# ChatGPT의 개인정보 이슈와 딥시크(Deepseek)의 보안 이슈, 그 의미와 시사점

정진근
강원대학교 법학전문대학원 조교수
jkjeong@kangwon.ac.kr


## AI, 우리는 아직 잘 모른다

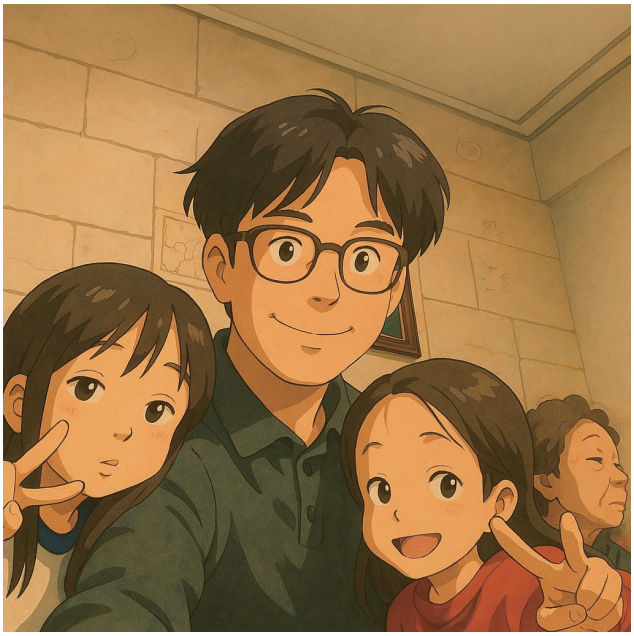
2016년 뉴럴 네트워크라는 인공신경망 기술로 무장한 알파고(AlphaGo)가 이세돌 9단과의 바둑 대국에서 승리했을 때만 하더라도, AI는 여전히 인간이 지시하는 일을 똑똑하게 처리하는 SW에 불과하다고 했다. 반면, 필자는 인공신경망 기술을 토대로 할 때 약인공지능과 강인공지능의 구별은 무의미하며, AI는 지속적이고 비약적인 발전을 거듭할 것이라고 예상했다. 대규모 언어 모델인 ChatGPT가 출현했을 때 사람들은 ChatGPT의 거짓말을 얘기했다. 반면, 필자는 언어 모델은 말 잇기 게임과 같은 것이므로 AI가 한 말의 진실은 중요하지 않으며, 얼마 지나지 않아 AI는 데이터를 토대로 진실을 이야기할 것이라고 예상했다.

데이터의 기억·인식 오류가 있는 인간에 비해 AI는 빠른 속도로 진실에 가까워지고 있으며, 추론 능력의 향상에 따라 훨씬 논리적인 결론에 도달하게 될 것이다. 그렇더라도 AI는 무엇인가를 '의욕'할 수는 없으므로 여전히 도구에 불과하다고 얘기한다. 반면, 필자는 그러한 가정에도 의문을 품는다. 이유 없이 폭력을 휘두르는 AI, 수년 동안의 업무에서 죽음으로라도 벗어나려는 듯 계단 아래로 뛰어드는 AI… 이러한 여러 사건들을 접하면서 인공신경망은 인간의 생각, 낙관과 비관, 우울과 기쁨까지 모방하는 것이 아니냐는 의문이 생긴다.

## 우리의 일상을 파고든 AI

AI가 무엇인지 제대로 알기도 전에 AI는 우리 일상에 깊숙이 파고들었다. 학생들의 리포트 작성에 AI가 이용되기 시작한 것은 이미 오래전의 일이다. 회사의 의사결정 과정에 AI의 응답은 이미 큰 역할을 하고 있다. 번역은 AI의 일이 되었다. 국제학술대회 자료 역시 AI를 이용하면 한 시간 내에 번역이 완료된다. 인간의 심리치료 영역에도 AI가 이용되고 있으며, 외로운 사람들이 AI와 대화하며 마음을 달래기 시작했다. 2022년 미드저니(Midjourney)로 생성한 이미지가 미국 콜로라도 주립 박람회 미술대회 디지털아트 분야의 우승을 차지해 화제가 되기도 했다. 『새벽의 자리야(Zarya of the Dawn)』라는 만화의 저작권 문제가 시비가 되기도 했다. 스테판 탈러(Stephan Thaler) 박사가 2018년 AI 다부스(DABUS)를 발명자로 명시해서 특허 출원한 사건으로 주요 국가들이 AI를 이용한 발명에 대해 논의하기 시작했다.

그림 1 - 필자의 사진을 이용하여 '지브리풍'으로 만든 그림



급기야 '지브리(Ghibli)' 열풍이 불었다. <이웃의 토토로>, <하울의 움직이는 성>, <센과 치히로의 행방불명>과 같은 우리에게 익숙한 지브리 스튜디오 애니메이션에 나오는 인물과 비슷하게 생긴 사람들이 프로필 화면에서 웃고 있다. 반면, 미야자키 하야오(Miyazaki Hayao)는 2023년 AI가 만든 애니메이션에 대해 "생명 그 자체의 모욕"이라고 말하며 강하게 비판한 바 있다.[1]

1 김민진(2025.05.), "지브리 스타일 이미지 만들어주는 'AI' 저작권 문제 없나?", 월간 Secu N, 81쪽

## ‘지브리’가 쏘아 올린 저작권 이슈

지브리 그림으로 제기되는 문제는 저작권과 관련이 있다. 주요 요지는 1) ‘풍’이나 ‘스타일’은 저작권으로 보호되지 않으므로 지브리풍 원작자의 저작권을 침해하는 것은 아니다. 2) 다만, 딥러닝(Deep-learning)을 위해 지브리풍 만화를 복제했을 테니 그 과정에서 저작권 침해 가능성이 있다는 것이다. 이와 관련된 일반적인 해석론은 다음과 같다.

> *오픈AI가 지난 3월 25일 출시한 신규 이미지 생성 AI 모델인 ChatGPT-4o 이미지 생성 기능을 이용해 만든 이 ‘지브리’의 이미지는 엄밀히 말하면 ‘지브리풍’의 이미지로, ‘저작권’의 영역을 살짝 비껴가고 있다. ‘화풍’에는 저작권이 없는 탓이다. 온 세상이 ‘지브리 천지’이지만 정작 저작권은 침해하지 않는다. AI가 화풍을 습득하기 위해서는 원본 그림을 ‘학습’해야 하는데, 오픈AI는 그림이 아니라 ‘텍스트’ 기반의 학습을 시켰다고 말하고 있으니, 원본이 학습되었다는 것을 증명하기도 어려워 보인다. ChatGPT-4o 이미지 생성 기능이 출시되자마자 지난해 말 기준 3억 5,000만 명 수준이던 ChatGPT의 주간 이용자 수는 5억 명을 넘어섰다.*[2]
>
> *AI가 지브리 스타일을 모방했을 뿐 작품을 모방한 것은 아니기 때문이다. 일각에서는 AI가 훈련, 학습하는 과정에서 지브리의 작품을 대가 없이 무단으로 활용했다면 침해 소지가 있지만 작품을 구매해서 학습시켰다면 저작권 침해가 아니라는 의견을 내놓기도 한다. 하지만 이 경우에도 최종적으로는 모방을 위한 구매이기에 위법이라는 이야기가 많다. 애초에 AI 모델에 학습시키려면 작품의 저작권자에게 허락과 동의를 받아야 한다는 것이다.*[3]

이러한 해석론은 법리 오해로 볼 수 있는 부분이 있다. 우선, ‘풍’이나 ‘스타일’은 저작물로 보호되지 않더라도, 그러한 ‘풍’이나 ‘스타일’을 표현함으로써 지브리풍 만화의 캐릭터 등과 실질적으로 유사한 그림이 나왔다면 저작권 침해가 될 수 있다. 그러한 사례는 매우 많을 것으로 예상된다. 다음으로, 딥러닝을 위한 저작물 복제를 저작권 침해로 볼 수 있는지는 여전히 불분명하다. 비록, 미국에서 최근 딥러닝을 위한 데이터 복제가 공정이용에 해당하지 않는다는 하급심 판결[4]이 나왔지만, 일본과 유럽 국가들은 성문으로 공정이용을 인정하는 법 규정을 두고 있다. 미국에서 최소한 연방순회항소법원 판결이 나오기 전에는 판례에 대한 논쟁 역시 계속될 것이다.

2 박정미(2025.05.), “AI열풍의 그림자 - 지브리 열풍이 불러온 진짜 ‘열풍’”, 월간환경, 72~73쪽

3 김민진(2025.05.), “지브리 스타일 이미지 만들어주는 ‘AI’ 저작권 문제 없나?”, 월간 Secu N, 81쪽

4 THOMSON REUTERS ENTERPRISE CENTRE GMBH v. ROSS INTELLIGENCE INC(2025), United States District Court, D. Delaware. Docket No: No. 1:20-cv-613-SB, Decided: February 11, 2025

## '지브리'가 쏘아 올린 진짜 이슈는 개인정보

이처럼 지브리의 이슈는 저작권 이슈뿐일까? 필자는 개인정보가 진짜 이슈라고 생각한다. 개인정보란 개인을 알아볼 수 있는 정보 또는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 말한다(개인정보 보호법 제2조 제1호). 그중 가장 중요한 개인정보 중 하나가 얼굴 사진이다. 개인의 식별 데이터로써 얼굴 사진은 매우 중요하다. AI가 학습하는 데 가장 어려움을 느끼는 것이 사진을 식별하는 것이다. AI가 수학 계산에 능통하기는 쉬워도 고양이와 개를 구별하는 것은 어렵다. 더 나아가 사진 데이터는 구하기도 어렵거니와 그 값도 비싸다. AI 플랫폼들이 늘 아쉬워하는 것이 사진 데이터이다.

그런데, 지브리 열풍으로 오픈AI는 수십억 명의 얼굴 사진을 갖게 되었다. 다만, 얼굴 사진을 저장해 놓지는 않았을 것이라고 예상한다. 동의 없이 얼굴 사진을 저장하는 것 그 자체가 개인정보 보호법제를 위반할 가능성이 크기 때문이다. 그렇더라도 오픈AI의 ChatGPT는 얼굴 사진에 관하여 최고의 전문 AI가 되었다. 수십억 건의 얼굴 사진을 학습했기 때문이다. 얼굴 사진을 텍스트로 묘사하여 저장해서 개인정보의 문제를 회피하고 있을 수도 있다.

언론 기사를 보면, 오픈AI 샘 올트먼(Sam Altman) CEO는 "그래픽 처리장치(GPU)가 녹아내리고 있다"고 한다. 실제로 GPU가 녹아내리지는 않았겠지만, 그만큼 많은 이용자들이 ChatGPT를 이용하고 있음을 의미한다. 아마도 GPU가 녹아내리는 것을 보면서 샘 올트먼 CEO는 쾌재를 부르고 있을지 모르겠다.

전 세계의 우리 모두의 얼굴이 ChatGPT에 의해 학습되었다. 이 얼굴들은 접속 경로, SNS 프로필 사진, 이런 것들과 결합하여 개인의 식별 도구로 쓰이지는 않을까? 개인의 식별 도구로까지 쓰이지는 않더라도 AI 플랫폼의 경쟁력 향상을 위한 도구로 쓰이는 것은 분명해 보인다.

## 딥시크의 출현

딥시크의 출현을 '스푸트니크 모멘트(Sputnik Moment)'라고 한다. 기술 우위를 자신하던 미국이 소련의 인공위성에 놀란 일을 가리킨다. 딥시크는 중국의 AI 기술 수준이 미국 못지않다는 점을 보여주기도 했고, 더 나아가 개발비가 턱없이 저렴하다는 점을 보여줌으로써, 서방을 두 번 놀라게 했다.

딥시크-V3를 발전시킨 딥시크-R1은 일부 성능 테스트에서 오픈AI가 지난해 9월 출시한 추론 AI 모델 'o1'보다 앞선 것으로 나타나 충격을 주었는데, 딥시크 보고서에 따르면 미국 수학경시대회인 'AIME 2024 벤치마크 테스트'에서 R1은 정답률 79.8%를 얻어 o1의 79.2%를 앞섰고, 코딩 부문 라이브벤치 평가

결과에서 R1은 65.9%의 정확도를 기록해 o1(63.4%)보다 높은 성적을 기록했다고 한다.[5] 한편, 딥시크-V3의 경우 개발에 557만 6,000달러(약 80억 원)가 투입됐는데, 이는 메타가 AI 모델인 '라마 3(Llama 3)' 개발에 사용한 비용의 10분의 1 수준이다.[6]

기술적으로 보면, 딥시크는 통상적으로 숫자를 소수점 32자리까지 기록하는 기존 방법을 버리고 소수점 8자리로 기록해 메모리 사용량을 4분의 1로 줄이고, 단어를 하나씩 읽는 방식을 버리고 문장을 한 번에 처리하는 방법을 도입했다고 하며, 모든 정보를 한 모델이 처리하는 방식 대신 필요에 따라 전문가 시스템을 호출하는 방식으로 설계했다고 한다. 또한 전체 6,710억 개의 매개변수를 어떤 순간에 다 활성화시키지 않고 20분의 1인 약 340억 개만 활성화함으로써 추론 비용과 메모리 사용량을 줄이면서도 높은 성능을 유지하는 방법을 사용하고 있다고 한다.[7]

이런 딥시크를 바라보는 우리와 서방 국가들의 심사는 매우 복잡해 보인다. 우선, AI 모델인 딥시크-R1과 딥시크-V3 수준의 성능을 국내에서 재현하기는 어려울 것으로 분석되고 있는데, 딥시크 구현에는 약 2,000개의 엔비디아 GPU H800이 사용됐다고 알려진 한편, 딥시크 개발사인 하이플라이어(High-Flyer)만큼 GPU 클러스터를 확보한 국내 기관 자체가 존재하지 않는다는 우려가 제기되고 있다.[8] 또한, 그만큼의 GPU 클러스터를 확보했다고 하더라도 딥시크의 딥러닝 과정은 여전히 베일에 싸여 있으며, 딥시크의 개발 비용은 고급 기술자 인건비가 비싼 서방 국가에서는 넘을 수 없는 벽이다. AI의 핵심은 SW보다 딥러닝과 HW에 있음은 이미 짐작이 간다.

## 딥시크의 보안 이슈, 명(明)과 암(暗)

딥시크와 관련된 가장 큰 우려는 개인정보 또는 산업기밀 등이 중국으로 유출된다는 것이다. 아래 기사는 이러한 우려를 제기하고 있는 예이다.

> *중국 인공지능(AI) 스타트업 딥시크(DeepSeek)의 데이터베이스가 노출되며 100만 건 이상의 사용자 데이터가 유출됐을 가능성이 제기됐다. 노출된 정보는 클릭하우스(ClickHouse)라는 오픈소스 데이터 관리 시스템에 저장됐으며 이 정보에는 API 인증 키, 시스템 등 100만 개가 넘는 로그가 포함됐다. 이에 업계 관계자들은 오픈소스 기반 AI 모델의 보안 취약성을 지적했으며 실제로 미국 의회와 국방부 등 정부기관에서도 속속*

5 서재창(2025.03.), "'딥시크 충격' 이후 한 달, AI 생태계 변화 얼마나 이뤄냈나", 전자기술, 42쪽
6 양승갑(2025.05.), "샘 알트먼 '딥시크 모델, 가격 대비 성능 면에서 인상적'", Embeded, 29쪽
7 이경전(2025.04.), "모두를 위한 AI... 전환점 만든 딥시크", 한경MONEY, 43쪽
8 양승갑(2025.03.), "'가성비' 딥시크, 기술 리포트 공개했지만… 국내선 구현 어려워", Embeded, 34~35쪽

*딥시크 차단에 나섰다. 폐쇄형인 오픈AI와 달리 딥시크의 R1 모델은 누구나 접근 가능한 상태로 소스 코드 등을 확인하고 미세조정을 통해 성능을 극대화할 수 있었다. 이런 장점에 많은 개발자들의 환영을 받으며 딥시크는 빠른 속도로 성능 개량을 달성했다. 그러나 이런 딥시크의 개방성이 금번 사태에서는 고스란히 문제점으로 드러난 것이다. 업계 관계자는 "일부 오픈소스 대규모 언어 모델은 다른 서비스와 연결할 수 있도록 API라는 기능을 제공한다. 기업이 자체적으로 생성형 AI 시스템을 만들더라도 이 시스템은 오픈소스 대규모 언어 모델이 설치된 클라우드 서버와 연결될 수 있다"고 설명했다. 특히 "이런 방식은 결국 외부 서비스와 연결되는 것과 같기 때문에 기업의 중요한 정보가 외부로 유출될 위험이 있다는 우려가 있다"고 강조했다.*[9]

그러나 이러한 문제 제기에는 일부 오해가 있다. 오픈소스 모델은 소스 코드가 공개되어 있기 때문에 용이하게 스파이 기능 또는 트로이의 목마 기능을 캐치할 수 있다. 설령 다른 서비스와 연결할 수 있는 API 기능을 가지고 있다면 이를 제거한 후 이용하면 된다. 딥시크가 공개한 오픈소스는 MIT 라이선스 모델을 채택하고 있기 때문에 이를 제거하고 이용하는 데 아무런 걸림돌이 없기 때문이다.

그림 2 - 딥시크 라이선스 내용(ChatGPT를 이용해 생성)

| 항목 | 필수 여부 | 비고 |
|---|---|---|
| 라이선스 사본 제공 | ✅ 예 | 파생 모델 배포 시 |
| 저작권 고지 유지 | ✅ 예 | 원작자 표시 필요 |
| 수정 사항 명시 | ✅ 예 | 모델 변경 시 |
| 파생 모델 오픈소스 공개 | ❌ 아니요 | 자유 선택 가능 |
| DeepSeek 라이선스 그대로 유지 | ❌ 아니요 | 단, 사용 제한 조건은 유지 필수 |

이와 같이, 딥시크는 AI 전문가 모델 간의 통신에 있어 처리량을 높이고 대기 시간을 줄이는 라이브러리를 공개하고, AI 모델의 학습과 추론에 필수적인 일반 행렬 곱셈의 정확성과 효율성을 높이기 위한 라이브러리를 공개했다. 또한 AI 학습 및 추론 부하를 조절하는 고성능 분산 파일 시스템 등 딥시크 AI

9 양유진(2025.05.), "'성능 좋아도 불안해서 못써요', 딥시크 오픈소스AI 한계 드러나나?", 월간 Secu N, 66쪽

모델 훈련의 핵심인 컴퓨팅과 통신, 스토리지 등에서 하드웨어의 성능을 어떻게 극대화했는지를 자세하게 공개했다고 하면서, 딥시크가 진정한 오픈AI가 되고 있다고 보는 설명도 찾아볼 수 있다.[10]

그럼에도 불구하고, 딥시크의 모든 소스 코드가 공개된 것은 아니다. 공개되지 않은 소스 코드가 존재한다면, 어떠한 추가적인 작업이 이루어질 것인지는 아무도 알 수 없게 된다. 딥시크는 시스템의 전체 구조와 재현 방법이 공개되지 않고, 부하 분산 방법이나 분산 메모리 시스템과 같은 핵심 구성 요소는 여전히 불투명해서 전체적인 검증이 불가능해지고, 진정한 오픈소스 투명성에 못 미쳤다는 평가도 있고, 인프라와 모델 가중치는 공개했지만 데이터와 학습 과정에 대한 것은 거의 알리지 않았다는 지적도 있다. 그런 이유로 겉으로는 오픈소스를 표방하지만, 실제로는 중요한 부분을 비공개로 숨기는 이른바 '오픈 워싱(Open-washing)'이라고까지 박한 평가를 당하기도 하지만, 다른 AI-플랫폼들 역시 소스 코드와 데이터를 충분히 공개하지 않는 것은 마찬가지이다. 상대적으로 딥시크는 그 공개의 범위가 더 넓다고 본다.[11]

이런 점을 종합적으로 고려할 때, 딥시크가 보안의 문제에서 우려스럽다는 주장은 딥시크가 오픈소스라는 점에서 오히려 반론 제기가 가능하다고 판단된다. 그렇다면, 딥시크가 오픈소스임에도 불구하고 보안 문제에서 자유롭지 않은 이유는 무엇인가? 그 이유는 딥시크 역시 AI-플랫폼이며, AI-플랫폼은 오픈소스 외에 비밀소스를 포함하는 것이 가능하고, AI-플랫폼 자체는 블랙박스(Black Box)가 되어 입력되는 정보가 무엇인지, 이들 정보가 저장되어 어떻게 이용되는지 알 수가 없다는 것이다. 클라우드 컴퓨팅은 이를 더욱 알기 어렵게 하였고, 인공신경망 기술로 이제 이 모든 것을 아는 것은 불가능해졌다.

## 맺으면서

ChatGPT의 지브리 열풍과 딥시크의 보안 우려를 보면, 그 본질은 모두 개인정보 유출 등 보안 이슈로 평가될 수 있다. 그럼에도 불구하고, 지브리 열풍은 이용자들의 환호를 받고 있는 반면, 딥시크는 근거가 충분히 제시되고 있지 않는 가운데 이용자들의 눈총을 받고 있는 상황이다. 이런 상황에서 우리는 AI-플랫폼이 가져올 수 있는 개인정보와 보안 이슈에 대해 정확하게 인식하고, 그 대책을 마련하기 위한 노력을 경주해야 한다.

AI-플랫폼의 특징은 이용자가 제공한 개인정보 또는 산업기밀을 저장하는지 여부를 이용자가 알 수 없으며, 설령 그 정보나 기밀을 저장하지 않더라도 딥러닝을 통해 AI의 인공신경망은 저장한 것이나 다를 바 없게 된다는 점이다. 이러한 점에서 신뢰할 수 있는 AI-플랫폼 개발이 필요하다. 예를 들어 삼성은 삼성의 AI-

10 이경전(2025.04.), "모두를 위한 AI... 전환점 만든 딥시크", 한경MONEY, 43쪽

11 본절은 이경전(2025.04.), "모두를 위한 AI... 전환점 만든 딥시크", 한경MONEY, 44쪽을 참조하여 보완한 것임

플랫폼을 가지고 경쟁력 강화를 꿈꾸어야 하며, LG는 LG의 AI-플랫폼을 가지고 경쟁력을 다져야 한다. 삼성전자가 애플의 AI-플랫폼을 이용하여 가전제품 기술을 향상 및 발전시킨다면, 결국 삼성전자의 산업 기밀은 애플로 유출되는 결과가 생긴다. 우리 기업들의 AI-플랫폼 구축에 딥시크 등에서 제공하는 오픈 소스를 활용하는 것은 개발 기간의 감축은 물론이거니와 진보적인 기술의 수용이라는 점에서 매우 중요하다.

한국의 AI 전략으로서 폐쇄 AI 전략과 오픈소스 AI 전략을 융합하는 '연합 AI 전략'을 채택해야 하며, 연합 학습을 통해 개별 기관이 데이터를 외부에 노출하지 않고도 독립적으로 AI 모델을 학습한 뒤, 이들 모델을 결합해 강력한 통합 모델을 구축하는 방식이 마련되어야 한다[12]는 의견은 이러한 관점에서 의미가 있다고 평가될 수 있다.

결국, AI의 경쟁력이 산업의 경쟁력이 될 것이며, AI를 도구로 활용하지 않는 산업은 도태될 수밖에 없다. 이때 AI 경쟁력은 딥러닝에서 결정되는데, 독과점을 형성한 AI-플랫폼은 자발적인 이용자들에 의해 딥러닝을 위한 데이터를 충분히 공급받게 되고, 이는 다시 독과점을 형성한 AI-플랫폼의 지능을 향상시켜 독과점이 강화될 것이다. 이와 같이, AI-플랫폼 개발 및 활용의 시장은 개별 기업들이 참여해야 하는 전장(戰場)이다.

**참고문헌**


- 김민진(2025.05.), "지브리 스타일 이미지 만들어주는 'AI' 저작권 문제 없나?", 월간 Secu N
- 박정미(2025.05.), "AI열풍의 그림자 - 지브리 열풍이 불러온 진짜 '열풍'", 월간환경
- 서재창(2025.03.), "'딥시크 충격' 이후 한 달, AI 생태계 변화 얼마나 이뤄냈나", 전자기술
- 양승갑(2025.05.), "샘 알트먼 "딥시크 모델, 가격 대비 성능 면에서 인상적"", Embeded
- 양유진(2025.05.), "'성능 좋아도 불안해서 못써요', 딥시크 오픈소스AI 한계 드러나나?", 월간 Secu N
- 이경전(2025.04.), "모두를 위한 AI... 전환점 만든 딥시크", 한경MONEY
- THOMSON REUTERS ENTERPRISE CENTRE GMBH v. ROSS INTELLIGENCE INC(2025), United States District Court, D. Delaware. Docket No: No. 1:20-cv-613-SB, Decided: February 11, 2025


12 이경전(2025.04.), "모두를 위한 AI... 전환점 만든 딥시크", 한경MONEY, 47쪽