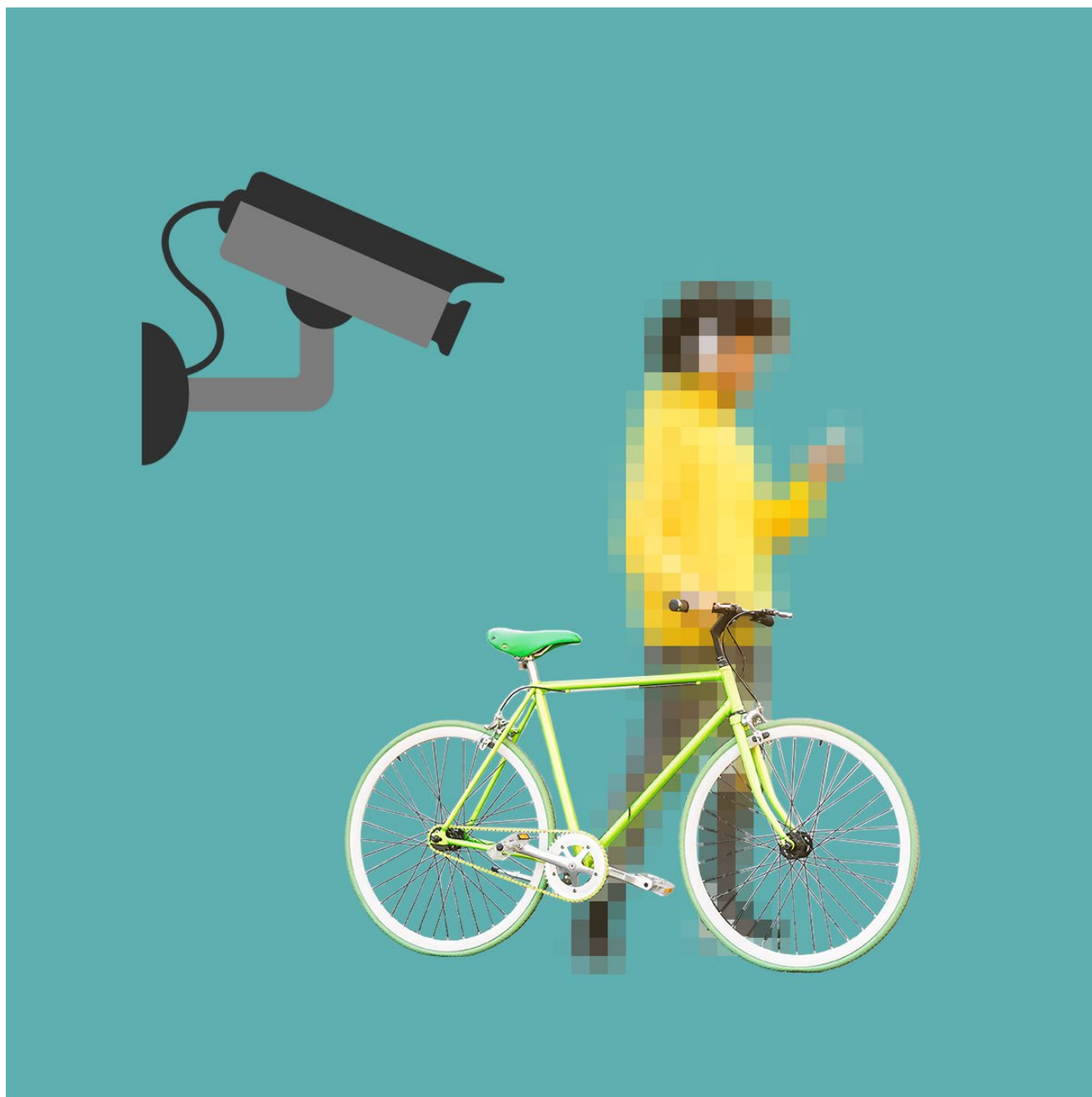




Intelligent kameraovervåking med personvern i fokus

Sluttrapport fra sandkasseprosjektet med Doorkeeper

Februar 2023

Innhold

SAMMENDRAG	3
INTRODUKSJON	4
OM PROSJEKTET	5
MÅL FOR PROSJEKTET	8
FORMÅLSBEGRENSNING OG DATAMINIMERING.....	9
RETTLIG GRUNNLAG FOR DOORKEEPERS BRUK AV INTELLIGENT VIDEOANALYSE	12
VURDERING AV TRE BRUKSEKSEMPLER.....	14
UTLEVERING AV PERSONOPPLYSNINGER	20
SIKKERHETSUTFORDRINGER	21
VEIEN VIDERE	24

Hva er sandkassa?

I sandkassa utforsker deltakere sammen med Datatilsynet personvernrelaterte spørsmål, for å bidra til at tjenesten eller produktet deres etterlever regelverket og ivaretar personvernet på en god måte.

Datatilsynet tilbyr veiledning i dialog med deltakerne, og konklusjonene fra prosjektene er ikke vedtak eller forhåndsgodkjenning. Deltakerne står fritt i valget om å følge rådene de får.

Sandkassa er en verdifull metode for å utforske problemstillinger der jussen har få praktiske eksempler å vise til, og vi håper konklusjoner og vurderinger i rapporten kan være til hjelp for andre med liknende problemstillinger.

Sammendrag

Mål med sandkasseprosjektet

Virksomheten Doorkeeper ønsker å fremme personvern i moderne kameraovervåkingsløsninger. De vil gjøre dette ved å bruke intelligent videoanalyse til å sladde identifiserende opplysninger – som ansikter og menneskeformer – i videostrømmen. I tillegg vil de legge til rette for at færre opptak lagres – i forhold til det som er vanlig i mer tradisjonelle overvåkingsløsninger.

Formålet med dette sandkasseprosjektet er å utforske noen av de mest relevante regulatoriske problemstillingene som oppstår ved bruk av intelligent videoanalyse.

Hovedpunkter

- **Rettslig grunnlag for intelligent videoanalyse**

I sandkassen har vi drøftet problemstillinger knyttet til det rettslige grunnlaget ved tre forskjellige bruksområder av Doorkeepers løsning. Problemstillingene er overførbare til andre virksomheter som skal utvikle lignende løsninger. Et viktig moment er at intelligent videoanalyse – som er utformet for å gjøre behandlingen av personopplysninger mindre inngripende – kan påvirke hvorvidt en behandling er lovlig etter personopplysningsregelverket.

- **Alternative utforminger av løsningen**

Doorkeeper har to alternative utforminger for bruken av intelligent videoanalyse. Disse er at analysen og sladdingen enten skjer i kamerahuset, eller på en ekstern plattform. Valg av utforming påvirker hvordan personopplysninger behandles i løsningen. I denne rapporten har vi drøftet at dette kan ha konsekvenser for hvor inngripende overvåkingen er for de som registreres i videostrømmen.

- **Dataminimering**

I denne rapporten viser vi at det er mulig å gjennomføre tiltak for dataminimering i intelligent videoanalyse. Slike tiltak kan gjennomføres ved å konfigurere løsningen til å begrense mengden personopplysninger som hentes inn og behandles til det som er nødvendig for å oppnå formålet. Utbredelsen av funksjonaliteter i overvåkingssystemer som gjør behandlingen av personopplysninger mindre inngripende, vil også gjøre at virksomheter i sikkerhetsbransjen i større grad må vurdere hvilke personopplysninger som er *nødvendige* å behandle for å oppnå formålet med overvåkingen.

- **Utlevering av personopplysninger**

Doorkeeper sin løsning er utformet på en måte som gjør at det lagres færre opplysninger som kan utleveres – i forhold til kameraer som gjør løpende opptak. Det kan gjøre det enklere for virksomheter som Doorkeeper å etterleve innsyns krav ettersom virksomheten vil lagre færre videoopptak som kan være aktuelle. Likevel vil reglene for utlevering av personopplysninger være de samme for Doorkeeper, som for øvrige behandlingsansvarlige.

- **Sikkerhetsutfordringer**

I sandkassen har vi diskutert at Doorkeeper må sørge for at sikkerheten i løsningen er *vedvarende*. Dette betyr at sikkerheten i løsningen skal følge den tekniske utviklingen, at eventuelle sårbarheter må adresseres og håndteres fortløpende, og at opplysninger skal slettes når formålet er oppnådd.

Veien videre

I sandkassen har Doorkeeper fått utforsket spørsmål de har hatt i utviklingen av intelligent videoanalyse med potensielt personvern fremmende funksjoner. Diskusjonene i denne rapporten kan brukes av Doorkeeper for å bedre imøtekomme kravene i personvernregelverket og sikre et bedre personvern i løsningen. Datatilsynet håper også at diskusjonene vil være til hjelp for andre virksomheter som utvikler lignende teknologi.

Gjennom arbeidet i sandkassen har også Datatilsynet lært mye om mulighetene innen intelligent videoanalyse. Denne kompetansen vil vi videre bruke for å forbedre vårt veiledningsarbeid.

Introduksjon

Formålet med dette sandkasseprosjektet er å utforske løsningene til virksomheten Doorkeeper, som vil bruke kunstig intelligens for å begrense hvilke personopplysninger et overvåkingskamera fanger opp.

Hvis man forestiller seg et overvåkingskamera i en norsk dagligvarebutikk på 1990-tallet, var kameraet stort og framtreddende, og koblet med en fysisk ledning til en videoopptaker i butikkens bakrom. Siden den tid har teknologien utviklet seg drastisk – med forbedringer i bildeoppløsning, programvare, lagring og trådløse forbindelser. Samtidig har kamerløsninger generelt blitt billigere og mer tilgjengelige. Men det største teknologiske skiftet kom på 2010-tallet med bruken av kunstig intelligens og maskinlæring for å analysere videostrømmene.

Med løsninger som er basert på kunstig intelligens, kan alt som befinner seg i videostrømmen bli automatisk analysert. Dette gjør det teknisk mulig å samle inn enorme mengder opplysninger om personene som blir fanget opp av kameraet. Samtidig har økt prosesseringskraft og fremskritt innen *edge computing* gjort at maskinlæringsalgoritmer kan kjøres i kamerahuset, hvilket betyr at opplysninger i større grad blir analysert før de gjøres tilgjengelige for mennesker. Dette endrer hvordan personopplysninger behandles i overvåkingsløsninger.

Datatilsynet erfarer at kameraovervåking er et tema som engasjerer mange. Gjennom vår veiledningstjeneste har vi de siste tiårene erfart jevn pågang med henvendelser om temaet. Vi mottar blant annet spørsmål fra privatpersoner som opplever seg overvåket av videokameraer, og fra virksomheter som har spørsmål om hvordan de kan bruke kameraovervåking i tråd med regelverket.

Overvåking av mennesker er en utøvelse av makt som medfører inngrep i den enkeltes personvern. Som vi skal se i denne rapporten, må dette inngrepet vurderes opp mot det konkrete brukstilfellet. Løsninger som tar i bruk kunstig intelligens kan være både *mer* og *mindre* inngripende i forhold til eldre overvåkingsteknologi. Det finnes flere som ser personvern som et konkurransefortrinn i markedet, og Datatilsynet ser det som positivt at flere vil gå i denne retningen.

Tilstedeværelsen av et overvåkingskamera vil i seg selv medføre en følelse av å bli overvåket – uavhengig av om kameraet er «intelligent» eller ikke. Det overordnede overvåkingstrykket i Norge er et spørsmål som vi ikke diskuterer i denne rapporten, men som må være gjenstand for en bredere debatt i samfunnet.

Om prosjektet

I dette kapittelet beskriver vi hvem Doorkeeper er, deres prosjekt, og hvordan de planlegger å bruke intelligent videoanalyse.

Om Doorkeeper

AS Doorkeeper er en norsk oppstartsvirksomhet som ble etablert i 2021. Virksomheten utvikler, produserer og selger sikkerhetsløsninger, som adgangskontroll og kameraovervåking. Det er kun kameraovervåking som har vært tema i dette sandkasseprosjektet.

Hva er Doorkeeper sin tjeneste?

En hovedårsak til at Doorkeeper ble valgt ut som deltager i sandkassen var at de vil benytte intelligent videoanalyse («Intelligent Video Analytics») for å tilby mer personvernvennlig kameraovervåking på markedet. Intelligent videoanalyse er teknologi som automatisk analyserer innhold fra overvåkingskameraer.

For å oppnå bedre personvern, skal Doorkeeper bruke kunstig intelligens og maskinlæring for å sladde identifiserende opplysninger i videostrømmen. Dette inkluderer ansikter, kropper, registreringsnumre, tekst og logoer. De skal også konfigurere løsningen slik at det ikke gjøres løpende videoopptak så lenge ingen forhåndsdefinerte hendelser skjer. Det vil gjøres en kortsiktig lagring i kamerahuset, men denne vil slettes fortløpende og vil normalt ikke være tilgjengelig for operatøren.

Intelligent videoanalyse kan innstilles på mange forskjellige måter for å tilpasse overvåkingen til formålet. I sandkassen har vi begrenset våre diskusjoner til å i hovedsak handle om tre funksjoner i løsningen:

- Sladding av identifiserende opplysninger fra videostrøm i sanntid
- Registrering og varsling om brann- og røykutvikling
- Registrering og varsling om kriminelle handlinger

Doorkeeper ønsker å være en totalleverandør. Det vil si at de vil tilby alle deler av løsningen; kameraer, nettverk, overvåkingsplattform, konfigurasjon, vaktentral og operatører. Formålet med dette er blant annet å sikre at tjenesten benyttes på en måte som ivaretar personvernet og sikkerheten til de det gjøres opptak av.

Hvordan fungerer løsningen?

Under beskriver vi hvordan Doorkeeper sin løsning for intelligent videoanalyse fungerer. Beskrivelsen legger grunnlaget for de juridiske vurderingene som kommer senere i rapporten.

Ved utarbeidelsen av rapporten var løsningen fortsatt i utviklingsfasen. Derfor kan beskrivelsen under skille seg fra den endelige løsningen.

En trinnvis forklaring av løsningen

Løsningen består av flere komponenter: overvåkingskameraer, et grensesnitt for intelligent videoanalyse og en overvåkingsplattform («Video management system» - VMS). Overvåkingsplattformen henter videostrøm fra kameraet og gir operatøren et brukergrensesnitt å forholde seg til. Operatøren som følger med på videostrømmen, gjør dette via plattformen.

Doorkeeper har to alternative utforminger for oppsettet av løsningen. Den viktigste forskjellen mellom oppsettene, er *hvor* analysen foregår:

- A. Den ene utformingen omfatter bruk av Doorkeeper sine egenutviklede kameraer. Disse kameraene har en innebygd prosesseringsenhet – som er spesiallaget for bruk til kunstig intelligens. Denne gjør at kameraet kan analysere og prosessere videostrømmen i sanntid. Resultatet er blant annet at ansikter og menneskeformer kan sladdes lokalt i kameraet, og minimerer overføring av personopplysninger fra kameraet og til plattformen.

Det lagres en logg både lokalt i kamerahuset og i plattformen. I loggen står det når hendelser oppdages, når sladdingen fjernes, og hvem som har logget seg på systemet.

- B. Den andre utformingen omfatter bruk av kameraer som ikke er levert av Doorkeeper. Dette kan være aktuelt for virksomheter som allerede har montert kameraer fra andre leverandører. For slike løsninger vil den intelligente videoanalysen gjennomføres på plattformen. Det betyr at videostrømmen som sendes fra kameraet og til plattformen vil inneholde en usladdet og «rå» videostrøm.

Ettersom Doorkeeper ikke kan styre eventuell logging av aktivitet i tredjepartskameraer, vil loggingen kun foregå på plattformen.

Etter at kunden har valgt utforming (A eller B), konfigureres overvåkingen. Vi begrenser oss til de alternativene vi har diskutert i sandkasseprosjektet.

1. Først må virksomheten konfigurere sladdefunksjonen. De kan velge å sladde:
 - Ansikt (løsningen vil identifisere ansikter i videostrømmen som vil sladdes)
 - Mennesker (løsningen vil identifisere menneskeformer i videostrømmen som vil sladdes i sin helhet)
 - Registreringsnumre for biler (løsningen vil identifisere bilskilt som vil sladdes)
 - Skrift (alle bevegelige flater med skrift vil bli identifisert og sladdet)
2. Deretter må virksomheten konfigurere hvilke hendelser som løsningen skal detektere. Dette kan inkludere:
 - Ild og røyk
 - Om noen krysser en definert «linje» (om et menneske går et uønsket sted – for eksempel i et togspor)
 - Objekter (om det er potensielt farlige objekter – som våpen, propantanker eller bensinkanner – på videostrømmen)

Når grensesnittet oppdager en av de forhåndsdefinerte hendelsene, utløses det et signal som fjerner sladdingen. Deretter starter det et opptak og overføring med permanent lagring på plattformen. Samtidig blir det utsendt en alarm til operatøren.

Hvis operatøren tror at en hendelse har oppstått og som løsningen ikke har identifisert, kan sladdingen deaktiveres manuelt. I slike tilfeller må operatøren oppgi årsak til at sladdingen skal fjernes, tidsrommet den skal fjernes for, og sin egen bruker-ID. Dette gjelder både ved sladding i kamerahuset og på plattformen.

For at hendelser og mennesker skal gjenkjennes i videostrømmen, må algoritmen trenes. Doorkeeper gjør dette ved å mate algoritmen med bilder fra kommersielt tilgjengelige databaser. Deretter blir handlingsmønstre og analyser definert. I samme prosess foretar Doorkeeper manuelle justeringer av treningsparameterne for at algoritmen skal gi mer riktige resultater. Doorkeeper trener ikke algoritmen sin med opptak – eller annen type informasjon – hentet fra sine kameraer.

For begge løsninger vil Doorkeeper mellomlagre («cache») de siste minuttene med video, slik at eventuelle opptak med permanent lagring også inkluderer minuttene før en hendelse har oppstått. Mellomlageret slettes fortløpende og operatøren har ikke adgang til dette. Lengden av mellomlagringen vil vurderes ut ifra det konkrete brukstilfellet, men skal alltid være så kort som mulig. Opptak kan ikke slettes manuelt av operatøren, men vil lagres i en definert tidsperiode.

Doorkeeper sikter på å kommunisere tydelig om bruken og tilstedeværelsen av deres kameraer. De planlegger blant annet å ha en rød front på kamerahusene som er lett synlige, og skilting som informerer om bruken av «intelligent overvåking».

Sikkerheten i løsningen

For å sikre kommunikasjonen mellom kameraene og plattformen vil Doorkeeper blant annet kryptere videostrømmen og benytte egne nettverk ved overføring. Doorkeeper vil også ha noe kontroll over hvordan løsningen konfigureres, for å bedre sørge for at den benyttes på en personvernvennlig og sikker måte. Vi kommer tilbake til dette i kapittelet om *sikkerhetsutfordringer* senere i rapporten.

I installeringen og bruken av deres tjenester, setter Doorkeeper en rekke krav til kunden. Blant annet må kunden benytte seg av installatør med ekomnettautorisasjon ([se Nasjonal kommunikasjonsmyndighet sin nettside](#)). Videre må systemet settes opp etter Doorkeepers spesifikasjoner.

En åpenbar svakhet ved bruk av sladdealgoritmer er at operatøren som styrer kameraene kan vilkårlig skru av eller endre sladdenivå- og kriterier, eller aktivere opptaksfunksjon selv når det ikke har vært en hendelse. Doorkeeper har derfor vurdert å begrense kundenes tilgang og gjøre det nødvendig å ta kontakt med en vaktentral for å gjøre endringer.

Hvilke opplysninger registrerer løsningen?

Det er ingen tvil om at Doorkeeper behandler personopplysninger, selv om flere identifiserende opplysninger blir sladdet i videostrømmen.

Ved bruk av *utforming A* sladdes videostrømmen direkte i kameraet før den sendes videre til plattformen. Det vil si at mange av de identifiserende opplysningene kun behandles i kameraet i en normalsituasjon – altså når en hendelse *ikke* er detektert. Det lagres også usladdet opptak midlertidig i kameraet («cache»). Dette slettes etter et gitt tidsintervall, for eksempel fem minutter.

Doorkeeper har iverksatt tiltak som gjør at operatørene ikke får direkte tilgang til opptaket som lagres i kameraet. Operatørene får derfor kun tilgang til den sladdede videostrømmen. Når kameraet detekterer en forhåndsdefinert hendelse, fjernes sladdingen fra videostrømmen og det settes i gang opptak som overføres til plattformen.

Opptaket som gjøres etter at en hendelse er detektert, inkluderer minuttene med usladdet opptak som er lagret i kameraet. Slik kan operatøren se hva som har skjedd i minuttene før hendelsen oppstod.

Ved bruk av *utforming B* vil løsningen behandle samme opplysninger som ved utforming A. Forskjellen er at sladdingen foregår på plattformen. Dette betyr at usladdet videostrøm må overføres mellom kamera og plattform. Tilgangen for operatøren vil likevel være den samme som ved utforming A.

Når en sladdet strøm er tilgjengelig, kan det ikke utelukkes at videostrømmen likevel kan knyttes til enkeltpersoner. For eksempel, hvis kameraet fanger opp en person som er relativt høy, og som passerer samme sted til omtrent samme tid hver dag. Videre vil personer også kunne være identifiserbare basert på kontekster (hvor de er til hvilken tid), hvis opplysninger brukes i kombinasjon med andre kilder (for eksempel annen kameraovervåking uten sladding eller der hvor det samles inn andre type opplysninger som kan kobles til fysiske personer – for eksempel der det registreres logger).

Det kan også være mulig å avlede personopplysninger fra tekst eller logoer som vises i et bilde – for eksempel der hvor firmanavn eller firmalogo på et kjøretøy kan kobles direkte til en fysisk person – såfremt dette ikke er sladdet.

Mål for prosjektet

Datatilsynet og Doorkeeper har satt som mål å diskutere følgende temaer og problemstillinger knyttet til intelligent videoanalyse:

- **Formålsbegrensning og dataminimering**
Hvordan skal prinsippet om formålsbegrensning forstås i sammenheng med intelligent videoanalyse?
Og hvordan skal man ivareta prinsippet om dataminimering?
- **Rettslig grunnlag for bruk av intelligent videoanalyse**
Ved bruk av intelligent videoanalyse, hva er de sentrale momentene virksomheten skal vurdere om det rettslige grunnlaget for behandling av personopplysninger?
- **Alternative utforminger av løsningen**
Doorkeeper vurderer to alternative utforminger av deres løsninger, hvor videostrømmen enten sladdes i kamerahuset eller på en ekstern plattform (VMS). Hvordan påvirker disse forskjellige utformingene det rettslige grunnlaget for løsningen?
- **Utlevering av personopplysninger**
Hvilke vurderinger må gjøres med tanke på utlevering av personopplysninger fra sladdet videostrøm?
- **Sikkerhetsutfordringer**
Sikkerheten i løsningen vil være avgjørende for om Doorkeeper og lignende virksomheter vil kunne etterleve kravene i regelverket. Men hvilke sikkerhetsutfordringer er aktuelle ved den type teknologi som Doorkeeper vil bruke, og hva er de overordnede juridisk kravene til sikkerhet?

Hvordan reguleres kameraovervåking?

I sandkasseprosjektet har vi bare diskutert ansvaret som følger av personvernregelverket. Det er likevel andre regelverk som også kan gjøre seg gjeldende ved kameraovervåking.

Når en arbeidsgiver ønsker å installere overvåkingskamera på arbeidsplassen, gjelder også reglene om *kontrolltiltak* i arbeidsmiljøloven (kapittel 9) og spesialreglene i forskrift for kameraovervåking i virksomhet.

For politiets bruk av kameraovervåking for politimessige formål, kommer personvernregelverket ikke til anvendelse (jf. forordningen artikkel 2. nr. 2 bokstav d). Politiloven § 6a gir politiet rettslig grunnlag til kameraovervåking på offentlig sted når det er nødvendig for å gjennomføre de politimessige oppgavene i politiloven paragraf 2 nr. 1-4. Politiets behandling av personopplysninger på kameraopptak for disse formålene reguleres av politiregisterloven og politiregisterforskriften.

Formålsbegrensning og dataminimering

Et av målene i sandkassen var at Datatilsynet skulle vurdere betydningen av Doorkeepers løsning i forbindelse med prinsippene om formålsbegrensning og dataminimering.

Formålsbegrensning

Før en virksomhet kan behandle personopplysninger, er det nødvendig å klart formulere formålet med behandlingen. Nært tilknyttet dette er prinsippet om *formålsbegrensning*. Formålsbegrensning betyr at personopplysninger kun skal behandles for *spesifikke, uttrykkelig angitte og berettigede* formål. Personopplysninger skal ikke viderebehandles på en måte som er uforenelig med disse formålene.

Når behandlingen av personopplysninger starter, skal formålene allerede være fastsatt. Dette innebærer at man ikke kan behandle personopplysninger bare fordi at de kan vise seg å komme til nytte i fremtiden. Formålene skal også være definert og forklart på en tilstrekkelig *spesifikk* måte. Dette betyr at de «registrerte» – altså de personene som virksomheten behandler opplysninger om – har en klar og entydig forståelse av hva personopplysningene skal brukes til. At formålet skal være *berettiget* betyr at det – i tillegg til å ha et rettslig grunnlag – også skal være i samsvar med øvrige etiske og rettslige normer.

- [Les mer om formålsbegrensning her](#)

De som er registrert har krav på forståelig informasjon om formålet med behandlingen av deres opplysninger (i henhold til forordningen artikkel [12](#), [13](#), [14](#), og [15](#)). Det er derfor viktig at formålene er formulert på en konkret og åpen måte og dokumentert skriftlig.

Dersom en virksomhet vil benytte seg av kameraovervåkning, vil det ikke være tilstrekkelig å vise til en vag og upresis begrunnelse, som for eksempel «sikkerhet». Formålet må defineres mer konkret og være knyttet opp mot et reelt behov, for eksempel at det er en nærliggende fare for tyveri eller hærverk. Overvåking for konkrete sikkerhetsformål kan heller ikke brukes for andre uforenelige formål, som for eksempel overvåkning av ansatte.

Dataminimering

Dataminimering er et viktig prinsipp som virksomheter må overholde for å møte kravene i personvernregelverket. Personvernregelverket – herunder [prinsippet om dataminimering \(lovdata.no\)](#) – stiller krav om at opplysningene som brukes skal være adekvate, relevante og begrenset til det som er nødvendig for å oppnå formålet de behandles for. Det betyr at det ikke skal behandles flere personopplysninger enn det som er nødvendig for å oppnå formålet.

Moderne kameraovervåkingsteknologi – inkludert Doorkeepers løsning – har potensielt muligheten til å gjøre behandlingen av personopplysninger mindre inngripende og at man kan i større grad unngå å samle inn opplysninger som ikke er relevant for formålet.

Dataminimering i praksis: intelligent videoanalyse av trafikknettet

Doorkeeper har stor kontroll over hvilke personopplysninger som registreres i løsningen. I tråd med dette har Doorkeeper og Datatilsynet drøftet to hypotetiske brukseksempler som illustrerer hvordan det kan legges til rette for dataminimering. Begge eksemplene omhandler registrering av kjøretøy i trafikknettet.

Sandkasseprosjektet har ikke gjort ytterligere juridiske vurderinger av eksemplene – som for eksempel om det finnes mer egnede tiltak enn bruk av overvåkingskamera.

- **Eksempel 1:**

Formålet med overvåkningen er å registrere antall og type kjøretøy i trafikknettet ved bruk av intelligent videoanalyse. Hensikten er å registrere hvor mange kjøretøy med forskjellige klassifiseringer (personbiler, personbil med henger, buss, motorsykkel) som reiser på norske veier.

Doorkeeper vurderte at det er en teoretisk mulighet å registrere antall og type kjøretøy uten å gjøre opptak eller sende en videostrøm ut av kamerahuset. Systemet kan for eksempel kjøre en kode i kamerahuset som konverterer de lokale opptakene av kjøretøy til numre som oppsummerer antallet og type kjøretøy. Selv om videostrømmen behandles i kamerahuset – som tilsier at det behandles personopplysninger – vil behandlingen potensielt være betydelig mindre inngripende for trafikantenes personvern enn ved utforminger som baserer seg på løpende videoopptak eller andre metoder som involverer lagring av personopplysninger.

Hvis det er teknisk mulig å oppnå det overnevnte formålet med en form for analyse hvor ingen personopplysninger behandles, tilsier dataminimeringsprinsippet videre at dette alternativet velges.

- **Eksempel 2:**

Formålet med overvåkningen er å identifisere ild og røykutvikling i veinettet, for å varsle ved veiulykker. I dette tilfellet kan det være hensiktsmessig å ha et kamera som kan sende opptak hvis en hendelse blir detektert. Opptak i veien vil imidlertid føre til at Doorkeeper (eller kunden) behandler identifiserende informasjon, som for eksempel ansikter av sjåfører eller passasjerer og registreringsnummer på kjøretøy. I tillegg kan også annen tekst på biler være personopplysninger, ettersom for eksempel firmanavn ofte kan kobles mot en konkret fysisk person.

I dette tilfellet vil det være hensiktsmessig for den behandlingsansvarlige å begrense hva som samles inn av identifiserende informasjon i videostrømmen. Derfor vil sladding av både ansikter, biler (inkludert tekst som kan vise firmanavn og lignende) være hensiktsmessig for å ivareta dataminimeringsprinsippet.

Behandlingens nødvendighet og vurdering av alternative tiltak

Hvis den behandlingsansvarlige eksempelvis ønsker å forhindre kriminalitet mot egen eiendom, kan vedkommende i stedet for å installere et kameraovervåkingssystem vurdere å benytte alternative sikkerhetstiltak, for eksempel å gjerde inn eiendommen, sette inn regelmessig vakthold, bruke vakter, sørge for bedre belysning, installere sikkerhetslåser, innbruddssikre vinduer og dører eller påføre antigraffiti-belegg eller -folie på vegger. Den behandlingsansvarlige må i hvert enkelt tilfelle vurdere om slike tiltak kan gi en mindre inngripende løsning for personvernet for enkeltindivider.

Før den behandlingsansvarlige tar i bruk et kameraovervåkingssystem, er vedkommende forpliktet til å vurdere hvor og når kameraovervåking er nødvendig.

Hvem har ansvar for at prinsippene etterleves?

Etter personvernforordningen er det den behandlingsansvarlige som er ansvarlig for overholdelsen av kravene til behandling av personopplysninger – inkludert prinsippene om formålsbegrensning og dataminimering.

Den behandlingsansvarlige er den som bestemmer formålet med en behandling og hvilke midler – som tekniske løsninger – som skal brukes for å oppnå formålet. Hvem som er behandlingsansvarlig skal avgjøres på grunnlag av de faktiske forholdene. Det er med andre ord den som tar de faktiske beslutningene om hvorvidt en behandling skal gjennomføres, formålene med behandlingen og hvordan behandlingen skal gjennomføres, som regnes som den behandlingsansvarlige.

Den behandlingsansvarlige vil – som hovedregel – være kunden som kjøper et frittstående kamera, eller sikkerhets-/overvåkingssystemer der kameraovervåking inngår. I tilfeller der leverandøren behandler personopplysninger på vegne av kunden, vil denne være databehandler.

Avhengig av hvilke tjenester en leverandør av kamera tilbyr, kan det tenkes at leverandøren har behandlingsansvar for deler av behandlingen ved bruk av kameraovervåking. Det kan for eksempel hende at leverandøren behandler enkelte personopplysninger for å justere algoritmen etter en hendelse hos en kunde, slik at de kan sørge for at algoritmen

fungerer etter hensikt hos andre kunder. Dersom to eller flere behandlingsansvarlige, i fellesskap, fastsetter formålene og midlene for en behandling av personopplysninger, vil de være felles behandlingsansvarlige (artikkel 26). Dette sandkasseprosjektet har ikke tatt stilling til hvorvidt Doorkeeper er behandlingsansvarlig, felles behandlingsansvarlig eller databehandler etter personvernforordningen.

En leverandør av overvåkingssystemer, som etter en konkret vurdering ikke er å anse som behandlingsansvarlig, vil i utgangspunktet ikke ha et direkte ansvar for å overholde dataminimeringsprinsippet. Det er imidlertid viktig at systemet som leveres legger til rette for at den behandlingsansvarlige i praksis kan overholde regelverket. I motsatt fall vil ikke leverandørens kunder lovlig kunne benytte systemet til *behandling av personopplysninger*. Det er derfor viktig at Doorkeeper har et bevisst forhold til dataminimering ved utvikling av løsningen, uavhengig av om de er å anse som behandlingsansvarlig eller ikke.

Det samme vil gjelde for regelen om innebygd personvern i personvernforordningen artikkel 25. Bestemmelsen sier at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre effektiv gjennomføring av personvernprinsippene og ivaretagelse av de registrertes rettigheter og friheter i løsningen. Videre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. På lik linje med kravet til dataminimering skaper bestemmelsen om innebygd personvern en direkte forpliktelse for den behandlingsansvarlige, som også er relevant for Doorkeeper å ta hensyn til.

Fordi behandlingsansvarlige uansett må sørge for innebygd personvern i løsningene de benytter, synes det lettere å velge en løsning som allerede har dette bygd inn fra start, sammenlignet med å bygge personvern inn i en løsning som ikke har det. Tilpassing av ferdig utviklede løsninger i etterkant kan være kostbart. Løsninger med innebygd personvern kan derfor i mange tilfeller ha et konkurransefortrinn i forhold til løsninger som ikke har det.

Rettslig grunnlag for Doorkeepers bruk av intelligent videoanalyse

Et av målene i sandkassen var å vurdere hvordan rettslig grunnlag for bruk av intelligent videoanalyse skal vurderes, med utgangspunkt i Doorkeepers løsning.

Behandling av personopplysninger er bare lovlig dersom behandlingen har et *rettslig grunnlag* (jf. personvernforordningen artikkel 6 nr. 1 bokstav a–f).

- En oversikt over de rettslige grunnlagene finnes her: [Behandlingsgrunnlag | Datatilsynet](#). Se også kapittel 1 i Datatilsynets veileder om kameraovervåking [her](#).

Hvilke rettslige grunnlag er relevante for bruk av intelligent videoanalyse?

I enkelte situasjoner vil samtykke (etter artikkel 6 nr. 1 bokstav a) kunne utgjøre et rettslig grunnlag for kameraovervåkning. Det er likevel strenge krav til hva som anses som et gyldig samtykke etter personvernregelverket, og *samtykke* er derfor i mange tilfeller ikke egnet. Noen situasjoner hvor det kan tenkes at det vil være gyldig er, for eksempel, ved forskning, behandling på pasientrom, i omsorgsboliger eller lignende.

Et annet mulig rettslig grunnlag for bruk av kameraovervåking, er at tiltaket er *hjemlet i lov*. Dette vil imidlertid i hovedsak være mest relevant for offentlige virksomheter. For offentlige virksomheter vil det være mest relevant å vurdere artikkel 6 nr. 1 bokstav c og e som rettslige grunnlag. Disse involverer at personopplysninger kan behandles dersom det er nødvendig for å oppfylle en rettslig plikt, utføre en oppgave i allmennhetens interesse, eller for å utøve offentlig myndighet. Videre vil offentlige myndigheter ikke kunne bruke «interesseavveining» (jf. artikkel 6 nr. 1 bokstav f) under utførelsen av myndighetsoppgaver.

For private aktører som skal ta i bruk kameraovervåking, vil *samtykke*, eller *hjemmel i lov*, sjeldent være aktuelle rettslige grunnlag.

Nærmere om «berettiget interesse» som et rettslig grunnlag

Når private aktører skal vurdere bruk av kameraovervåking, vil det – i de fleste tilfeller – være «berettiget interesse» (jf. artikkel 6 nr. 1 bokstav f) som er det mest relevante grunnlaget. Denne bestemmelsen gir grunnlag for behandling av personopplysninger der behandlingen er nødvendig for formål knyttet til den behandlingsansvarliges eller tredjepersons berettigede interesser, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger.

For å kunne basere behandlingen på dette rettslige grunnlaget må det først foretas en avveining mellom den behandlingsansvarliges og de registrertes interesser. Den behandlingsansvarliges berettigede interesse må være lovlig, klart definert, reell og saklig begrunnet. Behandlingen må videre være *nødvendig* for å forfølge den berettigede interessen. I dette ligger det at kameraovervåkning må være et *egnet* virkemiddel for å oppnå formålet, og at formålet heller ikke med rimelighet kan oppnås effektivt gjennom mindre inngripende tiltak.

I interesseavveiningen må de registrertes interesser, rettigheter og friheter – herunder deres rimelige forventninger sett opp mot forholdet til den behandlingsansvarlige – vurderes opp mot den behandlingsansvarliges berettigede interesse. I relasjon til kameraovervåkning kan de registrertes interesser involvere retten til privatliv og personvern og kan knyttes til hvor inngripende overvåkingen er.

Hvis den behandlingsansvarlige vil knytte flere formål til den samme behandlingen av personopplysninger, må de vurdere det rettslige grunnlaget opp mot hvert av de enkelte formålene. Hvorvidt artikkel 6 nr. 1 bokstav f gir rettslig grunnlag for å behandle personopplysninger beror på en konkret vurdering for hver enkelt behandling.

Som hovedregel kan personopplysninger bare viderebehandles for nye formål som er forenelige med formålene som begrunnet den opprinnelige behandlingen, jf. artikkel 6 nr. 4. Dette er bare relevant for formål som eventuelt kommer til etter innsamlingstidspunktet. Alle formål som er aktuelle ved innsamlingstidspunktet må vurderes opp mot artikkel 6 nr. 1 på vanlig måte.

Teknologien som vurderingsmoment

Hvordan påvirker KI-teknologien som Doorkeeper har utviklet, avveiningen mellom en berettiget interesse til å overvåke og inngrepet i personvernet som overvåkingen fører til? Hvis vi utelukkende ser på hvordan personopplysninger behandles i løsningen, så kan Doorkeeper gjøre tiltak som gjør innsamlingen av opplysninger mindre inngripende.

- I en normalsituasjon behandles personopplysningene kun av Doorkeeper sin algoritme for å sladde videostrømmen. Opplysningene sladdes i sanntid og det lagres bare et tidsbegrenset opptak som slettes fortløpende – såfremt en forhåndsdefinert hendelse ikke har oppstått.
- Selv om personopplysninger behandles i løsningen, skal ingen personer få tilgang til den usladdede videostrømmen før systemet har oppdaget en forhåndsdefinert hendelse, eller dersom operatøren deaktiverer sladdingen manuelt.
- Operatører må oppgi årsak, tidsrom og bruker-ID om de vil deaktivere sladdingen manuelt. Hendelsen logges i systemet. Denne barrieren vil sannsynligvis bidra til å forhindre og avdekke snoking, dersom det er en ansvarlig og regelmessig gjennomgang av loggene.

Dette er alle relevante momenter når en virksomhet skal vurdere om den berettigede interessen utgjør et gyldig rettslig grunnlag og kan tippe vekten mot den berettigede interessen.

Doorkeepers løsning kan utformes ved at sladdingen av identifiserende opplysninger enten skjer i kamerahuset eller på en plattform. Den behandlingsansvarlige må vurdere hvilken betydning forskjellene i de ulike løsningene har for hvor inngripende behandlingen av personopplysninger vil være. Plattform-løsningen innebærer behandling av personopplysninger i større utstrekning enn løsningen med sladding i kamerahus, ettersom opplysningene må overføres fra kameraet til plattformen før de sladdes. Den behandlingsansvarlige bør blant annet vurdere om en løsning med sladding i kamerahuset derfor i noen tilfeller kan vurderes som mindre inngripende enn på plattform.

Opplevelsen av å bli overvåket som et vurderingsmoment

I vurderingen av hvor stort inngrepet i personvernet er for de registrerte, må man ta utgangspunkt i den faktiske behandlingen av personopplysninger. I tillegg er følelsen av å bli overvåket også relevant. Denne følelsen ligger til grunn for regelen om uekte kamerautstyr i personopplysningsloven § 31. I forarbeidene til denne bestemmelsen vises det til at «uekte overvåkingsutstyr kan oppleves som et stort inngrep i personvernet selv om det ikke finner sted noen reell behandling av personopplysninger, og ... at følelsen av å bli overvåket i seg selv er integritetskrenkende og dermed egnet til å medføre endringer i atferd».

Den registrerte vil altså kunne oppleve seg overvåket uavhengig av hvor inngripende behandlingen av personopplysninger faktisk er. Teknologien som blir brukt har ikke nødvendigvis innvirkning på denne følelsen, da den registrerte i de fleste tilfeller ikke har tilstrekkelig kunnskap om hvordan teknologien fungerer. Dette er et moment man må ta med i vurderingen av den registrertes interesser. Her kan imidlertid åpenhet og god informasjon ha en rolle.

Et viktig moment i vurderingen av hvor inngripende overvåking oppleves, er hvilke forventninger den registrerte har til den behandlingsansvarlige. Her vil konteksten for behandlingen kunne ha stor betydning. Det finnes situasjoner hvor den registrerte i større grad forventer privatliv, slik som for eksempel i treningsstudio, spa og badebasseng. I andre situasjoner, som for eksempel på kollektivtransport eller i en butikk, vil den enkelte som regel ha en lavere forventning om privatliv.

I noen tilfeller vil det at et område er kameraovervåket oppleves som en trygghet for de registrerte. Et kamera kan i noen tilfeller ha en preventiv effekt for å unngå kriminelle hendelser og samtidig gi en økt opplevelse av sikkerhet. Dette kan også være et relevante momenter i vurderingen av den registrertes interesser.

Vurdering av tre brukseksempler

I sandkasseprosjektet har vi sett på hvordan Doorkeepers teknologi kan påvirke vurderingen av rettslige grunnlag i forbindelse med kameraovervåking. For å synliggjøre noen av de relevante problemstillingene, ser vi i dette kapittelet nærmere på tre brukseksempler for Doorkeepers teknologi. Eksempelene er valgt fordi de representerer mulige bruksområder for Doorkeepers løsning. Samtidig reiser de også problemstillinger som er overførbare for andre virksomheter som skal utvikle lignende løsninger.

Eksempelene vi har valgt å se nærmere på er:

1. Kameraovervåking av fasade på et næringsbygg med formål å unngå tyveri
2. Kameraovervåking i gatebildet med formål å sikre virksomhetens omdømme
3. Bruk av kamera for å detektere ild og røyk på ytterveggene av en stavkirke

Det første eksempelet gjelder en situasjon hvor det i mange tilfeller vil finnes rettslig grunnlag for å sette opp kameraovervåking i dag. I eksempelet drøfter vi derfor hvilken betydning Doorkeeper sin teknologi har for vurderingen av rettslig grunnlag i disse situasjonene.

Det andre eksempelet gjelder et tilfelle hvor det i utgangspunktet *ikke* er lovlig for private aktører å sette opp kameraovervåking. I eksempelet drøfter vi om Doorkeeper sin teknologi kan gjøre det mulig å bruke kameraovervåking i større utstrekning enn i dag.

I det tredje eksempelet beskriver vi et tilfelle hvor bruk av kamera uten sladding og med løpende opptak ikke vil oppfylle kravet til nødvendighet i vurderingen av det rettslige grunnlag. Deretter drøfter vi om bruk av en type kameraovervåkingsløsning – slik som den Doorkeeper tilbyr – likevel kan oppfylle dette kravet.

Felles for alle eksemplene er at opptak kun lagres midlertidig i et kort intervall, men mindre en forhåndsdefinert hendelse blir detektert.

I det følgende skal vi vurdere Doorkeepers teknologi opp mot «berettiget interesse» som et rettslig grunnlag for overvåkingen og hvilken betydning teknologien har for vurderingen av kravet til nødvendighet når det kommer til rettslig grunnlag (jf. artikkel 6 i personvernforordningen). Felles for eksemplene er at det vurderes å sette opp overvåkingskamera på steder der allmennheten ferdes. Flere momenter i vurderingen vil være felles for disse eksemplene.

En overordnet problemstilling er hvilken betydning Doorkeeper sin teknologi har for utfallet av vurderingen av rettslig grunnlag og om dette skiller seg fra kameraovervåking uten tilsvarende sladdefunksjon og med løpende opptak.

Eksempelene gir ikke en uttømmende behandling av alle momenter som er relevante å ta i betraktning i vurderingen av rettslig grunnlag, men fokuserer på de elementene som vi mener er særlig relevante å vurdere sett hen til Doorkeeper sin teknologi.

For generell informasjon om lovlighet ved bruk av kameraovervåking, se Datatilsynets veileder [her](#).

1. Eksempel 1: Overvåking av fasade på et næringsbygg med formål å unngå tyveri

Det første brukseksemplet gjelder kameraovervåking av fasaden på et forretningslokale i en gågate. I dette eksemplet er den behandlingsansvarlige en privat virksomhet som eier lokalet.

Virksomhetens formål med overvåkingen er å forhindre og å varsle om innbrudd. Løsningen skal gjøre dette ved å registrere og sende et varsel hvis noen knuser butikkvinduet og går inn i lokalet. Når tjenesteleverandøren installerer kameraet, vinkler de det mot fasaden. Løsningen er konfigurert slik at menneskeformer sladdes i videostrømmen.

I en normalsituasjon gjøres det ikke opptak i kameraet (med unntak av en tidsbegrenset lagring i hurtigminnet – «cache») eller på plattformen. Opptak vil først aktiveres dersom løsningen registrerer at butikkvinduet er knust.

Vurdering

I mange tilfeller vil bruk av kameraovervåking være tillatt også der det gjøres kontinuerlig opptak og hvor mennesker ikke sladdes fra videostrømmen. Derfor er spørsmålet i dette eksempelet hvorvidt Doorkeepers løsning påvirker vurderingen av det rettslige grunnlaget, og om valget mellom sladding i kamera eller på plattform har betydning for denne vurderingen.

Forebygging av kriminalitet rettet mot virksomheten kan være en berettiget interesse, og forebygging av og varsling om innbrudd og tyveri kan være legitime formål som den behandlingsansvarlige kan forfølge. Denne vurderingen vil likevel være betinget av at faren for slike hendelser er reell – hvis ikke er heller ikke interessen i å beskytte seg mot slike hendelser reell.

Kameraovervåkingen må begrenses til det som er nødvendig i tid og rom. Dersom risikoen for innbrudd kun er reell etter stengt tid, kan det ikke overvåkes innenfor virksomhetens åpningstid. Som hovedregel er det kun offentlige myndigheter som kan overvåke et offentlig sted, men det kan likevel være tillatt for private aktører å fange opp en uvesentlig del av offentlig gate dersom det er nødvendig, eksempelvis rett nedenfor butikkens fasade.

I forkant av å installere et overvåkingskamera må den behandlingsansvarlige vurdere andre alternative tiltak. Alternative tiltak som kan være egnet til å oppnå formålet er fysisk sikring, vakthold og andre typer alarmsystemer som ikke innebærer behandling av personopplysninger. Dersom alternative tiltak ikke er egnet, må den behandlingsansvarlige også vurdere hvilken type kamerateknologi som er nødvendig for å oppnå formålet. I dette eksempelet vil det bare være nødvendig å fange opp mennesker når en deteksjon av fasadebrudd har gått.

Siden kameraet fanger opp og varsler om fasadebrudd, kan det være egnet til å oppnå formålet. Dette tilsier at bruken av Doorkeepers løsning kan oppfylle kravet til *nødvendighet*. Løsningen gjør det også lettere å kun behandle personopplysninger i det omfanget som er *nødvendig* for å oppnå formålet, siden personer sladdes umiddelbart med mindre de fanges opp når alarm har blitt utløst.

Når kameraet som er rettet mot fasaden befinner seg utenfor butikken, ved en gågate, vil kameraet potensielt fange opp svært mange personer, inkludert forbipasserende. Dette kan til en viss grad begrenses gjennom vinkling og/eller sladding av områder som ikke er nødvendige å overvåke. Likevel, omfanget av registrerte er i alle tilfeller uforutsigbart og kan endre karakter avhengig av tid på døgnet, ukedag, og hvorvidt det er andre virksomheter og arrangementer i nærheten.

I en gågate vil de registrerte ha en viss forventning om å fanges opp av overvåkingskameraer inne i forretningene i åpningstiden, men også til en viss grad i umiddelbar nærhet utenfor på andre tider av døgnet. Dette kan tale for at bruk av overvåkingskamera som er montert utenfor og rettet mot butikken, i en gågate, som utgangspunkt ikke oppleves som særlig inngripende.

Doorkeepers løsning vil også rent faktisk være mindre inngripende for personene som blir fanget opp av kameraet, sammenlignet med kamera hvor det kontinuerlig lagres opptak uten sladding av mennesker. Behandlingen av personopplysninger for de aller fleste som fanges opp av kameraet vil være svært begrenset. Likevel, i dette eksempelet vil Doorkeepers dataminimerende løsning kanskje ikke ha betydelig innvirkning på de registrertes følelse av å bli overvåket og oppfatning av hvor inngripende overvåkingen er. Overvåking i gågate gjør det mindre sannsynlig at forbipasserende og kunder blir oppmerksomme på typen kamerateknologi selv om det er skiltet med informasjon om hvordan løsningen fungerer. Det vil derfor ikke nødvendigvis være samsvar mellom de registrertes oppfatning og den reelle behandlingen av personopplysninger.

Oppsummering

I dette eksempelet vil det være hensiktsmessig å konfigurere overvåkingskameraet slik at tiltaket i større grad ivaretar kravene til dataminimering. I kravet til nødvendighet ligger det en plikt for den behandlingsansvarlige til å velge den minst inngripende teknologien som er egnet til å oppnå formålet med overvåkingen. Når mer personvernvennlig teknologi blir tilgjengelig, endres også vurderingen av hvilken behandling av personopplysninger som er nødvendig for å oppnå formålet. Teknologien påvirker imidlertid ikke nødvendigvis de registrertes følelse av å bli overvåket, og inngripen i personvernet må derfor vurderes i likhet med andre kameraovervåkingsløsninger når det kommer til opplevelsen av å bli overvåket.

2. Eksempel 2: Overvåking i gatebildet med formål å verne virksomhetens omdømme

I forlengelsen av det forrige eksempelet, så ønsker virksomheten også å overvåke lenger ut i gågaten. Formålet med dette er å forbygge, oppdage og varsle om uønskede hendelser som ikke direkte retter seg mot virksomheten, men som likevel kan påvirke virksomhetens omdømme og økonomiske interesser. Dette kan omfatte aktiviteter som gjør at området virksomheten ligger i oppfattes som mer utrygt – og derfor mindre attraktivt å oppsøke for potensielle kunder.

I dette eksempelet kan formålet oppnås gjennom at kamerateknologien kan gjenkjenne objekter som våpen (for eksempel store kniver), i tillegg til den generelle forbyggende effekten av synlig kameraovervåking av området.

Vurdering

Spørsmålet er her om Doorkeepers løsning med objektgjenkjenning og sladding av menneskeformer kan gjøre at virksomheten har rettslig grunnlag til å overvåke lenger ut i gaten, for formål av en mer generell karakter.

Å trygge området i nærheten av virksomheten vil – isolert sett – kunne være en berettiget interesse dersom risikoen for uønskede hendelser er reell og forutsatt at virksomheten berøres direkte eller indirekte. Forebygging av uønskede hendelser eller kriminalitet i det offentlige rom er imidlertid en oppgave som er lagt til offentlige myndigheter, hovedsakelig politiet. Dette kan tilsi at å sørge for at orden på et offentlig sted ikke er en *berettiget interesse* som kan forfølges av private virksomheter, selv om de kan påvirkes negativt av kriminalitet eller andre uønskede hendelser i området.

Hovedregelen er også at bare offentlige myndigheter kan overvåke offentlige steder. Politiet har hjemmel til å bruke kameraovervåking for politimessige formål, herunder å forebygge og stanse kriminell virksomhet. Doorkeepers løsning kan ikke påvirke vurderingen av om virksomheten har en berettiget interesse eller et berettiget formål med overvåkningen.

Vurderingen, i dette eksemplet, er at kameraovervåking kan være nødvendig for å oppnå formålet, men at overvåkningen likevel *ikke* vil være tillatt så lenge formålet med den ikke er legitimt å forfølge for virksomheten.

De registrerte kan ha en forventning om at gaten overvåkes, men da av offentlige myndigheter, ikke av virksomhetene som har lokaler der. Dette kan tilsi at de registrertes rettigheter og interesser uansett vil måtte gå foran virksomhetens interesse i overvåking.

Oppsummering

Valg av en dataminimerende teknologi vil ikke senke terskelen for hva som er lovlig kameraovervåking i tilfeller der virksomheten ikke har en berettiget interesse med overvåkningen.

3. Eksempel 3: Bruk av kamera for å detektere ild og røyk på ytterveggene av en stavkirke

I det siste eksempelet vurderes bruk av kameraovervåking av ytterveggen på en stavkirke med hensikt å kunne utløse alarm ved branntilløp.

I dette eksempelet er formålet med kameraovervåkingen deteksjon av ild og røyk for å raskt kunne slukke en eventuell brann og avverge skader på bygningen. Kameraet vil fungere som en sensor som fanger opp flamme- eller røykmønster, og det vil konfigureres slik at menneskeformer sladdes i videostreamen. Kameraløsningen kan innrettes slik at sladdingen ikke kan fjernes og uten at videostreamen mellomlagres («cache»).

Selv om formålet i dette eksempelet ikke er å fange opp personer på videostreamen, så vil overvåkingen likevel innebære en behandling av personopplysninger som krever et rettslig grunnlag etter personvernforordningen. Dette er fordi personer som beveger seg rundt kirken kan fanges opp av kameraet.

For dette eksempelet kan det være relevant å vurdere ulike rettslige grunnlag. Om det er en offentlig eller privat aktør som er behandlingsansvarlig vil påvirke denne vurderingen. Uavhengig av hvilket rettslig grunnlag en slik behandling er

basert på, så er det et krav om at behandlingen skal være «nødvendig», jf. dataminimeringsprinsippet. I det følgende drøfter vi kravet til *nødvendighet* og deretter si noe om interesseavveiningen (under artikkel 6 nr. 1 bokstav f). Vi legger til grunn at det å slukke brann og avverge skader på en stavkirke er en *berettiget interesse* i tråd med artikkel 6 nr. 1 bokstav f.

Vurdering

I dette eksempelet er det særlig interessant å vurdere om Doorkeepers løsning kan anses «nødvendig» i et tilfelle der en kameraovervåkingsløsning uten sladding og med løpende opptak ikke vil oppfylle kravet til nødvendighet.

En løsning uten sladding og med lagring av opptak vil i de fleste tilfeller ikke oppfylle kravet til nødvendighet, fordi formålet med rimelighet vil kunne oppnås effektivt med andre og mindre inngripende midler. Som beskrevet i eksemplene ovenfor, så vil Doorkeeper sin teknologi behandle personopplysninger i mindre utstrekning enn en løsning uten de samme sladd-egenskapene og med lagring av opptak. Behandlingen vil på denne måten være mindre inngripende for de registrerte.

Et kamera som ikke har en alarmfunksjon, vil heller ikke være like godt egnet til å oppfylle formålet med behandlingen. Dersom et slikt kamera skal kunne brukes til å oppdage røyk eller ild, så forutsetter det at en eller flere personer kontinuerlig følger med på videostreamen og klarer å fange opp en eventuell røykutvikling. Dette vil antageligvis ikke være en særlig praktisk løsning, og det vil være svært inngripende for de registrerte.

For formålet å oppdage ild eller røyk, vil en røykvarsler eller en annen sensor være et nærliggende alternativ. Et ild- og røykvarslingssystem som innebærer bruk av kameraovervåking vil være mer inngripende for de registrerte enn bruk av røykvarsler eller lignende sensorer. Dette er fordi det behandles personopplysninger i kameraovervåkingsløsningen. Dersom Doorkeepers løsning likevel er bedre egnet til å oppnå formålet enn det mindre inngripende alternativ er, så kan kravet til nødvendighet være oppfylt. Et sentralt spørsmål er dermed om Doorkeepers løsning er bedre egnet til å oppdage ild og røyk enn et brannvarslingssystem basert på sensor.

Ifølge Doorkeeper er det vanskelig å styre ild eller røyk inn i en sensor ved brann på en yttervegg. Røykdeteksjon reagerer ofte for sent, fordi røyken først samler seg når brannen er godt i gang eller ferdig brent. Det kan ikke monteres varmedetekterende kabel på vernede bygg, og dette er heller ikke en effektiv måte å oppdage brann på. Ifølge tester Doorkeeper har fått gjennomført, så vil en type sensor med kabel bruke åtte minutter før en alarm utløses, mens for Doorkeepers kameraløsning tar det seks sekunder. Dette kan bety svært mye for å redde bygget. Datatilsynet legger til grunn Doorkeepers beskrivelse av denne funksjonen for vår vurdering.

I dette eksemplet vurderte vi det slik at Doorkeeper sin kameraløsning kan oppfylle nødvendighetskravet, da løsningen kan innebære en betraktelig mer effektiv brannvarsling enn de beskrevne alternativene med røykvarsler eller lignende sensorer. Bruk av en type kamerateknologi slik Doorkeeper beskriver, kan på denne måten oppfylle kravet til nødvendighet i en situasjon der en kameraovervåkingsløsning uten sladding og med løpende opptak trolig ikke vil gjøre det.

Når det kommer til interesseavveiningen, kan det å sikre en stavkirke mot brann vurderes som en tungtveiende interesse. Samtidig vil det kunne oppleves inngripende å bli videoovervåket i forbindelse med besøk til en kirke – hvor de registrerte kan ha lavere forventning til å bli overvåket enn for eksempel i et butikklokale. Likevel, de registrerte kan også ha en forventning om at en stavkirke beskyttes mot brann og andre skader og at dette kan inkludere kameraovervåking. Dataminimeringen i Doorkeeper sin løsning innebærer at den faktiske behandlingen av personopplysninger vil være svært begrenset og dette vil kunne gjøre det enklere å konkludere at det kan settes opp. I dette eksempelet kan dermed dataminimeringen i Doorkeeper sin løsning bidra til at interesseavveiningen slår ut i favør av kameraovervåking.

Oppsummering

Bruk av en type kamerateknologi slik Doorkeeper beskriver det, kan trolig oppfylle kravet til nødvendighet i en situasjon der det blir brukt til å oppdage brann på ytterveggen av en stavkirke. Dette forutsetter at løsningen er bedre egnet til å oppnå formålet enn det mindre inngripende løsninger er, slik som for eksempel en røykvarsler.

Dataminimeringen i Doorkeeper sin kameraovervåkingsløsning gjør at behandlingen av personopplysninger vil være svært begrenset. Interesseavveiningen kan muligens slå ut i favør av kameraovervåking i dette eksempelet.

Hvordan vil valg av utforming påvirke vurderingen av det rettslige grunnlaget?

I alle brukseksemplene vil de juridiske vurderingene kunne påvirkes av hvilken utformingen Doorkeepers løsning har. Deres løsning kan utformes på to forskjellige måter: ved at sladdingen av menneskeformer og andre identifiserende opplysninger enten skjer i kamerahuset eller på en plattform. Den behandlingsansvarlige må vurdere hvilken betydning forskjellene i de ulike løsningene har for hvor inngripende behandlingen av personopplysninger vil være for de registrerte i det konkrete tilfellet.

Selv om de to løsningene kan innrettes med samme nivå av sikkerhet, vil sårbarhetsflaten være større for løsningen med sladding på plattform, i forhold til der hvor sladdingen skjer i kamerahuset. Plattform-løsningen innebærer behandling av personopplysninger i flere ledd enn løsningen med sladding i kamerahuset. Dette er fordi at ved sladding på plattform, vil opplysninger overføres fra kameraet til plattformen før de sladdes. En løsning med sladding i kamerahuset – som involverer færre ledd – vil derfor i noen tilfeller kunne vurderes som mindre inngripende enn løsningen med sladding på plattform. Dette er blant annet fordi flere har tilgang til plattformen?

Videre kan det tenkes at dersom de registrerte har kjennskap til løsningene, så vil de oppleve en løsning hvor videostrømmen sladdes i kamerahuset som mindre inngripende, i forhold til en utforming hvor videostrømmen sendes til en plattform før sladdingen bli gjort. Dette forutsetter imidlertid god informasjon til de registrerte og vil derfor trolig ha størst relevans der kameraet er satt opp på et område der den behandlingsansvarlige har en viss kontroll med at man får gitt tilstrekkelig informasjon til de som beveger seg inn på området.

Utformingen av løsningen kan derfor ha betydning for vurderingen av det rettslige grunnlaget. Risikoen for at personopplysningene kan komme til å behandles på en måte som ikke var tilsiktet, vil være et element i helhetsvurderingen når man vurderer hvilke av de to løsningene som skal brukes. Det er den behandlingsansvarlige som må vurdere i det konkrete tilfellet om forskjellen mellom utformingene tilsier at det ene alternativet må velges over den andre.

Særlige kategorier av personopplysninger

En særlig problemstilling ved bruk av kameraovervåking er at det kan være vanskelig å vite i forkant hvilke opplysninger man kommer til å behandle. I alle brukseksemplene er det en risiko for at særlige kategorier med personopplysninger blir behandlet. Som særlige kategorier regnes personopplysninger om etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering (se forordningen artikkel 9).

Før en behandlingsansvarlig setter opp et videokamera, er det viktig å vurdere om den aktuelle behandlingen kan innebære behandling av denne type personopplysninger. Dette er særlig aktuelt for eksempelet hvor det settes opp kamera utenfor en stavkirke der det avholdes gudstjenester. I et slik eksempel vil det være relevant å ta stilling til om det behandles opplysninger om de registrertes tilhørighet til en religion. I tråd med dataminimeringsprinsippet bør den behandlingsansvarlige utforske hvordan kameraet kan vinkles for å – i størst mulig grad – unngå å behandle personopplysninger.

Behandling av særlige kategorier opplysninger er i utgangspunktet forbudt. Dersom man kommer til at særlige kategorier omfattes av behandlingen, må man oppfylle et av unntakene i artikkel 9 andre ledd for at behandlingen skal være lovlig.

Det Europeiske Personvernrådet viser i sin veileder fra 2020 (EDPB Guidelines 3/2019, side 17) til at selv om videoovervåking er egnet for å samle inn store mengder opplysninger, så vil det ikke alltid innebære behandling av særlige kategorier opplysninger. Dersom videoopptak blir behandlet med hensikt å avdekke særlige kategorier av personopplysninger, så vil artikkel 9 komme til anvendelse.

I august 2022 kom det en dom fra EU-domstolen (C-184/20) som legger opp til en betydelig videre tolkning av hva som anses å være særlige kategorier personopplysninger etter artikkel 9. I den aktuelle saken kom EU-domstolen til at opplysninger om en fysisk persons seksuelle orientering indirekte kunne utledes av informasjon om ektefelles navn, og at dette var omfattet av begrepet «særlige kategorier» i artikkel 9.

Domstolen peker blant annet på at det skal undersøkes om opplysninger som «.... gjennom en intellektuel refleksjon, som består i sammenstilling eller deduksjon» kan avsløre denne type informasjon (se premiss 120 og 123). Videre viser domstolen til at formålene bak personvernforordningen støtter opp under en bred fortolkning av begrepet «særlige kategorier personopplysninger», idet det «består i at sikre et højt niveau for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred» (se premiss 125 og 127). Samtidig synes domstolen å legge stor vekt på konteksten i den aktuelle saken.

Domstolen legger her til grunn at uttrykket «særlige kategorier» i artikkel 9 favner temmelig vidt. Samtidig gir ikke domstolen noen klar veiledning om hvordan den konkrete vurderingen skal foretas eller hvilke utslag vurderingen kan få i andre type situasjoner der personopplysninger behandles. Det er usikkert hvor grensen går for hvilke behandlinger som skal anses å indirekte avsløre særlige kategorier personopplysninger og trigge anvendelsen av artikkel 9. Likevel, dommen er relevant å ta i betraktning når en behandlingsansvarlig vurderer å bruke kameraovervåking. Datatilsynet oppfordrer behandlingsansvarlige til å følge med på rettsutviklingen.

Utlevering av personopplysninger

Et av målene i sandkassen var å vurdere om bruk av Doorkeeper sin teknologi påvirker vurderingen av om en virksomhet har rettslig grunnlag for å utlevere videoopptak.

Virksomheter som har overvåkingskamera kan oppleve å bli bedt om å utlevere opptak, for eksempel av politiet eller forsikringsselskaper. Personopplysningene som det da vil dreie seg om er i hovedsak opptak som har blitt lagret som følge av at et opptak er aktivert ved en registrert hendelse.

Dataminimeringen i løsningen kan gjøre det enklere rent praktisk å utlevere opptak på den måten at man har færre personopplysninger å forholde seg til. Likevel, for de personopplysningene den behandlingsansvarlige behandler, så vil reglene som gjelder for utlevering være de samme som ellers. De rettslige vurderingene for utlevering av personopplysninger ved bruk av Doorkeeper sin teknologi vil altså være de samme som ved bruk av annen kamerateknologi.

Utlevering av personopplysninger er en behandling av personopplysninger. For å kunne utlevere personopplysninger, må man derfor ha et rettslig grunnlag etter artikkel 6 i personvernforordningen. Ofte vil det være mest aktuelt å innhente samtykke fra de som er på opptakene, men det kan også foreligge andre rettslige grunnlag for utleveringen.

Personopplysninger kan gjenbrukes til nye formål dersom det nye formålet er forenelig med det opprinnelige formålet som personopplysningene ble samlet inn for. Det må også foreligge et rettslig grunnlag for den nye behandlingen, se artikkel 6(4) i personvernforordningen.

- **Utlevering av personopplysninger til andre virksomheter**

I sandkassen diskuterte vi om det var mulig for behandlingsansvarlig å utlevere opptak av hendelser til forsikringsselskap. Datatilsynets vurdering er at denne problemstillingen følger de generelle bestemmelsene som gjelder for all utlevering av personopplysninger. Dette vil si at en virksomhet må ha et rettslig grunnlag for å utlevere personopplysninger.

- **Utlevering av personopplysninger til politiet**

Hvis den behandlingsansvarlige får en henvendelse fra politiet om å utlevere opptak av registrerte personer, så må de selv vurdere om de har rettslig grunnlag for å utlevere personopplysningene. Dersom politiet har et utleveringspålegg, vil den behandlingsansvarlige som regel ha en plikt til å utlevere opplysninger. I andre tilfeller bør den behandlingsansvarlige kunne motta tilstrekkelig informasjon fra politiet, for å kunne vurdere om det er andre rettslige grunnlag for utlevering.

- **Den registrertes innsynsrett**

Den registrerte – som blir fanget opp av overvåkingskameraet – har en rett til innsyn i egne personopplysninger. Dette følger av artikkel 15 i personvernforordningen. Ved utlevering av opptak til den registrerte må behandlingsansvarlig ta stilling til om det å gi innsyn har negativ innvirkning på andres rettigheter og friheter. Her kan sladding av tredjepersoner nettopp være et tiltak for å minske slik negativ virkning hvis andre personer er å se i videostrømmen.

Sikkerhetsutfordringer

I dette kapittelet vil vi løfte noen sikkerhetsutfordringer som er aktuelle ved den type teknologi som Doorkeeper vil bruke, og gi noen overordnede kommentarer om de juridiske kravene til sikkerhet.

Sikkerhet er et stort tema, som i mange tilfeller er et premiss for et godt personvern. Det er vanskelig å sørge for personvernet uten tilstrekkelig sikkerhet. I denne rapporten har vi ikke muligheten til å dekke sikkerhet i sin helhet. Vi tar derfor kun med det som ble diskutert i arbeidsmøtene med Doorkeeper.

Rettslig krav til personopplysningssikkerhet

Personvernforordningen [artikkel 32](#) regulerer kravene til personopplysningssikkerhet. Både Doorkeeper og kundene deres er forpliktet til å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen». Hvilke tiltak som er påkrevd for å etterleve regelverket vil derfor variere i takt med risikoene som de ulike virksomhetene er utsatt for og det generelle risikonivået i samfunnet. Som leverandør og utvikler av løsningen bør Doorkeeper sørge for at de kan tilby en svært sikker løsning.

Doorkeeper må videre sørge for at sikkerheten i løsningen er *vedvarende*, både ved at sikkerheten i løsningen følger den tekniske utviklingen, og at eventuelle sårbarheter blir adressert fortløpende. En god måte å sørge for vedvarende sikkerhet på er å være i forkant – å stadig følge med på hva som anses for å være beste praksis og kontinuerlig implementere beste praksis i produktene en utvikler.

Loven stiller krav til både tekniske og organisatoriske tiltak. «Organisatorisk» må forstås vidt og kan også omfatte fysiske tiltak. For å sikre konfidensialiteten til personer som er underlagt lovlig kameraovervåking kan det altså være aktuelt med en rekke forskjellige tiltak. Eksempler på slike tiltak er å:

- sikre rommet som det overvåkes fra, slik at uvedkommende ikke kan komme inn eller se skjermene fra utsiden
- utarbeide rutiner for bruk av systemet
- sørge for tilstrekkelig hendelseshåndtering
- grundig opplæring av brukerne
- forplikte brukerne til en taushetserklæring
- definere tilgangen til ulike brukerkontoer
- utarbeide rutiner for regelmessig gjennomgang av loggene

Sikring av kommunikasjonen mellom kamera og plattform

Ett av diskusjonstemaene i arbeidsmøtene var sikring av kommunikasjonen mellom kamera og plattform i Doorkeepers løsning. Vil de to utformingene til oppsettet av løsningen påvirke hvilke sikkerhetstiltak Doorkeeper må iverksette i tråd med personvernregelverket?

Hvis videostreamen som kameraet sender fra seg ikke inneholder opplysninger om identifiserbare enkeltpersoner, så vil personvernregelverket kun komme til anvendelse for behandlingen som skjer inni kameraet (og ikke kommunikasjonen videre til plattformen). Dette forutsetter imidlertid at kameraet til enhver tid sender fra seg helt anonyme opplysninger, som sannsynligvis ikke vil være tilfelle for Doorkeeper sin løsning.

Terskelen for å kunne kalle en opplysning for anonym er svært høy. Selv ved sladding av hele menneskekropper vil det ikke være mulig å utelukke at noen av sladdene sannsynligvis vil ha en utforming som gjør at man kan knytte dem til enkeltpersoner. For eksempel en relativt høy person som passerer på samme sted til omtrent samme tid hver dag.

Ettersom det neppe vil være mulig å garantere full anonymitet ved sladding, og kameraet selv ved utforming A tidvis skal kunne sende usladdet video, bør utgangspunktet være at kommunikasjonen mellom kamera og plattform sikres som om det alltid overføres personopplysninger. Dette synes likevel ikke som noen stor utfordring, ettersom de aller fleste moderne overvåkingskameraer har en form for innebygget kommunikasjonssikkerhet, for eksempel i form av transportkryptering («transport layer security»).

I løsninger hvor det ikke brukes kryptering, må den behandlingsansvarlige – og eventuelle databehandlere – kompensere med andre tiltak for å sikre at uvedkommende ikke kan få tilgang til å se eller endre videostreamen.

Det følger logisk at løsninger som gjør analyse og sladding i kamerahuset (utforming A), sannsynligvis medfører lavere risiko enn løsninger som gjør tilsvarende på en plattform (utforming B). Dette er blant annet fordi videostrømmen ved utforming A ikke overføres over et nettverk før den behandles, med mindre en hendelse oppdages og sladdingen fjernes. Uvedkommende som tilegner seg tilgang til videostrømmen vil derfor vanligvis kun få tilgang til sladdet video. Ved å redusere mengden opplysninger som overføres reduserer en også sårbarhetsflaten, fordi en angriper bare kan få tilgang til usladdet video ved å tilegne seg tilgang til videostrømmen gjennom programvaren i selve kameraet. At risikoen kan være lavere ved utforming A betyr imidlertid ikke at utforming B må medføre uakseptabel risiko. Dette må vurderes opp mot hvilke andre sikkerhetstiltak man kan iverksette. Det samme vil gjelde for løsninger som ikke tar i bruk noen form for videoanalyse eller sladding.

Det er opp til de behandlingsansvarlige og databehandlerne å vurdere om de innebygde sikringstiltakene i kameraene er tilstrekkelige. Da sandkasseprosjektet startet, hadde Doorkeeper allerede lagt opp til at løsningene deres benytter egne nettverk som var separate fra kundens. Formålet med dette var å unngå utfordringer og risikoer ved bruk av nettverk som Doorkeeper ikke kan kontrollere. Diskusjonene vi hadde i sandkassen førte til at Doorkeeper gjorde ytterligere endringer i løsningen deres, hvor de ønsker å benytte en VPN-løsning («Virtual Private Network») som leveres av en tredjepart for å ytterligere sikre kommunikasjonen mellom kameraene og plattformen. Slik vil de skape ende-til-ende kryptering mellom kamera og plattform, og dermed sikre kommunikasjonen bedre enn med alminnelig transportkryptering. Dette kan øke sikkerheten i begge tilnærmingene til Doorkeeper.

Regelmessig oppdatering av produktene

Gjennom diskusjonene i sandkassen har Doorkeeper forklart at kameraer med kjente sårbarheter, som ikke blir reparert, er en utfordring for sikkerhetsbransjen. Noen virksomheter fortsetter å benytte slike kameraer uten å installere oppdateringer, ofte til tross for at produsenten har gjort oppdateringer tilgjengelige.

Hvis det ikke iverksettes tiltak for å fjerne sårbarheter vil det føre til høyere risiko og kan medføre brudd på personvernregelverket. Det er også verdt å påpeke at jo færre aktører man har i leverandørkjeden, jo færre aktører må man forholde seg til for å holde produktene man bruker oppdatert.

En sårbarhet i en VPN-løsning kan føre til at uvedkommende får tilgang til en virksomhet sitt interne nettverk. Tilsvarende kan en sårbarhet i et kamera føre til at uvedkommende får tilgang til videostrømmen. Når angripere får kjennskap til sårbarheter, vil de generelt sett forsøke å utnytte dem så fort som mulig. Produsentene må derfor publisere oppdateringer så fort som mulig når sårbarheter blir kjent for dem, slik at sikkerheten kan opprettholdes. Det kan imidlertid være flere årsaker til at produsenten ikke lager oppdateringer til det aktuelle produktet. For eksempel at produsenten har stanset produktstøtten, at produsenten mangler evne til å støtte produktene sine eller at produsenten har gått konkurs. Hvis det ikke er mulig å få tak i oppdateringer fra produsenten, må de behandlingsansvarlige eller databehandlerne vurdere om sårbarheten kan fjernes med andre tiltak eller om utstyret må erstattes.

Det er vel så viktig å ha en mekanisme for å få med seg nyheter om sårbarheter i produktene man benytter, som å faktisk oppdatere produktene. Hvis man ikke vet om sårbarhetene, mangler man forutsetninger for å gjøre noe med dem.

Styring av tilgang

Styring av tilgang til både kameraene og plattformen i et videoovervåkingssystem er nødvendig for å sørge for at videostrømmen kun er tilgjengelig for de som skal ha tilgang den, for å unngå snoking eller for å unngå at opplysninger fra overvåkingen blir brukt til andre formål enn det som opprinnelig ble fastsatt. For Doorkeeper og deres kunder vil det blant annet si at de må vurdere hvem som skal ha tilgang til systemene og hvor vide tilgangene skal være. Det kan for eksempel handle om en bruker sin tilgang til å

- følge med på videostrømmen,
- fjerne sladdingen manuelt,
- gjennomgå lagrede opptak,
- manuelt slette opptak som ble satt i gang ved en feil eller
- oppdatere kameraer og andre deler av systemet.

En operatør som skal følge med på den aktuelle videostrømmen må nødvendigvis ha tilgang til å se videostrømmen, men vil antageligvis ikke trenge tilgang til å installere systemoppdateringer. Direktøren i virksomheten vil sannsynligvis ikke trenge tilgang til noe annet enn opptakene som er lagret i etterkant av en reell hendelse. Administratoren av

systemet vil trenge tilgang til å oppdatere kameraer og andre produkter. Systemet bør altså være utviklet på en måte som gjør at det er mulig å definere tilgangsnivået for hver bruker eller brukergruppe.

Doorkeeper legger til grunn at de skal konfigurere løsningene for sine kunder, for å minimere risikoen for at løsningen brukes på måter som ikke er forenlige med Doorkeeper sine intensjoner. Diskusjonene om dette temaet har videre ført til at Doorkeeper vurderer å opprette sin egen vaktsentral med egne operatører, slik at de kan ha mer kontroll over hvordan overvåkingssystemene deres benyttes. Doorkeeper fremholder at det er svært viktig for dem at løsningene de tilbyr blir benyttet på en lovlig og etisk forsvarlig måte.

Hva hvis teknologien ikke fungerer slik den er ment?

En aktuell risiko med løsningen som Doorkeeper utvikler kan være at algoritmen utløser *falske positive* eller *falske negative*. Da vil løsningen fjerne sensuren og starte permanent lagring av opptak uten at det har skjedd en hendelse, eller så vil løsningen overse en hendelse den er ment å oppdage.

Falske positive kan medføre at behandlingen av personopplysninger blir mer omfattende enn behandlingsansvarlig har lov til. I motsetning vil *falske negative* kunne medføre at overvåkingen ikke oppfyller formålene den er ment/trent å oppfylle. Enhver som benytter kunstig intelligens må følge med på eventuelle falske positive og negative, og kontinuerlig tilpasse løsningen deres slik at den fungerer etter hensikt.

De rettslige vurderingene i denne rapporten tar utgangspunkt i beskrivelsen av løsningen som Doorkeeper har forelagt oss. Datatilsynet har ikke etterprøvd eller gjort tester for å kvalitetssikre hvordan løsningen *faktisk* fungerer. Hvis en løsning ikke fungerer slik som den er tiltenkt, kan dette ha store konsekvenser for lovligheten av overvåkingen. For eksempel, hvis en løsning har feil eller mangler som gjør at den samler inn mer opplysninger enn forespeilet, vil dette kunne medføre brudd på dataminimeringsprinsippet i artikkel 5.

Helhetlig sikkerhet

Leverandører av komplette tjenester – i motsetning til leverandører av enkeltkomponenter – vil ofte ha et bedre utgangspunkt for å sikre løsningene de tilbyr. Dette er fordi de kan utøve mer kontroll av produktene som inngår i tjenesten.

Doorkeeper fremmer at de primært ønsker å være en tjenesteleverandør. Dette betyr at de vil ha stor kontroll over både kameraene, nettverket og plattformen. Dersom de velger å opprette en vaktsentral vil de også ha kontroll over denne og operatørene. Økt grad av kontroll kan legge til rette for et høyere sikkerhetsnivå, men innebærer også ytterligere ansvar for Doorkeeper – et ansvar som er viktig for dem å være bevisste på.

Ved å kontrollere videostrømmen fra den genereres i kameraet til operatøren kan se den på en skjerm, kan Doorkeeper i større grad ta ansvar for kommunikasjonssikkerheten i alle komponentene. Doorkeeper vil også ha større kontroll over at løsningen er konfigurert på en sikker og personvernvennlig måte og redusere sannsynligheten for at konfigurasjonen endres til en som er mindre sikker. Ved å opprette en egen vaktsentral og ansette egne operatører kan Doorkeeper innrette vaktsentralen på en sikker måte, og de kan sørge for å lære opp operatørene etter deres egne standarder.

Dersom Doorkeeper oppnår målet om å være tjenesteleverandør, blir det viktig for dem å være oppmerksomme på utfordringer som kan være særlig aktuelle for slike. De vil for eksempel ha direkte kontroll med flere komponenter enn om de kun opptrer som leverandør av kameraer. Dette betyr at de vil ha et ansvar for at et stort antall komponenter skal operere på en sikker måte. Denne utfordringen kan bli større hvis kundemassen øker, eller hvis ulike kunder har behov for ulike konfigurasjoner. Det blir viktig for Doorkeeper å være bevisste på disse utfordringene, og at de har et styringssystem som er dekkende for å ivareta sikkerheten i hele tjenesten.

Veien videre

Diskusjonene i denne rapporten kan brukes av Doorkeeper for å bedre imøtekomme kravene i personvernregelverket og sikre et bedre personvern i løsningen. Datatilsynet håper også at diskusjonene vil være til hjelp for andre virksomheter som utvikler lignende teknologi.

Gjennom arbeidet i sandkassen har også Datatilsynet lært mye om mulighetene innen intelligent videoanalyse. Denne kompetansen vil vi videre bruke for å forbedre vårt veiledningsarbeid.

En mer personvernvennlig form for overvåking?

I denne rapporten viser vi at det er mulig å gjennomføre tiltak for dataminimering i intelligent videoanalyse. Slike tiltak kan gjennomføres ved å konfigurere løsningen til å begrense mengden personopplysninger som hentes inn og behandles til det som er nødvendig for å oppnå formålet. Rent praktisk kan dette gjøres blant annet ved å analysere opplysningene i sanntid – uten lagring av permanente opptak – og ved å fortløpende fjerne identifiserbare opplysninger fra videostrømmen.

Datatilsynet har også drøftet i denne rapporten at Doorkeeper sin kameraløsning potensielt kan bety – i spesielle tilfeller – en utvidelse av situasjoner der det er lovlig å bruke kameraovervåking. Dette vil i hovedsak gjøre seg gjeldende der hvor kameraer brukes som sensorer hvor alt av menneskeformer sladdes i alle ledd og hvor idet ikke gjøres opptak i det hele tatt.

Diskusjonene viser likevel at potensielle «personvernvennlige» løsninger vil i hovedsak ikke endre *hvor* det er mulig å overvåke personer med kamera – for eksempel i en offentlig gate. Valg av dataminimerende tiltak vil ikke senke terskelen for hva som er lovlig kameraovervåking i tilfeller der virksomheten ikke har en berettiget interesse eller berettiget formål med overvåkingen.

Utbredelsen av funksjonaliteter i overvåkingssystemer som gjør behandlingen av personopplysninger mindre inngripende, gjør at virksomheter i sikkerhetsbransjen må i større grad vurdere hvilke behandling av personopplysninger som er *nødvendig* for å oppnå formålet til overvåkingen.

Økt kompleksitet – mer sårbarhet?

Sikkerhetsutfordringene som vi har diskutert i rapporten er ikke uttømmende. Intelligent videoanalyse kan føre til mer kompleksitet i løsningene enn ved mer tradisjonelle alternativer. Dette kan igjen medføre større trusler mot sikkerheten i løsningen og en større fare for personvernet. Kompleksiteten som intelligent videoanalyse kan medføre, tilsier at virksomhetene som ønsker å gå over til slike løsninger må øke kompetansen sin innen informasjonssikkerhet.

Gjennom sandkasseprosjektet har Doorkeeper drøftet hvordan de kan tenke sikkerhet i både utvikling, utforming, konfigurasjon og bruk av løsningene de tilbyr. Det vil være essensielt for Doorkeeper å ha en effektiv strategi for å opprettholde dette fokuset i fremtiden. Håndtering av flere kunder og ulike konfigurasjoner vil for eksempel oppta mer ressurser og medføre vedlikehold av en større infrastruktur.

Nye sikkerhetstrusler vil også synliggjøre seg i tråd med den teknologiske utviklingen. Datatilsynet ser på det som hensiktsmessig for både virksomhetene og tilsynsmyndigheten å følge med på det videre trusselbildet som råder i sikkerhetsbransjen.

Hvilke utviklinger er viktige å følge med på?

I tråd med diskusjonene i sandkassen vil Datatilsynet særlig peke på at *edge computing* – som ved kameraovervåking innebærer at større deler av videobehandlingen kun skjer i kamerahuset – er et felt som kan endre hvordan personopplysninger behandles i overvåkingssystemer i årene fremover. Dette kan blant annet føre til at færre personopplysninger lagres i overvåkingssystemer og at – i en normalsituasjon – færre opplysninger vil være tilgjengelige for operatørene.

Som følge av at intelligent videoanalyse blir mer utbredt, er det rimelig å forvente en større diskusjon om hvilke samfunnsmessige konsekvenser som mer teknologisk avanserte overvåking vil medføre. Dette er ikke et tema som vi diskuterer i denne rapporten, men som bør være gjenstand for en bredere debatt.



**Datatilsynets regulatoriske
sandkasse for ansvarlig
kunstig intelligens**

Besøksadresse:
Trelastgata 3, Oslo

Postadresse:
Postboks 458 Sentrum
0105 Oslo

sandkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no/sandkasse
personvernbloggen.no
twitter.com/datatilsynet