Sveriges advokatsamfund

Stockholm den 22 april 2025

R-2025/0434

Till Justitiedepartementet
Ju2020/04525

Sveriges advokatsamfund har genom remiss den 18 februari 2025 beretts tillfälle att yttra sig över utkastet till lagrådsremiss Ett mer heltäckande straffansvar vid angrepp på företagshemligheter.

Synpunkter

Advokatsamfundet, som hänvisar till sina tidigare synpunkter i förevarande frågor,[1] har följande synpunkter när det gäller utkastet till lagrådsremiss.

Avgränsningen av straffansvaret till angrepp på tekniska företagshemligheter

I lagrådsremissutkastet (s. 25) anser regeringen att bristen i det straffrättsliga skyddet är särskilt allvarlig för företag och forskningsinstitutioner som ägnar sig åt – i vid bemärkelse – teknisk produktion av varor eller tjänster. Samtidigt anför regeringen att inriktningen på en kriminalisering därför bör vara att träffa sådana angrepp som typiskt sett medför stor skada – eller risk för sådan – för företag och forskningsinstitutioner, och som även påverkar svenskt företagande och svensk innovation negativt. Vare sig i den underliggande departementspromemorian eller i utkastet till lagrådsremiss refereras det till något underlag som visar att angrepp på teknisk produktion av varor eller tjänster skulle vara särskilt allvarlig. Samtidigt anger

[1] Se Advokatsamfundets remissyttrande den 10 mars 2021 över departementspromemorian 2020:26 Bättre skydd för tekniska företagshemligheter.

Laboratoriegatan 4, Box 27321, 102 54 Stockholm
Tfn 08-459 03 00, advokatsamfundet.se, info@advokatsamfundet.se

regeringen att kriminaliseringen ska träffa sådana angrepp som medför stor skada, vilket i många fall kan röra sig om angrepp på kommersiella företagshemligheter.

Det meddelas omkring tio till femton domar om året i civilrättsliga mål om angrepp på företagshemligheter. En stor andel av dessa domar avser angrepp på kommersiella företagshemligheter såsom kundlistor, prislistor, inköps- och försäljningspriser, ekonomisk information och affärsplaner. Ett typfall av angrepp på företagshemligheter som ofta blir föremål för domstolstvister är angrepp på kundregister. Meddelade domar rörande företagshemligheter utgör naturligtvis inget representativt underlag för att bedöma vilka angrepp på företagshemligheter som sker hos svenska företag och forskningsinstitutioner. Det kan dock konstateras att företagen anser att kommersiella företagshemligheter har ett sådant högt värde att det är värt att inleda domstolsprocess för att hindra fortsatta angrepp.

En kriminalisering av endast tekniska företagshemligheter framstår som inkongruent och osystematiskt. En teknisk företagshemlighet behöver inte nödvändigtvis ha ett högt värde och ett angrepp på en teknisk företagshemlighet behöver inte nödvändigtvis leda till stor skada. Det är helt beroende av vilken företagshemlighet det rör sig om. Motsatsvis kan en kommersiell företagshemlighet ha ett stort värde och ett angrepp leda till stor skada. Ett exempel på en sådan situation är AD 2017 nr 12 där ett angrepp på ett kundregister fick stora effekter på det angripna företagets omsättning.

I förarbetena till den första lagen om skydd för företagshemligheter (SFS 1990:409), påtalas det särskilt att olika typer av företagshemligheter inte kan särskiljas från varandra och att gränserna för vad som är att anse som en företagshemlighet sätts genom andra kriterier i lagen (se prop. 1987/88:155, s. 34, och SOU 1983:52, s. 286 och 372). Av beaktandesats 14 i direktivet om företagshemligheter framgår vidare att lagstiftningen inte bör skilja mellan olika typer av företagshemligheter.

> *”Det är viktigt att införa en enhetlig definition av begreppet* företagshemlighet, *utan att man begränsar det föremål som ska skyddas från angrepp. En sådan definition bör således utformas så att den täcker know-how, företagsinformation och teknisk information i fråga om vilken det finns både ett legitimt intresse av konfidentialitet och berättigade förväntningar på att konfidentialiteten bevaras. Vidare bör sådan know-how eller information ha antingen faktiskt eller potentiellt*

kommersiellt värde. Sådan know-how eller information bör anses ha kommersiellt värde, till exempel om dess olagliga anskaffande, utnyttjande eller röjande sannolikt skadar intressen hos den person som lagligen kontrollerar den, genom att undergräva den personens vetenskapliga och tekniska potential, affärsintressen eller ekonomiska intressen, strategiska ställning eller konkurrensförmåga. Definitionen av företagshemlighet omfattar inte obetydlig information eller den erfarenhet och de färdigheter som arbetstagare får vid normal yrkesutövning och inte heller information som är allmänt känd bland eller lättillgänglig för personer inom de kretsar som normalt hanterar typen av information i fråga."

Ett angrepp på företagshemligheter omfattar ofta eller nästan alltid såväl tekniska som kommersiella företagshemligheter. Om angrepp på tekniska företagshemligheter kriminaliseras blir följden att sådana angrepp åtalas av åklagare och prövas i straffrättslig ordning. Polis och åklagare får också tillgång till straffrättsliga tvångs- och bevissäkringsåtgärder. Målsäganden i ett brottmål står inte risken för rättegångskostnader och åklagaren kan framföra målsägandens enskilda anspråk. Om angreppet omfattar även kommersiella företagshemligheter kommer dessa att behöva skiljas ut från brottmålet och hanteras i en civilrättslig tvist som, beroende på olika straff- och civilprocessuella forumregler, kan komma att handläggas i olika domstolar. En sådan ordning är inte önskvärd.

Ur ett allmänpreventionsperspektiv framstår det också som anmärkningsvärt att angrepp på kommersiella företagshemligheter – som kan ha ett motsvarande eller högre värde än tekniska företagshemligheter – skulle vara straffritt, medan angrepp på tekniska företagshemligheter skulle vara ett allvarligt brott med upp till sex års fängelse i straffskalan.

Sverige är idag det enda landet i Europa där angrepp på företagshemligheter som angriparen har lovlig tillgång till är undantagna straffansvar. Våra nordiska grannländer har infört straffrättsligt skydd för företagshemligheter, men detta skydd är inte begränsat till tekniska företagshemligheter (se 10 kap. 18 § i den danska loven om forretningshemmeligheder, nr 309 af 25/04/2018, 9 och 10 §§ i den norska loven om vern av forretningshemmeligheter, LOV-2020-03-27-15 och 15–17 §§ i den finska lagen om företagshemligheter (10.8.2018/595). Även i tysk rätt omfattas företagshemligheter

i allmänhet av straffrättsligt skydd (se 23 § Gesetz zur Umsetzung der Richtlinie [EU] 2016/943 zum Schutz von Geschäftsgeheimnissen von rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung).

Definitionen av teknisk företagshemlighet

Legalbegreppet ”teknisk företagshemlighet” definieras i förslaget till 26 a § punkten i företagshemlighetslagen enligt följande:

> *[en företagshemlighet] […] som avser information som är ägnad att användas i produktionen av en vara eller utförandet av en tjänst (teknisk företagshemlighet)*

Begreppet ”teknisk företagshemlighet” är ett, ur semantiskt perspektiv, vitt och vagt begrepp. I utkastet har regeringen försökt precisera begreppets innehåll och angivit att lokutionen kan omfatta ritningar, recept, källkoder, datorprogram, forskningsresultat eller forskningsunderlag, tekniska förebilder eller andra modeller samt annan teknisk information om uppfinningar, produkter eller tjänster. Preciseringen är sannolikt, även om den är vid, alltför snäv, exempelvis nämns inte företagshemligheter av teknisk natur såsom:

- Metodologiska tillvägagångssätt och metodbeskrivningar
  Detaljerade interna rutiner för testning, analys, tillverkning eller verifiering.
- Tillverkningsprocesser och processparametrar
  Information om tryck, temperatur, cykeltider, materialflöden och styrsystem.
- Systemarkitektur och integrationslösningar
  Exempelvis hur programvarukomponenter eller maskinvara samverkar i en produktionsmiljö.
- Maskininlärningsmodeller och träningsdata
  Modellens struktur och de data den tränats på.
- Databaser och datamodeller
  Inkluderar struktur, metadata, indexering och urvalskriterier.
- Prototyper och testresultat från valideringsstudier
- Information som ger inblick i produktens framtida prestanda eller funktion.

- Simuleringsdata och simuleringsmiljöer
- Kombinationer av tekniska modeller och affärskritiska tolkningar
- Teknisk dokumentation för intern användning
- Kodbibliotek och interna utvecklingsverktyg
- Tekniska specifikationer
- Definitioner av prestanda, dimensioner, material, kompatibilitet etc.
- Algoritmer
  Sekvenser av instruktioner för beräkning, styrning, optimering eller analys.
- Modeller (beräknings-, funktions- eller beslutsmodeller)
- Matematiska eller tekniska modeller som beskriver ett systems funktion eller prestanda

Ovan nämnda exempel utgör även exempel på information som skulle kunna befinna sig i gränslandet mellan tekniska och kommersiella företagshemligheter. Vid en straffrättslig prövning är ett angrepp på en teknisk företagshemlighet straffbar, men om företagshemligheten i stället skulle anses vara av kommersiell natur skulle gärningen inte vara straffbar. I ett brottmål kommer således distinktionen mellan tekniska och kommersiella företagshemligheter bli helt central för huruvida straffansvar föreligger.

Lokutionen ”ägnad att” som förekommer inom upphovsrätten (26 k § lagen [1960:729] om upphovsrätt till litterära och konstnärliga verk) har lett till tolkningsfrågor i praxis. I NJA 2016 s. 490 uttalade Högsta domstolen följande beträffande lokutionen ”särskilt ägnad för framställning av exemplar för privat bruk”.

> *”Lagens krav att anordningarna ska vara särskilt ägnade för privatkopiering kan rent språkligt uppfattas på två sätt. Det kan förstås antingen så att anordningarna ska ha speciellt tilldelats funktionen att användas för privatkopiering eller så att det är tillräckligt att de har egenskaper som gör dem i hög grad lämpade för privatkopiering.”*

HD konstaterade avslutningsvis (domskäl 20 och 21) att mobiltelefoner kan antas användas för piratkopiering i en inte oväsentlig omfattning och att de därmed var särskilt ägnade för framställning av exemplar av verk för privat bruk. Om motsvarande synsätt skulle tillämpas på definitionen av en teknisk företagshemlighet (dock med den

skillnaden att ”ägnat” inte kvalificeras av ”särskilt”) skulle det innebära att en teknisk företagshemlighet är [en företagshemlighet] […] som avser information som inte i oväsentlig omfattning kan antas användas i produktionen av en vara eller utförandet av en tjänst (teknisk företagshemlighet).

En ytterligare otydlighet beträffande definitionen är vad som avses med ”produktionen av en vara eller utförandet av en tjänst”. Enligt dess ordalydelse bör definitionen omfatta varje information som har betydelse för produktionen av en vara eller en tjänst, vilket innebär att definitionen potentiellt är mycket omfattande. Det framgår inte heller vad som avses med ”vara” eller ”tjänst” och om begreppen avser ”färdiga” varor eller tjänster eller även tjänstekoncept eller produktprototyper.

Eftersom tekniska företagshemligheter omfattas av ett särskilt straffstadgande i LFH är det inte ur rättssäkerhetssynpunkt lämpligt med en styrande definition som präglas av sådan vaghet som definitionen av ”teknisk företagshemlighet”.

Den föreslagna straffsanktionen omfattar inte tillägnande och anskaffande av teknisk företagshemlighet

Av 3 § första stycket företagshemlighetslagen följer att begreppet ”angrepp på företagshemlighet” omfattar att någon 1. bereder sig tillgång till, tillägnar sig eller på något annat sätt anskaffar företagshemligheten, 2. utnyttjar företagshemligheten, eller 3. röjer företagshemligheten. I 3 § andra stycket företagshemlighetslagen preciseras ytterligare vad som omfattas av begreppet ”utnyttjande”. De civilrättsliga sanktionerna för angrepp på företagshemligheter (bl.a. skadestånd, förbud, interimistiskt förbud, överlämnande och förstörelse) följer av 6, 7, 9, 11–18 §§ företagshemlighetslagen. Av 10 § följer att den som uppsåtligen eller av oaktsamhet annars anskaffar en företagshemlighet ska ersätta den skada som uppkommer genom förfarandet. Genomgående för de civilrättsliga sanktionerna är, med undantag för 8 §, att obehörigt anskaffande i alla dess former av en företagshemlighet utgör ett förfogande som är sanktionerat.

Genom att de föreslagna straffbestämmelserna endast skulle vara tillämpliga på utnyttjande och röjande av företagshemligheter uppstår en tydlig diskrepans mellan de civil- och straffrättsliga sanktionerna, med konsekvensen att anskaffande av en företagshemlighet av teknisk natur på annat vis än genom 26 och 27 §§, vilka inte

omfattar anskaffande av företagshemligheter som anskaffaren har lovlig tillgång till, skulle vara straffritt.

Mot bakgrund av att syftet med de föreslagna lagändringarna är att stärka skyddet för tekniska företagshemligheter förefaller det märkligt att det angreppssätt som i förarbetena till lagen om skydd för företagshemligheter (prop. 1987/88:155 s. 14 f.) pekades ut som den primära skaderisken, dvs. ”den risk för skada för den rättmätige innehavaren som inträder redan genom det olovliga anskaffandet” undantas från kriminaliseringen. En konsekvens av att anskaffande i formen av tillägnande undantagits är vidare att polis och åklagare inte får tillgång till straffrättsliga tvångsmedel när det primära angreppet (anskaffande), men möjligen inte sekundära angreppet (utnyttjande eller röjande), inträffat. Eftersom försök och förberedelse till utnyttjande och röjande av en företagshemlighet av teknisk natur enligt den föreslagna 26 b § bestämmelsen omfattas av försöks- och förberedelsebrotten i 23 kap. 4 § är det möjligt att tillägnande av en företagshemlighet ändock omfattas av straffansvar, vilket innebär att syftet med att undanta anskaffande från kriminaliseringen genom att inte ange anskaffande i 26 a och 26 b §§ i företagshemlighetslagen möjligen inte uppnås.

I det s.k. Ericsson-målet (Svea hovrätts dom den 20 oktober 2003 i mål nr B 5221-03), som var upprinnelsen till att 2007 års utredning om skyddet för företagshemligheter utredde och föreslog en kriminalisering av angrepp på företagshemligheter, hade en anställd, inom ramen för sina arbetsuppgifter, anskaffat företagshemligheter i form av säkerhetsklassade dokument hos Ericsson och därefter röjt informationen för en person som i sin tur vidarebefordrade informationen till en utländsk underrättelseofficer. Anskaffandet ansågs i denna dom vara straffritt eftersom den anställde hade lovlig tillgång till informationen. Med de nu föreslagna straffbestämmelserna hade den anställdes anskaffande i syfte att röja känsliga företagshemligheter alltjämt varit straffritt, medan röjandet hade fallit under straffbestämmelsen i 26 a § företagshemlighetslagen. Mot bakgrund av vad som anförs på s. 31 i utkastet till lagrådsremiss rörande statsstyrt företagsspionerі som genomförs med hjälp av personer som jobbar under täckmantel i t.ex. bulvanföretag eller forskningsdelegationer och behovet av att myndigheter och rättsväsendet har goda och effektiva möjligheter att motarbeta sådant spionerі, förefaller det märkligt att anskaffande i form av tillägnande av en företagshemlighet av teknisk natur, som anskaffaren har lovlig tillgång till, inte omfattas av kriminaliseringen.

Den föreslagna straffsanktionen omfattar inte styrelseledamöter och revisorer

I utkastet under rubriken ”Nya hot har ökat behovet av ett förstärkt straffrättsligt skydd” anför regeringen bland annat följande skäl för varför angrepp på tekniska företagshemligheter föreslås straffsanktioneras:

> *”Ett sätt att komma åt information är genom anlitande av insiders på målföretagen, dvs. anställda med lovlig tillgång till känslig information. Det kan i ett sådant fall handla om informationskedjor där flera personer på olika positioner och med olika befogenheter inom ett och samma företag medverkar. Även den typen av angrepp underlättas i någon mån av teknikutvecklingen på så sätt att det är möjligt att på kort tid komma över och tillgodogöra sig stora mängder information. Ett angrepp av det slaget kan röja ett företags centrala företagshemligheter och leda till stor skada. Även lärosäten och forskningsutförare riskerar att utsättas för sådana angrepp.”*

En utgångspunkt för förslaget är således att insiders med lovlig tillgång till information kan anlitas, exempelvis av en utländsk underrättelsetjänst. Styrelseledamöter tillhör typiskt sett den personkrets som får del av flest och känsligast tekniska företagshemligheter. En aktör som vill åtkomma tekniska företagshemligheter kan därför ha ett starkt intresse av att anlita en styrelseledamot. En styrelseledamot har förvisso ett, i förhållande till LFH, begränsat skadeståndsansvar enligt aktiebolagslagen, men en styreledamots angrepp på tekniska företagshemligheter är inte straffsanktionerat i aktiebolagslagen. Förslaget i utkastet innebär således att den som potentiellt kan ställa till störst skada genom angrepp på tekniska företagshemligheter helt är undantagen straffansvar, medan anställda i lägre positioner omfattas av straffansvar.

Styrelseledamöter omfattas inte idag av de civilrättsliga påföljderna och sanktionerna i LFH. I aktiebolagslagen finns, utöver skadeståndsansvar, inga påföljder och sanktioner som motsvarar påföljder och sanktioner i LFH. Om styrelseledamöter undantas från straffansvar för angrepp på tekniska företagshemligheter blir effekten att den enda sanktion en styrelseledamot kan bli föremål för är civilrättsligt skadeståndsansvar enligt aktiebolagslagen och möjligen straffansvar för trolöshet mot huvudman. De skäl

som regeringen anför mot att styrelseledamöter och revisorer ska undantas från straffansvar är inte bärkraftiga.

Ringa brott

I förslaget till 26 a § LFH undantas ringa fall från straffansvar: Bestämmelsen har följande lydelse:

> *”I ringa fall ska det inte dömas till ansvar. Vid bedömningen av om gärningen är ringa ska det särskilt beaktas om gärningen är mindre allvarlig på grund av att den har begåtts efter att ett sådant deltagande som avses i första stycket 2 har upphört.*

I utkastet anför regeringen bl.a. följande skäl för varför angrepp som inträffar efter att deltagandet har upphört endast undantagsvis ska kunna föranleda straffansvar:

> *”Liksom promemorian funnit bör angrepp som sker efter att deltagandet i verksamheten eller rörelsen upphört endast undantagsvis ska kunna föranleda straffansvar. En annan ordning skulle innebära risk för inlåsningseffekter på arbetsmarknaden. Det skulle även innebära ett omotiverat avsteg från huvudregeln om arbetstagares frihet att utnyttja sin kunskap och erfarenhet på den öppna arbetsmarknaden.”*

Motiveringen är svårförståelig. Arbetstagares kunskap och erfarenhet utgör enligt 2 § LFH inte en företagshemlighet (”[e]rfarenheter och färdigheter som en arbetstagare har fått vid normal yrkesutövning är inte en företagshemlighet.”) vilket innebär att sådana angrepp varken kan bli föremål för civil- eller straffrättsliga sanktioner. Den risk för avsteg från huvudregeln om arbetstagarnas frihet på arbetsmarknaden som regeringen ser finns av detta skäl inte.

Skadeeffekten av ett angrepp i form av ett obehörigt anskaffande är densamma oavsett om angreppet inträffar under deltagande i en verksamhet eller efter. Ett angrepp som inträffar efter det att deltagandet i verksamheten upphört är typiskt sett mer allvarligt då innehavarens rättsliga kontroll över företagshemlighet försvagas. Det typiska angreppet i form av utnyttjande och röjande av företagshemligheter till tredje man sker i många fall medvetet efter det att deltagandet i verksamheten upphört eftersom upptäcktsrisken i normalfallet då är lägre. Om ett angrepp inträffar mycket lång tid efter att deltagandet har upphört kan det innebära att skadan är mindre om den

tekniska företagshemligheten har förlorat sin aktualitet. Det innebär att ett angrepp som inträffar i anslutning efter att deltagandet upphört i typsituationen är lika allvarligt eller t.o.m. allvarligare än ett angrepp som inträffat under deltagandet.

Ur ett allmänpreventionsperspektiv förefaller det vidare märkligt att angrepp som inträffar efter att deltagandet i en verksamhet har upphört undantas från kriminaliseringen.

Det är tydligt av civilrättslig praxis rörande angrepp på företagshemligheter att företagshemligheter angrips av personer, anställda eller uppdragstagare, som har lovlig tillgång till hemligheterna inom ramen för en anställning eller ett uppdrag. Ett typfall av angrepp är en arbetstagare som under sin anställning tillägnar sig arbetsgivarens företagshemligheter genom att framställa kopior av arbetsgivarens digitala handlingar och i direkt eller nära anslutning till anställningens upphörande utnyttjar företagshemligheterna i en egen nystartad verksamhet eller i en konkurrents verksamhet. Det innebär i sin tur att bestämmelsen i 7 § andra stycket LFH ” Om ett utnyttjande eller röjande har ägt rum sedan anställningen upphört gäller ansvaret enligt första stycket endast om det finns synnerliga skäl.” ofta kommer att tillämpas. Vid prövningen om det föreligger synnerliga skäl ska enligt förarbetena (prop. 1987/88:155, s. 45–46) till LFH följande faktorer beaktas:

- Att arbetstagaren tagit anställning hos arbetsgivaren i syfte att åtkomma företagshemligheter.
- Att arbetstagaren under pågående anställning förberett överförande av företagshemligheter till konkurrerande verksamhet.
- Att företagshemligheten missbrukats genom dokumentation i någon form.
- Att arbetsgivarens skada är omfattande.
- Att arbetstagaren har haft en särskild förtroendeställning hos arbetsgivaren (vilket inte ensamt utgör synnerliga skäl).
- Brott mot sekretessavtal.

I utkastet (s. 56) upprepas ovan nämnda omständigheter som innebär att ett angrepp ska anses särskilt illojalt och anges att ett angrepp typiskt sett inte är ringa när 7 § andra stycket LFH aktualiseras. Den föreslagna bestämmelsen kommer dock, enligt sin ordalydelse, sannolikt att läsas som att en gärning är mindre allvarlig på grund av att

den har begåtts efter att ett deltagande har upphört vilket inte rimmar med de verkliga typsituationerna eller hur särskilt illojala angrepp beskrivits i specialmotiveringen.

Av specialmotiveringen framgår vidare att agerandet ska anses särskilt illojalt om en mottagare av en angripen företagshemlighet är en konkurrent. I den kontexten bör det också anges att angreppet ska anses särskilt illojalt om den angripna företagshemligheten överförts till den f.d. anställdes eller uppdragstagarens egen verksamhet eller om överförts till någon i syfte att skada innehavaren av en företagshemlighet som obehörigen har kvarhållits efter deltagandet i verksamheten upphört.

Förhållandet mellan 26 a § och direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.

Genom ändringarna i företagshemlighetslagen som trädde i kraft den 1 juli 2018 genomfördes bestämmelserna i företagshemlighetsdirektivet (direktiv [EU] 2016/943). Eftersom det civilrättsliga skyddet för företagshemligheter numera är harmoniserat kommer EU-domstolens tolkningar av företagshemlighetsdirektivet enligt principen om direktivkonform tolkning att utgöra tolkningsunderlag för företagshemlighetslagen, exempelvis när det gäller definitionen av begreppet företagshemlighet i 2 §. Den föreslagna straffbestämmelsen i 26 a § i företagshemlighetslagen utgör en svensk nationell straffrättslig bestämmelse som inte omfattas av direktivet och därmed inte heller, formellt, av EU-domstolens tolkningsbesked. Detsamma gäller för de befintliga straffrättsliga bestämmelserna i 27 och 28 §§ företagshemlighetslagen.

Det faktum att samma begrepp faller inom och utanför det harmoniserade området kan leda till tolkningsfrågor eftersom de rättsliga begreppen i de straffrättsliga bestämmelserna i formell mening inte, eftersom de faller utanför harmoniseringen, behöver tolkas direktivkonformt utan kan ges en egen nationell innebörd. Motsvarande frågeställning uppstår på det immaterialrättsliga området där Patent- och marknadsöverdomstolen valt att utgå från EU-domstolens tolkningar exempelvis på varumärkes- och upphovsrättsområdet även när domstolen tillämpat straffrättsliga varumärkes- och upphovsrättsliga bestämmelser som faller utanför det harmoniserade området. Ett civilrättsligt exempel är NJA 2007 s. 431 som rörde förutsättningarna för slutligt vitesförbud vid varumärkesintrång. I det fallet begärde Högsta domstolen

förhandsbesked från EU-domstolen om förutsättningarna för att meddela slutligt vitesförbud vid intrång i ett gemenskapsvarumärke. Högsta domstolen meddelade slutligt vitesförbud avseende intrånget i gemenskapsvarumärket och uttalade beträffande intrånget i kärandens svenska varumärke att det saknades anledning att göra en annan bedömning.

Det är sannolikt att svenska domstolar skulle tillämpa även de straffrättsliga bestämmelserna i enlighet med EU-domstolens kommande förhandsbesked rörande företagshemlighetsdirektivet. Eftersom det rör sig om straffrättsliga bestämmelser är det dock, av legalitetsskäl, lämpligt att det i lagrådsremissen förtydligas huruvida även dessa bestämmelser ska tolkas med utgångspunkt i EU-domstolens förhandsbesked, exempelvis när det gäller begreppen ”anskaffande”, ”röjande”, ”utnyttjande” ”företagshemlighet” eller om de ska ges en självständig svensk nationell tolkning.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander