Juni 2017

Danske myndigheders registrering af borgernes adfærd på internettet – regelgrundlaget og de tilhørende kontrolmekanismer

Professor, dr.jur. Henrik Udsen, Center for informations- og innovationsret, Det Juridiske Fakultet, Københavns Universitet

1. INDLEDNING

Gennem de senere år har myndigheder i stigende omfang indsamlet og brugt oplysninger om borgernes adfærd på internettet. Dette er en naturlig konsekvens af internettets øgede betydning: Myndighedernes kontrol med og efterforskning af borgernes adfærd må ske, hvor borgerne befinder sig. På den ene side er udviklingen således nødvendig for, at myndigheder effektivt kan udøve den kontrol og efterforskning, som vores samfundsindretning og de bagvedliggende lovregler forudsætter. På den anden side giver denne form for kontrolmulighed for en mere intensiv registrering af borgernes adfærd og dermed en større risiko for, at registreringen krænker borgernes ret til privatliv og egne personoplysninger.

De regler, der giver myndigheder adgang til at indsamle og bruge oplysninger om borgernes internetadfærd[1], skal derfor afveje væsentlige modsatrettede hensyn. Navnlig siden Snowden-afsløringerne har det været drøftet, om de gældende regler er udtryk for en hensigtsmæssig afvejning, eller om myndighedernes adgang til at registrere borgenes internetadfærd er for vidtgående, og om der er tilstrækkelige kontrol med myndighederne. Denne diskussion vanskeliggøres af, at det kan være svært at få et overblik over de gældende regler, som er placeret i en række forskellige love. Nærværende rapport foretager en samlet præsentation af de regler, der giver myndigheder adgang til at indsamle og bruge oplysninger om borgernes internetadfærd (afsnit 2) og de tilknyttede kontrolmekanismer (afsnit 3). Formålet er at give et samlet overblik over reglerne. For en mere indgående beskrivelse af de enkelte regler henvises til speciallitteraturen.

Afvejningen mellem de skitserede modsatrettede hensyn er primært af politisk karakter. Det er ikke formålet med denne redegørelse at drøfte, hvordan denne afvejning skal foretages. Derimod er der knyttet nogle overordnede bemærkninger til kvaliteten af de eksisterende regler (afsnit 2.5) og nogle bemærkninger til den demokratiske kontrol (afsnit 3.6).

2. REGELGRUNDLAGET

Den følgende beskrivelse af regelgrundlagt for myndigheders overvågning af borgernes internetadfærd er opdelt i fire kategorier af regler. Den første omhandler de regler, der giver myndigheder ret

[1] Med "internetadfærd" menes her i bred forstand de aktiviteter, som borgerne udøver på internettet, som f.eks. e-mailkorrespondance, hjemmesidebesøg, kommunikation på sociale medier mv.

til at indsamle[2] oplysninger. Den anden omhandler de regler, der giver myndigheder ret til at videregive indsamlede oplysninger til andre myndigheder. Den tredje omhandler private parters adgang til at videregive oplysninger til myndigheder. Disse regler er væsentlige, da mange private virksomheder indsamler store mængder af oplysninger om borgernes internetadfærd, som kan være relevante for myndigheder at få adgang til. Den fjerde omhandler regler, der pålægger private parter at registrere oplysninger om borgernes internetadfærd med henblik på, at myndighederne kan få adgang hertil. I praksis udgøres denne fjerde kategori af logningsreglerne, der har stor betydning for adgangen til oplysninger om borgernes internetadfærd. Beskrivelsen af regelgrundlaget fokuserer på de mere generelle regler og inddrager ikke eventuelle særlovsbestemmelser[3].

2.1. Regler der giver myndigheder ret til at indsamle oplysninger

Lovgivningen om myndigheders adgang til indsamling af oplysninger om borgernes internetadfærd sondrer mellem indsamling foretaget af politiet, efterretningstjenesterne og andre myndigheder. I det følgende beskrives først de regler, der gælder for myndigheder generelt i persondataloven. Herefter beskrives forskellige regelsæt, der gælder for politiet, og afslutningsvist de regelsæt, der gælder for henholdsvis Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste og Center for Cybersikkerhed.

2.1.1. Myndigheder generelt - persondataloven

En myndigheds egen indsamling af personoplysninger fra internettet vil udgøre en behandling af personoplysninger i persondatalovens[4] forstand og derfor være omfattet af lovens krav. Der skal derfor være hjemmel til indhentelse af oplysningerne i lovens § 6 (almindelige personoplysninger), § 7 (følsomme personoplysninger) eller § 8 (semi-følsomme personoplysninger).

Efter § 6, stk. 1, nr. 6, kan en offentlig myndighed behandle personoplysninger, når behandlingen er nødvendig for, at myndigheden kan udføre sine opgaver. Det samme gælder for semi-følsomme oplysninger efter § 8, stk. 1. Tilsvarende gælder efter § 7, stk. 6, når behandlingen af følsomme personoplysninger er nødvendig for en myndigheds udøvelse af sine opgaver på det strafferetlige område. Uden for det strafferetlige område må myndigheder anvende et af de øvrige hjemmelsgrundlag i § 7 for at kunne behandle følsomme personoplysninger. Efter § 7, stk. 2, nr. 4, er der hjemmel til at behandle følsomme oplysninger, når det er nødvendigt for at kunne afgøre, om den registrerede har et retskrav. Denne bestemmelse vil ofte hjemle offentlige myndigheders behandling af borgernes følsomme oplysninger.

For alle de nævnte bestemmelser gælder, at behandlingen kun må finde sted, når den er "nødvendig" for myndighedens virke. Dette indebærer bl.a., at en indsamling af oplysninger ikke kan finde sted

[2] Med "indsamling" menes alle de aktiviteter, hvorved en myndighed skaffer sig adgang til oplysninger. Der sondres som udgangspunkt ikke mellem de situationer, hvor myndigheden selv kan skaffe oplysninger, og de situationer, hvor myndigheden kun kan skaffe oplysningerne ved henvendelse til tredjemand. I lovene om efterretningstjenesterne anvendes begrebet "indsamling" om den situation, hvor oplysningerne er umiddelbart tilgængelige for myndigheden, og begrebet "indhentning" om den situation, hvor oplysningerne skal skaffes fra en tredjemand.

[3] Et eksempel herpå er skattekontrollovens § 8D (som dog kort omtales i afsnit 2.5.2 i forbindelse med vurderingen af lovgivningens konsistens).

[4] Lov nr. 429 af 31/05/2000 om behandling af personoplysninger.

uden en konkret anledning, og at denne anledning – i overensstemmelse med den generelle offentlige retlige regulering – bl.a. skal være saglig og ligge inden for myndighedens kompetenceområde (specialitetsprincippet). Kravet om nødvendighed indebærer endvidere en vis form for kvalificering af, hvorfor indsamlingen skal finde sted i den enkelte sag. I praksis vil det dog ikke altid være muligt på forhånd at vide, om en indsamling af oplysninger vil være nødvendig i det enkelte tilfælde, hvorfor myndigheder må være overladt et vist råderum til – på baggrund af f.eks. tidligere indhentede erfaringer fra lignende sager – at træffe beslutning om at søge oplysninger om en eller flere borgere på internettet.

Det er endvidere en forudsætning for indsamlingens lovlighed, at den overholder de generelle krav til behandling af oplysninger i lovens § 5. Det betyder bl.a., at behandlingen kun må ske til udtrykkeligt angivne og saglige formål, at oplysninger skal være relevante og ikke omfatte mere, end hvad der kræves til opfyldelse af formålet, og at behandlingen i øvrigt skal være i overensstemmelse med god databehandlingsskik.

Det vil bero på en konkret vurdering, om kravene er opfyldt. Er det tilfældet, vil myndigheder kunne indsamle oplysninger om borgernes internetadfærd. Kravene om nødvendighed og proportionalitet indebærer dog, at en myndighed ikke vil kunne foretage masseindsamlinger efter persondataloven.

2.1.2. Retshåndhævende myndigheder – retshåndhævelsesloven

Med virkning fra 30. april 2017 er retshåndhævende myndigheders behandling af personoplysninger omfattet af retshåndhævelsesloven[5], når behandlingen finder sted med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Retshåndhævelsesloven erstatter således persondataloven – og fra 25. maj 2018 den generelle databeskyttelsesforordning – i forhold til politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger på hele det strafferetlige område. Enhver indsamling og behandling af personoplysninger, der foretages som led i efterforskningen mv. af strafbare forhold eller som led i politiets ordenshåndhævelse, vil således falde under retshåndhævelsesloven.

Retshåndhævelsesloven indeholder en række af de samme principper som persondataloven og databeskyttelsesforordningen, dog med en række tilpasninger i lyset af de særlige forhold, der gør sig gældende på retshåndhævelsesområdet. For så vidt angår de grundlæggende behandlingsregler, fremgår det af lovens § 9, at behandling kun må finde sted, når behandlingen er nødvendig for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed. Dette indebærer i praksis, at eksempelvis politiet vil have adgang til at behandle personoplysninger, når dette er nødvendigt for at varetage de opgaver, der ved lov er henlagt til politiet i medfør af f.eks. retsplejelovens kapitel 67-75 b om efterforskning mv., jf. nedenfor.

[5] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

2.1.3. Politiloven

Politilovens[6] § 2 a, stk. 2, hjemler adgang for politiet til at indsamle og behandle oplysninger fra offentligt tilgængelige kilder, når det er nødvendigt af hensyn til udførelsen af politiets opgaver, jf. § 2. I medfør af bestemmelsen har politiet adgang til at indsamle oplysninger, både personoplysninger og andre oplysninger, fra enhver offentligt tilgængelig kilde. Begrebet "offentligt tilgængelige kilder" skal ifølge lovforarbejderne forstås bredt og omfatter således enhver informationskilde af både elektronisk og ikke-elektronisk karakter, herunder internettet, som inden for rammerne af gældende ret og uden gennemførelsen af et straffeprocessuelt tvangsindgreb kan tilgås i det offentlige rum. Oplysninger og kilder, der er tilgængelige på almindelige kommercielle vilkår, f.eks. gennem betaling af abonnement eller andre former for betalingstjenester, anses tillige som offentligt tilgængelige efter bestemmelsen.

Politiets indsamling af oplysninger fra offentligt tilgængelige kilder skal ske inden for rammerne af retshåndhævelsesloven og retsplejeloven.

Den nærmere vurdering af, hvornår indsamling og behandling af oplysninger fra offentligt tilgængelige kilder er nødvendig for udførelsen af politiets opgaver, skal foretages med udgangspunkt i den lovgivning mv., der regulerer politiets virksomhed. Der vil således skulle foretages en konkret politifaglig vurdering af, om det er nødvendigt for udførelsen af politiets opgaver, når der indsamles og behandles oplysninger fra offentligt tilgængelige kilder.

Politiets brug af oplysninger fra offentligt tilgængelige kilder vil blive reguleret nærmere på bekendtgørelsesniveau, jf. politilovens § 2 a, stk. 3.

2.1.4. Strafferetlig efterforskning – straffeprocessuelle regler

En række bestemmelser i retsplejeloven[7] giver hjemmel til, at politiet kan indsamle oplysninger om (bl.a.) borgernes internetadfærd som led i en strafferetlig efterforskning.

Efter retsplejelovens § 780 har politiet i visse situationer ret til at foretage *indgreb i meddelelseshemmeligheden*. Dette indebærer bl.a. en ret til at tilbageholde, åbne og gøre sig bekendt med indholdet af breve og andre forsendelser. "Andre forsendelser" omfatter bl.a. e-mails, og bestemmelsen kan således give politiet hjemmel til at indsamle e-mails, der er under forsendelse. Bestemmelsen kan ligeledes anvendes til at kræve udlevering af de oplysninger om borgernes internetadfærd, som teleselskaberne logger efter § 786, stk. 4 og den tilhørende logningsbekendtgørelse, jf. herom afsnit 2.4 nedenfor. Indgreb i meddelelseshemmeligheden forudsætter overholdelse af en række krav, herunder til lovovertrædelsens grovhed, indgrebets betydning for efterforskningen og proportionaliteten af indgrebet[8].

[6] Lovbkg. nr. 956 af 20. august 2015 om politiets virksomhed med senere ændringer.
[7] Lovbkg. nr. 1257 af 13. oktober 2016 om rettens pleje med senere ændringer.
[8] Se nærmere retsplejeloven §§ 781 og 782.

Efter retsplejelovens § 791 b kan politiet under nærmere betingelser aflæse ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (*dataaflæsning*). Politiet kan eksempelvis installere et "snifferprogram", der registrerer og videregiver alle de indtastninger, som brugeren af en computer foretager. Kravene til indgrebet svarer i det væsentlige til de krav, der gælder for indgreb i meddelelseshemmeligheden[9].

Efter retsplejelovens § 793 kan politiet foretage *ransagning* af bl.a. boliger og andre husrum, dokumenter, papirer og lignende som led i en strafferetlig efterforskning. Bestemmelsen omfatter også oplysninger, der er lagret på digitale medier, og har bl.a. givet hjemmel til, at politiet kunne logge ind på en brugers Facebook-profil og få adgang til oplysninger derfra efter at have skaffet sig brugerens adgangskode via telefonaflytning[10].

Efter retsplejelovens § 801 kan politiet foretage *beslaglæggelse*, bl.a. til sikring af bevismidler. Bestemmelsen er bl.a. blevet anvendt til at pålægge en e-mailudbyder at udlevere e-mails til politiet. Beslaglæggelse forudsætter en proportionalitetsvurdering og som udgangspunkt forudgående retskendelse[11].

Efter retsplejelovens § 804 kan politiet anmode om at *få udleveret genstande (edition)*, der kan tjene som bevis i sagen fra en person, der ikke er mistænk i sagen. "Genstande" omfatter også information, og bestemmelsen er bl.a. blevet anvendt til at pålægge Den Blå Avis at udlevere en IP-adresse anvendt af en person, der havde oprettet en annonce i en andens navn[12]. Bestemmelsen vil ligeledes kunne anvendes til at kræve udlevering af oplysninger fra sociale medier, f.eks. oplysninger på en brugers Facebook-profil. Edition forudsætter på samme måde som beslaglæggelse en proportionalitetsvurdering og som udgangspunkt forudgående retskendelse[13].

2.1.5. Politiets Efterretningstjeneste (PET)

Persondataloven og retshåndhævelsesloven gælder ikke for PET´s behandling af personoplysninger, jf. persondatalovens § 2, stk. 11 og retshåndhævelsesloven § 1, stk. 2. Rammerne for PET´s behandling af personoplysninger er i stedet fastlagt i PET-loven[14].

Efter PET-loven § 3 kan PET indsamle og indhente oplysninger, der kan have betydning for PET´s virksomhed. Det eneste krav efter bestemmelser er således, om indsamlingen/indhentelsen "kan have betydning" for PET´s virksomhed. Kravet giver PET betydeligt videre rammer for indsamling af oplysninger, end myndigheder generelt har efter det nødvendighedskrav, der følger af persondataloven og retshåndhævelsesloven som beskrevet ovenfor. Oplysningen kan således indsamles, hvis det ikke på forhånd kan udelukkes, at oplysningen har relevans for PET´s arbejde.

[9] Se nærmere retsplejeloven § 794.
[10] Se U.2012.2614H.
[11] Se nærmere retsplejeloven § §§ 805 og 806.
[12] Se U.2008.843V.
[13] Se nærmere retsplejeloven § §§ 805 og 806.
[14] Lovbkg. nr. 231 af 7. marts 2017 om Politiets Efterretningstjeneste (PET).

Bestemmelsen gælder alle former for oplysninger, og dermed også oplysninger om borgernes internetadfærd.

Bestemmelsen giver ikke kun hjemmel til at indsamle oplysninger om den mistænkte, men også personer i dennes omgangskreds. Det følger endvidere af lovens forarbejder, at PET kan indhente oplysninger om potentielle ofre for terrorisme, spionage mv. samt kilder, personer og organisationer, hvis virksomhed indgår som baggrundsviden til forståelse af de almindelige samfundsforhold. PET vil således kunne indsamle oplysninger om en bredere personkreds, end myndigheder generelt vil kunne efter persondataloven.

Det forekommer ikke entydigt, om bestemmelsen giver PET mulighed for at foretage masseindhentning af oplysninger om borgernes internetadfærd. På den ene side synes FE at have en sådan mulighed med hjemmel i en bestemmelse i FE-loven, der opererer med samme kriterium om "kan have betydning" som bestemmelsen i PET-loven, jf. om FE-bestemmelsen nedenfor. På den anden side synes forarbejderne at forudsætte, at PET´s indsamling og indhentning af oplysninger relaterer sig til bestemte typer af personkredse. Begrebet "rådata", der i FE-loven anvendes om masseindhentning af oplysninger, anvendes heller ingen steder i PET-loven eller dens forarbejder. På den baggrund giver bestemmelsen næppe hjemmel til at, at PET kan foretage masseindhentning af oplysninger om borgernes internetadfærd.

Efter § 5 gælder skærpede krav, såfremt indsamlingen af oplysninger sker som led i en undersøgelse rettet mod en konkret person. En sådan undersøgelse må kun foretages 1) i forbindelse med forebyggelse og efterforskning af overtrædelser af straffelovens kap. 12 og 13 om forbrydelser med statens selvstændighed og sikkerhed, statsforfatningen og de øverste statsmyndigheder, terrorisme mv. eller 2) såfremt undersøgelsen er nødvendig til varetagelsen af tjenestens øvrige opgaver.

PET´s indsamling af oplysninger skal overholde de straffeprocesuelle regler om indgreb i meddelelseshemmeligheden mv. efter retsplejelovens regler om tvangsindgreb, jf. nærmere herom afsnit 2.1.4 ovenfor.

2.1.6. Forsvarets Efterretningstjeneste (FE)

Persondataloven og retshåndhævelsesloven gælder ikke for FE´s behandling af personoplysninger, jf. lovens § 2, stk. 11. Rammerne for FE´s behandling af personoplysninger er i stedet fastlagt i FE-loven[15].

Efter FE-loven § 3 kan FE indsamle og indhente oplysninger, der 1) kan have betydning for FE´s efterretningsmæssige virksomhed eller 2) er nødvendige for FE´s øvrige virksomhed. FE´s muligheder for at indsamle og indhente oplysninger af betydning for den efterretningsmæssige virksomhed svarer til reguleringen af PET´s adgang til at indhente oplysninger efter PET-loven som beskrevet ovenfor og er dermed ikke undergivet kravet om nødvendighed.

[15] Lovbkg nr. 1 af 4. januar 2016 om Forsvarets Efterretningstjeneste (FE) med senere ændringer.

Det følger ikke klart af loven, i hvilket omfang FE kan foretage masseindsamling af oplysninger fra internettet, og hvilke krav der i givet fald gælder for denne indsamling. Oplysninger, der masseindsamles fra internettet uden endnu at være behandlet, betegnes "rådata", men loven indeholder ingen eksplicit regulering af adgang til indhentelse af rådata[16]. Det følger forudsætningsvist af lovens forarbejder, at FE kan indsamle rådata, herunder også på dansk territorium. Loven synes således at give hjemmel til, at FE kan masseindsamle oplysninger fra bl.a. den danske del af internettet. Det følger videre af lovens forarbejder, at indhentning af rådata "principielt" udgør en behandling af personoplysninger, men at lovens regler om intern behandling og videregivelse af oplysninger først finder anvendelse, når rådata er bearbejdet og indholdet erkendt. Dette indebærer bl.a., at begrænsningerne i adgangen til at videregive oplysninger efter lovens § 7 ikke gælder for rådata.

FE´s virksomhed er rettet mod forhold i udlandet, men tjenesten kan som led i sin efterretningsvirksomhed medtage oplysninger om personer, der er hjemmehørende i Danmark[17], jf. § 3, stk. 2. FE må ikke af egen drift iværksætte elektronisk indhentning af oplysninger om personer hjemmehørende i Danmark men kan medtage sådanne oplysninger, når de har karakter af såkaldte "tilfældighedsfund". FE kan dog foretage målrettet elektronisk indhentning af oplysninger om fysiske personer hjemmehørende i Danmark, når personen opholder sig i udlandet, og der er bestemte grunde til at formode, at den pågældende deltager i aktiviteter, der kan indebære eller forøge en terrortrussel mod Danmark, jf. § 3, stk. 3. Dette kræver, at der indhentes en forudgående retskendelse, jf. § 3 a.

Retsplejelovens regler om indgreb i meddelelseshemmeligheden mv. gælder ikke for FE´s virke.

2.1.7. Center for Cybersikkerhed (CFCS)

Persondataloven og rethåndhævelsesloven gælder ikke for CFCS´s behandling af personoplysninger, da CFCS er en del af FE, jf. CFCS-loven[18] § 1, stk. 2 og § 8, stk. 1 og persondataloven § 2, stk. 11.

Hvornår CFSC kan indsamle og i øvrigt behandle personoplysninger er reguleret i CFCS-lovens §§ 9-11. Disse bestemmelser svarer i det væsentlige til bestemmelserne i persondataloven §§ 6-8. I tilknytning hertil rummer CFCS-loven imidlertid en særlig regulering af CFCS´s adgang til at indsamle data gennem sin netsikkerhedstjeneste.

Efter lovens §§ 4 og 5 kan CFCS behandle pakke- og trafikdata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område og for øvrige myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten. Det samme gælder for øvrige myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten, når der er en begrundet mistanke om en sikkerhedshændelse, myndigheden/virksomheden anmoder om midlertidig tilslutning, der højest kan vare i to måneder, og

[16] Den eneste bestemmelse i loven, der omtaler "rådata", er § 6, stk. 2, der angiver, at rådata skal slettes 15 år efter indhentelsestidspunktet.
[17] Dette omfatter 1) danske statsborgere, 2) nordiske statsborgere og andre med ret til ophold i Danmark tilmeldt folkeregistret, 3) asylansøgere med kendt ophold i Danmark i mere end 6 måneder og 4) juridiske personer med overvejende tilknytning til Danmark.
[18] Lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed (CFCS-loven).

behandlingen af oplysningen er væsentlig for CFCS´s sikring af samfundsvigtig IT-infrastruktur, jf. lovens § 6. Ved "pakkedata" forstås indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester[19]. Dette gælder eksempelvis indholdet af e-mails og tilgåede hjemmesider. Ved "trafikdata" forstås data, som behandles med henblik på at transmittere pakkedata[20]. Dette omfatter eksempelvis IP-adresser, e-mailadresser, hjemmesideadresser og information om kommunikationens varighed og tidspunkt.

CFCS´s netsikkerhedstjeneste kan endvidere behandle enhver form for data (dvs. ikke kun pakkedata og trafikdata), når der er en begrundet mistanke om en sikkerhedshændelse, myndigheden/virksomheden anmoder om netsikkerhedstjenestens bistand og stiller data til rådighed, og oplysningen er væsentlig for CFCS´s sikring af samfundsvigtig IT-infrastruktur[21].

CFCS's adgang til at videregive oplysninger til andre myndigheder er beskrevet i afsnit 2.2.4 nedenfor. Da CFCS organisatorisk og i forvaltningsmæssig forstand er en del af FE, følger det af forarbejderne til CFCS-loven, at CFCS's eventuelle videregivelse af oplysninger til øvrige dele af FE i overensstemmelse med almindelige forvaltningsretlige principper ikke er omfattet af lovens regulering af videregivelse til andre myndigheder. Forsvarsministeriet har imidlertid udstedt "Retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste" af 30. juni 2014, der begrænser CFCS' adgang til at videregive oplysninger til andre dele af FE. Efter retningslinjernes § 2 forudsætter udveksling af data med den øvrige del af FE, at 1) udvekslingen er nødvendig for at understøtte et højt informationssikkerhedsniveau, 2) at udvekslingen sker med udtrykkeligt angivne og saglige formål og 3) at der er begrundet mistanke om en sikkerhedshændelse. Det sidstnævnte kriterie svarer til det kriterie, der gælder for, at CFCS må videregive data til politiet efter CFCS-lovens § 16, stk. 1, nr. 1. De to førstnævnte kriterier følger ikke af § 16.

2.2. Myndigheders videregivelse af oplysninger til andre myndigheder

2.2.1. Myndigheder generelt

Persondataloven – og i relevant omfang retshåndhævelsesloven – regulerer alle former for behandling af personoplysninger, herunder også adgangen til at videregive oplysninger. De regler, der ovenfor er beskrevet om myndigheders adgang til at indsamle oplysninger, gælder derfor også for myndigheders videregivelse af oplysninger.

Persondataloven og retshåndhævelsesloven regulerer kun, hvornår myndigheder (og andre) har en *ret* til at behandle personoplysninger, men ikke hvornår der består en *pligt* til at behandle. Lovene giver derfor heller ikke hjemmel til at pålægge hverken myndigheder eller private at udlevere personoplysninger, som de er i besiddelse af.

[19] CFCS-loven § 2, nr. 2.
[20] CFCS-loven § 2, nr. 3.
[21] CFCS-loven § 7.

En sådan pligt følger imidlertid af forvaltningslovens[22] § 31. Bestemmelsen angiver, at en myndighed, der er berettiget til at udlevere oplysninger, også er forpligtet til det, når en anden myndighed begærer oplysningerne udleveret, og de er af betydning for myndighedens virke. I denne situation vil en myndighed være forpligtet til at udlevere oplysninger om borgernes internetadfærd, som myndigheden er i besiddelse af.

For udlevering af oplysninger til PET suppleres forvaltningsloven § 31 af PET-loven § 4, hvorefter andre forvaltningsmyndigheder skal videregive oplysninger til PET på dennes anmodning, når PET vurderer, at oplysningerne må antages at have betydning for PET´s varetagelse af opgaver vedrørende overtrædelser af straffelovens kap. 12 og 13 om forbrydelser mod statens selvstændighed og sikkerhed, statsforfatningen og de øverste statsmyndigheder, terrorisme mv. I denne situation skal den afgivende forvaltningsmyndighed ikke foretage sin egen vurdering af, om PET er berettiget til at modtage oplysningerne, men skal lægge PET´s vurdering til grund.

2.2.2. Politiets Efterretningstjeneste

PET´s adgang til at videregive oplysninger er reguleret i PET-loven § 10.

Efter § 10, stk. 1, kan PET videregive oplysninger til FE, hvis videregivelsen kan have betydning for varetagelsen af tjenesternes opgaver. Kravet om, at videregivelsen "kan have betydning", svarer til kravet i PET-loven § 3 om PET´s indsamling af oplysninger, som beskrevet ovenfor.

Efter § 10, stk. 2, kan PET videregive oplysninger til andre danske og udenlandske myndigheder i overensstemmelse med § 7. Dette indebærer bl.a., at videregivelsen skal overholde de grundlæggende behandlingsprincipper i persondataloven § 5, og at videregivelsen kun kan ske, hvis den 1) sker med samtykke fra borgeren, 2) må antages at have betydning for PET´s varetagelse af opgaver vedrørende overtrædelser af straffelovens kap. 12 og 13 om forbrydelser med statens selvstændighed og sikkerhed, statsforfatningen og de øverste statsmyndigheder, terrorisme mv. eller 3) er nødvendig for varetagelsen af tjenestens øvrige opgaver. Er der tale om følsomme eller semi-følsomme oplysninger, forudsætter videregivelse, at betingelserne i persondataloven § 8, stk. 2, er opfyldt. Det vil de bl.a. være, hvis videregivelsen er nødvendig for en myndigheds udøvelse af sin virksomhed. Det er endvidere et krav, at videregivelsen efter en konkret vurdering må anses for forsvarlig, jf. § 10, stk. 4.

PET-loven indeholder ikke regler, der forpligter PET til at videregive oplysninger til andre myndigheder. En sådan pligt følger af den ovenfor omtalte almindelige regel i forvaltningslovens § 31, som PET er omfattet af.

2.2.3. Forsvarets Efterretningstjeneste

FE´s adgang til at videregive oplysninger er reguleret i FE-loven § 7, der i sit indhold svarer til PET-lovens § 6, således, at FE er berettiget til at videregive personoplysninger til PET, der kan være af "betydning for varetagelsen af tjenesternes opgaver". FE og PET's adgang til at videregive oplysninger

[22] Lovbkg. nr. 433 af 22. april 2014.

til hinanden og til øvrige myndigheder er således den samme. Som beskrevet i afsnit 2.1.6 gælder begrænsningerne for FE's videregivelse efter § 7 ikke for de såkaldte rådata.

2.2.4. Center for Cybersikkerhed

CFCS´s adgang til at videregive oplysninger følger af CFCS-loven §§ 10-12, der som nævnt i det væsentlige svarer til persondataloven §§ 6-8. I tillæg hertil rummer loven imidlertid en særlig regulering af adgang til at videregive data, navnlig pakkedata og trafikdata, der er indhentet som led i CFCS´s netsikkerhedstjeneste efter §§ 4-7 (omtalt i afsnit 2.1.7 ovenfor).

Loven indeholder ingen begrænsninger i adgangen til at videregive pakkedata og trafikdata, der hidrører fra myndigheder på Forsvarsministeriets område. Videregivelsen skal dog overholde de generelle betingelser for behandling af personoplysninger i § 9. Det følger bl.a. heraf, at behandlingen skal ske til udtrykkeligt angivne og saglige formål, og at oplysningerne skal være relevante og ikke omfatte mere, end hvad der kræves til opfyldelsen af formålet med behandlingen.

Pakkedata kan herudover kun videregives til politiet ved begrundet mistanke om en sikkerhedshændelse, hvor det kan være relevant at indlede strafferetlig efterforskning, jf. CFCS-loven § 16, nr. 1. Der kan i denne situation ligeledes videregives trafikdata til politiet.

Trafikdata (men ikke pakkedata) kan endvidere videregives til myndigheder og virksomheder, når der foreligger en begrundet mistanke om en sikkerhedshændelse, og videregivelsen er nødvendig for netsikkerhedstjenestens opgaver, jf. CFCS-loven § 16, nr. 2.

CFCS kan ikke videregive pakkedata og trafikdata i andre situationer, end de ovenfor anførte. Som beskrevet i afsnit 2.1.7 ovenfor regulerer loven ikke CFCS' videregivelse til andre dele af FE. Denne videregivelse er dog undergivet tilsvarende begrænsninger i henhold til Forsvarsministeriets "Retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste" af 30. juni 2014.

2.3. Privates udlevering af oplysninger til myndigheder

Privates adgang til at videregive personoplysninger til myndigheder følger af persondataloven. Videregivelsen har karakter af en behandling i lovens forstand på samme måde, som det gælder for myndigheders videregivelse. Heraf følger, at videregivelsen skal have hjemmel i §§ 6-8 for hhv. almindelige, følsomme og semi-følsomme oplysninger. For alle typer af oplysninger kan videregivelsen ske, hvis den registrerede har givet sit samtykke. Det kan således følge af en privat virksomheds brugsvilkår, at brugerne accepterer udlevering af deres oplysninger. Overholder et sådant samtykke kravene til et gyldigt samtykke i persondataloven, vil virksomheden kunne videregive oplysninger til myndigheder. Uden et samtykke må hjemlen findes i en af de øvrige bestemmelser i §§ 6-8.

Hverken persondataloven, retshåndhævelsesloven eller lovene om efterretningstjenesterne rummer hjemmel til at pålægge private at udlevere oplysninger til myndigheder[23].

[23] Efter § 13 i teleloven (lovbkg. nr. 128 af 7. februar 2014 om elektroniske kommunikationsnet og –tjenester med senere ændringer) skal teleselskaber og andre udbydere af elektroniske kommunikationsnet eller –tjenester til slutbrugere på

En sådan forpligtelse må pålægges med hjemmel i retsplejelovens regler om indgreb i meddelelseshemmeligheden, beslaglæggelse og editionspligt eller særlovsregler. De straffeprocessuelle regler, der er beskrevet ovenfor i afsnit 2.1.4, kan således både give politiet hjemmel til selv at indsamle oplysninger og til at kræve udlevering fra andre.

Både retsplejelovens § 780 om indgreb i meddelelseshemmeligheden og § 801 om beslaglæggelse er blevet anvendt til at pålægge internetudbydere at udlevere e-mails til politiet. Reglerne om editionspligt i retsplejelovens § 804 er bl.a. blevet anvendt til at kræve udlevering af IP-adresser fra Den Blå Avis, udlevering af oplysninger fra en brugers Facebook-profil og udlevering af en IP-adresse og e-mailadresse ved oprettelse af en Facebook-profil[24]. Bestemmelsen om ransagning i § 793 vil efter omstændighederne også kunne anvendes til at kræve udlevering af denne type oplysninger.

2.4. Regler der pålægger private parter at registrere oplysninger - logningsbekendtgørelsen

Mange virksomheder, herunder internettjenester, lagrer frivilligt store mængder data om deres brugere, da disse data er en forudsætning for selve tjenesten (f.eks. sociale netværkstjenester) eller for den bagvedliggende forretningsmodel (brug eller videresalg af oplysninger med henblik på markedsføring mv.). Virksomheder vil imidlertid ikke have nogen pligt til at lagre oplysninger om deres brugere, medmindre dette følger af lovgivningen.

De væsentligste regler, der pålægger en pligt til at lagre visse oplysninger om borgernes internetadfærd, udgøres af reglerne i logningsbekendtgørelsen[25]. Bekendtgørelsen er udstedt med hjemmel i retsplejelovens § 786, stk. 4, hvorefter udbydere af telenet eller teletjenester skal foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Bekendtgørelsen pålægger en pligt til at lagre en række oplysninger om en brugers adgang til internettet, herunder tildelt brugeridentitet og IP-adresse samt tidspunkt for kommunikationens start og afslutning. Et krav om logning af såkaldte sessionsdata, der indeholder småstykker af selve informationsindholdet, blev afskaffet med en ændring af bekendtgørelsen i juni 2014[26]. Ved en dom af 8. april 2014[27] fastslog EU-Domstolen, at EU´s logningsdirektiv[28] var i strid med EU´s charter om grundlæggende rettigheder. Denne dom blev fulgt op af en ny dom fra EU-Domstolen den 21. december 2016[29], hvor EU-Domstolen igen udtalte sig om de kriterier, som nationale logningsregler skal iagttage. Dommen bekræfter kriterierne opstillet i den første dom men fastslår herudover, at national lovgivning ikke kan pålægge teleselskaber en generel pligt til at logge alle teledata om alle brugere uden nogen form for mistanke eller afgrænsning i øvrigt. På denne baggrund vil det være

begæring af politiet udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester. Dette omfatter ifølge lovforarbejderne e-mailadresser og statiske ip-adresser. Derimod giver bestemmelsen ikke politiet hjemmel til at kræve udlevering af dynamiske IP-adresser, da disse ifølge forarbejderne er omfattet af logningsbekendtgørelsen og derfor kun kan udleveres efter retsplejelovens regler om edition.

[24] U.2016.3605Ø.

[25] Bekendtgørelse nr. 988 af 28. september 2006.

[26] Bekendtgørelse nr. 660 af 19. juni 2014.

[27] Forenede sager C-293/12 og 594/12.

[28] Direktiv 2006/24.

[29] Forenede sager C-203/15 og 698/15.

nødvendigt at justere de eksisterende danske logningsregler. Dette arbejde pågår i øjeblikket i Justitsministeriet.

2.5. Nogle betragtninger om lovgivningen

Som anført indledningsvist er det ikke formålet med denne rapport at tage stilling til den balance mellem privatlivsbeskyttelse på den ene side og kriminalitetsbekæmpelse, myndighedsudøvelse mv. på den anden side, som lovgivningen er udtryk for. Derimod skal i det følgende knyttes nogle bemærkninger til selve kvaliteten af den lovgivning, der regulerer myndighedernes registrering af borgernes internetadfærd. Disse bemærkninger tager udgangspunkt i de tre overordnede krav, at lovgivningen bør være overskuelig, konsistent og transparent.

2.5.1. Overskuelighed

Med "overskuelighed" menes, at det er muligt at overskue det samlede regelsæt, der regulerer myndighedernes adgang til at registrere borgernes internetadfærd.

Som det er fremgået af den ovenstående regeloversigt, er der en lang række regler, der tilsammen tegner billedet af myndighedernes mulighed for registrering af borgernes internetadfærd. Den samlede regulering kan på den baggrund ikke betegnes som overskuelig men nærmere som det modsatte.

Dette er dog nok en uundgåelig følge af, at myndigheders registrering af borgernes internetadfærd dækker over en lang række forskellige situationer og handlinger, hvoraf nogle kræver særskilt regulering, mens andre kan omfattes af mere generelle regler. I tilknytning hertil dækker reguleringen mange forskellige typer af myndigheder.

Det er derfor næppe hellere hverken muligt eller hensigtsmæssigt at foretage en samlet regulering af myndigheders registrering af borgernes internetadfærd.

De begrænsninger i overskueligheden af lovreguleringen, som dette fører med sig, må i stedet imødegås ved andre initiativer. Denne rapport er tænkt som et bidrag hertil.

2.5.2. Konsistens

Med "konsistens" menes, at balancen mellem privatlivsbeskyttelse og kriminalitetsbekæmpelse mv. er nogenlunde ens på tværs af regelsættene. Det vil være uhensigtsmæssigt, hvis én myndighed har en langt mere vidtgående adgang til registrering af oplysninger efter ét regelsæt, end en anden myndighed har efter et andet regelsæt, hvis ikke særlige grunde tilsiger denne forskel (hvad der eksempelvis er tilfældet for efterretningstjenesterne).

Dette krav synes grundlæggende at være opfyldt. De relevante regelsæt synes generelt at have et blik for reguleringen af de tilsvarende temaer inden for andre dele af lovgivningen.

Størst risiko for manglende konsistens vil der formentlig være inden for særlovgivningen. Der er ikke fundet konkrete tilfælde af inkonsistens i særlovgivningen (som dog heller ikke er analyseret nærmere), og inkonsistens synes således ikke at være et problem i praksis.

At problemstillingen kan forekomme illustreres af bestemmelsen i skattekontrolloven § 8D. SKAT brugte i en årrække bestemmelsen som hjemmel for at kræve udlevering af bl.a. oplysninger om borgernes internetadfærd fra bl.a. teleselskaber. Bestemmelsen kræver ikke en forudgående dommerkendelse og forudsætter endvidere blot, at adgangen til oplysningerne efter myndighedernes skøn er af væsentlig betydning for skatteligningen. Hermed havde SKAT en langt videre adgang til udlevering af oplysninger, end politiet har efter reglerne i retsplejeloven, som beskrevet ovenfor. Det virker besynderligt, at de retssikkerhedsgarantier, lovgiver mener er nødvendige, for at politiet kan kræve udlevering af oplysninger ved efterforskning af straffesager, ikke skulle være nødvendige at iagttage ved SKAT's efterforskning af eventuel skatteunddragelse. Som led i den såkaldte "Retssikkerhedspakke I" besluttede skatteminister Karsten Lauritzen da også i september 2015, at SKAT's adgang til at indhente oplysninger om borgernes brug af mobiltelefoner efter § 8D ikke ville blive taget i brug igen som led i det almindelige kontrolarbejde. Med den såkaldte "retssikkerhedspakke III" lægges der op til en revision af skattekontrolloven, der bl.a. afskærer SKAT's adgang til teleoplysninger. Bestemmelsen i § 8D og SKAT's tidligere anvendelse af den illustrerer imidlertid fortsat vigtigheden af at sikre en konsistens mellem reglerne, herunder også inden for særlovgivningen.

2.5.3. Transparens

Med "transparens" menes, at de enkelte regelsæt gør det tydeligt, hvornår, hvordan og under hvilke betingelser offentlige myndigheder må registrere oplysninger om borgernes internetadfærd. Mens kravet om "overskuelighed" skal sikre mulighed for at skaffe sig et overblik over den samlede regulering af området, skal kravet om "transparens" sikre muligheden for at forstå indholdet og konsekvenserne af de enkelte regelsæt.

Det er et ideal, at den enkelte borger kan forstå sine rettigheder og pligter ved at blot at læse loven. I praksis er lovgivningen så kompleks, at dette sjældent kan lade sig gøre. Det gælder også de ovenfor beskrevne regelsæt, der regulerer adgangen til oplysninger om borgernes internetadfærd.

Selvom de relevante regelsæt således kan forekomme svært tilgængelige, er der ikke grundlag for generelt at kritisere reglerne for manglende transparens.

På ét område er der dog grund til at rejse kritik af en manglende transparens. Som beskrevet ovenfor giver FE-loven FE adgang til at indsamle og videregive "rådata" uden at iagttage lovens krav til indsamling og videregivelse af personoplysninger. Hermed får FE i realiteten en meget vid adgang til at indsamle og videregive oplysninger om borgernes internetadfærd. Dette følger imidlertid ikke ret klart af loven, og først ved en nærmere læsning af lovens forarbejder fremgår det, at FE har denne adgang (uagtet at det heller ikke er udtrykkeligt angivet i forarbejderne). Uanset at efterretningstjenesterne har et behov for at holde deres metoder hemmelige, bør en så vidtgående beføjelse fremgå klart af loven. Formuleringerne i forarbejderne gør det endvidere uklart, hvorvidt Tilsynet med Efter-

retningstjenesternes kompetence omfatter tilsyn med indsamling og videregivelse af rådata. Det forekommer heller ikke klart, hvorvidt PET kan have en tilsvarende adgang til at indsamle rådata, jf. ovenfor.

3. KONTROLMEKANISMER

Myndigheders registrering og eventuelle videregivelse af oplysninger om borgernes internetadfærd er indgribende foranstaltninger, ikke mindst set i lyset af hvor intensivt mange bruger internettet, omfanget af oplysninger, der kan indsamles, og de profiler, der kan skabes ved at sammenstille sådanne oplysninger. Det er derfor afgørende, at der føres en grundig kontrol med myndighedernes indsamling, brug og videregivelse af disse oplysninger. I det følgende beskrives en række mekanismer i lovgivningen, der skal sikre denne kontrol.

3.1. Domstolskontrol

Det er et grundlæggende princip, at borgere kan få prøvet myndigheders afgørelser ved domstolene. Dette gælder også afgørelser truffet om registrering af borgerens adfærd og behandling af personoplysninger i øvrigt, og uanset om behandlingen foretages af efterretningstjenesterne, politiet eller andre myndigheder. Det er dog et krav, at borgeren har en retlig interesse i sagen.

Den almindelige domstolsprøvelse forudsætter, at borgeren selv indbringer sagen for domstolene og får dermed normalt karakter af en efterfølgende prøvelse. I nogle situationer forudsætter myndigheders handlinger, herunder indsamling af oplysninger, en forudgående domstolsprøvelse. Dette gælder ved de ovenfor beskrevne tvangsindgreb efter retsplejeloven (indgreb i meddelelseshemmeligheden[30], aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem[31], ransagning[32] og beslaglæggelse[33]) og efter FE-lovens § 3 a (indgreb i meddelelseshemmeligheden i forhold til personer hjemhørende i Danmark, der opholder sig i udlandet).

3.2. Uafhængig tilsynskontrol

3.2.1. Folketingets Ombudsmand

Folketingets Ombudsmand er valgt af Folketinget men fungerer i øvrigt uafhængigt af dette, jf. ombudsmandslovens[34] § 10.

Ombudsmanden kan behandle klager over alle dele af den offentlige forvaltning, herunder også efterretningstjenesterne. Ombudsmanden kan endvidere tage sager op af egen drift.

Ombudsmanden kan fremsætte kritik og afgive henstillinger, men har ikke i øvrigt sanktionsbeføjelser. Såfremt ombudsmanden finder, at der er begået fejl at større betydning, skal ombudsmanden informere Folketingets Retsudvalg og den relevante minister.

[30] Retsplejeloven § 783.
[31] Retsplejeloven § 791 b, stk. 3.
[32] Retsplejeloven § 796.
[33] Retsplejeloven § 806.
[34] Lovbkg. nr 349 af 22/03/2013 om Folketingets Ombudsmand.

Ombudsmanden har tavshedspligt med hensyn til de forhold, som ombudsmanden bliver bekendt med under udøvelsen af sin virksomhed, såfremt hemmeligholdelse ifølge sagens natur er påkrævet.

3.2.2. Datatilsynet

Datatilsynet fører tilsyn med overholdelsen af persondataloven og retshåndhævelsesloven og fungerer som et uafhængigt tilsyn, jf. nærmere persondataloven §§ 55 ff. og retshåndhævelseslovens §§ 37 ff.

Datatilsynet kan behandle klager fra enkeltpersoner og tage sager op af egen drift mv.

Datatilsynet kan pålægge en privat part at ophøre med en behandling, der er ulovlig efter persondataloven. Datatilsynet kan efter persondataloven påtale en myndigheds ulovlige behandling over for myndigheden men har ikke i øvrigt beføjelser over for myndigheden. Datatilsynet offentliggør løbende sager på sin hjemmeside, hvor private og myndigheder ikke har overholdt gældende lovgivning.

Da efterretningstjenesterne som nævnt ikke er omfattet af persondataloven og retshåndhævelsesloven, fører Datatilsynet ikke tilsyn med tjenesterne.

3.2.3. Tilsynet med Efterretningstjenesterne

Tilsynet med Efterretningstjenesterne fører tilsyn med den behandling af oplysninger, herunder personoplysninger, der foretages af PET, FE og CFCS i henhold til de tre respektive love for disse enheder, jf. PET-loven §§ 16 ff., FE-loven §§ 13 ff. og CFCS-loven §§ 19 ff. Det synes at følge af forarbejderne til FE-loven, at FE´s indsamling af rådata, herunder masseindhentning af oplysninger om borgernes internetadfærd, ikke er omfattet af tilsynets kontrol.

Tilsynet varetager sine opgaver i fuld uafhængighed.

Tilsynet kan både behandle klager og tage sager op af egen drift.

Tilsynet kan afgive udtalelser over for tjenesterne, herunder afgive kritik eller henstillinger. Tjenesterne er ikke bundet af tilsynets henstillinger, men forudsættes normalt at følge dem. Følges en henstilling ikke, skal sagen forelægges den relevante minister til afgørelse (justitsministeren for PET og forsvarsministeren for FE). Såfremt ministeren ikke følger tilsynets henstilling, skal tilsynet orientere Folketingets Kontroludvalg. Tilsynet skal endvidere underrette justitsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

Tilsynet kan kræve udlevering af alle oplysninger og alt materiale, der er af betydning for dets virksomhed.

3.3. Egenkontrol

Med egenkontrol menes mekanismer, der giver borgeren mulighed for selv at kontrollere hvilke oplysninger om den pågældendes internetadfærd, som myndighederne indsamler og behandler.

Persondataloven indeholder forskellige former for egen kontrolmekanismer. Efter lovens §§ 28-29 har den, der indsamler personoplysninger, pligt til at oplyse den registrerede om indsamlingen. Der gælder en række undtagelser til oplysningspligten, herunder hvis oplysningen er umulig eller uforholdsmæssig vanskelig, eller hensynet til den registrerede findes at burde vige for afgørende hensyn til offentlige interesser. Oplysningspligten gælder ikke for den, der videregiver oplysningerne, eller for anden form for behandling end indsamling.

Efter lovens § 31 er den, der behandler personoplysninger om en anden, forpligtet til at informere om, hvilke oplysninger der behandles og formålet hermed, når den registrerede begærer en sådan indsigt. Når begæringen rettes til en offentlig myndighed, er indsigtsretten undergivet samme indskrænkninger, som gælder efter reglerne om aktindsigt i offentlighedsloven.

Retshåndhævelsesloven indeholder ligeledes bestemmelser om oplysningspligt og indsigtsret, der overordnet svarer til bestemmelserne i persondataloven, jf. lovens §§ 13 ff.

Forvaltningsloven indeholder også regler om aktindsigt. Som udgangspunkt har borgere krav på at blive gjort bekendt med dokumenter i sager, hvor de er part, og hvor der vil blive truffen en afgørelse, lovens § 7.

Efterretningstjenesterne er ikke omfattet af persondataloven eller af forvaltningslovens regler om aktindsigt, jf. PET-loven § 14 og FE-loven § 11, og efterretningstjenesterne har som udgangspunkt ikke pligt til at give en borger indsigt i hvilke oplysninger om den pågældende, tjenesterne behandler, jf. PET-loven § 12 og FE-loven § 9. En sådan indsigt kan kun gives, hvis særlige forhold taler for det. Den enkelte borgers primære kontrolmulighed består derfor i at anmode Tilsynet med Efterretningstjenesterne om at undersøge, hvorvidt tjenesten uberettiget behandler oplysninger om den pågældende. Tilsvarende er Center for Cybersikkerhed ikke omfattet af persondataloven eller forvaltningslovens regler om aktindsigt, jf. CFCS-loven § 8. Det forudsættes dog af bemærkningerne til CFCS-loven, at CFCS i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, herunder at CFCS som led i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse mv. Tilsvarende forudsættes det, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven. Som følge heraf følger CFCS i praksis reglerne i offentlighedsloven og forvaltningsloven, medmindre der er tale om anmodning om adgang til netsikkerhedstjenestens indsamlede data eller dokumenter, der vedrører øvrige dele af FE, og som dermed har efterretningsmæssig karakter.

3.4. Parlamentarisk kontrol

Det primære formål med parlamentarisk kontrol er ikke at kontrollere den konkrete sagsbehandling men at vurdere, om myndigheder på et mere generelt plan overskrider deres beføjelser, og om lov-

givningen er hensigtsmæssigt indrettet. Parlamentarisk kontrol får særlig betydning, når hemmeligholdelseshensyn indebærer, at information om, hvordan myndigheden behandler oplysninger, ikke kan offentliggøres. Dette gør sig særligt gældende for efterretningstjenesternes behandling af oplysninger.

Generelt har folketingsmedlemmer ret til at indhente oplysninger fra en minister gennem samråd eller ved at stille spørgsmål. Ministeren er imidlertid ikke forpligtet til at besvare spørgsmål, som efter deres særlige karakter kræver hemmeligholdelse. Dette vil som regel omfatte spørgsmål om efterretningstjenesternes arbejdsmetoder, herunder hvordan der sker indsamling og behandling af oplysninger. Ministerens mulighed for at give oplysninger vil endvidere være begrænset af reglerne om tavshedspligt for offentligt ansatte i straffelovens § 152.

For at give Folketinget større indsigt i efterretningstjenesternes arbejde er der i henhold til særlig lovgivning[35] nedsat et Udvalg vedrørende Efterretningstjenesterne (også kaldet Kontroludvalget). Udvalget skal årligt modtage en orientering fra regeringen om efterretningstjenesternes virksomhed. Som led heri kan udvalget selv anmode om oplysninger om efterretningstjenesternes virksomhed, herunder statistiske oplysninger. Udvalgets medlemmer har tavshedspligt om alt, de erfarer som led i udvalgsarbejdet. Udvalget kan tilkendegive sin mening over for regeringen og afgiver en årlig beretning til Folketinget men har ikke i øvrigt nogen beføjelser. Da beretningen er offentlig, kan den ikke indeholde oplysninger, der er underlagt tavshedspligt.

3.5. Offentlighedskontrol

Offentlighedskontrol er som begrebet antyder offentlighedens mulighed for at føre kontrol med myndigheders adfærd gennem adgang til information om denne adfærd. På samme måde som parlamentarisk kontrol er offentlighedskontrol primært en kontrol af, om myndigheder på et mere generelt plan overholder lovgivningen, og om myndighedernes praksis er hensigtsmæssig. Effektiviteten af offentlighedskontrol afhænger af, hvilken adgang offentligheden har til oplysninger om myndighedernes adfærd og praksis.

Generelt har myndigheder *ret* til at offentliggøre oplysninger om deres praksis. Også her gælder dog reglerne om tavshedspligt for offentligt ansatte i forvaltningslovens § 27 og straffelovens § 152.

I praksis spiller det en større rolle, hvornår myndigheder har *pligt* til at udlevere oplysninger. En sådan pligt følger navnlig af offentlighedsloven[36]. Lovens udgangspunkt er, at enhver kan forlange at blive gjort bekendt med dokumenter, der er indgået til eller oprettet af en myndighed m.v. som led i administrativ sagsbehandling i forbindelse med dens virksomhed, § 7. Dette udgangspunkt er dog undergivet nogle væsentlige modifikationer af betydning for kontrollen med myndigheders registrering af borgernes internetadfærd. Efterretningstjenesterne og Center for Cybersikkerhed er således undtaget fra offentlighedsloven, jf. PET-loven § 14, FE-loven § 11 og CFCS-loven § 8. Aktindsigten omfat-

[35] Lovbkg. nr 937 af 26. august 2014 om etablering af et udvalg vedrørende politiets og forsvarets efterretningstjeneste.
[36] Lov nr. 606 af 12. juni 2013 om offentlighed i forvaltningen med senere ændringer.

ter endvidere ikke sager inden for strafferetsplejen, § 19, og heller ikke myndigheders interne dokumenter, § 23. Efter lovens § 31 kan retten til aktindsigt begrænses, i det omfang det er af væsentlig betydning for statens sikkerhed eller rigets forsvar.

Som beskrevet ovenfor spiller private virksomheder også en rolle for myndigheders adgang til at registrere borgenes internetadfærd, idet private virksomheder ofte er den oprindelige indsamlingskilde, hvorfra myndighederne får udleveret oplysningerne. Offentlighedskontrol afhænger derfor også af muligheden for at få oplysninger udleveret fra disse private virksomheder.

Som udgangspunkt har private virksomheder en fri *ret* til at offentliggøre oplysninger om virksomheden, herunder i hvilket omfang virksomheden indsamler og udleverer oplysninger til myndigheder, begæringer om udlevering mv. Denne type oplysninger vil som regel ikke rumme information om specifikke personer og derfor heller ikke være omfattet af persondatalovens regler. Efter retsplejelovens § 189 sammenholdt med § 804 kan domstolene og politiet pålægge parter, der udleverer oplysninger efter editionsreglerne i § 804, tavshedspligt om udleveringen, når hensynet til fremmede magter, til statens sikkerhed eller til opklaring af alvorlige forbrydelser taler derfor. En række virksomheder, herunder eksempelvis Google og Facebook, offentliggør løbende statistik over myndigheders begæring om udlevering af oplysninger.

Private virksomheder har ingen *pligt* til at offentliggøre oplysninger om udleveringer mv.

3.6. Nogle betragtninger om demokratisk kontrol

Som det fremgår af det ovenstående kan en kontrol både rette sig mod 1) den enkelte behandling af oplysninger, 2) mod myndighedens generelle overholdelse af lovgivningen og i bredeste forstand 3) mod indretningen af lovgivningen, hensigtsmæssigheden af den myndighedspraksis, der følger af lovgivningen og dermed de mere generelle samfundsimplikationer, der følger af lovgivningen.

Alle disse tre former for kontrol er væsentlige i et demokratisk samfund, men navnlig den sidstnævnte er afgørende for at sikre den fornødne demokratiske legitimitet til myndigheders registrering af borgernes internetadfærd. Det er helt centralt, at der findes en demokratisk og åben debat om omfanget af denne adgang for myndighederne.

Denne form for demokratisk kontrol er i vidt omfang til stede i Danmark. Dette illustreres godt af den intensive debat om logningsreglerne, der har været ført flere gange og senest i forbindelse med regeringens forslag om udvidet sessionslogning.

Debatten om logningsreglerne har dog også vist, at det kan være svært at få et klart billede af reglernes praktiske konsekvenser og effekter. Lige præcis effekten af sådanne regler er dog central for debatten om omfanget af myndighedernes beføjelser (og privates forpligtelser til at bistå i forbindelse hermed). Det kunne derfor overvejes, om lovgivningen mere eksplicit skulle pålægge myndigheder at oplyse om, hvordan reglerne bruges. En sådan oplysningspligt er i et vist omfang forudsat for CFCS' virke, jf. bemærkningerne til CFCS-loven § 24, hvorefter Tilsynet med Efterretningstjenesternes årlige redegørelse for tilsynet med CFCS bl.a. skal indeholde statistiske oplysninger om CFCS

behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centeret som tilsynet, oplysninger om antallet af aktindsigtssager og afgørelsen af disse samt oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centeret. Tilsvarende kunne det overvejes, om private parter skulle pålægges at oplyse om, i hvilket omfang de udleverer oplysninger til myndigheder. Som beskrevet ovenfor offentliggør en række virksomheder på frivillig basis sådanne oplysninger.

At føre en tilstrækkelig demokratisk kontrol udgør en særlig udfordring i relation til efterretningstjenesterne. Karakteren af tjenesternes arbejde gør, at en stor del af deres virke må hemmeligholdes. Det er således også åbenbart, at der kun i begrænset omfang kan føres en offentlighedskontrol med efterretningstjenesterne. Kontrollen må derfor primært varetages af Tilsynet med Efterretningstjenesterne og Folketingets Udvalg vedrørende Efterretningstjenesterne (Kontroludvalget). Om disse kontrolmekanismer samlet set sikrer en optimal demokratiske kontrol må anses for tvivlsomt.

Tilsynet med efterretningstjenesterne har navnlig til formål at kontrollere, om efterretningstjenesterne behandler oplysninger i overensstemmelse med lovens regler herom. Den bredere demokratiske kontrol må derfor primært ske gennem en parlamentarisk kontrol. Hermed bliver den demokratiske kontrol i høj grad knyttet an på Kontroludvalget. Udvalget har imidlertid begrænsede beføjelser og består alene af fem folketingsmedlemmer, der er underlagt tavshedspligt og dermed også betydeligt er begrænset i, hvilke forhold de kan drøfte med Folketingets øvrige medlemmer. På den baggrund kan det anbefales at gennemføre en undersøgelse af det nuværende kontrolsystem. En sådan undersøgelse kunne tage udgangspunkt i forskningsrapporten "Ten standards for oversight and transparency of national intelligence services"[37] udarbejdet af en række forskere ved Amsterdam Universitet og i øvrigt sammenholde det danske kontrolsystem med kontrolsystemer i andre vestlige lande.

[37] Tilgængelig fra https://www.ivir.nl/publicaties/download/1591.pdf