「시민사회와 NGO」 제23권 제1호(2025.5): 195-245
https://doi.org/10.35981/ngo.2025.23.01.195

일반논문

AI 학습데이터와 개인정보 권리의 경계 : 에이닷(A.) 사례를 통해 본 통제와 거버넌스의 과제

유성희*, 서효중**

생성형 인공지능(Generative AI)의 확산은 방대한 양의 고품질 학습 데이터를 필수 자원으로 만들고 있으며, 이에 따라 개인정보 수집·활용을 둘러싼 법적·윤리적 문제는 더욱 복잡하고 구조화된 형태로 전개되고 있다. 특히 통신 기반 AI 서비스는 실시간으로 민감 데이터를 수집할 수 있는 구조를 갖추었으나, 이러한 데이터가 인공지능 학습에 활용되는 과정에서 그 정당성과 책임 구조는 여전히 불투명하다.

본 연구는 SK텔레콤의 AI 비서 서비스 '에이닷(A.)' 사례를 통해 통화 데이터, 대화 기록, 제3자 연동 정보 등 고위험 개인정보 활용 방식과 이에 따른 사용자 통제권 침해, 제3자 권리 미보장, 알고리즘 불투명성의 문제를 분석하였다. 특히 통화 데이터의 처리 과정은 개인정보보호법(PIPA)상 목적 제한성 원칙 및 사전 동의 체계와 충돌하며, 기존 법제도가 AI 학습 데이터의 복합성과 재사용 가능성을 충분히 포섭하지 못하고 있음을 실증적으로 드러낸다.

또한 Stack Overflow 사례를 통해, 공개된 데이터라도 정보 주체의 권리 고지, 활용 목적의 명확성, 저작권 보호 등 최소한의 규범 요건이 충족되지 않으면 법적·윤리적 위반으로 전환될 수 있음을 밝혔다. 이러한 분석을 바탕으로 GNU GPL 라이선스의 핵심 원칙 – '공개', '책임 공유', '권리 연속성' – 을 AI 데이터 거버넌스 구조에 적용할 수 있는 가능성을 탐색하였다.

결론적으로 본 연구는 기술·법·윤리 통합적 관점에서 새로운 데이터 규범 설계 필요성을 제시하며, AI 생태계의 투명성과 책임성, 디지털 시민사회의 정보주권 강화를 위한 기반을 제공하고자 한다.

주제어 : AI 학습데이터, 개인정보 권리, 통화 데이터, 데이터 거버넌스, 시민사회, 에이닷, 오픈 라이선스

* 주저자, 서울시어르신돌봄종사자종합지원센터장.
** 교신저자, 가톨릭대학교 컴퓨터정보공학부 교수.

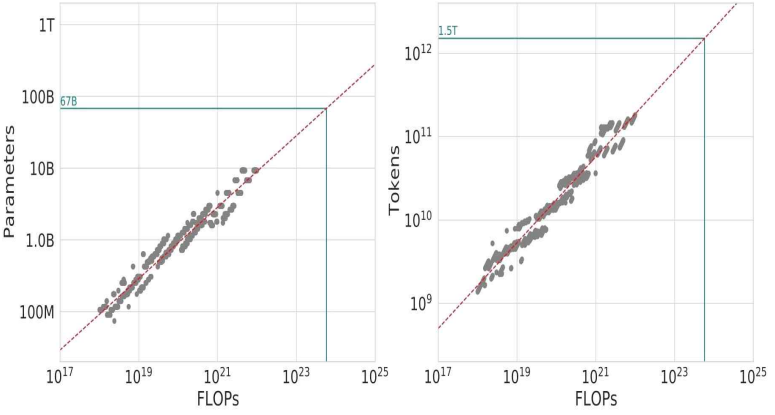
I. 연구 배경과 문제 설정

1. 연구 배경

디지털 전환이 가속화되면서 데이터는 현대 경제와 기술 발전의 핵심 자원으로 자리매김하고 있다. 특히 인공지능(Artificial Intelligence, AI) 기술의 비약적인 진보와 맞춤형 서비스의 확산은 개인 데이터의 수집과 활용을 핵심 요소로 만들고 있으며, AI 시스템의 성능 역시 데이터의 양과 질에 크게 의존한다.

Hendricks는 'Chinchilla 스케일링 법칙'을 통해, 대규모의 고품질 데이터를 활용할 경우 모델 파라미터 수가 적더라도 우수한 AI 성능을 발휘할 수 있음을 실증적으로 제시하였다(Hendricks, 2024). 이는 AI 기술의 발전에서 데이터 확보가 연산 능력(FLOPs)[1]이나 모델 복잡도 못지않게 중요함을 시사한다. 즉, AI 성능을 향상시키기 위해서는 연산 능력(FLOPs)의 증가와 함께 더 많은 데이터(토큰 수)와 파라미터(모델 복잡도)가 필요하다.

1) FLOPs (Floating Point Operations)는 AI 모델이 연산을 수행하는 데 필요한 계산량을 측정하는 단위로, 모델의 연산 복잡도를 나타낸다.



(출처:Hendricks, 2024)

〈그림 1〉 딥러닝 스케일링 법칙

〈그림 1〉에서 보여지는 딥러닝 스케일링 법칙처럼, 데이터 양과 AI 성능 간의 비례 관계는 AI 기술 발전의 핵심 동력 중 하나로 작용한다. 특히, AI 모델이 높은 성능을 발휘하기 위해서는 양질의 데이터가 필요하며, 이 과정에서 순수하게 인간이 생성한 데이터가 AI 성능 개선에 중요한 자원으로 평가받고 있다(Hendricks, 2024).

그러나 최근 인터넷에서 수집되는 데이터 중 상당수는 인간이 아닌 AI 모델이 생성한 2차 데이터로 대체되고 있으며, 이는 AI가 자신이 생성한 데이터를 반복 학습하면서 원래의 데이터 분포를 왜곡시키는 '모델 붕괴(model collapse)' 현상[2]을 초래할 수 있다(Shumailov et al., 2024). 따라서 고성능 AI를 안정적으로 유지하기 위해서는 인간이 직접 생성한 원천 데이터를 지속적으로 확보하는 것이 필수적이다.

이러한 맥락에서 이동통신망 사업자는 대규모의 인간 생성 데이터를

2) AI 모델이 AI가 생성한 데이터를 반복적으로 학습함으로써 원래의 인간 데이터 분포를 잃고 성능이 저하되는 현상이다. Shumailov et al.(2024) 등이 이 문제를 지적하였다.

확보할 수 있는 인프라적 강점을 가진다. 특히, SK텔레콤의 에이닷(A.) 서비스는 사용자 대화 기록, 검색 패턴, 통화 내역 등 민감한 데이터를 수집하여 AI 기반 맞춤형 서비스를 제공하고 있다. 이는 소비자에게 높은 편의성을 제공하는 동시에, 개인정보의 비동의 수집 및 활용에 따른 프라이버시 침해 가능성을 내포하고 있다(Meurisch, 2021).

최근 연구와 언론 보도에 따르면, 사용자 동의가 명확히 이루어지지 않은 상태에서 수집된 데이터가 AI 학습에 활용되는 사례가 다수 보고되고 있으며, 이는 기업의 신뢰도뿐 아니라 시민 개개인의 정보 통제권과 집단적 감시 저항력에도 중대한 영향을 미친다. Andreotta 등은 AI 기술의 상업화 과정에서 사용자의 동의 절차가 무력화되고, 수집된 데이터가 본래의 목적을 벗어나 재사용되는 문제를 지적하였다(Andreotta et al., 2021). 이러한 데이터 윤리 문제는 특히 한국에서 더욱 두드러지며, 기술 발전 속도에 비해 법적·제도적 보호 장치가 미흡하다는 비판이 지속적으로 제기되고 있다(김경민 외, 2024).

이에 본 연구는 SK텔레콤의 에이닷(A.) 서비스를 중심으로, AI 학습 데이터 활용 과정에서 발생하는 개인정보 보호 문제를 고찰하고자 한다. 특히, 데이터 수집 시 사용자 동의 절차의 부재 및 데이터 오남용 가능성을 중점적으로 분석하며, 이를 해결하기 위한 법적·윤리적 대응 방안을 제안한다. 더 나아가, 이러한 문제들이 디지털 시민사회의 감시 체계 강화, 데이터 주권 약화, 그리고 공공 신뢰 기반의 침식으로 이어질 수 있는 구조적 위험을 비판적으로 분석하고자 한다[3].

3) 디지털 시민사회는 정보 환경 속에서 시민이 감시와 통제의 대상이 되는 동시에, 데이터에 대한 권리와 책임을 자각하며 능동적으로 대응하는 주체로서 기능하는 개념이다. 이와 관련하여 Isin과 Ruppert는 데이터를 통해 시민의 정체성과 권리가 구성되는 과정을 '디지털 시민권(data subjectivity)'이라는 개념으로 설명한다(Isin & Ruppert, 2015).

2. 디지털 시대의 데이터 활용과 문제점

디지털 시대가 도래하면서 데이터는 "21세기의 석유"로 불릴 만큼 중요한 자원으로 부상하였다. 데이터는 인공지능(AI) 기술의 핵심 동력으로 기능하며, 맞춤형 서비스, 예측 분석, 자동화 시스템 등 다양한 기능의 기반이 된다. 이러한 기술은 사용자 맞춤형 광고, 금융 리스크 평가, 의료 진단 시스템 등 다양한 분야에 적용되며, 데이터 축적을 통해 성능을 지속적으로 개선한다(Sebastian, 2023).

AI 기반 서비스는 대규모 사용자 데이터를 수집하여 개인화된 경험을 제공하며, 사용자 편의를 극대화하는 데 기여한다. SK텔레콤의 에이닷(A.) 서비스는 이러한 대표적인 예로, 사용자 대화 내용, 검색 기록, 통화 데이터 등 민감한 정보를 활용하여 AI 비서 기능을 구현하고 있다. 그러나 이와 같은 데이터 수집 및 활용 과정은 여러 법적·윤리적 쟁점을 수반하며, 특히 프라이버시 침해 가능성이 주요 문제로 지적되고 있다. 특히 데이터 수집 과정에서 사용자 동의 절차가 형식적이거나 불충분한 경우가 많고, 수집 목적과 범위가 충분히 설명되지 않는 경우가 다수 존재한다[4].

이는 데이터 주체로서의 권리를 심각하게 침해할 수 있으며(Meurisch et al., 2020), 개인이 디지털 플랫폼에서 제공한 정보가 당초 제공 목적을 벗어나 상업적으로 재이용되거나 제3자에 의해 2차적으로 활용되는 것에는 다양한 위험과 윤리적 함의가 존재한다. Hutton과 Henderson은 이와 같은 데이터 활용이 투명한 동의 없이 이루어지는 경우, 명백한 윤리적 침해로 이어질 수 있음을 강조하였다(Hutton & Henderson,

---

[4] "SKT의 "에이닷 통화 내용 삭제" 설명, 사실이 아니었다", 한겨레신문 2024/06/13 기사. 기사에 따르면, "오병일 진보네트워크센터 대표는 "통화 원본 파일은 삭제됐다고 하더라도 통화 당사자가 인지하지 못한 상태에서 통화 내용 요약 정보를 제3자가 보유하고 있다면 통비법 위반 가능성이 커 보인다"고 말했다." https://www.hani.co.kr/arti/economy/economy_general/1144731.html.

2017). 양관석은 “정보주체는 일단 사전동의를 하고 나면 자신의 데이터가 그 이후 어떻게 활용되는지 알 수 없으며, 이에 대한 우려가 발생한다”고 지적한다(양관석, 2019; pp.150-151).

이러한 현실은 데이터 활용에 있어 투명성, 설명 가능성, 동의 기반성을 핵심 가치로 설정할 필요성을 시사한다. 그러므로 개인정보 보호법의 실질적 적용과 함께, 데이터 수집과 활용 전 과정에 대한 제도적 감시와 사회적 책임 구조 마련이 필요하다(Meurisch & Mühlhäuser, 2021).

3. 연구 목적 및 연구 질문

AI 기술의 고도화와 데이터 기반 서비스의 확산은 개인화된 편의와 정보 접근성을 제공하는 동시에, 개인정보 권리 침해와 통제력 상실에 대한 사회적 우려를 증폭시키고 있다. 특히, 사용자 데이터가 하나의 서버 내에서 AI 학습에 재활용되는 방식은, 정보 주체나 서비스 운영자조차 데이터의 실제 흐름과 활용 범위를 명확히 파악하기 어려운 기술적 사각지대를 형성하고 있다[5]. 이는 단순한 기술적 문제를 넘어 데이터에 대한 시민의 민주적 통제력 부재와 기술 권력의 독점이라는 사회적 문제로 이어진다(Zuboff, 2019).

이러한 우려는 SK텔레콤이 운영하는 AI 비서 서비스 ‘에이닷(A.)’ 사례에서 구체적으로 드러난다. 해당 서비스는 통화 녹음 및 대화 요약 기능을 통해 민감한 음성 정보를 수집·활용하고 있으며, 특히 통화 상대방

5) 김명주 AI안전연구소 소장은 “한 회사가 보유한 같은 서버 내에서 학습된 데이터는 사용자나 관리자가 모르는 사이 다른 서비스에 재사용될 가능성이 있으며, 그 융합 경로를 현재 기술로는 추적하기 어렵다”고 지적했다. 「SKT 에이닷도 골머리…AI가 학습한 개인정보 어떻게 관리될까」, 뉴스핌, 2023.11.10. https://www.newspim.com/news/view/20231101001157.

의 동의 없이 이루어질 수 있는 데이터 수집 및 AI 학습 활용 구조는 심각한 법적·윤리적 쟁점을 야기하고 있다. 실제로 2024년 2월 언론 보도에 따르면, 해당 기능은 통신비밀보호법 및 개인정보 보호법 위반 소지가 있다는 전문가의 지적과 함께, 사전 고지 및 선택권 제공이 충분치 않다는 시민사회의 비판을 받고 있다[6]. 또한, 디지털 권리단체 및 일부 보도에서도 에이닷의 대화 요약 및 AI 학습 기능이 사용자 인식 없이 작동할 가능성을 지속적으로 제기해 왔으며, 이에 따라 개인정보보호위원회 등 유관 기관의 정책적 검토 필요성이 강조되고 있다. 대화 중 개인정보 제공 여부에 대한 사용자 안내가 미흡하다는 지적은, 이 서비스가 기술적 설계와 현행 법제 간 괴리를 보여주는 대표 사례임을 시사한다.

이에 더해서, SKT가 제시한 개인정보 처리방침과 실제 사용자 인터페이스 간의 괴리는 AI 서비스의 설명 가능성과 외부 감시 가능성 측면에서 중요한 쟁점을 형성하고 있다. 더욱이 현재 한국은 세계적으로 유일하게 이동통신사가 이러한 통화 녹음 및 요약 기반의 AI 서비스를 상용화하고 있는 국가로, 이에 대한 제도적·학술적 대응은 매우 미흡한 실정이다[7].

이러한 문제는 단순한 사생활 침해를 넘어, 정보 주체의 통제권 약화, 데이터 감시 구조의 확산, 기술 거버넌스의 부재와 같은 시민사회적 함의를 동반한다. 본 연구는 특히 데이터에 대한 개인과 기업의 절대적 소유권 개념을 넘어 데이터를 공동의 자산으로 보는 공동체주의적 소유권 이론과 시민들의 공적 담론을 통해 데이터 거버넌스의 정당성을 확보해야 한다는 하버마스의 공론장 이론을 결합하여, AI 학습 데이터 활용 과정에서 시민사회 기반의 실질적 개인정보 보호와 데이터 통제력 강화 방안을 모색하는 것을 목적으로 한다. 또한 GNU GPL의

6) 「'AI 통화녹음 도청 논란' 에이닷 잘나가자, KT·LGU+도 슬쩍」, 한겨레신문, 2024.02.14. https://www.hani.co.kr/arti/economy/economy_general/1128334.html.

7) 해당 보도에 따르면, "전 세계에서 유일하게 한국에서만 이동통신사가 직접 제공하는 통화 녹음 및 내용 요약 서비스가 확산하고 있다." 위 기사 참조.

원칙인 공개성, 권리 연속성, 책임 공유를 AI 데이터 거버넌스에 적용함으로써 데이터 활용의 투명성 및 사회적 책임성을 제고하는 가능성을 탐색하고자 한다.

이를 위해 본 연구는 다음의 연구 질문을 중심으로 전개된다.

첫째, SK텔레콤의 에이닷 서비스는 AI 학습 데이터로서 사용자 개인정보를 어떤 방식으로 수집·활용하고 있는가? 둘째, 이 과정에서 발생하는 주요 법적·윤리적 문제는 무엇이며, 기존 법제는 이에 적절히 대응하고 있는가? 셋째, 데이터 주체의 권리를 보호하고, 정보 활용의 투명성을 제고하기 위한 제도적·정책적 장치는 무엇인가? 넷째, 오픈소스의 GPL 라이선스 원칙[8]을 포함한 자율 규범적 접근은 새로운 AI 데이터 거버넌스의 대안이 될 수 있는가? 다섯째, 기술 민주주의와 데이터 생태학, 데이터 노동 등의 새로운 담론은 데이터 거버넌스 논의를 어떻게 발전시킬 수 있으며, 이를 에이닷 서비스의 문제 해결에 적용할 수 있는가?

본 연구는 위 질문들을 바탕으로, 기술 발전과 시민사회 보호라는 이중 과제를 모두 고려한 지속 가능한 AI 데이터 활용 모델을 제안하고자 한다.

4. 연구 범위와 방법

1) 연구 범위

본 연구의 분석 대상은 SK텔레콤의 AI 기반 개인화 서비스 '에이닷(A.)'에 한정된다. 에이닷은 대화형 인터페이스와 통화 녹음 요약 기능을

8) GNU GPL (General Public License)은 자유 소프트웨어 재사용을 허용하는 대표적인 오픈소스 라이선스로, '공개', '권리의 연속성', '책임 공유'를 주요 원칙으로 한다. 본문에서는 이를 AI 데이터 거버넌스에 적용하는 가능성을 논의한다.

중심으로 사용자로부터 다양한 유형의 민감 정보를 수집하고 있으며, 특히 통화 데이터에는 제3자의 음성 및 식별 가능한 정보가 포함될 수 있어, 그 법적·윤리적 위험성이 매우 높다. 이에 본 연구는 해당 서비스가 수집하는 대화 내용, 통화 기록, 검색 이력 등을 중심으로, 이들 정보가 AI 학습에 어떠한 방식으로 활용되는지를 고찰하였다.

또한 주목할 점은, 에이닷 서비스가 국내 이동통신사 중 유일하게 통화 내용 수집 및 요약 기반 AI 학습을 제공하는 상용 서비스라는 사실이다. 이는 기술적 선도성과 동시에 규범적 사각지대가 존재함을 의미하며, 이러한 사례에 대한 학술적 분석은 현 시점에서 필수적이다[9].

2) 연구 방법

본 연구는 질적 사례연구(qualitative case study) 접근을 기반으로 하며, 다음의 세 가지 방법론을 중심으로 분석을 수행하였다. 첫째, 문헌 분석을 통해 AI 기술 발전과 데이터 기반 서비스 구조, 프라이버시 권리와 통제 개념에 관한 선행 연구를 검토하였다. 이를 통해 디지털 환경에서 개인정보의 의미 변화와 시민사회적 권리 구조의 재편 양상을 이론적으로 정립하였다.

둘째, 제도 분석은 개인정보보호법(PIPA)을 중심으로 수행되었다. 본 연구는 PIPA의 목적 제한성 원칙, 동의 구조, 가명정보 처리 조항 등을 중심으로 AI 학습 데이터 활용과 관련된 규범적 한계를 검토하였다. 통신비밀보호법과 전기통신사업법은 고위험 정보인 통화 데이터의 법적 맥락을 보완적으로 이해하는 차원에서 간략히 참조하였다.

---

9) 에이닷은 현재까지 국내 이동통신 3사 중 유일하게 통화 녹음 및 요약 기능을 상용화한 AI 서비스이며, 이는 2024년 2월 기준 한겨레 보도를 통해 확인된다. 자세한 내용은 한겨레신문, 「'AI 통화녹음 도청 논란' 에이닷 잘나가자, KT·LGU+도 슬쩍」(2024.2.14) 참고.

셋째, 사례 분석을 통해 SK텔레콤의 AI 비서 서비스 '에이닷(A.)'의 개인정보 수집 및 활용 구조를 분석하였다. 특히 사용자 동의 구조, 제3자 정보 포함 가능성, 고위험 정보의 활용 방식에 주목하였으며, 분석 자료로는 기업의 개인정보 처리방침, 서비스 안내서, 정책 보고서, 언론 보도 등 공개된 2차 자료를 활용하였다.

이와 함께 본 연구는 GNU GPL 라이선스의 '공개', '권리 연속성', '책임 공유' 원칙을 AI 데이터 거버넌스에 적용 가능한 자율 규범 모델로 논의하고자 하였다. 이를 통해 기존 제도에서 발생하는 법적 공백을 보완할 수 있는 기술-법 융합적 대안을 제시하고자 하며, 개인정보 통제권과 시민사회의 권리 구조에 대한 비판적 문제의식 또한 분석 전반에 반영하였다.

Ⅱ. 이론적 배경 및 선행 연구

1. 개인정보 보호와 데이터 거버넌스의 이론적 기반

프라이버시 바이 디자인(Privacy by Design)은 개인정보 보호를 기술과 정책의 설계 초기부터 내재화하는 원칙으로, AI 시스템 설계에 있어 핵심적인 이론적 기반이 된다[10]. 최근 연구들은 이 개념이 단지 선언적인 원칙이 아니라, 실제 설계 방법론으로 기능할 수 있도록 구체화되어야 한다는 점을 강조한다. Zhang과 Yu는 프라이버시 설계를 체계화하기

10) 이 원칙은 Cavoukian이 제시한 7가지 핵심 원칙(사전 예방, 기본 설정으로서의 프라이버시, 설계에 내재된 프라이버시, 완전한 기능성, 전체 수명 주기 보호, 가시성 및 투명성, 사용자 프라이버시에 대한 존중)을 바탕으로 한다(Cavoukian, 2012).

위한 방법론으로 'Privacy-based Design(PbD)'을 제시하며, AI 서비스 개발 단계에서 다양한 프라이버시 시나리오를 예측하고 설계에 반영하는 프레임워크를 제안하였다(Zhang & Yu, 2023).

데이터 최소화 원칙(data minimization) 또한 주요한 법적·윤리적 기준으로 자리잡고 있다[11]. 이는 AI가 불필요한 개인정보를 수집하거나 저장하지 않도록 제한함으로써, 정보 주체의 권리를 보다 실질적으로 보장하려는 목적을 가진다. 특히 통화 내역과 같이 AI 서비스가 고위험 정보를 포함하는 경우, 이 원칙은 데이터 축소 설계의 기준이 된다. Descalzo는 이 원칙이 단순한 법적 요건을 넘어, AI 시스템의 신뢰성과 지속가능성을 확보하는 윤리적 기준이 되어야 함을 강조한다(Descalzo, 2024).

또한 디지털 플랫폼의 데이터 상업화는 개인정보의 상품화라는 더 큰 윤리적 쟁점을 낳는다. Sadowski는 현대 자본주의에서 데이터가 새로운 자본의 형태가 되었지만, 이 과정에서 개인의 데이터가 동의나 정당한 보상 없이 추출되어 이용되는 착취적 구조를 형성한다고 비판한다(Sadowski, 2019). 이러한 문제의식은 디지털 시민사회의 관점에서 데이터 활용과 감시, 통제의 관계를 중심으로 한 이론적 논의로 확장된다. Zuboff는 디지털 기술이 개인 데이터를 경제적 자원으로 변환하면서 시민을 지속적 감시의 대상으로 만드는 현상을 '감시 자본주의(surveillance capitalism)'로 비판하며, 이 과정에서 기술 권력과 시민 권리 간의 구조적 불균형이 심화됨을 지적하였다(Zuboff, 2019).

이에 따라 시민사회 이론은 이러한 불균형을 해결하기 위해 기술 민주주의, 데이터 생태학, 데이터 노동과 같은 새로운 프레임을 제안하며

11) 목적에 필요한 최소한의 데이터만을 수집하고 저장해야 한다는 개인정보 보호의 기본 원칙이다. 특히 AI 시스템이 고위험 정보를 처리하는 경우, 이 원칙은 기술 설계의 핵심 기준이자 신뢰 확보의 윤리적 기반으로 작용한다(Descalzo, 2024).

(Morozov, 2013; Kitchin, 2014; Casilli, 2019), 데이터 주권의 민주적 관리와 공론장 참여를 통한 정당성을 강조한다(Singh & Vipra, 2019). 그러므로 데이터 기반 사회에서 시민은 더 이상 단순한 법적 권리의 수혜자가 아니라, '능동적 데이터 행위자(data subjectivity)'로서 데이터를 통해 자신의 권리와 정체성을 적극적으로 재구성해야 한다(Isin & Ruppert, 2015). 이러한 이론적 논의는 AI 시스템과 데이터 주권 논의를 시민사회의 맥락에서 재구성하는 데 중요한 기반을 제공한다.

공론장 이론과 공동체주의 소유권 이론은 데이터 거버넌스의 사회적 정당성을 확보하는 데 중요한 이론적 근거를 제공한다. Habermas는 시민들이 이성적·비판적 담론을 통해 공적 사안에 참여할 수 있는 공론장의 존재를 민주주의의 핵심으로 보았으며(Habermas, 1989), 이는 데이터의 공개성과 관리에 있어 투명성과 시민 참여의 필요성을 뒷받침한다. 한편, 공동체주의 철학자들은 데이터 소유권을 단순한 개인의 권리로 보지 않고, 공동체적 가치와 공공선을 고려해야 한다고 본다. Sandel은 자유주의의 탈맥락적 자아 개념을 비판하며 공동체 속 연루된 자아의 도덕적 책임을 강조했고, MacIntyre는 개인의 권리와 행동이 공동체적 실천과 덕성에 기초해야 한다고 주장하였다(Sandel, 2009; MacIntyre, 1981). 이러한 이론들은 데이터의 공공성과 투명성을 보장하는 GPL의 '공개', '책임', '자유' 정신과 결합될 때, 데이터 관리와 활용에 있어 공동체적 책임성과 민주적 정당성을 강화하는 이론적 기반이 된다.

GNU GPL 라이선스의 원칙을 데이터에 적용하는 것에 대한 타당성 논의는 신중한 접근이 필요하다. 본래 GPL은 소프트웨어 코드라는 저작권 보호 대상에 초점이 맞춰져 있으며, 데이터는 개인정보, 데이터베이스 권리, 저작물 등 다양한 유형과 복합적 성격을 가진 권리의 대상이다. 특히 개인정보는 재산권이 아닌 인격권적 성격을 가지며, 정보주체의 권리가 명확히 설정되어 있다(Nonju & Ihua-Maduenyi, 2024). 이러한 근

본적 차이는 GPL 라이선스를 데이터에 직접 적용하는 데 한계를 발생시킬 수 있다.

그럼에도 불구하고, GPL 라이선스가 강조하는 '공개성', '권리의 연속성', '책임 공유' 원칙은 데이터 활용의 투명성과 책임성 증대라는 측면에서 AI 데이터 거버넌스에 유용하게 응용될 수 있는 가능성을 제공한다. GPL의 정신을 부분적으로 수용하면서 비식별화, 차등 프라이버시 등 개인정보 보호 기술을 결합해 제한적 공개와 책임성을 실현하는 방식은 현실적인 대안이 될 수 있다(Kaissis et al., 2020; Carmody et al., 2021). 이는 데이터의 사회적 가치와 지속 가능한 혁신을 위한 기반을 마련하는 데 기여할 수 있다(Viljoen, 2021; Stallman, 2013).

따라서 본 연구는 데이터의 특성과 법적 제약을 반영하여, GPL 원칙을 직접적이고 전면적으로 적용하기보다는 'GPL에서 영감을 받은' 새로운 형태의 라이선스나 데이터 이용약관 구축을 제안한다. 이를 통해 개인정보 보호와 데이터 활용의 투명성 및 책임성 간 균형을 실현하고, 기술 민주주의와 데이터 거버넌스의 공공적 가치를 제고하는 것을 목표로 한다.

2. AI 개인정보 활용에 대한 선행연구 검토

AI 기반 서비스의 개인정보 활용과 관련하여, 다양한 분야에서 법적·윤리적 논의가 이루어지고 있다. 국제 연구에서는 AI 시스템의 인퍼런스(inference)[12]가 사용자 인식 없이 민감한 정보를 추론해내는 방식에 대한 우려가 증가하고 있다. Asthana 등은 AI 기반 개인화 추천 시

12) AI 시스템이 학습된 데이터를 바탕으로 새로운 정보나 사용자의 속성(예: 성별, 감정 상태, 정치 성향 등)을 추론하는 과정을 말한다. 특히 사용자의 직접 제공 없이도, 간접적인 행동 데이터를 통해 민감한 정보를 예측하는 데 사용될 수 있다.

스템이 유저 동의 없이 민감 정보를 유추할 수 있다는 사실에 대해 사용자들이 거부감을 보이며, 기존 동의 메커니즘의 한계를 지적하였다(Asthana et al., 2024).

Nonju와 Ihua-Maduenyi는 AI의 데이터 활용 능력이 기존의 개인정보 보호법제를 빠르게 무력화시키고 있으며, GDPR 등 기존 규제도 AI 고유의 학습 방식에 맞춰 재조정될 필요가 있다고 주장하였다(Nonju & Ihua-Maduenyi, 2024). Kaissis 등은 의료 데이터 처리에서 연합학습(federated learning)과 프라이버시 보존 기술을 결합해 데이터 보호와 AI 효율성의 균형을 제시하였다(Kaissis et al., 2020). 이는 사용자 데이터를 중앙 서버로 전송하지 않고도 AI를 학습시키는 방식으로, 에이닷 서비스에도 적용 가능한 설계 방식이다.

Carmody 등은 스마트 미터 데이터를 활용한 AI 분석이 소비자의 일상 패턴까지 추론 가능한 민감 정보를 생성한다는 점을 지적하며, 데이터의 2차 활용이 야기하는 프라이버시 침해 가능성을 경고하였다(Carmody et al., 2021). 이는 통화 기록이나 대화 내용이 AI에 의해 재구성될 때 발생할 수 있는 위험과 구조적으로 유사하다. Wang과 Zare는 헬스케어 AI 시스템에서 발생하는 데이터 권리 문제를 분석하며, GDPR의 적용 기준과 국내 법제도의 간극을 지적하였다(Wang & Zare, 2023). 특히 데이터 소유권, 삭제권, 동의 철회권 등에 대한 명확한 기준 부재는 AI 기반 플랫폼의 신뢰성을 저하시킬 수 있다.

Tat와 Rabbat은 AI 알고리즘의 편향성과 법적 책임 문제를 중점적으로 분석하며, 데이터 왜곡이 실제 서비스에서 어떻게 법적 위험으로 전이될 수 있는지를 실증적으로 제시하였다(Tat & Rabbat, 2021). 이는 잘못된 데이터 기반의 학습이 사용자 권리에 미치는 영향을 분석하는 데 유용한 프레임이다. 또한, Shimpo는 일본과 유럽연합의 법제를 비교하며, AI 시스템의 데이터 기밀성 확보를 위한 규제 설계의 필요성을 강조

하였다(Shimpo, 2020). 이는 기술 혁신과 법적 안정성 간의 균형 필요성을 시사하며, 에이닷 서비스가 수집하는 민감 데이터 보호의 제도적 보완 필요성을 뒷받침한다.

국내 연구에서는 김현경이 공개된 개인정보를 AI 학습 데이터로 사용할 때 발생할 수 있는 법적 쟁점을 분석하고, 정보주체의 통제권 보장을 위한 기준 설정의 필요성을 강조하였다(김현경, 2023). 이유정과 김민호는 미국의 사후동의(opt-out) 제도를 중심으로 국내 개인정보 동의제도의 실효성을 분석하고, AI 학습데이터 활용의 투명성과 책임성을 강화하기 위한 입법 방향을 제시하였다(이유정·김민호, 2023). 이와 함께 생성형 AI 기술의 법적 쟁점, 개인정보보호 제도 개선 방향 등을 중심으로 한 연구가 있으나(라기원 외, 2024), 개별 플랫폼이나 실제 상용 서비스에서 발생하는 데이터 수집 및 활용 구조에 대한 구체적 사례 분석은 아직 충분히 축적되지 않은 상황이다.

정부기관인 개인정보보호위원회는 AI 학습에 사용될 수 있는 「인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서」를 발표하였다(개인정보보호위원회, 2024). 이 안내서는 생성형 AI 개발 시 준수해야 할 기본 원칙을 제시하고 있으나, 실제 상용 플랫폼에 적용할 수 있을 정도로 구체적이고 실효적인 기준으로 보기에는 한계가 있다[13]. 특히 민감정보, 제3자 정보, 동의 범위 등에 대한 세부 규정은 미흡하다는 지적도 제기된다.

본 연구는 위에서 논의된 기술적·법적·윤리적 이론과 함께, 감시 자본주의와 데이터 시민권 이론을 통합적으로 반영하여 SK텔레콤의 에이닷(A.) 서비스 사례를 분석한다. 프라이버시 보호 원칙, 데이터 최소화, 사용자 권리 중심의 설계 프레임워크와 함께, 시민사회가 직면한 디지털 감

13) 이 안내서에서는 '공개된 개인정보'에 대한 정의를 제시하지만, 플랫폼 사업자가 어떤 조건하에 이를 수집·활용할 수 있는지에 대한 명확한 기준이나 사례는 포함되어 있지 않다.

시 구조와 권력 불균형 문제를 비판적으로 고찰함으로써 AI 데이터 활용의 사회적 맥락을 확장한다.

이를 통해 AI 기반 서비스의 기술적 효율성과 시민의 정보 권리 보장 간의 균형을 구체적으로 탐색하며, 실무적·정책적 대안을 제시하고자 한다. 기존 연구들이 AI 기술 전반의 개인정보 위험을 주로 제도적·기술적 관점에서 추상적으로 논의한 데 반해, 본 연구는 구체적 서비스 사례에 시민사회 이론과 기술 규범을 함께 적용하고, 정보 통제와 공공성 회복이라는 측면에서 디지털 전환 이후 시민의 권리 지형을 재조명한다는 점에서 차별화된다.

Ⅲ. SKT 에이닷 서비스 개요 및 문제점

1. 에이닷 서비스 개요

SK텔레콤의 에이닷(A.)은 2022년 공식 출시된 이후, 통신사 기반의 데이터 중심형 AI 비서 서비스로 빠르게 성장하고 있다. 해당 서비스는 사용자의 일상 대화, 검색 기록, 통화 음성 데이터를 중심으로 딥러닝 기반의 자연어 처리(NLP)와 머신 러닝(ML) 기술을 활용하여, 맞춤형 정보 제공, 콘텐츠 추천, 일정 관리, 통화 분석 등 다양한 개인화 기능을 제공한다. 특히 에이닷은 단순한 명령 수행형 AI를 넘어, 사용자의 행태를 장기적으로 학습하고 맥락적 정보를 파악함으로써 적응형 AI 비서(adaptive assistant)로 진화하고 있다. 이는 사용자의 언어 패턴, 감정, 시간대별 행위 패턴 등을 인지하여 상황별 응답을 생성할 수 있는 능력

을 포함한다.

이와 같은 고도화된 서비스 구현은 SK텔레콤이 보유한 대규모 통신 인프라와 가입자 기반을 토대로 가능하다[14]. 2024년 기준으로 에이닷은 통화 기능을 포함한 AI 서비스를 도입한 이후 가입자 수 500만 명을 돌파했으며, 이는 통신사 주도의 AI 시장 진출 전략의 성공 사례로 평가된다.

SK텔레콤은 기존 이동통신 데이터에 더해, 음성 녹음 데이터, 사용자 상호작용 기록, 제3자 연동 서비스 사용 정보 등을 통합적으로 수집하여 다층적 사용자 프로파일링을 수행한다. 이와 같은 데이터 수집 및 활용 구조는 SK텔레콤의 공식 '개인정보 처리방침(2024년 10월 기준)' 및 과학기술정보방송통신위원회 국정감사 자료에 명시되어 있으며, 실제 통화 음성과 제3자 정보까지 AI 학습에 활용된다는 사실이 확인되었다. 이러한 전략은 AI 성능 향상 측면에서 유의미하지만, 민감 정보의 수집과 활용, 알고리즘의 비투명성, 법적 정당성의 불분명성이라는 비판도 동시에 제기되고 있다[15].

실제로 최근 연구에 따르면, 통신사를 중심으로 구축되는 AI 비서 서비스는 데이터 통제력의 불균형을 심화시키고, 사용자에게 실질적인 거부권이나 데이터 삭제 권한이 부재한 경우가 많다는 점에서 프라이버시 자율성을 위협할 수 있다는 지적이 제기되고 있다(Zhan et al., 2023). 또한, SK텔레콤은 자사의 AI 전략 보고서에서 "고객의 다양한 행태 기반

14) 2024년 11월 14일에 에스케이(SK)텔레콤이 자사 통화앱 '티(T)전화'에 인공지능(AI) 기능을 결합한 서비스 명칭을 '에이닷 전화'로 변경함에 따라 기존의 티전화 고객은 일괄 A. 서비스로 이관되었다.

15) 국회 과학기술정보방송통신위원회 소속 더불어민주당 황정아 의원이 발표한 자료에 따르면 에이닷 전화는 통화내용 요약 텍스트, 음성, 이미지, 영상, 문서 파일 등 이용자가 입력한 정보를 수집하는 것으로 파악됐다. 황 의원은 이용자의 콘텐츠 미디어 이용 이력, 연락처와 통화 내역, 열람한 뉴스 채널, 구글 캘린더 등도 데이터 수집 대상이라고 비판했다. 또한 이러한 데이터 수집에 동의하지 않으면 서비스를 이용할 수 없도록 해 개인정보보호법을 위반했다고 지적했다. 자세한 내용은 연합뉴스, 「AI 더한 SKT 전화, 개인정보 수집내역만 1천160글자」 (2024.10.15.) 참고.

으로 실시간 상황인지형 AI를 설계한다"고 밝히고 있으나, 이러한 "상황인지형 추론 AI"가 어떤 기준과 알고리즘으로 작동하는지에 대한 정보는 공개되지 않아, 사용자와 기업 간의 정보 비대칭과 알고리즘 블랙박스 문제가 발생할 수 있다[16]. 이는 국내외에서 설명 가능 AI(eXplainable AI)에 대한 규범적 요구가 강화되고 있는 이유이며, 알고리즘의 결정 기준과 추론 과정에 대한 공개는 사용자 권리 확보의 핵심 요소로 간주된다(European Commission, 2023).

마지막으로, 에이닷의 전화 기능은 통화 내용을 기반으로 한 대화 이해와 응답 설계를 포함하고 있는데, 이는 사용자 본인뿐만 아니라 통화 상대방의 음성까지도 AI 학습의 입력값이 될 수 있다는 점에서, 제3자의 프라이버시 문제까지 고려되어야 하는 복합적 쟁점을 내포한다.

2. 학습 데이터 수집 방식

에이닷(A.) 서비스는 사용자의 다양한 활동 데이터를 수집하여 AI 모델 학습에 활용하고 있으며, 이 과정에서 자연어 처리(Natural Language Processing, NLP), 음성 인식(Speech Recognition), 추천 알고리즘(Recommender Systems) 등 다양한 기술이 통합적으로 적용된다. 이러한 구조는 최근 다수의 연구에서 분석된 AI 기반 개인 비서 시스템의 일반적 기술 메커니즘과 유사한 양상을 보인다(Zhan et al., 2023).

16) 전문가들은 아직까진 AI의 학습 알고리즘을 운영자도 정확히 파악하기 힘들다는 것이 한계점이라고 지적한다. 블랙박스는 인공지능에선 원하는대로 결과값을 도출할 순 있지만 무엇을 어떻게 학습해서 나온 결과인지 알 수 없는 상황을 일컫는다. 개발단계에서 발생하는 일종의 사각지대다. 자세한 내용은 뉴스핌, 「SKT 에이닷도 골머리…AI가 학습한 개인정보 어떻게 관리될까」 (2023.11.01.) 참고.

현재까지 에이닷의 학습 데이터 수집 구조에 대해 기술적으로 분석한 국내외 학술 연구는 거의 전무하며, 정책 수준에서도 주로 제도적·법적 논의에 한정되어 있다. 따라서 본 절에서는 기존 AI 비서 시스템에 관한 해외 기술연구들을 참조하여, 에이닷 서비스가 활용하는 데이터 유형과 수집 방식을 구조적으로 분석하고자 한다. 이를 통해 향후 AI 학습 구조에 대한 법적·윤리적 쟁점 논의의 기술적 기반을 제공할 수 있을 것이다.

(1) 대화 기록 : 에이닷은 사용자와의 음성 또는 문자 기반 대화 내용을 실시간으로 수집하고 이를 AI 학습 데이터로 활용한다. 사용자의 언어적 표현, 감정 상태, 문맥적 흐름 등을 모델이 학습하여 더욱 정교한 응답을 생성할 수 있게 하며, 이는 자연어 생성 성능 향상에 핵심적이다(Zhan et al., 2023).

(2) 통화 음성 데이터 : 에이닷 전화 서비스는 통화 내용 전체를 녹음하고 이를 분석에 활용한다. 이 데이터는 음성 기반 특성(억양, 발음, 간격, 반응 속도 등)을 학습하여 상황 반응형 응답 모델을 구축하는 데 사용되며, 음성 인식 정밀도와 감정 분석 알고리즘의 정교화에 기여한다. 그러나 동시에 해당 데이터는 제3자의 정보까지 포함할 가능성이 높아 동의 범위 및 데이터 소유권에 대한 법적·윤리적 우려가 제기된다(Ruff et al., 2021).

(3) 검색 기록 및 콘텐츠 소비 패턴 : 사용자의 검색 키워드, 앱 사용 이력, 시간대별 접속 패턴 등은 개인의 선호도를 반영하는 주요 지표로 활용되며, 맞춤형 콘텐츠 추천 및 UX 개선을 위한 핵심 데이터로 기능한다. 이는 AI가 사용자의 관심 영역을 정확히 파악하고, 정보 노출을 최적화하는 방식으로 발전하고 있다(Babatunde et al., 2024).

(4) 제3자 연동 서비스 데이터 : 에이닷은 일정, 날씨, 음악, 금융 등 다양한 외부 애플리케이션과 연동되어 작동하며, 이때 연동된 앱의 데이터

역시 학습 데이터로 수집된다. API 통합 구조를 통해 외부 데이터까지 통합 분석할 수 있으나, 이 과정에서 데이터가 제3자 플랫폼과 공유될 가능성이 존재하며, 이에 대한 사전 고지 또는 명시적 동의가 부족할 경우 정보주체의 통제권 약화로 이어질 수 있다(Pridmore et al., 2019).

이처럼 다양한 경로를 통해 수집되는 데이터는 사용자의 민감한 신체·정서·행동 정보를 학습자료로 변환하는 구조를 갖고 있으며, 통신 인프라를 바탕으로 작동하는 AI 비서 시스템의 특성상 데이터 주체의 실질적 통제권 부재, 동의 절차의 형식화, 제3자 정보 침해 등의 문제를 동시에 내포한다. Sabharwal 등은 AI 비서 기반 서비스의 확산이 사용자의 프라이버시 감각을 마비시키고, 장기적으로 신뢰 기반의 정보 생태계를 해칠 수 있다고 지적한다 (Sabharwal et al., 2023).

〈표 1〉 에이닷과 타통신사의 개인정보 필수동의항목 비교

항목	SKT 에이닷 (필수항목)	LG U+ (필수항목)
수집목적	서비스 제공 및 계약 이행 서비스 최적화 및 개인화 AI 모델 학습 및 개선 (음성 데이터 및 텍스트 데이터 활용) 이용자 식별 및 인증	이동통신 서비스 제공 고객 분석 및 맞춤형 서비스 제공 요금 관리 및 청구
수집항목	이용자의 성명, 전화번호, 이메일 위치정보 통화 녹음 파일 정보(통화연결여부, 통화시간, 통화상태방 연락처) 음성 파일(통화음성 녹음 파일) 텍스트 데이터 (명령어 및 음성 파일을 문서로 변환한 대화 기록) 기기 정보 (IP 주소, 접속 기록 등)	고객 성명, 전화번호, 주소 이동통신 요금 정보 및 서비스 이용 기록 계약 정보 및 결제 기록
보유 및 이용기간	음성 데이터: 수집일로부터 24개월, 서비스 탈퇴해도 24개월동안 보관됨. 기타 데이터: 법적 요구에 따라 보유	서비스 종료 후 5년 법적 요구에 따라 요금 정보는 10년까지 보유

(출처: SKT 에이닷 홈페이지, LG U+ 홈페이지)

3. 학습 데이터 활용 방식

에이닷(A.)은 수집한 사용자 데이터를 바탕으로 다양한 인공지능 기능을 구현하며, 이 과정은 자연어 처리(NLP), 추천 시스템, 사용자 행동 분석 등의 기술로 구성된다. AI 개인 비서 시스템에서 이와 같은 데이터 활용 구조는 다음과 같은 네 가지 핵심 영역으로 요약할 수 있다:

첫째 영역은 개인화 추천 (Personalized Recommendation)이다. 사용자의 검색 이력, 콘텐츠 소비 패턴, 앱 사용 데이터를 기반으로 AI는 개인 맞춤형 콘텐츠와 서비스를 추천한다. 이 과정은 사용자의 선호도와 관심사를 지속적으로 학습하며, 추천 정확도를 높이는 데 기여한다. 이러한 개인화 기능은 사용자 만족도를 높이지만, 과도한 데이터 분석이 프라이버시 침해로 이어질 가능성도 제기된다(Raji et al., 2024).

두 번째로, 대화 응답 답 최적화 (Conversational Optimization)이다. 이는 수집된 대화 데이터를 통해 NLP 모델은 문맥 기반 응답 생성을 수행하는 것으로, 감정 인식, 발화 패턴 분석, 맥락 추적 기능 등을 통해 자연스럽고 상황에 맞는 대화를 설계하는 것이 가능하다. 이러한 방식은 사용자와의 상호작용 품질을 높이는 데 기여하지만, 민감한 감정 정보의 내재적 처리 문제가 동반될 수 있다(Alijoyo et al., 2024).

세 번째로는 사용자 프로파일링 (User Profiling)이 가능하다는 점이다. AI는 사용자의 언어 습관, 시간대별 행동 패턴, 대화 흐름 등을 분석해 디지털 프로필을 구성한다. 이 프로파일은 광고 타게팅, 추천 콘텐츠 세분화 등 상업적 목적에도 활용될 수 있다. 그러나 이 과정은 정보 주체가 자신의 데이터가 어떻게 해석되고 활용되는지 알기 어려운 정보 비대칭 구조를 초래할 수 있으며, 장기적으로 사용자 신뢰 저하로 이어질 가능성이 있다(Wilson & Iftimie, 2021).

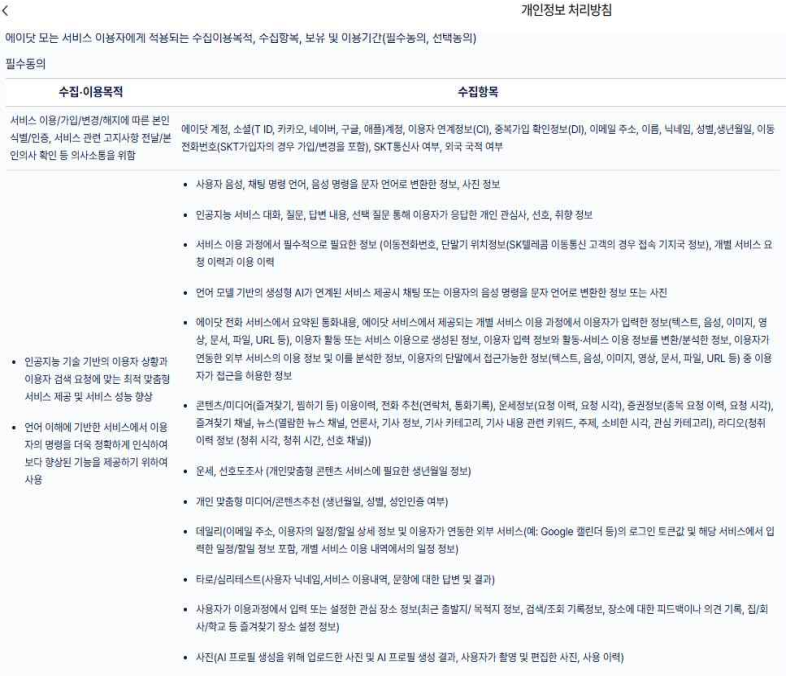
마지막으로 제3자 협업 및 데이터 공유의 영역이다. 에이닷은 일정,

음악, 뉴스 등 다양한 외부 애플리케이션과 연동되어 사용자 경험을 통합적으로 제공한다. 이 과정에서 제3자와의 데이터 공유가 불가피하며, 이는 사용자가 인지하지 못한 채 개인 정보가 외부 기업에 전송될 가능성을 내포한다. 특히, 데이터 공유 투명성이 보장되지 않으면, GDPR과 같은 개인정보보호법 위반 소지가 있다(Piñeiro-Martín et al., 2023).

4. 개인정보 수집 및 활용에 대한 동의 절차

에이닷(A.) 서비스는 사용자로부터 다양한 개인정보를 수집하며, 이에 대한 법적 정당성 확보 수단으로 '동의(consent)' 절차를 운영하고 있다. 그러나 이 동의 절차는 그 형식성과 비가시성, 그리고 정보 비대칭으로 인해 실질적인 프라이버시 보장 장치로 기능하지 못하고 있다는 비판이 제기되고 있다.

우선적으로, 초기 동의 절차가 있으나, 이는 형식적 동의와 정보 불균형의 문제를 안고 있다. 에이닷 서비스 가입 시 제시되는 약관과 개인정보처리 동의서는 다수의 세부 항목을 포함하고 있으나, 사용자는 이를 충분히 숙지하지 못한 채 '일괄 동의'하는 방식으로 서비스를 시작하게 된다. 이는 다수의 디지털 플랫폼이 채택하고 있는 '클릭통과(click-through)' 동의 방식의 대표적 사례로, 사용자의 자발적이고 구체적인 동의라고 보기 어렵다(Valtysson et al., 2021). 개인정보보호위원회와 한국인터넷진흥원이 실시한 '2022년 개인정보보호 및 활용조사'에 따르면, 개인정보를 제공할 때 수집·이용·제공 등 처리에 대한 동의 내용을 자세히 확인한다는 응답은 37.8%에 그쳤으며, 즉 국민 10명 중 6명 이상이 동의 내용을 잘 확인하지 않는 것으로 나타났다(개인정보보호위원회, 2023).


개인정보 처리방침

에이닷 모는 서비스 이용자에게 적용되는 수집이용목적, 수집항목, 보유 및 이용기간(필수동의, 선택동의)

필수동의

수집·이용목적	수집항목
서비스 이용/가입/변경/해지에 따른 본인 식별/인증, 서비스 관련 고지사항 전달/본인의사 확인 등 의사소통을 위함	에이닷 계정, 소셜(T ID, 카카오, 네이버, 구글, 애플)계정, 이용자 연계정보(CI), 중복가입 확인정보(DI), 이메일 주소, 이름, 닉네임, 성별,생년월일, 이동전화번호(SKT가입자의 경우 가입/변경을 포함), SKT통신사 여부, 외국 국적 여부
• 인공지능 기술 기반의 이용자 상황과 이용자 검색 요청에 맞는 최적 맞춤형 서비스 제공 및 서비스 성능 향상 • 언어 이해에 기반한 서비스에서 이용자의 명령을 더욱 정확하게 인식하여 보다 향상된 기능을 제공하기 위하여 사용	• 사용자 음성, 채팅 명령 언어, 음성 명령을 문자 언어로 변환한 정보, 사진 정보 • 인공지능 서비스 대화, 질문, 답변 내용, 선택 질문 통해 이용자가 응답한 개인 관심사, 선호, 취향 정보 • 서비스 이용 과정에서 필수적으로 필요한 정보 (이동전화번호, 단말기 위치정보(SK텔레콤 이동통신 고객의 경우 접속 기지국 정보), 개별 서비스 요청 이력과 이용 이력 • 언어 모델 기반의 생성형 AI가 연계된 서비스 제공시 채팅 또는 이용자의 음성 명령을 문자 언어로 변환한 정보 또는 사진 • 에이닷 전화 서비스에서 요약된 통화내용, 에이닷 서비스에서 제공되는 개별 서비스 이용 과정에서 이용자가 입력한 정보(텍스트, 음성, 이미지, 영상, 문서, 파일, URL 등), 이용자 활동 또는 서비스 이용으로 생성된 정보, 이용자 입력 정보와 활동·서비스 이용 정보를 변환/분석한 정보, 이용자가 연동한 외부 서비스의 이용 정보 및 이를 분석한 정보, 이용자의 단말에서 접근가능한 정보(텍스트, 음성, 이미지, 영상, 문서, 파일, URL 등) 중 이용자가 접근을 허용한 정보 • 콘텐츠/미디어(즐겨찾기, 찜하기 등) 이용이력, 전화 추천(연락처, 통화기록), 온세정보(요청 이력, 요청 시각), 증권정보(종목 요청 이력, 요청 시각), 즐겨찾기 채널, 뉴스(열람한 뉴스 채널, 언론사, 기사 정보, 기사 카테고리, 기사 내용 관련 키워드, 주제, 소비한 시각, 관심 카테고리), 라디오(청취 이력 정보 (청취 시각, 청취 시간, 선호 채널)) • 운세, 선호도조사 (개인맞춤형 콘텐츠 서비스에 필요한 생년월일 정보) • 개인 맞춤형 미디어/콘텐츠추천 (생년월일, 성별, 성인인증 여부) • 데일리(이메일 주소, 이용자의 일정/할일 상세 정보 및 이용자가 연동한 외부 서비스(예: Google 캘린더 등)의 로그인 토큰값 및 해당 서비스에서 입력한 일정/할일 정보 포함, 개별 서비스 이용 내역에서의 일정 정보) • 타로/심리테스트(사용자 닉네임,서비스 이용내역, 문항에 대한 답변 및 결과) • 사용자가 이용과정에서 입력 또는 설정한 관심 장소 정보(최근 출발지/ 북적지 정보, 검색/조회 기록정보, 장소에 대한 피드백이나 의견 기록, 집/회사/학교 등 즐겨찾기 장소 설정 정보) • 사진(AI 프로필 생성을 위해 업로드한 사진 및 AI 프로필 생성 결과, 사용자가 촬영 및 편집한 사진, 사용 이력)

(출처: SKT 에이닷 홈페이지)

〔그림 2〕 에이닷 개인정보 필수동의 항목

초기 동의 절차 이후에 통신사는 추가 데이터 수집에 대한 동의를 받는데, 이 과정에서 절차적 명확성이 결여될 수 있다. 서비스 이용 중 추가적으로 수집되는 통화 녹음, 검색 이력, 제3자 앱 연동 데이터 등은 초기 동의와는 별개로 추가적인 동의가 요구되는 민감한 정보이다. 그러나 이러한 동의는 서비스 중간 단계에서 충분히 공지되지 않거나, 사용자가 특정 기능을 이용함으로써 묵시적 동의가 발생하는 구조로 설계되어 있다(Drozd & Kirrane, 2020). 이는 GDPR이 요구하는 '명확하고 구체적인 동의(informed and specific consent)' 요건을 충족하지 못할 가능성이 높다.

이에 더해서, 동의 절차의 형식화 및 기술적 대응의 문제를 살펴봐야 한다. 기존 연구에 따르면, 디지털 플랫폼의 동의 절차는 일반적으로 형식적이고 비효율적인 정보 전달을 반복하는 구조로 설계되어 있으며, 사용자는 개인정보 처리 내용을 제대로 인식하지 못한 채 서비스를 이용하게 된다(García-Gasulla et al., 2020). 이에 대한 기술적 대안으로는 프라이버시 시각화(privacy visualization), 개인정보 대시보드, 계층형 정보 제공 시스템 등이 제시되고 있다. 특히, 블록체인 기반 동의 관리 시스템은 동의 내역의 변경, 철회, 추적 가능성을 기술적으로 보장함으로써 향후 디지털 서비스에서의 실질적 사용자 권리 보장 수단으로 주목받고 있다(Ameyed et al., 2021).

5. 에이닷 서비스 기반 데이터 활용의 구조적 쟁점

SK텔레콤의 에이닷(A.) 서비스는 고도화된 AI 알고리즘과 방대한 통신 데이터를 결합하여 개인 맞춤형 서비스를 제공하고 있으나, 그 과정에서 몇 가지 구조적인 위험 요소가 발견된다. 이러한 문제는 기술적 설계와 서비스 운영 차원에서 비롯되며, 사용자 권리, 투명성, 통제 가능성 측면에서 심각한 한계를 내포하고 있다.

에이닷은 다양한 형태의 사용자 데이터를 수집하지만, 각 데이터가 정확히 어떤 AI 기능에 어떻게 사용되는지에 대한 구체적인 설명이 부족하다. 이는 사용자가 자신의 데이터가 단순 서비스 제공 목적을 넘어, 모델 훈련, 상업적 목적, 제3자 연계 등에 활용되는지 여부를 인식하기 어렵게 만든다(Piñeiro-Martín et al., 2023). 또한, 사용자 대화, 통화, 검색 기록 등은 AI에 의해 정교하게 분석되어 행동 예측 및 성향 분류(profile inference)에 사용된다. 이는 사용자의 편의성 증대뿐 아니라, 정보 감시

(surveillance) 구조로 기능할 수 있는 잠재성을 함께 내포하며, 자율성과 프라이버시 침해 가능성이 동시에 존재한다(Wilson & Iftimie, 2021).

앞서 Ⅱ-4에서 분석한 바와 같이, 에이닷은 방대한 양의 민감 데이터를 처리하면서도, 이에 대한 사용자의 실질적인 통제를 보장하지 않는다. 특히 서비스 초기 설정 시의 일괄 동의, 동의 철회의 어려움, 추가 수집에 대한 고지 부족 등은, 사용자로 하여금 데이터 흐름과 위험성을 제대로 파악하지 못하게 만드는 구조로 작동한다(Drozd & Kirrane, 2020). 이에 더하여, 에이닷은 AI 처리 기능의 상당 부분을 클라우드 기반 인프라에서 수행하고 있으며, 이는 데이터 전송 및 저장 과정에서의 보안 취약성을 유발할 수 있다. 특히 외부 해킹, 제3자 위탁 처리, 데이터 복제 등의 문제는 기술적 보안과 법적 보장 사이의 간극을 드러낸다(Abdel-Wahid, 2024).

이와 같은 쟁점들은 에이닷 서비스에 국한되지 않고, 통신사 기반의 AI 개인 비서 시스템 전반에 내재한 구조적 문제로서 기능하며, 이후 장에서는 이러한 기술 구조가 개인정보 보호법, 이용자 권리, 윤리적 설계 원칙 등과 어떻게 충돌하거나 보완될 수 있는지를 구체적으로 분석할 필요가 있다.

Ⅳ. AI 데이터 활용의 법적·윤리적 한계

1. 법적 한계

AI 기반 서비스에서 데이터를 수집하고 활용하는 과정은 개인정보보호법(PIPA) 및 관련 법률에 의해 엄격하게 규제된다. 한국의 경우, 개인

정보보호법(PIPA)과 정보통신망법 등이 대표적인 규제 장치로 작용하며, 데이터의 수집, 처리, 저장, 활용 과정에서 발생하는 다양한 문제를 포섭하고자 한다. 개인정보보호법 제15조는 명확한 목적 하에 동의를 받아야 한다는 수집의 원칙을, 제17조는 제3자 제공 시의 사전 동의 의무를, 그리고 제18조는 수집된 개인정보를 당초 목적 외로 활용할 수 없다는 제한을 각각 규정하고 있다. 이러한 규정은 AI 서비스가 사용자 데이터를 학습용으로 재활용하려 할 때 주요한 법적 장벽으로 작용한다.

실제로 2021년 발생한 '이루다 AI 챗봇' 사건은 이러한 법적 한계를 실증적으로 보여주는 대표 사례이다(전승재·고명석, 2021). 해당 서비스는 사용자 대화 데이터를 사전 동의 없이 수집해 챗봇 학습에 활용하였고, 그 결과 개인정보보호법 제18조 위반으로 법적 책임이 부과되었다[17]. 이 사건은 AI 학습 과정에서의 데이터 활용이 단순한 기술적 문제를 넘어, 명확한 법적 기준을 충족해야 한다는 점을 사회적으로 환기시켰다. 또한 이루다 사례는 본 연구의 분석 대상인 에이닷(A.) 서비스와 마찬가지로 민감 정보의 비동의 수집, 목적 외 활용, 제3자 정보 포함이라는 구조적 유사성을 보이며, 현재 법제가 AI 기술의 데이터 활용 방식에 충분히 대응하지 못하고 있음을 보여준다. AI 학습 데이터 수집의 법적 불안정성은 특히 고위험 정보일수록 심화된다. 통화 데이터와 같이 실시간적이고 비정형적인 정보는 그 목적 명확성이 애초에 모호하며, 이에 대한 정보주체의 실질적 통제권 또한 제한될 수밖에 없다[18].

---

17) 개인정보보호위원회(개인정보위)는 2021. 4. 28. 인공지능(AI) 챗봇서비스인 '이루다'서비스의 개발 및 운영과정에서 카카오톡 대화 내용을 사용한 행위에 개인정보보호법 위반의 점이 있다고 판단하고 과징금 및 과태료 1억 330만원 등을 부과할 것을 의결했다. 관련 내용은 법률신문, 「'이루다' 사건에 대한 개인정보위 결정의 의미와 시사점」(2021/05/14). 참고.

18) 한국의 개인정보보호법(PIPA)은 유럽연합의 일반개인정보보호법(GDPR)과 유사한 규범 구조를 가지고 있으며, 데이터 수집 시 명확한 목적 설정과 사전 동의, 정보주체 권리 보장을 기본 원칙으로 설정하고 있다. 특히 제15조는 개인정보 처리의 목적 제한성 원칙을 명시하고 있으며, 제17조는 제3자 제공 시 명확한 동의를 요구하며, 제28조는 가명처리

〈표 2〉 이루다 AI 챗봇 사건과 SKT 에이닷(A.) 비교: 법적 쟁점과 구조적 유사성

구분	이루다 AI 챗봇 사건	SKT 에이닷(A.) 서비스
데이터 수집 방식	기존 SNS 대화 데이터 수집 (비동의 상태)	실시간 대화·통화 데이터 수집 (형식적 동의)
수집 정보의 민감성	사적 대화, 연애 감정 등 고민성 데이터	통화 내용, 제3자 음성, 검색 이력 등 고위험 정보
동의 절차	사용자 동의 없이 타 플랫폼 데이터 활용	초기 일괄 동의, 추가 고지는 불명확
법적 쟁점	PIPA 제18조 '목적 외 이용' 위반	PIPA 목적 제한 원칙, 제3자 동의 미비 가능성
제3자 정보 포함 여부	SNS 대화 상대방의 정보 포함 가능성	통화 상대방 정보 직접 포함 (제3자 동의 불명확)
사회적 파장	대중의 신뢰 저하, 법적 제재 발생	감시 우려 증폭, 통제권 부재 지적
제도적 시사점	개인정보 동의 구조 재정비 필요성 제기	고위험 AI 데이터에 대한 별도 보호체계 요구

AI 기술의 진보는 음성 기반의 상호작용을 중심으로 한 개인화 서비스의 확산을 가능하게 하였고, 이에 따라 통화 데이터와 같은 민감 정보의 수집과 활용이 점점 더 중요해지고 있다. 통화 데이터는 일반 텍스트 데이터와 달리, 높은 맥락성, 비정형성, 그리고 제3자의 정보까지 포함할 수 있는 특수한 성격을 가지기 때문에, 법적으로 더욱 정밀하고 신중한 접근이 요구된다. 특히 이러한 데이터가 AI 학습 시스템에 활용되는 경

된 개인정보라 하더라도 재식별 가능성이 있는 경우 엄격히 통제할 것을 요구한다. 그러나 본 연구에서 분석한 에이닷(A.) 서비스 사례와 같이, 실제 AI 학습 데이터 수집 및 활용 과정에서는 이러한 원칙이 실효적으로 작동하지 않는 경우가 많다. 첫째, 데이터 수집 목적이 AI 모델 훈련이라는 2차적이고 광범위한 목표를 포함할 경우, '명확한 목적 설정' 요건을 충족하기 어렵다. 특히, 통화 데이터와 같은 고위험 민감 정보가 서비스 제공 목적과 학습 목적 간 경계를 명확히 하지 않은 채 수집될 경우, 개인정보의 목적 외 활용 문제가 발생한다. 둘째, GDPR과 달리 PIPA는 동의 철회, 알고리즘 설명권, 자동화된 결정에 대한 이의 제기권 등의 정보주체 권한을 구체적으로 규정하지 않거나, 실효성 있게 작동하지 못하고 있다. 셋째, 재식별 위험 관리와 관련해 GDPR은 '적절한 기술적·조직적 보호조치'의 구체 기준을 지속적으로 보완하고 있는 반면, PIPA는 가명정보의 범위, 결합 절차, 재식별 금지 원칙 등에 대한 실무 적용 매뉴얼이 부족해, AI 데이터셋 운영 과정에서 법적 불확실성이 크다.

우, 통신이라는 본래 목적을 벗어난 '2차적' 활용이라는 점에서, 개인정보보호법(PIPA) 제15조와 제18조가 규정하는 수집 목적의 명확성 및 목적 외 사용 금지 조항과 충돌할 수 있다.

이와 같은 법적 한계를 보완하기 위한 제도적 시도로, 2024년 제정된 『인공지능의 발전 및 신뢰 기반 조성에 관한 법률』(AI 기본법)은 고위험 인공지능 시스템에 대한 별도 규제를 명시하였다. 이 법은 특히 음성, 이미지, 생체정보와 같이 민감도가 높은 데이터에 대해 활용 목적 및 범위의 명시, 설명 가능한 알고리즘 설계, 위험 평가 및 감시 체계의 마련 등을 의무화하고 있다. 이는 통화 데이터를 학습에 활용하는 AI 서비스에 직접 적용될 수 있는 규범적 근거를 제공하며, 개인정보보호법과의 입법적 보완 관계를 통해 법적 일관성을 높이는 효과도 기대할 수 있다. 특히 생성형 AI에 대해서는 그 결과물에 대한 설명 책임까지 부과하고 있다는 점에서, 통화 기반 응답을 생성하는 에이닷 서비스 역시 이에 대한 법적·윤리적 정당성을 갖추어야 한다는 요구를 받게 된다(김법연, 2023).

그러나 AI 기본법은 여전히 다음과 같은 측면에서 한계를 드러낸다. 첫째, 고위험 AI의 범위와 적용 기준이 추상적으로 제시되어 있어, 통화 데이터와 같은 실시간·비정형·제3자 정보를 포괄하는 복합적 활용 사례에 직접적인 적용이 어렵다. 둘째, 자율 규제와 산업 진흥을 법의 핵심 기조로 삼고 있어, 정보주체의 권리 보장이나 시민사회의 민주적 통제 원칙은 부차적인 위치에 머무르고 있다. 셋째, 통화 상대방의 정보와 같이 '비사용자'의 데이터 처리에 대한 규율은 여전히 공백 상태에 가깝다. 이는 고위험 정보에 대한 실질적 통제를 가능하게 할 사회적 거버넌스 구조가 미비하다는 점을 의미한다.

따라서 에이닷(A.) 서비스와 같은 통화 기반 AI 시스템의 규범적 정당성을 확보하기 위해서는 단순히 법률의 조문을 보완하는 수준을 넘어서야 한다. 데이터 수집 구조 자체에 대한 기술적 감시체계 구축, 제3자 권

리 보장을 위한 제도 설계, 시민사회 참여 기반의 투명성 확보 절차 등이 병행되어야 한다.

이러한 문제의식은 실제로 시민사회 단체들이 AI 기본법 시행령 검토 의견을 통해 반복적으로 제기하고 있으며, 특히 통신 기반 AI에서의 고위험 정보 보호 미비, 비사용자 정보의 규제 공백, 산업 중심 정책 설계에 대한 비판이 수렴되고 있다[19]. 이는 AI 데이터 활용이 특정 기업의 이익을 넘어 사회 전체의 신뢰와 감시 체계에 영향을 미치는 만큼, 시민사회 역시 이 문제에 적극적인 주체로 참여해야 함을 시사한다. 민주적 통제권 확보와 데이터 주권 실현은 이제 기술 정책의 부속 요소가 아니라, AI 시대의 핵심 규범적 과제로 재구성되어야 한다.

2. 제3자 정보 보호와 윤리적 설계 과제

통화 데이터의 구조적 특성은 단지 사용자(통화 개시자)의 정보만을 포함하는 것이 아니라, 상대방의 발화와 관련된 제3자의 정보 역시 함께 포섭된다는 점에서 윤리적으로 보다 복잡한 문제를 야기한다. 그러나 현재의 AI 관련 데이터 규율은 통상적으로 서비스 이용자의 동의와 권리 보장을 중심으로 구성되어 있으며, 통화 상대방에 대한 정보 보호 조치는 매우 미비한 수준에 머물러 있다. 이로 인해 다음과 같은 권리 공백이 발생한다: 첫째, 제3자의 정보가 비동의 상태에서 수집될 가능성이 상존하며, 둘째, 제3자가 자신의 정보에 대해 열람, 삭제, 수정 등의 권리를 행

19) 민주사회를 위한 변호사모임 디지털정보위원회·정보인권연구소·진보네트워크센터·참여연대, 「『인공지능 기본법』 시행령에 대한 시민사회 의견 제출」, 민변 공식 웹사이트, 2025.04.02. https://www.minbyun.or.kr/?p=63140. 해당 의견서에서는 고위험 AI 정의의 구체화, AI 감시체계에서의 정보주체 및 제3자 권리 보장 미비, 산업진흥 중심의 입법기조 문제 등을 지적하면서, 시민의 인권과 안전조치 규정을 요구하고 있다.

사할 수 있는 제도적 경로가 불명확하며, 셋째, 음성 데이터의 소유권과 처리 권한에 대한 법적 기준이 명시되어 있지 않아, 실제 AI 학습 데이터 셋에서의 권리 귀속이 불분명하다.

이러한 문제는 정보 주체의 범위를 명확히 하지 못하는 현행 법제의 한계를 드러내며, 통화 데이터가 기존 개인정보 보호 구조와 충돌하는 지점을 보여준다. 유럽연합의 GDPR은 공동 데이터 관리자의 개념을 통해 이와 유사한 문제를 부분적으로 해결하고자 하나, 현재 한국의 개인정보 보호법(PIPA)은 제3자의 정보에 대한 별도 보호 조항을 포함하고 있지 않으며, 통화 상대방이 정보 주체로서 권리를 행사할 수 있는 법적 근거도 부재하다. 이는 '비이용자 데이터 보호' 측면에서 입법적 사각지대를 형성한다.

더욱이, 통화 데이터를 처리하는 AI 시스템은 단순한 법적 규제 준수를 넘어 윤리적 설계 원칙(ethics by design)을 구현할 책임이 있다. 민감한 정보가 포함된 통화 내용은 서비스 과정에서 의도하지 않게 사적 맥락을 침해하거나, 제3자의 발화를 무단으로 수집하는 등 다양한 위험을 동반한다. 따라서 다음과 같은 기술적 설계 조치가 병행되어야 한다: 첫째, 민감 표현의 자동 마스킹 처리, 둘째, 제3자 발화를 탐지하고 학습에서 제외하는 알고리즘의 적용, 셋째, 대화 파편화 및 정교한 비식별화 처리를 통한 재식별 가능성의 최소화. 이러한 기술적 조치는 통화 데이터가 AI 학습에 활용되는 과정에서 발생할 수 있는 윤리적 위협을 완화하고, 사용자 및 사회의 신뢰 기반을 확보하는 데 기여할 수 있다. Sabharwal 등은 이러한 윤리적 설계의 부재가 장기적으로 서비스 수용성과 기업의 사회적 정당성을 약화시킬 수 있음을 지적한 바 있다(Sabharwal et al., 2023).

결과적으로, 통화 데이터는 그 민감도와 맥락성으로 인해 일반 개인정보보다 더 높은 수준의 규범적 보호가 요구되며, AI 기술과 결합될 경우 기존 법제와 윤리 체계를 초과하는 새로운 통제 메커니즘이 필요하다. 이

를 위해 통화 데이터를 고위험 정보로 별도 분류하고, 제3자 권리 행사 절차를 명문화하며, 특히, 고위험 데이터로서 통화 정보는 별도의 수집 동의 단계, 제3자 알림 시스템, 사후 열람·삭제 청구권 보장을 위한 전자 동의 대시보드 설계 등이 병행되어야 한다. 데이터 활용의 불투명성은 개인의 정보 통제권 침해를 넘어, 시민사회의 정보 감시 체계 강화와 자율성 약화를 초래하는 구조적 문제로 연결되며, 이는 AI 서비스의 지속 가능성을 위협하는 핵심 요인이 된다. 따라서 향후 AI 관련 법제는 통화 데이터를 중심으로 보다 정교한 권리 설계와 기술·제도 간의 통합적 거버넌스 체계를 수립함으로써, 기술 혁신과 정보 권리 보호 사이의 균형을 확보해야 할 것이다.

V. Stack Overflow AI 학습 데이터 사건: 공개 데이터와 AI 윤리의 경계

1. 공개 데이터에 대한 과신과 법적 쟁점

AI 기술의 확산은 방대한 양의 데이터 수집과 활용을 필수 요소로 만들었으며, 그 일환으로 인터넷상에 축적된 공개 데이터셋이 학습 자원으로 광범위하게 이용되고 있다. 특히 개발자 커뮤니티인 Stack Overflow는 자연어 처리(NLP) 및 코드 기반 모델 학습에 적합한 구조로 인해, 여러 AI 기업들이 데이터 수집 및 모델 훈련에 주요 출처로 활용해 왔다. 그러나 이와 같이 "공개된" 데이터조차도 법적·윤리적 책임으로부터 자유롭지 않다는 점은, Stack Overflow 사건을 통해 명확히 드러난다.

Stack Overflow는 CC BY-SA 4.0 라이선스를 채택하여 콘텐츠의 자유로운 사용을 허용하지만, 그 전제는 저작자 명시와 동일 라이선스 조건의 유지이다. 하지만 AI 개발자들이 이를 무시하거나 고지 없이 데이터를 수집·사용하는 경우가 빈번하게 보고되었다(Lucchi, 2024). 특히 저작자 고지 누락, 라이선스 조건 위반, 데이터 활용 사실 비공개, 사후 삭제 요청 거부 등은 단순한 기술적 실수로 보기 어려우며, AI 개발 과정에서의 규범적 무관심을 반영한다. 이는 공개 라이선스의 오남용과 데이터 주체의 권리 침해라는 이중 구조를 형성하며, AI 학습 전 단계에서 데이터의 법적 지위를 명확히 해야 할 필요성을 제기한다.

특히 Stack Overflow의 게시물은 일반적인 자연어 문장과 달리 기술적 명세, 코드, 해결방안 등 고유한 지적 재산을 포함하고 있으며, 이러한 데이터를 학습한 AI 모델이 생성하는 출력물이 원저작물의 파생물로 해석될 경우, 저작권 침해 여부는 더욱 복잡해진다(Buick, 2024). 이러한 맥락에서 AI 학습과정에서의 투명성과 동의 절차는 단순한 규제 이행의 문제가 아니라, 정보 주체의 권리를 보장하는 핵심 기제로 기능해야 한다.

또한, Stack Overflow 사례는 데이터의 "공공성" 개념 자체에 대한 재검토를 요구한다. 데이터가 공개되어 있다고 해서 그것이 무조건적으로 학습 목적에 사용 가능한 것은 아니며, 특히 상업적 목적의 AI 개발에 활용될 경우, 데이터 주체의 사전 동의, 데이터 처리 목적의 명확성, 이용 조건 고지 등은 필수 요건이 된다(Ørstavik, 2025). 공개 데이터와 AI 학습 사이의 경계는 여전히 불명확하며, 이에 대한 보다 정교한 법적·제도적 구획이 필요하다.

2. 데이터 윤리와 알고리즘 편향성: Stack Overflow와 에이닷 사례의 접점

Stack Overflow 사건은 기술 중심 커뮤니티의 특성상 특정 성별, 언어, 지역, 직업군 중심의 데이터가 과도하게 반영되었고, 그 결과 AI 모델이 특정 사회집단에 유리하거나 불리한 편향성을 내포할 위험이 있다(Papakyriakopoulos & Xiang, 2023). 이는 알고리즘 공정성에 대한 윤리적 우려로 이어지며, 데이터 출처의 사회적 맥락까지 고려하지 않는 한, AI는 비의도적 차별을 고착화하는 기술로 작동할 수 있다.

동시에, 데이터 수집 및 학습 과정 전반이 불투명하게 이루어졌다는 점에서 알고리즘의 설명 가능성과 책임성 결여도 심각한 문제로 지적된다. 유럽연합 AI 법안(AI Act)이나 저작권지침(CDSM)은 학습 데이터의 출처 및 사용 조건을 공개할 의무를 일부 도입했지만, 여전히 AI 출력물의 저작권 귀속, 학습데이터의 구성, 설명 책임 범위 등은 명확히 정의되지 않고 있다 (Buick, 2025). 유럽저작권학회(ECS)가 2025년 발표한 공식 의견서[20]에 따르면, 2019년 디지털단일시장 저작권지침(CDSM)과 2024년 EU AI Act로 구축된 규제 체계 하에서도 여러 법적 불확실성이 남아 있다고 지적한다(ECS, 2025).

이러한 쟁점은 앞서 논의한 에이닷(A.) 사례와도 구조적으로 밀접하게 연결된다. Stack Overflow 사건은 공개 커뮤니티 기반 데이터의 수집·활용 과정에서 동의 절차의 결여와 저작권 침해 가능성을 부각시킨 반면, 에이닷은 비공개 고위험 데이터인 실시간 통화 정보를 활용하면서 제3자 동의, 민감 정보 보호, 투명성 확보 등의 문제를 노출시켰다. 이처럼 상이한 맥락의 두 사례는, AI 학습 데이터 활용 전반에 걸쳐 반복적으로 등장하는 법적 공백과 윤리적 불균형을 보여주는 실증적 사례로 작동하며, '데이터 윤리 거버넌스' 구축의 필요성을 강하게 지지한다.

---

20) EU AI Act 및 CDSM Directive 하에서 남은 법적 불확실성을 분석한 공식 의견서임.

양 사례는 서로 다른 데이터 유형과 처리 맥락을 가짐에도 불구하고, 정보 주체 권리의 사전 보장 부재, 알고리즘 투명성 결여, 규제체계의 불충분성 등 핵심적 문제를 공유하고 있다. 이러한 공통성과 차이점을 구조적으로 비교해보는 것은, AI 기술 전반에서 반복적으로 발생하는 규범적 리스크의 유형을 식별하고, 제도 설계의 우선순위를 정립하는 데 중요한 단서를 제공한다. 다음 〈표 3〉은 Stack Overflow와 에이닷 사례의 법적·윤리적 쟁점을 항목별로 비교한 것이다.

〈표 3〉 Stack Overflow 사건과 에이닷 사례의 법적 · 윤리적 쟁점 비교

쟁점 유형	Stack Overflow 사건	에이닷(A.) 사례
데이터 출처 유형	공개된 커뮤니티 콘텐츠 (CC BY-SA 4.0 기반)	비공개 통화 데이터 (실시간 수집)
법적 문제	저작권 고지 누락, 라이선스 위반	개인정보보호법(PIPA) 목적 외 이용, 제3자 동의 미확보
정보 주체의 권리 보장	사용자에 대한 데이터 학습 고지 없음, 동의 미수집	사용자 일괄 동의, 통화 상대방의 권리 보호 미비
윤리적 쟁점	투명성 부족, 알고리즘 편향 가능성	설명 불가 응답, 사회적 감시 구조에 대한 우려
규제의 한계	저작권 기반 라이선스 관리 체계 미비	AI 기본법 및 개인정보보호법 간 불일치
대표적 공통점	사전 동의 및 정보 고지 부재, 데이터 권리 경시	데이터 활용의 정당성 및 윤리성 확보 실패
정책적 시사점	라이선스 조건 준수의무 강화, 학습 투명성 확보	고위험 AI에 대한 동의구조 개선, 제3자 권리 설계 필요

이러한 비교를 통해 AI 학습 데이터 활용에서 단순히 '공개 여부'에 초점을 맞추는 방식보다는, 정보 주체의 권리 구조를 명확히 설계하고, 법적·윤리적 책임을 다층적으로 분산할 수 있는 거버넌스 메커니즘이 규제의 핵심 기준이 되어야 함을 확인할 수 있다. 데이터의 접근 가능성만을 기준으로 한 기존 기술 중심적 접근은 정보 권리 보호에 있어 구조적 취약성을 내포하고 있으며, 이는 AI 생태계 전반의 지속 가능성에도 부정적 영향을 미친다.

결론적으로 Stack Overflow 사건은 단순한 저작권 침해 논의를 넘어,

공개된 데이터조차도 법적·윤리적 책임으로부터 면제될 수 없다는 점을 명확히 부각시키는 전환점적 사례로 작용한다. 이 사건은 AI 개발자 및 기업이 데이터 활용에 있어 기술적 효율성이나 시장 논리만을 우선할 것이 아니라, 정보 주체의 권리 보장, 알고리즘의 설명 가능성과 투명성 확보, 사회적 공정성이라는 원칙을 포함한 통합적 데이터 윤리 관리 체계를 수립할 필요성을 강하게 시사한다.

이러한 문제의식은 다음 장에서 제시할 GPL 기반 오픈소스 규범 체계와도 직접적으로 연결되며, 기존 법제도의 한계를 보완할 수 있는 실질적 대안으로 기능할 수 있다. AI 시대의 법제 설계는 이제 기술 진흥을 넘어, 데이터 정의와 권리, 책임의 구조화를 중심으로 재편되어야 할 것이다.

Ⅵ. AI 데이터 거버넌스를 위한 GPL 라이선스 원칙의 탐색

AI 학습 시스템이 방대한 양의 데이터를 처리하는 과정에서 발생하는 법적·윤리적 문제는, 단순히 특정 플랫폼이나 서비스에 국한된 개별 사건으로만 해석되기 어렵다. 앞서 분석한 에이닷(A.) 사례는 실시간 통화 데이터와 같은 민감 정보의 활용에서, Stack Overflow 사건은 공개적 데이터셋조차도 동의 구조와 저작권 준수 여부에서, 각각 규범적 결손을 드러낸 바 있다. 이처럼 다양한 서비스 유형과 데이터 구조에서 공통적으로 반복되는 문제는, 현재 개인정보보호법, 저작권법, AI 기본법 등이 각각의 한계를 지닌 채 개별적으로 작동하고 있기 때문이다.

이에 따라 본 장에서는 기존 제도의 보완 수단으로서, 오픈소스 소프트

웨어 영역에서 축적된 GNU General Public License(GPL)[21]의 규범 원칙이 AI 학습 데이터 거버넌스에 부분적으로 적용될 수 있는 가능성을 탐색한다. 이는 법적 대안으로의 전면적 도입이 아니라, 앞서 제기된 문제를 조율할 수 있는 자율규범적 모델의 가능성을 모색하는 탐색적 시도이다.

1. GPL 원칙과 그 적용 가능성

GPL(GNU General Public License)은 자유 소프트웨어 운동의 일환으로 탄생한 대표적인 오픈소스 라이선스이다. 이 라이선스는 기술 공동체 내부에서 형성된 자율적 통제 메커니즘으로서, 법적 강제력이 아니라 조건부 공유와 책임의 구조화를 통해 기술의 공개성과 공공성을 확보하고자 한다. 특히 copyleft 조항은 파생 저작물 역시 동일한 라이선스 조건을 유지하도록 하여, 소프트웨어의 탈공공화 또는 독점화를 방지하는 데 목적을 둔다[22](Schmit et al., 2023). AI 학습 데이터 활용에 있어 이와 같은 원칙을 고려해보는 것은, 기존 규제 체계의 한계 지점을 보완하기 위한 하나의 탐색적 접근이라 할 수 있다.

GPL의 핵심 원칙은 크게 세 가지로 정리된다. 첫째, 복제 및 배포의 자유는 명확한 조건 하에 데이터 또는 소프트웨어를 공유할 수 있도록 하며, 둘째, 수정 및 파생물 재배포의 자유는 가공된 결과물 역시 동일한 조건 하에 공유되도록 하여 책임을 회피할 수 없도록 한다. 셋째, 소스코드 공개의무는 기술적 구조와 처리 방식의 투명성을 보장하며, 이는

21) GPL은 1989년 자유 소프트웨어 재단(Free Software Foundation)에 의해 제정되었으며, 사용자로 하여금 소프트웨어의 자유로운 이용, 복제, 수정, 재배포를 허용하되, 동일한 자유를 다음 사용자에게도 보장해야 하는 조건을 부과한다.

22) Copyleft는 저작권을 보유한 주체가 자신의 권리를 포기하는 대신, 모든 파생물 역시 동일한 조건으로만 공유될 수 있도록 요구함으로써, 오픈소스 소프트웨어의 공공성을 유지하는 법적 장치이다.

AI의 설명 가능성과 감시 가능성 확보 측면에서 핵심적이다.

그러나 GPL은 본래 소프트웨어 코드라는 명확한 저작권 대상으로 설계된 것이며, 데이터는 개인정보, 데이터베이스 권리, 저작물 등 다양한 권리의 대상이 혼재되어 있고, 특히 개인정보는 인격권적 성격을 가지고 있어 동일한 방식의 접근이 제한될 수 있다(Nonju & Ihua-Maduenyi, 2024). 이러한 근본적인 차이는 GPL 라이선스를 AI 학습 데이터에 직접적으로 적용하기에는 분명한 한계를 나타낸다.

2. 제한적 적용과 보완 방향

앞서 밝힌 바와 같이 GPL은 소프트웨어 라이선스로 설계되었기 때문에, AI 데이터셋과 같은 비정형 정보 자산에 그대로 적용되기는 어렵다. 또한 상업적 AI 모델의 개발 및 운영 환경에서는 독점적 알고리즘과 학습 데이터가 경쟁력의 핵심 자산이 되기 때문에, 완전한 공개와 자유로운 재배포는 현실적으로 제약이 있다. 그럼에도 불구하고, 다음과 같은 방향에서 GPL의 원칙을 조정·보완하여 적용할 수 있는 가능성이 제기된다.

첫째, 제한된 공개성에 기반한 투명한 메타데이터 기록 체계의 구축이다. AI 데이터셋에 대해 수집 경로, 전처리 방식, 가공 이력 등을 명시하고, 이를 별도 메타데이터 구조로 관리함으로써, 설명 가능한 AI와 외부 감시 가능성을 확보할 수 있다.

둘째, 파생 데이터의 조건부 공유를 통한 규범 일관성 확보이다. AI 모델이 학습한 원본 데이터가 가공되어 2차적으로 활용될 경우에도, 초기 조건(예: 동의, 공개 범위, 수정 제한 등)이 이어지도록 설계할 필요가 있다. 이는 copyleft 원칙의 연장선상에 있다(Basso et al., 2022).

셋째, 민감 정보 보호와 공개성 간의 균형적 설계이다. GPL이 추구하

는 자유로운 공유는 공공적 가치 실현에 유효하지만, AI 학습 데이터에는 개인정보, 생체정보 등 고위험 정보가 포함될 수 있어, 접근 계층화와 보안 체계 구축이 병행되어야 한다.

넷째, AI 특화형 규범 체계의 개발이 요구된다. GPL 원칙을 전면적으로 수용하기보다, 이를 참조한 형태의 AI 데이터 전용 라이선스(AI-GPL, Open Data Pledge 등)를 설계함으로써, 상업적 서비스 환경과 개인정보 보호법, 저작권법 등과의 충돌을 조정할 수 있다(Duan et al., 2024).

결론적으로, GPL의 구조는 AI 학습 데이터 거버넌스의 여러 난제를 해결할 수 있는 직접적인 해법은 아닐 수 있으나, 데이터의 공개·수정·재사용·책임 연속성이라는 측면에서 제도적 실마리를 제공하는 유의미한 참조 모델이 될 수 있다. 물론 상업적 AI 서비스와의 조화, 국가 간 법제 차이, 기술적 구현 가능성 등 여러 과제가 존재하나, GPL적 접근 방식은 공공성과 공정성을 중심으로 한 새로운 AI 데이터 거버넌스 모델의 기반이 될 수 있는 잠재력을 지니고 있다. 특히 법제도의 형식적 틀을 넘어, 기술과 규범이 상호 구조화된 상태에서 작동하는 자율 규범적 데이터 정의 거버넌스 모델을 설계하기 위한 출발점으로 기능할 수 있다.

Ⅶ. 결론: 디지털 시민사회를 위한 AI 데이터 활용의 새로운 거버넌스 모델

1. 연구 결과 요약

본 연구는 SK텔레콤의 AI 비서 서비스인 에이닷(A.) 사례를 중심으로,

AI 학습 데이터를 둘러싼 법적·윤리적 쟁점을 분석하였다. 특히 통화 데이터와 같은 고위험 정보의 활용은, 개인정보보호법(PIPA)의 목적 제한성 원칙과 사전 동의 요건에 저촉될 가능성이 높으며, 통화 상대방과 같은 제3자 정보가 포함되는 경우 그 법적 불확실성은 더욱 증폭된다.

또한 Stack Overflow 사건을 통해 '공개 데이터'라 하더라도 저작자 고지, 동의 구조, 활용 목적의 명확성이 결여될 경우 심각한 법적·윤리적 문제가 발생함을 실증적으로 확인하였다. 두 사례는 모두 AI 학습 데이터 활용이 기술적·법적 조건을 초월하여 사회적 신뢰 인프라와 직결된 문제임을 보여준다.

이러한 문제의식에 기반하여, 본 연구는 GNU GPL(GNU General Public License)의 규범 원칙—특히 copyleft, 책임 연속성, 투명한 조건부 공유—를 AI 데이터 거버넌스에 부분적으로 적용할 수 있는 가능성을 탐색하였다. 이는 기존 제도의 공백을 보완할 수 있는 자율 규범 기반의 대안적 접근으로 제안되었다. 다만, GPL이 원래 저작권 기반의 소프트웨어 라이선스로 설계되었고, 개인정보와 같은 인격권적 데이터에는 직접 적용이 곤란하다는 점을 인식하고, 그 원칙을 참조하여 기술적·제도적으로 조정된 데이터 특화형 규범 체계 개발의 필요성을 함께 제시하였다.

2. 연구의 학문적 및 정책적 함의

첫째, AI 학습 데이터 활용에서 발생하는 권리 침해 문제를 단순한 이용자-플랫폼 간 계약의 문제가 아닌, 디지털 사회 전반의 감시 구조, 데이터 주권, 정보 통제권의 문제로 확장하여 분석함으로써, 개인정보 보호 담론을 개인주의적 틀에서 사회구조적 틀로 전환하였다. 이는 디지털 시민사회론과 데이터 민주주의 이론 간의 연결 가능성을 열어준다[23].

둘째, 개인정보보호법과 AI 기본법 등 기존 법제의 규범적 한계와 실무적 불일치를 비판적으로 진단하고, 기술적 설계와 법적 원칙이 상호작용할 수 있는 통합형 데이터 거버넌스 모델의 가능성을 제시하였다. 특히 GPL 기반의 구조는 법제 외적 규범 장치로 기능할 수 있는 "기술적 자율규범"으로 해석되며, 이는 실무 적용 가능성이 높은 이론적 틀이다(Schmit et al., 2023).

셋째, AI 데이터 거버넌스를 위한 핵심 원칙들—투명성, 권리 연속성, 수정 이력 공개, 설명 가능성—을 정립하고 이를 구체 사례에 적용함으로써, 실질적 실행이 가능한 규범적 기준을 제안하였다. 이는 학문적 공헌뿐만 아니라, 정책 설계 단계에서의 실질적 참조 기준으로 활용될 수 있다. 특히 투명한 메타데이터 구조, 제한된 공개와 접근 계층화, 파생 데이터의 조건부 공유 등은 향후 AI 데이터 라이선스 모델(AI-GPL 등) 개발에 실질적 기초가 될 수 있다.

넷째, 본 연구는 기술 중심의 AI 담론을 넘어, 데이터 주체의 권리 회복과 민주적 통제 가능성에 주목하였다. 특히 에이닷 사례는 시민이 데이터 활용의 객체가 아닌 주체로 자리매김할 수 있는 제도적 기반 구축의 필요성을 환기시킨다. 이는 데이터 정의권(data definitional authority) 확보를 위한 시민 주권 기반 AI 거버넌스로 나아가기 위한 이론적 전환점이라 할 수 있다.

3. 연구의 한계 및 후속 연구 제언

본 연구는 질적 사례 분석에 기반한 이론 탐색 중심으로 구성되었기

23) 데이터 민주주의(Data Democracy)는 데이터의 수집, 활용, 관리 전 과정에서 시민의 참여와 권리를 제도적으로 보장하려는 규범적 패러다임이다. 감시사회 이론(Zuboff, 2019)과 결합되어 시민 주권 기반 AI 규제 틀로 확대되고 있다.

때문에, 실제 사용자 경험을 반영한 정량적 분석이나 사회적 수용성 평가는 포함하지 못하였다. 향후 연구에서는 인터뷰, 설문, 이용자 로그 기반의 분석을 통해 실증적 데이터를 축적하고 이론적 틀을 검증하는 작업이 필요하다. 또한 본 연구는 주로 한국의 법제도(PIPA, AI 기본법)를 중심으로 분석되었기에, GDPR이나 미국의 TDM 예외 제도, 일본의 AI법제 등 국제적 법제 간 비교 분석은 미흡하였다. 향후 연구는 다양한 국가의 제도적 맥락과 오픈 라이선스 구조를 비교·통합하는 방향으로 확장될 수 있다.

AI 기술 발전 속에서 데이터는 단지 기술 자원을 넘어서, 공공성, 권리, 민주주의를 지탱하는 핵심 인프라로 기능하고 있다. 본 연구는 이 전환점에서 AI 학습 데이터 수집 및 활용의 법적·윤리적 문제를 다층적으로 분석하고, 기술과 규범이 결합된 대안적 거버넌스 모델을 모색하였다.

GPL의 원칙은 비록 법적 직접 적용에는 한계가 있지만, 그 철학과 구조는 AI 데이터 거버넌스의 규범적 기초로서 실질적인 참조모델이 될 수 있다. 향후 AI-GPL, 데이터 정의권 보장 규약 등으로 구체화 된다면, 법제도 공백을 보완하고 기술 생태계 내부의 책임성과 투명성을 제도화할 수 있는 실천적 대안으로 발전할 수 있다. 이는 단지 법적 대안이 아닌, 디지털 시민사회를 위한 윤리적 인프라로서의 AI 데이터 규범을 구축하기 위한 기초로 기능할 수 있다. 향후 AI 시대의 거버넌스 설계는, 기술 효율성과 함께 시민 권리를 중심에 둔 규범 구조를 반드시 내장해야 한다.

(2025년 4월 9일 접수, 5월 10일 심사완료, 5월 10일 게재확정)

참고문헌

개인정보보호법. 2025. 법률 제19234호, 국가법령정보센터.

개인정보보호위원회·한국인터넷진흥원. 2023.「2022년 개인정보보호 및 활용조사」.

개인정보보호위원회. 2024.「인공지능 개발·서비스를 위한 공개된 개인정보 처리 안내서」.

김경민·이용준·강장묵. 2024, "인공지능 발전에 따른 책임과 법적 규제에 대한 연구",「한국산학기술학회 논문지」25(7), 490-496.

김법연. 2023. "인공지능 통제수단으로서 주요국 규제 입법의 동향과 시사점",「유럽헌법연구」제42호, 유럽헌법학회.

김현경. 2023. "공개된 개인정보의 법적 취급에 대한 검토: AI학습용 데이터로서 활용방안을 중심으로".「미국헌법연구」34(1), 157-192. 미국헌법학회.

라기원·이유봉·윤길준. 2024.「AI 활용과 대응을 위한 입법분야 조사 연구」, 연구보고 24-20-4, 한국법제연구원.

양관석. 2019.「인공지능의 빅데이터 활용을 위한 법적 연구: 저작물과 개인정보를 포함한 빅데이터를 중심으로」(박사학위논문). 단국대학교.

이유정, 김민호. 2023. "인공지능 학습데이터와 개인정보보호법상 동의제도에 관한 연구: 미국의 사후동의(opt-out)제도를 중심으로".「미국헌법연구」34(2), 1-37. 미국헌법학회.

인공지능 기본법. 2025. 법률 제20676호. 국가법령정보센터. (시행 2026.1.22.).

전승재, 고명석. 2021, "이루다 사건을 통해서 보는 개인정보의 인공지능 학습데이터 활용 가능성",「정보법학」25(2), 103-133. 한국정보법학회.

정보통신망 이용촉진 및 정보보호 등에 관한 법률. 2024. 법률 제20260호, 국가법령정보센터.

Abdel-Wahid, T. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. International Journal of Information Technology and Electrical Engineering (IJITEE)-UGC Care List Group-I, 13(3), 11-19.

Aldboush, H., & Ferdous, M. (2023). “Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust.” International Journal of Financial Studies. https://doi.org/10.3390/ijfs11030090.

Alijoyo, F. A., Sri, S. S. S., Alapati, P. R., & Yuldashev, D. (2024). “Ethical considerations in explainable AI: Balancing transparency and user privacy in English language-based virtual assistants.” In 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 399-406). IEEE.

Ameyed, D., Jaafar, F., Charette-Migneault, F., & Cheriet, M. (2021). “Blockchain based model for consent management and data transparency assurance.” In 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 1050-1059). IEEE.

Andreotta, A., Kirkham, N., & Rizzi, M. (2021). “AI, big data, and the future of consent.” Ai & Society, 37, 1715 - 1728. https://doi.org/10.1007/s00146-021-01262-5.

Asthana, S., Im, J., Chen, Z., & Banovic, N. (2024). "“I know even if you don't tell me": Understanding Users' Privacy Preferences Regarding AI-based Inferences of Sensitive Information for Personalization.” In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (pp. 1-21).

Babatunde, S. O., Odejide, O. A., Edunjobi, T. E., & Ogundipe, D. O. (2024). “The role of AI in marketing personalization: A theoretical exploration of consumer engagement strategies.” International Journal of Management & Entrepreneurship Research, 6(3), 936-949.

Basso, A., Ribeca, P., Bosi, M., Pretto, N., Chollet, G., Guarise, M., Choi, M., Chiariglione, L., Iacoviello, R., Banterle, F., Artusi, A., Gissi, F., Fiandrotti, A., Ballocca, G., Mazzaglia, M., & Moskowitz, S. (2022). “AI-Based Media

Coding Standards." SMPTE Motion Imaging Journal, 131, 10-20. https://doi.org/10.5594/JMI.2022.3160793.

Bielova, M., & Byelov, D. (2023). "Challenges and threats of personal data protection in working with artificial intelligence." Uzhhorod National University Herald. Series: Law. https://doi.org/10.24144/2307-3322.2023.79.2.2.

Buick (2024), "Copyright and AI Training Data—Transparency to the Rescue?", Journal of Intellectual Property Law & Practice, 20 (3), 182-192. https://doi.org/10.1093/jiplp/jpae102.

Carmody, J., Shringarpure, S., & Venter, G. (2021). "AI and privacy concerns: a smart meter case study." J. Inf. Commun. Ethics Soc., 19, 492-505. https://doi.org/10.1108/jices-04-2021-0042.

Casilli, A. A. (2019). En attendant les robots-Enquête sur le travail du clic. Média Diffusion.

Cavoukian, A. (2012). "Privacy by design: leadership, methods, and results." in European Data Protection: Coming of Age (pp. 175-202). Dordrecht: Springer Netherlands.

Descalzo, F. (2024). "Designing Artificial Intelligence with Privacy at the Center." In 2024 IEEE Biennial Congress of Argentina (ARGENCON) (pp. 1-4). IEEE.

Drozd, O., & Kirrane, S. (2020). "Privacy CURE: Consent comprehension made easy." In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 124-139). Cham: Springer International Publishing.

Duan, M., Zhao, R., Jiang, L., Shadbolt, N., & He, B. (2024). ""They've Stolen My GPL-Licensed Model!": Toward Standardized and Transparent Model Licensing." arXiv preprint arXiv:2412.11483.

ECS(European Copyright Society). (2025). Opinion on copyright and generative AI. Brussels: ECS.

Garcia-Gasulla, D., Cortés, A., Alvarez-Napagao, S., & Cortés, U. (2020). "Signs

for ethical AI: A route towards transparency." arXiv preprint arXiv:2009.13871.

Gray, M. L., & Suri, S. (2019). Ghost work: How to stop Silicon Valley from building a new global underclass. Harper Business.

Habermas, J. (1989). The structural transformation of the public sphere: An inquiry into a category of bourgeois society (T. Burger & F. Lawrence, Trans.). MIT Press. (Original work published 1962)

Habermas, J. (1991). The structural transformation of the public sphere: An inquiry into a category of bourgeois society. MIT press.

Hendricks, D. (2024). ""Introduction to AI Safety, Ethics, and Society: Scaling Laws." https://www.aisafetybook.com/textbook/scaling-laws.

Hijmans, H., & Raab, C. (2022). "Ethical Dimensions of the GDPR, AI Regulation, and Beyond." Direito Público. https://doi.org/10.11117/rdp.v18i100.6197.

Hutton, L., & Henderson, T. (2017). "Beyond the EULA: Improving consent for data mining." ArXiv,abs/1701.07999. https://doi.org/10.1007/978-3-319-54024-5_7.

Isin, Engin & Ruppert Evelyn (2015), Being Digital Citizens, London: Rowman & Littlefield International.

Kaissis, G., Makowski, M., Rückert, D., & Braren, R. (2020). "Secure, privacy-preserving and federated machine learning in medical imaging." Nature Machine Intelligence, 2, 305-311. https://doi.org/10.1038/s42256-020-0186-1.

Kitchin, R. (2014). The data revolution: Big data, open data, data infrastructures and their consequences. Sage.

Lucchi, N. (2024). "ChatGPT: a case study on copyright challenges for generative artificial intelligence systems." European Journal of Risk Regulation, 15(3), 602-624.

MacIntyre, A. (1981). After virtue: A study in moral theory. University of Notre

Dame Press.
McDonald, S. M. (2022). On Forging a Path to Digital Rights. Centre for Int'l Governance Innovation.
Meurisch, C. (2021). "Data Protection in Personalized AI Services: A Decentralized Approach." Darmstadt, https://doi.org/10.26083/TUPRINTS-00019355.
Meurisch, C., & Mühlhäuser, M. (2021). "Data Protection in AI Services." ACM Computing Surveys (CSUR), 54, 1 - 38. https://doi.org/10.1145/3440754.
Meurisch, C., Bayrak, B., & Mühlhäuser, M. (2020). "Privacy-preserving AI Services Through Data Decentralization." Proceedings of The Web Conference 2020. https://doi.org/10.1145/3366423.3380106.
Morozov, E. (2013). To save everything, click here: The folly of technological solutionism. PublicAffairs.
Nonju, D. K. D., & Ihua-Maduenyi, A. B. (2024). "The Impact of Artificial Intelligence on Privacy Laws." International Journal of Research and Innovation in Social Science, 8(9), 2150-2174.
Open Data Commons Open Database License (ODbL), Open Knowledge. https://opendatacommons.org/licenses/odbl/summary/.
Ørstavik, IB (2025). "Development of Large Language Models: Copyright Law Perspectives for Research Institutions and Research Libraries", International Journal of Legal Information, 53(1), 1-12, doi:10.1017/jli.2024.46.
Papakyriakopoulos, O., & Xiang, A. (2023). "Considerations for Ethical Speech Recognition Datasets." Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining. https://doi.org/10.1145/3539597.3575793.
Piñeiro-Martín A., García-Mateo C., Docío-Fernández L., & López-Pérez M.d.C. (2023). "Ethical Challenges in the Development of Virtual Assistants Powered by Large Language Models." Electronics, 12(14):3170.

https://doi.org/10.3390/electronics12143170.

Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P. C., & Liao, Y. (2019). Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. Surveillance & Society.

Radanliev, P., & Santos, O. (2023). "Ethics and Responsible AI Deployment." ArXiv, abs/2311.14705. https://doi.org/10.48550/arXiv.2311.14705.

Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). "E-commerce and consumer behavior: A review of AI-powered personalization and market trends." GSC Advanced Research and Reviews, 18(3), 066-077.

Ruff, C., Horch, A., Benthien, B., Loh, W., & Orlowski, A. (2021). "DAMA-A transparent meta-assistant for data self-determination in smart environments." In Open Identity Summit 2021 (pp. 119-130). Gesellschaft für Informatik eV.

Sabharwal, D., Kabha, R., & Srivastava, K. (2023). "Artificial intelligence (ai)-powered virtual assistants and their effect on human productivity and laziness: Study on students of delhi-ncr (india) & fujairah (uae)." Journal of Content, Community and Communication, 17(9), 162-174.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. Big data & society, 6(1), 2053951718820549.

Sandel, M. J. (2009). Justice: What's the right thing to do? Farrar, Straus and Giroux.

Schmit, C. D., Doerr, M. J., & Wagner, J. K. (2023). "Leveraging IP for AI governance. Science." 379(6633), 646-648.

Sebastian, G. (2023). "Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4454761.

Shimpo, F. (2020). “The Importance of ‘Smooth’ Data Usage and the Protection of Privacy in the Age of AI, IoT and Autonomous Robots.” Global Privacy Law Review. https://doi.org/10.54648/gplr2020006.

Shumailov, I., Shumaylov, Z., Zhao, Y. et al. (2024). “AI models collapse when trained on recursively generated data.” Nature 631, 755-759 . https://doi.org/10.1038/s41586-024-07566-y.

Singh, P. J., & Vipra, J. (2019). Economic rights over data: A framework for community data ownership. Development, 62(1), 53-57.

StackExchange. Share-alike style License for data that will be used to train machine learning models. https://opensource.stackexchange.com/.

Stallman, R. (2013). “Why Free software is more important now than ever before.” For Free Information and Open Internet, 57.

Tat, E., & Rabbat, M. (2021). “Ethical and legal challenges.” Machine Learning in Cardiovascular Medicine, 395-410. Academy Press. https://doi.org/10.1016/B978-0-12-820273-9.00017-8.

Valtysson, B., Jørgensen, R. F., & Munkholm, J. L. (2021). “Co-constitutive complexityUnpacking Google’s privacy policy and terms of service post-GDPR.” Nordicom review, 42(1), 124-140.

Viljoen, S. (2021). A relational theory of data governance. The Yale Law Journal, 573-654.

Wang, P., & Zare, H. (2023). “A Case Study of Privacy Protection Challenges and Risks in AI-Enabled Healthcare App.” 2023 IEEE Conference on Artificial Intelligence (CAI), 296-297. https://doi.org/10.1109/CAI54212.2023.00132.

Wilson, R., & Iftimie, I. (2021). “Virtual assistants and privacy: An anticipatory ethical analysis.” In 2021 IEEE international symposium on technology and society (ISTAS) (pp. 1-1). IEEE.

Zhan, N., Sarkadi, S., & Such, J. (2023). “Privacy-enhanced personal assistants

based on dialogues and case similarity." In European Conference on Artificial Intelligence. IOS Press.
Zhang, Jiehuang & Yu, Han. (2023). "A Design Methodology for Incorporating Privacy Preservation into AI Systems." In Proceedings of the International Workshop on Trustworthy Federated Learning (TrustFL@IJCAI 2023).
Zuboff, Shoshana. (2019), The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power , New York: PublicAffairs.

Abstract

The Boundary Between AI Training Data and Personal Information Rights: Governance and Control Challenges in the Case of "A.", an AI Assistant by SK Telecom

Yoo Sunghee, Suh Hyo-Joong***

The rapid expansion of generative AI has significantly increased the demand for large-scale, high-quality training data, raising critical legal and ethical concerns regarding the use of personal information. Telecommunication-based AI services, such as SK Telecom's "A." assistant, have structural access to sensitive data, including call logs and voice content. This study examines how such data is utilized for AI training, highlighting challenges related to user control, third-party rights, and algorithmic transparency.

Through a case analysis of A., and a comparison with the Stack Overflow incident, this study highlights how even publicly available datasets can cause harm when proper consent,

* Director, Seoul Elderly Care Workers Support Center, first author.
** Professor. Department of Computer Science and Information Engineering, The Catholic University of Korea, Corresponding author.

attribution, and legal compliance are absent. Existing legal frameworks, such as Korea's Personal Information Protection Act (PIPA), are found to be inadequate in addressing AI-specific risks, particularly concerning high-risk data types.

As a normative response, this paper explores the applicability of governance principles derived from the GNU General Public License (GPL), including openness, shared responsibility, and continuity of rights. The findings indicate a need for hybrid governance models that integrate legal, technical, and ethical mechanisms to ensure transparency, accountability, and data sovereignty in the era of artificial intelligence(AI).

Key words : AI training data, Personal information rights, Data governance, Consent and transparency, GPL license