셀을 통해 인증문자(SMS)나 ARS(자동응답) 음성이 탈취됐을 가능성"이 제기되고 있고, 단순히 기지국 장비 문제만이 아니라 이미 유출된 개인정보(DB)와 결합된 조직적 공격 가능성도 거론되고 있다. 이 사건은 통신 인프라의 보안 취약성과 기존 유출된 개인정보의 악용이 결합된 형태로, 어느 한 조직만의 문제로 보기 어렵다는 점이 특징이다. 또한 피해 대응 및 책임 소재가 명확히 정립되기 이전에 피해 규모가 확대된 점, 그리고 기업 내부의 모니터링 및 보안 체계가 사전에 기능하지 못했던 점이 지적되고 있다. 이번 사례는 특히 AI와 데이터 기반 사회에서의 개인정보 리스크가 단순히 '식별정보 유출' 차원을 넘어서 통신 및 인증 수단까지 영향을 받는 복합형 리스크로 진화했음을 보여주는 AI 시대의 중대한 경고 신호라 할 수 있다.

3. 규제적 함의 및 시사점

AI 악용사례는 단순한 기술적 결함이 아닌 거버넌스의 공백, 법제 미비, 인력 역량 부족, 개인정보 감수성의 부족 등 다양한 요인이 복합적으로 작용한 것으로 평가할 수 있다.

우선, AI 서비스 전 주기에 걸친 개인정보보호 점검 체계가 불충분한 것으로 평가된다. 개발·학습·운영 단계별 책임주체를 명확히 구분하고, 사전 영향평가 및 인증제도를 강화할 필요가 있다.

둘째, AI의 복잡한 학습구조로 인해 개인정보 침해의 인과관계를 규명하기 어려운 만큼, 집단적 분쟁조정 및 피해구제 시스템을 개선해야 한다. 현행 「개인정보분쟁조정위원회」의 역할을 확장하거나, AI 관련 전문 분쟁해결 기구를 신설하는 방안도 검토될 수 있다.

셋째, 악용 방지의 관건은 기술적·인적 역량의 강화이다. 개인정보보호 담당자, 개발자, 법률가가 협력하여 'AI 프라이버시 엔지니어링(Privacy by Design for AI)'을 구현할 수 있도록 전문인력 양성 및 역량 강화 체계가 필요하다. 결국 AI 악용사례에 대응하기 위한 핵심은 "규제 중심의 사후 대응"에서 "예방 중심의 신뢰 프레임워크"로 무게추를 옮기는 패러다임 전환이 필요하며, 이는 개인정보보호의 정책적 중요성과 인적 역량 강화 논의의 기초가 된다.

04 개인정보보호의 정책적 중요성 및 핵심적 고려요소

1. AI 시대 개인정보 감수성

AI 시대의 개인정보보호는 단순한 법적 규제나 기술적 대응의 문제만이 아니라, 인간의 존엄성과 사회적 신뢰를 지탱하는 근본 가치의 문제로 자리 잡아 가고 있다. 생성형 AI와 초대규모 데이터 분석 기술이 확산되면서, 개인은 자신도 모르는 사이에 다양한 경로를 통해 정보가 수집·결합·활용되는 환경에 놓여 있다. 이러한 상황에서 개인정보의 의미는 단순한 "데이터 항목"을 넘어, 개인의 정체성과 사생활, 그리고 사회적 존재로서의 자율성을 포함하는 것으로 확장되고 있다. 이러한 변화 속에서 가장 중요한 것은 '개인정보 감수성(personal data sensitivity)'의 회복이다. 개인정보 감수성이란 타인의 개인정보를 단순한 정보가 아닌 '개인의 삶을 구성하는 요소'로 인식하고, 이를 다룰 때 주의와 존중을 기울이는 윤리적 태도를 의미한다. 이는 정보주체인 개인뿐 아니라, 데이터를 처리하고 관리하는 기업·공공기관의 실무자와 책임자에게도 필수적인 덕목이다. 기업의 경우 개인정보 감수성은 법규 준수(compliance)를 넘어, 신뢰 기반의 경영문화와 조직 윤리의 척도로 삼아야 한다. AI 모델 개발자나 데이터 관리자, 경영진이 데이터의 가치와 위험을 동시에 인식하고, 사소한 부주의가 개인의 기본적 자유와 권리에 대한 침해뿐만 아니라 사회적 신뢰를 무너뜨릴 수 있음을 자각해야 한다. 정부와 공공기관 역시 마찬가지로, 행정의 효율성이나 혁신만을 앞세우기보다 국민의 개인정보를 다루는 과정 전반에서 세심한 존중과 투명한 설명 책임을 실천해야 한다. 결국 실무자·책임자·정책결정자 모두가 개인정보 감수성을 기본자세로 내면화할 때, 공공과 민간의 데이터 거버넌스는 진정한 신뢰를 얻게 된다.

AI 시대의 개인정보 감수성 존중은 기술 혁신의 속도를 늦추기 위한 제약이 아니라, 지속 가능한 AI 디지털 신뢰 생태계를 위한 전제조건이다. 개인정보가 인간 중심적 가치 속에서 존중받을 때만이 AI 시스템 역시 사회로부터 정당성을 부여받을 수 있다. 따라서 정부 정책은 개인정보보호를 단순한 규제나 의무로 한정하기보다, 개인·조직·사회 전반의 개인정보 감수성을 강화하는 방향으로 설계되어야 한다.

이러한 관점에서 개인정보보호는 "AI 시대의 시민적 교양"으로 이해될 수 있다. 데이터 리터러시 교육, 공공·민간의 인식제고 프로그램, 책임자 대상의 전문교육 등 개인정보 감수성 중심의 역량 강화 정책이 병행되어야 하며, 이를 통해 개인정보보호는 기술 혁신과 대립하지 않고 신뢰와 투명성의 기반 위에서 AI 발전을 지탱하는 공공 인프라로 기능하게 될 수 있다.

2. 개인정보보호와 데이터 활용 간의 균형

AI 시대의 개인정보보호 논의는 필연적으로 데이터 활용과 보호의 균형이라는 핵심적 과제에 직면한다. 데이터는 AI 혁신의 원천이지만, 동시에 개인정보 침해의 주요 경로가 되기도 한다. 지나치게 엄격한 규제는 혁신을 저해하고, 반대로 완화된 규제는 국민의 신뢰를 훼손한다.

현재 가명정보 처리 특례 규정 등을 통해 개인정보 활용을 유연화하고 있지만, 현실적으로는 법적 불확실성으로 인해 데이터 활용이 위축되는 현상이 여전하다.

3. 법제·거버넌스 체계의 다층화 및 역할 분담

AI와 개인정보보호를 둘러싼 법제 환경은 복잡하게 다층화되고 있다. 국내에서는 AI기본법, 개인정보 보호법, 정보통신망법, 데이터산업법, 공공데이터법, 위치정보법, 신용정보법, 전자정부법 등 다수의 법률이 병존하며, 기관 간 역할이 중첩되는 현상이 발생하고 있다. 현재 개인정보보호위원회는 개인정보 관련 독립적 감독기구로서의 지위를 확보하고 있으나, AI 신뢰성·안전성 측면에서는 과학기술정보통신부, 산업통상부, 중소벤처기업부, 방송통신미디어위원회 등 여러 부처가 관련 업무를 병행하고 있다. 이러한 분절적 거버넌스 구조는 법령 해석의 불일치와 정책 실행의 비효율을 초래할 가능성이 있다. 결국 거버넌스 이슈의 핵심은 "일관성을 보장하는 통합·조정과 현장의 실행력"을 동시에 확보하는 것이며, 이를 위해 기관 간 역할 분담과 협력 프로토콜을 제도화하는 것이 중요하다.

4. 사회적 신뢰 회복과 디지털 안전망 구축

AI의 신뢰성과 개인정보보호는 상호 의존적인 가치이다. 개인정보 유출이나 AI 오남용 사건이 반복될수록 국민의 디지털 서비스에 대한 신뢰가 약화되고, 이는 국가 전체의 디지털 전환 속도를 저하시킨다. 따라서 개인정보보호는 단순한 법적 규제가 아니라 사회적 신뢰 인프라(Social Trust Infrastructure)로 인식되어야 한다. 특히 최근 공공시스템 화재, 금융·배달·의료 분야 해킹 등 일련의 사건은 AI 기반 및 데이터 보안의 물리적·제도적 취약성을 여실히 드러냈다. 이러한 사건들은 국민에게 AI·디지털 전환의 혜택보다 불안과 불신을 더 크게 인식시키는 결과를 낳고 있다. 이에 대응하기 위해 정부는 최근 정보보호 및 개인정보보호를 강화하기 위한 대책을 마련하고 있는데, 아래와 같은 방향이 중대하게 고려 또는 반영되어야 한다.

- **전 생애주기 데이터 보호체계 확립:** 수집·저장·활용·삭제 등 데이터의 전 생애주기에서 개인정보의 안전성을 평가하고 관리하는 통합적 보호체계 마련
- **AI 신뢰성 검·인증 체계의 신속한 구축:** AI 서비스의 개인정보보호 수준과 안전성을 객관적으로 검증하는 AI 신뢰성 검인증 체계를 글로벌 동향과 보조를 맞추면서도 실효성을 가질 수 있도록 신속하게 구축
- **공공 데이터 인프라 보호 강화:** 국가정보자원관리원, 지방자치단체 등 공공 데이터센터의 보안·복구체계 강화 및 정기적 취약성 점검 제도화

- **사회적 공감대 형성:** 개인정보보호를 단순한 '규제'가 아닌 'AI·디지털 기반'으로 인식시키기 위한 대국민 홍보·교육 강화.

이와 같은 신뢰기반 체계는 AI G3 국가전략의 핵심 인프라이며, 데이터경제와 인공지능산업 발전의 지속가능성을 보장하는 필수 요소가 될 것이다.

5. 정책 방향성

AI 시대의 개인정보보호는 기술·법제·사회·경제 전반을 아우르는 핵심적인 거버넌스 문제로 진화하고 있다. 개인정보의 개념과 보호대상이 확장됨에 따라, 규제의 패러다임 역시 단일 법률 중심이 아니라 다층적·협력적 구조로 재설계되어야 한다. 또한 개인정보보호는 국가 경쟁력의 제약 요인이 아니라, 신뢰기반 AI·디지털 경제의 촉진자(enabler)로 인식되어야 한다. 이를 위해 '사후규제'와 '사전예방'의 적절한 조화와 함께 '법률 집행'에만 의존하지 않고 '역량강화'에도 정책적 중심추를 놓아야 한다.

05 맺음말

AI 시대의 개인정보보호는 더 이상 기술적 문제나 법적 규율의 단편적 접근만으로 해결될 수 없는 복합적 과제가 되었다. 데이터를 설계하고 분석하고 관리하는 과정의 모든 지점에서, 인간의 이해력과 판단력, 그리고 책임의식이 핵심적인 역할을 한다. AI 시스템의 신뢰성은 결국 사람의 선택과 규범적 기준 위에 세워지는 것이며, 이를 떠받치는 것은 인적 역량(human competence)이다. 기업과 공공기관은 망분리, 고도화된 기술 보호조치나 규제 준수에 머물지 않고, AI 개발자·데이터 관리자·개인정보보호책임자(CPO) 등 실무자들이 스스로 위험을 식별하고 대응할 수 있는 '개인정보 감수성' 기반의 전문성을 갖추도록 지원해야 한다. 이는 단순한 교육 차원을 넘어, 조직 내 의사결정 구조와 문화 전반에 개인정보 존중 원칙을 내재화하는 과정이 되어야 한다. 정책적으로도 개인정보보호를 "AI 혁신의 제약"이 아니라 "지속 가능한 AI 혁신의 인프라"로 인식해야 한다. 정부와 기업이 공동으로 개인정보보호 인력을 체계적으로 양성하고, 실무 중심의 훈련과 인증제도를 강화함으로써 데이터 거버넌스 전반의 질적 수준을 끌어올릴 필요가 있다. 또한 현장 실무자들이 법령 해석과 기술 이해를 동시에 습득할 수 있도록 융합형 인재 양성 체계를 마련해야 한다. AI와 개인정보보호의 관계는 이제 경쟁이 아니라 공존의 영역으로 나아가야 한다. 개인정보가 신뢰받지 못하는 사회에서는 AI의 발전도 결코 지속될 수 없으며, 데이터를 다루는 사람의 개인정보 감수성 수준이 곧 사회의 디지털 신뢰 수준을 결정한다는 인식을 모두 공유해야 한다. 결국 인적 역량 강화는 AI 윤리, 데이터 거버넌스, 보안 정책을 연결하는 모두의 노력과 많은 시간이 요구되는 힘든 길이지만, 가장 근본적이면서도 현실적인 효과가 확실히 보장되는 전략적인 해법인 셈이다. 결국 AI 시대의 개인정보보호는 사람과 신뢰의 문제이며, 제도와 기술이 이를 뒷받침해야 한다. 지속 가능한 AI·디지털 전환의 토대로서 미래 세대를 위한 가장 중요한 투자가 될 것이다.

정보보호ISC가 바라본 AI 시대 ISC의 역할과 시사점

- **AI 기술 확산에 따른 적합한 인재양성 체계 전환**

  생성형 AI와 대규모언어모델(LLM)의 급속한 확산은 산업 전반의 업무 방식과 가치사슬을 재편하고 있다. 데이터를 어떻게 활용하고 보호하느냐가 곧 기업과 국가의 경쟁력을 좌우하는 시대가 도래하였다.

  현재의 환경 변화에 대응하기 위해서는 개인정보보호 관련 법·제도에 대한 이해, 기술적 역량과 더불어 AI 및 데이터 활용·관리 역량을 겸비한 융합형 전문인재 양성이 요구된다. 따라서 산업 현장의 수요에 부합하는 다양한 역량을 종합적으로 다루는 교육 콘텐츠를 확충할 필요가 있다.

  또한, 빠른 변화가 이루어지는 산업 특성에 따라 개인정보보호 분야의 산업동향과 직무변화를 정기적으로 모니터링하고, 이를 통해 도출된 직무역량이 NCS와 SQF에 신속히 반영되도록 지원하여 인력양성체계의 기반을 강화해 나가야 할 것이다.

- **산업 전반의 개인정보보호 감수성 제고**

  AI 기술의 확산은 개인정보 침해 양상을 변화시키고 있다. 사회 전반에서 나타나는 생성형 AI를 활용한 개인정보 재식별, 학습 데이터 불법 수집 등은 기술적 문제를 넘어 개인정보 보호에 대한 인식 부족에서 비롯된 결과로도 볼 수 있다.

  AI 시대의 '개인정보보호'는 법무나 보안부서만의 과제가 아닌 전 직군이 내재화해야 할 기본 역량으로 자리 잡아가고 있다. 따라서 산업 전반에 '개인정보보호'를 조직의 신뢰와 경쟁력 확보의 핵심 가치로 인식하게 하는 문화적 전환이 필요하다.

  이를 위해 산업현장의 인력이 갖추어야 할 개인정보보호 기초 역량에 대한 정의가 선행되어야 한다. 또한 주요 위험요인을 반영한 '개인정보 감수성 향상 교육'을 개발·확산하고, 개인정보 취급 수준에 따라 사례 중심의 실무교육 강화를 지원함으로써, 사회 전반의 개인정보보호 수준을 지속적으로 높여 나가야 할 것이다.

현시대의 '개인정보보호'는 단순한 기술적 과제를 넘어 사회적 신뢰와 책임의 문제로 확장되고 있다. 기술과 인식이 조화를 이룰 때 비로소 지속 가능한 혁신 또한 가능하므로, 개인정보보호와 AI가 균형을 이루며 발전할 수 있도록 관련 인력양성과 정책 기반 마련에 꾸준히 주력할 필요가 있다.

정보보호 인적자원개발위원회

Issue Report

AI 시대의 개인정보보호 패러다임 전환과 인적 역량 강화의 중요성

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

(05717) 서울특별시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회