KAPITTEL 4

Droner og personvern

Elisabeth Krauss-Svensrud og Helge Veum

Du sitter på plenen din og nyter en fortjent fridag når du hører en irriterende summing over hustaket. Du ser opp og finner raskt ut at lyden ikke stammer fra et stort insekt. Over eiendommen din henger en drone. Du er både forstyrret og du vet at dronene stort sett har et kamera, og du trives slett ikke med at noen du ikke vet hvem er, trolig filmer deg der hvor du forventer å være i fred. Dette er allerede virkeligheten for mange som blir utsatt for dronepiloter som ikke tar nok ansvar og hensyn. Selv om teknologien er fascinerende, er det ikke alle som lar seg fascinere.

La oss ta et annet scenario frem i tid. Dronene er så små at vi ikke nødvendigvis merker at de er nær oss. De kommer i svermer og er rundt oss sammen med mer naturlige insekter. De observerer ved hjelp av ulike sensorer, selvfølgelig lyd og bilde, men også mer avanserte sensorer som blant annet henter informasjon fra mobilen vår. De kan identifisere oss og følge oss der vi beveger oss. De kan registrere hva vi sier, hva vi gjør og hvem vi er sammen med. Dronene tilhører staten. Om landets styre ikke lenger er like godt på lag med innbyggerne som dagens norske samfunn, er det mulig å se at dronens inntog kan føre med seg et overvåkningssamfunn ingen av oss ønsker.

Forhåpentligvis vil vi ikke ende opp i et samfunn som skissert ovenfor. Men vi kommer til å ta mange steg i en slik retning. Stegene kommer til å være rasjonelle sett opp mot behovet for å effektivisere, sikre og trygge samfunnet vårt. Som for eksempel:

- Søk etter savnede personer
- Politiets spaning

- Trafikkovervåkning
- Trafikkontroll av den enkelte bilist
- Terrorovervåkning

Bruk av droner i regi av staten er derfor et område som vi særlig må balansere mot den enkelte borgers personvern og privatliv.

I det følgende skal vi forklare hva personvern er, og hvilke lover vi har i Norge som har til formål å ivareta personvernet vårt. Deretter skal vi se nærmere på når personvernreglene gjelder ved bruk av droner og hvilke grunnleggende krav personvernreglene stiller til den som skal fly med drone. Vi vil også se på hvilke regler som gjelder ved deling av film- og bildemateriale fra drone.

Deretter skal vi beskrive fem personvernutfordringer vi ser ved dagens dronebruk, før vi avslutter med å gi noen anbefalinger som kan bidra til et bedre personvern ved bruk av droner. Til slutt i dette kapitlet har vi samlet det vi mener er de sentrale lovhenvisningene i personvernregelverket ved bruk av drone. Alle norske lovtekster finner du i sin helhet på www.lovdata.no.

Hva er personvern?

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Alle mennesker har en ukrenkelig egenverdi. Som enkeltmenneske har du derfor rett på en privat sfære som du selv kontrollerer, hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker (Datatilsynet 2016). Dette prinsippet er blant annet forankret i Den europeiske menneskerettighetskonvensjonen, hvor det i artikkel 8 heter:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse» (Menneskerettsloven 1999).

I Norges Grunnlov er også personvern tatt inn i § 102:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.»

Personvern er ikke bare en viktig menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet og privatliv. Personvern er

også viktig for å sikre felles goder i et demokratisk samfunn. Uten retten til å ha et privatliv vil det ikke være mulig for det enkelte menneske å skape seg et rom til å utvikle refleksjoner og vurderinger på et selvstendig grunnlag, uten å bli forstyrret eller kontrollert av andre (Datatilsynet 2016).

Et dårlig ivaretatt personvern vil også sette demokratiet i fare ved at borgerne begrenser sin deltakelse i åpen meningsutveksling og politisk aktivitet. Den enkelte kan frykte at opplysninger om personlige forhold kan bli trukket frem og gjort til allmenn oppmerksomhet. Man kan også sette begrensninger på seg selv fordi man frykter at myndighetene registrerer og lagrer opplysninger om ens kommunikasjon med andre, ens ferdsel, interesser eller uttrykk for holdninger (Datatilsynet 2016).

Personvernbegrepet refererer ikke bare til vernet av privatlivets fred og den enkeltes personlige integritet. I norsk forståelse innebærer begrepet i stor grad også vernet av individers rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Den enkelte skal i størst mulig grad kunne bestemme over egne personopplysninger (Datatilsynet 2016).

Det er flere prinsipper knyttet til personvern, og de fleste av dem er relevante i forbindelse med hvordan vi tar i bruk droner i samfunnet vårt. Datatilsynet har beskrevet de følgende prinsippene:

- Privatlivets fred og personlig integritet
- Samtykke
- Proporsjonalitet
- Formålsbestemthet
- Relevans og prinsippet om å samle inn et minimum av opplysninger
- Fullstendighet og kvalitet
- Informasjon og innsyn
- Informasjonssikkerhet
- Anonymitet og sporfri ferdsel

Vi har ikke rom for å gå gjennom prinsippene i detalj her, men de ligger til grunn i vurderingene videre i kapitlet. Og du kan lese mer om personvern på Datatilsynets nettsted.[3]

3 Se www.datatilsynet.no/om-personvern/hva-er-personvern/

Hvilke norske lover er ment å ivareta personvernet vårt?

Retten til privatliv, familieliv og vern av vår korrespondanse er nedfelt i Den europeiske menneskerettighetskonvensjonen og i den norske Grunnloven. Begge disse regelsettene er bindende for norske myndigheter. Det betyr at den norske stat er forpliktet til å vedta norske lover som skal beskytte den enkelte mot at deres personvern blir krenket.

Personopplysningsloven og personopplysningsforskriften utgjør det generelle norske regelverket som har til formål å beskytte fysiske personer mot at personvernet blir krenket. I 2018 skjer en stor oppdatering av dette regelverket. Da blir EUs forordning for personvern norsk lov (Regulation (EU) 2016/679, 2016). Det betyr at vi får nye regler for personvern i Norge som gir både offentlige og private virksomheter nye plikter, og enkeltpersoner får nye rettigheter.[4]

Både dagens personopplysningslov og EUs nye forordning for personvern er teknologinøytrale. Det avgjørende for om reglene gjelder, er i hovedsak knyttet til om det skjer en behandling av personopplysninger. Det er med andre ord ikke av betydning hva slags teknologi som brukes til å samle inn personopplysningene, eller i hvilket samfunnsområde det skjer innenfor. De generelle reglene om personvern har dermed et svært vidt nedslagsfelt.

Når gjelder personvernreglene ved bruk av droner?

Ved bruk av drone gjelder de generelle personvernreglene når dronen behandler personopplysninger. Begrepet «behandling av personopplysninger» er derfor sentralt og krever nærmere forklaring.

En personopplysning er alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Dette er en vid definisjon. Dersom for eksempel

4 Personvernforordningen skal gjennomføres «som sådan» i norsk rett, jf. EØS-avtalen artikkel 7 (a). Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett, ble sendt på høring sommeren 2017. Personvernforordningen er forventet å tre i kraft i Norge i løpet av mai 2018. Det er mulig å lese mer om de nye personvernreglene på Datatilsynets nettside.

droner tar bilder som kan identifisere en person, vil det skje en behandling av personopplysninger. Det samme gjelder også dersom dronen samler inn andre opplysninger som kan knyttes til en enkeltperson, som for eksempel lokasjon, bosted, biometriske kjennetegn eller registreringsnummer på en bil. Det avgjørende er om det er mulig å identifisere en eller flere personer i dataene som dronen har samlet inn. Hvis det er mulig, er det personopplysning.

En behandling av personopplysninger er enhver bruk av personopplysninger. Eksempler på ulike behandlinger kan være innsamling, registrering, analyse, lagring eller utlevering av personopplysninger. Ved bruk av drone kan det på kort tid skje flere ulike behandlinger av personopplysninger. For eksempel vil det skje både en innsamling og utlevering av personopplysninger der du først gjør et filmopptak av enkeltpersoner fra lufta, og hvor filmen etterpå deles på internett.

Vi kan på denne bakgrunn slå fast at personvernreglene gjelder ved bruk av drone hvis filmen, bildet eller andre typer data som dronen registrerer (sensordata, lokasjonsdata mv.), inneholder personopplysninger. Siden mye bruk av drone skjer i nærheten av der enkeltpersoner bor og oppholder seg, vil personvernreglene i utgangspunktet gjelde og dermed påvirke hva som er lovlig bruk av drone i Norge i dag.

Personvernreglene gjelder ikke ved journalistisk virksomhet

De fleste regler gjelder imidlertid ikke uten unntak, og noen typer behandling av personopplysninger som skjer ved hjelp av en drone, er unntatt fra personvernreglene. Det er særlig to tilfeller som er unntatt. Det første unntaket knytter seg til behandling av personopplysninger som skjer for litterære, kunstneriske, journalistiske og akademiske formål (Regulation (EU) 2016/679, 2016). Dette unntaket er begrunnet i ytringsfrihet, og innebærer for eksempel at en journalist som bruker drone for å dekke en nyhetssak, ikke må følge personvernreglene. Journalisten må for eksempel ikke ha samtykke fra den eller de som er avbildet, for å offentliggjøre et bilde som er tatt ved hjelp av drone.

Selv om journalister ikke må følge personvernreglene når de bruker personopplysninger i sin journalistiske virksomhet, må vi likevel presisere

at journalister som regel er underlagt andre retningslinjer som sier noe om hva slags bilder eller informasjon som er etisk riktig å offentliggjøre. For eksempel inneholder Vær Varsom-plakaten slike regler.

Personvernreglene gjelder ikke ved privat bruk av droner

Det andre viktige unntaket fra personvernreglene knytter seg til behandling av personopplysninger som utføres av fysiske personer som ledd i rent personlige eller familiære aktiviteter (Regulation (EU) 2016/679, 2016). Flyr du drone på hobbybasis, og du kun bruker filmopptak eller bilder av enkeltpersoner i privat sammenheng, omfattes ikke en slik behandling av personvernreglene.

Bakgrunnen for dette unntaket er begrunnet i at det fremstår som et uønsket inngrep i den enkeltes privatliv om staten skulle vedta regler som åpner for kontroll med hvordan privatpersoner bruker personopplysninger rent privat. Samtidig er personvernkonsekvensene av denne formen for privat behandling av personopplysninger som regel beskjedne.

Et typisk eksempel på situasjoner hvor dette unntaket fra personvernreglene gjelder ved bruk av drone, er hvis du arrangerer en grillfest i din egen hage og bruker drone til å ta film av venner og familie som er til stede på festen.

Selv om denne typen rent personlig eller familiær behandling av personopplysninger ikke er omfattet av personvernreglene, er det likevel viktig å være klar over at det gjelder strenge regler for deling og publisering av bilder og film, for eksempel på internett. Disse reglene vil se nærmere på seinere i dette kapitlet.

Det er videre ofte en risiko for at denne typen bruk av drone oppleves invaderende eller krenkende for andre mennesker, selv om dronepiloten ikke nødvendigvis tar bilde eller film av andre. En slik misforståelse oppstår gjerne fordi personer som ser dronen, ikke vet hvorfor dronen er der, hvem som eier den, eller om den samler inn personopplysninger. I slike tilfeller er det viktig at dronepiloten tar hensyn til at andre kan føle seg overvåket.

Et annet viktig poeng er at selv om personvernreglene ikke gjelder ved behandling av personopplysninger til rent personlige eller familiære akti-

viteter, kan slik aktivitet være ulovlig etter andre regelverk. For eksempel kan bruk av drone være ulovlig etter luftfartsregler (Forskrift om luftfartøy som ikke har fører om bord mv. (2015). Bruken av dronen kan også være ulovlig etter regler i straffeloven. For eksempel der bruken av drone innebærer en krenkelse av privatlivets fred (§ 266) eller annen hensynsløs adferd (§ 267) (Straffeloven 2005). Hvis noen opplever slik droneaktivitet, bør politiet kontaktes.

Det er den personen som bruker dronen, som alltid er ansvarlig for å holde seg informert om hvilke regler som til enhver tid gjelder for sin egen dronebruk. Hvis dronepiloten ikke overholder gjeldende regelverk, kan det medføre både pålegg og bøter.

Hvilke krav stiller personvernreglene til den som skal fly med drone?

Vi har så langt sett på hvilke generelle regler for personvern vi har i Norge, og når disse reglene gjelder ved bruk av drone. Nå skal vi gå et steg videre og se på hvilke krav personvernreglene stiller til den som skal fly med drone. Vi presiserer at denne fremstillingen ikke er en uttømmende gjennomgang av alle krav som finnes i personvernreglene. Hensikten er å vise de viktigste kravene personvernreglene stiller til den som skal bruke drone.

Som utgangspunkt kan du tenke deg følgende scenario: Et eiendomsmeglerfirma benytter seg av en drone for å lage en video som skal vise frem et hus. Dronen flyr et godt stykke over huset og filmer bygningen, eiendommen for øvrig og nabolaget rundt. På den ene siden av huset kan man se bilen til naboen og alle lekene som ligger i hagen, mens på den andre siden ser man tydelig en annen nabo gå ut av huset sitt og inn i bilen. Filmen samles inn gjennom et innebygd kamera på dronen og lagres i en skytjeneste som eiendomsmeglerfirmaet bruker. I dette scenarioet er fokuset til dronen rettet mot huset som skal selges, og ikke omgivelsene rundt. Likevel, fordi dette skjer i et tettbebygd område, vil filmen inkludere bilder av naboene og deres eiendommer. I et slikt tilfelle vil eiendomsmeglerfirmaet derfor behandle personopplysninger, og virksomheten vil ha en plikt til å behandle disse personopplysningene i samsvar med kravene i personvernreglene.

Når det er klart at eiendomsmeglerfirmaet behandler personopplysninger ved sin bruk av drone, er det neste virksomheten må gjøre, å foreta en vurdering av om kravene for behandling av personopplysninger er oppfylt (Regulation (EU) 2016/679, 2016). Disse kravene er som følger:

- Virksomheten må ha et behandlingsgrunnlag.
- Personopplysninger skal bare brukes til bestemte formål.
- Virksomheten kan ikke samle inn flere personopplysninger enn nødvendig.
- Personopplysningene skal være korrekte og oppdaterte, og ikke lagres lenger enn nødvendig.
- Virksomheten skal gi de registrerte informasjon og innsyn.
- Personopplysningene skal behandles på en informasjonssikker måte.
- Virksomheten skal bruke innebygd personvern som standardløsning.

Behandlingsgrunnlag

Mulige behandlingsgrunnlag ved behandling av personopplysninger kan være:

- det er fastsatt i lov at det er adgang til slik behandling,
- den det har blitt samlet inn opplysninger om samtykker til det,
- det er nødvendig for å oppfylle en avtale med den registrerte,
- det er nødvendig for å kunne oppfylle en rettslig forpliktelse,
- det er nødvendig for å vareta den registrertes vitale interesser,
- det er nødvendig for å utføre en oppgave av allmenn interesse,
- det er nødvendig for å utøve offentlig myndighet, eller
- det er nødvendig for å vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Hvilket behandlingsgrunnlag som legitimerer innsamlingen av personopplysninger i forbindelse med bruk av droner, må vurderes helt konkret i hvert enkelt tilfelle. I vårt tenkte eksempel over, vil det være mulig å be naboene om samtykke til at det filmes. Da kan de selv ta stilling til om de ønsker dette. Dette utelukker imidlertid ikke at et av de andre behandlingsgrunnlagene kan legitimere dronebruken for eiendomsmeglerfirmaet.

Personopplysninger kan bare brukes til bestemte formål

Det er bare lov til å behandle personopplysninger som er samlet inn til uttrykkelige angitte formål, og disse formålene må være saklig begrunnet i virksomheten. Det er ikke lov til å benytte opplysningene til andre formål. Virksomheten må altså definere på forhånd hva som er formålet med innsamlingen av personopplysninger. I eksempelet over er formålet å lage en film i forbindelse med salg av bolig. Det betyr at opplysningene bare kan benyttes i forbindelse med selve salget og ikke til andre formål.

Det er ikke tillatt å samle inn flere personopplysninger enn nødvendig

Den som flyr dronen, må sette i verk tiltak som gjør at det samles inn færrest mulig personopplysninger. Dette kan blant annet gjøres ved å fly på tidspunkt hvor det er få mennesker til stede, bruke kun de nødvendige sensorene (for eksempel unngå video hvis det ikke er nødvendig), bruke anonymiseringsteknikker (sladding av ansikter og registreringskilter) og slette unødvendige personopplysninger automatisk.

Personopplysninger skal ikke lagres lenger enn nødvendig

Etter personvernreglene er det ikke lov å lagre personopplysninger lenger enn det som er nødvendig for å oppnå formålet med innsamlingen. Hvis formålet er å selge huset som filmes, må personopplysningene som utgangspunkt slettes når huset er solgt. Da er formålet med innsamlingen oppnådd, og det vil ikke lenger være nødvendig å lagre personopplysningene.

Informasjon og innsyn

En stor utfordring for virksomheter som tar i bruk droner, er å få gitt tilstrekkelig informasjon til de personene som blir filmet. Dersom bruken av drone medfører at virksomheten samler inn personopplysninger, har virksomheten en plikt til å informere de enkeltpersonene som får sine per-

sonopplysninger registrert. Det betyr at det blant annet skal informeres om hvem som flyr dronen og hvorfor (til hvilket formål) personopplysningene samles inn.

Det finnes flere måter å nå ut med informasjon til folk som blir fanget opp av en drone. For eksempel kan du bruke flyers eller annet informasjonsmateriale, informasjon på virksomhetens hjemmeside, beskjed gjennom media eller sosiale medier. Det er virksomheten som er ansvarlig for å gi klar og tydelig informasjon til de berørte. Informasjonen skal være lett forståelig og lett tilgjengelig.

En annen grunnleggende rettighet som er nært knyttet til informasjonsplikten, er innsynsretten. De som blir filmet, har rett til innsyn i de personopplysningene som lagres om dem. Det betyr at virksomheter som bruker droner, må utarbeide rutiner for hvordan de skal oppfylle denne retten hvis en person henvender seg til dem og ber om innsyn i egne personopplysninger.

Informasjonssikkerhet

Alle virksomheter som samler inn personopplysninger ved hjelp av drone, må sørge for tilfredsstillende informasjonssikkerhet. Det betyr at det skal iverksettes planlagte og systematiske tiltak for å sikre opplysningenes konfidensialitet, integritet og tilgjengelighet.

Privacy by design

Privacy by design, eller innebygd personvern, betyr at det skal tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Ved å sørge for innebygd personvern i droner minimeres innsamlingen og lagringen av personopplysninger, og personvernkonsekvensene reduseres. I tillegg vil det være mye lettere for virksomhetene som skal ta i bruk disse systemene at personvernkonsekvensene er tenkt ut på forhånd, fremfor at man må justere på dette i etterkant. Datatilsynet har laget eget veiledningsmateriell som skal hjelpe norske virksomheter å forstå og etterleve kravet om innebygd personvern i personvernforordningen (Datatilsynet 2017).

Særlig om systemleverandører

Bruk av drone forutsetter bruk av et styringssystem. Slike styringssystemer gir en rekke muligheter for styring av dronen og for lagring av informasjon som samles inn. Lagring av personopplysninger i slike systemer vil kunne innebære en utlevering av opplysninger til en tredjepart. Dette betyr at virksomheter som tar i bruk slike styringssystemer, må finne ut av to ting: Vil leverandøren av styringssystemet være å anse som en databehandler? Innebærer bruken av styringssystemet en overføring av personopplysninger til utlandet?

Dersom leverandøren av styringssystemet behandler personopplysninger på vegne av virksomheten, vil leverandøren være å anse som en databehandler. Det må i så fall inngås en databehandleravtale (Datatilsynet 2017). Dersom bruk av styringssystemet innebærer at det blir overført personopplysninger til utlandet, er det viktig å sjekke at det aktuelle landet sikrer en forsvarlig behandling av personopplysningene. I utgangspunktet er det kun land innenfor EU/EØS-området som kan anses å sikre en forsvarlig behandling. Skal du overføre personopplysninger til land utenfor EU/EØS, må du i visse tilfeller ha tillatelse fra Datatilsynet (Datatilsynet 2016). Det er derfor viktig at virksomheten undersøker hva som er aktuelt for dem.

Regler for offentliggjøring av personbilder

Selv om et filmopptak fra en drone er lovlig tatt opp, for eksempel et filmopptak fra en grillfest i din egen hage, må du likevel som hovedregel ha samtykke fra de som er filmet hvis du vil dele filmen med andre (Datatilsynet 2017).

Når du skal dele eller publisere bilder eller film der personer er motivet, må du forholde deg til både personopplysningsloven og åndsverkloven. I tillegg bør du vurdere om det er etisk riktig å videreformidle bildene eller filmene. Hvis det oppstår en konflikt, er det den som har delt bildene eller filmen, som må bevise at et frivillig, uttrykkelig og informert samtykke til deling virkelig er gitt (Datatilsynet 2017).

Skal du publisere bilder som viser en eller flere bestemte personer (altså bilder der personene er hovedmotivet), på nett eller dele dem med andre (selv om det er i lukkede grupper), må du ha samtykke fra den eller de som er avbil-

det før bildet publiseres. Dette gjelder også film, og det gjelder enten du har tatt bildene eller bare videreformidler dem. Dersom det gjelder bilder av barn eller andre personer som ikke kan gi gyldig samtykke selv, må foresatte eller verger eventuelt gi samtykke på vegne av dem det gjelder (Datatilsynet 2017).

Samtykke skal hentes inn før offentliggjøringen. Publiserer du familiebilder eller festbilder av omgangskretsen, må du derfor ha samtykke fra alle som kan identifiseres på bildene. Dette gjelder selvsagt uansett om bildene publiseres på en hjemmeside, på en blogg, på sosiale medier eller andre nettsider. Det gjelder også om bildene deles i lukkede grupper, slik som Facebook-grupper med flere medlemmer. Brudd på disse reglene kan være straffbart etter straffeloven.[5]

Situasjonsbilder kan derimot offentliggjøres uten samtykke fra de avbildede så lenge bildene er harmløse og ikke på noen måte er krenkende for de som er avbildet (Datatilsynet 2017). Situasjonsbilder kan defineres som bilder der selve situasjonen eller aktiviteten er det egentlige motivet i bildet. Akkurat hvem som er med på bildet, er da mindre viktig enn hovedinnholdet i bildet. Eksempler på dette kan være en gruppe mennesker på en konsert, et idrettsarrangement, i 17. mai-tog eller hendelser som har allmenn interesse. Når det gjelder bilder av krenkende situasjoner eller mer spesielle anledninger, for eksempel der man ser ventende på et legekontor eller personer i et badeanlegg eller på en strand, bør disse normalt ikke publiseres på nett eller deles med andre uten samtykke.

Det kan av og til være vanskelig å avgjøre hva som er situasjonsbilde og ikke, og om situasjonen kan være krenkende for noen. Som hovedregel bør man derfor be om samtykke dersom bilder eller filmer skal offentliggjøres (Datatilsynet 2017).

Fem personvernutfordringer ved bruk av droner

I svært mange tilfeller bidrar bruk av droner til at en rekke samfunnsoppgaver blir løst mer effektivt og med mindre risiko for skade på materiell

5 Jf. dom fra Asker og Bærum tingrett. TAHER-2016-136649. 18 år gammel gutt, 17 år på hendelsestidspunktet, ble dømt til 90 dager ubetinget fengsel for å ha delt et bilde av to personer som hadde samleie på Snapchat.

og mennesker. I tillegg er en voksende dronenæring egnet til å skaffe både arbeidsplasser og økt omsetning for norsk næringsliv. Til tross for slike positive virkninger av droneteknologi er det viktig å samtidig ha en fot i bakken og se på hvilke risikoer den samlede bruken av droner kan medføre for personvernet vårt. Nedenfor presenterer vi de mest alvorlige personvernutfordringene vi ser ved bruk av droner i dag og i fremtiden.

Terskelen for overvåkning senkes med ny teknologi

Ny teknologi gir oss nye muligheter til både å løse nye oppgaver og løse tidligere oppgaver mer effektivt og bedre enn tidligere. Dette er i utgangspunktet et gode. Men det kan også medføre at de aktiviteter som utfordrer personvernet, blir billigere å ta i bruk.

Et eksempel er vanlig kameraovervåkning, som tidligere var kostbart og bare ble satt opp av profesjonelle aktører. I dag kan alle kjøpe kraftig overvåkningsutstyr i butikken og ta det i bruk, som oftest supplert med fjerntilgang over internett. Her har vi tre observasjoner; utstyret er blitt mer tilgjengelig, utstyret har blitt kraftigere, og de som tar utstyret i bruk, er ikke like profesjonelle som tidligere. Det gjør at personvernet blir krenket i større grad enn tidligere gjennom bruken av slik overvåkningsteknologi.

Når det gjelder droner, er det udiskutabelt at innføringen av disse har senket terskelen for filming fra luften. Selv om overvåkning ofte ikke er utgangspunktet, medfører det naturlig nok en vesentlig økning av krenkende filming fra luften, som eksempelet i starten av dette kapitlet illustrerer.

Når vi har et nytt teknologiområde som vi vet kommer til å krenke personvernet på flere områder, må vi spørre oss hvordan vi kan kompensere for dette. Da er det relevant å se til personvernprinsippene, som vi var innom tidligere.

Et tiltak som medfører en inngripen i personvernet, må være proporsjonalt. Det betyr at nytten av tiltaket må stå i forhold til ulempen det medfører, dersom vi velger å gjennomføre tiltaket. Dersom tiltaket er for inngripende, må vi la være, eller vi kan forsøke å gjøre tiltaket mindre inngripende. Her ligger det et stort handlingsrom i hvordan teknologien tas i bruk.

La oss ta et eksempel. Eieren av en lakseelv har adgang til å kontrollere om de som fisker i elven, har løst fiskekort. Å ta i bruk droner til dette automatiserer denne kontrollen og øker kontrolltrykket, ikke bare på fiskerne,

men også på andre som ferdes langs elven. Trolig er innføringen av en slik kontroll utenfor det som er akseptabelt, og elveeieren må holde seg til den gode gamle formen for kontroll.

Et annet eksempel er redningstjenestens søk etter savnede personer. Dette er nok et område hvor det vil være proporsjonalt å effektivisere søket ved bruk av droner. Men har bruken noen begrensninger? Vi ser tilbake til starten av kapitlet med droner som flyr i svermer. Om søk etter savnede med dronesvermer gjøres nærmest vedvarende og allestedsværende, vil nok dette også være et tiltak som ikke er proporsjonalt. Det vil innebære en for stor inngripen i personvernet til alle andre som blir fanget opp av dronene. Men igjen, aktiv bruk av droner innenfor en konkret leteaksjon vil nok være et gode for samfunnet.

Proporsjonaliteten kan påvirkes på mange vis. For eksempel hvor godt det informeres om aktiviteten, eller hvordan en begrenser innsamlingen av opplysninger. Det siste kalles dataminimalisering, og handler om å unngå eller begrense mengden personopplysninger som behandles. Kan for eksempel data som ikke er relevante, slettes fortløpende? Eller kan personer i et opptak endres slik at de ikke kan kjennes igjen? Et eksempel her er droner som benytter kamera for navigasjon og inspeksjon av kraftlinjer. Personene som eventuelt fanges opp, er ikke av interesse, og kan sladdes bort eller erstattes med «kakemenn» i videostrømmen.

Et annet sentralt prinsipp er formålsbestemthet – at personopplysninger benyttes til det formålet de er innsamlet for. Det betyr at informasjonen vi samler inn i en sammenheng, bare kan benyttes i den sammenhengen og ikke til andre formål. Tilbake til eksempelet med leteaksjonen – å benytte informasjon som ble samlet inn under leteaksjonen, til at kommunen kan kontrollere om hyttebyggingen i et område er lovlig, vil være et helt annet formål enn det opprinnelige, og vil nok ikke være akseptabelt.

Krevende å gi riktig informasjon til riktig tid til de registrerte

For å kunne utøve selvbestemmelse og kontroll over egne personopplysninger er det en forutsetning at vi får informasjon om hvem som behandler personopplysninger om oss, og hvorfor behandlingen finner sted. Plikten til

å gi informasjon ved innsamling og bruk av personopplysninger er derfor lovbestemt (Regulation (EU) 2016/679, 2016).

Plikten til å gi informasjon inntrer som hovedregel «på tidspunktet for innsamlingen» når informasjonen samles inn fra den registrerte selv. Personvernreglene stiller i tillegg en rekke krav til hvordan informasjonen skal gis, og hva det skal gis informasjon om. Informasjonen skal være kortfattet, klar og tydelig, lett forståelig og lett tilgjengelig, og det skal blant annet gis informasjon om formål med behandlingen og hvor lenge opplysningene skal lagres (Regulation (EU) 2016/679, 2016).

Ved bruk av drone er det en utfordring for droneoperatøren å gi den informasjonen personvernreglene krever, til riktig tid, altså «på tidspunktet for innsamlingen». En droneoperatør vet ikke nødvendigvis hvilke personer som oppholder seg i det området hun skal fly i, og det er heller ikke gitt hvordan hun skal kommunisere med de registrerte før dronen eventuelt filmer disse personene. Vanlige måter å gi informasjon på som for eksempel skilting, informasjonsskriv eller pop up-vinduer på PC-en egner seg ikke som informasjonskanaler der en drone filmer eller registrerer andre personopplysninger fra luften. Dette reiser spørsmålet om en stor del av den alminnelige droneaktiviteten som er vanlig i dag, faktisk er ulovlig ettersom informasjonsplikten etter personvernreglene ikke blir overholdt.

Fravær av informasjon har og andre følger enn mulig brudd på personvernreglene. En annen alvorlig konsekvens er den manglende forutsigbarheten fravær av informasjon medfører for den enkelte. For en person som observerer en drone utenfor vinduet sitt, i hagen, ved båten, på hytta eller i fjellet, har som regel ikke anledning til å vite hvem som eier dronen, hva den filmer, om personopplysninger om dem blir lagret og eventuelt hva informasjonen blir brukt til. Denne følelsen av å være overvåket og delvis miste kontroll over opplysninger om seg selv oppleves ofte krenkende for den det gjelder. Dette ubehaget manglende informasjon medfører for den enkelte, er derfor en alvorlig personvernutfordring ved bruk av droner.

Inngripende bruk av droner i regi av myndighetene

Et område hvor vi bør vise særlig aktsomhet, er hvordan myndigheter tar i bruk droner i sin kontrollaktivitet. Myndighetenes kontroll med hvordan

innbyggerne lever sine liv er særlig inngripende. Som vi skrev innledningsvis, er innbyggere som er frie fra en omfattende overvåkning, en forutsetning for et sunt demokrati. Vi kan likevel akseptere noe overvåkning under gitte tilfeller, blant annet i trafikken og for politiets håndtering av viktige områder. Men vedvarende overvåkning av befolkningen vil i de aller fleste tilfeller være uakseptabelt.

Når vi erstatter tidligere teknologi i staten med ny teknologi – som droner, må vi være svært bevisst på hva endringen medfører av ulemper for personvernet, og om endringen er proporsjonal og om den er forsvarlig sett opp mot det samfunnet vi ønsker å ta vare på. Som en del av dette må vi vurdere om den nye bruken er innenfor lovhjemlene som er satt for bruken.

La oss ta et eksempel. Kystvakten har vide fullmakter til å overvåke og kontrollere. Dette skjer både fra fartøy og fra luften ved bruk av helikopter og fly. Det er naturlig at Kystvakten ser på hvordan dette arbeidet kan effektiviseres ved hjelp av droner. En slik rasjonell overgang til ny teknologi kan ses fra to perspektiv. På den ene siden kan Kystvakten si at de gjør det samme som tidligere. Kystvakten har som sagt vide fullmakter i lov til å overvåke og kontrollere fra luften, og bruk av droner utgjør ingen forskjell fra nåværende bruk av fly og helikopter. Mens fra den andre siden kan en argumentere for at der et fåtall fly og helikoptre erstattes med et utall av droner, utgjør dette en helt ny og intensivert overvåkning. I tillegg vil overvåkningen være mindre synlig og forutsigbar enn tidligere. For å ikke snakke om hva som kan oppnås med svermer av droner som følger med på det enkelte fartøy, eller det enkelte fiskeredskap for den saks skyld.

Kystvakten arbeider med disse spørsmålene på en faglig og seriøs måte. Vi er likevel av den oppfatning at Kystvaktens situasjon er illustrerende; innføringen av droner medfører endring i overvåkning og endrede personvernkonsekvenser. Derfor er det viktig at en vurderer personvernkonsekvensene av teknologibyttet i slike prosjekt. Dette forutsetter god personvernkompetanse i slike prosjekter. Som en del av konsekvensvurderingen må myndighetsorganet også vurdere om etaten er innenfor lovhjemlene for overvåkningen, og om det er tiltak etaten kan innføre for å begrense inngrepet i personvernet.

Et tilsvarende eksempel kan vi tenke oss for politi og trafikkontroll som kan gjennomføres fra helikopter i dag, men hvor bruk av droner åpner helt nye muligheter og utfordringer.

Det er en alvorlig utfordring for personvernet dersom droner tas i bruk ukritisk til offentlig overvåkning og kontrollformål.

Manglende informasjonssikkerhet

De fleste droner vi kjenner, kommuniserer tilbake til piloten eller kontrollsenteret. Personopplysninger, inkludert film, som samles inn via dronen, må sikres slik at de ikke kommer på avveie, går tapt eller kan endres. Når vi arbeider med informasjonssikkerhet, sier vi som oftest at personopplysningene skal sikres med hensyn til konfidensialitet, integritet og tilgjengelighet. For å vurdere om sikkerheten er god nok benytter vi risikovurderinger hvor vi ser på hva som kan gå galt, sannsynligheten for at det går galt og konsekvensene av det.

For droner er det mest sentrale at kommunikasjonen mellom dronen og bakken krypteres slik at uvedkommende ikke kan få tilgang. Andre tiltak vil være tidsstempling av opptak og bilder for å sikre ektheten av disse. Videre er adgangskontroll og sikre protokoller for samhandling viktig slik at dronen ikke lar seg bli hacket og kan overtas av andre.

Det er også andre grunner til å sikre opptakene enn personvern. Dette kan være rettigheter til bilder tatt med dronen eller forretningsmessig viktig informasjon fra dronens sensorer, eller at en kapret drone kan benyttes i et fysisk angrep mot personer eller infrastruktur.

Dagens IT-verden er tilkoplet. Vi skal også være oppmerksom på om leverandøren av dronen får informasjon fra dronen dersom de har en tilknytning til leverandøren. Dersom det er personopplysninger som sendes videre, må det være en grunn til å gjøre det, og leverandøren vil være det vi kaller for en databehandler. Da plikter vi å regulere i en avtale hva leverandøren gjør med dataene. Dersom data overføres til utlandet, kan dette bli ytterligere komplisert. Den ansvarlige for dronen må kjenne til hvordan løsningen fungerer og om den er akseptabel.

Personopplysningene må sikres både i dronen, i kommunikasjonen med bakkeutstyret og i bruken av opplysningene etterpå. Ved bruk av droner, særlig i mindre virksomheter med få ansatte, kan det være en utfordring å sørge for at opplysninger om enkeltpersoner håndteres med tilstrekkelig grad av informasjonssikkerhet. Dette gjelder spesielt i tilfeller der flere aktører har tilgang til personopplysningene som samles inn. Ved ny teknologi

er det også en fare for at det er funksjonalitet i droneløsningen som blir prioritert fremfor sikkerheten i løsningen.

Manglende opplæring og kjennskap til reglene

Droneeiere er ikke en ensartet gruppe med samme bakgrunn, kunnskapsnivå og forståelse av lover og regler. Droneeiere er alt fra barn som eier et leketøy, hobbyflyvere som er interessert i teknologi og fotografering, private næringsdrivende som utvikler produkter og tjenester, mediehus som driver med journalistikk eller offentlige myndigheter som skal løse sine samfunnsoppgaver på mest mulig effektiv måte.

Det sier seg selv at en så mangfoldig gruppe bruker dronene sine på forskjellige måter, og i stor grad har ulike lovkrav og regler de må forholde seg til. Det er for eksempel stor forskjell på hvilke krav en vil stille til et barns bruk av en leketøysdrone i hagen og en politidrone som brukes til å skaffe oversikt over et ulykkesområde. En betydelig utfordring oppstår likevel når samtlige droner er utstyrt med teknologi som kan samle inn personopplysninger om andre mennesker. Dersom droneeieren ikke er bevisst hvilke begrensninger personvernhensyn setter for akkurat den bruken av dronen han eller hun driver med, er det stor sannsynlighet for at det medfører dårligere kår for personvernet vårt. Det er derfor viktig at den enkelte droneeier setter seg inn i personvernreglene og gjør en konkret vurdering av om droneaktiviteten medfører en behandling av personopplysninger som må følge personvernreglene.

Vår erfaring tilsier imidlertid at det for både privatpersoner og virksomheter er vanskelig å skaffe seg oversikt over personvernreglene og følge disse når dronen skal brukes. Det kan tenkes flere årsaker til dette. For eksempel kreves det ingen sertifisering eller forkunnskaper for å kjøpe og bruke en drone. Videre er personvernreglene vage. Det kan derfor være krevende å finne ut hva reglene betyr.

Å følge personvernreglene krever kunnskap og systematisk arbeid over tid hos droneoperatørene. Sett i sammenheng med den veksten dronenæringen er spådd i fremtiden, fremstår tilstrekkelig kunnskap om personvern og deretter vilje til å etterleve personvernreglene hos den enkelte droneeier som en nøkkel for at vi skal kunne ivareta selvbestemmelse og kontroll med egne personopplysninger.

Personvernfremmende tiltak ved bruk av droner

I denne delen skal vi gi noen generelle anbefalinger som vi mener vil bidra til et bedre personvern ved bruk av droner. Hensikten er å gi leseren oversikt over hva de ulike aktørene kan gjøre for å avhjelpe personvernutfordringene vi har beskrevet tidligere i dette kapitlet. Anbefalingene vi presenterer, er ikke ment som en uttømmende oversikt for hvilke plikter den enkelte aktør har etter personvernreglene (Article 29, Data Protection Working Party 2015).

Anbefalinger for droneoperatører

Det første en droneoperatør må gjøre, er å avklare om personvernreglene gjelder ved den datainnsamlingen som skjer ved hjelp av dronen. Spørsmålet du må stille deg er: Kommer du til å behandle personopplysninger? Dette er helt grunnleggende spørsmål på lik linje som andre flytekniske avklaringer du som droneoperatør må gjøre før start. Det kan være vanskelig å svare sikkert på om du vil behandle personopplysninger. Du må likevel gjøre en konkret og grundig vurdering. Kanskje du må undersøke Datatilsynets nettside for veiledning, eller be om en vurdering fra juridisk avdeling der du jobber?

Hvis du kommer til at datamaterialet fra dronen inneholder personopplysninger, må du vite hvilket rettslig grunnlag som legitimerer innsamlingen og eventuell senere bruk av personopplysningene. Har for eksempel de registrerte samtykket til behandlingen, eller har du adgang til å samle inn personopplysningene fordi du har en lovhjemmel som tillater det? Dette er igjen en konkret vurdering som du må ta. Hvis du ikke har et rettslig grunnlag for å behandle personopplysningene, har du heller ikke lov til å behandle dem.

Den eller de personene som får sine personopplysninger behandlet, har videre en rekke rettigheter etter personopplysningsreglene som du som droneoperatør har plikt til å ivareta. Du må utarbeide en internkontroll med rutiner som sørger for at du er i stand til å ivareta rettighetene til de registrerte. For eksempel rutiner for hvordan du gir informasjon om behandlingen, og hvordan du svarer på eventuelle henvendelser om sletting eller innsyn.

Som droneoperatør må du ha fastlagt roller ved behandlingen av personopplysningene. Dette skal fremgå av internkontrolldokumentasjonen din. Hvem er databehandler og hvem er behandlingsansvarlig? Du må ha oversikt over hvem som har tilgang til personopplysningene. Lagrer du personopplysninger i en skytjeneste? Hvor ligger skyen? Hvem har tilgang til skyen? Hvor lenge har du lov til å lagre personopplysningene? Kan du anonymisere personopplysningene, bør du gjøre det. Videre bør du som droneoperatør alltid tenke innebygd personvern ved valg av drone og teknologi. Dette kan bidra til å gjøre vurderingene vi har beskrevet over, mindre kompliserte. For eksempel vil du trolig unngå å behandle personopplysninger og måtte forholde deg til personopplysningsloven dersom du ikke bruker filmkameraet på dronen når du flyr.

For droneoperatører som er organisert i medlemsorganisasjoner eller andre sammenslutninger, vil vi anbefale at droneoperatørene går sammen og utarbeider bransjenorm for håndtering av personopplysninger i sin sektor. Ved å følge en slik bransjenorm vil du få på plass de viktigste rutinene for å etterleve personvernreglene. I tillegg kan tilslutning til en bransjenorm brukes som et element i å dokumentere at du oppfyller lovens krav om tilstrekkelig informasjonssikkerhet.

Anbefalinger for de som utvikler droner og styringssystemer

For de som utvikler droner og styringssystemer, er vår anbefaling å tenke personvern i alle utviklingsfaser av systemene. Dette innebærer at der du utvikler nye løsninger, skal disse oppfylle personvernprinsippene og ivareta de registrertes rettigheter som standardinnstilling. Systemene bør langt på vei unngå eller minimere behandlingen av personopplysninger til det som er absolutt nødvendig. For eksempel ved automatisk sladding av personer og bilskilt, og automatisk begrensning av lagringstid.

Vi anbefaler at de som utvikler droner og styringssystemer, involver et personvernombud i utviklingsfasen av nye systemer.

Vi anbefaler også, så langt det er mulig, at utviklere og produsenter lager dronesystemer som er synlige på avstand, for eksempel med lyd, lys eller tydelige farger.

Anbefalinger for statlige myndigheter

Ved salg av droner anbefaler vi at myndighetene sørger for at det følger med informasjonsskriv som viser hvilke regler som gjelder ved bruk av drone. Et slikt informasjonsskriv bør inneholde både luftfartsregler og personvernregler.

Vi anbefaler at myndighetene vurderer å innføre krav om opplæring og avlegging av prøve for å fly drone til kommersielle formål. Innføring i personvernregler bør være en del av denne opplæringen.

Når det gjelder myndighetenes egen bruk av droner, anbefaler vi at myndighetene prioriterer å skaffe seg god personvernkompetanse i statlige droneprosjekter. Myndighetene må sørge for at det gjøres grundige personvernkonsekvensvurderinger både i enkeltprosjekt og i lovarbeid. Det er viktig at lovgrunnlag som regulerer bruk av droner, er forutsigbare og lette å forstå, slik at myndighetenes bruk av droner er forutsigelige for den enkelte borger.

Avslutning

I dette kapitlet har vi belyst hva personvern er, hvilke personvernregler som gjelder ved bruk av droner, og hvilke personvernutfordringer vi ser ved dagens dronebruk.

Det er åpenbart at innføring av droner senker terskelen for overvåkning fra luften. Det er stor spredning i profesjonalitet for gruppen som bruker droner. Og i tillegg er reglene som skal ivareta personvernet vårt, svært skjønnsmessig utformet. Dette taler dessverre mot en tro på at vi kan oppnå et godt personvern for den enkelte samtidig som dronenæringen skal vokse og bli en integrert og viktig del av samfunnet vårt. Det betyr derimot ikke at vi skal gi opp, men snarere tvert imot; droneindustrien må jobbe målrettet for å ivareta personvernet for å legge grunnlaget for en forsvarlig utvikling til det beste for industri og innbygger.

Skal vi fremheve et særlig viktig område å arbeide med, så er det å sikre kunnskap om personvern på alle nivå – fra produktutvikler til dronepilot.

Oversikt over lovhenvisninger i personvernregelverket som er relevante ved bruk av drone

Grunnlovens beskyttelse av privatliv og privat korrespondanse	Grunnloven § 102
Folkerettslige forpliktelser om privatliv	EMK Artikkel 8
Materielt virkeområde for de generelle personvernreglene	REGULATION (EU) 2016/679 (GDPR) artikkel 2
Unntak fra det materielle virkeområde for de generelle personvernreglene	REGULATION (EU) 2016/679 (GDPR) artikkel 2 (2) bokstav c (rent personlige og familiære aktiviteter) og artikkel 85 unntak ved behandling av personopplysninger i relasjon til ytrings- og informasjonsfrihet
Krav for behandling av personopplysninger	REGULATION (EU) 2016/679 (GDPR) artikkel 5, 6 og 9
Informasjonsplikt	REGULATION (EU) 2016/679 (GDPR) artikkel 12,13 og 14.
Andre rettigheter for registrerte	REGULATION (EU) 2016/679 (GDPR) artikkel 12-22
Krav om informasjonssikkerhet	REGULATION (EU) 2016/679 (GDPR) artikkel 32
Krav om personvernvennlige innstillinger og innebygd personvern	REGULATION (EU) 2016/679 (GDPR) artikkel 25
Krav om databehandleravtale	REGULATION (EU) 2016/679 (GDPR) artikkel 28
Krav om personvernkonsekvensvurdering	REGULATION (EU) 2016/679 (GDPR) artikkel 35
Krav om internkontroll	REGULATION (EU) 2016/679 (GDPR) artikkel 30
Straffelovens bestemmelser om vern av privatlivets fred	§§ 266 og 267
Åndsverklovens bestemmelse om eget bilde	§ 45 c

Litteratur

Norsk lov og forskrift

Menneskerettsloven (1999). Lov om styrking av menneskerettighetenes stilling i norsk rett. Justis- og beredskapsdepartementet.

Kongeriket Norges Grunnlov (1814). Justis- og beredskapsdepartementet.

Straffeloven (2005). Lov om straff. Justis- og beredskapsdepartementet.

Åndsverkloven (1961). Lov om opphavsrett til åndsverk m.v. Kulturdepartementet.

Personopplysningsloven (2000). Lov om behandling av personopplysninger. Justis- og beredskapsdepartementet.

Forskrift om luftfartøy som ikke har fører om bord mv. (2015). Samferdselsdepartementet.

Norsk rettspraksis

Dom fra Asker og Bærum tingrett (2016). TAHER-2016-136649.

Regelverk fra EU

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016).

Rapporter/uttalelser fra EU-organer

Article 29 Data Protection Working Party (2015). Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. Hentet fra http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

Nettside med organisasjon som forfatter

Datatilsynet (2016). Hva er personvern? Hentet fra https://www.datatilsynet.no/om-personvern/hva-er-personvern/

Datatilsynet (2016). Personvernprinsippene. Hentet fra https://www.datatilsynet.no/om-personvern/personvernprinsippene/

Datatilsynet (2017). Programvareutvikling med innebygd personvern. Hentet fra https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/

Datatilsynet (2017). Databehandleravtale. Hentet fra https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/

Datatilsynet (2016). Overføre opplysninger til utlandet. Hentet fra https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/
Datatilsynet (2017). Behandle personopplysninger. Hentet fra https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/
Datatilsynet (2017). Deling av bilder. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/internett-og-apper/bilder-pa-nett/