Høringsnotat

København, den 6. februar 2019

Høringssvar over udkast til forslag til lov om Center for Cybersikkerhed. (Initiativer til styrkelse af cybersikkerheden).

(Sagsnr. 2018/006599).

Ved mail af 7. januar 2019 har Forsvarsministeriet anmodet om Amnesty Internationals eventuelle bemærkninger til ovennævnte udkast til ændring af lov om Center for Cybersikkerhed.

Generelle bemærkninger

Amnesty International er enig i den grundlæggende betragtning bag udkastet: At det er af afgørende betydning, at det danske samfund sikres en effektiv beskyttelse mod cyberangreb.

Men når man læser udkastet, efterlades man med et indtryk af, at de seneste ti-tolv års diskussioner om forholdet mellem borgernes sikkerhed og borgernes retssikkerhed – og hvordan vi sikrer, at borgernes retssikkerhed ikke kommer unødigt under pres - er gået ubemærket hen i Forsvarsministeriet, FE og Center for Cybersikkerhed.

Diskussionen om sikkerhed og retssikkerhed har fyldt meget – især i 2006-2008 i forbindelse med diskussioner om politiets beføjelser til at iværksætte aflytninger og overvågninger - og den retlige prøvelse af mistankekrav og nødvendighed.

I 2016 afgjorde EU-domstolen i en sag mod Sverige, at logningsdirektivet var i strid med retten til privatliv efter artikel 8 i Den Europæiske Menneskerettighedskonvention – og afgørelsen burde have ført til, at den danske regering havde ophævet den danske logningsbekendtgørelse (som påbyder danske internetudbydere at gemme trafikdata i et år) – hvilket som bekendt ikke skete og endnu ikke er sket.

Disse og mange andre diskussioner om afvejningen mellem sikkerhed på den ene side og retssikkerhed på den anden ses ikke at have sat sig nogen spor i det fremsendte udkast.

Tværtimod indeholder forslaget meget betydelige udvidelser af Center for Cybersikkerheds beføjelser, uden at der på nogen måde søges at indføre nogen former for uafhængig kontrol med Centeret, således at man kunne have talt om en balance mellem de betydeligt udvidede beføjelser og behovet for at beskytte myndighedernes, virksomhedernes og borgernes privatliv.

Det fremgår af bemærkningerne, at formålet med forslaget blandt andet er at få flere myndigheder og virksomheder til at indgå i Centerets netsikkerhedstjeneste. Hidtil har alene et fåtal af myndigheder og virksomheder ønsket at lade sig indrullere i Centerets netsikkerhedstjeneste, hvilket i bemærkningerne henføres til, at det har været for dyrt at deltage. Derfor skal det fremover være gratis at være omfattet af netsikkerhedstjenesten.

Det er dog, som om forslagsstillerne ikke selv tror på, at det er gebyret, som er grunden til, at især virksomheder har afholdt sig fra at slutte sig til netsikkerhedstjenesten. En af de vigtigste nyskabelser i forslaget er, at Centeret for Cybersikkerhed, hvis forslaget vedtages, kan *pålægge* myndigheder og virksomheder at slutte sig til netsikkerhedstjenesten. (Så vidt Amnesty har kunnet forstå på de seneste dages drøftelser i medierne, har kun to private virksomheder sluttet sig til netsikkerhedstjenesten under den hidtidige ordning.)

Det afgørende nye er, at hvor Center for Cybersikkerhed i dag kun monitorerer datatrafik på de forbindelser, der går ind og ud af de tilsluttede myndigheder og virksomheder, skaber lovforslaget mulighed for at installere sikkerhedssoftware på f.eks. pc'ere, servere, tablets, mobiltelefoner m.v. hos de myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten.

Som noget nyt er det meningen, at Centeret skal kunne installere sikkerhedssoftware, ikke bare i den ydre firewall, men også på den indre firewall, herunder servere og stationære pc'er hos den pågældende myndighed eller virksomhed. Efter forslaget skal også tablets og mobiltelefoner kunne tilsluttes.

Man må forstå, at de tilsluttede myndigheder og virksomheder vil blive underrettet, når der installeres sikkerhedssoftware, honey pots, sink holes osv. Men de medarbejdere, som arbejder med de pågældende netværk og pc'er, m.v. nævnes ikke. De skal ikke underrettes om, at deres færden bliver overvåget.

Man savner i det hele taget et overslag over de praktiske konsekvenser, over hvor mange myndigheder, virksomheder, netværk, pc'er eller brugere, der samlet set forventes at blive omfattet eller "ramt" af Center for Cybersikkerheds fremtidige udvidede adgang til transportdata, pakkedata og stationære data.

Som forslaget er formuleret, efterlader det – bevidst eller ikke bevidst – et billede af, at det blot er et hjørne af vores samfund, der undergives en tættere, ureguleret overvågning, hvor man reelt skulle anerkende, at der snarere er tale om, at vores samfund som sådant kan gå fra et niveau af ureguleret overvågning til et andet.

Særligt savnes en reel begrundelse for det gennemgående fravær af domstolskontrol med Centerets tilgang til oplysninger hos myndigheder og virksomheder.

Konkrete bemærkninger

Om indgreb omfattet af grundlovens § 72.

Udkastet indeholder en række bestemmelser – i udkastet til lovs kapitel 4 – indgreb omfattet af grundlovens § 72, hvor der er tale om at foretage indgreb i retten til privatliv – eller indgreb i brevhemmeligheden.

Af udkastet til § 4 fremgår, at Center for Cybersikkerhed skal kunne behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder *uden retskendelse* med henblik på at understøtte et højt informationssikkerhedsniveau.

Hvor det i dag alene er netværkskommunikation, Centeret kan behandle, vil Centeret fremover kunne behandle enkelte enheder (pc'ere) på lokale netværk, smartphones og tablets.

Det anføres videre i bemærkningerne, side 18, at *"Det bemærkes, at anvendelsen af sikkerhedssoftware – både med passiv og aktiv funktionalitet – vil indebære en udvidelse af Center for Cybersikkerheds muligheder for at foretage indgreb, der er omfattet af grundlovens § 72 om bl.a.*

undersøgelse af breve og andre papirer (elektroniske data) og brud på meddelelseshemmeligheden (kommunikation gennem email og anden internetkommunikation) med henblik på at imødegå sikkerhedshændelser. Efter grundlovens § 72 kan sådanne indgreb, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse."

Det fremgår videre af bemærkningerne, at forslaget betyder, at de data, som kunne udløse en sikkerhedsbegivenhed efter forslaget ikke blot er data, som bevæger sig mellem to forskellige virksomheder, men også kan være "private" data, der befinder sig lagret på en pc hos en medarbejder – som der derfor kan blive tale om at tilgå.

Det konkluderes i bemærkningerne, at en sådan tilgang til disse "private" data vil kunne udgøre et indgreb omfattet af grundlovens § 72, hvorfor der efter ministeriets opfattelse er behov for en udtrykkelig hjemmel.

Forsvarsministeriet har derfor overvejet, om der er behov for en ordning, hvor der sker forudgående indhentelse af retskendelse – men når side 18 frem til, at det vil være for besværligt, og at man derfor ikke bør indføre krav om en retskendelse – hverken forudgående eller efter den eventuelle sikkerhedshændelse:

"Indgrebet vil imidlertid som udgangspunkt ske automatiseret, når sikkerhedssoftwaren løbende scanner – og dermed tilgår – filer for at identificere eventuelle sikkerhedshændelser, og da indgrebet dermed netop sker ved scanning af ukendte data for at fastslå, om der er tale om sikkerhedshændelser, vil en domstolsprøvelse i givet fald 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, at der anvendes sikkerhedssoftware. ***Dette område vurderes på den baggrund ikke at være egnet til domstolsprøvelse."*** (Vores udhævning).

Denne argumentation for ikke at anvende domstolskontrol er efter Amnestys opfattelse bagvendt. Når en domstol skal tage stilling til, om der er tilstrækkeligt grundlag for at gennemføre en ransagning eller iværksætte en aflytning/overvågning, så sker det vel også ud fra en *samlet vurdering af "trusselsbilledet"*, og ikke ud fra en forventning om kvaliteten af de konkrete data, som forventes at komme frem ved ransagningen.

Forsvarsministeriet leverer ikke en holdbar argumentation for, hvordan det retfærdiggøres, at det, som ministeriet *selv* kalder et indgreb omfattet af grundlovens § 72, ikke i fremtiden skal kræve domstolskontrol.

Endelig skal det bemærkes, at de retlige kriterier for at tilgå disse data er ganske løst formulerede – idet det eneste krav er, at behandlingen sker for at understøtte "*et højt informationssikkerhedsniveau i samfundet."*

Om forslag til ny § 5.

Efter forslaget til § 5 skal Centeret – ved **begrundet mistanke** om en sikkerhedshændelse – kunne behandle stationære data (dvs. data, som er lagret i netværk og pc'er *i virksomheden eller hos myndigheden)* fra en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten – ***uden retskendelse*** – når myndigheden/virksomheden har anmodet Centeret om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen – **og** behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Også for § 5 anerkender Forsvarsministeriet, at bestemmelsen isoleret omhandler situationer/indgreb, der er omfattet af grundlovens § 72 – og at der derfor er behov for positiv lovhjemmel til at foretage de pågældende indgreb.

Særligt i en situation hvor der efter ministeriets opfattelse kan være tale om myndigheder eller virksomheder med så mange ansatte, at det reelt ikke er muligt at indhente samtykke fra alle berørte medarbejdere, er det nødvendigt – konkluderer ministeriet - at der tilvejebringes hjemmel til at foretage indgreb omfattet af grundlovens § 72.

Det anføres i bemærkningerne, side 22:

"De sikkerhedstekniske undersøgelser er aktiviteter, der til en vis grad kan sammenlignes med de mange områder, hvor offentlige myndigheder foretager stikprøvekontroller, og hvor det ikke sker efter forudgående retskendelse, idet en domstolsprøvelse ikke vil være meningsfuld, når der er tale om stikprøver. Når der samtidig henses til, at undersøgelsen foretages på baggrund af et samtykke fra myndigheden eller virksomheden selv – og ***at det således er vanskeligt at opstille et retligt kriterium, som domstolene vil kunne påse overholdelsen af – bør undersøgelsen kunne foretages uden retskendelse."***
(Vores udhævning)

Efter Amnestys opfattelse er Forsvarsministeriets argumentation for ikke at kræve domstolskontrol med indgreb, som åbenbart vil være omfattet af grundlovens § 72 også her nærmest bagvendt.

For det første kan man ikke sammenligne med stikprøvekontroller i fødevareindustrien og andre brancher, hvor stikprøvekontrol skal sikre en forsvarlig kvalitet. De varer, som kontrolleres i fødevareindustrien – og ikke lever op til den krævede standard - er ikke omfattet af retten til privatliv eller brevhemmeligheden. Videre kan man ikke læne sig tilbage og sige, at alt er godt, når blot man har samtykke fra myndighedens eller virksomhedens ledelse. Det ændrer ikke på, at det vil være et indgreb omfattet af grundlovens § 72 over for medarbejderne, når Centeret går ind og undersøger samtlige medarbejderes pc'er, smartphones, tablet etc.

Endelig kortsluttes ræsonnementet i forhold til domstolskontrollens formål, når ministeriet konstaterer, at når det **"således er vanskeligt at opstille et retligt kriterium, som domstolene vil kunne påse overholdelsen af – bør undersøgelsen kunne foretages uden retskendelse."**
(Vores udhævning).

Efter Amnestys opfattelse må svaret være, at hvis man ikke kan opstille et retligt kriterium, som skal være opfyldt, for at Centeret kan gå ind og kontrollere en given myndighed eller virksomhed, (og som kan efterprøves af en domstol) så bør Centeret afholde sig fra - eller ikke have myndighed til at foretage sådanne handlinger.

Også her er kravet om, at behandlingen skal vurderes at bidrage til at understøtte et højt informationssikkerhedsniveau et nærmest tomt kriterium.

Om forslag til § 6

Også i forhold til de beføjelser, som Center for Cybersikkerhed får til at behandle trafikdata, pakkedata og stationære data hidrørende fra de tilsluttede myndigheder og virksomheder – uden retskendelse - må man efterlyse en retlig konstruktion, hvorefter Centeret ville være undergivet uafhængig kontrol – domstolskontrol. Som udkastet er formuleret, vil Centeret kunne tilgå en lang række personlige og rent private data om borgerne, der ikke har saglig relevans for sikkerhedshændelse.

Om forslag til § 17, opbevaringstid

Det fremgår af § 17, stk. 1, at data, der er omfattet af kapitel 4 – om indgreb, der er omfattet af grundlovens § 72 – skal slettes, når formålet med behandlingen er opfyldt, eller efter højst 5 år, uanset om formålet er opfyldt.

Data, som ikke hidrører fra en sikkerhedshændelse, men fra bestemte myndigheder, som særligt beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold – og virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, må højst opbevares i 3 år. Er data i medfør af § 16 videregivet til andre end den myndighed eller virksomhed, som de pågældende data hidrører fra, finder stk. 1 og 2 ikke anvendelse.

Dét forstår Amnesty International således, at der ikke gælder nogen længste frist for sletning af data, der er videregivet til andre myndigheder eller virksomheder end den, som de pågældende data hidrører fra.

Det er ikke indlysende, hvorfor man skal kunne gemme data, som ikke hidrører fra en sikkerhedshændelse, i 3 år, eller hvorfor slettefristen efter denne lov helt ophæves, hvis data gives videre til andre myndigheder eller virksomheder end dem, som oplysningerne stammer fra.

En generel slettefrist på 5 år forekommer også at være unødigt og uønskeligt lang, når man betænker fraværet af uafhængig retlig kontrol med Center for Cybersikkerhed.

Amnesty International, 6. februar 2019.