Privata spår i jobbmobilen

Risker med utsuddade gränser mellan arbete och privatliv i uppkopplade arbetsredskap

2021

Unionen

Innehåll

Förord

Integritet i arbetslivet är ett område som omfattar en rad komplexa frågor. Gemensamt är att de omfattar vad en arbetsgivare vet och bör veta om sina anställda. Grundprincipen måste alltid vara att arbetsgivaren ska veta så lite som möjligt och bara samla in information om de anställda som är nödvändig för att kunna leda och fördela arbetet.

Samtidigt befinner vi oss i en tid där gränsen mellan vad vi håller privat och vad vi är offentliga med blir allt mer flytande. Tekniska möjligheter att dela med sig av sitt privatliv till omvärlden och i rollen som konsument är drivande faktorer.

Utvecklingen äger rum parallellt med att gränsen mellan arbetsliv och privatliv suddas ut. Den privata sfären äger delvis rum i laptops och smartphones som personer har via jobbet. Vi får en skärningspunkt mellan arbete, integritetsfrågor och digital utveckling. Här finns risker, både uppenbara och mer subtila.

Digital integritet i arbetslivet är förvisso ingen ny fråga. Unionen, andra aktörer och debattörer har återkommande lyft frågan under 2000-talet. Utvecklingen mot ett ökat distansarbete och innovationer i datadrivna arbetsmetoder innebär dock att samtalet om digital integritet i arbetslivet förtjänar än mer genomlysning. För även om debatten inte är ny saknas fortfarande svar.

Unionen vill bland annat se en heltäckande lagstiftning för integritet i arbetslivet, men det finns saker som behöver göras även utöver det. Vi tror och hoppas att samtalet om digital integritet i arbetslivet kommer att bli viktigare för allt fler under de kommande åren. Vi ser fram emot att lyssna uppmärksamt på vad andra har att säga och att själva delta aktivt.

Det här är den första av två rapporter som Unionen publicerar om digital integritet i arbetslivet under 2021. I den här rapporten ligger fokus vid digitala spår i arbetsenheter. Den andra rapporten kommer att gå på djupet i frågan om hantering av data som genereras av arbetstagare.

Katarina Lundahl
Chefsekonom

Inledning

Användning av en uppkopplad digital enhet lämnar spår i form av data. Dessa spår, denna information om vår användning av den digitala enheten, kan samlas in, struktureras och analyseras. Det väcker frågor om bland annat integritet, värdet av data, möjligheter och risker med att vara ständigt uppkopplad, samt om demokrati.

Under de senare åren har vi fått en debatt om de relativt nya, men ändå oerhört stora aktörer som har som affärsidé att hantera våra digitala spår. Aktörernas storlek anses av flera röster hämma konkurrens, bidra till en försämring av det demokratiska samtalet och ha osunt djupa insikter om sina användare. Digitala spår har blivit en samhällsfråga.

Liknande problematik som diskuteras på en samhällsnivå återfinns i arbetslivet. Det är inte ovanligt att bärbara datorer och smartphones som en person har tillgång till genom sitt arbete används för privat bruk. Det kan till och med vara så att privata konton hos leverantörer av e-post, musik- eller filmtjänster och sökmotorer är aktiverade på arbetsenheter. Att ha sin arbetstelefon som sin privata telefon är inte ovanligt.

En risk med digitala spår är att de kan användas för att göra integritetskränkande intrång. Att filtrera delar av sitt privatliv genom enheter som ägs av arbetsgivaren medför därmed vissa problem. Samtidigt har en stor andel av oss ett beteende som inte tar hänsyn till sådana risker. Ibland kan vårt användande av digitala arbetsenheter tvärtom stå i direkt motsats till hur vi borde göra.

I den här rapporten analyseras risker med digitala spår i arbetsenheter utifrån ett fackligt perspektiv och vad som kan göras för att förebygga sådana risker. Med rapporten vill Unionen väcka diskussion om digital integritet i arbetslivet.

Digitala spår

Digitala spår

Varje interaktion en individ har med en digital enhet lämnar någon form av digitalt spår. Dessa spår kan samlas, kategoriseras och analyseras av den eller de som har tillgång till spåren. Genom en sådan analys kan en ”digital version” av individen skapas.

Ju fler spår som finns från en individ, desto större är sannolikheten att denna digitala version av en individ överensstämmer med den verkliga individen, åtminstone i vissa avseenden. En individ som exempelvis lämnar stora mängder spår relaterade till nyfödda barn kan antas vara i färd med att bilda familj eller precis ha blivit föräldrar.

Med en digital version av en individ kan en rad antaganden göras om exempelvis personens beteende och livssituation, som i sin tur kan komma att leda till sannolika förändringar i bland annat individens konsumtionsmönster.

Digitala spår kan därmed sägas ha ett värde, åtminstone för den som kan använda informationen för att till exempel sälja en produkt. Under 2000-talet har en rad framgångsrika affärsmodeller uppkommit, där analys av digitala spår utgör en kärna.

Ett illustrativt exempel är plattformar för sociala medier. Få ägare av sociala medier-plattformar tar ut en avgift av sina användare. Det beror på att den data, som genereras av användaren på olika sätt är mer värdefull för plattformsägaren, än vad samma användare skulle vara villig att betala för möjligheten att närvara på plattformen.

Lockelser att lämna fler digitala spår

Att använda smartphone-applikationer för att navigera (till fots eller i fordon) är smidigt och ger användarvärden i vardagen. Men att användarvärdet skapas genom att de som äger och utvecklar applikationerna samlar data om hur användaren rör sig geografiskt – och kan spåra vilka butiker användaren har besökt – är sällan något användaren tänker på.

Varje steg och hjärtslag kan registreras av hälsoklockor, smartphone-applikationer eller fitness-armband. Det kan uppfattas som positivt, eftersom användaren då kan få information som leder till att hen kanske söker läkarvård och upptäcker hjärtsjukdomar eller inspireras till ökad mängd motion. Men att informationen kan

sammanställas i en databas med andra användares information och analyseras, tycks förbises.

Under 2020 har det uppstått oro kring ökad digital övervakning av tjänstemän som arbetar på distans till följd av covid-19, främst i USA och Storbritannien. Det är en debatt som lär bli mer intensiv under de kommande åren.

Digitala spår i arbetet

Diskussioner om digitala spår sker ofta inom ramen för vilken information vi som samhällsmedborgare och konsumenter delar till privata aktörer. En angelägen aspekt av det är de spår som lämnas till en arbetsgivare, och vad som kan hända med sådan information.

Digitala spår i arbetet är inte en ny fråga

Dåvarande Datainspektionen, numera Integritetsskyddsmyndigheten, undersökte redan 2005 arbetsgivares kontroll av anställdas aktivitet på internet. Myndigheten fann då bland annat att flertalet arbetsgivare hade policys för hur anställda får använda arbetsenheter för internetsurf och att omkring hälften av de undersökta arbetsgivarna utövade någon form av kontroll.

Arbetsmiljöverket har i sin föreskrift om arbete vid bildskärm (AFS 1998:5) följande skrivningar:

”Användningen av bildskärmar och datorer i arbetslivet kan möjliggöra en ökad kvalitativ eller kvantitativ kontroll av arbetstagarna. Detta kan upplevas som integritetskränkande samt öka den psykiska belastningen i arbetet om det sker utan arbetstagarnas vetskap.

Det är inte heller förenligt med kraven på en god arbetsmiljö i psykiskt och socialt avseende att utnyttja datortekniken så att uppgifter om enskild anställd används på ett sätt som medför att den personliga integriteten kränks.”

Arbetsdomstolen fann i ett mål 1999 (AD 1999 nr 49) att en saklig grund för uppsägning (i det enskilda fallet) utgjordes av att en arbetstagare utan medgivande hade ”installerat internet”. Arbetsgivaren i fallet kunde genom att studera en fil på datorn konstatera att av 2700 webbplatsbesök var flertalet av privat karaktär.

Intresseorganisationen American Management Association (AMA) publicerade 2007 en kartläggning av övervakning på arbetsplatsen i USA. Enligt AMA hade fler än var fjärde av de tillfrågade arbetsgivarna någon gång avskedat en anställd på grund av felaktigt användande av en e-post-klient.

I dag ser vi att digitala spår, ofta i form av e-postmeddelanden, används som bevisning i arbetsrättsliga tvister i Sverige. Det är snarare regel än undantag att skriftlig bevisning som härrör från digitala miljöer åberopas i sådana tvister.

Mest förekommande skäl till avsked var överträdelser av företagspolicys, olämpligt språkbruk, överdrivet personligt bruk och överträdelser av sekretessklausuler. Utöver det identifierades att det förekommer att arbetsgivare spårar tangentslag och tid vid tangentbordet, förvaring och påseende av lagrade filer och tid som anställda talar i telefon.

Under 2020 fick frågan ny aktualitet i och med att många tjänstemän över världen flyttade sitt arbete från kontor till hemmet, för att hindra spridning av covid-19.

Privatliv och arbetsliv flätas samman

Gränserna mellan privatliv och arbetsliv har under 2000-talet blivit mindre tydliga för tjänstemän. Det har blivit enklare att ta med sig arbetet hem. Det beror på att bärbara arbetsverktyg (som laptops och smartphones) har fått bättre prestanda, samtidigt som snabba internetuppkopplingar och wifi-nätverk i hemmet har blivit vanligare. Möjligheter att svara på e-post och att arbeta med och dela dokument från hemmet har ökat.

För vissa tjänstemän har det möjliggjort ett mer flexibelt arbetsliv, men det har också medfört att vissa upplever sig som ständigt tillgängliga, vilket påverkar återhämtning och privatliv negativt.

Det ofrivilliga (men av många välkomnade) distansarbetet för tjänstemän till följd av covid-19 har kraftigt ökat antalet personer som i sin vardag har att hantera sådana mer oklara gränser. I en rapport från Post- och telestyrelsen beskrivs hur vissa uppger att de även föredrar att använda privata datorer och andra verktyg i sitt distansarbete, då de av arbetsgivaren tillhandahållna verktygen inte håller måttet.

Det mer gränslösa arbetslivet gör att arbetsenheterna också riskerar att användas på ett mer gränslöst vis. Det finns en stor sannolikhet att de, helt eller delvis, sammanför privatliv och professionellt liv. Arbetsenheter kan användas till exempelvis privata bankärenden, shopping, privat mediekonsumtion eller spel, beroende på vilka inställningar och begränsningar på enheten som har installerats av arbetsgivaren.

Vissa aktiviteter som är möjliga att använda enheten till kan dessutom vara otillåtna enligt gällande policy. Oavsett om det är tillåtet eller inte är det tydligt att vissa privata förehavanden äger rum i professionella enheter. I och med det äger en del av privatlivet rum i en enhet som tillhör en arbetsgivare.

Vissa digitala spår kan läsas av arbetsgivare

En central aspekt av digitala spår och arbetsenheter rör arbetsgivares tillgång till sådana digitala spår. Vilka digitala spår en arbetsgivare kan ha tillgång till är dock en fråga med flera svar. En grundläggande faktor är i vilket syfte de digitala spåren och annan information i en arbetsenhet undersöks.

Om en arbetsgivare vill undersöka vilka webbplatser som har besökts på en arbetsenhet kan det vara motiverat om det handlar om säkerhet. Men om syftet är att kontrollera webbläsaranvändning i realtid är det inte tillåtet (om det inte handlar om att arbetstagarnas säkerhet utsätts för risk).

Att som arbetsgivare läsa arbetstagares e-post kan enligt liknande principer vara tillåtet i vissa sammanhang. Om det finns starka misstankar om illojalitet eller brottslighet får privat e-post sannolikt läsas. Samma sak kan gälla korrespondens om arbetsuppgifter som arbetsgivaren informerat om på förhand att hen kan komma att läsa, under förutsättning att det finns laglig grund. Ytterst måste, i det enskilda fallet, en intresseavvägning göras mellan arbetstagarens integritetsintresse i förhållande till arbetsgivarens kontrollintresse.

Det ska påpekas att en arbetstagare som utgångspunkt inte kan samtycka till vilka personuppgiftsbehandlingar som helst, genom att exempelvis skriva på en policy. Det beror på att arbetstagare befinner sig i ett ojämnt styrkeförhållande gentemot arbetsgivaren, vilket försvårar ett samtycke utifrån jämlika positioner. Brott mot GDPR[1] kan äga rum även om arbetstagaren har samtyckt.

Det är dock svårt, för att inte säga omöjligt, att lista i detalj vad en arbetsgivare får och inte får göra med digitala spår i arbetsenheter. Huruvida en viss hantering av digitala spår (i realtid eller i efterhand) är tillåten eller inte beror på förhållandena i varje enskild situation. Men det är samtidigt tydligt att digitala spår inte automatiskt är hemliga för arbetsgivaren. En bedömning måste alltid göras i det enskilda fallet.

Om arbetsgivare vill studera vissa digitala spår är sådan hantering alltid begränsat till ett tydligt syfte. Det är inte så att digitala spår som samlas in och hanteras för ett syfte sedan kan användas till något annat. Oavsett krävs att arbetsgivaren i förväg informerar om

[1] Dataskyddsförordningen är en lag som gäller i hela EU, vars engelska namn General Data Protection Regulation, förkortat GDPR, oftast används.

att läsning av e-post kommer att äga rum eller att ett datorsystem ska användas för att mäta och/eller utvärdera prestationer. I annat fall kan det röra sig om en överträdelse av GDPR.

Till sist ska det påpekas att om en otillåten hantering av digitala spår äger rum är skadan (åtminstone delvis) redan skedd. Även om hanteringen i efterhand bedöms som otillåten. Risker finns även att digitala spår tillgängliggörs genom läckor eller hackerattacker. Det är skäl nog att som arbetstagare vara ytterst restriktiv i sin användning av uppkopplade arbetsenheter.

Alldeles oavsett om data som arbetsgivaren har tillgång till har genererats på ett tillåtet eller otillåtet sätt, kan arbetsgivaren använda den om det uppstår en tvist.

Risker med arbetsgivarens hantering av digitala spår

I undersökningen som har gjorts till den här rapporten (och som presenteras längre fram i rapporten) svarade omkring 25 procent att de har god kännedom om hur arbetsgivaren hanterar digitala spår som lämnas i arbetsenheter.[2] Med andra ord har en stor grupp inte tillräckligt god kännedom om hur digitala spår hanteras, trots att de regelbundet lämnar sagda spår. Det medför en rad problem, som beskrivs mer ingående i det här kapitlet.

Risker relaterade till privat användning av arbetsenheter

Att använda sin jobbmobil och jobbdator till privata ändamål, i någon utsträckning, tycks vara relativt vanligt. Framför allt gäller det jobbmobiler, där undersökningen som har gjorts till den här rapporten visar att en hög andel av de digitala spår som lämnas i jobbmobiler är av privat karaktär.

Det ska inte tolkas som att personer inte arbetar utan i stället sitter och tittar på privata appar i sin telefon. Snarare visar det att jobbmobilen används relativt lite i arbetet och desto mer efter arbetsdagens slut. Det i sin tur ger en fingervisning om att många har sin jobbmobil även som sin privata mobil.

Att skilja på arbetsliv och arbetstid å ena sida, och privatliv och fritid å andra sidan, blir svårare om båda äger rum i samma enheter. Inte minst i en tid när allt mer av arbetet och privatlivet innefattar användning av enheter på ett sätt som lämnar digitala spår.

Genom att lämna en digital representation av sig själv i en arbetsenhet ökar risken för att ens integritet kommer att utsättas för en kränkning. Det är en risk som kan tyckas liten för den som ”inte har något att dölja”.

Men personlig integritet och digitala spår är inte en fråga om att dölja hemligheter. Snarare rör det sig om en värderingsförskjutning, där vi inte tycker att de är konstigt att anställda i praktiken

[2] De respondenter som har svarat 4 eller 5 på en femgradig skala, där 5 motsvarar hög kännedom, på frågan "Din användning av jobbdator och jobbmobil lämnar spår, i form av exempelvis surfhistorik, geografisk information, kakor/cookies och dylikt. Känner du till hur din arbetsgivare hanterar sådana spår?"

registrerar vilka tv-program de tittar på, eller vart de har befunnit sig på fritiden, genom att använda program och appar i arbetsgivarens enheter.

I förlängningen handlar det om förflyttningar av gränserna mellan privatliv och arbetsliv som sannolikt inte ligger i arbetstagarens intresse. Även om det stora flertalet arbetsgivare inte studerar informationen.

Otillåten hantering av digitala spår

Riskerna med att använda arbetsenheter till privat bruk är i viss mån möjligen abstrakta. Det gör dem inte mindre viktiga. Men det finns även mer konkreta risker, rörande hur arbetsgivaren hanterar de digitala spåren, oavsett om de är privata eller lämnas som en del i användningen av enheterna i arbetet.

En stor risk är att om kunskapen om hantering av digitala spår är begränsad, kan en arbetsgivare hantera digitala spår på ett sätt som inte är tillåtet, utan att en misstanke om att så sker uppstår. Det gäller både medveten hantering som kan sägas stå i rak motsats till arbetstagarens intressen, men även omedveten eller oreflekterad hantering.

Digitala spår om privatlivet kan i värsta fall bli ett maktmedel i en konflikt mellan arbetsgivare och arbetstagare. Även om det hör till ovanligheterna är blotta risken för den sortens integritetskränkning något som kräver ett gediget förebyggande arbete.

Vissa datorsystem har funktioner som registrerar data på olika sätt utan att anställda informeras. En analys av sådan data kan framstå som potentiellt produktivitetshöjande för den som läser den. Samtidigt finns risk att läsaren av informationen saknar kunskap om exempelvis GDPR, eller förutsätter att allt är i sin ordning. Även i det här fallet finns behov av ett arbete för att förebygga att digitala spår används på fel sätt, oavsett syfte.

Unionen avser att i en rapport under 2021 återkomma mer i detalj gällande hur arbetsgivare hanterar data som genereras av arbetstagare.

Säkerhetsrisker med digitala spår i arbetsenheter

Under det senaste decenniet har vi kunnat bevittna en rad incidenter där hemliga data på ett eller annat sätt läcker ut. Inte sällan har det handlat om känsliga personuppgifter. Frågan är inte längre *om* det kommer att hända igen utan *när* det kommer att hända.

Datorsystem utsätts regelbundet för angrepp, samtidigt som det finns en rad system i bruk som inte lever upp till ett adekvat skydd.

Här finns ytterligare argument för att avhålla sig från att använda arbetsenheter till privat bruk. De spår som lämnas kan helt enkelt hamna i fel händer. Det går att föreställa sig dels att hackare får del av enskilda personers digitala spår som de inte vill att arbetsgivaren ska ta del av. Dels att hackare tar sig in i datorsystem genom säkerhetsluckor, med hot om att stjäla företagshemligheter.

Det är inte ovanligt att individer har vad som kan anses vara en undermålig säkerhetsnivå i användningen av digitala enheter. Det kan till och med sägas att för en stor andel av oss verkar det närmast omöjligt att uppnå en tillräckligt hög säkerhetsnivå.

Om det beror på bristande insikter, att en hög säkerhetsnivå är för tekniskt komplicerat utan hjälpmedel som lösenordshanterare, eller något annat kan diskuteras. Oavsett blir effekterna att risknivån ökar. Därmed utsätts även arbetsenheter för ytterligare risk, när de även används i privata syften.

I samtal om digital säkerhet omtalas ofta vikten av svårknäckta och unika lösenord. Vi uppmanas att inte öppna filer i e-post från osäkra källor, med mera. Det är förvisso goda råd. Men samtidigt kan säkerhetsansvaret i användningen av arbetsenheter inte enbart vila på den enskilde. Ambitionen att alla ska hålla ett högt och konsekvent säkerhetsläge kommer sannolikt inte att vara nåbar fullt ut, i nästan någon organisation.

Bättre är att rekommendationer om medvetet säkerhetsbeteende kommer tillsammans med robusta säkerhetssystem. Ett viktigt förhållningssätt är att den enskilde användaren inte ska ha möjlighet att genom användning av en arbetsenhet kunna äventyra säkerheten i systemet. Ansvaret för säkerheten måste alltid vara arbetsgivarens.

Integritetsparadoxen

Den här rapporten har hittills diskuterat hur privat användning av arbetsenheter medför risker. I det här kapitlet diskuteras hur det kan komma sig att sådan användning ofta äger rum mot bättre vetande. Det visar sig nämligen att människor tycks ha hyfsat starka tankar kring integritetskränkningar relaterade till digitala spår. Samtidigt leder sådana åsikter inte till ett beteendemönster i linje med sådana åsikter.

I den här rapporten kategoriseras detta som ”integritetsparadoxen”. En paradox uppstår när något i en teori eller förklaringsmodell inte fullt ut kan förklara det som sker i det mänskliga beteendet. Det kan exempelvis handla om mänskliga beteenden som äger rum trots att all förståelse av beteendet borde leda till att det inte äger rum. I det här fallet då ett beteende som ökar risken för integritetskränkningar genom användning av arbetsenheter, trots en generell hög känsla för integritet.

Integritetsparadoxen är centrerad kring följande: Trots att flertalet uppger att de är oroliga för hur deras integritet kan överträdas i samband med att de använder digitala arbetsenheter, gör de mycket lite (eller ingenting alls) för att skydda eller förhindra att personuppgifter och data om beteenden samlas in, när de använder digitala arbetsenheter.

I botten för den här teorin ligger kunskap om människors allmänna inställning till integritet och digitala enheter. Kunskapen vittnar om en dikotomi mellan integritetsattityder och faktiskt beteende. Det är till och med så att många frivilligt delar information om sig själva i utbyte mot en ökad grad av skräddarsydda erbjudanden, baserade på den digitala representationen av ens person.

Inom sociala medier finns samma mönster. Även om det går att begränsa hur ens kommunikation tillgängliggörs för andra, tycks oro för att tredje part kan ligga i bakgrunden och samla data ofta inte i praktiken leda till att sådan begränsning görs. Privat information läggs upp relativt öppet, ibland även med ett aktivt tidsangivande och vid vilken fysisk plats inlägget görs. Det ligger nära att anta att många hanterar arbetsenheter på ett liknande sätt.

Undersökning av integritetsparadoxen

För att utforska frågan om digital integritet i arbetslivet använder den här rapporten en metodik som bygger på observationer av en grupp respondenters digitala beteenden, i en undersökning som Unionen har låtit genomföra.

Respondenternas digitala beteenden har undersökts via en applikation som med individens samtycke har installerats på en digital enhet. Observationerna har kombinerats med en enkätundersökning om respondenternas syn på digital integritet och relaterade frågor.

Här beskrivs metoden mer i detalj, innan själva undersökningen presenteras.

Metod

Under en period om fyra veckor registrerades respondenternas surfhistorik och söktermer, applikationsanvändning samt tillbringad tid på enheten, varefter den analyserades. Respondenterna fick även svara på en enkätundersökning med frågor relaterat till digitalt beteende. Kombinationen möjliggör ett utforskande av respondenternas attityder och åsikter och hur det står i relation till deras faktiska digitala beteende.

Respondenterna rekryterades i en webpanel, representativ för Sveriges befolkning 25–79 år. De fyllde i ett rekryterings- och profileringsformulär som samlade in demografisk, sociodemografisk och attitydmässig (framförallt i relation till teknik och syn på integritet) information. De fick även frågan om de kan tänka sig att installera en applikation som samlar in data kring det digitala beteendet på en valfri enhet (smartphone, dator eller tablet).

Omkring 10 procent av respondenterna som fyllde i profileringsformuläret godkände användandet av applikationen. Det ska noteras att undersökningen genomfördes innan covid-19-pandemin. Insamlingen pågick under perioden juni-september 2019. För att säkerställa representativiteten i denna grupp har insamlad data viktats på kön, ålder och region samt utifrån deras förhållningssätt och inställning till teknik och integritet. Efter avslutad registrering av det digitala beteendet fick respondenterna en uppföljande enkät med mer ingående frågor kring digital integritet och digitalt arbetsliv.

Att analysera den omfattande mängden insamlade data som den här typen av metodik genererar innebär att man behöver ha ett datadrivet angreppssätt. Vidare får man låta data informera analytikern om vad som är viktigt att fokusera på, snarare än att validera på förhand satta teser eller frågeställningar. I vissa fall vilar insikter på många individers beteenden eller svar, och i andra fall är det en enskild persons beteende som ligger till grund för vilka slutsatser som dras. Analysen i rapporten vilar därmed både på kvantitativa och kvalitativa angreppssätt.

Det totala antalet respondenter som rapportens insikter vilar på är 190 personer som antingen förvärvsarbetar eller är egenföretagare. Alla 190 personerna har haft en applikation installerad på en digital enhet och har svarat på den uppföljande enkäten. Bland dessa finns 17 respondenter som har installerat applikationen på vad de anger är en smartphone tillhandahållen av sin arbetsgivare. I snitt registrerades cirka 5 000 spårbara aktiviteter hos respondenter med en laptop under en 30-dagarsperiod. Samma siffra för smartphones var cirka 3 700. Respondenter som registrerades på en smartphone de hade via arbetet registrerade cirka 6 100 spårbara aktiviteter.

Observation av en dag i en respondents liv

För att demonstrera nivån av information som tillgängliggörs av digitala spår återges här ett utdrag ur en respondents faktiska beteende, ur Unionens undersökning. Det går att följa varje digitalt steg respondenten tar, vilken tid som ägnas åt olika saker och vad hen tar del av. Informationen återgiven här är blott en bråkdel av totalen av respondentens data och en oerhört liten del av den totala informationsmängden som genererats i undersökningen.

07.07 startar hen sin dator. Loggar in på Facebook. Därefter Google och Microsoft Outlook. Timmen mellan 07–08 ägnas åt Microsoft Word, en PDF-läsare och att besöka etsy.com i en webbläsare.

08–09 verkar hen vara mer fokuserad på sitt arbete. Alternerar mellan Microsoft Outlook och Edge.

09–10 Fortsätter arbetet och går över till VISMA administration. Även sociala medier bryter av arbetsdagen med jämna mellanrum, främst i form av Facebook.

10–11 arbetar hen koncentrerat i VISMA administration.

11–12 blir aktiviteten mer disparat. Hen besöker loppi.se, besöker familjeliv.se och läser en del trådar kring olika familjerelaterade problem och utmaningar.

Genom att i detalj (ovan redovisade timmar i respondentens digitala liv är en översikt) studera digitala spår tecknas en bild av en person. Det är inte en särskilt grannlaga uppgift att lägga ihop det pussel som utgörs av en användares samlade digitala spår, för att skapa sig en uppfattning om vem personen är, vad hen gillar, vad hen oroar sig över, hur hen rör sig, hur hen interagerar med sin omvärld och så vidare. Sannolikheten att framgångsrikt identifiera vem personen är ökar med tillgänglighet till fler digitala spår.

Intentioner, digitala spår och paradoxer hos respondenterna

Respondenterna i undersökningen fick vid sidan av registreringen av digitala spår svara på en enkät. Svaren har sedan analyserats utifrån hur de använder sina enheter, för att ge en bild av när paradoxer uppstår och hur det ser ut.

Vi börjar med att titta på hur stor del av användningen av arbetsenheter som var arbete och hur stor del som var annat.

Tabell 1: Genomsnittlig fördelning av användning av jobbmobil/ jobbdator

Enhet	Ej jobbrelaterad användning	Jobbrelaterad användning	(summa)
Jobbmobil	89%	11%	100%
Jobbdator	58%	42%	100%
N=190			

Det visar sig att på respondenternas jobbdatorer är nästan 60 procent av aktiviteten inte jobbrelaterad. På jobbmobilerna är det bara strax över 10 procent som används till jobbrelaterad aktivitet. Med andra ord så används både datorer och mobiler till en hel del som inte har med jobbet att göra.

Här ska det påpekas att tabellen inte ska tolkas som att den som har en jobbdator bara jobbar 43 procent av en arbetsdag och gör annat resten av tiden. All aktivitet, även den utanför normalarbetstid, finns redovisad ovan.

Poängen är att illustrera vad vi gör med enheterna utöver arbete. När det gäller mobiltelefonerna blir det särskilt tydligt. En möjlig tolkning är att den som får en mobiltelefon i arbetet inte känner att det är lönt att ha en privat telefon utöver det. Dessutom kan siffrorna läsas som att den moderna mobiltelefonen, trots sina stora möjligheter, är underutnyttjad som arbetsredskap, varför en så stor andel av användningen inte är jobbrelaterad.

Siffrorna är intressanta utifrån att det är relativt få som uppger att de har en mycket god kännedom om hur arbetsgivaren, som äger enheterna, hanterar de digitala spår som registreras på dem.

Tabell 2: Din användning av jobbdator och jobbmobil lämnar spår, i form av exempelvis surfhistorik, geografisk information, kakor/cookies och dylikt. Känner du till hur din arbetsgivare hanterar sådana spår?

1. Jag har ingen kännedom om hur min arbetsgivare hanterar sådana spår	38%
2.	12%
3.	25%
4.	12%
5. Jag har mycket god kännedom om hur min arbetsgivare hanterar sådana spår	13%
(summa)	100%
N=190	

Noterbart är att hälften av respondenterna har svarat 1 eller 2 på den femgradiga skalan. Samtidigt uppger en övervägande majoritet att de har hög medvetenhet om arbetsgivarens policy gällande icke-arbetsrelaterad användning av jobbenheter.

Tabell 3: Är du medveten om policyns innehåll gällande icke-arbetsrelaterad användning av din jobbmobil/jobbdator?

	Jobbmobil	Jobbdator
1. Jag har ingen aning om vad som står i policyn	1%	1%
2.	0%	1%
3.	6%	6%
4.	38%	38%
5. Jag är fullt medveten om policyns innehåll	55%	54%
(summa)	100%	100%
N = 65/62		

En tolkning är att det finns förståelse för vad enheterna får användas till, men mindre insikt kring hur digitala spår hanteras. Det kan då tyckas paradoxalt att en så stor andel av användningen av enheterna inte är jobbrelaterad, när de som använder enheterna samtidigt inte vet hur deras spår hanteras.

Ett sätt att förklara det är att värdet i att kunna använda enheten till annat än arbete är större än eventuella risker, alternativt att man inte anser att det föreligger några risker.

Hög kännedom om digitala spår och hantering av dessa tycks inte nämnvärt påverka privat användning av arbetsredskap.

Tabell 4: Andel som uppger att de använder sin jobbmobil/jobbdator även för privata ändamål

	Jobbmobil	Jobbdator
Har jobbenhet (N = 105)	76%	82%
Har policy för jobbenhet (N = 62)	81%	76%
Fullt medveten om innehållet i policy (N = 57)	80%	74%
Fullt medveten om digitala spår OCH hanteringen av dessa (N = 43)	78%	71%
N = 190		

Ytterligare en förklaring är att respondenterna litar på att deras spår inte hanteras på ett klandervärt sätt.

När respondenterna ställs inför en rad situationer kring digitala spår och får kategorisera dem utifrån om de utgör en kränkning syns en del intressanta svar.

Tabell 5: I vilken utsträckning utgör dessa situationer enligt dig en kränkning?

	4. 5. Kränkande/i hög grad kränkande	3.	1.2. Inte/inte alls kränkande
Din arbetsgivare säljer delar av dina digitala spår, exempelvis platstjänster, till ett annat företag	85%	8%	7%
Din arbetsgivare har genom att titta på dina digitala spår fått kännedom om en händelse i ditt privatliv och ställer frågor om det	78%	16%	6%
En blivande arbetsgivare begär att få tillgång till dina sociala-medier konton innan ni skriver anställningsavtal	73%	14%	13%
Din arbetsgivare använder de digitala spår du lämnat efter dig som en faktor för din lönesättning och/eller dina karriärmöjligheter	70%	23%	7%
Ett sociala medier-företag använder spår från dina aktiviteter på internet och i appar för ekonomisk vinning	68%	21%	11%
Din arbetsgivare begär att få gå igenom all din epost-, chatt- och surfhistorik på din jobbdator	54%	20%	26%
Din arbetsgivare har genom att titta på dina digitala spår fått kännedom om att du har besökt en hemsida med känsligt material och tar upp det för diskussion	46%	30%	24%
Din arbetsgivare begär att få gå igenom all din användning av din jobbmobil	40%	25%	35%
N = 190			

Vissa av de hypotetiska situationer som respondenterna har fått ta ställning till upplevs av en tydlig majoritet som kränkande. Samtidigt är det inte en oro som leder till ett riskminimerande beteende. Av svaren går det inte att utläsa om det beror på exempelvis en hög tillit till att digitala spår hanteras korrekt av arbetsgivaren.

Det är dock att betrakta som paradoxalt att många tycks känna stor oro, samtidigt som det privata användandet av enheter är högt och det saknas djupare insikter hos flertalet gällande hur digitala spår hanteras.

Unionens förslag för en förbättrad digital integritet i arbetslivet

1. Heltäckande lagstiftning gällande integritet i arbetslivet

Lagstiftning kring integritetsfrågor i arbetslivet finns i dag bland annat i grundlagarna, i brottsbalken, i arbetsrättslig lagstiftning inbegripen arbetsmiljölagstiftning, i straffrättslig lagstiftning och i dataskyddsförordningen. Med andra ord är lagstiftningen inte sammanhållen, vilket öppnar för kontextberoende subjektivitet och inkonsekvens i bedömningar. Det är ett problem då relationen mellan arbetsgivare och arbetstagare inte är att betrakta som ett jämlikt styrkeförhållande.

Unionen vill se en heltäckande lagstiftning gällande integritet i arbetslivet. Sådan lagstiftning ska inte bara omfatta digital integritet, utan även exempelvis frågor om utdrag ur belastningsregister, kameraövervakning och drogtester.

Frågan om förbättrad lagstiftning gällande integritet i arbetslivet har debatterats och utretts under hela 2000-talet. Inget förslag om samlad lagstiftning har dock lagts fram, trots ett konstaterat behov. Utmaningarna och riskerna med digital integritet som har diskuterats i den här rapporten ökar ytterligare angelägenheten i att få sådan lagstiftning till stånd.

2. Partsgemensamt arbete kring digital integritet

Unionen ser stora fördelar med att parterna tillsammans tar sig an utmaningar som en högre andel uppkopplade arbetsenheter innebär för arbetsmarknadens utveckling. Det finns skäl till att gemensamt arbeta kring frågan om hur digital integritet ska hanteras, vid sidan av den lagstiftning som Unionen vill se.

Unionen uppmuntrar till en bredare partsgemensam dialog kring frågan om digitala spår i arbetslivet. Precis som med många andra frågor finns det stora variationer gällande vilka utmaningar och möjligheter som finns med digital integritet, beroende på sektor på arbetsmarknaden. Den svenska partsmodellen utgör ett väletablerat ramverk för sådan dialog. Att lyfta digital integritet partsgemensamt har dessutom potential att utveckla partsmodellen vidare.

Unionen rekommenderar att lokala parter tillsammans fastställer exempelvis policy för användning av arbetsenheter. Sådan policy kommer att behöva existera i samklang med robusta säkerhetssystem. Det är i sammanhangen viktigt att säkerställa att sådan

policy förankras hos alla medarbetare i företaget, samt att policy eller säkerhetssystem inte innebär brott mot exempelvis GDPR.

3. Rekommendation till Unionens medlemmar

I den här rapporten illustreras problem och risker med privat användning av digitala arbetsenheter, vanligtvis laptops och smartphones som tillhandahålls av arbetsgivaren. Unionen rekommenderar sina medlemmar att generellt undvika att använda arbetsenheter i privat syfte, om möjligt.

Privat användning av arbetsenheter kan framstå som harmlöst. Ett sociala medier-konto i telefonen, ett roligt filmklipp på datorn under lunchen, och så vidare. Förvisso är varje enskild privat användning av digitala arbetsenheter inte en stor sak. Men en blir ofta fler. Långsamt sker en förskjutning av gränser som inte är sund och som utsätter både den enskilde såväl som arbetsgivaren för risker.

Det finns inte mycket att förlora på att undvika privat användning av arbetsenheter, utom möjligen ett gott skratt. Men den effekten borde gå att uppnå under en paus med den egna mobilen.

Källor

AD 1999 nr 49

AMA & ePolicy Institute Research (2007): 2007 Electronic Monitoring & Surveillance Survey

Post- och telestyrelsen (2021): “Digital omställning till följd av covid-19”.

Vi befinner oss i en tid där gränser mellan vad vi håller privat och vad vi är offentliga med blir mer otydliga. Utvecklingen äger rum parallellt med att gränser mellan arbetsliv och privatliv suddas ut. Det leder bland annat till att den privata sfären delvis äger rum i laptops och smartphones personer har via jobbet. Vi får ett möte mellan arbete, integritetsfrågor och digital utveckling. Här finns risker, både uppenbara och mer subtila.

I den här rapporten diskuteras riskerna med privata spår i uppkopplade arbetsenheter ur ett fackligt perspektiv. Rapporten är den första av två om digital integritet i arbetslivet som Unionen ger ut 2021.

UNIONEN

SVERIGES STÖRSTA FACKFÖRBUND
Hos oss är alla tjänstemän i det privata arbetslivet
välkomna, oavsett utbildning och befattning.
Bland våra medlemmar hittar du många chefer
och dessutom både egenföretagare och studenter.
Vår vision är att tillsammans skapa framgång,
trygghet och glädje i arbetslivet.

Tnr 3174-1 Produktion: Unionen