INSTITUT FOR
MENNESKE
RETTIGHEDER

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Danmark
E-mail: fmn@fmn.dk med kopi til tbl@fmn.dk og sbu@fmn.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 9132 5761
MAAK@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 19/00103-2

4. FEBRUAR 2019

HØRING OVER UDKAST TIL FORSLAG TIL LOV OM ÆNDRING AF LOV OM CENTER FOR CYBERSIKKERHED (INITIATIVER TIL STYRKELSE AF CYBERSIKKERHEDEN)

Forsvarsministeriet har ved e-mail af 7. januar 2019 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til et udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (initiativer til styrkelse af cybersikkerheden).

Instituttet har valgt at fokusere på følgende dele af udkastet: 1) påbud om tilslutning til netsikkerhedstjenesten, 2) udvidet adgang til indgreb i meddelelseshemmeligheden, og 3) ændrede frister for sletning af data.

SAMMENFATNING

Instituttet bemærker indledningsvist, at udkastet varetager det væsentlige og anerkendelsesværdige formål at sikre Danmark mod cybertrusler i form af blandt andet cyberspionage, cyberkriminalitet og infrastrukturangreb og at sikre, at Danmark har et højt cybersikkerhedsniveau.

Udkastet lægger op til betydelige kompetenceudvidelser for Center for Cybersikkerhed på en række områder med den konsekvens, at centret kommer i besiddelse af en betydelig mængde personoplysninger, herunder følsomme personoplysninger.

Dette sker blandt andet ved en tvunget tilslutning til centrets såkaldte netsikkerhedstjeneste, hvorfra centret kan monitorere al digital korrespondance til og fra virksomheden eller myndigheden samt såkaldt stationær data, som for eksempel private data på en medarbejders pc.

Centret har i øvrigt også adgang til sådanne private data hos virksomheder og myndigheder, der ikke er tilsluttet netsikkerhedstjenesten – og uden et krav om retskendelse.

For samtlige de indhentede data er centret i øvrigt ikke forpligtet til at slette disse før efter 5 år, hvis oplysningerne knytter sig til en sikkerhedshændelse og 3 år, hvis oplysningerne ikke knytter sig til en sikkerhedshændelse. En sikkerhedshændelse er blandt andet en hændelse, der negativt påvirker tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Efter gældende ret er fristerne henholdsvis 3 år og 13 måneder.

Alt i alt kommer Center for Cybersikkerhed til at være i besiddelse af en betydelig mængde data – og for en længere periode – end centret hidtil har haft beføjelse til at indsamle og behandle.

Udvidelserne kan hver for sig og samlet føre til indgreb i retten til respekt for privatliv, beskyttet i Den Europæiske Menneskerettighedskonvention artikel 8, ligesom enkelte af udvidelserne udgør et indgreb i meddelelseshemmeligheden, beskyttet i grundlovens § 72.

- Instituttet anbefaler blandt andet, at ministeriet overvejer at indsætte et krav om efterfølgende retskendelse ved Center for Cybersikkerheds indhentelse af oplysninger, som udgør indgreb i meddelelseshemmeligheden.

Instituttet vurderer endvidere, at der er risiko for uproportionale indgreb ved en slettefrist på 3 år i stedet for 13 måneder for oplysninger, som ikke vedrører sikkerhedshændelser.

- Instituttet anbefaler, at ministeriet i lovbemærkningerne nøje redegør for, hvorledes det vil sikres, at en udvidelse af slettefristen fra 13 måneder til 3 år ikke vil føre til uproportionale indgreb i retten til respekt for privatliv.

Mere generelt har instituttet principielle betænkeligheder ved centrets placering under Forsvarets Efterretningstjeneste (FE), som instituttet også har rejst tidligere.

Instituttet bemærker i den forbindelse, at det eneste retsgrundlag, som adskiller deling af oplysning fra Center for Cybersikkerhed til FE's efterretningsfunktioner er en vejledning fra Forsvarsministeriet.

Disse principielle bekymringer får fornyet aktualitet ved en udvidelse af centrets beføjelser – navnlig i fraværet af effektive retsgarantier som for eksempel krav om retskendelse og skærpede slettefrister.

- Instituttet anbefaler, at der i udkastet indføres en bestemmelse om betingelserne for videregivelse af data fra centret til resten af Forsvarets Efterretningstjeneste, således at forholdet reguleres på lovniveau.

UDKASTETS INDHOLD

PÅBUD OM TILSLUTNING TIL CENTER FOR CYBERSIKKERHEDS NETSIKKERHEDSTJENESTE

Med udkastet vil der blive skabt mulighed for, at Center for Cybersikkerhed i særlige tilfælde kan påbyde særligt samfundsvigtige virksomheder eller myndigheder at blive tilsluttet centrets netsikkerhedstjeneste (udkastets § 3, stk. 4).

Netsikkerhedstjenesten er en samlebetegnelse for Center for Cybersikkerheds aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser (sikkerhedshændelser er i udkastets § 2 defineret som hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester). Netsikkerhedstjenesten omfatter alle de kapaciteter ved Center for Cybersikkerhed, der på forskellig vis bidrager til monitorering, herunder CERT (Computer Emergency Response Team), aktiviteter på det civile og militære område, sikkerhedstekniske aktiviteter samt støttefunktioner (jf. de særlige bemærkninger til § 1, nr. 1).

Virksomheder og myndigheder, der varetager samfundsvigtige funktioner, er ifølge udkastet navnlig funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet. Som eksempler på virksomheder, der har mulighed for at blive tilsluttet netsikkerhedstjenesten, nævnes forsyningsselskaber, teleudbydere, internetudbydere, medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige eller for andre samfundsvigtige virksomheder

Imidlertid omfatter begrebet også virksomheder, som ikke i sig selv er samfundsvigtige, men som kan være vigtige ud fra et sikkerhedsperspektiv, for eksempel fordi deres servere er blevet inficeret gennem et cyberangreb og nu anvendes som en del af en angrebsaktørs infrastruktur (jf. de særlige bemærkninger til § 1, nr. 1).

En tilslutning til netsikkerhedstjenesten indebærer, at Center for Cybersikkerhed kan monitorere en række kategorier af data, herunder pakkedata (indholdet af digital kommunikation) og stationær data (se nærmere nedenfor).

Center for Cybersikkerheds påbud om tilslutning til netsikkerhedstjenesten kan påklages administrativt til Forsvarsministeriet og kan indbringes for domstolene.

UDVIDET ADGANG TIL INDGREB I GRUNDLOVENS § 72

En af de beføjelser, som udvides med udkastet, er Center for Cybersikkerheds adgang til indgreb i meddelelseshemmeligheden uden krav om retskendelse.

Meddelelseshemmeligheden er beskyttet i grundlovens § 72 og er tillige omfattet af retten til respekt for privatliv, som beskyttet i Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8.

Det følger af udkastet, at Center for Cybersikkerhed fremadrettet blandt andet skal kunne tilgå data, som opbevares på en lokal enhed (såkaldt stationær data, som er data, der opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende jf. udkastets § 2, nr. 4).

For så vidt angår virksomheder og myndigheder, som er tilknyttet netsikkerhedstjenesten kan centret tilgå disse data uden retskendelse og uden mistanke om en sikkerhedshændelse, forudsat det understøtter et højt informationssikkerhedsniveau i samfundet (forslagets § 4).

For så vidt angår virksomheder og myndigheder, som ikke er tilknyttet, har Center for Cybersikkerhed adgang til lokale enheder (stationær data) uden retskendelse, hvis der er begrundet mistanke om en sikkerhedshændelse og den pågældende virksomhed eller myndighed enten har givet samtykke eller hvis behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet (§ 5).

Af udkastet fremgår nærmere, at stationær data kan være private data, som en medarbejder f.eks. har gemt på en pc, en arbejdsmobil eller lignende.

Forsvarsministeriet fastslår i udkastet, at indgrebet ikke er egnet til domstolsprøvelse, da indgrebet oftest vil ske automatiseret og ved scanning af ukendt data for at fastslå, om der overhovedet er tale om en sikkerhedshændelse i lovens forstand. En eventuel domstolsprøvelse vil derfor ifølge ministeriets vurdering ikke kunne basere sig på en vurdering af karakteren af de pågældende data, men alene på en meget overordnet og generel vurdering af, om f.eks. trusselsbilledet i tilstrækkelig grad begrunder indgrebet (de almindelige bemærkninger, afsnit 3.3.2)

Den foreslåede ordning vil ikke indebære en ændring af betingelserne for, hvornår Center for Cybersikkerhed manuelt må foretage analyse af indhold af filer og kommunikation, men derimod en udvidelse af, hvilke filer og kommunikation, centret kan tilgå.

ÆNDREDE SLETTEFRISTER

Med udkastet ændres Center for Cybersikkerheds forpligtelser til at slette oplysninger markant.

Efter gældende ret skal data slettes, når formålet med behandlingen er opfyldt. Endvidere følger det af gældende ret, at uanset at formålet med behandlingen ikke er opfyldt, må data der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, mens data der ikke knytter sig til en sikkerhedshændelse, højst må opbevares i 13 måneder.

Fremadrettet vil centret i medfør af udkastet have en slettefrist på 5 år ved konstaterede sikkerhedshændelser og 3 år for data, der ikke knytter sig til en sikkerhedshændelse.

Data omfattet af den nye 3 års frist (som altså ikke er knyttet til en sikkerhedshændelse) vil ifølge udkastet stamme fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold (jf. de almindelige bemærkninger, afsnit 3.8.3.2).

FORSVARSMINISTERIETS VURDERING AF UDKASTET EFTER DEN EUROPÆISKE MENNESKERETTIGHEDSKONVENTION

I udkastet vurderer ministeriet, at de foreslåede ændringer er forenelige med artikel 8 om respekt for privatlivet i Den Europæiske Menneskerettighedskonvention (EMRK).

Ministeriet vurderer i den forbindelse, at den praksis, som Den Europæiske Menneskerettighedsdomstol (EMD) har udviklet vedrørende indgreb i meddelelseshemmeligheden, ikke kan finde anvendelse på centrets behandling af personoplysninger.

Ministeriet anfører i de almindelige bemærkninger, afsnit 4:

> ”I modsætning til ved egentlig efterretningsvirksomhed og politiets efterforskning foretager Center for Cybersikkerhed imidlertid ikke en decideret registrering af de personoplysninger, som centeret behandler, ligesom der ikke opereres med sager om enkeltpersoner. […] De indgreb i meddelelseshemmeligheden, som uundgåeligt foretages af centeret […], vurderes på den baggrund at indebære et mindre intensivt indgreb i privatlivet end de indgreb, der foretages med henblik på at udfinde målpersoner.”

INSTITUTTETS BEMÆRKNINGER

UDVIDET ADGANG TIL PERSONOPLYSNINGER MV.

Instituttet bemærker indledningsvist, at udkastet varetager det væsentlige og anerkendelsesværdige formål at sikre Danmark mod cybertrusler i form af blandt andet cyberspionage, cyberkriminalitet og infrastrukturangreb og at sikre, at Danmark har et højt cybersikkerhedsniveau.

Udkastet lægger op til betydelige kompetenceudvidelser for Center for Cybersikkerhed på en række områder, blandt andet: 1. adgang til at meddele påbud om tilslutning til netsikkerhedstjenesten med den følge, at centret har adgang til en stor mængde data i form af trafikdata, pakkedata og stationær data, 2. adgang til stationær data hos virksomheder og myndigheder, der ikke er tilsluttet netsikkerhedstjenesten, og 3. lempeligere slettefrister.

Hertil kommer en adgang til oplysninger, som retten kan pålægge virksomheder at udlevere om brugeren af en e-mailkonto, ip-adresse eller et domænenavn til centret (edition). I straffeprocessuel sammenhæng kræver edition mistanke om en strafbar lovovertrædelse. I de foreslåede regler vil der derimod alene være krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser.

Disse udvidelser kan hver for sig og samlet føre til indgreb i retten til respekt for privatliv, beskyttet i EMRK artikel 8.

Alt i alt kommer Center for Cybersikkerhed til at være i besiddelse af en betydelig mængde data, blandt andet personoplysninger (herunder følsomme personoplysninger), end centret hidtil har haft beføjelse til at indsamle og behandle.

Center for Cybersikkerheds adgang til at påbyde tilslutning til netsikkerhedstjenesten er betinget af, at en virksomhed eller en myndighed af centret anses for at varetage samfundsvigtige funktioner.

Samfundsvigtige virksomheder og myndigheder som defineret i udkastet er en ganske vid kategori, uden nærmere kvalificerede kendetegn. Påbudskompetencen kan således få et bredt anvendelsesområde på tværs af sektorer.

En tilknytning til netsikkerhedstjenesten indebærer, at centret har adgang til langt mere data om virksomheder og myndigheder og disses medarbejdere, end hvad der har været adgang til efter gældende ret (i form af trafikdata, pakkedata og stationær data). Denne adgang er ikke betinget af retskendelse eller noget mistankekrav om en sikkerhedshændelse men skal alene understøtte et højt informationssikkerhedsniveau i samfundet (§ 4).

For så vidt angår virksomheder og myndigheder, der ikke er tilknyttede, har centret ligeledes en vid adgang til oplysninger – uden retskendelse – hvis der er en begrundet mistanke om en sikkerhedshændelse. I disse tilfælde skal centret (i fraværet af samtykke) blot vurdere, at behandlingen understøtter et højt informationssikkerhedsniveau i samfundet (§ 5, nr. 2).

Instituttet bemærker, at kravet om, at behandlingen af oplysninger understøtter et højt informationsniveau i samfundet ikke kan anses for en selvstændigt kvalificeret juridisk vurdering, men derimod blot er sammenfaldende med selve formålet med Center for Cybersikkerhed, jf. således lovens formålsbestemmelse, § 1.

Instituttet bemærker, at der i tilfælde, hvor virksomheden eller myndigheden ikke er tilsluttet netsikkerhedstjenesten, eller er tilsluttet efter påbud, er tale om et særligt intensiveret indgreb vis-a-vis virksomheden/myndigheden, som efter EMRK artikel 8, stk. 2, er underlagt en tilsvarende skærpet proportionalitetsvurdering.

I øvrigt bemærker instituttet, at det er tvivlsomt, om et samtykke fra virksomheden eller myndigheden, eller frivillig tilslutning til tjenesten, vil ændre på proportionalitetsvurderingen i forhold til centrets adgang til følsomme personoplysninger om medarbejdere.

Ministeriet anfører, at indgrebet efter §§ 4 og 5 ikke er egnet til domstolsprøvelse, da indgrebet skal fastslå, om der overhovedet er tale om en sikkerhedshændelse i lovens forstand.

Instituttet bemærker, at denne usikkerhed vedrørende indholdet af den identificerede data ikke nødvendigvis adskiller sig fra andre indgreb i meddelelseshemmeligheden, hvorfor der netop stilles mere eller mindre kvalificerede mistankekrav i de straffeprocessuelle regler, og hvorfor disse netop er underlagt domstolsprøvelse.

Den betydelige udvidelse af kompetencer, som udkastet vil indebære, stiller tilsvarende krav til fornødne retsgarantier. Ellers risikerer indgrebene at være i strid med retten til respekt for privatliv, som blandt andet beskyttet i EMRK artikel 8.

Efter instituttets vurdering gør det ikke i sig selv indgrebet uegnet til domstolsprøvelse, at det er forbundet med usikkerhed, om der er en sikkerhedshændelse.

Instituttet bemærker i øvrigt, at ministeriet ikke har taget stilling til, om et krav om efterfølgende retskendelse ville være muligt henset til, at indgrebet i første omgang sker automatisk.

- Instituttet anbefaler, at ministeriet i lovbemærkningerne redegør for, hvordan usikkerheden ved en sikkerhedshændelse adskiller sig fra usikkerheder, når der i øvrigt foretages indgreb i

meddelelseshemmeligheden samt overvejer at indsætte et krav om efterfølgende retskendelse
- Uanset om ministeriet indarbejder anbefalingen om efterfølgende retskendelse, anbefaler instituttet, at kravet om adgang til stationær data fra myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten eller som er tilsluttet ved et påbud, skærpet betydeligt og ikke blot betinges af et krav, der har samme ordlyd, som centrets formålsbestemmelse i § 1.

LEMPELIGERE SLETTEFRISTER

Adgangen til data skal tillige ses i lyset af slettefristerne, som yder en retsgaranti i tilfælde, hvor en myndighed har videregående beføjelser til personoplysninger.

Instituttet anerkender, at det er væsentligt, at Center for Cybersikkerhed er i besiddelse af de fornødne oplysninger for effektivt at beskytte mod cyberangreb.

Imidlertid skal centrets vide – og længerevarige – adgang til oplysninger være proportionalt med formålet hermed.

Navnlig for så vidt angår adgangen til fremadrettet at opbevare oplysninger, som ikke vedrører en sikkerhedshændelse i 3 år i stedet for 13 måneder kan dette efter instituttets vurdering føre til et uproportionalt indgreb.

Instituttet bemærker i den forbindelse, at der allerede ved en lovændring af 11. juni 2014 (L 192), skete en betydelig udvidelse fra den dagældende slettefrist på 14 dage til 13 måneder.[1]

- Instituttet anbefaler, at ministeriet i lovbemærkningerne nøje redegør for, hvorledes det vil sikres, at en udvidelse af slettefristen fra 13 måneder til 3 år ikke vil føre til uproportionale indgreb i retten til respekt for privatliv.

CENTER FOR CYBERSIKKERHEDS ORGANISERING

Center for Cybersikkerhed er organiseret under Forsvarets Efterretningstjeneste (FE).

Instituttet skal i den forbindelse på ny fremhæve de principielle bekymringer, som instituttet tidligere har rejst i forhold til Center for

[1] Se instituttets høringssvar til den dagældende ændring her: https://menneskeret.dk/sites/menneskeret.dk/files/media/researchpublications/hoeringssvar/hoeringssvar_afgivet_i_2014/marts%202014/marts_2014_tilgaengeligt/24_b_center_for_cybersikkerhed.pdf

Cybersikkerheds placering under FE, når centret varetager centrale, civile samfundsstrukturer.[2]

Det eneste retsgrundlag, som adskiller deling af oplysning fra Center for Cybersikkerhed til FE's efterretningsfunktioner er en vejledning fra Forsvarsministeriet.

Instituttet har tidligere fremhævet det betænkelige ved, at der ikke på lovniveau er sikret en retssikkerhedsmæssig garanti imod videregivelse af oplysninger fra centret til FE til brug for efterretningstjenestens øvrige arbejde inden for det militære område.

Disse principielle bekymringer får fornyet aktualitet ved en udvidelse af centrets beføjelser – navnlig i fraværet af effektive retsgarantier (som domstolsprøvelse og skærpede slettefrister).

- Instituttet anbefaler, at der i udkastet indføres en bestemmelse om betingelserne for videregivelse af data fra centret til resten af Forsvarets Efterretningstjeneste, således at forholdet reguleres på lovniveau.

Netop på grund af centrets placering under FE skal instituttet i øvrigt bemærke, at centerets indsamling og håndtering af personoplysninger skal vurderes i lyset af den retspraksis fra EMD, som vedrør efterretningstjenesters adgang til og behandling af personoplysninger. Instituttet er således ikke enig i, at centerets adgang til personoplysninger er et mindre intensivt indgreb, end indgreb foretaget i øvrigt af politiet og efterretningstjenesterne.

Instituttets bemærker i den forbindelse, at EMD's praksis og betingelserne etableret heri, naturligvis skal anvendes tilpasset til det formål og de opgaver, som Center for Cybersikkerhed varetager.

- På grund af Center for Cybersikkerheds organisatoriske placering under Forsvarets Efterretningstjeneste anbefaler instituttet, at ministeriet i lovbemærkningerne redegør for centrets adgang til personoplysninger i lyset af den relevante praksis fra Den Europæiske Menneskerettighedsdomstol om efterretningstjenesterne.

Der henvises til ministeriets sagsnummer 2018/006599.

Med venlig hilsen

Marya Akhtar
SPECIALKONSULENT

[2] Ibid.