SafeTeam

Smart kamera-bevakning med AI

Oändliga möjligheter, men vad är den verkliga nyttan?

Förord

Företag har använt kamerabevakning nästan lika länge som SafeTeam har funnits – i nästan 60 år. I början var det främst i säkerhetssyfte, till exempel för att övervaka bankområden och andra säkerhetskänsliga platser. Kamerorna var fast monterade och filmade kontinuerligt. De var ofta anslutna till monitorer som övervakades av säkerhetspersonal. Denna metod var begränsad eftersom den krävde ständig mänsklig uppmärksamhet och lätt kunde missa kritiska händelser.

I slutet av 1990-talet togs ett stort tekniksprång genom digitaliseringen av bevakningskameror. Detta gjorde det möjligt att automatiskt upptäcka rörelse och utlösa ett larm. Detta var videoanalys i sin linda.

Drygt ett decennium senare gjordes nästa tekniksprång. Video management software (VMS) gjorde det möjligt att i realtid lagra digitala videoströmmar centralt och analysera dem i efterhand.

Nu befinner vi oss i ett nytt tekniksprång. De konventionella ”osmarta” bevakningskamerorna, som fångar det som hände framför linsen som ettor och nollor och skickar det till ett VMS, ersätts med ”smarta kameror” som själva analyserar vad som händer och vidtar åtgärder. Det är inbyggd artificiell intelligens (AI) som gör detta möjligt.

Om du har köpt en bevakningskamera under de senaste åren har du förmodligen köpt en smart kamera. Men använder du den på ett smart sätt? Många utnyttjar inte alla de möjligheter som smarta kameror erbjuder. Förmodligen för att de inte är medvetna om allt de kan göra. Det vill vi ändra på med den här e-boken.

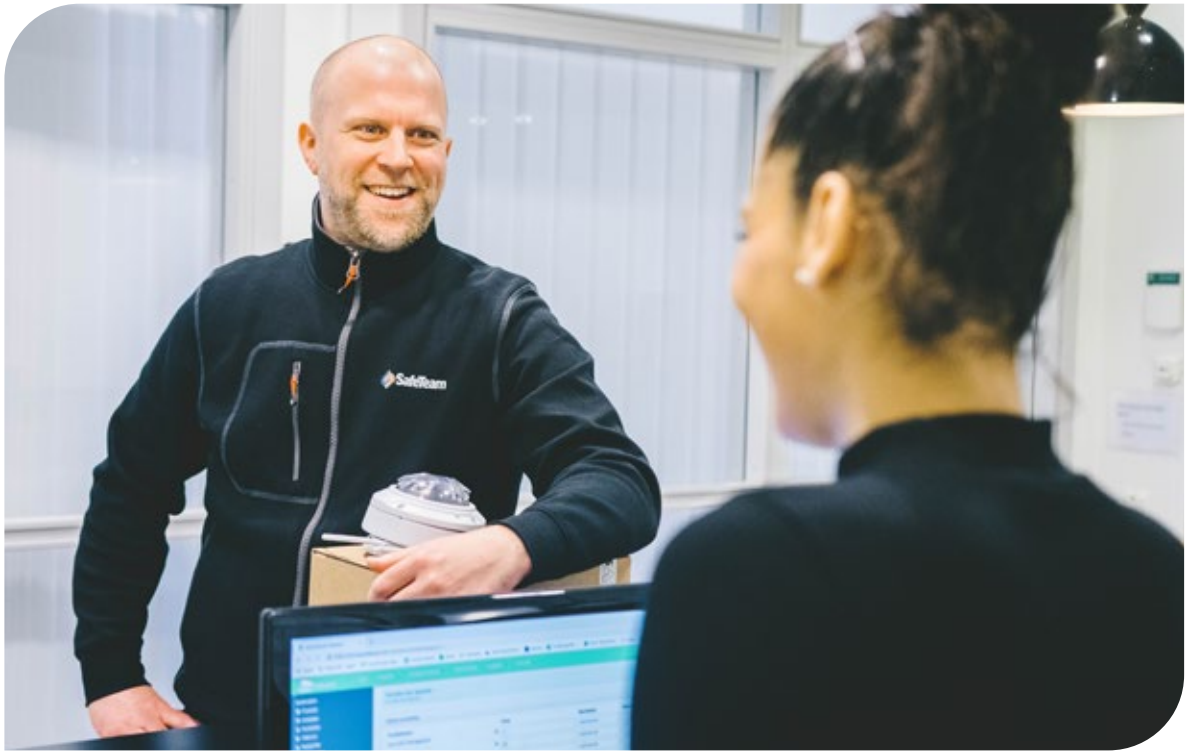
God läsning önskar

Thomas Benneklint,
vd på SafeTeam

Innehåll

1. Videoanalys

Denna bok handlar om smarta kameror. De kan beskrivas som bevakningskameror med inbyggd videoanalys och beslutslogik. Beslutslogiken är ganska enkel – ”om det brinner, då skickas larm till brandkåren”. Videoanalysen är det som gör smarta kameror ”smarta”. Därför inleder vi med att titta närmare på just möjligheterna med videoanalys.



Några begrepp

Video är en teknik för att elektroniskt fånga, lagra, bearbeta och återge en sekvens av bilder. Dessa bilder visas i en snabb följd för att skapa illusionen av kontinuerlig rörelse. Video kan åtföljas av ljud och kan spelas upp på olika enheter som tv-skärmar, datorer eller mobiltelefoner.

Video kan vara *analog* vilket innebär att bild- och ljudinformationen representeras av variationerna i amplitud och frekvens hos en elektrisk signal (som till exempel kan spelas in på ett VHS-band). Video kan också vara *digital* vilket innebär att bild- och ljudinformationen representeras av ettor och nollor (som till exempel kan skickas över internet).

Videoanalys avser processen att granska och tolka analog eller digital video för att extrahera meningsfull information.

Analysen kan göras *manuellt* av en person som granskar video synkront eller asynkront och drar slutsatser. Analysen kan göras *automatiskt* av en algoritm, till exempel artificiell intelligens, som letar efter mönster.

Manuell och automatisk analys kan göras *synkront* genom att analysera videon när den fångas i realtid. Då sägs ofta att analysen görs *on-line*, *live* eller i *realtid*. Analysen kan också göras *asynkront* genom att i efterhand analysera inspelad video. Då sägs ofta att analysen görs *off-line* eller i en *batch*.

Digital video sägs vara *strömmande (streaming)* när den överförs och visas i realtid utan behov av att ladda ned en fil med videodata.

Gen 0: Innan automatisk videoanalys

Från kamerabevakningens barndom, under 1940-talet, och ända fram på 1980-talet var videoanalys huvudsakligen manuell och synkron. Den gjordes av operatörer som tittade på en skärm som visade händelseförloppet i realtid.

Med början under 1980-talet och i allt större utsträckning under 1990-talet, i takt med ökad användning av bevakningskameror, kom manuell och asynkron videoanalys att bli allt vanligare.

Från kamerabevakningens barndom ända fram till 1990-talet var videoanalysen manuell och utfördes på analog video. Det är först med digitalisering av video som automatisk videoanalys blir verklighet. Vi kallar därför denna föregångstid

för den nollte generationens automatiska videoanalys eller ”gen 0” kort och gott.

Gen 1: Grundläggande rörelsedetektering

Åren runt millennieskiftet markerar övergången från analog video (sådan som spelas in på till exempel VHS-band) till digital video (sådan som kan skickas över IP-nätverk inklusive internet). Det möjliggjorde automatisk videoanalys.

I början låg fokus på synkron automatisk videoanalys. Det var framför allt rörelse man ville detektera, till exempel om någon person kommer in i bild. Detta gjordes med en algoritm som jämförde bildrutor som följde på varandra för att upptäcka förändringar i bildens pixelvärden.

Det finns många anledningar till att pixelvärden ändras – regn, löv som rör sig i vinden, skräp som flyger förbi, djur som passerar och så vidare. Så denna första generationens automatiska videoanalys (”gen 1”) var ganska primitiv med många falsklarm som resultat.

Gen 2: Mönsterigenkänning

Samtidigt som digital video blev vanligare växte behovet av att effektivt hantera alla datorfiler som skapas när digital video sparas på en hårddisk. Det gav upphov till en ny sorts mjukvara som kallas *videohanteringsmjukvara (video management software, VMS)*.

Från början var VMS ett verktyg för att lagra, hitta och visa video. Med tiden blev de allt mer sofistikerade, och från mitten av 2000-talet började de få möjlighet till avancerad videoanalys.

Denna videoanalys byggde på mönsterigenkänning. Föremål, djur och människor kändes igen på sin storlek och form. Det öppnade upp nya möjligheter:

- **Förenklad sökning och granskning:** VMS med videoanalys kan snabbt identifiera specifika händelser och tidpunkter i videomaterialet. Detta sparar tid och arbete jämfört med manuell granskning av timmar av inspelningar.

- **Händelsedetektering i realtid:** Systemet kan omedelbart identifiera och varna för säkerhetsincidenter så snart de inträffar. Detta förbättrar säkerheten genom snabbare respons jämfört med att manuellt övervaka flöden.
- **Affärsintelligens och kundinsikter:** Videoanalys ger insikter om kundbeteenden och butikstrafik. Detta kan leda till bättre affärsbeslut jämfört med traditionella gissningsbaserade metoder.
- **Operationell effektivitet:** Genom att övervaka och analysera arbetsflöden och processer kan systemet identifiera flaskhalsar och ineffektiviteter. Detta ökar produktiviteten jämfört med företag som inte använder sådan analys.
- **Riskhantering och efterlevnad:** Videoanalys kan hjälpa till att säkerställa att företag följer lagar och förordningar genom kontinuerlig övervakning. Det minskar risken för böter och rättsliga problem jämfört med företag som inte övervakar compliance lika noggrant.

De algoritmer som använder mönsterigenkänning baseras på specifika, förutbestämda regler och matematiska modeller för att känna igen form, storlek, färg, textur och liknande egenskaper som särskiljer objekt från bakgrunden och möjliggör klassificering och spårning av dem. Algoritmerna använder allt från enkla tekniker som tröskelvärden och kantdetektering till sofistikerade tekniker som konturanalys och optisk flödesanalys.

Vi kallar videoanalys som använder mönsterigenkänning för andra generationens automatiska videoanalys (”gen 2”). Även om gen 2 först dyker upp i VMS så dröjde det inte länge innan det också fanns bevakningskameror med mönsterigenkänning inbyggd.

Den andra generationens videoanalys är effektiv för enklare eller väldefinierade uppgifter där variationerna mellan olika objekttyper är klara och konsekventa. Men gen 2 kommer till korta i mer komplexa och föränderliga situationer.

Gen 3: Artificiell intelligens

För att hantera mer komplexa och oberäkneliga situationer, där mönsterigenkänning inte räcker till, började man mot slutet av 2010-talet ta hjälp av AI.

AI kan förstås som en algoritm som inte är utarbetad i detalj av människor, utan som har bildats genom att jämföra algoritmens svar med önskat svar för en ofantlig mängd exempel.

Missförstå inte begreppet generation.
En ny generation ersätter inte en äldre. Alla samexisterar. Ibland är första generationens videoanalys tillräckligt. Ibland är andra generationens videoanalys att föredra framför tredje generationens. Ibland är tredje generationens videoanalys den enda lösningen. Vad som är rätt val beror på situationen.

AI som används för videoanalys har formats på detta sätt genom att mata den med videoklipp efter videoklipp och återkoppla om svaret är rätt eller fel. Resultatet blir en AI-algoritm som när den får en videoström med stor sannolikhet kan ge önskad respons.

Från början skedde formandet av algoritmen, som kallas *maskininlärning*, innan den togs i bruk. När den väl togs i bruk kunde algoritmen inte ”lära” sig något nytt. Men numera är det vanligt att låta algoritmen forstätta att formas samtidigt som den används. Det gör den adaptiv till helt nya förhållanden.

Vi kallar videoanalys som använder AI för igenkänning av objekt och händelser för tredje generationens videoanalys (”gen 3”).

Objekt, egenskaper och beteenden

För att förstå möjligheterna med smarta kameror behöver vi bekanta oss med några termer som ofta används inom videoanalys.

I videoanalys avser objekt något som skiljer ut sig från bakgrunden och som kan identifieras och följas. Det kan till exempel vara ett fordon, en människa, ett djur.

En *egenskap* avser de distinkta attribut eller kännetecken som ett objekt kan ha och som kan identifieras genom videoanalys. Dessa egenskaper kan inkludera färg, storlek, form, eller specifika kännetecken såsom ett registreringsnummer på ett fordon.

Beteende refererar till mönster eller sekvenser av rörelser eller handlingar som ett objekt uppvisar i videon, till exempel stillastående, hastig rörelse, gå, springa, falla, öka hastigheten och bromsa.

Filter och regler

Här kommer ytterligare två termer som det är bra att känna till:

Ett *filter* väljer ut vilka kombinationer av objekt, egenskaper och beteenden som är relevanta händelser. Med ett filter kan händelsen att en människa går mot en port flaggas som relevant, medan händelsen att en människa går från samma port flaggas som irrelevant.

En *regel* styr vad som ska hända när en händelse inträffar. Med en regel kan händelsen att en människa går mot en port resultera i att ett varningsmeddelande spelas upp, video börjar spelas in och väktare uppmärksammas på händelsen.

Förebygg problem i portuppgången

En smart kamera kan lösa problem med personer som uppehåller sig för länge eller i för stora grupper på platser där man vill att människor ska få vara, men bara tillfälligtvis. Ett typiskt exempel är portuppgångar.

Kameran programmeras för att räkna antal personer i portuppgången och hålla koll på hur länge var och en är på plats.

Under dagen kan vem som helst uppehålla sig i upp till femton minuter i portuppgången. (Vi är frikostiga med tiden eftersom det kan vara en pensionär som väntar på färdtjänst.) På natten tillåter vi bara fem minuter.

Om någon uppehåller sig längre spelas ett meddelande upp som vänligt påminner om att portuppgången inte är ett uppehållsutrymme. Meddelandet upplyser också om att området är kamerabevakat och video skickas till larmcentral och sparas för eventuell brottsutredning. Samtidigt skickas videoströmmen till VMS för inspelning och till larmcentral.

Samma sak händer om fler än fem personer samlas i portuppgången och inte skingras inom fem minuter.

En poäng är att kameran inte streamar och inte spelar in något utan föregående varning. På så sätt skyddas de boendes personliga integritet.

2. Artificiell intellligens

Det går inte att skriva en bok om smarta kameror utan att prata om artificiell intelligens (AI). Det är ju AI som gör bevakningskamerorna smarta. Innan vi fördjupar oss i olika tillämpningsområden för smarta kameror kommer här en snabbkurs i AI.

Artificiell intelligens

Artificiell intelligens (artificial intelligence, AI) är ett omfattande begrepp som refererar till maskiners förmåga att utföra uppgifter som traditionellt kräver mänsklig intelligens. Detta inkluderar inlärning, problemlösning och anpassning till nya situationer. Denna förmåga skapas med en algoritm. Det finns allt från enkla algoritmer som kan lösa specifika problem, till avancerade system av algoritmer som kan ”förstå” och ”reagera” på komplexa indata.

Tidiga försök med AI inom kamerabevakning använde sig av enklare algoritmer. Men det som gör smarta kameror just smarta är deras förmåga att ”förstå” och ”reagera” på det som de ser.

Maskininlärning

Maskininlärning (machine learning, ML) är den förhärskande tekniken för att åstadkomma AI. Istället för att vara explicit programmerade att utföra en uppgift, använder ML-algoritmer data för att själva identifiera mönster och förbättra sin prestanda över tid. Detta kan involvera allt från att identifiera objekt på bilder till att förutsäga framtida händelser.

I sin enklaste form kan ML liknas vid en algoritm som drar en linje som så nära som möjligt approximerar mätdatan i ett xy-diagram, och sen använder linjen för att förutsäga y-värdet för ett givet x-värde.

Artificiella neurala nätverk

En mer avancerad form av ML är *artificiella neurala nätverk (artificial neural networks, ANN),* som är löst baserade på hur nervceller är sammankopplade i mänskliga hjärnor. Precis som hjärnan består av miljarder nervceller kopplade till varandra, är ett ANN uppbyggt av *noder* som representerar konstgjorda nervceller. Dessa noder är organiserade i lager: ett lager som tar emot signaler (t.ex. det en videokamera filmar), ett utgångslager som ger ett svar (t.ex. aktivera ett larm) och däremellan dolda lager. Varje nod förändrar signalen den tar emot och skickar det vidare till nästa lager.

Övervakad inlärning

Det finns flera olika sätt att ”lära upp” ett ANN. Den enklaste metoden kallas *övervakad inlärning (supervised learning)*. Då jämförs nätverkets svar med förväntat svar. Skillnaden används sedan för att justera hur noderna förändrar inkommande signal innan den skickas vidare.

Övervakad inlärning kan användas för att lära en smart kamera att se skillnad på människor och djur. Kamerans ANN matas med videosignaler som visar människor och olika djur i olika kombinationer, i olika positioner, med olika rörelsemönster, under olika väder- och ljusförhållanden.

Oövervakad inlärning

Ett annat sätt att ”lära upp” ett ANN kallas *oövervakad inlärning (unsupervised learning)*. I detta tillvägagångssätt finns inga fördefinierade svar. Istället justeras hur noderna förändrar inkommande signal innan den skickas vidare, så att det uppkommer ett så tydligt mönster eller en så tydlig gruppering som möjligt.

Oövervakad inlärning kan användas för att generera värmekartor från kundrörelser inom en butik. Genom att analysera videodata med en smart kamera utrustad med ett ANN, kan systemet upptäcka vilka områden i butiken som frekventeras mest. Denna process skapar värmekartor baserade på rörelsemönster och uppehållstider, vilket underlättar förståelsen av kundbeteende och bidrar till effektivare butikslayout.

Förstärkningsinlärning

Förstärkningsinlärning (reinforced learning, RL) är ett tredje sätt att ”lära upp” ett ANN. Precis som vid övervakad och oövervakad inlärning justeras hur noderna förändrar inkommande signal innan den skickas vidare för att komma så nära ett mål som möjligt. Vid övervakad inlärning är målet att minimera skillnaden mellan svar och önskat svar. Vid oövervakad inlärning är målet att skapa en så tydlig uppdelning av data som möjligt. Och vid förstärkt inlärning är målet att maximera belöning (och minimera straff) över tid. Belöning och straff utdelas av en annan belöningsfunktion som är en algoritm som utvärderar vad som blir resultatet av den utdata som ANN ger.

Förstärkt inlärning kan tillämpas på händelsedetektion i smarta kameror. Genom förstärkningsinlärning lär sig kameran att skilja på normala och misstänkta aktiviteter. Systemet belönas för korrekt identifierade incidenter och straffas för missar eller falsklarm. Således förbättras kamerans förmåga att fokusera på relevanta händelser över tid, vilket optimerar säkerhet och minskar onödiga avbrott.

Djupinlärning

Djupinlärning (Deep Learning, DL) har, namnet till trots, inget att göra med hur ANN lär sig något. Djup syftar på djupet av nätverket mätt i antal dolda lager. Desto fler lager, desto mer komplexa uppgifter kan systemet lösa. Ett bättre namn hade varit ”djupt artificiellt neuralt nätverk”.

För videoanalys kan antalet dolda lager sträcka sig från ett tiotal, för enklare uppgifter som rörelsedetektering, till hundratals dolda lager, för mer avancerade uppgifter, såsom ansiktsigenkänning.

Stor språkmodell

Stor språkmodell (Large Language Model, LLM) är ett djupt artificiellt neuralt nätverk som med oövervakad inlärning har ”lärt sig” sannolikheter för olika ord i olika sammanhang genom att ”läsa” ett stort antal böcker, tidningar, webbsidor med mera.

En stor språkmodell kan användas för att tolka text skriven på vanlig svenska och för att svara på samma sätt. Den mest kända stora språkmodellen i skrivande stund är Open AI:s GPT som används i både Open AI:s ChatGPT och Microsoft Copilot.

Generativ AI

Generativ AI kallas AI som fokuserar på att skapa innehåll. Det kan vara text, bilder, musik, eller annan media. Generativ AI involverar skapandet av ny data som är liknande men inte identisk med den data som modellen tränats på. Detta skiljer sig från diskriminativa AI-modeller, som istället fokuserar på att kategorisera eller tolka inkommande data.

Eftersom stora språkmodeller kan användas för att generera text, genom att helt enkelt lägga till ett ord i sänder, är de exempel på generativ AI.

3. Smarta kameror

En *smart kamera* är en bevakningskamera som utför videoanalys i realtid med hjälp av inbyggd artificiell intelligens (AI). Kameran filtrerar objekt och beteenden i realtid och avgör själv vilken åtgärd som krävs. Resultatet av analysen kan även skickas till en användare eller ett system för vidare bearbetning och åtgärd.

Edge AI

En smart kamera har inbyggd AI, vilket innebär att den har en processor och AI-programvara som kan analysera video direkt i kameran. Detta står i kontrast till traditionella bevakningskameror som skickar videoströmmar till en central enhet (till exempel en VMS) för analys.

Edge AI är den specifika termen för att använda AI i enheter vid ”kanten” av nätverket, i detta fall kameran. Det ger en mer distribuerad och skalbar AI-lösning

Det finns separat hårdvara med edge AI för videoanalys som kan placeras intill bevakningskameror som inte är smarta kameror. På så sätt kan ett äldre system dra nytta av edge AI utan att kameror behöver bytas.

Videoanalys i kameran

Fördelarna med att göra videoanalys i realtid i kameran istället för att skicka en videoström till ett VMS är många:

- **Snabbare respons:** Analysen sker i realtid, direkt i kameran, vilket eliminerar behovet av att skicka videoströmmar till en central enhet. Det gör att händelser identifieras och åtgärdas snabbare.
- **Lägre kostnader:** Endast analysresultatet skickas, vilket sparar bandbredd och lagringsutrymme.
- **Förbättrad säkerhet:** Känslig video lämnar inte kameran, vilket förbättrar datasäkerheten.

Flera typer av videoanalys kan utföras i kameran, inklusive:

- **Objektigenkänning:** Upptäcka specifika objekt, typ av fordon, djur, människor med mera.
- **Identifiering:** Känna igen enskilda individer på ansiktet eller annan biometrisk identifikation.
- **Ljudigenkänning:** Känna igen skrik, glaskross och liknande med kamerans mikrofon.
- **Beteendigenkänning:** Identifiera snabba rörelser och andra ovanliga eller oönskade beteenden.
- **Räkna:** Räkna antal objekt som passerar en linje.
- **Avläsa:** Läsa av text och siffror (till exempel på registreringsskyltar)
- **Mäta:** Mäta avstånd eller ytor inom kamerans synfält, till exempel för att uppskatta folktäthet eller övervaka tillgängligheten av utrymme i realtid.
- **Maskera:** Maskera ansikten och annat som skulle kunna vålla problem med GDPR.

Filter

En smart kamera har filter som analyserar relevanta händelser och ignorerar oviktiga detaljer. Exempel på filter inkluderar:

- **Storleksfilter:** Filtrerar objekt baserat på storlek (till exempel för att ignorera små djur).
- **Färgfilter:** Filtrerar objekt baserat på färg (till exempel för att identifiera röda fordon).
- **Platsfilter:** Filtrerar objekt baserat på plats i bilden (till exempel för att fokusera på en specifik zon).

Regler

Regler används för att avgöra om en händelse kräver åtgärd. Dessa kan baseras på:

- **Objekt:** En typ av objekt finns där de inte ska finnas (till exempel en människa där bara fordon är tillåtna).
- **Beteende:** En typ av beteende som inte är tillåtet (till exempel att klättra över ett stängsel).
- **Plats:** Ett objekt eller beteende identifieras på en plats där det inte får vara respektive ske (till exempel människa befinner sig i ett spårområde).
- **Tidpunkt:** Ett objekt eller beteende identifieras vid en tidpunkt när det inte ska ske (till exempel en människa befinner sig i lokalen efter 22).
- **Tidsåtgång:** Ett objekt uppehåller sig för länge på samma plats (till exempel en person som hänger i ett trapphus).

Resultat istället för video

I många fall är det inte nödvändigt att skicka hela videoströmmen till en server. Det räcker att skicka resultatet av analysen, till exempel identifiering av ett objekt eller en varning om en händelse. Detta sparar bandbredd och lagringsutrymme.

Exempel:

- En kamera skickar en varning om en person identifieras i trädgården.
- En kamera skickar en bild till ett trafikövervakningssystem av ett fordon som kör för fort.

Larma och skicka vidare

När en smart kamera identifierar en händelse skickas denna information vidare till ett centralt system för vidare bearbetning och åtgärder.

Detta kan inkludera att larma säkerhetspersonal, dokumentera händelsen för framtida granskning, eller aktivera andra säkerhetssystem. Genom att endast skicka relevanta händelser minimeras överflödet av data och personal kan reagera snabbare på faktiska hot eller problem.

Ett exempel från industrin är kameror som ser skillnad på lastbilar och andra fordon och enbart öppnar grinden för lastbilar. Samtidigt plingar en klocka i lagerlokalen så att personalen kan gå och möta lastbilen. En mer sofistikerad variant är att kameran känner igen behöriga lastbilar baserat på registreringsnumret och bara öppnar för dem.

Smart kamera som sensor

En smart kamera är inte enbart en konventionell bevakningskamera med en extra möjlighet att styra när och hur den ska larma med filter och regler. Den är också en sensor och kan användas som en intelligent sensor.

En *sensor* är en enhet som omvandlar fysiska egenskaper till mätvärden. Därför är en smart kamera som räknar antal personer i en lokal och skickar den informationen istället för att skicka en videoström ett exempel på en sensor.

En *intelligent sensor* är en sensor som också agerar baserat på insamlade mätvärden. Därför är en smart kamera som räknar antal personer som går in och ut ur en lokal och slår på larmet fem minuter efter att sista personen har lämnat lokalen ett exempel på en smart kamera som fungerar som en intelligent sensor.

Smarta kamerors filter gör dem till mycket mångsidiga sensorer:

- Ett filter som särskiljer och kategoriserar objekt kan till exempel användas för att räkna människor men inte djur som passerar förbi en kamera, eller för att räkna antal fordon av vardera fordonsslag som passerar en grind.
- Ett filter som identifierar beteenden kan till exempel användas för att räkna dem som uppehåller sig på en plats men inte för dem som bara passerar, eller för att räkna antal personer som rör sig mot eller från en dörr.
- Ett filter som känner igen egenskaper eller text kan till exempel användas för att räkna antal röda bilar på en parkeringsplats eller räkna antal svenska respektive utländska registreringsskyltar som sitter på fordon som passerar en grind.

Insamlad mätdata kan användas med regler i kameran för att direkt vidta åtgärder, till exempel larma på en lokal när den blir folktom.

Mätdata kan också skickas vidare till andra system. Till exempel kan antal parkerade bilar på en parkeringsplats eller i ett P-hus skickas till ett system som kan jämföra antalet parkerade bilar med antal giltiga P-biljetter; finns fler bilar parkerade än giltiga P-biljetter kan denna information skickas till P-vakter.

Visualisering

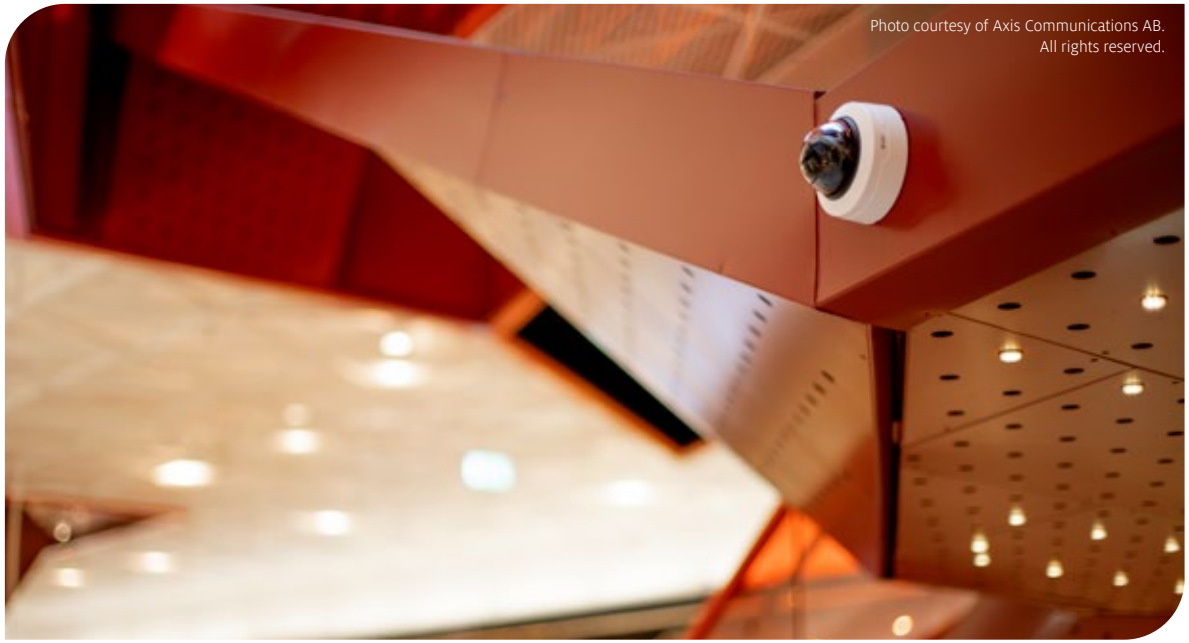
Mätdata som samlas in av smarta kameror kan med program visualiseras som grafer och diagram för att förenkla analys och förståelse.

Ofta är det graferna i sig som är det intressanta. Då behöver ingen video överföras, vilket sparar bandbredd, lagringsutrymme och uppfyller kraven i GDPR och kamerabevakningslagen.

Men ibland är det relevant att visa både mätdata och video live. Då kan mätdata läggas i ett genomskinligt lager ovanpå videon så att båda syns samtidigt. Till exempel kan bevakning av parkeringsplatser för elbilar i samma bild visa vilka laddstationer som laddar och hur mycket.

Datareducering

Om mätdata är det intressanta och inte videon som den grundas på finns egentligen ingen anledning att skicka eller spara videon. Det räcker med att spara mätdatan. Det spar oerhört mycket bandbredd och lagringsutrymme. I stället för att ha en dyr videoserver kan bara mätadata skickas till molnet för nästan ingen kostnad alls.



Om mätdatan används för att fatta ett beslut som loggas, till exempel att skicka larm till larmcentral, så kan beslutet loggas tillsammans med en kort videosekvens, istället för hela videoflödet. Återigen sparas bandbredd och lagringsutrymme.

Tidsserier och prognoser

Smarta kameror har inbyggd klocka. Det kan användas för att skapa tidsserier med mätvärden. Dessa kan sedan visualiseras i ett tidsdiagram för enklare analys och beslut. Till exempel kan en tidsserie ge en bild över hur trafiken genom en tunnel varierar över tid. Genom att använda smarta kamerors förmåga att kategorisera objekt kan användare välja att se variationer för olika fordonsslag.

Tidsserier kan också användas för att skapa modeller som gör det möjligt att skapa prognoser. Till exempel kan en tidsserie med antal kunder i butik samköras med data från vädertjänster och business intelligence (BI) för att skapa en modell som förutser kundflöden efter aktuell väderprognos.

Integritet

En stor fördel med att använda smarta kameror som sensor istället för att använda dem som en konventionell bevakningskamera är att det inkräktar på den personliga integriteten mycket mindre eller inte alls. Det gör det också lättare att efterleva GDPR.

En smart kamera som direkt, utan att lagra eller skicka videoströmmen, omvandlar videoströmmen till mätvärden torde inte inkräkta på den personliga integriteten hos dem som befinner sig framför kameran, förutsatt att mätvärdet i sig inte är en personuppgift.

Ett tänkbart användningsområde är att använda smarta kameror som sensor för att upptäcka om en vårdtagare har ramlat ur sängen. Kamerans filter gör att den bara reagerar om en person ramlar ur sängen, inte om ett lakan, en kudde eller en bok faller ur sängen. Kamerans regler gör att den larmar vårdpersonalen när en person har ramlat ur sängen. Ingen video lagras eller skickas. Inte ens när larmet går. Sådan användning av smart kamera torde inte kräva tillstånd.

Maskering

Så fort en videoström lagras eller skickas finns en uppenbar risk att det faller under kamerabevakningslagen och GDPR. Det är självklart om syftet är att filma personer. Men även om syfte inte är att filma personer så kan blotta möjligheten att

någon syns i bild göra att kamerabevakningslagen och GDPR gäller. Men det finns saker smarta kameror kan göra för att minska eller helt ta bort intrånget i den personliga integriteten.

En smart kamera som direkt, utan att lagra eller skicka videoströmmen, maskerar ansikten och allt som kan utgöra en personuppgift (till exempel fordons registreringsskyltar) på ett sätt som gör det omöjligt att någonsin identifiera en person, torde inte falla under kamerabevakningslagen eller GDPR.

Ibland kan det dock finnas goda skäl att återskapa videoströmmen som den var före maskering. Det kan till exempel gälla utredning av ett allvarligt brott. Då ger smarta kameror två andra möjligheter. En metod tillåter personer med behörighet att få en separat videoström utan maskering. En annan metod maskerar med kryptoteknik vilket gör det möjligt att avmaska med en kryptonyckel.

Videomanipulation och deep fake

Det är en tidsfråga innan en åtalad person, ställd inför bevisning i form av video från en bevakningskamera, hävdar att videoklippet är ”deep fake”.

Deep fake är en manipulerad video där verkliga bilder har förvanskats med AI-teknik för att skapa falska händelser eller handlingar.

En smart kamera kan göra det svårare att hävda att en video har manipulerats eller är en deep fake genom att använda digital vattenstämpling och kryptering.

- **Digital vattenstämpling:** Detta innebär att kameran inbäddar en unik, osynlig kod i varje bildruta som kan verifiera videons ursprung och autenticitet. Om videon ändras, även subtilt, kommer detta att påverka koden, vilket indikerar att en manipulation har skett.
- **Kryptering:** Genom att kryptera videodata direkt vid inspelningtidpunkten kan kameran säkerställa att endast behöriga användare med rätt dekrypteringsnyckel kan se videon i dess ursprungliga form. Detta hjälper till att bevara videons integritet från kameran till slutanvändaren.

Genom att kombinera dessa metoder kan smarta kameror bidra till att skapa ett trovärdigt system där videomaterial kan verifieras och skyddas mot falska påståenden om manipulation.

AI är inte lösningen på allt

Bara för att AI är hett är det inte alltid bäst.

Första och andra generationens bevakningskameror – som saknar AI – brottas med hög andel falsklarm. Tillspetsat kan man säga att de ger falsklarm nio gånger av tio.

Tredje generationens bevakningskameror – smarta kameror – gör det möjligt att med filter och regler minimera falsklarm. Men då finns en liten risk att kameran missar att larma när den ska. Det kan lösas genom att skapa två uppsättningar filter och regler: En som är gjord för att undvika falsklarm. Och en backup där man accepterar en hög andel falsklarm.

Poängen är att om en hög andel falsklarm inte är ett problem, så kan en äldre bevakningskamera fortfarande duga. Det är inte alltid nödvändigt med en smart kamera.

Videoanalys i butiksmiljö

Butikers utformning och hur produkter placeras påverkar kundens köpbeteende. Det är alltså bra att veta hur kunderna beter sig, och vi kan använda videoanalys för att räkna kunder i olika sektioner av butiken. Resultatet presenteras i ett färgdiagram *(heat map)*.

Färgdiagrammet använder färger för att visa var folk befinner sig. En kall blå färg indikerar ett litet antal personer. En varm röd färg indikerar ett stort antal. Och däremellan visar olika nyanser av blått, grönt, gult, orange och rött ett växande antal.

Genom att göra en film av färgdiagrammet vid olika tidpunkter kan man få en överskådlig bild över var det finns utrymmen som inte används effektivt. Det gör det lättare att förbättra butikens utformning och placering av produkter, utan att behöva besvära kunderna.

Samma teknik kan användas för att upptäcka köer till kassan. Det kan kopplas till högtalarsystemet som gör automatiskt utrop till personalen att öppna en kassa till.

I dessa exempel används bevakningskameror utan att filma någon. Du kan alltså använda kameror för att göra undersökningar, utan att påverka den personliga integriteten.

4. Många möjligheter

Smarta kameror har många användningsområden för att förbättra säkerhet, effektivitet och insikter. Sällan har uttrycket ”endast fantasin sätter gränser” stämt så väl som nu. Nedan beskrivs några olika möjligheter med exempel.

Rörelsemönster
(Movement Patterns)

Smarta kameror kan analysera och förstå hur objekt eller människor rör sig inom ett område, vilket kan hjälpa till med planering och säkerhet.

Exempel: Ett varuhus använder kameror för att kartlägga kundernas rörelser, vilket möjliggör optimering av butikslayouten för att förbättra kundflöden och öka försäljningen.

Objektigenkänning
(Object Recognition)

Denna funktion gör det möjligt för kameror att känna igen och identifiera specifika objekt eller personer.

Exempel: Ett säkerhetssystem i en kontorsbyggnad identifierar en obehörig person och larmar automatiskt säkerhetspersonalen.

Händelsedetektion
(Event Detection)

Kameror kan upptäcka och varna för ovanliga eller misstänkta aktiviteter i realtid.

Exempel: En kamera i ett lager upptäcker rökutveckling och skickar omedelbart en varning till brandkåren.

Demografisk analys
(Demographic Analysis)

Kameror analyserar och samlar statistik om demografiska faktorer som ålder och kön hos personer inom kamerans synfält.

Exempel: En reklambyrå analyserar åldersfördelning och kön hos besökare vid en reklamskylt för att skräddarsy framtida reklaminnehåll.

Emotionsanalys
(Emotion Analysis)

Genom att tolka ansiktsuttryck och kroppsspråk kan ett kamerasystem bedöma människors känslor.

Exempel: En detaljhandel använder kameror för att identifiera nöjda och missnöjda kunder för att kunna förbättra kundservicen.

Fordonsigenkänning
(Vehicle Recognition)

Denna teknik identifierar olika typer av fordon och kan användas för säkerhets- och övervakningsändamål.

Exempel: En kamera vid en gränsövergång känner igen och spårar registreringsskyltar för att upptäcka stulna fordon.

Föremålsspårning
(Object Tracking)

Tekniken gör det möjligt för kameror att följa rörelserna hos specifika objekt eller personer.

Exempel: En distributionscentral använder smarta kameror för att spåra och dokumentera ett pakets väg genom sorteringssystemet.

Hälsoövervakning
(Health Monitoring)

Kameror används för att analysera beteenden för att identifiera potentiella hälsoproblem, särskilt hos äldre eller personer med särskilda behov.

Exempel: Ett äldreboende använder kameror för att upptäcka om en vårdtagare faller i sitt rum.

Interaktionsspårning
(Interaction Tracking)

Kameror utvärderar interaktioner mellan människor eller mellan människor och objekt för att få insikter om beteenden.

Exempel: Ett museum analyserar hur besökare interagerar med olika utställningar för att optimera framtida utställningsdesign.

Räkning
(Counting)

Kameror räknar personer, fordon eller objekt för att tillhandahålla användbar statistik och analys.

Exempel: En tågstation använder smarta kameror för att räkna antalet passagerare och anpassa tidtabeller och personalbehov efter detta.

Områdesintrång
(Area Intrusion)

Kameror identifierar när personer eller objekt går in i eller lämnar definierade zoner.

Exempel: Ett företagsområde använder smarta kameror för att detektera och larma om obehöriga intrång efter arbetstid.

Värmekartor
(Heat Maps)

Kameror skapar visuella representationer baserade på rörelsemönster och fördelningen av människor över tid.

Exempel: En detaljhandelskedja använder värmekartor för att analysera vilka områden i butiken som besöks mest, vilket bidrar till mer informerade beslut om produktplacering och butiksdesign.

Fordonshastighet
(Vehicle Speed)

Kameror övervakar och mäter fordonshastigheter för att identifiera överskridanden av hastighetsbegränsningar.

Exempel: En kommun installerar kameror som mäter hastigheten på fordon för att identifiera och varna fortkörare i bostadsområden.

Ljusförhållanden
(Lighting Conditions)

Justering av kamerainställningar baserat på nuvarande ljusförhållanden för att säkerställa optimal bildkvalitet.

Exempel: En kamera på en parkeringsplats anpassar sig automatiskt till förändrade ljusförhållanden under dagen för att leverera tydliga bilder.

Kvalitetssäkring
(Quality Assurance)

Kameror övervakar och analyserar tillverkningsprocesser för att upptäcka defekter eller avvikelser.

Exempel: En produktionslinje för elektronik använder smarta kameror för att tidigt upptäcka och sortera bort defekta produkter.

Integration
(Integration)

Integration av smarta kameror med andra system och teknologier för förbättrad funktionalitet och datainsamling.

Exempel: Ett sjukhus integrerar smarta kameror med patienthanteringssystemet för att övervaka patienternas säkerhet och välbefinnande.

Ansiktsigenkänning
(Face Recognition)

Teknik för att identifiera och verifiera individer baserat på deras ansiktsdrag.

Exempel: Ett säkerhetssystem på en flygplats använder ansiktsigenkänning för att snabbt och säkert verifiera passagerares identiteter.

Djurövervakning
(Animal Monitoring)

Kameror identifierar när personer eller objekt går in i eller lämnar definierade zoner.

Exempel: Ett företagsområde använder smarta kameror för att detektera och larma om obehöriga intrång efter arbetstid.

Köhantering
(Queue Management)

Teknik som låter kameror mäta och hantera kölängder och väntetider för att förbättra kundupplevelsen.

Exempel: En flygplats implementerar smarta kameror för att övervaka kölängder vid säkerhetskontrollen och öppnar ytterligare linjer vid behov.

Beteendeanalys
(Behavior Analysis)

Vi låter kameror utvärdera och analysera beteenden och kroppsspråk för att dra slutsatser om individers eller grupper av individers tillstånd.

Exempel: Ett köpcentrum använder kameror för att studera kunders beteenden och identifiera mönster som kan förbättra kundnöjdheten.

Miljöövervakning
(Environmental Monitoring)

Kameror övervakar och rapporterar förändringar i miljön för att bidra till hållbarhet och säkerhet.

Exempel: En kommun använder smarta kameror för att övervaka vattenflöden och vattennivåer för att tidigt upptäcka översvämningar.

Avvikande detektion
(Unusual Detection)

Denna funktion upptäcker och varnar för ovanliga beteenden eller händelser som avviker från det normala.

Exempel: En bilfirma använder smarta kameror för att identifiera och larma om oväntade händelser, som en person som klättrar över ett staket eller om obehöriga fordon kör in på parkeringen efter stängningstid.

Dröjsmålsdetektion
(Loitering Detection)

Smarta kameror uppmärksammar när personer stannar för länge i ett specifikt område, vilket kan vara ett tecken på misstänkt beteende.

Exempel: En bank installerar smarta kameror för att detektera och varna för personer som dröjer sig kvar utanför bankomaterna under natten, vilket kan indikera planering av olaglig aktivitet.

Gränsöverträdelsedetektion
(Linecross Detection)

Funktion som gör att kameror larmar när ett objekt korsar en fördefinierad virtuell gräns.

Exempel: Ett industriområde använder smarta kameror för att övervaka och varna när obehöriga personer korsar områdesgränser under icke-arbetstider.

Snatteridetektering
(Snatch Detection)

Kameror detekterar och registrerar snabba, oväntade rörelser som kan tyda på stöld eller annan aggressiv handling.

Exempel: En mobiltelefonbutik använder smarta kameror för att upptäcka och larma om plötsliga rörelser som kan indikera en väskryckning eller snatteri.

Sabotagedetektion
(Tampering Detection)

Funktion som varnar när en kamera manipuleras, antingen genom fysisk förflyttning eller blockering av linsen.

Exempel: En kamera monterad i en offentlig park varnar automatiskt om den blir flyttad, om den täcks över eller om något ställs framför den.

Detektion av övergivna föremål
(Unattended Luggage Detection)

Teknik för att identifiera föremål som lämnats utan uppsyn en längre period, vilket kan vara en säkerhetsrisk.

Exempel: En flygplatsterminal använder smarta kameror för att upptäcka övergivet bagage och varna säkerhetspersonalen.

Passeringsdetektion
(Tailgating Detection)

Med kamerabevakning kontrollerar vi om fler än en person eller fler än ett fordon passerar en kontrollpunkt på en gång, vilket kan tyda på obehörig åtkomst.

Exempel: Ett företags kontorsbyggnad använder smarta kameror för att upptäcka och larma om en person följer direkt efter en annan genom en säkerhetskontrollerad dörr utan att visa passerkort.

Ansiktsdetektion
(Face Detection)

Teknik för att skilja ansikten från andra objekt utan att identifiera dem, vilket kan användas för att upprätthålla privatliv och efterlevnad av GDPR.

Exempel: En detaljhandel använder smarta kameror för att upptäcka ansikten och analysera kundflöden utan att samla in eller lagra personlig information.

Falldetektion
(Fall Detection)

Kameror uppmärksammar när en person faller till marken, vilket kan vara ett tecken på en olycka eller medicinsk nödsituation.

Exempel: Ett vårdhem använder smarta kameror för att upptäcka när en brukare faller. Larm går ut till personalen.

Branddetektion
(Fire Detection)

Kameror identifierar tecken på eld eller rök, vilket möjliggör snabb åtgärd för att förhindra skador eller förluster.

Exempel: En lagerbyggnad installerar smarta kameror med branddetektion för att tidigt upptäcka och reagera på potentiella bränder, vilket minimerar skaderisk och säkerhetsrisker.

Rökdetektion
(Smoke Detection)

Kameror uppmärksammar när det finns rökutveckling, vilket kan indikera en början på en brand.

Exempel: Ett hotell använder smarta kameror med rökdetektion för att varna personalen om det finns tecken på brand, vilket möjliggör snabb evakuering och åtgärd.

Registreringsskyltsigenkänning
(License Plate Recognition)

Kameror identifierar och lagrar information från fordonsskyltar för säkerhet, övervakning eller automatiserad åtkomstkontroll.

Exempel: Ett parkeringshus använder smarta kameror för att automatiskt läsa av registreringsskyltar och hantera tillträde samt betalning utan behov av manuell inmatning.

Felkörningsdetektion
(Wrong Way Detection)

Kameror varnar när fordon rör sig i fel riktning, exempelvis in på en enkelriktad gata eller motorvägsavfart.

Exempel: En motorvägsoperatör installerar smarta kameror för att upptäcka fordon som kör åt fel håll. Andra förare kan varnas via trafikskyltar.

Obehörig parkeringsdetektion
(Unauthorized Parking Detection)

Kameror identifierar fordon som parkerar olagligt eller en ovanligt lång period.

Exempel: Ett bostadsområde använder smarta kameror för att upptäcka och varna för fordon som blockerar nödutgångar eller parkerar på handikapparkering utan tillstånd.

Sensorer

En smart kamera kan användas som en sensor som i realtid omvandlar det som är framför linsen till data och insikter. Några exempel:

En smart kamera kan mäta mängden sopor i ett sopkärl. När kärlet är nästan fullt, skickar den ett meddelande till fastighetsskötaren som ser att det är dags att byta kärl. Det gör att fastighetsskötaren inte behöver rondera soprummen. Samma smarta kamera kan också larma om sopkärlet har vält eller hamnat fel.

Ventilationen i en lokal kan styras av en smart kamera som räknar antal personer i lokalen. Kameran instruerar ventilationssystemet att ändra luftflödet så att det ökar när det är många personer i lokalen. Kameran kan ersätta en dyr CO2-sensor, som dessutom reagerar först när det är för mycket koldioxid, istället för att vara proaktiv som kameran.

Förmodligen har du redan bevakningskameror med dessa möjligheter. De flesta kameror sålda de senaste åren är smarta kameror. Genom att utnyttja dessa kamerors avancerade funktioner kan din organisation öka effektiviteten och reaktionsförmågan utan den komplexitet som ytterligare sensorer innebär. Detta gör smarta kameror till ett kostnadseffektivt och mångsidigt verktyg i moderna övervaknings- och automationssystem.

5. Framtiden

Vad är nästa steg i utvecklingen av videoanalys och smarta kameror? Vi lämnar de fantasifulla framtids-spaningarna därhän och fokuserar på vad som ligger precis om hörnet.

I dagsläget kan smarta kameror skilja människor från djur, känna igen olika typer av fordon och identifiera färger bland annat. Närmaste tiden kommer vi sannolikt få ännu fler möjligheter att kategorisera objekt. AI-tekniken i kamerorna har få begränsningar i detta avseende. Det är mest en fråga om vad för sorts data de är tränade på under inlärningen.

Det är inte otänkbart att den som ska sätta upp filter och regler kan beskriva dem i klartext. Exempel:

Om tre eller fler personer uppehåller sig två minuter eller längre i trappuppgången ska du läsa upp följande meddelande: "Var vänlig och lämna trappuppgången!" Skicka larm till larmcentralen om de tre minuter därefter fortfarande uppehåller sig i trappuppgången.

Smarta kameror kommer sannolikt använda generativ AI för att larma och rapportera i klartext. Det skulle kunna se ut så här:

Tre personer har uppehållit sig i trappuppgången under 5 minuter och inte lämnat efter att röstmeddelande har spelats upp.

Även VMS kommer sannolikt få liknande möjlighet att både ta emot en instruktion och ge svar med klartext i form av en chat. En dialog skulle kunna se ut så här:

Har en person med gul jacka passerat idag?

Ja, en person med gul jacka passerade idag klockan 13.10.

Svenskar positiva till kamerabevakning

Flertalet studier visar att majoriteten är positiva till kamerabevakning, eftersom det ökar den personliga säkerheten. De flesta av oss anser att kamerabevakning inte inkräktar på vår personliga integritet.

I opinionsundersökningar som Lunds universitet och Kantar Sifo gjorde 2017, 2018 och 2019 svarade 88–90 procent av alla tillfrågade att de var positiva till bevakningskameror på allmän plats.

Många tror att de behöver tillstånd för kamerabevakning, men tillstånd krävs bara för företag, myndigheter och organisationer som utför uppgifter av allmänt intresse, till exempel skolor, vårdcentraler och lokaltrafik.

En bostadsrättsförening eller ett företag som inte utför uppgifter av allmänt intresse behöver inte söka tillstånd för kamerabevakning. Däremot måste de följa reglerna i kamerabevakningslagen (KBL) och dataskyddsförordningen (GDPR).

Enligt KBL måste du tydligt visa att det finns kameraövervakning, enklast i form av tydliga skyltar. Har du kameror på en arbetsplats måste du förhandla med facket. Du har dessutom tystnadsplikt.

Enligt GDPR måste du visa att kamerabevakningen är nödvändig (till exempel för säkerhet och brottsförebyggande ändamål) och att nyttan väger tyngre än den enskildes önskan att inte bli bevakad.

GDPR ställer också krav på uppgiftsminimering. Bevakning får endast ske i den utsträckning som är motiverad av ändamålet. Materialet ska hanteras på ett säkert sätt och får inte sparas längre än nödvändigt.

Tillsammans skapar vi trygghet

Vi skapade denna e-bok för att visa styrkan i smarta kameror. Dagens smarta kameror reagerar och löser uppgifter utifrån förutbestämda regler, och det är mer fantasin än tekniken som sätter gränser för bevakningskamerans nytta i samhället.

Du är alltid välkommen att höra av dig till oss för kostnadsfri konsultation. Våra behöriga ingenjörer inom kamerabevakning tycker det här är det mest spännande som finns, och vi har glädjen att arbeta med kunder som ligger i framkant vad gäller ny kamerateknik – tillsammans med oss.

Vi följer med dig hela vägen från projektering, installation, utbildning och service. Besök vår webbplats för mer inspiration och tveka inte att kontakta oss.

www.safeteam.se

SafeTeam

Utgiven av SafeTeam i Sverige AB 2024