



**< kahn
> pedersen**

Fredrik Sandström, Hanna Bogsjö Österberg
och Staffan Malmgren

Är företagshemligheter på väg att bli mjukvarans viktigaste skydd?

Den svenska patent- och marknadsöverdomstolen (PMÖD) meddelade den 10 juni 2026 dom i ett mål om skyddet för källkod. Bakgrunden var en relativt klassisk avhopparsituation. Tidigare anställda på mjukvarubolaget Phenixid hoppade av och startade ett nytt bolag, Fortifiedid. Efter att Fortifiedid lanserat en konkurrerande lösning gjorde Phenixid gällande att den utvecklats med hjälp av Phenixids källkod, och väckte efter en inträngsundersökning talan på två grunder: dels upphovsrättsintrång, dels angrepp på företagshemligheter.

I upphovsrättsdelen lämnades talan utan bifall. Phenixid gav in ett urval av sin källkod utan att redovisa vare sig urvalskriterierna eller hur delarna förhöll sig till varandra och till mjukvaran i dess helhet. Vilket datorprogram källkoden hörde till, och om det handlade om ett skyddat verk eller flera, gick enligt domstolen inte att avgöra. Källkoden som helhet kunde därmed inte identifieras som ett verk, och under alla förhållanden ansåg domstolen att det inte var visat att valet, dispositionen och kombinationen av beståndsdelar gav uttryck för sådana kreativa val som krävs. Prövningen tvingades därför ned till att bedöma de enskilda källkodsfilerna för sig. Phenixids bevisning tog emellertid sikte på kod-

basen som helhet och räckte därför inte.¹

I frågan om angrepp på företagshemligheter blev utgången den motsatta. Lagen om företagshemligheter skyddar information som är hemlig som helhet eller i den form dess beståndsdelar ordnats och satts samman.² Den sammansättningsregeln saknar motsvarighet i upphovsrätten. PMÖD fann därför, till skillnad från underinstansen,³ att

- 1 Domstolen framhöll samtidigt att kravet på individualiserad bevisning inte hade ställts lika högt om prövningen gällt ett helt datorprogram. Referenten var skiljaktig och ansåg att identitetskravet var uppfyllt så snart alstret lagrats på ett medium och därmed kommit till uttryck i någon form. Han ansåg även att originalitetskravet var uppfyllt och att källkoden alltså utgjorde ett upphovsrättsligt skyddat verk. Att det ingivna materialet var begränsat och ostrukturerat var enligt honom en fråga för originalitetsbedömningen, inte för identifieringen.
- 2 § första stycket 2 lagen (2018:558) om företagshemligheter.
- 3 Underinstansen ansåg att källkoden i och för sig kunde kvalificera sig som företagshemlighet, men att inte samtliga element i den kunde göra det, och att Phenixid därför måste knyta varje påstått angrepp till kod där en företagshemlighet kunde verifieras. PMÖD delade underinstansens bedömning att informationen varit hemlig, att rimliga hemlighållandeåtgärder vidtagits och att ett röjande varit ägnat att medföra skada i konkurrenshänseende.

källkoden i sin sammansatta form varit skyddsvärd även om den delvis bestått av bland annat öppen källkod som var för sig varit allmänt känd. PMÖD sammanfattade saken så att det av allt att döma funnits ”en marknad för källkoden som helhet, inte dess olika enskildheter”. Även angreppet ansågs avse koden i dess helhet.

Fortifiedid förbjöds vid vite att utnyttja eller röja uppgifterna i den ingivna källkoden med undantag för vissa filer, och förpliktades även att betala skadestånd.

Domen visar tydligt att den som vill hävda upphovsrätt till en modern mjukvaruprodukt har en omfattande bevis- och förklaringsbörda. Domstolen understryker att den (eller någon annan som inte är sakkunnig på området) inte kan bedöma hur alstrets olika delar (källkodsfiler) förhåller sig till varandra. Det urval som Phenixid gjort från den totala mängden källkod som ligger till grund för företagets produkter har inte heller hjälpt domstolens bedömning då Phenixid inte förklarat vilka delar som getts in, vad som har utelämnats och varför. Inte heller de sakkunnigutlåtanden som getts in av Phenixid har lett till att domstolen kunnat göra någon bedömning av vad verket egentligen kan sägas bestå av.

Som följd därav är en ytterligare reflektion är att skyddet för före-

tagshemligheter får allt större praktisk betydelse för skyddet av mjukvara. Målet är ett tydligt exempel på att det på samma processmaterial många gånger kan vara lättare att vinna framgång i ett påstående om angrepp på företagshemligheter än upphovsrättsintrång. Och ett vitesförbud behöver, till skillnad från vad som gäller på immaterialrättsens område, inte utformas så att det ansluter till det angrepp som angriparen faktiskt har utfört.⁴

Därtill kommer att det sedan den 1 januari 2026 är straffbart att uppsåtligt och olovligen utnyttja eller röja en teknisk företagshemlighet som man har fått del av till följd av sin anställning eller en affärsförbindelse.⁵ Samma handlingsmönster i dag hade alltså också kunnat prövas straffrättsligt mot de tidigare anställda personligen.⁶

Fokusförflyttningen från upphovsrätt mot företagshemligheter förstärks ytterligare av att modern mjukvaruutveckling i allt större grad sker med hjälp av AI-verktyg. Upphovsrätten skyddar endast det som utgör upphovsmannens egen intellektuella skapelse. Ju större andel av en kodbas som genereras av AI-verktyg, desto svårare blir det att visa att den är upphovsrättsligt skyddad och i vilka delar. Lagen om företagshemligheter ställer däremot ingen fråga om vem eller vad som har skapat informationen, utan bara

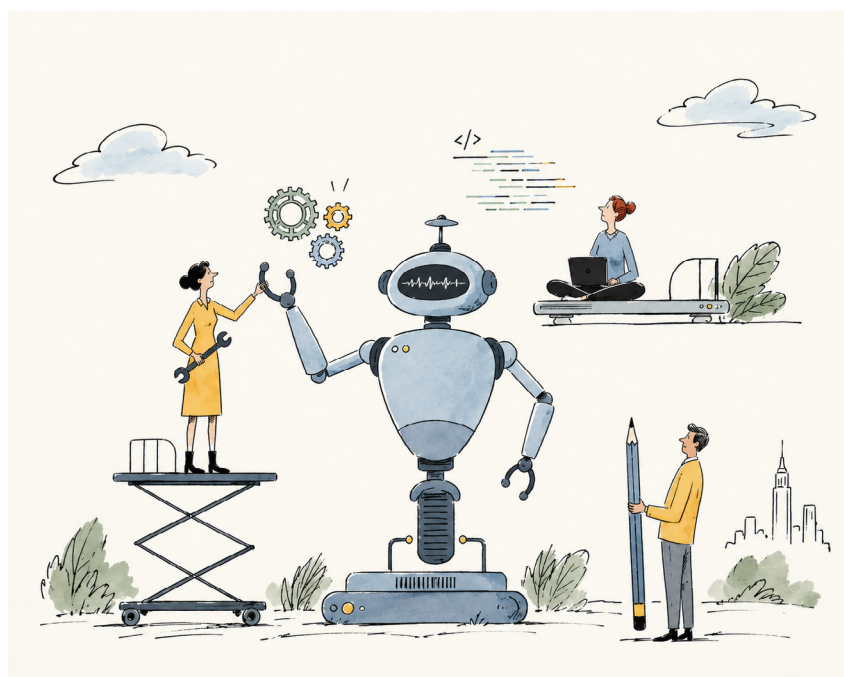


Illustration: Coulorbox/ChatGPT

om den varit hemlig, om rimliga åtgärder vidtagits för att hemlighålla den och om ett röjande varit ägnat att medföra skada i konkurrenshänseende.⁷

Baksidan är att användningen av AI-verktyg också riskerar att underminera skyddet. AI-verktyg för kodning levereras ofta som en tjänst,⁸ vars användande förutsätter att hela eller delar av kodbasen avslöjas för – eller uppstår hos – en extern leverantör. Och ett sådant röjande kan påverka bedömningen av om rimliga hemlighållandeåtgärder har vidtagits. Villkoren för AI-verktygen, dvs. var koden får behandlas, av vem och med vilka förbehåll om lagring och träning, blir därför en central fråga.

Båda parter har överklagat domen till Högsta domstolen. I skrivande stund har frågan om prövningstillstånd inte avgjorts.

Frågorna som aktualiseras är ytterst unionsrättsliga,⁹ och ett avgörande kan därmed få betydelse för rättstillämpningen i hela Norden.

Fredrik Sandström, advokat och Managing Associate på Advokatfirman Kahn Pedersen, arbetar främst med juridiska frågor kopplade till IT, digitalisering och teknikintensiva projekt inom bl.a. bank, försäkring, energi och industri.

Hanna Bogsjö Österberg, advokat på Advokatfirman Kahn Pedersen. Hon arbetar inom byråns specialistområde Digital och särskilt med juridiska frågor i samband med digital transformation, IoT och strategiska sourcingprojekt.

Staffan Malmgren, Legal Technology Officer på Advokatfirman Kahn Pedersen och jobbar särskilt med teknikenära frågor inom bl.a. informationssäkerhetsreglering, it-avtal och dataskydd.

4 12 § lagen om företagshemligheter och prop. 2017/18:200 s. 162.

5 26 a § lagen om företagshemligheter. Källkod och datorprogram anges uttryckligen som exempel på tekniska företagshemligheter i förarbetena (prop. 2024/25:208 s. 54).

6 26 a § tredje stycket lagen om företagshemligheter samt prop. 2024/25:208 s. 51 och 58. Att gärningen begås efter att anställningen upphört innebär dock att den normalt ska bedömas som ringa och därmed vara straffri om inte agerandet framstår som särskilt illojalt, till exempel genom att överföringen av information till konkurrenten förbets redan under anställningen.

7 2 § första stycket lagen om företagshemligheter. I kravet på skada i konkurrenshänseende ligger att informationen ska ha kommersiellt värde på grund av att den är hemlig (prop. 2017/18:200 s. 139).

8 Exempelvis Github Copilot, Claude Code eller OpenAI Codex.

9 Den nya svenska straffbestämmelsen är däremot ett nationellt tillägg.