Teknologirådet

Ansiktsgjenkjenning og personvern

Ansiktsgjenkjenning blir tatt i bruk på stadig flere områder, som å låse opp telefonen eller betale. Det er raskt, enkelt og sikkert. Men samtidig gjør teknologien det mulig å drive masseovervåkning – uten at vi er klar over at det skjer.

Kunstig intelligens driver utviklingen

Mellom 2014 og 2018 gikk suksessraten for systemer for ansiktsgjenkjenning fra 96 til 99,8 prosent. Teknologien har nå blitt så treffsikker at den er bedre enn mennesker til å kjenne igjen ansikter, og mange anser den som sikrere enn passord.

Maskinlæring og det store antallet bilder og videoer på internett bidrar til at teknologien blir stadig bedre. Det er heller ikke behov for spesialisert utstyr – programvare for ansiktsgjenkjenning kan brukes på bilder fra de fleste datamaskiner, smarttelefoner og digitale kameraer.

For at en maskin skal kunne brukes til ansiktsgjenkjenning, må den først være i stand til å finne et ansikt på et bilde. Dette kan være et fotografi, eller en video i sanntid fra et overvåkningskamera.

Deretter analyseres ansiktene og det lages en biometrisk mal basert på den enkeltes distinkte kjennetegn, som avstand mellom øynene, nese og munn, eller mer abstrakte kjennetegn. Denne malen sammenliknes deretter med et annet bilde eller en database av bilder for å se etter treff.

SAMMENDRAG

- Ansiktsgjenkjenning er en sikker, billig og effektiv måte å identifisere mennesker på.
- Teknologiutviklingen har gått raskt de siste årene, og bruksområdene blir stadig flere. Ansiktet erstatter passord, brukes for betaling, ved adgangskontroll og i sikkerhetsarbeid.
- Ansiktsgjenkjenning åpner for masseovervåkning fordi kapasiteten blir enorm, det kan gjøres på avstand og uten samtykke. Det er allerede omfattende bruk i Kina, og mange steder er det nå umulig å ferdes anonymt.
- Personvernforordningen GDPR regulerer bruken i Norge, men forbyr den ikke. For eksempel har svensk politi fått grønt lys for å ta teknologien i bruk.
- Lokale myndigheter, teknologiutviklere og andre etterlyser nå et forbud.

Ulike typer ansiktsgjenkjenning

Ansiktsgjenkjenning kan brukes på flere måter. Ved verifisering og identifisering brukes ansiktet som biometrisk informasjon.

Verifisering: Er du den du sier?

Ved verifisering sammenliknes to bilder for å avgjøre om bildene er av samme person, for eksempel for å låse opp smarttelefonen.

Identifisering: Hvem er du?

Et bilde sammenliknes med en forhåndsdefinert liste av bilder for å se etter treff. Dette kan brukes både med fotografier og video fra overvåkningskameraer. Et eksempel er når politiet sammenlikner et bilde av en person mot en liste over ettersøkte personer.

I tillegg kan teknologien brukes til ansiktsanalyse. Dette innebærer at algoritmen kategoriserer personer basert på deres utseende. Dette brukes for å lage persontilpasset reklame, men også av kinesiske myndigheter for etnisk kategorisering av uighur-befolkningen. Det finnes også eksempler på at det kan brukes innen medisin, til å diagnostisere depresjon, eller måle hjerterytme på avstand.

Allerede stor spredning

Ansiktet er noe man har med seg hele tiden, og ansiktsgjenkjenning kan gi mindre risiko for identitetstyveri, eller at informasjon kommer på avveie. Fordi man ikke trenger å huske passord eller koder, blir slike løsninger også praktiske for brukerne.

I 2017 lanserte Apple iPhone X som inneholdt Face ID. Dette ga for første gang brukerne mulighet til å låse opp telefonen med ansiktet. I 2024 tror man ansiktsgjenkjenning kommer til å brukes på 90 prosent av alle smarttelefoner.

Betaling med ansiktet

I Spania har CaxiaBank installert minibanker hvor PIN-koden er byttet ut med identifisering via ansiktsgjenkjenning.

Kina satser stort på digitalisering innen bank og finans og er i en ledende posisjon globalt. Kinesiske forbrukere kan allerede betale på butikken bare ved å vise ansiktet foran kameraet på kasseapparatet. Nettgiganten Alibabas betalingsplattform Alipay leder utviklingen, og subsidierer butikker og forbrukere som tar utstyret i bruk. I Oslo tester TINE og DNB ut en liknende betalingsløsning.

Sikkerhet og overvåkning

Både private og offentlige aktører bruker ansiktsgjenkjenning i sikkerhetsarbeid. Det kan være selskaper som er ansvarlige for sikkerhet på store arenaer, kjøpesentre, eller politi og sikkerhetstjenester.

En internasjonal kartlegging viser at aktører i rundt 65 land bruker ansiktsgjenkjenning til overvåking. På tyske togstasjoner testes nå ansiktsgjenkjenning som sikkerhetstiltak og som et verktøy for å gi støtte til politiet. I januar 2020 kunngjorde også politiet i London at de skulle ta i bruk ansiktsgjenkjenning på ulike offentlige steder i byen.

Teknologien har spredd seg raskt til en rekke land. På grunn av kinesiske myndigheters store satsing på kunstig intelligens og gode tilgang til ansikter, er flere kinesiske selskaper ledende i teknologiutviklingen. Myndigheter i 52 land bruker kinesisk teknologi for ansiktsgjenkjenning.

Under OL i Tokyo vil ansiktsgjenkjenning bli tatt i bruk for å lose utøvere, støtteapparat og media raskt og effektivt gjennom ulike kontrollposter. Det planlegges også bruk av ansiktsanalyse for å oppdage unormal oppførsel. Heathrow lufthavn tester nå om bruk av ansiktsgjenkjenning istedenfor kontrollposter kan bidra til redusert tidsbruk for de reisende og bedre flyt av passasjerer gjennom avgangshallen.

Stadig mer tilgjengelig

Etter hvert som teknologien blir billigere og mer tilgjengelig, vil man trolig også se nye typer tjenester. Appen Clearview gjør det mulig å ta et bilde av en person, og deretter søke etter treff i selskapets database som består av over tre milliarder bilder. Bildene er hentet fra åpne kilder på nett, inkludert Facebook og Youtube.

Dette innebærer at man med stor sannsynlighet kan identifisere en tilfeldig person på gata. I følge selskapet er Clearview nå tatt i bruk av flere hundre politidistrikter i USA, og flere private sikkerhetsselskaper.

Masseovervåkning

De samme egenskapene som gjør at ansiktsgjenkjenning kan gi effektive og brukervennlige løsninger, skaper også rom for at ansiktsgjenkjenning kan brukes til masseovervåkning. At teknologien kan brukes i sanntid, på avstand og uten samtykke gjør det vanskelig å oppdage. I tillegg er kapasiteten så stor at man kan analysere millioner av ansikter på svært kort tid.

Ansiktsgjenkjenning har derfor potensial til å bli et verktøy for totalitære regimer, der innbyggerne er under konstant overvåkning uten at de legger merke til når eller hvordan det skjer.

Både i Ungarn og i India har myndighetene foreslått å sette opp omfattende systemer for overvåkning ved hjelp av ansiktsgjenkjenning, for å kunne identifisere kriminelle. I Ungarn skal systemet brukes til alt fra trafikkforseelser til nasjonal sikkerhet.

Kina dominerer

Kinesiske myndigheter har som mål å bli verdensledende innen kunstig intelligens, og har derfor tatt i bruk teknologien på mange områder.

Teknologien brukes for eksempel til å identifisere og henge ut fotgjengere som går på rødt lys, og i politiets smarte briller for å identifisere mistenkte i kriminalsaker. Innbyggere som vil tegne abonnement på internettjenester eller få nytt mobilnummer må identifisere seg via ansiktsgjenkjenning.

Xinjiang regionen, nordvest i Kina, har blitt brukt til å teste ut mange ulike former for overvåkning. Ansiktsgjenkjenning har blant annet blitt brukt for å overvåke og kontrollere uighur-befolkningen. Systemet ser spesielt etter uighurene basert på deres utseende, og registrerer hvor de beveger seg.

I Hong Kong har politiet hatt tilgang til teknologi for ansiktsgjenkjenning i flere år, men myndighetene har unngått å svare på om de bruker teknologien til å kartlegge demonstranter under protestene som startet i 2019. Demonstrantene ser ut til å ta for gitt at de blir overvåket, og bruker både ansiktsmasker og paraplyer for å hindre at ansiktene deres filmes. Det har også være tilfeller hvor demonstranter har revet ned og demontert smarte lyktestolper som de mistenker brukes til ansiktsgjenkjenning.

Risiko for forskjellsbehandling

Selv om maskinlæring og algoritmene for ansiktsgjenkjenning har blitt mye bedre de siste årene, er det fortsatt flere utfordringer knyttet til bruken.

Omgivelsene varierer

En utfordring er om teknologien faktisk fungerer slik den skal. Selv om treffsikkerheten til algoritmene er god, er det stor forskjell på om bildene som brukes er tatt i kontrollerte omgivelser (som for eksempel på en politistasjon), eller er fra et utendørs overvåkningskamera.

Et forsøk med bruk av ansiktsgjenkjenning under Champions League finalen i South Wales i 2017, viste for eksempel at da dagslyset forsvant, klarte ikke lenger kameraet å finne ansikter i videostrømmen. I 92 prosent av tilfellene hvor algoritmen indikerte treff blant publikum, målt mot en liste over kriminelle, viste det seg å være feil. Dette viser at selv små forstyrrelser i bildestrømmen kan bidra til at treffsikkerheten synker betraktelig.

Forskjellsbehandling

En annen utfordring kommer av kvaliteten på treningsdataene. Algoritmene analyserer mange bilder for å lære seg hva et ansikt er. I 2016 lagde Microsoft en database med bilder av kjendiser, som har blitt svært mye brukt, både av forskere, private selskaper og myndigheter. Flertallet av bildene var av hvite menn. Dette gjør at treffsikkerheten er lavere når algoritmen analysere bilder av mennesker med annen hudfarge, kvinner eller eldre.

Dette kan føre til falske positive, hvor algoritmen indikerer treff når dette ikke er riktig, eller falske negative, hvor algoritmen ikke klarer å se at to bilder faktisk er den samme personen.

Fordi treffsikkerheten varierer avhengig av en persons utseende, kan det føre til forskjellsbehandling: Mennesker med minoritetsbakgrunn vil kunne oppleve at de oftere enn andre blir stoppet i kontroller fordi de blir flagget av systemet, eller at algoritmene ikke klarer å bekrefte at de er den de sier de er.

I 2018 testet menneskerettighetsorganisasjonen ACLU Amazons system for ansiktsgjenkjenning, og fikk en rekke falske positive treff. For eksempel ga bilder av 28 amerikanske kongressmedlemmer treff i en database med bilder av kriminelle. De fleste av disse kongressmedlemmene var mørkhudete.

Regulering av ansiktsgjenkjenning

Ansiktsgjenkjenning kan være svært inngripende i privatlivet. Selv om det kan være nyttig og effektivt i enkelte sammenhenger, kan bruken få store samfunnsmessige konsekvenser i andre. For personvern anonymitet og demonstranter kan skadevirkningene bli langt mer alvorlige enn det problemet man forsøker å løse.

Særlig muligheten for å overvåke og identifisere mennesker uten involvering eller samtykke er problematisk. Det bryter med grunnleggende rettigheter, krenker personvernet, og kan føre til en nedkjølingseffekt hvor mennesker endrer adferd av frykt for å bli overvåket.

I Norge er det ikke kjent at myndighetene så langt har tatt i bruk ansiktsgjenkjenning til å overvåke og identifisere personer i offentligheten.

GDPR og nasjonalt handlingsrom

Biometriske kjennetegn, som når ansiktet brukes til identifisering, er kategorisert som sensitive personopplysninger under personvernforordningen GDPR. Det innebærer at det er strengt regulert hvordan slike opplysninger kan brukes.

En svensk skole ble i 2019 ilagt bot for å ha brukt ansiktsgjenkjenning til å registrere oppmøte blant elevene. Skolen hadde innhentet samtykke fra elevene det gjaldt, men Datainspektionen slo fast at dette ikke var gyldig, da elevene står i et avhengighetsforhold til skolen.

Samtidig åpner GDPR for at myndigheter kan ta i bruk ansiktsgjenkjenning, hvis de kan vise til berettiget interesse av å bruke teknologien til å løse sine oppgaver. I oktober 2019 godkjente for eksempel Datainspektionen i Sverige at politiet kunne ta bruk ansiktsgjenkjenning for å identifisere mistenkte. Dette gjør at politiet kan sammenligne bilder med signalementsregisteret, som inneholder over 50 000 bilder.

Personvernforordningen krever at det skal gjennomføres en vurdering av personvernkonsekvenser, som skal sikre at personvernet til de berørte ivaretas. Dette inkluderer en vurdering av konsekvensene for grunnleggende rettigheter, som detåbevegesegfrittutenåværereddforåbliovervåket.

Forslag om forbud

I flere land har både myndigheter og organisasjoner tatt til orde for forbud mot bruk av ansiktsgjenkjenning. Ønsket er at dette gir rom for å gjøre en grundig vurdering av konsekvensene av teknologien, og få på plass tiltak for risikovurdering.

San Fransisco har vedtatt et forbud mot bruk av teknologi for ansiktsgjenkjenning. Forbudet begrunnes med frykten for misbruk av teknologien, og at selv minimal bruk kan bidra til å dytte USA i retning av en overvåkningsstat. I etterkant har flere andre byer fulgt etter med liknende regulering.

I EU-kommisjonens «White Paper on Artificial Intelligence» fra februar 2020 trekkes ansiktsgjenkjenning på avstand frem som en anvendelse av kunstig intelligens med høy risiko. Kommisjonen vil sette i gang en bred europeisk debatt om det finnes omstendigheter der teknologien kan tas i bruk. I prinsippet er det opp til nasjonale myndigheter å autorisere bruk eller ikke.

Også private selskaper støtter midlertidige forbud, slik at man får gjort en grundig vurdering av konsekvensene av teknologien. Alphabet-sjefen Sundar Pichai har gått ut og støttet et midlertidig forbud. Han har uttalt at Google ikke tilbyr tjenester med ansiktsgjenkjenning fordi farene for misbruk er så store.

Motstanderne av slike forbud mener det vanskeliggjør politiets arbeid med å sikre innbyggerne, og at teknologiutvikling og innovasjon hindres. Trump-administrasjonen ønsker at myndighetene skal regulere kunstig intelligens så lite som mulig, og heller fremme innovasjon og økonomisk vekst.

Forfattere: Tore Tennøe, Adele Flakke Johannessen og Marianne Barland
Publisert: Februar 2020, oppdatert mars 2020
Kontakt: post@teknologiradet.no / www.teknologiradet.no

Teknologirådet gir råd til Stortinget og regjeringen om ny teknologi
Dokumentet med kilder finnes på www.teknologiradet.no