Företagshemligheter i digital miljö

Fredrik Jonasson, Awapatent

Ett seminarium i observatoriets serie
Ensamrätter i ny miljö – tre seminarier

En rapport från
det IT-rättsliga observatoriet rapport

Förord

Informations- och kommunikationstekniken innebär att traditionell reglering av immateriella rättigheter ställs inför nya prövningar och utmaningar. Nästan dagligen uppmärksammas problem med piratkopiering och spridning av programvara, musik och annat digitalt material.

Även rättspolitiska frågor, som har att göra med utformningen av regleringen och dess lämplighet i den nya miljön, är aktuella. Ett exempel är diskussionen kring patent för datorprogram och för affärsmodeller och processer. Ett drag som möjligen kan skönjas i utvecklingen är att gränsen mellan formskydd och innehållsskydd i upphovsrätten håller på att suddas ut eller flyttas.

Det IT-rättsliga observatoriet genomförde under år 2001 tre seminarier för att analysera hur regleringen av immateriella rättigheter står sig i konfrontationen med en ny digital miljö. Kan den befintliga regleringen tillämpas utan behov av ytterligare anpassning, eller behövs en revision? Gör sig andra intressen gällande, intressen som kan föranleda att de principer som ligger till grund för regleringen bör omvärderas?

Seminarieserien kom att omfatta följande områden

- *Företagshemligheter i en digital miljö – Fredrik Jonasson*
- *Upphovsrätt - nya distributionsformer – Niklas Lundblad*
- *Open source - Ur ett praktiskt juridiskt perspektiv – Mattias Andersson*
- *Något om patenterbarhet av datorprogram i svensk rätt – Mikael Pawlo och Patrik Wallström*
- *Tekniska skyddsåtgärder och upphovsrätt – Daniel Westman*

Varje område har haft en egen presentatör (se ovan) vars uppgift varit att skriva ett diskussionsunderlag inför ett seminarium. Dessa underlag återfinns i respektive rapport. Vid diskussionerna framkomna synpunkterna utgör grunden för det inledande sammanfattande avsnittet.

Stockholm, oktober 2002

Peter Seipel
ordförande

Summering

Information synes få ett allt större värde samtidigt som den flyter alltmer fritt och man kan fråga sig om det med hänsyn till det ökade flödet av information över huvud taget praktiskt möjligt att skydda företagshemligheter idag.

Externa kontakter hos företagen har redan förändrats bl.a. genom ökade risker för avlyssning och intrång. Dock är externa intrång som regel redan straffbelagda. Här finns således tillräckliga medel i form av lagstiftning.

Spridningsproblemet internt innebär däremot en ökad risk för att hemligheter läcker ut genom att fler har åtkomst till dem. Ett sådant exempel är s.k. hopkopplade system - en ny företeelse som medför att flera kan komma att dela på en företagshemlighet. Frågan uppkommer hur man hanterar hemligheter som uppstår i kontakten mellan två eller flera parter. Kan det finnas samägda företagshemligheter? Någon exklusiv koppling till någon viss juridisk person föreligger inte vid tillämpningen av lagen.

Grundreglerna i lagen om företagshemligheter (FHL), bl.a. definitionen av "företagshemlighet" i 1 §, kommer att påverkas av hur IT förändrar den miljö där lagen kommer att tillämpas. Är den definition av kravet på hemlighållande som tillämpas i Sverige lämplig?

En annan fråga, som behöver övervägas i anledning av den nya tekniken, är om vi överhuvudtaget bör skydda företagshemlig information. FHL innebär som sagt ett krav på att information hålls hemlig för att skydd skall föreligga. Om lagen inte fanns skulle detta förhållande tvinga företagen att bättre se över sin situation visavi viktig information. Efter en sådan översyn kanske skyddet kan utformas bättre genom avtal, som kan anpassas till såväl teknisk utveckling i allmänhet som den enskilda situationen.

Det är vidare möjligt att tänka sig att patent på affärsmetoder kan användas som substitut. Som framgår av senare seminarier föreligger dock svårigheter att formulera patentkrav. Likaså tillkommer kostnader för att söka och utöva patent.

Ett värde får anses ligga i lagens hybridnatur och att lagen riktar sig mot sådant beteende som inte bör förekomma i konkurrensförhållanden. Lagen är således ett skydd mot illojalt beteende från konkurrenter.

Det rena kunskapsföretaget intar en särskild position vad gäller företagshemligheter genom att i stor utsträckning vara hänvisade till det skydd som lagen ger för företagets enda egentliga tillgång.

Slutligen kan man fråga sig om den avvägning som lagen gör mellan anställdas kunskap och företagens kunskap är lämplig? Ett problem är kopplingen av företagshemlighetsbegreppet till arbetstagarbegreppet. Hemlighetsbegreppet anknyter till arbetstagarbegreppet genom principen att arbetstagaren bara skall ha tillgång till vad denne behöver för att lösa sina arbetsuppgifter. Företagen måste således ha noggrann kontroll över vad som utgör ”hemligheter” och hur dessa hanteras inom organisationen. Vad som är företagets kunskap och vad som är den anställdes egen kunskap är inte alltid enkelt att avgöra - hur förhåller sig för övrigt detta till ”tyst kunskap” som formaliseras och på det viset förs över till företagets sfär?

Observatoriets slutsats är att FHL i och för sig är funktionsduglig och att det finns ett behov av en reglering av det slag som FHL utgör. Brister som uppmärksammats återfinns i utbildning, kunskap om lagstiftningen och strategier för dess användning.

En översyn bör dock göras av lagens arbetstagarbegrepp samt anpassningen av lagen till nya organisationsformer. När det gäller anknytningen till arbetstagarbegreppet vill observatoriet peka på de två projekt som observatoriet tidigare genomfört och som bl.a. berör denna fråga.

I det ena projektet togs ett diskussionsunderlag rörande behovet av nya associationsformer fram – ”Behov av nya associationsformer!? – ett diskussionsunderlag” - författat av Christina Helgesson.[1] I det andra projektet ”Fri agent, egenanställd, Ny daglönare ?!” belyser observatoriet på olika sätt det nya

[1] Det IT-rättsliga observatoriets rapport 15/2000 (www.itkommissionen.se/observ)

soloföretagandet. Även här fördes en diskussion om arbetstagarbegreppet, men också om behovet av en tredje anställningsform.[2]

[2] Se bl.a. Observatorierapport 31/2001 och IT-observatoriePM 14:2001 (www.itkommissionen.se/observ)

Inledning

Uppdraget

IT-kommissionen har givit Awapatent AB i uppdrag att för det IT-rättsliga observatoriets räkning författa en promemoria om ämnet företagshemligheter i en digital miljö. I promemorian skall ges en beskrivning av den verklighet i vilken reglerna om företagshemligheter skall tillämpas. Vidare skall göras en analys av rådande reglerings lämplighet för den digitala miljön samt lämnas eventuella synpunkter på hur regleringen bättre kunde utformas med hänsyn till de problem som IT-samhället medför för tillämpningen av reglerna.

Disposition

Promemorian är upplagd på följande sätt. Nedan följer ett inledande avsnitt. Detta avsnitt följs av en genomgång av vad som är kännetecknande för den miljö inom vilken reglerna för företagshemligheter skall tillämpas. Därefter följer en analys av om nuvarande reglering är lämplig med hänsyn till de förändringar den ökade användningen av digitala hjälpmedel medfört och hur regleringen eventuellt skulle kunna förbättras. Slutligen kommer en sammanfattning av promemorians slutsatser samt avslutande kommentarer.

Inledande kommentarer

Skyddet av företagshemligheter regleras i svensk rätt framförallt i lagen (1990:409) om skydd för företagshemligheter, nedan kallad FHL. En företagshemlighet definierar i 1 § FHL som ”sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende”. I FHL samlas regler om straff för brottsliga förfaranden med företagshemligheter, skadestånd för angrepp på en näringsidkares företagshemligheter och förbud vid vite att utnyttja eller röja en företagshemlighet. FHL har både då den infördes och senare utsatts för kritik av olika slag. Lagen beskylldes bland annat vid sin tillkomst för att inskränka yttrandefriheten. Lagen har på senare tid kritiserats för att den inte kan möta de krav som användning av ny teknik gett upphov till. Närmast kommer frågan om vilka förändringar användandet av den nya tekniken medfört att behandlas.

1. Kännetecken för den miljö inom vilken reglerna för företagshemligheter skall tillämpas.

Den ökade användningen av datorer och digital teknik påverkar snart sagt alla delar av samhället. Under en relativt kort tidsperiod har en stor del av företagen i Sverige genomgått en omvälvande datorisering, där allt fler rutiner och arbetsuppgifter sköts med hjälp av datorer. Hur har detta påverkat dessa företags hantering av företagshemligheter? Hur ser den verklighet ut i företagen i vilken reglerna om företagshemligheter skall tillämpas?

Externa intrång

En stor mängd företag har sina datorer anslutna till datornätverk med möjlighet till extern uppkoppling mot Internet. I dessa nätverk tar större delen av det informationsflöde som sker inom företagen plats. Hur dessa nätverk mer specifikt är uppbyggda varierar naturligtvis mellan företagen, men många av dem innefattar ett internt nätverk för informationsutbyte, e-post, såväl internt som externt, och tillgång till varandras filer. Lagring av företagshemlig information i nätverk med uppkoppling till Internet och framförallt sändande av företagshemlig information i e-brev medför betydande säkerhetsrisker för företagen. De flesta känner nog till att e-posttrafik kan avlyssnas, men använder av bekvämlighetsskäl eller i vissa fall av tanklöshet ändå e-brev som kommunikationsform. Nätverkens uppkoppling mot Internet medför ökade risker för intrång utifrån, med ökad risk för att företagshemligheter sprids utanför företagen som följd.

Intern tillgång till digitalt lagrad information

Samtidigt som företagens sårbarhet för angrepp utifrån ökar, är det så att de flesta dataintrång sker internt, det vill säga av de anställda själva. Ett sätt att komma över information man egentligen inte är behörig till är att gå in i andras datafiler och läsa eller kopiera dem. Vad gäller tillgång till andras filer, innehåller de flesta nätverk möjligheter att begränsa andras tillgång till de egna filerna. I verkligheten är det i många fall så att dessa möjligheter inte används, av bekvämlighetsskäl eller av okunskap. Det är inte heller konstigt, eftersom det i många fall kan vara motiverat att en person har tillgång till en annans persons filer, till exempel när denne är sjuk eller befinner sig på annan ort. Problem uppstår när man inte definierar vem som skall ha tillgång till vilka filer, utan låter alla ha tillgång till alla filer. Följden blir att anställda

har tillgång till information de egentligen inte behöver för att kunna sköta sina arbeten, varibland kan finnas även företagshemlig information. Denna företagshemliga information äventyras därmed i onödan, genom att informationen finns hos fler personer än nödvändigt.

Karaktären hos den information som lagras digitalt

I hur hög grad företagens sårbarhet ökar i och med användningen av digitala hjälpmedel beror naturligtvis på vilken information som lagras digitalt och vilken medvetenhet som finns hos de anställda i företagen om vad som är en företagshemlighet och hur den skall hanteras. Som nämnts inledningsvis definieras företagshemligheter i FHL som information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende. Under denna definition faller en stor mängd information av olika slag. Som exempel kan tänkas den lilla fiskkonservfabriken vars viktigaste företagshemlighet utgörs av receptet till en sillinläggning. Man kan också tänka sig uthyrningsföretagets kundförteckning, men också informationen om vilka kunder företaget har, även om denna information aldrig dokumenterats utan bara existerar i de anställdas huvuden. Förmodligen är det så att en stor del av företagshemligheterna inte finns på något medium utan bara i medarbetares huvuden. Denna information påverkas inte av den ökade användningen av digitala hjälpmedel. Samtidigt medför den ökade möjligheten att informera personalen via interna nätverk sannolikt att fler uppgifter sprids inom företagen än tidigare, framförallt eftersom det anses vara viktigt för medarbetarnas delaktighet i arbetet att de är så väl informerade som möjligt.

Kopiering

Att informationen är lagrad på ett digitalt medium påverkar också möjligheterna till kopiering och kontrollen av hur många exemplar som framställts av ett dokument. Att duplicera en fil på en dator går sekundsnabbt, medan exempelvis fotokopiering tar längre tid. Fotokopieringen blir mycket mer synlig än motsvarande handling på datorn, eftersom det syns på den framställda fotokopian att det är en kopia och inte ett original. Därtill kommer att man i de flesta fall måste lämna sitt skrivbord och gå bort till en kopiator för att kopiera. Om någon snabbt kopierar en datafil sittandes vid sitt skrivbord är chanserna mindre att någon skall upptäcka detta. Information som finns tillgänglig i pappersform kan enkelt överföras till ett

digitalt medium genom skanning. Härigenom uppstår de konsekvenser som beskrivits ovan.

Den enkelhet med vilken datafiler kan mångfaldigas medför också sämre kontroll av hur många exemplar som framställts av ett visst dokument. Om ett dokument i pappersform skall distribueras till tio personer, blir det påtagligt att dokumentet mångfaldigas när det kopieras. Om dokumentet däremot finns i form av en datafil, blir det inte lika uppenbart att tio exemplar av dokumentet framställts när ett e-brev med dokumentet bifogat sänts till tio mottagare. Inte bara kontrollen av antalet exemplar blir sämre, utan också kontrollen av innehållet. När tio exemplar av en datafil distribuerats, lever dessa tio filer ett eget liv. De kan med lätthet ändras av den som innehar filen och därmed är det inte längre en kopia av det ursprungliga dokumentet, även om det ser så ut. Det finns idag tekniska hjälpmedel som gör att man kan spåra vilka ändringar som gjorts i ett dokument och av vem, men det är långtifrån alla företag som använder sig av dessa system. Det är dessutom så att detta inte alltid hjälper när den ändrade kopian av en datafil skrivs ut i pappersform, eftersom det inte behöver framgå på pappret vilka ändringar som gjorts och av vem. Å andra sidan kan de företag som använder tekniska hjälpmedel för spårning faktiskt uppnå ett bättre skydd än man hade när informationen inte lagrades digitalt, eftersom man med teknikens hjälp kan identifiera den som gjort intrång.

Nätverksorganisationer

Utöver den direkta effekt på hanteringen av företagshemligheter som den utökade användningen av digitala hjälpmedel medför, påverkar andra förändringar inom företagen också denna hantering. Företagen organiseras allt oftare i vad som kan kallas nätverksorganisationer, som kännetecknas av att de är mindre hierarkiska och mer platta organisationer där ansvar delegeras i stor omfattning. I denna typ av organisationer arbetar de anställda ofta i olika projektgrupper eller nätverk, som definieras av den uppgift man för stunden har att lösa eller den särskilda kompetens man besitter inom gruppen. Dessa grupper löper ofta tvärs genom företag utan hänsyn till exempelvis geografisk placering. Samma person kan också vara med i flera olika grupper. I nätverksorganisationerna flödar informationen mellan medarbetarna som en del av det dagliga arbetet. I en mer traditionell, hierarkisk organisation skall informationen upp till chefsnivå, vidare mellan cheferna och sedan ned till en annan anställd. En viss del av informationen kommer då inte att vandra hela vägen, vilket

minskar informationsflödet. Den utökade användningen av nätverksstrukturer, där information flyter mer fritt än i mer traditionella organisationer, leder till att företagshemligheter blir mer spridda och därmed utsätts för större risker att spridas utanför företaget.

Kunskapsföretag

I samband med att den ökade användningen av digitala hjälpmedel och då främst datorer diskuteras, måste en näraliggande företeelse, de s k kunskapsföretagen, nämnas. Dessa företag är affärsdrivande verksamheter som erbjuder kunskapsbaserade tjänster. De viktigaste tillgångarna utgörs ofta av företagens affärsidéer och de anställdas kunskaper. I dessa företag blir frågorna om vad som är en företagshemlighet och hur de kan skyddas särskilt aktuella och tydliga, eftersom företagens viktigaste tillgångar inte kan skyddas på så många andra sätt än genom FHL. Kunskapsföretagens situation kommer därför närmare att beröras i nästa avsnitt, som rör frågan om hur ändamålsenlig FHL:s reglering är med hänsyn till de förändringar som den utökade användningen av digitala hjälpmedel medfört.

2. Nuvarande reglerings lämplighet med hänsyn till de förändringar den ökade användningen av digitala hjälpmedel medfört.

Den ökade användningen av digitala hjälpmedel har som ovan påpekats påverkat företagens hantering av företagshemlig information såväl gentemot utomstående som inom företaget. Externt har de interna nätverkens uppkoppling mot Internet lett till ökad sårbarhet för angrepp. Internt har åtkomsten till andras datafiler inom företagen, karaktären hos den information som lagras digitalt och kunskapen om denna informations företagshemliga karaktär, möjligheten till kopiering av datafiler, utvecklingen av nätverksorganisationer samt kunskapsföretagens speciella situation lett till ökad risk för att företagshemlig information sprids till en allt större krets av anställda för att slutligen hamna utanför företaget. Nedan skall analyseras om FHL:s reglering av skyddet för företagshemligheter är lämplig med hänsyn till de förändringar som den ökade användningen av digitala hjälpmedel lett till.

Externa intrång

Så som framgått ovan, har företagens ökade användning av datanätverk, uppkopplade mot Internet, lett till ökad risk för intrång utifrån. Den ökade användningen av extern e-post har lett till ökad risk för avlyssning av meddelanden. Härigenom har företagens sårbarhet ökat, eftersom risken att företagshemlig information hamnar utanför företagen, i fel händer, har ökat. Här rör det sig dock om angrepp som är straffbelagda, bland annat som företagsspionerі enligt 3 § FHL eller som dataintrång enligt 4 kap. 9c § brottsbalken. Genom att kriminalisera handlingarna, har lagstiftaren tillgripit det starkaste medlet att bekämpa ett icke-önskvärt beteende som finns att tillgå. Lagstiftningen har således inte blivit omodern på grund av den tekniska utvecklingen, utan omfattar denna typ av situation. Det finns inte heller något som tyder på att straffstadgandenas utformning skulle medföra problem vid lagföring. Om det är så att denna typ av brottslighet ökar, är det snarare så att mer resurser bör satsas på utredning och lagföring av dessa brott än att reglerna bör ändras. Utöver detta torde bättre tekniskt skydd och utbildning av anställda om företagshemligheter samt ökad medvetenhet om säkerhetsproblemen vara framkomliga vägar för att komma åt problemet.

Intern tillgång till digitalt lagrad information

Det har anmärkts ovan att anställda i allt större omfattning har tillgång till varandras datafiler. Den tekniska möjligheten att få tillgång till andras datafiler, medför dock inte att det är tillåtet att bereda sig tillträde till dessa filer. Att anställda olovligen bereder sig tillträde till information och sedan sprider denna, utgör i praktiken ett större problem än externa intrång. De anställda gör sig dock skyldiga till brott på samma sätt som de som externt bereder sig tillträde till information. Vad gäller detta problem hänvisas därför till föregående avsnitt.

Den ökade möjligheten till fildelning leder till ökad spridning av olika sorters information, bland annat företagshemlig sådan. Härigenom uppkommer två problem, dels ökar risken för att informationen hamnar utanför företaget varje gång ytterligare en anställd får ta del av informationen, dels riskerar information att ha fått sådan spridning att den inte längre utgör en företagshemlighet. Att information riskerar att hamna utanför företaget på grund av att den sprids till alltför många inom företaget, är en fråga av mer praktisk art. Ju fler personer som känner till en

hemlighet, desto större är risken att hemligheten röjs. Liksom vid situationen där intrång sker utifrån är här fråga om att företagen blir mer sårbara. Detta påverkas inte av hur FHL:s reglering är utformad, eftersom det här är fråga om att rent praktiskt minimera företagens risker genom att kontrollera spridningen av företagshemlig information.

Vad gäller risken att informationen upphör att vara en företagshemlighet, framgår av 1 § FHL att med företagshemlighet avses ”sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller *hemlig*...” (författarens kursivering). Företagshemligheter måste alltså, per definition, hållas hemliga, annars utgör de inte företagshemligheter och skyddas därmed inte av FHL. Vad gäller kravet på hemlighållande uttalade departementschefen följande i propositionen till FHL. ”I uttrycket hemlig ligger att informationen inte får vara tillgänglig för envar som kan ha ett intresse av att ta del av den. Hemlighållandet har således en relativ innebörd. Inom företag kan information rent allmänt sägas vara hemlig, om den inte får yppas till andra än de anställda som behöver den för att fullgöra sitt arbete. I ett mindre företag kan detta innebära att alla inom företaget känner till hemligheten. Inom ett storföretag kan informationen vara känd inom en eller flera avdelningar men likväl – totalt sett – vara hemlig.”[3] FHL:s hemlighetsbegrepp ställer således stora krav på företagen. Det är nödvändigt att se till att endast de som behöver informationen för sitt arbete har tillgång till den. I de lite större företagen är det därmed inte självklart att alla anställda kan ha tillgång till informationen och därför måste det interna informationsflödet både analyseras och kontrolleras.

Företagen kan naturligtvis inte agera helt oberoende av andra, inte heller vad gäller skyddet av företagshemligheter. Vad gäller kravet på hemlighållande vid kontakter utanför företaget, uttalade departementschefen följande i propositionen till FHL. ”Inte ens företaget som sådant bildar emellertid en absolut gräns för hemlighållandet. Vid exempelvis organiserat samarbete, licensgivning eller legotillverkning innebär inte det förhållandet att informationen förs utanför det egna företaget att hemlighållandet gått förlorat. När spridningen går utanför företaget får den dock inte vara allmän och okontrollerad. För att bibehålla sin status av hemlig får

[3] Proposition 1987/88:155 om skydd för företagshemligheter, sid. 35.

informationen således inte spridas utanför en krets som åtminstone i princip är identifierbar och sluten.”[4] Det är således inte så att viss spridning av information utanför företaget automatiskt leder till att denna information inte utgör en företagshemlighet. Avgörande för om informationen fortsätter att utgöra en företagshemlighet är kontrollen av dess spridning, att informationen bara delges en viss, väl definierad grupp.

Är de krav på hemlighållande som redogjorts för ovan väl avvägda? Hemlighetskravet utgör en central del av definitionen av vad som skyddas såsom en företagshemlighet. FHL syftar till att skydda information som är viktig för verksamheten. Denna information hålls med anledning därav hemlig och ett röjande av densamma leder till skada i konkurrenshänseende. Tar man bort kravet på att informationen skall vara hemlig, måste hela definitionen av en företagshemlighet omarbetas, för vilken skada medför ett röjande av redan känd information? Även om man skulle vara villig att göra detta, skulle det då inte längre vara fråga om en lagstiftning om skydd för företagshemligheter. Därmed är det inte sagt att den avvägning av hur hemlighållandet skall ske är den enda möjliga. Det förefaller visserligen som en mycket god idé att knyta an till om informationen behövs för arbetet internt och om det är en kontrollerad, väl definierad spridning externt. Vad som däremot kan ifrågasättas är den koppling till anställning som rent generellt görs i FHL och mer specifikt i departementschefens ovan citerade uttalande avseende det interna hemlighetskravet. Hur skall olika former av uppdragstagare, exempelvis konsulter, behandlas? Dessa borde rimligen jämställas med anställda, i vart fall om de utför annat än helt kortvariga arbeten för företaget i fråga. Vad gäller kravet på hemlighet medför dock denna fokusering på anställda troligen inte något problem, eftersom uppdragstagarna ändock i de flesta fall måste anses vara en väl definierad och avgränsad grupp. Som framgått ovan åtnjuter då informationen skydd såsom en företagshemlighet. Vad gäller uppdragstagarna är det dessutom så att de befinner sig i någon form av avtalsförhållande med uppdragsgivaren. Frågor om bland annat sekretess kan således regleras i avtalet mellan dem. Detta kan vara ett bra sätt att upprätthålla skyddet för företagshemligheter, under förutsättning att parterna är jämbördiga, eftersom en underlägsen part kan påtvingas sekretessåtaganden långt utöver vad som är nödvändigt eller från en allmän utgångspunkt lämpligt.

---

[4] Proposition 1987/88:155 om skydd för företagshemligheter, sid. 35.

Karaktären hos den information som lagras digitalt

Mycket information av företagshemlig karaktär finns idag lagrad på digitala medier. Vilken information som lagras på detta sätt och hur tillgänglig informationen är för de anställda påverkar i hög grad hur väl skyddade företagshemligheterna är i ett visst företag. Som redan nämnts ett antal gånger är kunskap om vad en företagshemlighet är, vilken betydelse den har och hur den skyddas av yttersta vikt för att uppnå ett fullgott skydd för företagshemligheter. Likaså är det mycket viktigt att medvetandegöra de anställda om företagshemligheternas existens. Det räcker inte att veta vad en företagshemlighet är, man skall också överväga om något kan utgöra en företagshemlighet innan man lämnar ut information. För att bättre möta de problem som uppstår, krävs således kunskap om de regler som redan finns. Väl avvägda beslut om vilken information som över huvud taget lagras digitalt och vilka som skall ha tillgång till den kan förbättra företagens skydd, liksom höjd medvetandegrad hos de anställda om att information som de handskas med i sitt arbete kan vara en företagshemlighet. Det är alltså mer en fråga om utbildning och upplysning än ändrad lagstiftning. Detta är en praktisk fråga där det är svårt att ser hur man genom ändringar i FHL skulle kunna åstadkomma en lösning. Problemet är inte att FHL:s regler är otillräckliga, utan att det inom företagen saknas kunskap.

Kopiering

Lagring av information på digitala medier medför att det blir lättare att kopiera informationen och att kontrollen av hur många exemplar som framställts blir sämre. De förbättrade möjligheterna till kopiering leder till ökad sårbarhet för företagen, eftersom det underlättar illegala angrepp på företagshemligheter. Den försämrade kontrollen av hur många exemplar som framställts, leder till försämrad kontroll över vilken spridning den digitalt lagrade informationen har fått . Kontrollen av spridningen av informationen är som vi sett ovan viktig för att säkerställa att informationen alltjämt utgör en företagshemlighet. Kan man inte med säkerhet säga exakt hur många exemplar innehållande viss information som framställts, kan man heller inte med säkerhet avgöra om informationen är skyddad som en företagshemlighet.

Vad gäller frågorna om förenklad kopiering och försämrad kontroll av kopior, kan paralleller dras till resonemangen ovan kring ökad sårbarhet och FHL:s hemlighetsbegrepp. Den ökade sårbarheten är ett problem av praktisk natur,

eftersom olovliga tillgrepp av företagshemligheter är straffbelagda. Det finns således redan möjligheter att ingripa mot dem som gjort sig skyldiga till tillgreppet och det återstår därmed att försöka förhindra att dessa personer över huvud taget får tillgång till informationen. Det senare är en praktisk fråga som inte påverkas av utformningen av FHL:s regler.

Vad gäller risken att information sprids i sådan omfattning att den inte längre utgör en företagshemlighet, har FHL:s hemlighetsbegrepp analyserats ovan. Detta begrepp blir centralt för de problem som uppstår i anledning av ökad spridning av företagshemlig information. Så som anförts ovan, synes FHL:s reglering i denna fråga i huvudsak väl avvägd, även om man kan ha invändningar mot den anknytning till begreppet arbetstagare som görs.

Nätverksorganisationer

Ovan har konstaterats att företag allt oftare organiseras i nätverksorganisationer och att information flyter mer fritt i dessa organisationer än i mer traditionellt uppbyggda. Detta leder till att företagshemligheter blir mer spridda i denna typ av organisation och att dessa hemligheter därmed utsätts för större risker att spridas utanför företaget. På sätt som konstaterats ovan, aktualiserar ökad spridning av företagshemligheter inom ett företag problem med illegala tillgrepp inom företaget, ökad sårbarhet för företagets information och risk för att information blir spridd i en sådan omfattning att den inte längre utgör en företagshemlighet. Det första och det andra av dessa problem, ökad risk för illegala tillgrepp och ökad sårbarhet, kan inte avhjälpas genom förändrad lagstiftning. Det tredje problemet, risk för att informationen inte längre utgör en företagshemlighet, hör samman med FHL:s hemlighetsbegrepp. Vad gäller detta begrepp, som analyserats ovan, synes FHL:s reglering i huvudsak väl avvägd, även om man kan ha invändningar mot den anknytning till begreppet arbetstagare som görs.

Kunskapsföretag

Kunskapsföretagen nämndes mycket kort i föregående avsnitt. Det särskiljande för dessa företag var att deras viktigaste tillgångar ofta utgörs av företagens affärsidéer och de anställdas kunskaper. Dessa tillgångar, som är immateriella, blir företagen starkt beroende av. Inledningsvis är det viktigt att påpeka

att företagen ofta är hänvisade till antingen FHL:s regler eller till att genom avtal med de anställda skydda sig. Vissa affärsmetoder kan visserligen skyddas av patent. Affärsidéer som kommit till uttryck i till exempel pappersform eller i form av en databas kan åtnjuta upphovsrättslig skydd. I huvudsak är företagens affärsidéer och de anställdas kunskaper dock endast möjliga att skydda såsom företagshemligheter. Vilket skydd erbjuder då FHL dessa företag?

Vad gäller kunskapsföretagens affärsidéer behandlas dessa på samma sätt som annan för företagen viktig information. Affärsidéer är i allmänhet att anse som information om affärs- eller driftförhållanden i en näringsidkares rörelse och hålls dessa idéer hemliga, är ett röjande ägnat att medföra skada i konkurrenshänseende. De utgör därmed företagshemligheter som skyddas enligt FHL:s regler. Att den företagshemliga informationen utgörs av affärsidéer förändrar inte hur de behandlas. Några för kunskapsföretagen specifika problem rörande skyddet för affärsidéer uppstår således inte.

Vad gäller de anställdas kunskaper måste en skiljelinje dras mellan vad som å ena sidan är de anställdas personliga kunskaper och å andra sidan vad som är företagsspecifik information. Det skulle vara orimligt om all den kunskap, skicklighet och allmän levnadsvisdom som de anställda har när de påbörjar en anställning skulle vara företagens egendom, enkom av den anledningen att de blivit anställda av företaget. Lika orimligt skulle det motsatta förhållandet vara, att all kunskap om exempelvis affärsmetoder, kunder och tillverkningsprocesser skulle vara de anställdas egendom. De skulle då fritt kunna avsluta sin anställning, starta konkurrerande verksamhet och använda sig av de kunskaper de tillgodogjort sig hos sin tidigare arbetsgivare, utan att ha behövt göra de ansträngningar och i många fall de ekonomiska åtaganden som varit nödvändiga för att komma fram till den aktuella informationen. Dessa intressen måste således vägas mot varandra.

I propositionen till FHL uttalade departementschefen följande angående gränsdragningen mellan företagshemlig information och personlig skicklighet eller kunskap. ”En gräns måste emellertid dras mellan sådan information om affärs- och driftförhållanden som finns i näringsidkarens rörelse och vad som kan klassas som personlig skicklighet, erfarenhet och kunskap hos någon som är anställd i näringsverksamheten. Denna gräns kan visserligen mera sällan förväntas bli av praktisk betydelse. Principen bör vara att information som vem som helst med

adekvat utbildning kan omsätta i praktiskt resultat bör anses som information i näringsidkarens rörelse. Är emellertid informationen knuten till individen, så att den inte genom en instruktion eller en anvisning kan överflyttas till någon annan, bör den anses vara av personlig art och således inte ingå i näringsidkarens rörelse."[5] Denna gränsdragning kan i praktiken bli svår att dra. Departementschefen hänvisade i propositionen till ett utredningsbetänkande, där följande hjälpregel anges. "Som en ledande princip bör gälla att sådant som rimligtvis kan klassificeras som personlig skicklighet, erfarenhet och kunskap skall få fritt nyttjas av den som besitter det."[6] Detta innebär att en stor del av de anställdas kunskaper i kunskapsföretagen kommer att falla under begreppet "personlig skicklighet, erfarenhet och kunskap" och därmed inte utgöra en företagshemlighet. Detta får till följd att kunskapsföretagen inte kan uppnå skydd för en av sina viktigaste tillgångar.

Som ovan anförts, måste en intresseavvägning ske mellan vad som tillhör de anställda och företaget. Att låta all information vara ena partens förefaller helt orimligt. Den avvägning som gjorts kan kritiseras, framförallt därför att den är svårtillgänglig och det är svårt att avgöra i förväg vilken information som kommer att anses utgöra en företagshemlighet. Samtidigt är det oerhört svårt att definiera och avgränsa ett begrepp som innefattar så vitt skilda företeelser som företagshemligheter gör. I sammanhanget bör man också något se till i vilken situation problemen med företagshemligheter i kunskapsföretagen kan förväntas uppstå. Typfallet torde vara att de anställda lämnar ett företag för att starta eller medverka i konkurrerande verksamhet. Då uppkommer problemet vilken information som är arbetstagarens egen och vilken som tillhör den tidigare arbetsgivaren. Arbetstagarens övergång i konkurrerande verksamhet ger dock upphov till fler problem än de som rör företagshemligheter. Dessa problem löses i många fall av konkurrensklausuler, som reglerar arbetstagarens rätt att bedriva konkurrerande verksamhet. Svensk rätt har en sträng syn på sådana konkurrensklausuler, men i vissa fall kan de användas och då utgöra ett viktigt komplement till reglerna om skydd för företagshemligheter.

Räcker då det skydd som FHL, eventuellt kompletterad med en konkurrensklausul, ger? Det kan för kunskapsföretagens del vara tveksamt. Samtidigt

---

[5] Proposition 1987/88:155 om skydd för företagshemligheter, sid. 35.

[6] Proposition 1987/88:155 om skydd för företagshemligheter, sid. 35, SOU 1983:52 sid. 373.

bör man vara försiktig om man vill ändra den avvägning av olika intressen som gjorts. Om mer information blir företagshemlig på bekostnad av vad som tidigare ansågs vara arbetstagarens personliga skicklighet, erfarenhet och kunskap, riskerar arbetstagaren att bli hårdare bunden till arbetsgivaren. I slutändan kan det bland annat få effekter på arbetsmarknadens rörlighet. För det enskilda företaget kan ökad rörlighet på arbetsmarknaden upplevas som negativt, eftersom det kan medföra att betydelsefulla personer lämnar företaget. I ett vidare perspektiv är dock ökad rörlighet på arbetsmarknaden ett eftersträvansvärt mål, eftersom det underlättar för företag att rekrytera den personal man behöver och minskar arbetslösheten. Jag tycker därför det är tveksamt att ändra den avvägning som gjorts, i vart fall i avsaknad av indikationer på att detta skulle utgöra ett mycket stort problem.

3. Sammanfattande och avslutande synpunkter.

Ovan har olika aspekter av vad som är kännetecknande för den miljö inom vilken reglerna för företagshemligheter skall tillämpas med hänsyn till den ökade användningen av digitala hjälpmedel nämnts. Därefter har FHL:s möjligheter att svara mot de krav som utnyttjandet av den nya tekniken leder till analyserats. Den ökade användningen av digitala hjälpmedel har framförallt visat sig leda till en ökad sårbarhet för företagen på en mängd olika sätt. Det har kunnat konstateras att lösningen på dessa problem inte står att finna i ändrade regler för skydd av företagshemligheter, eftersom de inte kan sägas vara otidsenliga eller gammalmodiga. Dessa problem kan snarast avhjälpas med förbättrade tekniska lösningar för skydd av information, utbildning av de anställda om betydelsen av företagshemligheter och regleringen av desamma samt utarbetande av strategier för vilken information som skall lagras digitalt och i så fall hur. Företagen får ta ett större eget ansvar för att skydda sina företagshemligheter, till exempel genom att reglera handhavandet av dem i avtal med anställda och uppdragstagare.

Den nya tekniken har lett till problem vad gäller när information skall anses ha hållits hemlig och vilken information som tillhör arbetsgivare respektive arbetstagare. Vad gäller problemen kring hemlighetsbegreppet, som är centralt för definitionen av vad som är en företagshemlighet, har det visat sig svårt att ge förslag till ändringar av den avvägning som gjorts. Vad som kan kritiseras är den anknytning till arbetstagarbegreppet som görs, dels då vad som hållits hemligt skall definieras,

dels generellt i FHL. Med tanke på den utveckling som skett på arbetsmarknaden med inhyrd personal, s.k. outsourcing av hela enheter och användandet av konsulter verkar det tveksamt att låta reglerna helt anknyta till arbetstagarbegreppet. Uppdragstagarnas och de uthyrda arbetstagarnas situation är i många avseenden helt jämförbar och det verkar inte sakligt motiverat att inte behandla dem på samma sätt som arbetstagarna.

Vad slutligen rör vilken information som skall anses utgöra arbetsgivarens respektive arbetstagarens egendom, har det konstaterats att avvägningen mellan de inblandades intressen är mycket svår att göra och att nuvarande reglering inte bör ändras, med mindre det framkommer att den medför mycket stora problem.

Diskussionsfrågor inför seminariet

- Är det med hänsyn till det ökade flödet av information över huvud taget praktiskt möjligt att skydda företagshemligheter idag? Finns det någon lösning på det förhållandet att information synes få ett allt större värde samtidigt som den flyter alltmer fritt?

- Bör vi överhuvudtaget skydda företagshemlig information? Görs inte detta bättre genom avtal, som kan anpassas till såväl teknisk utveckling i allmänhet som den enskilda situationen?

- Är den definition av kravet på hemlighållande som tillämpas i Sverige lämplig?

- Är den avvägning som görs mellan anställdas kunskap och företagens kunskap i Sverige lämplig?