Sporing i det offentlige rom

Bruk av WiFi, Bluetooth, nettvarder (beacons) og intelligent videoanalyse.

Juni 2016 (oppdatert desember 2016)

Datatilsynet

Innhold

INNLEDNING – FRA SPORING PÅ NETT TIL SPORING I DEN FYSISKE VERDEN 3
Avgrensning 3

WIFI- OG BLUETOOTH-SPORING 4
Utbredelse og bruk 5
Personvernkonsekvenser 6
Retningslinjer for bruk av WiFi- og Bluetooth-sporing 8

NETTVARDER / BEACONS 9
Utbredelse og bruk 10
Personvernkonsekvenser 10
Retningslinjer for bruk av nettvarder 12

INTELLIGENT VIDEOANALYSE 13
Utbredelse og bruk 14
Automatisk nummerskiltgjenkjenning 15
Personvernkonsekvenser 16
Retningslinjer for bruk av intelligent videoanalyse 17

HVA HAR VI I VENTE? 18
Oppsummering 18

Innledning – fra sporing på nett til sporing i den fysiske verden

Å se hvordan en person beveger seg rundt på internett er verdifull kunnskap for en rekke virksomheter. Facebook, Google og Microsoft, samt de mange tusen selskapene i reklamebransjen, lever av å kjenne sine brukere, og det benyttes ulike teknologier for å følge personers bevegelser på nett.

De mest kjente teknologiene er bruk av *cookies* (nettkapsler), *alltid på* (at man forblir pålogget til man aktivt logger av) og *device fingerprint* (gjenkjennelse av utstyr). Det er mulig å spores på tvers av enheter. Selv om vi logger av når vi bruker PC-en, er vi fortsatt på nett gjennom mobiltelefonene våre. Lenge var det bare våre bevegelser på nett som ble registrert. Utbredelsen av smartere mobiltelefoner og andre enheter som vi hele tiden har med oss, har endret dette. Mobiltelefonene gjør det mulig å spore oss også i den fysiske verden.

De siste årene har også norske aktører øynet større interesse for bevegelsene våre i den fysiske verden. Noen aktører vil bruke sporingsteknologi for å kunne regne ut køtid i rushtrafikken eller for å beregne tid gjennom sikkerhetskontrollen på flyplassen. Andre vil kartlegge og analysere kundenes bevegelser i detalj i butikker og kjøpesentre. Aktørene er altså svært forskjellige og har ulike formål med sporingen sin.

Sporingsteknologi som brukes i det offentlige rom er temaet for denne rapporten. Med det offentlige rom mener vi steder som er offentlig tilgjengelige, slik som kjøpesentre, butikker, gater, transportknutepunkt og underholdningsarenaer. Vi er opptatt av sporings-teknologi fordi sporing og overvåking av enkeltpersoners bevegelser og atferd kan krenke retten til privatliv og vern av personlige opplysninger. Personvernet til den enkelte krenkes dersom sporing skjer i det skjulte eller på en inngripende måte.

Rapporten er bygd opp ved at vi først gir en beskrivelse av sporingsteknologien – hvordan den fungerer og utbredelsen av den. Deretter vil vi se på personvernkonsekvensene ved bruk av slik teknologi. Vi kommer så med noen retningslinjer til virksomhetene om hvordan de kan bruke sporingsteknologi på en lovlig måte slik at personvernet til enkeltpersoner ikke blir krenket.

Google og sporing

Google var den første aktøren som i større omfang begynte å sanke nøyaktig informasjon om våre bevegelser i den fysiske verden. Mobilappen Google Maps kan innhente brukernes posisjon ved hjelp av GSM-basestasjoner, GPS-satellitter og lignende.

I 2008 begynte Googles Street View-biler å kartlegge plasseringen av WiFi-nettverk, slik at også hvilket WiFi-nett brukerne er i nærheten av kan brukes til å fastslå hvor de befinner seg. Slik har Google skaffet seg kunnskap om sine brukeres bevegelser.

Avgrensning

Rapporten ser på fire forskjellige teknologier som kan brukes til sporing: WiFi, Bluetooth, nettvarder (beacons) og intelligent videoanalyse (IVA). Teknologier som GSM-, GPS- og IP-sporing, RFID og lydsporing vil vi ikke gå nærmere inn på her, men enkelte av dem vil nevnes underveis for å illustrere hva sporingsteknologi kan brukes til.

WiFi- og Bluetooth-sporing

WiFi

WiFi er en trådløs teknologi som gjør det mulig for elektroniske enheter, slik som mobiltelefoner, å koble seg til internett. Steder der WiFi brukes kalles gjerne for trådløse nettverk eller WiFi-soner. WiFi-soner finnes i dag «overalt», det vil for eksempel si i private hjem og på arbeidsplassen, tog, kafeer, dagligvarebutikker, fly og bensinstasjoner. WiFi er populært fordi det som regel er rimeligere og raskere å bruke til surfing på nett enn bruk av mobildata.

Når WiFi er aktivert på mobilen, søker mobiltelefonen kontinuerlig etter WiFi-soner i nærheten. En WiFi-sone kan ha en rekkevidde på 50 til 100 meter fra et WiFi-punkt. Søkingen skjer ved at mobilen sender ut et unikt signal – en såkalt MAC-adresse. Hvis du går i et område hvor det er satt opp flere WiFi-punkter, vil din mobiltelefons MAC-adresse kunne bli registrert på hvert av disse punktene. Informasjonen kan fortelle hvor lenge du har oppholdt deg på stedet og hvilken retning du går i.

Mac-adresse

En MAC-adresse er et unikt identifikasjonsnummer som kan identifisere din mobiltelefon. Det er tildelt av produsenten. En MAC-adresse defineres som en personopplysning når den samles inn gjennom WiFi-sporing.

WiFi-sporing går ut på å registrere og lagre MAC-adresser som mobiltelefoner sender ut til andre formål enn bare å gi mobilen tilgang til WiFi. Siden de fleste av oss i dag har en mobiltelefon, vil antall MAC-adresser innenfor et område gi et ganske presist bilde av hvor mange mennesker som befinner seg der, og hvilket bevegelsesmønster de har. Eieren av WiFi-nettverket kan på denne måten samle inn opplysninger om mobilbrukernes posisjon (posisjonsdata) innenfor WiFi-sonen.

De aktørene som bruker WiFi-sporing er interesserte i posisjonsdata. De ønsker å få kunnskap om *hvor* eieren av mobiltelefonen er, for slik å kunne telle, analysere og sammenligne informasjonen om mobileierens bevegelser til ulike formål.

En MAC-adresse kan altså kobles til en bestemt person, fordi den er unik for personens mobiltelefon. Denne personen kan direkte og indirekte identifiseres på flere måter. For eksempel kan mobiloperatørene og leverandørene lagre informasjon om hvilke MAC-adresser en telefon har. Videre må man ofte oppgi identifiserende opplysninger slik som e-postadresse for å få tilgang til offentlig tilgjengelige WiFi-nettverk, og disse opplysningene kan kobles sammen med MAC-adressen. Personen kan også identifiseres indirekte gjennom posisjonsdata, vaner og bevegelsesmønstre som WiFi-sporingen avdekker. Dette er grunnen til at MAC-adresser er definert som personopplysninger.

WiFi-sporing kan ikke skje dersom WiFi er helt skrudd av på mobilen eller enheten. Vær oppmerksom på at noen WiFi-funksjoner kan forbli aktiverte på enkelte mobiler selv om WiFi tilsynelatende er deaktivert. For å sikre at WiFi er helt skrudd av, må man i noen tilfeller gå inn i telefonens avanserte innstillinger.

Bluetooth

Bluetooth er en trådløs teknologi som brukes til å overføre data mellom elektroniske enheter, for eksempel mellom en mobiltelefon og en PC. Bluetooth har mange likhetstrekk med WiFi, men bruker mindre strøm og har en kortere rekkevidde enn WiFi.

Mobiltelefoner sender ut et unikt signal, en såkalt Bluetooth-MAC-adresse, når Bluetooth er aktivert på mobiltelefonen. Bluetooth-sporing går ut på å registrere og lagre Bluetooth-MAC-adressen som mobiltelefonen sender fra seg. Dette brukes til å spore brukerens bevegelser.

Fordelen med å bruke Bluetooth fremfor WiFi til sporing, er at teknologien gir mer nøyaktig informasjon om hvor brukeren befinner seg innenfor et avgrenset område på grunn av den korte rekkevidden.

Bluetooth-sporing kan forhindres ved å skru av Bluetooth på mobilen eller enheten. Vær oppmerksom på at Bluetooth kan bli aktivert automatisk på enkelte mobiler etter oppdateringer eller når telefonen skrus av og på. For noen enheter er det mer problematisk og noen ganger umulig å enkelt deaktivere Bluetooth, for eksempel i biler.

Utbredelse og bruk

Det er stor interesse for WiFi-sporing, og slike løsninger brukes i hele Norge. Siden det finnes flere avarter av WiFi-sporing, er det imidlertid vanskelig å si noe konkret om utbredelsen.

Det finnes løsninger som gjør det mulig å telle personer over tid. Det finnes også løsninger som gjør det mulig å koble MAC-adressen sammen med direkte identifiserende opplysninger. Det finnes også løsninger som gjør det mulig å koble MAC-adressen sammen med direkte identifiserende opplysninger. For eksempel har noen WiFi-nettverk funksjonalitet som gjør at når man logger seg på Facebook i WiFi-sonen, kan nettverket hente ut opplysninger fra Facebook om brukeren. En butikk kan på den måten for eksempel kartlegge hvilke interesser kundene har.

WiFi-sporing

Hvis du oppgir e-postadressen din eller navnet ditt når du kobler deg til en WiFi-sone, vil nettverkseieren kunne koble MAC-adressen fra telefonen din sammen med din identitet. Slik vil det være mulig å følge dine bevegelser innenfor WiFi-sonen gjennom signalene som sendes ut kontinuerlig fra mobilen din. Står det et WiFi-punkt inne på sportsbutikken, vet nettverkseieren at du har vært i butikken og nøyaktig klokkeslett for når du var der.

I tillegg kan mange gjestenett på konferansesentre og hoteller huske MAC-adresser for automatisk tilkobling til kjente enheter, men dette skjer ikke for å spore personene. Datatilsynet har ikke grunn til å tro at WiFi-sporing er veldig utbredt på handlearenaer, men vi kjenner til at flere kjøpesentre har begynt å se på slike løsninger.

Et fremtredende eksempel på bruk av WiFi-sporing finner vi i sikkerhetskontrollen på Oslo Lufthavn Gardermoen. Flyplassen bruker WiFi-sporing for å beregne tiden det tar for de reisende å gå gjennom sikkerhetskontrollen. Sporingen foregår slik at det er plassert ut et antall WiFi-punkter før og etter sikkerhets-kontrollen. Passeringstidspunkt før og etter sikkerhetskontrollen blir slått sammen for å regne ut hvor lang tid det har tatt for den reisende å bevege seg mellom punktene. Dette gir en nokså presis indikasjon på gjennomsnittlig passeringstid gjennom sikkerhets-kontrollen. Denne informasjonen gis videre til de reisende på oppslagstavler som oppdateres jevnlig.

Et annet eksempel fra Norge på bruk av WiFi-sporing finner vi på kjøpesenteret CC Stadion i Hamar. Teknologien som kjøpesenteret har anskaffet, gjør det mulig å kartlegge og analysere kundeatferd, som igjen kan brukes til å tilpasse reklame og optimalisere produktplassering. Senterledelsen sier[1] at de alltid vil innhente kundens samtykke før de vil bruke teknologien til å analysere den enkeltes bevegelser og gi tilpasset reklame. Uten samtykke vil senteret kun telle antall besøkende – ikke analysere den enkelte kundes bevegelser.

I andre europeiske land har det vært flere personvern-saker om WiFi-sporing. I Sverige gjennomførte det svenske datatilsynet, Datainspektionen, en kontroll med WiFi-sporing i 2015[2]. Her ble WiFi-sporing brukt i en by for å kartlegge folks bevegelser i sentrumskjernen. Formålet var å innhente MAC-adresser for å utarbeide statistikk om besøkstall i sentrum. Datainspektionen mente WiFi-sporingen var ulovlig fordi sporingen gjorde det mulig å overvåke enkeltpersoners bevegelser i det offentlige rom. Selskapet som sto for sporingen ble pålagt å endre praksisen eller stanse den. Selskapet gjennomførte endringer som gikk ut på at MAC-adressene nærmest umiddelbart ble slettet, slik at statistiske data ikke lenger kunne kobles tilbake til mobileierne. I tillegg ble det hengt opp informasjons-tavler rundt om i sentrum og på nettstedet til virksomheten. Datainspektionen fant disse tiltakene tilstrekkelige og aksepterte WiFi-sporingen slik den da ble gjennomført.

I Nederland gjennomførte det nederlandske datatilsynet i 2015 et tilsyn med et selskap som lagde WiFi-systemer

[1] Hamar Arbeiderblad (8.11.2014): http://www.h-a.no/nyheter/overvaaker-kundenes-bevegelser

[2] Datainspektionen.se (23.6.2015): http://www.datainspektionen.se/press/nyheter/2015/besoksflodena-i-vasteras-mats-for-noggrant-/

for sporing i butikker[3]. Sporingssystemet ble brukt for å registrere bevegelsene til kundene i butikkene gjennom registrering av mobiltelefonenes MAC-adresser. Også mobiltelefonene til forbipasserende på gata utenfor butikken ble registrert. Formålet var å analysere kundenes bevegelser og handlemønster og dataene ble lagret i ubegrenset tid. Verken kundene i butikken eller de forbipasserende fikk noen informasjon om at signaler fra deres telefoner ble registrert og lagret. Det nederlandske datatilsynet slo ned på praksisen på grunn av mangel på informasjon, samt manglende anonymisering og sletting av MAC-adresser.

Personvernkonsekvenser

WiFi- og Bluetooth-sporing bruker vårt eget utstyr til å spore oss. Dette er utstyr som har frivillig kommunikasjon som opprinnelig formål. Med WiFi- og Bluetooth-sporing kan utstyret vårt brukes til nye formål uten at vi er klar over det. Videre kan overvåking av våre bevegelser for telling, kartlegging og analyse oppleves som ubehagelig og krenkende, særlig hvis vi ikke vet hvem som overvåker oss og hvorfor de gjør det.

I vår verden er ikke aktørene som driver med sporing like synlige som geitekillingen i eventyret (se boks). Det er vanskelig, mange ganger umulig, å vite om mobil-telefonens WiFi- og Bluetooth-signaler blir sporet. I sakene fra Nederland og Sverige som er nevnt over, foregikk WiFi-sporingen i det offentlige rom i det skjulte før datatilsynsmyndighetene grep inn. Skjult sporing får konsekvenser for personvernet vårt fordi vi mister oversikten over egne personopplysninger, og vi fratas retten til å ta informerte valg eller på annen måte øve påvirkning.

Når noen aktører vet masse om oss, mens vi ikke vet noe om dem, blir deres makt styrket. Dette kan fort skape et overtak for den som vet mest – et overtak aktørene kan bruke til å påvirke oss eller treffe beslutninger som får praktiske konsekvenser for oss. Et eksempel er at prisen for en vare blir forskjellig for to kunder basert på en analyse av hvor mye den ene kunden er villig til å betale. Videre fører det til informasjonssvikt, som er en form for markedssvikt. Når forbrukeren ikke har kjennskap til hva som foregår, kan de heller ikke kreve tjenester som gir bedre personvern. Den ujevne fordelingen av informasjon resulterer i en konkurransesituasjon som oppmuntrer markedsaktørene til å ta i bruk mer og mer personverninngripende virkemidler.

Et grunnleggende personvernprinsipp er at innsamling av personopplysninger ikke skal skje i det skjulte. Derfor skal det alltid informeres om at WiFi- og Bluetooth-sporing foregår – det krever personopplysningsloven.

Informasjon setter oss i stand til å vareta egne rettigheter og skaper åpenhet. Åpenhet kan bidra til legitim og rettferdig bruk av personlige opplysninger. Alle som blir sporet har for eksempel innsynsrett i hvilke personopplysninger om en selv som behandles.

Geitekillingen som kunne telle til ti

Eventyret om geitekillingen som kunne telle til ti av Alf Prøysen, kan illustrere ubehaget ved mangel på informasjon. Det var en gang en liten geitekilling som hadde lært å telle til ti, begynner eventyret. Den begynte å telle de andre dyrene uten å forklare hva telling var for noe. Det falt ikke i god jord fordi dyrene ble redde og sinte når geitekillingen telte dem uten å forklare hvorfor. Derfor bestemte de seg for å «ta» geitekillingen og gi ham en lærepenge. Heldigvis endte det hele godt, fordi geitekillingen reddet alle dyrene fra å drukne da hans telleferdigheter kom til nytte på en båt som bare tålte ti passasjerer.

Eventyret illustrerer hvor viktig det er med gjennomsiktighet og forståelse for hvorfor noe gjøres. I eventyret om geitekillingen var det ingen stor aktør som telte dyrene – det var bare en liten geitekilling. Den klarte likevel å gjøre de store dyrene sinte og redde fordi den telte dem uten å fortelle hva det var han gjorde og hvorfor.

[3] Autoriteit Persoonsgegevens (1.12.2015): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_bluetrace_investigation.pdf

Personopplysningsloven sier at sporing krever samtykke. Det at vi kan velge å ikke gi vårt samtykke gir oss valgfrihet og kontroll over egne personopplysninger. Noen ganger kan imidlertid ren telling foregå dersom det er nødvendig for å vareta en berettiget interesse som veier tyngre enn den enkeltes personvern. Siden sporing utgjør et inngrep i vårt privatliv, må den være nødvendig og den må begrunnes. Hvis vi opplever bruk av sporingsteknologi som nyttig for felles formål, er det lettere å godta den.

Når MAC-adresser leses av for å telle mennesker, kan det være nødvendig å ta vare på adressene i et visst tidsrom. Lagringen kan for eksempel skje for å unngå dobbelttelling – man må ha en oversikt over hvilke MAC-adresser som allerede er talt for å ikke telle dem på nytt.

På en annen side kan for lang lagringstid gjøre det mulig å spore oss over sted og tid. Når flere WiFi-punkter er koblet til samme nettverk, vil nettverkseier kunne se hvilke punkter en person var i nærheten av, og til hvilken tid. Dermed vil det være mulig å følge bevegelsene til vedkommende. For eksempel vil det kunne spores hvordan man beveger seg i et kjøpesenter i løpet av et år, eller hver gang man går inn i en butikk i samme kjede.

Derfor er det viktig at man ikke tar vare på MAC-adressen lenger enn nødvendig. Den skal slettes så snart som mulig for å unngå inngripende og uforholdsmessig sporing.

§ Samtykke

Når en virksomhet behandler personopplysninger, skal den i størst mulig grad basere det på samtykke. Det innebærer at du godtar at virksomheten behandler personopplysninger om deg.

For at et samtykke skal være gyldig, må det være aktivt, frivilling og informert.

Noen ganger kan steder vi besøker fortelle noe om vår helsetilstand, religiøse tro, politiske synspunkter eller seksuelle legning. Dette er sensitive personopplysninger, og det gjelder strenge regler for når det er lov å behandle slike opplysninger. Derfor bør WiFi-sporing unngås på slike steder, for eksempel hos helsetilbydere, i gudshus eller under politiske demonstrasjoner.

Retningslinjer for bruk av WiFi- og Bluetooth-sporing

1. WiFi- og Bluetooth-sporing kan finne sted dersom det innhentes et gyldig **samtykke** fra personene som blir sporet. Kortvarig telling kan finne sted uten samtykke dersom tiltaket er nødvendig for å vareta en berettiget interesse som veier tyngre enn den enkeltes personvern. Dette innebærer at man må vurdere om det er mulig å oppnå formålet med mindre inngripende tiltak, for eksempel ved sensorer som ikke samler inn personopplysninger.

2. **Kobling** av WiFi- og Bluetooth-sporing med e-postadresse, kundekonto, Facebook-profil eller lignende kan kun finne sted dersom det innhentes samtykke fra de som blir sporet.

3. Sporing av personer **over tid** kan kun finne sted dersom det innhentes samtykke fra personene som blir sporet.

4. **Formålet** med sporingen må være klart definert. Tiltaket kan bare brukes i tråd med dette formålet, og personopplysninger som samles inn kan ikke brukes til andre formål senere.

5. Man kan ikke samle inn flere personopplysninger enn det som er **nødvendig og relevant** for formålet.

6. **Unngå** å bruke sporingsteknologi på steder som kan fortelle noe om personers helsetilstand, religiøse tro, politiske synspunkter eller seksuelle legning.

7. Virksomheten må iverksette **sikkerhetstiltak** for å beskytte personopplysningene slik at de ikke kommer på avveier.

8. Det skal **informeres** om at det foregår sporing, for eksempel ved skilting eller annen tydelig informasjon. Det skal fremgå av informasjonen hva slags sporing som foregår og hva formålet er, for eksempel utarbeidelse av kundestatistikk. Det skal også stå hvem som er behandlingsansvarlig med kontaktinformasjon. Dersom virksomheten har en personvernerklæring, skal informasjonen også fremgå der.

9. Virksomheten må ha **klare rutiner** for hvor lenge MAC-adresser skal lagres. MAC-adressene skal slettes så raskt som mulig slik at det ikke er mulig å koble opplysningene tilbake til individer. I mellomtiden skal sikkerheten ivaretas på en tilstrekkelig måte ved at MAC-adressene pseudonymiseres.

10. Tiltaket skal **meldes** til Datatilsynet.

Nettvarder / beacons

Nettvarder, også kalt *beacons,* er små batteridrevne enheter som sender ut informasjon som kan plukkes opp av mobiltelefoner i nærheten. Signalene sendes ut ved hjelp av Bluetooth-teknologi, og dekningsområdet kan ha en radius på opptil 70 meter. I utgangspunktet er det appen til virksomheten som har plassert ut nettvardene som kan lese det av, men i praksis kan også andre apper og operativsystemer (som iOS og Android) lese av utplasserte nettvarder.

Alle nettvarder sender ut en unik ID. Når en app leser av ID-en, kan det utløse en handling i appen, for eksempel at det gis en beskjed eller reklame til brukeren. For mange meldinger kan imidlertid irritere brukeren, så noen ganger vil det ikke vises at en nettvarde har blitt lest av. Appen kan registrere om en mobiltelefon kommer inn eller går ut av forutbestemt sone, og appen kan registrere dette i bakgrunnen. Den som er ansvarlig for appen kan altså kartlegge hvilke nettvarder brukeren har vært i nærheten av, hva avstanden var og tidspunkt for når brukeren var i nærheten, uten at brukeren merker det.

Eksempel

En kunde har lastet ned appen til en sportsbutikk på mobilen. Sportsbutikken har utplassert nettvarder. Når kunden er i sports-butikken, kan appen *se* at kunden bruker mesteparten av tiden i sykkelavdelingen. Idet kunden går ut av butikken, popper det opp en melding på mobilen med tilbud om 20 prosent avslag på sykkelutstyr neste gang kunden handler i butikken.

Det finnes ulike tekniske løsninger for nettvarder, som hver har sine fordeler og ulemper. Man kan dele nettvardene inn i tre hovedgrupper:

- *iBeacons*, som er Apples løsning
- *Eddystone*, som er Googles løsning
- Andre nærhetsbeacons, slik som *AltBeacon* (*The Open and Interoperable Proximity Beacon*)

Apple opplyser at en app sin bruk av **iBeacon** for lokalisering, krever samtykke fra brukeren på forhånd. Brukeren vil også bli varslet ved at en lokasjonspil vises i statuslinjen øverst på skjermen.

Googles Eddystone kan sende ut URL-adresser (lenker til nettsider) som kan leses av nettleseren Chrome. Det betyr at man ikke behøver å laste ned en dedikert app for forskjellige nettvarder – alle fungerer med Chrome. For å unngå spam vil alle URL-er fra Eddystone bli vist på mobilen som push-meldinger først slik at brukeren kan velge om han vil åpne dem. Informasjon om brukeren vil ikke bli lagret før lenken åpnes. Dermed vil eierne av ulike nettvarder ikke ha kunnskap om hvem som er i nærheten av disse nettvardene før brukeren besøker nettstedene lenkene viser til.

AltBeacon benytter en åpen løsning for nettvarder. Åpne løsninger gjør det mulig for en enkelt app å håndtere nettvarder utplassert av flere forskjellige virksomheter. For eksempel vil et kjøpesenters app kunne håndtere meldinger og lokalisering for de ulike butikkene. Vi vil derfor kunne se apper som leser nettvarder på kryss av virksomheter og lokasjoner. Den mest kjente løsningen for dette er *Facebook Place Tips for Businesses*.

På samme måte som for Bluetooth-sporing, kan sporing med nettvarder forhindres ved å skru av Bluetooth på mobilen eller enheten.

Nettvarder kan også overføre informasjon ved hjelp av andre teknologier, for eksempel lyd med frekvenser mennesker ikke kan høre. En slik tjeneste er Googles tjeneste *Like ved*. Denne tjenesten bruker en kombinasjon av WiFi, Bluetooth og ikke-hørbar lyd for å koble til enheter i nærheten.

Lydsporing trenger ikke trenger egne nettvarder, siden lydsignaler kan sendes ut fra de fleste elektroniske enheter. For eksempel kan lydsignaturer spilles av på PC-en vår når vi besøker en bestemt nettside eller av TV-en under en reklamefilm. Disse lydsignalene kan plukkes opp av andre enheter, for eksempel mobiltelefonen vår, og registreres. Derfor vil denne teknologien gjøre det lettere å spore personer på tvers av enheter og mellom internett og den fysiske verden.

Utbredelse og bruk

Nettvarder har vært tilgjengelig på markedet en stund, og etterspørselen er økende. Det anslås at det allerede er utplassert mange tusen nettvarder i Norge alene. Dette tallet vil etter all sannsynlighet øke. Nettvarder brukes blant annet på opplevelsesarenaer, på sportsarenaer, i butikker, på konferanser, av transportselskaper og av aktører innen telekom. De brukes også i reklameflater og av eiendomsselskaper.

Nettvarder kan som nevnt brukes av butikker til å sende kunder push-meldinger om spesialtilbud når de er i nærheten av butikkene. En teleoperatør har for eksempel brukt nettvarder til å tilby en mobil ladestasjon til forbipasserende kunder når den dedikerte appen har registrert at kunden har lite strøm på mobilen. Som nevnt behøver imidlertid ikke bruken av nettvarder å resultere i en melding til bruker. Teknologien kan også brukes til å kartlegge og registrere kundens besøk og bevegelser i butikker eller kjøpesentre uten at appen gir uttrykk for dette.

Nettvarder kan også brukes til å knytte sammen personers bevegelser i virkeligheten og deres tilstedeværelse på nett. *Retargeting* er når reklameannonser på internett tilpasses etter hvilke sider man tidligere har besøkt og hva man har foretatt seg på disse sidene. Frem til nå har retargeting kun bygget på våre bevegelser på nett. Med nettvarder er det nå mulig å tilby markedsføring på internett basert på våre bevegelser i den virkelige verden og hvilke butikker vi har besøkt. Det finnes selskaper som spesialiserer seg på denne typen løsninger, men Datatilsynet har ikke inntrykk av at slike løsninger er utbredt på det norske markedet ennå.

Det er appen som avgjør hva signaler fra nettvarder skal brukes til. Derfor kan de brukes til mange ulike formål på forskjellige steder. De kan for eksempel brukes i billettsystemer og til informasjon i kollektivtrafikken eller til innsjekking på fly eller hoteller.

Eksempel

Dyreparken i Kristiansand plasserte sommeren 2015 ut nettvarder som et pilotprosjekt. Besøkende som lastet ned dyreparkens app, kunne få varsler om hendelser i parken, slik som for eksempel mating av løvene.

Formålet med tiltaket var å kartlegge de besøkendes adferd i parken for å gi dem bedre service. Appen kunne ved hjelp av nettvardene måle hvor lenge de besøkende oppholdt seg på ett sted, kartlegge hvordan de bevegde seg og be om tilbakemelding på attraksjoner de besøkende hadde vært innom. Dyreparken uttalte til Aftenbladet (23.7.2015)* at sporingen var basert på samtykke fra de besøkende.

(*http://www.aftenbladet.no/nyheter/innenriks/Dyreparken-folger-gjestenes-bevegelser-3739737.html)

Personvernkonsekvenser

Sporing og sammenstilling

Nettvarder kan brukes til å fastslå plasseringen vår gjennom apper på mobiltelefonen. Siden nettvarder bruker Bluetooth-teknologi, kan plasseringen vår fastslås mer nøyaktig enn ved bruk av WiFi-sporing. Over tid kan informasjon fra nettvarder fortelle noe om vanene og interessene våre. Dette griper inn i privatlivet vårt. Utgangspunktet er at man har rett til sporfri ferdsel uten å bli unødvendig registrert.

For at sporing skal være tillatt, må det skje med personens samtykke. Videre må sporingen ha et saklig formål og ikke være uforholdsmessig inngripende. For at brukeren skal kunne samtykke må han også få informasjon om hva sporingen innebærer: Vil nettvarder kun brukes til å gi meldinger og reklame, eller vil også brukerens bevegelser registreres? Hvem står bak sporingen, og hva er formålet? Innhenting av samtykke og informasjon kan håndteres av appen. Det er derfor viktig at appen utvikles på en både brukervennlig og personvernvennlig måte.

Det skal også gis spesifikk informasjon i lokaler der nettvarder er i bruk, for eksempel ved skilt eller annen tydelig informasjon. Det vil nemlig ikke alltid være tydelig i appen hvor sporingen foregår, og noen apper kan registrere nettvarder på mange forskjellige lokasjoner, for eksempel alle butikkene i en butikkjede. Det er ikke alltid brukeren er klar over dette. Denne informasjonen vil videre komme personer som ikke har lastet ned den aktuelle appen, til gode. Disse personene ville ellers ikke fått informasjon, og som nevnt kan

operativsystemer og andre apper potensielt lese av nettvarder selv om den aktuelle appen ikke er installert.

Med nettvarder kan våre bevegelser i den fysiske verden sammenkobles med våre bevegelser på nett. Appen kan bruke dem til å fastslå vår posisjon og til og med hvilke butikkhyller vi tilbringer tid ved. Samtidig kan appen være knyttet til sosiale medier, kundeklubber eller andre tjenester som vet mye om våre vaner og interesser på nett. Appen kan også inneholde andre opplysninger om oss. Slik sammenkobling av personopplysninger er særlig inngripende.

Akkurat som WiFi-sporing, kan nettvarder plassert på enkelte steder fortelle noe om vår om vår helsetilstand, religiøse tro, politiske synspunkter eller seksuelle legning. Det er viktig at appen ikke bruker opplysninger om oss på en diskriminerende måte, for eksempel at tilbud gis basert på antakelser om betalingsevne eller etnisitet.

Noen leverandører av nettvarder eller nettvarde-løsninger, kan ønske å bruke opplysninger fra nettvardene for egne formål, for eksempel for å forbedre egne tjenester. Dette er en problemstilling som kan oppstå med Facebook sine nettvarder – nettvarder Facebook gir gratis til virksomheter. Når man plasserer ut en nettvarde har man ansvar for å ha full oversikt over hvordan personopplysninger vil behandles og at opplysningene ikke utleveres til andre med mindre det foreligger et samtykke.

Sikkerhet

Det er et grunnleggende personvernprinsipp at personopplysninger skal beskyttes fra uvedkommende. Med nettvarder er det mulig at våre bevegelser kartlegges av andre enn virksomheten som har utplassert nettvardene, slik som utviklere av andre apper og operativsystemer.

Det finnes også andre sikkerhetsproblemer ved nettvarder som kan utfordre personvernet. Slike sikkerhetsproblemer kan være:

- manglende mulighet for autentisering,
- kloning og kopiering,
- endring, hacking og omprogrammering,
- misbruk.

Det er mulig å skanne etter nettvarder, lese av ID-en deres og deretter lage en app som kan reagere på de samme ID-ene. Det er dermed mulig å kapre brukere og gi varslinger fra konkurrerende apper. For eksempel kan en butikk velge å gi deg et tilbud idet du går inn i en konkurrerende butikk. Løsninger for rullerende beacon-ID, slik som *Googles Ephemeral Identifiers*, vil kunne hjelpe noe på dette problemet. Slike løsninger bytter ID fortløpende, og kun autoriserte enheter kan benytte seg av signalet.

Som nevnt kan noen nettvarder sende ut URL-adresser. Det er mulig å plassere farlig kode i URL-ene. Skadelig kode er kode som for eksempel svekker sikkerheten til en mobil og åpner for tilgang for uvedkommende. Det ser ut til at den eneste måten å stoppe slik hacking av nettvarder på, er å sørge for at appene som gir mulighet for å kjøre denne typen kode, ikke blir godkjent i appbutikkene.

Deaktivere nettvarder/beacons?

Når du laster ned apper, vil det å måtte godta nettvarder ofte være en del av vilkårene. Dersom du ikke ønsker dette, må du i praksis avinstallere appene eller deaktivere Bluetooth.

Å deaktivere Bluetooth er imidlertid en *alt eller ingenting-løsning*. For eksempel kan det være at man ønsker og har nytte av enkelte nettvarder, mens man ønsker å unngå andre. Dessuten er det mange som ikke kjenner til teknologien og dermed ikke klarer å beskytte seg. Noen bruker videre Bluetooth til andre formål, slik som å koble smartklokke til mobilen eller lytte til musikk med trådløse hodetelefoner, og kan derfor ikke uten videre skru av Bluetooth. Enkelte operativsystemer vil dessuten automatisk aktivere Bluetooth etter oppdateringer eller omstart uten at brukeren vet det. I enkelte enheter, slik som biler, er det heller ikke mulig å skru av Bluetooth.

De siste versjonene av mobiloperativsystemene åpner for muligheten til å åpne og stenge enkeltappers tilganger til ulike tjenester, men disse løsningene er ennå vanskelig tilgjengelige for vanlige brukere.

Retningslinjer for bruk av nettvarder

1. Sporing ved hjelp av nettvarder kan kun finne sted dersom det innhentes et gyldig **samtykke** fra personene som blir sporet. For at samtykket skal være gyldig må det være tydelig hvordan sporingen vil foregå, hvem som er behandlingsansvarlig og hva formålet er. Dersom sporingen innebærer sammenkobling av våre bevegelser i den fysiske verden og på nett, må dette klart fremgå.

2. Innhenting av samtykke kan skje i appen. Samtykket må være separat fra andre vilkår, og det må være mulig å trekke tilbake samtykket i appen.

3. **Formålet** med sporingen må være klart definert. Tiltaket kan bare brukes i tråd med dette formålet, og personopplysninger som samles inn, kan ikke brukes til andre formål senere.

4. Man kan ikke samle inn flere personopplysninger enn det som er **nødvendig og relevant** for formålet.

5. Virksomheten må ha **full oversikt** over hvordan personopplysningene behandles. Virksomheten må sørge for at opplysningene ikke utleveres til andre med mindre personen samtykker.

6. Appen kan **ikke** bruke opplysningene på en diskriminerende eller krenkende måte.

7. **Unngå** å bruke sporingsteknologi på steder som kan fortelle noe om personers helsetilstand, religiøse tro, politiske synspunkter eller seksuelle legning.

8. Virksomheten må **minimalisere muligheten for misbruk og iverksette sikkerhetstiltak** som gjør at ikke andre virksomheter kan ta i bruk virksomhetens nettvarder. Videre må det iverksettes sikkerhetstiltak for å beskytte personopplysninger slik at de ikke kommer på avveier.

9. Det skal gis **informasjon** på steder der nettvarder er utplassert, for eksempel ved skilting eller annen tydelig informasjon. Det skal fremgå av informasjonen hvordan sporingen vil foregå, hvem som er behandlingsansvarlig og hva formålet er. Dersom sporingen innebærer sammenkobling av våre bevegelser i den fysiske verden og på nett, må dette klart fremgå. Dersom virksomheten har en personvernerklæring, skal informasjonen også fremgå der.

10. Virksomheten må ha **klare rutiner** for hvor lenge opplysningene appen samler inn skal lagres. Opplysningene kan ikke lagres lenger enn det som er nødvendig for formålet.

11. Tiltaket skal **meldes** til Datatilsynet.

Intelligent videoanalyse

Intelligent videoanalyse, *Intelligent Video Analytics (IVA)*, er teknologi som automatisk analyserer innhold fra overvåkingskameraer. Videoanalysen kan blant annet kartlegge hva slags objekter som er i bildet, utløse alarmer basert på hvor og hvordan objektene beveger seg og gjenkjenne ansikter. Dette kan for eksempel brukes til å oppdage når noen klatrer over et gjerde eller fjerner en verdifull gjenstand, telle mennesker eller analysere bevegelser i butikker og på offentlige steder.

Enkelt sagt bygger videoanalyse på å tolke endringer fra bilde til bilde, altså endringer i bildepiksler i en strøm av bilder. Videoanalyse baseres på forskjellige sett av matematiske regler, algoritmer. Analysen kan gjøres i lagrede opptak eller i selve overvåkingskameraet, som nå ofte har prosesseringskraft og programvare. Gjennom videoanalysen lages det metadata, altså data om hva som finnes eller hva som skjer i bildene. Typiske metadata om objektene er farger, retning, fart og størrelse, og om objektet er et kjøretøy eller et menneske. Disse metadataene kan søkes i.

Tidligere var det nødvendig med et menneske til å se gjennom overvåkingsmaterialet for å i det hele tatt kunne nyttiggjøre seg innholdet. Med intelligent videoanalyse er altså ikke dette lenger nødvendig.

Ordet «intelligent» i kan være misvisende, siden det ikke er snakk om kunstig intelligens, men heller noe som skjer automatisk. Det brukes for øvrig flere begreper på teknologien. *Video Content Analytics* (VCA) og *Video Analytics* (VA) brukes forholdvis synonymt.

Funksjoner

Intelligent videoanalyse har forskjellige funksjoner, og er gjerne rettet mot spesifikke bruksområder etter behov. Derfor kan det være nyttig å dele opp bruksområdene i tre hovedkategorier.

Deteksjon og sporing. Med intelligent videoanalyse er det mulig å oppdage «nye» objekter, slik som at en person eller en bil kommer inn i bildet. Alt som beveger seg gis en hendelsesmarkør og en tidsmarkør, noe som gir mulighet til å spore objektets videre bevegelser: hvor og hvordan objektet beveger seg, retning, fart, om objektet stopper opp eller tidsbruk. Videoanalysen kan også detektere brann eller røyk.

Beskrive objekter. Videoanalyse kan også registrere hva som kjennetegner et objekt (for eksempel farge eller størrelse) eller klassifisere objektet (for eksempel kjøretøy eller menneske). Andre kjennetegn kan være temperatur, antatt alder, kjønn og etnisitet. Videoanalysen kan også gi mer avanserte objektbeskrivelser, slik som å kategorisere en persons følelser ut fra ansiktets mimikk. Det er også mulig å identifisere alle ansikter for så automatisk å lagre ansiktsbildene i en egen bildedatabase.

Identifisere objekter. Intelligent videoanalyse kan per i dag brukes blant annet til ansiktsgjenkjenning. Det er også mulig å knytte ansikt til en allerede kjent identitet i en svarte- eller hvitelisting av personer. Likeledes vil nok systemet kunne gjenfinne samme ansikt i andre overvåkingsbilder, eller på tvers av systemer, uten at man kjenner personens identitet. Systemene vil sannsynligvis også etter hvert kunne kombinere teknikker, for eksempel ansiktsgjenkjenning og ganglag, for å gjenkjenne personer.

Automatisk nummerskiltgjenkjenning (ANPR) kan identifisere kjøretøyers registreringsnummer i et bilde eller en videostrøm, og automatisk lese av og lagre registreringsnummeret som metadata. Systemene kan basere seg på dedikerte kameraer som er satt opp og justert for best mulig å kunne fange opp nummerskilt (for eksempel i et parkeringshus). Det er også mulig å analysere video fra kameraer som blir brukt til andre formål. Kameraene som brukes kan være fastmonterte, mobile sjekkpunkter eller montert i kjøretøyer.

Bruksområder

Intelligent videoanalyse og metadata muliggjør tre ulike bruksområder. Det er verd å merke seg at disse funksjonene kan brukes på mange forskjellige måter, og være til nytte for svært ulike formål.

Det kan etableres **automatiserte varslinger** eller alarmer basert på forhåndsdefinerte kriterier. Kriteriene kan for eksempel være at en person krysser en linje eller befinner seg i et område mer enn to minutter, at det danner seg ansamlinger av personer i et område eller at en bli kjører mot kjøreretningen.

Det er mulig å **søke** i opptakene, for eksempel etter store, svarte biler i nordgående retning innenfor et angitt tidsrom. Tidligere måtte man se etter det som var relevant gjennom tidkrevende leting og spoling.

Det kan generes **statistikk** fra videomaterialet, for eksempel over hvor mange kunder som har beveget seg gjennom et område, eller hvordan kundemassen beveger seg i et butikklokale. Dette kalles kundestrømsanalyser.

Kundestrømsanalysen kan også gi statistikk om for eksempel hvor stor andel av kundene som er kvinner.

Formål

Tradisjonelt har kameraovervåking i hovedsak vært bruk til ulike sikkerhetsformål, slik som vern av liv og helse og for å forebygge og oppklare straffbare handlinger. Intelligent videoanalyse representerer slik både kontinuitet og brudd. Sikkerhetsformålene har ikke falt bort, men nye formål og bruksområder har kommer til. Det er særlig ett bruksområde – eller kanskje riktigere et knippe formål med en fellesnevner – som peker seg ut, nemlig kommersielle hensyn. Begrepet *customer intelligence* og reklame står sentralt her. I tillegg kan videoanalyse være tjenlig for et tredje formål, arbeidsledelse og planlegging.

Sikkerhet. De funksjonene som blir mulige med intelligent videoanalyse, er i stor grad hensiktsmessige for sikkerhetsformål. En del av løsningene på markedet retter seg også tydelig mot dette formålet. Løsningene kan tilby forhåndsdefinerte alarmregler som varsler når virtuelle gjerder forseres, objekter flyttes (tyverideteksjon), «mistenkelig» adferd finner sted og liknende. Det kan brukes både til sikring av verdier og mennesker. Ansiktsgjenkjenning med søk opp mot bilder av kriminelle kan også brukes til sikkerhetsformål. I tillegg kan systemene gjøre det lettere å søke etter spesifikke hendelser etter at en sikkerhetsrelatert begivenhet har inntruffet.

Kommersielle hensyn. Kameraovervåking har tradisjonelt ikke påvirket bunnlinjen ut over å begrense tap forårsaket av tyveri og skadeverk. Intelligent videoanalyse endrer dette, for nå kan kameraovervåking på forskjellige måter bidra til å øke inntjeningen. Sporing av enkeltmenneskers tilstedeværelse og handlinger kan aggregeres til statistikk. Gjennom å skaffe seg informasjon om sine kunder kan aktørene optimalisere reklame og butikklokaler. I sin avanserte form kan videoanalyse inngå som et ledd i å tilpasse reklame i det fysiske rom basert på kundens kjønn og alder, eller til å måle verdien av reklamekampanjer. Eventuelt kan systemet gjenkjenne en person i en butikk som en stamkunde eller en ny kunde, noe som kan gi betjeningen nyttig informasjon om hvordan de skal møte kunden.

Arbeidsledelse og planlegging. Alarmer behøver ikke å handle om sikkerhetshendelser – det kan dreie seg om mindre alvorlig ting, som kø i kassa eller kaos på parkeringsplassen. Intelligent videoanalyse kan bistå ledere i å oppdage problemer og løpende styre ressurser deretter. Når må vi ha mange på jobb og når kan vi klare oss med få? Gjennom god kundestatistikk kan man vite når det er mange kunder og når det er rolig. Besøk kan også kobles mot andre data (slik som for eksempel været), og på den måten kan man få gode modeller for å planlegge bemanning ut fra værmeldingen. Sammenlignet med sikkerhet og kommersielle hensyn fremstår imidlertid dette bruksområdet som mindre sentralt i utviklingen så langt.

Den automatiserte analysen av videoinnhold handler altså ikke bare om nye midler til gamle formål. I prinsippet er det bare fantasien som setter grenser for hva som kan analyseres i bildene, og hvordan informasjonen kan brukes videre. Utviklingen får betydning for hvilken overvåkingspraksis som eksisterer i samfunnet – i hvilket omfang kameraovervåking benyttes, hvilke formål kameraovervåking brukes til og hvordan overvåkingsanlegg og opptak brukes i det daglige. Det er vanskelig å forutse det fulle spekteret av konsekvenser over tid.

Utbredelse og bruk

Sikkerhet og kommersielle formål

Datatilsynet har undersøkt markedet for intelligent videoanalyse, og vært i kontakt med en rekke aktører som leverer produkter og tjenester knyttet til dette. Vårt inntrykk er at teknologien er i fremvekst, men at den ennå ikke er vanlig. Teknologien ser særlig ut til å brukes for sikkerhetsformål og i kommersiell virksomhet.

Etter hva vi erfarer tilbyr de fleste leverandørene av kameraovervåkingsutsyr, løsninger for intelligent videoanalyse. Leverandørene peker på at teknologien blant annet brukes for å sikre eiendom og verdier utendørs. Videoanalyse brukes på byggeplasser, på fabrikker, i renovasjonsbransjen og i forbindelse med logistikk og lagring. Disse bruksområdene har det til felles at formålet ofte er å avverge straffbare handlinger eller å verne liv og helse.

Intelligent videoanalyse har vært mer kostbart enn vanlig kameraovervåking, og derfor har etterspørselen frem til nå hovedsakelig kommet fra større aktører. Flere leverandører understreker imidlertid at prisene er på vei ned, noe som har ført til økende interesse blant kundene. Videre virker det som om det er lettere for virksomheter å forsvare ekstrakostnaden dersom den også er en investering i økt inntjening – altså at løsningene i tillegg kan brukes til kommersielle formål. Denne etterspørselen har stor betydning for hvilke løsninger som utvikles.

Eksempler på bruk

En av aktørene Datatilsynet har snakket med, tilbyr løsninger som særlig er egnede for sikkerhetsformål. Nå jobber aktøren med å utvikle flere løsninger for kundeanalyse, siden etterspørselen etter slike løsninger er stor. Løsningene vil kunne kartlegge kunders bevegelser i butikker og identifisere kundenes kjønn, samt til en viss grad alder og ansiktsuttrykk. Løsningene vil også kunne identifisere hva slags bil kunden kjører, som igjen kan brukes til å trekke slutninger om kundens økonomi. Opplysningene kan så benyttes til å måle effekten av salgskampanjer eller tilpasse butikker, varer og tilbud til kundene.

Én aktør jobber med å utvikle intelligente videoanalyseløsninger som kan brukes i helse- og omsorgssektoren.

I et annet tilfelle brukes løsningene utelukkende til å sikre infrastruktur i elektrobransjen.

Det finnes løsninger for kundeanalyse basert på informasjon fra varmekameraer eller andre sensorer i stedet for vanlige overvåkingsbilder. Denne typen løsninger kan altså generere mye av den samme informasjonen, samtidig som konsekvensene for personvernet reduseres sammenliknet med bruk av alminnelige bilder eller film. Dette er imidlertid ikke ensbetydende med at dataene er anonyme. I en del sammenhenger, typisk på arbeidsplasser, vil man kunne vite hvem noen av personene er, selv om de ikke kan gjenkjennes ut fra hvordan de ser ut på bildene. For eksempel kan en ansatt i en butikk lett skilles fra kunder basert på hvor vedkommende står, hvor han eller hun beveger seg og hvor lenge vedkommende er der.

Dersom opplysninger fra varmekameraene kobles med personopplysninger fra andre kilder, for eksempel bruk av adgangskort eller fordelskort, kan også personer identifiseres. I så fall vil materialet i større eller mindre grad være personopplysninger.

Det er derfor viktig å merke seg at også fastmonterte varmekameraer kan være kameraovervåking i lovens forstand, og da gjelder det særskilte regler om blant annet skilting og sletting.

Intelligent videoanalyse kan også kombineres med reklameskilt. Kameraene vil kunne analysere forbipasserende, og deretter tilby reklame tilpasset vedkommende.

Eksempler på bruk

På Kastrup lufthavn i Danmark vises det reklame på skjermer basert på opplysninger om de reisende fra Amadeus-systemet og fra intervjuer, som for eksempel at forretningsreisende ofte reiser til visse tider eller fra visse gater. Ved reklameskjermene er det montert kameraer for å se om forbipasserende ser på dem. Disse kameraene er imidlertid også i stand til å analysere kjønn og hvilken aldersgruppe vedkommende tilhører. På sikt er tanken å bruke denne videoanalysen til å tilpasse innholdet på skjermene til den eller de som til enhver tid passer skjermene.

Andre norske aktører har brukt løsninger for videoanalyse i reklamekampanjer for virksomheter som Chess, Kappahl, Coca Cola, Sony Music, DNB og Oreo Mondelez.

Automatisk nummerskiltgjenkjenning

Automatisk nummerskiltgjenkjenning brukes både av offentlige og private aktører.

Politiet, Tolletaten og Statens vegvesen bruker nummerskiltgjenkjenning til å sjekke biler mot andre registre, og kontrollere kjøretøy med avvik. For eksempel kan kjøretøy som ikke har betalt årsavgift, forsikring eller lignende, stoppes. Både fastmonterte anlegg og mobile kontrollpunkter blir brukt til dette. Teknologien brukes også til innkreving av bompenger. Den kan videre brukes til automatisk trafikkovervåking

(snitthastighetsmålinger) og måling av trafikkflyt for å gi informasjon om kjøretid og ruteforslag.

Enkelte parkeringsselskaper bruker i dag teknologien til å registrere kjøretøyer som kjører inn og ut av parkeringshus. Denne informasjonen blir brukt til å fakturere kunder eller kontrollere at betaling har funnet sted. Videre kan nummerskiltgjenkjenning fungere som tilgangskontroll til private parkeringshus og parkeringsplasser ved at porter eller bommer bare åpner seg dersom bilens nummerskilt er på listen over godkjente numre.

Personvernkonsekvenser

Med intelligent videoanalyse blir vi både fanget opp på bilde og analysert. Personvernkrenkelsen er dermed større enn for vanlig kameraovervåking. Systemet kan trekke slutninger om enkeltpersoner selv om det ikke er noen som ser på opptakene. Videoanalysen kan for eksempel registrere at vi blir stående på et sted lenge, kartlegge hvilke hyller vi besøker i butikken eller lagre våre bilpasseringer. Dette genererer opplysninger om vår adferd og våre vaner. Videre kan intelligent videoanalyse muliggjøre sporing over sted og tid fordi noen systemer kan gjenkjenne ansikt eller nummerskilt.

Alle har imidlertid en viss rett til sporfri ferdsel og privatliv, selv på offentlige steder. Hvis man ikke trenger å registrere identifiserende opplysninger, har enkeltindividet rett til å være anonymt. Innsamling av personopplysninger skal videre være formålsbestemt og begrenses til det definerte formålet. Det er viktig at man ikke analyserer mer enn man har behov for å vite, slik at det ikke gjøres større inngrip i privatlivets fred og integriteten enn nødvendig. Dessuten skal all innsamling av personopplysninger være proporsjonal med formålet, slik at det er balanse mellom virksomhetens interesser og den enkeltes personvern.

Det er viktig å være klar over at intelligent videoanalyse er en form for kameraovervåking, og da må reglene for kameraovervåking følges. Frem til nå har overvåkingskameraer for det meste blitt brukt til tungtveiende formål, som for eksempel oppklaring av kriminalitet eller vern av liv og helse, og opptakene har for det meste vært kortlivede og bare blitt utlevert til politiet. Med intelligent videoanalyse kan det bli mer attraktivt å sette opp overvåkingskameraer på nye steder eller bruke eksisterende kameraer til flere formål fordi kameraene kan samle inn verdifulle kundedata. Disse dataene kan det være attraktivt å ta vare på lenger og bruke annerledes enn tradisjonelle opptak. Reglene for kameraovervåking setter imidlertid grenser for når, hvor og hvordan kameraovervåking og opptak kan brukes.

Det er et grunnleggende prinsipp at man skal få informasjon når ens personopplysninger behandles. Derfor er det viktig at det informeres godt på steder med kameraovervåking. Intelligent videoanalyse utgjør imidlertid noe mer enn hva folk forbinder med kameraovervåking. Der videoanalysen innebærer for eksempel ansiktsgjenkjennelse eller nummerskiltgjenkjenning, er det viktig at dette også informeres om, slik at man forstår hvordan personopplysningene behandles.

Dersom videoanalyse misbrukes, kan det føre til diskriminering. Kameraene kan stilles til å utløse varsler dersom personer med visse karakteristikker er tilstede. Eksempler på slike karakteristikker er hudfarge, alder og om bilen personen kjører er dyr eller ikke. Opplysninger om rase eller etnisk opphav er for øvrig sensitive personopplysninger. Disse trenger særlig vern, og det er strengere regler for når det er lov å behandle denne typen opplysninger.

Noen ganger kan imidlertid videoanalyse virke til personvernets fordel. Når en uønsket hendelse inntreffer, vil man kunne hoppe rett til hendelsen uten å måtte se eller spole gjennom hele opptaket. Dermed vil det meste av opptakene forbli usett til det slettes. Det er ikke nødvendigvis teknologien i seg selv som er problemet, men heller bruken av den. Dersom man benytter seg av intelligent videoanalyse på en personvernvennlig måte og i tråd med loven, kan dette vise seg å være et nyttig verktøy.

Retningslinjer for bruk av intelligent videoanalyse

1. Kameraer med intelligent videoanalyse kan bare brukes når det ellers er lov å overvåke med kamera. Tiltaket må ha **et tungtveiende formål**, slik som forebygging eller oppklaring av gjentatt eller alvorlig kriminalitet, eller vern av liv og helse. Det er normalt ikke tillatt å overvåke med kamera for å samle inn kundedata. Tiltaket må være proporsjonalt med personvern-krenkelsen og formålet som søkes oppnådd.

2. Formålet med videoanalysen må være klart definert. Intelligent videoanalyse kan bare brukes i tråd med dette formålet, og metadata eller personopplysninger kan ikke brukes til andre formål senere.

3. Man kan ikke samle inn flere personopplysninger enn det som er **nødvendig og relevant** for formålet.

4. Virksomheten må ha **klare rutiner** for hvilke analyseregler og alarmkriterier som settes og hvilke søk man foretar. Analysen må ikke være for inngripende, og det er ikke lov å analysere mer enn det som er relevant og nødvendig. For eksempel vil det normalt ikke være nødvendig å analysere kjønn og alder.

5. Det skal ikke analyseres på en måte som er diskriminerende eller krenkende, for eksempel ved at man varsles dersom personer med en bestemt hudfarge er tilstede.

6. **Unngå** å bruke sporingsteknologi på steder som kan fortelle noe om personers helsetilstand, religiøse tro, politiske synspunkter eller seksuelle legning.

7. Automatisk skiltgjenkjenning kan brukes på kommersielle parkeringsplasser dersom det er mulig å gjøre opp for seg på stedet, og dersom opplysningene fra skiltgjenkjenningen slettes når man gjør opp for seg.

8. Virksomheten må iverksette **sikkerhetstiltak** for å beskytte opptak og metadata slik at de ikke kommer på avveier.

9. Det skal **informeres** om at det overvåkes med kamera, for eksempel ved skilting. Dersom det utføres ansiktsgjenkjenning eller automatisk skiltgjenkjenning, bør dette fremgå av informasjonen eller skiltet. Det skal også stå hvem som er behandlingsansvarlig med kontakt-informasjon. Dersom det foretas lydopptak, skal dette også fremgå. Dersom virksomheten har en personvernerklæring, skal informasjonen også stå der.

10. Alle **opptak skal slettes** når det ikke lenger er nødvendig for formålet å oppbevare dem, og senest sju dager etter opptak. Dersom det er sannsynlig at et opptak vil bli utlevert til politiet, kan opptaket oppbevares i inntil 30 dager. Opptak fra bank eller postlokaler, inkludert opptak fra kasse med bank i butikk og post i butikk, kan oppbevares i inntil tre måneder.

11. Metadata fra intelligent videoanalyse skal slettes sammen med opptaket de stammer fra.

12. Statistikk kan bare utarbeides så lenge det skjer i tråd med formålet og det lar seg forsvare i avveiningen av virksomhetens og enkeltpersoners interesser. Man kan altså ikke bruke sikkerhets-relatert overvåking til å hente ut kundestatistikk. Statistikken kan lagres fritt så lenge dataene er helt anonyme, slik som hvor mange ganger en spesifikk sikkerhetshendelse har skjedd i løpet av en periode. Enkeltdataene som statistikken er basert på, kan ikke lagres ut over lagringstiden til opptakene, se punktet over om metadata.

13. Kameraovervåking skal **meldes** til Datatilsynet.

Hva har vi i vente?

I denne rapporten har vi skrevet om fire teknologier som sporer oss i det offentlige rom, men det finnes flere teknologier som vi tror kommer til å påvirke personvernet vårt i årene som kommer.

RFID (radiofrekvensidentifikasjon) er en teknologi som nyttiggjør seg av brikker som kan motta og svare på radiofrekvenssignaler fra en RFID-leser. RFID brukes i dag til mange formål, blant annet i for å sikre varer i butikker, i reisekort eller i bombrikker. I klesbutikker festes RFID-brikker på klær, men forskere har nå utviklet en metode som gjør det mulig å veve RFID-brikker inn i selve plagget. Dette kan hjelpe butikkene å motarbeide tyveri siden det blir umulig å fjerne brikkene, men samtidig vil enhver butikk kunne se hvordan kunder beveger seg gjennom butikken, uten at de vet det eller har mulighet til å motsette seg dette. Videre kan det være mulig å spore RFID-brikker over store avstander avhengig av hvilken standard man velger. Dårlig sikring av RFID-brikker i adgangskort, betalingskort, pass eller lignende kan gi mulighet for trådløs kopiering av data.

En nyvinning som er nevnt i denne rapporten er bruken av **lydsporing** for å kunne identifisere brukere på tvers av plattformene de bruker. Lydsporing kan fungere ved at reklamer på TV og internett spiller av en høyfrekvent lyd som mennesker ikke oppfatter, men som registreres av mobiltelefonen til brukeren. Informasjon om hvilke reklamer som har blitt registrert kan sendes videre til markedsførerne, som kan kartlegge hvilke reklamer vi ser på, hvor lenge vi ser på dem og om vi senere søker etter det aktuelle produktet på internett.

I dag består de fleste overvåkingskameraer av ett kamera med én linse, men dette er i endring. Det er utviklet prototyper på kameraer som består av **mange mikro-kameraer som ser ut gjennom samme linse**. Oppløsningen på overvåkingsbildene kan blir så stor som én gigapiksel (1000 megapiksler). Til sammenligning har kameraet på en iPhone 6s en oppløsning på 12 megapiksler. Konsekvensen av dette er at man kan få ekstremt detaljerte bilder av store områder. Man kan for eksempel ta et enkelt oversiktsbilde av en fotballstadion eller en hel by og kunne identifisere enkeltpersoner.

Dette i seg selv er en ubehagelig tanke. Sett i sammenheng med at videoanalyse vil bli raskere og mer nøyaktig i fremtiden, blir potensialet for inngripende overvåking dramatisk.

Oppsummering

Opplysninger samlet inn ved bruk av sporingsteknologi kan ha stor verdi, både kommersielt og for samfunnet. Både intelligent videoanalyse og RFID kan for eksempel brukes for å avverge kriminalitet. WiFi-sporing kan brukes på flyplasser og andre steder for å sikre god flyt av passasjerer. Med nettvarder kan virksomheter tilby oss nye tjenester og effektivisere hverdagen. Teknologiene i seg selv er ikke problemet – så lenge de brukes i tråd med personvernreglene.

Personvernutfordringene kommer som et resultat av hvordan teknologien blir brukt. Ofte får vi for dårlig informasjon når sporingsteknologi benyttes. Med informasjon om hvordan personopplysningene våre behandles er vi i stand til å fatte informerte beslutninger og beskytte privatlivet vårt. Informasjon og åpenhet er derfor avgjørende fremover, og det kan oppnås uten å bruke store ressurser. Virksomheter som gir god informasjon om hvordan de behandler person-opplysninger og viser at de tar kundenes personvern på alvor, kan få et konkurransefortrinn.

Personvern har vært satt høyt på agendaen de siste årene. I 2018 får vi nye, styrkede personvernregler gjennom EUs nye personvernforordning som også blir norsk lov. Reglene vil skjerpe plikten til å gi forståelig og tilgjengelig informasjon. Videre vil det innføres et krav om innebygd personvern, altså at det skal tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette er både kostnadsbesparende og mer effektivt enn å endre et ferdig system. Målet er at nye løsninger skal bli mer personvernvennlige, slik at teknologi og personvern kan spille på lag.

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep.,
0034 Oslo

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

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet