



A Juridik White Paper

Finns det juridiska skäl för att logga – och är det tillåtet?

Abstract

Loggning av anställda och användning av spärprogram föranleder en rad juridiska frågor, bland annat beträffande det straffrättsliga medverkansansvaret, arbetsrättsliga aspekter samt rättsregler till skydd för den personliga integriteten. Här ska vissa viktiga sådana aspekter behandlas. Allmänt sett kan sägas att det, ur en juridisk synvinkel, är önskvärt att arbetsgivaren tar till vara möjligheten att, genom åtgärder såsom utnyttjande av loggning och spärprogram, utöva viss kontroll över de anställdas surfvanor mm. Arbetsgivarna bör dock vara noga med att redovisa vilka åtgärder som kommer att vidtas och syftet med dem. Det är också lämpligt att åtgärderna såvitt möjligt förankras i anställningsavtalen.

PM:en görs med utgångspunkt från svensk lag. Denna bygger dock i sin tur i viss utsträckning (särskilt beträffande integritetsaspekter) på EG-rättsliga direktiv, samt även på en gemensam rättstradition. Det är därför troligt att det rättsläge som beskrivs ger en någorlunda god bild av vad som gäller också i de nordiska grannländerna.

Fokus kommer att ligga på loggning. Att använda spärprogram (filter) är en mindre ingripande åtgärd. De juridiska skälen för att använda spärprogram är ungefär desamma som för loggning. Spärprogram innebär i huvudsak heller inte att en personuppgift "behandlas". Det råder därför knappast någon tvekan om att sådana program är lagliga ur en integritetsaspekt. Att börja använda ett sådant kan liknas vid att en av organisationens rum läses och att personalen förbjuds att gå in i rummet. Arbetsgivaren kan vidta en sådan åtgärd utan större juridiska problem.

Harry Schüssler
Jur kand och expert på IT-juridik

PM:en består av två delar enligt följande:

I. Juridiska skäl för loggning	3
• Arbetsgivarens ansvar vid fildelning	3
• Barnpornografibrott mm	4
• Bedrägeri (phishing mm) – juridiska risker för en passiv arbetsgivare	4
• Vad som gäller inom arbetsrätten – vikten att ha kontroll	4
II. Är loggning och spärrprogram förenligt med personuppgiftslagen mm?	5

I. Juridiska skäl för loggning

Arbetsgivarens ansvar vid fildelning

Det kan finnas flera skäl till att en arbetsgivare vill motverka att anställda ägnar sig åt fildelning på arbetsplatsen och/eller bedriver sådan verksamhet med hjälp av arbetsgivarens arbetsredskap. Det kan exempelvis finnas en risk för att organisationens rykte försämras av att förknippas med något olagligt. Även strikt juridiskt finns det risker för arbetsgivaren med att låta sådan verksamhet fortgå. Förbudet mot fildelning återfinns i upphovsrättslagen. Enligt 46 § i denna är det i princip förbjudet för den som inte har upphovsrätten att göra framställningar tillgängliga för allmänheten (genom exempelvis fildelning). Straffet är dagsböter eller fängelse i högst två år, se 53 §.

Det är dock inte endast den som själv aktivt fildelar som kan dömas för brott mot upphovsrättslagen. Det finns också ett så kallat medverkansansvar. Den som främjar gärningen genom att exempelvis tillhandahålla utrustning riskerar således att dömas för upphovsrättsbrott. Det har varit oklart i vilken utsträckning som det har funnits ett medverkansansvar på upphovsrättens område. Den europeiska unionens parlament har dock våren 2007 antagit ett direktiv (IPRED2) som lägger fast ett medverkansansvar. I framtiden kommer det därför knappast att råda någon tvekan om att även en medverkande kan dömas för upphovsrättsbrott.

Förutom det straffrättsliga ansvaret riskerar den som har medverkat att bli skadeståndsansvarig mot den som har upphovsrätten till det verk som fildelas. En egenhet med brott mot upphovsrättslagen är att det inte krävs så kallat uppsåt. För att någon ska dömas är det tillräckligt att denne varit grovt oaktsam. I praktiken kan detta betyda att den som på ett flagrant sätt försummat att vidta tekniska åtgärder för att förhindra fildelning kan dömas för upphovsrättsbrott, trots att personen var omedveten om att fildelning verkligen pågick. Den grad av aktsamhet som krävs varierar. I takt med ökade tekniska möjligheter att motverka fildelning ökar också de krav som kan ställas på arbetsgivare. I nuläget kan det räcka med att informera de anställda samt att iaktta viss vaksamhet. Men den arbetsgivare som vill vara på den säkra sidan och samtidigt vara rustad för den skyddsnivå som i en snar framtid är nödvändig bör överväga att använda spärprogram och ett system för loggning.

En speciell situation är att fildelningen görs som ett led i utförandet av en arbetsuppgift. Den anställda kan exempelvis ha fått i uppgift att ta fram ett underlag inför en konferens och har löst uppgiften genom att begagna sig av fildelning. Arbetsgivaren riskerar då att få betala skadestånd genom det principalansvar som följer av skadeståndslagen 3:1. Skyldigheten för organisationen att utge skadestånd föreligger även om arbetsgivaren inte alls gjort något värdslost. Vid sidan av den skadeståndsrättsliga sanktionen finns en risk för förverkande av de tekniska hjälpmedel (exempelvis hårddiskar mm) som använts vid fildelningen. Detta följer av upphovsrättslagen 53a §.

Det finns också andra juridiska fördelar med ett adekvat skyddssystem, förutom att risken för straff och skadestånd minskar. Om fildelning har ägt rum på arbetsplatsen kan denna bli utsatt för husrannsakan respektive inträngsundersökning. Husrannsakan beslutas normalt sett av åklagaren och genomförs av polisen i avsikt att samla bevis om brott. Inträngsundersökning görs på begäran av en rättighetsinnehavare (exempelvis ett musikförlag). Tingsrätten fattar beslut om en inträngsundersökning och denna genomförs sedan av kronofogdemyndigheten. Inträngsundersökningen syftar till att säkra bevis om att intrång i en rättighet har skett. Dessa åtgärder (husrannsakan och inträngsundersökning) innebär inte i sig att arbetsgivaren misstänks ha begått något fel, men självfallet kan de störa verksamheten och leda till ryktesspridning.



Barnpornografibrott mm

Att en organisation inte vill förknippas med barnporr är givet. Vid sidan av etiska skäl, och risker för en försämrad goodwill, finns det juridiska orsaker till att barnpornografi och så kallad grooming bör motverkas genom loggning mm. Det är numera straffbart att inneha barnpornografi, se brottsbalken 16:10 a§. Grooming (som något förenklat innebär att en vuxen i sexuellt syfte kontaktar en person under 15 år) väntas bli straffbart framöver.

För barnpornografibrott kan även den straffas som medverkar till huvudbrottet. Detsamma lär komma att gälla för grooming. Noteras kan dock att barnpornografi normalt sett är ett brott som kräver uppsåt, vilket minskar risken för exempelvis en VD eller annan chef att bli dömd med anledning av att en anställd begått ett brott. Om barnporr sprids i yrkesmässig verksamhet eller i förvärvssyfte räcker det dock med oaktsamhet för att bli dömd.

En positiv sidoeffekt av loggning är att en person som felaktigt har anklagats för exempelvis grooming har lättare att värja sig om det finns loggfiler till hands som den anklagade kan använda för att bevisa sin oskuld.

Bedrägeri (phishing mm) – juridiska risker för en passiv arbetsgivare

På Internet förekommer en rad olika bedrägeriförsök. Dessa riktar sig i vissa fall mot den enskilde anställda, men kan också vara ekonomiskt kännsbara för arbetsgivaren. En möjlig situation är exempelvis att den anställda besöker en oseriös hemsida och ofrivilligt ingår ett avtal å bolagets vägnar, genom att klicka i en kryssruta. Organisationen kan då under vissa förutsättningar bli tvungen att prestera enligt avtalet, exempelvis betala den summa som anges i "avtalsvillkoren". En förutsättning för sådan bundenhet är i princip att den anställda haft behörighet att ingå avtalet. Som arbetsgivare bör man då betänka att alla anställda har en viss, större eller mindre, behörighet (se avtalslagen 10 § 2 stycket). Behörighetens omfattning framgår av sedvänjan. Avgörande är alltså vad en anställd med denna typ av arbete brukar få göra. Om den anställda har behörighet att ingå avtal kan organisationen slippa ifrån avtalet (med stöd av avtalslagen 11 § 1 stycket) genom att bevisa att motparten kände till eller borde ha känt till att den anställda enligt organisationens interna instruktioner saknade rätt att ingå just den här typen av avtal (befogenhet). Detta är normalt sett svårt.



Även i situationer där den anställda luras att ingå avtal men saknar behörighet kan bundenhet uppstå, nämligen om arbetsgivaren är passiv och inte meddelar motparten att organisationen inte önskar ingå något avtal.

Konsekvensen av ovanstående är dels att det kan vara tillrädligt att genom information och spårprogram undvika att den anställda besöker olämpliga sidor, dels att arbetsgivaren bör hålla sig informerad om de sidor som har besökts så att oönskade avtal kan avstyras. En ytterligare fördel med en hög säkerhetsnivå är att det i händelse av ekonomisk skada blir lättare att få ut försäkringsersättning. I försäkringsavtal förekommer regelmässigt en skrivning som innebär att försäkringsbolagets skyldighet att utge ersättning helt eller delvis faller bort när försäkringstagaren har varit grovt vårdslös (alternativt endast vårdslös). Risken för en sådan invändning från försäkringsbolagets sida minskar kraftigt om organisationen har varit aktsam nog att skydda sig genom att använda program för loggning och filtrering mm.

Vad som gäller inom arbetsrätten – vikten att ha kontroll

Många organisationer har varit noga med att reglera de anställdas möjligheter att surfa på Internet. Detta kan ha skett genom konkreta angivelser i det individuella anställningsavtalet. Vanligare är dock att detta görs i en internetpolicy, som den anställda informeras om och förbinder sig att följa. Det är viktigt att det som står i policyn överensstämmer med vad som verkligen gäller inom organisationen. En hård policy och en överslätande attityd i praktiken kan göra att policyn tappar sin juridiska verkan. Den anställda kan, i händelse av en senare arbetsrättslig tvist, med fog hävda att arbetsgivaren har haft en tillåtande attityd och att detta därigenom har förändrat innehållet i avtalet. En kanske mödosamt framtagen och ändamålsenlig policy blir därmed, åtminstone delvis, utan verkan.

II. Är loggning och spårprogram förenligt med personuppgiftslagen mm?

Det torde inte råda någon tvekan om att bruket av ett spårprogram i sig är förenligt med personuppgiftslagen. Den övervakande myndigheten, Datainspektionen, har själv uttryckt sig positivt om företeelsen (se DI:s rapport 2005:3, sidan 16), och har konstaterat att ett spårprogram kan övervägas om arbetsgivaren vill undvika oetisk surfning. Även så kallad loggning är tillåten. Men både för spårprogram och loggning gäller att organisationen måste använda metoderna på ett sätt som överensstämmer med reglerna rörande integritetsskydd och arbetsrätt.

Det är naturligt att anta att en loggning görs så att enstaka personer senare kan sökas fram ur de filer som produceras. Resultatet kan med andra ord sägas vara, i juridisk mening, strukturerat. Därmed gäller personuppgiftslagens hanteringsregler. Detta innebär i sin tur att hanteringen av personuppgifter måste ha stöd i personuppgiftslagen. Motsvarande gäller bruket av spårprogram, om detta avsåtter resultat i form av en rapport eller liknande. Om det endast är ett filter som hindrar besök på vissa webbsidor uppstår inget problem rörande regler om integritetsskydd. Däremot kan det finnas anledning att förhandla med facket innan åtgärden genomförs. (Se medbestämmandelagen 10-14 §§.)

Ett sätt att göra användningen av loggning (och spårprogram som resulterar i rapporter) förenligt med personuppgiftslagen är att de personer vars uppgifter ska behandlas lämnar sitt samtycke. Det är då viktigt att den enskilde individen själv lämnar sitt samtycke. Det räcker inte att facket gör det. (Däremot är det lämpligt att en förhandling tas upp med facket innan systemet med loggning införs.) Vidare måste individen som samtycker vara välinformerad. Denne måste veta vad det är för behandling av personuppgifter som hon samtycker till. Den enskilde måste informeras om vad behandlingen består i och vad som är syftet med denna. Se bland annat personuppgiftslagen 3 §. Annars kan det bli så att samtycket saknar verkan.



Även om något samtycke inte har inhämtats kan loggningen mm vara tillåten. Personuppgiftslagen har en allmän regel som tillåter behandling av personuppgifter efter en intresseavvägning (10 § f). De intressen som ska vägas mot varandra är arbetsgivarens intresse av loggningen mm, å ena sidan, och det ingrepp i integriteten som detta för med sig, å andra sidan. Loggningen tillgodoser en rad viktiga behov. Risken för att organisationen blir förknippad med en företeelse såsom fildelning, rasism eller barnporn kan exempelvis minskas. Det torde därför inte råda någon tvekan om att intresseavvägningen utfaller på ett sätt som gör loggning mm tillåten trots att samtycke inte har lämnats. Detta förutsätter att loggningen inte går utöver vad som är nödvändigt med tanke på syftet med loggningen. Av detta skäl (men också på grund av andra regler i PUL) är det viktigt att loggningen exempelvis inte *i onödan* görs på individnivå, att det inte är fler personer än nödvändigt som har tillgång till uppgifterna, och att gallring sker när uppgifterna inte längre behövs. Hur ofta gallringen bör göras hänger samman med hur ofta loggningen genomförs och i vilket eller vilka syften den görs. Ett riktmärke kan vara att uppgifterna sparas i högst tre månader, såvida inte en utredning pågår.

Det är vidare viktigt att ändamålet med loggningen mm anges någorlunda exakt och att personalen informeras. I det sammanhanget bör personalen lämpligen informeras om vilken privat användning av Internet och e-postande som är tillåten. Ribban bör inte sättas för högt "för säkerhets skull". Det är exempelvis fel att förbjuda all privat användning och sedan i praktiken se mellan fingrarna på att bankärenden utförs på lunchtid. Informationen ska med andra ord korrekt återge de regler som verkligen tillämpas.

Personalen behöver för övrigt inte informeras vid varje enstaka tillfälle som en loggning sker. Det är tillräckligt med allmän information om att loggning kan komma att göras, vad som är ändamålet med den och hur den genomförs etcetera. I den information som görs ska konkreta hänvisningar göras till § i PUL. Detta gör det, enligt Datainspektionen, lättare för den enskilde individen att ta tillvara sina rättigheter.

Harry Schüssler, Jur kand och expert på IT-juridik
Mejl: harry@schussler.se, Telefon: 0709-56 99 55

WP – LEG – SE 06/07