Rådet for
Digital Sikkerhed

OVERVÅGNING PÅ ARBEJDSPLADSEN

Arbejdsgiverens ledelsesret og beskyttelse af medarbejdernes ret til privatliv

Overblik og perspektiv

Juni 2024

1. Introduktion

Arbejdsgiverens ret til overvågning og medarbejderens ret til privatliv

Arbejdsgivere har interesse i og ret til at holde øje med, at deres medarbejdere udfører deres arbejde. Ledelsesretten betyder, at det er arbejdsgiveren, som leder og fordeler arbejdet – herunder gennemfører ansættelser, udstede direktiver for arbejdets udførelse, fastlægger arbejdstiden, indfører kontrolforanstaltninger og gennemfører afskedigelser. Databeskyttelsesretligt betyder dette, at arbejdsgiveren bliver dataansvarlig for behandling af personoplysninger relateret til ansættelsesforholdet.

Ledelsesretten kan dog indskrænkes og/eller præciseres gennem de kollektive overenskomster. Hertil kommer, at medarbejderne har ret til respekt for deres privatliv og beskyttelse af deres personoplysninger – også når de benytter arbejdsgivers udstyr. Denne ret til privatliv og databeskyttelse fremgår bl.a. af Den europæiske unions charter om grundlæggende rettigheder[1] og Den Europæiske Menneskerettighedskonvention[2].

I takt med digitaliseringen er arbejdsgiverens muligheder for digital overvågning af sine medarbejdere blevet stadigt flere i relation til fx tids- og resultatstyring samt overvågning af deres fysiske færden, deres internetbrug og e-mailkorrespondance. Hertil kommer, at forskellige applikationer installeret på medarbejdernes arbejdscomputer og mobiltelefon opsamler data om den ansattes brug heraf, dennes kontakter og profildata, og det er vanskeligt for både arbejdsgiver og arbejdstager at danne sig et overblik over den omfattende dataindsamling. På samme tid gør den øgede anvendelse af hjemmearbejdspladser det sværere at drage en klar grænse mellem arbejds- og privatliv.

I dette papir gennemgås først noget af den viden, vi har om indsamlingen af medarbejderdata på danske arbejdspladser. Herefter beskrives dem overordnede retlige ramme, der sættes af arbejds- og databeskyttelsesretten for indsamlingen af medarbejderdata. Endelig drøftes grænserne for arbejdsgivers ledelsesret og medarbejdernes privatliv, og det dilemma arbejdsgiveren står overfor i forbindelse med til- og fravalg af de mange nye muligheder for overvågning. Disse nye muligheder kalder på fastlæggelse af en af praksis for brug af nye teknologier. Det samme gør de situationer, hvor personoplysninger videregives uden arbejdsgivers vidende.

2. Hvad ved vi om indsamling af medarbejderdata på danske arbejdspladser?

ADD-projektets undersøgelser om overvågning på arbejdspladsen

Det er først i de allerseneste år, at vi i Danmark har gennemført undersøgelser om dataindsamling og digital overvågning på arbejdspladsen. I december 2022 offentliggjorde ADD-projektet[3] den første danske kortlægning af medarbejdernes holdninger og erfaringer på feltet.[4] Undersøgelsen blev i september 2023 fulgt op med en undersøgelse af lederes holdninger til og oplevelser med indsamling af medarbejderdata.[5]

[1] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:da:PDF, artikel 7 og 8
[2] https://www.retsinformation.dk/eli/lta/1996/423 , artikel 8
[3] Projektet Algoritmer, Data og Demokrati – ADD-projektet – er et flerårigt forsknings- og analyseprojekt støttet af Villumfonden og Veluxfonden. Læs mere om ADD-projektet
[4] ADD-projektet 2022/12
[5] ADD-projektet 2023/9

Medarbejdersynsvinklen

ADD-projektets undersøgelse (2022/12)[6] er den første repræsentative undersøgelse af danske arbejdstageres holdninger og erfaringer med dataindsamling og overvågning på arbejdspladsen. Undersøgelsen viser følgende:

- 63 % af medarbejderne oplever, at der indsamles digitale data om dem på arbejdspladsen.
- Medarbejdere opfatter, at de digitale værktøjer, der anvendes på danske arbejdspladser, indsamler navnlig data om medarbejdernes tidsforbrug, møde- og gåtider, mødeaktiviteter samt data i forbindelse med trivsels- og tilfredshedsundersøgelser. I mindre omfang vurderes det, at der indsamles data om medarbejdernes kommunikation (fx screening af e-mails og telefonopkald), performancemålinger (fx kundetilfredshed og økonomiske resultater), digitale brug (fx hjemmesider og apps) og lokation.
- Medarbejdere, der føler sig digitalt overvåget på arbejdspladsen, giver i stor udstrækning udtryk for, at det hænger sammen med det generelle tillidsniveau mellem ledelse og medarbejdere.
- Godt 70 % af arbejdstagerne udtrykker i høj eller nogen grad opbakning til, at der indsamles data for at imødegå potentiel kriminelle handlinger og i tilknytning til trivsels- og kompetencemålinger.
- I noget mindre omfang (godt 60%) er der opbakning til at indsamle data om stress, performance og tidsforbrug.
- Den laveste opbakning (hvor 60-70 % udtrykker lav eller ingen opbakning) knytter sig til dataindsamling vedrørende fysisk sundhed og medarbejdernes privatliv på sociale medier.
- 24 % af medarbejderne oplever, at de har godt kendskab til de regler, der regulerer arbejdspladsens indhentning af medarbejderdata. Godt 20 % angiver, at de tilnærmelsesvis ikke har kendskab til reglerne.
- 25 % af medarbejderne oplever, at deres leder har talt med dem om, hvorfor der indsamles data om dem.
- 54 % af danske medarbejdere er bekymret for, at indsamling af medarbejderdata skader forholdet mellem leder og medarbejder.

Ledersynsvinklen

Den anden undersøgelse fra ADD-projektet (2023/9) omfatter et repræsentativt udsnit af ledere på danske virksomheder.[7] På visse punkter sammenholdes lederundersøgelsen med ovennævnte medarbejderundersøgelse. Undersøgelsen viser følgende:

- Knap 80 % af danske ledere angiver, at der indsamles data om medarbejderne på arbejdspladsen. Der er altså forskel i vidensniveauet mellem medarbejdere og ledelse om arbejdspladsens dataindsamling.[8]

[6] ADD-projektet 2022/12. Undersøgelsen omfatter 1120 respondenter og er repræsentativ for danskere i arbejde på parametrene alder, køn og geografi.
[7] ADD-projektet 2023/9. Undersøgelsen omfatter 600 respondenter fra offentlige og private arbejdspladser og er repræsentativ på parametrene virksomhedsstørrelse (antal ansatte), ledelsesniveau og -ansvar, alder og medarbejdergruppe
[8] ADD-projektet 2023/9 angiver, at forskellen i forhold til de 63 % blandt medarbejdere med viden skyldes, at 15 % af medarbejderne i ADD-projektet 2022/12 har besvaret 'ved ikke' til spørgsmålet.

- 96 % af danske virksomheder med mere end 100 ansatte anvender medarbejderdata i deres ledelsespraksis. Det samme gælder 76 % af virksomheder med færre end 25 ansatte. Virksomhedens størrelse har således betydning for om indsamling og anvendelse af medarbejderdata finder sted.
- Indsamlingen finder sted bredt i alle brancher uden store udsving på brancheniveau.[9]
- Dataindsamling i forbindelse med trivsels- og tilfredsundersøgelser, møde- og gåtider og tidsforbrug topper listen af formål. Her er der således stor samklang mellem ledelsens og medarbejdernes opfattelse af de væsentligste formål. Det hører dog med, at dataindsamling på disse områder set fra en ledelsesoptik er markant mere udbredt end medarbejdernes opfattelse.
- Ledere angiver i højere grad end medarbejdere, at der indsamles data til flere formål. Dataindsamling i tilknytning til performance, lokation og fysisk sundhed er således mere fremtrædende i ledelsens formålskatalog set i forhold til medarbejdernes opfattelse af virksomhedens dataindsamling.
- Ledelsesniveauet er generelt mere positivt stemt for indsamling og anvendelse af medarbejderdata (46 % blandt ledere og 26 % blandt medarbejdere er helt eller delvist enig i tilkendegivelsen). Der er dog også udtalt skepsis blandt ledere med 38 %, der angiver sig helt eller delvist uenige i at være positivt stemt.
- 54 % af lederne er opmærksomme på, at indsamling af medarbejderdata kan skade forholdet mellem ledelse og medarbejdere – her er risikovurderingen på niveau med medarbejdernes. Omvendt er 37 % af lederne helt eller delvist uenige, at forholdet kan lide skade – her er blot 18 % af medarbejdere tilnærmelsesvis sikre på, at indsamling af medarbejderdata ikke er forbundet med risici.
- Oplevelsen af mistillid og oplevelsen af overvågning angives som de vigtigste risikotemaer i forholdet mellem ledelse og medarbejdere.[10] Risikoen i forhold til de personlige relationer mellem ledelse og medarbejdere og oplevelsen af, at privatlivet krænkes, angives også. Blot 5 % angiver muligheden for, at digitale værktøjer anvendes forkert eller giver et forkert billede, som risikofaktor.
- 98 % af lederne angiver, at deres arbejdsplads ikke har anvendt data til andre formål, end det de oprindeligt var indsamlet til. 90 % føler sig sikre på, at arbejdspladsen overholder gældende lovgivning.
- Der er stor forskel blandt ledere og medarbejdere i oplevelsen af, om der er dialog på arbejdspladsen om dataindsamlingen. 68 % af lederne mener at dialogen finder sted, mens 25 % af medarbejderne har samme oplevelse.
- Knap 60 % af lederne føler sig ikke fuldt klædt på til dialog med medarbejderne om arbejdspladsens dataindsamling med medarbejderne. Undersøgelsen peger på manglende viden om digitale værktøjers anvendelse og lovgivning på området samt i et vist omfang mangel på digitale kompetencer.
- Knap 30 % af virksomhederne har etableret politik og retningslinjer for indsamling og anvendelse af medarbejderdata (udover de krav, som fremgår af lovgivningen).

[9] ADD-projektet 2023/9 angiver, at medarbejderdata anvendes i lige stort omfang på tværs af de brancher, som undersøgelsen omfatter (stort set). Resultaterne er dog ikke statistisk signifikante.
[10] Blandt de 54 % af lederne, der angiver dataindsamling som forbundet med risici.

3. Hvad siger loven om overvågning på arbejdspladsen?

3.1 Datatilsynets vejledning om databeskyttelse i ansættelsesforhold

I marts 2023 udgav Datatilsynet en opdateret vejledning om databeskyttelse i ansættelsesforhold.[11] Vejledningen fokuserer på de mest almindeligt forekommende databeskyttelsesretlige problemstillinger ved behandling af personoplysninger i ansættelsesforhold.

I vejledningen gennemgås de databeskyttelsesretlige regler og praksis, herunder samspillet mellem databeskyttelsesforordningen og databeskyttelsesloven (særligt §§ 8, 11 og 12) for behandling af personoplysninger før, under og efter ansættelsen f.eks. indhentelse af straffe- og børneattester, personlighedstests, MUS-samtaler, APV og videregivelse af oplysninger, samt brugen af overvågning på arbejdspladsen.

3.2 Aftale om kontrolforanstaltninger mellem LO og DA

I 2001 indgik LO (nu FH, Fagbevægelsens Hovedorganisation) og DA en aftale om kontrolforanstaltninger[12]. Ifølge denne aftale må arbejdsgiveren iværksætte kontrolforanstaltninger, hvis de er begrundet i driftsmæssige årsager, har fornuftige formål, er proportionale, ikke-krænkende eller til nævneværdig ulempe eller forvolde tab for medarbejderne, og de skal annonceres med seks ugers varsel m.v. Der kan fastsættes uddybende regler i kollektiv overenskomst.

Al overvågning på arbejdspladsen skal vurderes efter disse kriterier. Hvis en kontrolforanstaltning er lovlig efter denne aftale, vil den typisk også være det efter databeskyttelsesretten og menneskeretten. Herefter stilles der overordnet krav om, at behandlingen skal være saglig og proportional, at der er et lovligt behandlingsgrundlag, og at de registrerede skal være oplyst.[13] I vurderingen heraf, lægges der efter praksis vægt på følgende elementer:

3.3 Eksempler på typiske overvågningstiltag på arbejdspladsen

Overvågning: Komme-gå-tider

Arbejdsgiver kan overvåge, hvornår medarbejderne møder på og forlader arbejdspladsen. Formålet vil være dokumentation af, at den aftalte arbejdstid overholdes. Registreringen kan ske ved, at alarmer slås fra, at der anvendes nøglekort m.v. Der vil som hovedregel ikke kunne benyttes biometri til registreringen (se Datatilsynet journalnummer 2018-211-0135[14]). Fra 1. juli 2024 skal arbejdsgiver tilmed foretage denne overvågning med henblik på at kunne dokumentere, at medarbejderne overholder arbejdstidsloven (jf. dom fra EU Domstolen, C-55/18 fra 2019[15]).

---

[11] Datatilsynet 2023/3
[12] https://fho.dk/wp-content/uploads/lo/2017/03/aftaleomkontrolforanstaltninger.pdf
[13] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/aug/tilsyn-med-arbejdsmarkedets-tillaegspension-atp - sag fra praksis hvor Datatilsynet tager stilling til, hvor grundig oplysningen skal være.
[14] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/maj/vejledende-udtalelse-om-anvendelsen-af-fingeraftryk-til-brug-for-registrering-af-ansattes-komme-gaa-tider
[15] https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A62018CJ0055

Overvågning: Medarbejdernes trivsel m.v.

Nogle medarbejdere vil betragte arbejdsgivers undersøgelser af deres trivsel m.v. som overvågning, og ADD-projektet har således betragtet trivselsundersøgelser og arbejdspladsvurderinger som overvågning.

De fleste arbejdsgivere er ifølge arbejdsmiljølovgivningen imidlertid pålagt at gennemføre arbejdspladsvurderinger. Hertil kommer, at medarbejdersudviklingssamtaler og medarbejdertrivselsundersøgelser kan, hvis de følger af kollektiv overenskomst, gennemføres efter databeskyttelseslovens § 12, stk. 1, og hvis de ikke følger af kollektiv overenskomst, efter databeskyttelseslovens § 12, stk. 2.

Overvågning: Optagelse af telefonsamtaler

For at sikre dokumentation til uddannelsesformål eller kvalitetssikring kan arbejdsgiver optage medarbejdernes samtaler, såfremt optagelse er egnet og nødvendig herfor. Offentlige arbejdsgivere kan således foretage optagelse efter databeskyttelsesforordningens artikel 6. stk. 1, litra e, og private arbejdsgivere kan foretage optagelser efter artikel 6, stk. 1, litra f. Der skal naturligvis også være hjemmel til at optage den anden part i samtalen og Datatilsynet har udgivet en vejledning herom.[16]

Overvågning: Brug af internet og e-mail

Praksis på dette område har været fastlagt siden årtusindskiftet bl.a. jf. Datatilsynets journalnummer 2000-632-0001 (opsummeret Årsberetningen fra 2000, pp. 31-33). Hvis det er sagligt, dvs. ledelses-, drifts-, eller sikkerhedsmæssigt begrundet, og hvis der er lavet en politik for overvågning, som er kommunikeret til medarbejderne, kan arbejdsgiver gennemføre kontrol af medarbejdernes brug af mail og internet.

Hvis arbejdsgiver bliver bekendt med, at mails har et privat indhold, skal arbejdsgiver dog ophøre med at læse indholdet, hvilket bl.a. er fastslået af Højesteret i U 2015.1525 H, som i øvrigt i overensstemmelse med Menneskerettighedsdomstolens afgørelser.[17]

Databeskyttelsesforordningen stiller samtidig betydelige krav til de dataansvarlige for at sikre, at der ikke sker brud på f.eks. compliance (artikel 24), design (artikel 25) og sikkerhed (artikel 32). Tilsvarende stilles også skarpe krav til, at den dataansvarlige kan dokumentere sine foranstaltninger (artikel 5, stk. 2). Generelt må der siges at være vide rammer til at etablere en passende sikkerhed, hvilket også understreges af præambelbetragtning 49, hvorefter "Behandling af personoplysninger i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerhed… udgør en legitim interesse for

[16] https://www.datatilsynet.dk/Media/638477264404280979/Optagelse%20af%20telefonsamtaler.pdf
[17] Den kommenterede udgave af Databeskyttelsesforordningen, pp. 397-199. Afgørelsen skal i øvrigt ses i lyset af, at det efter Straffelovens §263, stk. 2, nr. 1 er strafbart uberettiget at åbne et brev.

den berørte dataansvarlige". Uanset artikel 11, som præciserer, at den dataansvarlige ikke skal opbevare identificerende personoplysninger til andre formål, pålægger databeskyttelsesforordningen den dataansvarlige en pligt til at opfylder sikkerhedsmæssige formål efter f.eks. artikel 32, som den dataansvarlige finder hjemmel til i artikel 6, stk. 1, litra e eller f. Planlagte risikobaserede foranstaltninger, som skal reducere borgeres eller kunders risici ved behandlingen, vil ofte veje tungt – også selvom disse foranstaltninger implicerer en grad af overvågning af de ansatte. Når arbejdsgiveren indfører disse, er det imidlertid centralt, at der er fastlagt et tilstrækkeligt præcist formål, eller at der foretages en vurdering – bl.a. efter artikel 6, stk. 4 – om hvorvidt et andet formål er foreneligt.

Overvågning: Bevægelseskontrol

Arbejdsgiver kan have en interesse i at registrere medarbejdernes bevægelser – særligt, hvor der er tale om ansættelse af chauffører. I en sag om et taxaselskab (journalnummer 2012-211-0038[18]) finder Datatilsynet, at overvågning med GPS af alle taxaer er proportionalt og sagligt kan anvendes med det formål bl.a. at behandle sager om klager og overfald. Det er imidlertid centralt, at chaufførerne er oplyst om overvågningen. Det er samtidig centralt, at overvågningen kan slås fra, når chaufføren ikke er på arbejde. Det Slovenske datatilsyn fandt i en sag fra oktober 2022, at chaufføren selv skal kunne bestemme, hvornår der er risiko for en værdifuld transport og slå GPS til.[19]

Overvågning: Blod- og urinprøver

Arbejdsgiver kan vedtage interne regler for brug af narkotika og alkohol. Herefter vil det kunne være lovligt, at påbyde medarbejdere generelt at underkaste sig tests. Arbejdsretten har i en sag af 23. februar 2000 mellem Dansk Sø-Restaurations Forening og restaurationsbranchens Forbund på den ene side og DFDS A/S på den anden side afgjort, at uvarslet testning for alkohol og narkotika af sikkerhedsmæssige årsager var retmæssig. Testen foregik af sundhedsuddannet personale fra et firma uafhængig af arbejdsgiveren og i lukket enrum. Tilsvarende fik Maersk i 2003 tilladelse til at behandle oplysninger om alkohol og narkotikatests for ansatte, der skulle arbejde på boreplatform.[20] Det er centralt, at de hensyn, der er aftalt mellem arbejdsgiver og arbejdstager i LO/DA-aftalen, iagttages. I en sag bad en murermester en elev efter konkret mistanke og efter indgåelse af bilateral aftale herom at lade sig teste for misbrug af narkotika. Testen blev imidlertid gennemført ved, at eleven blev bedt om at tisse i en spand, som ikke var rengjort og steril, hvorefter mester anvendte en testmetode, der ikke er fri for fejlkilder. Arbejdsretten afgjorde, at mester ved denne fremgangsmåde misbrugte ledelsesretten (AR2010.0051[21]).

Overvågning: TV-overvågning

Arbejdsgiver kan implementere TV-overvågning, hvor det er begrundet i forebyggende eller opklarende kriminalitetsbekæmpelse. Reglerne i TV-overvågningsloven og databeskyttelsesretten skal overholdes. Det er dog afgørende, at medarbejderne er informeret grundigt herom.

I en konkret sag overvågede en arbejdsgiver en ansat i en Matas-butik i hovedstaden fra sin private adresse i Hobro. Overvågningen skete i 30-45 minutter. Arbejdsgiver kunne konstatere, at medarbejderen sminkede sig i butikken i modstrid med de interne retningslinjer. Arbejdsgiver kontaktede medarbejderen, skældte

[18] https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2015/jul/taxaselskabs-registrering-af-oplysninger-om-vognmaends-faerden-via-gps
[19] https://www.edpb.europa.eu/news/national-news/2022/safety-property-can-be-legitimate-interest-gps-tracking-measure-must-be_en
[20] Blume og Kristiansen: Persondataret i ansættelsesforhold, pp. 148-152, Udgivet 2011.
[21] https://www.elov.dk/afgoerelser/arbejdsretten/dom/10-02-2011/sag-ar20100051/

vedkommende ud, og dagen efter blev medarbejderen afskediget. Overvågningen skete til andre formål end kriminalitetsbekæmpelse og var derfor hverken i overensstemmelse med aftalen mellem LO og DA eller databeskyttelsesretten (F-60-06[22]).

I en anden konkret sag havde Fitness World A/S foretaget overvågning i sine centre herunder af medarbejderne for at forebygge og opklare kriminalitet, af sikkerheds- og forsikringsmæssige årsager samt for at kunne gøre retskrav gældende i forbindelse med ansættelsesforhold.[23] Der blev skiltet og medarbejderne var oplyst, og Datatilsynet fandt dermed overvågningen lovlig.

I en sidste sag har Datatilsynet politianmeldt Danske Shoppingcentre P/S for ikke at have begrænset overvågning i et toiletområde i tilstrækkeligt omfang, hvilket medførte utilstrækkelig dataminimering, og overvågning af en meget privat situation.[24]

3.4 Fremtiden – ingen eller uklar praksis

Overvågning: Mobiltelefoner og MDM

I henhold til eksemplerne ovenfor kan arbejdsgiver gennemføre kontrol af medarbejdernes brug af internet og e-mail, hvis det er sagligt, der foreligger en politik herom, medarbejderne er oplyst, og arbejdsgiver undlader at gøre sig bekendt med oplysninger af privat karakter. En række andre opsamlinger af logs, EDR m.v. kan også anvendes til at overvåge medarbejdernes aktivitet på udstyret. Praksis har i høj grad haft fokus på brug af internet og e-mail fra virksomhedens udstyr (i form af desktops og laptops) og med forventning om ingen eller begrænset privat anvendelse.

Hvis arbejdsgiver stiller en arbejdsmobiltelefon (dvs. en mobiltelefon som ikke er til rådighed for privat brug og ikke beskattes) til rådighed, vil praksis formodentlig kunne anvendes direkte på en sådan mobiltelefon, da reglerne kun tillader meget begrænset privat brug. Arbejdsmobiltelefonen vil ofte have adgang til en række tjenester (f.eks. borgeres oplysninger, ruter og vagtplaner) og tilsvarende sikkerhedsforanstaltninger som på desktops og laptops, må derfor kunne forventes. Datatilsynet har f.eks. i et tilsyn hos Mariagerfjord Kommune (Journalnummer: 2022-423-026) afgjort, at Tilsynet fandt, at det var en passende foranstaltning, ”at medarbejderne ikke har rettigheder til at installere programmer på egne mobile enheder og computere, der har adgang til det netværk hvor produktionsdata tilgås”.[25] Dette må implicere, at Datatilsynet finder, at de ansatte ikke må installere apps på en arbejdsmobiltelefon.

Hvis arbejdsgiver omvendt har udleveret en arbejdsgiverbetalt telefon (som benyttes både privat til løsning af arbejdsopgaver og som beskattes) vil medarbejderen formodentlig forvente en betydelig grad af privatliv i forbindelse med sin brug af telefonen, og at arbejdsgiveren ikke gør sig bekendt med, hvilke hjemmesider der besøges og hvilke apps, der installeres. Omvendt vil der formodentlig fra mobiltelefonen være adgang til f.eks. mails og andre personoplysninger. Dette betyder, at arbejdsgiver som dataansvarlig skal installere en række sikkerhedsforanstaltninger efter artikel 32. Det er i så fald afgørende, at arbejdsgiver konkret oplyser medarbejderne om, hvordan mobiltelefonen overvåges, og hvad der installeres af sikkerhedsforanstaltninger.

[22] https://www.elov.dk/afgoerelser/so-og-handelsretten/dom/06-12-2007/sag-f-0060-06/?sog=overv%C3%A5gning

[23]

[24] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/danske-shoppingcentre-indstilles-til-boede

[25] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/alvorlig-kritik-af-mariagerfjord-kommune

Typisk må det forventes, at arbejdsgiver installerer en MDM-løsning, som opdeler telefonen i to dele: en virksomhedsdel med f.eks. begrænsning af ret til at installere apps, adgang til mail, logning og andre sikkerhedsbetingede overvågningstiltag samt en privat del med adgang til at installere apps og bruge internet uden overvågning. Nogle sikkerhedsforanstaltninger kan gå igen på de to dele – f.eks. antivirus, sporing og remote sletning, men hvor der er opstillet gennemsigtige og minimerede krav til f.eks. sporing (f.eks. kun ved tyveri).

Overvågning: Tilsigtet algoritmisk ledelse eller bossware

Med ønsker om effektivitet, bedre kundeservice, bedre arbejdsmiljø og generelt bedre kvalitet i arbejdet, kan nogle arbejdsgivere have et ønske om at installere software til bl.a. at kortlægge, hvor meget tid en medarbejder bruger på forskellige arbejdsopgaver, på hvilket udstyr, i hvilke forskellige programmer, med hvilke data, med hvilke interne og eksterne samarbejdspartnere og under overholdelse af interne politikker. I mere omfattende udgaver kan softwaren også tænde kamera og måle opmærksomhedsniveau (også på hjemmekontoret), fastlægge GPS-placering og logge tastetryk. Ultimativt kan der laves en meget omfattende profilering af medarbejderen, og nogle løsninger lover, at kunne opdage usædvanlig adfærd fra medarbejderne – f.eks. tyveri af data eller om medarbejderne er ved at skifte job.

Arbejdsgiver kan have et stort potentiale i at benytte sådanne medarbejdergenererede data til at udvikle virksomheden og sikre innovationen. Men hvor nogle medarbejdere vil føle glæde ved at få adgang til data om sig selv, så de kan måle og optimere deres egen performance, vil andre føle sig krænkede og stressede over kontinuerlig måling. Bl.a. det franske datatilsyn, CNIL, har fastslået, at der er grænser for, hvor meget medarbejderne kan overvåges henset til effektivitet og fundet det ulovligt "to set up a system measuring work interruptions with such accuracy, potentially requiring employees to justify every break or interruption".[26]

Iværksættelsen af sådanne foranstaltninger forudsætter således fastsættelsen af meget klare formål, at der foreligger hjemmel til denne type måling, og at det er gennemsigtigt for medarbejderne. Jo flere data om medarbejderne der behandles, jo mere indgribende vil profileringen være, og jo mindre sandsynligt er det, at den dataansvarlige kan finde overvågningen proportional. Det er også vigtigt, at den dataansvarlige sikrer sig, at data kun behandles under instruktion, eller at der er hjemmel til at data behandles til leverandørens selvstændige formål.

Overvågning: Utilsigtet overvågning

Det er arbejdsgiver, som er ansvarlig for at kortlægge, hvilke data der behandles i de tjenester og på det udstyr, som stilles til rådighed for medarbejderne. Det gør den dataansvarlige typisk gennem dialog med leverandøren, kontrakt om leverancen og ved indgåelse af databehandleraftale samt under overholdelse af ovenfor beskrevne praksis.

I en række tilfælde benytter en arbejdsgiver tjenester, hvor der sker en uigennemsigtig behandling af data – herunder personoplysninger. Det er arbejdsgivers pligt at gøre sig klart, hvilke data der behandles i løsningen og hvilke datastrømme, der finder sted[27] - herunder at fastslå om behandlingen kan komme arbejdstageren til skade. Arbejdsgiver kan således ikke bare holde sig selv i uvidenhed, for at omgå reglerne. Omvendt, når arbejdsgiveren ikke ved gennemgang af det juridiske grundlag eller anvendelse af tjenesten har været i stand til at identificere mulige videregivelser, sker behandlingen uden arbejdsgiverens vidende, og arbejdsgiveren

[26] https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million.
[27] Se afgørelserne i Chromebook-sagen: https://www.datatilsynet.dk/afgoerelser/afgoerelser.

vil derfor ikke have fastslået et formål for – eller givet en instruktion til – sådan en behandling. Den endelige ansvarsfordeling mellem arbejdsgiver og arbejdsgivers leverandører for sådanne behandlinger er uafklaret.

Det forhold at arbejdsgiver er ansvarlig for behandlingen kunne også lede arbejdsgiver i retning af at stille krav til mitigerende foranstaltninger for at reducere risikoen for de registrerede – særligt hvor behandlingen er uigennemsigtig. Det kan således fra arbejdsgiver overvejes og anbefales at stille krav til leverandørens anvendelse af f.eks. aggregering, kryptering og anonymisering.

Overvågning: Arbejdsgivers brug af AI

Arbejdsgiver har også mulighed for at overvåge medarbejderne med brug af AI eller overvåge medarbejdernes brug af AI. AI er reguleret i EU's "AI Act", på dansk "AI forordningen", som flere steder i forordningsteksten[28] fremhæver risici forbundet med brug af AI til overvågning af ansatte. For det første kan nævnes forordningens artikel 5, stk.1, litra f, hvori der nedlægges et decideret forbud mod brug af AI "*to infer emotions of a natural person in the areas of workplace*". For det andet kan nævnes præambelbetragtning 57, hvoraf fremgår, at en bred vifte af AI-anvendelser i en ansættelsesretlig kontekst vil blive underlagt "Højrisiko"-kravene (fx "*AI systems used in employment…, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in workrelated contractual relationships, should also be classified high-risks…*"). Såfremt en konkret use-case falder i "Højrisiko"-kategorien, medfører dette en lang række skærpede krav, herunder til udarbejdelse af udførlig dokumentation for datagrundlag og datastyring, jf. forordningens artikel 10. For det tredje kan nævnes artikel 26, stk. 7 og præambelbetragtning 92, hvorefter arbejdsgivere får en udtrykkelig oplysningspligt ift. anvendelsen af højrisiko AI-systemer overfor deres ansatte. Forordningen træder trinvist i kraft i løbet af de kommende år, og det er derfor endnu for tidligt at sige noget endeligt om reglernes praktiske betydning.

4. Dataetiske anbefalinger om indsamling af medarbejderdata

4.1 Anbefalinger fra arbejdsmarkedets parter

I december 2023 udgav et partnerskab bestående af arbejdsgiver- og arbejdstagerorganisationerne: Dansk Erhverv, Dansk Industri, Djøf, Dansk Magisterforening, IDA, Finansforbundet og Forsikringsforbundet et anbefalingskatalog om ansvarlig og værdiskabende anvendelse af medarbejderdata.[29] Anbefalingskataloget blev udarbejdet i samarbejde med ADD-projektet.

Parterne betoner i forordet, at anbefalingskataloget *"… søger at finde balancen imellem at bruge medarbejderdata til at skabe stærkere arbejdspladser, uden at tillid og arbejdsmiljø sættes over styr i processen. Det er anbefalinger, som både belyser de muligheder, der kan opstå, når data håndteres med ansvarlighed og transparens, men også de udfordringer indsamling og brug af medarbejderdata kan medføre."*

De 4 anbefalinger er følgende:

- Styrk *tillid og transparens* gennem klar ansvarsfordeling og dataforståelse på arbejdspladsen.
- Styrk de *digitale kompetencer* på arbejdspladsen

[28] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.
[29] Partnerskab om anvendelse af medarbejderdata 2023/12

- Brug eksisterende muligheder til at *facilitere dialogen* om indsamling og brug af medarbejderdata på arbejdspladsen
- Bliv inspireret af eksisterende *dataetiske retningslinjer* for brug og indsamling af medarbejderdata

Styrk tillid og transparens

I tilknytning til at fremme tillid og transparens omkring virksomhedernes dataindsamling og dataanvendelse understreger partnerskabet blandt andet, at virksomheder og ledelsen har en særlig udfordring i forhold til at navigere i komplekse systemer, som ofte er udviklet af eksterne leverandører, hvis produkter har forskellige underliggende mekanismer, indlejrede antagelser og benchmarks.

I forhold til at styrke transparens og tillid omkring indsamling af medarbejderdata fremhæver partnerskabet følgende:

- Transparens er kun meningsfuldt og tillidsskabende i det omfang, at det kobles med en aktiv indsats for at øge forståelse og kompetence i virksomheden.
- Transparens handler ikke om at gøre al den indsamlede information tilgængelig. Det handler om, at der er klarhed om, hvem på arbejdspladsen der sidder med den relevante information på et givent område i dataindsamlingsprocessen, og hvad data skal bruges til.
- Transparens indebærer både en afklaring af lederens rolle og oplysning af medarbejderne om regler og rettigheder.
- Som arbejdsplads kan man etablere en tydelig ansvarsfordeling i forhold til, hvem der er ansvarlig for, og har overblikket over, de forskellige systemer til indsamling af medarbejderdata. Det skal sikre, at hverken ledere eller medarbejdere føler, at den enkelte leder står alene med ansvaret for hele datafødekæden.
- Transparensen kan øges ved at tage udgangspunkt i eksisterende regler og aftaler herunder GDPR, Den europæiske menneskerettighedskonventions artikel 8 (retten til privatliv)[30] samt de enkelte aftaler med arbejdsmarkedets parter.
- En øget grad af transparens i indsamling og brug af medarbejderdata kan bidrage til et åbent og tillidsfuldt arbejdsmiljø. Derudover vil en tydelig ansvarsfordeling mindske uoverskueligheden i dataindsamlingsprocesserne, når både ledere og medarbejdere bliver komfortable i, hvor de skal gå hen med eventuelle tvivlsspørgsmål.
- Et øget fokus på at inkorporere eksisterende regler vil også sikre, at medarbejderne er bevidste om deres rettigheder, hvilket kan skabe øget tryghed om dataindsamlingen, f.eks. ved at være informeret om, at arbejdspladsen kun kan indsamle data om medarbejderne, hvis der er et tydeligt angivet formål.

Styrk de digitale kompetencer

Partnerskabet fremhæver, at den øgede digitalisering stiller krav til, at lederen både skal være en kompetent og kritisk bruger af digitale værktøjer til indsamling af medarbejderdata samt være en garant for, at medarbejderne føler sig trygge i processen. Det kan kalde på et ledelsesmæssigt kompetenceløft, der dels handler om at øge forståelsen for systemerne, reglerne og dilemmaerne, men i lige så høj grad om at klæde lederne på til at føre en åben, informeret og gensidig dialog med medarbejderne.

På medarbejdersiden er der ligeledes brug for, at udvalgte tillidsvalgte får et relevant kompetenceløft, der gør dem i stand til at repræsentere medarbejderne i datarelaterede problemstillinger. Det er vigtigt at

[30] Den europæiske menneskerettighedskonvention 1950

understrege, at ingen arbejdsplads er ens, så kompetenceløftet kan tilpasses de forskellige niveauer og behov på arbejdspladserne i forskellige brancher.

Kompetenceløftet kan fokusere på tre overordnede temaer 1) Best practice for værdiskabende og meningsfuld dataindsamling, 2) Hvordan lederen og tillidsvalgte kan navigere og kommunikere effektivt på arbejdspladser med datadrevet ledelse og 3) Indføring i de væsentligste juridiske og etiske principper.

Faciliter dialogen om virksomhedens indsamling og brug af medarbejderdata

Partnerskabet indikerer - som det blandt andet er kommet til udtryk i ovennævnte undersøgelser fra ADD-projektet – at der kan være uoverensstemmelse mellem ledernes og medarbejdernes opfattelse af, hvad god og tilstrækkelig kommunikation indebærer på området.

Det er et oplagt behov for ledere til at informere medarbejdere om, hvordan de indsamler og anvender deres data i fora, hvor der er mulighed for en åben og gensidig diskussion. På den måde kan man proaktivt gribe eventuelle problemstillinger an, så medarbejderne føler sig set og hørt, og ledere har endnu bedre forudsætninger for at udøve datadrevet ledelse på en ansvarlig måde

De eksisterende fora, der er etableret på de fleste arbejdspladser – fx stormøder, afdelingsmøder, arbejdspladsvurderinger, samarbejdsudvalg mv. – er en god ramme for at styrke dialogen om dataindsamling og dens anvendelse i virksomheden.

Fastlæg virksomhedens dataetiske retningslinjer

Det understreges, at fravær af dataetiske retningslinjer skabe uklarhed hos medarbejderen omkring deres rettigheder i forhold til deres egne data. Det kan også placere lederen i en sværere position, når der skal kommunikeres om, og navigeres i, de dataetiske dilemmaer, der kan opstå med brugen af medarbejderdata.

Det kan imidlertid være en større ressourcemæssig opgave for særligt små- og mellemstore virksomheder at fastlægge specifikke dataetiske etiske retningslinjer for deres virksomhed og branche.

Partnerskabet peger på, at virksomheder og organisationer, der allerede har dataetiske retningslinjer til deres arbejde med kunde-, klient- og medlemsdata, kan lade sig inspirere i udarbejdelsen af dateetiske retningslinjer til indsamling og brug af medarbejderdata.

For det andet kan man overveje at udarbejde retningslinjer, som tager udgangspunkt i, eller blot henviser til, de dataetiske principper, som man kan finde i eksterne guides hos blandt andet Dataetisk Råd, Erhvervsstyrelsen og IDA. I de guides finder både ledere og medarbejdere gode værktøjer til at diskutere proportionalitet om data og formål samt metoder til at udøve dataminimeringsprincipper i praksis.

4.2 Dataetisk Råds guide 'Dataetik – sådan gør du'

Dataetisk Råd har i april 2022udgivet en 5-trins guide med tilhørende dataetisk canvas som inspiration og værktøj til arbejdet med dataetik.[31]

I guiden har Dataetisk Råd fastlagt 10 centrale dataetiske værdier, som kort omtales her:

[31] Dataetisk Råd 2022/4

- *Velfærd.* Behandling af data skal ske med respekt for og hensyn til sociale forhold, samfund og demokrati.
- *Værdighed.* Mennesker skal prioriteres før kommercielle og institutionelle interesser.
- *Privatliv.* Behandling af data skal ske med respekt for privatliv og under beskyttelse af personlige oplysninger.
- *Selvbestemmelse.* Behandling af data skal støtte mennesket i at træffe oplyste og selvstændige valg.
- *Lighed.* Behandling af data må ikke diskriminere eller reproducere fordomme, der marginaliserer og stigmatiserer befolkningsgrupper.
- *Frihed.* Behandling af data skal ske med respekt for grundlæggende frihedsrettigheder i et demokratisk samfund. Herunder ytrings-, informations-, religions-, forsamlings- og foreningsfriheden.
- *Retssikkerhed.* Behandling af data skal ske med respekt for grund - læggende retssikkerhedsmæssige garantier og rets - sikkerhedsniveauet i samfundet.
- *Gennemsigtighed.* Behandling af data skal være tilstrækkelig gennemsigtig. Der skal være adgang til indsigt i egne data.
- *Sikkerhed.* Behandling af data skal være tilstrækkelig sikker, robust og pålidelig.
- *Ansvarlighed.* Det skal være muligt at stille mennesker til ansvar. Det skal i alle led være klart hvem, der er ansvarlig for konsekvenserne for udvikling og anvendelse af data.

Som nævnt indeholder guiden også en 5-trins guide til arbejdet med dataetik på organisations- og projektniveau. Hvert af de 5 trin er ledsaget af relevante hjælpespørgsmål, der kan bistå projektudviklingen, analysen og dialogen i virksomheden.

1. *Identificer*. Det første skridt er at beskrive, hvordan relevante data bliver håndteret i projektet samt hvad det overordnede formål med behandlingen af data er.
2. *Analysér*. Næste skridt er, at du skal finde ud af hvilket dataetisk dilemma, du står over for. Du kommer frem til det dataetiske dilemma ved at analysere, hvilke hensyn der taler for og imod den påtænkte eller anvendte databehandling
3. *Afvej modstående hensyn*. Når du har identificeret hvad, der taler henholdsvis for og imod den påtænkte eller anvendte databehandling, skal du foretage en konkret afvejning. Formålet er at finde frem til en rimelig balance mellem de positive hensyn ved behandlingen af data og de negative konsekvenser.
4. *Beslut hvilke hensyn der vejer tungest*. Dataetik handler ikke blot om de overvejelser, som du bør gøre dig, men i lige så høj grad om de valg og handlinger, som du foretager dig.
5. *Evaluer de dataetiske konsekvenser løbende*. Sidste skridt handler om, hvordan du løbende vil evaluere de dataetiske konsekvenser, der kan være forbundet med din behandling af data.

5. Rådet for Digital Sikkerheds perspektiv på indsamling af medarbejderdata

ADD-projektets to repræsentative undersøgelser understreger, at virksomhedernes indsamling af medarbejderdata bliver stadig mere omfattende hvad angår indsamlingsomfanget, den databaserede overvågning og anvendelsen af komplekse it-systemer. Virksomhederne ser og har store potentialer i datadreven styring og ledelse, og ADD-projektet peger på, at man på ledelsesniveauet mange steder er begyndt at indhøste gevinsterne.

Imidlertid peger analyserne også på, at der kan være et mismatch mellem medarbejdernes og ledelsens opfattelse af, hvad der er på spil. Medarbejdernes viden og opmærksomhed i forhold til, hvad der rent faktisk indsamles og de indsamlingsformål som tilgodeses, svarer ikke til ledelsens perspektiv. Undersøgelserne indikerer således, at den høje grad af tillid på tværs i organisationen, som kendetegner den danske virksomhedskultur, er udfordret.

Rigtig mange ledere og medarbejdere har stiftet bekendtskab med EU's databeskyttelsesforordning (GDPR). Rådet finder, at det er centralt for tilliden til digitaliseringen, at arbejdsgiver sikrer efterlevelse af forordningen. Rådet for Digital Sikkerhed kan derfor kun applaudere Datatilsynet for den kvalificerede vejledning om databeskyttelse i ansættelsesforhold. Vejledningen er et nødvendigt redskab for at sikre, at virksomhedernes indsamling af medarbejderdata er i overensstemmelse med lovgivningen, og for medarbejderne tjener vejledningen til større indsigt i egne rettigheder og virksomhedens forpligtelser på området. Tilsvarende ser Rådet med stor glæde på den praksis, der over de sidste 25 år har udviklet sig på området, og som bidrager som guidelines for de dataansvarlige.

Dialog er nøglen til at udvikle tilliden mellem medarbejdere og ledelse i en tid, hvor datadreven virksomhedsudvikling og kunstig intelligens finder vej til de danske arbejdspladser. Partnerskaber, der samler arbejdsgiver- og arbejdstagerorganisationer om de nævnte udfordringer, er godt for at understøtte konkrete initiativer på mange virksomheder. Partnerskaber såvel nationalt som på den lokale arbejdsplads, hvor der drøftes overvågning og arbejdsmiljø i f.eks. SU er en god vej frem, således at der er fokus på medarbejdernes sikkerhed og sundhed. Rådet hæfter sig ved pointen om, at transparens nok kan handle om politikker og retningslinjer, men den vedvarende og aktive dialog om nye dataindsamlingsmetoder og anvendelsesformer på branche-, virksomheds- og medarbejdergruppeniveau i sig selv skaber gennemsigtighed gennem involvering.

I den forbindelse hæfter Rådet sig også ved det store behov for kompetenceudvikling. Ansvarlig anvendelse af medarbejderdata bør anskues som et kompetencefelt på linje med virksomhedernes andre fagkompetencer, der løbende skal udvikles. For - udover medarbejderne selv - er data om medarbejderne en aktiv ressource for virksomhedens drift og innovation.

Også på ledelsesniveauet er der behov for kompetenceudvikling. Ledelsesansvaret – og dermed også ledelsesværktøjskassen - i forhold til at fremme virksomhedens resultater og sikkerhed samt medarbejdernes arbejdsglæde og effektivitet forandres i takt med den øgede anvendelse af digital teknologi. Feltet mellem ledelsesretten, respekten for medarbejdernes privatliv og deres oplevelse af at være overvåget forrykker sig fundamentalt med etableringen af gennemdigitaliserede arbejdspladser.

I tråd hermed er det en aktualiseret problemstilling, at dataindsamlingen ofte sker ved anvendelse af systemer og software, hvor dataindsamlingen opsamles af 3. parts-leverandører og kan videredistribueres til helt andre formål. Det er centralt, at arbejdsgiver foretager en ansvarlig kortlægning af dataflow og overvejer at stille krav om brug af mitigerende foranstaltninger som f.eks. aggregering, kryptering og anonymisering for at reducere risikoen for de ansatte. I den forbindelse må vi imødese udvikling af praksis om videregivelse af personoplysninger til tredjepart.

Sammenfattende er det Rådet for Digital Sikkerheds vurdering, at vi med de senere års fokus på problemstillingen omkring indsamling af medarbejderdata er godt på vej til at aktivt få integreret persondatabeskyttelsen i den ledelsesmæssige værktøjskasse. Det handler om virksomhedens ret og pligt, respekt for de ansattes fundamentale rettigheder, tillid og dialog gennem aktiv involvering samt ikke mindst kompetenceudvikling på alle niveauer med henblik på at udvikle ansvarlig dataanvendelse som et aktiv for

datadrevne virksomheder. Rådet for Digital Sikkerhed opfordrer til, at vi fortsætter og videreudvikler på det spor.

Samtidig er det Rådets vurdering, at vi bør sætte yderligere fokus på offentlige og private virksomheders indkøb af digital software og aftaler med system- og cloudleverandører. Virksomheder i Danmark skal selvsagt overholde lovgivningen og varetage det dataetiske ansvar i forhold til medarbejderne, men vi har behov at skabe mere klarhed over, hvilke krav man som virksomhed bør stille til leverandørerne af digital teknologi.