

## 생성형 AI API 활용의 제문제

- OpenAI사의 'Sora' 등 생성형 AI API 이용에 따른 법률 쟁점 등을 중심으로 -

OpenAI사는 2024. 2. 15. 텍스트로부터 동영상을 생성하는 디퓨전 모델(diffusion model) 'SORA'를 공개하였습니다. OpenAI사의 설명에 따르면 SORA는 사용자의 프롬프트를 준수하면서 최대 1분 길이의 고품질 비디오를 생성할 수 있고, 특히 여러 캐릭터, 특정 유형의 움직임, 피사체 및 배경의 정확한 디테일이 있는 복잡한 장면을 구현할 수도 있습니다. 이와 같은 생성형 AI는 대체로 '웹 API' 형태로 제공되는데, 이를 통해 생성형 AI를 기업 실무에 적용할 시에는 다양한 법률적 이슈가 발생할 여지가 있습니다. 이에, 이번 뉴스레터에서는 생성형 AI API를 기업 실무에 활용하며 발생할 수 있는 법률 이슈·책임 관련 문제를 간략하게 개관하고자 합니다.

### 1. API의 개념 및 생성형 API 주요 사례

API는 애플리케이션 프로그램 인터페이스(Application Programming Interface)의 줄임말로, 일정한 소프트웨어가 상호간 요청과 응답을 사용하여 서로 통신하는 방법에 관한 규약을 나타냅니다.<sup>1</sup> API는 상호통신을 위해 소프트웨어 개발자가 이용하는 규약에 불과하여 그 유형을 한정하기는 어려우나, 최근에는 웹 API가 폭넓게 사용되며 맥락에 따라 'API'라는 표현은 웹 API만을 통칭하는 표현으로 사용되기도 하는 것으로 보입니다.

OpenAI를 비롯한 생성형 AI를 서비스로서 제공하는 여러 회사는 자사의 파운데이션 모델을 직접 공개하기보다는 해당 모델에 대한 웹 API만을 공개하고 있으며, 국내외 많은 개발자는 이를 활용한 다양한 소프트웨어 개발을 시도하고 있습니다. 예컨대 OpenAI는 자사의 GPT(텍스트 생성), DALL-E(이미지 생성)에 대한,<sup>2</sup> Google은 자사의 Gemini(텍스트 생성)에 대한,<sup>3</sup> 네이버는 최근 공개된 HyperCLOVA에 대한<sup>4</sup> 웹 API 규격을 공개한 바 있습니다.

기업은 실무 환경에서 자사의 필요에 부합하는 생성형 AI 활용을 위하여 단순히 생성형 AI 업체가 제공하는 완성형 서비스를 이용하는 외에도, 생성형 AI API를 사용한 맞춤형 서비스를 도입할 수 있습니다. 그러나 그와 같은 과정에서 AI 활용에 따른 각종 법률상의 위험 내지 책임 소재가 정리되지 않는다면 맞춤형 서비스 구축 비용을 들여 생성형 AI 서비스를 쉽사리 도입하기 어려운 것이 현실입니다. 특히 생성형 AI

<sup>1</sup> AWS, "API란 무엇인가요?", (2024. 2. 3. 접근, <https://aws.amazon.com/ko/what-is/api/>)

<sup>2</sup> <https://platform.openai.com/docs/api-reference/chat/create>

<sup>3</sup> [https://ai.google.dev/?gad\\_source=1&gclid=EAlalQobChMI7ZG6kNjAhAMVzNIWBR0Aaw4tEAAAYASAAEgUjb\\_D\\_BwE](https://ai.google.dev/?gad_source=1&gclid=EAlalQobChMI7ZG6kNjAhAMVzNIWBR0Aaw4tEAAAYASAAEgUjb_D_BwE)

<sup>4</sup> <https://apiindocloud-docs.com/docs/ai-naver-dovastudio-summary>

API는, 이용자가 지정한 프로그램 내에서 입력을 받고 외부 서버에서 일정한 산출물을 생성하므로, 그 각 과정에 대한 적절한 법률적 검토가 없다면 차후 생성형 AI 이용에 따른 법률적 위험에 대한 대비가 제대로 될 수 없습니다. 이에, 아래에서는 기업이 생성형 AI API를 사용하는 경우 발생할 수 있는 법률 내지 책임 문제를 개관하겠습니다.

## 2. 생성형 AI API 사용 시의 법률 문제

생성형 AI API는 대체로 웹 API의 형태로 제공되며, 그에 따라 생성형 AI 사용 시 학습, 생성(생성 과정 및 산출물), 그리고 정보 보안의 측면에서 법률적인 문제가 발생할 수 있습니다.

### <학습 단계에서의 문제>

일반적으로 공개된 생성형 AI API는 백엔드(backend; 실제 정보가 처리되는 서버측)의 AI 모델에 대한 직접적인 접근을 허용하지 않으므로, AI 학습과 관련한 각종 분쟁이 직접적으로 문제될 여지는 적습니다. 다만, OpenAI는 일정한 요건을 충족한 이용자에 대하여 모델의 미세 조정(fine-tuning)을 위한 API를 제공하므로, 이 경우 학습 데이터의 수집·이용 시 발생할 수 있는 각종 저작권 침해, 개인정보 보호법 위반 등이 문제될 수 있습니다.

### <산출물 생성 단계에서의 문제>

산출물 생성 단계에서는 산출물이 여타 저작물과 유사하거나, 개인정보 등을 포함하여 타인의 권리를 침해하는 경우가 핵심적으로 문제됩니다. 이와 같은 생성 단계에서의 문제는 크게 학습 데이터에 의한 문제와, 입력 데이터에 의한 문제로 구별될 수 있습니다.

전자의 경우, 파운데이션 모델의 학습 과정이나 미세 조정 과정에서 이용 권한을 확보하지 못한 데이터를 무단으로 사용하거나, 동의 등 처리 요건을 충족하지 못한 개인정보가 학습 데이터에 포함되는 경우가 특히 문제됩니다. 다만, 파운데이션 모델의 학습이나 미세 조정 자체는 생성형 AI API를 제공하는 기업이 수행하는 경우가 일반적이므로 API를 사용하는 이용자나 기업이 해당 문제를 직접 관리하기는 어려울 것으로 보이고, 다만 이용자로서는 생성된 산출물이 타인의 권리(각종 지식재산권, 인격권, 개인정보 등) 내지 원 학습데이터의 라이선스(특히 오픈소스 라이선스 위반 등)를 침해하는 경우가 발생하지 않는지 여부를 검토하여 법률적 위험을 최소화할 필요가 있습니다. 참고로 OpenAI 등 일부 생성형 AI 사업자는 최근 이와 같은 문제를 인지하고 이른바 '저작권 방패' 등 정책을 도입하여 생성형 AI의 산출물로 인한 이용자의 면책을 제공하고 있습니다.<sup>5</sup>

한편, 생성형 AI API 이용 과정에서 이용자는 산출물 생성을 위하여 생성형 AI API의 호출 과정에서 텍스트, 이미지, 음성 등 데이터를 파라미터로 제공하게 되는데, 이때 이용자가 산출물 생성을 위해 타인의 권리를 침해하거나 이용권한을 얻지 못한 데이터를 입력하고, 그에 따라 생성된 산출물이 타인의 권리를 침해하는 경우를 상정하여 볼 수 있습니다. 이와 같은 경우 해당 데이터를 입력한 주체는 해당 권리 침해 등에 대하여 책임을 질 가능성이 존재하므로, 사전에 입력 데이터에 대한 검수절차를 마련할 필요가 있습니다.

<sup>5</sup> <https://www.etnews.com/20231108000274>

### <산출물의 권리 인정 문제>

생성형 AI API 등을 활용하여 일정한 산출물을 이용자가 생성케 한 경우 해당 산출물의 권리 귀속이 문제됩니다. 특히 저작권과 관련하여, 현행 저작권 법제 및 유관기관은 일정한 경우를 제외하면 어떠한 표현 행위에도 인간의 창작적 개입이 있었다고 볼 수 없는 AI 산출물에 대한 저작권 등록을 불허하고 있으므로 <sup>6</sup> AI를 활용한 산출물의 권리 보호를 위해서는 사람과 AI 작업의 구별 등 적절한 등록기관의 가이드를 따르되, 별도의 입법 등을 확인할 필요가 있습니다.

### <정보보안의 문제>

생성형 AI API가 온프레미스 환경(On-premise; 기업이 서버를 자체적으로 보유하고 직접 설치 및 운영)에서 구동되지 않는다면, 이용자는 생성형 AI API를 사용하는 과정에서 민감한 정보나 기밀 정보를 공개된 인터넷망을 통하여 전송할 수 있습니다. 이 경우 해당 정보가 위협행위자에 의하여 외부로 노출될 가능성이나, 차후 AI의 학습에 이용되어 간접적으로 다수의 이용자에게 유출될 가능성을 배제할 수 없으므로, 기업은 관련 정보의 보호를 위한 별도의 방안을 마련할 필요가 있습니다.

## 3. 시사점

최근 국내외 생성형 AI업체가 앞다투어 생성형 AI 모델의 API를 공개하며 이를 활용한 다양한 제3자 애플리케이션이 우후죽순 등장하고 있습니다. 이와 더불어 24%가 넘는 국내 기업은 생성형 AI를 이미 자사의 업무에 도입하였으며, 68%가 넘는 기업이 생성형 AI의 도입을 검토 중이거나 도입을 위한 준비를 진행 중인 것으로 조사되었습니다.<sup>7</sup> 특히, 생성형 AI API 서비스를 활용한 맞춤형 AI의 활용은 기업 맞춤형 AI를 제작할 수 있어 그 잠재력이 더욱 크므로 시간이 경과함에 따라 API를 이용한 업무사례의 확산은 점차 가속화될 것으로 보입니다.

다만 생성형 AI API를 활용한 서비스는 이상과 같은 일정한 법률적 리스크를 가지고 있으며, 특히 타인의 권리 침해에 따른 책임 문제 내지 보안 문제로부터 완전히 자유롭다고 보기 어렵습니다. 따라서 생성형 AI API를 통해 맞춤형 서비스를 구축하려는 기업은 관련된 지식재산권, 개인정보, 정보보안 등의 이슈를 선결적으로 파악하고 이에 대비할 필요가 있습니다.

화우의 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점)등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

## Contacts

### 이광욱

T. (+82) 2 6003 7535

파트너변호사

E. kwlee@yoonyang.com

### 이근우

T. (+82) 2 6003 7558

파트너변호사

E. klee@yoonyang.com

### 이수경

T. (+82) 2 6182 8132

파트너변호사

E. sgvi@yoonyang.com

### 배종우

T. (+82) 2 6182 8745

변호사

E. jwbai@yoonyang.com

---

<sup>6</sup> 한국저작권위원회, 「생성형 AI 저작권 안내서」(2023. 12), 41면.

<sup>7</sup> <https://www.samsungds.com/kr/insights/2023-ai-survey.html>