법무법인(유) 린

Tech Legal Insights

A.P.T. – Legal Tech Team ***2026. 09.***

기업 내 생성형 AI 사용과 비밀정보 보호

생성형 AI가 기업의 일상적인 업무도구로 자리 잡으면서 새로운 법적 문제가 등장하고 있습니다. 임직원이 법무팀이나 외부 변호사의 지시 없이 계약상 분쟁, 내부조사, 규제위반 가능성 등 민감한 법률문제와 관련된 정보를 생성형 AI에 입력하는 경우, 어떠한 법적 문제가 발생할 우려가 있을까요?

이와 관련하여 참고가 될 수 있는 미국 판례를 소개하면서, 사내 생성형 AI 가이드라인의 제정 및 검토의 필요성에 대해서 논의하고자 합니다.

1. *United States v. Heppner* 사건

2026년 2월 10일 미국 뉴욕남부연방지방법원은 United States v. Heppner 사건에서 피고인이 생성형 AI와 주고받은 대화를 기록한 문서는 변호사-의뢰인 간 비밀유지권(ACP)이나 work-product doctrine(소송준비자료 보호 법리)에 따라 보호할 수 없다는 구두 결정을 내리고, 2026년 2월 17일 그 이유를 설시한 서면 결정문(Memorandum)을 공개했습니다.[1)]

해당 사건에서 피고인은 이미 대배심 소환장을 받고 자신이 수사대상임을 인식한 상태에서, 공개형 생성형 AI를 이용하여 예상되는 혐의와 방어전략 등에 관한 자료를 작성했습니다. 피고인의 주장에 따르면 일부 입력정보에는 변호사로부터 전달받은 내용도 포함되어 있었으며, 피고인은 AI를 이용하여 작성한 자료를 이후 변호사에게 공유했습니다. 이 자료(약 31건의 문서)는 디스커버리가 아닌 2025년 피고인 체포 당시 FBI가 압수수색을 하는 과정에서 압수되었고, 피고인은 이에 대해 비밀유지권과 work-product 법리를 주장했습니다.

Contact

구태언 변호사
T. 02-3477-8695
E. tekoo@law-lin.com

이상강 변호사
T. 02-3477-8695
E. sangkang.lee@law-lin.com

1) https://www.akingump.com/a/web/ssTGsd5NHbtZ1onzXQMTye/1_25-cr-503-27-memorandum.pdf

그러나 중요한 사실이 하나 있었습니다. 변호사가 피고인에게 생성형 AI를 사용하도록 지시한 사실이 없었다는 점입니다. 법원은 먼저 생성형 AI와 피고인 사이의 대화 자체는 변호사와 의뢰인 사이의 의사소통이 아니라고 판단했습니다. 또한 AI 사업자의 개인정보처리방침이 이용자의 입력 및 출력 정보를 수집해 모델 학습에 이용하고 정부 규제기관을 포함한 제3자에게 제공할 수 있다고 명시하고 있는 점을 고려할 때, 입력정보의 비밀성이 유지된다고 합리적으로 기대하기 어렵다고 보았습니다. 또한 해당 AI가 자신은 공식적인 법률자문을 제공할 수 없다는 점을 스스로 밝히고 있어 AI로부터 법률자문을 받으려는 목적이었다는 것도 인정되지 않았습니다. 아울러 법원은, 피고인이 변호사로부터 전달받아 AI에 입력한 정보 자체가 비밀유지권의 대상이었다고 하더라도, 이를 제3자인 AI 및 AI 사업자와 공유한 것은 비밀유지권을 포기한 것이라고 보았습니다.[2)]

특히 주목할 부분은 피고인이 AI를 이용하여 만든 자료를 나중에 변호사에게 공유했다는 사정만으로 기존 AI 대화에 소급하여 비밀유지권이 부여되는 것은 아니라고 판단한 점입니다. work-product 법리에 관해서도, 법원은 해당 자료가 소송을 대비해 작성된 것이라고 가정하더라도 변호사가 작성하거나 변호사의 요청에 따라 작성된 것이 아니고, 변호인의 전략을 반영한 것도 아니므로 보호 대상이 아니라고 보았습니다. 위 판례는 기업 임직원이 법무팀이나 외부 변호사에게 문의하기 전에 외부 생성형 AI에 내부 기밀이나 법률문제, 구체적인 사실관계를 입력한 경우에 발생할 수 있는 문제점을 시사하고 있습니다.

다만, Heppner 결정은 변호인이 있는 형사 피고인이 변호인의 지시 없이 AI를 이용한 사안에서 비밀유지권에 대한 판단을 한 것이므로, AI를 이용하여 작성한 자료가 어떠한 경우에도 보호되지 않는다는 의미로 확대 해석해서는 안 됩니다. 실제로 같은 시기에 한 민사 사건에서는 변호사 없이 소송을 수행한 원고가 공개형 생성형 AI를 이용하여 작성한 자료에 work-product 법리에 따른 보호가 부여될 수 있고, AI를 사용했다는 사정만으로 그 보호가 포기되는 것은 아니라는 취지의 결정이 내려지기도 했습니다.[3)] 이처럼 생성형 AI 사용에 따른 법적 보호 여부는 문제되는 법리와 절차, 당사자의 지위 등에 따라 판단이 달라질 수 있다는 점에 유의할 필요가 있습니다.

2. 시사점 – 업무수행 중 생성형 AI의 남용 가능성

먼저, 임직원이 법무팀 등 관련 부서 또는 외부 변호사에게 법률검토를 의뢰하기에 앞서서 다음과 같은 질문을 공개형 생성형 AI에 입력하는 상황을 생각해 볼 수 있습니다.

2) 이 사건의 피고인은 개인입니다. 기업의 경우 비밀유지권의 주체는 회사이므로, 임직원이 변호사의 자문 내용을 AI에 입력한 사정만으로 회사가 비밀유지권을 포기한 것으로 볼 수 있는지는 별도의 쟁점이 될 수 있습니다.
3) Warner v. Gilbarco, Inc., E.D. Mich. 2026. 2. 10., https://law.justia.com/cases/federal/district-courts/michigan/miedce/2:2024cv12333/379552/94/

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

- "(계약서 파일을 첨부하며)거래처와 체결한 계약을 일방적으로 해지할 수 있는가?"
- "회사 직원의 이러한 행위가 뇌물죄에 해당할 수 있는가?"
- "퇴직한 직원이 회사 자료를 가지고 경쟁사로 이직했는데 영업비밀 침해 주장으로 대응할 수 있는가?"
- "개인정보 유출 사고가 발생했는데 회사는 어떠한 조치를 취해야 하는가?"
- "정부기관으로부터 자료제출 요구를 받았는데 어떻게 대응해야 하는가?"

문제는 이러한 질문을 위해 실제 계약내용, 이메일, 내부보고서, 거래정보 또는 관계자의 개인정보, 소송자료까지 외부 AI 솔루션에 입력될 가능성이 있다는 점입니다. 향후 구체적인 사안에 관하여 법무팀이나 로펌이 후속적으로 관여하게 되더라도, 이미 외부 AI 솔루션에 기업의 내부 정보가 전달된 상태이므로, 해당 기록이 나중에 변호사에게 전달되었다는 이유만으로는 디스커버리나 수사기관의 압수 · 수색 등의 절차에서 법적으로 보호를 받지 못하는 상황이 발생할 수 있습니다.

이는 글로벌 기업 입장에서는 즉각적으로 발생할 우려가 있는 리스크에 해당한다고 볼 수 있으며, 국내 기업의 경우에도 내부 기밀정보가 외부 AI 솔루션에 노출되는 상황 자체는 정보보안, 개인정보보호, 영업비밀 보호(비밀관리성), 역외 분쟁 대응 등 다양한 영역에서 문제가 될 우려가 있습니다. 특히 국내에서도 개정 변호사법(2027년 2월 20일 시행) 제26조의2는 변호사와 의뢰인 사이에서 법률 조력을 목적으로 이루어진 '비밀인' 의사교환 내용을 공개하지 않을 수 있는 권리를 규정하고 있는데, 비밀성이 보호 요건으로 규정되어 있는 만큼 외부 AI에 입력한 정보에 대한 비밀유지권의 인정 여부가 쟁점이 될 가능성을 배제하기 어려워 보입니다.

위와 같은 우려가 있다고 하더라도, 생성형 AI의 업무상 활용을 원천적으로 금지하는 것은 실무적 관점에서 타당하지 않습니다. 따라서, 기업의 생성형 AI 정책은 단순히 "기밀정보를 AI에 입력하지 말 것"이라는 원칙을 넘어, 내부 정보보안 등이 확실한 기업용 AI를 도입하고, 일정한 법률적 위험이 감지되는 경우 AI를 사용하기 전에 법무팀에 먼저 문의하도록 하는 가이드라인을 도입할 필요가 있습니다. 이어지는 내용에서는 이를 고려한 AI 사용 가이드라인 구축에 대해서 살펴보고자 합니다.

3. 생성형 AI 사용 가이드라인 구축

먼저, 기업은 내부 데이터 보안 등이 검증된 기업용 AI를 도입함으로써, 임직원이 기밀정보를 범용 생성형 AI 솔루션에 입력하는 등의 남용행위를 하지 않도록 관리할 수 있습니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

그리고 내부적으로 기업용 AI를 도입할 때에는 최소한 다음과 같은 사항을 검토할 필요가 있습니다.

(1) 입력정보의 AI 학습 이용 여부

기업이 입력한 prompt와 자료가 모델의 학습이나 서비스 개선에 이용되는지 확인할 필요가 있습니다.

(2) 데이터 보관정책

입력 및 출력정보가 얼마 동안 보관되는지, 기업이 보관기간을 제한하거나 삭제할 수 있는지 확인해야 합니다.

(3) 접근권한 및 제3자 제공

AI 사업자의 임직원 등이 기업 데이터에 접근할 수 있는지, 어떠한 경우에 제3자 또는 정부기관에 정보가 제공될 수 있는지 검토할 필요가 있습니다.

(4) 개인정보 및 국외이전

AI 서비스의 서버 및 데이터 처리구조에 따라 개인정보의 제3자 제공이나 국외이전 규제가 문제될 수 있습니다.

(5) 계약상 보장 및 대화기록 보존 · 제출 대응

개인정보처리방침이나 일반 약관이 아닌 기업용 계약(데이터처리계약 등)을 통해 학습 이용 금지, 제3자 제공 제한 등이 보장되는지 확인할 필요가 있습니다.

위 사항에 대하여 충분한 검토를 거쳐 기업용 AI를 도입한 경우에도, 보안 등의 관점에서의 AI 솔루션에 대한 점검, 임직원의 오남용 방지 등에 대해서는 사내의 AI 거버넌스 관리 체계를 통해 계속적으로 관리가 이루어져야 합니다.

한편, United States v. Heppner 결정에서 주목할 또 하나의 사실은 법원이 피고인의 AI 사용이 변호사의 지시에 따른 것이 아니었다는 점을 중요하게 고려하였다는 것입니다. 다만, 법원은 변호사의 지시가 있었다면 달리 볼 여지가 있었다고만 언급했을 뿐이므로, 변호사의 지시만으로 법적 보호가 보장되는 것이 아니라 비밀성 등 다른 요건도 함께 갖추어야 한다는 점에 유의해야 합니다.

기업에서는 이를 고려하여 AI 사용을 업무의 위험도에 따라 구분하는 방법도 생각할 수 있습니다.
일상적인 번역, 문서작성 및 아이디어 도출 등은 승인된 AI 솔루션을 자유롭게 사용하도록 하는 것을 원칙으로 하되, 계약 체결, 소송 또는 분쟁, 조사 업무, 개인정보 관리, 컴플라이언스 관련 업무 등에 있어서는 법무팀에 우선적으로 보고하여 지원 요청을 하도록 하거나, 법무팀의 관리영역 내에서만 생성형 AI가 활용될 수 있도록 하는 체계를 설계할 수 있습니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

그리고 생성형 AI를 법무에 활용하는 경우에는 누가 AI 사용을 하였는지, 어떠한 목적으로 사용하였는지, 법무팀 또는 외부 변호사의 지시에 따른 것인지, 어떠한 시스템을 이용하였는지 등을 기록·관리하는 것이 향후 법적 보호 여부를 판단하는 데에도 도움이 될 수 있습니다.

4. 결론

2026년 2월 내려진 United States v. Heppner 결정은 생성형 AI 사용 자체가 법적 보호의 인정 여부를 결정하는 것이 아니라, AI 사용의 목적과 방식, 변호사의 관여, 정보의 비밀성 및 제3자에 대한 공개 가능성 등 구체적인 사정이 중요할 수 있음을 보여줍니다.

따라서, 기업의 대응 역시 생성형 AI를 전면적으로 금지하는 것보다는 업무와 정보의 위험도에 따라 사용 가능한 AI 환경과 절차를 구분하고, 특히 소송, 조사, 컴플라이언스와 같은 업무영역에서는 법무팀이 임직원의 AI 사용을 사전에 통제하고 관리할 수 있는 체계를 구축하는 방향으로 발전시켜 나갈 필요가 있습니다.

***

법무법인(유) 린 APT(AI, Platform, Technology) 그룹 리걸테크팀은 국내 기업들의 규제 이슈에
전략적인 원스톱(One-Stop) 토탈 솔루션(Total Solution)을 제공하고 있습니다.
상기 내용에 대해 문의사항이 있으시면 언제든지
법무법인(유) 린 APT(AI, Platform, Technology) 그룹 구태언 팀장 (tekoo@law-lin.com),
이상강 변호사(sangkang.lee@law-lin.com)에게 문의해 주시기 바랍니다.

서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com