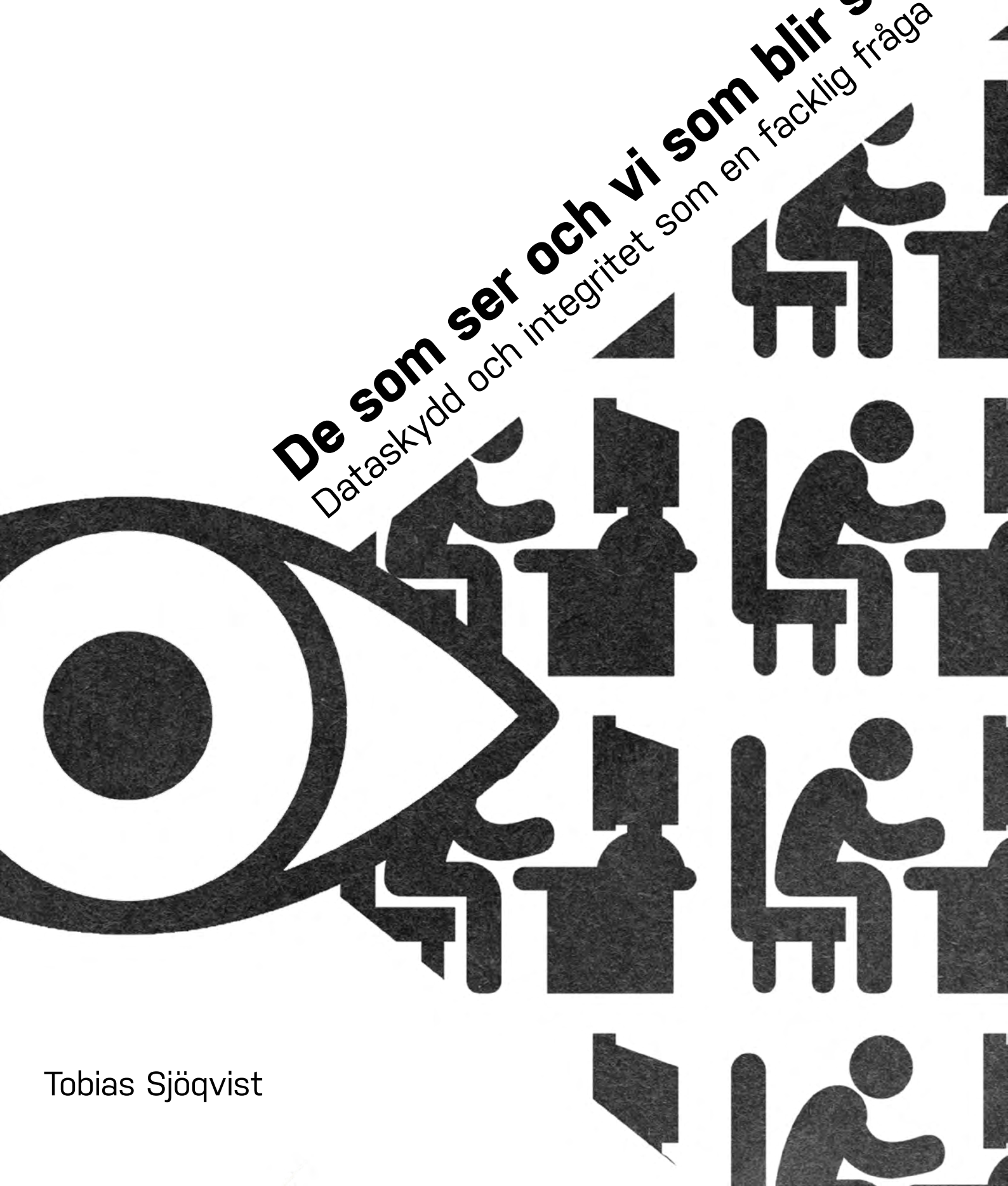
arena idé
December 2023

De som ser och vi som blir sedda

Dataskydd och integritet som en facklig fråga



Tobias Sjöqvist

arena idé | December 2023 | ISBN: 978-91-985543-5-9

Rapporten i korthet

De som ser och vi som blir sedda

– Dataskydd och integritet som en facklig fråga

Tobias Sjöqvist, författare

Jurist på LO.

German Bender, redaktör

Utredningschef på Arena Idé och doktorand i företagsekonomi vid Handelshögskolan.

Rapporten i en mening:
Genom konkreta exempel och övergripande resonemang redogör denna rapport för hur arbetstagare och fackföreningar kan skydda den personliga integriteten i arbetslivet.

Rapporten tar sin utgångspunkt i den svenska arbetsrättsliga modellen och analyserar hur dataskyddsförordningens bestämmelser fungerar på den svenska arbetsmarknaden. Vilka rättigheter har arbetstagare vad gäller de personuppgifter som de alstrar under sin arbetstid? Hur ska fenomenet data och personuppgifter förstås i ett arbetsliv som digitaliseras i rasande takt? Och hur tar arbetstagare och fackföreningar bäst tillvara på de rättigheter som trots allt finns?

Rapportens övergripande slutsats är att dataskyddet i arbetslivet fungerar dåligt idag. Reglerna är dåligt anpassade till arbetslivet och efterföljs dessutom dåligt. Trots att fackföreningsrörelsen, regeringen och riksdagen efterfrågat en mer ändamålsenlig anpassning av reglerna till arbetsmarknaden har inget hänt. De verktyg som fackföreningsrörelsen har till sitt förfogande skulle kunna användas för att reglera dataskydd i mycket större utsträckning än vad som sker idag. I rapporten blandas konkreta exempel med övergripande resonemang om hur det skulle kunna bli verklighet.

Rapporten är riktad mot de som på olika sätt kommer i kontakt med frågor som rör integritet och personuppgiftsbehandling i arbetslivet. En förhoppning är att den som har låga förkunskaper på ämnet med hjälp av rapporten ska kunna förstå vilka typer av problem som personuppgiftsbehandling i arbetslivet för med sig. För den som aktivt arbetar med frågorna så är tanken att rapporten ska kunna fungera som ett underlag i olika behandlings- och förhandlingssituationer.

I rapporten presenteras tre olika fall, som sedan följer läsaren i genomgången av dataskyddsdirektivet. De består av typsituationer där olika rättigheter och skydd i dataskyddsförordningen skulle kunna användas; vid algoritmisk arbetsledning på ett lager, vid gps-spårning inom hemtjänsten och vid distansarbete i hemmet.

Innehåll

Inledning 4

Kort om arbetsrätt 7

Lag om medbestämmande i arbetslivet (MBL) 7

Tolkningsföreträde 8

Arbetsmiljölagen (AML) 9

Utvecklingsavtalet (UVA) 9

Fallen ABC: Digitala rättigheter i tre verksamheter 11

Fall A – Algoritmisk styrning på lager 11

Fall B – GPS-data i hemtjänsten 12

Fall C – Övervakning av kontorsarbete 12

Rättsligt ramverk för anställdas digitala rättigheter 14

Integritet – en blind fläck för den svenska modellen? 14

Integritetskänsliga åtgärder som arbetstvister 16

Europakonventionen 18

GDPR 20

Definitioner 20

Grundläggande principer för behandling av personuppgifter 21

Rättslig grund 22

Myndigheters behandling av anställdas personuppgifter 27

Proportionalitetsbedömning 28

Om ändamålet med behandlingen 39

Ändamålsglidning och ändamålsbegränsning 40

Sanktioner 42

Nationell lagstifting och kollektivavtal 43

Digitala rättigheter och övervakningskapitalism 46

Övervakningskapitalism eller nyfeodalism – olika perspektiv på det digitala livet 46

Algoritmisk arbetsledning 49

Sammanfattning integritet, data och algoritmisk arbetsledning 53

Bilaga I 54

Inledning

Arbetsgivares möjlighet att leda och fördela arbetet har ökat i takt med att teknologiska framsteg har gjorts. Genom att hacka upp arbetet i mindre och mindre delmoment, och samtidigt hålla ordning på att rätt person gör rätt sak och att tillräckligt mycket personal finns tillgänglig, kan sofistikerade algoritmer ta över hela eller delar av arbetsledningen. En förutsättning för sådan algoritmisk arbetsledning är skapandet och behandlingen av data och personuppgifter vilka matas in som bränsle i algoritmerna.

Skaparna av teknologin befinner sig ibland långt borta, och utom räckhåll för den svenska arbetsmarknaden och dess aktörer. Detta innebär att de verktyg som aktörerna på arbetsmarknaden tidigare har använt sig av måste granskas igen i ljuset av arbetsmarknadens utveckling. EU har i viss mån tagit på sig rollen som motvikt till ”big tech” och påbörjat arbetet med att skapa gemensamma regler för AI, plattformar, datahantering och arbetsvillkor. Detta arbete leder samtidigt till en standardisering av de respektive ländernas lagstiftning, vilket också underlättar för företag att bedriva gränsöverskridande verksamhet inom unionen. Sedan 2009 års Lissabonfördrag beskriver EU sig själv som en social marknadsekonomi, och har sedan dess gjort stora åtaganden inom socialpolitiken. Att EU har gått från att vara en liberal-konservativ institution till att ta steg mot att allt mer lägga fram förslag som ligger i linje med klassisk socialdemokratisk politik är både en nödvändig och en efterlängtad utveckling. Unionen har samtidigt utvidgat sin kompetens på dessa områden, vilket har resulterat i att det på sistone har kommit ett stort antal direktiv som utmanar den svenska social- och arbetsrätten.

Inom arbetsrätten finns en större diskussion om dess bakomliggande idé.[1] Lite förenklat går det att säga att det finns flera olika tankar om och anspråk på vad arbetsrätten är, och därmed vilket problem som aktörerna inom det arbetsrättsliga systemet har att lösa med stöd av regelverket. Vilken idé som framhärdar i debatten styr också vilka alternativ som uppfattas som ändamålsenliga då systemet reformeras eller utvecklas. Historiskt har det funnits en spridd uppfattning om att arbetsrätten är ett intervenerande rättsområde som ska kompensera arbetstagare på grund av den maktobalans som råder mellan arbetsgivare och arbetstagare. Denna uppfattning går stick i stäv med den bild av arbetsrätten som företrädare från

1 Se t.ex. J Malmberg: "Vad handlar arbetsrättslig reglering om" 2010 och A. Hyde: *The Idea of the Idea of Labour Law: A Parable i The Idea of Labour Law*, Langille & Davidov (red.), 2011.

tech-branschen vill förmedla, där rättsområdet beskrivs som en stelbent marknadsrestriktion vars tillämpning stävjar innovation och begränsar människors frihet.

När fenomenet AI fortfarande befann sig i sin linda gjordes studier som pekade på att AI skulle medföra en stor så kallad teknologisk arbetslöshet.[2] Teknologin har än så länge inte resulterat i arbetslöshet för stora segment på arbetsmarknaden, däremot har många chefsuppgifter gått från att utföras av människor till att utföras av maskiner.[3] Algoritmisk mjukvara får i allt högre grad utföra uppgifter som att allokera, optimera och utvärdera arbete som utförs av en mycket varierande del av arbetsstyrkan. Detta kallas för algoritmisk arbetsledning. AI är än så länge relativt nytt men allt pekar på att *datafieringen* i arbetslivet och den algoritmiska arbetsledningen kommer att öka.[4]

Med **datafiering** menas processen att förvandla ett fysiskt fenomen till mätbara data.

I Sverige finns en långtgående tradition att från statens sida överlämna stora delar av arbetsrättens utformning till arbetsmarknadens parter, vilket i viss mån kan förklara att det i nuläget inte finns någon nationell särreglering av användandet av AI och data på arbetsplatser. I avsaknaden av lagar och kollektivavtal är det en stor distans till de instrument som kommer från överstatliga och internationella organisationer, som främst är riktade mot stater, och den svenska arbetsrätten, vars bestämmelser om god sed på arbetsmarknaden i många fall utgör enda riktmärket för vad som är lagligt.

Förflyttandet av chefsuppgifter, från arbetsledande chefer till mer eller mindre sofistikerade algoritmer, ger upphov till en rad olika konflikter. Arbetsgivares anspråk på att samla information om sin verksamhet och förbättra beslutsprocesser står i vissa aspekter i motsättning till arbetstagares behov av skydd av sitt privatliv och inflytande över sitt eget arbete och arbetsledningen. I takt med att arbetsgivare har fått mer sofistikerade verktyg som allt effektivare kan leda och fördela arbetet och övervaka de som utför detta har de strategier och verktyg som arbetstagare tidigare har kunnat använda sig av för att skydda sina intressen mot arbetsgivaren fått minskad effekt. Samtidigt har nya verktyg tillkommit som ännu inte nått sin fulla potential. Ett sådant verktyg är dataskyddsförordningen, General

2 Se C. Benedikt Frey & M. A. Osborne: The Future of Employment: *How Susceptible are Jobs to Computerisation?* 2013. https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

3 Se VD. Stefano & A. Aloisi: *Your boss is an algorithm, Artificial Intelligence, Platform Work and Labour*, 2022.

4 VD. Stefano & M. Wouters: *AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework*, Osgoode Legal Studies Research Paper, 2022.

Data Protection Regulation eller kort: GDPR.

Syftet med denna rapport är att visa på värdet av privatliv och integritet i arbetslivet och hur det i allra högsta grad är en facklig fråga som fackföreningsrörelsen, arbetsgivare och myndigheter måste ta på allvar. Rapporten är också ett praktiskt hjälpmedel för arbetstagare och fackföreningar som vill använda dataskyddsförordningen för att få inflytande över frågorna på arbetsplatsen. Det finns också en analys om vilket utrymme som finns att stifta en lag om integritet i arbetslivet och/eller träffa kollektivavtal för att reglera frågorna. Rapporten innehåller dessutom tre typfall som är tänkta att illustrera hur reglerna kan användas i praktiken.

Kort om arbetsrätt

Arbetsrätten kan beskrivas som den juridiska metoden för att bestämma vad som finns i ett anställningsavtal. Det finns såklart många olika sätt att beskriva vad en anställning innebär; en ekonom skulle kanske räkna på hur mycket pengar en arbetstagare får, en sociolog skulle kanske beskriva hur en viss anställning påverkar vilken position i samhället den anställde får. Arbetsrätten är metoden för att avgöra om det överhuvudtaget finns ett anställningsavtal, eller ett kollektivavtal, hur förhållandet ser ut dem emellan, och vilka rättigheter och skyldigheter de båda parterna har enligt lag och avtal. En utgångspunkt inom arbetsrätten är att maktförhållandet mellan arbetsgivaren och den enskilde arbetstagaren är i grunden ojämlikt till arbetsgivarens fördel. Det är arbetsrättens uppgift att på olika sätt kompensera för den ojämlikheten genom att stärka arbetstagarens möjligheter att utmana arbetsgivarens beslut.

Lag om medbestämmande i arbetslivet (MBL)

I medbestämmandelagen finns regler om bland annat hur förhandlingar mellan arbetsmarknadens parter ska gå till. MBL är en så kallad lex generalis, vilket betyder att om den krockar med bestämmelser i andra lagar så har dessa företräde. Detta kan också kallas för att MBL är subsidiär i förhållande till andra lagar. I vissa fall kan den också gälla parallellt med andra lagar; detta är vanligtvis fallet i förhållandet till arbetsmiljölagen.

Inom arbetsrätten finns det tre olika typer av förhandlingar: avtalsförhandlingar (eller intresseförhandlingar), tvisteförhandlingar och samverkansförhandlingar. Dessa tre begrepp används för att beskriva vilket regelverk som är tillämpbart på förhandlingssituationen och därmed vilka handlingsalternativ som står parterna till buds. Gränserna mellan dessa förhandlingar är inte alltid knivskarpa, utan ofta går förhandlingarna in i varandra och en fråga som i ett tidigare skede behandlades som en samverkansförhandling kan i ett senare skede dyka upp igen i form av en avtalsförhandling. Avtalsförhandlingar syftar till en överenskommelse (oftast ett kollektivavtal) mellan parterna i en situation där det finns en intressekonflikt.

Tvisteförhandlingar syftar till att parterna ska kunna hantera en värdekonflikt genom att enas om hur en lag eller ett kollektivavtal ska tolkas, eller hur ett arbetsrättsligt ärende ska hanteras inom organisationen.

Samverkansförhandlingar behandlar frågor om mål och medel i verk-

samheten, till exempel hur arbetet ska organiseras på bästa sätt. Det innebär att arbetsgivaren på eget bevåg ska förhandla innan en viktigare förändring av sin verksamhet, eller innan beslut som innebär en viktigare förändring av arbets- eller anställningsförhållandena för en arbetstagare eller grupp av arbetstagare som tillhör organisationen. Arbetsgivaren har rätt att innan förhandlingen göra förberedande utredningar av olika handlingsalternativ utan att meddela arbetstagarorganisationen.

Den allmänna förhandlingsrätten är tillämpbar på alla typer av förhandlingar och garanterar att en organisation som har, eller har haft, en medlem som är eller har varit anställd får förhandla med sin motpart. Den allmänna förhandlingsrätten innebär ingen skyldighet att komma överens.

Tolkningsföreträde

I ett vanligt avtalsförhållande har vardera parten rätt att hålla inne med sin prestation till dess att den anser att motparten har uppfyllt sin del. Det är inte ovanligt att en köpare betalar hela köpeskillingen först när säljaren slutlevererat sin del. Inom arbetsrätten gäller inte denna princip. Arbetstagarna är i princip skyldiga att arbeta även om en tvist har uppstått som gäller deras arbetsskyldighet eller rätt till ersättning. Detta innebär att det är arbetsgivarens tolkning av vad avtalet eller lagen innehåller som gäller fram till dess att tvisten har lösts. Detta kallas för tolkningsföreträde. För att åstadkomma en bättre balans mellan arbetsgivare och arbetstagare vid tvister innehåller MBL speciella regler för när tolkningsföreträdet övergår till arbetstagarsidan. Det finns även regler om tolkningsföreträde i förtroendemannalagen.

Arbetstagarsidan har tolkningsföreträde i frågor som rör:

- Medbestämmanderätt enligt kollektivavtal.
- Kollektivavtal om påföljd för arbetstagare som begått avtalsbrott.
- Arbetstagares arbetsskyldighet och rätt till betalning.
- Tvist om facklig förtroendeman, dennes verksamhet eller rätt till ledig tid.

Möjligheterna till tolkningsföreträde vid frågor som rör medbestämmanderätt enligt kollektivavtal gäller alla kollektivavtal, oavsett om kollektivavtalet kallas för ett medbestämmandeavtal eller ej. Det innebär att om kollektivavtalet innehåller regler som ger arbetstagarsidan inflytande över arbetsgivarsidans beslut i vissa frågor, så får arbetstagarsidan också tolkningsföreträde vad gäller de bestämmelserna. Det kan till exempel gälla frågor om att ingå eller avsluta ett anställningsavtal, ledningen och fördelningen av arbetet eller verksamheten i övrigt. Frågan måste täckas

av de förhållanden som avses i 32 § MBL.

Verkningarna av ett tolkningsföreträde är olika beroende på kollektivavtalets innebörd. Om arbetsgivaren är skyldig att informera, samråda eller förhandla inför ett beslut och tvist uppstår om huruvida beslutet täcks av förhandlingsrätten, och arbetstagarsidan lägger sitt tolkningsföreträde, så måste arbetsgivaren förhandla innan beslutet fattas. För att arbetsgivaren ska slippa förhandla måste denne tvista om förhandlingsrättens innebörd eller acceptera arbetstagarsidans uppfattning av avtalets innebörd.

Arbetsmiljölagen (AML)

Arbetsmiljölagen innehåller regler om inflytande dels för den enskilda arbetstagaren personligen, dels för dennes representanter genom skyddsombuden och skyddskommittéerna. Det finns inte en enda systematik som kan förklara möjligheterna till inflytande i en specifik fråga. Hur en fråga handläggs beror på vilken fråga det rör sig om och vilka val som aktörerna gör i ärendet. I många fall finns det inte heller en knivskarp gräns för var en fråga kan regleras då den kan dyka upp och avhandlas på flera ställen. Till exempel kan en fråga om arbetstidsförläggning vara en del av det systematiska arbetsmiljöarbetet, för att sedan bli föremål för att skyddsombuden hänvänder sig till Arbetsmiljöverket genom 6 kap. 6 a § AML, och till sist avgöras genom ett kollektivavtal mellan parterna.

Enligt 3 kap. 1 a § AML ska arbetsgivare och arbetstagare samverka för att åstadkomma en god arbetsmiljö. Enligt 6 kap. 4 § ska skyddsombud företräda arbetstagarna i arbetsmiljöfrågor och verka för en tillfredställande arbetsmiljö.

Vad som avses med samverkan är inte helt lätt att sätta fingret på, men det är ett begrepp som har funnits och utvecklats från lagen om yrkesfara fram till dagens arbetsmiljölag. Samverkan har motiverats i lagstiftningen som ett sätt att uppnå en säker och sund arbetsmiljö, men också som ett sätt att skapa balans mellan den bestämmande parten och de som utsätts för riskerna i arbetsmiljön.

Samverkan ska ske i alla frågor som omfattas av AML. Arbetsgivaren ska samverka med skyddsombuden och i skyddskommittéerna på ett sätt som medger en möjlighet till ”reellt inflytande”. Om arbetsgivaren inte gör detta så är det att betrakta som hindrande av skyddsombudets verksamhet och grund för skadeståndstalan enligt 6 kap. 11 § AML.

Utvecklingsavtalet (UVA)

UVA innehåller en rad bestämmelser som är tänkta att på olika sätt främja samarbetet mellan arbetstagare, arbetstagarorganisationer och arbetsgivare lokalt. Avsikten med avtalet var att främja ett gemensamt arbete mellan de lokala parterna för att utveckla det egna företaget.

Parterna ville genom UVA verka för:

- Utveckling och effektivisering av företagen i alla funktioner och på alla nivåer.
- Ökad sysselsättning.
- Ökad trygghet och utveckling i arbetet.
- Bättre utnyttjande av de anställdas yrkeskunnande och yrkeserfarenheter
- Ökad decentralisering av ansvar och beslut inom företagen.

För att uppnå dessa mål innehåller UVA en rad bestämmelser som tar sikte på framför allt tre olika områden av arbetsgivarens verksamhet: utveckling av arbetstagarorganisationen (§ 3), teknisk utveckling (§ 4) och företagets ekonomi och resursfrågor (5 §). Dessa tre verksamhetsområden är naturligtvis svåra att särskilja och går många gånger in i varandra. Om arbetstagarorganisationen har svårt att analysera betydelsen av en förändring av verksamheten på grund av dess komplexitet har de rätt att under vissa förutsättningar anlita en arbetstagarkonsult som kan hjälpa dem med den analysen. Se 12 § mom. 2.

UVA är tänkt att fungera som en påbyggnad och vidareutveckling av de regler som då redan fanns i MBL, och i viss mån även i AML. Det ges förslag på hur samverkansformerna i MBL kan kompletteras genom olika förfaranden, men det är inte någon uttömmande lista. Avtalet andas en stor tilltro till att de lokala parterna bäst hittar former för hur samverkan ska gå till – i kommentarerna till avtalet nämns att tolkningsföreträde i vissa fall skulle kunna vara möjligt men att detta ska användas mycket sparsamt för att vårda den anda av samverkan som avtalet är stöpt i. Likväl finns det en hel del tydligt formulerade skyldigheter och rättigheter som arbetsgivaren måste följa för att inte anses begå kollektivavtalsbrott.

Fallen ABC: Digitala rättigheter i tre verksamheter

I denna del introduceras tre olika typer av fall där arbetstagares digitala rättigheter på något sätt påverkas. Frågorna som aktualiseras kommer sedan följa rapporten och vävs in i de avsnitt där de kan illustrera olika aspekter av regelverket. Det är viktigt att komma ihåg att även om fallen är beskrivna så noggrant som möjligt, och med verkliga situationer i åtanke, kan de ändå skilja sig mycket från hur andra situationer ser ut. Det är alltså inte säkert att det går att dra samma slutsatser i verkligheten även om det till synes kan vara liknande situationer.

Fall A – Algoritmisk styrning på lager

Arbetstagare A jobbar som plockare på ett stort lager. Lagret använder sig av tekniken röststyrd plockning (pick-by-voice). Det innebär att A har på sig ett headset. I headsetet får A instruktioner upplästa av den algoritm som i realtid följer alla artiklar och arbetare på lagret. När A har fått sin order av algoritmen styrs hon av algoritmen till den plats på lagret där nästa artikel på listan finns, till dess att hon har plockat hela ordern. Efter varje plockad artikel berättar A för algoritmen hur arbetet fortskrider. A kan också berätta om avvikelser, såsom saknade eller defekta varor. Algoritmen håller reda på vilken tid A tar på sig för att plocka ordern och hur många order hon har plockat. Underlaget används för att följa upp hur A har presterat utifrån de måltal som företaget har bestämt. Syftet med pick-by-voice-systemet är att leda och följa upp arbetet på lagret. Företaget som A jobbar för har försäkrat både personalen och fackklubben att ingen övervakning eller arbetsledning sker i realtid.

Sedan systemet med pick-by-voice har införts har arbetstempot gått upp och A upplever att hon inte längre har tid till att stanna och prata med sina kolleger eftersom hon är rädd att det skulle påverka hennes måltal. Företaget hon jobbar för säger att ingen där har tillgång till arbetstagarnas position eller rörelse, men hon upplever ofta att om hon och några kolleger tar en spontan rast tillsammans dröjer det inte länge innan hennes chef går förbi och frågar vad som händer. Det har också hänt att cheferna

råkat försäga sig och avslöja att de har iakttagit när någon har tagit en, i deras ögon, opassande lång rast eller toalettpaus.

Frågorna som aktualiseras i detta fall är om arbetsgivaren har rättslig grund för behandlingen – är personuppgifterna som samlas in genom systemet känsliga, vilka möjligheter har A att undgå att bli styrd av ett pick-by-voice-system och vad kan arbetstagare A göra för att hindra att arbetsgivaren missbrukar pick-by-voice-systemet?

Fall B – GPS-data i hemtjänsten

Arbetstagare B jobbar i hemtjänsten i en mindre kommun. Inför varje arbetspass tilldelas han en rutt där han ska göra mellan 10 och 20 besök hos brukare. Ibland kör han bil mellan brukarna och ibland använder han en cykel. Han styrs med hjälp av arbetsgivarens telefon vari det finns två appar. Den ena används för att planera hans rutt och vad han ska göra hos varje brukare, och den andra använder han för att låsa upp dörren hos de brukare som inte själva kan öppna dörren för honom. Varje arbetsdag loggar han in i de båda apparna med sitt för- och efternamn.

Appen som planerar B:s rutt och de besök han ska göra tillhandahålls av ett företag som har sitt säte i USA. Genom appen kan arbetsgivaren ta del av platsinformation samt beräkna ankomsttid för B när han befinner sig mellan två brukare.

Frågorna som aktualiseras i detta fall är om arbetsgivaren har rättslig grund för behandlingen och om arbetsgivaren har rätt att föra över personuppgifter till tredje land.

Fall C – Övervakning av kontorsarbete

Arbetstagare C jobbar som tjänsteman för ett mindre företag. Hon har sedan covid-19-pandemin bröt ut arbetat hemifrån, till en början fem dagar i veckan och på senare tid två till tre dagar per vecka. När hon började arbeta från hemmet fick hon en bärbar dator och en webbkamera från sin arbetsgivare, och ny programvara installerades som tillät onlinemöten, chattfunktion och interna forumsidor för hennes arbetsgrupp. Hennes kolleger och hennes chef kan kontakta henne via dessa. C identifierar sig varje gång hon sätter på datorn och mobiltelefonen genom en personlig kod. Om C är frånvarande från datorn händer det att hennes chef ringer henne på hennes mobil för att fråga var hon håller hus.

När C skulle ha sitt första lönesamtal efter pandemins utbrott fick hon reda på att hon inte når de mål som har satts för henne och att hon presterar sämre än sina kolleger. Hon fick också höra att hon inte var lika närvarande i den programvara som arbetsgivaren hade inhandlat för att hon skulle kunna sköta sitt arbete hemifrån. När C frågade arbetsgivaren

vad hen baserade detta på hänvisade arbetsgivaren till uppgifter som de sammanställt med information från de appar C använt för att utföra sitt arbete på distans. När C ville få se uppgifterna vägrade arbetsgivaren att lämna ut dem till henne.

Frågorna som aktualiseras i detta fall är om arbetsgivaren har rätt att neka C att granska de personuppgifter de har samlat om henne, om arbetsgivaren har rättslig grund för sin behandling, och om det har skett en ändamålsglidning i arbetsgivarens behandling av personuppgifter.

Rättsligt ramverk för anställdas digitala rättigheter

Integritet – en blind fläck för den svenska modellen?

Frågan om vilka rättigheter som finns och borde finnas för arbetstagare vad gäller deras integritet har utretts av den svenska lagstiftaren vid flera tillfällen. Vid två tillfällen har regeringen tagit emot offentliga utredningar som har behandlat frågan specifikt, SOU 2002:18 Personlig integritet i arbetslivet och SOU 2009:44 Integritetsskydd i arbetslivet. Båda utredningarna kom fram till att en ny lag som reglerar frågan skulle behövas. I SOU 2002:18 pekade utredaren på att Sverige har ett ansvar för att skydda integriteten i arbetslivet eftersom skyddet utgör en mänsklig rättighet. Utredaren konstaterade sedan att skyddet skulle göra sig bäst om det kom till uttryck i lagstiftning. I SOU 2009:44 skrev utredaren att det regelverk som fanns till skydd för arbetstagares personliga integritet var svåröverskådligt och bestod av disparata regler i olika lagstiftningar. Bristerna i det dåvarande regelverket medförde att skyddet för den personliga integriteten i arbetslivet behövde förtydligas och stärkas genom lagstiftning, enligt utredaren. Trots de båda förslagen har ingen regering lagt fram ett skarpt förslag om en speciell lag angående integritet i arbetslivet.

Integritetsutredningen, som kom med sitt förslag 2002, noterade fenomen i arbetslivet som på olika sätt kränker arbetstagares integritet. Enligt utredningen har ”alla personer rätt till en personlig sfär där ett oönskat intrång, såväl fysiskt som psykiskt, kan avvisas”. Vidare, konstaterar utredningen, varierar storleken och omfånget på denna sfär över tid, kultur, etnicitet och religiös och social bakgrund, vilket gör det vanskligt att dra upp exakta gränser i lagstiftning för vad som är tillåtet och inte.[5]

I lagförslaget från 2002 diskuteras ett förbud för arbetsgivaren att ta del av arbetstagares privata uppgifter, som till exempel e-post och andra elektroniska uppgifter som skulle kunna florera i verksamheten. Förbudet skulle gälla avsiktliga intrång och således inte gälla uppgifter som insam-

5 SOU 2002:18 s. 53.

lats utan att arbetsgivaren varit medveten om detta. Till detta förbud föreslogs två undantag: om arbetstagaren gett sitt samtycke till inhämtningen samt om uppgifterna var nödvändiga i arbetsgivarens verksamhet.

Vidare föreslogs en reglering av när arbetsgivaren skulle kunna behandla uppgifter om arbetssökandes och arbetstagares hälsa och droganvändning, personlighetstest samt personuppgifter om lagöverträdelser. Integritetsutredningen föreslog vidare hur insyn, kontroll och säkerhet skulle regleras, bland annat föreslogs en regel om att arbetsgivaren i första hand skulle vända sig till arbetstagaren för att inhämta uppgifter och bara när det inte var möjligt skulle få lov att inhämta uppgifter från andra källor. Dessutom föreslogs regler om hur fackligt inflytande skulle gå till; utredningen föreslog att reglerna skulle vara tvingande men med möjlighet för ytterligare precisering i kollektivavtal. För att uppmuntra parterna att träffa kollektivavtal på området, och därmed skapa välanpassade regler bransch- eller företagsvis, hade vissa bestämmelser lämnats avsiktligt vaga.

Utredningen SOU 2009:44 föreslog också en speciell lag för integritetsskydd i arbetslivet. Utredningen konstaterade att rätten till privatliv och personlig integritet är en mänsklig rättighet som staten har ett ansvar för att upprätthålla ett skydd för. Eftersom skyddet för arbetstagares personliga integritet bedömdes som både svåröverskådligt och varierande beroende på sektor så kom utredningen fram till att en lagstiftning som täckte större delen av arbetsmarknaden skulle vara ändamålsenlig. Lagen som utredningen föreslog tog sin utgångspunkt i dåvarande personuppgiftslagen men föreslog tre avsteg från den: (i) särskilda bestämmelser för registerkontroll och medicinska undersökningar, (ii) en generell bestämmelse som förbjuder övervaknings- och kontrollåtgärder om dessa har en påtaglig integritetsinverkan och (iii) ett generellt förbud mot integritetskränkande åtgärder i övrigt, med undantag i form av en avvägningsregel där den tillåtna kränkningen ska ha ett berättigat ändamål och som anses godtagbar efter en proportionalitetsbedömning.

I kommittébetänkandet *Så stärker vi den personliga integriteten*, SOU 2017:52, beskrevs i och för sig många risker för kränkningar av den personliga integriteten i arbetslivet. Bland annat såg kommittén allvarliga risker med både positioneringssystem och kameraövervakning i arbetslivet. Kommittén konstaterade att reglerna om integritetsskydd i samhället i stort inte verkar ha fått något vidare genomslag på den svenska arbetsmarknaden, utan att det verkar finns någon uppenbar anledning till att det förhåller sig så.[6] Till skillnad från tidigare utredningar av frågan, lyckades inte kommittén nå fram till att stödja ett lagförslag, utan föreslog istället att regeringen skulle ålägga Arbetsmiljöverket att ta fram uppfö-

6 SOU 2016:41 s. 73.

randekoder för hur integritet arbetslivet ska garanteras.[7]

På internationell nivå har också olika initiativ tagits för att få till en reglering av skyddet av personuppgifter i arbetslivet, med olika utfall.[8] ILO antog 1996 en "Code of Practice on the Protection of Workers' Personal Data".[9] Europarådet skrev i sin rekommendation från 1989, Protection of personal data used for employment purposes[10], att det är önskvärt med specifika regler som styr användningen av personuppgifter i arbetslivet. Efter att dataskyddsdirektivet antogs 1995 försökte EU-kommissionen ta initiativ till att komplettera de allmänt hållna dataskyddsreglerna med regler specifika för arbetslivet. Mellan 2001 och 2003 höll kommissionen överläggningar med arbetsmarknadens parter för att få till sådana regler, men utan framgång.[11]

Initiativen för att skapa olika specialregleringar för integritetsfrågor i arbetslivet har varit många, både nationellt i Sverige och på EU-nivå. Samtidigt kräver samtliga fackliga centralorganisationer i Sverige att frågan ska utredas återigen för att klargöra vad som gäller på den svenska arbetsmarknaden och för att stärka arbetstagares position i förhållande till arbetsgivaren.[12] De Hert & Lammerant pekar i sin rapport på behovet av att regler om integritetsskydd måste förankras hos och accepteras av arbetsmarknadens parter för att de ska få genomslag i arbetslivet.[13]

Integritetskänsliga åtgärder som arbetstvister

När en tvist uppstår i förhållandet mellan en arbetstagare och en arbetsgivare, en så kallad arbetstvist eller rättstvist, så ska tvisten handläggas enligt lagen om rättegången i arbetstvister (LRA). Begreppet arbetstvist definieras som tvister om kollektivavtal och andra tvister rörande förhållandet mellan arbetsgivare och arbetstagare.[14] Att en tvist handläggs enligt LRA innebär att Arbetsdomstolen är behörig domstol, ibland som enda instans, och ibland som följdinstans till tingsrätten.[15]

---

7 SOU 2017:52 s. 101.

8 De Hert & Lammerant: Protection of personal data in work-related Relations, European Parliament Directorate General for Internal Policies PE 474.440, 2013.

9 ILO: Code of practice on the protection of workers' personal data, Geneva, International Labour Office, 1997.

10 Europarådet: Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment Purposes, 1989.

11 EU-kommissionen: Communication from the Commission, First stage consultation of social partners on the protection of workers' personal data, 2003, http://ec.europa.eu/social/main.jsp?catId=708&langId=en

12 Se till exempel TCO:s krav om lag om personlig integritet i arbetslivet: https://kollega.se/arbetsratt/tco-kraver-ny-lag-om-personlig-integritet 2021-05-12, LO skriver i sitt remissyttrande över SOU 2016:41 att "det är nödvändigt med lagstiftning på dessa områden", Saco skriver i sitt remissvar till samma utredning att "Saco har sedan länge efterfrågat en lagreglering kring skyddet av den personliga integriteten i arbetslivet".

13 De Hert & Lammerant: Protection of personal data in work-related Relations, European Parliament Directorate General for Internal Policies PE 474.440, 2013, s. 60 ff.

14 1 kap. 1 § LRA.

15 Förhållandet mellan domstolarna bestäms i 2 kap. 1 och 2 §§ LRA.

Arbetstvister rör vanligtvis tolkningar av innehållet i ett kollektivavtal eller en regel, eller hur tillämpningen av dessa ska gå till. Intressetvister, däremot, är tvister som rör en förändring av ett kollektivavtal, eller möjligheten att träffa ett kollektivavtal. Intressetvister handläggs inte enligt lagen om rättegången i arbetstvister. När en tvist uppstår om innehållet i dataskyddsförordningen eller hur den ska tillämpas i förhållande till arbetstagare och arbetsgivare ska denna handläggas enligt lag om rättegången i arbetstvister.

När en arbetsgivare beordrar en arbetstagare att underkasta sig en integritetskänslig åtgärd är arbetstagaren som utgångspunkt skyldig att lyda. Om åtgärden står i strid med lag, eller med god sed på arbetsmarknaden, får arbetstagaren vägra att utföra det som arbetsgivaren beordrat. Om arbetsgivaren inte delar arbetstagarens uppfattning om att den tilltänkta åtgärden är olaglig, gäller arbetsgivarens tolkning av situationen till dess att rättsprocessen har haft sin gång. I vissa undantag får arbetstagaren vägra att underkasta sig en åtgärd om det föreligger fara för arbetstagarens, eller andras, liv eller hälsa. Arbetstagaren riskerar i dessa fall att bli av med sin anställning om hen gör en felbedömning av situationen, arbetsgivaren riskerar å sin sida skadeståndsansvar. Enligt Grahn och Kjällström kan en arbetstagare i princip bara få en integritetskränkande åtgärd prövad av domstol som ett brott mot LAS och som ett brott mot dataskyddsförordningen, eller som ett brott mot kollektivavtal om frågan skulle vara reglerad där (vilket är ovanligt).[16] Detta får följden att i de situationer där en fråga faller utanför dataskyddsförordningens tillämpningsområde måste en arbetstagare i princip riskera sin anställning för att kunna få prövat om en åtgärd som arbetsgivaren beordrat är lagenlig. Grahn och Kjällström pekar på att en sådan rättsordning möjligtvis inte stämmer överens med den europeiska konventionen för de mänskliga rättigheterna.

Eftersom en felbedömning kan få långtgående konsekvenser för båda parter är det viktigt att den lagstiftning och praxis som finns på området är enkel att förstå och tillämpa för båda parter. I avsaknad av ett sådant rättsläge finns det goda argument för båda parterna att träffa kollektivavtal som förtydligar vilka rättigheter och skyldigheter som gäller. Om ett kollektivavtal väl finns på plats får arbetstagarsidan möjlighet att lägga tolkningsföreträde vid tvister, vilket skulle garantera en större rättssäkerhet för arbetstagare då meningsskiljaktigheter om rättsläget uppkommer.[17]

16 Grahn & Kjällström: *Anställdas integritetsskydd*, s. 23.

17 Se Grahn & Kjällström: *Anställdas integritetsskydd*, s. 44.

Europakonventionen

Artikel 8 Europakonventionen

- Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens.
- Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Av artikel 8.1 följer att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Denna rätt får endast inskränkas med stöd av lag och om det är nödvändigt av de anledningar som listas i artikel 8.2. Artikel 8 skyddar privat- och familjelivet samt en persons korrespondens. Vid en första anblick kan det verka som att artikeln inte ger skydd för en arbetstagare i arbetslivet. Gränsen mellan vad som utgör den privata sfären och arbetslivet är inte helt enkel att dra. Europadomstolen har i domar kommit fram till att artikeln skyddar en arbetstagares rätt till privatliv också när det äger rum i arbetslivet.

I Bărbulescu[18] mot Rumänien prövade Europadomstolen för första gången en privat arbetsgivares övervakning av elektronisk kommunikation. Europadomstolen gör i domen en noggrann genomgång av de internationella regler som finns och som är tillämpbara på situationen. Europadomstolen listar sex punkter som ska utredas vid avvägningen mellan arbetsgivarens och arbetstagarens intressen. Dessa är:

- huruvida arbetstagaren informerats om att övervakning kan komma att ske
- hur långtgående övervakningen varit och graden av intrång i arbetstagarens privatliv
- huruvida arbetsgivaren har presenterat legitima skäl som rättfärdigar övervakningen
- huruvida det varit möjligt att vidta mindre ingripande åtgärder
- vilka konsekvenser övervakningen fått för arbetstagaren och hur arbetsgivaren använt resultatet av övervakningen
- huruvida arbetstagaren fått tillgång till adekvata skyddsåtgärder. Sådana skyddsåtgärder ska särskilt tillförsäkra ett skydd mot att arbetsgivaren kan få tillgång till innehållet i kommunikationer utan att arbetstagaren förvarnats om att det kan komma att ske.

18 Europadomstolen nr 61496/08.

Europakonventionen riktar sig mot stater och staters ansvar att upprätthålla rätten till privatliv för de medborgare som den härbärgerar. Grahn och Kjällström pekar på att artikel 8 i Europakonventionen för de mänskliga rättigheterna (EKMR) får allt större inflytande i integritetsfrågor och att Bărbulescu-domen är viktig vägledning vid tolkning av dataskyddsförordningen. Det regelverk som finns i dataskyddsförordningen har också vuxit fram ur artikel 8 EKMR under en längre tid.

GDPR

Syftet med dataskyddsförordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd för personuppgifter. Dataskyddsförordningen syftar till att harmonisera det lapptäcke av olika regler som dess föregångare, dataskyddsdirektivet, hade tillåtit genom medlemsstaternas olika införlivande av direktivet i nationell lag. Förordningen skapar därmed ett enhetligt skydd för personuppgifter inom hela unionen, samtidigt som den tar bort de barriärer för företag som verkar gränsöverskridande inom unionen som tidigare fanns genom skillnader i nationella lagstiftningar.

Definitioner

En *personuppgift* är information som kan knytas till och identifiera en fysisk person.

En *behandling* är en åtgärd eller en kombination av åtgärder beträffande personuppgifter, oavsett om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning, justering eller sammanförande, begränsning, radering eller förstöring.

En *personuppgiftsansvarig* är en fysisk eller juridisk person, myndighet, institution eller annat organ som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgiften.

Ett *personuppgiftsbiträde* är en fysisk eller juridisk person, offentlig myndighet eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Samtycke av den registrerade är varje slag av frivillig, specifik, informerad och otvetydig viljeyttring genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Särskilda kategorier av personuppgifter, så kallade *känsliga personuppgifter*, är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Behandlingen av dessa uppgifter är, precis som behandling av personuppgifter i allmänhet förbjuden som huvudregel. Skillnaden mellan dessa särskilda kategorier

av personuppgifter är att kraven för när det finns rättslig grund för behandling är mer strikta.

FALL A: Är personuppgifterna som samlas in genom pick-by-voice-systemet känsliga personuppgifter?

Inspelning och behandling av en persons röst är att anse som en behandling av en personuppgift enligt dataskyddsförordningen. Eftersom rösten innehåller upplysningar om en fysisk person som går att identifiera är kriterierna i artikel 4.1 dataskyddsförordningen uppfyllda. En människas röst innehåller information om kroppen som skapar rösten, till exempel kan en röst avslöja information om stämband och lungkapacitet. Detta är en form av biometriska data. Rösten kan också innehålla uppgifter om sjukdomstillstånd, till exempel går det i vissa fall att höra om någon är sjuk i parkinson. En människas tal kan också innehålla information om etniskt ursprung och olika sociala markörer som sociolekt.

Eftersom det skulle kunna vara möjligt att identifiera biometriska data, hälsotillstånd och biometriska uppgifter genom rösten skulle röstinspelningar kunna vara en så kallad känslig personuppgift (särskild kategori av personuppgifter) enligt artikel 9.1 dataskyddsförordningen. Enligt samma bestämmelse är behandling av sådana personuppgifter som huvudregel inte tillåtna. Men är röstinspelningar alltid en känslig personuppgift på grund av detta? Europeiska dataskyddsbyrån svarar på frågan genom sin riktlinje 3/2019 för behandling av personuppgifter genom videoenheter. Där illustrerar byrån med ett exempel där videosekvenser visar en registrerad person som bär glasögon och menar att sekvensen i sig inte utgör en känslig personuppgift. Det är inte förrän den personuppgiftsansvarige behandlar sekvensen för att specifikt ta fram den känsliga personuppgiften i fråga som artikel 9 blir tillämpbar. Personuppgifterna som samlas in genom pick-by-voice-systemet blir alltså inte känsliga personuppgifter om inte arbetsgivaren specifikt behandlar uppgifterna på ett sätt som gör att en känslig personuppgift framgår ur inspelningen.

Om arbetsgivaren skulle börja undersöka personuppgifterna för att se om till exempel arbetstagarnas hälsotillstånd stod bra till, då skulle också frågan om så kallad ändamålsglidning aktualiseras, eftersom uppgifterna har samlats in i syfte att leda och följa upp arbetet på lagret, men sedan använts i andra syften.

Grundläggande principer för behandling av personuppgifter

Det är den personuppgiftsansvarige som ansvarar för att principerna vid behandling av personuppgifter följs. Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De ska samlas in för särskilda uttryckligt angivna och berättigade ändamål, och inte senare behandlas på ett sätt som inte är förenligt med dessa ändamål. Personuppgifterna ska vara adekvata, relevanta, och inte för omfattande i förhållande till de ändamål för vilka de behandlas. De ska vara korrekta och, om nödvändigt, uppdaterade. Personuppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt. Vidare ska personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling.

FALL B: Har arbetsgivaren haft rätt att föra över personuppgifter till tredje land (icke EU-land)?

I fall B har arbetsgivaren köpt en tjänst av ett företag med säte i USA. Det framgår inte tydligt vilken struktur det företaget har, men i exemplet kan vi föreställa oss att de har sitt kontor någonstans i USA och att de inte har någon närvaro i EU. Detta innebär att de för över personuppgifter till USA för att kunna underhålla det elektroniska system som arbetsgivaren har köpt. Är detta förenligt med den personuppgiftsansvariges ansvar att skydda personuppgifterna mot otillåten eller obehörig behandling?

Under vissa förutsättningar är det tillåtet att överföra personuppgifter utanför EU/EES:

- Det finns ett beslut från EU-kommissionen om att exempelvis ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå.
- Den personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder, till exempel bindande företagsbestämmelser (så kallade binding corporate rules, BCR) eller standardavtalsklausuler (så kallade standard contractual clauses, SCC).
- Särskilda situationer och enstaka fall.

Det fanns tidigare ett beslut från EU-kommissionen att USA, eftersom de uppfyllde avtalet mellan parterna som kallades Privacy Shield, uppfyllde så kallad adekvat skyddsnivå. År 2020 ogiltigförklarade EU-domstolen avtalet genom den så kallade Schrems II-domen. Sedan dess har Biden-administrationen stärkt dataskyddet i USA och nu återstår det att se om EU-kommissionen på nytt kommer komma med ett beslut om att USA säkerställer så kallad adekvat skyddsnivå. I väntan på ett sådant beslut måste den personuppgiftsansvarige själv vidta lämpliga skyddsåtgärder för de personuppgifter som de överför till landet.

Rättslig grund

Som huvudregel, enligt dataskyddsförordningen, gäller att det är förbjudet att behandla en personuppgift. För att en behandling av en personuppgift ska vara laglig krävs det att den personuppgiftsansvarige har en rättslig grund att vila på. De rättsliga grunderna finns i artikel 6.1 i dataskyddsförordningen. Den lista som finns där är uttömmande, vilket innebär att det finns inga andra grunder som en personuppgiftsansvarig kan använda sig av för att göra en laglig behandling av personuppgifter.[19]

I dataskyddsförordningen finns två olika typer av rättsliga grunder. Den ena är när den registrerade har lämnat sitt samtycke till behandlingen. Denna grund finns i artikel 6.1 (a). För att ett samtycke ska vara giltigt enligt dataskyddsförordningen krävs att datasubjektet har möjlighet att fritt ge, vägra att ge eller återkalla sitt samtycke. På grund av den maktobalans som finns i relationen mellan arbetsgivare och arbetstagare har, som huvudregel, arbetstagare inte möjlighet att samtycka på det sätt som dataskyddsförordningen kräver. Arbetsgivare måste därför förlita sig på någon annan rättslig grund än samtycke, till exempel att det för arbetsgivaren är nödvändigt att behandla personuppgifterna för att tillvarata ett berättigat intresse.[20]

19 Se t.ex. EU-domstolens mål c-582/14 Breyer punkt 57.

20 Artikel 29 Integritet i arbetslivet s. 4.

Den andra typen av rättslig grund uppstår när den registrerade inte lämnar sitt samtycke men där behandlingen ändå är nödvändig för att den personuppgiftsansvarige ska kunna bedriva sin verksamhet. Dessa rättsliga grunder återfinns i artikel 6.1 b–f och tar alla utom den sista sikte på specifika situationer. Behandlingen är tillåten om den är nödvändig för att

» fullgöra ett avtal där den registrerade är en part (artikel 6.1 b),
» fullgöra en rättslig förpliktelse som åligger den personuppgiftsansvarige (artikel 6.1 c),
» skydda intressen som är av grundläggande betydelse för den registrerade eller för annan fysisk person (artikel 6.1 d),
» utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e), samt
» tillgodose ett berättigat intresse efter en intresseavvägning (artikel 6.1 f).

För att fullgöra förpliktelser som följer enligt kollektivavtal har det i svensk rätt införts förtydliganden om att både en rättslig förpliktelse och en uppgift av allmänt intresse kan uppstå genom kollektivavtal, se 2 kap. 1–2 §§ lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Kollektivavtalet har i den svenska modellen en central ställning. Löntagares rättigheter återfinns för stora grupper på arbetsmarknaden i princip uteslutande i överenskommelser mellan arbetsmarknadens parter; till exempel lön, arbetstider och semesterbestämmelser är vanligt förekommande föremål för reglering enligt kollektivavtal. Härtill förekommer också reglering av pensioner, försäkringar, föräldratillägg, semesterlön, övertidsersättning och så vidare. På grund av kollektivavtalens centrala ställning i Sverige har lagstiftaren ansett att en rättslig förpliktelse som följer av kollektivavtal är att likställa med lag och därmed utgör rättslig grund för behandling av personuppgift.[21] Med kollektivavtal avses skriftligt avtal mellan arbetsgivare (eller arbetsgivarorganisation) och arbetstagarorganisation om anställningsvillkor för arbetstagare eller om förhållandet i övrigt mellan arbetsgivare och arbetstagare.[22]

För att en rättslig förpliktelse ska kunna utgöra rättslig grund för databehandling enligt dataskyddsförordningen måste syftet med behandlingen framgå av förpliktelsen.[23] Syftet med avtalet kan inte vara att tillåta en behandling av personuppgifterna ifråga, detta skulle vara ett cirkelresonemang. För att ett kollektivavtal ska kunna utgöra rättslig grund för en personuppgiftsbehandling måste alltså kollektivavtalet vara skrivet så att

21 Se prop. 2017/18:105 s. 51 ff.
22 23 § MBL.
23 Se artikel 6.3 andra stycket första meningen dataskyddsförordningen.

det är möjligt för den registrerade att förstå vilken behandling av hens personuppgifter som sker och varför. Se mer om ändamål med personuppgiftsbehandling nedan.

Berättigat intresse artikel 6.1 (f)

Om en personuppgiftsansvarig inte hittar någon rättslig grund för en behandling som hen vill göra är det möjligt att behandlingen kan vara laglig ändå. I artikel 6.1 (f) finns en möjlighet att hitta en rättslig grund om behandlingen utförs med ett berättigat syfte och grundar sig på en intresseavvägning gjord av den personuppgiftsansvarige. Bestämmelsen samlar upp den behandling av personuppgifter som lagstiftaren anser ska få förekomma, men som inte ryms under några av de andra grunderna. Tanken är inte att det ska vara en så kallad slasktratt, utan snarare att bestämmelsen ska användas för att ge den registrerade ett bättre skydd än vad hen annars skulle ha fått om en annan rättslig grund användes. Med det sagt rör det sig om en mycket allmänt hållen rättslig grund, som är tänkt att användas på en mycket varierande uppsättning av situationer. När en arbetsgivare behandlar en arbetstagares personuppgifter är det i vissa hänseenden ganska likartade situationer, vilket ger vissa grundläggande premisser att utgå från. Trots detta kan det ändå skilja sig mycket beroende på vilken slags verksamhet det rör sig om.

För att artikel 6.1 (f) ska ge en personuppgiftsansvarig rättslig grund att behandla personuppgifterna ska behandlingen utgöra ett berättigat intresse. Det berättigade intresset ska sedan vägas mot datasubjektets rättigheter. Detta är en av de viktigaste rättsliga grunderna i dataskyddsförordningen.[24] Den som ska ha ett berättigat intresse kan vara den personuppgiftsansvarige, men det kan också vara en så kallad tredje person, alltså någon som inte är registrerad eller personuppgiftsansvarig, personuppgiftsombud eller personuppgiftsbiträde enligt dataskyddsförordningen, men som ändå kan eller ska få tillgång till de aktuella personuppgifterna.

Det finns inte någon uttömmande lista för vad som är ett berättigat intresse.[25] Vad som utgör ett sådant kan skilja sig från situation till situation. Begreppet förekommer på många ställen i dataskyddsförordningen, men någon generell vägledning finns inte för vad som är ett berättigat intresse. Som minsta krav på ett berättigat intresse, bör intresset vara förenligt med rättsordningen. Det vill säga att den som för ett olagligt ändamål, till exempel utpressning eller i syfte att motverka att arbetstagare organiserar sig fackligt, samlar in och behandlar personuppgifter har inte något berättigat intresse att göra detta.[26]

24 Grahn och Kjällström s. 92.

25 Grahn och Kjällström s. 93.

26 Yttrande 03/2013 artikel 29-gruppen, s. 19, jämför också principen om pactum turpe, som innebär att avtal om brottslig verksamhet inte är bindande juridiskt.

I skäl 47 i dataskyddsförordningen framgår att ett berättigat intresse kan finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige, som när den registrerade arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning som inbegriper huruvida den registrerade vid inhämtandet av personuppgifterna kunde förvänta sig att uppgiftsbehandlingen för ändamålet ifråga kan komma att ske.

EU-domstolen ger inte mycket vägledning när det kommer till vad ett berättigat intresse kan vara, men den har kommit fram till att det ”inte råder något tvivel” om att det är ett berättigat intresse att få tillgång till personuppgifter som krävs för att väcka talan om ersättning i en rättsprocess.[27] Arbetsdomstolen har kommit fram till att fackförbund har ett berättigat intresse av att kontrollera kollektivavtals efterlevnad avseende samtliga arbetstagare inom avtalsområdet.[28] Integritetsmyndigheten, IMY, har i ett beslut slagit fast att Spotify hade ett berättigat intresse då de behandlade personuppgifter för att motverka bedrägerier.[29]

Intresseavvägning artikel 6.1 (f)

Precis som att det inte finns någon färdig lista för vilka intressen som ska anses vara berättigade finns det vid intresseavvägningen inga färdiga mallar för hur den ska utfalla. EU-domstolen framhäver i sina avgöranden att det inte går att kategoriskt eller generellt på förhand avgöra hur en intresseavvägning ska utfalla, det måste alltid göras en helhetsbedömning.[30] Därför går det inte att ge några definitiva svar på förhand, men nedan följer en redogörelse för olika resonemang som har ansetts intressanta.

Digital konsekvensbedömning

Innan en behandling av personuppgifter som kan innebära risker för de registrerade ska, enligt artikel 35 i GDPR , en konsekvensbedömning göras. Konsekvensbedömningen ska ta sikte på vilken behandling som görs, omfattningen, kontexten och ändamålet med behandlingen. De risker som upptäcks vid en konsekvensbedömning ska åtgärdas. När en arbetsgivare gör en konsekvensbedömning ska hen samråda med fackföreningen på arbetsplatsen, detta följer av både artikel 35 och MBL. Om ett samråd slutar i oenighet ska arbetsgivaren motivera särskilt varför hen väljer att gå vidare med behandlingen.

En intresseavvägning är en helhetsbedömning där den tilltänkte personuppgiftsansvariges intresse av att behandlingen utförs ställs mot den registrerades skydd för den personliga integriteten och rätten till privatliv. En arbetsgivare får alltså med andra ord behandla personuppgifter efter

27 Rigas Satiksme C-13/16 punkt 29.

28 AD 2018 nr 65 & AD 2010 nr 87.

29 IMY Beslut DI-2020-10541.

30 Se till exempel de förenade målen ASNEF och FECEMD, C-468/10 och C-469/10, punkterna 47 och 48, Breyer C-582/14 punkt 62, och Rigas Satiksme C-13/16 punkt 31.

en intresseavvägning, om det är nödvändigt och intresset av att behandla uppgifterna är större än den anställdes intresse av att uppgifterna inte behandlas. Det går alltså inte att säga att en intresseavvägning ska falla ut på ett visst sätt, men det finns vissa generella principer som borde iakttas. I lagstiftningsärenden rörande personuppgiftslagen har lagstiftaren påpekat att företagsekonomiska skäl väger lättare än säkerhetsmässiga vid en intresseavvägning.[31] Detta ställningstagande har också Datainspektionen kommit fram till.[32]

Mot arbetsgivarens intresse ska den anställdes intresse av skydd för den personliga integriteten och rätten till privatliv ställas. Datainspektionen slår fast att en arbetsgivare alltid måste beakta att en anställd befinner sig i en beroendeställning gentemot denne.[33] Den registrerades intresse av skydd kan variera beroende på vilken typ av uppgifter det rör sig om.[34] I fallet Rigas Satiksme ville en privatperson få ut personuppgifter från en myndighet i form av videomaterial från en övervakningskamera, i syfte att kunna väcka talan om skadestånd i samband med en trafikolycka. EU-domstolen ansåg i fallet att privatpersonen hade ett berättigat intresse av att hävda sin rätt vid en domstol och säger att utfallet vid intresseavvägningen är beroende av de konkreta omständigheterna i det enskilda fallet. Domstolen pekar också på att det vid intresseavvägningen är möjligt att beakta allvaret i den kränkning som utlämning av namn, adress och personnummer (vilka domstolen bedömde som nödvändiga uppgifter för att med tillräcklig precision kunna stämma vid domstol) innebär och pekade vidare på att allvaret i kränkningen minskar om sådana uppgifter i medlemslandet normalt sett är tillgängliga för allmänheten.[35]

FALL C: Har arbetsgivaren rättslig grund för sin behandling?

Eftersom samtycke som huvudregel inte kan användas som rättslig grund för behandling av personuppgifter i arbetslivet behöver arbetsgivaren mest sannolikt luta sig mot en intresseavvägning enligt artikel 6.1 f i dataskyddsförordningen. För att den ska kunna ge arbetsgivaren rätt att behandla personuppgifterna i fråga krävs att arbetsgivaren har ett berättigat intresse av behandlingen. Om det finns ett berättigat intresse ska en intresseavvägning göras och om arbetsgivarens intresse väger tyngre än arbetstagarens så finns det rättslig grund för behandlingen.

Att mäta arbetstagares prestationer och göra säkerhetskontroller för att hindra utomstående från att få tillgång till organisationens system är båda berättigade intressen enligt dataskyddsförordningen. Frågan blir därför om arbetsgivarens intresse av att mäta arbetstagares prestationer och garantera sin it-säkerhet

31 SOU 1997:39 s. 365.

32 Datainspektionen: Intresseavvägning enligt personuppgiftslagen. Datainspektionen informerar, 2015, s. 11.

33 Datainspektionen: Intresseavvägning enligt personuppgiftslagen. Datainspektionen informerar, 2015, s. 12.

34 Grahn & Kjällström s. 95, AD 2010 nr 87.

35 Rigas Satiksme C-13/16 punkt 31.

väger tyngre än arbetstagarens intresse av att inte bli övervakad vid distansarbete. Frågan om arbetsgivarens övervakning av arbetstagaren är proportionerlig aktualiseras också.

I förevarande fall så blir arbetstagare C på olika sätt övervakad av sin arbetsgivare i sitt hem, och inte på sin arbetsplats. Detta gör att en eventuell integritetskränkning blir ännu allvarligare eftersom den försiggår i det rum där C i normalfallet har ett andrum från sitt arbetsliv, och det är där C:s personliga sfär existerar.

Mycket av den behandling av personuppgifter som tekniken vid distansarbete tillåter, till exempel att logga tangentnedslag och musrörelser, ta skärmdumpar på arbetstagarens dator, aktivera webbkameror eller samla in inspelat material, är väldigt långtgående i hur integritetskränkande de är. Att mäta när en arbetstagare sitter vid sin dator och när hen inte gör det är också en långtgående integritetskränkning när det sker i en arbetstagares hem eftersom det kan ge arbetsgivaren information om hur arbetstagaren beter sig och vilka vanor denne har. Vid en proportionalitetsbedömning ska den personuppgiftsansvarige bedöma om det finns andra, mindre integritetskränkande metoder, som kan åstadkomma samma syfte.

Artikel 29-gruppen kommer fram till att behandling som övervakar distansarbetare i normalfallet inte kan vara proportionerlig och att arbetsgivare därför inte har någon rättslig grund för att utföra sådan behandling.[36] Detta ställningstagande stämmer överens med ett beslut från 2005 där Datainspektionen kom fram till att inspelning av säljsamtal på ett callcenter, där uppgifterna lagrades i 3–18 månader i syfte att säkerställa kvalitet i samtalen mot kunderna, inte kunde tillåtas efter en intresseavvägning.[37]

Vad gäller kontrollen av arbetstider som arbetsgivaren har gjort har Datainspektionen tagit ställning i ett fall där en arbetsgivare använde sig av data från tjänstebilars GPS för att direkt registrera arbetstid. Datainspektionen ansåg inte att detta var tillåtet eftersom ändamålet kunde uppnås med mindre ingripande åtgärder. [38]

Sammanfattningsvis finns det mycket som tyder på att den övervakning som C:s arbetsgivare bedriver av C förmodligen inte är proportionerlig, och den väger förmodligen inte tyngre än C:s intresse av att inte bli övervakad i sitt eget hem.

Myndigheters behandling av anställdas personuppgifter

När myndigheter ska behandla personuppgifter vid *fullgörandet av sina uppgifter* får de inte använda sig av en intresseavvägning som rättslig grund. Det är inte klarlagt vad fullgörandet av sina uppgifter innebär i en svensk kontext. Det finns två olika tolkningar av begreppet, som ger vitt skilda resultat i praktiken. Den ena tolkningen innebär att fullgörandet av sina uppgifter tar sikte på en myndighets myndighetsutövning. Det skulle innebära att andra uppgifter som en myndighet utför, som är mer allmänt hållna, som till exempel administration som rör myndighetens arbetsgivarfunktioner, skulle falla utanför förbudet. I så fall får en myndighet använda sig av en intresseavvägning som rättslig grund för att behandla sina arbetstagares personuppgifter, under förutsättning att behandlingen inte

36 Artikel 29-arbetsgruppen för uppgiftsskydd: Yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen, WP 249.

37 Datainspektionens beslut dnr 121-2005.

38 Datainspektionens beslut dnr 806-2007.

faller under begreppet ”fullgörande av sina uppgifter”, och att behandlingen i övrigt uppfyller de krav som ställs vid en behandling av personuppgifter efter en intresseavvägning.

En annan tolkning av förbudet i artikel 6.1 dataskyddsförordningen är att myndigheter inte får använda sig av intresseavvägningar överhuvudtaget i sin verksamhet. I så fall måste den offentliga arbetsgivaren hitta en annan rättslig grund för att behandla sina anställdas personuppgifter.

SKR skriver i sin rapport *Personuppgifter i arbetslive*t att kommuner och regioner bör kunna använda sig av den rättsliga grunden uppgift av allmänt intresse, artikel 6.1 e dataskyddsförordningen, när de behandlar personuppgifter som de inte har direkt lagstöd för och som ligger utanför den myndighetsspecifika verksamheten.[39] För att en personuppgiftsansvarig ska kunna luta sig mot 6.1 e måste det emellertid röra sig om en uppgift som myndigheten är ålagd att utföra enligt lag. Databehandlingen, för att ha rättslig grund, måste vara nödvändig för att myndigheten ska kunna utföra sin uppgift, och det måste framgå ur lagen tydligt och precist nog för att det ska vara förutsägbart för de registrerade att deras personuppgifter kan komma att behandlas. Detta specificeras i artikel 6.3 och skäl 41 dataskyddsförordningen.

FALL B: Vilken rättslig grund kan arbetsgivaren (kommunen) använda sig av för att övervaka sina anställda?

Vad som gäller i fall då kommuner övervakar sina anställda genom olika GPS-system är inte klarlagt. Frågan här blir vilken rättslig grund som myndigheten (kommunen) har använt sig av för införandet av GPS-systemet. Kommunen kan ha använt sig av en intresseavvägning för att hitta rättslig grund för systemet. B har rätt till information om vilken rättslig grund som använts, i enlighet med artikel 14 dataskyddsdirektivet. Som huvudregel får myndigheter inte använda sig av intresseavvägning vid fullgörandet av sina uppgifter, se ovan. Det är oklart om detta förbud också gäller när kommunen utför behandlingar av personuppgifter i egenskap av sin roll som arbetsgivare. Oaktat detta så är det inte säkert att GPS-övervakning inom hemtjänsten skulle kunna anses vara en handling som kommunen utför i sin roll av arbetsgivare, och alltså inte omfattas av förbudet som gäller då kommunen "fullgör sina uppgifter". Svaret på denna fråga beror på hur man ska klassificera GPS-övervakning vid utförandet av hemtjänstuppgifter. De personuppgifter som arbetstagare genererar då de använder sig av systemen är inte främst uppgifter som krävs för arbetsgivaren att utföra sina uppgifter i egenskap av arbetsgivare. Systemen syftar snarare mot att erbjuda hemtjänst åt kommunens medborgare. Om förbudet gäller, behöver kommunen ett bemyndigande i lag för att använda sig av GPS-system för att övervaka sina anställda.

Kommunen är skyldig att erbjuda omvårdnad i form av hemtjänst enligt socialtjänstlagen. Det är emellertid inte säkert om en sådan skyldighet tillräckligt tydligt ålägger kommunen att införa GPS-system inom hemtjänsten att det skulle kunna utgöra en rättslig grund i dataskyddsförordningens mening.

Det får anses oklart vilken rättslig grund som kommunen kan använda för att utföra GPS-övervakning av sina anställda, om det överhuvudtaget finns någon.

39 Sveriges Kommuner och Regioner: *Personuppgifter i arbetslivet*, 2021, s. 10f.

Proportionalitetsbedömning

Artikel 29-gruppen rekommenderar alla arbetsgivare att göra ett proportionalitetstest, i enlighet med skäl 4 till dataskyddsförordningen, innan behandlingen påbörjas. Testet ska göras för att ta reda på om behandlingen är nödvändig för ett berättigat ändamål och vilka åtgärder som eventuellt behöver vidtas för att försäkra sig om att rätten till privatliv och kommunikationshemligheter kränks så lite som möjligt.[40]

Enligt artikel 29-gruppen är det viktigt att arbetsgivaren vidtar specifika åtgärder i syfte att upprätthålla den rätta balansen mellan arbetsgivarens berättigade intressen och arbetstagarnas grundläggande fri- och rättigheter. Sådana åtgärder bör, beroende på vilken typ av integritetskränkning som är aktuell, bland annat handla om att begränsa kränkningen så långt det är möjligt. Vid övervakning av arbetstagare kan det vara lämpligt att begränsa övervakningen till att bara gälla vissa geografiska områden, eller vissa specifika uppgifter, eller så kan övervakningen begränsas till vissa tider.

I en informationsskrift från 2015 ger Datainspektionen vägledning om vilka intressen som kan vara berättigade i arbetslivet, och vilka som normalt sett inte är det. Generellt sett, menar myndigheten, är det så att intressen som har sin grund i säkerhetsskäl väger tyngre än intressen som beror på företagsekonomiska effektivitetsskäl.[41]

FALL A: Har arbetsgivaren rättslig grund för behandlingen?

Det är i princip inte möjligt att finna rättslig grund i samtycke för behandlingen av personuppgifter inom ramen för förhållandet mellan arbetstagare och arbetsgivare. Frågan blir då om arbetsgivaren kan finna rättslig grund genom en intresseavvägning, och om åtgärden är proportionerlig.

Frågan blir sedan om arbetsgivaren har ett berättigat intresse av att behandla personuppgifterna. Begreppet berättigat intresse är mycket brett. Som minsta krav måste intresset vara förenligt med rättsordningen, alltså inte vara direkt olagligt. I sina riktlinjer om personlig integritet i arbetslivet skriver dåvarande Datainspektionen att det är ett berättigat intresse att planera, leda och följa upp arbetet.

Eftersom det rör sig om ett berättigat intresse från arbetsgivarens sida måste en intresseavvägning göras. Där står arbetsgivarens intresse av att styra organisationen på ett ekonomiskt effektivt sätt på ena sidan och arbetstagare A:s intresse av att inte få sin personliga integritet kränkt på andra sidan. Enligt praxis väger företagsekonomiska effektivitetsskäl väldigt lätt och bör som regel inte väga tyngre än arbetstagares personliga integritet. I den offentliga utredningen Integritet, Offentlighet, Informationsteknik skriver utredningen att rent kommersiella intressen måste ha en särskild tyngd för att väga över den enskildes intresse av skydd för den personliga integriteten. [42]

Mot arbetsgivarens intresse ställs arbetstagarens intresse av skydd. Som alltid

40 Yttrande 8/2017 artikel 29-gruppen.

41 Se bilaga I.

42 SOU 1997:39 s. 365.

när det rör sig om förhållandet mellan arbetsgivare och arbetstagare måste det beaktas att arbetstagare befinner sig i en beroendeställning gentemot arbetsgivaren och att de därför är extra utsatta. I denna del spelar det roll vilken typ av uppgift det rör sig om. I förevarande fall rör det sig om röst och tal, samt arbetsprestationer som på olika sätt behandlas och kan knytas till den enskilde arbetstagaren. Eftersom det ur röst och tal kan utvinnas sekundära, känsliga uppgifter, kan dessa uppgifter vara mer känsliga och därför väga tyngre vid en intresseavvägning. Exakt hur en domstol skulle resonera i detta fall är däremot svårt att säga på förhand.

Vid en sammantagen bedömning är det svårt att säga om arbetsgivaren har rättslig grund för behandling av personuppgifterna som samlas in och behandlas genom pick-by-voice-systemet. Det finns faktorer som påverkar åt båda hållen.

Att övervaka arbetstagarna och deras arbete på arbetsplatsen i realtid är i jämförelse mycket mer integritetskränkande. Vid en intresseavvägning skulle arbetstagarnas rätt till skydd för sin integritet i detta fall väga ännu tyngre, och det är svårt att se att det skulle finnas rättslig grund till denna typ av övervakning efter en intresseavvägning. Den information som arbetsgivaren har spridit på arbetsplatsen har också uttryckligen uppgett att syftet med pick-by-voice-systemet inte har varit att kunna följa arbetstagarna i realtid. Om arbetsgivaren skulle börja använda sin tillgång till systemet för att följa arbetstagarna i realtid aktualiseras också frågan om det har skett en så kallad ändamålsglidning.

Rätt till information

Rätten till information är hörnstenen i det skydd som finns i dataskyddsförordningen. Gränserna för vilken information som ska lämnas, antingen på arbetsgivarens initiativ eller på arbetstagarens, utgör i mångt och mycket också gränserna för vad arbetstagaren och arbetstagarorganisationen kan påverka. För att kunna värna den personliga integriteten på arbetsplatsen måste arbetstagarna få reda på vilka personuppgifter som lagras om dem, när och vid vilket tillfälle personuppgifterna inhämtades och från vilken källa.

Om personuppgifter om den anställde har samlats in från en annan källa än från den anställde själv ska arbetsgivaren informera den anställde om detta inom rimlig tid, dock senast en månad efter att personuppgifterna samlats in enligt artikel 14.3 dataskyddsförordningen.

Oavsett om data har insamlats från den registrerade eller en annan källa ska information lämnas om

- den personuppgiftsansvariges identitet och kontaktuppgifter, och kontaktuppgifter till dataskyddsombudet, om ett sådant finns
- ändamålen för databehandlingen och den rättsliga grunden
- vilka som ska ta emot personuppgifterna
- vissa rättigheter som den registrerade har, till exempel att begära tillgång till och rättelse eller radering av personuppgifter, eller begränsning av behandling, rätten att invända mot behandling, samt rätten till dataportabilitet

» hur länge personuppgifterna kommer att behandlas eller hur den perioden fastställs

» eventuellt automatiserat beslutsfattande.

Jämför här Arbetsmiljöverkets föreskrift AFS 1998:5 10 §, där det framgår att kvantitativ eller kvalitativ kontroll av arbetstagares insats via ett datasystem inte får utföras utan dennes vetskap.

Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att tillhandahålla informationen i en klar, tydlig, begriplig och lättillgänglig form. Den registrerade har också rätt att få informationen muntligen om hen begär detta.[43] I ett avgörande från 2014 uttalar sig EU-domstolen om räckvidden för rätten till information. Avgörandet kom innan dataskyddsförordningen trädde i kraft men kan i relevanta delar ändå ge vägledning. EU-domstolen skriver att varje registrerad har rätt att få information om samtliga personuppgifter om honom eller henne som behandlas av den personuppgiftsansvarige. Informationen ska vara begriplig, det vill säga att den gör det möjligt för den registrerade att få kännedom om dessa uppgifter och kontrollera att de är korrekta och att de behandlas på ett sätt som är förenligt med direktivet, i syfte att den registrerade, i förekommande fall, ska kunna utöva de rättigheter som tillförsäkras honom eller henne.[44]

I artikel 14.5 b dataskyddsförordningen finns några undantag för när den personuppgiftsansvarige är skyldig att lämna ut information. Om det skulle visa sig omöjligt att lämna ut informationen behöver den personuppgiftsansvarige inte lämna ut den. Detsamma gäller om det skulle medföra en oproportionerligt stor ansträngning att lämna ut informationen. Dessa två undantag är i praktiken inte tillämpbara i arbetslivet eftersom det inom ramen för ett anställningsförhållande bör finnas ett löpande informationsutbyte mellan arbetstagare och arbetsgivare.[45]

Om utlämnandet av informationen skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen behöver den personuppgiftsansvarige inte heller lämna ut information. Detta undantag tar sikte på till exempel om en personuppgift förekommer i ett visselblåsarärende eller till exempel vid utredning om brott mot diskrimineringslagen, eller liknande personalärende, där utredningen av ärendet skulle komma att försvåras i det fall att den registrerade skulle få information om ärendets existens.

Om den personuppgiftsansvarige avser använda sig av något av undantagen ovan, som finns i artikel 14.5 b i dataskyddsförordningen, ska

43 Se artikel 12.1 dataskyddsförordningen.

44 EU-domstolen de förenade målen C-141/12 Rechtbank Middelburg och C-372/12 Raad van State, s. 57.

45 Grahn & Kjällström: Anställdas integritetsskydd, s. 169.

hen vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, samt göra uppgifterna tillgängliga för allmänheten. Med detta avses en skyldighet att utforma information om hur personuppgifterna behandlas generellt, som är tillgänglig för alla arbetstagare på arbetsplatsen.

I vissa fall kan information behöva lämnas igen till den registrerade. Till exempel om personuppgifterna ska användas för ett nytt ändamål, så kallad ändamålsglidning.

Rätten att invända

Enligt artikel 21.1 i dataskyddsförordningen ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 f. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter. Detta innebär att det krävs en särskild typ av intresseavvägning i fall där den registrerade har motsatt sig behandlingen av hens personuppgifter. I denna särskilda intresseavvägning krävs det att den personuppgiftsansvarige har ”tvingande berättigade skäl” som väger tyngre än den registrerades intressen för att få fortsätta sin databehandling.

Rätt till tillgång

Rätten till tillgång är i själva verket en del av rätten till information, men tar sikte på när den registrerade själv vänder sig till den personuppgiftsansvarige för att få information om den databehandling som hen utför.

Rätten till tillgång består av tre komponenter: bekräftelse på om personuppgifter behandlas eller inte, tillgång till dessa personuppgifter om så skulle vara fallet och tillgång till information om processen. Rätten till tillgång finns i artikel 15 dataskyddsförordningen. Det finns inga formkrav på hur en förfrågan om rätten till tillgång ska se ut. Europeiska dataskyddsbyrån menar att en personuppgiftsansvarig borde erbjuda mallar för hur en registrerad kan hävda sin rätt till tillgång, men att detta inte betyder att den personuppgiftsansvarige kan avvisa andra förfrågningar om de kom genom andra kanaler.[46]

Enligt artikel 15 i dataskyddsförordningen har den registrerade rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör hen håller på att behandlas och i så fall få tillgång till personuppgifterna, ett så kallat registerutdrag, samt information om

» ändamålen med behandlingen

46 Europeiska dataskyddsstyrelsen, Guidelines 01/2022 on data subject rights – Right of access s. 2.

» vilka kategorier av personuppgifter som behandlingen gäller

» vilka mottagarna av uppgifterna är

» under vilken period som personuppgifterna kommer att lagras, eller vilka kriterier som används för att fastställa denna period

» rätten till rättelse, radering, begränsning samt till invändning

» rätten att inge klagomål till tillsynsmyndighet

» varifrån personuppgifterna har samlats in om det inte är från den registrerade

» förekomsten av automatiserat beslutsfattande.

Precis som vid rätten till information ska information om behandlingen ges i en klar, tydlig, begriplig och lättillgänglig form. Vad detta innebär mer precis får avgöras från fall till fall beroende på de omständigheter som föreligger. Faktorer som spelar in är vilken typ av verksamhet och behandling som är aktuell samt den registrerades förmåga att tillgodogöra sig innehållet i olika former för informationen.[47]

Det finns vissa begränsningar av rätten till tillgång i dataskyddsförordningen. Enligt artikel 15.4 får inte rätten att få ett registerutdrag gå ut över andras rättigheter och friheter. Med detta åsyftas att andra registrerades rätt till privatliv måste respekteras när till exempel registerutdrag lämnas ut. Det är enligt Europeiska dataskyddsbyrån den personuppgiftsansvarige som har bevisbördan för att ett utlämnande av denna typ skulle få påverkan på andras rättigheter och därmed inte bör göras.[48] Det är också möjligt för en personuppgiftsansvarig att avslå förfrågningar som är grundlösa eller för omfattande, eller ta ut en avgift för dessa enligt artikel 12.5.

FALL C Vilken rätt har C till information om de personuppgifter som arbetsgivaren har samlat om henne?

I Fall C har den registrerade begärt att få tillgång till uppgifterna som arbetsgivaren har samlat in om henne. Enligt artikel 15 ska C få tillgång till uppgifterna som arbetsgivaren har samlat in. Såvida arbetsgivaren inte kan hitta ett tillämpbart undantag till denna rätt så har C rätt att ta del av dessa personuppgifter. Det är svårt att se att något av undantagen skulle vara tillämpbara i C:s fall.

Rätt till rättelse

Den registrerade ska ha rätt att utan dröjsmål få felaktiga personuppgifter rättade. Om det påverkar ändamålet med personuppgiftsbehandlingen

47 Europeiska dataskyddsstyrelsen, Guidelines 01/2022 on data subject rights – Right of access s. 3.

48 Europeiska dataskyddsstyrelsen, Guidelines 01/2022 on data subject rights – Right of access s. 4.

ska den registrerade ha rätt att komplettera ofullständiga personuppgifter.[49] En av grundprinciperna som den personuppgiftsansvarige måste följa är att uppgifterna måste vara korrekta och om nödvändigt uppdaterade. Enligt artikel 18.1 a kan den registrerade begära att den personuppgiftsansvarige ska begränsa sin behandling om den registrerade anser att uppgifterna inte är korrekta. Den personuppgiftsansvarige är därefter tvungen att underrätta den registrerade när kontrollen av uppgifterna är gjord och begränsningen upphör.

Rättigheter i förhållande till automatiskt beslutsfattande

Enligt artikel 22 i dataskyddsförordningen har en registrerad rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Denna rättighet är i praktiken ett förbud mot automatiskt beslutsfattande, som trots lydelsen inte kräver att den registrerade åberopar bestämmelsen för att den ska gälla. Hur långt detta förbud sträcker sig är inte helt tydligt. Artikeln är omgiven av en rad osäkerheter, vad gäller omfång, tillämpbarhet och bakomliggande syfte.[50] I skrivande stund finns ett mål i EU-domstolen som rör artikelns omfång. I mål C-634/21, som ännu inte är avgjort, har generaladvokaten yttrat sig bland annat om kriteriet att ett beslut enbart ska grundas på automatiskt beslutsfattande för att förbudet ska inträda.

Generaladvokaten påpekar att termen beslut ska tolkas brett. Det kan röra sig om åsikter eller ställningstaganden som kan få juridiska, ekonomiska eller sociala konsekvenser. Generaladvokaten anser också att artikeln inte innebär att beslutet enbart ska grunda sig på ett automatiskt beslutsfattande. Även om det är en människa som formellt tar ett beslut kan förbudet träda in, om människan som tar beslutet i fråga är assisterad av ett automatiskt system som tillhandahåller ett underlag som i praktiken bestämmer hur beslutet ska bli. Det måste alltså finnas en reell möjlighet för en människa att ta ett beslut som går emot det AI:n föreslår. Om AI:n har levererat ett underlag måste alltså den människa som i slutändan står för beslutet ha haft en praktisk möjlighet att granska och göra om det underlag som AI:n levererat. Generaladvokatens åsikt vid EU-domstolen är ett slags förberedande arbete som sedan kommer ingå i beslutsunderlaget när domstolen fattar sitt beslut. Domstolen kommer inte nödvändigtvis fatta samma beslut eller grunda det på samma omständigheter som generaladvokaten, men ofta ger generaladvokatens åsikt en fingervisning om hur beslutet kommer bli.

49 Se artikel 16 dataskyddsförordningen.

50 Se genomgången av artikeln i B. Waas: *Artificial Intelligence and Labour Law*, HIS-Working Paper No. 17, december 2022, s. 145 ff.

Förbudet gäller inte då beslutet är uttryckligen tillåtet enligt unionsrätten eller en medlemsstats nationella rätt som fastställer lämpliga åtgärder för skydd för den registrerade. Om behandlingen krävs för ingående eller fullgörande av ett avtal, eller om den registrerade har gett sitt samtycke till behandlingen, får den ändå genomföras. I dessa fall krävs att den personuppgiftsansvarige ska genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna uttrycka sin åsikt och bestrida beslutet.

Vid automatiskt beslutsfattande där känsliga personuppgifter utgör en del av underlaget gäller inte de undantag mot förbudet som beskrivs ovan. Känsliga personuppgifter får endast ligga till grund för automatiskt beslutsfattande om den registrerade har medgivit behandlingen med vad som kallas för explicit samtycke[51], eller om det är nödvändigt för ett substantiellt allmänintresse.[52] Ett explicit samtycke är ännu mer kvalificerat än det vanliga samtycket enligt artikel 6 dataskyddsförordningen. De skiljer sig åt på så sätt att ett explicit samtycke kräver ett uttryckligt uttalande om samtycke från den registrerade.[53]

Artikel 29-gruppen anger att personuppgiftsansvariga som använder sig av automatiskt beslutsfattande måste vara extra varsamma i syfte att uppfylla kraven på transparens.

Gruppen menar att en personuppgiftsansvarig som använder sig av sådant automatiskt beslutsfattande som avses i artikel 22 dataskyddsförordningen måste

» berätta för den registrerade att de bedriver automatiskt beslutsfattande
» tillhandahålla meningsfull information om logiken bakom, och
» förklara relevansen och föreställda[54] konsekvenser av databehandlingen.[55]

Den personuppgiftsansvarige måste alltså hitta enkla sätt att berätta för den registrerade om rationaliteten som styr, eller vilka kriterier som avgör vilket beslut som fattats. Rätten till information och rätten till tillgång ger den registrerade en rättighet att få en förklaring av hur algoritmen fungerar, men det är inte helt tydligt hur långt den rätten sträcker sig och på

51 Enligt artikel 9.2 a dataskyddsförordningen.

52 Enligt artikel 9.2 g dataskyddsförordningen.

53 Article 29 Data Protection Working Party: Guidelines on consent under Regulation 2016/679, 05/2020, s. 20.

54 Här skriver artikel-29 gruppen "envisaged" som jag har valt att översätta till föreställda.

55 Article 29 Data Protection Working Party: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, s. 13

vilken nivå algoritmen behöver förklaras.

I de allra flesta fall är ett företags algoritmer affärshemligheter som de vaktar noggrant. Nick Seaver skriver om svårigheterna med att studera en algoritm och kommer fram till att det främst rör sig om två försvårande omständigheter: dels att tillgången till algoritmens funktionssätt är kraftigt begränsad eftersom de företag som äger algoritmen vanligtvis försöker neka insyn så gott det går, dels att det krävs stora förkunskaper för att kunna förstå den information som går att dela från algoritmen.[56] Det är alltså inte säkert att den information som en personuppgiftsansvarig har från en algoritms funktionssätt kan presenteras på ett sätt som gör att den går att förstå för en arbetstagare eller facklig företrädare med genomsnittliga förkunskaper på området.

Oaktat svårigheterna att ta till sig informationen är rätten till tillgång och rätten till information i förhållande till AI-system omdebatterade. Argument har framförts för att samma regler som gäller personuppgifter i övrigt också ska tillämpas på AI-system. Det innebär att information om behandlingen ska ges i en klar, tydlig, begriplig och lättillgänglig form, och att detta gäller samtliga detaljer för en algoritms funktionssätt. Motståndare till denna uppfattning menar att en sådan rätt inte existerar förutom, möjligtvis, i vissa undantagsfall. De pekar på att det i normalfallet räcker med en förklaring av AI-systemets funktionssätt på en mycket mer övergripande nivå, vilka personuppgifter som används och varför de bedöms vara relevanta.[57] När en arbetsgivare hävdar att information om ett AI-system inte går att göra begripligt finns det för ett fackförbund skäl att vara vaksam, eftersom denne kan ha ett egenintresse av att motparten inte har alla fakta vid en förhandling.

Kommissionen har i sitt förslag till AI-förordning valt en riskbaserad regleringsmodell som innebär att olika regler ska gälla beroende på vilken grad av risk ett AI-system bedöms ha. För så kallade högrisksystem, där AI som utför olika arbetsledande uppgifter kommer att ingå, innehåller förslaget krav på transparens gentemot den som använder sig av systemen. Exakt hur AI-förordningen ska få sin slutgiltiga utformning är oklart i dagsläget, men förhandlingarna inom den så kallade trilogen är i sitt slutskede i skrivande stund. Förhoppningsvis blir de oklarheter som finns i dataskyddsförordningen belysta av förtydliganden i AI-förordningen.

Rätten till begränsning av databehandling

I vissa fall kan den personuppgiftsansvarige bli ålagd av den registrerade

56 N. Seaver: Knowing Algorithms i J. Vertesi & D. Ribes (red.): digitalSTS, *A field guide to Science and Technology Studies* (2019), Princeton University Press s. 412–422.

57 Se till exempel S. Wachter, B. Mittelstadt & L. Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, Volume 7, Issue 2, 2017, s. 76–99, och B. Goodman & S. Flaxman: European Union regulations on algorithmic decision-making and a "right to explanation", AI Magazine, 38(3), 50–57.

att begränsa sin behandling av en eller flera personuppgifter. Det innebär att personuppgifterna i fråga enbart får lagras av den personuppgiftsansvarige, om inte den registrerade ger sitt samtycke till en viss behandling. Om behandling krävs för att göra gällande eller försvara ett rättsligt anspråk, eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för EU eller en medlemsstat får dock behandling ändå ske.

Den registrerade har rätt att kräva begränsning av behandling om

» den registrerade bestrider personuppgifternas korrekthet

» behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och istället begär en begränsning av deras användning

» den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen, men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk

» den registrerade har invänt mot behandling enligt artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

FALL A: Vilka möjligheter har arbetstagare A att inte bli styrd av ett pick-by-voice-system?

Enligt artikel 21 i dataskyddsförordningen har en registrerad rätt att motsätta sig en behandling som sker med grund i ett berättigat intresse, efter en intresseavvägning. Om arbetstagare A skulle framföra att hon inte vill att hennes personuppgifter ska behandlas genom ett pick-by-voice-system krävs det att arbetsgivaren har tvingande berättigade skäl för behandlingen som väger tyngre än A:s intresse av att inte tvingas ha sina personuppgifter cirkulerande i systemet. I en sådan intresseavvägning krävs ännu tyngre skäl för arbetsgivaren än vid en vanlig intresseavvägning. Grahn och Kjällström skriver att det är svårt att veta exakt hur en sådan intresseavvägning ska viktas men att det förefaller endast vara tillåtet med en fortsatt personuppgiftsbehandling om det inte finns något annat rimligt alternativ för att tillgodose intresset ifråga.[58] I förevarande fall, där pick-by-voice-systemet används av företagsekonomiska skäl, är det svårt att se att en fortsatt behandling av arbetstagare A:s personuppgifter skulle vara laglig.

I A:s fall fanns det indikationer på att hennes arbetsgivare använde sig av pick-by-voice-systemet för att övervaka arbetstagarnas förehavanden i realtid. Att bli övervakad i realtid av sin arbetsgivare är generellt sett en väldigt integritetskränkande åtgärd och är i de allra flesta fall förbjudet. Det kan dock finnas undantag, till exempel när det är påkallat av säkerhetsmässiga aspekter. För en arbetstagare som arbetar i gruva kan det upplevas som en betryggande åtgärd om alla kolleger vet om var hen befinner sig i realtid, medan samma åtgärd skulle upplevas som en grov integritetskränkning på ett kontor. Dessa aspekter måste

58 Grahn & Kjällström: Anställdas integritetsskydd, s. 99.

tas in vid en intresseavvägning. Det är inte troligt att arbetsgivaren i A:s fall kan ha rättslig grund för att realtidsövervaka henne efter en intresseavvägning.

I artikel 22 i dataskyddsförordningen finns ett förbud mot automatiskt beslutsfattande. Frågan är om ett pick-by-voice-system, eller användningen av det, skulle kunna klassificeras som ett automatiskt beslutsfattande. Om systemet genererar följder som kan få juridiska, ekonomiska eller sociala konsekvenser för A kan pick-by-voice-systemet omfattas av förbudet. Huruvida förbudet i artikel 22 är tillämpbart på systemet på A:s arbetsplats blir alltså till syvende och sist en fråga om hur det används, för vilket eller vilka ändamål och med vilka faktiska följder. Pick-by-voice-systemet ligger till grund för framtagning, bedömning och utvärdering av de måltal som sedan blir lönegrundande, så det går att argumentera för att systemet borde falla under förbudet i artikel 22.

Om A är medlem i en fackförening kan hon vända sig till den för att få hjälp med att förhandla med arbetsgivaren om AI-systemet som används på arbetsplatsen. Om det finns misstankar om att arbetsgivaren använder AI-systemet på ett olagligt sätt kan det vara en fördel att reglera hur användningen får gå till i ett lokalt kollektivavtal. Systemet skulle då kunna förses med loggar om vem som använder det och hur, som båda parter får ta del av. Akademikerförbundet SSR har gett ut en lathund om fackliga frågor och fackligt inflytande vid implementering och användning av algoritmer på arbetsplatsen. Den tilltänkta mottagaren av skriften är främst tjänstemän i offentlig förvaltning, men det finns många grundläggande aspekter som skriften tar upp som gäller lika för alla på svensk arbetsmarknad.[59] Oaktat vad den rätt till information om det algoritmiska systemet som finns i dataskyddsförordningen innehåller så finns det liknande rättigheter i både MBL och arbetsmiljölagen. Om arbetsgivaren är bunden av utvecklingsavtalet finns det också i detta en långtgående rätt till information. I utvecklingsavtalet finns också en rätt för arbetstagarsidan att hyra in en arbetstagarkonsult som arbetsgivaren måste stå för kostnaden för.

Rätten att bli glömd (eller rätten till radering)

Enligt artikel 17 dataskyddsförordningen ska den registrerade ha rätt att utan onödigt dröjsmål få sina personuppgifter raderade, och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om

- personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller behandlats (enligt artikel 5.1 e föreligger en skyldighet att på eget initiativ radera eller avidentifiera personuppgifterna ifråga)
- den registrerade återkallar sitt samtycke och det inte finns någon annan rättslig grund för behandlingen
- den registrerade invänder mot behandlingen och det saknas berättigade skäl för behandlingen som väger tyngre
- personuppgifterna har behandlats på ett olagligt sätt
- personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse.

59 Akademikerförbundet SSR: *Din kollega har blivit en algoritm: Digitalisering och automatisering ur ett fackligt perspektiv*, 2023.

Om en personuppgift har samlats in och lagras på grund av en rättslig förpliktelse som följer av ett kollektivavtal och kollektivavtalet sägs upp så behandlas inte längre personuppgifterna på ett lagligt sätt, och därmed existerar en rätt till radering enligt artikeln. Denna rättighet skulle kunna användas som en möjlig stridsåtgärd.

Rätt till dataportabilitet

Rätten till dataportabilitet innebär att en registrerad ska ha rätt att få ut de personuppgifter som rör honom eller henne i ett strukturerat, allmänt använt och maskinläsbart format i syfte att använda uppgifterna hos andra personuppgiftsansvariga. Rätten föreligger om behandlingen har sin rättsliga grund i samtycke eller i fullgörande av avtal, eller om behandlingen sker automatiserat. Syftet med artikeln är att skapa standardiserade format inom EU som tillåter interoperabilitet. Rättigheten har inte sin största betydelse inom arbetslivet.[60] Rättigheten skulle kunna få betydelse om det dyker upp digitala verktyg som riktar sig mot enskilda arbetstagare i deras yrkesutövning, där personuppgifter som arbetsgivaren har lagrat skulle kunna spela en viktig roll. Till exempel skulle det i framtiden kunna utvecklas appar för att hjälpa arbetstagare att på olika sätt påverka sin arbetsmiljö eller sin planering av arbetets utförande och som använder sig av personuppgifter som arbetsgivaren har insamlat. Rätten till dataportabilitet skulle då kunna aktualiseras. I dessa fall skulle en konflikt mellan arbetsgivarens arbetsledningsrätt och arbetstagarens rätt till dataportabilitet kunna aktualiseras.

Om ändamålet med behandlingen

När personuppgifter ska behandlas måste ändamålet med behandlingen bestämmas med stor omsorg. De ändamål som bestäms inledningsvis sätter sedan en ram för vad den personuppgiftsansvarige kan göra med uppgifterna under hela deras livscykel. Behandlingen måste vara nödvändig för att tillgodose ändamålet, och syftet måste passa in under någon av de rättsliga grunderna som anges i artikel 6 dataskyddsförordningen. Enligt artikel 5.1 b ska personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Kraven innebär att ändamålen med en personuppgiftsbehandling måste vara bestämd redan då personuppgifterna samlas in. Det krävs inte att detta ska ske skriftligen, men Grahn och Kjällström rekommenderar ändå att göra detta skriftligen i bevissyfte. [61]

Ändamålen måste vara särskilda, detta innebär att den personuppgiftsansvarige måste göra ett visst mått av precisering. Den minsta graden av

60 Grahn & Kjällström: *Anställdas integritet* s. 159.
61 Grahn & Kjällström: *Anställdas integritet* s. 109.

specificering som behövs borde vara en så pass precis formulering av ändamålen att det går att bedöma huruvida behandlingen kan uppfylla de krav som ställs enligt dataskyddsförordningens övriga bestämmelser.[62] Ett ändamål som är vagt eller generellt når inte upp till kriteriet för ändamålspecificering. Artikel 29-gruppen tar i sin vägledning upp exempel på ändamål som de bedömer vara för vaga; bland exemplen listar de ”förbättra användarupplevelsen”, ”marknadsföringsändamål”, ”IT-säkerhet” och ”framtida forskning” som för vaga och utan tillräcklig precision. De menar dock att det måste göras en fall-till-fall-bedömning och att graden av precision kan variera beroende på omständigheterna i övrigt.[63] Specificeringen måste ske innan insamlingen av personuppgiften sker.

Ändamålen måste vara uttryckligt angivna. Med detta menas att de ska uttryckas i någon form, och alltså inte bara existera i huvudet på den personuppgiftsansvarige. Målet med detta krav är att garantera att ändamålen för behandlingen är specificerade utan vaghet eller flertydighet. Ändamålen måste uttryckas innan insamlingen av personuppgifter sker.

Ändamålen måste också vara legitima. Här avses en vidare mening än att behandlingen av personuppgifter ska ha rättslig grund enligt artikel 6 i dataskyddsförordningen. Enligt artikel 29-gruppen måste också ändamålen vara förenliga med alla aspekter av dataskyddsförordningen, men också vara förenlig med andra lagar, såsom arbetsrätt, avtalsrätt och så vidare.[64]

Ändamålsglidning och ändamålsbegränsning

När ändamålet med en behandling av en personuppgift har bestämts får uppgiften inte senare behandlas på ett sätt som är oförenligt med detta ändamål.[65] Detta kallas för finalitetsprincipen. Huruvida ytterligare behandling är förenlig med de ändamål som ursprungligen angavs då personuppgifterna samlades in är föremålet för den prövning av ändamålsglidning som finns i artikel 6.4 dataskyddsförordningen. Hur den ska göras beror på vilken rättslig grund som behandlingen vilar på. Om den ytterligare behandlingen sker med samtycke från den registrerade eller om den nationella rätten eller EU-rätten föreskriver en begränsning av finalitetsprincipen i ett specifikt fall så är ytterligare behandling alltid tillåten.

I andra fall ska en prövning göras av om ändamålsglidningen är tillåten. Detta görs genom en bedömning om huruvida två ändamål är förenliga

62 Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation s. 15.

63 Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation s. 16.

64 Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation s. 20. De skriver: "The requirement of legitimacy means that the purposes must be 'in accordance with the law' in the broadest sense."

65 Artikel 7.1 b dataskyddsförordningen.

med varandra. Den bedömningen görs, enligt artikel 6.4, genom att beakta bland annat

» kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen
» det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige
» personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas, eller om personuppgifter behandlas som rör fällande domar i brottmål
» eventuella konsekvenser för registrerade av den fortsatta behandlingen
» förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 29-gruppen har i ett yttrande från 2013, vilket artikel 6.4 dataskyddsförordningen bygger på, utvecklat en metod för att bedöma huruvida två ändamål är förenliga med varandra. De pekar på tre olika typfall av vidare personuppgiftsbehandling som kan förekomma:

1. fall där ändamålen är så lika varandra att det ter sig som uppenbart att vidare behandling är tillåten,
2. fall där det nya ändamålet är relaterat till det ursprungliga men de inte är helt sammanfallande, där ytterligare analys måste göras för att bedöma om en ytterligare behandling är förenlig med det ursprungliga ändamålet, och
3. fall där ändamålen är uppenbart oförenliga eftersom en genomsnittlig person skulle uppfatta den vidare personuppgiftsbehandlingen som både oväntad och olämplig.[66]

I de typfall som hamnar under punkt 2, där ytterligare analys måste göras av den personuppgiftsansvarige, ska de punkter som listats ovan från artikel 6.4 beaktas.[67]

Vid en eventuell ändamålsglidning som är tillåten enligt artikel 6.4 är det oklart om en ny prövning av rättslig grund enligt artikel 6.1 dataskyddsförordningen måste göras. Grahn & Kjällström menar att det finns skäl som talar för att en ny prövning enligt artikel 6.1 dataskyddsförordningen bör göras och skriver att en personuppgiftsansvarig i dessa fall bör

66 Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation s.23.

67 För mer information om hur bedömningen ska göras se Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation s. 23 f. och Grahn & Kjällström: *Anställdas integritetsskydd – och dataskyddsförordningen* s. 113–116.

göra en ny prövning för säkerhets skull.

Oaktat om en ny prövning om rättslig grund måste göras återaktualiseras den personuppgiftsansvariges skyldigheter att lämna information om databehandlingen till den registrerade.

FALL C: Har det skett en ändamålsglidning?

De uppgifter som arbetsgivaren samlade in i detta Fall C, samlades in i syfte att garantera arbetsgivarens it-säkerhet, inte för att, som i fallet, kontrollera C:s närvaro vid datorn och utvärdera C:s arbetsinsats.

När arbetsgivaren använder sig av de uppgifter som de samlat in för att möjliggöra att arbetstagaren kan arbeta på distans till att utvärdera C:s arbetsinsats aktualiseras alltså frågan om det har skett en ändamålsglidning enligt dataskyddsförordningen. En ändamålsglidning har skett om personuppgifter behandlades för ett syfte inledningsvis och senare ytterligare behandlas av den personuppgiftsansvarige för ett annat syfte. Frågan som måste ställas då är om det ursprungliga syftet är förenligt med den senare behandlingen.

I arbetstagare C:s fall verkar det inte som att ändamålen it-säkerhet och värdering av arbetsinsats är två ändamål som är relaterade till varandra. Vid bedömningen av om ändamålsglidningen var tillåten enligt dataskyddsdirektivet så talar det mesta för att situationen skulle bedömas som uppenbart otillåtna ändamål enligt punkt 3, se föregående sida. Därmed är den ändamålsglidning som skett inte tillåten. Detta stämmer också överens med uttalanden som artikel 29-gruppen har gjort där de anser att det vid kameraövervakning i en reception för säkerhetsändamål inte är förenligt att också kontrollera om receptionisten sköter sitt jobb.[68]

Sanktioner

Av artikel 82.1 dataskyddsförordningen följer att varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen har rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan. I vissa fall kan även personuppgiftsbiträden bli skadeståndsansvariga om skadan uppkommit till följd av att biträdet brutit mot de bestämmelser som reglerar personuppgiftsbiträden i förordningen eller om ett biträde agerat utanför den personuppgiftsansvariges instruktion.[69] Av dataskyddsförordningens skäl 146 följer att begreppet skada bör tolkas brett mot bakgrund av EU-domstolens praxis. Enligt Dataskyddsutredningen ska dataskyddsförordningen tolkas så att ansvaret för skada i princip är strikt.[70] Detta innebär att den personuppgiftsansvarige är ansvarig för att ersätta skador oavsett vem som har orsakat skadan och oavsett uppsåt.

Ersättningen som utgår ska vara full och effektiv. Vad detta exakt innebär framgår inte av förordningen, men det är möjligt att dataskyddsförordningens tillkomst ger anledning för domstolarna att höja den skade-

68 Article 29: Opinion 03/2013 on purpose limitation s. 56.
69 Grahn & Kjällström: *Anställdas integritetsskydd* s. 200.
70 SOU 2017:52 s. 193 f.

ståndsersättning som tidigare gällt enligt Högsta domstolens praxis.[71] Dataskyddsutredningen kom fram till att vägledning för skadeståndsbedömningen bör kunna hämtas ur förarbeten och rättspraxis från dataskyddsdirektivets tid.[72] Exakt hur vägledande detta uttalande är har inte prövats än men det finns skäl som talar för att dataskyddsförordningens krav på ”full och effektiv” ersättning ställer krav på högre ersättning enligt förordningen jämfört med de ersättningar som dömdes ut vid brott mot personuppgiftslagen.

Arbetsdomstolen har ännu inte prövat frågan om tidigare praxis från personuppgiftslagen är tillämpbar eller om dataskyddsförordningen ställer högre krav på ersättningsnivåerna. Administrationssanktionerna som kan utdömas enligt dataskyddsförordningen kan leda till sanktioner på 20 miljoner euro eller 4 procent av den globala årsomsättningen, beroende på vilket belopp som är högst. I jämförelse med dessa sanktioner framstår det inte som orimligt att också skapa större incitament för arbetsgivare att följa förordningens bestämmelser. Eftersom det verkar finnas en konflikt mellan rättskällorna på nationell och EU-rättslig nivå verkar frågan vara lämplig att pröva med hjälp av ett så kallat förhandsavgörande från EU-domstolen.

Nationell lagstifting och kollektivavtal

Vilka möjligheter har arbetsmarknadens parter att påverka hur skyddet för integritet och personuppgifter ska se ut i arbetslivet? Det finns ett visst utrymme för att reglera frågan i kollektivavtal (och enligt nationell lagstiftning) enligt dataskyddsförordningen. Enligt artikel 88.1 dataskyddsförordningen får medlemsstaterna i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden.

Sådana regler får särskilt fastställas när det gäller

» rekrytering,

» genomförande av anställningsavtalet (inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter),

» ledning, planering och organisering av arbetet,

» jämställdhet och mångfald i arbetslivet,

» hälsa och säkerhet på arbetsplatsen,

» skydd av arbetsgivarens eller kundens egendom,

71 Grahn & Kjällström: *Anställdas integritetsskydd* s. 201. Grahn och Kjällström skriver inte ut vilken dom de åsyftar i boken, men det är inte ovanligt att arbetsdomstolen tidigare har hänvisat till NJA 2013 s. 1046 där Högsta domstolen etablerar en schablon för att beräkna kränkningsersättning för brott mot dåvarande PUL.

72 SOU 2017:39 s. 304.

» (individuellt) utövande och åtnjutande av rättigheter och förmåner som är knutna till anställningen och

» avslutande av anställningsförhållandet.

I enlighet med artikel 88.2 bör sådana regler innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till

» insyn i behandlingen,

» överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet och

» övervakningssystem på arbetsplatsen.

Uttrycket i artikel 88, att mer specifika regler får fastställas med kollektivavtal, verkar ge vid handen att det inte får röra sig om en inskränkning av de rättigheter som den registrerade har enligt dataskyddsförordningen, utan snarare om olika typer av fastställelser och förtydliganden av de rättigheter som redan finns i lagen.

I målet C-34/21 utvecklar EU-domstolen sin syn på vilket utrymme som finns för medlemsstaterna att använda sig av artikel 88 i dataskyddsförordningen. Domstolen påpekar att artikel 88 ska läsas tillsammans med skäl 8 i förordningen. Där anges att medlemsstaterna kan införliva GDPR i nationell rätt om det är nödvändigt för att skapa en samstämmig rätt inom unionen och om det behövs för att göra bestämmelserna begripliga för de personer som de är tillämpbara på. Vidare erinrar domstolen om att de principer som reglerar behandlingen av personuppgifter och de rättigheter som tillfaller den registrerade, speciellt de som finns i artikel 5 och 6 i förordningen, inte får inskränkas. Samtidigt skriver domstolen att artikel 88 i dataskyddsförordningen ger medlemsstaterna möjlighet att införa ytterligare strängare eller avvikande nationella regler, så länge förordningens innehåll och syften inte undergrävs. Domstolen menar vidare att uttrycket mer specifika regler också innebär att en ren hänvisning till eller upprepning av dataskyddsförordningen inte heller är förenlig med förordningen.

Domstolen förklarar dessutom i målet C-34/21 att den lista som finns i 88.1 inte är uttömmande, utan exemplifierar vad som är möjligt. Domstolen skriver vidare att för att kunna kvalificeras som en ”mer specifik regel” så måste lagen eller kollektivavtalet syfta till att skydda anställdas rättigheter och friheter i fråga om behandling av deras personuppgifter i anställningsförhållanden samt innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter. Med detta menar domstolen att en

mer specifik regel måste uppfylla kraven i artikel 88.2.

Inför dataskyddsförordningens ikraftträdande den 25 maj 2016 aktualiserades frågan om spelrummet för nationell lagstiftning för skydd av personuppgifter i arbetslivet i Finland. Finland var vid tidpunkten det enda landet i EU som hade en speciallagstiftning för personuppgiftshantering i arbetslivet.[73] Mia Eklund finner i sin artikel från 2017 att den finska lagen om integritetsskydd i arbetslivet inte till fullo överensstämde med de regler som finns i dataskyddsförordningen. Huruvida lagen skulle falla inom det nationella spelrummet som preciseras i artikel 88 dataskyddsförordningen uttalar sig inte Eklund om.[74] I en proposition som föreslog ändringar i den finska lagen om integritetsskydd i arbetslivet uttalar sig den finska lagstiftaren om det nationella utrymmet som finns i artikel 88. De skriver ”det finns inte någon entydig tolkning på i vilken mån artikel 88 i dataskyddsförordningen ger rätt att höja skyddet för den registrerade i förhållande till förordningen och till vilken del bestämmelserna kan vara strängare än förordningens betydelser”. Samtidigt skriver de att artikel 88 ger ”klart mer nationellt handlingsutrymme i fråga om behandlingen av personuppgifter i ett anställningsförhållande än i fråga om andra behandlingssituationer”.[75]

En bärande idé för den svenska modellen är att det går att åstadkomma stabila relationer på arbetsmarknaden och en acceptans för kollektivavtalssystemet hos både arbetsgivare och arbetstagare om båda parter kan vinna något på att komma överens i kollektivavtal. Exakt vilket utrymme som finns för att reglera frågan i kollektivavtal, och i nationella lagar, är inte tydligt i dagsläget, men det finns ett betydande utrymme för parterna att förhandla om, som skulle kunna leda till regler som är bättre anpassade till den arbetsmarknad, bransch och företag där de ska tillämpas. Det skydd som dataskyddsförordningen ger är svåröverblickbart och dåligt anpassat för arbetslivet. Som Grahn och Kjällström påpekar finns det goda argument för att träffa kollektivavtal för båda parterna för att förtydliga vilka rättigheter och skyldigheter parterna har.[76]

73 Se M. C. Eklund: Skyddet för privatliv i anställningsförhållanden och dataskyddsförordningens implikationer, JFT 6/2017 s. 897 – 941. Sådana speciallagar har föreslagits i både Sverige och Tyskland, dock utan att detta burit frukt, se De Hert & Lammerant: Protection of personal data in work-related Relations, Europaparlamentet Directorate General for Internal Policies PE 474.440, 2013, s. 27 f.

74 M. C. Eklund: Skyddet för privatliv i anställningsförhållanden och dataskyddsförordningens implikationer, JFT 6/2017 s. 897–941.

75 RP 97/2018 rd s. 9.

76 Se Grahn & Kjällström: *Anställdas integritetsskydd*, s. 44.

Digitala rättigheter och övervakningskapitalism

Övervakningskapitalism eller nyfeodalism – olika perspektiv på det digitala livet

Mark Fisher beskriver i sin bok *Kapitalistisk realism* från 2009 samtidens uppgivenhet inför kapitalismen som dominerande ekonomiskt system. Det numera mycket bevingade citatet ”Det är enklare att föreställa sig slutet på världen än slutet på kapitalismen” populariserades av Fisher, och summerar hans poäng elegant. Det Fisher inte kunde förutse när han skrev sin bok är den våg av kapitalismens dödförklaringar som svept över världen i det sista, från både höger och vänster. Det som för bara ett årtionde sedan verkade helt otänkbart för Fisher har sedan dess fått fäste och i vissa kretsar tagits som en etablerad sanning. Men det är inte, som många kritiker av kapitalismen har hoppats, en utopisk ny tid som tillåtit dessa dödförklaringar att se dagens ljus. Tvärtom så menar kritikerna att ur kapitalismens aska har en ny sorts feodalism rest sig. Begrepp som informationsfeodalism[77], digital feodalism[78], techno-feodalism[79] och neofeodalism har blivit nya modeord från både vänster och höger i debatten.[80]

I en artikel i *New Left Review* uppmärksammar Evgeny Morozov debatten. Feodalismen, enligt Morozov, var ett system där bönder med tillgång till gemensamt ägd mark och egna verktyg efter eget tycke fick organisera produktionen av de varor och tjänster som behövdes för att samhället skulle reproducera sig självt. Feodalherrarna kunde sedan med vapenmakt tvinga till sig vad de ansåg sig ha rätt till. Deras extrahering av överskottsvärde skedde därför med politisk makt. Under kapitalismen, däremot, sker extraheringen av överskottsvärde primärt genom ekonomiska mekanismer, där kapitalisten äger produktionsmedlen och organiserar hur arbetet ska utföras. Förflyttningen från ett feodalsamhälle till ett kapitalistiskt är enligt logiken sammanhängande med hur överskottet produceras och flyttas upp i hierarkin. Morozov menar att det finns en

77 P. Drahos: Information Feudalism in the Information Society, *The Information Society*, Volume 11 s. 209–222.

78 M. Mazzucato: Preventing Digital Feudalism, Project Syndicate, 2019.

79 K. Geddes: How Digital Platforms Sustain Technofeudalism, *Columbia Journal of Law & the Arts* 455, 2020.

80 T. E. Ström: Capital and Cybernetics, NLR 135 MAY JUNE 2022 s. 23

poäng i att analysera den sentida utvecklingen med begreppsparet kapitalism och feodalsamhälle om det går att identifiera vissa dynamiker eller processer som är liknande de som förekom under feodalismen. Då går det kanske att påvisa en viss återfeodalisering. Liknelsen mellan vasallens förläning med tillhörande allmoge och det digitala landskapets webbanvändare som förslavade till en plattform eller tjänst vars ägare på olika sätt tar ut hyra är inte helt utan poäng, men dess största värde är kanske det rent kommunikativa. Det blir en bra rubrik att likna ägarna i Silicon Valley vid feodalherrarna från förr.

Bland dem som inte tycker sig se en återgång till feodalismen har begrepp som algoritmisk kapitalism[81], kognitiv kapitalism[82], kommunikativ kapitalism[83], datakapitalism[84], plattformskapitalism[85], digital kapitalism[86] och övervakningskapitalism fått spridning. Shoshana Zuboff beskriver i sin bok *Övervakningskapitalismen* hur Google och Facebook i stor skala samlar in personuppgifter. Hon använder begrepp som datautvinning, ackumulationslogik, utvinningsoperationer och övervakningsplattformar. Bilden som målas upp är en slags kapitalistisk huggsexa som närmast påminner om hur utvinning av naturresurser i den globala periferin tidigare har organiserats.[87]

Jathan Sadowski vänder sig mot liknelsen att data skulle vara en typ av råvara eller naturresurs i sin text When data is capital: Datafication, accumulation, and extraction. Där gör han ett försök att reda ut om data är att beteckna som kapital eller som en vara. Sadowski beskriver hur termen datautvinning kan leda tankarna fel eftersom den associerar till en ackumulation av något som redan på förhand existerar. Sadowski pekar på att det snarare rör sig om ett aktivt, övervägt skapande av data. Han skriver: ”Data är en registrerad abstraktion av världen skapad och värderad av människor genom teknologi.”[88] Betraktat genom denna lins menar Sadowski att det finns en logik i en fortsatt datafiering[89] av samhället som liknar det imperativ som driver kapital och kapitalismen in i nya marknader. Dessutom pekar Sadowski på att det finns en rad olika sätt att skapa värde genom data, till exempel genom att profilera kunder och rikta produkter mot dem, genom att optimera olika system, genom att hantera och

81 M. A. Peters: Algorithmic Capitalism in the Epoch of Digital Reason, *Fast Capitalism*, Volume 14, Issue 1, 2017.

82 Y. M. Boutang: *Cognitive Capitalism*, Polity Press, Cambridge UK, 2011.

83 J. Dean: Communicative Capitalism and Revolutionary Form, *Millennium: Journal of International Studies* 2019.

84 S. Myers West: Data Capitalism: Redefining the Logics of Surveillance and Privacy, *Business & Society* 2019, Vol 58(1) 20–41.

85 N. Srnicek: *Platform Capitalism*, Cambridge Polity Press, 2017.

86 C. Fuchs: *Rereading Marx in the Age of Digital Capitalism*, London Pluto Press, 2019.

87 S. Zuboff: *Övervakningskapitalismen – vid maktens nya frontlinjer*, Ordfront Stockholm, 2021.

88 Data is a recorded abstraction of the world created and valorised by people using technology.

89 Med datafiering menas processen att förvandla ett fysiskt fenomen till mätbara data.

kontrollera, genom att modellera sannolikheter, genom att bygga digitala system och tjänster och genom att stimulera tillväxt på olika tillgångar. Variationen i hur data kan tillämpas och skapa värde påminner mer om hur en vara fungerar i ekonomin än hur kapital gör det, enligt Sadowski.[90]

Ibarra et al. pekar istället på att data är en form av arbete som utförs av den som skapar registreringen snarare än en biprodukt som kan extraheras med hjälp av långtgående användaravtal vid konsumtionen av en tjänst eller vara.[91] Tanken om data som en form av arbete öppnar diskursen för oss att tänka på nya sätt att organisera både den digitala samvaron och framtidens arbetsliv. Ibarra et al. ställer begreppsparen data-som-kapital och data-som-arbete mot varandra och pekar mot att förståelsen av data som en form av arbete också utökar användares roll till att mer likna en arbetstagares, och därmed hjälper oss att hämta inspiration från tidigare arbetarrörelsers strategier och taktiker i försöken att skapa bättre villkor för digitala användare.

Utan att ta ställning till diskursen om hur data och den digitala ekonomin ska klassificeras föreställer sig Diane Coyle och Paul Nemitz en ny vision om hur samhället bör förhålla sig till data.[92] De tar utgångspunkt i en analys om att dagens digitala ekosystem är exploaterande, kortsiktigt och skapar maktlöshet. Coyle och Nemitz föreslår en rad olika policyförslag som främst är riktade mot att transformera infrastrukturen mot ett mer öppet och interopererande digitalt ekosystem. Detta vill de åstadkomma genom att återta kontrollen över data från dominanta företag och garantera allmänhetens deltagande som en essentiell komponent i framtagandet av teknologisk policy. Med interoperabilitet avser de en förmåga för en vara eller ett system att fungera ihop med andra varor eller system. I rapporten beskriver författarna på flera ställen sin framtidsvision där digitala användare själva fritt kan forma sina upplevelser, eller överlåta utformningen åt en tredje part som inte nödvändigtvis är under kontroll av de stora plattformarna. Till exempel nämner de hur interoperabilitet skulle kunna bidra till större användaranpassning genom att en produkt syr ihop nyhetsflöden från flera olika källor och själv eller mot bakgrund av användarens instruktioner väljer ut vilka inlägg som ska visas eller ges prioritet. På liknande sätt skulle interoperabilitet mellan chattjänster kunna ge användaren möjlighet att använda en och samma tjänst för att kommunicera med samtliga tillgängliga användare.

Interoperabilitet får därför olika betydelse beroende på vilken typ av tjänst det rör sig om. Gemensamt för samtliga är att begreppet tar sikte på

90 J. Sadowski: When Data is Capital: Datafication, Accumulation, and Extraction, Big Data & Society.

91 I A. Ibarra et al.: Should We Treat Data as Labor? Moving Beyond "Free", *American Economic Association Papers & Proceedings*, Vol. 1, No. 1 2017.

92 D. Coyle & P. Nemitz: *Rethinking Data and Rebalancing Digital Power*, Ada Lovelace Institute, 2022.

att med hjälp av strukturella åtgärder minska dominanta företags möjlighet att med olika inlåsningsmekanismer styra användares val. Coyle och Nemitz är noggranna med att påpeka att interoperabilitet måste åtföljas av ett starkt skydd för användares integritet och privatliv samtidigt som det inte ökar spridningen av personuppgifter mellan olika produkter och system.

Coyle och Nemitz vision om hur framtidens digitala liv borde struktureras är imponerande i sin klarsynthet och berömvärd för optimismen den andas. Samtidigt visar den tydligt på motsättningarna och konflikterna som finns mellan ägare och användare av digitala tjänster.

Diskussionen om klassificeringen av den digitala ekonomin, data och användares rättigheter är intressant men anledningen till att den beskrivs här är inte främst akademisk. Vilka begrepp vi använder kring dessa fenomen styr vår förståelse av vad de är, och därmed hur vi kan och bör agera när vi förhåller oss till dem. De styr vår idé av vad som är möjligt. Förståelsen av företeelserna kommer också spilla över till arbetslivet, och påverka hur aktörerna på arbetsmarknaden kommer att förhålla sig till dem. För att nämna ett exempel skapar förståelsen av data som antingen arbete eller kapital helt olika förslag på politiska lösningar.

Som Ibarra et al. beskriver, blir en logisk följd av data som kapital att de som skapar och avhänds data blir konsumenter, och den politiska lösningen för att transferera ersättning tillbaka till konsumenter för de resurser som de har förlorat blir ofta förslag på basinkomst. Om en i stället tänker på dem om skapar data som arbetstagare skulle en logisk kompensation vara en lön eller bättre villkor för dem som arbetade, och vägen dit skulle kunna vara genom att organisera sig i en fackförening. Samma typ av analogi går att tillämpa på arbetslivet. Om de data som en arbetstagare producerar förstås som en form av kapital blir också data som samlas av arbetsgivaren en slags återbäring på investerat kapital, om data däremot är arbete faller det sig emellertid naturligt för arbetstagare att sälja dem till sin arbetsgivare, och samtidigt tillämpa de lagar och regler som vanligtvis används vid försäljning av arbete.

Algoritmisk arbetsledning[93]

Algoritmisk arbetsledning är en varierad samling av verktyg och tekniker som arbetsleder arbetstagare på distans och är beroende av datainsamling och övervakning av arbetstagare för att kunna fatta automatiserade eller halvautomatiserade beslut.

Algoritmisk arbetsledning är en central del i den så kallade plattform-

93 På engelska används termen algorithmic management. Se till exempel skäl 36 i Kommissionens förslag till AI-förordning: "AI-systems used in employment, workers management, and access to self-employment /…/ should be classified as high-risk." Jag föreslår att vi i Sverige använder termen algoritmisk arbetsledning för samma fenomen.

sekonomin, och har också börjat sprida sig till många andra branscher. Ponce del Castillo & Naranjo definierar algoritmisk arbetsledning som ett helt eller delvis automatiserat kalkyleringssystem som utför en eller fler av följande funktioner:

» leder och fördelar arbetet

» bestämmer rörlig ersättning per arbetsuppgift

» kontrollerar arbetstagare genom att övervaka, styra och utvärdera deras arbete och tiden de behöver för att utföra en specifik uppgift, inbegripet så kallad nudging

» mäter arbetstagares utförande gentemot beräknad tidsåtgång och/eller nödvändig ansträngning för att fullföra uppgift samt tillhandahåller rekommendationer för hur arbetstagaren kan förbättra sin arbetsinsats

» bestraffar arbetstagare till exempel genom uppsägning eller avstängning av konton.[94]

En betydande del av teknikerna har utvecklats på de plattformar som erbjuder olika typer av transporttjänster, som Uber, Lyft och Foodora[95]. Därifrån har teknikerna spridit sig och letat sig in i många andra branscher. För att kunna skapa förutsättningar för algoritmisk arbetsledning krävs att olika delar av verksamheten datafieras. Det innebär att ett moment eller en komponent i arbetets utförande görs om till data och sedan registreras av ett mätinstrument. Beroende på vilken verksamhet det rör sig om finns det alltså väldigt olika förutsättningar för att införa algoritmisk arbetsledning. Samtidigt skapas incitament för arbetsgivare att införa olika digitala hjälpmedel och verktyg för att på så sätt skapa mätpunkter som sedan kan användas i systemen. Detta får konsekvensen att allt fler arbetstagare utrustas med arbetsinstrument som tillåter en mycket sofistikerad övervakning av deras arbete.[96] PV. Moore et al. kallar fenomenet för Electronic performance monitoring (EPM), vilket omfattar bland annat mejlövervakning, telefon- och mikrofonavlyssning, spårning av datoranvändning, videoövervakning och GPS-spårning. Data som insamlas kan sedan omvandlas till produktivitetsindikatorer: mejlanvändning, surfande, användandet av skrivare och telefon – det är till och med möjligt att registrera tonläget och den fysiska aktiviteten under ett telefonsamtal.[97]

Algoritmiska hjälpmedel kan såklart vara till fördel för en arbetstagare,

94 Se bland annat Ponce del Castillo & Naranjo, ETUI Policy Brief 2022.08

95 A. Mateescu & A. Nguyen: *Explainer: Algorithmic Management in the Workplace*, Data & Society 2019.

96 I. Ajunwa: Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law (2019) *SAINT LOUIS UNIVERSITY LAW JOURNAL*, Vol. 63:21.

97 Moore, Phoebe, Upchurch, Martin, Whittaker, Xanthe (2018): *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, Palgrave Macmillan, s. 19ff.

ett arbetslag, en bransch och för samhället i stort. Som med all teknik är den, tagen för sig, närmast neutral. Införd på rätt sätt kan den medföra mängder med positiva förändringar, till exempel kan det förebyggande arbetsmiljöarbetet på arbetsplatsen utföras i realtid och med en kontinuerlig uppföljning. Algoritmisk arbetsledning kan ge arbetstagare och deras chefer tidiga varningar på förhöjda stressnivåer och kan också mäta arbetstagares aktivitetsnivå och nöjdhet. Vidare skulle olika algoritmiska arbetsledningssystem kunna ge arbetstagare större frihet att lägga upp arbetet hur de själva vill, och algoritmen skulle kunna leta efter synergier och stordriftsfördelar i samspelet med andra arbetstagare. Precis som i Coyle och Nemitz vision, om användarmakt och interoperabilitet på framtidens internet skulle en arbetsplats där digitala hjälpmedel var anpassade efter arbetstagares behov kunna utgöra en mycket positiv faktor i framtidens arbetsliv.

Hur digitala hjälpmedel införs på en arbetsplats bestäms i ett samspel mellan de berörda aktörerna, där ägare, chefer, arbetstagare och programmerare i teorin skulle kunna påverka utfallet. Det är dock viktigt att komma ihåg att ny teknologi inte introduceras in på ett blankt ark, utan den tas i bruk i ett utvecklat socialt sammanhang där den färgas av de maktförhållanden som råder där den blir till, och den får också sin användning inom dessa. Spånt Enbuske visar genom en enkät riktad till Kommunals skyddsombud att aspekter rörande arbetsmiljön vanligtvis blir ignorerade vid introducerandet av ny teknologi på arbetsplatser, att skyddsombud saknar insikt om övervakningens påverkan på arbetsmiljön och att det finns ett behov av att ge arbetstagare större möjlighet att begränsa arbetsgivarens övervakning.[98] Därför är det viktigt att ha i åtanke att ny teknologi som introduceras i arbetslivet färgas av den ojämlikhet som redan råder mellan arbetstagare och arbetsgivare, och kan användas för att förstärka arbetsgivarens position i förhållande till arbetstagarna. Så när algoritmer används för att expandera arbetsledningens kontroll över arbetstagare utvidgas också chefsbefogenheterna till nivåer utan tidigare motstycke.[99] I sin bok *Your boss is an algorithm* påpekar De Stefano hur arbetsrätten har skapat och utvecklat normer för värdighet i arbetslivet. Arbetsgivarens rätt att leda och fördela arbetet har med arbetsrätten kringskurits för att motverka de värsta former av missbruk som kan uppstå när en människa får makt över en annan, på det vis som sker i arbetslivet. Han skriver att algoritmisk arbetsledning riskerar att urholka denna modell, eftersom den tillåter chefer att kringgå de legala regler som begränsar deras chefs-

98 A. Spånt Enbuske: Digitalisation, work environment and personal integrity at work, *Transfer,* 2019, Vol. 25(2) s. 235–242.

99 V. De Stefano: Master and Servers: Collective Labour Rights and Private Government in the Contemporary World of Work (August 16, 2020). International Journal of Comparative Labour Law and Industrial Relations, 36(4), 2020.

befogenheter.[100]

De utmaningar som algoritmisk arbetsledning ger upphov till är inte nya, men de har förstärkts genom de nya befogenheter som arbetsgivare har fått genom att inkorporera AI i sin verksamhet. Utmaningarna som oftast tas upp är problem kopplade till övervakning, transparens, felaktiga och diskriminerande beslut och ansvarsutkrävande.[101]

I en policy-brief beställd på uppdrag av Europeiska arbetsmiljöverket identifierar Christenko et al. en rad olika riskområden vid algoritmisk arbetsledning.[102] Deras litteraturgenomgång visar bland annat att algoritmisk arbetsledning intensifierar arbetet samtidigt som arbetstagare upplever förlorad kontroll och autonomi. De menar att det finns stöd för att algoritmisk arbetsledning bidrar till att arbetstagare blir avhumaniserade och sedda som kuggar, så att det inte finns någon plats för dem som individer. Christenko et al. pekar på att den intensifiering av arbetet som skapas genom prestationsutvärdering och rankningssystem i realtid leder till att arbetstagare tar mer risker för att hålla uppe tempot, och ibland också åsidosätter viktiga säkerhetsmekanismer. Det finns dessutom stöd i litteraturen för att algoritmisk arbetsledning leder till mer repetitiva arbetsmoment och arbetsuppgifter som är sämre ur ett ergonomiskt perspektiv. Vidare, menar de, leder algoritmisk arbetsledning till att arbetstagare får nya arbetsuppgifter och att dessa nedkvalificeras, det vill säga att de blir mindre komplexa, vilket urholkar yrkeskunskapen och yrkesidentiteten för de som utför arbetet.

Enligt en omfattande metastudie av Kellogg, Valentine och Christin har algoritmer inte bara lett till ökad effektivitet utan dessutom försett arbetsgivare med nya metoder för att övervaka och kontrollera arbetstagare. Forskarna presenterar sex typer av vad de kallar för algoritmisk kontroll i arbetslivet: begränsning och uppmuntring, spårning och utvärdering samt utbytande och belöning.[103] De utgår från en förståelse av arbetsledningsprocesser som en omstridd terräng, där arbetsgivare introducerar ny teknologi för att öka värdet som arbetstagare skapar medan arbetstagare motarbetar och försvarar sin autonomi så gott de kan. De presenterar en matris för hur olika aspekter av algoritmisk kontroll upplevs ur ett arbetstagarperspektiv.

---

100 V. De Stefano: Your Boss is an Algorithm – Artificial Intelligence, Platform Work and Labour 2022, s. 121.

101 A. Mateescu & A Nguyen: Explainer: Algorithmic Management in the Workplace, Data & Society 2019.

102 A. Christenko et al.: Artificial Intelligence for Worker Management: Risks and Opportunities, European Agency for Safety and Health at Work 2022.

103 K. Kellogg, M. Valentine & A. Christin: Algorithms at Work: The New Contested Terrain of Control, *Academy of Management Annals*, Vol. 14, No. 1 (2020). På engelska presenteras "the 6 Rs, restricting and recommending, recording and rating, replacing and rewarding".

	Direction	Evaluation	Dicipline
Control mechanisms	Recommending restricting	Recording rating	Replacing rewarding
Worker experiences	Manipulation disempowerment	Surveillance discrimination	Precarity stress

Den effektivitet som algoritmisk arbetsledning lovar, och i vissa fall levererar, riskerar att komma på bekostnad av andra värden, som är viktiga för både arbetsgivare och arbetstagare och samhället.

Sammanfattning integritet, data och algoritmisk arbetsledning

Genom att digitalisera arbetslivet skapas inte bara hjälpmedel för arbetstagare, det skapas dessutom enorma mängder data som i många fall är personuppgifter, alltså eftersom de går att knyta till en fysisk person. Vår förståelse av dessa personuppgifter styr vilka krav vi anser vara rimliga att ställa på hur de ska kunna användas. Om personuppgifterna som genereras i arbetet beskrivs och analyseras som en vara faller det sig också naturligt att dessa tillfaller arbetsgivaren och kan förfogas av denne. För den som istället tänker att personuppgifterna är en slags form av arbete ter det sig istället naturligt att arbetstagarna som genererat personuppgifterna ska kunna förfoga över dem. I många branscher har det länge genererats stora mängder data. Genom att algoritmiska arbetsledningstekniker har förfinats har det emellertid blivit enklare att sortera, värdera och basera beslut på denna data. Dessa algoritmer kan i många fall utgöra fantastiska hjälpmedel för arbetstagare. Tyvärr visar många studier att verktygen istället ofta för med sig mer övervakning, minskad kontroll, ökat tempo och en generell avhumanisering av arbetstagare. I arbetsgivarens händer kan också verktygen tillåta en stor maktförskjutning i hens favör.

Bilaga I

I en informationsskrift från 2015 ger Datainspektionen vägledning om vilka intressen som kan vara berättigade i arbetslivet, och vilka som normalt sett inte är det. Generellt sett, menar myndigheten, är det så att intressen som har sin grund i säkerhetsskäl väger tyngre än intressen som beror på företagsekonomiska effektivitetsskäl. Det är viktigt att komma ihåg att listorna inte är uttömmande och att en bedömning måste göras i varje enskilt fall, oavsett vad en sådan lista säger. I listan framgår inte heller vilka typer av personuppgifter Datainspektionen anser kunna behandlas i varje situation, så det finns anledning att inte lägga stor vikt vid listan.

Datainspektionen menade att en intresseavvägning normalt sett kan ge stöd för att i arbetslivet behandla personuppgifter för att:

» planera, organisera, leda och följa upp arbetet

» mäta individuella prestationer

» kontrollera och övervaka anställda om det krävs av säkerhetsskäl

» kontrollera och övervaka anställdas användning av internet och e-postsystem genom loggning av tekniska eller säkerhetsmässiga skäl

» avsiktligt ta del av arbetstagares privata e-post eller annan privat elektronisk kommunikation vid misstanke om illojalt eller brottsligt beteende

» registrera uppgifter i rekryteringssystem och kompetensdatabaser

» lämna ut harmlösa uppgifter, till exempel namn och adress, till bolag inom samma koncern

» på en arbetsgivares webbplats publicera namn, befattning, avdelning, anställningsår, arbetstelefonnummer, e-postadress och liknande arbetsrelaterade personuppgifter

» i personalregister lagra fotografier av anställda som tagits av säkerhetsskäl.

Normalt kan en intresseavvägning inte ge stöd för att:

» ta sammanställningar av uppgifter som lagras för ett syfte, till exempel fakturering eller bemanningsplanering, och sedan använda dem i ett annat, till exempel individuell bedömning vid

lönesättning (så kallad ändamålsglidning är bara tillåten under vissa förutsättningar, se mer nedan under XX)

» registrera uppgifter om resultat från personlighetstester, personlighetsprofiler och liknande

» använda logguppgifter för andra ändamål eller syften än de ursprungligen bestämda

» läsa arbetstagares privata e-post eller annan privat elektronisk kommunikation

» upprätta spärrlistor eller liknande över tidigare anställda för att förhindra återanställning[104]

» sambearbeta register som förs med olika ändamål.

104 Jämför här Europadomstolen som i ett avgörande prövat om en svartlistning av en högerextrem lärare stred mot lärarens yttrandefrihet, vilket domstolen kom fram till att svartlistningen inte gjorde. Här prövade dock inte Europadomstolen om svartlistningen stred mot lärarens rätt till privatliv, vilken är grunden för GDPR. Se Selberg i *EU & Arbetsrätt* 4 2022 och Godenau mot Tyskland 80450/17, Europadomstolens dom den 29 november 2022.

Rapporten kan laddas ner från
www.arenaide.se/rapporter