POLITIETS NYE VÆRKTØJ: POL-INTEL

Et kvalitativt studie af de menneskeretlige konsekvenser ved analysebaseret politiarbejde (herunder "predictive policing").

Foto: www.learning.nexus.dk

AALBORG UNIVERSITET

Mette Bayer Kruhöffer

Vejleder: Jesper Lindholm

Titelblad

Dansk titel

Politiets nye værktøj: POL-INTEL. Et kvalitativt studie af de menneskeretlige konsekvenser ved analysebaseret politiarbejde (herunder ”predictive policing”).

Engelsk titel

The police's new tool: POL-INTEL. A qualitative study of the human rights consequences of analysis-based policing (including “predictive policing”).

Projekt

Kandidatspeciale ved Aalborg Universitet.

Projektets fagområde

Politiret og menneskeret.

Afleveringsdato

2. december 2021.

Omfang

142.615 anslag inkl. mellemrum.

Vejleder

Jesper Lindholm.

Udarbejdet af

Mette Bayer Kruhöffer.
Studienummer: 20153551

INDHOLDSFORTEGNELSE

Abstract

Crime is becoming more complex as technology evolves. This also leads to a development in terrorism and cyber-attacks, which poses a threat to national security. Therefore, the police may be forced to adopt new methods to be able to deal with this. The terrorist attack in 2015 in Copenhagen emphasized the need for new methods. This led to the implementation of section 2 a of the Danish Police Act and the purchase of POL-INTEL. The purpose of this thesis is to investigate the human rights issues related to the use of POL-INTEL in Denmark.

Firstly, POL-INTEL can be used for predictive policing which is why the thesis will shed some light on different types of policing. POL-INTEL is relatively new in Denmark and the legal situation regarding its use and possible issues are unclear. The thesis will examine the purpose of using a system such as POL-INTEL, which is based on algorithms, and clarify the scope of the application. For this purpose, section 2 a of the Danish Police Act, executive orders and legal motives will be accounted for. Secondly, the thesis presents the concepts of the right to respect for private and family life in Article 8 and the prohibition of discrimination in Article 14 of the European Convention on Human Rights. This is done to assess issues that the use of POL-INTEL raises in relation to these provisions. Furthermore, the thesis incorporates case law of the European Court of Human Rights on mass surveillance. Hereafter, criteria are derived on what Member States should observe in mass surveillance and the assessment of whether it constitutes an infringement of the fundamental rights of the individual. Finally, the thesis will briefly explain the right to an effective remedy in Article 13, as the assessment of the provision is closely related to the assessment of whether there has been a violation of Article 8.

Based on the assessment on the implementation of section 2 a of the Danish Police Act, the purchase of POL-INTEL and the analysis of case law from the European Court of Human Rights regarding mass surveillance, it can be concluded that the use of POL-INTEL raises human rights issues. It can also be concluded that the Ministry of Justice lacks the competence to make the assessment of what is "strictly necessary" in a democratic society. It is noted that the Danish regulation of POL-INTEL lacks sufficient and effective safeguards that can prevent abuse and arbitrariness. Therefore, it can be deduced on this basis that there is a considerable risk of violating the human rights specified in the convention, more specifically the Danes' right to privacy, family life, home and correspondence according to Article 8 and the right not to be subjected to discrimination under Article 14.

1. Indledning og problemformulering

Bekæmpelse af kriminalitet prioriteres højt, men ligesom samfundet udvikler sig, gør kriminaliteten det samme. Den stigende kompleksitet i kriminalitetsbilledet medfører at den retlige ramme, som dikterer politiets virksomhed[1], tilsvarende bliver mere kompleks. For at håndtere nye kriminalitetsformer kan politiet blive bedt om, eller være nødsaget til at tage nye eller andre midler i brug. Når politiet gør dette, kan der opstå problemer med at fastlægge de nye retlige rammer, hvorunder politiet skal arbejde. I den proces må man have det legitime formål om bekæmpelse af kriminaliteten for øje, men samtidig også vurdere, hvorvidt nye værktøjer kan være i strid med individers grundlæggende rettigheder.

Efter terrorangrebet i København i februar 2015 oplevede det danske politi, hvordan den komplekse kriminalitet var i udvikling. Terror er en trussel mod samfundet og en trussel, som kan være svær at bekæmpe, hvis ikke politiet har værktøjerne til det. Derfor indkøbte Danmark i 2017 det amerikanske IT-system POL-INTEL, som benytter sig af tværgående informationsanalyser. Dette er i et forsøg på at forhindre lignende hændelser. Indkøbet og anvendelsen af POL-INTEL er hjemlet i politilovens § 2 a, som blev indført i 2017.

POL-INTEL er udviklet af det amerikanske softwarefirma Palantir. De teknologiske systemer, som POL-INTEL, der muliggør overvågning, har været udsat for kritik i udlandet. Kritikken kommer bl.a. fra USA og Storbritannien. Noget af kritikken har været, at den data som POL-INTEL indeholder, kommer til at erstatte politi-intuition, og at algoritmer kommer til at afløse traditionelt politiarbejde.[2] Men det nyindkøbte system betyder også for politiet, at deres arbejdsprocesser angiveligt bliver hurtigere og mere effektive, bl.a. fordi der sker en sammenholdelse af data fra flere registre, hvilket dermed kan føre til en kortere efterforskningsperiode.

Et andet kritikpunkt har været på grund af det paradigmeskifte, som det kan medføre hos politiet. Paradigmeskiftet består i, at politivirksomheden går fra at være opklarende til at være forudsigende, også kaldet ”predictive policing”. Selvom POL-INTEL får meget kritik for det forudsigende element, så har vicepolitimester Ole Andersen i 2018 til en artikel hos Teknologiens Mediehus udtalt, at det danske politi ikke gør brug af ”predictive policing”, og dermed ikke anvender individualiseret brug af POL-INTEL. Dette skyldes, at man i Danmark mener. at datagrundlaget i dansk kriminalitet er for

[1] Lov nr. 444 af 9. juni 2004 om politiets virksomhed, jf. lovbekendtgørelse nr. 1270, af 29. november 2019 (Politiloven), § 2.
[2] Frederik Kulager, *”For fire år siden fik politiet et ”supervåben”. Her er, hvordan det har transformeret ordensmagten”*, Artikel på Zetland.dk, (https://www.zetland.dk/historie/sO9kBG7W-aOZj67pz-04ca0)

lavt.[3] Dog udtaler han også, at han synes "predictive policing" kunne være interessant.[4] Politilovens § 2 a forbyder ikke decideret analyser på individniveau eller forudsigende politiarbejde, men giver derimod en bred hjemmel til at indsamle og behandle oplysninger. Således har det danske politi en hjemmel til at udøve "predictive policing", selvom det på nuværende tidspunkt angiveligt ikke udøves.

Behandling af personoplysninger og en vis grad af øget overvågning af borgerne aktualiserer imidlertid visse menneskerettighedsrelaterede problemstillinger. Forebyggende politiarbejde giver særligt anledning til at overveje art. 8 i Den Europæiske Menneskerettighedskonvention (herefter EMRK) om retten til privatliv og familieliv, og art. 14 om forbud mod diskrimination. Hvor går grænsen mellem at sikre tryghed, beskytte friheden og retten til ikke at blive udsat for diskrimination, og på den anden side samfundets ønske om at bekæmpe kriminalitet?

Dette vil søges besvaret i specialeafhandlingen gennem besvarelse af følgende problemformulering:

Hvilke menneskeretlige problemstillinger aktualiseres gennem anvendelsen af POL-INTEL?

I specialet behandles først de forskellige typer af policing i afsnit 4, hvor fokus er på "predictive policing". Herefter vil afsnit 5 have fokus på at belyse politilovens § 2 a og de hensigter i lovforslaget, der lå til grund for implementeringen. I afsnit 5.3 vil der være en beskrivelse af POL-INTEL som analyseværktøj og Palantir som softwareudbyder. Afsnit 5.3.2 afslutter fremstillingen af POL-INTEL ved at inddrage relevant kritik til IT-systemet fra fagpersoner.

I afsnit 6 vil EMRK art. 8 og 14 blive beskrevet, hvoraf disse er særlige relevante for at besvare problemformuleringen. I forlængelse heraf vil der være en diskussion, hvor disse bestemmelser sammenholdes med de menneskeretlige problemstillinger, som aktualiseres ved brugen af POL-INTEL. I afsnit 6.5 vil retspraksis fra Den Europæiske Menneskerettighedsdomstol (herefter kaldet EMD), omhandlende masseovervågning, blive analyseret for at undersøge EMD's vurdering af relaterede problemstillinger. Herefter vil der på denne baggrund blive udledt en række kriterier for anvendelsen af IT-systemer, som POL-INTEL, der muliggør hemmelig masseovervågning.

I afsnit 6.7 vil art. 13, om retten til effektive retsmidler, blive kort omtalt. Specialets problemformulering er, hvilke menneskeretlige problemstillinger, der aktualiseres gennem

[3] Adam Fribo, "*Rigspolitiet lover: Vi bruger ikke Pol-intel til predictive policing*", Artikel på version2.dk, https://www.version2.dk/artikel/rigspolitiet-lover-vi-bruger-ikke-pol-intel-predictive-policing-1092642
[4] Adam Fribo, "*Rigspolitiet lover: Vi bruger ikke Pol-intel til predictive policing*", Artikel på version2.dk, https://www.version2.dk/artikel/rigspolitiet-lover-vi-bruger-ikke-pol-intel-predictive-policing-1092642

anvendelsen af POL-INTEL. På baggrund heraf er det naturligt at afslutte projektet med en kort omtale af at enhver, der krænkes ved brugen af POL-INTEL, og dermed krænkes ved de i konventionens anerkendte rettigheder og friheder, skal have adgang til effektive retsmidler.

2. Afgrænsning

En afgrænsning er særligt vigtig for at målrette indholdet af kandidatspecialet, således problemformuleringen på bedst mulig vis bliver besvaret. Det betyder, at der fokuseres på de menneskeretlige problemstillinger, som aktualiseres gennem anvendelsen af POL-INTEL efter politilovens § 2 a. En fremstilling af forskellige typer policing vil indgå, hvoraf den vigtigste i denne fremstilling er ”predictive policing”. Det betyder at ”smart policing” og ”intelligence-led policing” kun kort vil blive belyst. I forlængelse af implementeringen af politilovens § 2 a blev toldloven ligeledes ændret, hvilket angik oplysninger om flypassagerer. Dette er ikke relevant til besvarelsen af problemformuleringen, og vil derfor ikke blive behandlet.

For at kunne besvare problemformuleringen angående de menneskeretlige problemstillinger, er det relevant for forståelsen og diskussionen heraf, at belyse politilovens § 2 a, hertil hørende lovforslag, bekendtgørelser, høringssvar og diverse betragtninger.

Persondataretten er relevant ved diskussionen af POL-INTEL. Persondatalovens § 1, stk. 2, 1. pkt. vil kort blive nævnt i afsnit 5.1 for at belyse den hjemmelsmæssige forskel der er, når der skal foretages behandling og indsamling af personoplysninger i hhv. persondataloven og politiloven. Herefter vil persondataretten ikke nærmere blive gennemgået.

I afsnit 5.3.3 vil specialet kort komme ind på ytringsfriheden i art. 10 for at belyse et kritikpunkt til systemer som POL-INTEL. Art. 10 vil ikke blive behandlet selvstændigt, men bliver kort nævnt for at beskrive kritikken vedrørende ”the chilling effect”.

I afsnit 6.1.1 bliver de fire beskyttelsesinteresser i art. 8 gennemgået. Her vil begrebet ”familieliv” kun blive behandlet i et begrænset omfang. Grunden til denne afgrænsning skyldes at retten til respekt for familieliv ikke har en betydelig relevans for diskussionen af de menneskeretlige konsekvenser af POL-INTEL. Desuden vil definitionerne af de fire beskyttelsesinteresser kun blive gennemgået i relation til det, der har betydning for masseovervågning og POL-INTEL.

I forhold til retspraksis på området har det ikke været muligt at finde relevant retspraksis, som omhandler politilovens § 2 a. Dog vil der i forlængelse af den menneskeretlige diskussion blive

inddraget afgørelser fra EMD, som belyser problemstillingen ved masseovervågning af samfundets borgere og hvilke udfordringer det kan have i relation til de menneskeretlige garantier i EMRK art. 8 og 13. Afgørelserne angår ikke forbuddet mod diskrimination efter art. 14. Hertil skal det også bemærkes, at EMRK tillige indeholder et generelt forbud mod diskrimination i konventionens 12. tillægsprotokol. Den adskiller sig særligt fra art. 14, idet den ikke er bundet til, om det relevante forhold har en relation til konventionens materielle bestemmelser. Eftersom Danmark har valgt ikke at ratificere konventionens 12. tillægsprotokol, og denne afhandling drejer sig om POL-INTEL i Danmark, vil den ikke blive behandlet i afhandlingen.

Afsnit 6.7 om retten til effektive retsmidler efter art. 13 vil kort komme ind på sammenhængen mellem art. 13 og art. 35, men art. 35 vil ikke blive gennemgået selvstændigt.

3. Metode

3.1. Metodevalg

For at kunne foretage den menneskeretlige undersøgelse af anvendelsen af POL-INTEL, vil den retsdogmatiske metode blive anvendt. Dette omfatter en analyse af relevante retskilder på området med det formål at fastsætte, hvad gældende ret er (de lege lata).[5] Formålet med metoden retter sig ikke mod at løse konkrete tvister, men derimod at beskrive, analysere, systematisere og kategorisere gældende ret.[6] Dette er for at få fastlagt eventuelle retningslinjer eller kriterier for et område, som f.eks. i dette speciale, når der sker anvendelse af POL-INTEL, hvor retstilstanden er ny og dermed usikker.

I lyset af de menneskeretlige problemstillinger i forhold til POL-INTEL, vil specialet inddrage politiloven, lovforslag nr. 171 af 29. marts 2017, bekendtgørelse om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser, høringssvar fra Justitsministeriet og EMRK art. 8, 13 og 14. Retslitteratur og anden faglitteratur bidrager til forståelsen af en problemstilling på et område, hvor der ikke foreligger mange retskilder. Derfor vil relevante betragtninger blive inddraget fra Mette Volquartzen, ph.d. i jura, og Henrik Stevnsborg, dr.phil. ved Det Juridiske Fakultet ved Københavns Universitet. Denne litteratur anses ikke for en retskilde i den nordiske retskildemetode, men bidrager til fortolkningen og til at belyse retsstillingen. En rapport fra menneskerettighedsorganisationen Liberty vil også blive inddraget, hvilket kan betegnes som anden

[5] Carsten Munk-Hansen, "*Retsvidenskabsteori",* Jurist- og Økonomforbundets Forlag, 2018, 2. udgave, s. 64.
[6] Jens Evald & Sten Schaumburg-Müller, "*Retsfilosofi, retsvidenskab & retskildelære*", Jurist og Økonomforbundets Forlag, 2004, 1. udgave, s. 212.

faglitteratur. Heller ikke sådan en publikation er en retskilde, men kan medvirke til at belyse problemstillingen yderligere. Diverse artikler fra online nyhedsmedier vil også i et vist omfang inddrages for at belyse visse udtalelser fra bl.a. Rigspolitiet og Institut for Menneskerettigheder. Retspraksis fra EMD omhandlende masseovervågning vil blive analyseret for at bidrage til en forståelse af, hvilke menneskeretlige problemstillinger dette aktualiserer og særligt, hvordan EMD vurderer disse.

3.2. Retskilder

Retskilderne ifølge nordisk tradition er loven, retspraksis, sædvane og forholdets natur.[7] Sædvane og forholdets natur vil dog ikke få en større betydning for at besvare problemformuleringen. Udgangspunktet for nærværende speciale vil være loven, idet retstilstanden vedrørende POL-INTEL i Danmark er relativ ny. Politilovens § 2 a blev tilføjet til den daværende politilov i 2017 med Lov nr. 671 af 8. juni 2017 "Lov om ændring af lov om politiets virksomhed og toldloven". Med denne ændring og dermed tilføjelse til politiloven, fik politiet nu hjemmel til at anvende tværgående informationsanalyser med hjælp af det nyindkøbte POL-INTEL.

For at forstå hensigten og overvejelserne bag implementeringen af politilovens § 2 a, er det relevant at inddrage lovforslagets bemærkninger, som fremgår af 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)". Lovforslaget vil i den senere fremstilling blot omtales som "L171". Lovforarbejder anses ikke for en selvstændig retskilde[8], men bidrager derimod til fortolkningen af loven.[9] Samtidig med at forstå overvejelserne med implementeringen af § 2 a, er det også relevant at undersøge, hvorvidt der i overvejelserne ligeledes har været inddraget menneskeretlige perspektiver, og særligt om hjemlen til POL-INTEL har givet anledning til at overveje potentielle menneskeretlige problemstillinger.

Det er nødvendigt at belyse bekendtgørelse nr. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser (herefter kaldet bekendtgørelse nr. 1078), for at forstå den specifikke regulering af politilovens § 2 a. Bekendtgørelser er generelle og derfor bindende for borgeren og offentlige myndigheder ved kundgørelse i Lovtidende.[10] Det fremgår

[7] Jens Evald, "*Retskilderne og den juridiske metode*", Jurist- og Økonomforbundets Forlag, 2000, 2. udgave, s. 7.
[8] Jf. de fire angivne retskilder i Jens Evald, "*Retskilderne og den juridiske metode*", Jurist- og Økonomforbundets Forlag, 2000, 2. udgave, s. 7.
[9] I den deskriptive retskildeteori indtager forarbejder en central placering som retskilde, hvilket ikke ellers er tilfældet. Derfor vil det ikke blive behandlet yderligere her, Ibid, s. 9.
[10] Jens Evald, "*Retskilderne og den juridiske metode*", Jurist- og Økonomforbundets Forlag, 2000, 2. udgave, s. 33.

af politilovens § 2 a, stk. 3, at justitsministeren fastsætter nærmere regler for politiets behandling af oplysninger efter stk. 1 og 2, herunder formålet for behandling, samt hvilke foranstaltninger, der skal iagttages ved behandlingen. Disse regler er beskrevet i bekendtgørelsen, og en sådan administrativ udstedelse af regler, gør også at fremtidige ændringer i medfør af stk. 3 bliver lettere.

EMRK er central for at kunne besvare problemformuleringen vedrørende de menneskeretlige problemstillinger ved anvendelsen af POL-INTEL. EMRK blev i 1950 vedtaget af Europarådet i Strasbourg. D. 3. september 1953, samme år som EMRK trådte i kraft, ratificerede Danmark ligeledes konventionen, men først i 1992 blev EMRK gjort til en del af dansk lov.[11] Dette betyder at den danske lovgivning skal sikre, at borgernes rettigheder efter konventionen ikke krænkes. Art. 8, 13 og 14 vil blive diskuteret nærmere i fremstillingen. Belysningen af netop disse bestemmelser er vigtig for at kunne besvare problemformuleringen og danner grundlag for yderligere diskussion af de afgørelser, der inddrages fra EMD.

EMD's retspraksis er væsentlig for analysen i specialet. EMD blev etableret i 1959 og består af 47 medlemmer, én fra hvert medlemsland af Europarådet. Retspraksis er af betydning for, at borgerne kan forudse deres retsstilling ud fra princippet om at "lige skal behandles lige". Dermed bliver denne lighedsideologi grundlaget for at anse retspraksis for en retskilde.[12] Afgørelser fra EMD har ligeledes til "*formål at belyse, sikre og videreudvikle konventionens rettigheder og friheder*"[13], og bidrager dermed til at staterne overholder sine forpligtelser. Når menneskeretlige problemstillinger skal afgøres, er det svært at komme udenom anvendelse af praksis, idet EMD på mange retsområder har fastsat detaljerede generelle kriterier, som bør anvendes når konventionen skal fortolkes.[14] Det fremgår af inkorporeringslovens forarbejder "*at danske myndigheder må følge konventionsorganernes retsopfattelse med hensyn til konventionens fortolkning*".[15] Dette understreger betydningen af at inddrage retspraksis fra EMD, særligt når der er tale om en ny retstilstand i Danmark, som med implementeringen af § 2 a. Medlemsstaterne er som følge af art. 46, stk. 1 forpligtet til at rette sig efter EMD's endelige dom. Dermed er de fem afgørelser, som vil blive analyseret og diskuteret i den kommende fremstilling, vigtige for at kunne vurdere, om anvendelsen af POL-INTEL er i overensstemmelse med EMRK og EMD's praksis, vedrørende masseovervågning. Vigtigheden heraf skyldes særligt, at systemet er et nyt område i bekæmpelsen

[11] Lov nr. 285 af 29. april 1992 (Inkorporeringsloven).
[12] Carsten Munk-Hansen, "*Retsvidenskabsteori",* Jurist- og Økonomforbundets Forlag, 2018, 2. udgave, s. 215 f.
[13] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 15.
[14] Ibid.
[15] Betænkning nr. 1546/2014 af Justitsministeriet (Betænkning om inkorporering mv. inden for menneskeretsområdet), s. 47 f.

mod kompleks kriminalitet og terror. De fem afgørelser omhandler ikke direkte anvendelsen af POL-INTEL, men derimod masseovervågning af samfundets borgere, hvilket giver anledning til lignende menneskeretlige problemstillinger. Der er efter søgning i EMD's database ikke fundet afgørelser, der direkte relaterer sig til brugen af POL-INTEL, hvilket sandsynligvis skyldes, at der er tale om et relativt nyt system. I afsnit 6.1.4 vedrørende offentlige myndigheders behandling og registrering af oplysninger, vil to afgørelser fra EMD kort blive nævnt for at illustrere nogle relevante problematikker. De to afgørelser bliver ikke nærmere analyseret, men skal blot bidrage til forståelsen af de pågældende problemstillinger. Den første afgørelse vedrørende masseovervågning, der vil blive analyseret, er Klass m.fl. mod Tyskland, afsnit 6.5.1.1, som er afsagt d. 6. september 1978. Anden afgørelse er Roman Zakharov mod Rusland, afsnit 6.5.1.2, afsagt d. 4. december 2015 i "Grand Chamber". Tredje afgørelse er Szabó og Vissy mod Ungarn, afsnit 6.5.1.3, som blev afsagt d. 12. januar 2016 i "Fourth Section". Herefter vil to nye afgørelser fra d. 25. maj 2021 afsagt i "Grand Chamber" blive gennemgået, hvilket drejer sig om hhv. Centrum för rättvisa mod Sverige, afsnit 6.5.1.4 og B.B.W. m.fl. mod Storbritannien, afsnit 6.5.1.5. De tre afgørelser fra "Grand Chamber" tillægges stor præjudikatsværdi, idet dette er Storkammeret og EMD's svar på Højesteret.

På baggrund af analysen af ovenstående afgørelser vil der i afsnit 6.5.2 udledes en række kriterier ved hemmelig masseovervågning, som medlemsstaterne skal iagttage for ikke at krænke menneskerettighederne. Herefter vil det i afsnit 6.5.3 blive vurderet, hvorvidt implementeringen og anvendelsen af POL-INTEL er i overensstemmelse med kriterierne fra EMD. Formålet hermed er at beskrive, analysere og systematisere en ukendt retstilstand, som anvendelsen af POL-INTEL er. Dette følger af den retsdogmatiske metode.

4. Typer af policing

Det danske politi udvikler sig i takt med den internationale udvikling, hvilket betyder, at dansk politi anvender "smart policing". "Smart policing" er en paraplybetegnelse for et paradigmeskifte hos politiet[16], hvorunder "intelligence-led policing" og "predictive policing" indgår.

Da det danske politi i 2017 fik implementeret det nye IT-system, POL-INTEL, blev strategien med "smart policing" og anvendelsen af tværgående informationsanalyser til en realitet. På sigt betyder det, hvis ikke det allerede anvendes, at det er muligt at forudsige forbrydelser i Danmark og forudsige potentielle gerningspersoner og ofre, hvilket kaldes "predictive policing". Anvendelsen og baggrunden for POL-INTEL i Danmark vil nærmere blive belyst i afsnit 5.3.

Der vil i de følgende afsnit blive beskrevet de tre typer af policing, som hver især beskriver en måde, hvorpå politiet kan udøve deres virksomhed. Herefter vil der i afsnit 4.3.1. blive inddraget nogle betragtninger angående "predictive policing", og hvilke erfaringer man har med det i udlandet. Selvom det er uklart, hvorvidt Danmark anvender POL-INTEL til at forudsige kriminalitet, gør IT-systemet det muligt for det danske politi, hvis de ønsker det. Derfor er det relevant at have et udblik i verden, hvor man har erfaringer med "predictive policing", for at få et indblik i den verden vi i Danmark potentielt selv står overfor.

4.1. Smart policing

"Smart policing" er en strategi, der samlet beskriver "*ledelse, ressourcer og en bedre og øget brug af data og it"*.[17] Som en følge af det stigende og mere komplekse kriminalitetsbillede har politiet været nødsaget til også at tage andre midler i brug for at imødekomme dette, hvilket bl.a. skete i 2017 med implementeringen af POL-INTEL. POL-INTEL er en tydelig illustration af strategien "smart policing", fordi systemet gør brug af øget data og it.

I 2012 blev begrebet "smart policing" beskrevet af Rigspolitichef Jens Henrik Højbjerg som "*alle former for ledelse, der i sidste ende ville føre til bedre brug af de tilgængelige ressourcer i arbejdet med operationelle resultater*".[18] Ikke kun i Danmark er begrebet blevet beskrevet. I 2015 blev det i Indien defineret som "*et forsøg på at udnytte de risici, der er forbundet med politiarbejde i smart*

[16] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 171.
[17] Ibid.
[18] Ibid, s. 173.

cities".[19] I samme forbindelse har man i Indien beskrevet og udformet fem principper for politiarbejdet:

S: Strict and sensitive.
M: Modern and mobile.
A: Alert and accountable.
R: Reliable and responsive.
T: Techno-savvy and trained.[20]

Ud fra disse principper er der høje krav til politiarbejdet. Politiet skal i deres virke som politi være klar på eventuelle trusler mod den nationale sikkerhed og kunne reagere, samt disponere ved hjælp af IT-systemer og dataudtræk. Både Stevnsborg[21] og Volquartzen[22] beskriver dette koncept som et paradigmeskifte, hvor politivirksomheden går fra at handle overvejende reaktiv til at handle proaktivt[23], og beskriver at politiet er blevet et mere analytisk og datadrevet.[24] Paradigmeskiftet kan beskrives ved terminologien "intelligence-led policing" (herefter kaldet ILP)[25], som vil blive beskrevet i det følgende afsnit.

4.2. Intelligence-led policing

ILP er et koncept, der hører under begrebet "smart policing".[26] Det handler om en "klogere" og mere vidensbaseret politivirksomhed, hvor man i stedet for at handle reaktivt forsøger at forhindre kriminalitet og de tilknyttede risici, hvilket er det paradigmeskifte, som også beskrives i afsnit 4.1. Paradigmeskiftet skyldes hovedsagligt de omstændigheder, at politiet er nødt til at arbejde mere strategisk og målrettet for at udnytte deres ressourcer på bedst mulige vis.[27]

Den traditionelle efterforskningsmodel, som før i tiden gik fra menneske til menneske, bliver i stedet fra computer til menneske, hvorved det er computeren, der bearbejder de relevante data. Denne data analyseres i relation til andre sammenhænge i datamængderne, som kan bestå i alt fra mails, nummerpladescanninger, interaktioner på de sociale medier mm. Dette kaldes datamining.[28]

[19] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 173.
[20] Ibid.
[21] Henrik Stevnsborg, "*Hot spots, hot times, hot persons. Om fænomenet predictive policing*", 2021, s. 2.
[22] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 173.
[23] Ibid.
[24] Henrik Stevnsborg, "*Hot spots, hot times, hot persons. Om fænomenet predictive policing*", 2021, s. 2.
[25] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018., s. 174.
[26] Ibid.
[27] Nadja Kirchhoff Hestehave, "*Proaktiv kriminalitetsbekæmpelse*", Samfundslitteratur, 2013, 1. udgave, s. 13.
[28] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 175.

Datamining[29] kan hos bankerne anvendes til at forudsige dårlige betalere, hvorimod det ved brug i politiet kan anvendes til at forudsige potentielle gerningspersoner og potentielle ofre. Ved datamining anvendes algoritmer, som kan analysere på kriminalitetsmønstre, hvilket kan medføre en ændring og prioritering af politiets disponering.[30]

Volquartzen beskriver således, at paradigmeskiftet betyder et skift fra et synoptisk politi til et panoptisk politi.[31] Det synoptiske politi er det man i mange år har kendt til. Det er det synlige politi på veje og gader, hvor patruljering og generel tilstedeværelse skulle have en præventiv effekt. Det panoptiske politi er derimod overvågning i det skjulte, hvilket ikke er ukendt i Danmark. Ved grundlovens indførelse i 1849 var politispioner, der overvågede og infiltrerede grupper og personer af interesse, ikke unormalt.[32] Formålet med dette var sikkerhed og fred, hvilket bl.a. også var formålet med indkøbet af POL-INTEL. I forbindelse med politireformen i 1863 skiftede det danske politi tilbage til det synoptiske politiarbejde som vi kender det i dag.[33]

Volquartzen sætter spørgsmålstegn ved om det panoptiske politi, som vi kender det fra før 1849, igen bliver en realitet i det danske politi. Det afviser hun dog med henvisning til, at retsstaten og teknologien er en anden end dengang, samt mulighederne for at foretage overvågning gør, at omstændighederne vil være anderledes.[34] Hun anfører til sidst, til støtte for hendes påstand, at "*vi også oplever en helt anden præmis for overvågningens formål samt aktører*".[35] Dermed konkluderer Volquartzen ikke med at sige, at vi ikke kommer til at opleve politiet som panoptiske, men at vi kommer til at opleve det på en anden måde end tidligere.

4.3. Predictive policing

"Predictive policing" kan siges at være et begreb og en metode, som hører under ILP.[36] De to begreber har dét tilfælles at fokusset er på forudsigeligheden og analysen af mønstre. "Predictive policing" består af regressionsanalyser, hot spot analyser og datamining teknikker.[37] Det er brugen af algoritmer ud fra historiske kvantitative data, der er med til at problematisere en sådan metode. Som nævnt i

[29] Datamining er ikke en statistisk analyse, men en analyse, der afdækker sammenhænge i store datamængder, og fokuserer på resultaterne. https://denstoredanske.lex.dk/datamining
[30] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 176.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid, s. 177.
[35] Ibid.
[36] Ibid, s. 180.
[37] Ibid.

indledningen fastholder det danske politi, at de ikke anvender "predictive policing"[38], selvom de synes det er interessant. Dog giver systemet mulighed for at analysere på historiske data for at forudse fremtiden, og derfor kan det ikke udelukkes at dansk politi i fremtiden vil benytte det. Derfor er det relevant at undersøge, hvilke erfaringer, der har været med "predictive policing" i udlandet. Kan man forudsige fremtiden på baggrund af fortiden, og hvilke problemer kan der være ved, at politiet forsøger at være forudseende?

4.3.1. Betragtninger og erfaringer ved anvendelse af "predictive policing"

"Predictive policing" er ikke et nyt begreb i forsøget på at bekæmpe kompleks kriminalitet. I udlandet har man anvendt denne teknik, og anvender den stadig visse steder, hvilket gør, at man i disse lande kan udlede visse fordele og ulemper ved metoden.

I USA har det forudseende politi været kendt siden 1990'erne[39], og ca. 20 ud af de 50 største politikorps i landet har anvendt metoden.[40] Stevnsborg inddeler metoden i to elementer. Den første er det han kalder for prediktions-modellen, der går ud på, at der anvendes algoritmer til at beregne mulige kommende risici. Modellen bunder i den opfattelse, at "*forbrydelser ikke sker tilfældigt, og at fortiden – med de rette data og med den rette analysesoftware – kan forudsige fremtiden*".[41] Det andet element er en strategi for, hvordan politiet herefter skal fordele sine ressourcer for at forhindre eller mindske disse risici.[42]

Udover at opdele begrebet i to elementer mener Andrew G. Ferguson, juraprofessor fra Washington D.C., at "predictive policing" også kan opdeles i 3 faser. Generation 1.0 var første fase, hvormed man havde fokus på at identificere de såkaldte "hot spots" og "hot times" ved ejendomsforbrydelser.[43] Generation 2.0 var næste fase, hvor fokus også blev rettet mod personfarlig kriminalitet.[44] Her var "hot spots" og "hot times" stadig en del af fokusset. Den sidste fase var generation 3.0, hvor fokus blev flyttet over på "hot persons".[45] Det er særligt ved sidste fase og dermed generation 3.0, at

[38] Adam Fribo, "*Rigspolitiet lover: Vi bruger ikke Pol-intel til predictive policing*", Artikel på version2.dk, https://www.version2.dk/artikel/rigspolitiet-lover-vi-bruger-ikke-pol-intel-predictive-policing-1092642
[39] Henrik Stevnsborg, "*Hot spots, hot times, hot persons. Om fænomenet predictive policing*", 2021, s. 1.
[40] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 181.
[41] Henrik Stevnsborg, "*Hot spots, hot times, hot persons. Om fænomenet predictive policing*", 2021, s. 1.
[42] Ibid.
[43] Andrew G. Ferguson, "*Policing Predictive Policing*", Washington University Law Review, vol. 94, issue 5, 2017, s. 1127.
[44] Ibid, s. 1132.
[45] Ibid, s. 1137.

diskussionen om retten til privatliv og risiko for diskrimination bliver relevant, da man her analyserer på historiske data på individniveau.

4.3.1.1. Falske negativer og falske positiver

Når algoritmer erstatter mennesker, er der en øget risiko for hhv. falske negativer og falske positiver. Det sætter høje krav til udviklingen af teknologien og udfordringen bliver at udforme algoritmer, der kan analysere på alle relevante data, og ikke lade sig begrænse til de "kendte" data. Volquartzen beskriver falske negativer som personer, der ikke vil begå kriminalitet eller ikke er potentielle ofre. Falske positiver definerer hun som personer, der vurderes til at begå kriminalitet eller er i risiko for at blive ofre. Både risikoen for falske negativer og falske positiver er uundgåelig, uanset teknologiens udvikling.[46] Forskellen på beslutninger truffet af mennesker fremfor en computer er, at et menneske kan begrunde, forsvare og stå til regnskab for en beslutning. En person, der udsættes for kriminalisering eller bliver kategoriseret som et potentielt offer, har ikke mulighed for at stille en computer til regnskab for en sådan beslutning på samme måde.

I 2019 blev en rapport ved navn "Policing by Machine" udgivet fra en engelsk menneskerettighedsorganisation, Liberty. Rapporten belyser en række problemstillinger ved "predictive policing" baseret på erfaringer fra Storbritannien. Hannah Couchman (herefter kaldet Couchman) beskriver, hvordan et af de store problemstillinger ved algoritmerne er manglende forståelse for algoritmens bagvedliggende data. Risikoen på baggrund heraf bliver således, at medarbejderne hos politiet, der anvender algoritmen, ikke føler et ansvar for de beslutninger, som træffes af IT-systemet.[47] Det kan betyde, at den enkelte politibetjent i en vis grad har mulighed for at fralægge sig ansvaret. En anden problemstilling, som Couchman belyser er, at det er svært for befolkningen at få indsigt i, hvordan algoritmen er udformet og hvordan den anvendes. Dette er enten fordi algoritmen holdes hemmeligt af det private firma, der har solgt den til politiet, eller fordi politiet ikke ønsker en sådan indsigt i deres beslutningsmetoder.[48] Det kan have den konsekvens, at mennesker, der udsættes for at blive kategoriseret som falsk negativ eller falske positiv, kan have svært ved at holde politiet ansvarlige for uretmæssig profilering.

[46] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 182.
[47] Hannah Couchman, "*Policing by Machine*", Rapport fra Liberty, 2019, s. 39.
[48] Ibid, s. 40.

4.3.1.2. Risiko for bias og "præ-kriminalisering"

En af de store problematikker ved anvendelsen af algoritmer er risikoen for bias. Algoritmer er menneskeskabte og dermed er algoritmer ikke neutrale. Mennesker har forudindtagelser omkring forskellige ting, og kan være påvirket af det medierne fokuserer på at belyse. Disse forudindtagelser kan enten bevidst eller ubevidst blive overført som informationer til en computer og på baggrund heraf danne en algoritme. Det problematiske i dette er, når denne algoritme skal anvendes af politiet og politiet udøver deres virksomhed på baggrund heraf. Det er værd at bemærke, at det ikke er oplyst, hvorvidt algoritmen i POL-INTEL er stillet til rådighed af Palantir, eller om den er dannet af det danske politi. Såfremt algoritmen er udarbejdet af Palantir kan det give anledning til at overveje om amerikanske tilstande, der er kendt for en betragtelig racediskrimination, indirekte implementeres hos det danske politi gennem anvendelse af algoritmen.

Volquartzen beskriver særligt den systematiske bias som problematisk. Det bliver et problem når politiet systematisk indhenter tilgængelige oplysninger forbundet til personer, og herudfra forsøger at danne mønstre, som ikke eksisterer.[49] Men ikke kun bias i forhold til personer er en risiko. Couchman beskriver også, hvordan der kan være bias i forhold til de såkaldte "hot spots", hvormed hun skriver at "*data collected by the police does not present an accurate picture of crime committed in a particular area – it simply presents a picture of how police responded to crime*".[50] Et andet argument hun også belyser i relation til bias og "hot spots" er, at statistikker over antal anholdte på et givent sted ikke kan anvendes til at udpege særlige kriminelle områder uden en risiko for fejlprofilering, idet dét at være blevet anholdt ikke indikerer, at man er skyldig i en forseelse.[51]

Én af de største udfordringer ved "predictive policing" er den form for "præ-kriminalisering", som alle kan blive genstand for. Den særlige uskyldsformodning, "uskyldig indtil det modsatte er bevist", bliver sat på prøve, når man i politiet er proaktive i stedet for at være reaktive. Dette giver anledning til at sætte spørgsmålstegn ved, hvordan borgerne bliver beskyttet mod vilkårlighed, når politiet forsøger at forudse kriminalitet og dermed potentielle gerningspersoner. Argumentet for at købe et IT-system, som POL-INTEL, fremgår i regeringens udspil, "Et stærkt værn mod terror". Her anføres det at formålet er at bekæmpe og forhindre terror.[52] Problemet med "præ-kriminalisering" bliver dog en mulig realitet når man ikke kun anvender IT-systemet til at forhindre terror. Hvis POL-INTEL

[49] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 185.
[50] Hannah Couchman, "*Policing by Machine*", Rapport fra Liberty, 2019, s. 15.
[51] Ibid, s. 16.
[52] Regeringens udspil "*Et stærkt værn mod terror*", 2015, s. 1.

også anvendes til at bekæmpe andre kriminalitetsformer end terror, kan der være en betydelig risiko for "over-policing" og dermed risiko for at kriminalisere uskyldige.[53]

4.4. Sammenfatning

Sammenfattende kan det fastslås, *at* når man generelt taler om policing findes der forskellige typer, hvorunder særligt "predictive policing" og det "forudseende politi" kan være problematisk. Derudover kan det fastslås, *at* der er en stor risiko for falske negativer og falske positiver ved at anvende et system som POL-INTEL, *at* potentielle ofre for en sådan profilering kan have svært ved at forsvare sig mod en ukendt algoritme, hvor man ikke får en begrundelse for profileringen, og *at* der kan være en fare for ansvarsfralæggelse fra politiets side ved at anvende en computer som beslutningstager. Desuden kan det sammenfattes, *at* risikoen for bias med stor sandsynlighed er uundgåelig, idet data til algoritmer kommer fra mennesker, som også har forskellige forudindtagelser, samt *at* risikoen for at "præ-kriminalisere" et helt samfund er stor, hvorfor "over-policing" også kan forekomme.

5. Politilovens § 2 a

5.1. Bestemmelsens ordlyd

Politilovens § 2 a har følgende 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.*

[53] Hannah Couchman, "*Policing by Machine*", Rapport fra Liberty, 2019, s. 3.

Det følger således af bestemmelsens stk. 1, at politiet med indførelsen af bestemmelsen får adgang til at foretage informationsanalyser på tværs af de registre, som politiet har anvendt tidligere, og som politiet allerede kan tilgå, men også offentligt tilgængelige oplysninger. Disse registre er bl.a. Det Centrale Personregister (CPR), eller registre som følge af internationalt politisamarbejde som f.eks. Schengen-registret (SIS II), fingeraftryksregistreret (EURO-DAC) og Europols registre.[54] De offentligt tilgængelige oplysninger er bl.a. oplysninger fra Facebook eller Instagram, men ikke begrænset hertil.[55] Særligt omkring selve reguleringen af, hvad "tværgående informationsanalyser" er og hvornår sådanne analyser må finde sted, skal findes i bekendtgørelse nr. 1078. Dette vil særligt blive behandlet i afsnit 5.3.2.

Den retlige hjemmel for politiet til at indsamle og behandle oplysninger fremgår af stk. 2. Indsamling af oplysninger drejer sig om, at politiet sikrer sig oplysninger fra de ovennævnte registre og databaser.[56] Behandlingen af oplysningerne omfatter enhver behandling med eller uden brug af elektronisk databehandling. Til forskel fra databeskyttelseslovgivningen, som kun drejer sig om behandling af personoplysninger[57], er der i den retlige regulering af § 2 a tale om enhver oplysning, der undergives behandling, og dermed ikke begrænset til personoplysninger.[58]

Det fremgår både af stk. 1 og 2, at politiet indsamler og behandler oplysninger "*når det er nødvendigt af hensyn til udførelsen af politiets opgaver jf. § 2".* Vurderingen af om foretagelsen af tværgående informationsanalyser er berettiget skal således vurderes i lyset af de oplistede opgaver for politiet, som fremgår af politilovens § 2. Politilovens § 2 regulerer politiets almindelige ordens- og sikkerhedsopgaver og politiets tilsyns- og kontrolopgaver.[59] Herigennem kan de tværgående informationsanalyser ske i forbindelse med opgaver inden for og uden for strafferetsplejen, når det er nødvendigt. Det er, ifølge Ib Henricson, tilstrækkeligt at metoden anses for den mest effektive, uagtet om det er almindelig kriminalitetsforebyggelse, konkret efterforskning eller ordensopgaver.[60]

Hjemlen til at behandle oplysninger reguleres efter stk. 3. Hermed kan justitsministeren fastsætte den konkrete regulering af, hvilke formål, der skal være gældende for at kunne behandle oplysninger, samt særlige regler for sletning og tekniske og organisatoriske foranstaltninger. Politiets behandling

[54] Ib Henricson, *"Politiloven med kommentarer"*, Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 39.
[55] Ibid.
[56] Ibid, s. 40.
[57] Lov nr. 502 af 23. maj 2018 (Databeskyttelsesloven), § 1, stk. 2, 1.pkt.
[58] Ib Henricson, *"Politiloven med kommentarer"*, Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 40.
[59] Ib Henricson, *"Politiret",* Jurist- og Økonomforbundets Forlag, 2020, 6. udgave, s. 141.
[60] Ib Henricson, *"Politiloven med kommentarer"*, Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 40.

af oplysninger efter stk. 1 og 2 sker således efter nærmere fastsatte regler i bekendtgørelsesform fra Justitsministeriet. Den bekendtgørelse, der henvises til, er bekendtgørelse nr. 1078.

Sammenfattende betyder implementeringen af politilovens § 2 a, at politiet har fået et retligt hjemmelsgrundlag for en nyere form for politivirksomhed med det formål at kunne imødekomme det mere komplekse kriminalitetsbillede i et moderne samfund.

5.2. Implementeringen af Politilovens § 2 a

Danmark blev i februar 2015 ramt af en række terrorhændelser, hvilket satte det danske politi på en udfordrende opgave. Herefter blev der skrevet en evalueringsrapport og et udspil fra regeringen, "Et stærkt værn mod terror", som anbefalede en etablering af bl.a. en øget it- og analysekapacitet, herunder en tilvejebringelse af en fælles analyseplatform.[61] På baggrund af udspillet blev der d. 29. marts 2017 fremsat L171. Lovforslaget gik ikke ubemærket hen, og har også fået kritik fra bl.a. Institut for Menneskerettigheder, hvilket nærmere vil blive belyst i afsnit 5.3.3. På trods heraf blev lovforslaget vedtaget og implementeret d. 1. juni 2017.

Forud for lovforslagets vedtagelse fremlagde regeringen et udspil med 12 nye tiltag mod terror med ordene "*nye udfordringer kræver nye redskaber*".[62] De nye redskaber var bl.a. et ønske om at anskaffe et nyt og mere avanceret IT-system. Regeringen ville afsætte ca. 150 mio. kr. fra 2015 - 2018 til "*øget it og analysekapacitet hos PET og politiet*" og 200 mio. kr. til *"udbygning af politiets og PET's beredskabs- og overvågningsindsats".*[63] Formålet hermed var for bedre at kunne foretage tværgående informationsanalyser i et forsøg på et forhindre fremtidige terrortrusler. Nogle af ressourcerne skulle bl.a. anvendes til et nyt IT-system, som hurtigere og nemmere ville kunne registrere truende eller mistænkelig adfærd på nettet, heriblandt de sociale medier. IT-systemet, der henvises til, er det nyindkøbte POL-INTEL. Med et IT-system, der muliggør tværgående informationsanalyser, får politiet mulighed for bedre at identificere og registrere potentielle kriminelle ved hjælp af bl.a. opdateringer på Facebook eller Instagram[64], hvilket også betegnes som "open source"-kilder.

For bedre at forstå formålet og baggrunden for implementeringen af politilovens § 2 a, er det væsentligt at undersøge bemærkningerne til L171, hvilket nu vil blive belyst.

[61] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 3.
[62] Regeringens udspil "*Et stærkt værn mod terror*", 2015, s. 1.
[63] Ibid, s. 4.
[64] Ibid, s. 5.

5.2.1. Baggrund og formål med § 2 a

Forud for implementeringen af politilovens § 2 a, blev der i L171 argumenteret for baggrunden og hensigterne for at indføre en ny bestemmelse i loven. Baggrunden for implementeringen var et behov for "*en fortsat modernisering og effektivisering af dansk politi*".[65] Behovet herfor skyldes bl.a. at der de seneste år er oplevet en stigning i mere avancerede og teknologiunderstøttede kriminalitet, hvilket f.eks. er hackerangreb, identitetstyveri, organiseret berigelseskriminalitet, rocker- og bandekriminalitet og seksuelle krænkelser på internettet.[66] På baggrund heraf, er politiet udfordret og afhængig af at kunne identificere og analysere på tværs af data, for derigennem bedre at kunne genkende mønstre, og kunne disponere ressourcer på den mest effektive måde.

Det fremgår tydeligt, at formålet med implementeringen har været at "*tilvejebringe de retlige rammer for den fortsatte implementering af "intelligence-led policing" i dansk politi og for politiets ibrugtagning af en platform til tværgående analyser*".[67] Hermed får politiet hjemmel til på betryggende vis at anvende tværgående analyser af såkaldte "big data" for bedre at kunne håndtere et kriminalitetsbillede i teknologisk udvikling, både inden for og uden for strafferetsplejen.[68] Yderligere anføres det, at det daværende IT-system, inden implementeringen af § 2 a, har været ineffektivt og krævet mange ressourcer, idet dataanalyserne skulle krydstjekkes manuelt. Samtidig var risikoen for at overse visse mønstre og sammenhænge betragtelig.[69] Dette vil med implementeringen forbedres og medføre en bedre, og mere målrettet håndtering af terrortrusler i fremtiden.[70]

Som tidligere nævnt, har terrortruslerne i København i 2015 haft en betydning for politiets fremtidige virke. Udviklingen i kriminalitetsbilledet og risikoen for fremtidige terrortrusler betyder, at formålet med politilovens § 2 a, samtidig er for at kunne imødegå uvarslede hændelser og forudse kriminalitetsmønstre samt afvigelser fra normalbilledet.[71] Det angives bl.a. at ovenstående formål "*vanskeligt vil kunne løses uden brug af moderne tværgående analyseværktøjer*".[72] I forbindelse med samfundets udvikling observeres der også en udvikling inden for økonomisk it-kriminalitet, herunder med metoden "by proxy", hvor en gerningsperson har mulighed for at gemme sig bag skærmen.[73] Dette taler for at implementere et IT-system, der kan håndtere sådanne udfordringer og muliggøre

[65] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 3.
[66] Ibid, s. 4.
[67] Ibid, s. 3.
[68] Ibid, s. 5.
[69] Ibid, s. 6.
[70] Regeringens udspil "*Et stærkt værn mod terror*", 2015, s. 5.
[71] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 4.
[72] Ibid, s. 5.
[73] Ibid, s. 6.

opsporing af digitale spor. Det betyder, at selvom POL-INTEL er en del af regeringens udspil "Et stærkt værn mod terror", fremgår det tydeligt i L171 at formålet med implementeringen ikke kun er for at bekæmpe terror, men også er for at styrke politiets virke generelt.

Internettet er og bliver en større del af alles hverdag, hvad enten det tilgås som privatperson eller som led i ens arbejde. Derfor er offentligt tilgængelige kilder på f.eks. internettet via de sociale medier, nyhedsmedier, tv-udsendelser mm. en væsentlig informationskilde, som politiet har mulighed for at anvende og indhente oplysninger fra. Dette betegnes som "open source-intelligence".[74] Det fremgår af L171, at politiet i de kommende år forventer at anvende "open source"-kilder i større grad end tidligere, hvilket medfører nogle relevante overvejelser vedrørende det retlige grundlag herfor. Det er Justitsministeriets vurdering på baggrund heraf, at en sådan anvendelse af "open source"-kilder kræver en udtrykkelig lovhjemmel i politiloven.[75] I relation til dette bemærkes det i L171, at indsamling og behandling af offentlige tilgængelige informationer og kilder også skal vurderes i lyset af EMRK art. 8 om retten til privatliv.[76] I art. 8, stk. 2 angives nogle betingelser for at offentlige myndigheder må gøre indgreb i retten til privatliv. Det skal ske i overensstemmelse med loven, det skal varetage et anerkendelsesværdigt formål, og så skal det have proportionalitet i forhold til om det er nødvendigt i et demokratisk samfund for at opnå det ønskede mål. Det er Justitsministeriets vurdering, at den behandling af oplysninger, som L171 indebærer, vil kunne udgøre et indgreb efter art. 8, stk. 1. Samtidig vurderer Justitsministeriet, at implementeringen er nødvendig for at politiet har mulighed for at imødegå de udfordringer, som kriminalitetsbilledet og samfundsudviklingen medfører.[77] Justitsministeriet konkluderer afslutningsvis herpå at "*lovforslaget kan gennemføres inden for rammerne af Danmarks forpligtelser efter EMRK*".[78] Herudover vægtes det, at behandlingen af de indsamlede oplysninger kun må ske, når det vurderes til at være nødvendigt i lyset af politiets opgaver.[79] Dermed lægger L171 op til en begrænsning i retten til at behandle oplysninger efter § 2 a, således at ikke alle offentlige tilgængelige oplysninger om samfundets borgere bliver indsamlet og gjort til genstand for en tværgående informationsanalyse.

Sammenfattende fremgår det af lovforslaget, at baggrunden for implementeringen er den stødt stigende udvikling af kriminalitetsbilledet, hvilket er en følge af den teknologiske udvikling. Hermed har politiet brug for at kunne effektivisere deres arbejdsmetoder for at imødekomme dette. Herudover

[74] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 8.
[75] Ibid.
[76] Ibid, s. 21.
[77] Ibid, s. 22.
[78] Ibid.
[79] Ibid.

fremgår det, at formålet med implementeringen af § 2 a er at sikre det retlige grundlag, og den lovmæssige hjemmel for politiet til at indsamle og behandle offentligt tilgængelige oplysninger. På baggrund heraf vil politiet have de retlige rammer for forsat at implementere "intelligence-led policing". Ydermere er formålet også at sikre, at politiet har et klart retligt grundlag til at anvende et IT-system som POL-INTEL, for at kunne lave tværgående informationsanalyser. Det er vigtigt at bemærke at L171 ikke indebærer en regulering for politiets adgang til at indsamle oplysninger, men alene indebærer en regulering med det formål at sikre en klar hjemmel for politiet til at foretage tværgående informationsanalyser af oplysninger, som politiet allerede i dag kan indsamle med hjemmel i loven.[80]

5.3. POL-INTEL

Implementeringen af politilovens § 2 a var som nævnt bl.a. at sikre de retlige rammer for politiet til at anvende et nyt IT-system, der gav mulighed for at sammenkøre store mængder af data på tværs af politiet. Indkøbet af POL-INTEL blev på baggrund heraf en realitet i 2017. Politiets begejstring for indkøbet bliver der ikke lagt skjul på, hvis man henser til udtalelser som "*en revolution*" og "*et kvantespring*".[81] Samtidig hermed har Michael Kjeldgaard, chef for Nationalt Efterforskningscenter i Rigspolitiet, udtalt: "*Hvor vi tidligere brugte 80 procent af tiden på at søge oplysninger og 20 procent på efterforskning, bruger vi nu 20 procent på at søge oplysninger og 80 procent på at efterforske*".[82] Det er værd at bemærke, at navnet "POL-INTEL" kun nævnes i danske henvisninger og sammenhænge, og er derfor en dansk angivelse af IT-systemet. Begrebet findes ikke andre steder end i Danmark. POL-INTEL er indkøbt og skabt af det amerikanske softwarefirma Palantir, og er baseret på dele af Palantir's operative system ved navn "Gotham", som hos Palantir bemærkes som "*The Operating System for Global Decision Making*".[83]

5.3.1. Palantir

Palantir er et amerikansk softwarefirma grundlagt i 2003, der beskæftiger sig med datamining. Laves der en søgning på, hvad Palantir betyder, finder man ud af at intet er tilfældigt. Palantir betyder at kunne se hændelser i fremtiden, ligesom en krystalkugle. POL-INTEL er ikke en undtagelse i forhold

[80] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 13.
[81] Helene Kristine Holst & Kasper Kildegaard Sørensen, "*Vi er meget, meget sikre på, at det her bliver en succes"*, Artikel på Berlingske.dk, https://www.berlingske.dk/politik/dansk-politi-advarer-forbrydere-vi-er-klar-med-et-supervaaben
[82] Simone Scheuer-Hansen, "*Var det for meget, da politiet fangede en lommetyv med nyt supervåben?*", Artikel på Politiken.dk, https://politiken.dk/viden/Tech/art6650800/Var-det-for-meget-da-politiet-fangede-en-lommetyv-med-nyt-cyberv%C3%A5ben
[83] https://www.palantir.com/platforms/gotham/

til henvisningen med krystalkuglen, og er blot ét af de platforme som Palantir har udviklet og tilbyder. Nogle af Palantir's kunder er bl.a. den offentlige sektor i USA, hvoraf der f.eks. kan nævnes Pentagon, CIA, NSA, sundhedsministeriet og politimyndigheder i New York, New Orleans, Chicago og Los Angeles.[84] Private virksomheder er også interesseret i de datamining-redskaber, som Palantir tilbyder og generelt bestræber de sig på at kunne tilbyde deres software bredt, idet der på deres hjemmeside står: "*Big data solutions shouldn't just be for big companies*".[85]

Palantir har været udsat for en del kritik, hvilket især bunder i problematikken med at have et privat softwarefirma til at bidrage til myndighedsarbejdet rundt om i verden. Herudover har også borgerrettighedsadvokater udtalt kritik af Palantir's metoder og kaldt dem for forfatningsstridige.[86] Det kan være særdeles problematisk for bl.a. politimyndigheder eller andre offentlige myndigheder at forsvare anvendelsen af metoder, som omtales som værende forfatningsstridige af specialister og fagkyndige. Volquartzen nævner især sagen, hvor en medarbejder hos Palantir bidrog med personlige data på ca. 87 millioner Facebook-brugere til Cambridge Analytica, således der på baggrund heraf kunne dannes profiler på vælgere til brug for Donald Trumps præsidentkampagne i 2016. Palantir har som forsvar hertil udtalt, at medarbejderen gjorde det i sin fritid og fralægger sig dermed ansvaret.[87] Nok mener Palantir ikke de er politiske, men Peter Thiel, én af grundlæggerne og it-milliardær, har ydet stor støtte til Trump, herunder økonomisk støtte på 1,25 millioner dollar under valgkampen i 2016.[88] Desuden har Peter Thiel i 2009, i et selvskrevet essay, kritiseret samfundets stabilitet og velfærd i forhold til skatter, kvinder og de fattige.[89] Argumentet om ikke at være politisk anlagt kan således diskuteres, da sådanne politiske støtter og udtalelser taler herimod.

Problemstillingen ved at offentlige myndigheder anvender software fra ukontrollerede private firmaer, bliver således en risiko for at kompromittere borgerens rets- og privatlivsbeskyttelse. Ifølge Volquartzen er inddragelsen af den private sektor som magtspiller i samfundet en ukendt fare og faktor, idet det er uklart, hvilke retlige rammer der kontrollerer disse.[90] En anden bekymring ifølge Volquartzen er risikoen for anvendelse af "predictive policing" og dermed faren for stigmatisering og diskrimination af sårbare.[91] Som det allerede er konstateret, har det danske politi udtalt, at de ikke

[84] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 187.
[85] https://www.palantir.com/
[86] Mette Volquartzen, *"Forskydninger mellem det private og det offentlige",* 2018, s. 187.
[87] Ibid, s. 188.
[88] Ibid.
[89] Ibid.
[90] Ibid, s. 189.
[91] Ibid.

anvender "predictive policing" endnu, men finder det interessant. Derfor har det danske politi mulighed for at tage metoden i brug i fremtiden.

5.3.2. POL-INTEL som analyseværktøj

Som tidligere nævnt, var formålet med implementeringen af POL-INTEL, at sikre og understøtte det danske politi i deres opgavevaretagelse i et samfund, hvor kriminaliteten bliver mere teknisk og moderne. Inden implementeringen af POL-INTEL blev det analyserende politiarbejde udført at den enkelte politimand bl.a. ved brug af kendskab i lokalmiljøet eller meddelere.[92] I takt med teknologiens udvikling og dermed kriminalitetens kompleksitet blev datamængder større og dermed sværere at håndtere manuelt, hvilket indebar risiko for at overse sammenhænge. Det har betydet, at politiets tilgange til analyserelateret arbejde har været til revurdering, idet de hidtige analyseværktøjer- og tilgange ikke har været tilstrækkelige, og som nu har resulteret i indkøbet af POL-INTEL.[93]

Det overordnede formål med at implementere og indkøbe et IT-system som POL-INTEL har bl.a. været for at "*give politiet et sammenhængende it-system til bearbejdning og analyse af de store datamængder, der genereres både internt i politiet og som er tilgængelige fra eksterne datakilder*".[94] Med dét giver man udtryk for ønsket om at ændre tilgangen til politiarbejdet fremadrettet, således både ressourcer og manuelt analysearbejde bliver fordelt og anvendt, hvor det giver mening. Dette vurderes i L171 til at have en afgørende betydning, særligt for den alvorligste organiserede kriminalitet, hvor politiet hurtigere og bedre end hidtil kan være i stand til at identificere sammenhænge og relationer på tværs af sager.[95] Selvom den alvorligste organiserede kriminalitet er i fokus, så er også færdselsarbejdet nævnt som et område, hvor bl.a. effekten af tværgående informationsanalyser kan gavne. Dette kan bl.a. opnås ved at målrette færdselskontroller efter, hvor og hvornår bestemte færdselsovertrædelser finder sted.[96]

Det fremgår af høringssvar[97] fra Justitsministeriet at præciseringen af, hvornår tværgående informationsanalyser skal foretages og den nærmere regulering heraf "*mest hensigtsmæssigt fastsættes på bekendtgørelsesniveau, da det vil sikre en så konkret, teknologineutral og dækkende regulering som muligt*".[98] Dette førte til bekendtgørelse nr. 1078. Heraf fremgår det af § 3, stk. 2 at

[92] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 5.
[93] Ibid.
[94] Ibid, s. 6.
[95] Ibid.
[96] Ibid, s. 7.
[97] Kommenteret høringsoversigt vedr. Udkast til lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysning om flypassagerer).
[98] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 13.

tværgående informationsanalyser ikke må foretages som led i politiets rent administrative afgørelsesvirksomhed eller som led i generel informationssøgning. Det fremgår endvidere af L171, at der med indkøbet af POL-INTEL forudsættes at oplysninger, som angår enkeltpersoner, herunder følsomme personoplysninger, kun tilgås på systemniveau i videst mulige omfang.[99] Dette skal fortolkes på den måde at disse oplysninger kun kommer den enkelte politimedarbejder til kende når det anses for politifagligt nødvendigt, og at disse oplysninger kun i øvrigt stilles til rådighed, når det er proportionalt og nødvendigt.[100] Dette bliver bl.a. gjort ved hjælp af databeskyttelsesenheden, der blev oprettet af Rigspolitiet i 2016[101], men som i øvrigt er en vurdering, der tages af den enkelte politimedarbejder, under hensyntagen til politilovens opgavebeskrivelse i politilovens § 2. Hertil skal det dog bemærkes at der i L171 forudsættes, at analyser kun må gennemføres "*når der er en konkret og nærmere afgrænset anledning*".[102] For at sikre en sådan afgrænset anvendelse af tværgående informationsanalyser er der lagt op til at politiets systemunderstøttelse, ved enhver gennemførelse af disse analyser, stiller krav om, at analysen er tilknyttet en konkret sag.[103] Dette leder til det udgangspunkt at oplysningerne, der behandles skal pseudonyumiseres, jf. bekendtgørelse nr. 1078 § 6, stk. 1, som også skal ses i sammenhæng med bekendtgørelsens § 5, om situationer, som kan berettige en tværgående informationsanalyse. Kun i særlige tilfælde, hvor det er nødvendigt for politiet at behandle fuldt personhenførbare oplysninger, kan afmaskering af oplysningerne finde sted, jf. § 6, stk. 2 og 3. Således kan man så vidt muligt argumentere for, at der med implementeringen af POL-INTEL er taget højde for, at ikke alle behandlinger af oplysninger kan eller skal henføres til en specifik person uden nærmere grundlag herfor.

Når POL-INTEL anvendes til at foretage tværgående informationsanalyser, er det på baggrund af diverse informationskilder. Fastlæggelsen af disse informationskilder reguleres særskilt af § 8 i bekendtgørelse nr. 1078. Heraf fremgår det af stk. 1, nr. 1 at der kan være tale om "faste kilder", hvilket er registre, databaser mv. som politiet også i dag fører efter gældende ret. De såkaldte "øvrige kilder" efter stk. 1, nr. 2 er kilder som politiet efter gældende ret kan bringe i anvendelse som led i varetagelsen af deres opgaver.

Særligt at bemærke ved POL-INTEL er, at de analyser systemet udarbejder, ikke anses for et dokument, og dermed ikke er undergivet aktindsigt.[104] Bekendtgørelse nr. 1078 foreskriver i § 12, at

[99] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 14.
[100] Ibid.
[101] Ibid.
[102] Ibid, s. 27.
[103] Ibid.
[104] Ibid, s. 26.

en borger (den registrerede) ikke har indsigtsret i de oplysninger, der behandles i POL-INTEL. Den eneste mulighed for at få aktindsigt i en analyse fra POL-INTEL er, hvis der på baggrund af den tværgående informationsanalyse dannes en rapport og denne særskilt arkiveres på en sag i politiets sagsbehandlingssystem POLSAS. Hermed opnår analysen status som dokument, og giver dermed ret til aktindsigt.[105] I bekendtgørelse nr. 1078 henvises der i § 12 til særlige bestemmelser i Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (herefter kaldet retshåndhævelsesloven). I medfør af retshåndhævelseslovens § 16, stk. 4 har personer ikke ret til at få indsigt efter retshåndhævelseslovens § 15 i oplysninger behandlet i POL-INTEL og det samme gælder indsigt efter lovens § 13, stk. 2, jf. § 14, stk. 2. Det problematiske i dette er, at borgeren vil have svært ved at få indsigt i analysen og den data, der er anvendt hertil. Dermed stilles borgeren i en situation af uvidenhed, og får dermed svært ved bl.a. at kunne berigtige disse data, samt svært ved at kunne efterprøve om indgrebet har været proportionelt. Samtidig hermed er der en risiko for at blive udsat for en eventuel uhensigtsmæssig profilering. EMRK art. 13 om retten til effektive retsmidler, som vil blive belyst i afsnit 6.6, er på baggrund heraf i risiko for at blive illusorisk, hvis ikke det er muligt at få aktindsigt i analyserne.

Justitsministeriets generelle opfattelse af POL-INTEL er, at det er "*udtryk for, hvordan en moderne politistyrke bør løse sine opgaver*"[106], og overordnet set er der med L171 lagt op til mange kompetence- og analysemæssige fordele for det danske politi ved implementeringen. Dog har implementeringen ikke kun indsamlet positive kommentarer, men har især også modtaget kritik og skeptiske overvejelser fra bl.a. Institut for Menneskerettigheder, hvilket nu vil blive belyst.

5.3.3. Kritik af POL-INTEL

POL-INTEL er ikke et ukendt system og har fået en del kritik. Couchman beskriver bl.a. hvordan et sådant IT-system kan medføre "the chilling effect".[107] Ytringsfriheden i art. 10 påvirkes af "the chilling effect", idet Couchman henviser til nogle studier, der viser, at kvinder og yngre mennesker har en tendens til at "selv-censurere" som resultat af overvågning.[108] Som det fremgår af L171 og som tidligere er belyst, anvender politiet også "open source"-kilder til tværgående informationsanalyser, og "the chilling effect" er således ikke udelukket for også at kunne ske i Danmark. Særligt har Institut for Menneskerettigheder i høringssvar fra Justitsministeriet udtalt kritik omkring anvendelsen af "open source"-kilder. Kritikken går bl.a. på at offentlige tilgængelige kilder

[105] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 26.
[106] Ibid, s. 13.
[107] Hannah Couchman, "*Policing by Machine*", Rapport fra Liberty, 2019, s. 29.
[108] Ibid, s. 30.

ikke altid er korrekte eller fremskaffet på lovlig vis.[109] Der kan dermed være visse farer ved at analysere på sådanne data, idet de kan føre til uhensigtsmæssig eller uretmæssig profilering, eller i værste tilfælde tvangsindgreb.

Et andet kritikpunkt har også været algoritmerne, som POL-INTEL anvender. Jesper Lund, formand for IT-Politisk Forening, har bl.a. udtalt kritik af algoritmerne. Han taler bl.a. om de såkaldte "feedback loops"[110], som betyder, at hvis politiet har fokus på at patruljere i et bestemt område, vil dette område typisk angives af algoritmen til at være et sted, hvor der er en større kriminalitetsrate. Deraf opstår den "feedback loop" som ovenfor beskrevet, fordi systemet på baggrund heraf vil sende mere patruljering derud, og sådan fortsætter det. Et andet kritikpunkt fra Jesper Lund vedrørende algoritmer er, at "*systemet nedarver de fordomme, der ligger implicit i den data, som mennesker fodrer systemet med*".[111] Særligt her nævner han problemet ved forudseende politiarbejde, altså "predictive policing", idet det er baseret på data, som ikke er fri for bias.

Herudover har IT-Politisk Forening udtrykt en bekymring for, hvorvidt politiet differentierer mellem mistænkte personer og ikke-mistænkte når de indsamler oplysninger.[112] IT-Politisk Forening tilkendegiver således en frygt for om alle i Danmark bliver gjort til genstand for en tværgående informationsanalyse, eller om de holder det begrænset til de mistænkte. Dette er også en bekymring fra Institut for Menneskerettigheder. De bemærker, at det er særligt problematisk, hvis der foretages indgreb i EMRK art. 8, idet de skriver "*da det vil være muligt at foretage meget præcise kortlægninger af borgernes private forhold, herunder personer, som ikke er mistænkte*".[113] Dermed går bekymringen på om L171 kan danne grundlag for en mere generel overvågning i Danmark, og dermed mistænkeliggørelse af alle danskerne uden de retssikkerhedsmæssige garantier, der normalt følger ved efterforskningsskridt.[114] Det samme bemærker IT-Politisk Forening til politiets mulighed for at foretage tværgående informationsanalyser. Særligt bemærker de, meget lig Institut for Menneskerettigheder, at det "*skaber meget detaljerede personprofiler, hvor personens færden,*

[109] Kommenteret høringsoversigt vedr. Udkast til lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysning om flypassagerer), s. 7.
[110] Sally Jensen, "*Et supervåben mod kriminalitet eller en sprængfarlig bombe af diskrimination*?", Artikel på responsmedie.dk, https://www.responsmedie.dk/pol-intel/
[111] Ibid.
[112] Kommenteret høringsoversigt vedr. udkast til lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysning om flypassagerer), s. 11.
[113] Ibid, s. 13.
[114] Ibid.

interesser, kontakter og vaner kan undersøges, og der derfor er tale om en meget alvorlig indgriben i en persons privatliv".[115]

Således kan det konkluderes, at selvom L171 modtager stor begejstring og optimisme fra politiets side, får det samtidig meget kritik fra bl.a. Institut for Menneskerettigheder og IT-Politisk Forening. Meget af kritikken angår hovedsagligt risikoen for generel masseovervågning, herunder risikoen for at blive diskrimineret og dermed gøre indgreb i EMRK art. 14, men også risikoen for at gøre indgreb i retten til privatliv efter art. 8, hvilket begge nærmere vil blive diskuteret i afsnit 6.

5.4. Sammenfatning

Sammenfattende kan det konkluderes, *at* implementeringen af politilovens § 2 a fastsætter de retlige rammer for politiet til at foretage tværgående informationsanalyser, og muliggør anskaffelsen af et IT-system som POL-INTEL. Desuden kan det udledes, *at* formålet med bestemmelsen er for at imødekomme et ændret kriminalitetsbillede, hvormed politiets virke skal moderniseres og at dette også muliggør anvendelsen af "predictive policing". Herudover kan det konkluderes, *at* POL-INTEL er indkøbt af softwarefirmaet Palantir, *at* systemet er baseret på algoritmer, der kan medføre problematikker såsom forudindtagelser, samt *at* det er usikkert, hvor grænsen går når offentlige myndigheder, såsom politiet, anvender software fra private virksomheder, hvormed der ingen kontrol er. Derudover kan det fastslås, *at* borgernes ret til at få aktindsigt er indskrænket og det derved kan være uklart, hvilke oplysninger der er behandlet og analyseret, samt uklart hvorvidt man er blevet udsat for en profilering. Dette begrænser muligheden for, at borgerne kan kontrollere, berigtige eller få afprøvet et eventuelt tvangsindgreb eller profilering, baseret på disse analyser.

Implementeringen af politilovens § 2 a har skabt debat og som nævnt udsat for kritik fra forskellige fagpersoner. Kritikken går på risikoen for at krænke visse menneskeretlige rettigheder, hvilket i det følgende afsnit vil blive belyst og diskuteret.

[115] Kommenteret høringsoversigt vedr. udkast til lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysning om flypassagerer), s. 14.

6. Menneskeretlige problemstillinger

I det følgende vil EMRK art. 8 og 14 blive gennemgået for at undersøge, hvad den nærmere regulering indebærer. Efter gennemgang af bestemmelserne vil hhv. afsnit 6.2 og 6.4 nærmere belyse de problemstillinger, der aktualiseres ved anvendelsen af POL-INTEL. Dette vil herefter lede til en analyse af relevant retspraksis fra EMD, hvor art. 8 vurderes i forhold til masseovervågning.

6.1. Art. 8 – Retten til privatliv og familieliv

Én af de grundlæggende menneskerettigheder, som er relevant at diskutere i forhold til POL-INTEL, er EMRK art. 8. Denne bestemmelse angår retten til privatliv og familieliv, og det primære formål hermed er at "*beskytte individet mod uberettigede indgreb fra offentlige myndigheder*".[116] EMRK art. 8 har følgende ordlyd:

> *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 fremgår det af stk. 1, at de fire beskyttelsesinteresser er retten til respekt for privatliv, familieliv, hjem og korrespondance. Herefter påhviler der staten positive forpligtelser for at beskytte disse interesser, hvilket bl.a. indebærer at afstå fra at gøre indgreb i de beskyttede individuelle sfærer, og at yde bistand for at realisere rettighederne efter art. 8.[117] Bestemmelsens stk. 2 angår hovedsagligt statens negative forpligtelser, men betingelserne heri har ligeledes en betydning for at fastlægge omfanget af de positive forpligtelser efter stk. 1 og hvorvidt staten i den konkrete situation har opfyldt disse.[118] Udgangspunktet i stk. 1 kan fraviges efter stk. 2, hvis indgrebet (1) har hjemmel i loven, (2) er nødvendigt i et demokratisk samfund og (3) hvis det er af hensyn til national sikkerhed, offentlig

[116] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 887.
[117] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 644.
[118] Ibid, s. 763.

tryghed, den økonomiske velfærd i det pågældende land, for at forebygge uro eller forbrydelse, for at beskytte sundhed eller sædelighed eller for at beskytte andres ret og frihed.

6.1.1. De fire beskyttelsesinteresser

De fire beskyttelsesinteresser efter EMRK art. 8 er retten til respekt for privatliv, familieliv, hjem og korrespondance.

Begrebet "privatliv" er tæt knyttet til beskyttelsen af familieliv, hjem og korrespondance og er derfor et bredt begreb, idet det ofte skal vurderes i relation til disse.[119] Kjølbro nævner en række eksempler på, hvad der kan være omfattet af begrebet "privatliv", men påpeger også at det ikke er muligt at give en udtømmende definition. Dog fremhæver han, at det kan angå en persons fysiske og psykiske identitet, samt en persons fysiske og sociale identitet.[120] Det handler bl.a. om, at en person skal have ret til at udvikle sig, skabe relationer til andre mennesker og kunne leve privat uden uønsket opmærksomhed.[121] Alt sammen uden udefrakommende indblanding. Retten til respekt for privatliv omhandler både private forhold og erhvervsmæssige forhold, f.eks. udøvelse af dét erhverv man ønsker.

Når en offentlig myndighed indsamler, behandler og anvender persondata, der kan henføres til bestemte individer, er der en pligt for staten til at sikre passende garantier til beskyttelse heraf. Samtidig skal staten muliggøre en form for selvbestemmelse for borgeren.[122] Hvis politiet indsamler oplysninger såsom navn, adresse og informationer om strafbare forhold er det omfattet af retten til privatliv. Særligt interessant for denne fremstilling nævner Kjølbro politiets anvendelse af databaser. I de tilfælde, hvor politiet overvåger personers færden og bevægelser på baggrund af en registrering i en database, er det omfattet af retten til privatliv.[123] Det samme gælder ved opbevaring af vævsprøver, DNA, fotografier af en person, fingeraftryk og offentligt tilgængelige oplysninger, særligt når der er tale om forhold, som hører fortiden til.[124] Overvågning af personer på offentlige steder kontra overvågning af personer i deres hjem defineres forskelligt i forhold til retten til privatliv. Personer udsætter sig selv for overvågning i det offentlige rum bl.a. ved iagttagelse af andre personer og offentlige overvågningskameraer. Kjølbro nævner, at EMD har udtalt at "privatliv" og "hjem"

[119] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 649.
[120] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 859.
[121] Ibid.
[122] Ibid.
[123] Ibid, s. 862.
[124] Ibid.

ikke finder anvendelse ved steder, hvortil offentligheden har fri adgang.[125] Dog kan offentlig overvågning blive omfattet af begrebet "privatliv", hvis denne data bliver systematisk eller permanent opbevaret.[126]

Retten til respekt for "familieliv" indeholder, som udgangspunkt negative forpligtelser for staten, hvormed staten bør undlade at foretage indgreb.[127] Bestemmelsen angår et eksisterende familieliv og altså ikke retten til at stifte en familie, herunder adoption[128], men beskytter dog i et vist omfang et påtænkt familieliv. Påtænkt familieliv anses som værende ønsket om at indgå ægteskab og leve sammen.[129]

Tredje beskyttelsesinteresse efter art. 8 er retten til respekt for hjem. Begrebet "hjem" og beskyttelsen heraf er et selvstændigt konventionsbegreb, og dermed ikke afhængig af den nationale regulering.[130] "Hjem" bliver defineret på baggrund af forhold, som udgør en "*tilstrækkelig og vedvarende tilknytning til et bestemt sted*".[131] Hertil kræves det, at dette bestemte sted udgør den pågældendes aktuelle bolig.[132] Når man vurderer, hvorvidt der er tale om et hjem, der er omfattet af art. 8, er det ikke begrænset til den traditionelle forståelse af, hvad et hjem er.[133] Det kan derfor også omfatte skurvogne eller mobile hjem. Hvis definitionen af "hjem" ikke er opfyldt, er man ikke beskyttet efter art. 8. Indgreb i hjemmet vil typisk udgøre efterforskningsskridt i strafferetsplejen, hvilket bl.a. kan være ransagninger og beslaglæggelser.[134]

Den fjerde og sidste beskyttelsesinteresse efter art. 8 er retten til respekt for korrespondance. Denne beskyttelsesinteresse, sammen med retten til respekt for privatliv, er særlig interessant og vigtig for specialets problemformuering. Begrebet "korrespondance" skal forstås bredt og omfatter både skriftlige meddelelser, og mundtlige meddelelser, hvad enten det er elektroniske eller ikke-

[125] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 869.
[126] Ibid.
[127] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 706.
[128] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 875.
[129] Ibid, s. 878.
[130] Ibid, s. 881.
[131] Ibid.
[132] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 753.
[133] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 882.
[134] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 749.

elektroniske meddelelser.[135] Der skal ikke meget til for at en handling udgør et indgreb i retten til respekt for privatliv og korrespondance efter art. 8. Således kan brevåbning, aflytning af telefonsamtaler, telefax og e-mail, hemmelige indgreb i meddelelseshemmligheden, indhentelse af teleoplysninger og indhentelsen af IP-adresser for at identificere en bruger af en computer, udgøre et indgreb i retten til korrespondance.[136] Det er desuden uden betydning om korrespondancen er af privat, professionel eller erhvervsmæssig karakter.[137]

Legalitetskravet skærpes, når der foretages hemmelige indgreb i korrespondance. Hvis der foretages telefonaflytning, anses det som værende et alvorligt indgreb i retten til privatliv og korrespondance. På baggrund heraf kræves der strengere krav til retsgrundlaget således at der skal være nogle retssikkerhedsgarantier, der sikrer mod misbrug fra myndighedernes side.[138] Særligt når man snakker om masseovervågning, gælder der de samme minimumsgarantier som hvis der var tale om overvågning rettet mod enkeltpersoner.[139] Kjølbro oplister de minimumsgarantier, som skal og bør være fastlagt når der foretages overvågning. Minimumsgarantierne er herefter: Afgrænsning af de personer, der kan risikere at blive overvåget, angivelse af de kriminalitetsformer, herunder karakteren, der kan begrunde et indgreb, tidsmæssig begrænsning af indgrebet, procedure for behandling og opbevaring af data, herunder en optegnelse over indgreb og resultater, således der kan udføres kontrol og slutteligt regler om destruktion, særligt i tilfælde, hvor der sker frifindelse.[140] Hvis en stat anvender masseovervågning med henblik på at sikre statens sikkerhed, gælder der ikke et krav om "begrundet mistanke" eller "forudgående retskendelse", hvilket ville være tilfældet, såfremt overvågningen var på individniveau. EMD har anerkendt at staten er overladt en skønsmargin når det kommer til at masseovervåge for at sikre statens sikkerhed.[141] Dette er dog ikke uden begrænsninger, hvilket vil blive belyst i afsnit 6.5.1.

6.1.2. Legalitetskravet

Beskyttelsen efter EMRK art. 8, stk. 1 angår individers ret til privatliv, familieliv, hjem og korrespondance. Undtagelsen hertil fremgår af art. 8, stk. 2, hvorefter indgreb, for at være forenelig

[135] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 884.
[136] Ibid, s. 885.
[137] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 756.
[138] Ibid, s. 979.
[139] Ibid.
[140] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag 2020, 5. udgave, s. 980.
[141] Ibid.

med konventionen, skal være "i overensstemmelse med loven" eller som det direkte fremgår af bestemmelsen "in accordance with the law".

Legalitetskravet består af to led. For det første er der et krav om, at indgrebet skal have hjemmel i national lovgivning, og for det andet er der kvalitative hjemmelskrav.[142] Kravet om hjemmel i national lovgivning er en vurdering, der foretages af de nationale myndigheder. Dette vil som udgangspunkt ikke blive tilsidesat af EMD.[143] Dog gælder dette udgangspunkt ikke, hvis nationale prøvelsesorganer ikke har vurderet spørgsmålet. Andet led om kvalitative hjemmelskrav betyder, at de nationale retsregler skal være forenelige med retsstatsprincippet, altså et krav om tilgængelighed og forudsigelighed i retstilstanden.[144] Kjølbro understreger, at problematikken typisk ikke vedrører kravet om tilgængelighed, men derimod kravet om forudsigelighed. Forudsigeligheden indebærer at retsreglerne skal være formuleret klart og præcist, så borgerne har mulighed for at forstå og forudsige, hvilke konsekvenser en given handling kan have. Dog er der ikke krav om, at man skal kunne forudsige noget med sikkerhed, idet retsreglerne skal kunne tilpasse sig tiden og den løbende udvikling i samfundet.[145] Kravet om klarheden og forudsigeligheden af retsgrundlaget stiger i takt med indgrebets intensitet.[146]

Graden af tilgængelighed og forudsigelighed "*afhænger af indholdet af reguleringen, det regulerede retsområde, og antallet og karakteren af de private, som er berørt af reguleringen*".[147] Som også er beskrevet tidligere, er der et skærpet legalitetskrav når myndigheder foretager overvågning af borgerne, og dermed større krav til tilgængeligheden og forudsigeligheden i retstilstanden. Dog betyder kravet om forudsigelighed ikke, at borgerne skal kunne forudsige indgrebet, når der er tale om hemmelig overvågning.[148] Det er særlig vigtigt ved indgreb som hemmelig overvågning, at borgerne i tilstrækkelig grad beskyttes mod vilkårlighed fra det offentlige. I denne vurdering lægger EMD vægt på om afgørelsen af at foretage overvågning er tilstrækkelig begrundet, om borgeren er underrettet herom og om der er mulighed for domstolsprøvelse af afgørelsen.[149] Heri er også et krav om, at borgeren har mulighed for at anfægte indgrebet, og mulighed for at få foretaget en

[142] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag 2020, 5. udgave, s. 837.
[143] Ibid.
[144] Ibid, s. 839.
[145] Ibid, s. 840.
[146] Jens Elo Rytter, "*Individets grundlæggende rettigheder*", Karnov Group, 2021, 4. udgave, s. 211.
[147] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 841.
[148] Roman Zakharov mod Rusland, para. 229.
[149] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 842.

interesseafvejning i forhold til dennes interesser og samfundets interesser, hvilket også indebærer en proportionalitetsvurdering.[150]

Når der foretages indgreb såsom aflytning, overvågning, indsamling og opbevaring af persondata, skal der være fastlagt en række retssikkerhedsgarantier for at forhindre misbrug og vilkårlighed. Dette er bl.a. foranstaltninger og procedurer vedrørende varighed, opbevaring, brug, fortrolighed og destruktion.[151] Kravet om retssikkerhedsgarantier gælder også når indgreb er begrundet i statens sikkerhed.[152] EMD har udtalt at selv om argumentet er, at statens sikkerhed er på spil, skal der foretages en form for kontradiktorisk procedure for en uafhængighed myndighed. Den uafhængige myndighed skal have mulighed for at prøve begrundelsen for beslutningen, når der er tale om indgreb, der påvirker grundlæggende menneskerettigheder.[153]

De legitime formål, der kan begrunde et indgreb fra offentlige myndigheder i de fire beskyttelsesinteresser, er som nævnt i art. 8, stk. 2 oplistet som "den nationale sikkerhed", "den offentlige tryghed", "landets økonomiske velfærd", "forebyggelse af uro eller forbrydelse", "beskyttelse af sundheden eller sædeligheden" eller "beskyttelse af andres rettigheder og friheder". Disse legitime formål er udtømmende og skal fortolkes indskrænkende.[154] EMD's vurdering af om staten opfylder et legitimt formål efter stk. 2 er oftest uproblematisk, idet formålene er formuleret bredt og således relativt nemt kan begrunde et indgreb i de beskyttede rettigheder.[155]

6.1.3. Nødvendighedskravet (krav om proportionalitet)

Nødvendighedskravet efter art. 8, stk. 2 betyder, at der skal foretages en konkret afvejning af forholdet mellem hensynet til beskyttelsen af individets privatliv, familieliv, hjem og korrespondance og hensynet til de modstående samfunds- og individinteresser.[156] Dette kan også fortolkes som et krav om proportionalitet. Når EMD skal vurdere om nødvendighedskravet er opfyldt, er det en bedømmelse af om begrundelsen for indgrebet i den beskyttede rettighed er relevant og

[150] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 842.
[151] Ibid, s. 845.
[152] Ibid, s. 847.
[153] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 765.
[154] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 849.
[155] Ibid, s. 850.
[156] Jens Elo Rytter, "*Individets grundlæggende rettigheder*", Karnov Group, 2021, 4. udgave, s. 211.

tilstrækkelig.[157] Kravet betyder også at indgrebet skal være "nødvendigt i et demokratisk samfund" og dermed skal "*modsvare et presserende socialt behov*".[158]

Som nævnt tidligere har staten en vis skønsmargin, når der skal vurderes om et indgreb i en konventionssikret rettighed er nødvendig, samt hvilke midler, der skal anvendes hertil. Selve omfanget af denne skønsmargin skal bedømmes i relation til lovgivningsprocessen, hertil hvilke afvejninger, der er foretaget og hvor grundigt tilblivelsen af loven er undersøgt. Graden af skønsmargin stiger i takt med graden af afvejninger og vurderinger ved lovgivningsprocessen.[159] Dette er dog ikke absolut, idet statens skønsmargin varierer alt efter karakteren af den rettighed, der gøres indgreb i, rettighedens betydning og intensitet for borgeren, karakteren af de anerkendelsesværdige formål for indgrebet og særligt om der er tale om et retsområde under udvikling.[160] Når der er tale om at gøre indgreb for at beskytte statens sikkerhed, har staten en vid skønsmargin.[161] Den vide skønsmargin kan dog blive et problem, hvis indgreb ikke alene foretages over for mistænkte personer, men også foretages over for ikke-mistænkte personer. I disse tilfælde skal lovgivningen særskilt regulere, hvilke ikke-mistænkte personer, der kan blive gjort til genstand for et indgreb[162], og bør i videst mulige omfang begrænses for ikke at krænke rettighederne i EMRK.

Legalitetskravet indeholder et krav om tilstrækkelige garantier til beskyttelse mod misbrug, og det samme indeholder nødvendighedskravet. Bedømmelsen heraf vurderes ud fra karakter, omfang og varighed af indgrebet, herunder en regulering af, hvad der kan begrunde indgrebet og hvem der har kompetence til at udføre indgrebet.[163] Idet både legalitetskravet og nødvendighedskravet indebærer, at der skal foreligge tilstrækkelige garantier mod vilkårlighed og misbrug, lægger det op til at foretage en samlet vurdering af legalitet og nødvendighed.

6.1.4. Offentlige myndigheders behandling af oplysninger

Når offentlige myndigheder opbevarer data på enkeltpersoner, er det omfattet af retten til privatliv.[164] Offentlige tilgængelige oplysninger om enkeltpersoner kan også været omfattet af retten til privatliv, når disse oplysninger "*indsamles og opbevares systematisk i offentlige myndigheders registre*".[165]

[157] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 851.
[158] Ibid.
[159] Ibid, s. 852.
[160] Ibid, s. 853.
[161] Ibid, s. 855.
[162] Ibid, s. 981.
[163] Ibid, s. 980.
[164] Ibid, s. 958.
[165] Ibid, s. 959.

Dette gælder særligt, når der er tale om oplysninger, der ligger langt tilbage i tiden. Hvis offentlige myndigheder opbevarer og behandler data om enkeltpersoner uden mulighed for at berigtige disse, vil det udgøre et indgreb i retten til privatliv[166] og der vil på baggrund heraf kræves, at myndigheden kan retfærdiggøre det efter art. 8, stk. 2. Det er ikke et krav at de indsamlede oplysninger faktisk bliver anvendt for at kunne udgøre et indgreb efter art. 8, men blot opbevaringen af disse er i sig selv nok.[167]

Efterretningstjenester er én af de offentlige myndigheder, der indsamler og behandler data. Men når efterretningstjenester udfører hemmelig overvågning af borgerne, kan det være konventionsstridigt. Hemmelig overvågning er således kun i overensstemmelse med konventionen, "*hvis den er strengt nødvendig med henblik på at beskytte de demokratiske institutioner*".[168] Hvis opbevaringen eller registreringen af data sker i et hemmeligt register, skal der foretages en særlig afvejning af interesser for at det er legitimt. Afvejningen bliver på den ene side hensynet til statens sikkerhed og bekæmpelse af kriminalitet sammenholdt med karakteren af indgrebet og på den anden side individets ret til respekt for privatliv.[169] Som tidligere nævnt, har staten en vid skønsmargin når det kommer til at gøre indgreb i rettigheder efter EMRK. Men når der foretages hemmelig overvågning, indskrænkes denne skønsmargin, hvilket medfører strengere krav til legaliteten og proportionaliteten (nødvendighedskravet). Det betyder, at den nationale lovgivning nærmere skal regulere en vis begrænsning i efterretningstjenestens beføjelser, hvilket bl.a. kan være begrænsninger i forhold til, hvilke personer, der må foretages hemmelig overvågning af, betingelserne herfor og særligt at der foreligger en tilstrækkelig beskyttelse af borgeren i form af retssikkerhedsgarantier.[170]

Hvis efterretningstjenester opbevarer og behandler oplysninger af personer i et register, kan de pågældende personer have en interesse i at få adgang og indsigt i disse, evt. med henblik på at berigtige dem. Det kan dog være berettiget, af hensyn til at sikre effektiviteten af det hemmelige overvågningssystem, at nægte en sådan adgang.[171] EMD har i tidligere sager udtalt sig om problematikken. Én af sagerne var Brinks-sagen.[172] Sagen drejede sig om, at Brinks ikke måtte få adgang til, hvilke oplysninger den hollandske efterretningstjeneste havde registreret om ham. De

[166] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, 959.
[167] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 666.
[168] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 960.
[169] Ibid.
[170] Ibid.
[171] Ibid.
[172] Brinks mod Holland.

eneste oplysninger han kunne få var forældede og udgjorde ikke en risiko for at afsløre tjenestens arbejdsmetoder. Her udtalte EMD, at begrænsningen ikke udgjorde en krænkelse, idet den var begrundet i statens sikkerhed. Herudover var der effektive retssikkerhedsgarantier i den pågældende sag, eftersom to nationale domstole havde haft mulighed for at vurdere de tilbageholdte oplysninger, samt mulighed for at vurdere om hemmeligholdelsen var nødvendig. Det betyder derfor også, at såfremt der er en begrænsning i aktindsigten og der ikke er passende og effektive retssikkerhedsgarantier, er det en krænkelse af art. 8. Kjølbro understreger dog, at der kan opstå situationer, hvor der er en tvist mellem myndigheden og borgeren omkring oplysningerne i det hemmelige register. I disse tilfælde er det et krav, at "*borgerens processuelle rettigheder respekteres, hvilket kan indebære krav om adgang til oplysninger, så der er effektiv adgang til prøvelse*".[173] På baggrund heraf fremstår retsstillingen angående adgang til oplysninger i et hemmeligt register lidt uklar. Det beror derfor på en konkret vurdering, der skal sammenholdes med en vurdering efter art. 8, stk. 2, hvorvidt der bør gives aktindsigt i indsamlede oplysninger som led i overvågning. Men generelt giver art. 8 ikke krav på aktindsigt i hemmelige registre.[174]

Når politiet indsamler data, kan de i den forbindelse registrere oplysninger om personer i deres registre. Politiet kan i visse situationer have en interesse i at opbevare sådan en registerring, selv når der ikke er rejst tiltale. Problematikken opstår dog, hvis politiet registrerer væsentlige oplysninger om personer på et spinkelt grundlag, og uden mulighed for at personen kan berigtige dem, hvilket kan udgøre en krænkelse af art. 8.[175] Et eksempel herpå findes i Khelili-dommen.[176] Her havde politiet igennem flere år registreret en kvinde som "prostitueret" i deres database, på trods af, at hun ikke var dømt for prostitution. Den valgte registrering skete derfor blot på baggrund af en mistanke og det vurderede EMD var en krænkelse af art. 8. Det kan derfor medføre en række retssikkerhedsmæssige spørgsmål, hvis personer, som nævnt ovenfor, ikke har mulighed for aktindsigt i registreringerne og dermed ikke har mulighed for berigtigelse, hvis der er en risiko for, at man er fejlagtigt registreret på baggrund af en mistanke.

Offentlige myndigheder kan også udveksle og videregive oplysninger. Hvis en myndighed videregiver følesomme personoplysninger om private til en anden myndighed, vil det udgøre et

[173] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 962.
[174] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 687.
[175] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 969
[176] Khelili mod Schweiz.

indgreb i retten til privatliv.[177] Dette er uagtet at den modtagne myndighed har tavshedspligt, da oplysningerne ved videregivelsen vil blive kendt for en bredere personkreds og evt. med et andet formål end de oprindeligt er indsamlet til.[178] Særligt når der er tale om videregivelse af sundhedsoplysninger, er kravet til legaliteten skærpet. Som udgangspunkt har personer krav på fortrolighed af sundhedsoplysninger, når disse er tilvejebragt ved lægelig behandling.[179] Dog påpeger Kjølbro, at videregivelse af sådanne oplysninger kan ske til brug for politiets eller domstolenes behandling af en straffesag, hvis videregivelsen er underlagt betingelser, der iagttages, således art. 8 overholdes.

6.2. Problemstillinger ved anvendelse af POL-INTEL ift. EMRK art. 8

Justitsministeriet har i deres høringssvar selv udtalt, at POL-INTEL kan udgøre et indgreb i EMRK art. 8. Samtidig konkluderer Justitsministeriet, at implementeringen kan gennemføres på en sådan måde, så Danmark opfylder sine forpligtelser efter EMRK i henseende til art. 8, stk. 2.[180] Efter en gennemgang af art. 8 og særligt stk. 2, er det dog relevant nærmere at diskutere de potentielle problemstillinger som POL-INTEL aktualiserer.

Hvis politiet øger patruljeringen i et boligkvarter eller foretager en ransagning på baggrund af en tværgående informationsanalyse i POL-INTEL, kan det påvirke retten til privatliv, familieliv og hjem. Begrebet "privatliv" blev bl.a. defineret som retten til at leve et socialt liv uden udefrakommende påvirkning eller forstyrrelse. Såfremt der sker øget patruljering omkring ens hjem, hvor ens privatliv og familieliv særligt finder sted, er det muligt at personer bliver påvirket og forstyrret og måske tænker ekstra over deres adfærd. På den anden side kan øget patruljering være tryghedsskabende, hvilket man som borger i en vis grad må finde sig i. Ransagning af ens hjem er en større problemstilling end øget patruljering i denne henseende, hvis grundlaget herfor er baseret på en analyse i POL-INTEL. Alt dette kan medvirke til at påvirke personers hverdag uhensigtsmæssigt, og folk kan komme til at føle sig uberettiget overvåget, hvilket kan udgøre et indgreb efter art. 8.

Som det er konstateret, krævers der efter legalitetskravet nogle særlige minimumsgarantier for at en offentlige myndighed kan foretage overvågning, særligt overvågning i korrespondance, som bl.a. anvendelse af POL-INTEL kan anvendes til. Disse minimumsgarantier indebærer som det første krav

[177] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 963.
[178] Ibid, s. 671.
[179] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 964.
[180] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 22.

om en afgrænsning af personer, der kan risikere at blive overvåget, særligt hvis det også er ikke-mistænkte personer, der bliver indsamlet oplysninger af. Bekendtgørelse nr. 1078, som nærmere regulerer politiets brug af POL-INTEL, regulerer ikke en sådan afgrænsning af personer, der kan risikere at blive genstand for en tværgående informationsanalyse. Dermed har politiet mulighed for at overvåge og behandle oplysninger om personer uden begrænsning, herunder også af ikke-mistænkte personer.

Udover en afgrænsning af personer, kræves der også efter minimumsgarantierne en angivelse af de kriminalitetsformer og karakteren heraf, der kan berettige indgreb. Ydermere skal der angives en tidsmæssig begrænsning for indgrebet, procedure for behandling og opbevaring af data og regler om destruktion. Bekendtgørelse nr. 1078 angiver i §§ 4 og 5 at tværgående informationsanalyser kan anvendes, når det er nødvendigt til at bringe strafbar virksomhed til ophør og til konkret fareafværgelse. Herudover kan det også anvendes til øvrige formål og "andre opgaver"[181], der har tilknytning til politiets virksomhed, heriblandt kontrol og tilsynsopgaver, samt bistand til andre myndigheder. Hverken § 4 eller § 5 angiver konkrete kriminalitetsformer eller karakteren heraf, men er i stedet formuleret bredt og giver således en vid adgang til at foretage tværgående informationsanalyser. Efter § 9 er der fastsat særlige regler for opbevaring og sletning af oplysninger og §§ 13-15 regulerer behandlingssikkerheden, som er i henhold til kapitel 12 i lov om retshåndhævende myndigheders behandling af personoplysninger.[182] Sammenfattende kan det således konstateres, at mange af minimumsgarantierne fremgår af bekendtgørelse nr. 1078, men at der mangler en afgrænsning af personkreds, der kan risikere at blive udsat for indgreb efter politilovens § 2 a og at kriminalitetsformer, der kan berettige indgreb og karakteren heraf ikke er nærmere afgrænset, jf. angivelsen af øvrige formål og "andre opgaver". De manglende minimumsgarantier rejser retssikkerhedsmæssige problematikker. Dette skyldes at der ikke foreligger tilstrækkelige og effektive sikkerhedsforanstaltninger mod vilkårlige indgreb og misbrug. Dermed kan anvendelse af POL-INTEL indebære en krænkelse af art. 8.

Efter bekendtgørelse nr. 1078 § 12 er personer begrænset i at få adgang til de oplysninger, der behandles i POL-INTEL. Som det er nævnt i forhold til nødvendighedskravet, giver art. 8 som udgangspunkt ikke ret til aktindsigt i hemmelige registre. I den omtalte Brinks-sag statuerede EMD ikke en krænkelse, idet tilbageholdelsen af oplysningerne var blevet vurderet af to nationale domstole. Dette hænger samtidig sammen med det Kjølbro belyser, hvorefter der ved indgreb som overvågning,

[181] Bekendtgørelse nr. 1078 af 20. september 2017 (Bekendtgørelse om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser), § 5, stk. 1, nr. 6.
[182] Lov nr. 410 af 27. april 2017 (Retshåndhævelsesloven).

skal sikres mod vilkårlige indgreb ved, at der er mulighed for domstolsprøvelse af afgørelsen. Når personer er forhindret i at få indsigt i oplysningerne, som er registreret og evt. behandlet i POL-INTEL, bliver det svært at få afprøvet indgrebets proportionalitet ved domstolene. Det er samtidig hermed også konstateret, at lovhjemlen hos staterne til at gøre indgreb efter art. 8, stk. 1 efter stk. 2, som udgangspunkt ikke vil blive tilsidesat af EMD, hvis nationale prøvelsesorganer har vurderet spørgsmålet. Herudover har EMD også som nævnt udtalt, at på trods af at argumentet er statens sikkerhed, skal der foretages en form for kontradiktorisk procedure, hvor en uafhængig myndighed skal have mulighed for at prøve spørgsmålet, hvis indgrebet kan påvirke grundlæggende menneskerettigheder. Som det fremgår både af regeringens udspil "Et stærkt værn mod terror" og L171, var hovedargumentet for implementeringen af politilovens § 2 a, og indkøbet af POL-INTEL at forhindre terror, og blev også iværksat efter terrorhændelserne i København i 2015. Politilovens § 2 a og anvendelsen af POL-INTEL kan potentielt påvirke bl.a. EMRK art. 8, hvilket Justitsministeriet ligeledes selv har udtalt. POL-INTEL og de tværgående informationsanalyser er ikke blevet vurderet af prøvelsesorganer i Danmark endnu, hvilket kan være begrundet i uvidenheden omkring at et indgreb evt. er besluttet på baggrund af oplysninger i POL-INTEL, og den begrænsning til aktindsigt som § 12 i bekendtgørelse nr. 1078 indeholder. Derfor kan hjemlen til POL-INTEL i dansk lovgivning som udgangspunkt risikere at blive tilsidesat af EMD, såfremt EMD i fremtiden får en tvist herom.

Nationale stater har, som fastlagt, en vid skønsmargin. Denne skønsmargin skal vurderes i forhold til lovgivningsprocessen. Danmark har indhentet høringer fra relevante fagfolk, herunder IT-Politisk Forening og Institut for Menneskerettigheder. Dog mangler lovgivningsprocessen en afvejning af, hvilke personer, der skal tåle at blive indsamlet og behandlet oplysninger af i POL-INTEL. Såfremt det konstateres, at Danmark har en vid skønsmargin i forhold til at gøre indgreb i art. 8, er dette ikke uden begrænsninger. Særligt hvis POL-INTEL ikke alene anvendes over for mistænkte personer, men også anvendes over for ikke-mistænkte personer, og der ikke foreligger en særskilt regulering heraf, kan det aktualisere menneskeretlige problemstillinger. I relation til dette kan spørgsmålet om, hvad der berettiger en mistanke ligeledes diskuteres. Denne diskussion er særlig relevant i forhold til "predictive policing". Hvis politiet anvender POL-INTEL til at forudse potentielle gerningspersoner og ofre eller potentielle områder med kriminalitet, vil en sådan beslutning foretages på baggrund af data som algoritmen tilføres. Disse data vil ofte være baseret på oplysninger fra langt tilbage i tiden, hvilket tidligere i specialet er fastlagt til at være omfattet af retten til privatliv. Retssikkerhedsgarantien mod vilkårlige indgreb sættes på prøve, hvis man mistænkeliggør en befolkning på baggrund af fortiden for at forudse fremtiden. I Kelili-dommen blev Kelili mistænkt

og registreret som en prostitueret, uden at være anholdt for prostitution. Som det tidligere blev konkluderet, udtalte EMD, at denne registrering og mistænkeliggørelse var en krænkelse af EMRK art. 8. Det aktualiserer centrale retssikkerhedsmæssige spørgsmål, hvis POL-INTEL anvendes til at registrere væsentlige oplysninger om personer ud fra et spinkelt grundlag, som i Kelili-dommen. Således risikerer personer at blive registreret eller profileret som mistænkt, potentiel gerningsperson eller offer, hvilket særligt er problematisk, hvis ikke der er mulighed for at berigtige oplysningerne.

Sammenfattende kan det derfor konstateres, at anvendelsen af POL-INTEL aktualiserer visse retssikkerhedsmæssige og menneskeretlige problemstillinger i relation til EMRK art. 8, og kan udgøre et indgreb i borgernes ret til respekt for privatliv, familieliv, hjem og korrespondance.

6.3. Art. 14 – Forbud mod diskrimination

En anden grundlæggende menneskerettighed findes i art. 14, som forbyder diskrimination. Ordlyden af art. 14 er således:

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

Når det skal vurderes om en stat gør indgreb i diskriminationsforbuddet, skal der ifølge Kjølbro tages stilling til en række forskellige forhold. Forholdene, der skal vurderes er (1) om der sker en forskelsbehandling i en af de konventionssikrede rettigheder, (2) om forskelsbehandlingen er mellem sammenlignelige situationer og (3) om forskelsbehandlingen er saglig begrundet og proportionel.[183]

Rettigheden til respekt for privatliv efter art. 8 indeholdt hovedsagligt positive forpligtelser for staten, hvorimod art. 14 først og fremmest indeholder negative forpligtelser. Dog er dette ikke absolut, og der følger således også positive forpligtelser med bestemmelsen, hvilket dog udgør en begrænset rolle.[184] Blandt de positive forpligtelser for staten kan bl.a. nævnes myndigheders effektive efterforskning af racistisk, religiøst motiveret vold og overgreb, således det fører til straffeforfølgning. Det samme gælder ligeledes, hvor det er på grund af seksuel orientering.

[183] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1277.
[184] Ibid.

Undladelse heraf kan krænke diskriminationsforbuddet.[185] Dog er det uden større betydning, hvorvidt der er tale om en negativ eller positiv forpligtelse, da prøvelsen er den samme.[186]

6.3.1. Anvendelsesområde

Bestemmelsens og dermed beskyttelsens anvendelsesområde for art. 14 er væsentligt mere indsnævret end de andre bestemmelser i EMRK, idet den er "*begrænset til de i denne konvention anerkendte rettigheder og friheder*".[187] Det betyder at hvis klagens genstand ikke vedrører én eller flere af de materielle rettigheder i EMRK, finder beskyttelsen efter art. 14 ikke anvendelse.

Ved vurderingen af, om der er tale om diskrimination i relation til en rettighed, er det uden betydning om rettigheden kræves efter konventionen, eller om den stilles til rådighed af staten. Den eneste krav er, at diskriminationen blot skal vedrøre en rettighed. Hvis en person behandles mindre favorabelt end andre, uden rimelig grund herfor, og den favorable behandling ikke er påkrævet efter EMRK, er det omfattet af diskriminationsbegrebet.[188]

6.3.2. Kravet om identiske eller sammenlignelige situationer

Bedømmelsen af om der foreligger diskrimination, indledes med en vurdering af om andre personer i en identisk eller sammenlignelig situation, nyder en mere fordelagtig behandling. Selve vurderingen af sammenlignelige situationer er ikke stringent, og visse forskelle på personer udelukker ikke at situationen kan sammenlignes. Det er klagers ansvar at godtgøre, at situationen er sammenlignelig eller identisk.[189] Hvis der konstateres, at der er tale om forskelsbehandling, skal det dernæst vurderes om der foreligger en saglig begrundelse herfor.[190] Myndighederne har en vis skønsmargin når de skal vurdere om der er tale om sammenlignelige situationer, og det samme gælder bedømmelsen af, om der er en saglig og objektiv begrundelse for forskelsbehandlingen.[191] Det kan derfor give anledning til tvivl, hvorvidt der er tale om en saglig forskelsbehandling.

---

[185] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1277.
[186] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 10-59 samt tillægsprotokollerne)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 979.
[187] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1278.
[188] Ibid, s. 1279.
[189] Ibid, s. 1283.
[190] Ibid.
[191] Ibid, s. 1286.

Der skal ikke kun ske en vurdering af, om der er sket forskelsbehandling i sammenlignelige situationer, men også om der i sager, der ikke kan sammenlignes, er blevet behandlet ens. Dermed sagt skal ikke-sammenlignelige sager som udgangspunkt ikke behandles ens.[192] Samtidig hermed kan man differentiere mellem direkte og indirekte diskrimination. Er diskriminationen direkte, er det som følge af ordlyden af en lov eller ordlyden af en myndigheds begrundelse i en afgørelse. Er der derimod tale om en indirekte diskrimination, er det på baggrund af en administration af neutrale regler i praksis.[193] Indirekte diskrimination er sværere at påvise, og EMD vil i bevisvurderingen heraf være mere lempelig.[194]

Et andet forhold, der har betydning i vurderingen, er karakteren af de berørte personer. Staten har en vis forpligtelse til at beskytte særlige sårbare og udsatte personer. Hvis der på baggrund af et politisk eller racistisk motiv f.eks. er udøvet en hårdfør anholdelse, der i en vis grad kan karakteriseres som mishandling, skal diskriminationen kunne bevises "*uden for enhver rimelig tvivl*"[195], hvilket kan være svært.

6.3.3. Diskriminationsbegrebet og diskriminationsgrundene

Diskrimination efter art. 14 foreligger når en forskelsbehandling "*ikke er objektivt og rimeligt begrundet*"[196], hvilket betyder at begrundelsen ikke tjener et legitimt og anerkendelsesværdigt formål og ikke er proportional. Hvis en klager godtgør, at der er behandlet forskelligt i en sammenlignelige situation, er det op til staten at bevise at forskelsbehandlingen er berettiget. Det kan i visse sammenhænge være unødvendigt at vurdere art. 14 selvstændigt, hvis der er statueret en krænkelse af en af de andre konventionssikrede rettigheder, som medfører en forskelsbehandling.[197]

Som det fremgår af art. 14, omfatter beskyttelsen "*sex, race, color, language, religion, political or other opinion, national or social origin, association with a nation minority, property, birth or other status*". Dette kaldes også diskriminationsgrundene. Opregningen af diskriminationsgrundene er ikke udtømmende, jf. "or other status". Selve diskriminationen skal blot knytte sig til en persons karaktertræk eller status.[198] Der skal foretages en udvidende fortolkning når det skal vurderes, om "or

[192] Peer Lorenzen m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 10-59 samt tillægsprotokollerne)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave, s. 981.
[193] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1286.
[194] Ibid, s. 1287.
[195] Ibid.
[196] Ibid, s. 1288.
[197] Ibid.
[198] Jens Elo Rytter, "*Individets grundlæggende rettigheder*", Karnov Group, 2021, 4. udgave, s. 438.

other status" udgør en forskelsbehandling.[199] Som eksempel på andre forhold, der kan udgøre forskelsbehandling, har EMD bl.a. behandlet klager vedrørende alder, bopæl, fysisk handicap, psykiske lidelser, militærrang mm.[200]

Særligt når der er tale om forskelsbehandling på grund af køn kræver det "*meget tungtvejende og overbevisende grunde*"[201] for at kunne anses for berettiget. Målsætningen om at fremme ligestillingen mellem køn anses af EMD til at være et af de vigtigste mål for Europarådets medlemslande.[202] Hvis et medlemsland begrunder forskelsbehandlingen af køn med henvisning til traditioner, generelle opfattelser, sociale opfattelser eller generelt socioøkonomiske forhold, er dette ikke gyldige argumenter.[203] Det er dog ikke alle kønsmæssige forskelle, der udgør en diskrimination. Et eksempel herpå kan være, hvis en medlemsstat tilskriver forældremyndigheden til moderen af et født barn uden for ægteskab, hvilket i praksis tidligere er antaget til ikke at være diskrimination.[204]

Forskelsbehandling kan også være baseret på nationalitet eller statsborgerskab, selvom det ikke direkte er opregnet i art. 14, hvorimod "national oprindelse" og "tilhørsforhold til nationalt mindretal" er. Når der sker forskelsbehandling på grund af nationalitet, statsborgerskab eller national oprindelse, kræves der, for at retfærdiggøre det, "*tvingende eller meget tungtvejende grunde*"[205], og det samme gælder, når der er tale om forskelsbehandling på grund af tro, religion eller seksuel orientering. Eksempler på andre momenter, der kan udgøre diskrimination, og som ikke fremgår direkte af art. 14, er bl.a. forskelsbehandling på grund af bopæl og karakter af opholdstilladelse.

Det fremgår direkte af art. 14, at forskelsbehandling på grund af race eller etnisk oprindelse kan medføre diskrimination, også kaldet racediskrimination. EMD har udtalt, at de to begreber er tæt forbundne og overlapper hinanden. Ydermere har EMD vurderet at forskelsbehandling på baggrund heraf ikke kan retfærdiggøres i et nutidigt demokratisk samfund.[206] Bevisbyrden for, at der ikke er tale om diskrimination kan overgå til staten, hvis en bestemt befolkningsgruppe statistisk rammes hårdere end andre og der hermed skabes en formodning for diskrimination.[207] Myndighederne har et særligt ansvar for at håndtere overgreb, som er begrundet i race og nationalitet og Kjølbro fremhæver

[199] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1289.
[200] Ibid.
[201] Ibid, s. 1290.
[202] Ibid, s. 1291.
[203] Ibid.
[204] Ibid, s. 1295.
[205] Ibid, s. 1296.
[206] Ibid, s. 1301.
[207] Ibid, s. 1304.

bl.a. at samfundet skal fordømme racisme og at det bør sikres, at minoriteterne har tillid til at myndighederne ikke udsætter dem for diskrimination.[208]

6.4. Problemstillinger ved anvendelse af POL-INTEL ift. EMRK art. 14

Anvendelsen af POL-INTEL i det danske politi muliggør benyttelsen af det forudseende element, uagtet om det bliver benyttet i dag. Derfor er "predictive policing" relevant at diskutere i relation til beskyttelsen i art. 14. Som det er erfaret med "predictive policing", som belyst i afsnit 4.3, er der ved anvendelse af metoden en særlig øget risiko for falske negativer og falske positiver, bias og "præ-kriminalisering". Disse risici udgør samlet set en sandsynlig fare for, at uskyldige bliver mistænkt for noget de ikke har gjort, fordi politiet ud fra data i POL-INTEL vurderer, at de muligvis vil begå kriminalitet ud i fremtiden.

Når det forudseende element i politivirksomheden er baseret på algoritmer, giver det anledning til en række spørgsmål. Er algoritmen baseret på amerikanske tendenser og data, eller har Danmark selv haft indflydelse herpå? Hvor stammer dataene fra og hvem beslutter, hvilke data, der skal være en del af algoritmen? Særligt når man ikke har en forståelse af systemet bag POL-INTEL, kan man til en vis grad frygte at data og at algoritmen er udarbejdet af det amerikanske softwarefirma Palantir, hvorfor risikoen for amerikanske tendenser i det danske politi kan være en bekymring. USA er bl.a. kendt for diskrimination af befolkningsgrupper ud fra race og etnicitet, og derfor bør POL-INTEL ikke være baseret på amerikanske forhold, men bør derimod være tilpasset forholdene i Danmark for at undgå en sådan bias. Algoritmen i sig selv udgør ikke et selvstændigt problem. Dog bliver algoritmen et problem for hele udøvelsen af politivirksomheden, hvis algoritmen indeholder vurderingsmomenter som køn, race, national oprindelse, etnicitet, sprog, religiøs eller politisk tilknytning eller tilhørsforhold til et nationalt mindretal, og der træffes beslutning om indgreb eller overvågning mm. på baggrund heraf.

Ydermere er det blevet fastslået i specialet, at der en væsentlig begrænsning i indsigtsretten i de oplysninger systemet behandler. Det er som udgangspunkt borgeren, der skal bevise, at der er sket forskelsbehandling i en sammenlignelig situation. Når man ikke har mulighed for at få oplyst, hvilke oplysninger, der fremgår af systemet, og man heller ikke har mulighed for at få oplyst, om et indgreb er truffet på baggrund heraf, er det svært at fastslå om der er tale om diskrimination efter art. 14. Det stiller således personer i en retssikkerhedsmæssig ubalance i forhold til staten, fordi der ikke i samme

[208] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1305.

omfang kan stilles krav til staten om at retfærdiggøre indgreb truffet på baggrund af POL-INTEL. I relation til dette kan det også diskuteres, hvem ansvaret skulle gøres gældende overfor, såfremt det var muligt? Beslutningerne træffes på baggrund af nogle algoritmer i et IT-system, altså en maskine. Vi har ikke med et menneske at gøre, der har truffet en beslutning om at foretage et indgreb eller mistænkeliggøre nogen ud fra manuelt politiarbejde. I denne situation ville det være nemmere at pege på én i forhold til ansvar. Som Volquartzen fremhæver, kan det betvivles om politiet har en forståelse for IT-systemet, og hvordan systemet træffer beslutninger. Det gør det dermed svært for politiet at sikre, at der ikke sker forskelsbehandling i sammenlignelige situationer, og at der dernæst ikke er tale om diskrimination efter art. 14, fordi de ikke selv er inde og arbejde med oplysningerne.

Det kan derfor sammenfattende konstateres, at anvendelsen af POL-INTEL aktualiserer en række problemstillinger i forhold til EMRK art. 14. Det er derfor vigtigt ved anvendelsen af IT-systemer, der kan anvendes som beslutningstager hos offentlige myndigheder, at der er en forståelse af det bagvedliggende system og en forståelse for, hvilke forhold, systemet lægger vægt på. Ellers er det svært at sikre ligebehandling uden risiko for bias og herudover også svært at retfærdiggøre, hvis der skulle være behandlet forskelligt. Særligt når der er tale om "predictive policing" bør der foreligge en dybere forståelse for beslutningsprocessen for at sikre, at der ikke sker en krænkelse af art. 14.

6.5. Praksis ved Den Europæiske Menneskerettighedsdomstol

Når EMD skal træffe afgørelse og dermed vurdere, om der er sket en krænkelse af en eller flere rettigheder i EMRK, sker det bl.a. på baggrund af en dynamisk fortolkning af konventionen. Det betyder at bestemmelserne skal vurderes i lyset af "*den teknologiske, sociale og moralske samfundsudvikling, samt ikke mindst retsudviklingen i staterne*".[209] Derfor er de to afgørelser, hhv. Centrum for Rättvisa mod Sverige og B.B.W. m.fl. mod Storbritannien, vigtige for at bidrage til fortolkningen af retstilstanden, idet begge afgørelser er afsagt af Storkammeret i 2021. Afgørelserne Szabó og Vissy mod Ungarn fra 2015, og Roman Zakharov mod Rusland fra 2016 er ligeledes vigtige i fortolkningen af retstilstanden, idet afgørelserne stadig er relativt nye og sidstnævnte afgørelse ligeledes er en afgørelse fra Storkammeret.

[209] Frederik Harhoff (red.), Ulrike Barten, Sten Schamburg-Müller m.fl., *"Folkeret"*, Hans Reitzels Forlag, 2017, 1. udgave, s. 519 og Jens Elo Rytter, "*Individets grundlæggende rettigheder*", Karnov Group, 2021, 4. udgave, s. 83, med henvisning til afgørelserne Tyrer og Mazurek.

6.5.1. Retspraksis vedr. masseovervågning

6.5.1.1. Klass m.fl. mod Tyskland

Klass m.fl. mod Tyskland er en afgørelse af ældre dato, idet den er afsagt i 1978. På trods heraf er afgørelsen stadig relevant, fordi den tillægges betydning i nyere afgørelser i bedømmelsen af hemmelig overvågning i relation til art. 8 og i forhold til vurderingsmomenterne i art. 8, stk. 2. Klagernes argument for, at der forelå en krænkelse af art. 8 var, at myndighederne ikke var pålagt at underrette de berørte personer, når overvågningen var afsluttet. I den forbindelse afskar det disse personer i at få efterprøvet beslutningen og udøvelsen af indgrebet.[210] Formålet med den hemmelige overvågning var for at beskytte den nationale sikkerhed.[211]

EMD bemærker indledningsvist, at hemmelig overvågning indeholder et krav om, at det skal være "*strictly necessary for safeguarding the democratic institutions*".[212] Vurderingen af art. 8, stk. 2 skal tage udgangspunkt i om indgrebet er i overensstemmelse med loven, hvilket det i denne sag var.[213] Dernæst bemærkede EMD også, at kravet om "strictly necessary" var opfyldt, idet formålet med at sikre den nationale sikkerhed med rette sikkerhedsforanstaltninger var berettiget. I bedømmelsen vægtede EMD i denne afgørelse at terrorhandlinger er under udvikling i Europa og at kriminaliteten bliver mere avanceret, hvorfor stater kan være nødsaget til at tage hemmelig overvågning i brug.[214] På baggrund heraf mente EMD ikke at sådanne indgreb kunne undgås for at sikre de demokratiske institutioner og den nationale sikkerhed. I den pågældende sag var juridisk kontrol af den hemmelige overvågning gennem domstolsprøvelse ikke muligt efter den tyske lovgivning. Ifølge EMD udgjorde dette en risiko for misbrug, men fordi der var indledende kontrol af indgrebet, anså EMD det ikke for afgørende at der manglede en efterfølgende kontrol.[215]

Det forhold, at myndighederne ikke var pålagt at underrette de berørte om indgrebet, gav ikke anledning til større problematikker. EMD udtalte, at overvågningen kan vare i flere år og en underretning kan bringe formålet hermed i fare, samt afsløre arbejdsmetoder og i værste tilfælde efterretningstjenestens medarbejdere. Ydermere fandt EMD det umuligt at foretage en underretning

[210] Klass m.fl. mod Tyskland, para. 10.
[211] Ibid, para. 44.
[212] Ibid, para. 42.
[213] Ibid, para. 43.
[214] Ibid, para. 48.
[215] Ibid, para. 56.

i alle tilfælde. Når overvågningen var afsluttet og det blev vurderet, at formålet ikke længere kunne bringes i fare, skulle underretning gives.[216]

På baggrund af ovenstående konkluderede EMD, at overvågningen var "strengt nødvendig" i et demokratisk samfund for at forhindre kriminalitet og forstyrrelse af orden efter art. 8, stk. 2, og at der var foretaget tilstrækkelige sikkerhedsforanstaltninger for at forhindre vilkårlighed og misbrug.

Klagerne argumenterede ligeledes for, at det var en krænkelse af art. 13 at der ikke blev givet underretning om indgrebet. EMD lagde vægt på, at hemmeligholdelsen af indgrebet for de pågældende personer gjorde det besværligt for disse, hvis ikke ligefrem umuligt, at søge oprejsning.[217] EMD konstaterede, at hensigten med at udsætte underretningen til det tidspunkt, hvor der ikke længere var risiko for at bringe formålet i fare, ikke medfører en krænkelse af art. 13. Så snart underretningen kunne ske fik klageren adgang til effektive retsmidler.

EMD konkluderede derfor på baggrund af ovenstående, at der i den pågældende sag, hverken var sket en krænkelse af art. 8 eller art. 13.

6.5.1.2. Roman Zakharov mod Rusland

Roman Zakharov mod Rusland er en afgørelse fra 2015 afsagt i Storkammeret. Sagen drejede sig om, hvorvidt hemmelig aflytning og overvågning var i strid med EMRK art. 8 og 13.

Roman Zakharov påstod i sagen, at den hemmelige overvågning fra efterretningstjenesten FSB i Rusland krænkede hans ret til respekt for privatliv og korrespondance, og at han ikke havde tilstrækkelige sikkerhedsforanstaltninger til rådighed.[218] Lovgivningen i Rusland tillod masseovervågning for at kunne udføre operationelle efterforskningsaktiviteter[219], og dette var ikke begrænset til specifikke grupper af personer.

Rusland argumenterede som det første for, at Roman ikke kunne karakteriseres som offer for en eventuel krænkelse af art. 8, fordi han ikke havde klaget over, at han var blevet overvåget.[220] Efter art. 34 er der krav om, at en person skal være "directly affected" for at en klage kan indbringes for EMD. Men EMD udtaler i denne afgørelse, at den blotte eksistens af hemmelig overvågning udgør en risiko for, at personer udsættes for en potentiel krænkelse. EMD fastslog herefter kriterierne for,

[216] Klass m.fl. mod Tyskland, para. 58.
[217] Ibid, para. 68.
[218] Roman Zakharov mod Rusland, para. 3.
[219] Ibid, para. 11.
[220] Ibid, para. 149.

at man ved hemmelig overvågning kunne anses for klageberettiget. Kriterierne indebar en vurdering af omfanget af de personer, som den hemmelige overvågning kunne påvirke og tilgængeligheden af effektive retsmidler.[221] EMD konstaterede således, at kravet om "direkte påvirkning" ikke kan gøres gældende, hvor der er tale om hemmelig overvågning, som alle kan gøres til genstand for.[222] Derfor havde Roman ret til at indgive en klage efter art. 34.

For at indgreb i art. 8, stk. 1 ikke udgør en krænkelse, skal indgrebet kunne retfærdiggøres efter art. 8, stk. 2. EMD har udviklet seks minimumsgarantier, der skal sikre mod misbrug og som bør være foreskrevet i loven. De seks garantier, der skal angives, er karakteren af de lovovertrædelser, der kan give anledning til overvågning, kategorier af personer, der skal tåle overvågningen, tidsbegrænsning af indgrebet, procedure for indsamling, behandling og opbevaring af data, foranstaltninger ved videregivelse af data og regler om destruktion.[223]

I forhold til vurderingen af legitime interesser og beskyttelsen af statens sikkerhed overfor krænkelsen af grundlæggende menneskerettigheder, har staten en bred skønsmargin, hvis blot effektive sikkerhedsforanstaltninger til at beskytte mod misbrug iagttages.[224] Særligt i forhold til sikkerhedsforanstaltningerne er der ringe mulighed for de berørte til at klage til domstolene og anfægte lovligheden, hvis ikke disse underrettes om indgrebet i forbindelse med at indgrebet er afsluttet. Den russiske lovgivning gav ikke mulighed for sådan en underretning på noget tidspunkt og gav heller ikke adgang til de oplysninger, der var indsamlet og behandlet.[225] I Klass m.fl. mod Tyskland udtalte EMD, at den manglende underretning ikke var problematisk. Dette skyldtes bl.a. at der i den pågældende sag var indledende kontrol af indgrebet, hvilket der ikke var i Roman Zakharov mod Rusland. Derfor er dette ikke i modstrid med Klass m.fl. mod Tyskland, idet de foreliggende omstændigheder er forskellige. EMD bemærkede i relation hertil, at det var ønskeligt, at der var juridisk kontrol eller domstolsprøvelse for at garantere uafhængighed, upartiskhed og korrekt procedure.[226]

EMD udtalte kritik af at den russiske lovgivning ikke indeholdte effektive garantier mod vilkårlighed og misbrug, særligt når der var tale om hemmelig overvågning som politiet direkte havde adgang til. Derudover definerede lovgivningen ikke klart i hvilke tilfælde en offentlig myndighed kunne benytte sig af hemmelig overvågning. Opbevaringen af data var heller ikke reguleret, og derfor kunne

[221] Roman Zakharov mod Rusland, para. 171.
[222] Ibid, para. 174-175.
[223] Ibid, para. 231.
[224] Ibid, para. 232.
[225] Ibid, para. 302.
[226] Ibid, para. 234.

irrelevant data blive opbevaret uden at der var fastsat regler for opbevaring og destruktion. På baggrund heraf fandt EMD, at lovgivningen ikke fastsatte effektive sikkerhedsforanstaltninger og at lovgivningen ikke begrænsede sig til, hvad der er "nødvendigt i et demokratisk samfund" efter art. 8, stk. 2. Derfor forelå der en krænkelse af art. 8.[227]

Ved vurderingen af art. 13, udtalte EMD, at den russiske lovgivning ikke gav adgang til effektive retsmidler til personer, der mente, at de havde været udsat for hemmelig overvågning. På baggrund af disse fund og den nære tilknytning til klagen ved vurderingen af art. 8, fandt EMD ikke grund til at behandle art. 13 selvstændigt.[228]

6.5.1.3. Szabó og Vissy mod Ungarn

Afgørelsen Szabó og Vissy mod Ungarn blev afsagt d. 12. januar 2016. I den pågældende sag skulle EMD tage stilling til, hvorvidt hemmelig masseovervågning var i strid med EMRK art. 8 og 13.

De to ungarske klagere i sagen påklagede den ungarske lovgivning, som tillod efterretningstjenesten TEK at foretage hemmelig masseovervågning, med det formål at forhindre terror. Hovedpåstanden var at loven ikke i tilstrækkelig grad opfyldte kravene i art. 8, stk. 2, og ikke indeholdte tilstrækkelige garantier til at sikre mod misbrug og vilkårlighed. Den hemmelige masseovervågning bestod bl.a. i at foretage hemmelig ransagning og overvågning af hjem, tjekke fysisk post og e-mails, monitorere elektronisk kommunikation og datatransmissioner og registrere alt relevant data, hvilket relaterer sig til art. 8 om retten til privatliv, hjem og korrespondance. Påstanden var, at der ikke var tilstrækkelige sikkerhedsforanstaltninger i loven og det dermed medførte en krænkelse af menneskerettighederne. Klagerne ønskede herudover også retslig kontrol af overvågningen. EMD skulle derfor træffe afgørelse om, hvorvidt der lovmæssigt var truffet de nødvendige foranstaltninger til at sikre mod vilkårlige indgreb og misbrug.

EMD bemærkede som det første, at beføjelser til at foretage hemmelig overvågning af borgere kun er i overensstemmelse med konventionen, hvis det er "strengt nødvendigt" for at sikre de demokratiske institutioner med henvisning til dommen i Klass m.fl. mod Tyskland.[229] Hvis ikke en lovgivning, der tillader hemmelig overvågning er "strengt nødvendigt" som et generelt hensyn og er for at sikre de demokratiske institutioner, vurderer EMD overvågningen til at kunne misbruges af

[227] Roman Zakharov mod Rusland, para. 302-304.
[228] Ibid, para. 307.
[229] Szabó og Vissy mod Ungarn, para. 54.

myndighederne, især når disse har avanceret teknologi til rådighed.[230] Ligesom i afgørelsen af Roman Zakharov mod Rusland nævnte EMD også her de seks minimumsgarantier, der skal være reguleret.[231]

Herefter bemærkede EMD, at den ungarske lovgivning muliggjorde hemmelig overvågning af alle borgere i landet, og at loven ikke fastsatte kategorien af personer, som kunne gøres til genstand for indgrebet.[232] EMD udtalte i den forbindelse: "*It is of serious concern, however, that the notion of "persons concerned identified ... as a range of persons" might include any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens*".[233] Derfor konstaterede EMD, at kategorien af personer var for bred, og vurderede, at myndigheden på baggrund heraf undgik at skulle retfærdiggøre relationen mellem de berørte personer og forebyggelsen af terror. Her lagde EMD dog også vægt på, at den moderne og teknologiske udvikling i kriminalitetsbilledet nødvendiggør anvendelsen af avanceret teknologi og forebyggende foranstaltninger, heriblandt masseovervågning. Men samtidig understregede vigtigheden af, at den nævnte udvikling også samtidig bør medføre en udvikling i effektive sikkerhedsforanstaltninger for borgerne.[234] På baggrund heraf konkluderede EMD, at de ungarske sikkerhedsforanstaltninger var mangelfulde.[235]

Afslutningsvis fandt EMD, at justitsministeren generelt er ude af stand til at foretage vurderingen af, hvad der er "strengt nødvendigt", særligt pga. omfanget af personer, der er omfattet af hemmelig masseovervågning og med hensyn til, hvad der er på spil ved sådanne gennemgribende indgreb.[236] Derfor er en justitsminister ikke kompetent ved vurderingen af art. 8, stk. 2. I forlængelse heraf bemærkede EMD, at den hemmelige overvågning aldrig var blevet udsat for juridisk kontrol i Ungarn, og dermed var det ikke muligt at vurdere fordele og ulemper.[237] Den juridiske kontrol, heriblandt domstolsprøvelse, kan sikre uafhængighed, upartiskhed og korrekt procedure, når der er tale om indgreb i individets grundlæggende rettigheder. Dog fandt EMD at muligheden for juridisk kontrol i Ungarn var begrænset, idet personer udsat for hemmelig overvågning, var udvidende om indgrebet og ikke fik det oplyst.[238]

På baggrund heraf fandt EMD, *at* den ungarske lovgivning ikke havde de nødvendige sikkerhedsforanstaltninger, *at* overvågningen potentielt kunne påvirke alle borgere, *at* den

[230] Szabó og Vissy mod Ungarn, para. 73.
[231] Ibid, para. 56.
[232] Ibid, para. 66.
[233] Ibid, para. 67.
[234] Ibid, para. 68.
[235] Ibid, para. 70.
[236] Ibid, para. 75.
[237] Ibid, para. 77.
[238] Ibid, para. 82.

avancerede teknologi muliggjorde indsamling af massedata. samt *at* der manglende juridisk kontrol. Derfor statuerede EMD, at der forelå en krænkelse af art. 8.

I relation til vurderingen af art. 13 udtalte EMD, at bestemmelsen ikke skal fortolkes på en sådan måde at der kan stilles krav om et retsmiddel mod den nationale lovgivning i staten.[239] På baggrund heraf konkluderede EMD at den manglende domstolsprøvelse af overvågningen ikke var en krænkelse af art. 13.[240]

6.5.1.4. Centrum för rättvisa mod Sverige

Afgørelsen fra Storkammeret afsagt d. 25. maj 2021 var indbragt af fonden Centrum för rättvisa mod Sverige. Påstanden i klagen var, at den svenske lovgivning vedrørende masseovervågning af kommunikation, også kaldt "signals intelligence"[241], krænkede retten til privatliv og korrespondance efter art. 8. Særligt for denne sag i forhold til de tre foregående afgørelser var, at der blev anvendt begrebet "bulk interception"[242] om masseovervågningen. EMD tog således i denne sag stilling til en mere vidtgående masseovervågning end de foregående, som blot muliggjorde masseovervågning. Formålet med "bulk interception" i denne sag var for at sikre den nationale sikkerhed.[243] Derudover var påstanden også, at lovgivningen ikke indeholdte effektive retsmidler efter art. 13.

I vurderingen af om Centrum för rättvisa kunne indbringe klagen efter art. 34, uagtet at fonden var direkte krænket af lovgivningen, tillagde EMD vægt på de samme kriterier som i Roman Zakharov mod Rusland. Kriterierne var herefter: Omfanget af de personer som den hemmelige overvågning kunne påvirke og tilgængeligheden af effektive retsmidler.[244] Fordi der var tale om hemmelig overvågning, der potentielt kunne påvirke alle personers kommunikation, fandt EMD at en undersøgelse af den indgivet klage var berettiget.[245]

---

[239] Mulighed for domstolsprøvelse er ikke et krav efter art. 13. Retten til effektive retsmidler indeholder, udover opretning af allerede skete krænkelser, også et forebyggende og kompenserende element. Dette kan bl.a. være et objektivt kontrolorgan. Se nærmere Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1253.
[240] Szabó og Vissy mod Ungarn, para. 93.
[241] Definitionen af "signals intelligence" er at indsamle, behandle, analysere og rapportere efterretninger fra elektroniske signaler, Ibid, para. 14.
[242] "Bulk interception" er en proces af indsamling og behandling af data, hvor graden af indgreb i individets rettigheder efter art. 8 stiger i takt med at processen skrider frem. Processen medfører at en stor mængde data indsamles, hvormed også unødvendige data indsamles, jf. para. 239. Dermed får stater indblik i en stor mængde data på individer, uden at der er belæg herfor.
[243] Centrum för rättvisa mod Sverige, para. 22.
[244] Roman Zakharov mod Rusland, para. 171.
[245] Centrum för rättvisa mod Sverige, para. 177.

EMD bemærkede særligt i afgørelsen, at vi lever i en stadig mere digital tidsalder, og dermed foregår størstedelen af kommunikationen i dag digitalt. Derfor bliver masseovervågning en mere fremherskende metode for at indsamle efterretninger og identificere mulige trusler.[246] I takt med den digitale udvikling oplever man samtidig en udvikling i terrorisme og cyberangreb, som er en alvorlig trussel mod den nationale sikkerhed. Som konsekvens heraf udtalte EMD i denne afgørelse, at ved vurderingen af masseovervågning, er man nødt til at tillade stater en vis teknologisk kapacitet for at imødekomme udviklingen, dog med en regulering af sikkerhedsforanstaltninger for at hindre vilkårlighed og misbrug.[247] Ligesom afgørelserne Roman Zakharov mod Rusland og Szabó og Vissy mod Ungarn tillagde EMD også her vægt på minimumsgarantierne, der skal forhindre misbrug.[248] Derudover udtalte EMD tillige, at i sager vedrørende masseovervågning, hvor risikoen for misbrug er stor, er det ønskeligt, at der er mulighed for juridisk kontrol, for at sikre uafhængighed, upartiskhed og en ordentlig procedure.[249] Særligt for denne sag var EMD's stillingtagen til om "bulk interception" var i overensstemmelse med konventionen. Fokus var derfor på om der var tilstrækkelige og effektive foranstaltninger etableret mod misbrug, og om overvågningen blev gjort til genstand for "end-to-end" sikkerhedsforanstaltninger.[250]

Ved vurderingen af om indgrebet efter art. 8, stk. 2 er "nødvendigt i et demokratisk samfund", er staten tillagt en bred skønsmargin ved vurderingen af, hvordan dette bedst opnås.[251] Det samme udtalte EMD i Roman Zakharov mod Rusland. Særligt når der er tale om masseindsamling af data kan disse indeholde personlige informationer af privat karakter, der f.eks. identificerer geografiske lokationer, korrespondancer og mapping af sociale medier. EMD udtalte tillige at graden af indgreb i individets rettigheder efter art. 8 stiger i takt med at processen med behandlingen af oplysninger skrider frem.[252] Selvom art. 8 ikke i sig selv forbyder masseovervågning og staten har en bred skønsmargin for at beskytte den nationale sikkerhed, så udtalte EMD i afgørelsen, at når staten anvender et system til masseovervågning, skal det pågældende skønsmargin indsnævres og dertil skal der fastlægges sikkerhedsforanstaltninger.[253] Behovet for sikkerhedsforanstaltninger stiger når behandling af personlige oplysninger er underlagt en automatiseret behandling.[254] På baggrund heraf udledte EMD i denne afgørelse en række andre vurderingsmomenter end minimumsgarantierne, som

[246] Centrum för rättvisa mod Sverige, para. 236.
[247] Ibid, para. 237.
[248] Ibid, para. 249.
[249] Ibid, para. 250. Samme blev lagt til grund i Roman Zakharov mod Rusland, para 233 og Klass m.fl. mod Tyskland, para. 55-56.
[250] Ibid, para. 274.
[251] Ibid, para. 252.
[252] Ibid, para. 239.
[253] Ibid, para. 261.
[254] Ibid, para. 244.

skal bruges til at bedømme om staten har handlet inden for dens skønsmargin. Vurderingsmomenterne er herefter: (1) Grundene til at masseovervågning kan tillades, (2) omstændighederne der retfærdiggør overvågning, (3) proceduren for at tillade overvågning, (4) proceduren for indsamling, behandling og opbevaring af data, (5) forholdsregler ved videregivelse, (6) procedurer for varighed, opbevaring og destruktion, (7) procedurer for tilsyn af en uafhængig myndighed og (8) procedurer for efterfølgende kontrol.[255] Herudover fandt EMD det også nødvendigt at "bulk interception" autoriseres af en uafhængig myndighed og at denne bliver informeret om formålet med indgrebet, og hvem der gøres til genstand herfor.[256]

EMD konkluderede i afgørelsen, at der var sket en krænkelse af art. 8. EMD lagde vægt på, at den svenske lovgivning generelt var detaljeret beskrevet, begrænset og tilbød tilstrækkelige sikkerhedsforanstaltninger. EMD konstaterede dog en krænkelse på trods heraf, fordi lovgivningen manglede at regulere, hvordan indsamlet data, der ikke indeholdte personlige informationer, skulle destrueres, hvordan privatlivsinteresser blev sikret ved videregivelsen af data og den manglende efterfølgende effektive kontrol.[257] Dermed var det en krænkelse af art. 8, idet EMD ikke fandt, at der var foretaget tilstrækkelige foranstaltninger for at beskytte mod vilkårlighed og misbrug.

Vedrørende vurderingen af art. 13 fandt EMD ikke anledning til selvstændigt at bedømme bestemmelsen under hensynstagen til konklusionen vedrørende art. 8.[258]

6.5.1.5. B.B.W. m.fl. mod Storbritannien

Big Brother Watch (B.B.W.) m.fl. mod Storbritannien blev afsagt af Storkammeret samme dag som Centrum för rättvisa mod Sverige. EMD skulle i sagen tage stilling til om hemmelig masseovervågning i Storbritannien, herunder om "bulk interception" var en krænkelse af art. 8.

Klagerne til EMD blev indgivet efter Edward Snowden's afsløringer af overvågningsprogrammerne, der blev drevet af efterretningstjenester fra USA og Storbritannien. Klagerne i sagen mente alle, at de var blevet overvåget ved brug af overvågningsprogrammerne og således havde fået deres rettigheder efter art. 8 krænket. Afsløringerne fra Edward Snowden gik bl.a. på at Storbritanniens

[255] Centrum för rättvisa mod Sverige, para. 275.
[256] Ibid, para. 265 og 266.
[257] Ibid, para. 369.
[258] Ibid, para. 376-377.

efterretningstjenester gennemførte en operation kaldet ”TEMPORA”, som tillod dem at indsamle store mængder af data[259], med det formål at beskytte den nationale sikkerhed.[260]

Meget lig de foregående afgørelser, tillagde EMD i denne sag de samme vurderingsmomenter i bedømmelsen. EMD bemærkede som det første de seks minimumsgarantier, som også blev lagt til grund i ovenstående afgørelser. Et andet vurderingsmoment som også går igen i denne afgørelse er bedømmelsen af om indgrebet er ”nødvendigt i et demokratisk samfund” efter art. 8, stk. 2. Men som noget særligt udtalte EMD i denne afgørelse, at selvom ”bulk interception” kan benyttes til at efterforske alvorlig kriminalitet, fremstår det som om medlemsstaterne anvender metoden til at indsamle informationer for at forhindre cyberangreb, kontraspionage og terror[261], hvilket i nær relation har et forudseende element som ”predictive policing”. Tillige bemærkede EMD, at selvom ”bulk interception” ikke nødvendigvis anvendes målrettet på individer, så kan metoden dog anvendes hertil.[262]

Som det blev fastlagt i Roman Zakharov mod Rusland, er det vigtigt at der foretages en form for tilsyn med masseovervågningen. Når der er tale om ”bulk interception” forstærkes kravet herom pga. den betydelige øget risiko for misbrug.[263] Udover tilsyn skal metoden også gøres til genstand for ”end-to-end” sikkerhedsforanstaltninger.[264] EMD afsluttede med at bedømme de otte vurderingsmomenter[265], ligesom det blev gjort i Centrum för rättvisa mod Sverige, som var en tilføjelse til de seks berammede minimumsgarantier. Både de otte vurderingsmomenter og de seks minimumsgarantier vil ikke blive gennemgået igen, da de er gennemgået i de foregående afgørelser.

På baggrund af ovenstående momenter, som i store træk ligner momenterne i de tidligere afgørelser vedrørende masseovervågning, statuerede EMD en krænkelse af art. 8. EMD anerkender behovet for at anvende ”bulk interception” for at identificere trusler mod den nationale sikkerhed.[266] Men selvom behovet og metoden anerkendes, er risikoen for potentielt misbrug stor. I den pågældende sag lagde EMD vægt på, at der ikke var tilstrækkelige ”end-to-end” sikkerhedsforanstaltninger, og således var der ikke effektive garantier mod vilkårlighed og misbrug. Derfor var indgrebet ikke ”nødvendigt i et demokratisk samfund”, og var i strid med art. 8.

[259] B.B.W. m.fl. mod Storbritannien, para. 15.
[260] Ibid, para. 62.
[261] Ibid, para. 345.
[262] Ibid, para. 346.
[263] Ibid, para. 349.
[264] Ibid, para. 350.
[265] Ibid, para. 361.
[266] Ibid, para. 424.

6.5.2. Udledte kriterier fra retspraksis

Efter ovenstående gennemgang af relevant retspraksis vedrørende masseovervågning, er det dernæst relevant at sammenfatte de kriterier som EMD har udledt i forhold til, hvordan masseovervågning bør håndteres af medlemsstaterne.

Kriteriet om nødvendighed

Vurderingen af om indgrebet er "nødvendigt i et demokratisk samfund" efter art. 8, stk. 2, er et kriterie som EMD altid inddrager i bedømmelsen, og som bliver vurderet i alle fem afgørelser i specialet. Som det fremgår af Klass m.fl. mod Tyskland er graden af nødvendighed ikke kun begrænset til, hvad der er "nødvendigt", men derimod, hvad der er "strengt nødvendigt". Som EMD bl.a. udtaler i Klass m.fl. mod Tyskland er denne strengere bedømmelse af nødvendighedskravet et resultat at, at indgreb som hemmelig overvågning indebærer en stor risiko for vilkårlighed og misbrug. Dette medfører samtidig også, at nødvendighedskravet skal vurderes i lyset af om der er effektive sikkerhedsforanstaltninger til at beskytte herimod.

Ved vurderingen af nødvendighedskravet har EMD anerkendt behovet for, at medlemsstaterne skal have en form for teknologisk kapacitet, samt ibrugtagen af mere avanceret og indgribende foranstaltninger for at imødekomme et kriminalitetsbillede i stigende udvikling i en stadig mere digital tidsalder. Derfor er medlemsstaterne også overladt en forholdsvis bred skønsmargin, når det skal vurderes, om særligt indgribende foranstaltninger, som hemmelig overvågning, er nødvendige for at beskytte statens sikkerhed. Dog har EMD i Centrum för rättvisa mod Sverige udtalt, at på trods heraf, indsnævres det skønsmargin når der anvendes teknologiske systemer til overvågning.

En væsentlig og interessant vurdering fra EMD fremgår af afgørelsen Szabó og Vissy mod Ungarn. Her bemærkes det, at justitsministeren ikke er i stand til at vurdere om indgrebet er "strengt nødvendigt". Det forhold, at justitsministeren fastsætter de nærmere regler for, hvornår indgrebet kan og skal finde sted, og der ikke samtidig er juridisk tilsyn heraf, er efter EMD en central problemstilling. Derudover vurderer EMD, at justitsministerens manglende kompetence til at foretage vurderingen af, hvad der er "strengt nødvendigt", særligt begrundes i omfanget af potentielt krænkede personer ved hemmelig masseovervågning.[267]

[267] Szabó og Vissy mod Ungarn, para. 75.

Juridisk kontrol og domstolsprøvelse (sikkerhedsforanstaltning)

Når en stat foretager indgreb som hemmelig masseovervågning har EMD lagt vægt på, om der i lovgivningen var fastsat mulighed for juridisk kontrol eller domstolsprøvelse for at garantere uafhængighed, upartiskhed og korrekt procedure. Vurderingen heraf indgår bl.a. i bedømmelsen af om der foreligger tilstrækkelige og effektive sikkerhedsforanstaltninger. Det blev ikke vurderet til at være et krav, men var for EMD ønskeligt, hvilket bl.a. fremgik af Roman Zakharov mod Rusland og Centrum för rättvisa mod Sverige.

På trods af, at juridisk kontrol og domstolsprøvelse ikke er et krav, får det dog betydning i forhold til den samlede vurdering af om indgrebet udgør en krænkelse af art. 8. Som eksempel herpå blev der i Szabó og Vissy mod Ungarn bl.a. lagt vægt på, at der aldrig havde været foretaget en domstolsprøvelse af den hemmelige overvågning, hvilket gjorde det umuligt konkret at vurdere fordele og ulemper ved indgrebet. Derfor ønsker EMD, at juridisk kontrol og domstolsprøvelse iagttages af staterne ved hemmelig masseovervågning, således vilkårlighed og misbrug ikke bliver muligt.

De 6 minimumsgarantier og 8 vurderingsmomenter (sikkerhedsforanstaltning)

De seks minimumsgarantier, der indgår i EMD's vurdering, fremgår af alle ovenstående afgørelser med undtagelse af Klass m.fl. mod Tyskland. For at EMD kan tage stilling til, hvorvidt hemmelig overvågning er en krænkelse af art. 8, har EMD udviklet seks minimumsgarantier, der bør være reguleret ved lov for at forhindre misbrug. Vurderingen heraf indgår bl.a. i bedømmelsen af om der foreligger tilstrækkelige og effektive sikkerhedsforanstaltninger. De seks minimumsgarantier, der skal reguleres, er herefter:

1. Karakteren af lovovertrædelser som kan give anledning til indgreb.
2. Kategorier af personer, der kan blive gjort til genstand for indgrebet.
3. Tidsbegrænsning for indgrebet.
4. Procedure for indsamling, behandling og opbevaring af data.
5. Foranstaltninger ved videregivelse af data.
6. Omstændighederne for, hvornår indsamlet data bør og skal slettes og destrueres.

Udover de seks minimumsgarantier, har EMD i de to nyere afgørelser[268] fra 2021 afsagt af Storkammeret, tilføjet otte vurderingsmomenter til bedømmelsen. EMD har udtalt, at staterne er overladt en vid skønsmargin, når indgrebet er for at beskytte den nationale sikkerhed. Samtidig har

[268] Centrum för rättvisa mod Sverige og B.B.W. m.fl. mod Storbritannien.

EMD bestemt i Centrum för rättvisa at denne skønsmargin bør indsnævres når indgrebet udføres med hjælp af IT-systemer. Tillige bemærkes der i forlængelse heraf, at behovet for sikkerhedsforanstaltninger stiger når behandling af personlige oplysninger er underlagt en automatiseret behandling, særligt når der er tale om "bulk interception". Bedømmelsen af vurderingsmomenterne henviser også til spørgsmålet om, hvorvidt processen med indgrebet er genstand for "end-to-end" sikkerhedsforanstaltninger, hvilket både manglede i Centrum för rättvisa mod Sverige og B.B.W. m.fl. mod Storbritannien og dermed var bidragende til at EMD fandt at der var sket en krænkelse af art. 8. De otte vurderingsmomenter skal bidrage til bedømmelsen af om staterne har handlet inden for deres skønsmargin. De otte vurderingsmomenter er herefter:

1. Grundene til at hemmelig masseovervågning kan tillades.
2. Omstændighederne, der retfærdiggør overvågning.
3. Proceduren for at tillade overvågning.
4. Proceduren for indsamling, behandling og opbevaring af data.
5. Foranstaltninger ved videregivelse af data.
6. Procedurer for varighed, opbevaring og destruktion.
7. Procedurer for tilsyn af en uafhængig myndighed.
8. Procedurer for efterfølgende kontrol.

Som det måske bemærkes, ligner mange af vurderingsmomenter indholdet i minimumgarantierne. EMD tillægger både momenterne og garantierne en samlet vurdering, men som konstateret bidrager minimumsgarantierne til at bedømme om der foreligger tilstrækkelige og effektive sikkerhedsforanstaltninger til at berettige indgrebet, hvorimod vurderingsmomenterne bidrager til at bedømme om staterne handler inden for deres skønsmargin.

6.5.3. POL-INTEL i lyset af de udledte kriterier

De ovenfor gennemgåede afgørelser, omhandler hemmelig masseovervågning, hvad enten det benyttes på individniveau eller generelt mod alle personer. Derfor er det relevant at vurdere POL-INTEL i lyset af de ovenstående udledte kriterier fra EMD. Det anføres fra dansk politi, at POL-INTEL ikke anvendes på individniveau, men dette er uden betydning, idet IT-systemet kan anvendes hertil og samtidig muliggør hemmelig masseovervågning af danskerne. Denne vurdering er i overensstemmelse med EMD's vurdering i Roman Zakharov mod Rusland.

I forhold til det første kriterie om nødvendighed bemærker Justitsministeriet i L171, at implementeringen af politilovens § 2 a er "*nødvendig i et demokratisk samfund*"[269] og at "*lovforslaget*

[269] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 22.

kan gennemføres inden for rammerne af Danmarks forpligtelser efter EMRK.[270] Her har EMD i praksis ikke fundet det tilstrækkeligt at vurdere om indgrebet er "nødvendigt", men derimod om det er "strengt nødvendigt". Herudover fremgik det af Szabó og Vissy mod Ungarn, at justitsministeren ikke er i stand til at foretage denne vurdering. EMD finder det problematisk, at vurderingen efter art. 8, stk. 2 alene er underlagt justitsministerens vurdering samt regulering og ikke samtidig er underlagt juridisk tilsyn. Da POL-INTEL ikke har været genstand for domstolsprøvelse eller juridisk tilsyn, kan det konstateres, at Justitsministeriet ikke har kompetence til at vurdere nødvendigheden i et demokratisk samfund efter art. 8, stk. 2.

Dernæst er kriteriet om juridisk kontrol og domstolsprøvelse. Som det tidligere er angivet og som det fremgår af bekendtgørelse nr. 1078 § 12, har personer ikke ret til indsigt i de behandlede oplysninger, der behandles i POL-INTEL. Dette medfører at krænkede personer kan finde det svært, hvis ikke umuligt, at vide om et indgreb er foretaget på baggrund af en behandling i POL-INTEL, og dernæst at få afprøvet om indgrebet har været nødvendigt og proportionelt. Derudover tillægges det også betydning, at POL-INTEL aldrig har været til genstand for en domstolsprøvelse. I Szabó og Vissy mod Ungarn vurderede EMD, at manglende domstolsprøvelse gjorde det besværligt at vurdere fordele og ulemper ved den hemmelig masseovervågning. Dette kan derfor også være vanskeligt ved POL-INTEL.

Afslutningsvis er det relevant at vurdere POL-INTEL i lyset af kriteriet om de seks minimumsgarantier og de otte vurderingsmomenter. I forhold til minimumsgarantierne mangler det at blive reguleret, hvilke personer, der kan blive gjort til genstand for indgrebet. Det blev bl.a. lagt til grund i Roman Zakharov mod Rusland, at den russiske lovgivning ikke regulerede dette og bemærkede tillige at indgrebet ikke var begrænset til mistænkte personer, og således kunne ikke-mistænkte blive gjort til genstand for indgrebet.[271] Dette var medvirkende til, at EMD fandt at det var en krænkelse af art. 8. Det er på baggrund heraf særligt problematisk, at der ikke i bekendtgørelse nr. 1078 er reguleret kategorien af personer efter minimumgaranti nr. 2. Ved bedømmelsen af vurderingsmomenterne vil det i forhold til moment nr. 4 om proceduren for indsamling, behandling og opbevaring af data, kræve en dybere indsigt i, hvordan POL-INTEL behandler oplysningerne og hvordan algoritmen er bygget op. Dette kan muligvis blive svært, idet det kan betvivles, hvor meget indsigt politiet har i, hvordan POL-INTEL fungerer. Vurderingsmoment nr. 7 og nr. 8 om tilsyn og

[270] Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven), s. 22.
[271] Roman Zakharov mod Rusland, para. 182.

efterfølgende kontrol kan konstateres ikke at være reguleret. Dette lægger op til at Danmark potentielt set ikke handler inden for deres skønsmargin, ved implementeringen og anvendelsen af POL-INTEL.

6.6. Art. 13 – Retten til effektive retsmidler

Retten til effektive retsmidler efter art. 13 er relevant kort at belyse i nærværende fremstilling, idet det påhviler medlemsstaterne at beskytte menneskerettighederne i konventionen. Herudover er art. 13 også relevant i relation til vurderingen af art. 8, hvilket bl.a. fremgår af afgørelserne i afsnit 6.5.1. Bestemmelsen har følgende ordlyd:

> *Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.*

Der er en nær sammenhæng mellem art. 13 og art. 35, idet art. 35 regulerer, at de effektive retsmidler efter art. 13 skal udnyttes nationalt inden klagen indbringes for EMD. Efter art. 13 kræves der således "*at der skal findes et nationalt retsmiddel, der kan behandle indholdet af en rimelig begrundet klage i henhold til konventionen, og som kan sikre passende oprejsning*".[272] Først når en person bliver bekendt med et indgreb, har personen ret til effektive retsmidler.

Det er ikke et krav for at anvende art. 13, at der er statueret en krænkelse af en eller flere af de konventionssikrede rettigheder. Men da art. 13 indeholder et krav om diskutable eller rimeligt begrundede klager, får det betydning, hvis EMD statuerer krænkelse, fordi det uden videre vil opfylde kravet om "rimeligt begrundet klage".[273]

Begrebet "effektive retsmidler" består af et præventivt eller kompenserende element. Det betyder, at retsmidlet skal kunne forhindre en krænkelse eller en fortsat krænkelse eller skal kunne yde passende opretning for allerede skete krænkelser.[274] Det er ikke et krav efter art. 13, at der er tale om domstolsprøvelse. Særligt, når der er tale om hemmelig overvågning kan et objektivt kontrolorgan være tilstrækkeligt til at sikre retten til effektive retsmidler, så længe overvågningen er hemmelig.[275] Ved vurderingen af om den kontrollerende myndighed er kompetent, skal det tages i betragtning om denne er uafhængig og upartisk. Effektiviteten af retsmidlet består i, at myndigheder ikke uberettiget

[272] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1253.
[273] Ibid, s. 1255.
[274] Ibid, s. 1257.
[275] Ibid.

må hindre udnyttelsen af det.[276] Hvis en klager ikke har mulighed for prøvelse, er retsmidlet ikke effektivt. Særligt vedrørende hemmelig overvågning, som er begrundet i statens sikkerhed, bør der ske underretning så snart faren for at skade formålet med indgrebet ikke længere er aktuel.[277]

Som det fremgår af de fire afgørelser i specialet, hvor EMD tager stilling til art. 13, giver retten til effektive retsmidler ikke anledning til de store problemer. Det er efter EMD's praksis ikke altid nødvendigt selvstændigt at behandle bestemmelsen, hvis manglende adgang til effektive retsmidler bl.a. anses for at være en krænkelse af en processuel rettighed knyttet til art. 8.

[276] Jon Fridrik Kjølbro, "*Den Europæiske Menneskerettighedskonvention – For Praktikere*", Jurist- og Økonomforbundets Forlag, 2020, 5. udgave, s. 1259.
[277] Ibid, s. 1267.

7. Konklusion

Formålet med specialet har været at vurdere, hvilke menneskeretlige problemstillinger, der aktualiseres gennem anvendelsen af POL-INTEL. På baggrund af ovenstående analyse, kan det konstateres, at anvendelsen af POL-INTEL, udgør en risiko for at krænke grundlæggende menneskerettigheder efter EMRK.

Det kan indledningsvist konkluderes, at formålet med implementeringen af politilovens § 2 a, og indkøbet af POL-INTEL var for at imødekomme et ændret og mere komplekst kriminalitetsbillede, særligt efter terrorhændelserne i København i 2015. Formålet med POL-INTEL var for det første for at forhindre terrortrusler, men vil også blive anvendt til politiets almindelige ordens- og sikkerhedsopgaver. POL-INTEL muliggør foretagelsen af tværgående informationsanalyser og gør det samtidig muligt at foretage "predictive policing" på baggrund af en algoritme. Det kan i denne forbindelse konstateres, at "predictive policing" kan være problematisk, idet risikoen for bias og "præ-kriminalisering" er stor.

Hvad angår retten til privatliv efter EMRK art. 8 kan det konkluderes, at indgreb baseret på en analyse i POL-INTEL kan udgøre en krænkelse heraf. Kravet om nødvendighed efter art. 8, stk. 2 er ved hemmelig overvågning skærpet, hvilket betyder at indgrebet skal være "strengt nødvendigt" i et demokratisk samfund for at kunne være berettiget, jf. Klass m.fl. mod Tyskland. I relation til denne bedømmelse blev der i Szabó og Vissy mod Ungarn konstateret, at justitsministeren ikke er kompetent til at vurdere, hvorvidt hemmelig overvågning er "strengt nødvendigt". Den danske implementering og anvendelse af POL-INTEL er baseret på en vurdering fra Justitsministeriet, hvorpå det konkluderes at være "nødvendigt" i et demokratisk samfund. Derfor har Justitsministeriet ikke har foretaget en vurdering i overensstemmelse med det skærpede nødvendighedskrav efter EMD's praksis. Dernæst kan det ligeledes konstateres, at Justitsministeriet ikke har kompetence til at foretage denne vurdering. Dette betyder, at betingelserne for at et indgreb er foreneligt med konventionen efter art. 8, stk. 2, ikke er opfyldt. Det aktualiserer væsentlige menneskeretlige problemstillinger, idet anvendelsen af POL-INTEL i Danmark ikke er vurderet af en kompetent uafhængig myndighed til at være "strengt nødvendigt" i et demokratisk samfund.

I forhold til forbuddet mod diskrimination efter EMRK art. 14 kan det udledes at "predictive policing" udgør en særlig risiko for at uskyldige mistænkes, og bliver profileret som potentielle gerningspersoner eller ofre i fremtiden. Algoritmen i POL-INTEL er ikke i sig selv et problem, men hvis personer udsættes for et indgreb på grund af momenter som køn, race, etnicitet, sprog, religiøs

eller politisk tilknytning mm. udgør det et problem i relation til art. 14. Hertil kan det desuden konstateres, at algoritmens sammensætning og opbygning er ukendt. Derfor er det ligeledes ukendt, hvorvidt anvendelsen af POL-INTEL udgør en risiko for amerikanske tilstande i det danske politi. For at der kan statueres en krænkelse af art. 14, skal det vurderes om der har været forskelsbehandling i sammenlignelige situationer. Det kan konstateres at begrænsningen i indsigtsretten efter bekendtgørelse nr. 1078 § 12 gør det besværligt at få indblik i de oplysninger som et indgreb er baseret på, og dermed umuliggør en sådan vurdering.

Efter en analyse af retspraksis fra EMD vedrørende masseovervågning kan det fastslås, at der foreligger en række kriterier, som medlemsstaterne skal iagttage og som er afgørende for, hvorvidt EMD statuerer en krænkelse af art. 8. Første kriterie er kravet om at indgrebet skal være "strengt nødvendigt" i et demokratisk samfund. Som det allerede er konstateret, er nødvendighedskravet skærpet ved hemmelig masseovervågning. Herudover bør der i forbindelse med hemmelig masseovervågning være mulighed for juridisk kontrol eller domstolsprøvelse efter indgrebets afslutning. Dette er ikke et krav, men blev i Szabó og Vissy mod Ungarn bl.a. lagt til grund for at der var sket en krænkelse af art. 8. Det kan konkluderes, at POL-INTEL ikke har været genstand for en domstolsprøvelse, og at muligheden herfor er væsentligt begrænset, henset til den indskrænkede indsigtsret i bekendtgørelse nr. 1078 § 12.

EMD har herudover seks minimumsgarantier, som medlemsstaterne skal iagttage. Disse indgår i bedømmelsen af om der er sket en krænkelse af art. 8. Herefter skal det reguleres, hvilken karakter en lovovertrædelse skal have for at give anledning til indgreb, kategorien af personer, der kan blive gjort til genstand for en indgrebet, tidsbegrænsning, procedure for indsamling, behandling og opbevaring af data, foranstaltninger ved videregivelse af data og sidst omstændighederne for, hvornår data bør og skal slettes. Det kan på baggrund af disse konkluderes, at den danske regulering af POL-INTEL ikke indeholder en præcisering af de personer, der kan gøres til genstand for et indgreb. Denne manglende præcisering af personer var i Roman Zakharov mod Rusland medvirkende til at EMD statuerede en krænkelse af art. 8.

Medlemsstaterne er overladt en vid skønsmargin ved vurderingen af om indgreb skal foretages for at beskytte statens nationale sikkerhed. Det kan samtidig også konkluderes, at denne skønsmargin indskrænkes ved hemmelig overvågning. EMD har som noget nyt i to afgørelser fra 2021[278] udledt otte vurderingsmomenter, der særligt gælder for hemmelig masseovervågning. Disse indgår i

[278] Centrum för rättvisa mod Sverige og B.B.W. m.fl. mod Storbritannien.

bedømmelsen af om medlemsstaterne handler inden for deres skønsmargin. De otte vurderingsmomenter går for det første på om den pågældende medlemsstat har reguleret grundene til at hemmelig masseovervågning kan tillades, omstændighederne, der retfærdiggør overvågning og procedurer for tilladelse. Ligeledes skal det vurderes om der er procedurer for indsamling, behandling og opbevaring af data, foranstaltninger ved videregivelse af data, procedurer for varighed, opbevaring og destruktion, procedurer for tilsyn af en uafhængig myndighed og slutteligt procedurer for efterfølgende kontrol. Det kan konkluderes, at procedurer for tilsyn af en uafhængig myndighed og for efterfølgende kontrol ikke er reguleret i den danske lovgivning ved anvendelsen af POL-INTEL. Dette besværliggøres samtidig af den ovenfor konstateret indsigtsbegrænsning. Det kan derfor betvivles om Danmark handler inden for den i forvejen indskrænkede skønsmargin ved anvendelsen af POL-INTEL.

Hvad angår vurderingen af EMRK art. 13 om retten til effektive retsmidler, kan det på baggrund af retspraksis fra EMD udledes, at manglende adgang til effektive retsmidler anses for at være en krænkelse af en processuel rettighed knyttet til vurderingen af art. 8. Derfor kan det konkluderes, at art. 13 ikke i sig selv giver anledning til problematikker.

Samlet set bemærkes det, at POL-INTEL muliggør foretagelsen af hemmelig masseovervågning, herunder ”predictive policing”, hvilket medfører en stor risiko for misbrug og vilkårlighed. Det kan ligeledes konstateres, at den danske regulering af POL-INTEL mangler tilstrækkelige og effektive sikkerhedsforanstaltninger, der kan forhindre en sådan misbrug og vilkårlighed. Den væsentligste problematik er dog, at anvendelsen af POL-INTEL er baseret på en manglende kompetent vurdering og derfor er nødvendighedskravet efter art. 8, stk. 2 ikke opfyldt. På baggrund heraf aktualiserer anvendelsen af POL-INTEL en anseelig risiko for at krænke konventionssikrede menneskerettigheder og dermed danskernes ret til privatliv, familieliv, hjem og korrespondance efter art. 8 og retten til ikke at blive udsat for diskrimination efter art. 14.

8. Litteraturfortegnelse

8.1. Retslitteratur og anden faglitteratur

- Couchman, Hannah, *"Policing by Machine",* Rapport fra Liberty, 2019.
- Elo Rytter, Jens, *"Individets grundlæggende rettigheder",* Karnov Group, 2021, 4. udgave.
- Evald, Jens, "*Juridisk teori, metode og videnskab",* Djøf Forlag, 2020, 2. udgave.
- Evald, Jens, *"Retskilderne og den juridiske metode"*, Jurist- og Økonomforbundets Forlag, 2000, 2. udgave.
- Evald, Jens & Schaumburg-Müller, Sten, "*Retsfilosofi, retsvidenskab og retskildelære*", Jurist- og Økonomforbundets Forlag, 2004, 1. udgave.
- G. Ferguson, Andrew, "*Policing Predictive Policing*", Washington University Law Review, vol. 94, issue 5, 2017.
- Henricson, Ib, "*Politiloven med kommentarer"*, Jurist- og Økonomforbundets Forlag, 2020, 5. udgave.
- Henricson, Ib, "*Politiret*", Jurist- og Økonomforbundets Forlag, 2020, 6. udgave.
- Harhoff, Frederik (red.), Barten, Ulrike, Schamburg-Müller, Sten m.fl., *"Folkeret"*, Hans Reitzels Forlag, 2017, 1. udgave.
- Kirchhoff Hestehave, Nadja, "*Proaktiv kriminalitetsbekæmpelse*", Samfundslitteratur, 2013, 1. udgave.
- Kjølbro, Jon Fridrik, "*Den Europæiske Menneskerettighedskonvention for Praktikere",* Jurist- og Økonomforbundets Forlag, 2020, 5. udgave.
- Lorenzen, Peer m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 1-9)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave.
- Lorenzen, Peer m.fl., "*Den Europæiske Menneskerettighedskonvention med kommentarer (art. 10-59 samt tillægsprotokollerne)*", Jurist- og Økonomforbundets Forlag, 2011, 3. udgave.
- Munk-Hansen, Carsten, "*Retsvidenskabsteori",* Jurist- og Økonomforbundets Forlag, 2018, 2. udgave.
- Stevnsborg, Henrik*, "Hot spots, hot times, hot persons. Om fænomenet predictive policing"*, Tidsskrift for Kriminalret, 2021.
- 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, 1. udgave.

8.2. Retskilder

- Bekendtgørelse nr. 1078 af 20. september 2017 (Bekendtgørelse om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser).
- Betænkning nr. 1546 af 15. august 2014 (Betænkning om inkorporering mv. inden for menneskeretsområdet).
- EMRK: Den Europæiske Menneskerettighedskonvention.
- Inkorporeringsloven (Lov nr. 285 af 29. april 1992).
- Lov nr. 671 af 8. juni 2017 (Lov om ændring af lov om politiets virksomhed og toldloven).
- Lovforslag nr. 171 af 29. marts 2017 (Forslag til lov om ændring af lov om politiets virksomhed og toldloven).
- Persondataloven (Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger).
- 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. april 2017).

8.3. Andet materiale

- "*Et stærkt værn mod terror – 12 nye tiltag mod terror",* Regeringens udspil fra 2015.
- Kommenteret høringsoversigt vedr. Udkast til lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysning om flypassagerer).

8.4. Domsregister

Den Europæiske Menneskerettighedsdomstol

- B.B.W. m.fl. mod Storbritannien – Afsagt d. 25. maj 2021.
- Brinks mod Holland – Afsagt d. 5. april 2005.
- Centrum för rättvisa mod Sverige – Afsagt d. 25. maj 2021.
- Khelili mod Schweiz – Afsagt d. 18. oktober 2011.
- Klass m.fl. mod Tyskland – Afsagt d. 6. september 1978.
- Roman Zakharov mod Rusland – Afsagt d. 4. december 2015.
- Szabó og Vissy mod Ungarn – Afsagt d. 12. januar 2016.

8.5. Hjemmesider/artikler

- Fribo, Adam, ”*Rigspolitiet lover: Vi bruger ikke Pol-intel til predictive policing*”, Artikel på version2.dk, (https://www.version2.dk/artikel/rigspolitiet-lover-vi-bruger-ikke-pol-intel-predictive-policing-1092642), besøgt d. 5. september 2021.
- Holst, Helene Kristine & Sørensen, Kasper Kildegaard, ”V*i er meget, meget sikre på, at det her bliver en success*”, Artikel på Berlingske.dk, https://www.berlingske.dk/politik/dansk-politi-advarer-forbrydere-vi-er-klar-med-et-supervaaben, besøgt d. 27. oktober 2021.
- Jensen, Sally, ”*Et supervåben mod kriminalitet eller en sprængfarlig bombe af diskrimination?*”, Artikel på responsmedie.dk, https://www.responsmedie.dk/pol-intel/, besøgt d. 27. oktober 2021.
- Kulager, Frederik, *”For fire år siden fik politiet et ”supervåben”. Her er, hvordan det har transformeret ordensmagten”*, Artikel på Zetland.dk, (https://www.zetland.dk/historie/sO9kBG7W-aOZj67pz-04ca0), besøgt d. 5. september 2021.
- Milhøj, Anders og Englev, Michael, ”*Datamining i Den Store Danske*”, https://denstoredanske.lex.dk/datamining, besøgt d. 16. oktober 2021.
- Scheuer-Hansen, Simone, ”*Var det for meget, da politiet fangede en lommetyve med nyt supervåben?*”, Artikel på Politiken.dk, https://politiken.dk/viden/Tech/art6650800/Var-det-for-meget-da-politiet-fangede-en-lommetyv-med-nyt-cyberv%C3%A5ben, besøgt d. 20 oktober 2021.

9. Ordoptælling