

생성형 AI 사용자의 디지털 리터러시, 프라이버시 염려 및 개인정보 보호 행동 간의 구조적 관계 연구

최재은*

대한민국예술원 사무국 주무관

Structural Relationships Among Digital Literacy, Privacy Concerns, and Privacy Protection Behavior in the Use of GAI

Jaeun Choi*

Officer, Secretariat of the National Academy of Arts of the Republic of Korea, Seoul 06579, Korea

[요약]

본 연구는 디지털 리터러시를 디지털 생활 활용 리터러시와 온라인 개인정보 리터러시로 구분하고, 이들이 프라이버시 염려 및 개인정보 보호 행동과 어떠한 구조적 관계를 갖는지 조사하였다. 2023년 정보통신정책연구원의 지능정보사회 이용자 패널 중 생성형 AI 사용 경험이 있는 543명을 대상으로 구조방정식 모형을 적용하여 분석하였다. 분석결과, 디지털 생활 활용 리터러시는 프라이버시 염려 및 개인정보 보호 행동에 각각 유의한 정(+)의 영향을, 온라인 개인정보 리터러시는 개인정보 보호 행동에 유의한 부(-)의 영향을 주는 것으로 나타났다. 한편, 프라이버시 염려와 개인정보 보호 행동 간에는 유의미한 상관관계가 나타나지 않아, 프라이버시 역설 가설은 기각되었다. 본 연구 결과는 생성형 AI 서비스의 투명성 제고와 더불어, 개인정보 보호 행동을 촉진하기 위해 실질적인 디지털 리터러시 교육과 제도적·기술적 설계가 병행되어야 함을 시사한다.

[Abstract]

This study conceptualizes digital literacy in two dimensions—functional literacy for everyday digital tasks and online privacy literacy—and examines their structural relationships with privacy concerns and privacy protection behaviors. Structural equation modeling was conducted using the data of 543 generative AI users, obtained from the 2023 KISDI Intelligent Information Society Panel. The results reveal that functional literacy has significant positive effects on privacy concerns and privacy protection behaviors. However, privacy literacy is negatively associated with privacy protection behaviors. Moreover, privacy concerns are not significantly correlated with privacy protection behaviors, thereby contradicting the privacy paradox hypothesis. The findings of this study suggest that enhancing the transparency of generative AI services should be accompanied by practical digital literacy education and by institutional and technical measures to effectively promote privacy protection behaviors among users.

색인어 : 생성형 AI, 프라이버시 염려, 개인정보 보호 행동, 디지털 리터러시, 온라인 개인정보 리터러시

Keyword : Generative AI, Privacy Concerns, Privacy Protection Behavior, Digital Literacy, Online Privacy Literacy

<http://dx.doi.org/10.9728/dcs.2025.26.11.3115>



This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 28 August 2025; **Revised** 18 September 2025

Accepted 22 September 2025

***Corresponding Author, Jaeun Choi**

Tel: +82-2-3479-7233

E-mail: kibic99@naver.com

I. 서론

2025년 2월 생성형 Artificial Intelligence(AI) 답시크가 무단으로 사용자 정보를 제3자 기업에 넘긴 것이 확인되면서 국내 다운로드가 중단되는 사태가 발생했다. 답시크는 키보드 입력 패턴을 수집하여 특정인을 식별할 위험이 있으며, 데이터가 중국 내 서버에 저장되어 중국 정부가 얼마든지 열람할 수 있다는 점에서 논란이 되었다[1]. 하지만 서비스 잠정 중단 조치에도 답시크는 높은 성능의 생성형 AI 모델을 무료로 사용할 수 있다는 이점 때문에 AI 어플 사용자 수에서 상위권을 기록하였다[2]. 한편, 최근 개인정보보호위원회의 조사에 따르면 성인의 76%는 AI가 유발하는 개인정보 위험에 대해 심각하다고 인지하는 것으로 나타났다[3]. 자신의 프라이버시가 침해될까 염려하면서도 서비스로 인한 이익 때문에 사용을 계속하는 이른바 프라이버시 역설 현상이 생성형 AI 사용에 있어서도 일어나고 있는지 질문을 던질 수 있다.

한편, 인터넷 사용자들의 자기 보호 조치는 프라이버시 보호에 있어 점점 중요해지고 있다. 기업은 개인정보의 공개, 수집 및 거래를 통해 이익을 얻는 반면, 그들 스스로의 규제나 산업의 집단적 자율 규제는 인센티브가 부족하기 때문이다. 따라서 사용자 측면에서의 적극적인 행동이 더욱 중요해지고 있다[4]. 생성형 AI 사용에 있어서도 사용자 스스로의 프라이버시 보호는 중요하다. 관계기관은 논란이 된 답시크 뿐 아니라 Chat GPT, Gemini 등 다른 생성형 AI도 개인정보를 수집하고 있기 때문에 주민번호, 전화번호, 주소 및 금융정보 등 중요한 개인정보는 입력하지 말 것을 권고하고 있다[5].

생성형 AI와 관련해서는 AI와 관련한 프라이버시 염려가 구체적으로 어떤 것인지 실증적으로 규명[6]하거나, 프라이버시 염려 측정을 위한 PC-AIM(Privacy Concerns Related to AI Misuse) 척도를 개발·검증[7]하거나, 프라이버시 역설 현상이 AI 사용에서도 나타나는지 확인[6],[8],[9]하는 연구 등이 수행되었다. 선행연구에서 프라이버시 염려(Privacy Concerns)는 서비스에 대한 신뢰, 사용자의 정보 공개 의도, 개인정보 보호 행동 등과 유의미한 관계를 가지는 것으로 나타나기에[10], AI 사용자 연구에서도 주요하게 논의되고 있다.

한편 생성형 AI는 디지털 리터러시 역량이 높을수록 그 사용 또한 증가하는 것으로 알려져 새로운 디지털 격차의 가능성이 제기되고 있다[11]. 이와 같은 상황에서 디지털 리터러시 역량이 사용자의 프라이버시 염려와 개인정보 보호 행동과 어떤 구조적인 관계를 갖고 있는지, 디지털 리터러시 격차가 프라이버시 격차로 이어지고 있지는 않은지 확인할 필요가 있다.

본 연구에서는 디지털 리터러시를 선행연구를 통해 생활에 필요한 과업을 수행할 줄 아는 능력인 ‘디지털 생활 활용 리터러시’와 자신의 개인정보를 보호할 줄 아는 능력인 ‘온라인 개인정보 리터러시’로 나누고, 이들 리터러시가 생성형 AI 사용에서의 ‘프라이버시 염려’, ‘개인정보 보호 행동’과 어떤 관

계를 맺고 있는지 분석한다. 분석을 통해 국내 생성형 AI 사용자에게 프라이버시 역설 현상이 나타나는지 확인한다. 또 생성형 AI 사용이 확대되고 있는 현 시점에서 디지털 리터러시 격차가 프라이버시 격차로 이어지는지를 확인하고자 한다. 연구 결과는 생성형 AI 사용자 교육 프로그램 설계 및 관계기관의 가이드라인 수립 등에 기초자료로 활용될 수 있다.

II. 이론적 배경

2-1 생성형 AI와 개인정보 이슈

생성형 AI는 의료, 금융, 자동차 산업 등의 여러 분야에서 혁신적인 패러다임으로 부각되고 있으나 많은 윤리적 문제 또한 내재하고 있다[12]. 그중 하나가 ‘개인정보 문제’로 AI 모델이 학습 데이터를 통해 개인의 동의 없이 수집된 개인정보를 학습하거나, 개인의 행동을 무단 감시할 위험이 있다. 또 특정 개인을 유추할 위험, 정부 또는 기업이 AI를 활용하여 사용자의 행동을 추적하거나 분석할 가능성이 있다 [12],[13].

2-2 디지털 리터러시의 개념과 구성 요소

디지털 리터러시 역량과 생성형 AI 사용 경험 간에는 유의미한 관계가 있는 것으로 나타난다[11]. 따라서 본 연구는 디지털 리터러시 역량이 생성형 AI 사용 시 발생하는 개인정보 관련 요인에도 영향을 미치는지 살펴보고자 한다.

디지털 리터러시는 미디어 리터러시, 디지털 역량 등 기존의 다양한 리터러시를 포괄하는 개념으로 디지털 사회에서 시민이자 생활을 영위하는 구성원으로서 역할을 수행할 수 있게 하는 능력을 말한다[14]. 황용석 외는 문헌검토, 전문가 의견 수렴, 탐색적 요인분석, 확인적 요인분석 과정을 거쳐 디지털 리터러시 역량을 ‘기본기술 역량’, ‘생활 활용 역량’, ‘비판적 이해 역량’, ‘생산과 공유 역량’, ‘사회참여 역량’, ‘권리보호 역량’, ‘보안 역량’ 등 7개 하위영역으로 분류하였다[14].

1) 디지털 생활 활용 리터러시

본 연구에서는 타인의 도움을 받지 않고 문자/인스턴트 메시징, 인터넷, 이메일 등을 활용할 수 있는 스마트 기기 활용 능력이 높을수록 생성형 AI를 사용할 확률이 높아진다는 이해수와 이모란의 연구[11]를 참고하여 ‘디지털 생활 활용 리터러시’를 분석 변수로 채택하였다. 디지털 생활 활용 리터러시는 디지털 기술을 경제나 공공적인 목적으로 편의를 도모하기 위해 사용할 수 있는 역량을 의미한다[14].

2) 온라인 개인정보 리터러시

개인정보 보호와 관련된 디지털 리터러시의 논의는 주로 온라인 개인정보 리터러시(Online Privacy Literacy)와 관련하여 진행되었다[15]-[17].

Sabine Trepte 등은 인터넷 사용자들이 개인정보를 침해를

우려하면서도 실제로는 방법을 알지 못하여 자신의 개인정보를 보호하지 못한다고 주장하며 온라인 개인정보 리터러시의 중요성을 강조하였다[17]. 이들은 문헌연구를 통해 온라인 프라이버시 리터러시 척도를 개발하였는데, 여기에는 (1)기관 및 온라인 서비스 제공자의 데이터 처리 방식에 대한 지식, (2)온라인 프라이버시 및 데이터 보호의 기술적 측면에 대한 이해, (3)온라인 프라이버시 위협 및 위험에 대한 지식, (4)데이터 보호법의 법적 측면에 대한 이해, (5)개별 사용자의 온라인 프라이버시 보호 전략, (6)프라이버시 위협이 발생하였을 때 대응하는 방법에 대한 지식 6가지가 포함된다.

2-3 AI와 프라이버시 염려

AI의 효과성은 궁극적으로 사용되는 데이터의 질과 양에 결정되는데, AI 시스템이 점점 더 많은 개인정보를 처리하게 됨[12]에 따라 AI와 관련한 프라이버시 염려 관련 연구도 다수 진행되고 있다[6],[7],[18].

AI 사용자들은 데이터 유출 및 무단 접근, 불투명한 데이터 수집 및 활용, 데이터 오남용 가능성, 보안 취약점, 알고리즘의 편향성과 공정성 문제 등으로 AI에 대한 신뢰가 부족했으며, 이것이 프라이버시 염려로 이어지는 것으로 나타났다. 사용자들은 AI가 제공하는 개인화 서비스를 높게 평가하였음에도 프라이버시 염려 또한 크게 가지고 있는 것으로 나타나 인터넷 사용자들의 개인정보에 대한 태도와 행위 사이의 불일치 현상인 ‘프라이버시 역설’이 AI 사용에 있어서도 나타남을 확인할 수 있었다[6].

지능형 개인비서(IPA; Intelligent Personal Assistant) 사용자의 프라이버시 염려에 대한 연구[18]는 사용자가 장치의 해킹 가능성, 장치가 민감한 개인정보를 수집하고 있는 점, 사적인 대화를 녹음하는 것, 24시간 항상 듣고 있는 것, 필요 이상으로 많은 정보를 수집하는 것, 데이터 저장 방식의 불확실성 등에 대해 우려하고 있음을 밝혔다.

Philip Menard와 Gregory J. Bott는 기존 프라이버시 염려 측정 모델이 전자상거래, 온라인 검색 및 광고, 스마트폰과 SNS를 대상으로 수행되어 기존 온라인 서비스보다 더욱 광범위하게 사용자가 인식하지 못하는 방식으로 개인정보를 수집, 추론하는 AI에 적용하기에는 한계가 있음을 지적하며, AI 오용과 관련된 프라이버시 염려 측정 척도(PC-AIM)를 개발·검증하였다[7]. 이 모델에는 AI 기반 시스템이 특정 그룹에게 불리한 결정을 내릴 우려인 ‘알고리즘 편향’, 서로 다른 데이터 출처에서 수집된 데이터가 결합되어 개인을 재식별할 가능성인 ‘데이터 결합’, 데이터가 삭제되지 않고 영구적으로 저장될 가능성인 ‘데이터 영속성’, AI의 의사결정이 인간을 배제할 우려인 ‘판단력 감소’, 사용자가 제공한 정보가 동의 없이 다른 목적으로 활용될 가능성인 ‘무단 2차 활용’, 개인 데이터가 적절한 권한 없이 접근될 가능성인 ‘부적절한 접근’ 등 AI의 특성을 반영한 문항이 포함되었다.

2-4 개인정보 보호 활동의 개념과 유형

인터넷 환경에서 개인정보 침해가 초래할 수 있는 심각한 결과에 대비하여 많은 사용자들은 자신의 개인정보를 보호하기 위한 특정한 행동을 취한다. Son Jai-Yeol과 Kim Sung S. 는 기업의 정보 활용 방식이 자신의 개인정보 보호에 위협을 준다고 인식할 때 인터넷 사용자가 보이는 행동 반응의 집합으로 ‘정보 프라이버시 보호 반응(IPPR; Information Privacy-Protective Responses)’을 정의하였다. IPPR은 크게 정보제공, 개인적 행동, 공적 행동 세 가지로 나뉜다. 정보제공은 개인정보 제공 여부를 측정하는 항목으로 제공 자체를 거부하는 ‘거부’, 가짜 정보를 제공하는 ‘허위정보 제공’이 포함된다. 개인적 행동으로는 자신의 계정이나 개인정보를 삭제하는 ‘삭제’, 기업의 프라이버시 정책에 대한 불만을 다른 사람에게 공유하는 ‘부정적 구전’이 있고, 공적 행동으로는 온라인 기업에 직접 불만을 제기하는 것과 제3자 기관에 불만을 제기하는 것이 포함된다[19]. 이와 비슷한 연구로 Eva Orszaghova와 Grant Blank도 개인정보 보호 행동을 크게 두 가지 행동, ‘보안 조치’와 ‘예방 조치’로 나누었다. ‘보안 조치’에는 보안 업데이트 설치, 정기적인 비밀번호 변경, 강력한 비밀번호 생성과 같이 기술적 보안 강화를 위한 행동이 포함된다. ‘예방 조치’에는 쇼핑 습관 기록 방지, 광고 차단과 같이 개인정보 노출을 줄이기 위한 사전 예방적 행동이 포함되었는데, 이는 불필요한 정보 공유를 최소화하는 행동과 밀접한 관련이 있다[20].

III. 연구모형 및 가설설정

3-1 연구모형 제시

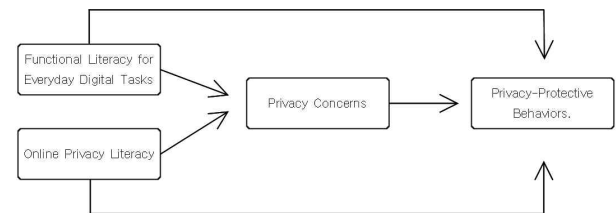


그림 1. 연구모형
Fig. 1. Research model

3-2 연구가설 설정

1) 디지털 생활 활용 리터러시와 프라이버시 염려의 관계

일상에서 디지털 기기를 활용할 줄 아는 디지털 생활 활용 리터러시와 프라이버시 염려의 관계에 관한 연구는 다양한 맥락에서 여러 차례 수행되었다. 다수의 연구 결과는 생활에 필요한 디지털 생활 활용 리터러시가 높을수록 프라이버시 염려 또한 높아짐을 규명하였다[21]-[24].

최재서 등은 개인용 컴퓨터와 스마트기기 사용 역량이 프

라이버시 염려와 전자상거래 사용 경험에 미치는 영향을 코로나19 전후로 비교하였다. 2019년에는 스마트 기기 리터러시만이 프라이버시 염려에 양의 영향을 주었으나 2021년에는 개인용 컴퓨터와 스마트 기기 리터러시 모두 프라이버시 염려에 양의 영향을 주는 것으로 나타나, 코로나19 이후 프라이버시 침해 인식이 확산된 것을 확인하였다[24].

김시정과 최상옥은 디지털 리터러시를 사용역량(도구적, 내용적)과 활용역량(사회적, 생산적)으로 나누고 이들이 개인 정보 위험인식에 유의미한 영향을 주는지 확인하였다. 연구결과, 디지털 생활 활용 리터러시인 도구적 사용역량이 개인정보 위험 인식에 유의미한 정적 영향을 미치는 것으로 나타났다[21].

류성진과 고흥석은 개인용 컴퓨터와 스마트기기 사용역량이 정보 프라이버시 염려에 미치는 영향을 디지털 원주민과 이주민 집단으로 나누어 살펴보았다. 2017~2020년의 데이터를 분석한 결과, 디지털 원주민은 각각의 리터러시가 정보 프라이버시 염려에 미치는 영향이 연도별로 동일하지 않았으나 디지털 이주민 집단은 일관되게 개인용 컴퓨터 리터러시가 프라이버시 염려에 양적 영향을, 스마트 기기 리터러시는 프라이버시 염려에 부적 영향을 주는 것으로 나타났다[23].

김현정과 김범수에 의하면 스마트기기 활용 역량이 프라이버시 염려에 유의미한 양의 영향을 주는 것으로 나타났다[22].

따라서 본 연구에서는 생성형 AI 사용에 있어서도 디지털 생활 활용 리터러시 역량이 프라이버시 염려에 정적 영향을 줄 것이라고 연구 가설을 수립하였다.

<연구가설1-1> 디지털 생활 활용 리터러시가 높을수록 생성형 AI의 프라이버시 염려가 높을 것이다.

2) 온라인 개인정보 리터러시와 프라이버시 염려의 관계

Christine Prince, Nessrine Omrani, Francesco Schiavone는 유럽 인터넷 사용자 15,000명 이상을 대상으로 온라인 개인정보 리터러시가 프라이버시 염려에 미치는 영향을 조사하였다. 온라인 개인정보 리터러시를 실제로 프라이버시 보호 행동을 수행할 수 있는 능력인 ‘절차적 지식’과 개인정보 보호와 관련된 법률과 권리를 알고 있는 ‘선언적 지식’으로 나누어 측정하였고, 이 둘의 상호작용 효과 역시 측정하였다. 회귀분석 결과, 세 리터러시 모두 프라이버시 염려에 유의미한 정적 영향을 주는 것으로 확인되었다[25].

따라서 본 연구에서도 생성형 AI 사용에 있어 온라인 개인정보 리터러시가 프라이버시 염려에 정적 영향을 줄 것이라고 연구 가설을 수립하였다.

<연구가설1-2> 온라인 개인정보 리터러시가 높을수록 생성형 AI의 프라이버시 염려가 높을 것이다.

3) 프라이버시 염려와 개인정보 보호 행동의 관계

인터넷 또는 AI 서비스 사용자들이 갖는 프라이버시 염려와 실제 그들의 개인정보 보호 행동에 관한 연구 다수는 프

라이버시 역설 현상을 확인하였다[8],[9],[26]. 프라이버시 역설(Privacy Paradox)이란, 프라이버시에 대한 태도와 행위 사이에 나타나는 괴리, 불일치가 존재하는 현상을 의미한다. 프라이버시 역설이 발생하면 프라이버시 염려로 인해 개인정보 보호 행위가 뒤따르는 것이 아니라 그 반대의 현상이 일어난다. 이와 같은 모순은 사용자가 자신의 개인정보를 제공함으로써 얻을 수 있는 편의성, 혜택, 정보 습득 등으로 인해 발생한다[27].

Jurgen Willems 등은 AI 기반 공공서비스 사용에 있어서 시민들이 개인정보 보호 염려에 따라 행동하는지 조사하였다. 오스트리아 시민 1,048명을 대상으로 한 비네트 실험 결과, 프라이버시 역설을 확인할 수 있었다. 즉, 시민들이 프라이버시 염려를 갖고 있더라도 실제 어플리케이션 다운로드 여부는 자신들이 제공해야 하는 개인정보의 양과 무관하게 결정되었다[9].

황용석 등은 AI 스피커와 관련된 포커스 집단 인터뷰를 실시하여 텍스트 데이터를 의미연결망으로 분석하였다. 연구결과, 프라이버시와 연관된 토픽의 중심성 분석에서 개인정보 수집의 불가피성과 개인정보 유출 염려가 유사성이 높은 중심부 군집의 공통 토픽으로 추출되어, 프라이버시 역설 현상을 확인할 수 있었다. 사용자들은 AI 발전에 따른 개인정보 오남용 및 유출을 염려하고 있지만 보다 다양한 혜택을 얻을 수 있다면 개인정보를 제공할 의향이 있었다[8].

이은성 등은 프라이버시 염려와 SNS 계정 공개 행동 간 관계를 연구하였는데, 프라이버시 염려가 높을수록 사람들은 자신의 SNS 계정을 불특정 다수에게 공개하는 정도가 더 큰 것으로 나타나 프라이버시 역설 현상을 확인할 수 있었다[26].

따라서 본 연구 역시 생성형 AI 사용자들이 프라이버시 염려를 갖고 있을수록 개인정보 보호 행동을 적게 할 것이라고 연구 가설을 수립하였다.

<연구가설2> 생성형 AI 사용자들은 프라이버시 염려가 높을수록 개인정보 보호 행동을 적게 할 것이다.

4) 디지털 리터러시와 개인정보 보호 행동의 관계

• 생활 활용 리터러시와 개인정보 보호 행동의 관계

디지털 생활역량과 개인정보 보호 행동 간의 관계는 디지털 생활 활용 역량이 높을수록 개인정보 보호 행동이 증가한다는 연구[4],[28]와 이 두 변수 간 관계가 없다는 연구[29]로 상반되게 나타났다.

Moritz Büchi, Natascha Just, Michael Latzer는 스위스 인터넷 사용자를 대상으로 파일 다운로드, 웹사이트 검색 등 일반적인 인터넷 기술이 개인정보 보호 행동에 영향을 주는 지 조사하였다. 구조방정식 분석 결과, 다른 여러 요인보다도 인터넷 기술이 개인정보 보호 행동을 설명하는 핵심 요소임을 발견하였다[4].

Matias Dodel과 Gustavo Mesch는 이스라엘 1,850명의

인터넷 사용자를 대상으로 사이버 안전 행동의 결정 요인이 무엇인지 조사하였다. 연구결과, 온라인 금융 활동을 자주 할수록 안티 바이러스 행동에 더 많이 참여할 가능성이 있는 것으로 나타났다. 이는 온라인 거래를 자주 하는 사용자일수록 금융 자산의 안전에 더 많은 관심을 가지게 되며, 이에 따라 안전한 사용 습관과 온라인 위협에 대해 학습하기 때문이라고 해석하였다[28]

최인호와 정세훈은 336명의 성인을 대상으로 디지털 리터러시가 개인정보 노출과 보호 행동에 미치는 영향을 조사하였다. 회귀분석 결과, 디지털 생활 활용 역량인 소비 리터러시는 개인정보 노출 및 보호 행동과 관련이 없는 것으로 나타났다[29].

선행연구 결과가 다소 상반되게 나타나지만, 본 연구에서는 생성형 AI 사용에 있어서 생활에 필요한 디지털 생활 활용 리터러시가 높을수록 개인정보 위협을 더 잘 인지하게 되고, 이에 따라 개인정보 보호 행동도 증가하게 된다고 연구가설을 설정하였다.

<연구가설3-1> 생성형 AI 사용자들은 디지털 생활 활용 리터러시가 높을수록 개인 정보 보호 행동을 많이 할 것이다.

• 온라인 개인정보 리터러시와 개인정보 보호 행동의 관계

개인정보 데이터의 처리 방식, 개인정보 보호 관련 법률, 그리고 실제 보호를 위한 기술적 지식을 포괄하는 온라인 개인정보 리터러시와 개인정보 보호 행동 간의 관계에 대해서는 상반된 연구 결과가 존재한다. 일부 연구는 두 변수 간의 정(+)적 관계를 제시하였다. 예컨대 Miriam Bartsch와 Tobias Dienlin은 인터넷 사용자의 온라인 개인정보 리터러시 수준이 높을수록 소셜미디어 상에서 개인정보 보호 행동을 더 많이 수행한다는 점을 확인하였다[15]. 반면, Chiara Respi 등이 이탈리아 인터넷 사용자를 대상으로 교육 수준, 온라인 개인정보 리터러시, 프라이버시 냉소주의, 개인정보 보호 행동 간의 구조적 관계를 분석한 결과, 프라이버시 리터러시가 높을수록 개인정보 보호 행동이 유의미하게 감소하는 것으로 나타났다[30].

이에 본 연구는 최신 연구 동향[30]에 근거하여, 온라인 개인정보 리터러시가 높을수록 개인정보 보호 행동은 감소할 것이라는 연구가설을 설정하였다.

<연구가설3-2> 생성형 AI 사용자들은 온라인 개인정보 리터러시가 높을수록 개인 정보 보호 행동을 적게 할 것이다.

5) 디지털 리터러시와 개인정보 보호 행동 간의 관계에서 프라이버시 우려의 매개효과

선행연구에서는 디지털 역량 또는 디지털 기술에 대한 효능감이 개인정보 보호 행동에 영향을 미칠 때 프라이버시 염려가 매개효과를 갖고 있음을 확인하였다[31],[32].

Wan Ying Lee, Chee-Seng Tan, Poh Chua Siah은 말

레이시아 235명의 대학생을 대상으로 기본적인 인터넷 기술을 적용할 수 있는 자신의 능력에 대한 판단인 ‘인터넷 자기 효능감’이 프라이버시 염려를 통해 개인정보의 기술적 보호에 미치는 영향을 미치는 것을 확인하였다. 즉, 프라이버시 염려가 인터넷 자기 효능감과 개인정보 보호 행동 사이를 매개하는 것으로 나타났다[32].

Walaa Bajnaid와 Shuaa Aljasir은 중동, 북아프리카 지역 디지털 미디어 사용자 1,040명을 대상으로 온라인 개인정보 리터러시가 개인정보 보호 행동에 주는 영향 관계에서 프라이버시 염려의 매개효과를 규명하였다[31].

이와 같은 선행연구를 바탕으로 본 연구에서는 디지털 생활 활용 리터러시와 온라인 개인정보 리터러시가 각각 프라이버시 염려를 매개하여 개인정보 보호 행동에 영향을 준다고 가설을 수립하였다.

<연구가설4-1> 디지털 생활 활용 리터러시와 개인정보 보호 행동 간의 관계에서 프라이버시 염려가 매개효과를 나타낼 것이다.

<연구가설4-2> 온라인 개인정보 리터러시와 개인정보 보호 행동 간의 관계에서 프라이버시 염려가 매개효과를 나타낼 것이다.

IV. 연구방법

4-1 연구대상

본 연구의 목적은 생성형 AI 사용자의 디지털 리터러시, 프라이버시 염려, 개인정보 보호행동 간 구조적 관계를 조사하는 것이다. 이를 위해 정보통신정책연구원(KISDI)이 매년 시행하는 국가승인통계인 「지능정보사회 이용자 패널조사 2023」의 비식별 원자료를 이용한 2차 분석을 수행하였다.

표 1. 인구통계학적 특성

Table 1. Demographic characteristics

	Category	Frequency	%
Gender	Male	263	48.43%
	Female	280	51.57%
Age group	Teens	34	6.26%
	20s	146	26.89%
	30s	169	31.12%
	40s	96	17.68%
	50s	67	12.34%
	60s	31	5.71%
	70s	0	0
Education	High school or below	133	24.49%
	College (less than 4 years)	103	22.84%
	University (4 years)	302	55.62%
	Graduate school	5	0.92%

동 조사는 지능정보서비스 확산에 따른 사용자 중심 정책 개발을 위한 실증적 근거를 마련하기 위해 실시되었으며, 스마트폰, 증강·가상현실, 웨어러블 디바이스 등 다양한 지능정보 기술 및 서비스의 이용 현황과 인식을 포괄한다. 원자료는 인공지능서비스 이용자정책 아카이브 (user-archive.kisdi.re.kr)에서 이용허락 승인을 받은 후 열람·다운로드할 수 있다. 연구자는 설문 설계와 1차 자료수집에 관여하지 않은 외부 연구자로서, 제공기관의 이용허락 조건을 준수한 뒤 제공된 원자료를 엑셀 형태로 다운로드하여 분석에 활용하였다.

원 데이터의 조사 모집단은 2023년 전국 17개 시도에 거주하는 만 15세 이상부터 만 69세 이하의 성인 중 스마트폰을 사용하면서 하루 1회 이상 인터넷을 사용하는 4,581명이다. 본 연구는 이중 생성형 AI를 사용한 경험이 있는 543명(12.3%)의 데이터만을 추출하였다.

이들 543명의 생성형 AI 이용 행태 파악을 위해 기초 분석을 실시하였다. 분석 결과, 이들이 가장 자주 사용하는 생성형 AI는 Chat GPT, Gemini와 같은 텍스트 생성 AI(81%)였고 이어 음성, 음악 생성 AI(10.5%), 도메인 이미지 생성 AI(4.8%), 이미지 생성 AI(3.6%) 등 순이었다.

본 연구 표본의 인구통계학적 특성은 표 1과 같다. 남성이 48%, 여성이 52%로 나타났으며, 연령별로는 20대가 27%, 30대가 31%로 2030 세대가 58%를 차지했다. 교육 수준으로는 4년제 대학 학력자가 56%로 가장 많았다.

4-2 변수측정 및 설문지 구성

본 연구는 「지능정보사회 이용자 패널조사 2023」의 Part D ‘생성형 AI에 대한 사용자 인식 및 경험’과 Part E ‘사회 환경요인’ 중 디지털 역량 측정 문항을 분석에 활용하였다.

주요 변수는 선행연구를 참조하여 구성하였으며, 전체 약 290개가 넘는 설문 문항 가운데 표 2에 제시한 21개 문항만을 선별하였다. 특히 ‘온라인 개인정보 리터러시’ 변수는 디지털 역량의 권리보호 및 보안 하위영역에서 관련 문항을 선별하여 통합 구성하였다. 모든 문항은 1점(‘전혀 그렇지 않다’)에서 5점(‘매우 그렇다’)의 리커트 척도로 응답되었고, 결측치는 존재하지 않았다.

4-3 분석 방법

본 연구에서는 구조방정식 모형 추정 시 Anderson, J. C. 와 Gerbing, D. W.의 2단계 접근법을 적용하였다. 1단계에서 요인구조에 대한 특정한 가설을 검증하기 위해 확인적 요인분석(CFA; Confirmatory Factor Analysis)을 실시하였다[33]. 최대우도 추정법으로 측정모형을 추정하고 모형 적합도를 χ^2 , CFI, RMSEA, SRMR를 통해 평가하였다. 또 지표변수가 이론적으로 정의된 내용을 얼마나 잘 대표하고 있는지 확인하는 구인 타당도를 검토하였다. 구인 타당도는 하나의 특성을 측정하는 값들 간의 높은 상관성이 있는지 확인하

표 2. 변수측정을 위한 설문문항

Table 2. Survey items for variable measurement

Latent Variable	Measurement Variable	Survey Question	Related Study
Functional Literacy	lifelit1	I can purchase goods online using simple payment services.	[14]
	lifelit2	I can find products at lower prices through price comparison on the Internet.	
	lifelit3	I can use e-government services for administrative tasks.	
	lifelit4	I can reserve or hail transportation using the Internet or apps.	
	lifelit5	I can subscribe to insurance products online.	
	lifelit6	I can use kiosks to order food, purchase movie tickets, transportation tickets, or pay at hospitals.	
Privacy Literacy	privlit1	I know how to report phishing and how to get remedies for damages.	[17]
	privlit2	I can set the visibility scope when posting on social media or forums.	
	privlit3	I can delete cookies and browsing history on PC, smartphone, or tablet.	
Privacy Concern	concern1	I am afraid that my personal information may be stored and used for learning.	[7]
	concern2	I am worried that my personal information may be provided to third parties without my consent.	
	concern3	I am concerned that my personal information may be used for marketing or advertising purposes.	
	concern4	I am worried that the personal information obtained may be misused for criminal activities.	
	concern5	I feel anxious that my privacy may be infringed.	
	concern6	I am concerned that I may be personally identified.	
Privacy Protection Behavior	act1	I try to avoid providing personally identifiable information (e.g., name, address).	[19]
	act2	I do not provide financial information.	
	act3	I avoid sharing sensitive information (e.g., medical history, sexual orientation).	
	act4	I avoid sharing passwords or security-related information.	
	act5	I avoid sharing personal photos or videos.	
	act6	I avoid sharing personally identifiable information (e.g., name, address) of others such as family or friends.	

는 수렴 타당도와 다른 특성을 측정하는 값들 간의 낮은 상관 이 있는지 확인하는 변별 타당도로 구성된다. 수렴 타당도는 요인부하량을 통해, 변별 타당도는 요인 간의 상관계수를 통 해 확인하였다.

2단계에서는 디지털 리터러시, 프라이버시 염려, 개인정보 보호 행동 간의 구조적 관계를 분석하는 구조모형 검증을 실 시하였다. 연구가설 경로가 유의한지 확인하였으며, 각 변수 들간의 영향관계를 검증하였다. 마지막으로 부스트래핑 신뢰 구간을 사용하여 간접효과를 검증하였다. 모든 분석은 Mplus Version 8.11를 사용하여 수행하였다.

V. 연구결과

5-1 신뢰도 분석

구조방정식 분석에 앞서 본 연구의 잠재변수로 사용된 각 각의 설문문항이 개념적으로 해당 변수를 잘 반영하고 있는 지 Cronbach's alpha 신뢰도 분석을 수행하였다. 분석결과 디지털 리터러시 중 디지털 생활 활용 리터러시가 0.86, 온라인 개인정보 리터러시 역량이 0.72, 프라이버시 염려가 0.82, 개인정보 보호 행동이 0.9로 나타났다. 추가로 CFA의 표준 화 부하량을 바탕으로 복합신뢰도(CR; Composite Reliability)를 계산한 결과, 디지털 생활 활용 리터러시 0.864, 온라인 개인정보 리터러시 0.726, 프라이버시 염려 0.82, 개인정보 보호행동 0.905로 모든 측정변수가 일관되게 잠재구성을 구성하는 것으로 나타나, 신뢰 수준이 좋다고 판 단하였다.

5-2 기술통계 분석

모든 측정변수의 표준편차와 평균, 왜도와 첨도를 표 3에 제시하였다. 대다수 문항의 왜도의 절대값은 1 이하 수준이 며, 모든 첨도의 절대값도 1 이하 수준으로 Rex B. Kline이 제시한 왜도 3, 첨도 10의 기준을 넘지 않아 다변량 정규성 가정에 문제가 없다고 판단하고 분석을 진행하였다[34].

5-3 측정모형 검증

측정모형의 적합도는 표 4와 같다. 설정한 측정모형의 χ^2 값은 675.673으로 5%의 유의수준에서 모형이 자료에 부합 한다는 영가설을 기각하였다. 하지만 χ^2 분포를 사용한 적합 도 검정에서 과도하게 영가설을 기각하는 경향이 있는 바 [35], 다른 근사적인 적합도 지수도 함께 살펴보면, CFI는 0.905로 Litze Hu와 Peter M. Bentler가 제시한 0.95에 다 소 못 미치는 것으로 나타난다[36]. 그러나 RMSEA는 0.07 로 괜찮은 적합도를 나타내며[35], SRMR은 0.073으로 Litze Hu와 Peter M. Bentler가 제시한 0.08 이하의 기준을 만족하는 것으로 나타나 전반적으로 실무 수준에서 수용할만 한 적합도라고 판단하였다[36].

표 3. 측정변수의 표준편차와 평균, 왜도와 첨도

Table 3. Mean, standard deviation, skewness, and kurtosis of measurement variables

Variable	ACT1	ACT2	ACT3	ACT4
SD	0.750	0.927	1.078	1.128
MEAN	3.488	3.460	3.280	3.326
Skew	-1.019	-0.397	-0.608	-0.695
Kurt	0.716	-0.030	-0.291	-0.327
Variable	ACT5	ACT6	CONCERN1	CONCERN2
SD	1.113	1.049	0.738	0.833
MEAN	3.320	3.368	3.694	3.656
Skew	-0.671	-0.768	-0.660	-0.356
Kurt	-0.270	-0.001	0.289	-0.016
Variable	CONCERN3	CONCERN4	CONCERN5	CONCERN6
SD	0.786	0.885	0.874	0.820
MEAN	3.637	3.604	3.586	3.622
Skew	-0.492	-0.348	-0.537	-0.586
Kurt	0.203	-0.243	0.182	0.258
Variable	LIFELIT1	LIFELIT2	LIFELIT3	LIFELIT4
SD	0.750	0.861	0.824	0.880
MEAN	4.029	3.969	3.862	3.943
Skew	-0.598	-0.615	-0.727	-0.503
Kurt	0.470	0.225	0.734	-0.392
Variable	LIFELIT5	LIFELIT6	PRIVLIT1	PRIVLIT2
SD	0.874	0.859	0.919	0.988
MEAN	3.773	3.923	3.357	3.494
Skew	-0.371	-0.426	-0.281	-0.779
Kurt	-0.278	-0.335	-0.396	0.344
Variable	PRIVLIT3	/		
SD	0.901			
MEAN	3.599			
Skew	-0.47			
Kurt	-0.199			

표 4. 측정모형의 적합도

Table 4. Goodness of fit of the measurement model

Degrees of Freedom	χ^2	χ^2/df	P
183	675.673	3.69	.000
CFI	RMSEA	SRMR	/
0.905	0.07	0.073	

표 5는 확인적 요인분석의 표준화 추정치이다. 수렴 타당 도 확인을 위해 AVE(Average Variance Extracted)를 계 산한 결과, 디지털 생활 활용 리터러시 0.515, 온라인 개인정 보 리터러시 0.482, 프라이버시 염려 0.433, 개인정보 보호 행동 0.617로, 몇몇 잠재변수는 0.5에 다소 못 미치는 것으로 나타났다. 그러나 요인부하량을 검토한 결과, 대부분이 0.6 이상이며 상당수가 0.7 이상으로 나타난다. Rex B. Kline은 수렴 타당성 충족의 기준으로 각 표준화된 추정치 0.7[34] 을, Joseph F. Hair et al은 0.5 이상을 제시한 바 있다[37].

따라서 본 연구의 측정모형은 어느정도 타당성을 확보하였다고 보았다. 다음으로 변별타당도를 확인하기 위해 HTMT(Heterotrait-Monotrait ratio)를 계산하였다. HTMT 행렬에서 모든 쌍이 0.1~0.5 수준으로 나타나 기준치로 여겨지는 0.8 이하를 충족하였다. 추가로 4개 잠재변수 간의 상관계수가 -0.155 ~ 0.541 수준으로 나타나 Rex B. Kline이 변별 타당도 기준으로 제안한 0.9보다 훨씬 작게 나타났다[34]. 수렴 타당도와 변별 타당도가 모두 충족되었으므로 구조모형 분석을 진행하였다.

표 5. 확인적 요인분석의 표준화 추정치 결과

Table 5. Standardized factor loadings from CFA

Latent Variable	Measurement Variable	Estimate	S.E	Est./S.E.	P-Value
Privacy Protection Behavior	ACT1	0.640	0.027	23.293	0.000
	ACT2	0.707	0.024	29.876	0.000
	ACT3	0.803	0.018	45.369	0.000
	ACT4	0.858	0.014	60.612	0.000
	ACT5	0.862	0.014	62.415	0.000
	ACT6	0.817	0.017	48.753	0.000
Privacy Concern	CONCERN1	0.696	0.028	24.969	0.000
	CONCERN2	0.649	0.031	21.250	0.000
	CONCERN3	0.559	0.035	16.096	0.000
	CONCERN4	0.656	0.030	21.979	0.000
	CONCERN5	0.708	0.027	25.982	0.000
	CONCERN6	0.669	0.029	22.878	0.000
Functional Literacy	LIFELIT1	0.802	0.020	40.754	0.000
	LIFELIT2	0.683	0.026	25.891	0.000
	LIFELIT3	0.629	0.029	21.485	0.000
	LIFELIT4	0.718	0.024	29.391	0.000
	LIFELIT5	0.693	0.026	26.691	0.000
	LIFELIT6	0.768	0.021	35.749	0.000
Privacy Literacy	PRIVLIT1	0.462	0.040	11.649	0.000
	PRIVLIT2	0.740	0.033	22.508	0.000
	PRIVLIT3	0.828	0.032	26.242	0.000

5-4 구조모형 검증

본 연구의 가설 검증 결과는 표 6과 같다. 먼저 디지털 생활 활용 리터러시가 높을수록 프라이버시 염려가 증가할 것이라는 <연구가설1-1>을 검정한 결과 $\beta=0.436(p<0.001)$ 로 나타나 가설이 채택되었다.

다음으로 온라인 개인정보 리터러시가 높을수록 프라이버시 염려 역시 높아질 것이라는 <연구가설1-2>를 검정한 결과 $\beta= -0.170(p=0.059)$ 로 나타났다. 즉 온라인 개인정보 리터러시가 높을수록 오히려 프라이버시 염려는 다소 낮아진다는 유의수준에 근접한 결과가 나왔다. 이로써 <연구가설 1-2>를 기각하였다.

표 6. 직접경로 분석

Table 6. Direct path analysis

Hypothesis	Path	Unstandardized Coefficient	Standard Error	Standardized Coefficient
1-1	Functional Literacy → Privacy Concern	0.436***	0.058	0.511
1-2	Privacy Literacy → Privacy Concern	-0.171	0.091	-0.142
2	Privacy Concern → Privacy Protective behavior	0.103	0.071	0.110
3-1	Functional Literacy → Privacy Protective behavior	0.126*	0.057	0.158
3-2	Privacy Literacy → Privacy Protective behavior	-0.288***	0.079	-0.255

다음으로 프라이버시 염려가 높을수록 프라이버시 보호 행동을 적게 할 것이라는 연구가설 2는 $\beta= 0.103(p=0.147)$ 로 나타나 기각되었다. 프라이버시 염려와 개인정보 보호 행동 간에는 유의하지 않은 양의 관계가 나타났다. 디지털 생활 활용 리터러시가 높을수록 개인정보 보호행동을 많이 할 것이라는 연구가설 3-1은 $\beta= 0.126(p<0.05)$ 로 나타나 채택되었다. 온라인 개인정보 리터러시가 높을수록 개인정보 보호 행동을 적게 할 것이라는 연구가설 3-2도 $\beta= -0.288(p<0.001)$ 로 나타나 채택되었다.

5-5 매개효과 검증

마지막으로 5,000회의 부트스트랩으로 산출한 95% 신뢰구간을 사용해 생활 활용 리터러시와 프라이버시 리터러시가 프라이버시 염려를 매개하여 개인정보 보호 행동에 미치는 간접효과를 표 7과 같이 검증하였다.

가설 4-1인 생활활용 리터러시의 간접효과의 95% 신뢰구간 [-.011, 0.110]에 0이 포함되어 간접효과가 유의하지 않은 것으로 나타났다. 가설 4-2인 프라이버시 리터러시의 간접효과 역시 95% 신뢰구간 [-0.060, 0.001]에 0이 포함되어 간접효과가 유의하지 않게 나타났다. 이로써 디지털 생활 활용 리터러시는 개인정보 보호 행동에 정적인 영향을, 온라인 개인정보 리터러시는 프라이버시 보호 행동에 부적인 영향을 주는 직접효과만 유의한 것을 확인하였다.

표 7. 매개효과 검증
Table 7. Mediation effect test

Hypothesis	Path	Unstandardized Coefficient	Standard Error (SE)	95% Confidence Interval (CI)
4-1	Functional Literacy → Privacy Concern → Privacy Protective behavior	0.045	0.030	[-0.11, 0.110]
4-2	Privacy Literacy → Privacy Concern → Privacy Protective behavior	-0.018	0.014	[-0.060, 0.001]

VI. 결론 및 시사점

생성형 AI와 관련된 개인정보 이슈가 점차 심화되는 가운데, 관련 연구는 주로 프라이버시 염려 및 프라이버시 역설 현상 규명에 관해 수행되었고, 디지털 리터러시와 프라이버시 염려, 개인정보 보호 행동에 관한 연구는 아직 수행되지 않은 것으로 조사되었다. 본 연구는 디지털 리터러시를 디지털 생활 활용 리터러시와 온라인 개인정보 리터러시로 나누고 이들 역량이 프라이버시 염려, 개인정보 보호 행동과 어떤 관계를 맺고 있는지 구조방정식을 통해 조사하였다. 선행연구를 통해 디지털 생활 활용 리터러시와 온라인 개인정보 리터러시가 프라이버시 염려에 각각 정(+)의 영향을 주고, 프라이버시 염려가 개인정보 보호 행동에 부(-)의 영향을 주는 프라이버시 역설이 나타날 것이라는 가설을 설정하였다. 또 디지털 생활 활용 리터러시와 온라인 개인정보 리터러시가 개인정보 보호 행동에 각각 정(+)의 영향과 부(-)의 영향을 준다는 가설을 설정하였다. 추가로 각각의 디지털 리터러시가 개인정보 보호 행동에 영향을 줄 때, 프라이버시 염려가 이를 매개할 것이라고 가설을 세웠다.

정보통신정책연구원의 2023년 지능정보사회 사용자 패널 조사에서 생성형 AI의 사용 경험이 있는 543명의 응답을 구조방정식으로 분석한 결과, 디지털 생활 활용 리터러시가 높을수록 프라이버시 염려가 증가한다는 연구가설 1-1은 채택되었다. 이와 같은 결과는 디지털 생활 능력이 높을수록 프라이버시 위협에 대해 잘 인지하게 되고, 이것이 프라이버시 우려로 이어진다는 선행연구[21]-[24]와 일치한다.

그러나 온라인 개인정보 리터러시가 높을수록 프라이버시 염려가 높을 것이라는 <연구가설1-2>는 기각되었다. 오히려 온라인 개인정보 리터러시가 높을수록 프라이버시 염려가 낮아지는 유의수준에 근접한 결과가 나왔다. 이는 프라이버시 리터러시와 염려 간의 정(+)의 관계를 규명한 선행연구의 연구와 대조되는 결과다[25].

프라이버시 염려가 높을수록 개인정보 보호 행동을 적게 할 것이라는 연구가설 2는 기각되었다. 이는 선행연구에서 AI 기반 공공서비스[9]와 AI 스피커[8]를 대상으로 프라이버시 역설을 확인한 결과와 대조된다. 국내 생성형 AI 사용자의 경우 프라이버시 염려와 개인정보 보호 행동 간에 유의한 관계가 나타나지 않았다.

디지털 생활 활용 리터러시가 높을수록 개인정보 보호 행동이 증가할 것이라는 연구가설 3-1은 채택되었다. 이는 선행연구[4],[28]와 일치하는 결과로 기본적인 디지털 기술이 개인정보 보호 행동을 수행하는데 있어 중요한 것을 확인할 수 있다.

온라인 개인정보 리터러시가 높을수록 프라이버시 보호 행동이 감소할 것이라는 연구가설 3-2도 채택되었다. 이는 온라인 개인정보 리터러시와 프라이버시 보호 행동 간에 부(-)의 관계를 규명한 선행연구[30]와 일치하는 결과이다.

디지털 생활 활용 리터러시와 온라인 개인정보 리터러시가 각각 프라이버시 염려를 매개하여 개인정보 보호 행동에 영향을 줄 것이라는 연구가설 4-1과 4-2는 기각되었다. 이는 말레이시아 대학생을 대상으로 한 연구[32]와 중동, 북아프리카에서 수행된 연구[31]와 상반되는 연구 결과다. 본 연구 모형에서 각각의 리터러시는 개인정보 보호 행동에 있어 프라이버시 염려를 매개하지 않고 직접효과만 갖고 있는 것으로 나타났다.

이와 같은 연구결과를 바탕으로 다음과 같은 시사점을 도출할 수 있다. 첫 번째, 생활에 필요한 기본적인 리터러시 역량이 높을수록 프라이버시 염려 또한 높아지는 것으로 나타났다. 선행연구[11]에서는 디지털 생활 리터러시가 높을수록 생성형 AI를 사용 경험이 늘어남을 밝힌 바 있다. 디지털 생활 리터러시가 높은 사용자는 생성형 AI를 비교적 자주 사용하고, 사용 시 느낀 데이터 수집 방식의 불투명성, 옵트아웃 기능 미비 등으로 프라이버시 염려를 갖게 되는 것으로 해석된다. 생성형 AI 서비스는 사용자의 명확한 개인정보 동의를 확보하고, 데이터 활용방식에 대한 투명성을 제공[12]하여 사용자의 프라이버시 염려를 줄여야 한다.

둘째, 본 연구에서는 생성형 AI 사용 시 프라이버시 염려와 개인정보 보호 행동 간에 부(-)적 관계가 존재할 것이라는 프라이버시 역설 가설을 수립하였으나, 분석 결과 두 변수 간에는 유의미한 관계가 나타나지 않았다. 최근 선행연구들은 개인정보 보호 행동이 단순히 프라이버시 염려에 의해 직접적으로 설명되지 않고, 다양한 심리적·기술적 요인의 영향을 받음을 보고하고 있다. 예컨대 Reza Mousavil 등은 프라이버시 우려가 곧바로 보호 행동으로 이어지지 않으며, 개인정보 위협에 직면했을 때 자신의 정보를 지켜야 한다는 보호동기(Protection Motivation)를 매개하여야만 보호 행동으로 연결된다는 점을 밝혔다[38]. 또한 Hanbyul Choi, Jonghwa Park, Yoonhyuk Jung은 개인정보 보호 행동에 있어 프라이버시 우려보다 프라이버시 피로감—즉, 개인정보를 효과적으로 통제할 수 없다고 인식하는 개인이 경험하는 피로감—이

더 큰 영향을 미친다고 규명하였다[39]. Athina Ioannou 등은 프라이버시 관련 행동이 웹사이트의 정보 배치 방식, 글꼴 등과 같은 인터페이스 설계 요소에도 영향을 받는다는 사실을 제시하였다[40]. 이 외에도 Alessandro Acquisti 등은 광범위하게 정의된 프라이버시 태도와 좁게 정의된 행동 간에 밀접한 연관이 없을 수도 있음을 지적한 바 있다[41]

따라서 본 연구의 결과는 생성형 AI 사용자의 개인정보 보호 행동을 이해함에 있어 단순히 프라이버시 염려 수준만을 고려하는 것이 충분하지 않음을 시사한다. 후속 연구에서는 보호동기, 프라이버시 피로, 인터페이스 설계와 같은 심리적·기술적 요인을 포괄적으로 고려하는 한편, 보다 구체적인 태도와 그에 수반하는 행동 간의 관계를 규명할 필요가 있다.

세 번째로, 디지털 생활 활용 리터러시가 높을수록 개인정보 보호 행동이 증가하는 것으로 나타났다. 생성형 AI와 관련한 프라이버시 침해 염려가 확산되고 있는 만큼, 개별 사용자의 적극적인 개인정보 보호 행동은 더욱 중요해지고 있다. 다만, 이러한 보호 행동은 기존 디지털 기기와 서비스를 능숙하게 사용하는 사용자에게서 더욱 두드러지게 나타나는 경향이 있다. 이에 따라, 디지털 생활 활용 리터러시가 낮은 디지털 소외 계층을 대상으로 생성형 AI의 올바른 사용 방법과 함께 개인정보 보호 행동 수칙도 체계적으로 교육하는 것이 필요하다.

네 번째로, 온라인 개인정보 리터러시가 높을수록 개인정보 보호 행동이 감소하는 것으로 나타났다. 이는 높은 리터러시가 이용자에게 더 큰 자신감을 부여하여 오히려 보호 행동을 축소시키거나, 시스템에 대한 이해도가 높을수록 신뢰가 증대되어 보호 행동의 필요성을 덜 느끼게 되기 때문일 수 있다[30]. 이러한 결과는 단순히 이용자의 온라인 개인정보 리터러시를 제고하는 교육이나 정보 제공만으로는 실제 보호 행동을 강화하기 어렵다는 점을 시사한다. 따라서 실무적으로는 리터러시 향상과 함께 이용자가 지속적으로 보호 행동을 실천하도록 유도할 수 있는 제도적·기술적 설계가 병행되어야 할 것이다.

본 연구는 공공기관의 패널 데이터를 재사용한 연구로서 잠재변수를 구성하기 위한 측정 문항 선택에 있어 제약을 가지고 있다. 생성형 AI와 관련한 프라이버시 리터러시와 프라이버시 염려, 개인정보 보호 행동의 다양한 측면을 반영하는 문항으로 측정모형을 구성하였다면 보다 정교한 연구가 되었을 것으로 보인다. 현재 생성형 AI와 관련한 프라이버시 염려 척도나 AI 리터러시 척도 개발 연구도 활발하게 진행되고 있다. 향후 연구에서는 AI 리터러시와 AI 프라이버시 염려, 생성형 AI 사용 시 행해지는 개인정보 보호 행동 간의 구조적 관계에 관한 연구가 수행된다면 생성형 AI와 관련한 사용자의 개인정보 이슈를 보다 정밀하게 분석할 수 있을 것으로 기대된다.

참고문헌

- [1] ChosunMedia. DeepSeek Used by 1.2 Million in Korea Handed over Data to China [Internet]. Available: https://www.chosun.com/economy/tech_it/2025/02/18/WB KLG2TAUJGD3H2XP2ZBE434RI/.
- [2] NewsTomato. Despite Data Breach Controversy, Users still Choose DeepSeek [Internet]. Available: <https://www.newstomato.com/readnews.aspx?no=1258040>.
- [3] Personal Information Protection Commission, 2024 Survey on Personal Information Protection and Utilization, Personal Information Protection Commission, Sejong, No. 11-1790365-000002-10, 2024.
- [4] M. Büchi, N. Just, and M. Latzer, "Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection," *Information, Communication & Society*, Vol. 20, No. 8, pp. 1261-1278, September 2016. <https://doi.org/10.1080/1369118X.2016.1229001>
- [5] Korea Internet & Security Agency. Security Advisory for Generative AI Usage [Internet]. Available: <https://www.boho.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000133&searchWrd=&menuNo=205020&pageIndex=1&categoryCode=&nttId=71652>.
- [6] A. K. Shrestha, A. Barthwal, M. Campbell, A. Shouli, S. Syed, S. Joshi, and J. Vassileva, "Navigating AI to Unpack Youth Privacy Concerns: An In-Depth Exploration and Systematic Review," arXiv:2412.16369, 2024. <https://arxiv.org/abs/2412.16369>
- [7] P. Menard and G. J. Bott, "Artificial Intelligence Misuse and Concern for Information Privacy: New Construct Validation and Future Directions," *Information Systems Journal*, Vol. 35, No. 1, pp. 322-367, July 2024. <https://doi.org/10.1111/isj.12544>
- [8] Y. S. Hwang, K. T. Kim, H. J. Lee, and W. T. Lee, "A Cognitive Mapping of Artificial Intelligence Speaker Experience and Latent Privacy Concerns," *Journal of Cybercommunication Academic Society*, Vol. 37, No. 3, pp. 195-231, September 2020. <https://doi.org/10.36494/JCAS.2020.09.37.3.195>
- [9] J. Willems, M. J. Schmid, D. Vanderelst, D. Vogel, and F. Ebinger, "AI-driven Public Services and the Privacy Paradox: Do Citizens Really Care about Their Privacy?," *Public Management Review*, Vol. 25, No. 11, pp. 2116-2134, April 2022. <https://doi.org/10.1080/14719037.2022.2063934>
- [10] Y. Kim, S. H. Kim, R. A. Peterson, and J. Choi, "Privacy Concern and Its Consequences: A Meta-analysis," *Technological Forecasting and Social Change*, Vol. 196,

2023. <https://doi.org/10.1016/j.techfore.2023.122789>
- [11] H. S. Lee and M. R. Yi, "Who Uses Generative AI?: Focusing on Demographic Variables, Digital Literacy, Digital Transformation Recognition," *Information Systems Review*, Vol. 26, No. 3, pp. 377-394, August 2024. <https://doi.org/10.14329/isr.2024.26.3.377>
- [12] K. Patel. Ethical Reflections on Data-Centric AI: Balancing Benefits and Risks [Internet]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4993089.
- [13] A. Golda, K. Mekonen, A. Pandey, A. Singh, V. Hassija, V. Chamola, and B. Sikdar, "Privacy and Security Concerns in Generative AI: A Comprehensive Survey," *IEEE Access*, Vol. 12, pp. 48126-48144, 2024. <https://doi.org/10.1109/ACCESS.2024.3381611>
- [14] Y. S. Hwang, S. M. Lee, Y. L. Kim, and H. J. Hwang, "Digital Competence: Conceptualization, Scale Development," *Journal of Communication Research*, Vol. 59, No. 2, pp. 5-48, 2022. <https://doi.org/10.22174/jcr.2022.59.2.5>
- [15] M. Bartsch and T. Dienlin, "Control Your Facebook: An Analysis of Online Privacy Literacy," *Computers in Human Behavior*, Vol. 56, pp. 147-154, December 2015. <https://doi.org/10.1016/j.chb.2015.11.022>
- [16] C. Prince, N. Omrani, A. Maalaoui, M. Dabic, and S. Kraus, "Are We Living in Surveillance Societies and is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns," *IEEE Transactions on Engineering Management*, Vol. 70, No. 10, pp. 3553-3570, August 2021. <https://doi.org/10.1109/TEM.2021.3092702>
- [17] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind, Do People Know about Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"(OPLIS), in *Reforming European Data Protection Law*, New York, NY: Springer, pp. 333-365, January 2014. https://doi.org/10.1007/978-94-017-9385-8_14
- [18] L. Manikonda, A. Deotale, and S. Kambhampati, "What's Up with Privacy? User Preferences and Privacy Concerns in Intelligent Personal Assistants," in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, New Orleans: LA, pp. 229-235, December 2018. <https://doi.org/10.1145/3278721.3278773>
- [19] J.-Y. Son and S. S. Kim, "Internet Users' Information Privacy-protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly*, Vol. 32, No. 3, pp. 503-529, September 2008. <https://doi.org/10.2307/25148854>
- [20] E. Orszaghova and G. Blank, "Does the Type of Privacy-protective Behaviour Matter? An Analysis of Online Privacy Protective Action and Motivation," *Information, Communication & Society*, Vol. 27, No. 14, pp. 2530-2547, April 2024. <https://doi.org/10.1080/1369118X.2024.2334906>
- [21] S. J. Kim and S. O. Choi, "The Influence of Digital Literacy on Privacy Concern," *Korean Society and Public Administration*, Vol. 30, No. 2, pp. 257-284, August 2019. <https://doi.org/10.53865/KSPA.2019.08.30.2.257>
- [22] H. J. Kim and B. S. Kim, "How Does Smart-device Literacy Shape Privacy Concerns: The Moderation of Privacy and the Mediation of Online Social Participation and Information Veracity," *Knowledge Management Research*, Vol. 24, No. 1, pp. 51-72, 2023 <https://doi.org/10.15813/KMR.2023.24.1.003>
- [23] S. J. Ryu and H. S. Koh, "Relative Effects of Digital Literacy on Information Privacy Concerns : Focusing on Media Device and Comparison Between Digital Natives and Digital Immigrants," *Korean Journal of Broadcasting and Telecommunication Studies*, Vol. 35, No. 6, pp. 149-186, 2021. <https://doi.org/10.22876/kab.2021.35.6.005>
- [24] J. Choi, C. Choi, S. Yang, and J. Kim, "Effects of Digital Literacy Capability and Privacy Concern on E-commerce Usage Experience: A Comparison Before and After COVID-19," *Journal of Digital Contents Society*, Vol. 25, No. 6, pp. 1641-1654, June 2024. <https://doi.org/10.9728/dcs.2024.25.6.1641>
- [25] C. Prince, N. Omrani, and F. Schiavone, "Online Privacy Literacy and Users' Information Privacy Empowerment: the Case of GDPR in Europe," *Information Technology & People*, Vol. 37, No. 8, pp. 1-24, 2024. <https://doi.org/10.1108/ITP-05-2023-0467>
- [26] E. Lee, S. Lee, and H. J. Keum, "Analysis of the Effects of Privacy Concerns on Restricted Disclosure of SNS : Digital Literacy as a Moderator," *Journal of the Korean Association of Information Education*, Vol. 27, No. 5, pp. 521-530, 2023.
- [27] H. J. Shim and Y. H. Cho, "A Study on Personal Information Disclosure Levels Based on Digital Competence: Focusing on the Mediating Effects of Value-Based Privacy Sharing Acceptance," *Korean Journal of Broadcasting and Telecommunication Studies*, Vol. 38, No. 6, pp. 44-85, November 2024. <https://10.22876/kab.2024.38.6.002>
- [28] M. Dodel and G. Mesch "Inequality in Digital Skills and the Adoption of Online Safety Behaviors," *Information Communication & Society*, Vol. 21, No. 5, pp. 712-728,

- February 2018. <https://doi.org/10.1080/1369118X.2018.1428652>
- [29] I. Choi and S.-H. Jeong, "Effect of Age, Income, and Digital Literacy on Online Personal Information Exposure and Protection Behaviors," *Korean Journal of Journalism & Communication*, Vol. 63, No. 5, pp. 233-266, 2019. <https://doi.org/10.20879/kjics.2019.63.5.007>
- [30] C. Respi, M. Gui, G. Scaduto, M. Serini, D. Pizzul, T. Gerosa, and C. Lutz, "Lower Cynicism, Not Higher Literacy, Promotes Protective Behavior: Exploring the 'Privacy Exception' in the Digital Inequality Framework," *Social Science Computer Review*, May 2025. <https://doi.org/10.1177/0894439325134120>
- [31] W. Bajnaid and S. Aljasir, "Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region," *Journalism and Media*, Vol. 6, No. 1, 8, January 2025. <https://doi.org/10.3390/journalmedia6010008>
- [32] W. Y. Lee, C.-S. Tan, and P. C. Siah, "The Role of Online Privacy Concern as a Mediator between Internet Self-Efficacy and Online Technical Protection Privacy Behavior," *Sains Humanika*, Vol. 9, No. 3-2, 2017. <https://doi.org/10.11113/sh.v9n3-2.1271>
- [33] J. C. Anderson and D. W. Gerbing, "Structural Equation Modeling in Practice: A Review and Recommended Two - Step Approach," *Psychological Bulletin*, Vol. 103, No. 3, pp. 411-423, 1988. <https://doi.org/10.1037/0033-2909.103.3.411>
- [34] R. B. Kline, *Principles and Practice of Structural Equation Modeling*, 4th ed. New York, NY: The Guilford Press, 2011.
- [35] S. Y. Kim, *Basics and Extensions of Structural Equation Modeling*, Seoul: Hakjisa, 2016.
- [36] L. T. Hu and P. M. Bentler, "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6, No. 1, pp. 1-55, November 2009. <https://doi.org/10.1080/10705519909540118>
- [37] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 7th ed. New York, NY: Pearson Education, 2010.
- [38] R. Mousavi, R. Chen, D. J. Kim, and K. Chen, "Effectiveness of Privacy Assurance Mechanisms in Users' Privacy Protection on Social Networking Sites from the Perspective of Protection Motivation Theory," *Decision Support Systems*, Vol. 135, August 2020. <https://doi.org/10.1016/j.dss.2020.113323>
- [39] H. Choi, J. Park, and Y. Jung, "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior*, Vol. 81, pp. 42-51, April 2018. <https://doi.org/10.1016/j.chb.2017.12.001>
- [40] A. Ioannou, I. Tussyadiah, G. Miller, S. Li, and M. Weick, "Privacy Nudges for Disclosure of Personal Information: A Systematic Literature Review and Meta-Analysis," *PLoS One*, Vol. 16, No. 8, August 2021. <https://doi.org/10.1371/journal.pone.0256822>
- [41] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science*, Vol. 347, No. 6221, pp. 509-514, January 2015. <https://doi.org/10.1126/science.aaa1465>



최재은(Jaeun Choi)

2023년 : 이화여자대학교 대학원 (문헌정보학 석사)

2025년 : 이화여자대학교 대학원 (문헌정보학 박사 수료-정보학 전공)

2016년~2017년: 경기도교육청 포천도서관 주무관

2017년~2024년: 국립중앙도서관 주무관

2024년~현 재: 대한민국예술원 사무국 주무관

※ 관심분야 : 정보 이용자 연구(Information User Studies), 디지털 큐레이션(Digital Curation), 학술커뮤니케이션(Scholarly Communication)