NEWS LETTER

2025-07-31

Legal Issue

- 데이터 중력:디지털 경제의 보이지 않는 힘, 문제점과 법적 과제
- EU AI Act의 핵심과 한국 법제의 방향성

MINWHO News

- 김경환 변호사, 제 21회 오피스키퍼 보안 세미나에서 '사이버 복원력 강화 차원에서 발생 가능한 법적 대응 전략과 기업 차원의 대응 프레임워크'를 주제로 강의
- 양진영 변호사, 중앙일보와 'AI학습과 저작권 분쟁에서 국내·외 판례 동향' 관련 인터뷰

Business CASE

법무법인 민후

법무법인 민후

Legal Issue

데이터 중력:디지털 경제의 보이지 않는 힘, 문제점과 법적 과제

김경환 대표변호사

2010년 데이브 맥클러리가 제시한 데이터 중력(Data Gravity)은 현대 디지털 경제의 구조와 권력 관계를 이해하는 핵심적인 개념이다. 이 개념은 한곳에 대규모로 축적된 데이터가 다른 데이터는 물론 애플리케이션, 서비스, 그리고 기술 인력까지 자신의 위치로 강력하게 끌어당기는 현상을 정확히 설명한다.

클라우드 컴퓨팅, 빅데이터 분석, 인공지능(AI) 서비스가 보편화되면서 데이터 중력은 시장의 공정 경쟁을 저해하고 국가의 데이터 주권까지 위협하는 중대한 이슈로 부상하고 있다.

가장 심각한 문제로 기술적·경제적 종속(Vendor Lock-in) 현상이 있다. 기업이 특정 클라우드 서비스 제공자에게 대량의 데이터를 저장하면, 이를 다른 사업자로 이전하는 것은 단순히 서버를 옮기는 차원의 문제가 아니다. 데이터를 외부로 전송할 때 부과되는 막대한 전송 비용은 물론, 애플리케이션 아키텍처를 전부 재설계해야 하는 기술적 복잡성, 데이터 이전 과정에서 발생할 수 있는 서비스 중단 위험, 그리고 새로운 플랫폼에 맞춰 내부 인력을 재교육하는 데 드는 막대한 시간과 비용 등 총체적인 전환 비용이 발생한다.

데이터 중력으로 국가의 데이터 주권이 심각하게 약화될 수 있다. 데이터가 국경을 넘어 해외의 특정 클라우드 영역에 집중될 경우, 해당 데이터는 물리적으로 위치한 국가의 법과 규제에 직접적인 영향을 받게 된다. 다국적 기업은 본사 소재국의 법률과 서비스 제공국의 법률 사이에서 어느 한쪽을 위반할 수밖에 없는 법적 딜레마에 빠지게 되며, 이는 자국의 데이터 주권을 심각하게 침해하는 결과를 낳는다.

데이터 중력은 시장의 공정 경쟁을 근본적으로 저해한다. 신규 사업자나 중소 사업자가 경쟁력 있는 서비스를 개발하더라도, 이미 형성된 데이터 중력의 장벽을 넘어 고객을 확보하는 것을 거의 불가능하게 만들어 시장의 혁신과 다양성을 저해하는 요인으로 작용한다.

또 데이터 중력은 보안 및 프라이버시 리스크를 기하급수적으로 증가시킨다. 대규모의 민감한 개인정보와 기업 데이터가 특정 소수 기업의 데이터센터에 집중되어 있는 곳에서 단 한 번의 대규모 해킹이나 유출 사고가 발생할 경우, 그 피해는 사회 전체로 확산될 수 있는 치명적인 약점이 된다.

이러한 문제들은 구체적인 법적 쟁점으로 이어진다. GDPR에서 전송요구권 권리가 법적으로 보장되더라도, 적용대상이 개인정보에 한정되어 있고, 원칙적으로 정보주체가 기업을 상대로 행사하는 권리로서 기업이 다른 기업에게 행사하는 게 한계가 있고, 기계가 읽을 수 있는 형태로 데이터를 제공하라고 규정할 뿐 서비스 간 완전한 상호운용성을 보장하지는 않는다.

이러한 상황 속에서 각국은 데이터 중력 문제에 대응하기 위한 입법적 노력을 가속화하고 있다. EU는 GDPR의 한계를 보완하기 위해 데이터 법(Data Act)을 통해 클라우드 서비스 간 기능적 동등성을 확보하고, 전환 비용에 상한을 두며, 불공정한 계약 조건을 금지하는 등 락인 문제를 직접적으로 해결하려는 강력한 규제를 도입했다.

반면 우리나라의 경우, '데이터 산업진흥 및 이용촉진에 관한 기본법'에서 데이터 이동성 원칙(제15조)을 선언하고 있지만, 이를 실효성 있게 만들기 위한 구체적인 제도적 뒷받침은 부재한 실정이다.

데이터 중력은 기술적 현상을 넘어선 법적·정책적 문제인바, 데이터가 특정 주체에게 종속되는 '중력'이 아닌, 사회 모두를 위한 혁신의 '동력'이 될 수 있도록 균형 잡힌 법제도를 구체적으로 설계하고 발전시켜 나가야 할 것이다.

김경환 대표변호사, 변리사

프로필 보기

02-532-3425
oalmephaga@minwho.kr

Legal Issue

EU AI Act의 핵심과 한국 법제의 방향성

현수진 변호사

1. 글로벌 AI 규제의 분수령, EU AI Act

유럽연합(EU)이 2024년 8월 발효한 EU AI Act(EU 인공지능법)는 전 세계 AI 규제의 기준을 제시한 최초의 포괄적 법안이다. 이 법안은 기업들의 AI 개발 방식을 변화시키며, 윤리적이고 책임 있는 AI 발전에 영향을 미칠 것으로 예상되어 그 중요성이 크다. 특히 AI Act의 적용범위는 EU를 넘어 확장되어 유럽 내에서 AI 시스템을 판매하거나 사용하는 전 세계 조직에 영향을 미친다. 한국 기업과 법조계는 EU 시장 진출 시 이 법의 영향력을 피할 수 없기에, 그 내용과 시사점을 심층적으로 분석해볼 필요가 있다.

2. EU AI Act의 4단계 위험 분류 체계

EU AI Act는 위험 수준에 따라 AI 시스템에 대한 규제 수준을 차등화하는 위험 기반 접근법(risk-based approach)을 취하고 있다. AI 시스템을 ▲허용불가 위험 ▲고위험 ▲제한적 위험 ▲최소 위험의 4단계로 분류하여 차등 규제하며, 특히 인간의 기본권 침해 가능성이 높은 기술을 원칙적으로 금지하고 있다.

(1) 허용불가 위험(Unacceptable Risk) AI 시스템

인간 존엄성을 침해하거나 사회적 차별을 유발하는 AI 시스템은 인간의 건강, 안전, 기본권 등에 중대한 위험을 초래할 수 있어 명문으로 규정된 특별한 예외가 없는 한 절대적으로 금지된다.

허용불가 위험 AI 시스템의 예시로는, ① AI 시스템이 인간의 잠재의식을 이용하거나 의도적으로 조작을 이용하여 사람이 정보에 기반한 의사결정을 내릴 능력을 현저하게 저해하여 심각한 피해를 초래하거나 초래할 가능성이 있는 의사결정을 내리는데 사용되는 경우, ② AI 시스템이 사람 혹은 특정 집단의 취약성(연령, 장애, 사회적 또는 경제적 상황 등)을 악용하여 사람의 행동을 심각하게 왜곡하여 심각한 피해를 초래하거나 초래할 가능성이 있는 경우, ③ AI 시스템이 일정 기간 사회적 행동이나 알려진, 추론된 또는 예측된 개인 또는 성격적 특성을 기반으로 자연인 또는 집단을 평가하거나 분류하는 경우, ④ AI 시스템이 인터넷이나 CCTV 영상에서 얼굴 이미지를 비대상으로 스크래핑하여 얼굴 인식 데이터베이스를 생성하거나 확장하기 위해 사용되는 경우, ⑤ 생체인식 데이터를 기반으로 개별 자연인을 분류하여 인종, 정치적 의견, 노조 가입, 종교 또는 철학적 신념, 성생활 또는 성적 지향을 추론하거나 유추하는 경우, ⑥ 직장과 교육기관에서 자연인의 감정을 추론하기 위해 AI 시스템을 사용하는 경우, ⑧ 법 집행 목적을 위해 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체인식 식별 시스템을 사용하는 경우가 있다.

(2) 고위험(High-Risk) AI 시스템

고위험 AI 시스템은 의료기기 및 생체인식, 교통시설 등 중요 인프라, 교육, 필수 서비스, 법 집행에 사용되는 AI 등을 포함한다. (단, 생체인식, 금융사기 탐지 등에 사용되는 AI에는 몇 가지 예외가 적용됨)한다.

이러한 AI 시스템은 엄격한 조건에서 배포가 가능하며, 고위험 AI 시스템 공급자와 운영자, 수입업자, 유통업자에게는 엄격한 적합성 평가와 투명성 의무가 부과된다.

(3) 제한적 위험(Limited Risk) AI 시스템

사람과 상호작용하는 AI 시스템 중에서 딥페이크 기술과 같이 비인격화, 기만, 조작 등의 문제를 일으킬 수 있는 기술은 제한된 위험성을 갖는 시스템으로 분류된다.

이러한 시스템에는 투명성 의무가 부과되는데, 생성형 AI의 경우 콘텐츠 출처 표시, 챗봇은 AI 상호작용 여부 고지 의무를 뜻한다. 예를 들어, 딥페이크 영상에는 "AI 생성" 라벨 부착의무가 있다.

(4) 최소 위험(Minimal Risk) AI 시스템

스팸 필터, 비디오 게임 등 일상적 기술에 기반한 저위험 AI 시스템에 대해서는 규제가 적용되지 않으며, 다만 거버넌스 메커니즘을 포함한 명확한 목표와 성과지표에 기초한 자발적인 행동 강령(Code of Conduct) 작성이 권장된다.

또한 EU AI Act에서는 범용 AI 모델(General Purpose AI Model)을 일반적인 AI 시스템과 구분하여, 영향력이 큰 GPAI 모델에는 훨씬 더 엄격한 의무를 부과하고 있다.

3. 한국 법제에 대한 시사점

EU AI Act는 단순한 기술 규제를 넘어 인간 존엄성 보장이라는 가치 지향적 프레임워크를 구축했다는 점에서 의의가 크며, AI 기술의 윤리적 사용을 촉진하는 동시에 글로벌 기업들의 전략적 대응을 요구하는 촉매제 역할을 할 전망이다.

한국의 입법 동향은 혁신 지원과 규제 완화에 초점을 맞추고 있다. 2024년 발의된 「인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률(가칭 "AI 기본법")」은 EU의 '고위험' 개념 대신 '고영향'이라는 가치중립적 용어를 사용하며, 생성형 AI에 대한 안전성 확보 의무를 명시하고 있다.

"고영향 AI"의 정의 및 그 규제 대상의 범위는 AI 기본법상 가장 민감한 규범 영역 중 하나이다. "고영향 AI"의 개념은 지나치게 추상적이어서 사업자의 예측가능성을 저해하고, 긍정적인 영향까지 포함되어 불필요한 규제 범위 확장을 초래할 수 있다는 점에서 여전히 해결과제로 남아있다.

EU AI Act의 위험 분류 체계에 비추어 볼 때, 우리 역시 '고영향'이라는 용어를 '고위험'으로 전환하는 것이 바람직해 보인다. 설령 "고영향 AI"의 개념을 유지하는 경우라도, EU처럼 구체적 위험 시나리오와 분야별로 유형화하거나, 판단 기준에 대한 시행령이나 가이드라인을 통해 규범의 구체성과 실효성을 담보할 필요가 있다.

또한, 미국 NIST의 AI 위험관리 프레임워크(RMF)처럼, 위험 평가와 관리에 대한 실질적 가이드라인을 도입해 사업자가 자율적으로 위험을 식별·관리할 수 있도록 지원하는 것이 바람직하다.

NIST의 AI RMF는 미국 정부가 2023년 1월에 공식 발표한 AI 리스크 관리 프레임워크로, AI 시스템이 초래할 수 있는 다양한 위험을 체계적으로 파악하고 완화할 수 있는 방법론을 제시한다. 이는 규제나 강제규범이 아닌 비의무적(voluntary) 가이드라인, 다양한 조직들이 자신의 기술과 목적에 맞게 자율적으로 적용할 수 있도록 설계되었다.

NIST의 AI RMF는 크게 두 부분으로 구성됩니다. 먼저 기반 요소(foundation layer)에서는 '신뢰할 수 있는 AI'를 정의하고, 위험이 무엇인지, 그리고 왜 위험을 관리해야 하는지를 설명한다. NIST가 제시하는 '신뢰할 수 있는 AI'의 7가지 핵심 속성은, Valid and Reliable (타당하고 신뢰 가능한), Safe (안전한), Secure and Resilient (보안적이고 복원력 있는), Accountable and Transparent (책임 있고 투명한), Explainable and Interpretable (설명 가능하고 해석 가능한), Privacy-Enhanced (프라이버시 보호 강화), Fair with Harm Mitigation (공정하고 해악 최소화)이다.

다음으로 핵심 요소(core functions)란 AI 위험을 관리하기 위한 4단계의 기능요소로 이루어진다. 핵심 기능은 AI 시스템이 작동하는 환경과 그에 따른 위험요소를 식별하는 Map(매핑), 위험의 규모와 영향을 정량·정성적으로 분석하는 Measure(측정), 위험을 줄이기 위한 전략적 조치 수행을 의미하는 Manage(관리), 조직 전체의 AI 리스크 관리체계 정착 및 책임 분배인 Governance(거버넌스)를 말한다.

NIST AI RMF는 법적 구속력 없이도 신뢰 가능한 AI 구현을 위한 표준화된 로드맵을 제시한다는 점에서 글로벌 AI 거버넌스의 핵심 참고자료로 평가받고 있다. 특히 AI 기술의 빠른 발전 속도를 고려할 때, 법적 규제가 미처 손을 대지 못하는 영역에서 기업 및 개발자들이 자율적으로 위험을 통제할 수 있는 유연한 도구로서의 가치가 매우 크다. 이를 참고하여, 한국 AI 기본법의 "고영향 AI" 개념의 모호성 문제를 해결하는데 참고하고 자율규제와 내부 점검 체계의 강화 수단으로 활용할 수 있다.

4. AI 거버넌스의 방향성

새롭게 마련된 AI 기본법은 EU와 유사한 위험기반 규제, 일본식 유연성, 미국 NIST의 위험관리 프레임워크 등 글로벌 스탠다드를 적극적으로 수용하고 있다.

그러나 우리 법제는 여전히 통합적 조정 기능의 부재, 고영향 AI 개념의 불명확성, 개인정보 보호와 AI 개발 간 균형 부족 등의 한계가 존재한다.

AI 거버넌스는 해외 주요국의 선진 사례를 참고하되, 우리 사회의 특수성과 미래지향적 비전을 반영한 '포용적이고 신뢰받는 AI 거버넌스 체계' 구축이 무엇보다 중요하다. 특히 급변하는 기술 환경에 대응할 수 있도록 산업계·시민사회·정부가 모두 참여하는 입법 체계를 정립하여, 이해관계자 간 상시 협의와 정책 조정, 국제 표준 논의 참여가 이루어질 수 있도록 해야 한다.

현수진 변호사

프로필 보기

02-532-3425
hyunsj@minwho.kr

법무법인 민후

MINWHO NEWS

김경환 변호사,
제 21회 오피스키퍼 보안 세미나 강의
‘사이버 복원력 강화 차원에서 발생 가능한 법적 대응 전략과 기업 차원의 대응 프레임워크’

김경환 변호사, 제 21회 오피스키퍼 보안 세미나에서 ‘사이버 복원력 강화 차원에서 발생 가능한 법적 대응 전략과 기업 차원의 대응 프레임워크’를 주제로 강의

법무법인 민후 김경환 변호사는 6월 24일, 지란지교소프트가 주최한 ‘제21회 오피스키퍼 보안 세미나’에서 보안 사고 대응 시 필요한 법적 대응 전략과 기업 차원의 대응 체계를 주제로 강연을 진행했습니다.

김 변호사는 최근 이슈가 된 ‘법 위반 통지서’를 사칭한 피싱 메일 사례를 중심으로, 해커들이 법률적 형식을 활용해 사용자를 속이는 사회공학적 공격이 늘고 있다고 지적하며, 단순한 기술적 방어를 넘어, 법적 리스크에 대한 대응력 확보가 필수라는 점을 강조했습니다.

강연에서는 특히 개인정보 유출 시 통지의무, 법적 보고체계 수립, 증거자료 보존, 이해관계자 대응 등 사고 이후 실질적인 피해를 줄이기 위한 법적 체크포인트들이 소개되었고, 보안 실무자 역시 이제 법과 규제에 대한 이해를 갖춘 대응 주체가 되어야 한다며, 기술·법무·경영 간 유기적 협력이 이루어질 때 진정한 사이버 복원력이 가능하다고 강조했습니다.

MINWHO NEWS

양진영 변호사, 중앙일보와 인터뷰

'AI학습과 저작권 분쟁에서 국내·외 판례 동향'

양진영 변호사, 중앙일보와 'AI학습과 저작권 분쟁에서 국내·외 판례 동향' 관련 인터뷰

법무법인 민후의 양진영 변호사는 최근 중앙일보와의 인터뷰에서, AI 학습과정에서 발생하는 저작권 침해 문제를 중심으로 미국과 한국의 판례 및 법리 차이에 대해 의견을 밝혔습니다.

미국에서는 최근 연방법원이 AI 기업 앤스로픽의 책 데이터 무단 사용에 대해 공정 이용을 인정하며 저작권 침해가 아니라고 판단한 사례가 나왔으며, 법원은 해당 AI 모델이 단순 복제가 아닌 변형적 이용을 통해 새로운 창작물을 만들어낸 것이라고 보았습니다.

이에 대해 양진영 변호사는 '국내 저작권법 체계는 미국보다 훨씬 보수적으로 공정 이용을 폭넓게 인정하기 어렵다'고 진단했으며, '미국은 변형성과 창작성에 방점을 두는 반면, 한국은 저작물 보호를 중심으로 판단하기 때문에 미국 판례를 그대로 적용하긴 어렵다'고 설명했습니다.

현재 국내에서도 AI 학습에 대한 저작권 분쟁이 본격화되고 있습니다. 주요 방송사들은 AI가 뉴스 콘텐츠를 무단 학습한 것과 관련해 네이버를 상대로 저작권 침해 소송을 제기했고, 한국신문협회도 공정위에 관련 신고를 진행 중입니다.

양 변호사는 '국내 법원에서 공정 이용이 AI 관련 사안에 어떻게 해석될지는 아직 불투명하다'며, 향후 법원의 판단과 사회적 합의가 핵심이 될 것이라고 강조했습니다. 이어 'AI 기술 발전과 창작자 권리 보호 사이의 균형점을 모색하는 법 해석과 입법이 시급하며, 단순한 해외 법제 모방을 넘어선 독자적 기준 정립이 필요하다'고 덧붙였습니다.

이번 인터뷰는 AI 시대의 저작권 분쟁이 단순한 기술 문제가 아니라, 혁신과 권리 보호라는 두 가치의 충돌 속에서 새로운 법 질서를 요구하고 있음을 상기시키는 계기가 되었습니다.

Business CASE

이달의 업무사례

1. 정보통신망법위반 형사사건에서 고소인을 대리해 벌금형 약식명령 처분 이끌어 승소

2. 가상화폐 거래소 해킹 사고로 인한 손해배상청구 사건에서 다수 원고들 대리하여 약 2억 3천여만 원 전부 승소

3. SW프로그램 저작권침해로 인한 손해배상청구 사건에서 피고를 대리하여 청구금액의 약 77% 감액된 수준으로 합의 도출

4. 본인 인증 문제로 인한 비트코인 인도청구 등 사건에서 원고를 대리하여 전액 반환 합의 도출

5. 특허침해 손해배상 소송에서 반도체 장비 제조사 대리해 생산금지 및 2억 5천만원 배상판결 도출

6. 아동 위치정보 서비스 신청 시 법정대리인 동의 요건에 대한 법률 자문 제공

7. 하도급 계약 해지 후 금전반환 미이행과 관련된 형사책임 검토 자문 제공

8. 데이터 거래소 서비스 운영을 위한 법인 명의 암호화폐 지갑 개설 관련 법률 자문 제공

9. 해외 거래 대금 처리 방식의 외국환거래법상 적법성 검토 자문 제공

10. 대규모 AI 데이터 구축 용역계약서 검토 및 위험 요소 점검 자문 제공

법무법인 민후

서울특별시 강남구 테헤란로 134, 포스코 타워 역삼 11층

Tel. +82-2-532-3483 **Fax.** +82-2-532-3486

www.minwho.kr

[변호사 소개 바로가기] [주요 업무사례 바로가기]

[전화 상담 바로가기] [카톡 상담 바로가기] [홈페이지 상담 바로가기] [이메일 상담 바로가기]

본 뉴스레터의 내용 또는 기타 법률 문의가 필요하신 경우
법무법인 민후로 연락주시면 담당 변호사님의 답변을 받으실 수 있습니다.