04-12-2020

Predictive policing i dansk politi

DEN RETLIGE REGULERING AF PREDICTIVE POLICING MED INDDRAGELSE AF MENNESKERETLIGE PERSPEKTIVER

LINDA CLARA JUUL BEYER

VEJLEDER: LENE WACHER LENTZ | Antal anslag: 128.144

Titelblad

Dansk titel
Predictive policing i dansk politi – Den retlige regulering af predictive policing med inddragelse af menneskeretlige perspektiver

Engelsk titel
Predictive policing in the Danish police – The legal regulation of predictive policing with the inclusion of human rights perspectives

Projekt
Kandidatspeciale ved Aalborg Universitet

Projektets fagområde
Politiret og menneskeret

Afleveringsdato
4. december 2020

Omfang
67 sider

Vejleder
Lene Wacher Lentz

Udarbejdet af
Linda Clara Juul Beyer
Studienummer – 2019-2712

Abstract

This thesis is about what the legal regulation is for predictive policing in Denmark. This involves answering three questions, including whether predictive policing is used in Denmark, what its legal regulation is, and whether a consideration has been made on the relevant human rights aspects. With regard to human rights, the focus will be on articles 8 and 14 of the European Convention on Human Rights, on the right to privacy, family life, home and correspondence, and on the right not to be subject to discrimination.

This will be sought to be answered by first reviewing the concepts "smart policing", "intelligence-led policing" and "predictive policing", followed by the Danish regulation of predictive policing. Subsequently, Article 8 of the European Convention on Human Rights will be reviewed and compared with the use of predictive policing, and here the judgments of Klass and others vs. Germany and Szabó and Vissy vs. Hungary will be included. Finally, Article 14 of the Convention will be reviewed and compared with the use of predictive policing.

The thesis concludes that it is not clear whether predictive policing is practiced in Denmark, as nothing has been reported about this, and that the legal basis for predictive policing is broad. In addition, it is concluded that due to the risk of bias, prejudice, over-policing and in light of the EMD's considerations and experience from other countries where predictive policing is exercised, it is necessary to ensure the human rights if the police have the authority to exercise predictive policing, which the Danish police have had since 2017. The thesis also concludes that no consideration has been made in Denmark on the human rights aspects which appear from the said judgments and from Article 14.

Indholdsfortegnelse

1. Indledning og problemformulering

I takt med den generelle samfundsudvikling sker der også en udvikling i kriminalitetsbilledet. For offentlige myndigheder, herunder politiet, byder nutidens samfund derfor på udfordringer af mere kompleks karakter, end hvad tidligere har været tilfældet. Dette kan være et resultat af personlig udvikling hos borgere generelt, og dermed også de, der deltager i kriminelle aktiviteter, eller et resultat af flere og bredere tekniske muligheder, eller noget helt andet. Uanset hvad der ligger til grund for den stadigt mere komplekse kriminalitet, er politiet nødt til at udvikle sig i takt hermed, og skabe de retlige rammer, der er nødvendige for at kunne bekæmpe den kriminalitet, der finder sted, og varetage de opgaver, der er pålagt politiet, jf. lov nr. 444 af 9. juni 2004 om politiets virksomhed, jf. lovbekendtgørelse nr. 1270 af 29. november 2019 (herefter: politiloven) § 2. Kravet om denne udvikling af de retlige rammer for politiet er ikke uden komplikationer, idet der er tale om områder, hvor det på grund af begrænsede praktiske erfaringer, kan være svært at forudsige de reelle udfald af lovgivning og kompetenceindhold. Samtidig kan der være udfordringer i forbindelse med at fastslå indholdet af de retlige rammer, idet de skal tilpasses den stadigt stigende kompleksitet.

Et af de mest fremtrædende eksempler på kompleks kriminalitet i udvikling, er terrorisme, som politimyndigheder verden over har udfordringer med at forebygge og bekæmpe. I Danmark besluttede regeringen, efter terrorhændelserne i København i februar 2015, at forbedre politiets IT-baserede virksomhed med henblik på at give politiet bedre muligheder for at forebygge og reagere på sådanne uforudsete hændelser. Dette resulterede i, at der i 2017 blev indført en ny bestemmelse i politiloven, § 2 a, som fremadrettet gav politiet hjemmel til at foretage tværgående informationsanalyser, der kan lægges til grund for politivirksomheden. Til at foretage disse dataanalyser blev IT-systemet Pol-Intel indkøbt og implementeret. På denne måde moderniseredes og effektiviseredes politivirksomheden, og politiet har nu bedre muligheder for at varetage deres opgaver.

I udlandet, herunder Storbritannien og USA, er lignende kompetencer set hos politiet, hvor politiet har anvendt en algoritme til at forudse kriminalitet. Dette er populært kaldet predictive policing. Denne måde at udøve politivirksomhed har ubestridt medført en effektivisering hos politimyndighederne, men har også været genstand for en del debat,

herunder i forhold menneskerettighederne, blandt andet fordi der kan være udfordringer forbundet med hvilke omstændigheder, politiet medtager personoplysninger om borgere i dataanalyserne, samt graden af overvågning, som borgere udsættes for, og risikoen for over-policing. Den menneskeretlige debat kommer af forhold, hvor politiet har anvendt en algoritme til forebyggende politivirksomhed, og dette har resulteret i potentielle eller konkrete krænkelser af grundlæggende rettigheder, herunder retten til privat- og familieliv, hjem og korrespondance efter artikel 8 i Den Europæiske Menneskerettighedskonvention (herefter: EMRK) og retten til ikke at blive diskrimineret efter EMRK artikel 14. Herefter opstår spørgsmålet, om politilovens § 2 a giver hjemmel til predictive policing, samt hvorvidt der er taget stilling til de menneskeretlige aspekter, som erfaringer fra udlandet lægger op til.

Dette leder til følgende problemformulering, som denne fremstilling vil søge at besvare:

Hvordan er den danske regulering af predictive policing?

Denne fremstilling vil undersøge den danske regulering af predictive policing med inddragelse af menneskeretlige perspektiver med særligt fokus på EMRK artikel 8 og 14 om henholdsvis retten til privatliv, og til ikke at blive diskrimineret. Herudover vil det søges belyst, hvilke risici, der er for borgerne i forbindelse med predictive policing.

Problemformuleringen vil søges besvaret ved at tage stilling til (1) om predictive policing anvendes i Danmark, (2) hvad den retlige regulering er, og (3) om man har taget stilling til det menneskeretlige aspekt.

Fremgangsmåden vil være som følger. Afsnit 4 indeholder en beskrivelse af politiets metode og strategi, herunder begreberne ”smart policing” i afsnit 4.1, ”intelligence-led policing” i afsnit 4.2. og ”predictive policing” i afsnit 4.3. Herefter vil der være en undersøgelse af politilovens § 2 a i afsnit 5, herunder bestemmelsens indhold og ordlyd i afsnit 5.1., implementeringen af bestemmelsen med inddragelse af det bagvedliggende lovforslag i afsnit 5.2., efterfulgt af en beskrivelse af politiets IT-system, Pol-Intel, og leverandøren heraf i afsnit 5.3. Afsnit 5.5. vil indeholde overvejelser omkring anvendelsen af predictive policing set i lyset af den danske lovgivning og erfaringer fra udlandet. Der vil i afsnit 5.6. være en sammenfatning, hvor der samles op på det i afsnit 4 og 5 fastslåede.

Herefter vil det menneskeretlige perspektiv inddrages i afsnit 6. Det drejer sig om EMRK’s artikel 8 om retten til respekt for privat- og familie og hjem og korrespondance i afsnit 6.1,

hvortil de fire beskyttelsesinteresser vil blive gennemgået i afsnit 6.1.1., og offentlige myndigheders behandling af oplysninger i 6.1.2. I hhv. afsnit 6.1.3. og 6.1.4. vil to afgørelser fra EMD Klass m.fl. mod Tyskland og Szabó og Vissy mod Ungarn blive gennemgået for at belyse artikel 8 i forhold til politiets hemmelige overvågning. Afsnit 6.2. vil indeholde overvejelser omkring predictive policing og hemmelig overvågning set i lyset af artikel 8 og de to afgørelser. Afsnit 6.3. omhandler retten til ikke at blive diskrimineret efter artikel 14, og afsnit 6.4. indeholder overvejelser omkring predictive policing i forhold til artikel 14 med inddragelse af erfaringer fra Storbritannien. Herefter vil der være en konklusion i afsnit 8, som besvarer problemformuleringen og de underliggende spørgsmål.

2. Afgrænsning

For at målrette indholdet af denne fremstilling til hvad der er væsentligt for at besvare problemformuleringen, er det nødvendigt at foretage en afgrænsning. Denne fremstilling vil have fokus på borgerens oplevelse af metoden predictive policing og politilovens § 2 a, stk. 1 og 2. Politilovens § 2 a, stk. 3, indeholder en hjemmel for justitsministeriet til at udstede bekendtgørelser med nærmere regler for politiets virksomhed efter bestemmelsens stk. 1 og 2, herunder om sletning og tekniske og organisatoriske foranstaltninger. Politilovens § 2 a, stk. 3, vil ikke være relevant at inddrage som led i besvarelsen af problemformuleringen, og vil derfor ikke blive behandlet yderligere.

I forbindelse med implementeringen af politilovens § 2 a, blev der indført en ændring af toldloven vedrørende oplysninger om flypassagerer. Dette vil ikke blive behandlet i denne fremstilling.

Implementeringen af det nye IT-system i politiet, som hedder Pol-Intel, og de muligheder, som denne nye form for digital politivirksomhed og tværgående analysearbejde giver, vil også indgå som en del af denne fremstilling. Dette skal ses i lyset af, at Pol-Intel giver politiet nye muligheder, som skal have hjemmel i loven.

Endelig er det relevant at inddrage artikel 8 og 14 i EMRK. Artikel 8 omhandler retten til respekt for privatliv, familie, hjem og korrespondance. Artikel 14 indeholder et forbud mod diskrimination. De to bestemmelser vil blive behandlet og inddraget i fremstilling i det omfang, det er relevant for at besvare problemformuleringen. Både artikel 8 og 14 indeholder mange interessante aspekter, og omfanget af begge bestemmelser er stort. Det er dog ikke alle områderne inden for bestemmelsernes omfang, der er relevante for besvarelsen af problemformuleringen i denne fremstilling, som derfor ikke vil behandle bestemmelsernes fulde område. Der afgrænses i denne forbindelse fra reglernes indhold om familiesammenføring, adoption, børn uden for ægteskab mv.

Endvidere afgrænses fra de øvrige bestemmelser i EMRK, da der i denne fremstilling udelukkende vil blive taget stilling til artikel 8 og 14 i forbindelse med predictive policing.

EMRK indeholder tillige et generelt forbud mod diskrimination i konventionens 12. tillægsprotokol, som adskiller sig fra diskriminationsforbuddet i artikel 14 ved ikke at være afhængig af, at forholdet relaterer sig til en af konventionens materielle bestemmelser. Danmark har ikke ratificeret denne tillægsprotokol, og den vil derfor ikke blive behandlet i denne fremstilling.

For så vidt angår politiets behandling af personoplysninger, findes der regler for politiet inden for persondataretten. Dette vil ikke indgå i denne fremstilling. Det samme gør sig gældende for politiets arbejde med automatisk nummerpladegenkendelse (ANPG), samt POLCAM, reglerne i retsplejeloven og politiets tv-overvågning.

Overordnet set vil denne afhandling dermed have fokus på borgernes oplevelse af predictive policing, politilovens § 2 a, stk. 1 og 2, Pol-Intel, og EMRK artikel 8 og 14 i det omfang, det er relevant for besvarelsen af problemformuleringen.

3. Metodeafsnit

3.1. Metodevalg

Denne fremstilling vil søge at besvare problemformuleringen ved anvendelse af den retsdogmatiske metode. Denne metode har til formål at fastslå, hvad der er gældende ret. Med metoden tilstræbes det at beskrive og analysere en retstilstand ved at foretage en juridisk vurdering på baggrund af lovtekster og andre relevante kilder, principper og begreber beskrevet i litteraturen[1].

Det vil i denne fremstilling søges belyst, hvordan retstilstanden er vedrørende anvendelse predictive policing i det danske politi, særligt set i lyset af retten til privatliv, familieliv, hjem og korrespondance i Den Europæiske Menneskerettighedskonvention (EMRK) og retten til ikke at blive diskrimineret efter konventionens artikel 14.

3.2. Retskilder

For at besvare problemformuleringen, er det nødvendigt at inddrage de relevante retskilder. Ved retskilder forstås national og international, som er gældende i Danmark, herunder lovbestemmelser og retspraksis, men også sædvane og forholdets natur, som dog vil spille en beskeden rolle i denne fremstilling[2].

For så vidt angår lovbestemmelser, vil denne fremstilling inddrage politilovens § 2 a. Denne bestemmelse er en senere tilføjelse til politiloven, og den blev indført i 2017 med LOV nr. 671 af 08/06/2017 "Lov om ændring af lov om politiets virksomhed og toldloven". Det er i kraft af denne bestemmelse, at politiet har hjemmel til at foretage tværgående informationsanalyser. Dette vil blive gennemgået i afsnit 5. For at opnå en grundlæggende forståelse for politilovens § 2 a, er det nødvendigt at inddrage bemærkningerne til lovforslaget, hvormed bestemmelsen blev vedtaget. Lovforslaget hedder L171 af 29. marts 2017 "Forslag til Lov om ændring af lov om politiets virksomhed og toldloven (Politiets

[1] Carsten Munk-Hansen: "*Retsvidenskabsteori*", 2014, s. 64
[2] Carsten Munk-Hansen: "*Retsvidenskabsteori*", 2014, s. 192

anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer)", men vil i denne fremstilling blive omtalt som L171.

Udover politiloven vil også EMRK blive inddraget. EMRK sikrer alle borgere i de stater, der har ratificeret konventionen, en række grundlæggende rettigheder. EMRK blev oprettet af Europarådet i 1950, ratificeret i Danmark i 1953 og inkorporeret i den danske lovgivning den 29. april 1992. Dermed er EMRK en del af dansk ret, og de danske domstole har pligt til at håndhæve EMRK i Danmark og sørge for, at de danske borgeres rettigheder efter denne konvention ikke krænkes[3].

Det menneskeretlige aspekt i denne fremstilling finder hjemmel i EMRK artikel 8 og 14. Disse bestemmelser vil blive inddraget i det omfang, det er relevant for besvarelse af problemformuleringen. Det er derfor blot de dele af bestemmelsernes indhold, der er relevante i forhold til predictive policing, som vil blive inddraget i denne fremstilling.

Ved retspraksis forstås afgørelser, der er afsagt ved domstolene. Dette omfatter i denne sammenhæng både afgørelser fra de danske domstole og fra Den Europæiske Menneskerettighedsdomstol (herefter omtalt EMD). EMD blev oprettet i 1959 for at sikre, at de ratificerede stater overholder reglerne i EMRK. Borgere i Danmark kan, hvis de er af den overbevisning, at deres menneskerettigheder efter EMRK er blevet krænket, klage til, eller lægge sag an ved, de nationale myndigheder, eller lægge sag an ved EMD med direkte henvisning til EMRK[4]. De afgørelser, der kommer fra EMD, bidrager, ifølge forhenværende dommer ved EMD Jon Fridrik Kjølbro, i høj grad til at fastslå, hvad indholdet af staternes forpligtelser efter EMRK er, og praksis vil, næsten uden undtagelser, skulle anvendes, når der opstår menneskeretlige spørgsmål. Dette har dommerne ved EMD for øje i afgørelsesvirksomheden, og det er derfor ikke kun hensigten med EMD's afgørelser at dømme i den konkrete sag, men også at fremkomme med en afgørelse, der kan anvendes mere generelt. EMD har helt konkret "*til formål at belyse, sikre og videreudvikle konventionens rettigheder og friheder*"[5]. EMD's afgørelser skal dermed medvirke til at præcisere og udfolde EMRK's bestemmelser.

[3] Carsten Munk-Hansen: "*Retsvidenskabsteori*", 2014, s. 267
[4] Ibid.
[5] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 15

Afgørelser, der er afsagt af EMD, vil blive inddraget i det omfang, de er relevante og kan belyse fremstillingens problemformulering. Da EMD's afgørelser i høj grad udformer indholdet af bestemmelserne i EMRK, vil det som oftest være afgørelser, som ligger til grund for, hvad der kan fastslås om bestemmelserne. EMD har så vidt ses ikke taget stilling til predictive policing, men fremstillingen vil inddrage to af EMD's afgørelser, hvori emnet i nogen grad behandles i forhold til politiets hemmelige overvågning af borgerne. Afgørelserne kan bruges som pejlemærker i forhold til predictive policing. Nærmere konkret vil dommene Klass m.fl. mod Tyskland (afgørelse nr. 5029/71 af 6. september 1978) og Szabó og Vissy mod Ungarn (afgørelse nr. 31138/14 af 12. januar 2016) blive inddraget i henholdsvis afsnit 6.1.3. og 6.1.4. De to afgørelser belyser indholdet af EMRK artikel 8 og 13 om retten til effektive retsmidler. Da denne fremstilling har fokus på artikel 8 og 14, vil artikel 13 kun i begrænset omfang blive inddraget.

3.3. Juridisk litteratur

Til brug for denne fremstilling og med henblik på at sætte problemstillingen i perspektiv, anvendes juridisk litteratur. Forfatterne bag den litteratur, som vil blive inddraget, er fagfolk, som via eksempelvis erfaring eller forskning har tilegnet sig viden omkring det område, som fremstillingen omhandler.

Til at beskrive begreberne "smart policing", "intelligence-led policing" og "predictive policing", inddrages kapitlet "Forskydninger mellem det private og det offentlige i smart politiarbejde" fra bogen "Ret SMART". Kapitlet er skrevet af Mette Volquartzen. Hertil inddrages også rapporten "Policing by Machine" fra borgerrettighedsgruppen Liberty. Rapporten er skrevet af Hannah Couchman. Til at beskrive politilovens § 2 a anvendes bogen "Politiloven med kommentarer" skrevet af Ib Henricson. Til belysning af indholdet af artikel 8 og 14 i EMRK anvendes "Den Europæiske Menneskerettighedskonvention: for praktikere" af Jon Fridrik Kjølbro.

4. Politiets metode og strategi

Politiets virksomhed er i dag, ifølge Volquartzen, genstand for et paradigmeskifte, og det nye politiparadigmes omdrejningspunkt er strategien "*smart policing*", som blandt andet går ud på, at politiet i stigende grad skal anvende data og IT som led i deres virksomhed[6]. Dette kan begrundes med, at kriminaliteten med tiden er blevet mere kompleks, og politiet har derfor et behov for at prioritere deres ressourcer for at udføre deres arbejde - der må i højere grad arbejdes med fokus på strategi og målrettethed[7].

I lyset af samfundsudviklingen må politiet i stigende grad anvende data og IT i politiarbejdet for at kunne følge med kriminalitetens kompleksitet. Dette kom især til udtryk, da politiet i 2017 implementerede det nye IT-system Pol-Intel. Pol-Intel er en digital platform, der er beregnet til at foretage dataanalyser ved at sammenkøre data fra forskellige systemer og registre. Som led i politivirksomheden er det hensigten, at politiet skal bruge Pol-Intel til at forebygge kriminalitet ved at forudsige forbrydelser ved hjælp af mønstre i kriminaliteten i bestemte områder. Dette går under betegnelsen *predictive policing*[8]. Implementeringen og anvendelsen af Pol-Intel vil blive gennemgået nærmere i afsnit 5.3. om politiets analyseplatform.

Smart policing og intelligence-led policing er to begreber, som læner sig op ad hinanden. Der findes ikke en klar linje mellem begreberne, men de er begge udtryk for politiets måde at udøve deres virksomhed på, og det nye politiparadigme. Følgende er en gennemgang af smart policing-strategien, efterfulgt af intelligence-led policing, samt metoden predictive policing.

4.1. Smart policing

Begrebet smart policing er defineret flere gange, herunder i 2012 af daværende Rigspolitichef Jens Henrik Højbjerg, der beskrev det som "*alle former for ledelse, der i sidste*

[6] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171
[7] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 174
[8] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171

ende ville føre til bedre brug af de tilgængelige ressourcer i arbejdet med operationelle resultater"[9].

I Indien i 2015 blev smart policing defineret som "*et forsøg på at udnytte de risici, der er forbundet med politiarbejde i smart cities. Risici som øget organiseret kriminalitet i byrummet og det globaliserede netværk blandt terrorister*", og det blev ledsaget med følgende fem principper for politivirksomheden inden for smart policing:

S: Strict and sensitive

M: Modern and mobile

A: Alert and accountable

R: Reliable and responsive

T: Techno-savvy and trained[10]

Set i lyset af disse definitioner kan smart policing beskrives som en overordnet strategi for politivirksomheden, der har fokus på ledelse, ressourcer, samt disponering og prioritering af ressourcer ved hjælp af øget og effektiviseret brug af data og IT. Volquartzen beskriver forbindelsen mellem begreberne "predictive policing" og "smart policing" således, at smart policing er den overordnede strategi, som finder anvendelse i det nye politiparadigme, og predictive policing som én metode blandt mange, der er omfattet af paraplybetegnelsen "smart policing"[11].

Volquartzen peger på flere ting, som er karakteristiske for smart policing og skiftet fra det gamle politiparadigme til det nye. For det første har politiet i mange år været overvejende reaktivt, men bliver nu i stigende grad proaktivt[12]. Politiets arbejde kommer dermed til at handle om at forebygge kriminalitet, hvor tendensen før var at reagere på kriminalitet og afværge den[13]. For det andet nævnes det, at politiet går fra at være synoptisk til at være panoptisk. Et synoptisk politi er det, vi kender fra de seneste mange år, som er synligt for alle, eksempelvis i forbindelse med patruljering. Omvendt er det panoptiske politi ikke synligt, men har en skjult og overvågende rolle, hvilket kan ses i sammenhæng med

[9] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 173
[10] Ibid.
[11] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171
[12] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 176
[13] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 174

overvågning som led i predictive policing[14]. Volquartzen fremhæver, at det panoptiske politi ikke er nyt i vores samfund, men tværtimod kan findes i det oprindelige politi fra før år 1863, hvor der skete det omvendte skifte fra et panoptisk til et synoptisk politi. I denne forbindelse sætter Volquartzen spørgsmålstegn ved, om politiet ved implementeringen af metoder som predictive policing er ved at vende tilbage til den panoptiske funktion, som politiet havde før 1863. Dette afviser Volquartzen dog på baggrund af, at vi i dag lever i en retsstat med andre muligheder for at foretage teknologisk overvågning, samt at præmisserne for, og formålet med, overvågningen har ændret sig siden 1863[15].

Volquartzen nævner, at kritikken kan lyde på, at mediernes rolle i dagens samfund medvirker til, at det ikke kun er politiet, der overvåger borgerne, men også borgerne, der overvåger politiet via sociale medier, TV og journalistik. Derfor stiller Volquartzen spørgsmålet, om vi er ved at overgå til et rent panoptisk politi i teoretisk forstand, eller om politiet i lige så høj grad er synligt for borgerne[16].

Smart policing indeholder dermed elementer fra politiets tidligere virksomhed fra før 1863, men det moderne samfund og den teknologiske udvikling sætter rammerne anderledes, og forhindrer dermed, at politiet vender tilbage til den oprindelige, overvågende virksomhed. Derudover medfører dette nye politiparadigme og smart policing en stigende grad af anvendelse af teknologiske hjælpemidler for en effektiviseret og moderniseret politivirksomhed.

4.2. Intelligence-led policing

Et andet begreb, der beskriver det nye paradigme i politiet, er "*intelligence-led policing*". Denne form for politivirksomhed bygger på to bærende elementer. For det første skal politiet som organisation være vidensbaseret. Dette er selve målet for strategien. For det andet skal politiets arbejde have fokus på den forebyggende indsats og risikostyring, frem for bekæmpelse af kriminalitet efter at forholdet er begået[17]. Intelligence-led policing kommer især til udtryk ved anvendelsen af de tværgående informationsanalyser, som kan foretages

[14] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 176
[15] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 177
[16] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 178
[17] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 174

med hjemmel i politilovens § 2 a. Predictive policing, som politivirksomhed efter § 2 a populært betegnes, er dermed en metode, der, ligesom ved smart policing, kan anvendes inden for intelligence-led policing-strategien[18].

I bemærkningerne til lovforslaget vedrørende politilovens § 2 a, L171 omtales strategien, der ligger til grund for implementeringen af § 2 a, generelt som "*intelligence-led policing*", hvilket også kan ses i lyset af, at intelligence-led policing er den mest udbredte policing strategi i den vestlige verden i dag[19]. Strategien nævnes i bemærkningerne til lovforslaget allerede indledningsvis i forbindelse med, at politiets behov for modernisering og effektivisering skal ske ved implementeringen af intelligence-led policing. Med dette menes både implementering og udvidelse af den analysebaserede indsats til flere områder, herunder eksempelvis patruljering[20].

I forhold til implementering af intelligence-led policing bemærkes det, at erfaringer fra "*Politianalyse vedrørende monitering og analyse*" fra 2013 har vist, at intelligence-led policing i udenlandsk politi har haft positive mærkbare effekter. Hvis strategiens fulde potentiale skal realiseres, er det ifølge disse undersøgelser dog essentielt, at politiet kan medtage så mange oplysninger i analysearbejdet som overhovedet muligt[21]. For at opnå både øget og bedre dataanvendelse har man, i forbindelse med vedtagelsen af politilovens § 2 a, indkøbt og implementeret et digitalt værktøj, kaldet Pol-Intel, som kan udføre det tværgående analysearbejde. Pol-Intel vil blive nærmere beskrevet i afsnit 5.3. om politiets analyseværktøj.

Denne forbedring af dataanvendelse har, ifølge bemærkningerne til L171, til formål at give politiet bedre forudsætninger for hurtigere genkendelse af mønstre på tværs af forskellige sager om alvorlig organiseret kriminalitet, og på baggrund af dette koncentrere og målrette efterforskningen med henblik på forebyggelse. Derudover forventes det, at tiltaget vil give politiet forbedrede muligheder for at bekæmpe økonomisk IT-kriminalitet, eksempelvis ved at muliggøre at Pol-Intel kan organisere og genkende mønstre og sammenhænge mellem

[18] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 180
[19] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 174
[20] Lovforslag nr. 171 af 29. marts 2017, s. 3
[21] Lovforslag nr. 171 af 29. marts 2017, s. 5

anmeldelser fra flere forskellige politikredse i forbindelse med phishing og lignende kriminalitet.

Phishing er et af mange eksempler på kriminalitet, der beror på tekniske midler, hvor der sendes e-mails eller sms'er med et link ud til en større mængde mennesker med det formål at få dem til at indtaste personoplysninger, kontooplysninger, adgangskoder mv. Særligt problematisk ved phishing er, ifølge bemærkningerne til L171, at gerningspersonen ofte befinder sig i udlandet på gerningstidspunktet, og modtagerne er flere personer, som bor i forskellige politikredse. Det er derfor nødvendigt at kunne lave en effektiv tværgående analyse og sammenkøre data fra forskellige politikredse for at kunne efterforske angrebene samlet[22].

Den vidensbaserede politivirksomhed, der kommer til udtryk i politilovens § 2 a og implementeringen af Pol-Intel, er dermed en del af intelligence-led policing-strategien, som, ifølge bemærkningerne til L171, anvendes i Danmark. Inden for intelligence-led policing findes mange muligheder, og man må forvente en vis grad af udvikling i politiets IT-baserede virksomhed over de næste mange år. Derudover medfører intelligence-led policing, at politivirksomheden i højere grad bliver vidensbaseret, og at dette vil afspejle sig i beredskabs- og patruljeringsvirksomheden, men også i efterforskningen, og de mere komplicerede sager om eksempelvis phishing. En af metoderne, der anvendes inden for strategien intelligence-led policing, er som tidligere nævnt predictive policing. Denne metode har vakt meget interesse og debat blandt forskere og i medierne, både i Danmark og i udlandet. Metoden "*predictive policing*" vil blive gennemgået nedenfor.

4.3. Predictive policing

Der findes ikke en klar definition af, hvad predictive policing er. Metoden handler først og fremmest om at analysere og genkende fortidens kriminalitetsmønstre og dermed forudsige, hvor der er sandsynlighed for, at der vil forekomme kriminalitet i fremtiden, og hvem der vil deltage i fremtidige kriminelle aktiviteter[23]. Analyserne såvel som genkendelser og udpegelser skal gøres ved hjælp af en algoritme i et IT-system. Dette skal ses i sammenhæng

[22] Lovforslag nr. 171 af 29. marts 2017, s.5
[23] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 180

med strategien intelligence-led policing og formålet hermed, som blandt andet er, at politivirksomheden skal have fokus på det forebyggende arbejde.

Der er, ifølge Mette Volquartzen, endnu ingen erfaringer med predictive policing i det danske politi. Det er dog ikke et nyt koncept i udlandet, herunder USA, som Volquartzen inddrager til illustration. Det amerikanske politi opsætter eksempelvis sensorer i udvalgte bandeområder, som kan alarmere politiet ved lyden af skud. Derudover anvendes digitale analyser til at udpege potentielle kriminelle personer eller farezoner, som politiet skal være ekstra opmærksomme på. Dette er kaldes henholdsvis *hot persons* og *hot spots*. I Chicago, USA, har man tillige udviklet en algoritme, som kan skabe en Strategic Subject List (*heat list*), som indeholder navne på dem, der ud fra algoritmen er potentielle gerningsmænd og ofre. De personer, der fremgår af en heat list, vil i forbindelse hermed blive informeret af politiet om, at de bliver overvåget[24]. Predictive policing kan dermed relatere sig til personer eller til steder.

Anvendelsen af predictive policing har dog ikke været uden komplikationer, og Volquartzen beskriver nogle forskellige opmærksomhedspunkter, som har været genstand for kritik eller udfordringer i forbindelse med anvendelsen af predictive policing i Chicago. Dette drejer sig blandt andet om neutraliteten hos politiets algoritmer. Non-profit organisationen ProPublica udgav en omfattende undersøgelse i 2016, som har vist, at der ikke foreligger tilstrækkelig grad af neutralitet og viden til, at politiet kan lægge analyserne til grund for deres virksomhed, idet der var tendens til både falske negativer og falske positiver. Eksempelvis kunne Anders Breivik, som stod bag angrebet på Utøya i 2011, falde uden for algoritmen på grund af sin hudfarve, tro og mål, som afveg fra algoritmens profil på en terrorist[25].

Samtidig er der risiko for, at uskyldige vil blive overvåget. Volquartzen inddrager et eksempel, hvor en hjemløs med større sandsynlighed vil blive overvåget end en pædofil, hvis den pædofile har et arbejde. Der er dermed en reel risiko for, at der vil ske overvågning og anholdelse af uskyldige borgere, og omvendt at algoritmen overser de, der i virkeligheden udøver kriminalitet, hvilket strider imod princippet om lighed for loven[26]. I forbindelse hermed nævner Volquartzen også problematikken i forhold til borgerrettigheder og retten til

[24] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 181
[25] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 182 f.
[26] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 183

privatliv, samt at overvågningen oftest vil ramme de sårbare og i forvejen stigmatiserede grupper af borgere[27].

Der er ifølge Volquartzen dog generelt optimisme blandt forskere omkring anvendelsen af predictive policing, men metoden har også været genstand for kritik, som blandt andet handler om, hvorvidt overvågningen af borgerne er blevet for vidtgående[28].

[27] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 184 f.
[28] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171 f.

5. Politilovens § 2 a

Politilovens § 2 a danner de retlige rammer for politiets virksomhed i forbindelse med tværgående informationsanalyser og sammenkørsel af data i større mængder. Nedenfor vil bestemmelsens indhold og ordlyd, samt baggrunden for implementeringen blive gennemgået nærmere.

5.1. Bestemmelsens indhold og ordlyd

> *Stk. 1: Politiet foretager tværgående informationsanalyser på grundlag af de oplysninger, politiet behandler, når det er nødvendigt af hensyn til udførelsen af politiets opgaver, jf. § 2.*
>
> *Stk. 2: Politiet kan indsamle og behandle oplysninger fra offentligt tilgængelige kilder, når det er nødvendigt af hensyn til udførelsen af politiets opgaver, jf. § 2*
>
> *Stk. 3: Justitsministeren fastsætter nærmere regler for politiets behandling af oplysninger, herunder den, der finder sted i medfør af stk. 1 og 2. Justitsministeren fastsætter herunder regler om, til hvilke formål oplysninger kan behandles, og hvornår sletning af oplysninger skal finde sted, og om de tekniske og organisatoriske foranstaltninger, der skal iagttages ved behandlingen.*

Således lyder politilovens § 2 a om politiets adgang til at foretage tværgående informationsanalyser, jf. stk. 1, og til at indsamle og behandle oplysninger fra offentligt tilgængelige kilder, jf. stk. 2. Bestemmelsen giver, som noget nyt, politiet hjemmel til at behandle en langt større mængde data i tværgående dataanalyser, når "*det er nødvendigt af hensyn til politiets opgaver*", jf. stk. 1 og 2.

Deler man bestemmelsen op, drejer stk. 1 sig om adgangen til at foretage tværgående informationsanalyser af data, som politiet i forvejen kan tilgå og behandle. Dette drejer sig om data fra politiets egne registre, herunder Det Centrale Kriminalregister og DNA-registret, eller andre registre, som politiet har adgang til. Dette omfatter blandt andet Det Centrale Personregister (populært kaldet CPR-registret), Europols register og fingeraftryksregistret (EURODAC)[29].

[29] Ib Henricson: *"Politiloven med Kommentarer"*, 2020, s. 39

Efter bestemmelsens stk. 2 kan politiet indsamle og behandle oplysninger fra offentligt tilgængelige kilder, også kaldet *open source*. Dette omfatter oplysninger, som politiet indhenter fra Tinglysningsregistret, Sundhedsplatformen eller opslag lagt op på sociale medier, herunder Facebook eller Instagram[30]. Kilderne anvendes i forbindelse med eksempelvis savnede personer og afvikling af store begivenheder, herunder fodboldkampe og koncerter[31].

Af både stk. 1 og 2 fremgår det, at det er et krav, at indsamlingen og/eller behandlingen af oplysningerne skal være "*nødvendigt af hensyn til udførelsen af politiets opgaver*". Ved "*politiets opgaver*" forstås de opgaver, der er oplistet i politilovens § 2, og behandling af oplysninger efter § 2 a kan dermed ske i forbindelse med opgaver både inden for og uden for strafferetsplejen, herunder også ordensopgaver. Vurderingen af, om den enkelte tværgående analyse er "*nødvendig*", må derfor foretages på grundlag af de i politilovens § 2 oplistede opgaver, som tilfalder politiet. Det er, ifølge Ib Henricson, tilstrækkeligt for at kunne foretage en tværgående analyse efter § 2 a, at denne metode i det konkrete tilfælde må vurderes at være den mest effektive, uanset om der er tale om opgavevaretagelse inden for eller uden for strafferetsplejen[32].

Politiloven giver dermed hjemmel for politiet til at sammenkøre og anvende data fra flere forskellige registre og open source-kilder. Behovet herfor er et resultat af samfundsudviklingen, og det har, på grund af udviklingen i kriminalitetsbilledet, været nødvendigt at implementere klar hjemmel for denne form for politivirksomhed. Nedenfor vil implementeringen af politilovens § 2 a, baggrunden for vedtagelsen og formålet blive beskrevet nærmere.

5.2. Implementering af politilovens § 2 a

Efter terrorhændelserne i København i februar 2015 blev det i evalueringsrapporten fra hændelserne anbefalet, at politiet i Danmark skulle modernisere og effektivisere deres metoder, for fremover at være bedre rustet til at håndtere uforudsete hændelser som denne[33].

[30] Ib Henricson: *"Politiloven med Kommentarer"*, 2020, s. 39 f.
[31] Lovforslag nr. 171 af 29. marts 2017, s. 6
[32] Ib Henricson: *"Politiloven med Kommentarer"*, 2020, s. 40
[33] Lovforslag nr. 171 af 29. marts 2017, s. 3

Efterfølgende udarbejdede den daværende regering et udspil med navnet "Et stærkt værn mod terror", som indeholdt 12 nye tiltag mod terror. Det indebar blandt andet, at der i 2015-2018 skulle bruges 200 millioner kroner til "*udbygning af politiets og PET's beredskabs- og overvågningsindsats*" og 150 millioner kroner til "*forbedring af IT- og analysekapacitet*"[34]. Det blev desuden i "Et stærkt værn mod terror" slået fast, at der skulle anskaffes et nyt IT-system, som kunne lave tværgående analyser ved anvendelse af overvågningskameraer og sociale medier for at identificere potentielle gerningsmænd forud for terrorangreb eller meget alvorlige forbrydelser[35].

For at dette skulle blive en realitet, fremsatte man i 2017 lovforslaget L171 af 29. marts 2017 "Forslag til Lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer)". L171 blev vedtaget den 1. juni 2017 og politilovens § 2 a blev indført.

5.2.1. Bestemmelsens formål

"Et stærkt værn mod terror" og behovet for modernisering og effektivisering af politiet i Danmark nævnes indledningsvist i bemærkningerne til L171, hvor det bliver fastslået, at dette skal ske ved hjælp af intelligence-led policing, og at denne indsats skal anvendes på forskellige områder i politivirksomheden, eksempelvis patruljering. Lovforslaget har til formål at skaffe politiet "*tidssvarende redskaber*" og klare retlige rammer til anvendelsen af redskaberne. Politiet har dermed de optimale muligheder for at imødegå det komplekse kriminalitetsbillede i det moderne samfund, og i øvrigt at sikre effektiv løsning af politiets opgaver inden for og uden for strafferetsplejen. Helt konkret er formålet med indførelsen af politilovens § 2 a at sikre en klar retlig regulering af anvendelsen af intelligence-led policing[36].

Med denne bestemmelse skal politiet kunne basere deres virksomhed på tværgående analyser af større mængder data, med henblik på genkendelse og identificering af kriminalitetsmønstre - både i forhold til den borgernære politivirksomhed og uvarslede hændelser (terrorhændelser)[37]. Det skal hertil bemærkes, at det af bemærkningerne til L171

[34] Regeringens udspil "*Et stærkt værn mod terror*", februar 2015, s. 2
[35] Regeringens udspil "*Et stærkt værn mod terror*", februar 2015, s. 5
[36] Lovforslag nr. 171 af 29. marts 2017, s. 3
[37] Ibid.

fremgår, at analyseværktøjet ikke skal anvendes til den rent administrative politivirksomhed, herunder eksempelvis våbentilladelser og aktindsigt[38]. Anvendelse af tværgående analyseværktøjer til at løse politiopgaver er, ifølge Justitsministeriet, hensigtsmæssigt og karakteristisk for et moderne politi[39].

For så vidt angår den borgernære politivirksomhed, giver § 2 a politiet mulighed for at disponere over ressourcer, herunder patruljer og færdselskontrol, på baggrund af tværgående informationsanalyser, som kan indikere, hvor der er større sandsynlighed for bestemte typer af lovovertrædelser[40]. Det bemærkes dog i tilknytning hertil i L171, at det ikke er hensigten at "*enkeltpersoner gøres til genstand for målrettede tiltag eller overvågning*"[41].

I forhold til uvarslede hændelser er fokus på det beredskabsmæssige aspekt. Bestemmelsen har til hensigt at give politiet en fordel ved at have et IT-system, der kan sammenkøre data og ud fra dette genkende og angive tendenser og kriminalitetsmønstre. Derudover er fokus på den efterforskningsmæssige indsats, idet der med § 2 a er mulighed for hurtigt at danne et overblik over en given situation ved at anvende data fra tværgående kilder[42].

Det er ifølge bemærkningerne til L171 også hensigten, at politiet med indførslen af § 2 a skal have et klart retligt grundlag, der regulerer anvendelsen af Pol-Intel[43]. Dette begrundes blandt andet med, at politiets indsamling og behandling af personoplysninger via open source eller fra de kilder, som politiet kan tilgå, kræver hjemmel efter EMRK artikel 8 om retten til privatliv[44].

Forholdet mellem politilovens § 2 a og EMRK artikel 8 beskrives i bemærkningerne til L171 således, at politiets anvendelse af tværgående analyser som udgangspunkt udgør et indgreb i retten til privat mv., men at dette kan retfærdiggøres, hvis indgrebet har hjemmel i loven, hvis det varetager et eller flere anerkendelsesværdige formål, og findes nødvendigt i et demokratisk samfund[45].

[38] Lovforslag nr. 171 af 29. marts 2017, s. 10
[39] Lovforslag nr. 171 af 29. marts 2017, s. 9
[40] Lovforslag nr. 171 af 29. marts 2017, s. 5
[41] Ibid.
[42] Lovforslag nr. 171 af 29. marts 2017, s. 6
[43] Lovforslag nr. 171 af 29. marts 2017, s. 4
[44] Lovforslag nr. 171 af 29. marts 2017, s. 10
[45] Lovforslag nr. 171 af 29. marts 2017, s. 15

Formålet med indgrebet beskrives herefter som værende styrkelse af politiets "*analyse- og vidensbaserede tilgang*" med henblik på at sikre, at politiet effektivt kan håndtere kriminaliteten, som den udvikler sig, hvilket konkret beskrives som varetagelse af "*hensynet til den nationale sikkerhed, den offentlige tryghed og til at forebygge uro eller forbrydelse*", og som nødvendigt i et demokratisk samfund[46].

Der lægges i denne vurdering blandt andet vægt på, at der er et naturligt behov for, at politiet kan analysere stigende mængder af data, at der kun er tale om data, som politiet i forvejen kan tilgå, samt at det i det konkrete tilfælde er en politifaglig vurdering, om behandlingen af oplysningerne er nødvendigt for at kunne udføre politiets opgaver[47].

For kortfattet at opsummere, blev politilovens § 2 a dermed indført for at sikre et klart hjemmelsgrundlag til politiets indsamling og behandling af oplysninger, herunder at lade oplysninger indgå i tværgående informationsanalyser for at modernisere og effektivisere politivirksomheden.

5.2.2. Baggrund for bestemmelsen

Behovet for modernisering og effektivisering udspringer, ifølge bemærkningerne til L171, af det komplekse kriminalitetsbillede i det moderne samfund. Kriminaliteten består i stigende grad af IT-kriminalitet, herunder hacking, phishing, identitetstyveri mv., samt avanceret, grænseoverskridende kriminalitet i forbindelse med eksempelvis narkotika eller rocker- og bandekriminalitet[48]. Mere og mere kriminalitet er i dag præget af den teknologiske udvikling, og politiet må derfor forbedre deres IT-mæssige muligheder for at kunne følge med.

Det fremgår af bemærkningerne til L171, at det altid har været afgørende for politiets arbejde, at de kan tilgå oplysninger om samfundet, men at dette før i tiden skete ved hjælp af politibetjentenes kendskab til lokalmiljøet. Dette er ikke længere tilstrækkeligt på grund af udviklingen i kriminalitetsbilledet og den stadigt stigende anvendelse af teknologi til at udøve kriminalitet. Der er med tiden opstået et behov for at inddrage større mængder af data for at kunne bekæmpe den moderne kriminalitet, herunder navnlig organiseret,

[46] Lovforslag nr. 171 af 29. marts 2017, s. 15
[47] Ibid.
[48] Lovforslag nr. 171 af 29. marts 2017, s. 3

grænseoverskridende kriminalitet og IT-kriminalitet. Samtidig findes der i nutidens samfund større mængder af data, som kan tilgås, da mere og mere data forekommer digitalt. Dette er populært kaldet "*big data*". Det er dermed rent teknisk en mulighed for politiet at tilgå større mængder af data end tidligere, såfremt de har det rette værktøj, som kan lave disse tværgående informationsanalyser[49].

5.3. Politiets analyseværktøj

Netop med henblik på at skaffe det rigtige værktøj, har politiet indkøbt den digitale platform, Pol-Intel. Prisen er ikke blevet offentliggjort, men ifølge Volquartzen er der tale om et beløb mellem 100 og 280 millioner kr.[50]. Pol-Intel blev implementeret i det danske politi i sommeren 2017 og har været genstand for både kritik og begejstring. Programmet er af Rigspolitiet blevet kaldt et revolutionerende "*supervåben*", men der er omvendt også mange, der har påpeget, at der er tale om en vidtgående overvågning af borgerne[51]. Med Pol-Intel forventes det, at politiet skal bruge 80 % af tiden på at indsamle data og 20 % på at analysere det, hvor det før var omvendt[52]. Der er overordnet set to interessante aspekter ved Pol-Intel, som vil blive gennemgået: Programmets funktion og formål, og programmets leverandør, Palantir, som i USA har været genstand for en del kritik.

5.3.1. Pol-Intel

Formålet med implementeringen af Pol-Intel er som nævnt at have et værktøj, som effektivt kan foretage tværgående informationsanalyser på tværs af flere databaser og politikredse. Politiet har som følge af udviklingen i kriminalitetsbilledet brug for at modernisere og effektivisere deres metoder, og hertil kommer behovet for, hvad der i bemærkningerne til L171 kaldes tidssvarende redskaber for at kunne udføre de opgaver, som politiet har i medfør af politilovens § 2[53].

Politiet arbejdede før implementeringen af Pol-Intel i isolerede IT-systemer, der havde den såkaldte "*silostruktur*". Det var en omfattende manuel proces, når der skulle indsamles data

[49] Lovforslag nr. 171 af 29. marts 2017, s. 4
[50] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 188
[51] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171 f.
[52] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 175
[53] Lovforslag nr. 171 af 29. marts 2017, s. 3

som led i efterforskningsarbejdet, da søgninger ikke kunne foretages på tværs af de forskellige systemer. At det ikke var muligt at foretage tværgående analyser var årsagen til, at politiets redskaber, ifølge bemærkningerne til L171, vanskeliggjorde effektiv og moderne politivirksomhed, og analyseværktøjerne kunne ikke understøtte politiets behov[54]. De beskrevne behov udspringer af, at det danske politi i mange år har været i gang med at implementere intelligence-led policing. Det var på baggrund af dette, at man indkøbte og implementerede Pol-Intel, således at man kunne forbedre dataanvendelsen og styrke det analyse- og vidensbaserede arbejde[55].

Analysearbejdet i Pol-Intel skal ligge til grund for politivirksomheden inden for forskellige områder. Dette omfatter blandt andet uvarslede hændelser, hvor det forventes, at IT-systemet kan genkende kriminalitetsmønstre og alarmere inden hændelserne sker, således at politiet kan reagere i tide. Det omfatter også færdselsrelateret politiarbejde og det generelle beredskabsmæssige arbejde, da det er meningen, at politiet skal kunne bruge Pol-Intels analyser til forbedret prioritering og disponering af deres patruljering[56].

Det er hensigten, at Pol-Intel skal være det understøttende element i analysearbejdet, og at oplysninger om enkeltpersoner, så vidt som muligt, kun tilgås på systemniveau. Dette kan være personfølsomme oplysninger om eksempelvis strafbare forhold. Hertil kommer, at medarbejderne i politiet, så vidt muligt, kun præsenteres for oplysninger på en måde, som kan identificere personen, når dette anses for at være "*politifagligt nødvendigt*". Derudover skal Pol-Intel med sine tekniske egenskaber sikre, at oplysninger indsamlet til en sag kun tilgængeliggøres til anvendelse i forbindelse med en anden sag, såfremt dette findes proportionalt og nødvendigt[57].

Der bliver med Pol-Intel, og med predictive policing i øvrigt, gjort op med den traditionelle efterforskningsmodel, hvor information videregives blandt mennesker. Nu behandles informationer i form af data i Pol-Intel, fordi det på denne måde kan gøres mere effektivt og tidsbesparende, end hvad mennesker kan alene. Denne form for databehandling, hvor en computer i blinde afprøver forskellige sammensætninger, er også betegnet som

[54] Lovforslag nr. 171 af 29. marts 2017, s. 4
[55] Lovforslag nr. 171 af 29. marts 2017, s. 5
[56] Lovforslag nr. 171 af 29. marts 2017, s. 6
[57] Lovforslag nr. 171 af 29. marts 2017, s. 10

datamining[58]. Politiet kan dermed bruge Pol-Intel til at prioritere deres ressourcer til de områder, der af systemet forudsiges at have øget risiko for kriminalitet[59].

5.3.2. Palantir

Pol-Intel leveres af den private amerikanske IT-virksomhed Palantir, som beskæftiger sig med datamining. Dette er et eksempel på mødet mellem det private, kommercielle marked og de offentlige myndigheder. Palantir har både private virksomheder og offentlige myndigheder som kunder. Blandt de offentlige myndigheder kan nævnes Pentagon, CIA og flere forskellige politimyndigheder i USA, og Palantir kan dermed, ifølge Volquartzen, i høj grad påvirke det offentlige myndighedsarbejde, navnlig fordi der antageligt ikke er nogen, der kontrollerer Palantir[60].

Palantir er underlagt stor kritik fra borgerrettighedsgrupper efter flere episoder, og deres metoder er, af borgerrettighedsadvokater, blevet kaldt forfatningsstridige[61]. Dette medfører, at de myndigheder, som bruger Palantirs softwareløsninger, herunder politiet, anvender metoder, som af fagpersoner er blevet kaldt forfatningsstridige.

En episode, hvor Palantir har været kritiseret, er i forbindelse med at have hjulpet virksomheden Cambridge Analytica med at anvende persondata fra omkring 87 millioner facebookbrugere i forbindelse med Donald Trumps præsidentkampagne i 2016. Dette forsvarede Palantir med, at medarbejderen havde gjort det uden for arbejdstiden[62]. Det skal hertil nævnes, at Palantir, ifølge virksomheden selv, ikke er politisk anlagt, selvom grundlæggeren Peter Thiel har ydet stor økonomisk støtte til Trump under valgkampen i 2016. Thiel har desuden skrevet et kritisk essay om, at det siden 1920'erne kun er gået den forkerte vej i velfærdssamfundet i forhold til blandt andet kvinder, skatter, fattige mv.[63]. Dette rejser spørgsmålet, om Palantir i nogen grad alligevel ér en politisk anlagt virksomhed, på trods af hvad de selv udtaler.

[58] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 175
[59] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171
[60] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 187
[61] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 188
[62] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 187 f.
[63] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 188

Den centrale problemstilling ved, at private virksomheder leverer IT-systemer til brug for offentlige myndigheder er, ifølge Volquartzen, at myndighederne er underlagt en masse regler inden for forvaltningsretten, som de private aktører ikke er underlagt. Dermed føres der ikke kontrol med virksomhederne, og der er ikke de samme krav på trods af, at deres ydelser anvendes som led i det offentlige virke. Der bør, ifølge Volquartzen, tages stilling til denne mangel på regulering og kontrol for at undgå, at private IT-udviklere kan påvirke den enkelte borgers retsstilling i form af stigmatisering og diskriminering[64].

5.4. Anvendes predictive policing i det danske politi?

Der findes ikke et endegyldigt svar på om predictive policing anvendes i det danske politi. Dette kan begrundes med at politiets interne metoder som udgangspunkt ikke er noget, som den almindelige borger kan tilgå, samt at der har ikke været en udmelding fra politiet om, at de fra en given dato vil tage predictive policing-metoden i brug. Derfor er det relevant at søge svaret i litteraturen og i den gældende lovgivning. Nedenfor vil dette søges belyst ved brug af lovforslaget L171 bag politilovens § 2 a, og herefter Mette Volquartzens tekst "Forskydninger mellem det private og det offentlige i smart politiarbejde" i bogen "Ret SMART" fra 2018, som også er inddraget tidligere.

5.4.1. Lovforslaget bag § 2 a

Af bemærkningerne til L171 fremgår det, at det med implementeringen af § 2 a og Pol-Intel er muligt at foretage tværgående informationsanalyser og dermed modernisere og effektivisere politiets virksomhed[65]. Dette rejser spørgsmålet, om formålet med implementeringen af § 2 a og Pol-Intel er predictive policing.

Predictive policing er, som før nævnt, en forebyggende indsats, hvor politiet på baggrund af en algoritme prioriterer deres ressourcer og retter dem mod områder eller personer, hvor der er risiko for kriminalitet. Det fremgår af bemærkningerne til lovforslaget, at de tværgående informationsanalyser kan lægges til grund for politivirksomheden både inden for og uden for strafferetsplejen. Konkret nævnes både uvarslede hændelser og det borgernære politi, herunder eksempelvis patruljering[66]. Dette formål harmonerer med definitionen af predictive

[64] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 189
[65] Lovforslag nr. 171 af 29. marts 2017, s. 3
[66] Ibid.

policing, selvom begrebet ikke nævnes i forbindelse med lovforslaget. Dog må det vurderes, at anvendelse af dataanalyser til prioritering af ressourcer i politiet er både definitionen på predictive policing og formålet med implementeringen af politilovens § 2 a og Pol-Intel. Dette medfører ikke i sig selv, at predictive policing anvendes på nuværende tidspunkt, men blot at det er hensigten, hvilket kan udledes af bemærkningerne til L171. Det må dog fastslås, at politiet med Pol-Intel og politilovens § 2 a, i 2017 har fået de retlige rammer og værktøjet til at anvende metoden.

For så vidt angår implementeringen af metoden i Danmark, lægges vægt på, at politiet ikke skal have adgang til flere oplysninger, end de allerede har, men at data blot skal kunne sammenkøres på tværs af databaser. Sammenkørsel af data skal ifølge bemærkningerne til L171 ske som led i politiets virksomhed i bred forstand, herunder i forbindelse med blandt uvarslede hændelser og pludseligt behov for beredskab, men også færdsel og lokal patruljering.

5.4.2. Mette Volquartzen

Volquartzens betragtninger er interessante, idet de giver et godt billede af, hvad predictive policing indebærer, og hvilke risici, der kan være forbundet med at bruge denne metode. Derudover er teksten relevant, fordi Volquartzen tager stilling til, hvorvidt der findes predictive policing i Danmark. Ifølge Volquartzen, er predictive policing noget, som på længere sigt skal anvendes ved hjælp af Pol-Intel[67]. Volquartzen lægger til grund, at predictive policing ikke anvendes i det danske politi endnu, hvorfor hun i sin tekst inddrager udenlandske erfaringer for at belyse udfordringerne ved predictive policing[68]. Der findes ikke en kilde, der understøtter udsagnet om, at politiet ikke anvender predictive policing, og derfor opstår spørgsmålet om, hvad Volquartzen lægger til grund herfor. Modsat kan det også ses som et udtryk for, at der ikke findes nogen indikationer på, at politiet rent faktisk anvender predictive policing. Dette skal dog ses i lyset af, at Mette Volquartzen må antages ikke at have indsigt i den interne del af politiets processer. Det er derfor usikkert, hvor stor betydning, Volquartzens udtalelse i denne forbindelse kan have, men det må dog inddrages i betragtningerne.

[67] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 171
[68] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 173

Forudsætningerne for at tage predictive policing i brug findes i politilovens § 2 a, og politiet har dermed haft hjemmel til at anvende predictive policing siden denne bestemmelse blev indført i 2017. Derudover har politiet de fornødne tekniske ressourcer til at tage metoden i brug, idet Pol-Intel rent praktisk kan foretage tværgående informationsanalyser, som kan lægges til grund for predictive policing.

Sammenfattende kan det dermed fastslås, *at* politiet i 2017 fik de retlige rammer til at anvende predictive policing, *at* politiet ved samme lejlighed fik et IT-system, som kan foretage det arbejde, der lægges til grund for predictive policing, samt *at* det ikke kan fastslås om der rent faktisk anvendes predictive policing, idet der ikke har været nogle udtalelser fra politiet eller andre offentlige myndigheder herom.

5.5. Overvejelser om anvendelsen af predictive policing

Predictive policing er en effektiv metode for politiet til hurtigt at kunne indsamle og analysere oplysninger, og på den måde mere effektivt bekæmpe kompleks kriminalitet. Det er utvivlsomt, at anvendelsen af Pol-Intel og muligheden for at sammenkøre data vil give politiet bedre muligheder for at foretage mere effektiv og omfattende efterforskning og samtidig kunne prioritere deres ressourcer anderledes og mere effektivt. Afsnit 5.4. giver dog anledning til flere overvejelser om anvendelsen af metoden. I dette afsnit gennemgås nogle af udfordringerne ved anvendelse af predictive policing. Dette omfatter falsk positiv og falsk negativ, forudindtagelse og bias, anvendelsens formål og over-policing.

5.5.1. Falsk positiv og falsk negativ

Ved anvendelsen af predictive policing vil en del af politiets beslutninger ikke længere blive taget af mennesker, men i stedet af computere. En væsentlige forskel er, at i modsætning til en computer, kan mennesker begrunde, forklare og retfærdiggøre en beslutning[69]. Der vil derfor være en reel chance for fejlidentifikation i form af falske positiver og falske negativer i algoritmens beregning af, hvor der vil forekomme kriminalitet og hvem, der vil udføre en kriminel handling[70]. Pol-Intel kan, i forhold til dette, ikke forsvare sine afgørelser, men det kan politiets ansatte. Omvendt vil politiet kunne få svært ved at forsvare eller forklare Pol-

[69] Hannah Couchman: "*Policing by Machine*", 2019, s. 39
[70] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 182

Intels resultater, medmindre de tilegner sig fuld forståelse for, hvordan systemet beregner sine resultater. Det er derfor vigtigt, at medarbejderne i politiet sætter sig ind i Pol-Intels måde at arbejde på, og får en dybdegående forståelse for dets funktion, så de kan arbejde sidestillet med IT-systemet. Dette udgør i sig selv en udfordring ved predictive policing, idet en borger til enhver tid har ret til at få en begrundelse, forklaring og afklaring på de beslutninger, som påvirker deres rettigheder - med andre ord skal man kunne holde politiet ansvarlig for deres beslutninger[71].

Denne problematik beskrives af Hannah Couchman i rapporten "Policing by Machine" fra den engelske menneskerettighedsorganisation Liberty. Hun påpeger i denne forbindelse et behov for, at politiet ikke ender med at arbejde blindt efter algoritmen, men har redskaberne til at efterprøve den og arbejde sidestillet med den. Dette kræver dybdegående research, analyser og tests over langt tid, og er derfor ikke noget, der kan realiseres i den nærmeste fremtid[72]. Couchman peger også på, at mennesket ikke forstår, hvordan algoritmen når frem til resultaterne, og dermed ikke kan kontrollere metoden løbende[73].

Implementeringen af Pol-Intel og § 2 a i 2017 åbnede op for, at politiet kunne tage denne metode i brug, og der vil derfor være et behov for, at medarbejderne i politiet forudgående har tilegnet sig viden om programmet. Det vil være nødvendigt for at sikre borgernes retssikkerhed, at politiet kan afklare, hvordan de udøver deres virksomhed, når denne baseres på Pol-Intels udregninger. Det må dermed, hvis predictive policing skal anvendes, være nødvendigt at højne niveauet hos politiet, således at de i deres arbejde har forståelse for algoritmen i Pol-Intel.

5.5.2. Forudindtagelse og bias

Et udbredt problem ved at anvende algoritmer generelt er bias. En algoritme er som overvejende hovedregel ikke neutral, og vil som udgangspunkt være forudindtaget. Denne forudindtagelse kommer af, at computere ikke selv opfinder den information, som anvendes af algoritmen. Computere skal have informationer fra mennesker, og de enkeltpersoner, der indtaster informationerne, vil dermed bevidst eller ubevidst have indvirkning på algoritmen. Konsekvenserne heraf er ikke som sådan katastrofale, når en algoritme i en privat

[71] Hannah Couchman: "*Policing by Machine*", 2019, s. 40
[72] Hannah Couchman: "*Policing by Machine*", 2019, s. 8
[73] Hannah Couchman: "*Policing by Machine*", 2019, s. 9

virksomhed er årsag til, at virksomheden mister et salg eller lignende. Dette kan dog ikke siges at være tilfældet, hvis en algoritme er årsag til fejlagtig politivirksomhed eller anden virksomhed i offentlige myndigheder, da dette vil have konsekvenser for retssikkerheden[74].

Volquartzen beskriver i denne forbindelse, hvordan det er nødvendigt for en vidensbaseret organisation at holde en vis afstand til anvendelsen af teknologi. Dette kommer af, at politiets øgede anvendelse af IT har skabt begejstring, men også frygt for at computerne vil erstatte mennesket. Det er derfor vigtigt for den vidensbaserede organisation at have fokus på, at teknologien blot er et redskab, som har behov for bistand fra mennesker til at udvælge data. Hertil kommer, at der så skal tages højde for, hvilke mennesker, der skal bidrage til algoritmen, samt hvordan juraen skal sikre retssikkerheden, således at private IT-virksomheder ikke får adgang til at påvirke myndighedsudøvelsen og borgernes retstilstand[75].

Pol-Intel anvender som nævnt data fra forskellige databaser og offentligt tilgængelige kilder, og laver på baggrund heraf tværgående analyser, som skal ligge til grund for en del af politiets virksomhed. Informationerne, der medtages i algoritmen, kommer dermed fra flere forskellige kilder, som kan være administreret af offentlige myndigheder, private selskaber eller indtastet af private personer på eksempelvis Facebook profiler. Det må derfor antages, at det ikke kan afklares, hvorvidt disse kilder yder information, der sikrer transparens i Pol-Intels analysearbejde, eller om det vil skabe forudindtagelse, hvilket der er risiko for.

5.5.3. Anvendelsens formål

Det er værd at bemærke, at ideen om at anvende tværgående analyser i det danske politi, som en del af et opsporende og forebyggende arbejde, har sine rødder i terrorhændelser, og at det i "Et stærkt værn mod terror" som før nævnt er tiltænkt forebyggelse af "*terror og andre meget alvorlige forbrydelser*"[76]. Læser man bemærkningerne til L171 vil man bemærke, at formålet med at indføre § 2 a er, at anvende styrket data- og analysebaseret arbejde i alle dele af politiets virksomhed, både i forhold til alvorlig, organiseret grænseoverskridende kriminalitet og den "borgernære" kriminalitet, både i forbindelse med

[74] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 184
[75] Mette Volquartzen: "*Forskydninger mellem det private og det offentlige*", 2018, s. 186
[76] Regeringens udspil "*Et stærkt værn mod terror*", februar 2015, s. 5

forebyggende og efterforskningsarbejde[77]. Formålet med at implementere det analysebaserede arbejde har dermed ændret sig siden starten af processen for implementeringen. Formålet med at åbne op for muligheden for at anvende dataanalyser i politiets arbejde har dermed udvidet sig fra terror og meget alvorlige forbrydelser til stort set alle andre dele af politiets arbejde.

I forhold til lovgivningen om, hvilken form for kriminalitet, der kan være årsag til at anvende tværgående analyser, er dette beskrevet i BEK nr. 1078/09/2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser. Denne bekendtgørelse er udstedt af Justitsministeriet med hjemmel i politilovens § 2 a, stk. 3, og indeholder generelle bestemmelser for politiets virksomhed efter § 2 a. Det fremgår af ordlyden i bekendtgørelsens § 3, stk. 2, at analysearbejde efter politilovens § 2 a ikke kan foretages i forhold til den rent administrative afgørelsesvirksomhed eller generel informationssøgning. Dette er det eneste sted, hvor der helt konkret afgrænses fra dataanalysearbejde på et bestemt område af politiarbejdet.

Ydermere fremgår det af bekendtgørelsens § 4, at personoplysninger kan behandles i dataanalyser i Pol-Intel, når det er nødvendigt for at bringe strafbar virksomhed til ophør, eller forfølge og efterforske strafbare forhold, jf. § 4, nr. 1, for at forebygge strafbare forhold eller afværge fare, herunder for den enkeltes eller den offentlige sikkerhed, eller forstyrrelse af den offentlige fred og orden i konkrete tilfælde, jf. nr. 2, som understøttelse af politiets opgaver i konkrete tilfælde, jf. nr. 3, i forbindelse med grænse- og udlændingekontrol, jf. nr. 4, eller strategiske og statistiske analyser til understøttelse af de i nr. 1-4 nævnte opgaver, jf. nr. 5.

Analysearbejdet i Pol-Intel kan også foretages på baggrund af pseudoanonymiserede oplysninger efter bekendtgørelsens § 6, stk. 1. Dette omfatter tilfælde vedrørende strafbare forhold, fare den enkeltes eller den offentlige sikkerhed, eller forstyrrelse af den offentlige fred og orden, jf. § 5, nr. 1 for forebyggelse og nr. 2 for afværgelse, bistand til borgere i andre faresituationer, jf. nr. 3, kontrol og tilsynsopgaver, jf. nr. 4, bistand til andre myndigheder, jf. nr. 5, andre opgaver med naturlig forbindelse til politiets virksomhed, jf. nr. 6, eller strategiske og statistiske analyser mv. til understøttelse af disse opgaver, jf. nr. 7.

[77] Lovforslag nr. 171 af 29. marts 2017, s. 5

Tværgående analyser efter § 5 kan ske uden anonymisering af oplysningerne, hvis dette må anses for at være strengt nødvendigt for politiets opgavevaretagelse. Rigspolitiet skal fastsætte nærmere regler for en sådan afmaskering, jf. § 6, stk. 3, og skal i øvrigt sikre og kunne bevise, at § 6, stk. 1-3, overholdes. Det er dermed Rigspolitiet, der har ansvaret for afmaskering af personoplysninger.

Formålet efter de beskrevne bestemmelser er ubestridt bredere, end hvad fremgår af regeringens udspil fra 2015 "Et stærkt værn mod terror", både ifølge bekendtgørelsen og lovforslaget L171. Dette er relevant i forhold til menneskeretten, herunder proportionalitets- og legalitetskravet i artikel 8 og dommen Klass m.fl. mod Tyskland, som vil blive gennemgået nedenfor i afsnit 6.3. og 6.4.

5.5.4. Over-policing

Behandling af personoplysninger, uanset om disse er anonymiserede eller ej, må dog antages at kunne resultere i, at nogle borgere i højere grad end andre overvåges og påvirkes af politiet. Tværgående informationsanalyser, som dem predictive policing baseres på, medfører naturligt denne risiko, navnlig set i lyset af risikoen for falske positiver. Det skal dog også ses i lyset af, at hvis en algoritme udpeger et bestemt boligområde, fordi der før har været meget kriminalitet, og politiet på baggrund af algoritmen øger patruljeindsatsen i dette område, vil dette påvirke alle de borgere, der bor i området, og ikke kun dem der er årsag til algoritmens analyseresultat. Det må antages at genkendelse af kriminalitetsmønstre, som er formålet med implementeringen af politilovens § 2 a og Pol-Intel, i nogen grad vil medføre en sådan politivirksomhed, såfremt der skal anvendes tværgående informationsanalyser til den borgernære kriminalitet og nærpolitiet. Henset til de ovenfor beskrevne former for kriminalitet, som analysearbejde efter politilovens § 2 a kan ligge til grund for, kan dette ikke udelukkes. Her menes blandt andet bekendtgørelsens § 5, nr. 3, om kontrol og tilsynsopgaver, og nr. 6, om andre opgaver med naturlig forbindelse til politiets virksomhed.

Denne form for politivirksomhed er før set i England, hvor der anvendes "*predictive mapping*"-programmer, som udpeger hot spots, hvor der er høj risiko for kriminalitet. Her baseres politivirksomheden på en analyse af data på tværs af politiets databaser[78]. Dette kan

[78] Hannah Couchman: "*Policing by Machine*", 2019, s. 3

umiddelbart minde om det, der er formålet med Pol-Intel. At basere den borgernære politivirksomhed på tværgående informationsanalyser efter politilovens § 2 a kan derfor potentielt medføre en risiko for diskrimination i strid med EMRK artikel 14, da der i de områder, hvor politiet prioriterer patruljevirksomheden, kan opstå *over-policing,* og folk, der bor i disse områder, risikerer at blive ofre for overvågning i højere grad end andre[79].

Derudover beskriver Couchman det som problematisk, at det indsamlede data ikke giver et korrekt billede af kriminaliteten i de respektive områder. Dataanalyserne viser blot, hvordan og hvornår politiet har reageret på kriminalitet, og det er altså ikke medregnet i algoritmen, at der findes meget kriminalitet, som ikke anmeldes til politiet, eller som politiet ikke følger op på. Dette vil være misvisende og kan føre til forkert prioritering af politiets ressourcer og over-policing[80]. Det er derfor essentielt at tage stilling til, hvilke former for data, der medtages i analysearbejdet.

5.6. Sammenfatning

Sammenfattende kan det fastslås, *at* politilovens § 2 a og implementeringen af Pol-Intel muliggør anvendelse af predictive policing i det danske politi, *at* det ikke med sikkerhed kan fastslås, at predictive policing faktisk anvendes, da der ikke er kommet en udmelding herom, samt *at* der er relativt vide retlige rammer for, i hvilke situationer, der kan anvendes tværgående informationsanalyser. Derudover kan det fastslås, *at* der er risiko for fejlidentifikation i form at falske positiver og negativer, *at* der kan være udfordringer for politiet i forbindelse med at skulle forsvare politivirksomheden, hvis politiets ansatte ikke har forståelse for algoritmen, *at* der er risiko for at Pol-Intels algoritme er forudindtaget, navnlig set i lyset af, at data både kommer fra offentlige myndigheder og privatpersoner på sociale netværk, samt *at* der ved brug at tværgående informationsanalyser er risiko for over policing i visse områder.

Anvendelsen af predictive policing i udlandet har skabt debat omkring forholdet til Den Europæiske Menneskerettighedskonvention, herunder artikel 8 om retten til respekt for privatliv, familieliv, hjem og korrespondance, samt artikel 14 om retten til ikke at blive diskrimineret. Følgende afsnit vil gennemgå disse menneskeretlige aspekter, og

[79] Hannah Couchman: "*Policing by Machine*", 2019, s. 3 f.
[80] Hannah Couchman: "*Policing by Machine*", 2019, s. 15 f.

sammenholde dette med anvendelsen af predictive policing efter politilovens § 2 a og Pol-Intel i Danmark.

6. Menneskerettighederne

EMRK artikel 8 og 14 vil i det følgende blive gennemgået hver for sig med henblik på at skabe en grundlæggende forståelse for, hvad disse hver især indebærer. I forbindelse med artikel 8 vil bestemmelsens anvendelse inden for fremstillingens område blive belyst af to afgørelser fra EMD.

Der vil efter gennemgangen af bestemmelserne være et afsnit med overvejelser omkring de belyste menneskerettigheder over for anvendelsen af predictive policing i Danmark.

6.1. Artikel 8: Retten til privatliv mv.

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Således lyder EMRK artikel 8, hvorefter alle har ret til respekt for deres privatliv, familieliv, hjem og korrespondance. Det er dermed efter stk. 1 som udgangspunkt statens ansvar at sørge for, at der ikke bliver foretaget indgreb i disse fire beskyttelsesinteresser. Dette udgangspunkt kan dog fraviges efter stk. 2 hvis indgrebet (1) har hjemmel i loven, (2) er nødvendigt i et demokratisk samfund, (3) bør foretages af hensyn til national sikkerhed, offentlig tryghed, landets økonomiske velfærd, forebyggelse af uro eller forbrydelse eller beskyttelse af sundhed, sædelighed eller andres rettigheder, jf. artikel 8, stk. 2.

Det følger af denne bestemmelse, at staten ikke må foretage indgreb i borgernes ret til privatliv, familieliv, hjem og korrespondance. Staten har endvidere i et vist omfang en positiv forpligtelse til at sikre, at borgernes rettigheder efter bestemmelsen ikke krænkes - heller ikke af andre private borgere. Vurderingen af om staten har en sådan forpligtelse, skal

bero på "*samfundets generelle interesser overfor individets*"[81]. Dog kan staten ikke pålægges en umulig eller uforholdsmæssig byrde i forbindelse med at skulle opfylde en positiv forpligtelse[82].

I følgende afsnit vil de fire beskyttelsesinteresser i artikel 8 blive gennemgået, og herefter vil der være en beskrivelse af, hvad bestemmelsens indhold er i forhold til offentlige myndigheders indsamling og behandling af personoplysninger.

6.1.1. Beskyttelsesinteresserne

EMRK artikel 8 beskytter retten til privatliv, familieliv, hjem og korrespondance. Disse fire beskyttelsesinteresser vil blive gennemgået i dette afsnit.

Begrebet "privatliv" i EMRK artikel 8 skal forstås bredt. Kjølbro beskriver flere eksempler på, hvad begrebet omfatter, men fastslår dog indledningsvis, at der ikke kan laves en udtømmende oplistning. Privatliv kan, i bestemmelsens forstand, omhandle både fysisk og psykisk integritet, og fysisk og social identitet[83]. Beskyttelse af fysisk og psykisk integritet omfatter blandt andet tvangsmæssig lægelig behandling, uanset hvor indgribende behandlingen i sig selv er[84]. Det kan omhandle retten til personlig udvikling, etablering og udvikling af relationer til andre mennesker, herunder familiemedlemmer, når det ikke omfattes af begrebet "familieliv", eller muligheden for at leve uden uønsket opmærksomhed. Det omfatter aktiviteter i både det private og det professionelle liv. Alt dette hænger sammen med, at det med beskyttelsen af privatliv er tilsigtet at sikre muligheden for personlig udvikling[85].

Også informationer om enkeltpersoners seksuelle aktiviteter og seksuelle orientering, samt informationer om etnicitet, religiøs orientering, tidligere ansættelsesforhold, private forhold og identitet, herunder fødsel, opvækst mv., er omfattet[86].

Retten til selvbestemmelse er også omfattet af denne bestemmelse, hvilket blandt andet indebærer, at voksne åndsfriske personer ikke må udsættes for lægehjælp imod

[81] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 887
[82] Ibid.
[83] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 859
[84] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 866
[85] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 859
[86] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 861

vedkommendes vilje. Det samme gælder lægebehandling af børn og unge under 18 år uden forældremyndighedsindehavers samtykke[87]. Retten til selvbestemmelse indebærer også beslutninger omkring fysisk fremtoning, selvrealisering og selvudfoldelse[88].

Ransagninger og anden indtrængen i hjemmet fra offentlige myndigheder, såvel som disses tiltvingelse af kontooplysninger og lignende, er også omfattet af bestemmelsen. Det samme gør sig gældende for standsning og visitation af personer i det offentlige rum, samt telefonaflytning, optagelse af telefonsamtaler, uanset om optagelserne tages i brug eller ej, og videreformidling af indholdet af sådanne optagelser[89]. Også indhentelse af teleoplysninger fra operatører er omfattet, herunder hvis politiet indhenter opkaldslister, uanset om de gøres bekendt med indholdet af opkaldene eller ej[90]. Overvågning af private personer er omfattet af bestemmelsen, hvis det sker i personens private hjem, men som udgangspunkt ikke på offentligt tilgængelige steder, medmindre der er tale om systematisk og permanent opbevaring af sådanne overvågningsdata[91].

Særligt interessant for denne fremstilling er, at myndigheders opbevaring, behandling, videregivelse og frigivelse af data om personers private forhold også er omfattet af bestemmelsen. Med dette menes blandt andet politiets opbevaring af data, som vedrører en persons navn, adresse, strafbare forhold, vævsprøver og fingeraftryk, DNA-profiler, fotografier uanset om disse offentliggøres eller ej, data i forbindelse med overvågning og systematisk indsamling og opbevaring af open source-data[92]. Offentlige myndigheders behandling af personoplysninger vil blive nærmere behandlet nedenfor i afsnit 6.1.2.

På samme måde som retten til privatliv beskyttes retten til familieliv også af artikel 8. Familieliv kan omfatte forholdet mellem ægtefæller, ugifte samlevende, andre par eller forholdet mellem andre nærtstående, herunder eksempelvis bedsteforældre[93].

Vurderingen af, om der er tale om et familieliv i bestemmelsens forstand, skal bero på momenter som forholdets varighed, om parterne har forpligtet sig over for hinanden eksempelvis ved at få børn, samt hvorvidt parterne bor sammen eller forholdet i øvrigt er af

[87] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 864
[88] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 866
[89] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 868
[90] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 869
[91] Ibid.
[92] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 862 f.
[93] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 879

varig karakter[94]. Tætte forhold, som af den ene eller den anden årsag ikke er omfattet af begrebet "familieliv", kan være beskyttet i bestemmelsen under betegnelsen "privatliv", som er beskrevet ovenfor[95].

Udover retten til privatliv og familieliv beskyttes også retten til hjemmet. Vurderingen af, om der er tale om et indgreb i denne beskyttelsesinteresse, skal bero på de faktiske omstændigheder, og hovedsageligt, om der er tale om "*tilstrækkelig og varig tilknytning til et bestemt sted*". Begrebet i denne konvention har selvstændig betydning i forhold til, hvad begrebet vil omfatte i national lovgivning, og det er derfor irrelevant for vurderingen af, om der er sket en krænkelse af retten til respekt for hjemmet, om en persons anvendelse af et bestemt sted som et "hjem" er ulovlig efter national lovgivning[96]. Generelt er fortolkningen af begrebet, ifølge Kjølbro, af udvidende og dynamisk karakter[97].

Begrebet kan omfatte den private bolig, også selvom denne ikke er en bolig i traditionel forstand, men det kan også omfatte erhvervslokaler, eksempelvis hvis en person arbejder og bor samme sted[98]. Det er retten til respekt for de fysiske rammer, en person har sat for sit privatliv, og retten til at kunne nyde dette område i fred, som skal forstås ved denne beskyttelse. Beskyttelsen omfatter både konkrete fysiske krænkelser, som indtrængen, og andre krænkelser, herunder støj og lugt mv.[99].

Indtrængen og ransagelse foretaget af offentlige myndigheder i privates hjem udgør som udgangspunkt et indgreb i henholdsvis retten til respekt for privatlivet og hjemmet for indtrængen og retten til respekt for hjemmet for ransagelse[100].

For så vidt angår retten til respekt for korrespondance, er det beskyttede "*middelbar kommunikation med andre*", herunder skriftlig korrespondance som sms og e-mail, men også mundtlig korrespondance som telefonsamtaler. Det er dog et krav, at afsender og modtager må antages at gå ud fra, at andre ikke gøres bekendt med indholdet af meddelelserne[101].

---

[94] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 875
[95] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 877
[96] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 881
[97] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 883
[98] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 882
[99] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 884
[100] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 884
[101] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 885

Der er som udgangspunkt foretaget et indgreb i denne rettighed, når offentlige myndigheder gøres bekendt med omstændighederne for, eller indholdet af, privates kommunikation med andre, eller når offentlige myndigheder forhindrer eller vanskeliggør privates kommunikation med andre. Staten har en positiv pligt til at sikre denne ret for borgerne, eksempelvis at indsatte kan korrespondere[102].

Der er et skærpet legalitetskrav i forbindelse med hemmelige indgreb, som overvågning af eksempelvis telefonsamtaler. Dermed er der høje krav til det retlige grundlag for offentlige myndigheder til, at kunne foretage hemmelig aflytning, uden at dette krænker borgernes ret til respekt for privatliv og korrespondance[103]. Derudover skal der være mulighed for prøvelse og kontrol for at modvirke misbrug. Dette medfører konkret, at det nationale retsgrundlag skal indeholde en afgrænsning af, hvem der kan aflyttes, hvilken karakter af kriminalitet, der berettiger et indgreb, en procedure for undersøgelse, anvendelse, opbevaring, videregivelse og sletning[104].

Et indgreb i den umiddelbare kommunikation skal ikke vurderes i forhold til beskyttelsen af korrespondance, men beskyttelsen af privatlivet eller hjemmet, da dette i praksis vil forekomme i form af overvågning af samtaler på steder, der er eller ikke er offentligt tilgængelige[105].

6.1.2. Offentlige myndigheders behandling af oplysninger

Som før nævnt er det, når offentlige myndigheder opbevarer "*data, der har forbindelse til enkeltpersoners privatliv*"[106], eller videregiver "*rent personlige oplysninger og følsomme oplysninger om private*" til en anden myndighed, et indgreb i retten til respekt for privatliv[107]. Det samme gør sig gældende med offentligt tilgængelige oplysninger, når indsamlingen og opbevaringen af disse bærer præg af at være systematisk, hvilket er tilfældet med de fleste af de offentlige myndigheders registre[108]. Såfremt der er tale om et indgreb, skal opbevaring af data med forbindelse til borgernes privatliv, samt systematisk indsamling og opbevaring

[102] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 886
[103] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 979
[104] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 979 f.
[105] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 885
[106] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 958
[107] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 963
[108] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 959

af offentligt tilgængeligt information om privatpersoner, retfærdiggøres for ikke at udgøre en krænkelse af EMRK artikel 8[109].

For så vidt angår registrering og opbevaring af personoplysninger, har EMD anerkendt, at der er krav om "*streng nødvendighed*" for at beskytte demokratiske institutioner, før der kan foretages hemmelig overvågning af borgerne, uden at der sker en krænkelse af retten til privatliv. Der skal her foretages en vurdering af, om der foreligger tilstrækkelig og relevant begrundelse for overvågningen, hvilket nærmere konkret indebærer en afvejning af hensynet til den nationale sikkerhed, samt forebyggelse af uro og forbrydelse over for indgrebets karakter og alvor. Der stilles i denne forbindelse strenge krav til proportionalitet og legalitet. Det skal blandt andet indgå i denne vurdering, om der er fastsat begrænsninger i forhold til de indsamlede oplysningers karakter, hvem der må overvåges, hvilke betingelser der skal være opfyldt for at kunne foretage overvågningen, hvordan denne skal udføres, hvilke krav der stilles til, hvornår oplysningerne skal slettes igen, og om der føres effektiv kontrol med efterretningstjenestens aktiviteter[110]. Desuden skal det indgå i vurderingen, om der er tilstrækkelige og effektive retssikkerhedsgarantier til at beskytte borgerne mod misbrug[111].

Kjølbro påpeger, at overvågning af mistænktes færden, eller at pålægge dem at melde sig hos politiet, kan ske uden, at dette er en krænkelse af artikel 8, eksempelvis som led i en sanktion i stedet for frihedsberøvelse, eller som led i en efterforskning, eksempelvis ved hjælp af GPS-sporing. I begge eksempler er der tale om et indgreb i retten efter artikel 8, som skal retfærdiggøres efter bestemmelsens stk. 2, og det skal kun foregå, så længe det er nødvendigt[112].

Særligt for registrering af dømte, sigtede og mistænkte mv. er, at indsamling og behandling af oplysninger kan have betydning for fremtidig efterforskning. Et sådant register kan, ifølge Kjølbro ,have en præventiv virkning, idet viden om at være registreret også vil medføre viden om, at politiet lettere vil kunne opklare forhold begået af personen efterfølgende. Dermed er der en chance for, at fremtidige kriminelle handlinger kan undgås ved at registrere dømte, sigtede og mistænkte mv. Dette kan også henføres til, at oplysninger om strafbare

[109] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 959
[110] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 960
[111] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 961
[112] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 970

forhold legitimt kan videregives til potentielle arbejdsgivere, som registrerede personer ønsker ansættelse hos[113].

Der er desuden krav til grundlaget for registrering og opbevaring af væsentlige oplysninger om personer. Dette blev fastslået i afgørelsen EMD 2011-10-18 Khelili mod Schweiz, hvorefter det, ifølge EMD, udgjorde en krænkelse, at registrering af en person som "prostitueret" i politiets IT-systemer i 15 år alene var foretaget på baggrund af en mistanke herom[114]. Registrering af sådanne oplysninger kan herefter ikke foretages på et spinkelt grundlag.

Udover registrering og opbevaring af oplysninger, er også videregivelse af personoplysninger, herunder navnlig helbredsmæssige oplysninger, mellem myndigheder, omfattet af artikel 8. Videregivelse af helbredsoplysninger til politiet eller domstolene i forbindelse med straffesager, kræver klar retlig regulering, således at det kan sikres, at artikel 8 ikke krænkes[115]. Oplysninger om personers strafbare forhold fra politiet til domstole og andre myndigheder, skal ved videregivelsen være korrekte og fuldstændige[116]. Sker videregivelsen i forbindelse med civile sager, skal denne begrænses mest muligt, og der må kun videregives oplysninger, der er "*strengt nødvendige*" for sagen[117].

Vurderingen af, om indgrebet er foretaget i overensstemmelse af bestemmelsens stk. 2, og dermed ikke udgør en krænkelse, skal bero på, om statens anførte grundlag for indgrebet er relevant og tilstrækkeligt[118]. Det har ved vurderingen betydning, om videregivelsen kan medføre strafansvar eller civilretligt ansvar, og om modtageren af oplysningerne har tavshedspligt[119].

Der må forinden offentliggørelse af oplysninger om enkeltpersoners privatliv foretages en konkret vurdering af, om dette er berettiget. Offentliggørelse af billeder af mistænkte, som er efterlyst, er anset for at være i overensstemmelse med artikel 8. Øvrige billeder, som

[113] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 967
[114] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 969
[115] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 964
[116] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 969
[117] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 964
[118] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 962
[119] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 963

myndigheder offentliggør af tiltalte og sigtede, skal kunne retfærdiggøres i det konkrete tilfælde[120].

Det vil dermed udgøre et indgreb i rettighederne efter EMRK artikel 8, når politiet eller andre myndigheder registrerer, opbevarer eller videregiver oplysninger om privatpersoner, og hvis offentligt tilgængelige oplysninger systematisk indsamles og opbevares i offentlige myndigheders registre. Indgrebet skal retfærdiggøres efter artikel 8, stk. 2, for ikke at være en krænkelse, hvilket indebærer, at det skal leve op til legalitets- og proportionalitetskrav. Legalitets- og proportionalitetskravene skærpes, såfremt der er tale om hemmelig overvågning.

6.1.3. Klass m. fl. mod Tyskland

Afgørelsen Klass m.fl. mod Tyskland er fra 1978, men er stadig relevant i dag på grund af de omstændigheder og udtalelser fra EMD, som afgørelsen indeholder. Gerhard Klass lagde, sammen med fire andre, sag an ved EMD med påstand om, at den tyske lovgivning indeholdt flere retsakter, der udgjorde en krænkelse af deres rettigheder efter EMRK artikel 8 og 13. Den nationale lovgivning gav staten hjemmel til at foretage hemmelig overvågning af post og telekommunikation uden at underrette de overvågede. Underretning af dem, der var blevet overvåget, kunne ske, når en sådan underretning ikke længere ville være til skade for formålet med overvågningen. Problemet bestod i, at dette medførte mange tilfælde, hvor der ikke blev underrettet overhovedet. Derudover var der ikke, efter den tyske lovgivning, mulighed for at klage og få prøvet sin sag vedrørende overvågningen, hvilket klager mente, var en krænkelse af EMRK artikel 13 om retten til effektive retsmidler.

EMD lagde til grund for sin afgørelse, at der forelå indgreb i retten efter artikel 8, og at et sådant indgreb kan finde sted, når der foreligger særlige omstændigheder, er tilstrækkelige garantier for at modvirke misbrug, og hvis indgrebet er nødvendigt i et demokratisk samfund, og forfølger et legitimt hensyn, i dette tilfælde hensynet til den nationale sikkerhed og til at forebygge uro og forbrydelse.

For så vidt angår kravet om, at det skal være nødvendigt i et demokratisk samfund, lagde EMD i denne afgørelse vægt på, at det demokratiske samfund i dag er truet af stadig mere komplekse former for terrorhandlinger, og derfor må det være nødvendigt, at staten har en

[120] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 966

vis adgang til at foretage hemmelig overvågning, jf. dommens pkt. 48. Retten udtalte i denne forbindelse, at hemmelig overvågning af post og telekommunikation under særlige omstændigheder kan være nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed og forebyggelse af uro eller forbrydelse, og dermed ikke udgør en krænkelse af artikel 8.

EMD lagde tillige vægt på, at der skal være tilstrækkelige garantier for at modvirke misbrug, hvilket nærmere konkret indebærer en adgang til effektivt at kunne få prøvet sin sag, samt et uafhængigt tilsynsorgan, der skal føre kontrol med efterretningstjenestens aktiviteter i forbindelse med den hemmelige overvågning. Dette var nødvendigt for at artikel 13 ikke var krænket. Det bemærkedes i denne forbindelse, at effektiv prøvelse ikke kan lade sig gøre, hvis borgeren ikke gøres bekendt med overvågningen, og dermed ikke kan klage, samt at underretning derfor skal ske, så snart dette ikke vil være til fare for formålet med overvågningen.

Overordnet set gjorde EMD i denne afgørelse klart, at indgreb i retten efter artikel 8 kan finde sted på grund af udviklingen i kriminalitetsbilledet, men at der er krav om, *at* der foreligger særlige omstændigheder, *at* det er nødvendigt i et demokratisk samfund og forfølger et legitimt hensyn, *at* der er tilstrækkelige garantier for at modvirke misbrug, herunder et uafhængigt kontrolorgan og mulighed at borgeren kan klage, samt *at* der sker underretning om overvågningen, så snart dette ikke er til fare for efterforskningens formål. Dette lagde EMD i afgørelsen til grund for, at der i denne sag ikke var sket en krænkelse af EMRK artikel 8 eller 13.

6.1.4. Szabó og Vissy mod Ungarn

I dommen Szabó og Vissy mod Ungarn af 12. januar 2016 måtte EMD igen tage stilling til hemmelig overvågning og EMRK artikel 8 og 13.

I denne dom påklagede to ungarske borgere, at den nationale lovgivning omkring hemmelig overvågning i forbindelse med terrorsager var i strid med deres menneskerettigheder. Klagerne menter, at de risikerede at blive ofre for overvågning som ikke var retfærdiggjort efter artikel 8, stk. 2. Centralt i denne afgørelse er spørgsmålet om tilstrækkelige midler til at modvirke misbrug, og det faktum, at overvågningen kunne finde sted uden retlig kendelse.

EMD udtalte i denne afgørelse, som i Klass m.fl. mod Tyskland, at stater anvender moderne teknologi til at bekæmpe terror på grund af udviklingen i kriminalitetsmidler, og at dette var nødvendigt for at bekæmpe den stadig mere komplekse kriminalitet. Dette omfatter også overvågning af borgeres kommunikation for at bekæmpe og forebygge terror. Som nævnt i forbindelse med Klass m.fl. mod Tyskland, er der dog, ved hemmelig overvågning som dette, krav om særlige omstændigheder, streng nødvendighed, et skærpet legalitetskrav, samt krav om tilstrækkelige garantier til at modvirke misbrug, herunder et upartisk kontrolorgan og mulighed for at kunne efterprøve sin sag. Det var på baggrund af kravet om tilstrækkelige retsgarantier til at modvirke misbrug, at EMD fandt, at den ungarske lovgivning herom var i strid med artikel 8, da dette ikke var opfyldt.

EMD lagde vægt på, at der med hjemmel i den omhandlede nationale lovgivning kunne foretages indgreb uden at der forelå en retlig prøvelse, og uden at der skulle foretages en nærmere vurdering af nødvendigheden af indgrebet. Derudover kunne indgreb efter denne lovgivning potentielt påvirke en stor persongruppe, som også omfattede personer, der ikke var mistænkte for en forbrydelse. EMD lagde også vægt på, at der var tendens til at de overvågede personer ikke efterfølgende blev underrettet om, at de havde været overvåget, og dermed ikke havde mulighed for at klage herom. Som før nævnt skal underretning ske, så snart dette ikke bringer formålet med overvågningen i fare.

På baggrund af ovenstående fandt EMD, at der forelå en krænkelse af artikel 8, da den ungarske lovgivning om hemmelig overvågning i forbindelse med terrorsager ikke levede op til kravene i bestemmelsen, fordi lovgivningen ikke var klar nok omkring underretning af overvågede, hvem der måtte overvåges, samt at iværksættelse af overvågningen kunne ske uden en egentlig nødvendighedsvurdering og uden retlig prøvelse.

6.2. Overvejelser om predictive policing i forhold til EMRK artikel 8

Metoden, predictive policing, giver, som det ses, anledning til flere overvejelser i forhold til den menneskeretlige beskyttelse af privatliv mv. I dette afsnit vil muligheden for predictive policing efter politilovens § 2 a blive sammenholdt med EMD's krav til indgreb i privatlivet mv., jf. artikel 8, stk. 2, om særlige omstændigheder, at der er tale om streng nødvendighed

i forhold til legitime hensyn, legalitetskravet og krav om tilstrækkelige garantier for at modvirke misbrug.

Som det fremgår af de to domme, kræver EMD, at der foreligger særlige omstændigheder, hvis politiet skal overvåge borgere, uden at de er klar over det. De særlige omstændigheder, der kan begrunde overvågningen, kan, ifølge de to domme, være terrorisme, idet terrorisme pr. definition udgør en trussel mod det demokratiske samfund. Dermed anerkender EMD, at der kan være et behov for at tage vidtgående metoder i brug for at forebygge og bekæmpe terrorisme. Det danske formål med implementeringen af Pol-Intel og politilovens § 2 a stemmer umiddelbart overens med EMD på dette punkt efter "Et stærkt værn mod terror". Dog synes det formål, som er beskrevet i bemærkningerne til L171 at gå videre end EMD. Som tidligere nævnt, er formålet med anvendelsen af databaseret politiarbejde bredere i lovforslaget og dækker over alle dele af politiets arbejde. Dette må antages at være udtryk for en tilkendegivelse om, at metoden kan anvendes af politiet på flere områder for at effektivisere deres arbejde, også ved mindre forbrydelser. Stadig er det tvivlsomt, hvorvidt der er tale om særlige omstændigheder i EMD's forstand, hvis politiet indsamler og behandler data som led i den borgernære virksomhed, herunder i forbindelse med færdsel eller lokalpoliti.

6.2.1. Streng nødvendighed og legitime hensyn ved hemmelig overvågning

I både Klass m.fl. mod Tyskland og Szabó og Vissy mod Ungarn er der tale om hemmelig overvågning i forbindelse med forebyggelse og bekæmpelse af terror. For at kunne sammenholde disse afgørelser med den danske lovgivning, er det nødvendigt at dataanalyser i Pol-Intel kan sidestilles med politiets hemmelige overvågning for at kunne anvende de to afgørelser til at belyse problemformuleringen. Derfor må det vurderes, om der ved politivirksomhed efter politilovens § 2 a og ved brug af Pol-Intel er tale om hemmelig overvågning.

Pol-Intel medtager store mængder af data i analysearbejdet, hvilket kan understøttes af, at det fremgår af bemærkningerne til L171, at der er behov for, at der i analysen medtages så meget data som muligt[121]. Dette må antageligt begrundes med et ønske om at gøre analyserne

[121] Lovforslag nr. 171 af 29. marts 2017, s. 5

så grundige som muligt og dermed også få de mest præcise resultater, som kan lægges til grund for politivirksomheden. Politiet indsamler og behandler derfor ofte store mængder af data via Pol-Intel, både fra open source-kilder og forskellige registre, og den hyppige forekomst af databehandling vil gøre det uhensigtsmæssigt og tidskrævende, at skulle underrette de berørte personer, hver gang data om disse medtages i analysearbejdet. Det skal hertil også nævnes, at politiet kan have et behov for at hemmeligholde overvågningen af hensyn til efterforskningen, hvilket også var tilfældet i de to afgørelser fra EMD. Det skal også inddrages, at hvis der er tale om tværgående analyser, som lægges til grund for patruljeringsvirksomheden, kan borgerne føle, at de bliver overvåget af de patruljerende betjente, men ikke nødvendigvis være klar over, om patruljeringen baseres på analyser af data om dem, eller på dataanalyser i det hele taget. Dermed må det antages, at Pol-Intel i nogen grad medfører hemmelig overvågning af borgerne i den forstand, at deres personoplysninger medtages i analyser og bliver vurderet af et IT-system med henblik på at forebygge kriminalitet.

I BEK nr. 1078 af 20/09/2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser, findes den retlige regulering af politiets pligt til at informere borgere ved behandling af personoplysninger i Pol-Intel. Denne regulering findes dermed på bekendtgørelsesniveau og ikke på lovniveau, hvilket medfører, at bestemmelserne udstedes af Justitsministeriet, og ikke skal igennem processerne for vedtagelse af lovbestemmelser i Folketinget. I bekendtgørelsens § 12, jf. Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger (herefter: retshåndhævelsesloven) § 16, stk. 4, fremgår det, at borgere ikke har ret til at blive informeret om behandling af oplysninger i Pol-Intel efter bekendtgørelsens §§ 15 og 13, stk. 2. Udsættelse, benægtelse eller begrænsning af indsigt i politiets behandling af oplysninger kan ske efter Retshåndhævelseslovens § 16, stk. 1, når borgerens interesse burde vige for visse hensyn til offentlige interesser. Disse interesser er oplistet i lovens § 14, og omfatter (1) for at undgå hindring af offentlige eller retlige undersøgelser, efterforskninger mv., (2) for at undgå at skade forebyggelse, afsløring, efterforskning, retsforfølgning af kriminelle forhold, eller for at beskytte (3) den offentlige sikkerhed, (4) statens sikkerhed, eller (5) borgeres rettigheder. Det må dermed antages, at politiet ikke skal informere borgerne om behandling af persondata i Pol-Intel, hvis undladelse, udsættelse mv., forfølger et af de i bestemmelsen nævnte hensyn.

Som også belyst af EMD i de to afgørelser kan der være udfordringer ved hemmelig overvågning, idet en borger reelt ikke vil kunne påklage overvågningen, da vedkommende ikke er bekendt med denne. Manglen på dansk retspraksis på dette område kan derfor være et udtryk for mangel på viden om overvågningen, og ikke at denne ikke medfører, at borgere føler, at deres menneskerettigheder krænkes. Dette skal ses i sammenhæng med, at EMD har slået fast, at underretning af den eller de overvågede skal ske, så snart dette ikke sætter efterforskningen på spil. Hensynene er i nogen grad sammenfaldende med de hensyn, der kan legitimere indgreb efter EMRK artikel 8, stk. 2. Bekendtgørelsens oplistning af hensyn, der kan legitimere hemmelig overvågning i Pol-Intel, skal ses i lyset af kravet om klar hjemmel og forfølgelse af et legitimt hensyn, som kan retfærdiggøre et indgreb i retten efter EMRK artikel 8.

I afgørelserne er der tale om hensynet til den offentlige sikkerhed og forebyggelse af forbrydelse og uro, og EMD har som før nævnt fastslået, at der ved hemmelig overvågning skal være tale om streng nødvendighed, hvilket medfører en skærpelse i forhold til det sædvanlige nødvendighedskrav.

Anvendelsen af Pol-Intels dataanalyser varetager, ifølge bemærkningerne til L171, hensynet til den offentlige sikkerhed, den offentlige tryghed eller forebyggelse af uro og forbrydelse[122]. Ved vurderingen af, om indgrebet efterlever nødvendighedskravet, skal der tages stilling til, om der er tilstrækkelig og relevant begrundelse for hemmelig overvågning. Ved Pol-Intels analysearbejde vil det dog i praksis give anledning til at overveje, hvordan det kan sikres, at nødvendighedsvurderingen sikrer borgernes rettigheder i forhold til hemmelig overvågning og overvågning i det hele taget. Dette skal ses i lyset af, at politiets medarbejdere ikke på samme måde kan forsvare, forklare og give indsigt i IT-systemets arbejdsmetoder, medmindre de har opnået fuld teknisk og praktisk forståelse herfor, som også før beskrevet. Når streng nødvendighed er et krav for at kunne registrere og behandle oplysninger om borgere, uden at de er klar over det, må der være foranstaltninger, der sikrer at nødvendighedsvurderingen lever op til EMD's krav.

[122] Lovforslag nr. 171 af 29. marts 2017, s. 15

6.2.2. Legalitet og kravet om tilstrækkelige midler til at modvirke misbrug

For så vidt angår legalitetskravet, har EMD fastslået, at der skal være klar hjemmel til at foretage hemmelig overvågning, herunder at der skal være begrænsninger til de indsamlede oplysningers karakter, hvem der må overvåges, hvilket betingelser der skal være opfyldt og krav til sletning. Disse regler om databehandling i Pol-Intel findes på bekendtgørelsesniveau, og bekendtgørelsen giver Rigspolitiet kompetence til at fastsætte yderligere bestemmelser internt. Det giver anledning til tvivl om, hvorvidt legalitetskravet er opfyldt, når bestemmelserne ikke findes på lovniveau, og nogle af reglerne tilmed udstedes internt i politiet. Det er fastslået i praksis, at også administrative forskrifter, uskrevet ret og retspraksis kan opfylde EMD's legalitetskrav, og derfor må det antages, at dette er opfyldt[123].

EMD stiller desuden krav om tilstrækkelige garantier for at modvirke misbrug. Dette indebærer helt konkret, at der sker løbende kontrol med overvågningsvirksomheden, og at der er adgang til et uafhængigt klageorgan. For så vidt angår løbende kontrol, fremgår det af førnævnte bekendtgørelses § 14, at Rigspolitiet skal foretage logning af behandlinger af personoplysninger i Pol-Intel med henblik på løbende kontrol med legitimiteten, integriteten og sikkerheden af personoplysningerne. Ifølge bestemmelsens stk. 2 skal Rigspolitiet desuden foretage yderligere logning for at understøtte proaktiv monitering af legitimiteten af databehandlingen. Det er ifølge § 15 Rigspolitiet, der skal fastsætte interne retningslinjer for adgang til, og behandling af, personoplysninger i Pol-Intel, samt foretage stikprøvekontrol i forhold til logning efter § 14. Som følge heraf er det Rigspolitiet, der har ansvaret for den løbende kontrol af overvågningsvirksomheden. Det kan diskuteres, hvorvidt dette lever op til EMD's krav, idet den løbende kontrol med Pol-Intel ikke foretages af et eksternt organ, men internt i politiet. Dette kan alt andet lige give borgere en følelse af, at de ikke kan vide sig sikre på, at denne kontrol føres i en sådan grad, at deres rettigheder sikres.

Dette er dog et krav i forhold til efterprøvelse af klagesager om hemmelig overvågning. Her skal borgere kunne få deres sag prøvet ved en uafhængig myndighed. Hvis borgeren skal have mulighed for at klage, er det en forudsætning, at vedkommende er blevet informeret om, at overvågning finder eller har fundet sted. Klager over politiets arbejde kan finde sted til Den Uafhængige Politiklagemyndighed, hvorfor dette krav må antages at være opfyldt.

[123] Ivashchenko mod Rusland (afgørelse nr. 61064/10 af 13. februar 2018), pkt. 71

Hertil skal det i øvrigt bemærkes, at EMD i Klass m.fl. mod Tyskland har slået fast, at manglende underretning af borgere om, at de bliver eller er blevet overvåget, ikke i sig selv kan udgøre en krænkelse af artikel 8.

Hvorvidt den danske lovgivning lever op til EMD's krav om tilstrækkelige garantier for at modvirke misbrug, skal ses i lyset af, at der ikke findes et eksternt kontrolorgan til løbende kontrol, samt at reglerne herom både skabes og efterleves internt i politiet. Dette kan tale for en vis grad af usikkerhed i forhold til, om misbrug reelt modvirkes med de garantier, der er.

6.2.3. Udenretlige beslutningsbeføjelser

I Vissy og Szabó mod Ungarn fastslog EMD, at politiets hemmelige overvågning ikke levede op til kravene i artikel 8, stk. 2, på grund af mangelfuld lovgivning. EMD lagde i afgørelsen vægt på, at beføjelserne til at foretage hemmelig overvågning var for vidtgående, idet der ikke var krav om retskendelse. Beslutning om hemmelig overvågning blev efter den ungarske lovgivning dermed taget uden om retten. Dette er relevant i forhold til, hvornår Pol-Intels tværgående analyser kan tages i brug.

Efter politilovens § 2 a kan indsamling og behandling af personoplysninger og andre oplysninger ske, når det er nødvendigt af hensyn til politiets opgaver. Dette skal bero på en politifaglig vurdering i det konkrete tilfælde[124]. Det må derfor antages, at vurderingen af, om der skal foretages tværgående analyser i det konkrete tilfælde, delvist tillægges politiets medarbejdere. Det er i denne forbindelse uklart, hvorvidt Pol-Intel selv vurderer, om der skal foretages tværgående informationsanalyser, herunder om analysearbejdet altid baseres på menneskelige beslutninger, eller om IT-systemet selv er beslutningstager. Dermed kan vurderingen siges at foregå udenretligt, hvilket EMD havde fokus på i Szabó og Vissy mod Ungarn. I dette tilfælde var det Justitsministeren, der skulle vurdere, om hemmelig overvågning skulle iværksættes, hvilket EMD fandt ikke levede op til kravene i artikel 8, da hemmelig overvågning dermed kunne ske uden retskendelse. Dette er relevant, både fordi vurderingen delvist er pålagt politiets medarbejdere, og fordi en del af reglerne om anvendelse og sletning af oplysninger i Pol-Intel er fastsat administrativt af Justitsministeriet og tillige af Rigspolitiet internt i politimyndigheden.

[124] Lovforslag nr. 171 af 29. marts 2017, s. 15

Sammenholdes den ungarske retlige regulering og EMD's udtalelser i disse afgørelser med de danske retlige rammer for hemmelig overvågning i form af tværgående analyser i Pol-Intel, som kan lægges til grund for størstedelen af politivirksomheden i Danmark, vil reguleringen af dette i Danmark antageligt være mangelfuld.

6.2.4. Overvejelser i forhold til de fire beskyttelsesinteresser

Ovenstående afsnit omhandler problematikkerne ved predictive policing i lyset af afgørelserne fra EMD, og dette afsnit vil sammenholde muligheden for at foretage tværgående analyser i Pol-Intel efter politilovens § 2 a og borgerens oplevelse heraf med de fire beskyttelsesinteresser i artikel 8.

For så vidt angår retten til privatliv, er det relevant at tage stilling til, hvorvidt Pol Intels analysearbejde kan udgøre en krænkelse af artikel 8. Dette er særligt interessant i forhold til, når dataanalyser bliver lagt til grund for den borgernære politivirksomhed. Retten til privatliv omfatter som nævnt retten til at udvikle sig og til at etablere sociale relationer. Dette kan være problematisk, hvis viden om politiets øgede tilstedeværelse kan resultere i, at borgere føler sig nødsaget til at blive hjemme for at undgå at blive overvåget. Beboere i boligområder med meget kriminalitet risikerer at blive ramt af dette, også selvom de ikke selv deltager i kriminelle aktiviteter, og netop derfor ikke ønsker at blive overvåget på lige fod med de beboere, der deltager i kriminelle aktiviteter. Sker der øget tilstedeværelse af politiet på gaden i et lokalområde, kan dette dermed påvirke borgernes privatliv ved, at de må indrette sig efter politiet for at undgå overvågning. Dette skal også ses i lyset af, at denne beskyttelsesinteresse omfatter retten til at leve uden uønsket opmærksomhed. Øget patruljering i et område, hvor der er meget kriminalitet, vil antagelig ikke være et engangstilfælde, men vil være noget, der foregår over længere tid og muligvis af flere omgange, idet Pol-Intel på baggrund af de indhentede oplysninger må antages at blive ved med at udpege det samme område. Beboerne i området vil dermed til en vis grad ikke kunne leve i fred og uden uønsket opmærksomhed, som artikel 8 sikrer dem retten til.

Retten til familieliv omfatter blandt andet retten til at have relationer til ægtefæller, familiemedlemmer eller andre nærtstående, hvor forhold bærer præg af at være varigt, eksempelvis hvis personerne har forpligtet sig over for hinanden. Dette er relevant, da predictive policing medfører en risiko for, at borgere ikke længere kan få besøg af deres familiemedlemmer, hvis de bor i et udsat boligområde, uden at familiemedlemmerne også

kan risikere at blive overvåget på grund af relationen eller tilstedeværelsen. Det kan også medføre, at man risikerer at blive udpeget af Pol-Intel, hvis man er i familie med en, der deltager i kriminelle aktiviteter, selvom man ikke selv gør det.

Med retten til respekt for hjemmet, beskyttes de fysiske rammer, som en borger sætter for sit privatliv. Retten til at leve uforstyrret og i fred er omfattet af denne beskyttelsesinteresse, hvis indgrebet sker i hjemmet. Gentagelse af indgreb foretaget af politiet på baggrund af Pol-Intels tværgående informationsanalyser, indebærer risiko for, at politivirksomheden bærer præg af chikanering af visse borgere, som dermed ikke kan leve uforstyrret i deres eget hjem. Dette gælder, uanset om der er tale om et hjem i traditionel forstand eller ej, idet der blot er krav om, at personen har en varig og tilstrækkelig tilknytning til et bestemt sted. Et eksempel herpå kan være, når hjemløse holder til på et bestemt sted, som er offentligt tilgængeligt. Såfremt tilknytningen til stedet er tilstrækkelig og varig, og politiet øger patruljeringen på området som resultat af en tværgående analyse i Pol-Intel, er der en risiko for, at dette udgør en krænkelse.

For så vidt angår beskyttelse af korrespondance, omfatter dette overvågning af kommunikation, som er gennemgået i forbindelse med de to afgørelser, og vil derfor ikke vil blive uddybet yderligere her.

6.3. Artikel 14: Retten til ikke at blive diskrimineret

> *The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a nation minority, property, birth or other status.*

Således lyder EMRK artikel 14, som sikrer retten til ikke at blive diskrimineret. Kjølbro opstiller en række forhold, der skal tages stilling til ved vurderingen af, om en stat har krænket en borgers ret efter denne bestemmelse. Vurderingen indebærer en stillingtagen til følgende: (1) om der er sket forskelsbehandling i forbindelse med en rettighed, som er beskyttet i EMRK, (2) om forskelsbehandlingen er sket i sammenlignelige situationer, (3) om den er sagligt begrundet og proportional[125].

[125] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1277

Hvor der i artikel 8 er tale om en positiv forpligtelse for staten, er der i artikel 14 tale om en negativ forpligtelse til ikke at diskriminere. Hertil kommer også visse positive forpligtelser til at sikre borgerne mod diskrimination, hvilket dog ifølge Kjølbro spiller en beskeden rolle i praksis. En positiv forpligtelse for staten efter denne bestemmelse kan eksempelvis være at sikre faktiske uligheder, beskytte voldsofre, når volden eller overgrebet er sket med racistiske eller religiøse motiver eller at reagere på racediskriminerende udtalelser, racistisk motiverede voldshandlinger, og vold mod kvinder i hjemmet mv. Statens positive forpligtelser efter artikel 14 kan også bestå i at beskytte ofre for politiets mishandling ved at foretage tilstrækkelig efterforskning, når påstanden om, at politiet har handlet politisk motiveret, er rimeligt begrundet[126]. Staten kan efter denne bestemmelse også have en pligt til at beskytte borgere imod usaglig afskedigelse og til at sikre, at handicappede personer har adgang til uddannelsesinstitutioner og lignende ved eksempelvis at foretage fysiske tilpasninger[127].

6.3.1. Diskriminationsbegrebet

Ved diskrimination efter artikel 14 forstås forskelsbehandling i sammenlignelige situationer, der ikke er rimeligt og objektivt begrundet. Forskelsbehandlingen skal som følge heraf varetage et legitimt eller anerkendelsesværdigt formål og være proportional hermed for ikke at udgøre en krænkelse af EMRK artikel 14. Det påhviler staten at bevise, at forskelsbehandlingen er retfærdiggjort, og skønsmarginen varierer alt efter sagens omstændigheder. Det skal indgå i vurderingen, hvilken gruppe af personer, der er berørt. Det taler for diskrimination, hvis der er tale om persongrupper, der i forvejen er særligt udsatte eller sårbare[128].

Diskriminationsgrundene fremgår af bestemmelsens ordlyd. Dette omfatter således "*køn, race, sprog, religion, politisk eller anden overbevisning, national eller social oprindelse, tilhørsforhold til et nationalt mindretal, formueforhold, fødsels eller ethvert andet forhold*", og forskelsbehandlingen skal være sket i forbindelse med en "*identificerbar, objektiv eller personlig karakteristik eller kendetegn eller forhold*"[129]. At der i bestemmelsen står "*ethvert andet forhold*" skal forstås således, at diskriminationsgrundene ikke udtømmende er oplistet

[126] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1277
[127] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1278
[128] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1287
[129] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1288 f.

i bestemmelsen. Dette skal fortolkes udvidende, og kan være personlige forhold, herunder seksuel orientering, fysisk handicap, og EMD har ligeledes anerkendt bopæl, opholdstilladelse, statsborgerskabs længde, helbredstilstand, militær rang, og andre forhold som diskriminationsgrunde[130].

Hvis forskelsbehandling sker på grund af køn, kræves der, for at retfærdiggøre dette, "*meget tungtvejende og overbevisende grunde*", idet ligestilling mellem køn, ifølge EMD, anses som et af de vigtigste mål for medlemsstaterne i Europarådet[131]. Hverken traditioner, generelle antagelser, social opfattelse eller budgetmæssige årsager kan lægges til grund for forskelsbehandling på baggrund af køn[132].

Forskelsbehandling på grund af nationalitet er også omfattet af EMRK artikel 14, også selvom det ikke fremgår udtrykkeligt af bestemmelsens ordlyd. Dog nævnes "national oprindelse" og "tilhørsforhold til nationalt mindretal" som diskriminationsgrunde i bestemmelsen. Såfremt forskelsbehandlingen er sket udelukkende på grund af nationalitet, kræves der tvingende eller meget tungtvejende grunde for at retfærdiggøre dette[133]. Det samme gør sig gældende, hvis forskelsbehandlingen finder sted på baggrund af national oprindelse[134]. Det samme gør sig også gældende, hvis det er på baggrund af religion[135] eller seksuel orientering[136]. Sker der forskelsbehandling på grund af bopæl, kan det udgøre diskrimination i strid med artikel 14. Dette vil dog være lettere at retfærdiggøre, end hvis diskriminationsgrunden er eksempelvis race eller national oprindelse, idet borgere selv vælger, hvor de vil bo[137]. Hvis forskelsbehandlingen sker på baggrund af "tilhørsforhold til et nationalt mindretal" eller "race eller etnisk oprindelse", vil der som udgangspunkt være tale om diskrimination i strid med artikel 14[138]. Ifølge EMD kan ingen forskelsbehandling retfærdiggøres i et demokratisk samfund, hvis forskelsbehandlingen alene eller i afgørende grad direkte eller indirekte er sket på grund af etnisk oprindelse. Det er dog ofte i tilfælde af indirekte forskelsbehandling på grund af nationalitet, race, etnisk oprindelse eller lignende

[130] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1289
[131] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1290
[132] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1291
[133] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1296
[134] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1299
[135] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1306
[136] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1310
[137] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1299
[138] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1301

svært for klager at opfylde konventionens beviskrav, altså at bevise uden for enhver rimelig tvivl, at der er sket forskelsbehandling[139]. Det er generelt reglen, at hvis der rejses påstand om, at en stat har handlet med politiske eller racistiske motiver, skal dette bevises "uden for enhver rimelig tvivl", og der skal ses på konteksten, handlingerne, og påstanden skal være støttet af objektive momenter[140].

Hvis der er tale om racistisk motiveret vold eller overgreb på grund af race, etnisk oprindelse mv., er dette ifølge EMD en "*særlig fornærmelse mod den menneskelige værdighed*", og derfor er der krav til myndighederne om, at der udvises særlig årvågenhed og reageres energisk[141]. Staten har efter EMRK artikel 2 og 3 en pligt til at indlede en undersøgelse i forbindelse med vold, men denne pligt er, ifølge EMD, skærpet, når der er mistanke om, at volden er racistisk motiveret[142]. Hvis staten ikke opfylder denne pligt, vil der foreligge en krænkelse af artikel 14. Den skærpede pligt begrundes med, at myndigheder skal styrke minoriteters tillid til, at de ikke vil blive udsat for racisme og etnicitetsbaseret had[143].

Foranstaltninger, der rammer en bestemt gruppe af borgere hårdere end andre, udgør, ifølge Kjølbro, ikke i sig selv forskelsbehandling. Statistiske oplysninger kan give en formodning herfor, men dog ikke i sig selv begrunde diskrimination, og herefter er bevisbyrden statens[144].

6.3.2. Beskyttelsens omfang

Omfanget af beskyttelsen i artikel 14 er begrænset til de rettigheder, som konventionen indeholder, og vil altid skulle anvendes i samspil med en eller flere bestemmelser i EMRK[145]. Der må dermed ikke ske diskrimination i forhold til konventionens anerkendte rettigheder, herunder retten til respekt for privatliv, familieliv, hjem og korrespondance, som er beskrevet ovenfor.

Der kan foreligge diskrimination selvom ingen af de øvrige rettigheder er krænket, og der er hverken krav om at klager fremlægger en påstand herom, eller at EMD fastslår at dette er

[139] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1302
[140] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1287 f.
[141] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1305
[142] Ibid.
[143] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1305 f.
[144] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1304
[145] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1278

tilfældet. Det er tilstrækkeligt, at der nedlægges påstand om, at der er sket forskelsbehandling, og at forskelsbehandlingen "*vedrører et forhold, der er omfattet af en af de øvrige materielle bestemmelser*"[146]. Hvis der ved EMD fastslås at foreligge en krænkelse efter en af de øvrige bestemmelser, vil det kun være relevant at tage stilling til, om der foreligger diskrimination, hvis dette er et centralt element i klagen[147].

6.3.3. Sammenlignelige situationer

Det skal indgå i vurderingen af, hvorvidt der foreligger diskrimination efter artikel 14, om der er andre i sammenlignelige eller identiske situationer, som får en mere fordelagtig behandling, og om der i så fald er en objektiv og rimelig begrundelse herfor[148]. Dette er klagers pligt at godtgøre[149]. Det er dermed omfattet af forbuddet mod diskrimination, hvis en stat behandler flere sammenlignelige eller ens tilfælde forskelligt. Omvendt er det også omfattet af diskriminationsforbuddet, hvis en stat behandler forskellige situationer ens[150].

Forskelsbehandlingen kan være direkte eller indirekte. Hvis der er tale om direkte forskelsbehandling, følger denne af ordlyden af en retsregel eller begrundelsen for en myndighedsafgørelse. Hvis forskelsbehandlingen er indirekte, er den forårsaget af neutrale regler, herunder hvis en generel politik eller foranstaltning medfører uforholdsmæssigt negative resultater for en bestemt persongruppe, også selvom det ikke er hensigten med foranstaltningen at påvirke denne gruppe af borgere. Det er dog stadig et krav, at forskelsbehandling er rimeligt og objektivt begrundet[151].

EMRK artikel 14 indeholder således et forbud mod direkte eller indirekte diskrimination. Diskrimination finder sted, når der er sket forskelsbehandling i sammenlignelige situationer på baggrund af de i bestemmelsen oplistede diskriminationsgrunde, og forskelsbehandlingen ikke kan retfærdiggøres. Retfærdiggørelse af forskelsbehandling finder sted, når forskelsbehandlingen er sket for at forfølge et legitimt og anerkendelsesværdigt formål, og er proportional.

---

[146] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1278 f.
[147] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1279
[148] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1283
[149] Ibid.
[150] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1286
[151] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1286 f.

6.4. Overvejelser om predictive policing i forhold til EMRK artikel 14

Uanset om der i det konkrete tilfælde er sket en krænkelse af artikel 8 eller 13, kan der være en risiko for, at der er sket en krænkelse af artikel 14, såfremt predictive policing medfører forskelsbehandling, som ikke kan retfærdiggøres efter bestemmelsens stk. 2. I forhold til diskriminationsforbuddet giver predictive policing anledning til flere forskellige overvejelser, som her vil blive gennemgået.

Risikoen for bias og forudindtagelse ved anvendelse af predictive policing er gennemgået i afsnit 5.5.2. Dette skal ses i sammenhæng med EMRK artikel 14, idet en algoritme, der potentielt er forudindtaget, potentielt vil have et uproportionalt fokus på de i forvejen udsatte grupper i samfundet. Dette er belyst af Couchman i Liberty rapporten, der beskriver de udsatte grupper som dem med anden etnisk baggrund og dem med lav indkomst[152]. Når forskelsbehandling rammer persongrupper, der i forvejen er udsatte eller sårbare, taler dette ifølge Kjølbro for diskrimination[153]. Såfremt Pol-Intel har de samme tendenser, som er beskrevet af Couchman, og som er set i England, vil det tale for diskrimination, hvis de udsatte grupper i Danmark, rammes i højere grad end andre af predictive policing. Hertil kommer, at forskelsbehandling skal retfærdiggøres efter artikel 14, herunder om den er proportional og sagligt begrundet.

Det er som nævnt borgeren, der skal bevise, at der er sket forskelsbehandling i sammenlignelige situationer. Hertil opstår spørgsmålet, om en borger ved predictive policing er i en position, hvor vedkommende har mulighed for at indse, at der sker forskelsbehandling, når det er begrænset, hvor meget indsigt, der er at få i Pol-Intels arbejde. Det må antages, at det er muligt for borgere at indse, hvis der patruljeres oftere i deres boligområde, men udfordringen opstår, når det skal fastslås, hvorfor dette er tilfældet. Politiet har længe kunnet målrette patruljeringen efter egne erfaringer, eksempelvis, hvis de har kendskab til et boligområde, hvor der som regel er problemer i weekenderne, og de derfor vælger at sende patruljer derud for at forebygge eller for hurtigt at kunne reagere. Grænsen mellem dette og predictive policing er ikke klar, men det må antages, at beslutningsprocessen bag patruljeringen udgør forskellen. Hvis politiet ud fra erfaringer om øget kriminalitet

[152] Hannah Couchman: "*Policing by Machine*", 2019, s. 7
[153] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1287

sender patruljer ud i et bestemt boligområde, sker dette på grund af antagelser om, at kriminalitet vil forekomme, hvilket ikke omfattes af artikel 14. De oplistede diskriminationsgrunde står ikke i vejen for forebyggende politivirksomhed. Udfordringen i forhold til diskrimination opstår, hvis Pol-Intels analysearbejde baseres på en algoritme, der lægger national oprindelse, indkomst-niveau, religion, seksuel orientering, nationalt mindretal, eller andre diskriminationsgrunde til grund for politiets patruljering. Hvis nationalt mindretal, etnisk oprindelse eller race er årsag til forskelsbehandling, er udgangspunktet, som nævnt, at der er sket en krænkelse af artikel 14[154]. Der kan her sættes spørgsmålstegn ved, hvor meget man egentlig ved om, hvad Pol-Intel medtager i sine beregninger, og hvad der lægges til grund for dataanalyserne.

Hvis en eller flere borgere kan bevise, at der er sket forskelsbehandling i sammenlignelige situationer, er det herefter statens opgave at bevise, at forskelsbehandlingen er retfærdiggjort, herunder om den forfølger et legitimt formål, og er proportional. Dette vil kræve, at politiet kan redegøre for Pol-Intels analysearbejde, herunder hvad der er årsag til øget patruljevirksomhed i det pågældende område. Det vil antageligt ikke være uden udfordringer for politiet at redegøre for, samt at føre kontrol med, at Pol-Intel opretholder transparens i dataanalyserne. Såfremt beslutningen reelt er taget af Pol-Intel og ikke at mennesker, vil det være svært for politiet at forsvare beslutningen.

6.4.1. Erfaringer med predictive policing i Storbritannien

I Couchmans rapport tages udgangspunkt i anvendelsen af predictive policing i politiet i Storbritannien. Det har her været anvendt i flere år, og rapporten belyser blandt andet udfordringerne i forhold til EMRK artikel 14, og forholder sig kritisk hertil. I Storbritannien findes predictive policing i form af "*individual risk assessment*"-programmer og "*predictive mapping*"-programmer.

Individual risk assessment-programmer evaluerer og analyserer data vedrørende menneskers adfærd med fokus på, hvor store chancer der er for, at en person vil udføre en kriminel handling eller blive offer for en[155]. Et eksempel er programmet Harm Assessment Risk Tool (HART), som anvendes i Durham Police. Dette program bruger 34 forskellige slags data om en person for at regne ud, hvor store chancerne er, for at personen vil udføre en kriminel

[154] Jon Fridrik Kjølbro: "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", 2020, s. 1301
[155] Hannah Couchman: "*Policing by Machine*", 2019, s. 4

handling inden for 2 år. 29 ud af de 34 former for data omhandler personens fortid inden for kriminalitet, og de resterende handler om personens øvrige karakteristika, herunder boligområde, postnummer og etnicitet. Herefter får

personen en score, som er enten lav, middel eller høj, og programmet er her indrettet til at overvurdere frem for at undervurdere[156].

I april 2018 kom det frem, at HART får data fra et selskab kaldet Experian via et system, der hed Mosaic. Dette system indsamlede demografiske oplysninger og klassificerede befolkningen i England i forskellige grupper, herunder "*crowded kaleidoscope*", som er dem med lav indkomst, og "*multi-cultural*", som er familier med høj indkomst, men som bor i det, der bliver kaldt "*cramped houses*" eller "*overcrowded flats*"[157]. Der bliver også draget paralleller mellem visse navne og egenskaber, eksempelvis navnene Terrence og Denise, som angiveligt skulle være "*low income workers*", og folk med navnene Terrence og Denise blev derfor på baggrund af deres navn, vurderet til at være borgere med lav indkomst[158].

Individual risk assessment-programmer henholder sig dermed til personer, og udfordringerne i forhold til EMRK artikel 14 opstår i forbindelse med, hvilke oplysninger om personerne, der lægges til grund for algoritmens analyseresultater.

Predictive mapping-programmer evaluerer og analyserer data fra politiets systemer og udpeger hot spots. Her kan potentielt opstå diskrimination, da der er risiko for over-policing, og folk, der bor i disse områder, vil opleve politiets tilstedeværelse i højere grad end andre[159]. Dette kan sammenlignes med formålet med Pol-Intel i forhold til patruljeringsvirksomheden og det borgernære politi, hvorefter Pol-Intels dataanalyser skal anvendes til at prioritere patruljeringsvirksomheden.

I rapporten anbefales det ikke at anvende disse programmer pga. risiko for over policing og diskrimination[160]. Det anbefales i øvrigt at sikre transparens, samt at implementere digitale værktøjer, der kan modvirke bias, og desuden at udvikle en "*human rights impact assessment*", som skal offentliggøres, og hvor der tages stilling til de risici, predictive policing medfører i forhold til menneskerettighederne[161]. Det samme kan henføres til det

[156] Hannah Couchman: "*Policing by Machine*", 2019, s. 5
[157] Ibid.
[158] Hannah Couchman: "*Policing by Machine*", 2019, s. 6
[159] Hannah Couchman: "*Policing by Machine*", 2019, s. 3 f.
[160] Hannah Couchman: "*Policing by Machine*", 2019, s. 10
[161] Hannah Couchman: "*Policing by Machine*", 2019, s. 10 f.

danske politis anvendelse af predictive policing, da der ikke, så vidt ses, er taget stilling til EMRK artikel 14 ved implementeringen af Pol-Intel og politilovens § 2 a. En sådan stillingtagen må anses for at være nødvendig, da § 2 a og Pol-Intel giver politiet muligheder, der i høj grad minder om de muligheder, det britiske politi har, og risikoen for krænkelse af EMRK artikel 14 ses tydeligt i Couchmans rapport, for så vidt angår det engelske politi. Anvendelse af predictive policing i Danmark vil dermed kræve, at der tages stilling til, og iværksættes foranstaltninger for at modvirke krænkelse af artikel 14.

Rapporten skal ses i lyset af, at Liberty er en borgerrettighedsgruppe, og dermed er rapporten holdningspræget. Dog kan man med fordel bruge rapportens nævnte anbefalinger i forhold til at sikre, at der med politilovens § 2 a og Pol-Intel ikke forekommer diskrimination.

7. Konklusion

Fremstillingens problemformulering er søgt belyst gennem de tre underspørgsmål, der lyder som følgende: (1) Anvendes predictive policing i Danmark? (2) Hvad er den retlige regulering af predictive policing i Danmark? (3) Er der taget stilling til de menneskeretlige aspekter? Disse spørgsmål vil blive besvaret nedenfor hver for sig.

7.1. Anvendes predictive policing i det danske politi?

Der findes ikke et klart svar på, hvorvidt predictive policing anvendes i Danmark. Dette kan begrundes med flere ting. Predictive policing ville være en del af politiets interne processer, og såfremt det anvendes i dansk politi, ville borgere antageligt ikke være klar over det, idet der ikke er kommet en officiel udmelding om, at metoden kan tages i brug. Det kan fastslås, at politiet har haft hjemmel i politilovens § 2 a til at udøve predictive policing siden bestemmelsen blev indført i 2017, men det kan ikke fastslås, hvorvidt politiet har udnyttet denne hjemmel. Dog kan det udledes af formålet med bestemmelsen, som fremgår af bemærkningerne til lovforslaget L171, at der er et ønske om at anvende metoden. Formålet med lovforslaget er en øget og forbedret IT-anvendelse i politiet, og ved hjælp af Pol-Intel at sammenkøre data fra forskellige registre til brug for det forebyggende politiarbejde, samt at kunne anvende dataanalyser i stort set alle dele af politiets virksomhed.

Det danske politi har i 2017 fået værktøjet, Pol-Intel, som kan foretage de dataanalyser, som kan lægges til grund for predictive policing. Dermed har politiet de tekniske og retlige muligheder for at udøve predictive policing, men ikke offentliggjort, hvorvidt de rent faktisk gør det.

7.2. Hvad er den retlige regulering af predictive policing i Danmark?

Den retlige regulering af predictive policing findes i politilovens § 2 a, og i bekendtgørelser, som har hjemmel i § 2 a, stk. 3, samt i interne regelsæt, som Rigspolitiet udsteder. Reguleringen af predictive policing synes fleksibel, idet størstedelen af de konkrete bestemmelser findes i bekendtgørelser. § 2 a giver en bred og overordnet hjemmel til

predictive policing på trods af, at metoden ved implementeringen eller i bestemmelsens ordlyd ikke er nævnt ved navn. På grund af bestemmelsens brede karakter, og formålet, som er beskrevet i bemærkningerne til L171, kan predictive policing foretages med hjemmel politilovens § 2 a. Politiet kan efter den danske regulering foretage tværgående analyser i Pol-Intel, som kan lægges til grund for politiets arbejde. Behandling af personoplysninger i Pol-Intel kan ske, når det lever op til de oplistede formål i § 4 i BEK nr. 1078/09/2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser. På denne baggrund er der sket en væsentlig udvidelse af formålet med anvendelse af dataanalyser, siden det først blev omtalt i regeringen udspil fra 2015, "Et stærkt værn mod terror", hvor det kun skulle anvendes i forbindelse med terrorhændelser og andre meget alvorlige forbrydelser.

Behandling af data i Pol-Intel kan ske uden underretning af de omhandlede personer efter retshåndhævelseslovens § 16, stk. 4, når borgerens interesse burde vige for de offentlige hensyn, der er oplistet i lovens § 14. Dette vil overordnet set medføre en lang række tilfælde, hvor borgere ikke skal informeres, hvis deres oplysninger er medtaget i informationsanalyser i Pol-Intel.

7.3. Er der taget stilling til EMRK i forhold til predictive policing i Danmark?

Anvendelse af dataanalyser som dem i Pol-Intel er af EMD blevet anerkendt som værende i overensstemmelse med EMRK artikel 8 i forbindelse med hemmelig overvågning i afgørelserne Klass m.fl. mod Tyskland og Szabó og Vissy mod Ungarn, hvis det lever op til kravet om, at der foreligger særlige omstændigheder, et skærpet krav om *streng* nødvendighed, et skærpet legalitetskrav, og at der skal være tilstrækkelige midler til at modvirke misbrug, herunder løbende kontrol og mulighed for borgeren for at påklage overvågningen. Dette vil kræve, at borgeren på et tidspunkt blive informeret om, at overvågningen har fundet sted.

Der er i bemærkningerne til L171 taget stilling til EMRK artikel 8, og i den forbindelse er kravene i artikel 8, stk. 2, gennemgået og § 2 a herefter retfærdiggjort. Gennemgangen er dog meget overordnet, og synes ikke at tage stilling til de ting, EMD har taget stilling til i de to nævnte afgørelser. Det samme gør sig gældende i forhold til bias, og hvordan transparens

kan sikres i Pol-Intel. Der er dermed kun i begrænset omfang taget stilling til artikel 8 ved implementeringen af § 2 a.

Så vidt ses, er der ikke taget stilling til politilovens § 2 a i forhold til EMRK artikel 14 om retten til ikke at blive diskrimineret, eller risikoen for over-policing. Dette kan medføre menneskeretlige udfordringer, henset til de erfaringer, der har været med lignende politivirksomhed i udlandet, hvor risiko for diskrimination har været genstand for debat.

9. Litteraturfortegnelse

9.1. Litteratur

- Henricson, Ib "*Politiret*"
  Jurist- og Økonomforbundets Forlag, 2020
- Kjølbro, Jon Fridrik "*Den Europæiske Menneskerettighedskonvention for Praktikere*"
  Jurist- og Økonomforbundets Forlag, 2020
- Couchman, Hannah "*Policing by Machine*"
  Rapport fra Liberty, 2019
- Volquartzen, Mette "*Forskydninger mellem det private og det offentlige*" Kapitel i "Ret SMART: Om smart teknologi og regulering" af Rønne og Stevnsborg
  Jurist- og Økonomforbundets Forlag, 2018
- Munk-Hansen, Carsten "*Retsvidenskabsteori*"
  Jurist- og Økonomforbundets Forlag, 2014
- "*Et stærkt værn mod terror – 12 nye tiltag mod terror*"
  Regeringens udspil fra 2015

9.2. Retskilder

- **EMRK**
  Den Europæiske Menneskerettighedskonvention
- **Politiloven**
  Lov nr. 444 af 9. juni 2004 om politiets virksomhed, jf. lovbekendtgørelse nr. 1270 af 29. november 2019
- **Retshåndhævelsesloven**
  Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger
- **Bekendtgørelse nr. 1078/09/2017**
  Bekendtgørelse om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser

10. Ordoptælling