Overvåking av ansattes bruk av elektronisk utstyr

Digitale arbeidsverktøy kan registrere store mengder opplysninger om arbeidstakerne. Overvåking av arbeidstakeres elektroniske utstyr er derfor i utgangspunktet ulovlig. Denne veiledningen går gjennom når forbudet gjelder og hvilke unntak som finnes.

Innledning

For arbeidstakere kan det være utfordrende å vite hvilke opplysninger som blir samlet inn, hva som lagres og hvordan opplysningene blir brukt. Arbeidsgivere kan også bruke muligheten som ligger i disse verktøyene til å følge med på de ansatte.

I Norge har vi en egen forskrift som gjelder for arbeidsgivers innsyn i ansattes e-postkasse og annet elektronisk lagret materiale. Forskriften har et forbud mot overvåking av ansattes bruk av elektronisk utstyr. I denne veiledningen vil vi ta for oss når forbudet mot overvåking gjelder og hvilke unntak som finnes.

E-postforskriften § 2, andre avsnitt

"Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av Internett, med mindre formålet med overvåkingen er

a. å administrere virksomhetens datanettverk eller

b. å avdekke eller oppklare sikkerhetsbrudd i nettverket."

Forskriften inneholder også regler for når arbeidsgiveren har lov til å gjøre enkeltstående innsyn, noe vi har forklart nærmere i en egen artikkel.
[/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/]

Hvilke regelverk gjelder?

Det kan være vanskelig for arbeidsgivere å orientere seg når de skal innføre tiltak som kan innebære overvåking. Det er fordi det finnes mange regelverk som kontrollerer forskjellige sider ved arbeidslivet og arbeidstakernes digitale rettigheter.

De mest relevante regelverkene er:

- Personopplysningsloven med personvernforordningen
  [https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven]
  (Datatilsynet fører tilsyn)
- Reglene om kontrolltiltak i arbeidsmiljøloven kapittel 9
  [https://lovdata.no/dokument/SF/forskrift/2018-07-02-1108?q=forskrift%20e-post]
  (Arbeidstilsynet fører tilsyn)
- Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale, e-postforskriften
  [https://lovdata.no/dokument/SF/forskrift/2018-07-02-1108?q=forskrift%20e-post]
  (Datatilsynet fører tilsyn)

E-postforskriften gjelder både for nåværende og tidligere arbeidstakere. Hvem som er arbeidstakere er definert i arbeidsmiljøloven § 1-8. Bestemmelsen ble nylig endret, og har virkning fra 1. januar 2024. Da blir grensen mellom oppdragstakere og arbeidstakere tydeligere.

Arbeidsmiljøloven § 1-8. Arbeidstaker og arbeidsgiver (gjeldende fra 1. januar 2024)

"Med arbeidstaker menes i denne lov enhver som utfører arbeid for og underordnet en annen. Ved avgjørelsen skal det blant annet legges vekt på om vedkommende løpende stiller sin personlige arbeidskraft til disposisjon, og om vedkommende er underordnet gjennom styring, ledelse og kontroll. Det skal legges til grunn at det foreligger et arbeidstakerforhold med mindre oppdragsgiver gjør det overveiende sannsynlig at det foreligger et selvstendig oppdragsforhold.

Med arbeidsgiver menes i denne lov enhver som har ansatt en arbeidstaker som nevnt i første ledd. Det som i denne lov er bestemt om arbeidsgiver, skal gjelde tilsvarende for den som i arbeidsgivers sted leder virksomheten."

Overvåking av **oppdragstakere eller kunder**, er ikke omfattet av dette regelverket, og blir bare regulert av personopplysningsloven med personvernforordningen.

Ønsker innspill

Det er verdifullt for oss å få innspill fra aktører som leser veiledningen - både om innhold og hvilke øvrige problemstillinger eller praktiske situasjoner det er behov for veiledning om.

Innspillene kan sendes **innen 1. desember 2023** til innspill@datatilsynet.no [mailto:innspill@datatilsynet.no]
. Innspillene vil ikke besvares, men alt blir lest og vi vil ta det med oss i det videre veiledningsarbeidet på området.

Hva er omfattet av forbudet?

E-postforskriften gir arbeidstakere i Norge et særlig vern mot overvåking fra arbeidsgiveren. Her vil vi utdype hva som er omfattet av forbudet.

Det er bare i to tilfeller det vil kunne være lovlig å overvåke de ansattes bruk av elektronisk utstyr. I alle andre tilfeller vil det være ulovlig overvåking. Før vi går nærmere inn på disse to tilfellene, vil vi se på hva som er omfattet av forbudet.

E-postforskriften § 2, andre avsnitt

"Arbeidsgiver har ikke rett til å **overvåke** arbeidstakers bruk av **elektronisk utstyr**, herunder bruk av Internett, med mindre formålet med overvåkingen er

a. å administrere virksomhetens datanettverk eller

b. å avdekke eller oppklare sikkerhetsbrudd i nettverket."

(våre uthevinger)

Av lovteksten ser vi altså at:

1. tiltaket må gjelde arbeidstakeres "bruk av elektronisk utstyr"
2. tiltaket må være "overvåking"
3. arbeidsgiveren må dessuten få tilgang til opplysningene

Når vi bruker ordet "tiltak" i denne sammenhengen, mener vi alt en arbeidsgiver gjør som kan innebære overvåking. Dermed kan overvåkingen både foregå manuelt og automatisk.

Rettskilder

Det er få rettskilder som belyser hvordan denne bestemmelsen skal forstås. Uttalelser fra lovgiveren i forbindelse med innføring og endringer av forbudet, er nyttige for å forstå hvilke tiltak og teknologier som lovgiveren har ment å forby:

- Proposisjonen til personopplysingsloven 2018 – Prop. 56 LS (2017–2018) – med forslag til den gjeldende e-postforskriften (regjeringen.no) [https://www.regjeringen.no/no/dokumenter/prop.-56-ls-20172018/id2594627/]
- Merknader til tidligere bestemmelser om overvåking i personopplysningsforskriften, 2009 (pdf, regjeringen.no) [https://www.regjeringen.no/globalassets/upload/fad/vedlegg/personvern/epostforskriften_merknader_rev.pd id=2176744]
- Høringsnotat fra reglene ble innført i 2006, "Forslag til regler om arbeidsgivers tilgang til ansattes e-post mv." (pdf, regjeringen.no) [https://www.regjeringen.no/globalassets/upload/kilde/fad/hdk/2006/0011/ddd/pdfv/293858-horingsnotat_epost.pdf]

1. Tiltaket må gjelde arbeidstakeres "bruk av elektronisk utstyr"

Forbudet er knyttet til "bruk av elektronisk utstyr, herunder bruk av internett". Dette henger sammen med e-postforskriftens virkeområde.

E-postforskriften § 1. Virkeområde

"Forskriften her gjelder arbeidsgivers rett til innsyn i opplysninger lagret i

1. e-postkasse som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet
2. arbeidstakers personlige områder i virksomhetens datanettverk eller annet **elektronisk utstyr** som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet.

Bestemmelsene gjelder tilsvarende for innsyn i opplysninger som er slettet fra områder som nevnt i første ledd som finnes på sikkerhetskopier eller tilsvarende."

Elektronisk utstyr omfatter stort sett alt som ansatte bruker på arbeidsplassen, så lenge det er verktøy som samler inn eller kan brukes til å utlede personopplysninger. "Elektronisk utstyr" skal forstås vidt, og bestemmelsen er ment å være teknologinøytral. Også tekniske løsninger som utvikles i fremtiden er ment å skulle omfattes av disse reglene.

Elektronisk utstyr kan for eksempel være:

- Datamaskiner
- Nettbrett
- Mobiltelefoner
- Printere

Arbeidsgiveren må ha gitt arbeidstakeren utstyret med det formålet at det skal benyttes i arbeidet for at forskriften skal gjelde. Arbeidstakere som også bruker utstyret i privat sammenheng er likevel beskyttet av forskriften.

Selv om mobiltelefon også er elektronisk utstyr, har vi vurdert **lydopptak** av telefonsamtaler til å falle utenfor i denne sammenhenen
Les mer om lydopptak i arbeidslivet
[/personvern-pa-ulike-omrader/overvaking-og-sporing/lydopptak/spesielt-om-lydopptak-i-arbeidslivet/]

2. Tiltaket må være "overvåking"

Hva som ligger i "overvåke" er ikke definert i forskriften. Siden begrepet er så skjønnsmessig og ladet, er det utfordrende å gi klar veiledning. Ut fra forarbeidene, vanlig språkbruk, praksis og juridisk teori, vil vi derfor her gi en retning for hva vi som tilsynsmyndighet legger i å overvåke arbeidstakeres bruk av elektronisk utstyr.

En vanlig språklig forståelse av overvåking, innebærer at arbeidsgiveren samler inn informasjon om ansatte for å kartlegge atferd eller holdninger.

Bestemmelsen omfatter slik vi ser det både den innledende kartleggingen av bruken av elektronisk utstyr, så vel som gjennomgangen av personopplysningene. Dette betyr at også det å samle inn personopplysninger, for eksempel gjennom logging, er omfattet, selv om arbeidsgiveren ikke nødvendigvis går gjennom opplysningene.

Eksempel

Logging av aktivitet for sikkerhetsformål, er tiltak som samtidig gir arbeidsgiveren mulighet til å følge med på hva den ansatte gjør. Logging for å ivareta informasjonssikkerheten vil imidlertid ofte kunne være et lovlig tiltak, på grunn av unntaket for sikkerhetsformål.

En **teoretisk** mulighet for at opplysningene kan brukes til å kontrollere de ansatte er ikke tilstrekkelig for å kalle det overvåking. Tiltaket må være over en viss terskel.

Eksempel

En vanlig funksjon i samhandlingsverktøy er en indikator (for eksempel farge eller ikon) som viser om arbeidstakeren er pålogget, borte eller frakoblet.

I utgangspunktet er dette ikke overvåking. Dersom arbeidsgiveren aktivt går inn for å registrere den ansattes tilstedeværelse for å kontrollere vedkommende, kan det imidlertid utgjøre overvåking.

Når hovedformålet er å kontrollere arbeidstakerne

Tiltakene som har som hovedformål å kontrollere arbeidstakerne, er åpenbart lettest å kategorisere. Det kommer for eksempel mye programvare fra land med en annen personvernlovgivning enn vår – programvare som er spesialutviklet for å samle inn, analysere og tilgjengeliggjøre data om den enkelte ansatte. Slik programvare kalles også for sjefsvare ("bossware")
Les mer i Fafo-rapporten Digitalisering, personvern og tillitsvalgtes medvirkning 2023:12
[https://www.fafo.no/zoo-publikasjoner/fafo-rapporter/digitalisering-personvern-og-tillitsvalgtes-medvirkning]
)

Sjefsvare kan måle arbeidstakernes følelser, tanker og meninger gjennom:

- opptak fra webkamera
- automatisk gjennomgang av meldinger i interne chattekanaler

Sjefsvare kan måle arbeidsutførelse gjennom:

- antallet tastetrykk på datamaskinen i løpet av en bestemt tidsperiode,
- hvilke applikasjoner som er benyttet
- bruk av sosiale media i arbeidstiden

De ansattes opplevelse av tiltaket

For tiltak som ikke har overvåking som hovedformål, er de ansattes opplevelse av å være overvåket et viktig moment i vurderingen av om tiltaket kan kalles overvåking.

Eksempel

En veiledningssak Datatilsynet hadde med LO og Abelia, gjaldt en virksomhet som arbeidet med kundeservice, og som gjorde skjermopptak av arbeidstakernes pc. Formålene med skjermopptakene var kompetanseheving og opplæring. Opptak ble bare gjort i 2,5 prosent av tiden, men de ansatte ble varslet om mulig opptak i 25 prosent av tiden.

I veiledningen la vi vekt på at det ikke var mulig for de ansatte å vite hvilke tidspunkt opptakene faktisk skjedde i. Vi la dessuten vekt på at den varslede tiden på 25 prosent utgjorde en betydelig del av arbeidsdagen. Siden tiltaket var utformet på en måte som kunne gi de ansatte en følelse av å være overvåket, mente vi at tiltaket ikke var i samsvar med e-postforskriften.

Tiltaket må ha en viss varighet

For at tiltaket skal defineres som overvåking, må det dessuten ha en viss varighet eller det må skje gjentatte ganger. Enkeltstående innsyn i e-post, vil derfor ikke defineres som overvåking, mens hyppige enkeltstående innsyn kan

tenkes å kunne defineres som overvåking.

Eksempel

Automatisk videresending av e-post regnes som overvåking av elektronisk utstyr, fordi det er kontinuerlig. Formålet med videresendingen er ofte å ivareta kundeforhold når arbeidstakere er fraværende.

Det er viktig for arbeidsgivere å være klar over at kundeforhold ikke er ett av unntakene som gjør automatisk videresending lovlig. Kundeforhold kan derimot forsvare enkeltstående innsyn-

Les mer om dette i artikkelen om arbeidsgiverens innsyn i epost og filer.
[/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/nar-er-innsyn-lovlig/]

3. Arbeidsgiveren må ha tilgang til personopplysningene

Den tredje delen av forbudet går ut på at arbeidsgiveren må ha tilgang til personopplysningene som behandles gjennom tiltaket.

Eksempel

I sandkasseprosjektet Secure Practice vurderte vi hvordan et verktøy som skulle profilere ansatte med formål å gi tilpasset opplæring i informasjonssikkerhet, kunne utformes
[/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/secure-practice---sluttrapport/kan-ki-verktoyet-tas-i-bruk-og-videreutvikles-lovlig/]
.

Anbefalingen fra sandkassa var å hindre at arbeidsgiveren fikk tilgang til opplysningene om hver enkelt ansatt. Så lenge både kontrakten mellom arbeidsgiveren og Secure Practice, samt tekniske tiltak hindret arbeidsgiveren i å vite hvilken interesse eller kunnskap enkeltansatte hadde om informasjonssikkerhet, var ikke tiltaket forbudt.

Med andre ord må arbeidsgiveren ha mulighet til å få tilgang til opplysninger om de ansatte, for at tiltaket skal være forbudt.

Unntak fra forbudet

I e-postforskriften er det som nevnt kun definert to tilfeller der tiltak som innebærer overvåking av ansattes bruk av elektronisk utstyr, vil kunne være lovlig.

De eneste tilfellene der overvåkingen vil være lovlig, er altså når:

1. tiltaket skal administrere virksomhetens datanettverk, eller
2. tiltaket skal avdekke eller oppklare sikkerhetsbrudd i nettverket.

Forskriften er tydelig på at overvåkingen bare er lovlig for disse to formålene. Dersom overvåkingen skjer for andre formål, uansett hvor aktverdige disse er, vil den være ulovlig.

Vilkårene i unntakene er ikke nærmere forklart, og må derfor forstås ut fra ordlyden og formålet med bestemmelsen. Unntakene må dessuten tolkes i lys av personvernforordningen, særlig prinsippene om dataminimering [/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/dataminimering/] og formålsbegrensning [/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/] .

Prinsippet om dataminimering innebærer at arbeidsgiveren alltid må vurdere hvilke opplysninger som er egnet og nødvendige for å oppnå et av de to lovlige formålene med overvåkingen. Prinsippet om formålsbegrensning forbyr arbeidsgiverne å bruke opplysningene til nye formål som er uforenelige med det opprinnelige.

Eksempel

En arbeidsgiver har gjennom logging hentet inn opplysninger om hvilke internettsider de ansatte besøker. Formålet er å ivareta informasjonssikkerheten. Det vil da være forbudt å bruke opplysningene som er samlet inn til å samtidig undersøke om arbeidstakeren har oppfylt pliktene sine etter arbeidsavtalen.

1. "Å administrere virksomhetens datanettverk"

Det første unntaket gjelder overvåking av de ansattes bruk av elektronisk utstyr for å administrere virksomhetenes datanettverk.

Ut fra en språklig forståelse må vilkåret antas å omfatte alle praktiske og tekniske tiltak som er nødvendige for at systemene, nettverk, utstyr og programvare skal fungere.

Emsempel

En arbeidstaker trenger brukerstøtte og gir samtykke til å dele skjerm med IT-personellet. Et slikt tiltak vil omfattes av unntaket om å administrere virksomhetens datanettverk.

Når arbeidstakeren gir samtykke til skjermdeling i de tilfellene behovet oppstår, er det imidlertid tvilsomt om tiltaket i det hele tatt utgjør overvåking.

2. "Å avdekke eller oppklare sikkerhetsbrudd i nettverket"

Med "sikkerhetsbrudd" forstår vi brudd på informasjonssikkerheten generelt. Det er vanlig å si at det handler om å sikre at informasjon i alle former:

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Informasjonssikkerhet omfatter dermed mer enn personopplysningssikkerhet som er regulert i artikkel 32 til 34 i personvernforordningen.

For å oppnå informasjonssikkerhet må virksomheten identifisere risikoer informasjonsverdiene er utsatt for, og planlegge og gjennomføre egnede tiltak som skal redusere risikoene til et akseptabelt sikkerhetsnivå for virksomheten.

Les mer om informasjonssikkerhet og personopplysningssikkerhet, slik det er regulert i personvernregelverket. [/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/]

Begrepene å "avdekke" eller "oppklare" innebærer etter vårt syn verktøy som motvirker sikkerhetsbrudd, og bruk av logger og lignende til etterarbeidet med å oppklare sikkerhetsbrudd.

Spamfilter

Et spamfilter identifiserer både virus og andre typer skadelig programvare. E-post som blir identifisert som spam, blir lagt i karantene og er ikke synlig for arbeidstakeren.

Så lenge e-posten ligger i karantene er den synlig for "admin" hos arbeidsgiveren. Aktuelle virkemidler for å begrense inngrepet i personvernet ved bruk av spamfilter, er å begrense tilgangen til spamfilteret til så få administratorer som mulig, utarbeide tydelige rutiner for hvordan administratorene skal utføre arbeid med spamfilteret, og logge administratorenes innsyn i spamfilteret slik at virksomheten kan avdekke eventuell snoking.

Logging

Logging er å holde oversikt over både pågående og tidligere hendelser i virksomhetens systemer. Det innebærer for eksempel at et selskap følger med på inn- og utgående trafikk i nettverket sitt for å avdekke unormal trafikk og potensielle angrep på nettverket.

Eksempler på logging kan være:

- Brannmur. Her logges trafikken i virksomhetens nettverk. Det vil si alle IP-adresser en arbeidstaker er inne på. Innsyn i denne loggen kan utgjøre overvåking, fordi innsynet gir oversikt over arbeidstakers bruk av elektronisk utstyr over tid.
- Loggføring av aktivitet/tilgangsstyring. Dette innebærer loggføring av hvem som går inn på tilgangsstyrte mapper i virksomhetens systemer, og når de har vært inne. For eksempel vil det være nødvendig i helsesektoren å overvåke når ansatte har vært inne i journaler.

Les mer om logging på Nasjonal sikkerhetsmyndighet sine nettsider (nsm.no)
[https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-beskyttelse-av-skjermingsverdig-ugradert-informasjonssystem/informasjonssystemsikkerhet/sikker-drift-og-hendelseshandtering/logging/]

Data loss prevention

Datatilsynet mottar ofte spørsmål om bruken av "data loss prevention"-verktøy (også kalt datatapsteknologi på norsk). Dette er verktøy som overvåker tilgang til, eksport av og endring av informasjon. Informasjonen som beskyttes kan for eksempel være forretningshemmeligheter eller annen virksomhetskritisk informasjon. Slike funksjoner aktiveres som regel av en arbeidsgiver med det formål å forhindre at ansatte tar med seg viktig informasjon ut av virksomheten, for eksempel i forbindelse med avslutning av arbeidsforhold.

Dersom virksomheten har innført et slikt verktøy etter en forutgående risikovurdering
[/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/]
, kan forskriften åpne for en slik bruk. En viktig forutsetning er at verktøyet er nødvendig for å oppnå et akseptabelt nivå av risiko

Sjekkliste for arbeidsgiveren

Vi har laget en kort oppsummering / sjekkliste dere kan gå gjennom dersom dere er usikre på om tiltaket dere vurderer å innføre vil være omfattet av forbudet mot å overvåke arbeidstakeres elektroniske utstyr.

1. Innebærer tiltaket behandling av personopplysninger [/rettigheter-og-plikter/personopplysninger/] ?

Hvis ja: Tiltaket må oppfylle de generelle kravene i personopplysningsloven og personvernforordningen. Gå videre til punkt 2.
Hvis nei: Reglene i personvernregelverket gjelder ikke.

2. Omfatter tiltaket:

- arbeidstakeres bruk av elektronisk utstyr, herunder internett?
- overvåking?
- at arbeidsgiveren får tilgang til opplysningene?

Hvis ja på alle disse: Gå videre til punkt 3.
Hvis nei på ett eller flere: Tiltaket omfattes ikke av forbudet mot overvåking i e-postforskriften, men må oppfylle de generelle kravene i personopplysningsloven med personvernforordningen.

3. Skjer overvåkingen for noen av disse formålene:

- Administrere virksomhetens datanettverk?
- Avdekke eller oppklare sikkerhetsbrudd i nettverket?

Hvis ja på et av disse: Unntaket er oppfylt. Tiltaket er lovlig, så lenge det oppfyller kravene i personvernforordningen.
Hvis nei: Tiltaket er ulovlig.

Råd til arbeidsgiveren og arbeidstakeren

For arbeidsgiveren

1. Vurder om tiltaket er lovlig, også dersom dere tar i bruk hyllevare.
2. Sett dere inn i hva innebygd personvern er
[/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern-og-personvern-som-standard/]
.
3. Vurder personvernkonsekvensene (DPIA) for arbeidstakerne (artikkel 35 i personvernforordningen)
[/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/]
. Hvis det behandles personopplysninger for systematisk monitorering av ansatte, for eksempel overvåking av ansattes internettaktivitet, elektroniske kommunikasjon og kameraovervåking, må virksomheten gjennomføre en DPIA.

Merk at dette blant annet også innebærer å:
- innhente synspunkter fra de ansatte eller deres representanter (artikkel 35 nr. 9)
- rådføre dere med personvernombudet, dersom dere har det (artikkel 35 nr. 2)

4. Vurder av informasjonssikkerheten
[/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/]
før dere setter i gang tiltak for sikkerhetsformål.
5. Undersøk om drøfting med de tillitsvalgte er pålagt i tariffavtalen, dersom dere har inngått en.
6. Undersøk om tiltaket er et kontrolltiltak etter arbeidsmiljøloven, slik at det er påbudt å drøfte tiltaket med de tillitsvalgte.
7. Gi informasjon til de ansatte.
[/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/]
En arbeidsgiver har plikt til å informere de ansatte om hvilke opplysninger som blir registrert.

For arbeidstakerne

1. Sett dere inn i ny teknologi og grunnleggende regler for personvern, slik at dere kan gi gode innspill til arbeidsgiveren
2. Gjør deg kjent med rettighetene dine etter personvernforordningen.
[/rettigheter-og-plikter/den-registrertes-rettigheter/]
3. Dersom arbeidsgiveren din planlegger å innføre tiltak, og du er usikker på lovligheten, kan du:
   - ringe veiledningstjenesten vår
   [/om-datatilsynet/kontakt-oss/]
   og få råd.
   - kontakte Arbeidstilsynet
   [https://www.arbeidstilsynet.no/kontakt-oss/]
   - kontakte tillitsvalgte dersom du er organisert

Dersom du mener at arbeidsgiveren overvåker deg ulovlig, har du mulighet til å klage til Datatilsynet
[/om-datatilsynet/kontakt-oss/klage-til-datatilsynet/]
.