Utlåtande GrUU 62/2024 rd─ RP 57/2024 rd

Grundlagsutskottet

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet)

Till kommunikationsutskottet

INLEDNING

Remiss

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) (RP 57/2024 rd): Ärendet har remitterats till grundlagsutskottet för utlåtande till kommunikationsutskottet.

Sakkunniga

Utskottet har hört
- regeringssekreterare Veikko Vauhkonen, kommunikationsministeriet
- lagstiftningsråd Eeva Lantto, finansministeriet
- dataadministrationschef Ari Apilo, riksdagen
- professor Olli Mäenpää
- professor Tuomas Ojanen
- professor Janne Salminen
- professor Veli-Pekka Viljanen.

Skriftligt yttrande har lämnats av
- biträdande professor Anu Mutanen
- professor Tomi Voutilainen.

PROPOSITIONEN

Regeringen föreslår att det stiftas en lag om hantering av cybersäkerhetsrisker. Dessutom föreslås det i propositionen att lagen om informationshantering inom den offentliga förvaltningen och 15 andra lagar ändras.

Lagarna avsågs träda i kraft den 18 oktober 2024.

I propositionen ingår ett avsnitt om lagförslagens förhållande till grundlagen samt lagstiftningsordning. Enligt regeringens uppfattning kan lagförslagen behandlas i vanlig

lagstiftningsordning. Regeringen anser det dock önskvärt att grundlagsutskottet lämnar utlåtande i ärendet.

UTSKOTTETS ÖVERVÄGANDEN

Utgångspunkter för bedömningen

(1) I propositionen föreslås det att det stiftas en lag om hantering av cybersäkerhetsrisker (lagförslag 1). Dessutom föreslås det att lagen om informationshantering inom den offentliga förvaltningen (lagförslag 2) och 15 andra lagar ändras. Genom de föreslagna lagarna genomförs EU:s cybersäkerhetsdirektiv (Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (nedan även NIS 2-direktivet. Målet med direktivet är att stärka EU:s gemensamma och medlemsstaternas nationella cybersäkerhetsnivå i fråga om sektorer och aktörer som anses vara kritiska för samhällets funktion.

(2) I propositionen ingår ett tämligen omfattande avsnitt om lagförslagens förhållande till grundlagen och lagstiftningsordning.

Myndigheternas rätt att få information

(3) Enligt 28 § i lagförslag 1 har tillsynsmyndigheten trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få förmedlingsuppgifter, lokaliseringsuppgifter och information om meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapporteringen av betydande incidenter. I 18 § i lagförslag 2 föreslås motsvarande bestämmelser om myndigheternas rätt att få uppgifter.

(4) I motiven granskas lagförslaget framför allt med tanke på skyddet för hemlighet i fråga om förtroliga meddelanden enligt 10 § i grundlagen. Enligt 10 § 2 mom. i grundlagen är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Enligt 10 § 4 mom. kan det genom lag föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

(5) Regleringen i grundlagen när det gäller förtroliga meddelanden motiveras främst av behovet att skydda innehållet i ett förtroligt meddelande gentemot utomstående. Genom grundlagen tillförsäkras var och en rätt till konfidentiell kommunikation utan att utomstående får information om innehållet i konfidentiella meddelanden som han eller hon skickar eller tar emot. Bestämmelsen tryggar dock också andra uppgifter om ett sådant meddelande som kan vara av betydelse för att meddelandet ska förbli konfidentiellt. Exempel på dylik information är enligt

förarbetena till reformen av de grundläggande fri- och rättigheterna ett samtals identifieringsuppgifter (RP 309/1993 rd, s. 57).

(6) Var och en har enligt artikel 8 i Europakonventionen rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Enligt artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt Europadomstolens rättspraxis omfattar begreppen privatliv och korrespondens i artikel 8.1 i konventionen såväl telefonkommunikation som e-postkommunikation och annan elektronisk kommunikation som är avsedd att vara förtrolig (Liberty m.fl. mot Förenade kungariket 1.10.2008). Enligt denna rättspraxis omfattar skyddet för korrespondens och privatliv både innehållet i kommunikationen och identifieringsuppgifter om kommunikationen (Malone mot Förenade kungariket 2.8.1984). En myndighet behöver inte i praktiken behandla uppgifterna för att det ska vara fråga om ingripande i privatlivet, utan redan det att myndigheten samlar in och lagrar uppgifter för senare användning ska betraktas som ingripande (S. och Marper mot Förenade kungariket, 4.12.2008, punkt 85). Enbart det att sådan lagstiftning existerar som gör det möjligt att hemligt observera kommunikationsförbindelser ingriper i de rättigheter som artikel 8 i Europakonventionen garanterar parterna i kommunikationen och även potentiella parter (Klass mot Tyskland, 6.9.1978 samt Liberty m.fl. mot Förenade kungariket, 1.10.2008; se även GrUU 36/2018 rd, s. 7—10).

(7) Den rätt att få uppgifter som nu föreslås sträcker sig till förmedlingsuppgifter, lokaliseringsuppgifter och uppgifter om meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando. I propositionen (s. 255) bedöms det att ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando och som skapats för att genomföra ett cyberattack inte är ett sådant förtroligt meddelande som avses i 10 § 2 mom. i grundlagen.

(8) Grundlagsutskottet har bedömt frågan om omfattningen av skyddet för konfidentiella kommunikationshemligheter i olika sammanhang. Utskottet har bland annat konstaterat att postpaket som innehåller varor i princip inte i sig kan betraktas som förtroliga meddelanden enligt grundlagen (GrUU 28/2000 rd, s. 3/II, GrUU 59/2006 rd). Inte heller bestämmelserna om öppnande av ett slutet brev för att reda ut mottagaren eller avsändaren innebar en sådan begränsning i hemligheten i fråga om ett förtroligt meddelande som finns uppräknad bland de tillåtna begränsningarna i nuvarande 10 § 4 mom. i grundlagen (GrUU 30/2001 rd).

(9) Grundlagsutskottet har ansett att fjärrstyrningen av obemannade luftfartyg exempelvis med hjälp av mobiltelefon eller dator inte handlar om sådana förtroliga meddelanden som avses i 10 § 2 mom. i grundlagen och som man genom bestämmelsen i grundlagen över huvud taget har för avsikt att ge grundlagens skydd (GrUU 22/2020 rd). Även om personer i och för sig också kan förmedla förtroliga meddelanden mellan sig i den kommunikationen, anser utskottet att det med hänsyn till verksamhetens karaktär och medvetenheten om att meddelandena lagras trots allt inte är fråga om en sådan handling som omfattas av det skydd grundlagens 10 § ger förtroliga meddelanden (GrUU 62/2010 rd, s. 5). Också Gränsbevakningsväsendets radiotekniska övervakning bedömdes delvis gälla sådan telekommunikation som inte omfattas av hemligheten i fråga om förtroliga meddelanden enligt 10 § 2 mom. i grundlagen (GrUU 15/2024 rd, stycke 9).

(10) I propositionen (s. 253) konstateras det att ett meddelande som innehåller ett skadligt datorprogram eller kommando ofta har genererats automatiskt av ett skadligt datorprogram och det inte har sänts av en fysisk person utan av ett skadligt program eller den som programmerat det. I ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando är det ofta fråga om ett tekniskt program eller kommando som är avsett att skada kommunikationsnätets eller informationssystemets funktion. Det kan röra sig om en automatiserad och teknisk åtgärd mellan datorsystem där ingen fysisk person är part eller där det utöver de tekniska egenskaperna inte finns något semantiskt innehåll. Ett meddelande som innehåller ett skadligt datorprogram eller kommando är enligt propositionsmotiven inte ett sådant meddelande mellan kommunikationsparter som traditionellt hör till kärnan i skyddet för förtrolig kommunikation och som har identifierad semantisk eller kommunikativ betydelse för parterna.

(11) Utifrån propositionsmotiven är det alltså inte fråga om kommunikation mellan två parter, utan snarare om verksamhet som allvarligt äventyrar de förtroliga meddelanden som skyddas av 10 § 2 mom. i grundlagen när den orsakar skada för kommunikationsnätets eller informationssystemets funktion. Sådan kommunikation omfattas inte av 10 § 2 mom. i grundlagen, eftersom det saknas ett sådant innehåll som uppkommer mellan fysiska personer som kan betraktas som parter i en kommunikation.

(12) Grundlagsutskottet noterar dessutom med anledning av propositionens motiv till lagstiftningsordningen att sådana i lagförslagen avsedda meddelanden som innehåller ett skadligt datorprogram eller kommando helt faller utanför tillämpningsområdet för hemligheten för förtroliga meddelanden i 10 § i grundlagen. Det är alltså inte bara fråga om en sådan omständighet som det hänvisas till i motiveringen till lagstiftningsordningen, det vill säga att ett sådant meddelande inte omfattas av kärnområdet i den rättighet som gäller sekretess i fråga om förtroliga meddelanden. Ett sådant meddelande åtnjuter inte skydd enligt 10 § 2 mom. i grundlagen, och bestämmelser om detta behöver inte bedömas utifrån de särskilda eller allmänna förutsättningarna för inskränkning av de grundläggande fri- och rättigheterna enligt 10 § 4 mom.

(13) Rätten att få information enligt 28 § i lagförslag 1 och 18 i § i lagförslag 2 gäller dock också förmedlingsuppgifter och lokaliseringsuppgifter. Grundlagsutskottet har i sin praxis ansett att behandlingen av lokaliseringsuppgifter anknyter till det skydd för privatlivet som tryggas i 10 § i grundlagen och vars utgångspunkt är individens rätt att leva sitt eget liv utan godtycklig eller ogrundad inblandning av myndigheter eller andra utomstående (GrUU 36/2002 rd, s. 5, GrUU 9/2004 rd, s. 5/I, GrUU 16/2018 rd, s. 4). Dessutom har bestämmelserna om utredning av lokaliseringsuppgifter samband också med den rörelsefrihet som tryggas i 9 § i grundlagen. (GrUU 36/2002 rd, s. 5/II, GrUU 9/2004 rd, s. 5/I, GrUU 16/2018 rd, s. 4).

(14) Förmedlingsuppgifterna omfattas å sin sida av skyddet för hemligheten i fråga om förtroliga meddelanden i 10 § 2 mom. i grundlagen (RP 309/1993 rd, s. 57/II). Med avseende på den nu aktuella regleringen är det dock relevant att identifieringsuppgifterna för ett meddelande i grundlagsutskottets tidigare etablerade praxis har ansetts ligga utanför kärnområdet för den grundläggande fri- och rättighet som skyddar hemligheten i fråga om förtroliga meddelanden (se t.ex. GrUU 33/2013 rd, s. 3/I—II, GrUU 6/2012 rd, s. 3—4, GrUU 29/2008 rd, s. 2—3 och GrUU 3/2008 rd, s. 2/I). Detta har inneburit att det särskilda lagförbehållet som numera ingår i 10 § 4 mom. i grundlagen inte som sådant har tillämpats på begränsning av hemligheten när det gäller

identifieringsuppgifter. Bestämmelser som inkräktar på skyddet för identifieringsuppgifter har dock enligt utskottets praxis behövt uppfylla de allmänna kriterierna för begränsning av grundläggande fri- och rättigheter (GrUU 62/2010 rd, s. 4/II, GrUU 23/2006 rd, s. 2—3). Således har det till exempel varit möjligt att föreskriva om befogenheter för teleövervakning också i en situation där det inte nödvändigtvis har varit fråga om brott som äventyrar individens eller samhällets säkerhet eller hemfriden enligt 10 § 4 mom. i grundlagen (GrUU 33/2013 rd, s. 3/I). Det har ansetts möjligt att få identifieringsuppgifter också i vissa situationer där det inte har varit fråga om begränsningsgrunder enligt 10 § 4 mom. i grundlagen (GrUU 62/2010 rd, s. 4/II).

(15) Grundlagsutskottet har sedan dess justerat sin praxis, eftersom identifieringsuppgifter som anknyter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6/II). Grundlagsutskottet har i sin senaste praxis ansett att regleringen om Gränsbevakningsväsendets radiotekniska övervakning i den då föreslagna omfattningen, särskilt med beaktande av de begränsningar som i lagen föreslås för tillsynen, framstår som ett relativt obetydligt ingrepp i skyddet av hemligheten i fråga om förtroliga meddelanden. Utskottet bedömde då bestämmelserna utifrån de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna (GrUU 15/2024 rd, stycke 12 och 13).

(16) I den reglering som nu föreslås är rätten att få information om förmedlingsuppgifter mycket begränsad. Myndigheten har rätt att få information, om det är nödvändigt för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapporteringen av betydande incidenter. Syftet med rätten att få information har att göra med tryggandet av en störningsfri kommunikation och säkerställandet av kommunikationsnätens funktion och säkerhet (se även GrUU 9/2004 rd, s. 4). Grundlagsutskottet anser att regleringen om rätten att få uppgifter om förmedlingsuppgifter i det nu aktuella regleringssammanhanget utgör ett relativt litet ingrepp i skyddet av hemligheten för förtroliga meddelanden. Den nu föreslagna regleringen om behandling av förmedlingsuppgifter måste bedömas utifrån de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. Regleringen är inte problematisk ur denna synvinkel.

(17) Grundlagsutskottet noterar dessutom att det i samband med ändringen av 10 § i grundlagen har ansett det motiverat att regeringen inleder ett utredningsarbete som i vidare bemärkelse täcker behovet av att ändra de begränsningsklausuler som gäller hemfriden och hemligheten i fråga om förtroliga meddelanden i grundlagen (GrUB 4/2018 rd, s. 6). Utskottet har senare påskyndat inledandet av utredningsarbetet (GrUU 6/2019 rd, s. 5, GrUU 12/2019 rd, s. 6). Utskottet upprepar med eftertryck att det är nödvändigt att utreda behovet av ändringar i begränsningsklausulerna i 10 § i grundlagen (se GrUU 5/2023 rd, stycke 9, GrUU 15/2024 rd, stycke 14, GrUU 47/2024 rd, stycke 13). Ändringsbehoven bör bedömas bland annat med beaktande av nya former av grov brottslighet (GrUU 5/2023 rd, stycke 9) och den tekniska utvecklingen (GrUU 30/2010 rd, s. 5/II—6/I).

Tillämpningsområdet

(18) Enligt propositionsmotiven (s. 273) är utgångspunkten i det föreslagna 3 § 1 mom. i lagförslag 2 (informationshanteringslagen) att lagen, inklusive den föreslagna regleringen i 4 a kap. som grundar sig på NIS2-direktivet, ska tillämpas på de myndigheter som avses i 4 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen), det vill säga också på riksdagens ämbetsverk samt på justitiekanslern i statsrådet och riksdagens justitieombudsman. Enligt propositionsmotiven (s. 273) ska informationshanteringslagens 4 a kap. tillämpas på riksdagens ämbetsverk på det sätt som framgår av 4 § 1 mom. 6 punkten i offentlighetslagen och dess motivering, eftersom begreppet ”parlament” i artikel 6.35 i direktivet syftar på folkrepresentationen, i Finland riksdagen och riksdagsarbetet.

(19) I det kapitlet i informationshanteringslagen föreslås bestämmelser om skyldigheter som gäller cybersäkerhet och tillsynen över att de fullgörs. Den tillsynsmyndighet som avses i detta kapitel är Transport- och kommunikationsverket, som är ett ämbetsverk inom centralförvaltningen inom kommunikationsministeriets förvaltningsområde och som sköter myndighetsuppgifter inom transport och elektronisk kommunikation. Enligt 4 a kap. i lagförslag 2 har tillsynsmyndigheten relativt långtgående befogenheter, till exempel rätt att få information, rätt att förrätta inspektioner och påföra påföljder.

(20) Enligt grundlagsutskottets uppfattning faller bland annat parlament utanför NIS 2-direktivets begrepp offentlig förvaltningsentitet, enligt en uttrycklig bestämmelse i direktivet (artikel 6.35). I propositionen (s. 214) har avgränsningen tolkats snävt så att den endast gäller riksdagsarbetet, det vill säga närmast plenum och utskotten. På grund av det nämnda tillämpningsområdet i fråga om riksdagens ämbetsverk hör riksdagens kansli till tillämpningsområdet för den lag som utfärdas för genomförande av direktivet.

(21) Enligt grundlagsutskottet finns det i sig inget hinder för att de allmänna förvaltningslagarna utvidgas till att gälla riksdagens ämbetsverk (GrUU 14/2018 rd, s. 11, se även GrUU 43/1998 rd, s. 6/II). Att ta in riksdagens ämbetsverk i tillämpningsområdet för 4 a kap. i lagförslag 2 skulle dock innebära att de tillsynsbefogenheter som i lagförslaget beviljas förvaltningsmyndigheter inom kommunikationsministeriets förvaltningsområde i stor utsträckning också skulle gälla riksdagen i dess helhet.

(22) Enligt 74 § i riksdagens arbetsordning ska riksdagens kansli skapa förutsättningar för riksdagen att fullgöra sina uppgifter som statsorgan. Enligt grundlagsutskottets uppfattning utgår propositionen från att riksdagsarbetet och myndighetsverksamheten vid riksdagens kansli kan särskiljas från varandra också i detta sammanhang. Enligt utredning till utskottet är en sådan åtskillnad dock inte möjlig. I riksdagens kanslis datasystem behandlas uppgifter som huvudsakligen hänför sig till riksdagsarbetet.

(23) Grundlagsutskottet anser att det konstitutionellt är problematiskt att särskilt riksdagens kansli i sin helhet tas in i lagens tillämpningsområde. Riksdagens kansli är en fast del av riksdagens organisation och kan inte avskiljas från riksdagens verksamhet som högsta statsorgan. Motsvarande synpunkter i anslutning till riksdagens verksamhet kan också framföras i fråga om riksdagens övriga ämbetsverk. Till exempel enligt 90 § 2 mom. i grundlagen finns det i

anknytning till riksdagen ett oavhängigt revisionsverk för revisionen av statsfinanserna och iakttagandet av statsbudgeten.

(24) Grundlagsutskottet har tidigare ansett att det med tanke på 2 § i grundlagen vore problematiskt med reglering som innebär att riksdagens ämbetsverks informationshantering skulle styras av finansministeriet. Det var enligt utskottet i sista hand fråga om en institutionell lösning som går tillbaka till 2 § i grundlagen. Den utgör en av grundbultarna i vårt statsskick, nämligen att det görs åtskillnad mellan det högsta statsorganet riksdagen, som utövar den lagstiftande makten och fattar beslut om statsfinanserna, och statsrådet, som utövar regeringsmakten. Enligt utskottets mening skulle det klart strida mot denna grundprincip om informationsförvaltningen vid riksdagens ämbetsverk styrdes av finansministeriet. Det betydde att lagen kunde stiftas i vanlig lagstiftningsordning bara om riksdagens ämbetsverk och inrättningar ströks ur lagförslagets tillämpningsområde (GrUU 46/2010 rd, s. 5).

(25) Grundlagsutskottet anser att det nu aktuella lagförslaget måste bedömas på liknande grunder som hänför sig till riksdagens ställning som högsta statsorgan. Förslaget är inte förenligt med riksdagens ställning som högsta statsorgan (se även GrUU 14/2018 rd, s. 10—11).

(26) Enligt grundlagsutskottets uppfattning förutsätter direktivet inte ett sådant tillämpningsområde som nu föreslås och som alltså också skulle omfatta riksdagens ämbetsverk. Utskottet anser att propositionens snäva tolkning av direktivets begrepp parlament inte är förenlig med de aspekter som hänför sig till riksdagens konstitutionella ställning. Lagförslag 2 i propositionen måste ändras så att 4 a kap. i informationshanteringslagen inte tillämpas på riksdagens ämbetsverk. Det är ett villkor för att lagförslag 2 ska kunna behandlas i vanlig lagstiftningsordning.

FÖRSLAG TILL BESLUT

Grundlagsutskottet föreslår

> *att lagförslagen kan behandlas i vanlig lagstiftningsordning, men lagförslag 2 bara om utskottets konstitutionella anmärkningar till tillämpningsområdet för dess 4 a kap. beaktas på behörigt sätt.*

Utlåtande GrUU 62/2024 rd

Helsingfors 12.12.2024

I den avgörande behandlingen deltog

ordförande Heikki Vestman saml
medlem Hannu Hoskonen cent
medlem Atte Kaleva saml
medlem Teemu Keskisarja saf
medlem Johannes Koskinen sd
medlem Jarmo Lindberg saml
medlem Mira Nieminen saf
medlem Johanna Ojala-Niemelä sd
medlem Karoliina Partanen saml
medlem Onni Rostila saf
medlem Ville Skinnari sd
medlem Paula Werning sd
medlem Johannes Yrttiaho vänst.

Sekreterare var

utskottsråd Mikael Koillinen
utskottsråd Liisa Vanhala.