Kommentar

Arbeidstakeres personvern – EMK og nye e-postregler[+]

Av Mette Borchgrevink*

Innholdsoversikt

---

* Mette Borchgrevink (f. 1954) er cand. jur. (UiO 1980), lic. jur. (UiO 1985), senioradvokat i Advokatfirmaet Steenstrup Stordrange DA siden 2001, medlem av Advokatforeningens lovutvalg for IKT og personvern. Tidligere praksis bl.a. som forskningsstipendiat ved Institutt for rettsinformatikk, UiO, Advokatfirmaet Schjødt DA, Datatilsynet, Direktoratet for arbeidstilsynet, NHO.

[+] Artikkelen er en omarbeidet versjon av et tidligere bidrag i Lov & Data 2009, nr. 1.

Arbeidsrett og arbeidsliv. Bind 4, s. 179-197 (2009)

1 Innledning

1.1 Introduksjon

Den nye "e-postforskriften" trådte i kraft 1. mars 2009. Dette er ikke en særskilt forskrift, men et nytt kapittel 9 om "Innsyn i e-postkasse mv" i personopplysningsforskriften (pof.),[1] som er gitt med hjemmel i personopplysningsloven (pol.).[2] Formålet med reglene er å beskytte ansatte mot krenkelser av deres personvern, samtidig som arbeidsgivers interesser i virksomhetsrelatert informasjon skal sikres. Forskriften utdyper og presiserer lovens generelle regler.

Reglene gjelder for innsyn i arbeidstakeres personlige e-postkasser samt i dokumenter på arbeidstakeres personlige områder, m.v. Reglene angir vilkår for når innsyn er tillatt, hvordan innsyn skal foregå, bestemmelser om varsling, rett til å være til stede ved innsyn, etc.

Denne artikkelen redegjør for reglenes betydning for arbeidstakeres personvern og for virksomhetens mulighet til å ta vare på forretningskritisk informasjon. Videre behandles hvordan disse reglene kan håndteres av partene i arbeidslivet i praksis. Her er "datainstruks" et virkemiddel. Med datainstruks forstås en instruks som er utferdiget av arbeidsgiver og som kan inneholde konkrete pålegg og rutiner for bruk av virksomhetens IKT-utstyr, bruk av e-post, innsyn, etc. Jfr. nærmere i avsnitt 7 nedenfor.

1.2 Bakgrunn

Bakgrunnen for de nye reglene var Datatilsynets anmeldelse av to selskaper for brudd på personopplysningsloven i 2006. Anmeldelsene ble henlagt da intet straffbart forhold hadde funnet sted. Året etter anmeldte Datatilsynet Bazar Forlag, der forlagssjefen hadde skaffet seg tilgang til inngående e-post til leder for forlagets kontor i Sverige.

---

1 Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften). Det nye kapittel 9 ble tilføyd ved forskrift 29. januar 2009 nr. 84 og trådte i kraft 1. mars 2009.

2 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

I Datatilsynets årsmelding for 2007[3] heter det om denne saken bl.a. (s. 50):

> ”Bakgrunnen for saken var at forlagssjefen i Bazar Forlag AS opprettet en ’overvåkingskonto’ med navnet backup@bazarforlag.com. Via ’overvåkingskontoen’ skjedde det en automatisk blindkopiering av inngående e-postkorrespondanse til leder for forlagets kontor i Sverige. Den ansattes personlige e-postkonto var beskyttet med brukernavn og personlig passord.
>
> Forlagssjefen gjorde innsyn i den ansattes inngående e-post gjennom ”overvåkingskontoen”. Den ansatte som fikk lastet ned og åpnet sin inngående e-post, fikk ingen informasjon vedrørende nedlastingen av e-postene, Etter Datatilsynets vurdering brøt Bazar Forlag AS personopplysningslovens bestemmelser på flere punkter, og etter tilsynets vurdering var lovbruddene av alvorlig karakter. Spesielt alvorlig var bruddene på informasjonsplikten etter personopplysningslovens § 19 og § 20.
>
> Politimesteren i Oslo siktet Bazar Forlag AS og forlagssjefen for brudd på informasjonsplikten og ila begge forelegg. Både forlaget og forlagssjefen vedtok forelegget.”

Arbeidslivslovutvalget foreslo i sin innstilling fra 2004 at arbeidsgiver *skulle ha* rett til innsyn i virksomhetsrelatert e-post. Forslaget fikk tilslutning fra både arbeidstakersiden og arbeidsgiversiden under høringen. Det ble likevel ikke fulgt opp av departementet, dels på grunn av innvendinger fra Datatilsynet og dels fordi det var igangsatt arbeid med særlige forskriftsbestemmelser, jf. Ot.prp. nr. 49 (2004–2005) s. 150. I oktober 2006 sendte Fornyings- og administrasjonsdepartementet (FAD) ut et høringsutkast om nye regler om arbeidsgivers adgang til ansattes e-post mv.[4] Utgangspunktet i forslaget til nytt kapittel 9 i personopplysningsforskriften, som ble sendt på høring sammen med forslag til forskriftshjemmel, var at arbeidsgivere *ikke* skulle ha rett til innsyn i ansattes e-post. Innsyn kunne etter forslaget likevel skje i ”virksomhetsrelatert” e-post i nærmere angitte tilfeller, blant annet dersom arbeidstakeren var fraværende i mer enn tre arbeidsdager. Det kom inn en lang rekke høringsuttalelser. Høringsinstansene

[3] Årsmeldingen er tilgjengelig på http://www.datatilsynet.no/upload/dokumenter/aarsmeldinger/avsendt%20datatilsynets%20årsmelding_2007%20til%20fad.pdf.

[4] http://www.regjeringen.no/nb/dep/fad/dok/horinger/horingsdokumenter/2006/forslag-til-regler-om-arbeidsgivers-adga/1.html?id=270943.

var delt i synet på utkastet.[5] Proposisjon ble lagt frem 27. juni 2008 med forslag bl.a. om å utvide forskriftshjemmelen i pol. § 3 fjerde ledd.[6] Det umiddelbare siktemålet med forslaget var å åpne for særlig regulering av arbeidsgiveres rett til innsyn i ansattes e-post mv. Om begrunnelsen heter det bl.a. i proposisjonen at "Datatilsynet har hatt en økende pågang av henvendelser fra arbeidsgivere og arbeidstakere om hvor grensen for lovlig innsyn går etter gjeldende rett" (s. 6). Justiskomiteen avga innstilling 20. november 2008,[7] endringsloven ble sanksjonert 9. januar 2009 (nr. 3), og e-postforskriften ble vedtatt 29. januar 2009.

Samtidig ble det tilføyd en ny § 9-5 i arbeidsmiljøloven (17. juni 2005 nr. 62) om "Innsyn i arbeidstakers e-post mv" med følgende ordlyd: "Arbeidsgivers rett til innsyn i arbeidstakers e-post mv. reguleres i forskrift gitt i medhold av personopplysningsloven § 3 fjerde ledd første punktum". Denne henvisningsbestemmelsen er begrunnet med "opplysningshensyn og … hensyn til sammenhengen med arbeidsmiljølovens regler om kontrolltiltak (kapittel 9), …[for å] gjør[e] det klart at arbeidsgiveres innsyn i e-post mv. bare kan skje når det følger av personopplysningslovens regler" (Ot.prp. nr. 71 (2007-2008), s. 34).

Formålet med e-postreglene er å klargjøre arbeidsgivers rett til innsyn i særskilte tilfeller, samt å verne arbeidstaker mot urimelig kontroll fra arbeidsgivers side.

1.3 EMK som bakteppe

Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8, og loven som inkorporerer konvensjonen i norsk rett,[8] gir "enhver" rett "til respekt for privatliv og familieliv, sitt hjem og sin korrespondanse." Respekten for privatliv og korrespondanse gjelder også på arbeidsplassen, virkeområdet for EMK artikkel 8 er generelt. At EMK artikkel 8 skal legges til grunn i norsk rett følger også av personopp-

---

5 Høringsuttalelsene er publisert på http://www.regjeringen.no/nb/dep/fad/dok/-horinger/horingsdokumenter/2006/forslag-til-regler-om-arbeidsgivers-adga/3.html?id=270945.

6 Ot.prp. nr. 71 (2007-2008) *Om lov om endringer i personopplysningsloven mv. (forskriftshjemmel, overtredelsesgebyr og innkreving av tvangsmulkt)*.

7 Innst. O. nr. 16 (2008-2009).

8 Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).

lysningsloven som gjennomfører EFs personverndirektiv[9] i nasjonal rett. Dette bygget også Arbeidslivslovutvalget på.

I Arbeidslivslovsutvalgets innstilling fra 2004 er det uttalt om EMK artikkel 8:[10]

> "Bestemmelsen beskytter retten til privatliv, som er retten til å leve sitt liv uten inngripen fra utenforstående. Dette omfatter rett til så vel fysisk og psykisk integritet som beskyttelse av ære og rykte. Retten til privatliv omfatter også beskyttelse mot overvåking og beskyttelse av informasjon om private forhold.
> I norsk rettspraksis er det bygget på det samme allmenne prinsippet om privatlivets fred som konvensjonen er uttrykk for. Artikkel 8 er en tolkningsfaktor i forhold til personopplysningsloven. Dette følger av at konvensjonen gjelder direkte som norsk lov (jf menneskerettsloven § 2). Videre slås det fast i fortalen til EUs personverndirektiv at nasjonal lovgivning skal sikre privatlivets fred i arbeidsforhold i samsvar med artikkel 8 nr. 1."

I personverndirektivets fortale pkt. 10 heter det:

> "De nasjonale lovgivninger om behandling av personopplysninger har som mål å verne de grunnleggende rettigheter og friheter, særlig retten til privatlivets fred, som er anerkjent både i artikkel 8 i Den europeiske konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter og i fellesskapsrettens generelle prinsipper. Derfor må tilnærmingen av lovgivningene ikke føre til en svekkelse av den beskyttelsen de gir, men tvert imot ha som mål å sikre et høyt vernenivå i Fellesskapet."

Forskriften har ikke selv noen referanse til EMK og retten til privat korrespondanse, slik høringsutkastet hadde. Men det følger av det som er sagt ovenfor, at dette ikke har noen betydning for tolking og anvendelse av reglene.

2 Reglenes saklige virkeområde

Forskriftens kapittel 9 gjelder innsyn i arbeidstakeres e-post, som er definert som den e-postkasse som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet, jf. § 9-1 annet ledd. Forskriften gir ikke arbeidsgiver hjemmel til innsyn i private e-postkasser som

---

9 Europa-Parlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

10 NOU 2004: 5 *Et arbeidsliv for trygghet, inkludering og vekst*, s. 408.

arbeidstakeren måtte ha,[11] eksempelvis hotmail, gmail, etc., da disse ikke er stilt til arbeidstakers disposisjon til bruk i arbeidet.

Forskriften bruker ikke begrepene ”privat” eller ”virksomhetsrelatert”, som Høyesterett brukte i dommen i Rt. 2002 s.1500 og slik høringsutkastet gjorde (jfr. i 1.2 ovenfor).

Forskriften gjelder også innsyn i andre elektroniske kommunikasjonsmedier som er stilt til arbeidstakers disposisjon av arbeidsgiver. Det typiske eksempelet er mobiltelefoner, hvor reglene om innsyn vil gjelde for innsyn i SMS og MMS-meldinger lagret på mobiltelefonen
Reglene gjelder videre for dokumenter som ikke er ledd i korrespondanse. Eksempler er notater, kundelister, strategiplaner, etc., som er lagret som Word-dokumenter, PowerPoint, e.l. Vilkåret er at dokumentene er lagret elektronisk på et personlig brukerområde og er beskyttet av personlig passord som kun arbeidstakeren har adgang til.
Motsatsen er dokumenter lagret på fellesområder på server, som alle eller grupper av ansatte har tilgang til. Reglene gjelder ikke her, da fellesområder ikke regnes som ”personlig brukerområde”. Arbeidsgiver har rett til å lese dokumenter som er lagret i slike fellesområder, og slik lesing regnes derfor ikke som ”innsyn” etter disse reglene.

Videre gjelder reglene dokumenter som er lagret i annet elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon. Eksempler på dette er dokumenter lagret på PDA (”lommedatamaskin”), PC og minnepinner.

Reglene gjelder ikke bare i arbeidslivet, de gjelder tilsvarende for organisasjoner, høyskoler, etc. Dette betyr at studenter som får tildelt e-postadresse på lærestedet, eller som har dokumenter på personlige områder på lærestedets server, kan risikere innsyn i sine e-poster og dokumenter. Det kan være aktuelt ved mistanke om ulovlig fildeling eller andre ulovlige forhold.

[11] Slike private e-postkasser inneholder privat kommunikasjon som er beskyttet av straffeloven (lov 22. mai 1902 nr. 10) § 145 annet ledd og EMK art. 8.

3 Materielle vilkår for innsyn

3.1 Generelle vilkår

Etter forskriftens § 9-2 er vilkårene for innsyn enten

a) at innsynet i e-post er nødvendig for å ivareta daglig drift eller andre berettigede interesser for bedriften,

eller

b) at det foreligger begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt pliktbrudd eller kan gi grunnlag for oppsigelse eller avskjed.

Det er et vilkår etter § 9-2 a) at innsynet må være ”*nødvendig*”. Det betyr at innsyn ikke kan foretas dersom informasjonen kan skaffes på annen måte. Arbeidsgiver kan eksempelvis skaffe seg tilgang til en e-post som er sendt til en fraværende ansatt ved å be avsenderen sende e-posten på ny til en annen ansatt. Dersom det er mulig, vil ikke nødvendighetskravet være oppfylt. Nødvendighetskravet i § 9-2 a) er en presisering av pol. § 11 b) og et eksempel på den proporsjonalitetsvurdering som må gjøres.

Nødvendighetskravet vil trolig måtte tolkes noe forskjellig avhengig av hva det skal gjøres innsyn i, jf. eksemplene nedenfor.

3.1.1 Innsyn i SMS/MMS

I praksis vil det måtte stilles strengere krav til ”nødvendighet” for innsyn i SMS fordi det ikke er mulig å skille mellom private og virksomhetsrelaterte meldinger. Det er mulig å ha egen privat e-postkonto, men for de fleste vil det være upraktisk å ha egen mobiltelefon til private samtaler og SMS. Hensynet til personvernet tilsier derfor at man bør legge til grunn en presumpsjon for at SMS er privat kommunikasjon. Innsyn i SMS vil derfor normalt krenke retten til privat kommunikasjon, jf. EMK artikkel 8.

3.1.2 Slettede filer

Arbeidstaker kan ha slettet e-poster og filer, eksempelvis for å rydde opp eller for å hindre at arbeidsgiver får tilgang til den slettede informasjonen. Informasjonen kan likevel være tilgjengelig på sikkerhetskopier, og vilkårene i § 9-2 gjelder også i slike tilfeller, jf § 9-1 annet ledd if. Det er mulig at kravet til nødvendighet må tolkes strengere for

slettet informasjon, nettopp fordi arbeidstaker faktisk har slettet dokumentene. Når man sletter dokumenter, kan det være fordi man ønsker at andre ikke skal kunne få innsyn i dem, eksempelvis fordi de er av privat art, eller man ønsker å destruere informasjonen av andre grunner.

3.1.3 Sikkerhetskopier

Sikkerhetskopier har til formål å fungere som backup slik at datasystemer og filer kan gjenopprettes når det er behov for det. Sikkerhetskopier tas regelmessig; gamle sikkerhetskopier vil ikke ha tilfredsstillende kvalitet for bruk til gjenoppretting. I slike tilfeller vil arbeidsgiver ikke lenger ha hjemmel til å beholde sikkerhetskopiene og må slette disse, jf. pol. § 28, jf § 11 e). Dersom arbeidsgiver vil foreta innsyn i gamle sikkerhetskopier, vil kravet til ”nødvendighet” trolig måtte tolkes strengere jo eldre sikkerhetskopiene er. Dersom sikkerhetskopiene er så gamle at sletteplikten må anses inntrådt, medfører det at arbeidsgiver overhodet ikke har hjemmel til å behandle personopplysningene i sikkerhetskopiene. I slike tilfeller medfører forskriftens § 9-2 ingen ny rett til å behandle personopplysninger.[12] I praksis er grensen for når sletteplikten, inntrer vanskelig å trekke, og derfor vil skjerpede krav til nødvendighet for gamle kopier kunne løse problemene i praksis.

3.1.4 Fravær

Forskriften har ingen regler om innsyn ved fravær. Fravær, og fraværets varighet, vil være et element i en totalvurdering av om innsyn er ”nødvendig” etter § 9-2 a). Dersom arbeidstakeren har sørget for videresending av virksomhetsrelatert e-post, eller automatisk svar med opplysning om hvor virksomhetsrelatert e-post skal sendes i vedkommendes fravær, vil dette redusere behovet for innsyn.

3.1.5 Mistanke

Dersom det er spørsmål om å foreta innsyn med hjemmel i § 9-2 b) om begrunnet mistanke om grovt pliktbrudd, etc., gjelder det etter ordlyden ikke et krav om «nødvendighet» i ordlyden, men et krav om

[12] Om hva som forstås med å ”behandle” personopplysninger, se pol. § 2 nr. 2.

"begrunnet mistanke" om klanderverdige forhold. Denne begrunnelsen kan Datatilsynet overprøve (jf. i avsnitt 10 nedenfor).

3.2 Samtykke gir ikke grunnlag for innsyn

Det følger direkte av ordlyden i forskriftens § 9-2, med uttrykket "bare", at samtykke ikke gir lovlig grunnlag for innsyn. Vilkårene for innsyn i § 9-2 er uttømmende. Dette er nytt. Tidligere ble samtykke ansett som et tilstrekkelig grunnlag for innsyn, forutsatt at det forelå et saklig behov etter lovens § 11.[13]

Forskriftens § 9-5 gir adgang til å fravike forskriftsreglene ved avtale eller instruks, men dette kan ikke gjøres til "ugunst for arbeidstaker". Spørsmålet er om § 9-5 gir hjemmel for at arbeidstaker kan samtykke i e-postinnsyn eller inngå individuell avtale med arbeidsgiver om dette.

Ifølge departementets merknader må slike avtaler/instrukser ikke gi dårligere vern enn forskriften gir, og merknadene viser til at formålet med forskriften er å verne mot urimelig kontroll fra arbeidsgivers side.[14] Dersom slik avtale gir arbeidstakere svekket personvernbeskyttelse, vil en slik avtale trolig være i strid med § 9-5.

Videre er det et vilkår at samtykket, eller avtalen, er inngått «frivillig». Det følger av samtykkedefinisjonen i pol. § 2 nr. 7: "Samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv." Kravet til frivillighet, som er forankret i EFs personverndirektiv, er kommentert av EU/EØSs "Artikkel 29-gruppe".[15] I gruppens Opinion 8/2001 heter det: "Reliance on consent should be confined to

---

[13] Jf. Datatilsynets veiledning om "e-post og filer" datert 10. mars 2008, tidligere publisert på www.datatilsynet.no.

[14] Fornyings- og administrasjonsdepartementets merknader til personopplysningsforskriften kapittel 9, publisert på departementets nettside pr 1. mars 2009, http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2009/fra-i-dag-gjelder-de-nye-reglene-for-inn.html?id=547499.

[15] Den såkalte Artikkel 29-gruppen består av direktørene for datatilsynsmyndighetene i EU og EØS. Gruppen lager "opinions" basert på EFs personverndirektiv 95/46/EF, som er implementert i alle EU- og EØS-land.

cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment" (s. 23).[16]
I arbeidsforhold er det i utgangspunktet asymmetri i maktforholdet mellom arbeidsgiver og arbeidstaker. Det kan derfor reises spørsmål om et samtykke fra arbeidstaker til innsyn vil være frivillig, fordi et samtykke neppe kan trekkes tilbake helt uten konsekvenser for arbeidstakeren. Personopplysningsloven krever at samtykke skal være frivillig avgitt for å være gyldig. Artikkel 29-gruppen har anbefalt andre behandlingsgrunnlag enn samtykke der samtykket ikke kan trekkes tilbake uten skade for arbeidstaker, jf sitatet ovenfor. Dette er trolig bakgrunnen for at departementet ikke lar samtykke være et rettslig grunnlag for innsyn.

Som følge av at samtykke fra arbeidstaker normalt ikke alltid kan anses som fullstendig frivillig avgitt, må det antas at samtykke, eller avtale mellom arbeidstaker og arbeidsgiver, neppe kan være gyldig grunnlag etter § 9-5.

Merknadene til forskriften legger for øvrig opp til at arbeidstaker "uoppfordret" kan gjennomføre sin plikt til å gjøre arbeidsgiver kjent med tjenstlig e-post ved å gi arbeidsgiver tilgang, for eksempel ved at en arbeidstaker på eget initiativ gir en kollega lesetilgang under fravær. "Uoppfordret" betyr at arbeidstakeren på eget initiativ og uten oppfordring gjør e-posten tilgjengelig for virksomheten. Dette er noe annet enn samtykke, som normalt avgis etter at man er blitt oppfordret til å gi samtykke. En oppfordring til å avgi samtykke kan oppfattes som press, slik at det ikke blir frivillig, i motsetning til "uoppfordret".

4 Fremgangsmåten ved innsyn

Ettersom vilkårene for når innsyn er tillatt er så generelle som de er, er det desto viktigere at saksbehandlingsreglene følges, og i § 9-3 er det gitt saksbehandlingsregler for innsyn.

De nye reglene gir arbeidstakere rett til:

- Å bli varslet før innsyn skjer
- Å få uttale seg på forhånd

[16] Opinion 8/2001 finnes på http://ec.europa.eu/justice_home/fsj/privacy/docs-/wpdocs/2001/wp48en.pdf.

- Å få begrunnelse for hvorfor arbeidsgiver mener at vilkårene for innsyn er oppfylt
- Å være tilstede på arbeidsplassen når innsynet blir foretatt
- Å ha med tillitsvalgt

I hastesaker er det mulig å foreta innsyn uten forhåndsvarsel. I slike tilfeller skal arbeidstaker informeres i ettertid. Informasjonen skal være skriftlig og inneholde opplysninger om metoden for innsyn, hvilke e-poster eller dokumenter som ble åpnet, og resultatet av innsynet. Slik informasjon skal også gis til arbeidstakere som har fått forhåndsvarsel.

I konflikttilfeller vil det være avgjørende at virksomheten kan dokumentere at vilkårene for innsyn er til stede, og at reglene er fulgt. Det bør derfor lages en protokoll i forbindelse med "innsynsforretningen"[17] som beskriver om arbeidstaker var forhåndsvarslet, hvem som var til stede, om arbeidstaker hadde innsigelser, og som skal inneholde det som skal gis av informasjon til arbeidstaker etter innsynet. En slik protokoll, undertegnet av de som var til stede, vil være hensiktsmessig for å sikre nødvendig dokumentasjon.

Denne dokumentasjonen kan ha betydning på to måter: For det første for å sikre seg mot eventuelle krav om bevisavskjæring, jf tvisteloven[18] § 22-7. For det andre kan slik dokumentasjon forebygge at Datatilsynet ilegger virksomheten overtredelsesgebyr på grunn av brudd på reglene.

5 E-post og dokumenter må slettes når ansatte slutter

Hovedregelen etter forskriftens § 9-4 er at arbeidsgiver skal slette innholdet i e-postkassen når en ansatt slutter. Kravet om sletting gjelder også for notater, rapporter og annen informasjon som er lagret elektronisk på arbeidstakerens personlige område i virksomhetens data-

[17] "Innsynsforretning" er etter min oppfatning en hensiktsmessig betegnelse på selve innsynet, og definerer det som en begivenhet som skal protokolleres. En slikt betegnelse kan også gi signal om at innsyn ikke er noe som bør gjøres uformelt eller uanmeldt.

[18] Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven).

nettverk. Dokumenter lagret på fellesområder for virksomhetens ansatte berøres ikke av disse reglene, jf. i avsnitt 2 ovenfor.

Plikten til å slette e-post og dokumenter omfatter ”dokumenter med innhold som er ikke nødvendig for den daglige driften av virksomheten”. Begrepet ”daglig drift” er ikke definert i forskriften, og departementets merknader (jf. note 14) omtaler kun hva som er av betydning for ”drift” av virksomheten, i motsetning til ”daglig drift”. Høringsutkastet hadde ikke noen tilsvarende regel; dermed er det ingen veiledning å hente der. Umiddelbart er ”daglig drift” et vesentlig snevrere begrep enn ”drift”. Begrepet ”*daglig* drift” må rent språklig tolkes som informasjon relatert til den løpende daglige drift, i motsetning til informasjon som skal arkiveres av hensyn til fremtidig dokumentasjonsbehov eller fremtidig forvaltning av ansvar eller rettigheter.

Noen eksempler kan belyse problemstillingen:

- Konsulentrapporter skrevet av tidligere ansatte for firmaets kunder kan være viktige for virksomhetens ansvar i tilfelle tvist hvor rapporten har betydning. Når rapporten er overlevert og kunden har betalt, er det ikke naturlig å si at rapporten er ”nødvendig for den daglige drift”.
- Dokumenter i tilknytning til utviklingsarbeid for prosjekter, eksempelvis dokumenter med kalkyler, tegninger, etc.

Slike dokumenter vil være arkivverdige, og kan også representere forretningshemmeligheter eller verdifull knowhow, uten at de dermed kan sies å være nødvendig for den *daglige* drift.

Tilbud med svarfrist er eksempel på hva som trolig må oppfattes som ”nødvendig for ”daglig drift”, men bare en kort tid.

Alt som ikke er nødvendig for den daglige drift, skal slettes, selv om det måtte være arkivverdig, bokføringspliktig eller forretningskritisk. Sletteplikten kan i praksis omfatte forretningshemmeligheter eller opphavsrettslig beskyttet materiale som er av stor økonomisk betydning for virksomheten.

Hva som er ”nødvendig for den daglige driften”, er et meget skjønnsmessig tema som kan gi rom for tvil og konfliktsituasjoner dersom virksomheten og arbeidstaker ikke er enige om vurderingen.

Departementet forutsetter i sine merknader at virksomheten må iverksette særlige tiltak for å ivareta personvernet til arbeidstakere

som slutter, i de tilfeller man ikke sletter reservekopier regelmessig. Slike tiltak kan beskrives i datainstruks eller avtale mellom arbeidsgiver og arbeidstaker, jf. forskriftens § 9-5, se i avsnitt 7 nedenfor.

6 Plikt til og pålegg om å oversende relevant informasjon

Forskriften begrenser arbeidsgivers adgang til ensidig å gi bestemmelser eller direktiver om og til å råde over informasjon som virksomheten kan ha materielle og immaterielle rettigheter til, og som kan være virksomhetskritisk informasjon. Til dette har FAD bemerket:

> ”Det presiseres også at bestemmelsene om innsyn i e-post ikke begrenser arbeidstakers plikt til, på eget initiativ, å gjøre arbeidsgiver kjent med e-post med tjenestlig innhold. Dette gjelder så vel i privat som offentlig virksomhet, og kan blant annet ha betydning i forhold til arbeidsgivers plikter etter arkivloven og bokføringsloven. Arbeidstaker har således plikt til å sørge for å gi arbeidsgiver tilgang til arkivverdig materiale.”[19]

I kraft av sin alminnelige styringsrett kan arbeidsgiver pålegge ansatte å videresende kommunikasjon fra forretningskontakter og annen klart virksomhetsrelatert kommunikasjon. Dersom et slikt dokumenterbart pålegg ikke etterleves, vil et innsyn i e-post kunne hjemles i § 9-2 b) fordi nektelsen er ordrenektelse, som i visse tilfeller vil kunne gi grunnlag for oppsigelse eller avskjed (jf. i 3.1 ovenfor).

Arbeidstaker må kunne nekte å videresende privat kommunikasjon, fordi slik normalt ikke vil være ”nødvendig for daglig drift eller andre berettigede interesser” (jf. § 9-2 a)). Ved tvil om en aktuell kommunikasjon er virksomhetsrelatert eller privat, vil et innsyn i e-posten eventuelt kunne hjemles i § 9-2 b, dersom vilkårene efter denne bestemmelsen ellers er til stede.

Når ansatte skal slutte, vil arbeidsgiver likeledes kunne pålegge den ansatte å gjennomgå sin e-postkonto og overlevere alt virksomhetsrelatert/arkivverdig. I FADs merknader sies det:

> ”Det mest praktiske vil da være at arbeidstaker sletter e-post eller andre dokumenter med privat innhold, og gir arbeidsgiver tilgang til all dokumentasjon med tjenstlig innhold.”

[19] Fra FADs merknader til personopplysningsforskriften (jf. note 14 ovenfor).

Det er viktig at man tar seg tid til en gjennomgåelse og overlevering av alt som er virksomhetsrelatert, og lager rutiner for dette, for eksempel i form av en datainstruks.

Der arbeidsforholdet slutter på en slik måte at slik overlevering ikke er mulig, eksempelvis ved arbeidstakers død, sier departementet i sine merknader:

> "Arbeidsgiver bør i slike situasjoner sørge for at det innen rimelig tid vurderes om det er grunnlag for videre behandling eller om dokumentene skal slettes i samsvar med personopplysningsloven § 28. Hva som er rimelig tid må vurderes konkret, men det må kunne forventes at arbeidsgiver har foretatt en vurdering i løpet av en seks måneders periode etter arbeidsforholdets opphør. Det bør i så fall foretas konkrete søk etter virksomhetsrelaterte dokumenter som sikrer videre oppbevaring av de dokumenter som er av betydning for drift av virksomheten, med tanke på sletting av det overflødige."

7 Datainstruks

Som nevnt ovenfor gir forskriftens § 9-5 hjemmel til å fravike reglene i forskriftens kapittel 9 ved avtale eller instruks, såfremt det ikke er til arbeidstakers "ugunst". Forskriften sikter her til det som i tariffavtaleterminologien til dels er kalt "datainstruks".[20] Efter tariffavtalenes bestemmelser er dette typisk en "instruks" som arbeidsgiver *skal* utarbeide *i samarbeid med* de tillitsvalgte og dersom partene i virksomheten ikke blir enige, kan saken bringes inn for de overordnede organisasjonene.[21] Dersom virksomheten ikke er tariffbundet av slike bestemmelser, kan arbeidsgiveren eventuelt utferdige en instruks i kraft av sin alminnelige styringsrett. Også i slike tilfeller bør instruksen drøftes med de ansatte på forhånd. En sik instruks bør også sendes de ansatte og bør være et vedlegg til ansettelsesavtalene. Følges reglene om "skriftlige arbeidsavtaler" i arbeidsmiljølovens §§ 14-5 flg., er det

---

[20] Dette er en reguleringsform som har sin bakgrunn i hovedavtalen (arbeidere) LO – N.A.F. (nå NHO), Tilleggsavtale IV, Rammeavtale om teknologisk utvikling og datamaskinbaserte systemer, og en rekke andre hovedavtaler m.v. De første "dataavtalene" ble inngått mellom 1975 og 1980; se nærmere M. Borchgrevink, *Ny teknologi i arbeidslivet ; Rettslige aspekter*. Oslo: Universitetsforlaget 1985, s.83-86 og 321-401.

[21] Se f.eks. hovedavtalen (arbeidere) LO – NHO 2006-2009, Tilleggsavtale IV, pkt. VI Behandling av personopplysninger.

ikke nødvendig at de ansatte undertegner på datainstruksen, men en kvittering på at instruksen er lest vil likevel være en fordel dersom det i tilfelle tvist er nødvendig å påberope datainstruksen.

Med de nye reglene vil alle virksomheter i praksis ha behov for slik instruks for å sikre forutberegnelighet og for å slippe å måtte slette forretningskritisk informasjon. Instrukser må imidlertid utformes slik at de ikke gir arbeidstaker dårligere vern mot urimelig kontroll enn forskriften gjør.

En datainstruks bør typisk sett inneholde:

- Rutiner for å sikre at virksomheten får tilgang til virksomhetsrelatert e-post ved fravær – eksempelvis ved videresending av e-post eller bruk av «fraværsassistent» i e-postsystemet ved fravær
- Instruks om hvordan e-poster og annen informasjon kan arkiveres, slik at virksomheten har tilgang til slik informasjon
- Rutiner for overlevering av dokumenter fra server etc., i tillegg til e-poster, når ansatte slutter
- Informasjon om hvordan personopplysninger behandles i virksomheten
- Særlige tiltak for å ivareta personvernet til arbeidstakere som slutter, i de tilfeller man ikke sletter reservekopier regelmessig.
- Det er viktig at virksomhetene lager rutiner som sikrer at informasjon sikres mot uønsket sletting i slike tilfeller.
- Instruksen kan gjøres kort, og suppleres med særskilte konkrete instrukser for hhv arkivering, rutiner for varsling og gjennomføring av innsyn, sletting og overlevering, samt maler som kan brukes for å dokumentere innsyn, varsling etc.
- En vedleggsliste kan for eksempel se slik ut:
    - Vedlegg 1: Arkiveringsinstruks
    - Vedlegg 2: Instruks om e-post under fravær
    - Vedlegg 3: E-post etc. ved avsluttet arbeidsforhold
    - Vedlegg 4: Erklæring om overlevering av e-post og elektronisk informasjon ved arbeidsforholdets opphør
    - Vedlegg 5: Instruks for innsyn i e-post og filer
    - Vedlegg 6: Mal for varsel om innsyn.

- Vedlegg 7: Mal for protokoll fra innsyn
- Vedlegg 8: Sikkerhetskopier: Innsyn og sletting
- Vedlegg 9: Sikkerhetsinstruks bruker

8 Overvåking

Personopplysningsforskriften kapittel 9 regulerer også overvåking av ansattes bruk av elektronisk utstyr, eksempelvis Internett. Dette er noe annet enn innsyn: Innsyn er noe som foretas i enkeltstående tilfeller og for konkrete formål, overvåking er en vedvarende og gjentatt automatisk aktivitet, jf. pol. § 36 som definerer fjernsynsovervåking som "vedvarende og regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotoapparat eller lignende apparat".

Virusscanning og lignende *sikkerhetstiltak* er tillatt, i den grad det er tillatt etter personopplysningsforskriften § 7-11, jf. § 9-2 if. Personopplysningsforskriften § 7-11 fritar *aktivitetslogger* i IT-systemer, eksempelvis brannlogger og e-postlogger, fra meldeplikt, på visse vilkår. Slik overvåking er tillatt, jf § 9-1 siste ledd, som forbyr all annen overvåking enn dette. Et eksempel på forbudt overvåking er saken vedrørende Bazar Forlag, se i 1.2 ovenfor. En slik overvåking faller klart utenfor det som er tillatt etter pof. § 7-11.

9 Riset bak speilet – overtredelsesgebyr fra Datatilsynet

Datatilsynet kan ilegge overtredelsesgebyr på inntil 10 G (728 810 kroner pr. 1. mai 2009) for overtredelser av personopplysningsloven og personopplysningsforskriften. Hjemmelen for å ilegge overtredelsesgebyr ble tatt inn som en ny § 46 i personopplysningsloven ved endringsloven av 9. januar 2009. Foreløpig finnes det ingen praksis om anvendelse av bestemmelsen. Ved vurderingen av om overtredelsesgebyr skal ilegges, og ved utmålingen, skal det etter pol. § 46 særlig legges vekt på

a) hvor alvorlig overtredelsen har krenket de interesser loven verner,
b) graden av skyld,

c) om overtrederen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen,
d) om overtredelsen er begått for å fremme overtrederens interesser,
e) om overtrederen har hatt eller kunne ha oppnådd noen fordel ved overtredelsen,
f) om det foreligger gjentakelse,
g) om andre reaksjoner som følge av overtredelsen blir ilagt overtrederen eller noen som har handlet på vegne av denne, blant annet om noen enkeltperson blir ilagt straff og
h) overtrederens økonomiske evne.

Det vil være meget interessant å følge med på hvordan denne hjemmelen brukes.

10 Vurdering av reglene

Formålet med reglene er å beskytte ansatte mot krenkelser av deres personvern, samtidig som arbeidsgivers interesser i virksomhetsrelatert informasjon skal sikres. Det kan med rette reises spørsmålstegn ved om denne målsetningen er nådd.

Det er uheldig at reglene ikke skiller mellom privat korrespondanse, som har EMK-vern, og virksomhetsrelatert korrespondanse. Hensynet til begge kommunikasjonspartneres personvern burde tilsi en slik beskyttelse. Forskriften skal brukes av arbeidsgivere uten kunnskap om EMK. Det er derfor uheldig at forskriften ikke beskytter privat informasjon bedre.

Virksomhetenes interesser er heller ikke tilstrekkelig ivaretatt. Dette er mest tydelig ved at reglene ikke anerkjenner den rolle e-post har i dagens arbeidsliv. Departementet ser ut til å mene at e-post kun er et forsendelsessystem. I næringslivet har e-postsystemer funksjon som kontraktsarkiv, vanlig postarkiv og felles hukommelse i tillegg til å være et forsendelsessystem. Vanlig post brukes nesten ikke. Reglene forutsetter at alle virksomheter har et effektivt fungerende elektronisk arkiv som brukes av alle ansatte, og at man alltid husker å arkivere alle virksomhetsrelaterte e-poster. Slik er ikke virkelighetens verden, og reglene om sletting ved arbeidsforholdets opphør kan, som illustrert, få store skadevirkninger.

Ved mistanke om pliktbrudd eller andre klanderverdige forhold vil prosedyrereglene sikre rettssikkerheten til den ansatte. Ved innsyn som foretas ved uplanlagt fravær, hvor man må håndtere innkommet e-post, synes disse prosedyrekravene å være unødig omstendelige.
Det er uheldig at det eneste unntaket fra kravene om sletting ved arbeidsforholdets opphør er knyttet til informasjon nødvendig for den "daglige drift", fordi dette utelukker informasjon som kan være virksomhetskritisk, men ikke nødvendig for daglig drift. Det utelukker også annen arkivverdig informasjon, eksempelvis korrespondanse forut for avtaleinngåelse.

Disse kravene til sletting må anses som en betydelig trussel mot virksomhetenes informasjonsverdier og kan få store skadelige følger. Virksomheter bør vurdere elektroniske arkivløsninger, ha rutiner for e-posthåndtering ved fravær, og sørge for en overlevering av slike dokumenter før ansatte slutter, for eksempel i form av en datainstruks.
Samtykke kan selvsagt bare gis på egne vegne og ikke på vegne av dem man kommuniserer med på e-post. Et eventuelt samtykke vil derfor bare kunne omfatte innsyn i dokumenter, og ikke i e-post eller annen elektronisk kommunikasjon. Dette gjelder i hvert fall privat kommunikasjon, og i slike tilfeller vil arbeidstakeren neppe kunne gi samtykke på vegne av private kommunikasjonspartnere.

For "ren" virksomhetsrelatert kommunikasjon, hvor både arbeidstakeren og kommunikasjonspartneren opptrer som virksomhetenes representanter, vil dette hensynet ha liten eller ingen betydning. Dersom arbeidstaker gir samtykke på egne vegne og gjør det klart at det er virksomhetsrelatert e-post, vil sterke grunner tale for at arbeidsgiver kan gjøre innsyn med hjemmel i lovens § 8 f), for kommunikasjonspartneres del. Her vil det være virksomhetens, og ikke privatpersonens, korrespondanse det er tale om.

For virksomhetsrelatert e-post, som antas å utgjøre mesteparten av den e-postkommunikasjon som skjer på jobben, vil hensynet til kommunikasjonspartneres personvern normalt ikke være noen aktuell problemstilling. I slike tilfeller er det underlig at samtykke fra ansatt til innsyn ikke skulle være et aktuelt behandlingsgrunnlag. Uoppfordret tilgang er noe annet enn samtykke. Etter min oppfatning er det en mangel ved forskriften at den ikke åpner for at frivillig samtykke fra

arbeidstaker skal være et mulig grunnlag for innsyn i virksomhetsrelatert kommunikasjon.

I enkelte eksisterende datainstrukser gir arbeidstakerne et generelt samtykke til innsyn i e-post. Et slikt samtykke vil ikke være rettsgyldig, verken etter personopplysningsloven eller de nye reglene, og slike instrukser bør revurderes.

Departementet har laget merknader til forskriften, som utfyller og kommenterer denne. Slike merknader er ingen tungtveiende rettskilde, selv om den praktiske betydningen kan bli stor. Departementet burde heller ha laget en ny forskrift og sendt denne på høring, enn å lage slike merknader.

Ut fra en totalvurdering må de nye reglene likevel anses som en forbedring i forhold til den tidligere rettstilstanden, som var preget av stor usikkerhet. Saksbehandlingsreglene må antas å ha betydning for å sikre arbeidstakeres personvern, samt å gi ryddigere forhold ved innsyn i e-post.