FOLKETINGET

Folketingstidende
Tillæg C

Til lovforslag nr. **L 215** Folketinget 2018-19

Vedtaget af Folketinget ved 3. behandling den 2. maj 2019

Forslag

til

Lov om ændring af lov om Center for Cybersikkerhed

(Initiativer til styrkelse af cybersikkerheden)

§ 1

I lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, som ændret ved lov nr. 443 af 8. maj 2018, foretages følgende ændringer:

1. *Kapitel 2* og *3* affattes således:

»Kapitel 2

Definitioner

§ 2. I denne lov forstås ved:

1) Sikkerhedshændelse: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.
2) Pakkedata: Indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester.
3) Trafikdata: Data, som behandles med henblik på at transmittere pakkedata.
4) Stationære data: Data, som opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende.
5) Malware: Trafikdata, pakkedata og stationære data, hvor der er særlig bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.
6) Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person.
7) Behandling: Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Kapitel 3

Center for Cybersikkerheds netsikkerhedstjeneste

§ 3. Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder, jf. stk. 2-4.

Stk. 2. De øverste statsorganer og statslige myndigheder kan efter anmodning blive tilsluttet netsikkerhedstjenesten.

Stk. 3. Regioner og kommuner samt virksomheder, der har samfundsvigtig karakter, kan efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 4. Center for Cybersikkerhed kan i særlige tilfælde påbyde virksomheder, der har særlig samfundsvigtig karakter, og regioner og kommuner at blive tilsluttet netsikkerhedstjenesten med henblik på monitorering af netværkskommunikation. Påbuddet kan kun omfatte de dele af virksomheden, regionen eller kommunen, der har en væsentlig betydning for Danmarks kritiske infrastruktur. Center for Cybersikkerhed skal mindst hvert halve år vurdere, om et meddelt påbud skal opretholdes.

Stk. 5. Forsvarsministeren kan fastsætte nærmere regler om vilkårene for tilslutning efter stk. 2 og 3. Forsvarsministeren kan desuden fastsætte nærmere regler om påbud efter stk. 4, herunder om, at myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten på baggrund af et påbud, skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og i den forbindelse skal stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten.«

2. *Kapitel 4* ophæves, og i stedet indsættes:

»Kapitel 4

Indgreb omfattet af grundlovens § 72

§ 4. Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virk-

Forsvarsmin., j.nr. 2018/004202

somheder, jf. § 3, stk. 2-4, med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 5. Ved begrundet mistanke om en sikkerhedshændelse kan Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse behandle stationære data fra en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten, når

1) myndigheden eller virksomheden har anmodet Center for Cybersikkerhed om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen og
2) behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 6. Efter aftale med en myndighed eller virksomhed, der er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste i medfør af § 3, stk. 2 og 3, kan netsikkerhedstjenesten ved begrundet mistanke om en sikkerhedshændelse uden retskendelse blokere, omdanne eller omdirigere trafikdata og pakkedata hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Stk. 1 finder tilsvarende anvendelse i forhold til stationære data hos tilsluttede myndigheder og virksomheder. Ved en konstateret sikkerhedshændelse kan netsikkerhedstjenesten endvidere efter aftale med den tilsluttede myndighed eller virksomhed slette de stationære data, der har forårsaget sikkerhedshændelsen.

§ 6 a. Med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kan Center for Cybersikkerhed gennemføre forebyggende sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed har anmodet centeret herom.

Stk. 2. Efter anmodning fra myndigheden eller virksomheden kan Center for Cybersikkerhed som led i den forebyggende sikkerhedstekniske undersøgelse

1) uden retskendelse behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden,
2) behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere og
3) iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

§ 6 b. Med henblik på at opnå viden om angrebsaktørers metoder og værktøjer kan Center for Cybersikkerhed opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Benytter en angrebsaktør et fiktivt angrebsmål til at deponere data, kan Center for Cybersikkerhed uden retskendelse behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

§ 6 c. Med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kan Center for Cybersikkerhed gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, forudsat at disse er ledige til registrering.

Stk. 2. Modtager Center for Cybersikkerhed som led i anvendelsen af it-infrastruktur efter stk. 1 data fra tredjemand, kan centeret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Kapitel 4 a

Edition

§ 7. Med henblik på at afdække sikkerhedshændelser kan der meddeles en juridisk eller fysisk person pålæg om at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed.

Stk. 2. Pålæg efter stk. 1 må ikke meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

§ 7 a. Afgørelse om pålæg om edition efter § 7 træffes af retten efter Center for Cybersikkerheds begæring.

Stk. 2. Afgørelsen træffes af retten ved kendelse. Retsmøder holdes for lukkede døre. I kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres.

§ 7 b. Inden retten træffer afgørelse om pålæg om edition efter § 7, skal der være givet den, der har rådighed over oplysningerne, adgang til at udtale sig.

Stk. 2. Taler hensynet til fremmede magter eller statens sikkerhed derfor, kan retten eller Center for Cybersikkerhed pålægge den, der har rådighed over oplysninger, som ønskes forevist eller udleveret efter § 7, tavshedspligt med hensyn til den pågældendes viden om sagen. Når pålæg meddeles en erhvervsvirksomhed, gælder dette også for andre juridiske og fysiske personer, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen.

Stk. 3. Pålæg efter stk. 2 kan ophæves af Center for Cybersikkerhed eller retten. Center for Cybersikkerheds nægtelse af at ophæve et pålæg skal efter begæring forelægges retten. Den pågældende skal gøres bekendt med adgangen hertil.

§ 7 c. Reglerne i retsplejelovens kapitel 63 om værneting og kapitel 85 om kære til højere ret finder tilsvarende anvendelse.

§ 7 d. Center for Cybersikkerhed foranlediger ved at rette henvendelse til den, der har rådighed over oplysningerne, at en kendelse om edition opfyldes. Rettens kendelse skal på begæring forevises den pågældende. Afviser den pågælden-

de uden lovlig grund at efterkomme pålægget, finder reglerne i retsplejelovens § 178 tilsvarende anvendelse.«

3. I *§ 8, stk. 1, 2. pkt.,* indsættes efter »forvaltningslovens kapitel 4-6«: », fra §§ 3 og 5 og § 8, stk. 2, i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter«.

4. *§ 8, stk. 2, nr. 1,* affattes således:

»1) centerets behandling af sager om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3 og 4,«.

5. Efter § 8 indsættes i *kapitel 5:*

»§ 8 a. Oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Stk. 2. Forsvarsministeren kan fastsætte nærmere regler om Center for Cybersikkerheds overførsel af oplysninger, der skal bevares for eftertiden, til Rigsarkivet og om centerets opbevaring af sådanne oplysninger, indtil overførsel til Rigsarkivet kan ske.

§ 8 b. Myndigheders og virksomheders samarbejde med Center for Cybersikkerhed er ikke begrænset af bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov, jf. dog stk. 2.

Stk. 2. Forsvarsministeren kan fastsætte regler om, at nærmere angivne bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov fortsat finder anvendelse på myndigheders og virksomheders samarbejde med Center for Cybersikkerhed.«

6. *§ 14, stk. 2,* ophæves.

7. *Kapitel 7* affattes således:

»Kapitel 7

Analyse, videregivelse og sletning af data

§ 15. Center for Cybersikkerhed kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data, der er omfattet af kapitel 4. Manuelle analyser af data, der er omfattet af kapitel 4, må alene finde sted i følgende tilfælde:

1) For at opdage, analysere og bidrage til at imødegå sikkerhedshændelser kan trafikdata analyseres i det omfang, det er nødvendigt.
2) Ved begrundet mistanke om en sikkerhedshændelse kan pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at afklare forhold vedrørende hændelsen.
3) Som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a kan trafikdata, pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at gennemføre undersøgelserne.
4) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af, om kommunikation indeholder klassificeret materiale, kan trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, analyseres.
5) Som led i tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder kan trafikdata og pakkedata analyseres i det omfang, det er nødvendigt for at gennemføre testen. Testen skal afsluttes, så snart formålet med testen er opfyldt. Analysen må alene foretages af medarbejdere, der varetager tekniske drifts- og udviklingsopgaver for Center for Cybersikkerhed. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra test. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i Center for Cybersikkerhed efter nr. 2.

§ 16. Center for Cybersikkerhed kan videregive trafikdata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af Center for Cybersikkerheds opgaver.
3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og såfremt det er nødvendigt for udførelsen af Center for Cybersikkerheds opgaver.

Stk. 2. Center for Cybersikkerhed kan videregive pakkedata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

Stk. 3. Center for Cybersikkerhed kan videregive stationære data, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den myndighed, virksomhed eller borger, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.
3) Andre netsikkerhedstjenester, såfremt Center for Cybersikkerhed har modtaget de pågældende data i medfør af § 6 b eller § 6 c.

Stk. 4. Center for Cybersikkerhed kan videregive malware, der er omfattet af kapitel 4, til:

1) Politiet.
2) Den myndighed eller virksomhed, hvorfra de pågældende data hidrører.
3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Stk. 5. Stk. 1-4 finder ikke anvendelse på data, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder. Center for Cybersikkerhed kan alene videregive sådanne data i følgende tilfælde:

1) Malware, der er opdaget ved en tilfældighed, kan videregives til politiet, til den myndighed eller virksomhed, hvorfra de pågældende data hidrører, til danske myndigheder, til udbydere af offentlige elektroniske kommunikationsnet og -tjenester og til andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.
2) Trafikdata kan videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

Stk. 6. Uanset stk. 1-4 må Center for Cybersikkerhed i forbindelse med forebyggende sikkerhedstekniske undersøgelser efter § 6 a alene videregive oplysninger vedrørende myndighedens eller virksomhedens medarbejdere, hvis det sker i anonymiseret form.

§ 17. Data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt.

Stk. 2. Uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i 5 år,
2) data, der ikke knytter sig til en sikkerhedshændelse, men som stammer 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, højst opbevares i 3 år og
3) øvrige data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Stk. 3. Fristerne i stk. 2 regnes fra tidspunktet for Center for Cybersikkerheds registrering af de pågældende data.

Stk. 4. Center for Cybersikkerhed kan opbevare backup af data i op til 4 måneder efter udløb af fristerne i stk. 1 og 2. Ved indlæsning af data fra backup skal Center for Cybersikkerhed sikre, at data, der tidligere er slettet efter stk. 1 eller 2, straks slettes igen.

Stk. 5. Er data i medfør af § 16 videregivet til andre end den myndighed eller virksomhed, som data hidrører fra, finder stk. 1 og 2 ikke anvendelse på disse data.

Stk. 6. I data, som Center for Cybersikkerhed får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, skal personoplysninger, der er indeholdt i disse data, endvidere slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Konstaterer Center for Cybersikkerhed, at der i de pågældende data er indeholdt følsomme personoplysninger, skal disse slettes uden unødigt ophold.

Stk. 7. Sletning efter fristerne i stk. 2, nr. 2 og 3, kan i helt særlige tilfælde kortvarigt suspenderes, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt. Tilsynet med Efterretningstjenesterne skal straks underrettes om suspension efter 1. pkt. og om baggrunden for suspensionen.

§ 17 a. § 17 finder ikke anvendelse på data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af § 6 c, såfremt Center for Cybersikkerhed ikke udtager disse data til nærmere vurdering. Disse data slettes hurtigst muligt. Udtager Center for Cybersikkerhed data til nærmere vurdering, skal sletning ske efter reglerne i § 17.«

8. I *§ 20* indsættes efter »kapitel 4,«: »4 a,«.

9. Efter kapitel 9 indsættes:

»Kapitel 9 a

Straffebestemmelser m.v.

§ 24 a. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der undlader at efterkomme et pålæg efter § 7 b, stk. 2.

Stk. 2. I regler, der udfærdiges i medfør af § 3, stk. 5, 2. pkt., kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.«

§ 2

Stk. 1. Loven træder i kraft den 1. juli 2019.

Stk. 2. Loven finder ikke anvendelse på data, der er indsamlet før den 1. juli 2019. For sådanne data finder de hidtil gældende regler anvendelse.

§ 3

Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning helt eller delvis sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger.

Folketinget, den 2. maj 2019

PIA KJÆRSGAARD

/ Erling Bonnesen