

<韓国>



商用 AI 特許は出願しない？

善英 IP グループ
所長
金 起文

顧客から呼ばれてゼミに行って「商用 AI を営業秘密のみで保護しようとする危険性」について話すチャンスがあり、そこで語らせることの一部をまとめて申し上げる。

人工知能を商業目的に使用する発明は、一般ソフトウェア特許とは異なる固有の特性を持ち、ノウハウ（営業秘密）単独での保護が特に危険である。

第一に、学習済みモデルやパラメータは成果物として流出する。商用 AI は API やアプリ形態で市場に配布され収益を得るが、配布されたモデルは知識蒸留やモデル抽出攻撃、大量クエリによる応答複製により、競合他社が同等性能の代替モデルを再現しうる。商用化そのものがノウハウの流出経路となり、秘密管理要件とサービス提供が根本的に衝突する。

第二に、出力や挙動が外部に露出し、独立再現が容易である。競合他社は推薦結果や生成物などの出力を観察・収集し、同一機能のモデルを独自に学習させうる。ノウハウ保護はこれを防げない一方、この観察可能性はむしろ特許侵害立証の有利な根拠となる。商用化された AI ほど、出力段階に合わせて請求項を設計すれば侵害検知が容易になるという逆説が成立する。

第三に、規制上の説明義務が秘密保持と相反する。医療・金融・信用評価など高リスク領域の AI は、アルゴリズム説明義務や偏向監査など透明性要求を受ける（EU AI Act 等）。規制対応の過程で中核ロジックを開示せざるを得ず、ノウハウのみで管理していた技術は保護根拠を失う。特許はこうした開示状況でも権利が維持される。

結論として、AI を商業的に活用するとは、モデル・出力・インターフェースを市場に露出させることであり、これは営業秘密保護の前提である秘密性管理と正面から相反する。商用化水準が高いほどノウハウ単独保護の脆弱性は増し、同時に特許侵害立証は容易になる。したがって商用 AI 発明は特許による権利化を原則とし、市場に露出しない学習手法のみを補充的に営業秘密として管理する二元化戦略が妥当である。

< Korea >

Should Commercial AI Inventions Go Unpatented?

Sunyoung International Patent & Law Firm
President

Kevin, Kim

A client invited me to speak at a seminar on the risks of protecting commercial AI solely through trade secrets. The following summarizes the points I intend to make.

Commercial AI inventions differ from conventional software inventions, making reliance on know-how (trade secrets) alone particularly risky.

First, trained models and parameters may leak through the products or services in which they are deployed. Commercial AI earns revenue through APIs or applications, but competitors may reproduce substitute models with equivalent performance through knowledge distillation, model-extraction attacks, or response cloning using high-volume queries. Commercialization itself thus becomes a channel for leaking know-how, creating a conflict between maintaining secrecy and providing AI services.

Second, observable outputs and behavior make independent replication easier. Competitors can collect recommendations, generated content, and other outputs, then train a model with the same functions. Trade-secret protection cannot prevent this. Yet such observability may help prove patent infringement. Paradoxically, the more extensively an AI system is commercialized, the easier infringement may be to detect if the claims cover conduct observable at the output stage.

Third, regulatory duties of explanation may conflict with confidentiality. AI used in high-risk fields such as healthcare, finance, and credit assessment faces transparency requirements, including algorithmic explanations and bias audits (under the EU AI Act, for example). Compliance may require disclosure of core logic, undermining protection based solely on know-how. Patent rights, by contrast, remain enforceable despite such disclosure.

In conclusion, commercial AI exposes models, outputs, and interfaces to the market, directly conflicting with the secrecy required for trade-secret protection. As commercialization increases, know-how-only protection becomes more vulnerable while patent infringement becomes easier to prove. Commercial AI inventions should therefore, as a rule, be patented, with only non-public training methods retained as trade secrets under a complementary dual-protection strategy.

(Translated by TIIP)