

Stockholm den 10 mars 2021

R-2020/2382

Till Justitiedepartementet

Ju2020/04525/L1

Sveriges advokatsamfund har genom remiss den 10 december 2020 beretts tillfälle att avge yttrande över departementspromemorian 2020:26 Bättre skydd för tekniska företagshemligheter.

### **Sammanfattning**

Advokatsamfundet har i huvudsak ingen erinran mot förslagen i promemorian, men önskar lämna nedanstående synpunkter när det gäller vissa enskilda bestämmelser.

### **Synpunkter**

Begreppet ”företagshemlighet av teknisk natur” står i strid med det straffrättsliga obestämbarhetsförbudet

Av förslaget till 26 a § i företagshemlighetslagen framgår att den som utnyttjar eller röjer en ”företagshemlighet av teknisk natur” ska dömas till fängelse i högst två år. Om brottet är grovt ska dömas till fängelse i lägst sex månader och högst sex år.

Av promemorian (s. 58) framgår att uttrycket ”företagshemlighet av teknisk natur” sedan tidigare finns i svensk rätt, närmare bestämt i 5 kap. 12 § konkurrenslagen. Begreppet preciseras på s. 60 i promemorian enligt följande:

*”Karakteristiskt för företagshemligheter av teknisk natur är att de typiskt sett utgör ett led i produktionen eller framställningen av en vara eller utförandet av en tjänst. Företagshemligheter av teknisk natur kan exempelvis vara ritningar, recept, källkoder, datorprogram, forskningsresultat eller forskningsunderlag, tekniska förebilder och andra modeller eller annan sådan teknisk information.”*

Begreppet ”företagshemlighet av teknisk natur” är ett, ur semantiskt perspektiv, *vitt och vagt* begrepp. I promemorian har departementet försökt precisera begreppets innehåll men preciseringen är sannolikt, även om den är vid, alltför snäv. Exempelvis nämns inte metodbeskrivningar, patenterbara uppfinningar, tekniska specifikationer, databaser, prototyper, modeller och algoritmer i definitionen. Redan i förarbetena till lagen om illojal konkurrens förorsakade lokutionen ”teknisk förebild” betydande tolknings- och avgränsningssvårigheter (se SOU 1966:71, s. 120). Lokutionen ”teknisk natur” har i sin tur ett ännu bredare tillämpningsområde än ”teknisk förebild”.

I den straffrättsliga legalitetsprincipen ryms fyra underprinciper, däribland det s.k. obestämbarhetsförbudet som innebär att föreskriften (i detta fall lagtexten) i rimlig utsträckning måste vara bestämd till sin utformning. Detta medför att det ställs krav på begriplighet och precision vid utformningen av lagtext. Risken är annars att det inte utifrån lagtexten går att förutse i vilka fall det finns förutsättningar för straffrättsligt ansvar.

Enligt Advokatsamfundets uppfattning är det olämpligt att i lagtext, i synnerhet när det gäller brott med upp till sex års fängelse i straffskalan, använda en så vid och vag lokution som ”av teknisk natur”. Analogin till konkurrenslagen är inte bärkraftig eftersom den aktuella bestämmelsen i konkurrenslagen inte är en straffrättslig sådan för vilka det uppställs högre krav på begriplighet och precision. Begreppet kommer med nödvändighet behöva preciseras i författningskommentaren till 26 a § vilket innebär att innehållet i ett straffbud inte anges genom lagtexten utan genom motivuttalanden. Med andra ord blir det fråga om lagstiftning genom motiv.

Advokatsamfundet föreslår därför att begreppet ”av teknisk natur” preciseras genom exempelvis följande lokution ”all teknisk information som rör utformning, forskning, utveckling, produktion, installation, underhåll, användning eller handhavande med avseende på en vara eller tjänst”.

#### Den föreslagna straffsanktionen omfattar inte alla former av angrepp

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 *anskaffande* 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.

Genom förslaget i 26 a § kriminaliseras utnyttjande respektive röjande av företagshemligheter av teknisk natur. Däremot omfattar inte kriminaliseringen den som bereder sig tillgång till, tillägnar sig eller på något annat sätt anskaffar företagshemligheten. Skälet till att anskaffande inte omfattas av kriminalisering anges i promemorian (s. 63) vara att utnyttjande och röjande är mer klandervärda förfoganden än anskaffande. 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 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 bestämmelsen i 26 b § omfattas av försöks- och förberedelsebrotten i 23 kap. 4 § är det tänkbart att beredandet av tillgång till, tillägnande eller anskaffande av en företagshemlighet ändå 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, se s. 32 i promemorian) 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 alltså varit straffritt medan röjandet hade fallit under straffbestämmelsen i 26 a § företagshemlighetslagen. Mot bakgrund av vad som anförs på s. 101 i promemorian rörande statsstyrkt företagsspioneri som genomförs med hjälp av personer som jobbar under täckmantel i t.ex. bulvanföretag eller forskningsdelegationer samt behovet av att myndigheter och rättsväsendet har goda och effektiva möjligheter att motarbeta sådant spioneri, förefaller det märkligt att *anskaffande* av en företagshemlighet av teknisk natur inte omfattas av kriminaliseringen.

I den föreslagna 26 a § anges inte att den angripna informationen ska ha anförtrotts angriparen i förtroende

Av 6 § företagshemlighetslagen (som i princip haft samma lydelse sedan lagens tillkomst) framgår att skadeståndsansvar uppstår om någon, uppsåtligen eller av oaktsamhet, angriper en företagshemlighet som han eller hon *i förtroende* fått del av i samband med en affärsförbindelse.

*6 § Den som uppsåtligen eller av oaktsamhet angriper en företagshemlighet hos en näringsidkare eller en forskningsinstitution som han eller hon i förtroende har fått del av i samband med en affärsförbindelse med näringsidkaren eller forskningsinstitutionen, ska ersätta den skada som uppkommer genom förfarandet. (vår understrykning).*

Förtroenderekvisitet är väsentligt eftersom det avgränsar vilken information mottagaren inte får angripna. Förtroendet manifesteras oftast genom ett sekretessavtal mellan den som delgivit företagshemligheten och den som fått del av den i förtroende. Även utan ett sekretessavtal kan det dock följa av omständigheterna att informationen lämnades ut i förtroende.

I den föreslagna 26 a § återfinns inte motsvarande lokution:

*26 a §*

*Den som uppsåtligen och olovligen utnyttjar en företagshemlighet av teknisk natur som han eller hon har fått del av i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution, eller genom att delta i en näringsidkares rörelse eller en forskningsinstitutionens verksamhet till följd av anställning eller uppdrag eller på annan liknande grund, ska dömas för olovligt utnyttjande av företagshemlighet till böter eller fängelse i högst två år.*

Konsekvensen av att lokutionen ”i förtroende” saknas i 26 a § är att straffbestämmelsen sträcker sig betydligt längre än motsvarande civilrättsliga bestämmelse i 6 § företagshemlighetslagen. För att 26 a § ska bli tillämplig är det nämligen tillräckligt att mottagaren *har fått del av* informationen, det krävs inte att denne fått del av informationen *i förtroende*. När det gäller angreppshandlingar har departementet (se avsnittet ovan) valt att undanta anskaffande från straffbestämmelsen, vilket indikerar en mildare syn på anskaffande än motsvarande civilrättsliga bestämmelser. Det förefaller inkonsekvent att samtidigt ha en strängare straffrättslig bestämmelse i 26 a § som kriminaliserar utnyttjande och röjande av information, oaktat om denna har emottagits i förtroende eller inte. Advokatsamfundet föreslår därför att lokutionen ”i förtroende” läggs till i 26 a §.

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 utgöra tolkningsunderlag för företagshemlighetslagen, exempelvis när det gäller definitionen av begreppet företagshemlighet i 2 §. De föreslagna straffbestämmelserna i 26 a § i företagshemlighetslagen är svenska nationella straffrättsliga bestämmelser 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 både inom och utanför det harmoniserade området kan leda till tolkningsfrågor eftersom de rättsliga begreppen i de straffrättsliga bestämmelserna i formell mening inte – då 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 ”röjande”, ”utnyttjande” ”företagshemlighet” eller om de ska ges en självständig svensk nationell tolkning.

Straffrättsliga ärenden rörande angrepp på företagshemligheter bör hanteras av Nationella Operativa Avdelningens utredningssektion hos Polisen och av de åklagare som är specialiserade på immaterialrättsbrott

Sedan 2008 hanteras immaterialrättsbrott av en särskild nationell samordnare inom Polisen. Immaterialrättsbrott hanteras av åklagare vid den Nationella gruppen mot

immaterialrättsbrott vid Riksenheten mot internationell och organiserad brottslighet som har särskild inriktning mot immaterialrättsliga brott.

Syftet med den nationella gruppen mot immaterialrättsbrott var att polis och åklagare skulle specialisera sig avseende immaterialrättsbrott och att denna brottslighet skulle ges en ökad prioritet. Utfallet av specialiseringen har varit mycket positivt och har inneburit effektivare och färre nedlagda förundersökningar. Mot bakgrund av att företagshemligheter i vart fall ligger nära det immaterialrättsliga området är det lämpligt att det i lagrådsremissen förordas att brott mot företagshemlighetslagen ska hanteras av den Nationella gruppen mot immaterialrättsbrott.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander