https://doi.org/10.33778/kcsa.2024.24.3.081

생성형 인공지능 모델의 개인정보 라이프 사이클에 따른 국내 개인정보 보호법 개선 고려 요소: GDPR과 개인정보 보호법의 비교·분석

장 재 영*

요 약

본 논문은 기존에 개발된 개인정보 라이프 사이클 모델을 정리 및 분석 후 이러한 개인정보 라이프 사이클 모델이 인공지능 학습에 적용 가능한지를 살펴보았다. 검토 결과 기존의 개인정보 라이프 사이클은 인공지능 학습의 적용에 일부 한계가 있음을 발견했다. 따라서 본 논문에서는 인공지능 학습에 적합한 개인정보 라이프 사이클을 제시했다. 새로운 개인정보 라이프 사이클은 수집-학습-보유-생성·추론-차단·재학습·삭제 단계로 구성했다. 새로운 모델 제시에 따라 현행 개인정보 보호법 조항과 일치 여부를 검토 후 향후 법령 개정 방향을 제시했다. 본 논문은 인공지능 학습과 개인정보 보호의 영역에서의 체계적 접근 가능성을 높였다는 측면에서 의의가 있다.

Considerations for the Improving Domestic Personal Information Protection Act in accordance with The Life Cycle of Personal Information In Generative Artificial Intelligence Model: Comparative analysis of GDPR and Personal Information Protection Act of Korea

Jaeyoung Jang*

ABSTRACT

The purpose of this paper is to derive considerations when improving the Personal Information Protection Act ba sed on the personal information protection life cycle of the generative artificial intelligence model as generative artifi cial intelligence models are introduced and used in Korea a lot. Through the study, the necessity of using open infor mation in the collection stage, using personal information preservation technology in the learning stage, and preparin g the basis for the development of protection technology in the holding stage was derived. It also revealed the nece ssity of managing the generated information in the generation and inference stage, re-learning in the limitation and destruction stage, and preparing a filtering basis. It is expected that the results of this study can be used to revise the Personal Information Protection Act and make policies in the future.

Key words : Generative, AI, Personal Information, Privacy, Lifecycle, Data Protection Act

접수일(2024년 08월 06일), 수정일(1차: 2024년 08월 23일), 게재확정일(2024년 09월 09일)

* 한국인터넷진흥원

1. 서 론

최근 인공지능 기술과 서비스가 급격히 발전하면서 개인정보 침해 또는 유출 사고도 증가하고 있다[1]. 국내의 대표적 사례가 '이루다' 서비스이다. '이루다' 서비스는 2020년에 서비스를 출시하자마자 성희롱 논란과 함께 개인정보 유출 의혹이 발생해 2021년 개인정보의 오·남용 문제로 개인정보보호위원회로부터 총액 1억 원이 넘는 과징금과 과태료를 부과 받았다. 글로벌 인공지능 챗봇 서비스인 ChatGPT도 360만원의 과태료를 부과 받았다[2]. 이처럼 다양한 사고와 처벌에도 불구하고 국내에서 인공지능은 대규모의 데이터 처리로 인해 향후에도 개인정보 유출이나 개인정보 보호 관련 법률 위반도 지속될 것으로 예상된다.

현재 전 세계는 인공지능으로 인한 부작용의 최소화를 위해 다양한 노력을 기울이고 있다. 특히 개인정보를 침해하는 인공지능 서비스는 운영할 수 없기 때문에 공공이나 민간 영역에서 인공지능 서비스를 활성화 하면서도 개인정보를 보호할 수 있는 제도와 기준을 앞 다투어 선보이고 있다. 개인정보 보호 제도를 선도하고 있는 유럽 연합은 2024년 3월 13일 세계 최초의 인공지능 법률인 EU AI Act를 통과시켰다[3]. 영국은 A pro-innovation approach to AI regulation을 발표했고 캐나다도 The Artificial Intelligence and Data Act를 입법했다[4]. 이러한 입법 활동은 각국의 인공지능 규제 경쟁의 한 단면일 뿐이다. 기업 차원에서는 구글이 AI Principles Progress Update를 지속 발표하고 있고[5], 마이크로소프트도 Responsible and Trusted AI - Cloud Adoption Framework [6] 등을 마련해 자사의 인공지능 서비스에 적용하고 있다.

국내에서도 2023년 3월 14일에 인공지능을 포함한 자동화된 의사 결정에 대한 정보주체의 권리 보호 강화를 위해 개인정보 보호법(이하 보호법)을 개정했다. 그러나 개정 법률에는 급속하게 변화하고 있는 생성형 인공지능에 대한 고려까지는 반영하지 못했다. 이에 따라 현재 다양한 생성형 인공지능 서비스가 시장에 출시되고 있음에도 불구하고 보호법이 이러한 새로운 서비스들을 제대로 규율하지 못하는 문제가 발생하고 있다.

본고에서는 인공지능의 개인정보 보호 규제 현황을 유럽과 한국 위주로 살펴보고자 한다. 유럽의 General Data Protection Regulation (GDPR)은 현재 전 세계적으로 개인정보 보호의 표준으로 자리 잡고 있다. 한국의 경우도 유럽 시장에의 접근성과 국내 기업의 법적 리스크 감소 등을 위해 GDPR의 여러 제도를 참고해 보호법을 개정하고 있다. 따라서 보호법 개정 요소를 도출할 때 유럽의 GDPR을 같이 검토하는 것이 향후 보호법 개정의 실효성을 높이는 데 도움이 될 수 있다[7]. 반면 미국은 현황 조사에서 제외하고자 한다. 미국의 경우, 개인정보 보호의 또 다른 주요 국가임에도 불구하고, 현재 자동화된 의사 결정을 규율하는 연방법이 존재하지 않는다. 캘리포니아 소비자 개인정보 권리법(The California Privacy Rights Act of 2020, CPRA)과 같은 주법이 존재하지만 CPRA에서도 자동화된 의사 결정과 관련한 명시적은 규정은 존재하지 않는다[8].

따라서 본 논문은 생성형 인공지능 모델의 규율을 위해 유럽의 GDPR과 국내법상의 인공지능의 규율 제도인 자동화된 의사 결정 제도에 대해 살펴보고자 한다. 이후 체계적인 법령 개정 요소 도출을 위해 인공지능의 개인정보 라이프 사이클 단계별로 보호법 적용 현황을 검토하고자 한다. 이후 생성형 인공지능을 규율할 수 있는 보호법 개선 시 고려 요소를 도출하고자 한다. 이를 통해 효과적인 보호법 개정 방안 마련에 기여하고자 한다.

이를 위해 2장에서는 인공지능 관련 규제 현황을 유럽의 일반 개인정보 보호법(이하 GDPR)과 국내의 보호법을 중심으로 살펴보고자 한다. 3장에서는 생성형 인공지능 모델의 개인정보 라이프 사이클에 따른 개인정보법적 규제 문제를 살펴보고자 한다. 4장에서는 개인정보 라이프 사이클 관점에서 인공지능 서비스를 규율하기 위한 법률적 고려 요소를 현행 보호법을 기준으로 제시해 보고자 한다.

2. 인공지능 관련 규제 현황

2.1 유럽 일반 개인정보 보호법 - 프로파일링

유럽의 GDPR은 정보주체(the data subject)인 자연인(natural person)의 기본권과 자유를 보호하고, EU 역내에서 개인정보의 자유로운 이동을 위해 제정됐다[9]. GDPR에는 인공지능을 다루는 별도의 규정을 두고 있지는 않지만 GDPR 제22조의 프로파일링 조항에 따라 인공지능을 규율할 수 있어 보인다. 이 법의 프로파일링 조항을 구체적으로 살펴보면 다음과 같다.

2.1.1 규제 대상

GDPR의 제4조4항은 규제 대상을 개인의 사적인 측면의 평가를 완전 자동화된 방식으로 처리하는 경우로 보고 있다. 개인의 사적 측면의 평가에는 직장에서의 업무 성과, 경제적 상황, 건강, 개인적 선호, 관심사, 신뢰성, 행동과 태도, 위치 정보가 포함된다.

프로파일링 중 규제 대상은 <표 1>의 3가지 모두를 포함하는 경우로 한정하고 있다. GDPR에서는 자동화된 의사 결정을 인간의 인적 개입이 전혀 없이 완전 자동화(solely automated)된 기술적 수단에 의해 처리하는 의사결정(decision-making)으로 보고 있다. 이러한 결정 중 인간에 대한 프로파일링만을 대상으로 보고 있다[10]. 따라서 인공지능이 이러한 요소를 모두 포함할 경우 GDPR에 따른 규제가 가능하다.

<표 1> 규제 대상인 프로파일링 구성 요소

번호	조항
1	자동화된 형태의 정보처리
2	개인정보에 대한 수행
3	자연인에 대한 개인적 측면들의 평가

2.1.2 정보주체의 권리

GDPR 제22조에 따른 규제 대상이 되는 방식으로 인공지능이 개인정보를 처리를 하는 경우 컨트롤러(개인정보법의 개인정보처리자에 해당)는 <표 2>에 해당하는 3가지 의무사항을 부담하게 된다. 이러한 의무는 일반 개인정보와 민감 개인정보 모두 포함된다.

<표 2> 컨트롤러의 의무 사항

번호	조항
1	정보 주체는 자동화된 의사결정 활동 유형에 참여하고 있음을 알려야 함
2	정보 주체에게 자동화된 의사결정에 사용되는 논리에 대한 의미 있는 정보를 제공해야 함
3	컨트롤러는 정보 처리의 중요성과 예상 결과를 설명해야 함

GDPR 전문 제71조에 따르면 정보주체는 해당 의사 결정이 법적 효력(legal effect)이나 법적 효력과 유사한 유의미한 효력(similarly significant effect)을 가지는 경우 프로파일링을 포함한 자동화된 의사 결정의 대상이 되지 않을 권리를 가지게 된다. 다만 정보주체는 GDPR 제22조제2항에 따라 그 결정이 컨트롤러와 정보주체 간 계약의 체결이나 이행, 법률, 명시적 동의에 기반을 둔 경우 콘트롤러의 프로파일링 처리를 제한할 수 없도록 하고 있다. 이 경우에도 정보주체는 GDPR 제22조제2항제a호와 제c호에 따라 완전히 자동화된 처리에 인적 개입(human intervention)을 요구할 수 있다. 또한 자신의 관점을 표현할 권리(to express his or her point of view), 완전 자동화된 처리에 따른 평가 후 도달한 결정의 설명 요구할 권리(to obtain an explanation of the decision reached after such assessment), 그러한 결정에 이의를 제기할 권리(to challenge the decision)를 가진다[11].

2.1.3 보호 조치

콘트롤러는 GDPR 제22조에 따른 완전 자동화된 프로파일링을 하는 경우 GDPR 전문 제71조에 따른 적절한 보호 조치(safeguard) 의무를 부담하게 된다. 해당 의무에는 처리의 공정성(fairness)과 투명성(transparency) 보장, 프로파일링 시 적합한 수학적(mathematical) 또는 통계적 방법(statistical methods)의 사용, 적절한 기술적·관리적 조치(appropriate technical and managerial measures) 등이 포함된다[12].

2.1.4 개인정보 영향평가 의무

콘트롤러가 GDPR 제22조에 따른 완전 자동화된 프로파일링을 하는 경우 사업자는 GDPR 제35조에 따라 정보처리에 따른 책임을 다하기 위해 개인정보 영향평가를 실시해야 한다. <표 3>은 영향평가 고려 사항을 정리한 것이다[13].

<표 3> 영향평가 고려 사항

번호	조항
1	프로파일링에 따라 예상되는 처리 절차와 목적에 대한 체계적인 설명
2	프로파일링 목적과 관련한 처리의 필요성 및 비례성 평가
3	예상되는 처리 절차와 목적에 대한 체계적인 설명과 관련한 정보주체의 권리와 자유에 대한 위험 평가
4	보호조치, 보안조치 및 메커니즘을 포함하여 위험을 해결하기 위한 조치

GDPR 제22조에서는 규제 대상과 범위, 정보주체의 권리와 콘트롤러의 의무를 규정하고 있다. 따라서 인공지능의 개인정보 처리 전체를 해당 조항만을 가지고 규율하기에는 한계가 있다. GDPR에는 수집 목적 제한, 처리 최소화와 같은 수집 단계의 고려 사항을 다루고 있다. 보유 기간의 설정 및 보유 단계의 정확성, 접근권과 정정권 원칙도 포함하고 있다. 또한 처리 제한권, 반대권, 삭제권도 다루고 있다. 그러나 이러한 조항들은 인공지능 모델의 개인정보 처리가 아닌 일반적인 콘트롤러와 프로세서를 규율하기 위한 규정이므로 이를 학습·생성 등과 같은 인공지능 고유의 개인정보 처리 방식에 그대로 적용하기에는 일정 부분 한계가 있어 보인다.

2.2 개인정보 보호법 - 자동화된 결정

보호법은 2023년 3월 14일 제37조의2(자동화된 결정에 대한 정보주체의 권리 등)를 신설했다. 이 조항은 인공지능 등의 발달로 자동화된 결정이 증가하면서 이러한 결정에 영향을 받는 정보주체의 권리 및 의무 사항에 중대한 영향이 발생하는 사안에 대해 정보주체의 거부권과 설명권을 보장하기 위해 마련됐다. 해당 조항은 2024년 3월 15일부터 시행 중이다[14].

2.1.1 규제 대상

보호법은 완전히 자동화된 시스템으로 개인정보를 처리한 의사 결정이 이루어지는 경우 중 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우 정보처리에 대한 거부권을 부여하고 있다. 다만 동법 제15조제1항제1호(정보주체의 동의), 제2호(법령상 규정) 및 제4호(계약의 이행 등)은 제외하고 있다[12].

보호법은 GDPR과 같이 구체적으로 프로파일링이라는 단어를 명시하지 않았고 규제 대상을 구체적으로 기술하지도 않았지만 기본적으로 GDPR과 유사한 내용이라 할 수 있다. 보호법의 특기할만한 점은 제37조의2의 완전히 자동화된 시스템에 인공지능 기술을 적용한 시스템을 포함한다고 명시하여 해당 조항이 인공지능을 위한 조항임을 명확히 하고 있다는 점이다. 따라서 보호법 제37조의2는 인공지능에 대한 규제 측면에서는 GDPR 보다는 조금 더 대상이 명확하다고 볼 수 있다.

2.1.2 정보주체의 권리

보호법 제37조의2제2항에서는 자동화된 결정이 이루어진 경우 그 결정에 대한 설명 요구권과 거부권 그리고 인적 개입에 의한 재처리·설명 등 필요한 조치를 취해야 한다고 명시하고 있다. 또한 제4조(정보주체의 권리) 제6호에서는 완전히 자동화된 결정에 대한 거부권 및 설명요구권을 권리로 명시하고 있다.

보호법은 인적 개입에 대한 재처리를 명시하고 있다. 이는 인공지능의 개인정보 관련 학습이나 처리를 고려한 조항으로 보인다. 이 조항은 GDPR에 비해서 인공지능의 특성을 보다 더 고려한 조항이라 할 수 있다.

2.1.3 처리 방식의 공개

보호법은 법 제37조의2제4항에서 자동화된 결정의 기준과 절차, 개인정보 처리 방식 등을 정보주체가 쉽게 확인할 수 있게 공개하도록 규정하고 있다. 해당

조항은 GDPR 전문 제71조에 따른 적절한 보호 조치의 내용을 일부 포함하고 있지만 그 보다는 보호법 제30조(개인정보 처리방침의 수립 및 공개)와 더욱 밀접한 조항으로 보는 것이 타당해 보인다. 인공지능의 자동화된 결정 기준과 처리 및 개인정보 처리 방식을 공개하도록 한 위 조항은 처리 방침의 공개를 통한 정보주체의 알 권리 강화라는 국내 보호법의 특징을 반영하고 있다. 따라서 본 조항은 GDPR과 차별화되는 조항이라 할 수 있다.

2.1.4 하위 법령 위임

보호법 제37조의2제5항에서는 제1항부터 제4항까지에서 규정한 조항 외의 사항에 대해서는 대통령령에서 정하도록 하고 있다. <표 4>는 해당 항목을 정리한 것이다.

<표 4> 제37조의2제5항에 따른 위임 항목

번호	조항
1	자동화된 결정의 거부·설명 등을 요구하는 절차 및 방법
2	거부·설명 등의 요구에 따른 필요한 조치
3	자동화된 결정의 기준·절차 및 개인정보가 처리되는 방식의 공개

GDPR은 위임 조항이 없으나 국내 보호법에서는 3가지 항목을 위임하고 있다. 이는 입법적인 측면과 해당 조항을 운영하는 측면에서 국내 보호법이 GDPR과 일부 차이가 나는 규제 방식이라 할 수 있다.

국내 보호법 제37조의2는 규제 대상, 정보주체의 권리, 처리 방식의 공개, 하위 법령 위임을 규정하고 있다. 이 조항들은 인공지능을 규제 대상으로 하고 있고, 재처리 등 인공 지능의 특성을 반영하고 있다. 또한 보호법도 GDPR과 마찬가지로 개인정보 주체의 권리와 개인정보처리자의 의무를 다양하게 부과하고 있다. 그러나 보호법의 법적 규정과 신설된 자동화된 결정 조항만으로 기존의 개인정보 처리 프로세스와 다른 생성형 인공지능 모델을 효과적으로 규율하기에는 일정부분 한계가 있어 보인다.

2.3 GDPR과 개인정보 보호법 관련 규정 비교

<표 5>와 같이 GDPR과 보호법은 인공지능을 각각 프로파일과 자동화된 결정으로 규제하고 있다. 두 법률은 규제 대상과 정보주체의 권리 측면에서는 유사한 내용을 담고 있다. 그러나 입법 방식의 차이에 따라 GDPR은 보호조치와 개인정보 영향평가를, 보호법은 처리 방식의 공개와 하위 법령 위임의 내용을 각각 포함하고 있다. 반면 보호법의 해당 조항이 보다 최근에 신설된 것이므로 인공지능 서비스의 특성을 조금 더 구체적으로 다루고 있다고 할 수 있다. 그러나 국내 보호법의 이러한 특성만으로 정보주체의 권리를 보장하고 인공 지능 서비스를 책임성 있게 규율한다고 볼 수는 없다.

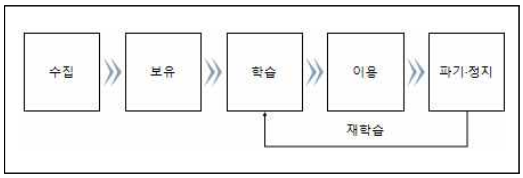
<표 5> 자동화된 결정 관련 규정 비교

항목	GDPR	보호법
규제 대상	프로파일링(개인의 사적인 측면의 평가)	완전히 자동화된 시스템으로 개인정보를 처리한 의사 결정
정보주체 권리	- 자동화된 결정에 대한 참여 권리 - 자동화된 결정의 논리 및 결과 설명 요구권 - 자동화된 결정에 이의 제기 권리	- 자동화된 결정에 대한 설명 요구권 및 거부권 - 인적 개입 요구권 및 재처리 요청권
처리 방식의 공개	처리의 투명성 보장	자동화된 결정의 기준, 절차, 개인정보 처리 방식의 공개
개인정보 영향평가 의무	의무 조항 있음	명시적 의무 없음
하위 법령 위임	위임 조항 없음	자동화된 결정 관련 절차와 방법 등을 대통령령으로 위임

3. 생성형 인공지능의 라이프 사이클 단계별 개인정보 보호 법령 검토

3.1. 개인정보 보호 라이프 사이클 모델

개인정보 보호 라이프 사이클은 개인정보를 생애주기 및 이에 따른 일정한 흐름에 따라 체계적으로 분석 및 관리·운영하는 기법이다[16]. 인공지능 중 생성형 모델에 대한 개인정보 라이프 사이클 모델은 (그림 1)과 같이 수집, 보유, 학습, 이용, 파기·정지 단계로 이루어져 있다[17].



(그림 1) 생성형 AI의 개인정보 라이프 사이클[16]

이러한 단계에 따라 보호법에 생성형 인공지능 모델을 규제함에 있어서 직접적인 근거 조항이 있는지를 살펴보면 <표 5>와 같다. 이 장에서는 라이프 사이클의 각 단계별 개인정보 보호 이슈를 보호법을 중심으로 살펴보고자 한다. 다만 정보주체의 권리를 기술하고 있는 보호법 제4조는 조사 대상에서 제외한다.

<표 5> AI 라이프 사이클의 보호법상 근거

대분류	소분류	보호법
수집	정보주체	제15조
	서비스	제15조
	공개정보	-
보유		제3조, 제29조
학습		-
이용	이용·제공	제15조, 제17조
	생성	-
	추론	제37조의2
파기·정지	파기	제21조,
	정정·삭제	제36조
	정지	제37조, 제37조의2

3.2 수집

우리나라의 보호법은 정보주체가 제공, 서비스를 위해 생성, 공개된 정보를 수집한 모든 정보의 수집에는 적정한 근거가 있어야 한다고 보고 있다. 그러나 현재 인공지능의 학습을 위한 공개된 정보의 수집에 대해서는 보호법에 명시적인 근거 규정이 마련되어 있지 않다.

대법원이 2016. 8. 17일 선고한 2014다235080(로앤비 사건)과 서울행정법원 2023. 10. 26. 선고 2021구합57117 판결(메타 케임브리지 애널리티카 스캔들)에서 공개된 개인정보의 성격과 목적 등을 고려해서 개인정보 처리 시 해당 항목들의 성격이 유지되는 범위 내에서 개인정보를 처리도록 하는 판례가 있다[18]. 또한 보호법 제15조제1항제6호에 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로 정보주체의 권리보다 명백하게 우선하는 경우는 처리가 가능하도록 한 조항을 적용할 수 있어 보인다.

그러나 이러한 근거만으로 온라인의 개인정보를 자유롭게 수집해서 생성형 인공지능을 학습시키는 것은 위험성이 있어 보인다. 다만 국내 신용정보법에는 신용정보주체가 스스로 사회관계망 서비스 등에 직접 또는 제3자를 통하여 공개한 정보에 대해서는 수집할 수 있는 명시적인 근거가 존재한다[19].

3.3 보유

보유 단계는 개인정보를 수집해서 파기하는 전체 단계와 관련이 있다. 따라서 라이프 사이클의 수집과 파기 중간 어느 단계에 포함시켜도 무방해 보인다. 다만 처리 흐름 이해의 일관성을 위해 학습 이전 단계에 넣는 것이 타당해 보인다.

보유 단계는 일반적인 개인정보 라이프 사이클의 역할과 동일하다. 생성형 인공지능 모델의 보유 단계에서는 시스템(Denial of Service, DoS), 시스템 취약점), 기기·인프라(Dos·Distributed DoS (DDoS) 및 인프라 취약점, 기기·인프라 해킹 등), 네트워크(Blackbox attack, DoS, DDoS, Jamming attack) 등에서 기존 보안 영역의 문제와 동일한 문제가 발생할 수 있다[20]. 더욱이 학습 데이터를 저장하는 데이터베이스 내의 데이터 위변조, 랜섬웨어, 악성코드 등 보안위협도 존재한다.

다만 인공지능 특유의 위협이 보유 단계에 존재할 수 있다. 인공 지능의 경우 학습 과정에서 poisoning attack, evasion attack, backdoor attack과 같은 보안 위협이 제기될 수 있다. 이러한 위협에 대해서는 보호법 제29조(안전조치 의무)에 일정 정도 근거가 마련되어 있다. 다만 생성형 인공지능이라는 새로운 기술에 대해 현행 법률 조항만으로 효과적으로 규율할 수 있을지에 대해서는 향후 기술의 발전과 이에 따라 발생 가능한 위협과 그리고 그에 따른 위험이 실제할 확률과 피해 크기 등을 면밀히 검토할 필요가 있다[21].

3.4 학습

생성형 인공지능 모델은 기존의 개인정보처리시스템과 달리 학습이라는 고유의 처리 단계를 거친다. 학습은 훈련(training)과 테스트(testing), 평가(validation) 과정이 모두 포함된다. 국내 보호법의 경우 제37조의2(자동화된 결정에 대한 정보주체의 권리 등)도 비슷하다. 다만 조문에 '인공지능 기술을 적용한 시스템을 포함한다'고 규정하고 있고, 재처리 등의 용어를 사용하고 있다는 점에서 근거가 조금 더 마련되어 있다고 할 수 있다.

3.5 이용

현행 보호법에서는 의사결정, 결정, 처리라는 개념으로 생성·추론 단계를 설명하고 있다. 또는 생성형 인공지능 모델은 저장된 데이터에 질의해서 나오는 출력 값을 제공하는 것이 아니라 확률적 모델(probabilistic model)이나 온도(temperature) 기법을 활용해 새로운 개인정보를 생성·추론할 수 있다.

개인정보의 생성과 추론에 대해서는 현행 보호법에 명시적인 규정은 없다. 다만 식별 가능한 자연인과 관련한 모든 정보라고 되어 있으므로 생성이나 추론의 결과로 만들어진 개인정보도 모두 현행 보호법상의 개인정보에 해당한다. 그런데 현행 보호법 제35조의2(개인정보의 전송 요구)제1항제2호에는 개인정보를 기초로 분석 및 가공해서 별도로 생성한 개인정보는 정보주체가 전송을 요구할 수 없도록 규정하고 있다. 이 조항은 생성 정보는 정보주체의 개인정보가 아닌 것으로 규정한다고 볼 소지가 있어 추가적인 논의가 필요해 보인다.

3.6 파기·정지

생성형 인공지능이 개인정보를 생성 및 추론하는 경우 정보주체는 개인정보 자기결정권 보호 측면에서 처리 결과의 정정, 정지, 삭제 및 파기 등 다양한 권리를 가질 수 있다. 정지 및 파기 단계는 라이프 사이클의 다른 단계에 비해 보호법에 상에 다양한 근거 조항이 마련되어 있다. 보호법은 제4조(정보주체의 권리)의 파기 조항, 제21조(개인정보의 파기), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지)가 있다.

생성형 인공지능은 정정, 정지, 삭제 및 파기(이하 파기 등)를 위해서 데이터베이스에서 개인정보를 삭제했다고 하더라도 학습한 알고리즘에 개인정보가 존재할 수 있다. 이 경우 법령에서 규정하고 있는 지체 없이 삭제하는 것이 용이하지 않을 수 있다.

특히 해당 개인정보를 삭제하기 위해서는 이미 학습해 놓은 모델(pre-trained)을 다시 학습 시켜야 하고 이러한 경우 새로운 학습을 위해 시간과 매몰비용이 발생할 수 있다. 더욱이 대규모 언어 모델과 같은 생성형 인공지능의 경우 이러한 처리에 소요되는 자원이 대규모로 발생할 수 있다는 측면에서 인공지능 기술이 법률을 준수하는 것에 한계가 발생할 수 있다는 문제점이 발생할 수 있다[22].

4. 보호법 근거 조항 마련 시 라이프 사이클 단계별 고려 요소

4.1 단계별 고려 요소

4.1.1 수집 - 공개된 정보 활용 근거 정비

현행 보호법에는 정보주체와 서비스 중의 개인정보 수집에 관한 법적 근거가 제15조에 마련되어 있다. 그

러나 인공지능 기술이 발전하면서, 인터넷 상의 공개 정보 등의 수집에 대한 구체적인 법적 근거가 부족한 상황이다. 생성형 인공지능 모델은 대규모 데이터 수집이 불가피한 측면이 있으므로, 공개된 정보 수집 시 동의 의사가 추단되는 범위나 관련 법령 정비의 필요성이 제기되고 있다. 이 경우, 정보주체의 권리 보호와 개인정보처리자의 합리적인 사업 영위를 균형 있게 고려하여 <표 6>과 같은 요소를 반영해 개인정보 수집이 정보주체의 권리와 자유를 침해하지 않도록 법령을 정비해야 한다.

<표 6> 공개 정보의 정보주체 권리 영향 요소

항목	정보주체의 권리침해 가능성	
	보호법익이 높음	보호법익이 낮음
공개된 개인정보의 성격	개인정보의 민감성이 높을 경우	공인에 관한 정보로서 알권리가 우선인 경우
공개의 대상 범위	접근 대상이 정해져 있는 경우	누구나 접근 가능한 정보
공개된 개인정보의 처리 방식	민감정보 추론 또는 프로파일링을 위한 처리방식	텍스트 배열 등 통계적 상관관계를 파악하기 위한 데이터 처리방식
정보주체의 예견가능성	정보주체가 당초 공개 목적·범위를 초과하여 합리적으로 기대가 어려운 방식으로 처리	동의한 서비스 이용약관, 개인정보처리방침 등에 AI 학습데이터 처리가 명시된 경우
정보주체 권리보장 방안	정보주체 외로부터 수집 개인정보의 수집출처 등 통지, 열람, 삭제, 처리정지권 등 법령에 따른 권리행사 보장이 불충분	정보주체의 개인정보자기결정권을 보장하기 위한 다양한 권리행사 방안·절차가 마련되는 경우

※ [23]의 내용을 일부 수정

정보주체의 개인정보나 서비스 중의 개인정보 수집의 경우에도, 인공지능은 생성과 추론을 특징으로 하므로 기존의 서비스에서 수집되는 개인정보와 성격이 다를 수 있다. 따라서 이러한 경우, 정보주체가 입력하는 프롬프트(prompts)를 포함한 수집되는 개인정보 항목에 대해 구체적으로 명시될 수 있도록 관련 조항의 개정을 고려할 필요가 있다.

또한 제3장에서 살펴본 바와 같이 헌법상 정보주체에게 부여된 개인정보 자기결정권을 침해하지 않으면서 개인정보처리자가 개인정보를 정당하게 처리할 수 있도록 하는 행정적 방법과 공개 정보 수집에 대한 법률적 근거를 마련하는 두 가지 방식 모두를 고민할 필요가 있다. 다만 개인정보처리자의 사업 영위에 과도한 부담을 주지 않도록 제도와 정책의 안정성 측면에서 국내 판례 등을 기반으로 근거 법령을 신설하는 것이 보다 바람직해 보인다.

인공지능은 대규모의 개인정보를 처리하므로 개인정보 수집 과정에서 개인정보처리자가 투명하게 수집하는 정보의 항목을 공개하고, 정보주체가 자신의 개인정보가 어떻게 사용될지 이해할 수 있도록 해야 한다. 이러한 과정에서 정보주체의 권리와 사업자의 필요 사이의 조화로운 해결책을 모색하며 공개된 정보의 활용 근거와 사용 목적을 명확히 하고, 정보주체의 권리에 대해 고지하는 공정성 및 투명성 확보 조항이 필요해 보인다.

4.1.2 보유 - 보호 기술 개발 근거 마련

생성형 인공지능의 보안이나 개인정보 보호 문제에 대해서는 현행 보호법 내에서 필요한 근거 조항이 존재한다(제3조, 제29조). 또한 개인정보의 안전성 확보 조치 기준(개인정보보호위원회 고시)도 존재한다.

다만 생성형 인공지능은 기존의 개인정보처리시스템이 가지고 있는 사이버 보안과 개인정보 침해 문제 외에도 인공지능이 가지고 있는 다양한 문제를 추가로 가지고 있다. 예를 들어, 인공지능은 수집한 개인정보에 아동 성착취 이미지 발견 등의 문제[24]가 발생할 수 있다. 보유 단계에서는 데이터 수집 출처 검증, 출력 단계에서는 암기된 학습에 사용한 문서를 재조립해 출력하는 역류(regurgitate) 문제[25], 보유한 개인정보의 학습 또는 생성 방지를 위한 미세조정(fine-tuning) [26]의 필요성이 존재한다. 이러한 문제를 체계적으로 검증하고 대책을 마련하기 위해, 정보주체의 권리와 사업자의 운영 효율성을 함께 고려하여 생성형 인공지능 서비스에 대한 개인정보 영향 평가를 의무화할 필요가 있다. 현재 유럽에서는 완전 자동화

된 프로파일링을 하는 경우, 콘트롤러에게 개인정보 처리에 따른 책임을 다하기 위한 개인정보 영향평가 의무를 부여하고 있다. 한국의 경우도 보호법에서 민감한 개인정보를 처리할 개연성이 높거나 정보주체의 권리와 의무에 중대한 영향을 미칠 수 있는 인공지능 서비스의 개발 및 운영의 경우 보호법에 따른 영향평가 의무를 부과할 필요가 있다.

또한 생성형 인공지능 모델에서 membership inference나 model extraction과 같은 새로운 개인정보 유출 및 침해 위협이 나타나고 있으므로 보호법에 Privacy Enhancing Technologies (PETs)나 Privacy Preserving Technologies에 대한 근거 조항을 마련해 차분 프라이버시, 연합학습, 동형 암호, 다자간 계산, 연합 학습과 같은 인공지능에 적용 가능한 보호 기술의 적용을 위한 근거 마련이 필요해 보인다. 이를 위해 개인정보 보호와 기술 개발의 균형을 맞춰 보호법 제7조의8(보호위원회의 소관 사무)에 인공지능 기술 개발의 지원 보급 및 산학연의 기술 개발 지원 항목을 신설하는 것도 가능해 보인다.

4.1.3 학습 - 개인정보 보호 기술의 사용 등

생성형 인공지능 모델의 가장 커다란 문제 중 하나는 개인정보를 학습해서 새로운 개인정보를 생성 및 추론을 통해 의도하지 않게 사생활 침해가 발생할 수 있다는 점이다. 따라서 개인정보를 학습하지 않고 유사한 효과를 낼 수 있다면 개인정보 유출 및 침해 문제가 상당부분 해소될 수 있을 것이다. 또한 학습 과정에서 수집 및 보유하는 개인정보를 최소화하는 것이 개인정보 보호 측면에서 보다 안전할 수 있다.

현행 보호법 제28조의2 내지 제28조의7에는 가명정보에 대한 규정이 있어서 개인정보 처리에 대한 기업의 영업의 자유를 보장하면서도 불필요한 개인정보 수집 문제의 해소에 대한 근거가 존재한다. 그러나 이 조항은 가명정보 처리를 허용하기 위한 일반적인 조항이란 측면이 강하다. 따라서 생성형 인공지능 모델의 사용으로 인한 의도하지 않은 개인의 식별을 방지하기 위한 추가적인 기술의 적용이 필요하다. 다만 기술적 요구 사항이 기업에게 과도한 부담이 되지 않도록 주의해야 한다. 또한 인공지능의 대규모 데이터를 필요로 하는 특성을 고려해, 데이터 규모 증가에 따른 개인정보의 식별 가능성을 관리하는 법적 근거도 필요하다. 가명 처리 등을 했다 하더라도 생성형 인공지능 모델에서는 재식별 위협이 존재할 수 있다. 따라서 이를 방지하기 위해 가명화·익명화 외에 <표7>에 나와 있는 합성 데이터, 차분프라이버시 기술을 사용해 학습하도록 법령에 근거 조항을 마련할 필요가 있다. 또한 학습 과정에서 개인정보를 최소한으로 처리하기 위한 연합학습 등의 기술의 적용 근거의 마련도 고려할 필요가 있다.

<표7> 인공지능의 프라이버시 강화 기술(PETs)

항목	세부 기술
데이터 보호	가명화, 익명화, 차분 프라이버시, 합성 데이터
학습 방식 보호	연합학습, 동형 암호, 다자간 계산

4.1.4 이용 - 생성·추론 정보의 관리 근거 정비

현재 생성 및 추론된 개인정보에 대해서는 정보의 소유 및 관리에 대한 구체적인 근거가 부족한 상황이다. 개인정보의 경우, 정보주체와 관련한 정보라 하더라도 정보주체가 제공하지 않고 개인정보처리자가 생성한 경우에 대해서는 해당 개인정보의 소유권과 권한에 대한 문제가 존재한다[27]. 따라서 보호법 내에서 기존 법령과의 충돌 가능성을 최소화하고, 새로운 생성 및 추론 정보의 법적 지위를 명확히 규정해 정보 주체의 권리 보호와 개인정보처리자의 권리 및 책임을 분명히 할 필요가 있다.

또한 인공지능 모델의 학습을 위해 수집한 개인정보가 다른 목적을 위해 사용되지 못하도록 근거 조항을 마련할 필요가 있다. 현행 보호법에서는 정보주체의 개인정보의 수집을 엄격히 하면서도 인공지능이 경우 기술적 특성으로 인해 개인정보를 포함한 데이터의 사용을 관대하게 바라보고 있다. 따라서 인공지능을 위해 수집한 데이터가 다른 데이터의 처리를 위해 사용되는 경우 차별의 문제가 발생할 소지가 있다.

그러므로 인공지능을 위해 수집한 데이터가 다른 용도로 사용되는 경우 이를 통제할 수 있는 근거 조항을 마련할 필요가 있어 보인다.

생성·추론된 개인정보의 경우도 정보주체의 동의를 받지 않고 어떠한 목적으로 어디까지 사용할 수 있는지에 대한 명확한 근거가 필요하다. 이를 위해서 정보주체가 개인정보처리자에 의해 생성·추론된 개인정보의 주체에 대해 해당 개인정보 주체가 통제할 수 있는 권한을 부여하고, 그에 따른 조치(정보 접근, 수정, 삭제 요청 등)를 보장할 수 있는 조항이 법령에 마련될 필요가 있다.

마지막으로 인공지능에서 개인정보의 이용, 제공, 생성, 추론이 원활히 처리되기 위해서는 정보주체와 개인정보처리자 간의 신뢰 관계 형성이 중요하다. 이를 위해서는 개인정보처리자가 이용, 제공, 생성, 추론한 개인정보에 대한 출처를 명확히 설명하고, 이를 투명하게 관리해야 한다. 또한 생성형 인공지능 서비스 등에서 이용, 제공, 생성, 추론한 개인정보가 오용 또는 잘못 생성 및 추론하여 정보주체에게 피해가 발생하는 경우 그에 따른 개인정보처리자 등의 책임을 보호법상에 명확히 규정해 법적 안정성을 확보할 필요가 있다.

4.1.5 파기·정지 - 재학습 및 필터링 근거 마련

현행 보호법에는 정보주체의 요구가 있는 경우 파기, 정정·삭제, 정지 권리가 보호법 제21조에 마련되어 있다. 생성형 인공지능 모델에서는 이러한 요구 사항을 충족시키기 위해서 해당 개인정보가 있는 데이터를 배치 처리(batch processing)해 재학습을 하거나 실시간 개인정보인 경우 트리거(trigger)를 발생시켜 필터링해야 한다.

다만 현행 보호법에서는 즉시 파기 등을 원칙으로 하고 있으나 생성형 인공지능은 기술적으로 즉시 파기 등이 쉽지 않을 수 있다. 예를 들어, 인공지능이 학습한 데이터를 바탕으로 개인의 정보를 재생성할 수 있기 때문에, 개인정보 파기 후에도 그 영향이 남을 수 있다. 따라서 필터링과 같은 임시 조치를 통해 개인정보 주체의 개인정보통제권은 보호하되 재학습을 통해 파기 등이 생성형 인공지능 서비스 제공의 안정성도 같이 모색할 필요가 있다. 생성형 인공지능의 기술 및 서비스 특성을 고려한 합리적인 파기 등을 위한 기간과 조건 등에 대해서는 보호법상에 명문의 규정을 마련할 필요가 있어 보인다.

또한 보호법 제36조제3항에는 삭제된 개인정보는 복구 또는 재생되지 못하도록 되어 있다. 그러나 생성형 인공지능의 학습 특성상 정형화된 특정 개인정보를 삭제했다 하더라도 권리주체가 제공한 또는 권리주체의 정보로 인해 개인정보가 아닌 정보가 다른 정보들과 결합하여 특정한 개인정보가 생성될 수 있다는 문제 또한 존재한다. 개인정보처리자가 합리적 조치를 취했음에도 불구하고 인공지능의 기술적 특성을 인해 삭제 또는 처리가 정지되어야 하는 정보가 정상적으로 처리되지 않는 경우의 면책 대상과 조건에 대해 보호법상의 기준을 마련할 필요도 있어 보인다. 또한 생성형 인공지능이 도입 초기임을 고려하여 특정 상황에서 개인정보처리자가 정보 주체의 요구를 거부할 수 있는 법적 근거와 예외 사항을 규정하여 법적 안정성의 확보도 고려할 필요도 있어 보인다.

4.2 요약

현행 보호법은 인공지능에 특화되어 있지 않으므로 생성형 인공지능의 효과적인 규제를 위해 보호법에 인공지능의 기술적 특성을 반영해 법령을 정비할 필요가 있다. 주요한 법령 정비 조항은 <표 8>에 정리했다.

<표 8> 인공지능의 기술적 측면을 고려한 법령 정비 요소

분류	보호법 정비 항목
수집	공개정보의 처리 근거 조항 마련
	정보주체 및 서비스 중 수집 정보의 항목 등을 명시
	수집 시 공정성 및 투명성 확보 조항 마련
보유	영향평가 의무 부과
	인공지능에 적용 가능한 보호 기술의 적용

	근거 마련
	보호위원회의 소관 사무에 인공지능 기술 개발의 지원 보급 및 산학연의 기술 개발 지원 항목 신설
학습	가명화·익명화 또는 합성 데이터, 차분프라이버시 기술을 사용해 학습하도록 법령에 근거 조항을 마련
이용	생성 및 추론된 정보의 권리 및 소유 근거 마련 검토
	인공지능 모델 학습을 위해 수집된 정보의 다른 용도 전용 제한 근거 마련
	생성 및 추론된 정보의 통제권 마련
파기·정지	필터링과 같은 임시 조치 근거
	합리적인 파기 등을 위한 기간과 조건 등 근거 마련
	정보가 정상적으로 처리되지 않는 경우의 면책 대상과 조건
	특정 상황에서 개인정보처리자가 정보 주체의 요구를 거부권

우선 수집 단계에서는 인공지능 기술의 발전에 따른 공개된 정보 수집에 대한 구체적 법적 근거를 마련할 필요가 있다. 보유 단계에서는 합성 데이터, 연합학습과 같은 추가적인 보호 기술의 사용에 대한 근거 조항을 마련할 필요가 있다. 학습 단계에서는 생성·추론 정보가 의도하지 않은 사생활 침해로 이어지지 않도록 개인정보를 최소로 사용하는 기술의 적용을 위한 근거 조항을 마련할 필요가 있다. 이용 단계의 경우 생성형 인공지능의 생성 및 추론된 정보에 대한 관리 방안을 규정할 필요가 있다. 마지막으로 파기 단계는 개인정보 파기 시, 인공지능 모델이 학습한 데이터에서 완전히 삭제되지 않을 가능성이 있고, 보호법에서 요구하는 즉시 파기가 기술적으로 어려울 수 있으므로, 정보주체의 권리 보호와 기업의 운영 효율성 간의 균형을 맞추는 파기 기준 마련이 필요하다.

5. 결론

본 연구에서는 인공지능 기술이 급격하게 발전하고 인공지능의 발전에는 개인정보 보호가 핵심 과제이기 때문에 유럽의 GDPR과 국내의 보호법상에서 생성형 인공지능 모델을 어떻게 규율하고 있는지를 프로파일링 조항과 자동화된 결정을 중심으로 살펴봤다. 이후 생성형 인공지능 모델의 라이프 사이클 단계별 개인정보 보호 법령상의 규제 근거 검토한 후 국내 보호법의 근거 조항 마련 시 라이프 사이클 단계별 고려요소를 도출했다. 이러한 과정을 통해 수집 단계의 공개된 정보 활용 근거 정비, 학습 단계의 개인정보 보존 기술의 사용, 보유 단계의 보호 기술 개발 근거 마련, 생성·추론 단계의 생성정보 등의 관리 근거 정비, 제한·파기 단계의 재학습 및 필터링 근거 마련 필요성을 도출했다.

본 연구는 개인정보 라이프 사이클을 기반으로 하고 있기 때문에 생성형 인공지능과 관련한 개인정보 보호 원칙과의 충돌 문제, 정보주체의 권리 보장 등에 대해서는 다루지 못한 한계가 있다. 그러나 생성형 인공지능을 중심으로 인공지능이 급격히 발전하고 있고 이에 따라 보호법의 개정 수요 압력도 거세지고 있다. 따라서 적절한 시기에 개인정보 라이프 사이클 단계별로 보호법 개정 요소들을 도출해 냈다는 측면에서 의의가 있다고 할 수 있다. 본 연구가 학계와 실무에 기여할 수 있기를 기대한다.

참고문헌

[1] J. Curzon, T. A. Kosa, R. Akalu, and K. El-Khatib, “Privacy and artificial intelligence,” IEEE Transactions on Artificial Intelligence, Vol. 2, No. 2, pp. 96-108, 2021.

[2] 손희정, “인공지능과 젠더 테크놀로지: 이루다 1.0 논란을 중심으로,” 젠더와 문화, Vol. 15, No. 2, pp. 67-94, 2022.

[3] M. Veale, F. Zuiderveen Borgesius, “Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach,” Computer Law Review International, Vol. 22, No. 4, pp. 97-112, 2021.

[4] 김도원, 김성훈, 이재광, 박정훈, 김병재, 정태인, 최은아, “ChatGPT(챗GPT) 보안 위협과 시사점,”

KISA INSIGHT, Vol. 2023, No. 3, pp. 1-26, 2023.
[5] GoogleAI, “AI Principles Progress Update, https://ai.google/static/documents/ai-principles-2022-progress-update.pdf,” Google, 2022.
[6] Microsoft, “Microsoft Cloud Adoption Framework for Azure,” Microsoft, 2023.
[7] S. Eskens, “Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to This Form of Personal Data Processing, and How Should It?”. 2016.
[8] L. Determann and J. Tam, “The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide.” Journal of Data Protection & Privacy, Vol. 4, No. 1, pp. 7-21. 2020.
[9] C. J. Hoofnagle, B. Van Der Sloot, and F. Z. Borgesius, “The European Union general data protection regulation: what it is and what it means,” Information & Communications Technology Law, Vol 28, No. 1, pp. 65-98. 2019.
[10] P. Voigt and A. Von dem Bussche, “The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed.,” Cham: Springer International Publishing, 10(3152676), 10-5555. 2017.
[11] K. Wiedemann, “Profiling and (automated) decision-making under the GDPR: A two-step approach,” Computer Law & Security Review, Vol. 45, 105662, 2022.
[12] S. Wachter, “Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR.” Computer law & security review, Vol. 34, No. 3, pp. 436-449. 2018.
[13] G. Georgiadis and G. Poels, “Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review,” Computer Law & Security Review, Vol. 44, 105640. 2022.
[14] 정혜영, “개정 개인정보보호법의 분석과 평가-개인정보자기결정권의 범위와 한계를 중심으로.” 동아법학, Vol. 102, pp. 1-35. 2024..
[15] 박노형, 김효권. “자동화된 결정에 관한 개인정보 보호법 정부 개정안 신설 규정의 문제점-EU GDPR 과의 비교 분석,” 사법, Vol. 1, No. 62, pp. 361-390, 2022.
[16] J. Y. Jang, T. H. Park, and B. S. Kim, “The life cycle model considering legal and technical characteristics of personal data,” The Journal of Society for e-Business Studies, Vol. 17, No. 3, pp. 43-60, 2012.
[17] J. Y. Jang and J. M. Kim, “Personal Information Life Cycle Model Considering the Learning Characteristics of Artificial Intelligence,” Convergence Security Journal, Vol. 24, No. 2-1, pp. 47-53, June 2024.
[18] R. Horn and J. Merchant, “Managing expectations, rights, and duties in large-scale genomics initiatives: a European comparison,” European Journal of Human Genetics, Vol. 31, No. 2, pp. 142-147, 2023.
[19] 김도엽, “인공지능에서의 개인정보 보호 고려사항,” NAVER Privacy White Paper, pp. 75-138, 2022.
[20] 유진호, 민경식, 박진상, 김관영, “AI 중심사회의 도래와 보안 이슈 분석,” KISA INSIGHT, Vol. 3, pp. 1-30, 2022.
[21] 개인정보보호위원회, “인공지능 시대 안전한 개인정보 활용 정책방향,” 2023. 8.
[22] Y. Viswanath, S. Jamthe, S., Lokiah, and E. Bianchini, “Machine unlearning for generative AI,” Journal of AI, Robotics & Workplace Automation, Vol. 3, No. 1, pp. 37-46, 2024.
[23] 개인정보보호위원회, “인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서,” 2024.
[24] 하수민, “AI 데이터에서 아동 성학대 이미지 발견… 전문가 "놀랍지 않다"” 머니투데이, 2023.12.21.
[25] Pen잡은루이스, “뉴욕타임스의 소송 제기에 따른 오픈 AI의 입장,” 2024.
[26] Z. Wang, B. Bi, S. K. Pentyala, K. Ramnath, S. Chaudhuri, S. Mehrotra, and S. Asur, “A Comp

rehensive Survey of LLM Alignment Techniques: RLHF, RLAIF, PPO, DPO and More," arXiv preprint arXiv:2407.16216. 2024.
[27] 이성엽 외, "데이터와 법" 박영사, Vol. 2. 2024.

〔저자소개〕

장 재 영 (Jaeyoung Jang)
2023년 8월 연세대학교 정보시스템학 박사
2003년 8월 ~ 현재 한국인터넷진흥원
2024년 3월 ~ 현재 고려대학교 겸임 교수

email : jyjang31@gmail.com