Security Eksamen

Martin, Frederiksen
cph-mf237@cphbusiness.dk
A klassen

Andreas, Vikke
cph-av105@cphbusiness.dk
A klassen

Forord

Denne rapport er udarbejdet af Martin Frederiksen og Andreas Vikke. Vi har som gruppe arbejdet hvad der er tilsvarende 50% hver på rapporten.

Indhold

1. Projektbeskrivelse

Vi vil i denne opgave undersøge cases inden for ansigtsgenkendelse og databehandling af brugerdata inden for større firmaer såsom Zoom. Vi vil også tage et kig på etikken bag tracking af personer og diverse data.

Case 1: Er det muligt med vores erfaring som datamatikerstuderende, at udvikle et stykke software der kan genkende et ansigt og i så fald, hvilken data får vi ud af det?

Case 2: Hvordan behandler større firmaer som fx Zoom og Microsoft persondata og hvad er etisk korrekt i forhold til ansigtsgenkendelse?

2. Persondataforordningen

GDPR, Databeskyttelsesforordningen og Persondataforordningen er det samme. GDPR står for General Data Protection Regulation, og er en lovgivning, som er indført af EU. Databeskyttelse blev særlig relevant d. 25. maj 2018, da alle virksomheder fra denne dato skulle efterleve GDPR-reglerne.[1]

Kort fortalt sikrer Persondataforordningen det fysiske menneskes rettighed til at bibeholde personoplysninger. En personoplysning er en oplysning, der kan henføres til en bestemt person. Fx. er din bils nummerplade en personoplysning, da denne oplysning kan henføres til dig som ejer af bilen. Det er naturligvis ikke muligt for dig som bilejer at få slettet din nummerplade fra nummerpladeregistret, men tværtimod har du ret til at denne oplysning fx ikke bliver delt på sociale medier eller andre uhensigtsmæssige steder. Persondataforordningen stammer faktisk helt tilbage fra d. 24 oktober 1995 og har udviklet sig med tiden.[2] Når vi snakker persondataforordning anno 2020, er det sidste nye skrig at nogle virksomheder og organisationer, nemlig dem hvis kerneaktivitet involverer regelmæssig og systematisk overvågning af personlige eller personfølsomme data, skal udpege en databeskyttelsesansvarlig, for at sikre at denne virksomhed eller organisation overholder persondataforordningen. Derudover er det helt essentielle for os som fysisk menneske rettigheden til at blive glemt. Det vil altså sige, at du har ret til som menneske, at få alt den persondata en hvilken som helst virksomhed har på dig slettet. Nedenfor kan de væsentligste regler inden for persondataforordningen læses:

Menneskets ret til oplysning: Skal medvirke til at give kontrollen tilbage til det fysiske mennesket. Mennesket har ret til at få oplyst, hvilken data en virksomhed har på dem. Endvidere skal denne data være læsbar og forståelig for det normale menneske.

Menneskets ret til sletning: Mennesket skal kunne få slettet den persondata en virksomhed har opsamlet om dem og virksomheden skal kunne dokumentere denne sletning.

Dataportabilitet: Mennesket skal kunne få sin persondata tilbage, så dette menneske fx kan videregive sin persondata til en anden virksomhed. Igen skal virksomheden kunne håndtere og dokumentere dette.

Vurdering af personlige konsekvenser: Alle processer en virksomhed har til håndtering af persondata, skal tage udgangspunkt i en risikovurdering i forhold til de her persondata. Altså hvor kritiske er de her persondata for det enkelte menneske og hvad er konsekvensen ved at de bliver lækket eller brugt til noget, som ikke var hensigten.

Privacy by design: Virksomheder skal have fokus på, at sikkerhed skal være indbygget i ethvert IT system som et grunddesign-parameter.

Privacy by default: Virksomheder skal have fokus på at IT-systemets sikkerhed, altid skal være slået til, så det ikke er noget virksomheden først slå til, når der er brug for sikkerheden. Sikkerhed er altså ikke noget man slår til, når der er behov for det!

Skærpede dokumentationskrav: Paradigmet bliver ændret fra at datatilsynet "muligvis" kan komme forbi til egenkontrol. Det betyder at virksomheder selv skal dokumentere de processer, de har, og at man rent faktisk også lever op til dem. Det er bl.a. det der også sker i fødevaresektoren hos restauranterne.

[1] https://gdpr.dk/

[2] https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Databeskyttelsesansvarlig: En virksomhed skal udnævne en databeskyttelsesansvarlig, som bl.a. har ansvaret for at virksomhedens egenkontrolsprocesser kører og skal være det primære bindeled mellem virksomheden og datatilsynet.

Transparens: Virksomheder har pligt til at oplyse om, hvad de gør med personoplysningerne.

Samtykke: Når en virksomhed behandler menneskets persondata, så skal alt der gøres med de her persondata, være i overensstemmelse med den præcise opgave, som virksomheden udfører for det pågældende menneske. Ellers skal der være givet et eksplicit samtykke til at virksomheden må gøre det med persondataen, som de rent faktisk gør. Det vil sige en virksomhed ikke må sammenkøre persondata på nye og spændende måder, bare fordi det er sjovt.

Indberetning og underretning: Hvis en virksomhed har en utilsigtet hændelse som fx tab af persondata skal det indberettes til datatilsynet senest 72 timer efter tabet og i nogle tilfælde, skal virksomheden også kunne underrette de berørte mennesker.

Sanktioner: Det er muligt for datatilsynet at udstede sanktioner til en virksomhed, der ikke overholder de gældende regler i persondataforordningen. Sanktioner i form af bødestraf kan løbe op i 4% af den årlige globale omsætning, hvis denne er større end 20.000.000€. Mindsteprisen for en sanktion i form af bødestraf er altså 20.000.000€. Det er dog også muligt at udstede en sanktion, i form at virksomheden får frakendt retten til at behandle persondata.

3. Ansigtsgenkendelse

"Ansigtsgenkendelse er en biometrisk metode til at identificere en bestemt person ud fra et billede."[3]

Biometri: Er en metode til at identificere en person ud fra specifikke kendetegn, såsom fingeraftryk, farven på regnbuehinden(iris), gangart og ansigtstræk. Biometriske teknologier bliver brugt til at måle og analysere karakteristika knyttet til menneskers fysiologi eller adfærd med henblik på at be- eller afkræfte en persons identitet.

Kunstig intelligens: Er videnskaben bag og ingeniørkunsten i at lave intelligente maskiner særligt intelligente computerprogrammer. Kunstig intelligens handler stort set altid om, at få computere og robotter til at gøre ting, som det hidtil kun har været mennesker, der har kunnet fx at spille skak, køre bil, føre en samtale, sammenligne fingeraftryk eller genkende et ansigt.

Autentifikation: Har traditionelt været enten noget man ved, fx din PIN-kode til dit dankort, eller noget du har fx kørekort, pas eller husnøgle.

Med biometri og kunstig intelligens opnås nye muligheder for autentifikation i form af, at man kan bruge noget, man er frem for noget, man enten ved eller har. For et par år tilbage var det fx på mode at implementere en fingeraftrykksscanner i smartphones, så brugeren ikke skulle indtaste en kode for at låse telefonen op, men derimod bare sætte fingeren på en knap eller på skærmen. Det samme gælder den nye generation af smartphones, hvor der så i stedet for en finger scanner er implementeret en mulighed for, at kameraet læser dit ansigt. Der har dog været en ret stor sikkerhedsrisiko ved udelukkende at bruge biometri som en "stand alone" sikkerhed. Nedenfor ses nogle af de sikkerhedsbrud, der har været i forbindelse med brug af biometri:

- I 2018 viste en test at 42 ud af 110 smartphones med aktiveret ansigtsgenkendelse, kunne låses op med et fotografi.[4]
- I 2017 blev Samsungs-irisscanner snydt af et foto og en kontaktlinse.[5]
- I 2013 blev Apples Touch ID omgået.[6]
- I 2004 viste en svensk ingeniør, at man med lidt snilde kan kopiere fingeraftryk og anvende disse falske fingeraftryk til at omgå sikkerhedssystemer.[7]

Selvfølgelig afhænger biometrisk sikkerhed af udstyrets kvalitet, men bør stadig kombineres med en anden sikkerhedsteknologi, når der ønskes høj sikkerhed, altså en to-faktor autentifikation. I begge tilfælde har producenterne nok tænkt mere på brugervenlighed frem for sikkerhed idet begge løsninger til en nemmere håndtering af skærmlåsen, har skabt komplikationer. Ansigtsgenkendelse og den kunstige intelligens bag bliver brugt til mere end bare sikkerhed i form af at låse din smartphone op. For eksempel bruger Facebook samme kunstige intelligens, der bruges i ansigtsgenkendelse til at "tagge" venner på deres hjemmeside, samt

[3] https://www.dr.dk/nyheder/penge/analyse-derfor-vil-eu-bremse-ansigtsgenkendelse
[4] https://www.version2.dk/artikel/se-oversigt-alle-disse-mobiler-kan-laases-med-foto-1087193
[5] https://www.computerworld.dk/art/240084/hackere-snyder-samsungs-sikre-irisskanner-med-et-foto-og-en-kontaktlinse
[6] https://arstechnica.com/information-technology/2013/09/touchid-hack-was-no-challenge-at-all-hacker-tells-ars/
[7] https://ing.dk/artikel/ingenior-kopierer-fingeraftryk-59310

i Københavns lufthavn bruges ansigtsgenkendelse til at verificere at du faktisk er den person, som der stå i dit pas.

Problemet med biometrisk sikkerhed, som vi ser det, er at det skal beskyttes utrolig godt. Vi har tidligere set store virksomheder miste persondata til hackere og det kan virkelig forårsage stor skade, hvis en hacker først får fat i din biometriske data. Det er data der ikke kan ændres igen, det vil sige, hvis en hacker først har dit ansigts data, kan hackeren udgive sig for at være dig på alle platforme, der bruger ansigtsgenkendelse som autentifikation. Vi vil nu prøve at skabe en forståelse for den data, der kan trækkes ud fra et ansigt, hvilket vi har gjort ved hjælp af Python og en række biblioteker.

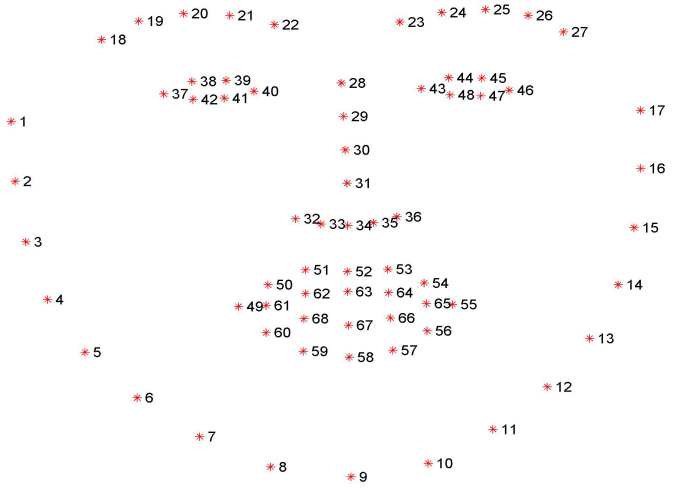
4. Ansigtsgenkendelse af studerende

Ansigtsgenkendelse kan lyde kompliceret på papiret, da der er mange ting der spiller ind. Men dykker man lidt ned og undersøger mulighederne, finder man hurtigt ud af, hvor mange "hjælpemidler" der findes. Mange firmaer der arbejder med kunstig intelligens, har nemlig lavet deres kode Open-Source, det vil sige at alt deres kode er public domain[8], så alle kan se og ændre i det.

Alle disse værktøjer gør at studerende nemt kan kode en ansigtsgenkender, som kan genkende personer på billeder eller video med meget høj nøjagtighed. Nedenfor ses et før- og efter-billede af to personer. Efter-billedet er resultatet af et simpelt program kodet på under 24 timer, hvor programmet både har genkendt personen og de optegnede ansigtstræk. Ansigtstrækkene er tegnet ud fra 68 punkter, som kaldes Facial Landmarks[9]. Disse punkter kan findes i alle ansigter og er med til at lokalisere og genkende ansigter på billeder.

Før- og efter-billede af Python script.

[8] https://creativecommons.org/share-your-work/public-domain/
[9] https://ibug.doc.ic.ac.uk/resources/300-W/



68. punkter i ansigtet.[10]

For at genkende et ansigt skal man først finde ansigtet ved hjælp af facial landmarks (se Figur 1). Programmet deler billedet op i mange små billeder, og ved hjælp af Deep Learning algoritmer[11] tjekker den, om de 68 punkter findes. Når der er fundet 68 punkter, kan selve genkendelsen finde sted ved hjælp af euklidisk afstand. Den euklidiske afstand er afstanden mellem to vektorer, som bruges til at matche to ansigtskodninger sammen (se Figur 2). Hvis distancen mellem to ansigtskodninger er indenfor tolerancen, standard 0.62, vil det betragtes som et match.[12]

[10]https://ibug.doc.ic.ac.uk/resources/300-W/
[11]https://www.datarobot.com/wiki/deep-learning/
[12]https://github.com/AndreasVikke/Facial-Recognition

```
'nose_bridge': [(545, 213), (545, 218), (545, 223), (545, 229)],
'nose_tip': [(529, 234), (534, 237), (539, 240), (544, 240), (547, 240)],
'right_eye': [(550, 219),
               (556, 221),
               (561, 223),
               (564, 226),
               (559, 225),
               (555, 223)],
```

Figur 1: Ansigtspunkter.

```
[-0.07571969 -0.01482243  0.04072434 -0.07702571 -0.18992785 -0.07810821
  0.07211791 -0.07879627  0.14458777 -0.07502627  0.20455274  0.00614579
 -0.25058562 -0.03185616  0.0191267   0.19200386 -0.07738723 -0.13590331
 -0.12517467 -0.04317361  0.08709161  0.02029088  0.00993162  0.15822816
 -0.09600716 -0.25545046 -0.06339568 -0.04970373 -0.10884313 -0.12245505
  0.00405512  0.16290073 -0.14114827 -0.05444335  0.07447183  0.05099896
 -0.13654102 -0.15968004  0.20759891 -0.03467317 -0.22628573  0.02542224
  0.09435484  0.16173097  0.22155693 -0.0499648   0.07323941 -0.0955795
  0.0894782  -0.29374641  0.07062758  0.14518088  0.08350948  0.06589392
  0.06774857 -0.16748236 -0.00785704  0.20955095 -0.29153451  0.05840774
  0.01710818 -0.17166784 -0.05158452 -0.10639998  0.16365197  0.15452382
 -0.16492303 -0.19075358  0.18780595 -0.19769034 -0.10371162  0.11241926
 -0.17530845 -0.27369416 -0.26411304  0.08506982  0.37726825  0.18424147
 -0.15874089  0.02793286 -0.08407538 -0.01819003 -0.05568617  0.13862896
  0.04896482 -0.12596039 -0.07707953  0.01810009  0.13109718 -0.01377862
 -0.05957094  0.31198588  0.05644756 -0.08948621  0.000687    0.07456229
 -0.07415488  0.00186294 -0.09018561 -0.02254114 -0.07600871 -0.08051776
  0.0099376   0.11664031 -0.12227118  0.12844318 -0.11560763 -0.00906333
 -0.08135984 -0.05450715 -0.10017477 -0.06716743  0.04412059 -0.30609012
  0.15971594  0.13829669  0.06547064  0.15098496 -0.02021937  0.11512014
  0.08081611 -0.09319629 -0.15930581 -0.01014403  0.12687998  0.03421677
  0.03468684  0.06290488]
```

Figur 2: Ansigtskodninger.

I ansigtsmodellen vi har brugt her, er der 68 punkter, men virksomheder såsom Apple bruger større modeller med flere punkter. De skaber nemlig en 3D-rendering af ansigtet ud fra et 2D-billede og finder punkter, som egentlig ikke findes på billedet. Alle disse punkter gemmes på telefonen og er ikke tilgængelige for brugere, men hvis en hacker fik fat i dem, ville det principielt være muligt at "Brute force" sig ind på iPhones ved at sende et array med de rigtige punkter, som telefonen er sat op med i stedet for at åbne kameraet og scanne.

Hvis studerende har adgang til disse værktøjer og kan udvikle programmer, der kan identificere ansigter og personer på billeder, er der rig mulighed for at firmaer med penge kan udvikle langt vildere og mere komplicerede ting. Private firmaer kan for eksempel have overvågning på deres grund, for at holde uvelkomne gæster ude og her kan ansigtsgenkendelse kobles på, for at gøre det nemmere men i nogle tilfælde også mere præcist.

5. Persondata og ansigtsgenkendelse hos større virksomheder

Der er mange store virksomheder der gør brug af ansigtsgenkendelse. Det bliver brugt til en bred vifte af ting og det kan skabe problemer i forhold til persondataforordningen.

Zoom som bliver brugt til online kommunikation, har gennem de sidste par år arbejdet med tanken om ansigtsgenkendelse. Ideen er at Zoom skal kunne genkende, hvem der er i opkaldene såsom navn, hvilket firma personen er ansat hos og personens profession. Information såsom, hvem der har været i opkaldet, er også smart til efterfølgende analyse. Dette scenarie er dog svært, da persondataforordningen har en masse restriktioner på, hvordan persondata skal gemmes. Spørgsmålet er om ansigtsindkodninger på en person for eksempel kan stjæles og hvordan man skal gemme data'en, for at det er sikkerhedsmæssigt forsvarligt. Zoom har allerede været under luppen, da det i 2020 kom ud, at de havde sendt brugerfølsomme data til Facebook uden brugerens tilladelse,[13] og at de har lækket flere tusinder af e-mailadresser til firmaer.[14]

Eric S. Yuan, som er grundlægger af Zoom, har også planner om at indføre ansigtsudtryks-genkender. Dette ville gøre det nemmere for ordstyreren i opkaldet at se om han for eksempel snakker for hurtigt, eller emnet han snakker om, er tungt for lytterne.[15]

Der er også andre firmaer såsom gigant firmaet Microsoft, der igennem flere år har eksperimenteret med ansigtsgenkendelse, og har i den forbindelse samlet et datasæt af ansigter, de kalder MS-Celeb.[16] Ideen bag MS-Celeb er at have et datasæt til at køre benchmark-opgaver på til at genkende en million berømtheder. Det er en smart ide, og det er der mange firmaer der bed fast i, såsom IBM, Panasonic og Sensetime.

Microsoft valgte at fjerne MS-Celeb fra deres servere[17] i 2019, i frygt om at det skulle misbruges til overvågning af befolkningen, som Kina bl.a. er et eksempel på, men også grundet GDPR-lovgivning om opbevaring af persondata, såsom billede, navn og profession. MS-Celeb havde al denne information på en million berømtheder uden deres samtykke, og derfor valgte de at slette dataen. I sammenhæng med at Microsoft slettede MS-Celeb, var Duke University og Standford University også ude og slette deres datasæt, Duke MTMC med to millioner ansigter og Brainwash med 12.000 ansigter.

Firmaet Sensetime, som er leverandør af softwareteknologisk udstyr til det kinesiske styre, brugte MS-Celeb til deres udvikling. Kina bruger ansigtsgenkendelse på gaderne ved hjælp af overvågningskameraer og tracker opførelse på borgere. Ved vejkrydsene kigger overvågningskameraerne på dem, der går over for rødt og det kobles sammen med andre sociale systemer, som f.eks. det at kunne låne penge i banken eller få et job.

[13] https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/
[14] https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos
[15] https://vmblog.com/archive/2017/12/04/zoom-video-communications-2018-predictions-ai-ar-facial-recognition-and-other-trends.aspx
[16] https://www.microsoft.com/en-us/research/wp-content/uploads/2016/08/MSCeleb-1M-a.pdf
[17] https://www.berlingske.dk/virksomheder/microsoft-sletter-kaempe-database-til-ansigtsgenkendelse

6. Etisk forsvarlighed

Under dette afsnit skal vi have grundlæggende rettigheder og friheder i henhold til respekt for privatliv, samt bevægelses- og ytringsfrihed i mente.

Har du nogensinde undret dig over, hvordan fx en reklame på en hjemmeside kan vise det produkt du for nylig har søgt på, imens du sad og surfede? Eller hvordan det er muligt at du kan stå i stuen foran dit smart tv og fortælle din samlever om et par adidas sko, du har tænkt på at købe, hvorefter du tænder computeren for at se på sko og den første reklame du ser er selvsamme adidas sko, du havde talt med din samlever om? Så har du måske været udsat for at virksomheder opsamler data om din væremåde og interesser på internettet. Reklamer er gemen markedsføring for virksomheder og en elementær salgsstrategi. Promovering af produkter kan give et øget salg af de promoverede produkter, hvilket vi selvfølgelig er klar over. Det skal dog siges at før i tiden var reklamer på internettet ikke nødvendigvis noget, der var skræddersyet til dine behov, men nærmere en ting der bare prøvede at ramme en så stor målgruppe som muligt, lidt ligesom de reklamer vi finder i postkassen. Nogle virksomheder har så taget skridtet videre og vha. teknologien, har de kunne indsamle data om deres brugere, så de kan promovere mere nøjagtigt. Der er nok ikke mange kvinder, der vil blive fanget af en annonce fra jem&fix med en billig boremaskine, hvorimod at annoncen nok vil interessere mange mænd. Forestil dig en gå tur gennem strøget hvor alle bannere, reklameskilte og annoncer var rettet specifikt imod dig. Ville det være i strid med privatlivets fred?

For at se på et andet eksempel har vi i Danmark faktisk over 1.5 mio. overvågningskameraer sat op. Det skal dog siges at 1 mio. af dem er opsat i virksomheder, 250.000 af dem er privatejet, altså opsat i personernes hjem, og 300.000 af dem er opsat i offentligheden fx metroerne, togstationer, lufthavne osv. Mange af disse overvågningskamera benytter sig ikke af ansigtsgenkendelsessoftware, men der er alligevel steder, hvor man er begyndt at integrere ansigtsgenkendelse som en del af sikkerheden. Nedenfor ses eksempler herpå.

- Brøndby IF anvender automatisk ansigtsgenkendelse ved indgangen til Brøndby Stadion. Meningen er at genkende en person der er pålagt karantæne fra Stadion og systemet skal så hjælpe kontrollørerne med at sætte ansigt på disse personer, så de kan nægtes adgang til Stadion.
- I Københavns lufthavn bruges ansigtsgenkendelse til at verificere at passagererne rent faktisk er dem, de udgiver sig for at være via deres pas.
- Dansk politi vil gerne fremadrettet bruge ansigtsgenkendelse til efterforskning ved terrorscenarier som fx Omar Hussein-sagen. Politiet mener at i dette tilfælde ville de have haft mulighed for at gribe ind meget tidligere, hvis de havde den fornødne teknologi.

Fordelen ved overvågning er den øgede sikkerhed, det kan give, men det er let at forestille sig, hvor vores samfund kan ende, hvis ansigtsgenkendelses-trenden får lov til at løbe løbsk. Lufthavne over hele verden arbejder faktisk på at gøre ansigtsgenkendelse til en del af check in- og sikkerhedssystemerne. I Helsinki Lufthavn er målet ifølge lufthavnsoperatøren, Finnavi, at have et ansigtsgenkendelsessystem på plads i 2021. Landets grænse- og toldmyndigheder er også interesseret i muligheden. Er vi på vej mod et overvågningssamfund som i Kina?

Det er måske lidt overdrevet at sammenligne Danmark med Kina, da vi i et meget lille omfang gør brug af ansigtsgenkendelse i forhold til Kina. Hvis vi tager et kig på Kinas brug af ansigtsgenkendelse, er det helt

surrealistisk, hvor vi kan ende. Kina har et social kredit system, som er et pointsystem, der bruges til at troværdighedsvurdere personer i samfundet. Det vil sige, hvis en person har en høj social kreditvurdering, får personen nogle frynsegoder som fx at leje en bil eller et hotelværelse uden at betale depositum. Hvis en person derimod har en lav social kreditvurdering, kan personen ikke gennemføre en booking af en flybillet eller anden offentlig transport, det bliver svært at få et job, tage et lån og nogle skoler vil ikke tage imod børn, hvis forældre har en lav social kreditvurdering. Måden hvorpå scoren bliver beregnet, er ud fra din adfærd i samfundet fx, hvis en person går over for rødt i et fodgængerfelt bliver der trukket lidt point fra deres samlede kreditvurdering. Kina sporer ikke kun deres befolknings adfærd, men også deres handlevaner. Det har faktisk en indflydelse på din samlede score, hvad du kommer i indkøbskurven, når du er ude at handle. Før det sociale kreditsystem blev opfundet, var der i tilfældet med personen, der gik over for rødt, en stander der viste, hvem der har "brudt" loven med et billede af personen for at "skamme" de mennesker, der havde gjort noget forkert. Det er efterfølgende blevet en del af nyhederne, så hele befolkningen får lov til at se, hvem der har gjort noget, de ikke burde.

Ansigtsgenkendelse i Kina bliver dog ikke kun brugt til at "skamme" men bliver faktisk anvendt positivt rigtig mange steder. På restauranter får du fx en anbefaling af mad, for at restauranten nemt kan ekspedere dig, altså restauranten ved faktisk hvad du plejer at bestille. Det er også muligt at betale i forretninger med dit ansigt vha. deres "smil for at betale"-teknologi. Deres ansigtsgenkendelse er så godt trænet, at den kan se det er dig, selvom du har en paryk på, eller har rigtig meget makeup på. Ansigtsgenkendelsen sætter endda også en stopper for spild af toiletpapir på offentlige toiletter, hvor du er nødt til at scanne dit ansigt for at få toiletpapir, hvilket du kun kan gøre hvert 9. minut. Hos nogle virksomheder findes brugen af ansigtsgenkendelse også til at åbne hoveddøren for ansatte eller en person, der har en aftale med virksomheden. Dette medfører så også at virksomheden ved præcist, hvad tid deres ansatte ankommer til arbejdspladsen og hvad tid de ansatte går igen. Regeringsbygningen har i stedet for dørmænd, ansigtsgenkendelse til at se, hvem der kommer og går fra bygningen. På den måde kan de se, hvor ofte ansatte kommer og går fra bygningen samt, hvor ofte registrerede og uregistrerede gæster kommer og går. De har altså et samlet billede af regeringsbygningerne og dem, der gør brug af dem. Hvor surrealistisk det her end lyder kommer der faktisk også noget godt ud af brugen af ansigtsgenkendelse fx Skynet. Skynet stammer fra terminator-filmen og er blevet udviklet som noget godt i forhold til terminator, hvor Skynet er indbegrebet af masseødelæggelse. Alt der sker i det offentlige rum, bliver overvåget og med ansigtsgenkendelse er det muligt at vide, hvad der sker hvert sekund i selv de mindste hjørner i det offentlige rum. Skynet opfanger fx alle ansigter på en metrostation i "real time" og krydstjekker ansigterne med en kriminel database, for at fange kriminelle. Der bliver herefter sendt en advarsel til politiet om, hvor den kriminelle befinder sig. Der er blevet anholdt mere end 3000 kriminelle i hele nationen på bare det første år, Skynet blev brugt. Vil du have noget imod at blive overvåget hver gang du forlader din bopæl? Går grænsen når regeringen vil ind i dit hjem med et kamera? Hvordan ville et liv uden et privatliv være?

7. Konklusion

Vores undersøgelser har virkelig givet stof til eftertanke. Det er enormt vigtigt at vi kan beskytte vores biometriske data, så de ikke kan misbruges. Beskyttelsen af persondata er naturligvis lige så vigtig, men vi ser bare en større mulighed for identitetstyveri ved tab af biometrisk data. Med den fortsat hurtige udvikling af kunstig intelligens, vil vi kunne se større og større spring mod en mere teknologisk hverdag, og det er derfor vigtig at lovgivningen følger med i lige så store spring. Det er også vigtig at lytte til befolkningen og deres bekymringer, så der kan blive sat restriktioner på teknologien, uden at krænke sikkerheden for befolkningen.