IT-Politisk Forening

Web: www.itpol.dk
Email: bestyrelsen@itpol.dk

6. marts 2025

Høringssvar vedr. ændring af lov om Politiets Efterretningstjeneste (PET), (Understøttelse af Politiets Efterretningstjenestes mulighed for at udføre data- og analysebaseret efterretningsvirksomhed m.v.), sagsnr. 2024-04082

IT-Politisk Forening har primært bemærkninger til de dele af lovforlaget, som vedrører indhentning og behandling af større sammenhængende datasæt, videregivelse af oplysninger fra andre forvaltningsmyndigheder, samt anmodninger til FE om søgning i rådata.

Henvisninger til paragraffer i høringssvaret vil, hvor intet andet er angivet, være eksisterende eller foreslåede paragraffer i PET-loven (f.eks. § 4 a som den foreslåede § 4 a i lovforslagets § 1, nr. 9).

Indledning og overordnede betragtninger om lovforslaget

1. Lovforslaget giver PET meget brede og generelle beføjelser til at indhente, indsamle, opbevare og behandle større sammenhængende datasæt fra en række kilder uden nogen reelle afgrænsninger udover PET's egne (interne) vurderinger af relevans. Der kan blive tale om ganske omfattende datamængder, hvor PET via sammenstilling og samkøring af forskellige større sammenhængende datasæt får mulighed for at lave meget præcise profiler af de personer, som optræder i de indhentede større sammenhængende datasæt.

2. Den omfattende registrering af potentielt store dele af befolkningen hos PET er egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning. Det gælder uanset at mange analyser af større sammenhængende datasæt muligvis vil have en overordnet karakter, idet lovgrundlaget eksplicit tillader "data mining" analyser med henblik på at udfinde ikke på forhånd identificerede personer, som opfylder bestemte søgekriterier.

3. For national lovgivning, der tillader hemmelig overvågning, fremhæver Den Europæiske Menneskerettighedsdomstol (EMD) i dens retspraksis, at det nationale lovgrundlag skal være tilgængeligt og forudsigeligt i dets anvendelse, og at lovgrundlaget samtidigt skal sikre, at foranstaltninger til hemmelig overvågning kun anvendes, når det er nødvendigt i et demokratisk samfund, herunder navnlig ved at fastsætte effektive retsgarantier og garantier mod misbrug.

4. De meget brede beføjelser i lovforslaget til at indhente, indsamle, opbevare og behandle større sammenhængende datasæt rejser efter IT-Politisk Forenings opfattelse alvorlig tvivl om, hvorvidt beføjelserne kan siges at være i overensstemmelse med loven, som fortolket i retspraksis fra EMD. Når næsten er tilladt for PET i forbindelse med større sammenhængende datasæt (jf. valget af "kan have betydning" kriteriet for alle bestemmelser med en enkelt undtagelse), kan PET's behandling af oplysninger ikke med rimelighed siges at opfylde krav om klarhed og forudsigelighed for de berørte personer.

5. Lovforslaget indgår i en evaluering af PET-loven, jf. Justitsministeriets rapport om erfaringerne med PET-loven fra juni 2022. Det er i den forbindelse beklageligt, at Justitsministeriets først og fremmest har forholdt sig til PET's ønsker om endnu mere dataindsamling og nye analysekapaciteter, og kun i yderst begrænset omfang har vurderet, om en række nye domme fra EMD siden 2013 om efterretningstjenesters (masse)overvågning giver anledning til at revidere PET-loven.[1]

Muligheder for at behandle store datasæt i den nuværende PET-lov

6. Med lovforslaget får PET en "bulk personal data"-kapacitet (benævnt "større sammenhængende datasæt"), der synes at være inspireret af Storbritannien, hvor en sådan ordning eksisterer.

7. Den nuværende PET-lov forhinder ikke som sådan indhentning af større datasæt uden nogen kriterier for målretning mod bestemte personer eller grupper af personer, idet indhentning efter § 3 kan ske på grundlag af "kan have betydning" kriteriet. Det betyder, at PET kan foretage indhentningen, medmindre det på forhånd kan udelukkes, at oplysningerne vil være relevante for tjenesten.

8. De efterfølgende behandlingsregler i den nuværende PET-lov for oplysninger indhentet efter § 3 sætter imidlertid grænser for hvor længe PET kan opbevare sådanne større datasæt uden at foretage en vis behandling af oplysningerne, herunder journalisering.

9. Ved indhentning af oplysninger fra andre danske forvaltningsmyndigheder (PET-lovens § 4) om en gruppe af personer, som ikke på forhånd er identificeret, har PET en forpligtelse til at foretage en vurdering af, om de personer, som oplysningerne vedrører, er af relevans for tjenestens opgavevaretagelse. Hvis det viser sig ikke at være tilfældet, skal oplysninger vedr. de pågældende (de ikke-relevante oplysninger) straks slettes.

10. Derudover er PET underlagt visse databeskyttelsesretlige regler i PET-lovens § 6 a for behandling af oplysninger om fysiske og juridiske personer. Det gælder bl.a. princippet om dataminimering i § 6 a, stk. 3, altså at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil

1 En af de relevante domme, som hverken rapporten fra juni 2022 eller lovforslaget forholder sig til, er *Roman Zakharov mod Rusland* (47143/06) af 4. december 2015. Der er også andre domme fra EMD og EU-Domstolen. Nogle er omtalt i dette høringssvar, men en fuldstændig liste ligger af praktiske årsager uden for rammene af høringssvaret.

oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

11. De eksisterende regler giver på den ene side PET meget brede beføjelser til at indhente oplysninger, som potentielt kan være relevante for tjenestens arbejde med at forebygge og efterforske trusler mod den nationale sikkerhed, mens der samtidig er visse retsgarantier for borgerne, som kan modvirke dataophobning hos PET. Det vil efter IT-Politisk Forenings opfattelse være stærkt problematisk, hvis PET registrerer oplysninger om hele befolkningen, eller har mulighed for at gøre dette. Den type overdreven registrering med sagsmapper på store dele af befolkningen forbindes normalt med totalitære regimer som Stasi i det tidligere DDR.

Større sammenhængende datasæt i lovforslaget (PET-lovens kapitel 6 a)

12. Lovforslaget ændrer fundamentalt på denne balance. PET får mulighed for generel og udifferentieret indhentning af oplysninger (bulkindhentning), længerevarende opbevaring af disse oplysninger (fem år eller mere), samt meget generelle betingelser (hvis nogen overhovedet) for analyser, herunder egentlige data-mining analyser, der kan finde ukendte målpersoner af mulig interesse for tjenesten. Med en enkelt undtagelse gælder ”kan have betydning” kriteriet for både indhentning eller indsamling og den efterfølgende behandling af oplysninger, hvilket i praksis betyder, at PET kan behandle oplysninger i forbindelse med større sammenhængende datasæt uden nogen reelle begrænsninger (fastsat i lovgivning).

13. Beføjelserne til PET kan sammenlignes med FE-lovens nuværende bestemmelser om indhentning af rådata og efterfølgende analyse vedr. personer, der ikke er hjemmehørende i Danmark. Sådanne meget vide beføjelser i en stats efterretningslovgivning er generelt rettet mod personer i udlandet, og de begrundes ofte med, at det er sværere at forebygge og efterforske trusler fra udlandet.[2]

14. Som indenrigsefterretningstjeneste er PET’s beføjelser imidlertid rettet mod danske borgere i ganske betydeligt omfang. PET kan eksempelvis indhente større sammenhængende datasæt fra andre danske forvaltningsmyndigheder. Det forhold gør i sig selv de nye beføjelser vedr. større sammenhængende datasæt særdeles vidtgående.

15. Lovforslaget giver mulighed for indhentning og analyser af større sammenhængende datasæt til alle PET’s opgaver i § 1 på grundlag af ”kan have betydning” kriteriet, altså medmindre det på forhånd kan udelukkes, at indhentningen eller analysen vil være relevant, en vurdering PET selv foretager. Det er en væsentlig udvidelse af beføjelserne sammenlignet med § 5 og §§ 7-8, hvor oplysninger kan behandles på grundlag af ”må antages at have betydning” kriteriet (der stiller krav om visse konkrete omstændigheder) til tjenestens opgaver efter straffelovens kapitel 12 og 13.

16. Lovforslagets almindelige bemærkninger pkt. 3.1.3.1 gør det klart, at større

2 Se eksempelvis præmis 51 af *Big Brother Watch m.fl. mod Storbritannien* (dom af 25. maj 2021 fra Den Europæiske Menneskerettighedsdomstol).

sammenhængende datasæt kan indeholde oplysninger om personer, som der ikke selvstændigt efter de almindelige regler i PET-loven er grundlag for at behandle oplysninger om.

17. I lovforslagets bemærkninger nævnes det, at analyser af større sammenhængende datasæt kan danne grundlag for dansk sikkerhedspolitik (side 99), følge udviklingen på internettet (side 61), og varetage hensyn til ikke bare den nationale sikkerhed, men også den offentlige tryghed og at forebygge uro eller forbrydelser (side 160).

18. Den samlede liste består således af meget generelle formål, som går langt udover beskyttelsen af statens væsentlige funktioner og grundlæggende samfundsinteresser.[3] Ikke desto mindre kan der til disse generelle formål behandles omfattende mængder personoplysninger, herunder følsomme personoplysninger, under omstændigheder, som må betegnes som særdeles indgribende i retten til privatliv, og som kan have en dæmpende effekt (”chilling effect”) på ytringsfriheden og udøvelsen af andre grundlæggende rettigheder (se punkt 35-38 nedenfor).

Det særskilte miljø for større sammenhængende datasæt

19. Større sammenhængende datasæt skal opbevares adskilt fra de øvrige oplysninger, som PET er i besiddelse af. Det særskilte miljø fremhæves som en retsgaranti i de almindelige bemærkninger pkt. 3.1.3.1. Mulighederne for at opbevare oplysninger om flere personer end tilladt i dag modsvares ifølge bemærkningerne (side 52) af, at der vil være skarpe grænser for hvordan PET vil kunne behandle oplysningerne i det særskilte miljø, herunder at behandlingen ikke kan være målrettet bestemte fysiske eller juridiske personer.

20. Denne beskrivelse af det særskilte miljø er efter IT-Politisk Forenings opfattelse misvisende. Det særskilte miljø for større sammenhængende datasæt gælder kun når behandlingen sker efter reglerne i kapitel 6 a, hvor analyse af oplysninger efter § 10 d kan ske på grundlag af ”kan have betydning” kriteriet. Til sådanne analyser kan PET ikke behandle større sammenhængende datasæt sammen med andre oplysninger.

21. De nye oplysninger indhentet, indsamlet og opbevaret til større sammenhængende datasæt kan imidlertid også behandles efter de almindelige behandlingsregler i §§ 7-8, som kan bruges til målrettede personundersøgelser efter § 5 eller efterforskninger efter § 6. Det forudsætter, at behandlingen opfylder ”må antages at have betydning” kriteriet i forhold til tjenestens opgaver efter straffelovens kapitel 12 og 13.

22. Efter de almindelige behandlingsregler kan PET analysere større sammenhængende datasæt sammen med øvrige oplysninger, dvs. behandle større sammenhængende datasæt uden for det særskilte miljø. Det gælder også oplysninger i større sammenhængende datasæt, som PET ikke i dag kan opbevare og efterfølgende behandle efter §§ 7-8.

3 Det er tvivlsomt om EU-traktaternes undtagelser for national sikkerhed kan påberåbes for alle disse opgaver og formål, jf. også punkt 101 nedenfor i høringsvaret. Af tidsmæssige årsager vil dette punkt ikke bliver nærmere berørt i høringssvaret.

23. Det særskilte miljø gælder altså reelt kun for den informationsbehandling, som ikke er tilladt i dag, dvs. muligheden for at behandle oplysninger på grundlag af "kan have betydning" kriteriet, når behandlingen ikke er målrettet bestemte personer.

24. Det er derfor vanskeligt at se, at det særskilte miljø med nogen rimelighed kan siges at modsvare de kraftigt udvidede beføjelser til at indhente, indsamle og opbevare oplysninger.

25. Tværtimod kan de nye oplysninger i større sammenhængende datasæt bruges til **både den eksisterende behandling** efter §§ 7-8 på grundlag af "må antages at have betydning" kriteriet **og den nye bestemmelse i § 10 d** om analyser, der ikke er målrettet bestemte personer, på det meget generelle "kan have betydning" kriterie (hvor behandlingen kan foretages, medmindre PET selv på forhånd kan udelukke, at behandlingen er relevant for tjenestens opgaver).

Større sammenhængende datasæt fra offentligt tilgængelige kilder (§ 10 c, stk. 1)

26. PET kan indsamle, indhente og opbevare større sammenhængende datasæt bestående af oplysninger fra offentligt tilgængelige kilder, når datasættet som helhed kan have betydning for varetagelsen af tjenestens opgaver (alle opgaver, ikke begrænset til national sikkerhed).

27. Offentlige tilgængelige kilder omfatter oplysninger på især internettet, som er alment tilgængelige for offentligheden, og oplysninger der kan erhverves på kommercielle formål fra eksempelvis datamæglere. Begrebet omfatter også oplysninger, som er lækket på internettet og kan stamme fra databrud, sågar lækkede oplysninger fra udenlandske offentlige myndigheder.

28. Den eneste reelle negative afgrænsning i forhold til oplysninger fra internettet er lukkede hjemmesider og private samtaler på chattjenester, email eller anden krypteret eller privat kommunikation. Disse undtagelser efterlader dog en vis fortolkningstvivl, idet offentlige diskussioner på sociale medier er eksplicit omfattet, og der er generelt en glidende overgang fra private diskussioner i grupper (mellem mere end to personer) til offentlige diskussioner på sociale medier.

29. En Telegram-gruppe kan eksempelvis både være privat kommunikation i en (mindre) gruppe eller en offentlig diskussion, som en større gruppe af personer kan få adgang til, enten med en personlig eller mere generel invitation afhængig af opsætningen af Telegram-gruppen. I begge tilfælde kan enten PET selv, eller en anden dataindsamler (privat virksomhed eller efterretningstjeneste), skaffe sig adgang til en lukket gruppe med et invitationslink (URL) og derefter påbegynde indsamling af oplysninger om diskussioner i gruppen.

30. PET kan modtage oplysninger fra den alment tilgængelige del af internettet fra andre efterretningstjenester, og formentlig også køb hos datamæglere, selv om dette ikke direkte nævnes. Oplysningerne skal blot være offentlige tilgængelige på det tidspunkt, hvor de indsamles, men det fremgår ikke af bemærkningerne hvordan PET skal kontrollere dette,

når dataindsamlingen er foretaget af andre aktører. Det forhold at et datasæt stilles til rådighed for PET udelukker ikke, at oplysningerne i virkeligheden er fremkommet ved eksempelvis hacking eller anden bevidst kompromittering af tjenester på internettet.

31. I de almindelige bemærkninger pkt. 3.1.2 fremhæver Justitsministeriet, at indsamlingen af oplysninger fra offentligt tilgængelige kilder principielt ikke adskiller sig fra den adgang, enhver har til f.eks. at søge i og downloade indhold fra internettet (side 46).

32. Der er imidlertid stor forskel på, at en fysisk person manuelt tilgår visse oplysninger på internettet, og den systematiske indsamling (”scraping”) fra internettet til et større sammenhængende datasæt, som PET-lovens § 10 c, stk. 1 giver mulighed for.

33. I sidstnævnte tilfælde sker der en systematisk behandling af personoplysninger til et nyt formål, som i mange tilfælde vil være uforeneligt med det oprindelige formål. En privat dataansvarlig vil generelt ikke kunne identificere et behandlingsgrundlag i GDPR artikel 6, stk. 1, som tillader systematisk indsamling af personoplysninger fra eksempelvis sociale medier til brug for analyseformål eller andre kommercielle aktiviteter (uanset at denne praksis synes at være udbredt). **Det forhold at personoplysninger er alment tilgængelige på internettet udgør ikke i sig selv et behandlingsgrundlag for en dataansvarlig.**

34. PET er ikke omfattet af GDPR, men indsamling af oplysninger fra internettet vil være et indgreb i retten til privatliv som sikret af artikel 8 i Den Europæiske Menneskerettighedskonvention (EMRK). Personer, der skriver beskeder på sociale medier, må som udgangspunkt have en berettiget forventning om, at deres indlæg ikke havner i en analysemaskine hos en efterretningstjeneste.

35. Efterretningstjenesters indsamling af oplysninger vedr. diskussioner på sociale medier har, udover at være et indgreb i retten til privatliv (EMRK artikel 8) også betydning for udøvelsen af andre grundlæggende rettigheder, navnlig ytringsfriheden (EMRK artikel 10) og forsamlingsfriheden (EMRK artikel 11).

36. Når offentlige diskussioner gøres til genstand for systematisk registrering og efterfølgende analyse (vurdering) hos en efterretningstjeneste, kan mange personer være tilbageholdende med at ytre sig offentligt, fordi de ikke vil registreres af statsmagten og måske udsættes for en indgribende profilering og katalogisering af deres politiske holdninger.

37. Denne ”chilling effect” for ytringsfriheden bør på ingen måder undervurderes. Konsekvenserne for borgernes grundlæggende rettigheder og oplevelsen af at leve i et frit samfund, hvor man kan ytre sig frit uden at blive registreret af statsmagten, kan være betydelige. **Lovforslaget forholder sig imidlertid overhovedet ikke til denne problematik.**

38. Det er i den forbindelse særligt alvorligt, at § 10 c, stk. 1 reelt tillader systematisk indsamling af oplysninger om borgernes politiske præferencer og holdninger fra sociale medie og andre kilder. Det er i direkte modstrid med de beskyttelseshensyn, der ligger bag

PET-lovens § 11. Der vil nærmest uundgåeligt være en risiko for politisk motiveret misbrug af disse oplysninger til overvågning og kontrol af borgernes meningsdannelse, især rettet mod ”afvigende holdninger” hos politiske og etniske minoriteter i samfundet.

Manglende klarhed og forudsigelighed i lovgrundlaget (EMD krav)

39. Ved indgreb i grundlæggende rettigheder stiller retspraksis fra Den Europæiske Menneskerettighedsdomstol (EMD) krav om, at lovgrundlaget er klart og tilgængeligt, og at det er muligt for de berørte personer at vurdere konsekvenserne af indgrebet.

40. Efter IT-Politisk Forenings opfattelse er det tvivlsomt om den meget generelle formulering i § 10 c, stk. 1 og de tilhørende bemærkninger opfylder kravene om klarhed og forudsigelighed. Der er ikke nogen nærmere indikation af de omstændigheder under hvilke PET kan indsamle oplysninger fra offentlige tilgængelige kilder. PET overlades en endog meget stor skønsmargen med det meget generelle ”kan have betydning” kriterie.

41. Der er ikke noget krav om vurdering af de enkelte oplysninger, heller ikke efter den indledende indhentning eller indsamling, idet kriteriet ”kan have betydning” kriteriet gælder for datasættet som helhed. Derudover vil ”kan have betydning” kriteriet nærmest per definition være opfyldt i næsten alle tilfælde, medmindre PET ligefrem selv vurderer, at oplysningerne eller datasættet ikke er relevant for tjenestens opgaver.

42. Ifølge de specielle bemærkninger til § 10 c, stk. 1 vil det være naturligt, at PET i forbindelse med indsamling overvejer, om datasættets omfang kan begrænses, f.eks. ved at udelade bestemte oplysningstyper. Men dette er ikke noget lovkrav, og større sammenhængende datasæt er eksplicit undtaget fra PET-lovens krav om dataminimering i § 6 a, stk. 3.

43. Undtagelsen fra § 6, stk. 3 er i sig selv yderst problematisk, fordi ophævelse af kravet om dataminimering skaber en overhængende risiko for, at større sammenhængende datasæt fører til ”dataophobning by design”.

Større sammenhængende datasæt erhvervet fra datamæglere

44. Offentlige tilgængelige kilder i § 10 c, stk. 2 omfatter tillige oplysninger, som kan erhverves på kommercielle vilkår fra eksempelvis datamæglere.

45. Det er velkendt, at datamæglere indsamler endog meget store datamængder fra sociale medier, smartphone apps, og de personoplysninger som behandles i forbindelse med målrettet annoncering på internettet via real-time bidding (RTB).

46. Nogle af disse datamæglere har ligefrem specialiseret sig i at sælge til efterretningstjenester, for eksempel den amerikanske virksomhed Venntel (datterselskab af Gravy Analytics), der sælger detaljerede profiler med lokationsdata indsamlet ved misbrug af personoplysninger behandlet til RTB.[4] På den måde har efterretningstjenester fået et meget uheldigt

4 Joseph Cox, *Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location*,

interessefælleskab med de amerikanske techgiganter og de største kommercielle datamisbrugere på internettet.[5]

47. Uagtet at oplysninger fra datamæglere betegnes som ”offentligt tilgængelige” i lovforslaget, er der generelt tale om oplysninger, som de berørte personer ikke er klar over eksisterer og udbydes til salg. Indsamlingen sker af private aktører i det skjulte, eksempelvis ved misbrug af RTB-processen, hvor brugerne af hjemmesider og smartphone apps muligvis frivilligt har givet, eller er blevet ulovligt afpresset, et samtykke til målrettet markedsføring, men hvor de samme brugere på ingen måde har givet samtykke til, eller er blevet informeret om, at deres personoplysninger systematisk indsamles og sammenstilles til profiler af eksempelvis lokationsdata (bevægelser i det offentlige rum).

48. Sådanne datasæt, indsamlet med bevidst vildledning af brugerne og derefter solgt til kommercielle og statslige overvågningsinteresser, kan ikke med nogen rimelighed siges at være ”offentligt tilgængelige”.

49. Det er endvidere principielt problematisk, at en dansk offentlig myndighed mod betaling kan erhverve personoplysninger, som må formodes at være indsamlet i strid med GDPR. Derved kommer den danske stat til direkte at understøtte ulovlige aktiviteter.

50. Oplysninger fra datamæglere kan i visse tilfælde bruges til at lave meget præcise profiler af personer, for eksempel deres bevægelser i det fysiske rum (lokationsdata) og deres sociale relationer (kontakter) med andre personer. Disse profiler kan være lige så detaljerede og indgribende, som tilsvarende profiler skabt ud fra bulkindhentet kommunikationsdata eller adgang til metadata lagret af telekommunikationsudbydere efter en logningspligt (hvor PET jf. § 6 skal indhente en retskendelse for at få adgang).

51. I USA har efterretningstjenesterne fået betydelig offentlig kritik for at omgå retsgarantier i Foreign Intelligence Surveillance Act (FISA) ved at erhverve oplysninger om amerikanske borgere fra datamæglere. I den amerikanske kongres er der fremsat lovforslag om at regulere (begrænse) denne adgang til oplysninger om amerikanske borgere.[6]

52. IT-Politisk Forening vil på den baggrund anbefale, at PET’s adgang til at erhverve oplysninger fra datamæglere begrænses, og at sådanne oplysninger ikke kan indgå i større sammenhængende datasæt.

Større sammenhængende datasæt fra andre forvaltningsmyndigheder (§ 10 c, stk. 2)

53. PET kan efter § 10 c, stk. 2 indhente og opbevare oplysninger i større sammenhængende

---

WIRED, 9. januar 2025 https://www.wired.com/story/gravy-location-data-app-leak-rtb/

5 Dette interessefælleskab er uddybende beskrevet i bogen Buron Tau, *Means of Control - How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State*, Crown 2024

6 Fourth Amendment Is Not For Sale Act https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-senators-reintroduce-the-fourth-amendment-is-not-for-sale-act (ikke vedtaget per 6. marts 2025)

datasæt fra andre danske forvaltningsmyndigheder, når datasættet som helhed må antages at have betydning for varetagelse af tjenestens opgaver.

54. Andre forvaltningsmyndigheder vil jf. den foreslåede § 4, stk. 5 være forpligtet til at videregive de oplysninger, som PET anmoder om, uden nogen selvstændig kontrol eller vurdering. Der er heller ikke krav om retskendelse eller forudgående godkendelse hos en anden uafhængig administrativ myndighed.

55. Betingelsen for indhentning efter § 10 c, stk. 2 til større sammenhængende datasæt er meget forskellig fra den nuværende § 4 (fremover § 4, stk. 1), uanset at begge bestemmelser anvender ”må antages at have betydning” kriteriet. I § 4, stk. 1 skal der foretages en vurdering for hver enkelt person (evt. umiddelbart efter indhentning om en større gruppe af personer), mens vurderingen i § 10 c, stk. 2 alene går på datasættet som helhed. Den praktiske konsekvens vil være, at PET fra andre forvaltningsmyndigheder får adgang til oplysninger om mange flere personer i forhold vil de nuværende regler i PET-loven.

56. Ifølge de specielle bemærkninger til § 10 c, stk. 2 vil det tale for at ”må antages at have betydning” betingelsen er opfyldt, når oplysningerne ikke kan indhentes på andre måder. Det vil selvsagt ofte være tilfældet med oplysninger fra andre myndigheder, eksempelvis sundhedsdata som er meget følsomme, og derfor har et særligt behov for beskyttelse mod adgang fra uvedkommende (hvortil PET må regnes).

57. Bemærkningerne nævner, at bestemmelsen kan omfatte sundhedsdata og udbetaling af offentlige ydelser, og at et større sammenhængende datasæt undtagelsesvist kan være et helt register fra en anden myndighed. Det sidste må indebære, at PET som hovedregel kun kan indhente dele af en anden myndigheds register som større sammenhængende datasæt. Lovforslaget angiver imidlertid ingen kriterier for de ”selektorer” eller andre søgekriterier, som PET i givet fald skal anvende for at udvælge og indhente det konkrete større sammenhængende datasæt.

58. Der er heller ikke i lovforslagets bemærkninger gjort noget forsøg på at beskrive under hvilke omstændigheder det overhovedet kan være relevant for PET at behandle store mængder følsomme sundhedsoplysninger eller oplysninger om udbetaling af offentlige ydelser. Det er ikke PET, som kontrollerer udbetaling af offentlige ydelser, og PET er heller ikke beskæftiget med sundhedsbehandling af borgerne.

59. At give PET adgang til følsomme sundhedsoplysninger om et stort antal personer er i sagens natur ekstremt indgribende i disse personers ret til privatliv. Ansatte i sundhedssektoren er som bekendt undergivet særlige krav om fortrolighed vedr. de personer, som de behandler. Denne fortrolighed mellem patienter og sundhedspersoner kompromitteres, når oplysninger videregives til PET. I værste fald kan det have en dæmpende effekt på borgernes villighed til at henvende sig til det eksempelvis psykiatriske behandlingssystem, hvis de derved risikerer at have i en stor PET-database, hvor indgribende dataanalyser med risiko-scoring efterfølgende bruges til at vurdere, om de

udgør en fare for samfundet.

60. Bemærkningerne ovenfor i punkt 39-43 om lovgrundlagets manglende klarhed og forudsigelighed gælder også i forhold til § 10 c, stk. 2 (og stk. 3 der behandles nedenfor).

61. Endelig vil IT-Politisk Forening opfordre til, at Justitsministeriet præciserer hvad der menes med denne sætning på side 208: ”*PET udgør organisatorisk en del af Rigspolitiet, og den foreslåede ordning vil således ikke berøre overførsel af oplysninger mellem tjenesten og det øvrige politi eller vedrøre tilgængeligheden af politiets centrale registre og systemer mv.*”

    Uanset at PET er en del af Rigspolitiet, vil PET’s adgang til oplysninger hos det øvrige politi indebære en videregivelse af personoplysninger, der hos det øvrige politi behandles efter retshåndhævelsesloven og EU-rettens databeskyttelsesregler, hvilket ikke er tilfældet, når oplysningerne er videregivet til PET.

Større sammenhængende datasæt om ikke-danske personer (§ 10 c, stk. 3)

62. Efter § 10 c, stk. 3 kan PET indsamle, indhente og opbevare større sammenhængende datasæt, som langt overvejende må antages at indeholde oplysninger om personer, der ikke er hjemmehørende i Danmark (ikke-danske personer). Kriteriet er ligesom i stk. 1, at datasættet som helhed ”kan have betydning” for varetagelsen af tjenestens opgaver. PET kan ikke indhente eller opbevare større sammenhængende datasæt bestående af rådata.

63. Det er meget uklart hvad denne bestemmelse reelt kan omfatte, fordi eneste afgrænsning er, at datasættet ikke kan være rådata, dvs. der skal være foretaget en vis bearbejdning af rådata. Ifølge bemærkningerne (side 210) synes det at være tilstrækkelig bearbejdning, hvis eksempelvis Forsvarets Efterretningstjeneste (FE) har bearbejdet indhentet rådata (bulkindhentning) med en udvælgelsesproces, som sikrer at antallet af oplysninger om i Danmark hjemmehørende personer er begrænset.

64. Det er efter IT-Politisk Forenings læsning af bemærkningerne også uklart, om § 10 c, stk. 3 kan omfatte oplysninger, der stammer fra bulkindhentning af kommunikationsdata. Bemærkninger udelukker umiddelbart ”*datasæt af en helt ubearbejdet karakter, når disse består af oplysninger, der hidrører fra masseindhentning af kommunikationsdata*”, men det er ikke videre klart, om en udvælgelse af ikke-danske personer (som i punkt 63) er tilstrækkelig bearbejdning.

65. Uanset kravene til bearbejdning vil indhentning af kommunikationsdata for udlændinge på generel og udifferentieret basis være et meget alvorligt indgreb i retten til privatliv. Selv om indhentning sker til større sammenhængende datasæt, kan de indhentede kommunikationsdata også blive anvendt til målrettede personundersøgelser efter § 5, og PET kan få adgang til metadata eller indholdet for privat kommunikation på en måde, som kan omgå kravet om retskendelse for indgreb i meddelelseshemmeligheden i § 6.

66. Bortset fra § 11 om lovlig politisk virksomhed skelner bestemmelserne i PET-loven ikke

mellem, om den fysiske eller juridiske person er i Danmark hjemmehørende eller ej. På den baggrund forekommer det besynderligt, at § 10 c, stk. 3 tillader en udvidet adgang til indhentning af større sammenhængende datasæt for personer, der ikke er hjemmehørende i Danmark. En sådan diskrimination på grundlag af nationalitet er i modstrid med de overvejelser, der ligger bag vedtagelsen af PET-loven i 2013.

Analyser af større sammenhængende datasæt (§ 10 d)

67. Efter den foreslåede § 10 d kan PET oversætte, strukturere og foretage analyser af større sammenhængende datasæt, når behandlingen "kan have betydning" for varetagelse af tjenestens opgaver. Det er en behandlingsbetingelse, som næsten altid vil være opfyldt (medmindre PET selv på forhånd kan udelukke at analysen vil være relevant for tjenesten).

68. Analyser kan være generelle analyser, hvor oplysninger om fysiske og juridiske personer behandles for at producere rapporter med aggregerede (eller anonymiserede) oplysninger.

69. Analyser kan imidlertid også foretages som led i målopdagelse. Dette begreb er ikke nærmere defineret i lovforslaget, men efter IT-Politisk Forening læsning kan det omfatte søgning efter ikke-identificerede personer, som opfylder bestemte søgekriterier, og på denne måde kan være interessante for PET (analyser med "data mining"). Den fortolkning understøttes af § 10 f, stk. 3, som fastsætter, at PET-lovens almindelige behandlingsregler finder anvendelse, hvis en analyse efter § 10 d fører til at der udarbejdes rapporter m.v. om en udfundet person.

70. Den eneste reelle begrænsning i § 10 d er, at analyser ikke må være målrettet bestemte identificerede personer. Hvis PET vil bruge større sammenhængende datasæt til dette formål, gælder PET-lovens almindelige behandlingsregler i §§ 7-8 og tærsklen for behandling af oplysninger er "må antages at have betydning" kriteriet, som kræver at der skal være en mere konkret formodning om, at oplysningerne vil have betydning for PET (opgaverne vedr. straffelovens kapitel 12 og 13).

71. Konsekvensen af dette er, at der gælder færre retsgarantier, når PET foretager data-mining analyser af større sammenhængende datasæt med søgninger efter ukendte målpersoner med henblik på eventuelt at indlede undersøgelser mod de personer, der opfylder bestemte søgekriterier, end hvis PET fra starten målretter søgningen mod en bestemt person i en undersøgelse.

72. Efter IT-Politisk Forenings opfattelse er data-mining analyser med henblik på at identificere ukendte personer til undersøgelser eller efterforskning på mange måder mere indgribende end at foretage tilsvarende foranstaltninger mod en bestemt (identificeret) person. Det gælder ikke mindst, når data-mining analyser kan foretages uden nogle retsgarantier for selve analysen (søgningen).

73. Brevåbning er et vidtgående efterforskningsskridt, fordi statsmagten får kendskab til en borgers private korrespondance. Retsplejeloven har derfor materielle og processuelle regler

til beskyttelse af borgerne, herunder krav om forudgående mistanke. Det vil imidlertid være endnu mere vidtgående at åbne og undersøge alle borgeres breve (som i fortidens sorte kabinetter[7]) med henblik på at indlede efterforskning mod de personer, hvor indholdet af deres breve matcher bestemte søgekriterier om mulige ulovlige forhold.

74. Data-mining analyser i § 10 d med henblik på at udfinde målpersoner sætter reelt alle personer under mistanke, og de får først tildelt visse retsgarantier i PET-loven, når de i analysen er blevet identificeret som målpersoner. Det undergraver væsentlige retsgarantier som uskyldsformodningen og retten til en retfærdig rettergang.[8]

75. **IT-Politisk Forening vil anbefale, at PET ikke får mulighed for at lave analyser af større sammenhængende datasæt med henblik på at udfinde målpersoner, som opfylder bestemte søgekriterier.** En sådan begrænsning vil medføre, at § 10 d kun kan anvendes til generelle analyser, hvor oplysninger om fysiske eller juridiske personer alene indgår i anonymiseret eller aggregeret form i analyserapporten. Denne type "statistiske" analyser er mindre indgribende i grundlæggende rettigheder, fordi analysen i sin helhed kan laves på pseudonymiserede personoplysninger, og re-identifikation (afmaskering) af fysiske (eller juridiske) personer er under ingen omstændigheder aktuelt i forbindelse med analysen.

Lovforslaget indeholder ingen krav til analyseværktøjer

76. Ligesom de øvrige bestemmelser vedr. større sammenhængende datasæt, stiller lovforslaget ingen formelle krav til de analyseværktøjer, som PET kan benytte til analyser efter § 10 d, udover at analysen som sådan ikke må være målrettet bestemte identificerede personer (hvor PET-lovens almindelige bestemmelser om behandling af oplysninger i §§ 7-8 i stedet skal anvendes).

77. Der er således ingen konkrete krav til de algoritmer eller AI-baserede værktøjer, som PET kan anvende. Justitsministeriet bemærker ligefrem i bemærkningerne (side 219), at analyser og sammenstillinger af oplysninger, der er foretaget af IT-systemer, **kan indeholde fejl, være diskriminerende eller på anden måde vise sig uegnede som grundlag for at indlede en undersøgelse eller efterforskning mod en person.**

78. Disse alvorlige mangler har imidlertid ingen konsekvenser for PET's anvendelse af analyseværktøjer, selv hvis de er diskriminerende, eller hvis resultaterne af analysen kan være biased eller direkte forkert. Der er alene i bemærkningerne til § 10 d en henvisning til,

7 Andreas Marklund, *Overvågningens historie: Fra sorte kabinetter til digital masseovervågning*, Gads Forlag 2020

8 Alle har noget at skjule, og hvis staten kan indhente store datamænger fra alle mulige kilder, og derefter analysere de indhentede datasæt med data-mining værktøjer til udfinding af målpersoner (mistænkte), kan staten finde belastende materiale på næsten alle borgere. Det klassiske citat fra den franske kardinal Richelieu (1585–1642), "If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him," illustrerer på brutal vis (efter nutidens menneskeretlige normer for det strafferetlige system) denne problemstilling. Citatet er også blevet brugt af whistlebloweren Edward Snowden i et tweet om NSA's masseovervågning (se https://xcancel.com/Snowden/status/653722120434921472).

at PET skal vurdere oplysninger, analyser og resultater kritisk.

79. Erfaringerne med komplekse databaserede analyseværktøjer til eksempelvis predictive policing eller andre automatiske analyser af store datasæt viser imidlertid, at der er en overdreven tillid til resultatet af disse analyser. Når en person udpeges som målperson af systemerne, er der en indbygget formodning om at reagere på dette resultat.[9]

80. Den menneskelige kontrol (human review) af en automatiseret udpegning af målpersoner er endvidere vanskelig at foretage, hvis analytikeren ikke har nogen reel mulighed for at forstå det resultat, som den automatiserede analyse kommer frem til.[10]

81. Alle personer, som optræder i større sammenhængende datasæt, risikerer derfor at blive offer for PET's anvendelse af fejlbehæftede, diskriminerende eller direkte racistiske algoritmer, hvor de efter at blive "udfundet" af algoritmens vilkårlige databehandling kan blive udtaget til indgribende undersøgelser eller efterforskning. Det gælder uanset at datasættet officielt er indsamlet på grund af dets generelle relevans for PET's arbejde, og at de fleste personer i datasættet måske aldrig vil blive direkte identificeret af PET.

82. Problemerne med eksempelvis diskrimination er naturligvis ikke unikke for algoritmer eller AI-baserede systemer. Men erfaringen viser, at eksisterende biases og diskrimination i politiets eller efterretningstjenesters arbejde vil blive afspejlet og forstærket i sådanne systemer, hvor meget store datamængder behandles, og at de negative konsekvenser for de berørte personer (især udsatte minoritetsgrupper) vil blive meget større.

83. Problemerne med diskrimination forværres desuden af, at borgerne med lovforslaget fuldstændig afskæres fra adgangen til effektive retsmidler i forhold til PET's anvendelse af større sammenhængende datasæt, herunder brugen af fejlbehæftede, vilkårlige og diskriminerende AI-systemer.

84. Anbefalingen i punkt 75 ovenfor om, at PET ikke må anvende § 10 d til at udfinde målpersoner, vil kun delvist adressere problemerne med diskrimination. Det skyldes at AI-systemers diskrimination også kan optræde i aggregerede analyser (diskrimination på gruppeniveau, der potentielt kan være endnu mere stigmatiserende).

Retspraksis fra EMD om bulkindhentning ift. større sammenhængende datasæt

85. Efter lovforslaget er der ingen uafhængig forudgående kontrol med PET's indsamling og indhentning af større sammenhængende datasæt.

86. I forhold til omfanget af indgrebet i grundlæggende rettigheder er der et betydeligt overlap

9 Se eksempelvis diskussionen af "presumption to intervene" i denne rapport om ansigtsgenkendelse i Storbritannien: Pete Fussey & Dr. Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, juli 2019, https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

10 Se argumenterne i præmis 194-195 i EU-Domstolens dom vedr. PNR-direktivet C-817/19 *Ligue des droits humains*.

med den bulkindhentning, som EMD tager stilling til i dommene *Big Brother Watch m.fl. mod Storbritannien* (58170/13, 62322/14 og 24960/15) og *Centrum för Rättvisa mod Sverige* (35252/08), begge af 25. maj 2021.

87. I de to domme forholder EMD sig til bulkindhentning af kommunikationsdata, men det betyder ikke, at kravet om forhåndsgodkendelse ved en uafhængig instans kun gælder for bulkindhentning af kommunikationsdata. Det samme gør sig gældende for de *end-to-end safeguards*, som spiller en central rolle for vurderingen af et system til bulkindhentning i de to EMD-domme.

88. I dommene vedr. Sverige og Storbritannien lægger EMD vægt på, at bulkindhentning anvendes til efterretningsmæssige formål, og at oplysninger fra bulkindhentning ikke senere kan anvendes som bevismidler i straffesager (præmis 369 i *Big Brother Watch m.fl.* og præmis 286-287 i *Centrum för Rättvisa*).

89. PET er både efterretningstjeneste og politimyndighed, og oplysninger indhentet til større sammenhængende datasæt kan efterfølgende anvendes til personundersøgelser efter § 5 og strafferetlig efterforskning efter § 6. Det kan ske ved brug af større sammenhængende datasæt til målrettede undersøgelser efter PET-lovens almindelige behandlingsregler, eller hvis analyser som led i målopdagelse efter § 10 d medfører, at der udfindes oplysninger om bestemte fysiske personer.

90. Dette forhold omkring PET's dobbelte rolle øger efter IT-Politisk Forenings opfattelse kravene til forudgående uafhængig kontrol med både indhentning og analyse af større sammenhængende datasæt.

Ingen adgang til effektive retsmidler i forbindelse med større sammenhængende datasæt

91. I forhold til EMD retspraksis er det endvidere særdeles problematisk, at borgerne reelt ikke har nogen adgang til effektive retsmidler i forbindelse med PET's indsamling, indhentning, opbevaring og analyse af større sammenhængende datasæt. Oplysninger fra større sammenhængende datasæt er først omfattet af den indirekte indsigtsordning i § 13, når der sker en behandling efter PET-lovens almindelige regler, eller når der udfindes oplysninger om bestemte personer i analyser efter § 10 d, og dette fører til udarbejdelse af efterretnings- eller analyserapporter m.v. (jf. § 10 f, stk. 3).

92. Der er ikke i lovforslaget nogen overvejelser om hvordan denne fuldstændige afskæring af adgangen til effektive retsmidler kan være foreneligt med kravene i EMRK artikel 13. Den indirekte indsigtsordning er efter ændringen af PET-loven i 2016 borgernes eneste mulighed for, at Tilsynet med Efterretningstjenesterne (TET) kan træffe en bindende afgørelse om sletning af oplysninger, der opbevares ulovligt af PET.

93. Når PET kan foretage søgninger efter bestemte personer i større sammenhængende datasæt i forbindelse med målrettede undersøgelser, må det samme være muligt, når der indgives en anmodning om indirekte indsigt. At sådanne søgninger muligvis er tidskrævende og

besværlige for PET kan ikke veje tungere end hensyn til borgernes grundlæggende rettigheder, herunder EMRK artikel 13.

94. Justitsministeriet anfører i de specielle bemærkninger til § 10 f, stk. 1, at den indirekte indsigtsordning ikke vil kunne fungere hensigtsmæssigt, fordi oplysninger om en person kan komme til medarbejdere i PET's kendskab alene i kraft af indsigtsanmodningen.

95. Dette principielle problem kan håndteres ved, at der i § 13 indsættes en bestemmelse om, at de oplysninger, som en fysisk eller juridisk personer selv angiver i en anmodning om indirekte indsigt alene må behandles med henblik på at undersøge, om PET behandler oplysninger om den pågældende. En sådan klar formålsbegrænsning, som sikrer at en anmodning om indirekte indsigt aldrig kan føre til yderligere registrering om en person hos PET, bør efter IT-Politisk Forenings opfattelse være underforstået af PET-lovens § 13 i sammenhæng med de databeskyttelsesretlige regler i § 6 a.

Videregivelse af oplysninger fra andre forvaltningsmyndigheder til PET (§ 4)

96. Under den gældende PET-lov skal andre forvaltningsmyndigheder videregive oplysninger til PET, hvis tjenesten vurderer, at oplysningerne må antages at have betydning for varetagelsen af tjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13 (jf. § 4, fremover § 4, stk. 1).

97. Med lovforslaget får andre forvaltningsmyndigheder endvidere pligt til at videregive større sammenhængende datasæt til PET, hvis datasættet som helhed må antages at have betydning varetagelsen af tjenestens opgaver (jf. § 4, stk. 9 og § 10 c, stk. 2).

Forholdet til databeskyttelsesforordningen (GDPR) og databeskyttelsesloven

98. Selve videregivelsen til PET er en behandling, der foretages af en dataansvarlig omfattet af GDPR. Personoplysninger behandles til et andet formål end det oprindelige, og denne nye behandling skal opfylde kravene i GDPR artikel 6, stk. 4. I den konkrete tilfælde vil det retlige grundlag for behandlingen (videregivelsen) være en national lov, der skal opfylde kravene i artikel 23, jf. GDPR artikel 6, stk. 4.

99. Det afgørende er her, at selve videregivelsen er underlagt EU-rettens databeskyttelsesregler, uagtet at den efterfølgende behandling hos PET ikke måtte være det. I forhold til GDPR er videregivelsen til PET en begrænsning af den registreredes rettigheder (artikel 23), og ikke en behandling som falder uden for GDPR.

100. Retspraksis fra EU-domstolen viser, at karakteren af og retsgarantier for den efterfølgende behandling af personoplysninger hos PET (national sikkerhed) i et vist omfang er relevante for vurderingen af, om videregivelsen opfylder EU-rettens krav om, at indgrebet i grundlæggende rettigheder skal være begrænset til det strengt nødvendige.

101. Som en overordnet betragtning udtaler EU-Domstolen i de forenede sager C-511-18, C-512-

18 and C-520-18 *La Quadrature du Net m.fl.* præmis 99, at selv om det tilkommer medlemsstaterne at fastsætte deres væsentlige sikkerhedsinteresser og at træffe de nødvendige foranstaltninger til at opretholde deres indre og ydre sikkerhed, kan alene den omstændighed, at en national foranstaltning er blevet truffet med henblik på at beskytte den nationale sikkerhed, ikke medføre, at EU-retten ikke finder anvendelse, og fritage medlemsstaterne fra at sikre den nødvendige overholdelse af denne ret.

102. I den forbindelse skal det bemærkes, at der sker en fuldstændig begrænsning af den registreredes rettigheder, når borgernes personoplysninger videregives til PET, jf. den foreslåede § 4, stk. 6 (der svarer til nuværende praksis).

103. De registrerede får ingen information om videregivelsen, og de har hos forvaltningsmyndigheden ingen mulighed for at få indsigt i de personoplysninger, som er videregivet til PET. Det påvirker bl.a. muligheden for at få berigtiget fejlbehæftede personoplysninger, som kan have alvorlige konsekvenser for borgerne, når oplysningerne bruges til automatiserede analyser af større sammenhængende datasæt efter § 10 d.

104. I de almindelige bemærkninger pkt. 11.1.2 lægger Justitsministeriet vægt på, at en fysisk eller juridisk person i stedet kan gøre brug af den indirekte indsigtsordning hos Tilsynet med Efterretningstjenesterne. Under den indirekte indsigtsordning får den fysiske eller juridiske person imidlertid altid det samme intetsigende svar om, at PET ikke uberettiget behandler om dem, uanset om PET rent faktisk gjorde dette eller ej. Det er en væsentlig forringelse af rettighederne under GDPR.

105. Derudover er oplysninger og behandlingen i store sammenhængende datasæt helt undtaget fra den indirekte indsigtsordning. Det indebærer en fuldstændig afskæring af borgernes adgang til effektive retsmidler.

106. EU-Domstolen har i C-362/14 *Schrems*, præmis 95 udtalt, at en lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, **ikke opfylder det væsentligste indhold** af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47.

107. Særligt for videregivelsen fra andre forvaltningsmyndigheder til større sammenhængende datasæt hos PET er det derfor tvivlsomt, om § 4, stk. 6 respekterer det væsentligste indhold af de rettigheder som er sikret af EU's Charter for Grundlæggende Rettigheder.

108. Når personoplysninger videregives til retshåndhævende myndigheder accepterer EU-Domstolen generelt kun en midlertidig begrænsning af pligten til, at underrette den registrerede om videregivelsen, så længe denne orientering kan forstyrre en igangværende efterforskning.

109. I den forbindelse er det generelt vanskeligt at se hvilken efterforskning, eller tilsvarende

undersøgelse, hos PET som vil blive forstyrret af en underretning af de registrerede om, at deres personoplysninger er videregivet til større sammenhængende datasæt hos PET. Det fremhæves netop i lovforslagets bemærkninger, at analyserne af disse datasæt ikke er rettet mod identificerede personer.

110. Det er meget muligt, at en underretning af borgerne om at deres måske stærkt følsomme personoplysninger (f.eks. sundhedsoplysninger) videregives til PET's store AI-baserede analysemaskine (større sammenhængende datasæt), vil afføde betydelige offentlige protester og kan give politiske problemer for den siddende regering. Nogle vil måske sige, at overvågningsstaten fungerer mest effektivt i den dybeste hemmelighed. Det er imidlertid ikke saglige hensyn for at begrænse pligten til at underrette de registrerede om videregivelsen.

Generel og udifferentieret videregivelse til større sammenhængende datasæt

111. Udover ovenstående bemærkninger vedrørende de registreredes rettigheder, er det problematisk og potentielt i strid med EU-retten, at videregivelsen af personoplysninger til større sammenhængende datasæt er generel og udifferentieret.

112. IT-Politisk Forening er opmærksom på, som det anføres i lovforslagets bemærkninger, at det generelt ikke er det fulde register fra en anden forvaltningsmyndighed, som videregives til PET i medfør af § 4, stk. 5 og § 10 c, stk. 2.

113. Lovforslagets fastsætter imidlertid ingen objektive kriterier for hvilke personoplysninger, der skal videregives til PET. Omfanget af videregivelsen sker alene efter PET's vurdering med kriterier, som ikke er fastsat i lovgivningen, jf. bemærkningerne ovenfor i høringssvaret. Derfor er det passende at betragte videregivelsen som generel og udifferentieret.

114. I C-623/17 *Privacy International* har EU-Domstolen vurderet en "Bulk Personal Data" ordning i Storbritannien, hvor efterretningstjenester kunne forlange metadata for elektronisk kommunikation (teledata) udleveret fra teleudbydere på generel og udifferentieret basis. Denne adgang til data var ikke tidsmæssigt begrænset til ekstraordinære situationer, hvor den nationale sikkerhed skal beskyttes mod en alvorlig trussel, som må anses for at være reel og aktuel eller forudsigelig. I dommen C-623/17 fandt EU-Domstolen, at den britiske lovgivning ikke overholdt kravene i e-databeskyttelsesdirektivets artikel 15, stk. 1.

115. I GDPR-sammenhænge modsvares e-databeskyttelsesdirektivets artikel 15, stk. 1 af GDPR artikel 23 (begrænsning af rettigheder sikret af hhv. e-databeskyttelsesdirektivet og GDPR).

116. På baggrund af EU-dommen C-623/17 vil det være relevant at overveje, om den generelle og udifferentierede videregivelse til større sammenhængende datasæt hos PET overholder EU-rettens krav om, at indgreb i grundlæggende rettigheder skal være begrænset til det strengt nødvendige.

117. Der er naturligvis forskelle mellem metadata for elektronisk kommunikation og de personoplysninger, som kan videregives til større sammenhængende datasæt. I forhold til kommunikationsdata lægger EU-Domstolen bl.a. vægt på risikoen for, at oplysninger kan bruges til at skabe detaljerede profiler af de berørte personer.

118. Muligheden for at skabe detaljerede profiler af borgerne er imidlertid også til stede med de personoplysninger, som kan videregives fra andre forvaltningsmyndigheder til PET, særligt fordi lovgrundlaget i PET-lovens kapitel 6 a ikke på nogen måde afgrænser de oplysninger, som kan indhentes, indsamles, opbevares og behandles af PET. Derudover har visse personoplysninger hos andre forvaltningsmyndigheder, navnlig sundhedsoplysninger, en indbygget følsomhed som direkte kan sammenlignes med kommunikationsdata.

Direkte elektroniske adgange til andre forvaltningsmyndigheders systemer

119. Lovforslagets § 4, stk. 2 giver mulighed for, at andre forvaltningsmyndigheder kan etablere direkte elektronisk adgang for PET til deres systemer.

120. Efter IT-Politisk Forenings vurdering er det yderst tvivlsomt, om de dataansvarlige kan overholde deres forpligtelser i GDPR artikel 32, hvis de giver PET direkte adgang til deres systemer. En sådan "bagdør" vil blandt andet øge risikoen for databrud, navnlig fordi der er tale om en systemadgang, som den dataansvarlige ikke kan systemovervåge og eksempelvis foretage logning af brugen af adgangen. Formålet med den direkte systemadgang er netop, at PET kan få adgang til oplysninger uden at det registreres i logfiler eller anden systemovervågning.

121. Den dataansvarliges forpligtelser i henhold til GDPR artikel 32 kan ikke begrænses eller fraviges af national lovgivning, som det reelt sker med lovforslaget. GDPR artikel 32 er ikke omfattet af de forpligtelser og rettigheder, der kan begrænses eller fraviges af national lovgivning i henhold til GDPR artikel 23, stk. 1.[11]

PET's anmodninger om søgning i rådata hos FE (§ 4 a)

122. Efter den foreslåede § 4 a kan PET's anmode Forsvarets Efterretningstjeneste om at foretage søgninger i allerede tilvejebragte rådata, når søgningen må antages at have betydning for varetagelsen af PET's opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.

123. Den foreslåede bestemmelse indeholder meget få kriterier og materielle bestemmelser, som effektivt kan afgrænse omfanget af en søgning. Der er ikke noget krav om, at en anmodning skal vedrøre en bestemt persons kommunikation, svarende til kravene for telefonaflytning i retsplejeloven. Det er problematisk, fordi resultatet af en søgning kan indeholde oplysninger om et stort antal personer og have karakter af masseovervågning af privat kommunikation.

11 Jf. analogt forenede sager C-203-15 og C-698-15 *Tele2 m.fl.* præmis 122, hvor EU-Domstolen konstaterer, at artikel 15, stk. 1 i e-databeskyttelsesdirektivet 2002/58/EF ikke gør det muligt for medlemsstaterne at fravige sikkerhedsbestemmelserne i artikel 4, stk. 1 eller stk. 1a med national lovgivning.

124. Der er i § 4 a, stk. 2 undtagelser, som beskytter kommunikation med personer, der er vidneudelukket i medfør af retsplejelovens § 170 (præster, læger, advokater, m.fl.), samt en beskyttelse af journalisters kommunikation, hvis den kan afsløre kildeforhold, medmindre hensynet til kildebeskyttelse må vige for hensynet til PET's opgavevaretagelse.

125. Derudover er der ingen konkrete bestemmelser om søgningerne, udover kravet om, at søgningen "må antages at have betydning". Anmodningen skal være udformet på en sådan måde, at det fremgår, hvilke personer eller søgekriterier, søgningen omfatter (side 193). Det er imidlertid først og fremmest en teknisk beskrivelse af søgningen, som er nødvendig for at FE overhovedet kan udføre den.

126. Beskrivelsen af søgekriterier i bemærkningerne tillader eksplicit "fiskeekspeditioner" efter ukendte personer, som opfylder de søgekriterier, der angives i anmodningen. I bemærkningerne nævnes en søgning efter danske mailadresser, eller andre identificerende kendetegn, som har været i kontakt med en bestemt person. En sådan søgning kan potentielt omfatte et stort antal personer, som udsættes for overvågning af deres private kommunikation uden forudgående mistanke eller anden konkret individuel forhåndsvurdering. Det vil være muligt efter § 4 a, stk. 1, fordi "må antages at have betydning" kravet i bestemmelsen vedrører søgningen som sådan, og ikke individuelle forhold vedrørende de personer hvis private kommunikation eller andre oplysninger gøres til genstand for søgningen.

127. Den meget generelle beskrivelse af søgekriterier betyder således, at der er overladt endog meget store skøn til PET. På grund af de manglende materielle bestemmelser om søgningerne vil det antageligt være vanskeligt for domstolene at foretage en effektiv kontrol (i det omfang søgningerne skal forelægges domstolene), herunder en proportionalitetsvurdering som det forudsættes i § 4 a, stk. 2.

128. Med hensyn til proportionalitetsvurderingen i § 4 a, stk. 2 finder IT-Politisk Forening det yderst betænkeligt, at Justitsministeriet nærmest på forhånd bestemmer resultatet af domstolens uafhængige vurdering ved i bemærkningerne (side 192) at forudsætte, at det vil kræve særlige grunde for at proportionalitetsvurderingen i sig selv fører til, at en søgning ikke kan foretages.

129. En anmodning om søgning i rådata hos FE kan omfatte personer, der er hjemmehørende i Danmark. Lovforslagets bemærkninger forholder sig i den forbindelse ikke til, at FE's bulkindhentning af kommunikationsdata (rådata) skal være rettet mod forhold i udlandet, og at oplysninger om i Danmark hjemmehørende personer, og personer der opholder sig i Danmark, kun må medtages som tilfældighedsfund, jf. FE-lovens § 3, stk. 2.

130. Umiddelbart giver det ikke videre mening at søge efter oplysninger vedrørende Danmark hjemmehørende personer i indhentede rådata hos FE, hvor disse personer kun må optræde i yderst begrænset omgang (som tilfældighedsfund).

131. Det undrer endvidere IT-Politisk Forening, at der kun er krav om retskendelse ved

søgninger, der vedrører i Danmark hjemmehørende personer eller personer der opholder sig i Danmark. Som anført ovenfor er der i PET-loven (bortset fra § 11) ingen diskrimination på grundlag af nationalitet eller hvor de berørte personer opholder sig. En søgning i rådata, som i høj grad formodes at bestå af bulkindhentede kommunikationsdata, kan bedst sammenlignes med indgreb i meddelelseshemmeligheden, hvor retsplejeloven heller ikke diskriminerer på grundlag af nationalitet. Der er altid krav om retskendelse.

132. I lovforslagets almindelige bemærkninger pkt. 3.5.1.2 begrundes denne diskrimination med, at det for øvrige udlændinge (der ikke opholder sig i Danmark) er PET-lovens almindelige tilvejebringelseshjemmel i § 3 og FE-lovens videregivelseshjemmel i § 7, stk. 1, der udgør begrænsningerne. FE-lovens § 7, stk. 1 gælder imidlertid for enhver videregivelse fra FE til PET, uanset om personen er i Danmark hjemmehørende.

133. Derudover må karakteren af det indgreb, som PET's søgning i rådata hos FE medfører, tillægges større betydning end FE-lovens videregivelsesbestemmelser i § 7, stk. 1. Det forhold, at PET senere kan bruge resultatet af søgningen i straffesager, bør i sig selv føre til, at der altid er forudgående domstolskontrol af søgningen.

134. **På den baggrund vil IT-Politisk Forening anbefale, at alle anmodning fra PET om søgninger i rådata skal underkastes domstolskontrol som i § 4 a, stk. 2.** Ud over den generelle forbedring af retssikkerheden, også for udlændinge, vil domstolskontrol for alle søgninger eliminere problemer ved de grænsetilfælde, hvor der tvivl om hvorvidt resultatet af søgningen vedrører i Danmark hjemmehørende personer.