

메타버스 환경에서의 개인정보 관리 모델 연구

이진규, 채봉수, 성민경, 양상운*

한국정보통신기술협회

[jkleee, duser, mksung, sangoon]@tta.or.kr

A Study on Personal Information Management Model in Metaverse Environment

Lee Jin Kyu, Chai Bong-Soo, Sung Min Kyung, Sangoon Yang*

Telecommunications Technology Association

요약

본 논문은 메타버스 환경에서 사용자 상호작용과 개인 데이터 생성 및 활용 방식이 기존 개인정보보호 모델로 효과적으로 관리하기 어려운 새로운 문제점을 만들어 냄에 따라, 이러한 변화에 적합한 개인정보 관리 모델 개발 필요성에서 출발하였다. 메타버스 환경은 사용자 데이터를 실시간으로 생성하고 활용하는 독특한 서비스를 제공하며, 이로 인해 기존 데이터 보호 법률과 규정으로 다루기 어려운 영역들이 발생하고 있다. 특히, 사용자의 익명성과 가상 정체성은 개인정보 자기결정권을 효과적으로 행사하는데 여러 어려움을 야기한다. 이에 따라 본 논문에서는 기존 메타버스에 적용 가능한 새로운 개인정보 관리 모델을 제안한다. 본 모델은 메타버스 기술의 발전과 사용자의 개인정보보호 필요성 사이의 균형을 찾고자 하는 시도로, 디지털 환경에서의 개인정보보호 방안을 재고해 보고자 한다.

I. 서론

개인정보보호는 디지털 시대의 중요한 이슈 중 하나로 유럽연합(EU)의 일반 데이터 보호 규정(GDPR: General Data Protection Regulation)은 2018년에 시행되어 개인정보 자기결정권을 강화하는 핵심 정책으로 자리 잡았다.[1] 이 규정은 개인이 자신의 정보를 어떻게 처리할지 스스로 결정할 수 있는 권리를 강조하며, 데이터 보호의 글로벌 기준을 제시하고 있다. 한편, 국내에서도 2023년 3월 개인정보보호법 전면 개정을 통해 개인의 자기 정보 권리 강화와 보호에 대한 본격적인 정책을 마련하였으며, 개인정보보호위원회를 통해 개인정보를 적절히 처리하는 방법에 대한 가이드라인을 제공하고 있다.[2] 이와 함께 과학기술정보통신부는 2023년 12월 메타버스 환경에서의 개인정보 처리 지침을 포함한 메타버스 실천 윤리를 발표하며, 가상 환경에서의 개인정보보호를 강조하고 있다.[3]

그러나 이러한 정책적 노력에도 불구하고, 메타버스 기술의 급속한 발전과 가상 환경의 확장으로 인해 새로운 유형의 개인정보보호 문제가 지속적으로 등장하고 있다. 메타버스 환경은 사용자 상호작용과 개인 데이터 생성 및 활용 방식을 근본적으로 변화시키고 있으며, 기존의 개인정보보호 모델로는 이러한 변화를 효과적으로 관리하기 어려운 상황이다. 특히, 메타버스에서 사용자 행동 데이터는 매우 다양하고 복잡하여, 전통적인 데이터 분류 및 관리 방식으로는 이를 적절히 처리하고 보호하는 데 한계가 있다.[4]

또한, 가상 환경에서의 익명성과 가상의 정체성 사용은 개인정보 자기결정권을 실질적으로 행사하기 어렵게 만든다.[5] 사용자는 자신이 누구인지를 숨기면서도 개인화된 경험을 원하므로, 이러한 요구를 충족시키는 동시에 개인정보를 보호할 수 있는 새로운 접근 방식이 필요하다. 이와 같은 문제를 해결하기 위해, 본 논문에서는 메타버스 환경에서 활동하는 개인이 자신의 개인정보를 메타버스 환경에 노출시키는 데 있어 개인정보 자기결정권을 적극적으로 활용할 수 있도록 지원하는 새로운 개인정보 관리 모델을 제안하고자 한다. 본 논문을 통해 메타버스 사용자들이 자신의

개인정보를 보다 효과적으로 관리하고 보호할 수 있는 방안을 제시함으로써, 개인정보의 자율적 관리와 보호를 위한 새로운 방향성을 살펴본다.

II. 본론

1. 자동화된 의사결정의 위험 관리

메타버스와 같은 가상 환경에서는 시각적, 공간적, 그리고 상호작용적 요소가 풍부하여 사용자는 실시간으로 대규모 데이터를 생성하며 이 데이터는 개인의 행동, 선호, 심지어 감정 상태까지 반영할 수 있다.[6] 하지만 기존 개인정보보호 모델은 이러한 새로운 데이터 형태와 상호작용의 복잡성을 충분히 관리하지 못하고 있다. 이와 같이 복잡성을 지닌 대규모 데이터 처리를 위해 자동화된 의사결정 시스템은 메타버스 환경의 필수 요소로 사용되고 있다.

하지만 의사결정 자동화가 확대됨에 따라 사생활 침해, 자유, 민주주의, 공정성에 대한 우려 또한 제기되고 있다.[7] EU의 GDPR 22조에서는 개인에게 자동화된 의사결정에 대한 투명성과 설명받을 권리를 보장하고 있으며, 국내 개인정보보호법(37조의 2)에서도 자동화된 의사결정의 근거 및 결과에 대한 설명의무를 명시하고 있다. 자동화된 의사결정으로 인해 발생하는 문제를 해결하기 위한 법적 노력이 상당한 진전을 이루고 있지만 이러한 법률이 개인의 권리와 민주적 가치를 효과적으로 보호하려면 지속적인 조정과 합의가 필요한 상황이다.

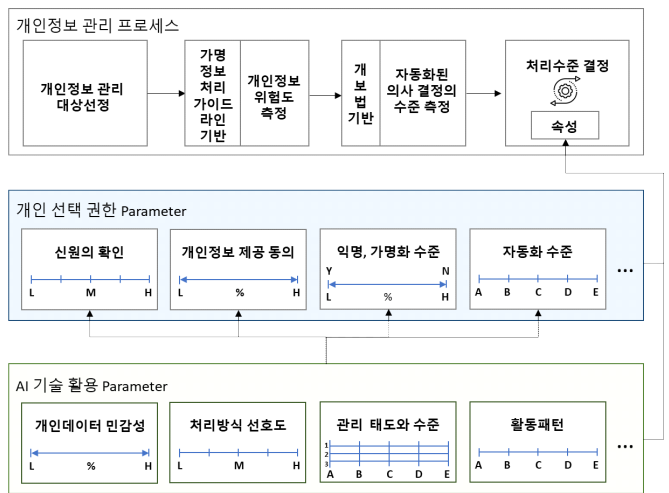
2. 가명정보 활용의 증가와 그 한계

특정 메타버스 환경에서는 사용자의 완전 익명화가 가능하다. 사용자는 자신의 진짜 신원을 숨길 수 있지만, 동시에 자신의 데이터 활용에 제약이 생겨 메타버스 서비스의 전체적인 품질에 영향을 미치기도 한다.[8] 메타버스의 주요 특징이 약점으로 작용하는 부분이다. 이러한 특성에 의해 개인 데이터 활용을 허용하면서 일정부분 익명성을 보장하기 위한 가명정보 활용이 AI와 메타버스 같은 새로운 기술 환경에서 중요한 역할을 하고 있다. 현재의 가명정보 제도·기술은 데이터의 유용성을 보존하면서 개인적

보를 보호하는 방법으로 주목받고 있으나, 재식별 가능성과 데이터 유출 위험은 여전히 큰 문제로 남아 있다.[9, 10] 또한 기술과 더불어 적절한 관리와 안전 조치 없이는 개인 사생활 보호와 데이터 안전성 보장이 어렵다.

3. 관리 모델 제안

이 모델은 메타버스의 독특한 요구사항을 충족시키면서 사용자가 자신의 개인정보를 효과적으로 통제할 수 있도록 설계되었다. 이 모델은 사용자 상호작용 편의성을 높이고 데이터 활용의 투명성을 제고하는 방향으로 구성하였다. 즉, 개인정보의 자율적 관리 및 보호와 동시에 익명성과 가상의 정체성 사용 복잡성을 보다 효과적으로 관리 할 수 있도록 설계하였다.



<그림1> 메타버스 환경에서의 개인정보 관리 모델

<그림1>과 같이 관리 모델은 개인정보 관리 프로세스가 최종적으로 개인 선택 권한 파라미터와 AI기술 활용 파라미터의 속성값을 전달받아 개인정보 처리 수준을 결정하도록 설계하였다.

3-1. 개인정보 관리 프로세스

개인정보 관리 프로세스는 <그림1>과 같이 4단계로 구성된다. 개인정보 관리 대상 선정 단계에서는 메타버스 환경 내에서 관리가 필요한 개인정보의 범위를 정의한다. 여기에는 사용자 활동 데이터, 개인 식별 정보, 거래 기록 등이 포함되며, 사용자 데이터 보호를 위한 주요 정보만을 포함하는 것을 목표로 한다. 가명정보 처리 가이드라인 기반 개인정보 위험도 측정 단계에서는 가명정보 처리 가이드라인을 바탕으로 개인정보의 위험도를 평가한다. 위험도 평가는 데이터 노출에 따른 잠재적 위험과 재식별 가능성을 고려해 수행된다. 이후 개인정보보호법 기반 자동화된 의사결정 수준 측정 단계를 통해 기존 개인정보 처리 시스템의 자동화된 의사결정 수준을 평가하고 위험도 측정이 완료된 개인정보와의 관계를 도출한다. 최종적으로, 적절한 개인정보 처리 수준에 대한 고려사항을 기존 시스템에 전달하는 역할을 하는 처리수준 결정 단계까지 프로세스가 동작한다.

3-2. 개인 선택 권한 파라미터

개인 선택 권한 파라미터는 개인정보 처리 수준 결정에 핵심이 되는 파라미터 값을 생성, 측정, 상호작용하는 역할을 한다. 사용자 입장에서 보면 스스로 자율성을 가지고 개인정보 처리 수준을 직접 컨트롤 할 수 있도록 기능이 제공되는 셈이다. 사용자는 자신의 신원 확인에 대한 요청을 거절, 수동, 자동 등의 수준으로 선택할 수 있게 된다. 이와 마찬가지로 자신의 개인정보를 어느 정도 제공할지 선택하는 개인정보 제공 동의의 수준, 익명·가명화시의 처리 수준, 전반적인 자동화의 수준 등의 파라미터를 제공할 수 있다. 파라미터는 다양한 수준에서 각 메타버스의 특성에 맞게 추가 개발 적용이 필요하다. 고정적으로 사용했을 유용한 효과를 나타내는 파라미터는 시스템에 의해 추천될 수 있다.

3-3. AI기술 활용 파라미터

AI 기술 활용 파라미터는 AI 학습과 분석 통해 파라미터를 제공한다. 예를 들면 메타버스 사용자들이 활동하면서 발생시킨 데이터를 학습하여 개인정보에 민감한 정도를 나타내는 개인정보 민감성이라는 파라미터를 생성할 수 있다. 이와 마찬가지로 개인정보 처리방식 선호도, 관리 태도와 수준, 활동패턴 등의 파라미터를 생성·제공할 수 있다. 이를 통해 AI학습 활용 시 생성된 파라미터는 개인 선택 권한 파라미터의 구성 데이터로 활용 가능하다는 것을 주요 포인트로 볼 수 있다. 결국, AI기술 활용 파라미터는 개인 선택 권한 파라미터의 값 조정 시 사용자들에게 올바른 범위와 가이드 제공, 접근할 수 있는 개인정보에 대한 새로운 인식을 제공한다.

III. 결론

본 연구에서는 메타버스 환경의 특성과 요구사항을 충족시키기 위해 새로운 개인정보 관리 모델을 제안하였다. 제안 모델은 메타버스의 독특한 상호작용과 데이터 생성 방식을 고려하여, 개인정보 관리 프로세스, 개인 선택 권한 파라미터, 그리고 AI 기술 활용 파라미터의 세 부분으로 구성되었다. 또한 세 부분은 상호 연결되어, 사용자가 자신의 개인정보를 보다 효과적으로 통제할 수 있도록 돕는 것에 초점을 맞춰 설계되었다. 기존의 개인정보보호 모델이 주로 정적인 데이터 보호에 초점을 맞춘 반면, 본 모델은 메타버스의 동적이고 상호작용적인 환경에 적합하도록 설계하였고, 이는 사용자의 데이터 관리와 개인정보보호 전략을 개선하는 데 중요한 역할을 한다. 본 연구를 통해 사용자들에게 보다 안전하고 투명한 디지털 경험을 제공할 것으로 기대된다. 향후 연구에서는 제안된 모델의 효과성을 평가하기 위한 실제 메타버스 환경에서의 적용 사례를 다뤄 모델의 세부 구성요소를 더욱 발전시키고 최적화할 수 있을 것이다. 또한, AI 기술 발전에 따라 새로운 기능을 통합하여, 개인정보 처리와 관련된 기술적, 윤리적 문제들에 대한 해결책을 추가로 제안하는 것도 향후 연구 과제이다.

ACKNOWLEDGMENT

논문 저자의 일부는 2021년 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받음(No.2021-0-00634, 대용량 정형 데이터 대상 개인정보 가명·익명처리 자동화 및 안정성 검증 기술개발)

참고 문헌

- [1] EU, "General Data Protection Regulation(GDPR)", 2018
- [2] 개인정보보호위원회, "가명정보 처리 가이드라인", 2022
- [3] 과학기술정보통신부, "메타버스 실천윤리", 2023
- [4] 이동혁, "안전한 메타버스 환경을 위한 속성레벨 프라이버시 보호 매커니즘", 2020
- [5] Alesia Zhuk, "Ethical implications of AI in the Metaverse", 2024
- [6] Simon Elias Bibri, "The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities-A Study in Science, Technology, and Society", 2022
- [7] 이상용, 이혜리, "개인정보보호법에 의한 자동화된 결정의 규율", 2024
- [8] Gaofeng Wang, Changhoon Shin, "Influencing Factors of Usage Intention of Metaverse Education Application Platform-Empirical Evidence Based on PPM and TAM Models", 2022
- [9] 성민경, 이강원, 한주연, 김동래, 김태훈, "가명처리 비정형데이터 유용성 측정을 위한 고려사항", 2023
- [10] 이주희, "가명정보 결합에 의한 재식별화 방지에 관한 비교법적 연구 - GDPR과 CCPA 및 개정 개인정보보호법 비교를 중심으로", 2021