FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

22. maj 2014

Notat
om
betydningen af EU-domstolens dom af 8. april 2014 om lognings-direktivet i forhold til lovforslag om Center for Cybersikkerhed (L 192) og om lovforslagets overensstemmelse med Den Europæiske Menneskerettighedskonventions artikel 8.

1. EU-Domstolen har ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 erklæret direktiv 2006/24/EF af 15. marts 2006 (herefter logningsdirektivet) ugyldigt under henvisning til, at det var i strid med artikel 7 og 8 i Den Europæiske Unions Charter om grundlæggende rettigheder (herefter Charteret). Domstolen fandt således, at EU-lovgiver med vedtagelsen af logningsdirektivet havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver henset til Charterets artikel 7, 8 og 52, stk. 1.

Charterets anvendelsesområde er defineret i Charterets artikel 51, stk. 1, hvoraf bl.a. følger, at dets bestemmelser kun er rettet til medlemsstaterne, når de gennemfører EU-retten. Det fremgår af forklaringerne til Charterets artikel 51, at det finder anvendelse, når medlemsstaterne handler inden for rammerne af EU-retten. EU-Domstolen har som følge heraf fastslået, at Charteret finder anvendelse, når national lovgivning falder ind under EU-rettens anvendelsesområde, jf. bl.a. sag C-617/10, Hans Åkerberg Fransson.

Det fremsatte lovforslag, hvorefter Center for Cybersikkerhed skal udføre opgaver, der vedrører den offentlige sikkerhed, forsvaret og statens sikkerhed, falder ikke inden for EU-rettens anvendelsesområde, men er derimod rent national regulering. Lovforslaget falder derfor uden for Charterets anvendelsesområde.

Det skal herudover bemærkes, at EU-Domstolens dom af 8. april 2014 om logningsdirektivet angår en anden problemstilling end den, som lovforslaget har til hensigt at regulere.

I dommen foretager EU-Domstolen en samlet vurdering af, om de regler, der var fastsat i logningsdirektivet, hvorefter medlemsstaterne skulle fastsætte regler, som pålagde teleudbydere at logge nærmere bestemte data om deres kunder med henblik på at sikre, at der var adgang til disse data i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet, var forenelige med Charteret. Sådanne regler er i dansk ret fastsat i retsplejelovens § 786, stk. 4, og i logningsbekendtgørelsen (bekendtgørelse nr. 988 af 28. september 2006).

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

Det fremsatte lovforslag vedrører den monitorering og lagring af datatrafikken hidrørende (frivilligt) tilsluttede myndigheder og virksomheder, som Center for Cybersikkerhed vil foretage med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser.

Selv om der i begge tilfælde i forskelligt omfang er tale om lagring af fysiske og juridiske personers data, er problemstillingen således forskellig, og dommen af 8. april 2014 vurderes derfor ikke at have betydning for lovforslaget.

2. Som nærmere redegjort for under afsnit 3.2.1-3.2.2 i de almindelige bemærkninger til lovforslaget finder Forsvarsministeriet, at den vurdering af lovforslagets forhold til artikel 8 i Den Europæiske Menneskerettighedskonvention (herefter EMRK) om retten til respekt for privatliv og familieliv, der blev foretaget i forhold til den såkaldte GovCERT-lov (lov nr. 596 af 14. juni 2011), er dækkende for det fremsatte lovforslags forhold til EMRK, og at lovforslaget således er i overensstemmelse med EMRK artikel 8.

Af afsnit 3.7 i de almindelige bemærkninger i lovforslaget til GovCERT-loven (lovforslag nr. L 197 af 27. april 2011) fremgår følgende om forholdet til EMRK artikel 8:

> *"3.7. Forholdet til Den* Europæiske Menneskeretskonvention
>
> Ifølge artikel 8, stk. 1, i Den Europæiske Menneskerettighedskonvention (EMRK) har enhver ret til respekt for sit privatliv og familieliv.
>
> Beskyttelsen efter artikel 8 omfatter både indgreb i meddelelseshemmeligheden, f.eks. overvågning af e-mailkorrespondance og internetkommunikation, og offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger generelt.
>
> Indgreb i kommunikation via bl.a. e-mails vil som udgangspunkt udgøre et indgreb efter EMRK artikel 8. Hvis en offentlig arbejdsgiver overvåger en ansats brug af e-mail og internet, vil det således udgøre et indgreb i den ansattes ret til privatliv og korrespondance, når den ansatte med rimelighed kunne forvente ikke at blive overvåget (se Copland mod Storbritannien, dom af 3. april 2007, præmis 41-42).
>
> Det samme vil være tilfældet, hvor en arbejdsgiver tillader en (anden) myndighed at overvåge den ansattes brug af e-mail og internet.
>
> Det forudsættes imidlertid, at den ansatte i forbindelse med afsendelse af privat e-mail giver samtykke til GovCERT-behandlingen. Når det er op til myndighedens personalepolitik, om medarbejderne må sende eller modtage privat e-mail, må myndigheden således også kunne fastsætte, at medarbejderne kun må sende privat e-mail mod at samtykke til GovCERT-behandlingen. Det antages på den baggrund, at iværksættelsen af overvågningen af udgående e-mails med privat indhold ikke i sig selv vil udgøre et indgreb i rettighederne efter EMRK artikel 8.

For så vidt angår indgående private e-mails samt offentlige myndigheders indsamling, opbevaring og anvendelse mv. af personoplysninger vil der derimod være tale om et indgreb i borgernes ret til privatliv.

Da det som følge af den ovenfor beskrevne tekniske opbygning af GovCERT ikke kan udelukkes, at GovCERT vil behandle personoplysninger om en persons privatliv, må aktiviteterne anses for et indgreb i retten til respekt for privatlivet, jf. konventionens artikel 8, stk. 1.

Det følger herefter af konventionens artikel 8, stk. 2, at et sådant indgreb kun kan foretages, hvis det er foreskrevet ved lov og er nødvendigt i et demokratisk samfund til varetagelse af nærmere bestemte anerkendelsesværdige formål.

Med den foreslåede lov vil der blive klar lovhjemmel for GovCERT's aktiviteter, som bygger på en legitim og helt åbenlys samfundsmæssig interesse i at håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark.

Indgrebet i privatlivet skal herudover efter artikel 8, stk. 2, have et sagligt formål og være proportionalt.

GovCERT har til formål at mindske konsekvenserne af sikkerhedshændelser på internettet gennem analyse, information, varsling og koordination. GovCERT's aktiviteter tilsigter således at beskytte den nationale sikkerhed, den offentlige tryghed og landets økonomiske velfærd samt andres rettigheder og friheder. Formålet må således anses for sagligt.

IT- og Telestyrelsens rapport om varsling af internettrusler fra 2007 konkluderede, at der i Danmark er behov for en særskilt tjeneste til at håndtere sådanne sikkerhedshændelser for det danske samfund som et led i den nationale it-sikkerhedsstrategi. Den varslingsopgave mv., som er tiltænkt GovCERT, må således siges at være både egnet til og nødvendig for at nå det beskrevne saglige mål om at forhindre hacker- og virusangreb mv.

Der kan i den forbindelse også henvises til den nedenfor i afsnit 8.1 beskrevne meddelelse fra EU-Kommissionen og resolution fra Europarådet om, at oprettelsen af statslige it-beredskabsenheder (»GovCERT'er«) er en måde, hvorpå medlemsstaterne kan løse de notoriske trusler mod staternes it-sikkerhed.

Den samfundsmæssige interesse i at forhindre og håndtere sikkerhedshændelser af it-mæssig karakter for offentlige myndigheder i Danmark må således anses at overstige hensynet til privatlivet for de personer, om hvilke GovCERT behandler personoplysninger. Aktiviteterne er endvidere begrænset til de tilsluttede myndigheder og virksomheders ind- og udgående data.

GovCERT's formål er som nævnt ikke i sig selv at indsamle personoplysninger. Indsamlingen er i stedet en uundgåelig konsekvens af varslingsopgaven. GovCERT vil i øvrigt kun opbevare oplysningerne, så længe opbevaringen er nødvendig i forhold til varslingsopgaven.

Personoplysningerne vil derudover heller ikke blive offentliggjort; tværtimod er opbevaringen af oplysningerne underlagt strenge sikkerhedsforanstaltninger, så bl.a. offentliggørelse undgås.

Hertil kommer, at GovCERT efter lovforslagets § 7 i supplement til Datatilsynets kontrol vil blive underlagt kontrol af et uafhængigt tilsyn.

Sammenfattende er det opfattelsen, at den behandling af personoplysninger, som er en nødvendig del af GovCERT's aktiviteter, vil opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention."