**Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta**

## ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi Suomen perustuslain sääntelyä luottamuksellisen viestin salaisuuden suojasta.

Perustuslakiin ehdotetaan lisättäväksi uusi säännös, johon koottaisiin luottamuksellisen viestin salaisuuden rajoittamista koskeva sääntely. Perustuslaissa ehdotetaan säädettäväksi, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Ehdotettu laki on tarkoitettu tulemaan voimaan mahdollisimman pian sen säätämisjärjestys huomioon ottaen.

_____

**SISÄLLYS**

## YLEISPERUSTELUT

### 1 Johdanto

Suomen perustuslaki tuli voimaan 1 päivänä maaliskuuta 2000. Perusoikeussäännökset otettiin uudistuksessa perustuslakiin asiallisesti sellaisina kuin ne sisältyivät Suomen Hallitusmuodon II lukuun 1.8.1995 voimaan tulleen perusoikeusuudistuksen mukaisina (L 969/1995).

Perustuslain oikeudellisen aseman ja merkityksen vuoksi sen muuttamiseen on syytä suhtautua pidättyvästi. Erityisen suurta pidättyvyyttä on syytä noudattaa harkittaessa perusoikeuksia koskevan sääntelyn tai valtiollisen järjestelmän kannalta keskeisten toimintasääntöjen tarkistamista. Perustuslain muuttamista koskevien ehdotusten tulee perustua tarpeisiin, joiden olemassaolosta vallitsee laaja yhteisymmärrys. On toisaalta pidettävä huolta siitä, että perustuslaki antaa oikean kuvan valtiollisen vallankäytön järjestelmästä ja yksilön oikeusaseman perusteista.

Pääministeri Juha Sipilän hallituksen ohjelman mukaan hallitus esittää säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle (VNT 1/2015 vp, s. 33). Tarvetta tiedustelua koskevan lainsäädännön valmistelulle oli selvitetty puolustusministeriön asettamassa tiedonhankintalakityöryhmässä (Suomalaisen tiedustelulainsäädännön suuntaviivoja, tiedonhankintalakityöryhmän mietintö, puolustusministeriö, 2015). Tiedonhankintalakityöryhmä arvioi, ettei tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, ehkä lukuun ottamatta pelkästään vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua. Hallitus päätti strategiakokouksessaan 20.8.2015, että sisäministeriö ja puolustusministeriö käynnistävät siviili- ja sotilastiedustelua koskevan lainsäädännön valmistelun. Lisäksi oikeusministeriön tuli ryhtyä toimenpiteisiin luottamuksellisen viestin salaisuuden suojaa koskevan perustuslakisääntelyn tarkistamiseksi.

Puolustusministeriön ja sisäministeriön 1.10.2015 asettamat työryhmät julkaisivat mietintönsä 19.4.2017 (Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi, työryhmän mietintö, puolustusministeriö, 2017; Siviilitiedustelulainsäädäntö, siviilitiedustelulakityöryhmän mietintö, sisäministeriön julkaisu 8/2017). Sisäministeriössä on valmisteltu työryhmän mietinnön pohjalta virkatyönä hallituksen esitys laiksi poliisilain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi. Puolustusministeriössä on vastaavasti valmisteltu hallituksen esitys laiksi sotilastiedustelusta.

Oikeusministeriö asetti 17.10.2016 työryhmän valmistelemaan lainsäädäntöä siviili- ja sotilasviranomaisten tiedustelutoiminnan valvonnan järjestämiseksi. Eduskunnan pääsihteeri asetti 23.12.2016 eduskunnan kanslian sisäisen työryhmän valmistelemaan tiedustelutoiminnan parlamentaarista valvontaa koskevan sääntelyn. Oikeusministeriö tarkisti 9.2.2017 oman työryhmänsä asettamispäätöstä siten, että työryhmän tehtävä rajattiin tiedustelutoiminnan laillisuusvalvontaa koskevan sääntelyn valmisteluun. Oikeusministeriön työryhmä julkaisi mietintönsä 19.4.2017 (Tiedustelutoiminnan valvonta. Työryhmän mietintö, oikeusministeriö, mietintöjä ja lausuntoja 18/2017) ja eduskunnan kanslian työryhmä 29.5.2017 (Tiedustelun parlamentaarinen valvonta — työryhmän mietintö, eduskunnan kanslian julkaisu 1/2017). Oikeusministeriön ja eduskunnan kanslian työryhmän ehdotukset sovitettiin jatkovalmistelussa yhteen. Oikeusministeriössä on tältä pohjalta valmisteltu hallituksen esitys laiksi tiedustelutoiminnan valvonnasta. Lisäksi tiedustelutoiminnan parlamentaarisen valvonnan järjestämiseksi eduskunnan kansliassa on valmisteltu puhemiesneuvoston ehdotus eduskunnan työjärjestyksen (40/2000) muuttamisesta.

Siviili- ja sotilastiedustelun ja sen valvonnan lainsäädäntöä on näin ollen valmisteltu samaan aikaan tämän perustuslain tarkistamista koskevan esityksen kanssa. Uuden tiedustelulainsäädännön voimaan tullessa siviili- ja sotilasviranomaiset saisivat uusia merkittäviä tiedustelutehtäviä ja -toimivaltuuksia. Kyse tulisi olemaan uudesta lainsäädännöstä, jolla olisi merkittäviä vaikutuksia perus- ja ihmisoikeutena turvattuun yksityiselämän suojaan ja erityisesti luottamuksellisen viestin salaisuuden suojaan.

Oikeusministeriön 28.9.2015 asettaman asiantuntijatyöryhmän tehtävänä oli selvittää ja valmistella perustuslain tarkistamista siten, että lailla voidaan tarpeellisiksi katsottavien edellytysten täyttyessä säätää kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan. Valmistelussa tuli ottaa huomioon Suomen kansainväliset ihmisoikeusvelvoitteet.

Työryhmä arvioi 11.10.2016 julkaistussa mietinnössään, ettei perustuslain sanamuodon ja sen nykyisen tulkintakäytännön valossa ole mahdollista säätää sellaisista rajoituksista luottamuksellisen viestin salaisuuteen, joiden tarkoituksena olisi laajemmalti kansallisen turvallisuuden kannalta välttämättömän tiedon hankkiminen vakavista uhkista erityisesti uhkiin varautumiseksi ja niiden ennakoimiseksi sekä valtion ylimmän johdon päätöksenteon tueksi. Perustuslain sanamuoto ei mahdollista luottamuksellisen viestin salaisuuden suojaan puuttumista tiedon hankkimiseksi esimerkiksi sellaisesta kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily, tai jota ei ole säädetty rangaistavaksi.

Työryhmä arvioi tarpeelliseksi lisätä perustuslakiin uusia hyväksyttäviä perusteita rajoittaa luottamuksellisen viestin salaisuutta. Työryhmä ehdotti, että perustuslain 10 §:ään lisättäisiin uusi 4 momentti seuraavasti: ”Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.” (Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen, oikeusministeriö, mietintöjä ja lausuntoja 41/2016.)

Oikeusministeriön, puolustusministeriön ja sisäministeriön työryhmät työskentelivät 11.12.2015 asetetun parlamentaarisen seurantaryhmän seurannassa. Seurantaryhmän toimikautta pidennettiin 4.5.2017 tehdyllä päätöksellä tiedustelulainsäädännön ja perustuslain tarkistamisen jatkovalmistelua varten.

## 2 Nykytila

### 2.1 Lainsäädäntö ja käytäntö

#### 2.1.1 Yksityiselämän suoja

Luottamuksellisen viestin salaisuuden suoja on osa yksityiselämän suojaa. Jokaisen yksityiselämä on perustuslain 10 §:n mukaan turvattu. Yksityiselämän käsite voidaan ymmärtää henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi. Yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. (HE 309/1993 vp, s. 52—53.)

Yksityiselämän suojan takaamiseksi valtiolta on perinteisesti edellytetty sen ohella, että se itse pidättäytyy loukkaamasta kansalaisten yksityiselämää, myös aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisten yksilöiden loukkauksia vastaan. Yksityiselämän suojaa koskeva säännös yhdessä perusoikeuksien turvaamista koskevan perustuslain 22 §:n kanssa edellyttää lainsäätäjän ylläpitävän tehokasta perustuslain 10 §:ssä turvattujen oikeushyvien suojaa. (HE 309/1993 vp, s. 53.)

Henkilötietojen suojasta säädetään perustuslain 10 §:n 1 momentin mukaan tarkemmin lailla. Perustuslakivaliokunnan käytännön mukaan lainsäätäjän liikkuma-alaa rajoittaa tämän säännöksen lisäksi se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuuden kannalta.

Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on perustuslain 10 §:n 2 momentin mukaan loukkaamaton. Lailla voidaan saman pykälän 3 momentin mukaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

Pykälä sai nykyisen sisältönsä perusoikeusuudistuksessa (hallitusmuodon 8 §), ja se otettiin vuoden 2000 perustuslakiuudistuksen yhteydessä muuttamattomana perustuslain 10 §:ksi.

### 2.1.2 Luottamuksellisen viestin salaisuuden suoja

Säännös luottamuksellisen viestin salaisuudesta perustuslain 10 §:n 2 momentissa on välineja tekniikkaneutraali. Kirje- ja puhelinsalaisuus on mainittu erikseen, mutta säännöksellä turvataan yleisesti kaikenlaisen luottamuksellisen viestinnän salaisuutta.

Luottamuksellisen viestin salaisuutta koskevan perustuslakisääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Perustuslailla turvataan jokaiselle oikeus luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tietoa hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Säännös antaa kuitenkin turvaa muillekin tällaista viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Tyypillisesti tällaisia ovat esimerkiksi puhelujen tunnistamistiedot. (HE 309/1993 vp, s. 53—54.)

Luottamuksellisen viestin suoja merkitsee suojaa esimerkiksi kirjeiden ja muiden suljettujen viestien avaamista ja hävittämistä sekä puhelujen kuuntelemista ja nauhoittamista vastaan. Sääntelyllä ei suojata ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus (HE 309/1993 vp, s. 53).

Viestintä ammattitoiminnassa voi toiminnan luonteen ja viestinnän osapuolten viestien taltiointia koskevan tietoisuuden vuoksi jäädä luottamuksellisen viestin salaisuuden suojan ulkopuolelle, vaikka tällaisessa viestinnässä voitaisiinkin sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä. Perustuslakivaliokunta arvioi esimerkiksi turvallisuustutkintalakiehdotuksen käsittelyn yhteydessä, että liikenteen ohjauksessa syntyvä puhe- ja viestiliikenne ei ole perustuslain 10 §:ssä tarkoitetun luottamuksellisen viestin salaisuuden piiriin kuuluvaa toimintaa (ks. PeVL 62/2010 vp, s. 5).

2.1.3 Luottamuksellisen viestin salaisuuden rajoittaminen

Perusoikeudet eivät yleisesti ole siten ehdottomia, ettei niitä saisi missään olosuhteissa ja missään laajuudessa rajoittaa. Perustuslakivaliokunta on johtanut perusoikeusjärjestelmän kokonaisuudesta ja oikeuksien luonteesta perustuslaissa turvattuina oikeuksina joitakin yleisiä perusoikeuksien rajoittamista koskevia vaatimuksia (perusoikeuksien yleiset rajoitusedellytykset). Näitä ovat vaatimukset

— lailla säätämisestä

— lain täsmällisyydestä ja tarkkarajaisuudesta

— rajoituksen hyväksyttävyydestä

— rajoituksen suhteellisuudesta

— perusoikeuden ydinalueen koskemattomuudesta

— oikeusturvajärjestelyjen riittävyydestä ja

— ihmisoikeusvelvoitteiden noudattamisesta. (PeVM 25/1994 vp, s. 5.)

Eräisiin perusoikeussäännöksiin on lisäksi sisällytetty erityisiä rajoituslausekkeita. Tällainen on myös perustuslain 10 §:n 3 momentissa. Erityisissä rajoituslausekkeissa yhtäältä annetaan tavallisen lain säätäjälle valtuus perusoikeuden rajoittamiseen ja toisaalta asetetaan lainsäätäjän harkintavaltaa rajoittavia lisäkriteerejä. Tällaisten ns. kvalifioitujen lakivarausten tarkoituksena on määrittää tavallisen lain säätäjän rajoitusmahdollisuus mahdollisimman täsmällisesti ja tiukasti siten, ettei perustuslain tekstissä anneta avoimempaa perusoikeuden rajoitusvaltuutta kuin välttämättä on tarpeen (PeVM 25/1994 vp, s. 5).

Perustuslain kvalifioidut lakivaraukset vastaavat rakenteeltaan esimerkiksi Euroopan ihmisoikeussopimuksen useisiin artikloihin sisältyviä rajoituslausekkeita (PeVM 25/1994 vp, s. 5). Sisällöltään 10 §:n 3 momentin lakivaraus kuitenkin poikkeaa Euroopan ihmisoikeussopimuksen mukaisista rajoitusperusteista.

Perustuslain 10 §:n 3 momentin lakivarauksessa mainitaan osin samoja edellytyksiä kuin perusoikeuksien yleisissä rajoitusedellytyksissä (lailla säätämisen vaatimus, rajoituksen välttämättömyys). Perusoikeuksien yleisiä rajoitusedellytyksiä sovelletaan lakivarausta täydentävästi.

Perustuslain 10 §:n 3 momentin lakivarauksessa yksilöidään, mitä seikkoja voidaan pitää hyväksyttävinä perusteina rajoittaa luottamuksellisen viestin salaisuutta. Momentin mukaan välttämättömistä rajoituksista luottamuksellisen viestin salaisuuteen voidaan säätää ensinnäkin yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa. Tällaisten rikosten piiriin kuuluvat esimerkiksi huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset (HE 309/1993 vp, s. 54). Myös sotarikosten ja rikosten ihmisyyttä vastaan sekä yleisvaarallisten rikosten vakavampien tekomuotojen samoin kuin törkeän laittoman maahanmuuton järjestämisen, törkeän sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittämisen, vakavimpien vapauteen kohdistuvien rikosten, joidenkin terrorismirikosten sekä vahingonteon, datavahingonteon, petosrikosten, parituksen ja ympäristön

turmelemisen törkeiden tekomuotojen on katsottu perustuslakivaliokunnan tulkintakäytännössä olevan perustuslain puheena olevassa säännöksessä tarkoitettuja rikoksia. Samoin erityisesti liike- tai ammattitoimintaan liittyvien taloudellisiin intresseihin kohdistuvien törkeiden rikosten tutkimiseksi on pidetty mahdollisena säätää rajoituksista luottamuksellisen viestin salaisuuteen. Tällöin edellytyksenä on kuitenkin ollut, että rikoksella on tavoiteltu erityisen suurta hyötyä ja rikos on tehty erityisen suunnitelmallisesti.

Rikoksen tutkinnan voidaan sanonnallisesti ymmärtää tarkoittavan vain jo tehtyjen rikosten selvittämistä. Rikoksen tutkintana pidetään perustuslain 10 §:n 3 momentissa tarkoitetussa mielessä kuitenkin myös sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei vielä olisi ehtinyt toteutuneen teon asteelle. Näin ollen esimerkiksi televalvontaa on katsottu perustuslain 10 §:n 3 momentin estämättä voitavan käyttää tiettyjen rikosten estämiseen (PeVL 5/1999 vp; PeVL 2/1996 vp). Pakkokeinolakia ja poliisilakia koskevissa lausunnossaan perustuslakivaliokunta totesi, että televalvonnan käyttäminen oli rajattava sellaisiin rikoksiin, joita voidaan pitää perustuslaissa tarkoitettuina yksilön ja yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavina rikoksina, tai niihin törkeysasteeltaan verrattaviin rikoksiin. Valiokunta ei myöskään pitänyt televalvonnan käyttämistä televalvonnan perusterikoksesta epäillyn tavoittamiseksi perustuslain 10 §:n 3 momentin perusteella valtiosääntöoikeudellisesti ongelmallisena. (PeVL 67/2010 vp, s. 4; PeVL 66/2010 vp, s. 7.)

Lailla voidaan perustuslain 10 §:n 3 momentin mukaan säätää välttämättömistä rajoituksista luottamuksellisen viestin salaisuuteen oikeudenkäynnissä. Lainkohdan perusteluissa esimerkkeinä tällaisesta rajoituksesta mainitaan oikeudenkäymiskaaren 17 luvun sääntely velvollisuudesta esittää yksityinen asiakirja tai tallenne oikeudenkäynnissä (HE 309/1993 vp, s. 55).

Perustuslakivaliokunnan lausuntokäytännössä mahdollisuutta rajoittaa luottamuksellisen viestin salaisuutta oikeudenkäynnissä on tarkasteltu myös konkurssimenettelyn kannalta. Lailla on voitu säätää konkurssipesän hoitajan oikeudesta avata velalliselle osoitetut pesän selvittämiseen liittyvät viestit, vaikka pesänhoitajan toiminta ei varsinaisesti olekaan oikeudenkäyntiä. (PeVL 13/2003 vp.)

Välttämättömiä rajoituksia voidaan säätää viestin salaisuuteen myös turvallisuustarkastuksessa. Joissakin tapauksissa erittäin tärkeä turvallisuusintressi voi edellyttää esimerkiksi oikeutta tarkastaa postilähetyksiä. Lailla on siten voitu säätää esimerkiksi oikeudesta avata suljettu kirje tilanteessa, jossa on syytä epäillä, että lähetys saattaa aiheuttaa vaaraa terveydelle tai omaisuudelle. (PeVL 56/2010 vp, s. 4; PeVL 30/2001 vp, s. 3.) Lisäksi valiokunta on katsonut, että niin sanotun rynnäkkötarkkailun sisältämän rajoituksen luottamuksellisen viestin suojaan voidaan arvioida kuuluvan perustuslain 10 §:n 3 momentissa rajoitusperusteena mainitun turvallisuustarkastuksen piiriin (PeVL 36/2017 vp, s. 4).

Luottamuksellisen viestin salaisuuden rajoittaminen sallitaan perustuslain 10 §:n 3 momentissa lisäksi vapaudenmenetyksen aikana. Ilmaisulla ”vapaudenmenetyksen aikana” tarkoitetaan säännöksessä esimerkiksi vankeusrangaistuksen, tutkintavankeuden ja pidätyksen aikaa sekä sitä aikaa, kun joku on tahdostaan riippumatta hoidettavana mielisairaalassa tai muussa vastaavassa laitoksessa taikka huostaan otettuna lastensuojelulainsäädännön perusteella. Viestin salaisuutta voidaan laitosoloissakin rajoittaa vain siinä määrin kuin se kussakin yksittäistapauksessa on perusteltua. (HE 309/1993 vp, s. 54.)

Perustuslakivaliokunnan aiemmassa vakiintuneessa käytännössä viestin tunnistamistietojen on katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3; PeVL 6/2012 vp, s. 3—4; PeVL 29/2008 vp, s. 2;

PeVL 3/2008 vp, s. 2). Tämä on merkinnyt, ettei perustuslain 10 §:n 3 momentin erityistä lakivarausta ole sellaisenaan sovellettu tunnistamistietojen salaisuuden rajoittamiseen. Tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on kuitenkin valiokunnan käytännön mukaan tullut täyttää perusoikeuksien rajoittamisen yleiset edellytykset (PeVL 62/2010 vp; PeVL 23/2006 vp).

Perustuslakivaliokunnan mukaan tunnistamistietojen saaminen on voitu jättää sitomatta tiettyihin rikostyyppeihin (PeVL 33/2013 vp; PeVL 67/2010 vp; PeVL 37/2002 vp; PeVL 26/2001 vp). Näin ollen on voitu säätää televalvontatoimivaltuudesta myös tilanteessa, jossa ei välttämättä ole kyse yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavista rikoksista (ks. esim. poliisilaki (872/2011) 5 luku 8 § 2 momentti 1 ja 3 kohta: rikos, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta; teleosoitetta tai telepäätelaitetta käyttäen tehty, automaattiseen tietojenkäsittelyjärjestelmään kohdistuva luvaton käyttö).

Tunnistamistietojen saamista on pidetty mahdollisena myös joissakin tilanteissa, joissa ei ole ollut kyse rikoksen tutkinnasta. Tällöinkin sääntelyä on arvioitu perusoikeuksien yleisten rajoitusedellytysten kannalta. (PeVL 62/2010 vp.)

Perustuslakivaliokunta on sittemmin kuitenkin todennut, että Euroopan unionin tuomioistuimen Digital Rights Ireland -asiassa antama tuomio (8.4.2014, C-293/12 ja C-594/12) on antanut perusteita arvioida jossain määrin uudelleen sähköisessä viestinnässä saatavien tunnistamistietojen suojaa luottamuksellisen viestin salaisuuden näkökulmasta. Valiokunnan mukaan käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen. (PeVL 18/2014 vp.) Valiokunnan uusimmasta lausuntokäytännöstä ei ole vielä selvästi pääteltävissä, miten tällainen uudelleenarviointi muuttaa aiempaa perusoikeuksien yleisiin rajoittamisedellytyksiin nojaavaa tulkintalinjaa.

### 2.1.4 Salaisia tiedonhankintakeinoja koskeva sääntely

Rikosten estämisen tarkoituksessa viranomaisille on säädetty eräitä samantyyppisiä toimivaltuuksia kuin mitä tiedustelussa arvioidaan tarvittavan. Nykylainsäädännössä on säädetty rikosten estämis- ja paljastamistarkoituksessa käytettäväksi salaisia tiedonhankintakeinoja. Sen sijaan tiedustelutoiminnassa keskeisistä toimivaltuuksista ei ole säädetty.

Poliisin salaisista tiedonhankintakeinoista säädetään perustuslakivaliokunnan myötävaikutuksella säädetyn poliisilain 5 luvussa. Poliisi saa käyttää tiedonhankinnan kohteilta salassa seuraavia tiedonhankintakeinoja: telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen tarkkailu (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto, tietolähdetoiminta ja valvottu läpilasku. Näistä tiedonhankintakeinoista luottamuksellisen viestin salaisuuteen kohdistuvia ovat seuraavat:

— telekuuntelu (poliisilaki 5 luku 5 §)

— tietojen hankkiminen telekuuntelun sijasta (poliisilaki 5 luku 6 §)

— televalvonta (poliisilaki 5 luku 8 §)

— televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella (poliisilaki 5 luku 9 §)

— tukiasematietojen hankkiminen (poliisilaki 5 luku 11 §)

— tekninen kuuntelu (poliisilaki 5 luku 17 §)

— teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (poliisilaki 5 luku 25 §).

Salaisten tiedonhankintakeinojen käytön yleisenä edellytyksenä on poliisilain 5 luvun 2 §:n mukaan, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja. Telekuuntelulla ja tietojen hankkimisella telekuuntelun sijasta tulee lisäksi voida olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Poliisilain 5 luvussa on lisäksi säädetty keinokohtaisia erityisiä edellytyksiä salaiselle tiedonhankinnalle. Erityisinä edellytyksinä ovat ennen muuta ne yksilöidyt rikokset, joiden estämiseksi kutakin keinoa voidaan käyttää. Salaisten tiedonhankintakeinojen valintaa ja käyttöä ohjaavat myös poliisilain 1 luvussa säädetyt yleiset periaatteet, joita ovat perus- ja ihmisoikeuksien kunnioittamisen periaate, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate.

Puolustusvoimien rikostorjunnasta säädetään puolestaan sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa (255/2014). Lain 86 §:n 1 momentin mukaan puolustusvoimien toimivalta rikosten ennalta estämisessä ja paljastamisessa kohdistuu rikoksiin, jotka liittyvät sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan tai sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan. Lain 89 §:n 1 momentin mukaan puolustusvoimissa rikosten ennalta estämistä ja paljastamista hoitavien virkamiesten toimivaltuuksista on voimassa, mitä poliisilaissa säädetään toimivaltuuksista rikosten ennalta estämiseksi ja paljastamiseksi. Poliisilain 5 luvussa tarkoitetuista salaisista tiedonhankintakeinoista ovat kuitenkin käytettävissä vain tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Luottamuksellisen viestin suojaan kohdistuvista salaisista tiedonhankintakeinoista puolustusvoimien käytettävissä ovat siten vain tukiasematietojen hankkiminen, tekninen kuuntelu ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen.

### 2.1.5 Tiedustelutoiminnan valvonta

#### 2.1.5.1 Lupa- ja ilmoitusmenettely

Tiedustelutoiminnan valvonta voidaan jakaa yhtäältä ennakkovalvontaan ja jälkikäteiseen valvontaan sekä toisaalta parlamentaariseen valvontaan ja laillisuusvalvontaan. Ennakkovalvontaan kuuluu ennen muuta tiedustelumenetelmän käytön lupamenettely. Päätösvalta eräiden salaisten tiedonhankintakeinojen käyttämisestä on osoitettu tuomioistuimelle. Poliisilain 5 luvun mukaisista toimivaltuuksista telekuuntelu, tietojen hankkiminen telekuuntelun sijasta ja tukiasematietojen hankkiminen edellyttävät tuomioistuimen lupaa. Myös televalvonnasta päättäminen kuuluu pääsääntöisesti tuomioistuimen toimivaltaan. Sellaisissa kiireellisissä tilanteissa, joissa poliisi voi tilapäisesti itse päättää televalvonnasta, asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua

keinon käytön aloittamisesta. Poliisi voi kuitenkin päättää televalvonnasta henkeä tai terveyttä uhkaavan vaaran torjumiseksi sekä henkilön suostumuksella tehtävästä televalvonnasta epäiltäessä sellaisia rikoksia, jotka suoraan liittyvät teleosoitteeseen tai telepäätelaitteeseen. Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 89 §:ään sisältyvän viittaussäännöksen mukaan tukiasematietojen hankkiminen edellyttää tuomioistuimen lupaa.

Salaisen tiedonhankintakeinon käyttöä koskeva vaatimus on poliisilain 5 luvun 45 §:n mukaan otettava viipymättä käräjäoikeudessa käsiteltäväksi vaatimuksen tehneen tai hänen määräämänsä asiaan perehtyneen virkamiehen läsnä ollessa. Asia on ratkaistava kiireellisesti. Asia voidaan ratkaista kuulematta henkilöä, jonka perustellusti voidaan olettaa syyllistyvän tai syyllistyneen rikokseen, ja pääsääntöisesti kuulematta teleosoitteen tai telepäätelaitteen haltijaa. Salaista tiedonhankintamenetelmää koskevassa lupa-asiassa annettuun päätökseen ei saa hakea muutosta valittamalla. Päätöksestä saa ilman määräaikaa kannella hovioikeuteen.

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta ja televalvonnasta on poliisilain 5 luvun 58 §:n mukaan viipymättä ilmoitettava tiedonhankinnan kohteelle sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Salaisen tiedonhankintakeinon käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta. Tuomioistuin voi pidättämiseen oikeutetun poliisimiehen vaatimuksesta päättää, että ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan. Edellytyksenä ilmoittamisen lykkäämiselle on, että lykkääminen on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

### 2.1.5.2 Parlamentaarinen valvonta ja laillisuusvalvonta

Suomessa ei ole sellaista parlamentaarista valvontaelintä, jonka laissa säädettynä nimenomaisena tai yksinomaisena tehtävänä olisi valvoa tiedustelutoimintaa. Parlamentaarinen valvonta toteutuu eduskunnan ja sen valiokuntien toiminnan ja tietojensaantioikeuden kautta. Eduskunnan valiokunnista perustuslaki-, ulkoasiain-, hallinto- ja puolustusvaliokunnat ovat yhteydessä suojelupoliisiin ja sotilasviranomaisiin ja saavat tietoja myös tiedustelutoiminnasta. Suojelupoliisi informoi perustuslaki-, hallinto- ja ulkoasiainvaliokuntia Suomen turvallisuustilanteen kehittymisestä. Puolustusvoimien tiedustelulaitos puolestaan informoi eduskunnan valiokuntia tarpeen mukaan sotilastiedustelukysymyksistä. Monet valiokunnissa käsiteltävät puolustushallinnon alan asiat perustuvat tiedustelutietoon. Valiokuntien harjoittama seuranta on pääosin yleispiirteistä ja sen sisältö ja muodot vaihtelevat valiokunnittain. Sisäistä turvallisuutta käsittelevänä valiokuntana hallintovaliokunnalla on tiivistä vuorovaikutusta suojelupoliisin ja muiden poliisitoiminnan yksiköiden kanssa, ja toiminta sisältää myös valvonnallisia elementtejä. Perustuslakivaliokunta puolestaan tapaa suojelupoliisin johtoa joitakin kertoja vaalikaudessa, ja puolustusvaliokunta järjestää asiantuntijakuulemisia tietyistä teemoista. Mikäli tiedusteluun liittyy ulko- ja turvallisuuspoliittisesti merkittäviä seikkoja, asiaa käsitellään ulkoasiainvaliokunnassa ja niissä valiokunnissa, joiden toimialaan asia liittyy.

Perustuslain 47 §:n mukaan eduskunnalla on oikeus saada valtioneuvostolta asioiden käsittelyssä tarvitsemansa tiedot. Asianomaisen ministerin tulee huolehtia siitä, että valiokunta tai eduskunnan muu toimielin saa viipymättä tarvitsemansa viranomaisen hallussa olevat asiakirjat ja muut tiedot. Valiokunnalla on lisäksi oikeus saada valtioneuvostolta tai asianomaiselta

ministeriöltä selvitys toimialaansa kuuluvasta asiasta. Valiokunta voi selvityksen johdosta antaa asiasta lausunnon valtioneuvostolle tai ministeriölle.

Tiedustelutoiminnan laillisuusvalvonta voidaan jakaa ulkoiseen ja sisäiseen laillisuusvalvontaan. Viranomaistoiminnan ulkoisesta laillisuusvalvonnasta huolehtivat ylimmät laillisuusvalvojat ja erityisvaltuutetut. Erityisvaltuutetut, kuten tasa-arvovaltuutettu, yhdenvertaisuusvaltuutettu ja tietosuojavaltuutettu, valvovat viranomaistoiminnan lainmukaisuutta omalla laissa säädetyllä toimialallaan. Ylimmistä laillisuusvalvojista tiedustelutoiminnan valvontaa suorittaa nykyään ennen muuta oikeusasiamies. Poliisin toimintaan ja puolustusvoimiinkin kohdistuvassa oikeusasiamiehen valvonnassa korostuu salaisten pakkokeinojen ja salaisen tiedonhankinnan valvonta. Oikeusasiamies valvoo salaisia tiedonhankintakeinoja pääasiassa tarkastuksin ja muuna oma-aloitteisena valvontana. Yksittäisissä tapauksissa myös oikeuskansleri käyttää toimivaltaansa ja ottaa tutkittavakseen tiedustelutoimintaan kuuluvia tai siihen liittyviä asioita.

Sisäministeriön ja puolustusministeriön on annettava oikeusasiamiehelle vuosittain kertomus sekä salaisista pakkokeinoista että salaisista tiedonhankintakeinoista. Kertomusten tulee kattaa myös näiden keinojen valvonta. (Ks. poliisilaki 5 luku 63 §; pakkokeinolaki 10 luku 65 §; laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa 129 §.) Oikeusasiamies antaa puolestaan eduskunnalle joka vuodelta kertomuksen toiminnastaan sekä lainkäytön tilasta ja lainsäädännössä havaitsemistaan puutteista. Perustuslakivaliokunta on edellyttänyt, että kertomukseen sisällytetään jakso telepakkokeinoista ja peitetoiminnasta (PeVM 15/2002 vp). Perustuslakivaliokunta on useita kertoja yhtäältä todennut, että oikeusasiamiehellä on ollut tärkeä rooli telepakkokeinojen valvonnassa ja valvontajärjestelmien kehittämisessä. Oikeusasiamiehen laillisuusvalvonta voi valiokunnan mukaan toisaalta kuitenkin ainoastaan täydentää hallinnon sisäisiä valvontamekanismeja. (PeVM 8/2007 vp; PeVM 17/2006 vp; PeVM 16/2006 vp.) Valiokunta on lisäksi muussa yhteydessä todennut olevan syytä huolehtia siitä, että telepakkokeinojen käyttöön liittyvän oikeussuojajärjestelmän — etenkin tuomioistuimen lupamenettelyn, viranomaisten sisäisen valvonnan ja oikeusasiamiehen laillisuusvalvonnan — toimivuus varmistetaan sekä säädöstasolla että käytännössä (PeVL 32/2013 vp). Myös oikeusasiamiehen vuotta 2015 koskevassa kertomuksessa on todettu, että oikeusasiamiehen valvonta on jälkikäteistä ja varsin yleiskatsauksellista. Oikeusasiamies ei voi ryhtyä ohjaamaan viranomaisten toimintaa tai muutoinkaan olla keskeinen rajojen asettaja, joka korjaisi lainsäädännön heikkoudet. Oikeusasiamiehelle annettavat kertomukset tai selvitykset ovat tarpeellisia, mutta eivät ratkaise valvonnan ja oikeusturvan ongelmia. (Eduskunnan oikeusasiamiehen kertomus vuodelta 2015, K 11/2016 vp, s. 181.)

Poliisin salaisten tiedonhankintakeinojen sisäisestä valvonnasta huolehtivat salaisia tiedonhankintakeinoja käyttävien yksiköiden päälliköt sekä sisäministeriö suojelupoliisin osalta ja Poliisihallitus alaistensa yksiköiden osalta. Käytännössä merkittävä osa salaisten tiedonhankintakeinojen sisäisestä valvonnasta tapahtuu Poliisihallituksen lisäksi poliisilaitosten oikeusyksiköissä. Puolustusvoimien johto valvoo puolestaan puolustusvoimien rikostorjuntaa. Lisäksi tiedusteluosaston osastopäällikkö valvoo rikosten ennalta estämistä ja paljastamista.

### 2.1.6 Uusi tiedustelulainsäädäntö

Suomessa ei ole säädetty siitä, millaista tiedustelutoimintaa voidaan harjoittaa tai mihin tiedustelutoiminnalla pyritään. Turvallisuuspoliittisen toimintaympäristön muutoksiin ja uusiin uhkiin vastaamisen on todettu vaativan laajaa keinovalikoimaa ja käytettävissä olevien keino-

jen kehittämistä. Tämän mukaisesti valtioneuvostossa on valmisteltu tiedustelulainsäädännön kokonaisuus.

Sisäministeriön valmistelemassa siviilitiedustelulainsäädäntöä koskevassa hallituksen esityksessä ehdotetaan säädettäväksi poliisilakiin uusi 5 a luku sekä laki tietoliikennetiedustelusta siviilitiedustelussa. Tässä lainsäädännössä säädettäisiin siviilitiedustelussa käytössä olevista tiedustelumenetelmistä, toimivaltuuksien käytöstä päättämisestä sekä tiedustelutoiminnassa noudatettavista periaatteista ja toiminnan sisäisestä valvonnasta. Esitys sisältää säädöspohjan sekä ulkomaan tiedustelutoimivaltuuksille että kotimaassa käytettäville tiedustelutoimivaltuuksille. Sääntely pohjautuisi menetelmällisesti poliisilain 5 luvussa säädettyihin salaisiin tiedonhankintakeinoihin. Toimivaltuudet nimettäisiin käyttötarkoituksensa mukaisesti tiedustelumenetelmiksi, ja niiden käyttöperusteena olisi tiedon hankkiminen kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedustelumenetelmiä olisivat 5 luvussa säädettyjen keinojen lisäksi paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten ja tietoliikennetiedustelu. Tietoliikennetiedustelusta säädettäisiin omassa laissaan siihen liittyvien erityispiirteiden vuoksi. Siviilitiedustelun toimivaltuudet osoitettaisiin suojelupoliisille.

Puolustusministeriön valmistelemassa hallituksen esityksessä ehdotetaan säädettäväksi laki sotilastiedustelusta. Esityksen tavoitteena on parantaa puolustusvoimien tiedonhankintaa puolustusvoimien tehtäviin liittyvistä vakavista kansainvälisistä uhista siten, että puolustusvoimilla olisi toimivaltuudet ulkomaan henkilötiedusteluun ja tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun. Sotilastiedustelusta annettavassa laissa säädettäisiin sotilastiedustelun kohteista ja tiedustelutoiminnassa noudatettavista periaatteista sekä toiminnan ohjauksesta ja sisäisestä valvonnasta. Sotilastiedusteluviranomaisia olisivat puolustusvoimien pääesikunta ja tiedustelulaitos. Laissa säädettäisiin lisäksi viranomaisten käytössä olevista tiedustelumenetelmistä ja toimivaltuuksien käytöstä päättämisestä sekä tiedustelutiedon ilmoittamisesta, tiedustelukielloista, kansainvälisestä yhteistyöstä ja tietojen rekisteröimisestä.

Oikeusministeriön valmistelemassa hallituksen esityksessä ehdotetaan säädettäväksi laki tiedustelutoiminnan valvonnasta. Uudella lailla säädettäisiin siviili- ja sotilastiedustelun laillisuusvalvonnasta sekä eräistä parlamentaarisen valvonnan yksityiskohdista. Tiedustelutoiminnan parlamentaarista valvontaa varten eduskuntaan perustettaisiin uusi erikoisvaliokunta, tiedusteluvalvontavaliokunta, jonka tehtävistä säädettäisiin eduskunnan työjärjestyksessä. Tiedusteluvalvontavaliokunnan perustaminen edellyttää eduskunnan työjärjestyksen tarkistamista. Tiedustelutoiminnan laillisuusvalvonnasta huolehtisi tietosuojavaltuutetun toimiston yhteyteen perustettava itsenäinen ja riippumaton uusi viranomainen, tiedusteluvaltuutettu. Valtuutetun tehtävänä olisi valvoa tiedustelumenetelmien käytön lainmukaisuutta sekä perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa. Valtuutetun nimittäisi valtioneuvosto enintään viideksi vuodeksi kerrallaan. Tiedusteluvalvontavaliokunnalla ja tiedusteluvaltuutetulla olisi laajat tiedonsaantioikeudet. Tiedusteluvaltuutetulle säädettäisiin lisäksi tarkastusoikeus sekä valtuudet määrätä tiedustelumenetelmän käyttö keskeytettäväksi tai lopetettavaksi, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa. Valtuutettu voisi myös määrätä lainvastaisesti hankitut tiedot viipymättä hävitettäviksi. Tiedusteluvaltuutetulle voitaisiin tehdä kanteluja ja tutkimispyyntöjä. Valtuutettu antaisi vuosittain eduskunnalle, oikeusasiamiehelle ja valtioneuvostolle kertomuksen toiminnastaan.

## 2.2 Kansainvälinen käytäntö sekä ulkomaiden ja EU:n lainsäädäntö

### 2.2.1 Luottamuksellisen viestinnän perustuslakisääntelystä eräissä maissa

Esityksen valmistelussa on tarkasteltu eräiden Suomen kannalta keskeisten valtioiden luottamuksellisen viestin salaisuuden suojaa koskevaa perustuslakisääntelyä. Tarkasteltavissa maissa on tiedustelua koskevaa lainsäädäntöä, ja useiden maiden tiedustelulainsäädäntö on myös ollut Euroopan ihmisoikeustuomioistuimen arvioitavana. Tiedustelutoiminnan ja sen valvonnan sääntelyä Euroopan maissa on kuvattu yksityiskohtaisemmin siviili- ja sotilastiedustelua sekä tiedustelutoiminnan valvontaa koskevien esitysten yleisperusteluissa.

#### 2.2.1.1 Ruotsi

Ruotsin hallitusmuodon (Regeringsformen, 1974, perusoikeussäännöksiä muutettu 2011) 2 luvun 6 §:ssä säädetään muun muassa, että jokaisella on suoja kirjeiden tai muiden luottamuksellisten lähetysten tutkimista, salakuuntelua ja puheluiden tai muiden luottamuksellisten viestien tallentamista vastaan. Hallitusmuodon 2 luvun 20 §:n mukaan sanottuja oikeuksia voidaan rajoittaa lailla. Rajoituksia voidaan 2 luvun 21 §:n mukaan säätää ainoastaan sellaisiin tarkoituksiin, jotka ovat hyväksyttäviä demokraattisessa yhteiskunnassa. Lisäksi rajoitusten tulee täyttää välttämättömyysedellytys, eivätkä ne saa olla niin pitkälle meneviä, että ne muodostaisivat uhkan kansanvallan perusteena olevalle vapaalle mielipiteenmuodostukselle. Rajoituksia ei myöskään saa säätää ainoastaan poliittisen, uskonnollisen, kulttuurisen tai muun vastaavan katsomuksen perusteella. Hallitusmuodon 2 luvun 22 §:ssä säädetään menettelystä perusoikeuksien rajoituksia sisältäviä lakiehdotuksia käsiteltäessä.

Muita kuin Ruotsin kansalaisia koskevia erityisiä rajoituksia voidaan hallitusmuodon 2 luvun 25 §:n mukaan säätää lailla myös luottamuksellisen viestinnän suojaan. Tällöinkin on noudatettava valtaosaa 2 luvun 22 §:n menettelysäännöksistä. Lisäksi tällaisia, kuten muitakin perusoikeusrajoituksia, koskee hallitusmuodon 2 luvun 19 §:n säännös siitä, ettei sääntely saa olla ristiriidassa Euroopan ihmisoikeussopimuksen kanssa.

Ruotsissa tiedustelutoiminnasta säädetään sotilastiedustelusta annetulla yleislailla (Lag om försvarsunderrättelseverksamhet, 2000:130) ja signaalitiedustelusta annetulla yleislailla (Lag om signalspaning i försvarsunderrättelseverksamhet, 2008:717). Tiedustelutoiminnan säädöskokonaisuuteen kuuluu lisäksi muun ohella laki puolustustiedustelutuomioistuimesta (Lag om Försvarsunderrättelsedomstol, 2009:966). Tiedustelutoiminnan laillisuusvalvonnasta vastaavasta valtion tiedustelutarkastuksesta (Statens inspektion för försvarsunderrättelseverksamheten) säädetään laissa puolustustiedustelutoiminnasta, laissa signaalitiedustelusta puolustustiedustelutoiminnassa ja erillisessä asetuksessa (Förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten, 2009:969). Ruotsissa ei ole parlamentaarista valvontaelintä, jonka yksinomaisena tai pääasiallisena tehtävänä olisi tiedustelutoiminnan valvonta; valvonta kuuluu parlamentin puolustusvaliokunnalle.

Ruotsalaisessa lainsäädäntökäytännössä hallitusmuodon 2 luvun 6 §:ää luottamuksellisen viestin salaisuuden suojasta on tarkasteltu muun muassa tiedustelulainsäädännön yhteydessä. Tällöin lakiehdotusten perustuslainmukaisuudesta lausuntoja antava neuvosto (Lagrådet) on kiinnittänyt huomiota muun muassa siihen, että valtioon kohdistuvien ulkoisten uhkien selvittäminen samoin kuin rikosten estäminen ovat hyväksyttäviä perusteita luottamuksellisten viestin suojan rajoittamiselle. Lagrådet on myös ottanut kantaa luottamuksellisen viestinnän suojan laajuuteen. Sen mukaan suojaa rajoitetaan jo sillä, että valtio hankkii pääsyn teleliikenteeseen

eikä vasta sitten, kun tietty viesti erotetaan hakutermien avulla tarkempaan analyysiin (ks. tarkemmin Lagrådetin pöytäkirjat 9.2.2007 ja 20.6.2012).

#### 2.2.1.2 Norja

Norjan perustuslain (Kongeriket Norges Grunnlov, 1814) perusoikeussäännöksiä on uudistettu vuoden 2014 perustuslakiuudistuksessa. Perustuslain 102 §:n aikaisempi, kotietsintään rajoittunut säännös on uudistuksessa korvattu yksityis- ja perhe-elämän, kodin ja viestinnän suojaa koskevalla säännöksellä. Sen mukaan jokaisella on oikeus nauttia muun muassa viestintäänsä kohdistuvaa kunnioitusta.

Norjan perustuslaissa ei erikseen säädetä perusteista, joilla lainsäätäjä tai viranomaiset voivat puuttua 102 §:ssä turvattuihin oikeuksiin. Perustuslain 102 §:n perusteluissa (Innst. 186 S (2013-2014)) ei juurikaan ole tehty selkoa siitä, millaisissa tilanteissa oikeuksia voitaisiin rajoittaa, mutta perustelujen mukaan säännökseen valittu sanamuoto ”respekt for” kuvaa sitä, ettei tarkoituksena ole sulkea pois mahdollisuutta lain nojalla tapahtuvaan tiedusteluun. Oikeuskäytännössä perustuslain 102 §:ää on tulkittu säännöksen esikuvina olevien ihmisoikeussopimusmääräysten (YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen 17 artikla sekä Euroopan ihmisoikeussopimuksen 8 artikla) kanssa samansuuntaisesti. Rajoitukset ovat siten mahdollisia, jos niistä on säädetty laissa, niillä on hyväksyttävä tarkoitus ja ne ovat oikeasuhtaisia. (Høyesterett Rt. 2014 s. 1105 ja Rt. 2015 s. 93.)

Tiedustelutoiminnasta säädetään tiedustelupalvelusta annetussa laissa (Lov om etterretningstjenesten, 1998-03-20 nr. 11). Tiedustelutoiminnan valvonnasta säädetään turvallisuusviranomaisille yhteisessä laissa (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste, 1995-02-03 nr. 07). Norjan parlamentin, suurkäräjien (Stortinget), EOS-valtuuskunta (Utvalget for kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste) huolehtii sekä parlamentaarisesta valvonnasta että laillisuusvalvonnasta.

#### 2.2.1.3 Tanska

Tanskan perustuslain (Danmarks Riges Grundlov, 1953) 72 §:ssä säädetään muun muassa luottamuksellisen viestinnän suojasta. Sen mukaan kirjeiden takavarikoinnille ja tutkimiselle sekä muulle puuttumiselle posti-, lennätin- ja puhelinsalaisuuteen on oltava tuomioistuimen lupa, jollei laissa säädetä tästä erityistä poikkeusta. Säännöksen sanamuotoa suojan kohteista on tulkittu laajentavasti niin, että säännös kattaa myös sähköisessä muodossa säilytettävän tiedon ja sähköisen viestinnän.

Luottamuksellisen viestin suojan rajoittamisen edellytyksenä on käytännössä myös rajoituksen välttämättömyys. Muuhun kuin tuomioistuimen lupaan perustuva puuttuminen voi lisäksi koskea vain tarkoin määriteltyä asiaa.

Tanskassa lainsäädäntökäytännössä on pidetty tarpeellisena tarkastella ehdotettujen säännösten suhdetta ihmisoikeussopimuksiin eikä niinkään perustuslakiin. Esimerkiksi tiedustelupalvelua koskevaa lainsäädäntöä onkin tarkasteltu Euroopan ihmisoikeussopimuksen määräysten kannalta (ks. Betænkning om PET og FE, Betænkning nr. 1529, Justitsministeriet 2012). Tiedustelutoiminnasta on säädetty turvallisuuspoliisia ja puolustusvoimien tiedustelupalvelua koskevissa laeissa (Lov om Politiets Efterretningstjeneste, nr. 604 af 12. juni 2013; Lov om

Forsvarets Efterretningstjeneste, nr. 602 af 12. juni 2013), joihin sisältyy myös säännökset laillisuusvalvonnasta. Tiedustelutoiminnan laillisuusvalvonnasta huolehtii vuonna 2013 perustettu riippumaton lautakuntamuotoinen valvontaviranomainen (Tilsynet med Efterretningstjenesterne). Tiedustelutoiminnan parlamentaarista valvontaa harjoittaa puolestaan parlamentin, kansankäräjien (Folketinget), tiedustelupalveluvaliokunta (Udvalg vedrørende Efterretningstjenesterne), jonka toiminnasta ja kokoonpanosta säädetään omassa laissaan (Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, nr. 378 af 6. juli 1988).

#### 2.2.1.4 Saksa

Saksan perustuslain (Grundgesetz für die Bundesrepublik Deutschland, 1949) 10 artiklassa säädetään luottamuksellisen viestinnän suojasta. Artiklan ensimmäinen kohta sisältää säännöksen kirjeenvaihdon, postin ja viestinnän yksityisyyden loukkaamattomuudesta. Artiklassa ei ole mainintaa suojan rajoittamisen hyväksyttävistä edellytyksistä.

Perusoikeuksien rajoittamisen yleisistä edellytyksistä säädetään perustuslain 19 artiklassa. Edellytyksenä perusoikeuden rajoittamiselle on, että perustuslaissa säädetään mahdollisuudesta rajoittaa kyseessä olevaa perusoikeutta. Perusoikeutta rajoittavan lain täytyy olla yleisesti sovellettava eikä se saa koskea vain yksittäistä tapausta. Rajoitus ei saa kohdistua perusoikeuksien ydinalueeseen. Lisäksi on turvattava tuomioistuinkontrollin mahdollisuus.

Erityissäännös luottamuksellisen viestinnän suojan rajoittamisesta on 10 artiklan 2 kohdassa. Sen mukaan rajoitusten tulee perustua lakiin. Jos rajoituksen tarkoituksena on suojata vapaata demokraattista yhteiskuntajärjestystä tai liitto- tai osavaltion olemassaoloa tai turvallisuutta, laissa voidaan säätää, ettei rajoituksen kohteena olevalle ilmoiteta rajoituksesta ja että 19 artiklan yleisistä rajoitusedellytyksistä poiketen oikeussuojasta huolehditaan muutoksenhakuoikeuden sijaan laissa nimetyn viranomaisen suorittamalla valvonnalla.

Saksassa tiedustelutoiminnasta on säädetty tiedusteluviranomaisista säädetyissä laeissa (Gesetz über den Bundesnachrichtendienst, 20. Dezember 1990, BGBl. I S. 2954, 2979; Gesetz über den militärischen Abschirmdienst, 20. Dezember 1990, BGBl. I S. 2954, 2977; Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, 20. Dezember 1990, BGBl. I S. 2954, 2970). Luottamuksellisen viestin sisältöön puuttuvista tiedustelumenetelmistä säädetään erikseen niin sanotussa G 10 -laissa (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 26. Juni 2001, BGBl. I S. 1254, 2298).

G 10 -laissa säädetään edellytyksistä, joilla tiedustelupalvelut saavat tarkastaa postin välittämiä luottamuksellisia viestejä ja kuunnella sekä nauhoittaa luottamuksellista televiestintää. Näiden toimivaltuuksien käyttö edellyttää toiminnasta vastaavan ministeriön lupaa ja laillisuusvalvontaelimen (G 10 -komissio) hyväksyntää. Tietojen hankkimisen perusteeksi on määritetty laaja joukko kansalliseen turvallisuuteen kohdistuvia rikoksia. Yksityiselämän ydinalue nauttii korostettua suojaa viranomaisten tiedonhankinnalta. Yksityiselämän ydinalue muodostuu henkilön intiimistä yksityiselämästä, johon esimerkiksi perhe-elämä ei sinänsä kuulu. Myös vuoden 2017 alussa voimaan tulleen ulkomaan signaalitiedustelua koskevan lain (Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, 23. Dezember 2016, BGBl. I S. 3346, 67) mukaan tiedustelulla ei saa loukata yksityiselämän ydinaluetta, johon kuuluu yksilön intimiteettisuoja.

G 10 -laissa osoitetaan eräitä luottamuksellisen viestin sisältöön kohdistuvien tiedustelumenetelmien valvontatehtäviä tiedustelutoiminnan parlamentaarista valvontaa harjoittavalle liittovaltiopäivien (Bundestag) valvontavaliokunnalle (Parlamentarische Kontrollgremium). Perussäännökset valvontavaliokunnasta sisältyvät perustuslakiin ja tiedustelun parlamentaarisesta valvonnasta annettuun lakiin (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, 29. Juli 2009, BGBl. I S. 2346).

#### 2.2.1.5 Sveitsi

Yksityisyyden suojasta säädetään Sveitsin perustuslain (Bundesverfassung der Schweizerischen Eidgenossenschaft, 1999) 13 artiklassa. Sen mukaan jokaisella on muun muassa oikeus kirjeenvaihtoonsa, postiinsa ja sähköiseen viestintäänsä kohdistuvaan kunnioitukseen.

Perusoikeuksien rajoittamisesta säädetään Sveitsin perustuslaissa erikseen. Sääntely muistuttaa jossakin määrin Suomessa perustuslakivaliokunnan käytännön mukaan omaksuttuja perusoikeuksien yleisiä rajoitusedellytyksiä. Rajoittamisen edellytyksiä ovat perustuslain 36 artiklan mukaan rajoituksen perustuminen lakiin, rajoituksen oikeutus yleisen edun tai muiden perusoikeuksien vuoksi ja rajoitusten oikeasuhtaisuus. Rajoitukset eivät saa koskea perusoikeuden ydinaluetta.

Sveitsissä tuli voimaan 1.9.2017 uusi tiedustelulaki (Bundesgesetz über den Nachrichtendienst, vom 25. September 2015), jolla sallittiin yksityisissä tiloissa tapahtuva tiedustelu, järjestettiin maan rajat ylittävä tietoliikennetiedustelu ja laajennettiin sotilastiedustelun toimivaltuuksia. Uudessa laissa tiedustelutoiminnan lainmukaisuuden valvonnan järjestäminen osoitetaan puolustusministeriölle, jonka yhteydessä toimivan tiedustelupalvelun valvontaosaston (Nachrichtendienstliche Aufsicht) toimivaltuuksia laajennettiin. Uudella tiedustelulailla Sveitsin liittoneuvosto (Bundesrat) sai oikeuden asettaa riippumattoman valvontaelimen (Unabhängige Kontrollinstanz) tarkastamaan signaalitiedustelun lainmukaisuutta. Sveitsissä on tarkoitus säätää tietoliikennekaapeleihin kohdistuvasta tiedustelusta. Tiedustelutoiminnan parlamentaarisena valvontaelimenä toimivasta parlamentin alahuoneen (Nationalrat) ja ylähuoneen (Ständerat) valvontavaliokuntien yhteisestä alivaliokunnasta (Geschäftsprüfungsdelegation) säädetään perustuslaissa ja parlamentin toimintaa ja organisaatiota koskevassa laissa (Bundesgesetz über die Bundesversammlung, vom 13. Dezember 2002).

#### 2.2.1.6 Ranska

Ranskassa perustuslain kokonaisuuteen kuuluvissa vuoden 1958 perustuslaissa (Constitution du 4 octobre 1958), vuoden 1789 ihmisoikeuksien julistuksessa (Déclaration des Droits de l'Homme et du Citoyen de 1789) ja vuoden 1946 perustuslain johdanto-osassa (Préambule de la Constitution du 27 octobre 1946) ei säädetä suoraan luottamuksellisen viestinnän suojasta. Oikeuden yksityisyyden suojaan ja luottamuksellisen viestinnän suojaan on kuitenkin katsottu johtuvan ihmisoikeuksien julkistuksen 2 artiklasta, jossa todetaan yleisesti jokaisen ihmisoikeuksien suoja. Vuoden 1958 perustuslain 34 artiklan mukaan perusoikeuksista säädetään tarkemmin lailla. Yksityis- ja perhe-elämän suojasta on säädetty siviilioikeuslain (Code civil) 9 artiklassa, jonka mukaan jokaisella on oikeus yksityiselämänsä kunnioitukseen. Yksityiselämän suojan katsotaan ulottuvan myös luottamukselliseen viestintään. Yksilöiden luottamuksellista viestintää turvataan lisäksi tietosuojasta annetulla lailla (Loi relative à l'informatique,

aux fichiers et aux libertés, n° 78-17 du 6 janvier 1978), jonka 1 artiklan mukaan informaatioteknologialla ei saa loukata ihmisoikeuksia, yksityisyyttä ja yksilönvapauksia.

Yksityiselämän tai luottamuksellisen viestinnän suojan käsitteitä ei ole määritetty lainsäädännössä, vaan niiden sisältö ja merkitys määräytyy tulkintakäytännössä. Oikeus yksityiselämään ei ole ollut käytännössä rajoittamaton. Tätä oikeutta on Ranskassa punnittu erityisesti suhteessa sananvapauteen ja lehdistönvapauteen. Tulkintakäytännössä on muodostunut joukko kriteereitä, joiden avulla pyritään löytämään tasapaino eri perusoikeuksien välille. Näihin rajoitus- ja punnintakriteereihin kuuluu välttämättömyys (esim. yleinen etu) ja suhteellisuus.

Tiedustelutoimivaltuuksista säädetään Ranskassa sisäisestä turvallisuudesta annetussa laissa (Code de la sécurité intérieure). Lain L241-1 artiklan mukaan luottamuksellisen viestinnän salaisuus elektronisessa tietoliikenteessä turvataan lailla. Säännöksen mukaan luottamuksellisen viestin salaisuuden suojaa voidaan kuitenkin rajoittaa poikkeuksellisissa olosuhteissa muun muassa terrorismin ehkäisemiseksi ja tiedustelutiedon keräämiseksi kansallisesta turvallisuudesta. Säännös kattaa muun muassa puhelin- ja sähköpostiviestinnän.

Ranskassa hyväksyttiin vuonna 2015 tiedustelulainsäädännön muutos (Loi relative au renseignement, n° 2015-912 du 24 juillet 2015), jolla lisättiin viranomaisten tiedustelutoimivaltuuksia. Lain mukaan tiedustelutoimiin ryhtymisen perusteena voi olla muun muassa kansallisen suvereniteetin tai tärkeiden ulkopoliittisten tai kaupallisten intressien turvaaminen taikka terrorismin tai järjestäytyneen rikollisuuden torjuminen. Tiedustelulaki sisältää säännökset tiedustelutoiminnan laillisuusvalvonnasta. Tiedustelutoiminnan parlamentaarisesta valvonnasta on sen sijaan annettu oma lakinsa (Loi portant création d'une délégation parlementaire au renseignement, n° 2007-1443 du 9 octobre 2007).

Tiedustelulainsäädännön perustuslainmukaisuus on viety useaan otteeseen arvioitavaksi Conseil d'État'han, joka on puolestaan lähettänyt asian arvioitavaksi edelleen Conseil constitutionneliin. Arvioinnin kohteena on ollut muun ohella uusien tiedustelutoimivaltuuksien laaja henkilöllinen kohdistaminen ja yksityisyyden suojan rajoittamisen perusteet sekä pääministerin laajat toimivaltuudet tiedustelutoiminnan käynnistämisessä ilman tuomioistuimen lupaa ja sitovaa valvontamenettelyä. Conseil constitutionnel on pitänyt perustuslain vastaisena säännöksiä, joiden perusteella myös terrorismista epäillyn lähipiirin tarkkailu olisi ollut mahdollista (Décision n° 2017-648 QPC du 4 août 2017; ks. myös Décision n° 2016-590 QPC du 21 octobre 2016). Lisäksi Conseil constitutionnel on pitänyt säännöksiä ulkomailla vastaanotetun tai lähetetyn tietoliikenteen tiedon keräämisestä ja säilyttämisestä perusoikeusnäkökulmasta liian epämääräisinä (Décision du Conseil constitutionnel, n° 2015-722 DC du 26 novembre 2015; ks. Décision du Conseil constitutionnel, n° 2015-713 DC du 23 juillet 2015). Tämän seurauksena tiedustelulaki säädettiin koskemaan vain Ranskan maaperällä toteutettavaa tiedustelua; kansainvälisen tietoliikenteen tarkkailua varten säädettiin erillinen laki (Loi relative aux mesures de surveillance des communications électroniques internationales, n° 2015-1556 du 30 novembre 2015).

Ranskassa asetettiin marraskuun 2015 terrori-iskujen jälkeen lailla poikkeustila (Loi prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions, n° 2015-1501 du 20 novembre 2015). Poikkeustilan julistamisen perusteena oli vakava uhka yhteiskunnalle tai yleiselle järjestykselle. Poikkeustilan aikana viranomaisilla on normaalioloja vahvemmat toimivaltuudet ja oikeudet yksilönvapauksien rajoituksiin. Poikkeustilalaki muun muassa valtuuttaa sisäministerin päätöksin kotietsintöihin ilman tuomioistuinlupaa ja toimenpiteisiin terrorismille myötämielisten tai terroritekoihin kehottavien internetsivujen sulkemiseksi. Poikkeustilan voimassaolo päättyi 1.11.2017, kun voimaan saatettiin uusi sisäistä turvallisuutta ja terrorisminvastaista taistelua koskeva laki (Loi

renforçant la sécurité intérieure et la lutte contre le terrorisme, n° 2017-1510 du 30 octobre 2017). Lain tavoitteena on vahvistaa olemassa olevaa lainsäädäntöä siten, että Ranska pystyy vastaamaan tehokkaasti terrorismin uhkaan ja samalla varmistamaan yksilönvapauksien toteutumista laajemmin kuin poikkeustilan aikana. Uuteen lakiin ei sisälly tiedustelutoimintaan kytkeytyviä seikkoja.

2.2.1.7 Alankomaat

Alankomaiden perustuslain (Grondwet voor het Koninkrijk der Nederlanden, 1983, minkä jälkeen useita pienempiä muutoksia, viimeksi 2008) 10 artiklassa säädetään yksityisyyden suojasta. Artiklassa todetaan jokaisen oikeus yksityiselämän suojaan, jota voidaan kuitenkin rajoittaa lailla. Perustuslain mukaan henkilökohtaisten tietojen tallentamisesta ja jakamisesta säädetään lailla, jossa samalla säädetään yksityisyyden suojasta. Kotirauhan suojasta säädetään erikseen perustuslain 12 artiklassa. Myös luottamuksellisen viestin salaisuuden suojasta säädetään erillisessä säännöksessä. Perustuslain 13 artiklan mukaan viestin luottamuksellisuutta ei saa loukata muutoin kuin lailla säädetyissä tapauksissa tuomioistuimen päätöksellä. Puhelin- ja sähkeviestintää ei saa loukata muutoin kuin lailla säädetyissä tapauksissa ja laissa säädetyn tahon määräyksestä. Muun muassa henkilötietolaissa (Wet bescherming persoonsgegevens, 2001) ja tietojen säilyttämisestä tietoliikenneviestinnässä annetussa laissa (Wet bewaarplicht telecommunicatiegegevens, 2009) on säännöksiä yksityisyyden suojasta.

Alankomaissa vuonna 2009 käynnistetyssä perustuslain muutoksessa on ollut yhtenä tavoitteena sopeuttaa perusoikeussääntelyä digitalisaation aikakauteen. Keskeiseksi seikaksi on noussut se, että perustuslain 13 artikla ei tarjoa välitöntä ja riittävää suojaa digitaaliajan uusien viestintämuotojen käytössä. Tämän seurauksena parlamentin edustajainhuone (Tweede Kamer) julkaisi keväällä 2012 raportin perustuslain 13 artiklan muutostarpeista (Verslag van een algemeen overleg, gehouden op 23 mei 2012, inzake de Kabinetsstandpunt rapport staatscommissie Grondwet en aanpassing artikel 13 van de Grondwet, 2012) Hallitus on valmistellut raportin pohjalta perustuslain 13 artiklan muutosehdotuksen (Kabinetsstandpunt Rapport Staatscommissie Grondwet, 2012). Ehdotuksessa todetaan muun ohella tarve päivittää perustuslain säännöksen vanhentunut sanamuoto. Uudessa säännöksessä ei mainittaisi erikseen mitään tiettyä viestinnänmuotoa, vaan viitataan yleisesti yksityisyyteen viestinnässä ja tietoliikenneviestinnässä. Tarkoituksena on laajentaa perustuslain 13 artikla suojaamaan kaikki jo olemassa olevat ja tulevat viestinnänmuodot, kuten sähköpostiviestintä, internetpuhelut ja henkilökohtainen viestintä sosiaalisessa mediassa. Rajoituksista tähän luottamuksellisen viestin suojaan tulisi edelleenkin säätää lailla. Perustuslain muutosehdotuksen käsittely on kesken.

Alankomaissa muun ohella poliisilla ja tiedusteluviranomaisilla on lailla säädetyt toimivaltuudet puuttua perustuslain turvaamaan luottamuksellisen viestin salaisuuden suojaan, mikäli lailla säädetty toimivaltainen viranomainen antaa tähän luvan. Tiedustelutoiminnasta säädetään vuoden 2017 kesällä voimaan tulleessa laissa tiedustelu- ja turvallisuuspalveluista (Wet op de inlichtingen- en veiligheidsdiensten, 2017). Lailla korvattiin aiempi vastaava laki vuodelta 2012. Uudistuksessa luotiin uusia tiedustelutoimivaltuuksia, parannettiin tiedustelutoiminnan oikeudellista valvontaa ja pyrittiin ottamaan huomioon teknologinen kehitys.

### 2.2.2 Kansainväliset ihmisoikeussopimukset

#### 2.2.2.1 Euroopan ihmisoikeussopimus

Euroopan ihmisoikeussopimuksen 8 artiklassa määrätään, että jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Tämä oikeus on ollut keskiössä Euroopan ihmisoikeustuomioistuimen viime vuosikymmeninä antamissa lukuisissa turvallisuus- ja tiedustelupalveluja sekä salaisia pakkokeinoja ja salaista tiedonhankintaa koskevissa ratkaisuissa. Ihmisoikeussopimuksen 8 artiklan ohella ratkaisuissa on tulkittu erityisesti 13 artiklaa tehokkaista oikeussuojakeinoista. Ihmisoikeussopimuksen 13 artiklan mukaan jokaisella, jonka yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt. Myös 10 artiklalla sananvapaudesta ja lähdesuojasta on ollut merkitystä ihmisoikeustuomioistuimen tulkintakäytännössä.

Euroopan ihmisoikeustuomioistuimen vakiintuneen ratkaisukäytännön mukaan sopimuksen 8 artiklan 1 kohdassa mainitut yksityiselämän ja kirjeenvaihdon käsitteet pitävät sisällään sekä puhelinviestinnän, sähköpostiviestinnän että muun luottamukselliseksi tarkoitetun sähköisen viestinnän (mm. Liberty ja muut v. Yhdistynyt Kuningaskunta, 1.7.2008; Klass ja muut v. Saksa, 6.9.1978). Suojan piirissä ovat viestinnän sisällön lisäksi viestinnän tunnistamistiedot (mm. Weber ja Saravia v. Saksa, 29.6.2006; Malone v. Yhdistynyt Kuningaskunta, 2.8.1984). Pelkkä sellaisen lainsäädännön olemassaolokin, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja potentiaalistenkin osapuolten sopimuksen 8 artiklan takaamiin oikeuksiin (Liberty ja muut v. Yhdistynyt Kuningaskunta, 1.7.2008; Klass ja muut v. Saksa, 6.9.1978).

Euroopan ihmisoikeussopimuksen 8 artiklan mukainen oikeus ei kuitenkaan ole rajoittamaton, sillä viranomaiset saavat puuttua sen käyttämiseen artiklan 2 kohdassa mainituilla edellytyksillä. Ihmisoikeussopimuksen 8 artiklan takaamiin oikeuksiin puuttumisen on perustuttava kansalliseen lakiin. Lisäksi oikeuden rajoittamisen on oltava välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Euroopan ihmisoikeustuomioistuin on ratkaisukäytännössään asettanut vähimmäisvaatimuksia salaisia tiedonhankintamenetelmiä koskevalle lainsäädännölle. Nämä vaatimukset soveltuvat niin perinteisiin salaisiin pakkokeinoihin, kuten telekuunteluun tai muuhun tekniseen tarkkailuun, kuin moderniin tietoverkoissa tapahtuvaan tiedonhankintaankin.

Vaatimus rajoituksen perustumisesta lakiin jakautuu neljään osaan: Ensinnäkin luottamuksellisen viestinnän suojaan puuttumisella on oltava oikeudellinen perusta. Toiseksi lainmukaisuuteen liittyy saavutettavuus: tiedon tilanteeseen sopivista oikeudellisista säännöistä on oltava saatavilla. Kolmantena osavaatimuksena on ennustettavuus. Tällä tarkoitetaan, että normien tulee olla riittävän tarkkarajaisia, jotta yksilö voisi päätellä tekojensa seuraukset. Neljännen osavaatimuksen muodostaa vallan väärinkäytön estäminen. (Rotaru v. Romania, 4.5.2000; Malone v. Yhdistynyt Kuningaskunta, 2.8.1984.)

Ihmisoikeustuomioistuin on lisäksi käytännössään määritellyt sellaisia lainsäädännön laatukriteerejä, jotka kansallisen normiston tulee täyttää. Huvig v. Ranska ja Kruslin v. Ranska -tapauksissa (24.4.1990) tuomioistuin määritteli kuusi salaisia pakkokeinoja koskevalta sääntelyltä edellytettävää kriteeriä. Lainsäädännössä tulee ilmaista valvonnan mahdolliset kohde-

ryhmät, sellaisten rikkomusten luonne, joissa valvonta tulee kyseeseen, valvonnan kesto, menetelmä, jolla valvotuista keskusteluista raportoidaan, varotoimenpiteet tietoa luovutettaessa sekä nauhoitusten hävittäminen. Ihmisoikeustuomioistuin ei kuitenkaan ole aina aivan johdonmukaisesti tarkastellut kaikkien kriteerien täyttymistä, vaan tarkastelu on määräytynyt puuttumisen vakavuusasteen perusteella (R.E. v. Yhdistynyt Kuningaskunta, 27.10.2015).

Luottamuksellisen viestinnän suojan rajoituksen välttämättömyyden testi sisältää kolme keskeistä osaa. Rajoitukselle on oltava painava yhteiskunnallinen tarve (*pressing social need*), puuttumisen ja tavoiteltavan hyväksytyn päämäärän tulee olla oikeassa suhteessa keskenään (*reasonable relationship between the interference and pursued legitimate aim*) ja puuttumiselle pitää olla riittävät ja hyväksyttävät perustelut. Euroopan ihmisoikeustuomioistuin on tiedustelua koskevissa tapauksissa usein tarkastellut lainmukaisuutta ja rajoituksen välttämättömyyttä niitä tarkemmin erottelematta (Zakharov v. Venäjä, 4.12.2015; Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010).

Kansallinen turvallisuus on yksi niistä perusteista, joka ihmisoikeussopimuksen 8 artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. Valtioilla on varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan. Tuomioistuimen ratkaisukäytännön perusteella ainakin sotilaallinen maanpuolustus, terrorismintorjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin (mm. Weber ja Saravia v. Saksa, 29.6.2006; Klass ja muut v. Saksa, 6.9.1978). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tuomioistuimen mukaan tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010).

Euroopan ihmisoikeustuomioistuimen käytännössä on edellytetty, että tiedonhankinnan tulee olla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi ja saatavan elintärkeän tiedon ehdottoman välttämätöntä tiedusteluoperaation kannalta. Salaiseen tiedonhankintaan pitää olla aina korkea kynnys. Järjestelmät pitää rakentaa siten, että niitä käytetään säästeliäästi ja ainoastaan erittäin perustelluissa tapauksissa. Mallit, joissa viranomaisille jätetään liikaa harkintavaltaa, ovat ihmisoikeustuomioistuimen mielestä aina alttiita väärinkäytöksille eivätkä ole siten yhteensopivia Euroopan ihmisoikeussopimuksen asettamien vaatimusten kanssa. (Szabó ja Vissy v. Unkari, 12.1.2016.)

Zakharov-tapauksessa tuomioistuin piti ongelmallisena muun muassa tiedusteluviranomaisille jäävää lähes rajatonta valtaa määritellä, missä tilanteissa ja millaisten tapahtumien perusteella viesteihin voidaan puuttua. Viranomaiset pystyivät tapauksessa lähes rajoituksetta määrittelemään tapahtumat ja toimenpiteet, jotka muodostavat uhkan turvallisuudelle (on kyse sitten kansallisesta, sotilaallisesta, taloudellisesta tai ympäristöturvallisuudesta). Viranomaisilla oli myös laaja harkintavalta sen määrittelemisessä, miten vakava uhka oikeuttaa salaisten tiedonhankintakeinojen käyttöön. Tällä tavoin avoin lainsäädäntö jätti tuomioistuimen mukaan mahdollisuuden väärinkäytöksille. (Zakharov v. Venäjä, 4.12.2015, kohta 248.)

Euroopan ihmisoikeustuomioistuin on lisäksi kiinnittänyt huomiota salaisiin tiedonhankintakeinoihin kohdistuviin valvontajärjestelmiin. Erityisesti valvonnan tehokkuus ja valvontaelimen riippumattomuus ovat nousseet tärkeiksi vaatimuksiksi. Valvonnan tehokkuuteen kytkeytyvät kysymykset valvontaviranomaisen tiedonsaantioikeudesta, oikeussuojakeinoista ja toimivaltuuksien käytöstä ilmoittamisesta niiden kohteelle jälkikäteen. Ihmisoikeustuomioistuin on tavallisesti edellyttänyt, että väitetyn loukkauksen kohteena olevalla henkilöllä on suora pääsy oikeussuojakeinoon ilman välikäsiä. Valitus- tai kantelumahdollisuuden käytön edellytyksenä on yleensä se, että henkilö saa viranomaiselta tiedon häneen kohdistetusta tiedonhan-

kinnasta sen jälkeen kun tiedonhankintakeinon käyttö on päättynyt. (Ks. Zakharov v. Venäjä, 4.12.2015; Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010; Association for European Integration and Human Rights & Ekimdzhiev v. Bulgaria, 28.6.2007; Popescu v. Romania, 26.4.2007; Weber ja Saravia v. Saksa, 29.6.2006; Klass ja muut v. Saksa, 6.9.1978.)

Ihmisoikeustuomioistuimen oikeuskäytännössä valvonnan riippumattomuutta koskevia vaatimuksia ei ole täyttänyt esimerkiksi järjestelmä, jossa valvojalla on läheinen suhde toimeenpanovaltaan. Myös liian läheiset poliittiset kytkökset ovat merkkinä siitä, että valvontajärjestelmä ei ole riittävän riippumaton. Vaikka ihmisoikeustuomioistuin korostaa, ettei valvontatahon tarvitse olla tuomioistuin, se on kuitenkin kiinnittänyt argumentoinnissaan huomiota toimielinten jäsenten ja valvontatehtäviin valittavien ammatilliseen pätevyyteen ja taustaan. Tuomioistuin on suhtautunut myönteisesti valvontamalleihin, joissa tehtävään valituilta edellytetään toimimista korkeissa tuomarin tehtävissä. Lisäksi tuomioistuin on todennut, että kansanedustuslaitoksen osallistumisella salaisten tiedonhankintatoimivaltuuksien valvontaan on demokratian suojelemisen kannalta merkitystä. (Ks. Szabó ja Vissy v. Unkari, 12.1.2016; Zakharov v. Venäjä, 4.12.2015; R.E. v. Yhdistynyt Kuningaskunta, 27.10.2015; Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010; Popescu v. Romania, 26.4.2007; Weber ja Saravia v. Saksa, 29.6.2006; Segerstedt-Wiberg ja muut v. Ruotsi, 6.6.2006; Kopp v. Sveitsi, 25.3.1998; Campbell v. Yhdistynyt Kuningaskunta, 25.3.1992; Leander v. Ruotsi, 26.3.1987; Klass ja muut v. Saksa, 6.9.1978.)

Euroopan ihmisoikeustuomioistuimessa on parhaillaan vireillä valituksia nykyaikaisista tiedonhankintakeinoista. Käsittelyssä olevat valitukset perustuvat pitkälti Edward Snowdenin tekemiin paljastuksiin Yhdysvaltain tiedusteluviraston (National Security Agency) toiminnasta ja sen yhteistyöstä muiden maiden tiedusteluorganisaatioiden kanssa. Ihmisoikeustuomioistuimen näissä tapauksissa antamilla ratkaisuilla voi olla vaikutusta ihmisoikeussopimuksen 8 artiklan mukaiselle luottamuksellisen viestin salaisuuden suojalle samoin kuin 10 artiklan mukaiselle sananvapaudelle, mukaan lukien lähdesuojan merkitykselle, annettavaan sisältöön. (Ks. Big Brother Watch ja muut v. Yhdistynyt Kuningaskunta, application no. 58170/13; Bureau of Investigative Journalism ja Ross v. Yhdistynyt Kuningaskunta, application no. 62322/14; Human Rights Organisations ja muut v. Yhdistynyt Kuningaskunta, application no. 24960/15.)

#### 2.2.2.2 Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus

Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (KP-sopimus) 17 artiklassa määrätään muun muassa viestinnän suojasta. Artiklan 1 kohdan mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. Artiklan 2 kohdan mukaan jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan. KP-sopimuksen 2 artiklan 1 kohdassa sopimusvaltioille asetetaan velvollisuus ryhtyä toimenpiteisiin sopimuksessa, mukaan lukien 17 artiklassa, turvattujen oikeuksien suojaamiseksi.

KP-sopimuksen täytäntöönpanoa valvova YK:n ihmisoikeuskomitea on antanut tulkintakannanottoja yksityisyyden suojaa koskevasta yleissopimuksen 17 artiklasta. Artiklaa koskevassa ihmisoikeuskomitean yleiskannanotossa (General Comment no. 16, 8.4.1988) tämän sopimusmääräyksen on tulkittu pitävän sisällään valtion velvollisuuden itse pidättäytyä 17 artiklan vastaisista toimenpiteistä ja lisäksi puuttua yksityisten tekemiin loukkauksiin lainsäädännöllisin keinoin. Artiklan ilmaisu ”kirjeenvaihto” tarkoittaa myös muita viestinnän muotoja, kuten

puhelinkeskustelua ja sähköpostia. Kaikenlainen yksityisen viestinnän pidättäminen, sensurointi, tarkastus tai julkaiseminen muodostaa puuttumisen kirjeenvaihtoon.

Sopimuksen 17 artiklassa ei luetella perusteita, joilla artiklassa turvattuja oikeuksia voitaisiin rajoittaa. Artiklassa ainoastaan nimenomaisesti kielletään mielivaltaiset ja laittomat puuttumiset oikeuksiin. Mielivaltaisen puuttumisen kiellolla tavoitellaan sitä, että myös lakiin perustuvien puuttumisten tulee olla KP-sopimuksen määräysten ja tarkoituksen mukaisia ja kohtuullisia kussakin tapauksessa. Oikeuskirjallisuuden mukaan tulkinta-apua hyväksyttäville rajoitusperusteille on löydettävissä KP-sopimuksen muiden artiklojen rajoittamiskriteereistä ja Euroopan ihmisoikeussopimuksen 8 artiklassa tarkoitetuista rajoitusperusteista.

KP-sopimuksen 4 artiklan mukaan sopimusvelvoitteesta voidaan poiketa ainoastaan yleisen kansallista olemassaoloa uhkaavan hätätilan aikana. Tällaisen hätätilan tulee olla virallisesti sellaiseksi julistettu. Tällöin sopimusvaltiot voivat ryhtyä toimenpiteisiin, jotka merkitsevät poikkeamista niille KP-sopimuksen mukaan kuuluvista velvoituksista siinä laajuudessa kuin tilanne välttämättä vaatii. Lisäedellytyksenä on se, että tällaiset toimenpiteet eivät ole ristiriidassa valtion muiden kansainvälisen oikeuden mukaisten velvoitusten kanssa eivätkä merkitse pelkästään rotuun, ihonväriin, sukupuoleen, kieleen, uskontoon tai yhteiskunnalliseen syntyperään perustuvaa syrjintää.

Yksityisyyden suojaa koskevan 17 artiklan loukkauksista on tehty useita valituksia KP-sopimuksen valinnaisen pöytäkirjan nojalla, mutta toistaiseksi tapaukset eivät ole käsitelleet tietoverkkoturvallisuutta, sähköistä viestintää tai tiedustelutoimintaa. Todennäköisenä voidaan pitää, että tällaiset kysymykset nousevat jatkossa näkyvämmin esille ihmisoikeuskomitean työssä. Sähköiseen viestintään kohdistuvaa tiedustelua on jo käsitelty sopimusvaltioiden määräaikaisraportoinnin yhteydessä. Yhdysvaltojen neljättä määräaikaisraporttia koskevissa kommenteissaan ihmisoikeuskomitea kiinnitti tiedustelulainsäädännön tarkastelun yhteydessä huomiota muun muassa siihen, että viestinnän suojaan puuttumisen tulee perustua lakiin. Lain tulee olla yleisesti saatavilla ja siinä on tarkasti säädettävä puuttumisen edellytyksistä, menettelystä, puuttumisen kohteeksi mahdollisesti joutuvasta henkilöpiiristä ja puuttumisen kestosta. Lisäksi tulee huolehtia riittävän valvonnan järjestämisestä ja varmistaa, että väärinkäytösten kohteeksi joutuneilla on käytettävissään tehokkaita oikeussuojakeinoja. (Ks. Concluding observations on the fourth periodic report of the United States of America, United Nations, 23.4.2014.)

### 2.2.3 EU-oikeus

#### 2.2.3.1 EU-oikeuden ja EU:n perusoikeuksien soveltuminen

EU:n perusoikeuskirjan (EUVL C 326, 26.10.2012) määräykset koskevat sen 51 artiklan 1 kohdan mukaan unionin toimielimiä, elimiä ja laitoksia toissijaisuusperiaatteen mukaisesti sekä jäsenvaltioita ainoastaan silloin, kun viimeksi mainitut soveltavat unionin oikeutta. EU:n perusoikeuskirjaa ei siten sovelleta tilanteissa, joissa on kysymys ainoastaan kansallisen lain soveltamisesta ja joita EU-oikeudessa ei säännellä. Kuitenkin EU-oikeuden soveltamisalan ulkopuolellakin perusoikeuskirjasta voidaan johtaa tulkinta-apua esimerkiksi tilanteissa, joissa Euroopan ihmisoikeustuomioistuin ei ole käsitellyt jotakin oikeutta tai siihen liittyvää kysymystä, josta on olemassa EU-tuomioistuimen oikeuskäytäntöä.

Perusoikeuskirjan 52 artiklan 3 kohdassa säädetään, että siltä osin kuin perusoikeuskirjan mukaiset oikeudet ja Euroopan ihmisoikeussopimuksessa turvatut oikeudet vastaavat toisiaan,

niillä on sama merkitys ja kattavuus. Tämä ei estä unionia myöntämästä ihmisoikeussopimusta laajempaa suojaa. Perusoikeuskirjassa myönnetty suojan taso ei saa olla vastaavaa ihmisoikeussopimuksessa taattua suojan tasoa matalampi, mutta voi ylittää sen. EU:n oikeusjärjestyksessä tunnustettujen perusoikeuksien sisällön ja suojan tason tulkinnassa tulee ensisijaisesti tukeutua kyseistä oikeutta koskevaan EU-tuomioistuimen oikeuskäytäntöön (lausunto EU:n liittyminen EIS:een, 2/13, EU:C:2014:2454, 170 kohta; tuomio Kadi ja Al Barakaat, C-402/05 ja C-415/04 P, 281—285 kohta; tuomio Internationale Handelsgesellschaft, C-11/70, 4 kohta).

EU-oikeuden soveltuminen tiettyyn asiaan edellyttää, että asialla on ”riittävä liityntä” EU-oikeuteen (määräys Burzio, C-497/14, 28—31 kohta; määräys Văraru, C-496/14, 21 kohta; määräys Petrus, C-451/14, 18—20 kohta). EU:lla olevan toimivallan olemassaolo ei yksinään riitä tuomaan asiaa EU-oikeuden soveltamisalan piiriin, vaan merkityksellistä on, onko unioni käyttänyt toimivaltaa antamalla sääntelyä asiasta. EU:n perusoikeudet tai yleiset oikeusperiaatteet sellaisinaan, ilman konkreettista liityntää EU-oikeuteen, eivät muodosta kyseisenkaltaista riittävää liityntää, eivätkä siten tuo asiaa EU-oikeuden soveltamisalan piiriin (määräys Pondiche, C-608/14, 21 kohta; määräys Balázs ja Papp, C-45/14, 23 kohta; tuomio Torralbo Marcos, C-265/13, 30 kohta; määräys Cholakova, C-14/13, 30 kohta; määräys Nagy ym., C-488/12—C-491/12 ja C-526/12, 17 kohta; tuomio Pelckmans Turnhout, C-483/12, 20 kohta; tuomio Åkerberg Fransson, C-617/10, 22 kohta).

Tiedustelulainsäädännön yhteydessä merkityksellisiä ovat EU-lainsäädäntöön sisältyvät poikkeukset, joiden perusteella EU-oikeuden soveltuminen on useissa säädöksissä rajattu kansallista turvallisuutta koskevien asioiden ulkopuolelle. Poikkeukset perustuvat Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan määräykseen, jonka mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Unionilla ei siten ole kansallista turvallisuutta koskevaa toimivaltaa. EU-oikeuden soveltamisalan rajautuminen pois kansallista turvallisuutta koskevan poikkeuksen perusteella ei kuitenkaan ole aina käytännössä yksiselitteistä. EU:n oikeusjärjestyksellä ja eräillä Euroopan unionin tuomioistuimen ennakkoratkaisuilla ja EU-lainsäädännön kumoamiskanteilla on siten merkitystä myös tiedustelutoiminnalle ja sitä koskevan kansallisen lainsäädännön kehittämiselle. Jäsenvaltion, joka vetoaa edukseen kansallista turvallisuutta koskevaan perusteeseen, on näytettävä toteen tarve turvautua kyseiseen perusteeseen (tuomio ZZ, C-300/11; tuomio Insinööritoimisto InsTiimi Oy, C-615/10, 35 kohta; tuomio komissio v. Suomi, C-284/05, 45 ja 47 kohta).

#### 2.2.3.2 Luottamuksellisen viestin salaisuuden suoja EU-oikeudessa

Säännös luottamuksellisen viestin salaisuuden suojasta sisältyy EU:n perusoikeuskirjan 7 artiklaan, jonka mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Lisäksi perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen suojaan kuuluvien tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava laissa määritettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Perusoikeuskirjan tulkinnassa huomioon otettavien perusoikeuskirjaa koskevien selitysten (EUVL C 303, 14.12.2007, s. 17—35) mukaan perusoikeuskirjan 7 artiklassa turvatut oikeudet vastaavat ja niillä on sama merkitys ja kattavuus kuin vastaavilla Euroopan ihmisoikeussopimuksen 8 artiklassa turvatuilla oikeuksilla. Euroopan ihmisoikeussopimuksessa käytetty

sana ”kirjeenvaihtonsa” on tekniikan kehityksen huomioon ottamiseksi korvattu perusoikeuskirjan 7 artiklassa sanalla ”viestiensä”.

Perusoikeuskirjan 7 ja 8 artikla eivät ole ehdottomia oikeuksia. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

EU-tuomioistuimen oikeuskäytännön mukaan lailla säätämistä koskevan vaatimuksen mukaisesti rajoituksen oikeudellisen perustan on muun muassa oltava riittävän selkeä ja täsmällinen, ja perustassa itsessään on annettava tietty suoja mahdollisia oikeudenloukkauksia vastaan (tuomio WebMind, C-419/14, 81 kohta). Kyseinen kriteeri muistuttaa läheisesti Euroopan ihmisoikeussopimuksen vastaavaa oikeuksien rajoitusedellytyksiä koskevaa ”säädetty laissa” -perustetta. Tämän vuoksi Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä voidaan saada tätä kriteeriä koskevaa tulkinta-apua erityisesti sellaisten perusoikeuskirjan määräysten osalta, jotka vastaavat Euroopan ihmisoikeussopimuksen sisältämiä oikeuksia.

EU-tuomioistuimen oikeuskäytännössä on korostettu yksityiselämän kunnioitusta ja henkilötietojen suojaa koskevien perusoikeuksien tärkeyttä erityisesti sähköisen viestinnän yhteydessä (mm. tuomio Schrems, C-362/14, 39 kohta; tuomio Digital Rights Ireland, C-293/12 ja C-594/12, 53 kohta; tuomio Google Spain ja Google, C-131/12, 53, 66 ja 74 kohta; tuomio Rijkeboer, C-553/07, 47 kohta).

Oikeuskäytännöstä käy ilmi, että muun muassa vakavan rikollisuuden torjunta yleisen turvallisuuden takaamiseksi (tuomio Tsakouridis, C-145/09, 46 ja 47 kohta) ja kansainvälisen terrorismin torjuminen kansainvälisen rauhan ja turvallisuuden ylläpitämiseksi (tuomio WebMind, C-419/14, 76 kohta; tuomio Al-Aqsa v. neuvosto, C-539/10 P ja C-550/10 P, 130 kohta; tuomio Kadi ja Al Barakaat, C-402/05 P ja C-415/05 P, 363 kohta) ovat unionin yleisen edun mukaisia tavoitteita, joiden perusteella on voitu säätää perusoikeusrajoitteita. Lisäksi kansallinen turvallisuus mainitaan nimenomaisesti Euroopan unionin toiminnasta tehdyn sopimuksen 4 artiklan 2 kohdassa, ja se on vakiintuneesti hyväksytty unionin tuomioistuimen oikeuskäytännössä oikeutetuksi tavoitteeksi rajoittaa perusoikeuksia (esim. tuomio komissio v. Suomi, C-284/05, 45, 47 ja 49 kohta).

EU-tuomioistuimen käytännössä perusoikeuksien rajoitusten suhteellisuusperiaatteen mukaisuuden arviointi on usein osoittautunut arvioinnin ratkaisevaksi vaiheeksi. Perusoikeuskirjan 52 artiklan 1 kohdan mukainen suhteellisuusperiaate kuuluu EU-oikeuden yleisiin periaatteisiin ja edellyttää EU-tuomioistuimen vakiintuneen oikeuskäytännön mukaan, että arvioitavana olevan toimen tai säädöksen oikeutetut tavoitteet ovat toteutettavissa unionin toimesta säädettyjen keinojen avulla ja että niillä ei ylitetä sitä, mikä on tarpeellista ja välttämätöntä näiden tavoitteiden toteuttamiseksi ja on tähän soveltuvaa (appropriate and necessary, esim. tuomio Schaible, C-101/12, 29 kohta; tuomio Sky Österreich, C-283/11, 50 kohta; tuomio Nelson ym., C-581/10 ja C-629/10, 71 kohta; tuomio Afton Chemical, C-343/09, 45 kohta; tuomio Schecke, C-92/09 ja C-93/09, 74 kohta). Käytännössä kyse on hyväksyttävän tasapainon löytämisestä eri intressien välille. Perusoikeutta koskevien poikkeuksien ja rajoitusten tulee olla välttämättömiä niin, että toimenpiteillä puututaan kyseiseen perusoikeuteen mahdollisimman vähän samalla, kun myötävaikutetaan tehokkaasti kyseessä olevan EU:n sääntelyn tavoitteiden toteutumiseen (tuomio WebMind, C-419/14, 82 kohta; tuomio R., C-285/09, 45 kohta; tuomio Schecke, C-92/09 ja C-93/09, 87 ja 88 kohta).

Digital Rights Ireland -tuomiossaan (C-293/12 ja C-594/12) EU-tuomioistuin edellytti teletunnistetietoihin pääsyä ja niiden käyttöä koskevien kriteerien suhteellisuusperiaatteen mukaisuutta. Tuomioistuin totesi teletunnistetietojen säilyttämistä koskevan direktiivin (2006/24/EY) pätemättömäksi. Tuomioistuimen mukaan direktiivin olisi tullut asettaa tavoitteeseensa liittyvät objektiiviset rajat sille, keiden henkilöiden tunnistamistiedot saadaan säilyttää. Lisäksi direktiivissä olisi tullut tarkemmin määritellä ne rikokset, joiden torjumiseksi säilyttämisvelvollisuus asetettiin.

Ratkaisussaan Schrems EU-tuomioistuin piti yksityiselämän kunnioitusta koskevan perusoikeuden keskeistä sisältöä erityisesti loukkaavana säännöstöä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön. Lisäksi tuomioistuin totesi, että tehokasta oikeussuojaa koskevan perusoikeuden keskeistä sisältöä loukkaavat sellaiset säännökset, joissa yksityisille ei anneta mahdollisuutta tutustua itseään koskeviin henkilötietoihin tai saada tällaiset tiedot oikaistuiksi tai poistetuiksi. (Tuomio Schrems, C-362/14, 94 ja 95 kohta.)

Tele2 Sverige -tuomiossa EU-tuomioistuin arvioi paikka- ja liikennetietojen tallentamista sähköisen viestinnän tietosuojadirektiivin valossa (2002/58/EY, muutettu direktiivillä 2009/136/EY). Tuomioistuin katsoi, että sähköisten viestintävälineiden kaikkien liikenne- ja paikkatietojen yleinen ja erotuksetta tapahtuva säilyttäminen ei ole EU-oikeuden mukaista. Tästä huolimatta jäsenvaltiot voivat säätää sekä tietojen kohdennetusta säilyttämisestä että toimivaltaisten kansallisten viranomaisten oikeudesta saada kyseisiä tietoja jonkin sähköisen viestinnän tietosuojadirektiivissä mainitun oikeutetun tavoitteen toteuttamiseksi. Tuomioistuin mainitsi nimenomaisesti ”vakavan rikollisuuden” (*serious crime*) esimerkkinä oikeutetusta tavoitteesta, koska tämä tavoite oli merkityksellinen pääasiaa koskevassa oikeudenkäynnissä. Tuomioistuin katsoi sähköisen viestinnän tietosuojadirektiivin 15.1 artiklan sisältävän tyhjentävän luettelon oikeutetuista tavoitteista, joihin kuuluvat muun ohella yleinen turvallisuus (*public security*) ja kansallinen turvallisuus (*national security*). Tuomioistuimen mukaan kyseisten kansallisten säännösten on oltava selviä ja täsmällisiä. Lisäksi tietojen säilyttämisen ja pääsyn niihin on suhteellisuusperiaatteen mukaisesti oltava rajoitettu täysin välttämättömään. (Tuomio Tele2 Sverige, C-203/15 ja C-698/15, 94—96, 102—103, 108—109, 116 kohta.)

Tele2 Sverige -tuomiossa EU-tuomioistuin luetteli kaikkiaan useita aineellisia ja menettelyllisiä seikkoja, jotka tulisi ottaa huomioon tietojen säilyttämistä ja käyttöä koskevissa kansallisissa säännöksissä. Sääntelyn tulee sisältää muun ohella asianmukaiset oikeussuojakeinot. Lisäksi kansallisen säännöstön tulee perustua objektiivisiin seikkoihin, joiden perusteella voidaan kohdentaa sellainen yleisö, johon liittyvät tiedot voivat paljastaa ainakin välillisen yhteyden vakavaan rikollisuuteen, myötävaikuttaa tavalla tai toisella vakavan rikollisuuden torjumiseen tai ehkäistä yleistä turvallisuutta koskeva uhka. Tuomion mukaan kansallisten säännösten laajuutta ja soveltamista voidaan rajoittaa ehdottoman välttämättömään edellytyksillä, jotka koskevat muun muassa aiotun säilytyksen kestoa, maantieteellisesti määriteltyä aluetta, henkilöpiiriä, tietoluokkia, viestintävälineitä ja kohdennettua yleisöä. Tuomioistuin katsoi lisäksi, että etukäteisvalvontaa, tietojen säilyttämistä unionin alueella, tietosuojan ja -turvan korkeaa tasoa, tietojen lopullista hävittämistä säilytysajan päätyttyä ja tietojen kohteena olevien henkilöiden tiedottamista on pidettävä edellytyksinä sille, että toimivaltaiset viranomaiset voivat saada kyseisiä tietoja. (Tuomio Tele2 Sverige, C-203/15 ja C-698/15, 106—111, 117—119, 120—122 kohta.)

Tietosuojaa koskevassa oikeuskäytännössään EU-tuomioistuin on kiinnittänyt kaikkiaan huomiota muun muassa arvioinnin kohteena olevan järjestelyn valvontaan, käytettävissä oleviin riittäviin oikeussuojakeinoihin, tiedon antamiseen ja tietoturvaan sekä henkilöpiiriä, ennakkolupaa, tietoihin pääsyä, tietojen säilytysaikaa ja niiden hävittämistä koskeviin edellytyksiin (ks. tuomio Tele2 Sverige, C-203/15 ja C-698/15, 106—111, 117—119, 120—122 kohta;

tuomio WebMind, C-419/14, 77—78 kohta; tuomio Schrems, C-362/14, 40 ja 95 kohta; tuomio Digital Rights Ireland, C-293/12 ja C-594/12, 56—67 kohta; tuomio UGT-Rioja ym., C-428/06—C-434/06, 80 kohta.)

## 2.3 Nykytilan arviointi

### 2.3.1 Yleistä

Perusoikeussäännökset otettiin vuoden 2000 uudistuksessa perustuslakiin asiallisesti sellaisina kuin ne sisältyivät hallitusmuodon II lukuun 1.8.1995 voimaan tulleen perusoikeusuudistuksen mukaisina. Perustuslain 9 §:n 3 momentin sääntelyä Suomen kansalaisen luovuttamisesta toiseen maahan on muutettu lailla 802/2007 ja vaali- ja osallistumisoikeuksia koskevaa 14 §:ää sekä perusoikeuspoikkeuksia poikkeusoloissa koskevaa 23 §:ää lailla 1112/2011. Muuten perusoikeussäännökset ovat olleet voimassa muuttumattomina vähän yli kahdenkymmenen vuoden ajan. Selvitettäessä perustuslakiuudistuksen toimivuutta ja mahdollisia tarkistustarpeita on perustuslain perusoikeussäännöstön arvioitu toimivan kokonaisuutena hyvin (Perustuslaki 2008 -työryhmän muistio, oikeusministeriö, työryhmämietintö 2008:8; Selvitys perustuslakiuudistuksen toimeenpanosta, perustuslain seurantatyöryhmän mietintö, oikeusministeriö, työryhmämietintö 2002:7).

Eduskunnan perustuslakivaliokunta on linjannut perustuslain muuttamiseen yleisesti liittyviä periaatteita käsitellessään ensimmäistä kokonaisuudistuksen jälkeen annettua perustuslain muutosesitystä. Valiokunta totesi asiasta näin: ”Perustuslain muuttamiseen tulee suhtautua pidättyvästi. Perustuslain muutoshankkeisiin ei pidä ryhtyä päivänpoliittisten tilannenäkymien perusteella eikä muutoinkaan niin, että hankkeet olisivat omiaan heikentämään valtiosäännön perusratkaisujen vakautta tai perustuslain asemaa valtio- ja oikeusjärjestyksen perustana. On toisaalta pidettävä huolta siitä, että perustuslaki antaa oikean kuvan valtiollisen vallankäytön järjestelmästä ja yksilön oikeusaseman perusteista. Perustuslain mahdollisia muutostarpeita tulee arvioida huolellisesti ja välttämättömiksi arvioidut muutokset tehdä perusteellisen valmistelun sekä siihen liittyvän laajapohjaisen keskustelun ja yhteisymmärryksen pohjalta.” (PeVM 5/2005 vp, s. 2.)

### 2.3.2 Erityinen rajoituslauseke

Kirje-, lennätin- ja puhelinsalaisuus oli ennen perusoikeusuudistusta voimassa olleen hallitusmuodon 12 §:n sanamuodon mukaan loukkaamaton, mikäli siitä ei ollut laissa säädetty poikkeusta. Perusoikeusuudistuksen valmisteluasiakirjojen mukaan hallitusmuotoa säädettäessä ajatuksena oli useiden oikeuksien osalta vain pidättää eduskuntalain alaan sellainen kansalaisten oikeuksia koskeva sääntely, joka Venäjän vallan aikana oli toteutettu hallinnollisessa järjestyksessä. Hallitusmuodon II luvun lakivaraukset eivät pääsääntöisesti sisältäneet ehtoja rajoittavalle tai täsmentävälle laille. (Perusoikeustyöryhmä 1992:n mietintö, oikeusministeriön lainvalmisteluosaston julkaisu 2/1993, s. 45.)

Perusoikeussäännösten aikaisempi hyvin yleinen muotoilu oli käytännössä vaikeuttanut niiden soveltamista tuomioistuimissa ja viranomaisissa, koska säännökset eivät tarjonneet lainsoveltajille riittäviä kiinnekohtia. Lisäksi ongelmallisena pidettiin sitä, ettei hallitusmuodossa täsmennetty useimpien perusoikeuksien rajoittamisedellytyksiä. Rajanveto sallitun ja kielletyn rajoittamisen välillä oli siten jäänyt hyvin tulkinnanvaraiseksi. (HE 309/1993 vp, s. 14.) Huo-

miota kiinnitettiin myös siihen, että lainsäädäntökäytäntö oli alkanut irtaantua säännösten sanamuodosta (PeVM 25/1994 vp, s. 4).

Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Sanotunkaltaisissa erityisissä rajoituslausekkeissa yhtäältä annetaan tavallisen lain säätäjälle valtuus perusoikeuden rajoittamiseen ja toisaalta asetetaan lainsäätäjän harkintavaltaa rajoittavia lisäkriteerejä (ks. esim. PeVM 25/1994 vp).

Kvalifioitujen lakivarausten tarkoituksena on määrittää tavallisen lain säätäjän rajoitusmahdollisuus mahdollisimman täsmällisesti ja tiukasti siten, ettei perustuslain tekstissä anneta avoimempaa perusoikeuden rajoitusvaltuutta kuin välttämättä on tarpeen (PeVM 25/1994 vp, s. 5). Perustuslain 10 §:n 3 momenttiin sisältyvän kvalifioidun lakivarauksen perustelujen mukaan säännöksessä luetellaan tyhjentävästi ja mahdollisimman suppeasti ja täsmällisesti mahdollisuudet rajoittaa luottamuksellisen viestin salaisuutta (HE 309/1993 vp, s. 54).

Luottamuksellisen viestin salaisuuden rajoittamisperusteet perustuslain 10 §:n 3 momentissa ovat enimmäkseen varsin konkreettisia ja yksityiskohtaisiakin (oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana). Rikosten tutkintaan kiinnittyvä peruste (yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa) on jossakin määrin yleisempi, erityisesti ottaen huomioon perustetta koskeva perustuslakivaliokunnan tulkintakäytäntö, joka on osin laajentunut koskemaan myös rikosten estämisen ja sellaisenkin rikollista tekoa koskevan tutkinnan, jonka tarkoituksena ei ole rikosvastuun toteuttaminen (PeVL 19/2008 vp). Luottamuksellisen viestin salaisuuden rajoittamisperusteet näyttäytyvät myös jossakin määrin konkreettisempina ja täsmällisempinä kuin niin ikään perustuslain 10 §:n 3 momentissa säännellyt perusteet sallituille kotirauhan piiriin ulottuville toimenpiteille.

Perusoikeusuudistuksen esitöissä luottamuksellisen viestin salaisuuden rajoittamisperusteet on kytketty tuolloin tunnistettuihin, konkreettisiin lainsäädäntötarpeisiin. Luottamuksellisen viestin salaisuuden suoja ulottuu viestinnän erilaisiin muotoihin tekniikkaneutraalisti. Luottamuksellisen viestin salaisuuden rajoitusperusteita muotoiltaessa ei kuitenkaan ole voitu kaikilta osin ennakoida tulevaa yhteiskunnallista ja teknistä kehitystä. Siten tiedustelutoimivaltuuksiin liittyviä kysymyksiä ei ole voitu perusoikeusuudistusta valmisteltaessa ottaa huomioon.

Myös ihmisoikeussopimuksiin, kuten Euroopan ihmisoikeussopimukseen, sisältyy erityisiä rajoituslausekkeita. Sallittujen rajoitusperusteiden sisältö perustuslain 10 §:n 3 momentissa eroaa kuitenkin esimerkiksi Euroopan ihmisoikeussopimuksen 8 artiklan mukaisista rajoitusperusteista. Ihmisoikeussopimuksen mukaan sallitut rajoitusperusteet ovat väljemmin ja abstraktimmin muotoiltuja kuin perustuslain 10 §:n 3 momentin mukaiset perusteet. Osittain eroja selittää sopimusmääräysten erilainen kirjoitustapa, niiden asema suojan minimitason asettajina ja valtioille ihmisoikeussopimuksen soveltamisessa jätettävä harkintamarginaali.

EU:n perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen viestejään kunnioitetaan. Artiklassa ei ole listattu oikeuden hyväksyttäviä rajoitusperusteita, mutta perusoikeuskirjan 52 artiklan 1 kohtaan sisältyvät yleiset määräykset oikeuksien rajoittamisen edellytyksistä.

Edellä tarkastelluissa, Suomen kanssa oikeuskulttuuriltaan samantyyppisten eurooppalaisten valtioiden perustuslaeissa ei myöskään ole löydettävissä vastaavia rajoitusperusteita luottamuksellisen viestin salaisuuden rajoittamiselle kuin perustuslain 10 §:n 3 momentissa on sää-

detty. Tätä seikkaa selittävät perustuslaeissa omaksutut erilaiset sääntelytavat ja osittain myös perustuslakien säätämisajankohdat.

### 2.3.3 Perustuslain muutostarve

Luottamuksellisen viestin salaisuutta voidaan perustuslain 10 §:n 3 momentin mukaan rajoittaa muun muassa tietynlaisten rikosten tutkinnassa. Rikoksen tutkinnan voidaan sanonnallisesti ymmärtää tarkoittavan vain jo tehtyjen rikosten selvittämistä. Perustuslain 10 §:n 3 momentin tulkinta on kuitenkin laajentunut kattamaan myös tiettyjen rikosten estämisen jo varsin pian perusoikeusuudistuksen jälkeen. Näin pitkäaikainen ja vakiintunut perusoikeussäännöksen sanamuodosta eroava lainsäädäntökäytäntö on omiaan muuttamaan perusoikeussääntelyä sanonnallisesti harhaanjohtavaksi.

Luottamuksellisen viestin salaisuuden rajoittamista koskevassa tulkintakäytännössä on asetettu vaatimus konkreettisesta ja yksilöidystä rikosepäilystä (esim. PeVL 37/2002 vp; PeVL 5/1999 vp, s. 2—3). Tällainen on käsillä silloin, kun jonkun on syytä epäillä tekevän tai tehneen rangaistavaksi säädetyn teon. Näin ollen nykyisen tulkintakäytännön valossa ei ole mahdollista säätää perustuslain 10 §:n 3 momentin nojalla sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen tai selvittäminen vaan laajemmalti kansallisen turvallisuuden kannalta välttämättömän tiedon hankkiminen vakavista uhkista erityisesti uhkiin varautumiseksi ja niiden ennakoimiseksi sekä valtion ylimmän johdon päätöksenteon tueksi. Perustuslain 10 §:n 3 momentin sanamuoto ei mahdollista luottamuksellisen viestin salaisuuden suojaan puuttumista tiedustelutiedon hankkimiseksi sellaisesta esimerkiksi kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily, tai jota ei ole säädetty rangaistavaksi.

Suomeen ja sen väestöön mahdollisesti kohdistuvien uhkien tunnistamiseksi ja niiden torjumiseksi on tarpeen saada tietoa sotilaallisesta toiminnasta ja sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tiedonhankinnan kohteena oleva toiminta ei välttämättä olisi rangaistavaksi säädettyä tai edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily. Tiedontarpeet kohdistuvat esimerkiksi turvallisuusympäristön kehitykseen ja valtiojärjestystä tai yhteiskunnan perustoimintoja vakavasti uhkaavan toimintaan, kuten terrorismiin liittyvään toimintaan tai väkivaltaiseen radikalisoitumiseen taikka ulkomaisten tiedustelupalvelujen toimintaan.

Tietoa sotilaallisesta toiminnasta ja sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, on välttämätöntä hankkia myös sellaisilla tavoilla, jotka saattavat rajoittaa luottamuksellisen viestin salaisuuden suojaa nykyaikaisessa viestinnässä. Perusoikeussäännökset suojaavat luonnollisia henkilöitä. Lisäksi perusoikeussäännökset ulottuvat oikeushenkilöihin välillisesti. Sitä vastoin valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp, s. 23; ks. esim. PeVL 9/2015 vp). Näin ollen esimerkiksi vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, eikä pelkästään tällaisten organisaatioiden viesteihin kohdistuvista toimivaltuuksista säätäminen muodostuisi perustuslain 10 §:n 3 momentin kannalta ongelmalliseksi. Tiedustelutoimivaltuuksia ei kuitenkaan arvioida olevan mahdollista kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin. Arvioitaessa onko kyse luottamuksellisen viestin salaisuuden rajoittamisesta, on otettava huomioon EU-

tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö, jonka mukaan tietojen kerääminen tai jo pääsy niihin muodostaa puuttumisen yksityiselämän suojaan.

Luottamuksellisen viestin tunnistamistietojen suojaa on aikaisemmassa lainsäädäntökäytännössä arvioitu eri tavalla kuin viestin sisällön suojaa. Perustuslakivaliokunta on kuitenkin unionin tuomioistuimen Digital Rights Ireland -asiassa antaman tuomion jälkeen arvioinut, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp). Valiokunnan uusimmasta lausuntokäytännöstä ei ole vielä selvästi pääteltävissä, miten tällainen uudelleenarviointi muuttaa aiempaa perusoikeuksien yleisiin rajoittamisedellytyksiin nojaavaa tulkintalinjaa. Unionin tuomioistuin on Tele2 Sverige -ratkaisussaan toistanut Digital Rights Ireland -asiassa tietojen kokoamisesta ja yhdistämisestä tekemänsä huomiot. Sekä perustuslakivaliokunnan käytäntö että EU-tuomioistuimen ratkaisut huomioon ottaen tunnistamistietoja koskevaa aikaisempaa käytäntöä ei voida sellaisenaan ottaa perustaksi tietoliikennetiedustelua koskevalle sääntelylle. Tämäkin seikka huomioon ottaen luottamuksellisen viestin salaisuuden suojaa rajoittavista tiedustelutoimivaltuuksista ei ole mahdollista säätää tavallisella lailla perustuslakia muuttamatta.

Ehdotetussa siviili- ja sotilastiedustelulainsäädännössä olisi kyse Suomessa uudesta sääntelystä, jolla olisi merkittäviä vaikutuksia perus- ja ihmisoikeutena turvattuun yksityiselämän suojaan ja erityisesti luottamuksellisen viestin salaisuuden suojaan. Aikaisempien perustuslain uudistusten yhteydessä on kiinnitetty huomiota siihen, että perustuslain sisällön tulisi antaa oikea kuva tavallisella lainsäädännöllä toteutettavista perusratkaisuista. Tästäkin syystä on perusteltua, että nyt käsillä olevasta uudesta ja merkittävästä luottamuksellisen viestin salaisuuden suojaan puuttumisen perusteesta säädetään perustuslaissa. Perustuslakivaliokunta on lisäksi pitänyt nimenomaisesti epätyydyttävänä tilannetta, jossa perustuslain 10 §:n 3 momentin soveltamiskäytäntö on osin erkaantunut säännöksen kieliasusta, ja kehottanut valtioneuvostoa harkitsemaan, millaisiin toimenpiteisiin tämän seikan johdosta olisi ryhdyttävä. Valiokunta kiinnitti tässä yhteydessä huomiota luottamuksellisen viestin salaisuuden suojan lisäksi kotirauhan rajoittamista koskevaan perustuslakisääntelyyn. (PeVL 36/2017 vp, s. 4—5.)

## 3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on tarkistaa perustuslain sääntelyä niin, että lailla voidaan säätää tarpeellisiksi katsottavien edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin suojaan. Perustuslain tarkistetun säännöksen on oltava sopusoinnussa Suomen ihmisoikeusvelvoitteiden kanssa.

Valmistelussa on harkittu luottamuksellisen viestin salaisuuden suojaa koskevan sääntelyn tarkistamista niin, että perustuslain 10 §:stä poistettaisiin tältä osin kvalifioitu lakivaraus. Tällöin luottamuksellisen viestin salaisuuden suojaa voitaisiin rajoittaa perusoikeuksien yleisten rajoitusedellytysten mukaisesti. Tällaista sääntelyvaihtoehtoa ei kuitenkaan ole pidetty perusteltuna. Kvalifikaation poistaminen ei sopisi hyvin luottamuksellisen viestin salaisuuden perinteisestikin voimakkaasti suojattuun asemaan eikä perustuslain perusoikeusluvun systematiikkaan. Tällainen muutos edellyttäisi perusoikeusluvun kirjoitustavan tarkastelua laajemminkin.

Lisäksi valmistelussa on harkittu perustuslain 10 §:n tarkistamista niin, että siihen ainoastaan lisättäisiin maininta kansallisen turvallisuuden kannalta välttämättömästä luottamuksellisen viestin salaisuuden rajoittamisesta. Tällaisen, varsin yleisluontoisen rajoitusperusteen lisääminen 10 §:ään olisi kuitenkin jossakin määrin ristiriidassa sen kanssa, että perustuslain 10 §:ää edeltäneen hallitusmuodon 8 §:n säätämiseen johtanutta perusoikeusuudistusta valmisteltaessa pyrittiin täsmentämään perusoikeuksien rajoittamisperusteita. Tuolloin arvioitiin, ettei ero kvalifioidun ja yksinkertaisen lakivarauksen välillä muodostu kovin suureksi, jos rajoittamisen edellytykset kirjoitetaan kovin väljiksi (esim. yleinen järjestys ja turvallisuus). Samoin arvioitiin, että tulisi välttää rajoittamisperusteiden kuvaamista niin väljin ilmaisuin, että lakivarauksen normatiivinen teho olennaisesti heikkenee (perusoikeuskomitean muistio Perusoikeuksien rajoittamisesta, 26.3.1990).

Ehdotettujen uusien siviili- ja sotilastiedustelun toimivaltuuksien sitominen perustuslain 10 §:n mukaiseen yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten tutkintaan on myös poissuljettu valmistelussa. Suomeen ja sen väestöön mahdollisesti kohdistuvien uhkien tunnistamiseksi ja niiden torjumiseksi luottamuksellisen viestin suoja tulee voida hyväksyttävillä perusteilla murtaa myös tilanteissa, joissa tiedonhankinnan kohteena oleva toiminta ei olisi rangaistavaksi säädettyä tai edennyt niin pitkälle, että siihen voitaisiin kohdistaa rikosepäily. Myöskään poliisi-, pakkokeino- ja puolustusvoimien rikostorjuntalain mukaisten salaisten pakkokeinojen soveltamisalaa ei ole katsottu mahdolliseksi laajentaa tässä tarkoituksessa nykyisestä.

Perustuslain 10 §:ää ehdotetaan muutettavaksi siten, että siihen lisätään uusi 4 momentti, johon otetaan luottamuksellisen viestin salaisuuden rajoittamista koskeva sääntely. Momentissa ehdotetaan säädettäväksi, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Muutoksella lisättäisiin erityiseen rajoituslausekkeeseen uusia hyväksyttäviä perusteita rajoittaa luottamuksellisen viestin salaisuutta.

Perustuslain 10 §:n 4 momentin alkuosa vastaisi asiasta nykyisin 10 §:n 3 momentissa säädettyä muuten, mutta ilmaisu ”rikosten tutkinnassa” korvattaisiin ilmaisulla ”rikosten torjunnassa”. Ilmaisu rikosten torjunta käsittäisi rikosten ennalta estämisen, paljastamisen ja selvittämisen. Muutoksella ei ole tarkoitus muuttaa oikeustilaa siitä, millaiseksi se on muodostunut nykyisen perustuslain 10 §:n 3 momentin tulkintakäytännössä, vaan tarkistaa säännöksen sanamuoto vastaamaan perustuslakivaliokunnan vakiintunutta tulkintaa.

Perustuslain 10 §:n 3 momentissa käytetyn ilmaisun ”rikosten tutkinta” tulkinta on erkaantunut säännöksen sanamuodosta jo varsin pian perusoikeusuudistuksen jälkeen. Rikoksen tutkintana on tulkintakäytännössä voitu pitää myös sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei vielä olisi ehtinyt toteutuneen teon asteelle. Näin ollen esimerkiksi televalvontaa on katsottu perustuslain 10 §:n 3 momentin estämättä voitavan käyttää tiettyjen rikosten estämiseen (PeVL 5/1999 vp; PeVL 2/1996 vp).

Uudessa 4 momentissa mahdollistettaisiin lisäksi luottamuksellisen viestin salaisuuden rajoittaminen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Luottamuksellisen viestin salaisuuden rajoittaminen olisi sidottu tiedon hankkimiseen säännöksessä tarkoitetusta toiminnasta. Perustuslain 10 §:ään ehdotetun uuden säännöksen arvioidaan sisällöltään ja kirjoitustavaltaan sopivan hyvin yhteen pykälän 3 momenttiin jo sisältyvien rajoituslausekkeiden kanssa.

Perustuslain 10 §:n 4 momenttiin ehdotettu uusi rajoitusperuste olisi muotoiltu niin, että sen perusteella voitaisiin tavallisessa laissa säätää tiedustelua koskevista toimivaltuuksista. Säännös rajoittaisi osin merkittävästikin sitä, millä edellytyksillä toimivaltuuksista voitaisiin säätää. Luottamuksellisen viestin salaisuuden rajoittamisen perusteena voisi olla tiedon hankkiminen vain sotilaallisesta toiminnasta tai sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tiedon hankkimisen kohteena olevalle toiminnalle asetettaisiin näin ollen korkea kynnys.

Ehdotetulla muutoksella lisättäisiin erityiseen rajoituslausekkeeseen uusi hyväksyttävä peruste rajoittaa luottamuksellisen viestin salaisuutta. Muihin rajoitusedellytyksiin perustuslain 10 §:ssä ei ehdoteta muutosta. Lisäksi perusoikeuksien yleiset rajoitusedellytykset tulevat sellaisinaan sovellettaviksi.

Säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiinkin kuuluvasta välttämättömyysvaatimuksesta ja vaatimuksesta rajoituksen sopusoinnusta kansainvälisten ihmisoikeusvelvoitteiden kanssa samoin kuin EU-oikeudesta seuraa vaatimuksia muun muassa toimivaltuuksien yksilöimiselle. Ehdotettu sääntely ei siten mahdollistaisi yleisestä, kohdentamattomasta ja kaikenkattavasta tietoliikenteen seurannasta säätämistä.

## 4 Esityksen vaikutukset

Perustuslain 10 §:n luottamuksellisen viestin salaisuutta koskevaa sääntelyä ehdotetaan muutettavaksi ensinnäkin niin, että siinä mainitaan sanotun perusoikeuden hyväksyttävänä rajoitusperusteena yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnan sijaan tällaisten rikosten torjunta. Ehdotuksella ei ole tarkoitus muuttaa oikeustilaa siitä, millaiseksi se on muodostunut perustuslain 10 §:n 3 momentin tulkintakäytännössä.

Perustuslain 10 §:ään ehdotetaan myös otettavaksi säännös siitä, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Ehdotettu muutos mahdollistaisi sellaisen lainsäädännön, jolla rajoitetaan luottamuksellisen viestin salaisuutta uusilla perusteilla. Käytännössä muutoksella mahdollistettaisiin tiedustelutoimivaltuuksia koskevan lainsäädännön säätäminen.

Ehdotettu perustuslain säännös mahdollistaa nykyistä laajemman puuttumisen luottamuksellisen viestin salaisuuden suojaan. Luottamuksellisen viestin salaisuuden suojaan puuttumista rajoittavat kuitenkin niin säännökseen ehdotetut verrattain tiukat edellytykset kuin perusoikeuksien yleiset rajoittamisedellytykset. Sääntelyn yksityiskohtaiset vaikutukset riippuvat viime kädessä ehdotetun perustuslain säännöksen mahdollistaman tavallisen lain tasoisen sääntelyn sisällöstä.

Ehdotetun säännöksen perusteella voidaan lailla säätää sellaisista tiedonhankintatoimivaltuuksista, jotka ovat välttämättömiä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sääntelyn tavoitteet kiinnittyvät näin ollen niin valtion itsemääräämisoikeuden ja toiminnan kuin myös väestön turvallisuuden varmistamiseen.

Ehdotetulla sääntelyllä ei ole välittömiä taloudellisia vaikutuksia tai vaikutuksia viranomaisten toimintaan. Kuitenkin perustuslain 10 §:n 4 momenttiin otettavaksi ehdotetun uuden rajoitus-

perusteen mahdollistamalla tiedustelulainsäädännöllä arvioidaan olevan osin merkittäviäkin vaikutuksia. Kansainvälisistä ihmisoikeussopimuksista ja perusoikeuksien yleisistä rajoitusedellytyksistä seuraa vaatimus tiedustelutoiminnan asianmukaisesta valvonnasta, millä arvioidaan olevan niin taloudellisia vaikutuksia kuin vaikutuksia viranomaisten toimintaan. Lupa- ja valvontaviranomaisilla tulee olla riittävät resurssit ja niiden henkilöstöllä tulee olla niin oikeudellista kuin teknistä osaamista.

## 5 Asian valmistelu

### 5.1 Valmisteluvaiheet ja -aineisto

Luonnos hallituksen esitykseksi valmisteltiin oikeusministeriön 28.9.2015 asettamassa asiantuntijatyöryhmässä. Työryhmän tehtävänä oli selvittää ja valmistella myöhemmin asetettua parlamentaarista valmisteluvaihetta varten perustuslain tarkistamista siten, että lailla voidaan tarpeellisiksi katsottavien edellytysten täyttyessä säätää kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan. Työryhmä kuuli työnsä aikana valtiosääntöoikeuden sekä siviili- ja sotilastiedustelun asiantuntijoita sekä teetti tarvitsemansa selvitykset. Työryhmä toimi 11.12.2015 asetetun parlamentaarisen seurantaryhmän seurannassa.

Työryhmän mietintö (Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen, oikeusministeriö, mietintöjä ja lausuntoja 41/2016) valmistui 23.9.2016 ja se julkaistiin 11.10.2016. Työryhmä ehdotti perustuslain 10 §:ää muutettavaksi niin, että siihen lisättäisiin uusi 4 momentti, johon koottaisiin säännökset luottamuksellisen viestin salaisuuden rajoittamisen edellytyksistä. Lailla voitaisiin ehdotuksen mukaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

### 5.2 Lausunnot ja niiden huomioon ottaminen

Työryhmän mietintö lähettiin lausuntokierrokselle 1.11.2016. Lausunnon antoi kaikkiaan 30 tahoa, joista 12 on viranomaisia ja 14 yhteisöjä sekä neljä yksityishenkilöitä. Lausunnoissa esitetyt kommentit kohdistuivat pääosin perustuslain muutosehdotuksen perusteluihin. Lisäksi tehtiin pykälätekstin muotoiluehdotuksia.

Suurin osa lausunnonantajista piti perustuslain muutosta tarpeellisena ja tarkoituksenmukaisena. Lausunnonantajat olivat laajasti yksimielisiä kvalifioidun lakivarauksen säilyttämistarpeesta perustuslain 10 §:ssä. Vakavaa uhkaa kansalliselle turvallisuudelle pidettiin sinänsä hyväksyttävänä perusteena luottamuksellisen viestin suojan jonkinasteiselle rajoittamiselle. Lisäksi lausunnoissa yhdyttiin laajasti työryhmän näkemykseen siitä, että perustuslain sanamuoto tulisi saattaa vastaamaan vakiintunutta soveltamiskäytäntöä rikostutkintaa koskevan viestinnän suojasta. Mietinnön ehdotuksiin kielteisesti suhtautuneissa lausunnoissa viitattiin siihen, ettei muutos ole välttämätön tai että sen tavoitteet voidaan saavuttaa muilla tavoilla. Varsin yleisesti tuotiin esille tarve sotilaallisen toiminnan ja kansallisen turvallisuuden käsitteiden tarkemmalle määrittelylle ja rajauksille ehdotuksen perusteluissa.

Useat lausunnonantajat ehdottivat niin sanotun massavalvonnan kiellon kirjaamista joko perustuslain 10 §:ään tai muutosehdotuksen perusteluihin. Lisäksi nähtiin täsmentämistarpeita ajallista ulottuvuutta koskevissa perustelujen kirjauksissa. Esille nostettiin myös tarve kattavammalle ja perusteellisemmalle Euroopan ihmisoikeustuomioistuimen ja EU-tuomioistuimen oikeuskäytännön huomioon ottamiselle sekä kansainvälisen vertailun syventämiselle. Lausunnoista on laadittu oikeusministeriössä lausuntotiivistelmä (Lausuntotiivistelmä mietinnöstä ”Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen”, oikeusministeriö, 29.6.2017).

Hallituksen esitys on viimeistelty oikeusministeriössä työryhmän mietinnön ja siitä saatujen lausuntojen pohjalta parlamentaarisen seurantaryhmän seurannassa.

## 6 Riippuvuus muista esityksistä

Esitys kytkeytyy sisäministeriössä ja puolustusministeriössä valmisteltuihin hallituksen esityksiin, joissa ehdotetaan säädettäväksi siviili- ja sotilastiedustelusta. Esitys liittyy myös oikeusministeriössä valmisteltuun hallituksen esitykseen, jossa ehdotetaan lain säätämistä tiedustelutoiminnan valvonnasta. Lisäksi esityksellä on kytkös tiedustelutoiminnan parlamentaarisen valvonnan järjestämiseksi eduskunnassa valmisteltuun puhemiesneuvoston ehdotukseen eduskunnan työjärjestyksen muuttamisesta.

## YKSITYISKOHTAISET PERUSTELUT

### 1 Lakiehdotuksen perustelut

**10 §.** *Yksityiselämän suoja.* Pykälään ehdotetaan lisättäväksi uusi 4 momentti siten, että nykyisen 3 momentin jälkimmäinen virke siirretään sisällöltään tarkistettuna 4 momenttiin.

Pykälän 4 momentissa ehdotetaan säädettäväksi, että lailla voidaan säätää välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Pykälän 4 momenttiin koottaisiin siten säännökset luottamuksellisen viestin salaisuuden suojan rajoittamisesta. Momentin alkuosa vastaisi muuten asiasta nykyisin 10 §:n 3 momentissa säädettyä, mutta ilmaisu ”rikosten tutkinnassa” korvattaisiin uudella ilmaisulla ”rikosten torjunnassa”. Momentin loppuosa olisi uusi.

Perustuslain 10 §:n 3 momentissa käytetyn ilmaisun ”rikosten tutkinnassa” tulkinta erkaantui säännöksen sanamuodosta jo varsin nopeasti vuoden 1995 perusoikeusuudistuksen jälkeen. Perustuslakivaliokunnan mukaan sanottu ilmaisu voidaan pelkin kielellisin perustein ymmärtää tarkoittavan vain jo tehtyjä rikoksia, mutta käytännössä ei ole kuitenkaan mahdollista vetää täsmällistä rajaa rikoksen tekohetken mukaan. Monien rikosten luonteesta johtuu, että niiden selvittäminen ei ole mahdollista, mikäli rikoksen tekeminen ei ylipäätään paljastu, mikä puolestaan saattaa vaatia ennakollista varautumista rikoksen tapahtumiseen (PeVL 2/1996 vp). Siten rikoksen tutkintana on tulkintakäytännössä voitu pitää myös sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei vielä olisi ehtinyt toteutuneen teon asteelle (PeVL 5/1999 vp; PeVL 2/1996 vp).

Ehdotuksella ei ole tarkoitus muuttaa oikeustilaa siitä, millaiseksi nykyisen perustuslain 10 §:n 3 momentin tulkinta on muotoutunut eduskunnan perustuslakivaliokunnan lausuntokäytännössä. Ehdotuksessa käytetty ilmaisu ”rikosten torjunta” käsittäisi siten rikosten ennalta estämisen, paljastamisen ja selvittämisen. Voimassa olevassa, perustuslakivaliokunnan myötävaikutuksella säädetyssä lainsäädännössä ilmaisu ”rikostorjunta” kattaa nämä mainitut toiminnat. Kielellisesti ”rikosten torjunta” sopii kuitenkin perustuslain tekstiin paremmin.

Momentissa säädettäisiin uusi hyväksyttävä peruste luottamuksellisen viestin salaisuuden suojan rajoittamiselle, ”tiedon hankkiminen sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Uudessa rajoitusperusteessa irtauduttaisiin rikosperusteisesta toiminnasta. Kyse olisi tiedonhankinnasta säännöksessä mainituista toiminnoista, joihin ei voida (ainakaan vielä tiedonhankintavaiheessa) kohdistaa konkreettista ja yksilöityä rikosepäilyä. Säännöksessä tarkoitetusta toiminnasta säädettäisiin tarkemmin tavallisella lailla.

Sotilaallisella toiminnalla säännöksessä tarkoitettaisiin sotilaallisesti järjestäytyneiden joukkojen toimintaa tai sotilaallisiin voimakeinoihin, kuten aseistukseen ja sotatarvikkeisiin liittyvää toimintaa taikka muuta näihin rinnastuvaa, sotavoimaa käyttävien joukkojen toimintaa. Kyse voisi olla sekä valtiollisesta että ei-valtiollisesta toiminnasta. Valtiollinen toiminta palautuu jonkin vieraan valtion asevoimien toimintaan tai siihen rinnastuvaan kansainvälisen, sotilaallisen liittouman tai järjestön toimintaan, kun taas ei-valtiollisella toiminnalla tarkoitetaan sel-

laista sotilaallisesti järjestettyä, aseistettua tai varustettua toimintaa, jolla ei ole edellä tarkoitettua valtiollista alkuperää tai sitä ei voida tunnistaa. Tiedon hankkiminen säännöksessä tarkoitetusta sotilaallisesta toiminnasta ei edellyttäisi, että tällaisesta toiminnasta aiheutuu vakavaa uhkaa kansalliselle turvallisuudelle. Sotilaallista toimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan tarvitsisi olla välittömästi uhkaavaa seurannan aikana.

Tiedon hankkiminen sisältäisi Suomeen kohdistuvien sotilaallisten ulkoisten toimenpiteiden kartoittamisen ja seuraamisen. Kyse olisi esimerkiksi Suomen turvallisuusympäristön kannalta merkityksellisen sotilaallisen toiminnan kehityksen seuraamisesta tilannekuvan muodostamiseksi. Ilmaisu kattaisi muun muassa jatkuvan tiedonhankinnan muiden maiden sotilaallisen suorituskyvyn kehittymisestä samoin kuin tiedonhankinnan Suomen maanpuolustukseen kohdistuvasta ulkomaisesta sotilastiedustelusta.

Vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Tällaisen viestinnän havaitsemiseksi voi kuitenkin olla välttämätöntä puuttua luottamuksellisen viestinnän salaisuuteen. Esimerkiksi tietoliikenteeseen kohdistuvassa tiedustelussa vieraan valtion viranomaisten käyttämän viestintäverkon osan yksilöiminen saattaa teknisesti edellyttää muuhun viestintään puuttumista. Tämän vuoksi tiedonhankintatoimivaltuuksien sääntelylle asettuu perusoikeusjärjestelmästä vaatimuksia myös vieraiden valtioiden toiminnan seurannassa.

Säännöksessä säädettäisiin myös mahdollisuudesta rajoittaa luottamuksellisen viestin salaisuuden suojaa tiedon hankkimiseksi sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Ilmaisua ”kansallinen turvallisuus” käytetään jo nykyisessä lainsäädännössä. Se esiintyy myös Euroopan unionin oikeusjärjestyksessä ja kansainvälisissä ihmisoikeussopimuksissa ihmisoikeuksien rajoitusperusteena. Käsitteelle ei ole annettu sen yleiskielen merkitystä tarkempaa sisältöä unionin oikeusjärjestyksessä tai ihmisoikeusvelvoitteissa. Esimerkiksi Euroopan ihmissoikeussopimuksen tulkinnassa valtioilla on katsottu olevan varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan (esim. Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010). Euroopan ihmisoikeustuomioistuin on kuitenkin asettanut salaisia tiedonhankintamenetelmiä koskevalle lainsäädännölle vähimmäisvaatimuksia, joiden tarkoituksena on estää mielivaltainen puuttuminen yksilön luottamuksellisen viestin suojaan (esim. Zakharov v. Venäjä, 4.12.2015). Euroopan unionin oikeuden soveltamisalalla käsitteitä yleinen tai kansallinen turvallisuus tulee tulkita unionin oikeuden ja näitä käsitteitä täsmentävän Euroopan unionin tuomioistuimen oikeuskäytännön valossa. EU-tuomioistuin lähtee vakiintuneesti siitä, etteivät jäsenvaltiot voi kukin yksinään ilman unionin toimielinten valvontaa määritellä unionin oikeuden soveltamiseen liittyen sellaisten käsitteiden kuin yleinen tai kansallinen turvallisuus ulottuvuuksia. (Ks. esim. tuomio J.N., C-601/15, 65—66 kohta.)

Kansallisella turvallisuudella säännöksessä viitataan viime kädessä valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiiviseen turvallisuuteen välittömästi tai välillisesti väkivaltaista ulkoista uhkaa vastaan. Kansallista turvallisuutta vakavasti uhkaavaa on tyypillisesti sellainen yleisvaarallinen ja siihen liittyvä toiminta, joka uhkaa suuren ja ennalta arvaamattoman, sattumanvaraisesti määräytyvän ihmisjoukon henkeä tai terveyttä. Tällaista on esimerkiksi terrorismiin, väkivaltaiseen radikalisoitumiseen taikka joukkotuhoaseisiin tai kansainvälisen rauhan ja turvallisuuden vaarantamiseen liittyvä muu toiminta.

Kansallisen turvallisuuden kannalta keskeisiä ovat sellaiset yhteiskunnan perustoiminnot, joiden häirintä tai lamauttaminen saattaisi viime kädessä johtaa ihmisten hengen tai terveyden vakavaan vaarantumiseen. Tällaisiin kuuluvat esimerkiksi sähkö-, viestintä- ja liikenneverkot

taikka elintarvike- ja lääkehuoltoa tai kansallista huoltovarmuutta kaiken kaikkiaan ylläpitävät toiminnot. Niihin kohdistuva uhka voi ilmetä avoimen väkivallan lisäksi esimerkiksi tietoverkkoon kohdistuvina hyökkäyksinä tai erilaisten keinojen yhdistelminä. Kansallista turvallisuutta vakavasti uhkaavaa voi siten olla yhteiskunnan perustoimintojen häiritsemiseen tai lamauttamiseen tähtäävä taikka perustoimintojen häirinnän tai lamauttamisen mahdollistamiseen liittyvä toiminta.

Kansanvaltainen valtio- ja yhteiskuntajärjestys ja kansanvaltaisen yhteiskunnan instituutiot muodostavat perustan yhteisössä elävien ja toimivien ihmisten turvallisuudelle. Kansallisen turvallisuuden kannalta on merkityksellistä, että ylimmät valtioelimet ja muut julkisen vallan toimielimet samoin kuin esimerkiksi yhteiskunnan perustoiminnoista huolehtivat voivat hoitaa tehtäviään ilman ulkoista häirintää. Kansallista turvallisuutta vakavasti uhkaavaa voi siten olla sellainenkin ulkoinen toiminta, joka tähtää kansanvaltaisen yhteiskunnan ja sen instituutioiden häirintään tai niiden toiminnan lamauttamiseen taikka mahdollistaa niiden toiminnan häirinnän tai lamauttamisen.

Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitettaisiin säännöksessä siten kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Edellytyksenä olisi kuitenkin se, että toiminnalla olisi jokin kytkentä Suomeen ja että se uhkaisi nimenomaan Suomen kansallista turvallisuutta, vaikka toiminta voisikin maantieteellisesti tapahtua Suomen rajojen ulkopuolella.

Säännöksessä tarkoitettu toiminta voisi olla sellaista, joka käytännön toimenpiteisiin edetessään olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin kyse voisi olla toiminnasta, joka ei lähtökohtaisesti ole Suomen lain mukaan rikos tai joka ei edetessäänkään voisi kehittyä rikokseksi, kuten ulkomaisten tiedustelupalvelujen laillinen toiminta Suomessa. Vaikkakin valtioiden harjoittama tiedustelutoiminta on maailmanlaajuisesti luonteeltaan vakiintunutta, ja valtiot sitä tosiasiassa toisiltaan tiettyyn rajaan asti sietävät, se voi jo ominaispiirteiltään muodostaa riskitekijöitä kansalliselle turvallisuudelle. Myös vakavat levottomuudet Suomen turvallisuuden kannalta keskeisen valtion alueella tai vakava rajaturvallisuuden vaarantuminen voivat muodostaa vakavan uhan kansalliselle turvallisuudelle.

Ilmaisu ”kansallinen turvallisuus” tarkoittaisi sitä, ettei säännöksessä tarkoitettu uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön. Kuitenkin myös esimerkiksi yksityishenkilöihin kohdistuvat väkivallanteot voisivat olla säännöksessä tarkoitettua toimintaa, jos ne laajuudeltaan tai merkitykseltään olisivat kansallisen turvallisuuden kannalta merkittäviä ja voisivat siten muodostaa vakavan uhan sille. On selvää, että esimerkiksi valtiojohtoon tai yhteiskunnan perustoiminnoista huolehtiviin henkilöihin samoin kuin heidän turvallisuusjärjestelyistään vastaaviin kohdistuvat uhat voivat muodostaa vakavan uhan kansalliselle turvallisuudelle.

Niin ikään Suomen kansainväliseen kriisinhallinta- tai avunantotehtäviin osallistuviin viranomaisiin tai henkilöihin kohdistuva uhkaava toiminta voisi olla säännöksessä tarkoitettua. Kriisinhallinta- ja avunantotehtävissä on kysymys Suomen valtion toiminnasta, jossa Suomi lähettää kriisinhallinta- ja avunantohenkilöstöään kansainvälisen rauhan ja turvallisuuden ylläpito- tai palauttamistehtäviin taikka humanitäärisiin avustustehtäviin. Tällainen toiminta sijoittuu alueille tai tilanteisiin, joissa on usein korkea turvallisuusriski. Suomen tällaiseen toimintaan ja näistä tehtävistä vastaaviin viranomaisiin ja henkilöihin kohdistuva uhka rinnastuisi siten kansallisen turvallisuuden uhkaan. Heihin kohdistuva uhka voi olla luonteeltaan myös sotilaallista. Tällaisilta uhilta suojautumiseksi lailla voidaan ehdotuksen mukaan säätää rajoi-

tuksia luottamuksellisen viestin salaisuuden suojaan tiedon hankkimiseksi sotilaallisesta toiminnasta tai kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Ilmaisu ”kansallinen turvallisuus” sisältäisi myös sen, ettei tietoa uhkaavasta toiminnasta voisi hankkia mikä tahansa turvallisuuteen liittyviä tehtäviä hoitava viranomainen, vaan tiedonhankinta voitaisiin lailla osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten tehtäväksi. Nykyisessä valtion organisaatiossa tällaiset tehtävät on osoitettu suojelupoliisille siviilitiedustelun osalta ja puolustusvoimille, sen pääesikunnalle ja tiedustelulaitokselle, sotilastiedustelun osalta.

Tiedonhankinta kansallisesta turvallisuudesta huolehtimiseksi samoin kuin ehdotetussa säännöksessä tarkoitetusta sotilaallisesta toiminnasta rajaa myös sitä, kenen käyttöön tietoja hankitaan. Kyse olisi tiedonhankinnasta valtion ylimmälle johdolle tilannekuvan muodostamiseksi ja päätöksenteon tueksi sekä kansallisten turvallisuusviranomaisten lakisääteistä toimintaa varten.

Säännös edellyttää sen soveltamisalan piiriin kuuluvalta toiminnalta, että siitä aiheutuu vakavaa uhkaa kansalliselle turvallisuudelle. Vakavuusedellytys nostaa säännöksen soveltamiskynnystä asettaessaan kvalifioinnin uhan laadusta. Siten pelkästään jonkinasteisen uhan kansalliselle turvallisuudelle muodostava toiminta ei vielä täyttäisi säännöksessä asetettua vaatimusta. Uhan vakavuusaste kytkeytyy myös edellä käsiteltyihin sisällöllisiin määrittelyihin siitä, millainen toiminta muodostaa säännöksessä tarkoitettua uhkaa. Lailla voitaisiin siten säätää rajoituksia luottamuksellisen viestin salaisuuden suojaan tiedon hankkimiseksi vain sellaisesta toiminnasta, joka luonteensa takia voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle.

Ilmaisulla ”uhkaa” tarkoitetaan sitä, ettei säännöksessä edellytettäisi kansallisen turvallisuuden olevan välittömästi vaarantumassa. Näin ollen säännöksessä tarkoitettu tiedonhankinta voisi koskea myös toimintaa, joka jatkuessaan vaarantaisi kansallista turvallisuutta.

Kansallista turvallisuutta vakavasti uhkaava toiminta olisi käsitteenä erillinen perustuslain 23 §:ssä tarkoitetusta kansakuntaa uhkaavista poikkeusoloista, jotka kiinnittyvät kansainvälisten ihmisoikeussopimusten mukaiseen yleisen hätätilan käsitteeseen ja joissa on kyse vakavasta uhasta kansakunnan elämälle ja olemassaololle (ks. HE 60/2010 vp, s. 36).

Säännösehdotuksen mukainen uusi rajoitusperuste merkitsisi käytännössä sitä, että tavallisen lain tasolla säädettävät viranomaisten uudet, luottamuksellisen viestin salaisuuden suojaa rajoittavat tiedonhankintatoimivaltuudet rajautuisivat vain säännösehdotuksessa tarkoitettuun toimintaan ja että toimivaltuuksien kohdentamisesta tällaiseen toimintaan tulisi säätää laissa tyhjentävästi.

Ehdotetulla muutoksella lisättäisiin perustuslain 10 §:n erityiseen rajoituslausekkeeseen uusi hyväksyttävä peruste rajoittaa luottamuksellisen viestin salaisuuden suojaa. Muihin perustuslain 10 §:ssä säädettyihin rajoitusedellytyksiin ei ehdoteta muutoksia, vaan ne säilyisivät nykyisellään. Lisäksi viestin salaisuuden suojaa rajoitettaessa sovellettaisiin sellaisenaan perusoikeuksien yleisiä rajoitusedellytyksiä (ks. niistä PeVM 25/1994 vp, s. 5).

Luottamuksellisen viestin salaisuuden suojan rajoittamisen on oltava nykyisen perustuslain 10 §:n 3 momentin mukaan välttämätöntä. Tämä edellytys seuraa myös perusoikeuksien yleisistä rajoitusedellytyksistä. Asian merkityksen, sääntelyn systematiikan ja useiden ns. kvalifioitujen lakivarausten kirjoitustavan vuoksi välttämättömyys mainittaisiin säännöksessä edelleen erikseen. Välttämättömyys tarkoittaisi, että rajoitus on sallittu vain, jollei hyväksyttävä

tavoite (tiedon hankkiminen säännöksessä tarkoitetusta toiminnasta) ole saavutettavissa luottamuksellisen viestin salaisuuteen vähemmän puuttuvin keinoin. Välttämättömyyskriteeri pitäisi sisällään vaatimuksen luottamuksellisen viestin salaisuuden suojaan puuttumisesta mahdollisimman kohdennetusti ja rajoitetusti.

Perusoikeuksien yleisiin rajoitusedellytyksiin kuuluu vaatimus, jonka mukaan perusoikeusrajoitusten on oltava sopusoinnussa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa. Tässä yhteydessä on erityinen merkitys Euroopan ihmisoikeussopimuksella, sellaisena kuin sen sisältö näyttäytyy Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Ihmisoikeustuomioistuimen oikeuskäytännön mukaan luottamuksellisen viestinnän salaisuuden rajoitukselle on aina oltava painava yhteiskunnallinen tarve, puuttumisen ja tavoiteltavan hyväksytyn päämäärän tulee olla oikeassa suhteessa keskenään ja puuttumiselle pitää olla riittävän painavat ja hyväksyttävät perustelut. Lisäksi rajoitusten on oltava lain sallimia. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä on painotettu lain laatua, kuten täsmällisyyttä sekä viranomaistoiminnan ennustettavuutta turvaavaa ja vallan väärinkäyttöä estävää sääntelyä.

Ihmisoikeustuomioistuin on pitänyt luottamuksellisen viestin salaisuuden rajoittamisen välttämättömyyden ja lainmukaisuuden kannalta ongelmallisena muun muassa tiedusteluviranomaisille laissa säädettyä rajoittamatonta toimivaltaa määritellä luottamuksellisiin viesteihin puuttumisen edellytykset (Zakharov v. Venäjä, 4.12.2015). Myös Euroopan unionin oikeus edellyttää tiedonhankinnan perustumista unionin perusoikeusjärjestelmän kannalta hyväksyttäviin päämääriin sekä sitä, ettei tiedonhankinnalla puututa yksityiselämän suojaan suhteettomasti tai tämän oikeuden keskeistä sisältöä loukaten. Euroopan unionin tuomioistuimen oikeuskäytännössä on erityisesti painotettu sitä, että tiedonhankinnan on oltava riittävän kohdennettua ja yksilöityä (tuomio Tele2 Sverige, C-203/15 ja C-698/15; tuomio Schrems, C-362/14; tuomio Digital Rights Ireland, C-293/12 ja C-594/12).

Välttämättömyysvaatimuksesta johtuu, ettei ehdotettu perustuslain 10 §:n 4 momentti salli rajoittamatonta puuttumista luottamuksellisen viestin salaisuuden suojaan. Ehdotettu sääntely ei siten mahdollista yleistä, kohdentamatonta ja kaiken kattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Tällaista kieltoa ei kuitenkaan ole tarpeen ottaa perustuslain tekstiin, sillä kielto seuraa jo välttämättömyysvaatimuksesta samoin kuin perusoikeuksien yleisistä rajoitusedellytyksistä. Ehdotettu säännös edellyttäisi rajoituksilta välttämättömyyden ohella oikeasuhtaisuutta. Rajoitusten tulee olla oikeassa suhteessa niillä tavoiteltuihin hyväksyttäviin päämääriin nähden. Rajoitusten tulee olla myös sopusoinnussa kansainvälisten ihmisoikeusvelvoitteiden ja Euroopan unionin oikeuden kanssa. Tavallisen lain tasoisessa sääntelyssä olisi näin ollen säädettävä tiedonhankintatoimivaltuuksien yksilöimisestä, toimivaltuuksien käytön yleisistä ja erityisistä edellytyksistä sekä niiden käytössä noudatettavista periaatteista.

Perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvan oikeusturvavaatimuksen vuoksi on lisäksi selvää, että tavallisen lain tasoisessa sääntelyssä on huolehdittava riittävistä oikeusturva- ja valvontajärjestelyistä. Oikeusturvavaatimuksella on läheinen yhteys myös oikeudenmukaista oikeudenkäyntiä ja hyvää hallintoa koskevaan perustuslain 21 §:ään. Tilanteisiin, joihin ei voida liittää muutoksenhakumahdollisuutta perusoikeuksia rajoitettaessa, kuten tiedustelutoiminnassa, on välttämätöntä luoda korvaavia oikeusturvajärjestelyjä. Näistä syistä uuteen 4 momenttiin ei ehdoteta otettavaksi nimenomaisia säännöksiä oikeusturva- tai valvontamenettelyistä tiedonhankintatoimivaltuuksien käytössä. Tällaisia mainintoja ei ole nykyisessäkään perustuslain 10 §:n 3 momentissa eikä muissakaan perusoikeusäännöksissä.

Nykyisten rikosperusteisten, salaisten tiedonhankintatoimivaltuuksien käytössä edellytetään pääsääntöisesti tuomioistuimen antamaa lupaa silloin, kun puututaan luottamuksellisen viestin

salaisuuden suojaan. Tuomioistuinmenettelyn on määrä estää toimivaltuuksien väärinkäyttö. Menettelyssä on keskeistä sen arviointi, täyttääkö lupahakemuksessa tarkoitettu tiedonhankintakeino tapauskohtaisesti laissa säädetyt edellytykset tosiseikaston ja muiden asiaan vaikuttavien tekijöiden osalta. Oikeusturvajärjestelyt voivat sisältää myös muita menettelyllisiä takeita, kuten velvollisuuden ilmoittaa tiedustelusta tiedonhankinnan kohteelle, yksilön mahdollisuuden riittävien oikeussuojakeinojen käyttöön ja tiedustelutoimivaltuuksien käytön dokumentointivelvoitteen samoin kuin rajoitukset tiedustelulla saadun tiedon käytölle sekä muiden perusoikeuksien suojaamiseen palautuvat rajoitukset tiedonhankinnalle, kuten lähdesuojan turvaaminen.

Vaatimukset oikeusturvajärjestelyjen ja valvonnan tehokkuudesta ja asianmukaisuudesta korostuvat erityisesti tiedustelutoiminnassa verrattuna nykyisen sääntelyn mahdollistamaan luottamuksellisen viestin salaisuuden suojan rajoittamiseen. Tämä johtuu paitsi siitä, että ehdotettu muutos mahdollistaa säädettäväksi lailla uusista viranomaistoimivaltuuksista, myös siitä, että muutosehdotuksen mahdollistamat toimivaltuudet saattavat tiedustelutoiminnan erityispiirteistä johtuen poiketa kohdentamiseltaan esimerkiksi nykyisistä rikosperusteisista salaisista tiedonhankintakeinoista. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta. Uusista toimivaltuuksista säädettäessä on huolehdittava riittävän parlamentaarisen valvonnan sekä tehokkaan ja riippumattoman laillisuusvalvonnan järjestämisestä. Laillisuusvalvonnalle on osoitettava vahvat toimivaltuudet puuttua tarvittaessa tiedusteluviranomaisten toimintaan yksilön oikeusaseman ja perusoikeuksien suojaamiseksi sekä toiminnan lainmukaisuuden varmistamiseksi.

## 2 Voimaantulo

Laki ehdotetaan tulevaksi voimaan mahdollisimman pian sen säätämisjärjestys huomioon ottaen.

## 3 Säätämisjärjestys

Esitys koskee perustuslain muuttamista. Se on siksi käsiteltävä perustuslain 73 §:ssä säädetyssä järjestyksessä.

Perustuslakivaliokunta on perustuslain suhteelliseen pysyvyyteen ja valtio-oikeudelliseen asemaan liittyvien näkökohtien vuoksi pitänyt tärkeänä, että perustuslain tekstin muutokset käsitellään pääsäännön mukaan perustuslain 73 §:n 1 momentin mukaisessa, ns. normaalissa perustuslainsäätämisjärjestyksessä. Perustuslain 73 §:n 2 momentin mukaista nopeutettua menettelyä ei valiokunnan mielestä tule käyttää, ellei perustuslain sanamuodon kiireelliselle muuttamiselle ole poikkeuksellisesti välttämätöntä tarvetta. (PeVM 5/2005 vp, s. 6.) Valiokunta on pitänyt varsin tärkeänä, ettei perustuslain kiireellistä muuttamismenettelyä käytetä muutoin kuin pakottavissa tilanteissa ja että perustuslain tavallinen muuttamismenettely vakiintuu pääsäännöksi myös käytännössä (PeVM 10/2006 vp, s. 6).

Siviili- ja sotilastiedustelulainsäädäntöä koskevissa hallituksen esityksissä on selvitetty seikkaperäisesti Suomen turvallisuustilanteen heikkenemiseen ja monimutkaistumiseen liittyviä näkökohtia. Suomen turvallisuustilanteen muutokseen ovat vaikuttaneet muun ohella sotilaallisen toiminnan ja jännitteen lisääntyminen lähialueillamme. Kansalliseen turvallisuuteen

kohdistuvat vakavimmat uhat ovat nykyään hyvin usein alkuperältään tai kytköksiltään kansainvälisiä ja siten vaikeammin hallittavia. Lisäksi viestintäteknologian nopea kehitys on tehostanut ja helpottanut Suomelle uhan muodostavien tahojen välistä yhteydenpitoa ja verkostoitumista sekä vaikeuttanut uhkien taustalla olevien tahojen tunnistamista. Teknologian kehittyminen on myös mahdollistanut kansallista turvallisuutta vaarantavien tekojen valmistelun ja toteuttamisen entistä lyhyemmässä ajassa. Samalla uhat ovat muuttuneet toteutuessaan vaikutuksiltaan aiempaa laajemmiksi, moniulotteisimmiksi ja vaarallisemmiksi yksittäisten ihmisten ja koko yhteiskunnan kannalta.

Suomen turvallisuustilanteen heikentyminen ja tarve varautua Suomen kansallista turvallisuutta uhkaavaan toimintaan muodostavat hallituksen näkemyksen mukaan sellaisen poikkeuksellisen tilanteen, jossa perustuslain kiireelliselle muuttamiselle on osoitettavissa välttämätön tarve.

Siviili- ja sotilastiedustelua koskevissa hallituksen esityksissä ehdotetaan tiedusteluviranomaisille uusia toimivaltuuksia. Luottamuksellisen viestin salaisuuden suojaan puuttuvat toimivaltuudet edellyttävät perustuslain 10 §:n 3 momentin tarkistamista. Jos nyt ehdotettu perustuslain muutos käsitellään normaalissa perustuslainsäätämisjärjestyksessä, voisivat näitä toimivaltuuksia koskevat säännökset tulla voimaan ehkä vasta vuoden 2020 alkupuolella. Käytettäessä kiireellistä perustuslainsäätämisjärjestystä säännökset voisivat tulla voimaan aikaisemmin, mahdollisesti jo vuoden 2018 lopulla esitysten eduskuntakäsittelystä riippuen. Jos esitysten eduskuntakäsittely jatkuu kuluvan vaalikauden lopulle asti, vähentää tämä tarvetta kiireellisen menettelyn käyttöön.

Edellä todettujen seikkojen perusteella hallitus ehdottaa, että perustuslain muutosesitys käsiteltäisiin eduskunnassa kiireellisessä perustuslainsäätämisjärjestyksessä.

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäväksi seuraava lakiehdotus:

*Lakiehdotus*

# Laki

**Suomen perustuslain 10 §:n muuttamisesta**

Eduskunnan päätöksen mukaisesti, joka on tehty perustuslain 73 §:ssä säädetyllä tavalla,
*muutetaan* Suomen perustuslain 10 §:n 3 momentti ja
*lisätään* 10 §:ään uusi 4 momentti, seuraavasti:

10 §

*Yksityiselämän suoja*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä.

Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

Helsingissä 25 päivänä tammikuuta 2018

**Pääministeri**

**Juha Sipilä**

Oikeusministeri Antti Häkkänen

*Liite*
*Rinnakkaisteksti*

# Laki

## Suomen perustuslain 10 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti, joka on tehty perustuslain 73 §:ssä säädetyllä tavalla,
*muutetaan* Suomen perustuslain 10 §:n 3 momentti ja
*lisätään* 10 §:ään uusi 4 momentti, seuraavasti:

| *Voimassa oleva laki* | *Ehdotus* |
|---|---|
| 10 § | 10 § |
| *Yksityiselämän suoja* | *Yksityiselämän suoja* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää *lisäksi* välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. | Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. |
| (*uusi 4 mom.*) | Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten *torjunnassa*, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana *sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta*. |
| | _____ |
| | *Tämä laki tulee voimaan päivänä kuuta 20* |
| | _____ |

**Regeringens proposition till riksdagen med förslag till lag om ändring av 10 § i Finlands grundlag**

## PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att den reglering i Finlands grundlag som gäller skyddet för hemligheten i fråga om förtroliga meddelanden ändras.

Det föreslås att det i grundlagen tas in en ny bestämmelse där all reglering om begränsning av hemligheten i fråga om förtroliga meddelanden samlas. Enligt den föreslagna grundlagsbestämmelsen ska det genom lag kunna föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning 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.

Den föreslagna lagen avses träda i kraft så snart som möjligt med beaktande av dess lagstiftningsordning.

---

**INNEHÅLL**

## ALLMÄN MOTIVERING

### 1 Inledning

Finlands grundlag trädde i kraft den 1 mars 2000. De bestämmelser om de grundläggande fri- och rättigheterna som togs in i grundlagen i samband med reformen motsvarade i sak de bestämmelser som hade tagits in i II kap. i Regeringsformen för Finland i samband med den reform av de grundläggande fri- och rättigheterna som trädde i kraft den 1 augusti 1995 (L 969/1995).

Eftersom grundlagen har en särskild rättslig ställning och betydelse är det skäl att förhålla sig restriktiv till ändringar av den. Man bör förhålla sig särskilt restriktiv när man överväger ändringar av regleringen om de grundläggande fri- och rättigheterna eller av de principer som är centrala med tanke på statssystemet. Förslag till ändring av grundlagen bör utgå från behov som det råder ett brett samförstånd om. Dessutom bör man se till att grundlagen ger en rättvisande bild av systemet för utövning av statlig makt och av grunderna för individens rättsliga ställning.

Enligt programmet för statsminister Juha Sipiläs regering föreslår regeringen att underrättelseinhämtning som avser utländska förhållanden och underrättelseinhämtning som avser datatrafik ska basera sig på lagstiftning (SRM 1/2015 rd, s. 35). Behovet av att bereda lagstiftning om underrättelseinhämtning utreddes av arbetsgruppen för en informationsanskaffningslag, som hade tillsatts av försvarsministeriet (Riktlinjer för en finsk underrättelselagstiftning, betänkande av arbetsgruppen för en informationsanskaffningslag, försvarsministeriet, 2015). Enligt arbetsgruppens bedömning verkade det som om det inte vore möjligt att stifta en lag om underrättelseinhämtning som avser datatrafik utan att grundlagen ändras, eventuellt med undantag för sådan underrättelseinhämtning som enbart avser en främmande stats datatrafik. Vid sitt strategimöte den 20 augusti 2015 beslutade regeringen att inrikesministeriet och försvarsministeriet skulle inleda beredningen av lagstiftningen om civil och militär underrättelseinhämtning. Dessutom skulle justitieministeriet vidta åtgärder för att revidera grundlagens reglering om skyddet för hemligheten i fråga om förtroliga meddelanden.

Arbetsgrupper tillsatta av försvarsministeriet och inrikesministeriet offentliggjorde sina betänkanden den 19 april 2017 (Förslag till lagstiftning om militär underrättelseverksamhet, arbetsgruppsbetänkande, försvarsministeriet, 2017; Lagstiftning om civil underrättelseinhämtning, betänkande av lagarbetsgruppen för civil underrättelseinhämtning, inrikesministeriets publikation 8/2017). Utifrån betänkandet av inrikesministeriets arbetsgrupp har man som tjänsteuppdrag vid ministeriet berett en regeringsproposition med förslag till lag om ändring av polislagen och till vissa lagar som har samband med den. Vid försvarsministeriet har man på motsvarande sätt berett en regeringsproposition med förslag till lag om militär underrättelseverksamhet.

Justitieministeriet tillsatte den 17 oktober 2016 en arbetsgrupp med uppgiften att bereda den lagstiftning som behövs för att organisera övervakningen av de civila och de militära myndigheternas underrättelseverksamhet. Riksdagens generalsekreterare tillsatte den 23 december 2016 en intern arbetsgrupp vid riksdagens kansli med uppgiften att bereda lagstiftning om parlamentarisk övervakning av underrättelseverksamheten. Justitieministeriet ändrade den 9 februari 2017 beslutet om tillsättandet av sin arbetsgrupp så att arbetsgruppens uppgift begränsades till beredning av lagstiftning om laglighetskontroll av underrättelseverksamheten. Arbetsgruppen vid justitieministeriet offentliggjorde ett betänkande den 19 april 2017 (Övervakning av underrättelseverksamheten, arbetsgruppens betänkande, justitieministeriet, betänkan-

den och utlåtanden 18/2017) och arbetsgruppen vid riksdagens kansli den 29 maj 2017 (Tiedustelun parlamentaarinen valvonta — työryhmän mietintö, eduskunnan kanslian julkaisu 1/2017). Förslagen från justitieministeriets och riksdagens kanslis arbetsgrupper samordnades vid den fortsatta beredningen. Regeringens proposition med förslag till lag om övervakning av underrättelseverksamheten har utifrån detta beretts vid justitieministeriet. Dessutom har man vid riksdagens kansli berett ett förslag av talmanskonferensen om att ändra riksdagens arbetsordning (40/2000) i syfte att ordna den parlamentariska kontrollen av underrättelseverksamheten.

Lagstiftningen om civil och militär underrättelseverksamhet och om övervakningen av verksamheten har alltså beretts samtidigt med denna proposition om revision av grundlagen. I och med den nya underrättelselagstiftningen får de civila och de militära myndigheterna nya, anmärkningsvärda uppgifter och befogenheter. Det är fråga om ny lagstiftning med betydande konsekvenser för skyddet för privatlivet, som garanteras i egenskap av grundläggande och mänsklig rättighet, och i synnerhet för skyddet för hemligheten i fråga om förtroliga meddelanden.

En expertgrupp tillsatt av justitieministeriet den 28 september 2015 hade i uppdrag att utreda och bereda en revision av grundlagen så att det, för att trygga den nationella säkerheten, genom lag kan föreskrivas om nödvändiga begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden, när de förutsättningar som ska anses vara behövliga är uppfyllda. I beredningen skulle Finlands internationella människorättsförpliktelser beaktas.

Arbetsgruppen bedömde i sitt betänkande av den 11 oktober 2016 att det i ljuset av grundlagens ordalydelse och nuvarande tolkningspraxis inte skulle vara möjligt att föreskriva om sådana begränsningar i hemligheten i fråga om förtroliga meddelanden som syftar till att i större utsträckning inhämta för den nationella säkerheten nödvändig information om allvarliga hot, i synnerhet för att kunna förbereda för och antecipera sådana hot samt till stöd för den högsta statsledningens beslutsfattande. Grundlagens ordalydelse möjliggör inte intrång i skyddet för hemligheten i fråga om förtroliga meddelanden för informationsinhämtningssyften t.ex. när det gäller verksamhet som hotar den nationella säkerheten men som inte har framskridit till ett sådant stadium att det mot verksamheten kunde riktas en konkret och individualiserad brottsmisstanke eller som inte är straffbelagd.

Enligt arbetsgruppens bedömning är det nödvändigt att till grundlagen foga nya godtagbara grunder på vilka hemligheten i fråga om förtroliga meddelanden kan begränsas. Arbetsgruppen föreslog att det till 10 § i grundlagen fogas ett 4 mom. enligt följande: ”Genom lag kan föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning 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.” (Hemligheten i fråga om förtroliga meddelanden. Granskning av grundlagsregleringen, justitieministeriet, betänkanden och utlåtanden 41/2016.)

Arbetsgrupperna vid justitieministeriet, försvarsministeriet och inrikesministeriet övervakades av en parlamentarisk uppföljningsgrupp, tillsatt den 11 december 2015. Uppföljningsgruppens mandatperiod förlängdes genom ett beslut av den 4 maj 2017 för den fortsatta beredningen av underrättelselagstiftningen och revisionen av grundlagen.

## 2 Nuläge

### 2.1 Lagstiftning och praxis

2.1.1 Skydd för privatlivet

Skyddet för hemligheten i fråga om förtroliga meddelanden utgör en del av skyddet för privatlivet. Vars och ens privatliv är tryggat enligt 10 § i grundlagen. Begreppet ”privatliv” kan förstås som ett samlande begrepp för en persons privata krets. Utgångspunkten för skyddet för privatlivet är att individen har rätt att leva sitt eget liv utan godtycklig eller ogrundad inblandning av myndigheter eller andra utomstående. (RP 309/1993 rd, s. 56—57.)

För att skyddet för privatlivet ska kunna garanteras förutsätts det av tradition inte bara att staten avhåller sig från att kränka medborgarnas privatliv utan också att staten vidtar aktiva åtgärder för att skydda privatlivet mot inblandning av andra individer. Bestämmelsen om skydd för privatlivet förutsätter tillsammans med grundlagens 22 § om respekt för de grundläggande fri- och rättigheterna att lagstiftaren upprätthåller ett effektivt skydd för de fri- och rättigheter som tryggas i grundlagens 10 §. (RP 309/1993 rd, s. 57.)

Närmare bestämmelser om skydd för personuppgifter utfärdas enligt 10 § 1 mom. i grundlagen genom lag. Enligt grundlagsutskottets praxis begränsas lagstiftarens spelrum utöver av denna bestämmelse också av att skyddet för personuppgifter delvis omfattas av skyddet för privatlivet, som tryggas i samma moment. Sammantaget handlar det om att lagstiftaren ska trygga denna rättighet på ett sätt som kan anses godtagbart med hänsyn till de grundläggande fri- och rättigheterna som helhet.

Brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden är enligt 10 § 2 mom. i grundlagen okränkbar. Enligt 3 mom. i samma paragraf kan det genom lag bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande.

Paragrafen fick sitt nuvarande innehåll i och med reformen av de grundläggande fri- och rättigheterna (8 § i regeringsformen), och i samband med grundlagsreformen år 2000 togs den in som 10 § i grundlagen i oförändrad form.

2.1.2 Skydd för hemligheten i fråga om förtroliga meddelanden

Bestämmelsen om hemligheten i fråga om förtroliga meddelanden i grundlagens 10 § 2 mom. är medie- och teknikneutral. Brev- och telefonhemligheten nämns särskilt, men bestämmelsen tryggar allmänt hemligheten i fråga om alla slag av förtroliga meddelanden.

Avsikten med grundlagsregleringen om hemlighet i fråga om förtroliga meddelanden är i första hand att mot utomstående skydda innehållet i ett meddelande som är avsett att vara förtroligt. Grundlagen tryggar var och en rätt till förtrolig kommunikation utan att utomstående orättmätigt kan få vetskap om innehållet i de förtroliga meddelanden som en person har sänt eller tagit emot. Bestämmelsen skyddar dessutom också annan information som kan ha betydelse för bevarandet av förtroligheten i ett meddelande. Ett typiskt exempel på sådan information är ett samtals identifieringsuppgifter. (RP 309/1993 rd, s. 57.)

Skyddet för hemligheten i fråga om förtroliga meddelanden innebär ett skydd bl.a. mot att brev och andra förslutna försändelser öppnas eller förstörs och mot att samtal avlyssnas eller

bandas. Regleringen skyddar inte bara avsändaren, utan det handlar om en grundläggande rättighet för båda parterna i kommunikationen (RP 309/1993 rd, s. 57).

I fråga om kommunikation i samband med yrkesverksamhet är det möjligt att kommunikationen, med hänsyn till verksamhetens karaktär och till att parterna i kommunikationen är medvetna om att meddelandena lagras, inte omfattas av skyddet för hemligheten i fråga om förtroliga meddelanden, även om personer i och för sig också kan förmedla förtroliga meddelanden mellan sig i den kommunikationen. Grundlagsutskottet bedömde t.ex. i samband med behandlingen av förslaget till lag om säkerhetsutredning av olyckor och vissa andra händelser att tele- och datakommunikation i samband med trafikledning inte omfattas av det skydd som grundlagens 10 § ger förtroliga meddelanden (se GrUU 62/2010 rd, s. 5).

2.1.3 Begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden

De grundläggande fri- och rättigheterna är allmänt taget inte ovillkorliga i den meningen att det inte under några som helst omständigheter skulle gå att begränsa dem i någon som helst utsträckning. Grundlagsutskottet har ur hela komplexet av grundläggande fri- och rättigheter och ur rättigheternas karaktär av grundlagsfästa rättigheter härlett vissa allmänna krav som ska uppfyllas för att de ska kunna begränsas (allmänna förutsättningar för begränsning av de grundläggande fri- och rättigheterna). Det handlar om krav på

— att det ska föreskrivas om begränsningarna i lag,

— att lagarna ska vara exakta och noggrant avgränsade,

— att begränsningarna ska vara acceptabla,

— att begränsningarna ska vara proportionerliga,

— att det inte görs inskränkningar i kärnan av en grundläggande fri- eller rättighet,

— ett adekvat rättsskydd, och

— förenlighet med människorättsförpliktelserna. (GrUB 25/1994 rd, s. 5.)

En del bestämmelser om grundläggande fri- och rättigheter är dessutom förknippade med särskilda restriktiva klausuler. En sådan finns även i grundlagens 10 § 3 mom. Särskilda restriktiva klausuler innebär dels att de som stiftar en vanlig lag ges befogenheter att inskränka någon grundläggande fri- eller rättighet, dels att det ställs upp ytterligare kriterier som kringskär lagstiftarens prövningsrätt. Syftet med dessa s.k. kvalificerade lagförbehåll är att så noggrant och strikt som möjligt bestämma vilka möjligheter till inskränkningar den som stiftar en vanlig lag har, så att det inte i grundlagen medges en vidare befogenhet att inskränka en grundläggande fri- eller rättighet än vad som är absolut nödvändigt (GrUB 25/1994 rd, s. 6).

De kvalificerade lagförbehållen i grundlagen motsvarar i strukturellt hänseende t.ex. de restriktiva klausulerna i ett flertal artiklar i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) (GrUB 25/1994 rd, s. 6). Till innehållet avviker dock lagförbehållet i 10 § 3 mom. från begränsningsgrunderna enligt Europakonventionen.

I lagförbehållet i grundlagens 10 § 3 mom. nämns delvis samma förutsättningar som i de allmänna begränsningsförutsättningarna för de grundläggande fri- och rättigheterna (kraven på att det ska föreskrivas om begränsningar i lag och på att begränsningarna ska vara nödvän-

diga). De allmänna begränsningsförutsättningarna för de grundläggande fri- och rättigheterna tillämpas kompletterande till lagförbehållet.

I lagförbehållet i grundlagens 10 § 3 mom. specificeras det vad som kan anses vara godtagbara orsaker att begränsa hemligheten i fråga om förtroliga meddelanden. Enligt momentet kan det föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga bl.a. vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden. Till dessa brott hör t.ex. narkotikabrott, grova våldsbrott samt lands- och högförräderi (RP 309/1993 rd, s. 58). Även krigsförbrytelser och brott mot mänskligheten samt allvarligare gärningsformer av allmänfarliga brott liksom också grovt ordnande av olaglig inresa, grov spridning av barnpornografisk bild, de allvarligaste brotten mot friheten, vissa terroristbrott samt grova gärningsformer av skadegörelse, dataskadegörelse, bedrägeribrott, koppleri och miljöförstöring har i grundlagsutskottets tolkningspraxis ansetts vara sådana brott som avses i den aktuella grundlagsbestämmelsen. Det har likaså ansetts vara möjligt att föreskriva om begränsningar i hemligheten i fråga om förtroliga meddelanden för utredning av grova brott mot ekonomiska intressen i samband med affärs- eller yrkesverksamhet. En förutsättning har då emellertid varit att det vid brottet har eftersträvats en synnerligen stor vinning och att brottet har begåtts särskilt planmässigt.

Uttrycket utredning av brott kan förstås så att det endast avser utredning av redan begångna brott. Utredning av brott i den mening som avses i grundlagens 10 § 3 mom. omfattar ändå även åtgärder som vidtas på grund av en konkret och specificerad misstanke om brott, även om brottet ännu inte har hunnit begås. Således har det ansetts att det trots 10 § 3 mom. i grundlagen är möjligt att använda t.ex. teleövervakning för att förhindra vissa brott (GrUU 5/1999 rd; GrUU 2/1996 rd). I sina utlåtanden om tvångsmedelslagen och polislagen konstaterade grundlagsutskottet att det krävdes att användningen av teleövervakning begränsas till brott som kan betraktas som i grundlagen avsedda brott som äventyrar individens eller samhällets säkerhet eller hemfriden eller brott som till svårhetsgraden kan jämställas med dem. Grundlagsutskottet ansåg dessutom att det inte utgör något konstitutionellt problem med avseende på grundlagens 10 § 3 mom. att använda teleövervakning för att nå den som misstänks för ett brott som motiverar teleövervakning. (GrUU 67/2010 rd, s. 4; GrUU 66/2010 rd, s. 7.)

Enligt grundlagens 10 § 3 mom. kan det genom lag också bestämmas om sådana begränsningar i hemligheten i fråga om förtroliga meddelanden som är nödvändiga vid rättegång. Som exempel på en sådan begränsning nämns i motiveringen till bestämmelsen 17 kap. i rättegångsbalken, där det föreskrivs om skyldigheten att förete en privat handling eller någon annan dokumentation i en rättegång (RP 309/1993 rd, s. 58).

I grundlagsutskottets utlåtandepraxis har möjligheten att vid rättegång begränsa hemligheten i fråga om förtroliga meddelanden granskats också med tanke på konkursförfarandet. Bestämmelser om konkursboets förvaltares rätt att öppna sådana meddelanden adresserade till gäldenären som hänför sig till utredningen av konkursboet har kunnat utfärdas genom lag, trots att förvaltarens verksamhet inte i sig kan betecknas som rättegång. (GrUU 13/2003 rd.)

Det kan även föreskrivas om nödvändiga begränsningar i meddelandehemligheten vid säkerhetskontroll. I vissa fall kan ett synnerligen viktigt säkerhetsintresse förutsätta t.ex. rätt att granska postförsändelser. Det har således varit möjligt att genom lag föreskriva om t.ex. rätten att öppna ett slutet brev om det finns skäl att misstänka att försändelsen kan orsaka fara för hälsa eller egendom. (GrUU 56/2010 rd, s. 4; GrUU 30/2001 rd, s. 3.) Grundlagsutskottet har vidare ansett att en begränsning i skyddet för förtroliga meddelanden som inkluderar s.k. stormningsobservation kan anses ingå i säkerhetskontroll, som alltså är en av begränsningsgrunderna enligt 10 § 3 mom. i grundlagen (GrUU 36/2017 rd, s. 4).

Begränsningar i hemligheten i fråga om förtroliga meddelanden tillåts enligt grundlagens 10 § 3 mom. även under frihetsberövande. Med uttrycket ”under frihetsberövande” avses i bestämmelsen t.ex. i samband med frihetsstraff, rannsakningsfängelse och anhållan, eller när en person oberoende av sin vilja vårdas på mentalsjukhus eller på någon annan motsvarande anstalt eller har tagits om hand med stöd av barnskyddslagstiftningen. Även på anstalter är det möjligt att begränsa meddelandehemligheten endast i den utsträckning det i det enskilda fallet är motiverat. (RP 309/1993 rd, s. 58.)

Grundlagsutskottet har tidigare i sin etablerade praxis ansett att identifieringsuppgifterna för ett meddelande inte ingår i kärnområdet av den grundläggande fri- och rättighet som skyddar hemligheten i fråga om förtroliga meddelanden (se t.ex. GrUU 33/2013 rd, s. 3; GrUU 6/2012 rd, s. 3—4; GrUU 29/2008 rd, s. 2 och GrUU 3/2008 rd, s. 2). Detta har inneburit att det särskilda lagförbehållet i grundlagens 10 § 3 mom. inte som sådant har tillämpats på begränsningar av hemligheten i fråga om identifieringsuppgifter. Bestämmelser som inkräktar på skyddet för hemligheten i fråga om identifieringsuppgifter ska enligt grundlagsutskottets praxis ändå uppfylla de allmänna begränsningsförutsättningarna för grundläggande fri- och rättigheter (GrUU 62/2010 rd; GrUU 23/2006 rd).

Enligt grundlagsutskottet har rätten att få identifieringsuppgifter inte behövt bindas till vissa typer av brott (GrUU 33/2013 rd; GrUU 67/2010 rd; GrUU 37/2002 rd; GrUU 26/2001 rd). Det har därmed varit möjligt att föreskriva om teleövervakningsbefogenheter också i situationer där det inte nödvändigtvis är fråga om brott som äventyrar individens eller samhällets säkerhet eller hemfriden (se t.ex. polislagens (872/2011) 5 kap. 8 § 2 mom. 1 och 3 punkten: ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år samt olovligt brukande som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning).

Det har ansetts vara möjligt att få identifieringsuppgifter också i vissa situationer där det inte handlar om utredning av brott. Även i dessa fall har regleringen bedömts med hänsyn till de allmänna begränsningsförutsättningarna för grundläggande fri- och rättigheter. (GrUU 62/2010 rd.)

Grundlagsutskottet har senare ändå konstaterat att Europeiska unionens domstols dom i målet Digital Rights Ireland (av den 8 april 2014, C-293/12 och C-594/12) har gett skäl att i viss mån omvärdera frågan om identifieringsuppgifter för elektroniska meddelanden med avseende på hemligheten i fråga om förtroliga meddelanden. Enligt utskottet kan i praktiken identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem 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.) Det är ännu inte möjligt att utifrån grundlagsutskottets senaste utlåtandepraxis entydigt avgöra vilka skillnader denna nya bedömning kan leda till jämfört med de tidigare tolkningarna, som stödde sig på de allmänna begränsningsförutsättningarna för grundläggande fri- och rättigheter.

### 2.1.4 Reglering om hemliga metoder för inhämtande av information

I syfte att förhindra brott har man för myndigheterna föreskrivit vissa liknande befogenheter som det bedöms att underrättelseinhämtningen kommer att förutsätta. I den nuvarande lagstiftningen finns bestämmelser om sådana hemliga metoder för inhämtande av information

som används för att förhindra och avslöja brott. Däremot finns det inga bestämmelser om befogenheter som är viktiga med tanke på underrättelseverksamheten.

Bestämmelser om polisens hemliga metoder för inhämtande av information finns i 5 kap. i polislagen, som stiftats med grundlagsutskottets medverkan. Polisen kan, i hemlighet för dem som informationsinhämtningen riktas mot, använda följande metoder för inhämtande av information: teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk observation (teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp, användning av informationskällor och kontrollerade leveranser. Av dessa metoder för inhämtande av information berörs hemligheten i fråga om förtroliga meddelanden av följande:

— teleavlyssning (polislagens 5 kap. 5 §),

— inhämtande av information i stället för teleavlyssning (polislagens 5 kap. 6 §),

— teleövervakning (polislagens 5 kap. 8 §),

— teleövervakning med samtycke av den som innehar teleadress eller teleterminalutrustning (polislagens 5 kap. 9 §),

— inhämtande av basstationsuppgifter (polislagens 5 kap. 11 §),

— teknisk avlyssning (polislagens 5 kap. 17 §), och

— inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning (polislagens 5 kap. 25 §).

En allmän förutsättning för användning av en hemlig metod för inhämtande av information är enligt 5 kap. 2 § i polislagen att man med metoden kan antas få information som behövs för förhindrande eller avslöjande av brott eller för avvärjande av risk för brott. Teleavlyssning och inhämtande av information i stället för teleavlyssning bör dessutom kunna antas vara av mycket stor betydelse för förhindrande och avslöjande av brott. I 5 kap. i polislagen föreskrivs det även om särskilda förutsättningar för de olika hemliga metoderna för inhämtande av information. Särskilda förutsättningar är framför allt de specificerade brott som metoden i fråga får användas för att förhindra. Valet och användningen av hemliga metoder för inhämtande av information styrs även av de allmänna principerna i 1 kap. i polislagen, nämligen principen om respekt för de grundläggande och mänskliga rättigheterna, proportionalitetsprincipen, principen om minsta olägenhet och principen om ändamålsbundenhet.

Bestämmelser om brottsbekämpning inom försvarsmakten finns i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014). Försvarsmaktens behörighet vid förebyggande och avslöjande av brott gäller enligt 86 § 1 mom. i den lagen brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret. Enligt lagens 89 § 1 mom. gäller i fråga om befogenheterna för de tjänstemän som sköter förebyggandet och avslöjandet av brott inom försvarsmakten vad som i polislagen föreskrivs om befogenheter vid förebyggande och avslöjande av brott. Av de hemliga metoder för inhämtande av information som avses i 5 kap. i polislagen har de dock till sitt förfogande endast inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning och inhämtande av identifieringsuppgifter för telea-

dresser eller teleterminalutrustning. Av de hemliga metoder för inhämtande av information som berör skyddet för hemligheten i fråga om förtroliga meddelanden har försvarsmakten därmed till sitt förfogande endast inhämtande av basstationsuppgifter, teknisk avlyssning och inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning.

### 2.1.5 Övervakning av underrättelseverksamheten

#### 2.1.5.1 Tillstånds- och underrättelseförfarande

Övervakningen av underrättelseverksamheten kan delas in för det första i föregripande övervakning och övervakning i efterhand och för det andra i parlamentarisk kontroll och laglighetskontroll. Föregripande övervakning innebär framför allt att det finns ett tillståndsförfarande för användning av metoder för informationsinhämtning. Det är domstolen som har beslutanderätt i fråga om användningen av vissa hemliga metoder för inhämtande av information. Av befogenheterna enligt 5 kap. i polislagen förutsätts tillstånd av domstol för teleavlyssning, inhämtande av information i stället för teleavlyssning och inhämtande av basstationsuppgifter. Det hör också i regel till domstolens befogenheter att besluta om teleövervakning. I sådana brådskande situationer där polisen tillfälligt själv kan besluta om teleövervakning, ska ärendet föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas. Polisen får dock besluta om teleövervakning för att avvärja allvarlig fara som hotar liv eller hälsa samt om teleövervakning med samtycke av en person, om man misstänker brott som direkt hänger samman med en teleadress eller teleterminalutrustning. I enlighet med hänvisningsbestämmelsen i 89 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten förutsätter inhämtande av basstationsuppgifter tillstånd av domstol.

Ett yrkande som gäller hemligt inhämtande av information ska enligt 5 kap. 45 § i polislagen utan dröjsmål tas upp till behandling i tingsrätten i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet. Ärendet ska avgöras skyndsamt. Ärendet får avgöras utan att den person hörs som med fog kan antas begå eller har begått brottet och i regel utan att innehavaren av teleadressen eller teleterminalutrustningen hörs. Ett beslut i ett tillståndsärende som gäller hemliga metoder för inhämtande av information får inte överklagas genom besvär. Klagan mot beslutet får anföras vid hovrätten utan tidsbegränsning.

Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning eller teleövervakning ska enligt 5 kap. 58 § i polislagen utan dröjsmål underrättas om detta efter det att syftet med inhämtandet av information har nåtts. Personen i fråga ska dock underrättas om det hemliga inhämtandet av information senast ett år efter att det har upphört. På yrkande av en anhållningsberättigad polisman får domstolen besluta att underrättelsen till den som varit föremål för åtgärden får skjutas upp med högst två år åt gången. En förutsättning för att underrättelsen ska få skjutas upp är att det är motiverat för att trygga pågående inhämtning av information, trygga statens säkerhet eller skydda liv eller hälsa. Domstolen får besluta att underrättelsen ska utebli, om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa.

#### 2.1.5.2 Parlamentarisk kontroll och laglighetskontroll

I Finland finns inget sådant parlamentariskt tillsynsorgan som enbart eller uttryckligen enligt lag skulle ha till uppgift att övervaka underrättelseverksamheten. Parlamentarisk kontroll sker

genom verksamheten i riksdagen och utskotten och genom rätten att få information. Av riksdagens utskott har grundlags-, utrikes-, förvaltnings- och försvarsutskottet kontakt med skyddspolisen och de militära myndigheterna och får även information om underrättelseverksamheten. Skyddspolisen informerar grundlags-, förvaltnings- och utrikesutskottet om utvecklingen i säkerhetsläget i Finland. Försvarsmaktens underrättelsetjänst informerar vid behov riksdagens utskott i frågor som berör militär underrättelseinhämtning. Många av de ärenden inom försvarsförvaltningens område som behandlas i utskotten grundar sig på underrättelseinformation. Den uppföljning som utskotten genomför är huvudsakligen av allmän karaktär, och innehållet i och formerna för uppföljningen varierar mellan utskotten. Förvaltningsutskottet, som behandlar ärenden som gäller inre säkerhet, har tät kontakt med skyddspolisen och andra polisenheter, och utskottets verksamhet omfattar också övervakning. Grundlagsutskottet träffar ledningen för skyddspolisen ett antal gånger per valperiod, och försvarsutskottet ordnar utfrågningar av sakkunniga om vissa teman. Om underrättelseinhämtningen berörs av utrikes- och säkerhetspolitiskt betydelsefulla aspekter, behandlas ärendet i utrikesutskottet och i de utskott vilkas behörighetsområde ärendet hänför sig till.

Enligt 47 § i grundlagen har riksdagen rätt att av statsrådet få de upplysningar som behövs för behandlingen av ett ärende. Den minister som saken gäller ska se till att utskott eller andra riksdagsorgan utan dröjsmål får handlingar och andra upplysningar som de behöver och som finns hos myndigheterna. Varje utskott har dessutom rätt att av statsrådet eller respektive ministerium få utredningar i frågor som hör till utskottets behörighetsområde. Utskottet kan med anledning av utredningen ge ett yttrande till statsrådet eller ministeriet.

Laglighetskontrollen av underrättelseverksamheten kan delas in i intern och extern laglighetskontroll. Den externa laglighetskontrollen av myndighetsverksamheten sköts av de högsta laglighetsövervakarna och av särskilda ombudsmän. De särskilda ombudsmännen, såsom jämställdhetsombudsmannen, diskrimineringsombudsmannen och dataombudsmannen, övervakar myndighetsverksamhetens lagenlighet inom sitt eget i lag fastställda ansvarsområde. Bland de högsta laglighetsövervakarna sköts övervakningen av underrättelseverksamheten i nuläget främst av justitieombudsmannen. I justitieombudsmannens övervakning av polisens verksamhet och av försvarsmakten ligger betoningen på övervakning av hemliga tvångsmedel och av hemligt inhämtande av information. Justitieombudsmannens övervakning av hemliga metoder för inhämtning av information sker huvudsakligen i form av inspektioner och annan övervakning på eget initiativ. I enskilda fall utövar också justitiekanslern sina befogenheter och undersöker ärenden som gäller eller berör underrättelseverksamheten.

Inrikesministeriet och försvarsministeriet ska årligen ge justitieombudsmannen berättelser om hemliga tvångsmedel och om hemliga metoder för inhämtande av information. Av berättelserna ska det även framgå hur dessa har övervakats. (Se 5 kap. 63 § i polislagen, 10 kap. 65 § i tvångsmedelslagen och 129 § i lagen om militär disciplin och brottsbekämpning inom försvarsmakten.) Justitieombudsmannen ger årligen till riksdagen en berättelse om sin verksamhet samt om rättskipningens tillstånd och om de brister i lagstiftningen som justitieombudsmannen har observerat. Grundlagsutskottet har förutsatt att teletvångsmedel och täckoperationer ska behandlas i berättelsen (GrUB 15/2002 rd). Å ena sidan har grundlagsutskottet ett flertal gånger konstaterat att justitieombudsmannen har spelat en viktig roll när det gäller att övervaka teletvångsmedlen och utveckla övervakningssystemen. Å andra sidan kan justitieombudsmannens laglighetsövervakning enligt utskottet ändå bara utgöra ett komplement till de förvaltningsinterna övervakningsmekanismerna. (GrUU 8/2007 rd; GrUU 17/2006 rd; GrUU 16/2006 rd.) Dessutom har grundlagsutskottet i ett annat sammanhang konstaterat att man måste se till att rättsskyddet i anknytning till teletvångsmedel — i synnerhet domstolarnas tillståndsförfarande, den interna myndighetsövervakningen och justitieombudsmannens laglighetskontroll — fungerar såväl på författningsnivå som i praktiken (GrUU 32/2013 rd). Det har också i justitieombudsmannens berättelse år 2015 konstaterats att justitieombudsman-

nens övervakning sker i efterhand och är rätt så generell. Justitieombudsmannen kan inte börja styra myndigheternas verksamhet eller i andra avseenden spela en central roll genom att ställa upp gränser för verksamheten i syfte att avhjälpa brister i lagstiftningen. De berättelser och utredningar som ska lämnas till justitieombudsmannen är nödvändiga men löser inte problemen med övervakningen och rättsskyddet. (Riksdagens justitieombudsmans berättelse år 2015, B 11/2016 rd, s. 186.)

Den interna övervakningen av polisens hemliga metoder för inhämtande av information sköts av cheferna för de enheter som använder hemliga metoder för inhämtande av information, samt dessutom av inrikesministeriet när det är fråga om skyddspolisen och av Polisstyrelsen när det är fråga om en enhet som är underställd Polisstyrelsen. Utöver inom Polisstyrelsen sker i praktiken en stor del av den interna övervakningen av hemliga metoder för inhämtande av information inom polisinrättningarnas rättsenheter. Brottsbekämpningen inom försvarsmakten övervakas av försvarsmaktens ledning. Dessutom övervakar avdelningschefen för underrättelseavdelningen förebyggandet och avslöjandet av brott.

### 2.1.6 Den nya underrättelselagstiftningen

I Finland finns det inte något regelverk om hurdan underrättelseverksamhet som får bedrivas eller om vad man eftersträvar med underrättelseverksamheten. Det har konstaterats att det krävs ett brett spektrum av metoder och att de metoder som står till buds utvecklas för att man ska kunna svara på förändringar i omvärlden och på nya hot. I enlighet med detta har det inom statsrådet beretts en underrättelselagstiftningshelhet.

I regeringspropositionen om civil underrättelseinhämtning, som har beretts vid inrikesministeriet, föreslås det att det fogas ett nytt 5 a kap. till polislagen och att det stiftas en ny lag om civil underrättelseinhämtning avseende datatrafik. Denna lagstiftning föreslås omfatta bestämmelser om de metoder för underrättelseinhämtning som står till förfogande vid civil underrättelseinhämtning, om beslutsfattandet om användningen av befogenheterna samt om de principer som ska följas i underrättelseverksamheten och om den interna övervakningen av verksamheten. Propositionen innehåller en rättsgrund både för befogenheter till underrättelseinhämtning som avser utländska förhållanden och för befogenheter till underrättelseinhämtning som utövas i det egna landet. Regleringen grundar sig metodmässigt på de hemliga metoder för inhämtande av information som det föreskrivs om i 5 kap. i polislagen. Befogenheterna ska namnges som metoder för underrättelseinhämtning i enlighet med användningsändamålen, och grunden för utövande av befogenheterna är inhämtande av information om verksamhet som allvarligt hotar den nationella säkerheten. Utöver metoderna i 5 kap. ska också platsspecifik underrättelseinhämtning, kopiering, kvarhållande av en försändelse för kopiering samt underrättelseinhämtning som avser datatrafik räknas som underrättelseinhämtningsmetoder. På grund av de särdrag som är förknippade med den underrättelseinhämtning som avser datatrafik föreslås bestämmelser om den i en separat lag. Befogenheterna för civil underrättelseinhämtning anvisas skyddspolisen.

I den regeringsproposition som har beretts vid försvarsministeriet föreslås det att det stiftas en lag om militär underrättelseverksamhet. Målet med propositionen är att förbättra försvarsmaktens informationsinhämtning om allvarliga internationella hot som anknyter till försvarsmaktens uppgifter på så sätt att försvarsmakten ska ha befogenheter till personbaserad underrättelseinhämtning som avser utlandet, till underrättelseinhämtning som avser utländska datasystem och till underrättelseinhämtning som avser datatrafik. I den föreslagna lagen om militär underrättelseverksamhet finns bestämmelser om föremålen för den militära underrättelseinhämtningen, om de principer som ska följas i underrättelseverksamheten och om styrningen och

den interna övervakningen av verksamheten. Enligt förslaget ska militärunderrättelsemyndigheter vara försvarsmaktens huvudstab och underrättelsetjänst. I den föreslagna lagen finns dessutom bestämmelser om de metoder för underrättelseinhämtning som står till myndigheternas förfogande och om beslutsfattandet om användningen av befogenheterna samt om anmälan om underrättelseinformation, förbud mot underrättelseinhämtning, internationellt samarbete och registrering av uppgifterna.

I en regeringsproposition som har beretts vid justitieministeriet föreslås det att det stiftas en lag om övervakning av underrättelseverksamheten. Genom den nya lagen föreskrivs det om laglighetskontrollen av civil och militär underrättelseinhämtning och om detaljerna kring den parlamentariska kontrollen. För den parlamentariska kontrollen av underrättelseverksamheten föreslås det att det vid riksdagen inrättas ett nytt fackutskott, underrättelsetillsynsutskottet. Bestämmelser om utskottets uppgifter ska utfärdas i riksdagens arbetsordning. För att underrättelsetillsynsutskottet ska kunna inrättas måste riksdagens arbetsordning ändras. Det föreslås att laglighetskontrollen av underrättelseverksamheten ska skötas av underrättelseombudsmannen, en ny självständig och oberoende myndighet som inrättas i samband med dataombudsmannens byrå. Ombudsmannens uppgift ska vara att övervaka lagenligheten vid användning av underrättelseinhämtningsmetoder samt tillgodoseendet av de grundläggande och mänskliga rättigheterna i underrättelseverksamheten. Ombudsmannen ska utnämnas av statsrådet för högst fem år i sänder. Underrättelsetillsynsutskottet och underrättelseombudsmannen ska ha en omfattande rätt att få information. Underrättelseombudsmannen ska dessutom ha rätt att göra inspektioner och befogenhet att bestämma att användningen av en underrättelseinhämtningsmetod ska avbrytas eller avslutas, om ombudsmannen anser att den övervakade har handlat lagstridigt i underrättelseverksamheten. Ombudsmannen kan också bestämma att uppgifter som skaffats på ett lagstridigt sätt ska förstöras utan dröjsmål. Hos underrättelseombudsmannen kan det anföras klagomål och göras begäran om undersökning. Ombudsmannen ska årligen lämna en berättelse om sin verksamhet till riksdagen, justitieombudsmannen och statsrådet.

## 2.2 Internationell praxis samt lagstiftningen i utlandet och i EU

### 2.2.1 Grundlagsreglering om förtroliga meddelanden i vissa länder

Vid beredningen av denna proposition har grundlagsregleringen om skyddet för hemligheten i fråga om förtroliga meddelanden i vissa länder som är centrala för Finland granskats. I de granskade länderna finns lagstiftning om underrättelseinhämtning, och många länders underrättelselagstiftning har även bedömts av Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen). Lagstiftningen om underrättelseverksamheten och om övervakningen av den i europeiska länder beskrivs närmare i allmänna motiveringen till propositionerna om civil och militär underrättelseverksamhet och övervakning av underrättelseverksamheten.

#### 2.2.1.1 Sverige

I 2 kap. 6 § i Sveriges regeringsform (1974, bestämmelserna om de grundläggande fri- och rättigheterna ändrade 2011) föreskrivs det bl.a. att var och en är skyddad mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt 2 kap. 20 § i regeringsformen får dessa rättigheter begränsas genom lag. Begränsningar får enligt 2 kap. 21 § göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna ska dessutom vara nödvändiga, och de får inte sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildning-

en såsom en av folkstyrelsens grundvalar. Begränsningar får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. I regeringsformens 2 kap. 22 § föreskrivs det om förfarandet vid behandlingen av lagförslag som innehåller begränsningar av de grundläggande fri- och rättigheterna.

Särskilda begränsningar för andra än svenska medborgare får enligt 2 kap. 25 § i regeringsformen göras genom lag, också i fråga om skyddet mot intrång i förtroliga försändelser och meddelanden. Även då ska största delen av förfarandebestämmelserna i 2 kap. 22 § tillämpas. Dessutom gäller för dessa begränsningar, liksom för andra begränsningar av de grundläggande fri- och rättigheterna, bestämmelsen i 2 kap. 19 § i regeringsformen, enligt vilken lagstiftningen inte får stå i strid med Europakonventionen.

I Sverige föreskrivs det om underrättelseverksamhet i den allmänna lagen om försvarsunderrättelseverksamhet (2000:130) och i den allmänna lagen om signalspaning i försvarsunderrättelseverksamhet (2008:717). Till författningshelheten om underrättelseverksamhet hör dessutom bl.a. lagen om Försvarsunderrättelsedomstol (2009:966). Bestämmelser om Statens inspektion för försvarsunderrättelseverksamheten, som svarar för laglighetskontrollen av underrättelseverksamheten, finns i lagen om försvarsunderrättelseverksamhet, lagen om signalspaning i försvarsunderrättelseverksamhet och förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (2009:969). I Sverige finns inget parlamentariskt tillsynsorgan som enbart eller huvudsakligen skulle ha till uppgift att övervaka underrättelseverksamheten, utan övervakningen sköts av riksdagens försvarsutskott.

I svensk lagstiftningspraxis har regeringsformens 2 kap. 6 § om skyddet mot intrång i förtroliga försändelser och meddelanden granskats bl.a. i samband med underrättelselagstiftningen. Lagrådet, som lämnar yttranden över lagförslags grundlagsenlighet, har då framhållit bl.a. att kartläggning av yttre hot mot landet och bekämpning och förebyggande av brott är godtagbara grunder för begränsning av skyddet mot intrång i förtroliga försändelser och meddelanden. Lagrådet har även tagit ställning till omfattningen av skyddet. Enligt Lagrådet begränsas skyddet redan genom att staten bereder sig tillgång till teletrafiken och inte först när ett visst meddelande avskils för analys genom sökbegrepp (se närmare Lagrådets protokoll av den 9 februari 2007 och den 20 juni 2012).

#### 2.2.1.2 Norge

Bestämmelserna om de grundläggande fri- och rättigheterna i Norges grundlag (Kongeriket Norges Grunnlov, 1814) ändrades i samband med grundlagsreformen 2014. I grundlagens 102 §, som före reformen gällde endast husrannsakan, föreskrivs det nu om skydd för privatliv och familjeliv, hem och kommunikation. Enligt bestämmelsen har var och en rätt till respekt för bl.a. sin kommunikation.

I Norges grundlag finns inga särskilda bestämmelser om på vilka grunder lagstiftaren eller myndigheterna kan ingripa i de rättigheter som garanteras i 102 §. I motiveringen till grundlagens 102 § (Innst. 186 S (2013-2014)) har man inte direkt klargjort i vilka situationer rättigheterna skulle kunna begränsas, men enligt motiveringen har ordalydelsen ”respekt for” valts för att synliggöra att avsikten inte har varit att utesluta möjligheten till underrättelseinhämtning med stöd av lag. I rättspraxis har grundlagens 102 § tolkats på motsvarande sätt som de bestämmelser i människorättskonventioner som ligger till grund för bestämmelsen (artikel 17 i FN:s internationella konvention om medborgerliga och politiska rättigheter och artikel 8 i

Europakonventionen). Begränsningar är således möjliga, om det föreskrivs om dem i lag, om de har ett godtagbart syfte och om de är proportionerliga. (Høyesterett Rt. 2014 s. 1105 och Rt. 2015 s. 93.)

Bestämmelser om underrättelseverksamhet finns i lagen om underrättelsetjänsten (Lov om etterretningstjenesten, 1998-03-20 nr. 11). Bestämmelser om övervakningen av underrättelseverksamheten finns i en lag som är gemensam för säkerhetsmyndigheterna (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste, 1995-02-03 nr. 07). Det norska parlamentet Stortingets EOS-kommitté (Utvalget for kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste) sköter både den parlamentariska kontrollen och laglighetskontrollen.

#### 2.2.1.3 Danmark

I 72 § i Danmarks grundlag (Danmarks Riges Grundlov, 1953) finns bestämmelser om bl.a. skyddet för hemligheten i fråga om förtroliga meddelanden. Enligt paragrafen måste man ha tillstånd av domstol för att få beslagta och undersöka brev och för att på andra sätt ingripa i post-, telegraf- och telefonhemligheten, om inte ett särskilt undantag föreskrivs i lag. Paragrafens ordalydelse om de skyddade objekten har tolkats i vid bemärkelse, så att bestämmelsen gäller också information som lagras i elektronisk form samt elektronisk kommunikation.

I praktiken förutsätter en begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden också att begränsningen är nödvändig. Andra inskränkningar i skyddet än sådana som grundar sig på tillstånd av domstol kan dessutom gälla endast exakt definierade ärenden.

I Danmarks lagstiftningspraxis har man ansett att föreslagna bestämmelser behöver granskas i förhållande till människorättskonventioner, inte i förhållande till grundlagen. Exempelvis lagstiftningen om underrättelsetjänsten har granskats med beaktande av bestämmelserna i Europakonventionen (se Betænkning om PET og FE, Betænkning nr. 1529, Justitsministeriet 2012). Bestämmelser om underrättelseverksamheten finns i lagarna om säkerhetspolisen och försvarsmaktens underrättelsetjänst (Lov om Politiets Efterretningstjeneste, nr. 604 af 12. juni 2013; Lov om Forsvarets Efterretningstjeneste, nr. 602 af 12. juni 2013), som även innehåller bestämmelser om laglighetskontroll. Laglighetskontrollen av underrättelseverksamheten sköts av en oberoende tillsynsmyndighet (Tilsynet med Efterretningstjenesterne), som inrättades 2013 och verkar i form av en kommitté. Den parlamentariska kontrollen av underrättelseverksamheten sköts av det danska parlamentet Folketingets underrättelsetjänstkommitté (Udvalg vedrørende Efterretningstjenesterne). Bestämmelser om kommitténs verksamhet och sammansättning finns i en separat lag (Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, nr. 378 af 6. juli 1988).

#### 2.2.1.4 Tyskland

I artikel 10 i Tyskland grundlag (Grundgesetz für die Bundesrepublik Deutschland, 1949) föreskrivs det om skydd för hemligheten i fråga om förtroliga meddelanden. Enligt artikel 10.1 är brev-, post och telehemligheten okränkbara. I artikeln nämns inte vilka förutsättningar som ska uppfyllas för att en begränsning av skyddet ska anses godtagbart.

Bestämmelser om de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna finns i grundlagens artikel 19. En förutsättning för begränsning av en grundläggande fri- eller rättighet är att det enligt grundlagen är möjligt att begränsa fri- eller rättigheten

i fråga. En lag som begränsar en grundläggande fri- eller rättighet måste vara allmänt tillämplig och får inte gälla endast ett enskilt fall. En begränsning får inte göra intrång i kärnan av en grundläggande fri- eller rättighet. Dessutom ska det finnas möjlighet till domstolskontroll.

En särskild bestämmelse om begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden finns i artikel 10.2. Enligt bestämmelsen ska begräsningar grunda sig på lag. Om begränsningen syftar till att skydda den fria demokratiska samhällsordningen eller fortbestånd-et av eller säkerheten i förbundsstaten eller ett förbundsland, kan det genom lag föreskrivas att den som är föremål för begränsningen inte ska underrättas om begränsningen och att rätts-skyddet, med avvikelse från de allmänna begränsningsförutsättningarna enligt artikel 19, tryg-gas genom i lag nämnda myndigheters övervakning i stället för genom rätten att söka ändring.

I Tyskland finns bestämmelser om underrättelseverksamheten i lagar om underrättelsemyn-digheterna (Gesetz über den Bundesnachrichtendienst, 20. Dezember 1990, BGBl. I S. 2954, 2979; Gesetz über den militärischen Abschirmdienst, 20. Dezember 1990, BGBl. I S. 2954, 2977; Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, 20. Dezember 1990, BGBl. I S. 2954, 2970). Separata bestämmelser om metoder för underrättelseinhämtning som innebär ett intrång i innehållet i förtroliga meddelanden finns i den s.k. G 10-lagen (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 26. Juni 2001, BGBl. I S. 1254, 2298).

I G 10-lagen fastställs de förutsättningar under vilka underrättelsetjänsterna får kontrollera förtroliga meddelanden som förmedlas av posten och avlyssna samt spela in förtrolig tele-kommunikation. För utövande av dessa befogenheter krävs tillstånd av det ministerium som ansvarar för verksamheten och godkännande av organet för laglighetskontroll (G 10-kommissionen). Som grund för inhämtning av information anges ett stort antal brott mot den nationella säkerheten. Kärnområdet i privatlivet omfattas av ett utvidgat skydd mot myndig-heternas informationsinhämtning. Kärnområdet i privatlivet består av en persons intima pri-vatliv, som inte i sig omfattar t.ex. familjelivet. Också enligt lagen om signalspaning som av-ser utländska förhållanden (Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bun-desnachrichtendienstes, 23. Dezember 2016, BGBl. I S. 3346, 67), som trädde i kraft vid in-gången av 2017, får underrättelseinhämtning inte göra intrång i kärnområdet i privatlivet, som omfattar individens integritetsskydd.

I G 10-lagen föreskrivs vissa uppgifter i samband med övervakningen av metoderna för under-rättelseinhämtning som riktas mot innehållet i förtroliga meddelanden för förbundsdagens (Bundestag) kontrollutskott (Parlamentarische Kontrollgremium), som sköter den parlamenta-riska kontrollen av underrättelseverksamheten. De grundläggande bestämmelserna om kon-trollutskottet finns i grundlagen och i lagen om parlamentarisk kontroll av underrättelsein-hämtningen (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, 29. Juli 2009, BGBl. I S. 2346).

#### 2.2.1.5 Schweiz

Bestämmelser om integritetsskydd finns i artikel 13 i Schweiz grundlag (Bundesverfassung der Schweizerischen Eidgenossenschaft, 1999). Enligt artikeln har var och en bl.a. rätt till re-spekt för sin korrespondens, sina postförsändelser och sin elektroniska kommunikation.

I den schweiziska grundlagen finns separata bestämmelser om begränsning av grundläggande fri- och rättigheter. Regleringen påminner i viss mån om de allmänna förutsättningar för be-

gränsning av grundläggande fri- och rättigheter som i Finland har etablerats i grundlagsutskottets praxis. Enligt artikel 36 i den schweiziska grundlagen är begränsningsförutsättningar att en begränsning grundar sig på lag, att begränsningen är berättigad med hänsyn till allmänna intressen eller till andra grundläggande fri- och rättigheter och att begränsningen är proportionerlig. Begränsningar får inte beröra kärnan i en grundläggande fri- eller rättighet.

I Schweiz trädde en ny underrättelselag (Bundesgesetz über den Nachrichtendienst, vom 25. September 2015) i kraft den 1 september 2017. Genom lagen tilläts underrättelseinhämtning i privata utrymmen, organiserades sådan underrättelseinhämtning som avser datatrafik som överskrider landets gränser och utvidgades befogenheterna för militär underrättelseinhämtning. Enligt den nya lagen är det försvarsministeriet som ska organisera laglighetskontrollen av underrättelseverksamheten, och underrättelsetjänstens kontrollavdelning (Nachrichtendienstliche Aufsicht), som verkar i anslutning till ministeriet, fick utökade befogenheter. I och med den nya lagen fick det schweiziska förbundsrådet (Bundesrat) rätt att tillsätta en oavhängig kontrollinstans (Unabhängige Kontrollinstanz) med uppgiften att kontrollera lagenligheten i signalspaningen. Avsikten är att man i Schweiz ska utfärda bestämmelser om underrättelseinhämtning som avser datakommunikationskablar. Den parlamentariska kontrollen av underrättelseverksamheten sköts av en delegation (Geschäftsprüfungsdelegation) som är gemensam för kontrollkommissionerna vid parlamentets underhus (Nationalrat) och överhus (Ständerat). Bestämmelser om delegationen finns i grundlagen och i lagen om parlamentets verksamhet och organisation (Bundesgesetz über die Bundesversammlung, vom 13. Dezember 2002).

#### 2.2.1.6 Frankrike

Till grundlagshelheten i Frankrike hör 1958 års grundlag (Constitution du 4 octobre 1958), 1789 års människorättsdeklaration (Déclaration des Droits de l'Homme et du Citoyen de 1789) och 1946 års preambel till grundlagen (Préambule de la Constitution du 27 octobre 1946). I dessa föreskrivs det inte direkt om skydd för förtroliga meddelanden. Det har dock ansetts att rätten till integritetsskydd och skydd för förtroliga meddelanden kan härledas från artikel 2 i människorättsdeklarationen, där det allmänt konstateras att vars och ens mänskliga rättigheter skyddas. Enligt artikel 34 i 1958 års grundlag utfärdas närmare bestämmelser om de grundläggande fri- och rättigheterna genom lag. Bestämmelser om skydd för privatlivet och familjelivet finns i artikel 9 i civilrättslagen (Code civil), enligt vilken var och en har rätt till respekt för sitt privatliv. Skyddet för privatlivet anses gälla också förtroliga meddelanden. Den enskildes förtroliga meddelanden skyddas dessutom genom lagen om datasekretess (Loi relative à l'informatique, aux fichiers et aux libertés, n° 78-17 du 6 janvier 1978). Enligt artikel 1 i den lagen får informationstekniken inte kränka de mänskliga rättigheterna, privatlivet eller den individuella friheten.

Begreppen skydd för privatlivet och skydd för förtroliga meddelanden har inte definierats i lagstiftningen, utan deras innehåll och betydelse fastställs i tolkningspraxis. Rätten till privatlivet har i praktiken inte varit obegränsad. Denna rättighet har i Frankrike vägts i förhållande till i synnerhet yttrandefriheten och pressfriheten. I tolkningspraxis har det uppstått ett antal kriterier med hjälp av vilka man strävar efter att finna en balans mellan de olika grundläggande fri- och rättigheterna. Dessa begränsnings- och avvägningskriterier omfattar nödvändighet (t.ex. allmänt intresse) och proportionalitet.

Bestämmelser om befogenheter till underrättelseinhämtning finns i Frankrike i lagen om inre säkerhet (Code de la sécurité intérieure). Enligt artikel L241-1 i den lagen garanteras hemligheten i fråga om förtroliga meddelanden i den elektroniska telekommunikationen genom lag.

Vidare enligt artikeln kan skyddet för hemligheten i fråga om förtroliga meddelanden trots det begränsas i undantagsfall, bl.a. för att förebygga terrorism och för att samla underrättelseinformation om den nationella säkerheten. Bestämmelsen gäller bl.a. telefon- och e-postkommunikation.

År 2015 erkändes i Frankrike en ändring av underrättelselagstiftningen (Loi relative au renseignement, n° 2015-912 du 24 juillet 2015), genom vilken myndigheternas befogenheter till underrättelseinhämtning utökades. Grunder för att inleda underrättelseinhämtning kan enligt lagen vara bl.a. tryggande av den nationella suveräniteten eller av viktiga utrikespolitiska eller ekonomiska intressen samt bekämpning av terrorism eller organiserad brottslighet. Underrättelselagen innehåller bestämmelser om laglighetskontrollen av underrättelseverksamheten. Bestämmelser om den parlamentariska kontrollen av underrättelseverksamheten finns däremot i en separat lag (Loi portant création d'une délégation parlementaire au renseignement, n° 2007-1443 du 9 octobre 2007).

Conseil d'État har ett flertal gånger fått i uppdrag att bedöma underrättelselagstiftningens grundlagsenlighet, och i sin tur lämnat ärendet till Conseil constitutionnel. Föremål för bedömningen har varit bl.a. det sätt på vilket de nya befogenheterna till underrättelseinhämtning i stor utsträckning kan gälla enskilda personer, grunderna för begränsning av integritetsskyddet samt premiärministerns omfattande befogenhet att inleda underrättelseverksamhet utan tillstånd av domstol eller bindande kontroll. Conseil constitutionnel har ansett att bestämmelser som möjliggör observation också av den närmaste kretsen till en person som är misstänkt för terrorism skulle strida mot grundlagen (Décision n° 2017-648 QPC du 4 août 2017, se även Décision n° 2016-590 QPC du 21 octobre 2016). Vidare har Conseil constitutionnel ansett att bestämmelser om insamling och lagring av information i datakommunikation som tas emot eller skickas utomlands är för inexakta med tanke på de grundläggande fri- och rättigheterna (Décision du Conseil constitutionnel, n° 2015-722 DC du 26 novembre 2015, se Décision du Conseil constitutionnel, n° 2015-713 DC du 23 juillet 2015). Den underrättelselag som stiftades gäller därför endast underrättelseinhämtning inom Frankrike. I stället stiftades en separat lag om observation av internationell datakommunikation (Loi relative aux mesures de surveillance des communications électroniques internationales, n° 2015-1556 du 30 novembre 2015).

Efter terrorattackerna i Frankrike i november 2015 infördes undantagstillstånd genom lag (Loi prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions, n° 2015-1501 du 20 novembre 2015). Undantagstillståndet motiverades av ett allvarligt hot mot samhället eller den allmänna ordningen. Vid undantagstillstånd har myndigheterna starkare befogenheter och rättigheter att begränsa individens friheter än under normala förhållanden. Genom lagen om undantagstillstånd möjliggörs bl.a. husrannsakan på beslut av inrikesministern, utan tillstånd av domstol, och åtgärder för att stänga webbplatser som förespråkar terrorism eller uppmanar till terrordåd. Undantagstillståndet upphörde den 1 november 2017, då en ny lag om inre säkerhet och kamp mot terrorismen trädde i kraft (Loi renforçant la sécurité intérieure et la lutte contre le terrorisme, n° 2017-1510 du 30 octobre 2017). Syftet med lagen är att stärka den sedan tidigare gällande lagstiftningen så att Frankrike effektivt kan bemöta hotet om terrorism och samtidigt tillgodose individens friheter bättre än vid undantagstillstånd. Den nya lagen innehåller inga aspekter som anknyter till underrättelseverksamhet.

2.2.1.7 Nederländerna

I Nederländernas grundlag (Grondwet voor het Koninkrijk der Nederlanden, 1983, varefter det har gjorts flera mindre ändringar, den senaste 2008) innehåller artikel 10 bestämmelser om integritetsskydd. Enligt artikeln har var och en rätt till respekt för sitt privatliv, men denna rättighet kan begränsas genom lag. Enligt grundlagen utfärdas bestämmelser om insamling och spridning av personliga uppgifter genom lag, i vilken det också föreskrivs om integritetsskydd. Separata bestämmelser om skydd för hemfriden finns i grundlagens artikel 12. Bestämmelser om skydd för hemligheten i fråga om förtroliga meddelanden finns också i en separat bestämmelse. Enligt grundlagens artikel 13 får hemligheten i fråga om förtroliga meddelanden inte kränkas, utom på beslut av domstol i situationer som det föreskrivs om i lag. Telefon- och telegrafhemligheten får inte kränkas, utom i situationer som det föreskrivs om i lag och med tillstånd av den som enligt lag är behörig. Bestämmelser om integritetsskyddet finns bl.a. i personuppgiftslagen (Wet bescherming persoonsgegevens, 2001) och i lagen om lagring av information i telekommunikation (Wet bewaarplicht telecommunicatiegegevens, 2009).

Ett av syftena med den nederländska grundlagsreform som inleddes 2009 har varit att anpassa bestämmelserna i grundlagen till den digitala tidsåldern. En central aspekt har visat sig vara att artikel 13 i grundlagen inte ger ett direkt och tillräckligt skydd vid användning av den digitala tidens nya kommunikationsformer. Som en följd av detta publicerade parlamentets underhus (Tweede Kamer) våren 2012 en rapport om behovet av att ändra artikel 13 i grundlagen (Verslag van een algemeen overleg, gehouden op 23 mei 2012, inzake de Kabinetsstandpunt rapport staatscommissie Grondwet en aanpassing artikel 13 van de Grondwet, 2012). Regeringen har utifrån rapporten berett ett förslag till ändring av artikel 13 i grundlagen (Kabinetsstandpunt Rapport Staatscommissie Grondwet, 2012). I förslaget konstateras det bl.a. att den föråldrade ordalydelsen i grundlagsbestämmelsen behöver uppdateras. Enligt förslaget ska det i den nya bestämmelsen inte nämnas några särskilda kommunikationsformer, utan det ska allmänt hänvisas till integritet i kommunikationen och i telekommunikationen. Syftet är att artikel 13 ska kunna tillämpas för att skydda alla redan existerande och alla kommande kommunikationsformer, såsom e-postkommunikation, internetsamtal och personliga meddelanden i sociala medier. Begränsningar av detta skydd för förtroliga meddelanden ska fortsättningsvis regleras genom lag. Behandlingen av förslaget om ändring av grundlagen pågår fortfarande.

I Nederländerna har bl.a. polisen och underrättelsemyndigheterna lagstadgade befogenheter att inskränka det grundlagsenliga skyddet för hemligheten i fråga om förtroliga meddelanden, om den enligt lag behöriga myndigheten ger tillstånd till det. Bestämmelser om underrättelseverksamhet finns i lagen om underrättelse- och säkerhetstjänsterna (Wet op de inlichtingen- en veiligheidsdiensten, 2017), som trädde i kraft sommaren 2017. Lagen ersatte motsvarande tidigare lag från 2012. I reformen tillkom nya underrättelsebefogenheter, förbättrades den rättsliga kontrollen av underrättelseverksamheten och togs den tekniska utvecklingen i beaktande.

### 2.2.2 Internationella konventioner om mänskliga rättigheter

#### 2.2.2.1 Europakonventionen

Enligt artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Denna rättighet har stått i centrum i Europadomstolens många avgöranden om säkerhets- och underrättelsetjänster, hemliga tvångsmedel och hemlig informationsinhämtning de senaste årtiondena. Vid sidan av Europakonventionens artikel 8 har Europadomstolen i sina avgöranden hänvisat i synnerhet till artikel 13 om effektiva rättsmedel. Enligt den artikeln ska var och en, vars i konventionen angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta

även om kränkningen utförts av en person som har handlat i egenskap av offentlig myndighet. Även artikel 10 om yttrandefrihet och källskydd har varit viktig i Europadomstolens tolkningspraxis.

Enligt Europadomstolens etablerade avgörandepraxis inbegriper begreppen privatliv och korrespondens, som nämns i artikel 8 punkt 1 i konventionen, både telefonkommunikation, e-postkommunikation och annan elektronisk kommunikation som ska anses konfidentiell (bl.a. Liberty m.fl. mot Förenade kungariket, 1.7.2008; Klass m.fl. mot Tyskland, 6.9.1978). Utöver kommunikationens innehåll omfattas också kommunikationens identifieringsuppgifter av skyddet (bl.a. Weber och Saravia mot Tyskland, 29.6.2006; Malone mot Förenade kungariket, 2.8.1984). Redan det att sådan lagstiftning existerar som möjliggör hemlig observation av kommunikationsförbindelser, ingriper i de rättigheter som artikel 8 i konventionen garanterar parterna i kommunikationen och även potentiella parter (Liberty m.fl. mot Förenade kungariket, 1.7.2008; Klass m.fl. mot Tyskland, 6.9.1978).

Rättigheten enligt artikel 8 i Europakonventionen är ändå inte obegränsad. Myndigheterna får nämligen inskränka rättigheten på de villkor som nämns i 2 punkten i artikeln. Inskränkningar av de rättigheter som garanteras i artikel 8 ska grunda sig på nationell lag. Vidare ska en inskränkning av rättigheten vara nödvändig i ett demokratiskt samhälle med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

Europadomstolen har i sin avgörandepraxis ställt upp minimikrav för lagstiftningen om hemliga metoder för informationsinhämtning. Dessa krav tillämpas på såväl traditionella hemliga tvångsmedel, såsom teleavlyssning och annan teknisk observation, som modern informationsinhämtning i informationsnät.

Kravet på att en begränsning ska grunda sig på lag består av fyra delar. För det första ska det finnas en rättslig grund för ingripande i skyddet för förtroliga meddelanden. För det andra beror lagenligheten på tillgänglighet: information om vilka rättsliga regler som tillämpas i en viss situation ska hållas tillgänglig. För det tredje krävs det förutsebarhet, vilket innebär att normerna ska vara tillräcklig noggrant avgränsade för att individen ska kunna sluta sig till följderna av sitt agerande. För det fjärde ska maktmissbruk förhindras. (Rotaru mot Rumänien, 4.5.2000; Malone mot Förenade kungariket, 2.8.1984).

Europadomstolen har dessutom i sin praxis fastslagit sådana kvalitetskriterier för lagstiftningen som de nationella normerna ska uppfylla. I fallen Huvig mot Frankrike och Kruslin mot Frankrike (24.4.1990) definierade domstolen sex kriterier som lagstiftningen om hemliga tvångsmedel ska uppfylla. Av lagstiftningen ska följande framgå: de möjliga målgrupperna för observationen, karaktären av de brott i fråga om vilka observation kan bli aktuellt, hur länge observationen kan fortgå, metoden för rapportering om konversationer som stått under observation, säkerhetsåtgärder vid överlämning av information och utplåning av inspelningar. Europadomstolen har ändå inte alltid varit helt konsekvent i sina bedömningar av om kriterierna har uppfyllts, utan bedömningarna har utgått från hur allvarliga ingreppen i rättigheterna har varit (R.E. mot Förenade kungariket, 27.10.2015).

Kravet på att en begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden ska vara nödvändig omfattar tre centrala delar. Det ska finnas ett vägande samhälleligt behov (*pressing social need*) av en begränsning, ingrepp och eftersträvade godtagbara mål ska stå i rätt proportion till varandra (*reasonable relationship between the interference and pursued legitimate aim*) och ingreppen ha tillräckliga och godtagbara motiveringar. I de fall som gäller underrättelseinhämtning har Europadomstolen ofta granskat lagenligheten och begränsningar-

nas nödvändighet utan att egentliga göra någon åtskillnad mellan dem (Zakharov mot Ryssland, 4.12.2015; Kennedy mot Förenade kungariket, 18.5.2010).

Den nationella säkerheten är en av de hänsyn utifrån vilka man enligt artikel 8 i Europakonventionen får ingripa i skyddet för privatlivet. Staterna har rätt omfattande prövningsmarginal i fråga om hurdan verksamhet de anser utgöra ett hot mot den nationella säkerheten. På basis av Europadomstolens avgörandepraxis omfattas åtminstone det militära försvaret, bekämpningen av terrorism och bekämpningen av olovlig underrättelseverksamhet av den nationella säkerheten (bl.a. Weber och Saravia mot Tyskland, 29.6.2006; Klass m.fl. mot Tyskland, 6.9.1978). Den nationella säkerheten kan emellertid utsättas för många slags hot som är svåra att förutse eller definiera på förhand. Av detta följer enligt domstolen att begreppet nationell säkerhet i första hand ska preciseras utifrån nationell praxis (Kennedy mot Förenade kungariket, 18.5.2010).

I Europadomstolens praxis har det förutsatts att informationsinhämtningen ska vara absolut nödvändig för att skydda de demokratiska institutionerna och att den mycket viktiga information som erhålls ska vara absolut nödvändig för en underrättelseinsats. Tröskeln för hemlig informationsinhämtning ska alltid vara hög. Systemen måste byggas upp så att de används sparsamt och endast i verkligt väl motiverade fall. Modeller där myndigheterna ges för stor prövningsrätt riskerar enligt Europadomstolens åsikt alltid att utsättas för missbruk och är således inte förenliga med kraven i Europakonventionen. (Szabó och Vissy mot Ungern, 12.1.2016.)

I fallet Zakharov ansåg domstolen att det var problematiskt bl.a. att underrättelsemyndigheterna hade nästan obegränsade möjligheter att definiera i vilka situationer och utifrån hurdana händelser ingrepp i meddelandehemligheten kunde göras. Myndigheterna kunde i fallet i fråga nästan helt obegränsat definiera vilka händelser och åtgärder som utgjorde ett hot mot säkerheten (i fråga om såväl nationell, militär och ekonomisk säkerhet som miljösäkerhet). Myndigheterna hade även stor prövningsrätt när det gällde att definiera hur allvarliga hot som berättigade hemliga metoder för informationsinhämtning. Eftersom lagstiftningen på det här sättet lämnade stort rum för tolkning, uppstod enligt domstolen en möjlighet till missbruk. (Zakharov mot Ryssland, 4.12.2015, punkt 248.)

Europadomstolen har dessutom granskat system för övervakning av hemliga metoder för informationsinhämtning. I synnerhet krav på övervakningens effektivitet och tillsynsorganens oberoende har ansetts vara av stor vikt. Frågor förknippade med övervakningens effektivitet gäller tillsynsmyndigheternas rätt att få information, rättsmedlen och att föremålen för underrättelseinhämtning i efterhand underrättas om att befogenheter har utövats mot dem. Europadomstolen har vanligen förutsatt att den person som påstås vara föremål för en kränkning har direkt tillgång till rättsmedel utan några mellanhänder. En förutsättning för möjligheten att anföra besvär eller klagomål är i allmänhet att personen av myndigheten blir underrättad om informationsinhämtning som riktats mot honom eller henne efter att användningen av metoden för informationsinhämtning har avslutats. (Se Zakharov mot Ryssland, 4.12.2015; Kennedy mot Förenade kungariket, 18.5.2010; Association for European Integration and Human Rights & Ekimdzhiev mot Bulgarien, 28.6.2007; Popescu mot Rumänien, 26.4.2007; Weber och Saravia mot Tyskland, 29.6.2006; Klass m.fl. mot Tyskland, 6.9.1978.)

I Europadomstolens rättspraxis har kraven på oberoende övervakning inte uppfyllts t.ex. i system där övervakaren har ett nära förhållande till den verkställande makten. Även alltför nära politiska kopplingar utgör tecken på att ett övervakningssystem inte är tillräckligt oberoende. Trots att Europadomstolen har understrukit att tillsynsorganet inte behöver vara en domstol, har den i sin argumentation betonat yrkeskvalifikationerna och bakgrunden hos medlemmarna i organet och hos dem som väljs att sköta tillsynsuppgifter. Europadomstolen har förhållit sig positiv till övervakningsmodeller där den som utses till uppdraget förutsätts ha en hög domar-

befattning. Dessutom har domstolen konstaterat att det har betydelse för skyddet av demokratin att parlamentet deltar i övervakningen av befogenheterna till hemlig informationsinhämtning. (Se Szabó och Vissy mot Ungern, 12.1.2016; Zakharov mot Ryssland, 4.12.2015; R.E. mot Förenade kungariket, 27.10.2015; Kennedy mot Förenade kungariket, 18.5.2010; Popescu mot Rumänien, 26.4.2007; Weber och Saravia mot Tyskland, 29.6.2006; Segerstedt-Wiberg m.fl. mot Sverige, 6.6.2006; Kopp mot Schweiz, 25.3.1998; Campbell mot Förenade kungariket, 25.3.1992; Leander mot Sverige, 26.3.1987; Klass m.fl. mot Tyskland, 6.9.1978.)

Vid Europadomstolen behandlas för närvarande besvär som gäller moderna metoder för informationsinhämtning. Besvären grundar sig i stor utsträckning på Edward Snowdens avslöjanden om verksamheten vid Förenta staternas underrättelsemyndighet (National Security Agency) och om myndighetens samarbete med underrättelseorganisationer i andra länder. Europadomstolens avgöranden i dessa fall kan komma att påverka vilket innehåll som ges till skyddet för hemligheten i fråga om förtroliga meddelanden enligt artikel 8 i Europakonventionen och till yttrandefriheten enligt artikel 10 i konventionen, inklusive betydelsen av källskyddet. (Se Big Brother Watch m.fl. mot Förenade kungariket, application no. 58170/13; Bureau of Investigative Journalism och Ross mot Förenade kungariket, application no. 62322/14; Human Rights Organisations m.fl. mot Förenade kungariket, application no. 24960/15.)

#### 2.2.2.2 Internationella konventionen om medborgerliga och politiska rättigheter

I artikel 17 i internationella konventionen om medborgerliga och politiska rättigheter (MP-konventionen) föreskrivs det bl.a. om skydd för kommunikation. Enligt artikel 17.1 får ingen utsättas för godtyckligt eller olagligt ingripande med avseende på privatliv, familj, hem eller korrespondens och inte heller för olagliga angrepp på sin heder eller sitt anseende. Enligt artikel 17.2 har var och en rätt till lagens skydd mot sådana ingripanden och angrepp. I artikel 2.1 i MP-konventionen förpliktas konventionsstaterna att vidta åtgärder för att garantera rättigheterna enligt konventionen, inklusive artikel 17.

FN:s kommitté för de mänskliga rättigheterna, som övervakar genomförandet av MP-konventionen, har tagit ställning till tolkningen av konventionens artikel 17 om integritetsskydd. Enligt tolkningen i kommitténs allmänna rekommendation om artikeln (General Comment no. 16, 8.4.1988) medför konventionsbestämmelsen en skyldighet för staterna att själva se till att de inte vidtar några åtgärder som strider mot artikel 17 och att genom lagstiftningen ingripa i kränkningar som begås av enskilda. Uttrycket ”korrespondens” i artikeln avser såväl brev som också andra kommunikationsformer, såsom telefonsamtal och e-postmeddelanden. Alla former av kvarhållande, censur, granskning och publicering av privata meddelanden utgör ingripanden i korrespondensen.

I artikel 17 i konventionen nämns inte de grunder på vilka de rättigheter som garanteras i artikeln kan begränsas. Enligt ordalydelsen i artikeln förbjuds endast godtyckliga och olagliga ingripanden i rättigheterna. Tanken bakom förbudet mot godtyckliga ingripanden är att också ingripanden som baserar sig på lag ska överensstämma med bestämmelserna i och syftet med MP-konventionen och att de i varje enskilt fall ska vara skäliga. Enligt rättslitteraturen erbjuder begränsningsgrunderna i andra artiklar i MP-konventionen och begränsningsgrunderna i artikel 8 i Europakonventionen tolkningshjälp för godtagbara begränsningsgrunder.

Enligt artikel 4 i MP-konventionen kan avvikelser från skyldigheterna enligt konventionen göras endast under allmänt nödläge som hotar nationens fortbestånd. Ett sådant nödläge ska ha kungjorts officiellt. Konventionsstaterna kan då vidta åtgärder som innebär avvikelse från deras skyldigheter enligt MP-konventionen i den utsträckning som oundgängligen behövs med hänsyn till situationens krav. En ytterligare förutsättning är att åtgärderna inte strider mot landets övriga förpliktelser enligt internationell rätt och att de inte innebär åtskillnad enbart på grund av ras, hudfärg, kön, språk, religion eller social härkomst.

Flera besvär om intrång i artikel 17, som gäller integritetsskydd, har lämnats in med stöd av det fakultativa protokollet till MP-konventionen, men hittills har fallen inte gällt datanätssäkerhet, elektronisk kommunikation eller underrättelseverksamhet. Det kan anses sannolikt att den här typen av frågor i fortsättningen blir mera synliga i det arbete som kommittén för de mänskliga rättigheterna bedriver. Underrättelseinhämtning som riktar sig mot elektronisk kommunikation har redan behandlats i samband med konventionsstaternas periodiska rapporter. I sina kommentarer om Förenta staternas fjärde periodiska rapport fäste kommittén i samband med granskningen av underrättelselagstiftningen uppmärksamhet vid bl.a. att ingripanden i skyddet för kommunikationen ska grunda sig på lag. Lagarna ska finnas allmänt tillgängliga och innehålla noggranna bestämmelser om förutsättningarna och metoderna för ingripande, om vilka personer som eventuellt kan bli föremål för ingripanden och om hur lång tid ingripandet kan fortgå. Dessutom ska man se till att det ordnas tillräcklig övervakning och försäkra sig om att de som har blivit föremål för missbruk har tillgång till effektiva rättsmedel. (Se Concluding observations on the fourth periodic report of the United States of America, United Nations, 23.4.2014.)

### 2.2.3 EU-rätt

#### 2.2.3.1 Tillämpningen av EU-rätten och EU:s grundläggande rättigheter

Bestämmelserna i EU:s stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012) riktar sig enligt artikel 51.1 i stadgan, med beaktande av subsidiaritetsprincipen, till unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten. Stadgan tillämpas alltså inte i situationer där det är fråga om tillämpning av enbart nationell lagstiftning och där det inte finns någon reglering i EU-rätten. Även i situationer som inte omfattas av EU-rätten kan stadgan emellertid erbjuda tolkningshjälp, t.ex. om Europadomstolen inte har behandlat en viss rättighet eller fråga som ansluter sig till en rättighet, men det finns rättspraxis om saken hos EU-domstolen.

I artikel 52.3 i stadgan fastställs det att i den mån som stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som i konventionen. Detta hindrar inte unionen från att tillförsäkra ett skydd som är mer långtgående än i Europakonventionen. Nivån på det skydd som tillförsäkras i stadgan får inte vara lägre än motsvarande nivå i Europakonventionen, men den får vara högre. Vid tolkningen av innehållet i och nivån på skyddet för de grundläggande rättigheter som erkänns i EU:s rättsordning ska man först och främst stödja sig på EU-domstolens rättspraxis i fråga om en viss rättighet (yttrande om EU:s anslutning till Europakonventionen, 2/13, EU:C:2014:2454, punkt 170; dom Kadi och Al Barakaat, C-402/05 och C-415/04 P, punkterna 281—285; dom Internationale Handelsgesellschaft, C-11/70, punkt 4).

För att EU-rätten ska vara tillämplig i ett visst ärende krävs det att ärendet har ”tillräcklig anknytning” till EU-rätten (beslut Burzio, C-497/14, punkterna 28–31; beslut Văraru, C-496/14, punkt 21; beslut Petrus, C-451/14, punkterna 18–20). Enbart existensen av EU:s behörighet

räcker inte för att ett ärende ska omfattas av tillämpningsområdet för EU-rätten, utan det som har betydelse är om unionen har använt sin behörighet till att utfärda bestämmelser som gäller ärendet. EU:s grundläggande rättigheter eller allmänna rättsprinciper som sådana, utan någon konkret anknytning till EU-rätten, utgör inte någon sådan tillräcklig anknytning som avses här och gör då inte heller att ett ärende ska omfattas av EU-rätten (beslut Pondiche, C-608/14, punkt 21; beslut Balázs och Papp, C-45/14, punkt 23; dom Torralbo Marcos, C-265/13, punkt 30; beslut Cholakova, C-14/13, punkt 30, beslut Nagy m.fl., C-488/12—C-491/12 och C-526/12, punkt 17; dom Pelckmans Turnhout, C-483/12, punkt 20; dom Åkerberg Fransson, C-617/10, punkt 22).

Av betydelse i anslutning till lagstiftningen om underrättelseinhämtning är de undantag som finns i EU-lagstiftningen och med stöd av vilka tillämpningen av EU-rätten har begränsats i flera rättsakter så att den inte omfattar ärenden som gäller nationell säkerhet. Undantagen grundar sig på den bestämmelse som finns i artikel 4.2 i fördraget om Europeiska unionen och enligt vilken den nationella säkerheten också i fortsättningen ska vara varje medlemsstats eget ansvar. Unionen har således ingen behörighet när det gäller nationell säkerhet. I praktiken är det dock inte alltid entydigt att utesluta tillämpningsområdet för EU-rätten på grundval av undantaget i fråga om nationell säkerhet. EU:s rättsordning samt vissa av EU-domstolens förhandsavgöranden och talan om ogiltighetsförklaring av EU-lagstiftning har alltså betydelse även för underrättelseverksamheten och utvecklandet av den nationella lagstiftningen om den. En medlemsstat som åberopar nationell säkerhet som grund måste påvisa ett verkligt behov av att ty sig till en sådan grund (dom ZZ, C-300/11; dom Insinööritoimisto InsTiimi Oy, C-615/10, punkt 35; dom kommissionen mot Finland, C-284/05, punkterna 45 och 47).

#### 2.2.3.2 Skyddet för hemligheten i fråga om förtroliga meddelanden i EU-rätten

En bestämmelse om skydd för hemligheten i fråga om förtroliga meddelanden finns i artikel 7 i EU:s stadga om de grundläggande rättigheterna. Enligt artikeln har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt artikel 8 i stadgan har var och en också rätt till skydd av de personuppgifter som rör honom eller henne. Uppgifter som omfattas av skyddet av personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Enligt de förklaringar som gäller stadgan och som ska beaktas vid tolkningen av stadgan (EUT C 303, 14.12.2007, s. 17—35) motsvarar de rättigheter som garanteras i artikel 7 i stadgan de rättigheter som garanteras i artikel 8 i Europakonventionen och de har samma innebörd och räckvidd. Med hänsyn till den tekniska utvecklingen har ordet ”korrespondens” i Europakonventionen ersatts med ”kommunikationer” i artikel 7 i stadgan.

Rättigheterna enligt artiklarna 7 och 8 i stadgan är inte absoluta. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Enligt EU-domstolens rättspraxis ska den rättsliga grunden för en begränsning, i enlighet med kravet på bestämmelser i lag, bl.a. vara tillräckligt klar och precis och den måste ge ett visst skydd mot eventuella ingrepp (dom WebMind, C-419/14, punkt 81). Detta kriterium påminner

nära om det som på motsvarande sätt fastställs i Europakonventionen om att villkoren för en begränsning av rättigheter ska vara föreskrivna i lag. Därför kan Europadomstolens rättspraxis erbjuda tolkningshjälp för detta kriterium i synnerhet när det gäller sådana bestämmelser i stadgan som motsvarar rättigheter som ingår i Europakonventionen.

Betydelsen av de grundläggande rättigheter som gäller respekten för privatlivet och skyddet av personuppgifter betonas i EU-domstolens rättspraxis, i synnerhet i samband med elektronisk kommunikation (bl.a. dom Schrems, C-362/14, punkt 39; dom Digital Rights Ireland, C-293/12 och C-594/12, punkt 53; dom Google Spain och Google, C-131/12, punkterna 53, 66 och 74; dom Rijkeboer, C-553/07, punkt 47).

Av rättspraxis framgår att bl.a. bekämpandet av grov brottslighet i syfte att garantera allmän säkerhet (dom Tsakouridis, C-145/09, punkterna 46 och 47) och bekämpandet av internationell terrorism i syfte att upprätthålla internationell fred och säkerhet (dom WebMind, C-419/14, punkt 76; dom Al-Aqsa mot rådet, C-539/10 P och C-550/10 P, punkt 130; dom Kadi och Al Barakaat, C-402/05 P och C-415/05 P, punkt 363) är mål som är förenliga med unionens allmänna samhällsintresse och på basis av vilka det har varit möjligt att föreskriva om begränsningar av de grundläggande rättigheterna. Dessutom nämns nationell säkerhet uttryckligen i artikel 4.2 i fördraget om Europeiska unionens funktionssätt och har av tradition godtagits i EU-domstolens rättspraxis som ett mål som berättigar till begränsningar av de grundläggande rättigheterna (t.ex. dom kommissionen mot Finland, C-284/05, punkterna 45, 47 och 49).

I EU-domstolens praxis har bedömningen av huruvida begränsningar av de grundläggande rättigheterna är förenliga med proportionalitetsprincipen ofta visat sig vara det avgörande steget i bedömningen. Den proportionalitetsprincip som nämns i artikel 52.1 i stadgan hör till EU-rättens allmänna principer och kräver enligt EU-domstolens etablerade rättspraxis att de berättigade målen för den åtgärd eller författning som ska bedömas kan genomföras med hjälp av de medel som föreskrivits av unionen och att de inte överskrider vad som är behövligt och nödvändigt för att målen ska nås samt vad som är lämpligt (appropriate and necessary, t.ex. dom Schaible, C-101/12, punkt 29; dom Sky Österreich, C-283/11, punkt 50; dom Nelson m.fl., C-581/10 och C-629/10, punkt 71; dom Afton Chemical, C-343/09, punkt 45, dom Schecke, C-92/09 och C-93/09, punkt 74). I praktiken handlar det om att hitta en godtagbar balans mellan olika intressen. Undantag och begränsningar som gäller en grundläggande rättighet ska vara nödvändiga så att åtgärderna innebär ett så litet ingrepp som möjligt i rättigheten samtidigt som man effektivt bidrar till att målen med den aktuella EU-regleringen nås (dom WebMind, C-419/14, punkt 82; dom R., C-285/09, punkt 45; dom Schecke, C-92/09 och C-93/09, punkterna 87 och 88).

I sin dom Digital Rights Ireland (C-293/12 och C-594/12) förutsatte EU-domstolen att det ges tillgång till teleidentifieringsuppgifter och att kriterierna för användning av dem är förenliga med proportionalitetsprincipen. Domstolen förklarade datalagringsdirektivet (2006/24/EG) ogiltigt. Enligt EU-domstolen borde direktivet ha innehållit objektiva gränser i anslutning till dess mål i fråga om vilka personers identifieringsuppgifter som får lagras. Dessutom borde det i direktivet närmare ha definierats vilka brott som skulle bekämpas med hjälp av skyldigheten att lagra uppgifter.

I sitt avgörande Schrems ansåg EU-domstolen att en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer i synnerhet anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet. Dessutom konstaterade domstolen att en lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att erhålla tillgång till, rätta eller radera uppgifter som rör dem inte respekterar det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd. (Dom Schrems, C-362/14, punkterna 94 och 95).

I dom Tele2 Sverige bedömer EU-domstolen lagring av lokaliseringsuppgifter och trafikuppgifter i ljuset av direktivet om integritet och elektronisk kommunikation (2002/58/EG, ändrat genom direktiv 2009/136/EG). Domstolen ansåg att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende elektroniska kommunikationsmedel inte överensstämmer med EU-rätten. Trots detta kan medlemsstaterna föreskriva om både en riktad lagring av uppgifterna och en rätt för behöriga nationella myndigheter att få uppgifterna i fråga för att uppnå ett legitimt mål som nämns i direktivet om integritet och elektronisk kommunikation. Domstolen nämnde uttryckligen ”grov brottslighet” (*serious crime*) som ett exempel på ett legitimt mål, eftersom detta mål var relevant i rättegången gällande det nationella målet. Domstolen ansåg att artikel 15.1 i direktivet om integritet och elektronisk kommunikation innehåller en uttömmande förteckning över de legitima målen, vilka bl.a. omfattar allmän säkerhet (*public security*) och nationell säkerhet (*national security*). Enligt domstolen måste de nationella bestämmelserna vara tydliga och precisa. Dessutom ska lagringen av uppgifter och tillgången till uppgifter i enlighet med proportionalitetsprincipen begränsas till vad som är strängt nödvändigt. (Dom Tele2 Sverige, C-203/15 och C-698/15, punkterna 94—96, 102—103, 108—109, 116.)

I dom Tele2 Sverige räknade EU-domstolen upp flera materiella och formella aspekter som ska beaktas i nationella bestämmelser om lagring och användning av uppgifter. Bestämmelserna ska bl.a. innehålla lämpliga rättsmedel. Dessutom ska de nationella bestämmelserna grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. Enligt domen kan omfattningen och tillämpningen av nationella bestämmelser begränsas till vad som är strängt nödvändigt under förutsättningar som gäller bl.a. längden på den tilltänkta lagringen, ett definierat geografiskt område, en viss krets av personer, slag av uppgifter, kommunikationsmedel och den personkrets som berörs. Domstolen ansåg dessutom att förhandskontroll, lagring av uppgifter inom unionens område, en hög nivå på säkerheten för eller skyddet av uppgifter, oåterkallelig förstöring av uppgifterna när deras lagringstid gått ut och givande av information till de personer som berörs av uppgifterna är förutsättningar för att de behöriga myndigheterna ska kunna få uppgifterna i fråga. (Dom Tele2 Sverige, C-203/15 och C-698/15, punkterna 106—111, 117—119, 120—122.)

I sin rättspraxis gällande integritetsskyddet har EU-domstolen ägnat uppmärksamhet åt bl.a. tillsynen över det arrangemang som ska bedömas, tillgången till tillräckliga rättsmedel, uppgiftslämning och informationssäkerhet samt villkoren i fråga om de personer som berörs, förhandstillstånd, tillgång till uppgifter, uppgifternas förvaringstid och förstöring av uppgifter (se dom Tele2 Sverige, C-203/15 och C-698/15, punkterna 106—111, 117—119, 120—122; dom WebMind, C-419/14, punkterna 77—78; dom Schrems, C-362/14, punkterna 40 och 95; dom Digital Rights Ireland, C-293/12 och C-594/12, punkterna 56—67; dom UGT-Rioja m.fl., C-428/06—C-434/06, punkt 80).

## 2.3 Bedömning av nuläget

### 2.3.1 Allmänt

De bestämmelser om de grundläggande fri- och rättigheterna som togs in i grundlagen i samband med 2000 års reform motsvarade i sak de bestämmelser som hade tagits in i II kap. i regeringsformen i samband med den reform av de grundläggande fri- och rättigheterna som trädde i kraft den 1 augusti 1995. I grundlagen har de bestämmelser i 9 § 3 mom. som gäller utlämnande av en finsk medborgare till ett annat land ändrats genom lag 802/2007 och de be-

stämmelser i 14 § om rösträtt och rätt till inflytande och i 23 § om undantag från de grundläggande fri- och rättigheterna under undantagsförhållanden genom lag 1112/2011. I övrigt har bestämmelserna om de grundläggande fri- och rättigheterna varit i kraft i oförändrad form i drygt tjugo år. Vid en utredning av hur reformen av de grundläggande fri- och rättigheterna fungerar och av eventuella behov av ändringar har man gjort bedömningen att bestämmelserna om de grundläggande fri- och rättigheterna i grundlagen som helhet fungerar bra (Promemoria av arbetsgruppen grundlag 2008, justitieministeriet, arbetsgruppsbetänkande 2008:8; Utredning om verkställigheten av grundlagsreformen. Betänkande av uppföljningsarbetsgruppen för grundlagen, justitieministeriet, arbetsgruppsbetänkande 2002:7).

Riksdagens grundlagsutskott har dragit upp allmänna riktlinjer för ändringar av grundlagen i samband med behandlingen av det första förslaget till ändring av grundlagen efter totalreformen. Utskottet konstaterade följande: ”Det gäller att vara återhållsam med ändringar i grundlagen. Man får inte sätta igång med att ändra grundlagen utifrån dagspolitiska scenarier och inte heller om det rubbar de konstitutionella grundlösningarnas stabilitet eller grundlagens funktion som stats- och rättsordningens fundament. Å andra sidan måste man se till att grundlagen ger en rättvisande bild av den statliga maktutövningen och grunderna för individens rättsliga ställning. Eventuella ändringsbehov bör övervägas noggrant och de ändringar som bedöms vara nödvändiga beredas grundligt utgående från en bred debatt i strävan efter samsyn.” (GrUB 5/2005 rd, s. 2.)

### 2.3.2 En särskild begränsningsklausul

Enligt 12 § i den regeringsform som gällde före reformen av de grundläggande fri- och rättigheterna var brev-, telegraf- och telefonhemligheten okränkbar, om det inte föreskrivits om ett undantag genom lag. I de handlingar som gäller beredningen av reformen av de grundläggande fri- och rättigheterna sägs att då regeringsformen stiftades var tanken bakom regleringen av ett flertal av medborgarnas grundläggande fri- och rättigheter som under den ryska makten hade förverkligats i administrativ ordning endast att denna reglering skulle förbehållas riksdagen genom grundlag. Lagförbehållen i II kap. i regeringsformen innehöll i regel inte några villkor för en begränsande eller preciserande lag. (Betänkande av arbetsgruppen för grundläggande fri- och rättigheter 1992, justitieministeriets lagberedningsavdelnings publikation 2/1993, s. 45.)

I och med att bestämmelserna om de grundläggande fri- och rättigheterna tidigare var väldigt allmänt formulerade försvårades i praktiken tillämpningen i domstolar och hos myndigheter, eftersom bestämmelserna inte gav lagtillämparna tillräckliga hållpunkter. Det ansågs dessutom vara ett problem att regeringsformen inte preciserade grunderna för begränsningar av flertalet grundläggande fri- och rättigheter. Gränsdragningen mellan tillåtna och förbjudna restriktioner stod därmed öppen för olika tolkningar. (RP 309/1993 rd, s. 15.) Det fästes också uppmärksamhet vid att lagstiftningspraxis allt mer hade fjärmats från lydelsen i bestämmelserna (GrUB 25/1994 rd, s. 4).

Enligt 10 § 3 mom. i grundlagen kan det genom lag bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande. Sådana särskilda restriktiva klausuler innebär dels att de som stiftar en vanlig lag ges befogenheter att inskränka någon grundläggande fri- och rättighet, dels att det ställs upp ytterligare kriterier som kringskär lagstiftarens prövningsrätt (se t.ex. GrUB 25/1994 rd).

Syftet med de kvalificerade lagförbehållen är att så noggrant och strikt som möjligt bestämma vilka möjligheter till inskränkningar lagstiftaren i samband med en vanlig lag har för att det inte genom grundlag medges en vidare befogenhet att inskränka en grundläggande fri- och rättighet än vad som är absolut nödvändigt (GrUB 25/1994 rd, s. 6). Enligt motiveringen till det kvalificerade lagförbehållet i 10 § 3 mom. i grundlagen räknar man i bestämmelsen uttömmande och så snävt och exakt som möjligt upp möjligheterna att begränsa hemligheten för ett förtroligt meddelande (RP 309/1993 rd, s. 58).

Grunderna för begränsningar av hemligheten i fråga om förtroliga meddelanden i 10 § 3 mom. i grundlagen är framför allt tämligen konkreta och även detaljerade (vid rättegång och säkerhetskontroll samt under frihetsberövande). Grunden i anslutning till utredning av brott (utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden) är i någon mån mera allmänt formulerad, i synnerhet med beaktande av grundlagsutskottets tolkningspraxis beträffande grunden, som till viss del har utvidgats till att gälla också förebyggande av brott och även sådan utredning av brottsliga gärningar som inte syftar till att förverkliga straffansvaret (GrUU 19/2008 rd). Grunderna för begränsningar av hemligheten i fråga om förtroliga meddelanden är också i någon mån mera konkreta och exakta än de likaså i 10 § 3 mom. i grundlagen föreskrivna grunderna för tillåtna åtgärder som ingriper i hemfriden.

I förarbetena till reformen av de grundläggande fri- och rättigheterna har grunderna för begränsningar av hemligheten i fråga om förtroliga meddelanden kopplats till då identifierade, konkreta lagstiftningsbehov. Skyddet för hemligheten i fråga om förtroliga meddelanden sträcker sig till olika former av kommunikation på ett teknikneutralt sätt. Vid utformningen av grunderna för begränsningar av hemligheten i fråga om förtroliga meddelanden har man dock inte till alla delar kunnat förutse den framtida samhälleliga och tekniska utvecklingen. Detta innebär att frågor som gäller befogenheter till underrättelseinhämtning inte har kunnat beaktas vid beredningen av reformen av de grundläggande fri- och rättigheterna.

Även i konventionerna om mänskliga rättigheter, t.ex. Europakonventionen, ingår särskilda begränsningsklausuler. Innehållet i de begränsningsgrunder som är tillåtna enligt 10 § 3 mom. i grundlagen skiljer sig dock från begränsningsgrunderna enligt t.ex. artikel 8 i Europakonventionen. De begränsningsgrunder som är tillåtna enligt Europakonventionen har formulerats mer fritt och abstrakt än de grunder som anges i 10 § 3 mom. i grundlagen. Skillnaderna förklaras delvis av det annorlunda sättet att skriva konventionsbestämmelser, deras ställning som fastställare av miniminivån på skyddet och staternas prövningsmarginal vid tillämpningen av konventionen.

Enligt artikel 7 i EU:s stadga om de grundläggande rättigheterna har var och en rätt till respekt för sina kommunikationer. Artikeln innehåller inte någon förteckning över godtagbara grunder för en begränsning av rätten, men i artikel 52.1 i stadgan finns allmänna bestämmelser om förutsättningarna för begränsningar av en rättighet.

I ovan granskade grundlagar i europeiska stater med en liknande rättskultur som i Finland finns det inte heller några grunder för begränsningar av hemligheten i fråga om förtroliga meddelanden som motsvarar dem i 10 § 3 mom. i grundlagen. Detta förklaras av de olika regleringsformerna i grundlagarna och delvis också av tidpunkten för stiftandet av dem.

### 2.3.3 Behovet av en grundlagsändring

Hemligheten i fråga om förtroliga meddelanden kan enligt 10 § 3 mom. i grundlagen begränsas bl.a. vid utredningen av vissa brott. Utredning av brott kan som uttryck förstås så att det

endast avser utredning av redan begångna brott. Tolkningen av 10 § 3 mom. i grundlagen utvidgades dock till att omfatta även förhindrande av vissa brott redan rätt snart efter reformen av de grundläggande fri- och rättigheterna. En så långvarig och etablerad lagstiftningspraxis som skiljer sig från formuleringen i bestämmelsen bidrar till att regleringen om de grundläggande fri- och rättigheterna uttrycksmässigt blir vilseledande.

I den tolkningspraxis som gäller begränsningar av hemligheten i fråga om förtroliga meddelanden har det ställts krav på en konkret och specificerad misstanke om brott (t.ex. GrUU 37/2002 rd, GrUU 5/1999 rd, s. 3—4). En sådan föreligger när det finns skäl att misstänka att någon begått eller ämnar begå en straffbar gärning. I ljuset av nuvarande tolkningspraxis är det därmed inte möjligt att med stöd av 10 § 3 mom. i grundlagen föreskriva om sådana begränsningar i hemligheten i fråga om förtroliga meddelanden som inte syftar till att bekämpa eller utreda ett specificerat brott utan till att i större utsträckning inhämta för den nationella säkerheten nödvändig information om allvarliga hot, i synnerhet för att kunna förbereda för och förutse sådana hot samt till stöd för den högsta statsledningens beslutsfattande. Ordalydelsen i 10 § 3 mom. i grundlagen möjliggör inte ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden för underrättelseinhämtningssyften t.ex. när det gäller sådan verksamhet som hotar den nationella säkerheten som inte har framskridit till ett sådant stadium att det mot verksamheten kunde riktas en konkret och specificerad brottsmisstanke eller som inte är straffbelagd.

För att kunna identifiera och avvärja eventuella hot mot Finland och dess befolkning är det nödvändigt att få uppgifter om militär verksamhet och sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Den verksamhet som informationsinhämtningen riktar sig mot är nödvändigtvis inte straffbar eller så långt framskriden att det vore möjligt att rikta en konkret och specificerad brottsmisstanke mot verksamheten. Information behövs t.ex. om utvecklingen i den säkerhetspolitiska miljön och om verksamhet som allvarligt hotar statsordningen eller grundläggande samhällsfunktioner, såsom verksamhet som hänför sig till terrorism eller våldsbejakande radikalisering eller till utländska underrättelsetjänsters verksamhet.

Information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten måste kunna inhämtas också på sådana sätt som kan begränsa skyddet för hemligheten i fråga om förtroliga meddelanden i den moderna kommunikationen. Bestämmelserna om de grundläggande fri- och rättigheterna skyddar fysiska personer. Dessutom sträcker sig bestämmelserna indirekt till juridiska personer. Däremot lämnas staten och andra offentliga samfund utanför skyddet för de grundläggande fri- och rättigheterna (RP 309/1993 rd, s. 25, se t.ex. GrUU 9/2015 rd). Detta innebär att t.ex. kommunikationen i en främmande stats militära organisation eller annan myndighetsorganisation inte åtnjuter skydd för hemligheten i fråga om förtroliga meddelanden och att en reglering av befogenheter som enbart gäller sådana organisationers kommunikation inte är problematisk med tanke på 10 § 3 mom. i grundlagen. Det bedöms dock inte vara möjligt att i samtliga fall rikta befogenheterna att inhämta underrättelser så exakt att det inte föreligger någon risk för att myndigheterna tillfälligt får tillträde till information om sådana enskilda personers kommunikation som inte har samband med ett underrättelseuppdrag. Vid bedömningen av om det är fråga om en begränsning av hemligheten i fråga om förtroliga meddelanden ska man beakta EU-domstolens och Europadomstolens rättspraxis, enligt vilken insamling av information eller redan tillgång till den utgör ett ingrepp i skyddet för privatlivet.

Skyddet för identifieringsuppgifter i fråga om förtroliga meddelanden har i den tidigare lagstiftningspraxisen bedömts annorlunda än skyddet för innehållet i ett meddelande. Grundlagsutskottet har dock efter EU-domstolens dom i ärendet Digital Rights Ireland bedömt att i praktiken kan identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem vara problematiska med hänsyn till skyddet för pri-

vatlivet 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). Det är ännu inte möjligt att utifrån grundlagsutskottets senaste utlåtandepraxis entydigt avgöra vilka skillnader denna nya bedömning kan leda till jämfört med de tidigare tolkningarna, som stödde sig på de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. EU-domstolen har i sitt avgörande Tele2 Sverige upprepat sina anmärkningar i ärendet Digital Rights Ireland när det gäller möjligheten att sammanställa och kombinera uppgifter. Med beaktande av både grundlagsutskottets praxis och EU-domstolens avgöranden är det inte möjligt att som sådan ta den tidigare praxisen gällande identifieringsuppgifter som grund för regleringen av underrättelseinhämtning som avser datatrafik. Med beaktande av även denna aspekt är det inte möjligt att föreskriva om sådana befogenheter till underrättelseinhämtning som begränsar skyddet för hemligheten i fråga om förtroliga meddelanden genom vanlig lag utan ändring av grundlagen.

I den föreslagna lagstiftningen om civil och militär underrättelseinhämtning är det fråga om sådan ny lagstiftning i Finland som har betydande konsekvenser för skyddet för privatlivet, som tryggas i egenskap av grundläggande och mänsklig rättighet, och i synnerhet för skyddet för hemligheten i fråga om förtroliga meddelanden. I samband med tidigare reformer av grundlagen har man fäst uppmärksamhet vid att grundlagens innehåll ska ge en rättvisande bild av de grundlösningar som genomförs i vanlig lagstiftning. Även av denna orsak är det motiverat att bestämmelser om den nu aktuella nya och betydande grunden för ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden tas in i grundlagen. Grundlagsutskottet har dessutom ansett att det är otillfredsställande att tillämpningen av 10 § 3 mom. i grundlagen i viss mån fjärmat sig från den språkliga utformningen i bestämmelsen. Utskottet har uppmanat regeringen att ta ställning till vilka åtgärder som kan behöva vidtas till följd av detta. I detta sammanhang fäste utskottet uppmärksamhet inte bara vid de bestämmelser i grundlagen som gäller begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden utan också vid de grundlagsbestämmelser som gäller begränsningar av hemfriden. (GrUU 36/2017 rd, s. 4—5.)

## 3 Målsättning och de viktigaste förslagen

Syftet med propositionen är att se över bestämmelserna i grundlagen så att det för att trygga den nationella säkerheten genom lag kan föreskrivas om nödvändiga begränsningar i skyddet för förtroliga meddelanden, när de förutsättningar som ska anses vara behövliga är uppfyllda. Den ändrade bestämmelsen i grundlagen ska vara förenlig med Finlands människorättsförpliktelser.

Vid beredningen har man övervägt en ändring av bestämmelserna om skyddet för hemligheten i fråga om förtroliga meddelanden så att det kvalificerade lagförbehållet till denna del stryks ur 10 § i grundlagen. I så fall kunde skyddet för hemligheten i fråga om förtroliga meddelanden begränsas i enlighet med de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. Ett sådant regleringsalternativ har dock inte ansetts motiverat. Ett slopande av kvalifikationen lämpar sig inte väl med tanke på den starkt skyddade ställning som hemligheten för förtroliga meddelanden traditionellt har eller med tanke på systematiken i grundlagens kapitel om grundläggande fri- och rättigheter. En sådan ändring skulle förutsätta att formuleringarna i kapitlet om de grundläggande fri- och rättigheterna ses över i ännu större utsträckning.

Vid beredningen har man dessutom övervägt att ändra 10 § i grundlagen så att det till paragrafen endast fogas ett omnämnande om sådana begränsningar i hemligheten i fråga om förtroliga

meddelanden som är nödvändiga med tanke på den nationella säkerheten. Att foga en sådan mycket allmän begränsningsgrund till 10 § skulle dock i någon mån strida mot det faktum att man vid beredningen av den reform av de grundläggande fri- och rättigheterna som resulterade i 8 § i regeringsformen, som föregick 10 § i grundlagen, strävade efter att precisera grunderna för begränsningar av de grundläggande fri- och rättigheterna. Då gjordes bedömningen att skillnaden mellan ett kvalificerat och enkelt lagförbehåll inte blir särskilt stort om begränsningsförutsättningarna är mycket allmänt utformade (t.ex. allmän ordning och säkerhet). Likaså gjordes bedömningen att man ska undvika att beskriva begränsningsgrunderna med så vaga formuleringar att lagförbehållets normativa effekt avsevärt försvagas (grundrättskommitténs promemoria Perusoikeuksien rajoittamisesta, 26.3.1990).

Vid beredningen har man också uteslutit möjligheten binda de föreslagna nya befogenheterna för civil och militär underrättelseinhämtning till utredningen av brott som äventyrar individens eller samhällets säkerhet enligt 10 § i grundlagen. För att kunna identifiera och avvärja eventuella hot mot Finland och dess befolkning måste det på godtagbara grunder vara möjligt att bryta skyddet för ett förtroligt meddelande även i sådana situationer där den verksamhet som informationsinhämtningen riktar sig mot inte är straffbar eller så långt framskriden att det vore möjligt att rikta en brottsmisstanke mot verksamheten. Det har inte heller ansetts vara möjligt att i detta syfte utvidga tillämpningsområdet för de hemliga tvångsmedel som det föreskrivs om i polislagen, tvångsmedelslagen eller lagen om militär disciplin och brottsbekämpning inom försvarsmakten.

Det föreslås att 10 § i grundlagen ändras så att det till paragrafen fogas ett nytt 4 mom. med bestämmelser om begränsning av hemligheten i fråga om förtroliga meddelanden. I momentet föreslås en bestämmelse om att det genom lag kan föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning 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. Genom ändringen tas det i en särskild begränsningsklausul in nya godtagbara grunder på vilka hemligheten i fråga om förtroliga meddelanden kan begränsas.

Början av 10 § 4 mom. i grundlagen motsvarar i övrigt det som för närvarande föreskrivs som saken i 10 § 3 mom., men uttrycket ”vid utredning av brott” ska ersättas med uttrycket ”vid bekämpning av brott”. Uttrycket bekämpning av brott omfattar förebyggande, avslöjande och utredning av brott. Avsikten med ändringen är inte att ändra rättsläget jämfört med hur det har utformats i praxisen för tolkningen av gällande10 § 3 mom. i grundlagen, utan att se över bestämmelsens ordalydelse så att den motsvarar grundlagsutskottets vedertagna tolkning.

Tolkningen av uttrycket ”utredning av brott” i 10 § 3 mom. i grundlagen fjärmade sig från bestämmelsens ordalydelse redan relativt snart efter reformen av de grundläggande fri- och rättigheterna. Utredning av ett brott har i tolkningspraxis också kunnat omfatta åtgärder som vidtas på grund av en konkret och specificerad misstanke om brott, även om brottet ännu inte har hunnit begås. Således har det ansetts att det trots 10 § 3 mom. i grundlagen är möjligt att använda t.ex. teleövervakning för att förhindra vissa brott (GrUU 5/1999 rd, GrUU 2/1996 rd).

I det nya 4 mom. görs det dessutom möjligt att begränsa skyddet för ett förtroligt meddelande för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Begränsningen av hemligheten i fråga om förtroliga meddelanden ska vara kopplad till inhämtande av information om den verksamhet som avses i bestämmelsen. Till både innehåll och skrivsätt bedöms den föreslagna nya bestämmelsen i 10 § i grundlagen passa väl ihop med de begränsningsklausuler som redan ingår i paragrafens 3 mom.

Den föreslagna nya begränsningsgrunden i 10 § 4 mom. i grundlagen ska vara utformad så att det med stöd av den är möjligt att i en vanlig lag föreskriva om befogenheterna för underrättelseinhämtning. Bestämmelsen begränsar till viss del betydligt de villkor på vilka det kan föreskrivas om befogenheterna. Grunden för begränsning av hemligheten i fråga om förtroliga meddelanden kan enbart vara inhämtande av information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Således uppställs en hög tröskel för den verksamhet som informationsinhämtningen riktar sig mot.

Genom den föreslagna ändringen tas det i en särskild begränsningsklausul in en ny godtagbar grund på vilken hemligheten i fråga om förtroliga meddelanden kan begränsas. Det föreslås inte några ändringar i de övriga begränsningsförutsättningarna i 10 § i grundlagen. Dessutom blir de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna direkt tillämpliga.

Av det krav på nödvändighet och på att begränsningen ska harmoniera med internationella människorättsförpliktelser som anges i bestämmelsen och som ingår i de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna liksom av EU-rätten följer krav bl.a. på att befogenheterna ska specificeras. Den föreslagna regleringen möjliggör därmed inte införande av lagstiftning om allmän, oriktad och heltäckande övervakning av datatrafik.

## 4 Propositionens konsekvenser

Det föreslås att bestämmelserna om hemligheten i fråga om förtroliga meddelanden i 10 § i grundlagen för det första ska ändras så att den godtagbara grunden för begränsning av denna grundläggande fri- och rättighet inte längre är utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden utan bekämpning av sådana brott. Avsikten med förslaget är inte att ändra rättsläget jämfört med hur det har utformats i praxisen för tolkningen av 10 § 3 mom. i grundlagen.

För det andra föreslås att det i 10 § i grundlagen tas in en bestämmelse om att det genom lag kan föreskrivas om nödvändiga begränsningar i meddelandehemligheten för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

Den föreslagna ändringen gör det möjligt att införa sådan lagstiftning där hemligheten för förtroliga meddelanden begränsas på nya grunder. I praktiken möjliggör ändringen lagstiftning om befogenheter att inhämta underrättelser.

Den föreslagna grundlagsbestämmelsen gör det möjligt att i större utsträckning än för närvarande ingripa i skyddet för hemligheten i fråga om förtroliga meddelanden. Möjligheten att ingripa i skyddet för hemligheten i fråga om förtroliga meddelanden begränsas dock av de relativt snäva förutsättningar som föreslås i bestämmelsen och av de allmänna förutsättningarna för begränsningar av de grundläggande fri- och rättigheterna. Regleringens konsekvenser i detalj är i sista hand beroende av innehållet i den reglering på nivån av vanlig lag som den föreslagna grundlagsbestämmelsen möjliggör.

Med stöd av den föreslagna bestämmelsen kan man genom lag föreskriva om sådana befogenheter att inhämta underrättelser som är nödvändiga för inhämtande av information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Må-

len för regleringen har alltså samband med säkerställandet av såväl statens självbestämmanderätt och verksamhet som befolkningens säkerhet.

De föreslagna bestämmelserna har inga direkta ekonomiska konsekvenser eller konsekvenser för myndigheternas verksamhet. Den underrättelselagstiftning som möjliggörs av den nya begränsningsgrund som föreslås bli intagen i 10 § 4 mom. i grundlagen bedöms dock ha delvis också betydande konsekvenser. Av de internationella konventionerna om mänskliga rättigheter och de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna följer ett krav på en behörig övervakning av underrättelseverksamheten, vilket bedöms ha både ekonomiska konsekvenser och konsekvenser för myndigheternas verksamhet. Tillstånds- och tillsynsmyndigheterna ska ha tillräckliga resurser och deras personal ska ha både juridiskt och tekniskt kunnande.

## 5 Beredningen av propositionen

### 5.1 Beredningsskeden och beredningsmaterial

Utkastet till regeringens proposition bereddes i en sakkunnigarbetsgrupp som tillsattes av justitieministeriet den 28 september 2015. Arbetsgruppen hade i uppdrag att för den parlamentariska beredning som tillsattes senare utreda och bereda en revision av grundlagen så att det för att trygga den nationella säkerheten genom lag kan föreskrivas om nödvändiga begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden, när de förutsättningar som ska anses vara behövliga är uppfyllda. Under arbetets gång hörde arbetsgruppen sakkunniga i statsförfattningsrätt och civil och militär underrättelseinhämtning och lät göra behövliga utredningar. Arbetsgruppens arbete övervakades av en parlamentarisk uppföljningsgrupp som tillsattes den 11 december 2015.

Arbetsgruppens betänkande (Hemligheten i fråga om förtroliga meddelanden. Granskning av grundlagsregleringen, justitieministeriet, betänkanden och utlåtanden 41/2016) blev klart den 23 september 2016 och publicerades den 11 oktober 2016. Arbetsgruppen föreslog att 10 § i grundlagen ska ändras så att det till paragrafen fogas ett nytt 4 mom. där alla bestämmelser om förutsättningarna för begränsning av hemligheten i fråga om förtroliga meddelanden samlas. Genom lag kan enligt förslaget föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning 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.

### 5.2 Remissyttranden och hur de har beaktats

Arbetsgruppens betänkande sändes på remiss den 1 november 2016. Remissyttranden lämnades av 30 instanser, varav 12 myndigheter, 14 sammanslutningar och fyra privatpersoner. De kommentarer som framfördes i yttrandena gällde framför allt motiveringarna till förslaget till ändring av grundlagen. Dessutom föreslogs det ändringar i paragraftextens formulering.

Största delen av remissinstanserna ansåg att ändringen av grundlagen är motiverad och ändamålsenlig. Remissinstanserna var i stor utsträckning eniga om att det finns ett behov att ta in ett kvalificerat lagförbehåll i 10 § i grundlagen. Ett allvarligt hot mot den nationella säkerheten ansågs i sig vara en godtagbar grund för en viss begränsning av skyddet för hemligheten i

fråga om förtroliga meddelanden. Dessutom delade remissinstanserna i stor utsträckning arbetsgruppens åsikt att grundlagens ordalydelse bör ändras så att den motsvarar den vedertagna tillämpningspraxisen gällande skyddet för kommunikationen vid utredning av brott. De remissinstanser som förhöll sig negativt till betänkandets förslag hänvisade till att ändringen inte är nödvändig eller att syftet med den kan uppnås på annat sätt. Rätt allmänt framhölls ett behov av att närmare definiera och avgränsa begreppen militär verksamhet och nationell säkerhet i motiveringen till förslaget.

Flera remissinstanser föreslog att ett förbud mot s.k. massövervakning ska skrivas in i antingen 10 § i grundlagen eller i motiveringen till ändringsförslaget. Dessutom ansåg remissinstanserna det att det fanns ett behov av att precisera de skrivningar i motiveringen som gällde den tidsmässiga dimensionen. De tog också upp ett behov av att mera täckande och grundligare beakta rättspraxisen vid Europadomstolen och EU-domstolen samt att fördjupa den internationella jämförelsen. Ett sammandrag av yttrandena har sammanställts vid justitieministeriet (Lausuntotiivistelmä mietinnöstä ”Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen”, justitieministeriet, 29.6.2017).

Regeringens proposition har färdigställts vid justitieministeriet utifrån arbetsgruppens betänkande och remissvaren gällande det under övervakning av en parlamentarisk uppföljningsgrupp.

## 6 Samband med andra propositioner

Propositionen hänger samman med de regeringspropositioner som beretts vid inrikesministeriet och försvarsministeriet och i vilka det föreslås bestämmelser om civil och militär underrättelseinhämtning. Propositionen hänför sig också till den regeringsproposition som beretts vid justitieministeriet och i vilken det föreslås att det ska stiftas en lag om övervakning av underrättelseverksamheten. Dessutom har propositionen kopplingar till det förslag av talmanskonferensen om ändring av riksdagens arbetsordning som beretts i riksdagen i syfte att ordna den parlamentariska kontrollen av underrättelseverksamheten.

## DETALJMOTIVERING

### 1 Lagförslag

**10 §.** *Skydd för privatlivet.* Det föreslås att det till paragrafen fogas ett nytt 4 mom. så att den andra meningen i nuvarande 3 mom. revideras till innehållet och flyttas till 4 mom.

I paragrafens 4 mom. föreslås det en bestämmelse om att det genom lag kan föreskrivas om sådana begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden som är nödvändiga vid bekämpning 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.

I 4 mom. samlas därmed alla bestämmelser om begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden. Början av momentet motsvarar i övrigt det som för närvarande föreskrivs om saken i 10 § 3 mom., men uttrycket ”vid utredning av brott” ska ersättas med det nya uttrycket ”vid bekämpning av brott”. Slutet av momentet är nytt.

Tolkningen av uttrycket ”vid utredning av brott” i 10 § 3 mom. i grundlagen avvek från bestämmelsens ordalydelse redan relativt snabbt efter reformen av de grundläggande fri- och rättigheterna 1995. Enligt grundlagsutskottet kan uttrycket på rent språkliga grunder förstås så att det endast avser redan begångna brott. I praktiken är det dock inte möjligt att dra en exakt gräns enligt gärningsögonblicket. Många brott är av sådan typ att det inte är möjligt att utreda dem, om det över huvud taget inte uppdagas att ett brott har begåtts, vilket i sin tur kan kräva att man på förhand bereder sig för att ett brott kommer att begås (GrUU 2/1996 rd). Därmed har utredning av ett brott i tolkningspraxis också kunnat omfatta åtgärder som vidtas på grund av en konkret och specificerad misstanke om brott, även om brottet ännu inte har hunnit begås (GrUU 5/1999 rd, GrUU 2/1996 rd).

Avsikten med förslaget är inte att ändra rättsläget jämfört med hur tolkningen av 10 § 3 mom. i grundlagen har utformats i grundlagsutskottets utlåtandepraxis. Förslagets uttryck ”bekämpning av brott” omfattar således förebyggande, avslöjande och utredning av brott. I den gällande lagstiftningen som har tillkommit med grundlagsutskottets medverkan omfattar uttrycket ”brottsbekämpning” dessa nämnda verksamheter. Språkligt sett passar dock ”bekämpning av brott” bättre i grundlagstexten.

I momentet anges en ny godtagbar grund för en begränsning av skyddet för ett förtroligt meddelande, dvs. ”för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten”. I den nya begränsningsgrunden frigör man sig från verksamhet som grundar sig på brott. Det är fråga om informationsinhämtning om de verksamheter som nämns i bestämmelsen men i fråga om vilka det inte ännu går att lägga fram någon konkret och specificerad brottsmisstanke (åtminstone inte ännu vid tidpunkten för informationsinhämtning). Närmare bestämmelser om den verksamhet som avses i bestämmelsen ska utfärdas genom en vanlig lag.

Med militär verksamhet avses i bestämmelsen militärt organiserade truppers verksamhet eller verksamhet i anslutning till militära maktmedel, såsom beväpning och militärmateriel, eller annan med denna jämställbar verksamhet som bedrivs av trupper som använder militär makt. Det kan vara fråga om både statlig och icke-statlig verksamhet. Statlig verksamhet härrör från verksamhet som bedrivs av en främmande stats väpnade styrkor eller från därmed jämställbar

verksamhet som bedrivs av en internationell militär allians eller organisation, medan icke-statlig verksamhet avser sådan militärt organiserad, beväpnad eller utrustad verksamhet som inte har ovan avsedda statliga ursprung eller där ett sådant ursprung inte kan identifieras. Inhämtande av information om i bestämmelsen avsedd militär verksamhet ska inte förutsätta att verksamheten utgör ett allvarligt hot mot den nationella säkerheten. Militär verksamhet måste ofta följas långsiktigt och systematiskt utan att den verksamhet som övervakas behöver utgöra en överhängande fara under den tid övervakningen pågår.

Inhämtningen av information omfattar kartläggning och övervakning av externa militära åtgärder som riktar sig mot Finland. Det handlar t.ex. om att följa utvecklingen av den militära verksamhet som är av betydelse med tanke på Finlands säkerhetsmiljö i syfte att skapa en lägesbild. Uttrycket omfattar bl.a. kontinuerlig informationsinhämtning om utvecklingen av andra länders militära kapacitet samt informationsinhämtning om militär underrättelseverksamhet utomlands som riktar sig mot Finlands försvar.

Kommunikationen i en främmande stats myndighetsorganisation åtnjuter inte skydd för hemligheten i fråga om förtroliga meddelanden. För att upptäcka sådan kommunikation kan det dock vara nödvändigt att ingripa i hemligheten i fråga om förtroliga meddelanden. Exempelvis vid underrättelseinhämtning som avser datatrafik kan identifieringen av en kommunikationsnätsdel som används av en främmande stats myndigheter tekniskt sett förutsätta ingrepp i annan kommunikation. Detta innebär att systemet med grundläggande fri- och rättigheter ställer krav på regleringen av befogenheterna att inhämta information även när det gäller övervakningen av främmande staters verksamhet.

I bestämmelsen tas det också in en möjlighet att begränsa skyddet för hemligheten i fråga om förtroliga meddelanden i syfte att inhämta information om sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Uttrycket ”nationell säkerhet” används redan i den nuvarande lagstiftningen. Uttrycket finns också som en grund för begränsning av de mänskliga rättigheterna i Europeiska unionens rättsordning och i internationella konventioner om mänskliga rättigheter. I unionens rättsordning eller i de förpliktelser som gäller mänskliga rättigheter har uttrycket inte getts närmare innehåll än dess betydelse enligt allmänt språkbruk. Exempelvis i tolkningen av Europakonventionen har staterna ansetts ha en ganska bred marginal för bedömning av vilken typ av verksamhet som de anser äventyrar den nationella säkerheten (t.ex. Kennedy mot Förenade kungariket, 18.5.2010). Europadomstolen har dock ställt upp sådana minimikrav för lagstiftningen om hemliga metoder för inhämtning av information som syftar till att förhindra ett godtyckligt ingripande i skyddet för en individs förtroliga meddelanden (t.ex. Zakharov mot Ryssland, 4.12.2015). Inom tillämpningsområdet för unionsrätten ska begreppen allmän och nationell säkerhet tolkas i ljuset av unionsrätten och den rättspraxis vid EU-domstolen som preciserar dessa begrepp. EU-domstolen utgår av hävd från att omfattningen av sådana begrepp som allmän och nationell säkerhet i anslutning till tillämpningen av unionsrätten inte kan definieras ensidigt av varje medlemsstat utan kontroll av unionens institutioner. (Se t.ex. dom J.N., C-601/15, punkterna 65—66.)

Med nationell säkerhet hänvisas i bestämmelsen i sista hand till ett yttre hot om våld som omedelbart eller indirekt riktas mot den kollektiva säkerheten hos människorna som omfattas av statens jurisdiktion. Ett allvarligt hot mot den nationella säkerheten är typiskt sett en sådan allmänfarlig och därtill ansluten verksamhet som hotar en stor och oförutsedd, slumpmässigt bestämd grupp människors liv eller hälsa. Härmed avses t.ex. verksamhet i anslutning till terrorism, våldbejakande radikalisering, massförstörelsevapen eller äventyrande av internationell fred och säkerhet.

Med hänsyn till den nationella säkerheten är sådana grundläggande samhällsfunktioner centrala som om de störs eller lamslås i sista hand kan leda till att människors liv eller hälsa även-

tyras allvarligt. Till dessa hör t.ex. el-, kommunikations- och trafiknät eller funktioner som upprätthåller livsmedels- och läkemedelsförsörjningen eller den nationella försörjningsberedskapen. Ett hot mot dessa kan visa sig i form av öppet våld eller t.ex. i form av attacker mot datanät eller kombinationer av olika metoder. Verksamhet som syftar till eller gör det möjligt att störa eller lamslå de grundläggande samhällsfunktionerna kan alltså allvarligt hota den nationella säkerheten.

En demokratisk stats- och samhällsordning och institutionerna i ett demokratiskt samhälle bildar grunden för säkerheten för de människor som lever och fungerar i gemenskapen. Med tanke på den nationella säkerheten är det viktigt att de högsta statsorganen och andra organ med offentlig makt liksom även t.ex. de som sörjer för de grundläggande samhällsfunktionerna kan sköta sina uppgifter utan yttre störningar. Även sådan yttre verksamhet som syftar till eller gör det möjligt att störa det demokratiska samhället och dess institutioner eller lamslå deras verksamhet kan alltså allvarligt hota den nationella säkerheten.

Med verksamhet som allvarligt hotar den nationella säkerheten avses i bestämmelsen därmed verksamhet som hotar den demokratiska stats- och samhällsordningen, grundläggande samhällsfunktioner, ett stort antal människors liv eller hälsa eller internationell fred och säkerhet. En förutsättning är dock att verksamheten har någon koppling till Finland och att den hotar uttryckligen Finlands nationella säkerhet, även om verksamheten geografiskt sett kan ske utanför Finlands gränser.

Den verksamhet som avses i bestämmelsen kan vara sådan att den när praktiska åtgärder vidtas utgör ett brott, men ingen konkret och specificerad brottsmisstanke kan ännu riktas mot verksamheten. Det kan också vara fråga om verksamhet som i princip inte är ett brott enligt finsk lagstiftning och som inte heller kan utvecklas till ett brott, t.ex. utländska underrättelsetjänsters verksamhet i Finland. Även om den underrättelsetjänst som staterna bedriver globalt sett är stabil till sin natur, och staterna de facto till en viss gräns accepterar den, kan den utifrån sina särdrag bilda riskfaktorer för den nationella säkerheten. Även allvarliga oroligheter i en stat som är central med tanke på Finlands säkerhet eller ett allvarligt äventyrande av gränssäkerheten kan utgöra ett allvarligt hot mot den nationella säkerheten.

Uttrycket ”nationell säkerhet” betyder att den hotfulla verksamhet som avses i bestämmelsen inte i första hand riktar sig mot en viss individ utan mer allmänt mot samhället och den mänskliga gemenskapen. Också t.ex. våldsdåd som riktar sig mot enskilda personer kan emellertid utgöra en sådan verksamhet som avses i bestämmelsen, om de till sin omfattning eller betydelse är av betydelse med tanke på den nationella säkerheten och således kan utgöra ett allvarligt hot mot den. Det är uppenbart att t.ex. hot som riktar sig mot statsledningen eller personer som sköter grundläggande samhällsfunktioner liksom personer som svarar för deras säkerhet kan utgöra ett allvarligt hot mot den nationella säkerheten.

Dessutom kan verksamhet som hotar myndigheter eller personer som deltar i Finlands internationella krishanterings- eller biståndsuppdrag vara verksamhet som avses i bestämmelsen. Vid krishanterings- och biståndsuppdrag är det fråga om verksamhet i finska statens regi, där Finland sänder krishanterings- och biståndspersonal till uppgifter som syftar till att upprätthålla eller återställa internationell fred och säkerhet eller till humanitära biståndsuppdrag. Sådan verksamhet är förlagd till områden eller gäller situationer där säkerhetsrisken ofta är hög. Hot mot sådan verksamhet eller mot myndigheter och personer som ansvarar för dessa uppgifter jämställs därmed med ett hot mot den nationella säkerheten. Hotet mot dem kan till sin natur också vara militärt. För att skydda sig mot sådana hot kan det enligt förslaget genom lag föreskrivas om begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden i syfte att inhämta information om militär verksamhet eller verksamhet som allvarligt hotar den nationella säkerheten.

Uttrycket ”nationell säkerhet” inbegriper också att vilken myndighet som helst som sköter uppgifter i anslutning till säkerheten inte får inhämta information om en hotande verksamhet, utan informationsinhämtningen ska genom lag kunna anvisas endast myndigheter som svarar för den nationella säkerheten. I statens nuvarande organisation har sådana uppgifter anvisats skyddspolisen när det gäller civil underrättelseinhämtning och försvarsmakten, dess huvudstab och underrättelsetjänst, när det gäller militär underrättelseinhämtning.

Inhämtande av information i syfte att sörja för den nationella säkerheten samt inhämtande av i den föreslagna bestämmelsen avsedd information om militär verksamhet begränsar också vem som kan använda den information som inhämtas. Det är fråga om inhämtande av information för den högsta statsledningen i syfte att skapa en lägesbild och stödja beslutsfattandet samt för de nationella säkerhetsmyndigheternas lagstadgade verksamhet.

Bestämmelsen förutsätter att verksamhet som omfattas av dess tillämpningsområde utgör ett allvarligt hot mot den nationella säkerheten. Kravet på att ett hot ska vara allvarligt höjer tröskeln för en tillämpning av bestämmelsen när arten av hotet fastställs. Detta innebär att verksamhet som utgör enbart ett visst mått av hot mot den nationella säkerheten inte ännu uppfyller det krav som bestämmelsen ställer. Hotets allvarlighetsgrad är också kopplad till de ovan behandlade innehållsmässiga definitionerna om hurdan verksamheten ska vara för att utgöra ett sådant hot som avses i bestämmelsen. Genom lag kan det således föreskrivas om begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden i syfte att inhämta information endast om sådan verksamhet som till sin natur kan utgöra ett allvarligt hot mot den nationella säkerheten.

Med uttrycket ”hotar” avses att bestämmelsen inte förutsätter att den nationella säkerheten omedelbart håller på att äventyras. I bestämmelsen avsett inhämtande av information kan således också avse verksamhet som, om den fortsätter, kommer att äventyra den nationella säkerheten.

Verksamhet som allvarligt hotar den nationella säkerheten ska vara ett begrepp som är skilt från de undantagsförhållanden som hotar nationen och som avses i 23 § i grundlagen. Sådana undantagsförhållanden hänför sig till begreppet allmänt nödläge i internationella människorättskonventioner och i dem är det fråga om ett allvarligt hot mot nationens liv och existens (se RP 60/2010 rd, s. 36).

Den föreslagna nya begränsningsgrunden innebär i praktiken att myndigheternas nya befogenheter till informationsinhämtning, om vilka det ska föreskrivas på nivån av vanlig lag och vilka begränsar skyddet för hemligheten i fråga om förtroliga meddelanden, endast omfattar verksamhet som avses i förslaget och att det i lag ska finnas uttömmande bestämmelser om hur befogenheter ska riktas till sådan verksamhet.

Genom den föreslagna ändringen fogas till den särskilda begränsningsklausulen i 10 § i grundlagen en ny godtagbar grund för en begränsning av skyddet för hemligheten i fråga om förtroliga meddelanden. I de övriga begränsningsförutsättningarna i 10 § i grundlagen föreslås det inte några ändringar, utan de kvarstår oförändrade. Vid begränsningar av skyddet för hemligheten i fråga om förtroliga meddelanden tillämpas dessutom de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna som sådana (se GrUB 25/1994 rd, s. 5).

Begränsningarna av skyddet för hemligheten i fråga om förtroliga meddelanden ska enligt gällande 10 § 3 mom. i grundlagen vara nödvändiga. Denna förutsättning följer också av de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. På grund av ärendets betydelse, systematiken i regleringen och flera sätt att skiva s.k. kvalificerade lag-

förbehåll ska det alltjämt nämnas särskilt i bestämmelsen att begräsningen är nödvändig. Detta innebär att en begränsning är tillåten endast om ett godtagbart mål (inhämtande av information om den verksamhet som avses i bestämmelsen) inte kan nås med metoder som gör mindre ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden. Nödvändighetskriteriet innehåller ett krav på att ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden ska ske så riktat och begränsat som möjligt.

I de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna ingår ett krav på att begränsningarna ska vara förenliga med Finlands internationella människorättsförpliktelser. I detta sammanhang har Europakonventionen särskild betydelse utifrån dess innehåll i ljuset av Europadomstolens rättspraxis. Enligt Europadomstolens rättspraxis ska det alltid finnas ett vägande samhälleligt behov av begränsningar av hemligheten i fråga om förtroliga meddelanden. Dessutom ska ingrepp och eftersträvade godtagbara mål stå i rätt proportion till varandra och ingreppen ha tillräckligt vägande och godtagbara motiveringar. Begränsningarna ska också vara tillåtna enligt lag. I Europadomstolens rättspraxis betonas lagens kvalitet, såsom exakthet, samt sådana bestämmelser som säkerställer förutsägbarheten i myndigheternas verksamhet och hindrar maktmissbruk.

Europadomstolen har ansett att det med tanke på att begränsningar av hemligheten i fråga om förtroliga meddelanden ska vara nödvändiga och lagliga är problematiskt bl.a. om underrättelsemyndigheterna i lag ges obegränsade befogenheter att fastställa förutsättningarna för ingrepp i förtroliga meddelanden (Zakharov mot Ryssland, 4.12.2015). Även Europeiska unionens rätt förutsätter att inhämtandet av information ska grunda sig på godtagbara mål med tanke på unionens system för grundläggande fri- och rättigheter samt att inhämtandet av information inte oproportionerligt ingriper i skyddet för privatlivet eller kränker själva kärnan i denna rätt. I EU-domstolens rättspraxis har det särskilt betonats att inhämtandet av information ska vara tillräckligt riktat och specificerat (dom Tele2 Sverige, C-203/15 och C-698/15; dom Schrems, C-362/14; dom Digital Rights Ireland, C-293/12 och C-594/12).

Av kravet på nödvändighet följer att den föreslagna bestämmelsen i 10 § 4 mom. i grundlagen inte tillåter obegränsade ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden. De föreslagna bestämmelserna möjliggör alltså inte allmän, oriktad och heltäckande övervakning av datatrafiken i underrättelseverksamheten. Något sådant förbud behöver dock inte tas in i grundlagstexten eftersom förbudet följer redan av kravet på nödvändighet och av de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna. Den föreslagna bestämmelsen förutsätter att begränsningarna inte bara är nödvändiga utan även proportionerliga. Begränsningarna ska stå i rätt proportion till de godtagbara mål som eftersträvas med dem. Begränsningarna ska också vara förenliga med internationella människorättsförpliktelser liksom med Europeiska unionens rätt. I reglering på nivå av vanlig lag ska det alltså föreskrivas om en individualisering av befogenheterna att inhämta information, om allmänna och specifika förutsättningar för utövande av befogenheterna samt om de principer som ska iakttas vid utövandet av dem.

På grund av det rättsskyddskrav som ingår i de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna står det dessutom klart att det i reglering på nivå av vanlig lag ska sörjas för tillräckliga rättskydds- och tillsynsarrangemang. Rättskyddskravet har också ett nära samband med bestämmelserna om en rättvis rättegång och god förvaltning i 21 § i grundlagen. För sådana situationer som inte kan förenas med en möjlighet att söka ändring vid begränsningen av de grundläggande fri- och rättigheterna, som t.ex. vid underrättelseverksamhet, är det nödvändigt att skapa ersättande rättsskyddsarrangemang. I det nya 4 mom. föreslås därför inte några uttryckliga bestämmelser om rättskydds- eller tillsynsförfarandena i anslutning till utövandet av befogenheterna att inhämta information. Sådana bestämmelser finns

inte heller i gällande 10 § 3 mom. i grundlagen eller i andra bestämmelser om de grundläggande fri- och rättigheterna.

Vid utövandet av de nuvarande befogenheterna till hemlig informationsinhämtning till följd av brott förutsätts i regel ett domstolstillstånd när det görs ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden. Avsikten med domstolsförfarandet är att förhindra missbruk av befogenheterna. Vid förfarandet är det centralt att från fall till fall bedöma om den metod för informationsinhämtning som avses i tillståndsansökan uppfyller de i lag föreskrivna förutsättningarna när det gäller sakförhållandena och andra faktorer om inverkar på ärendet. Rättsskyddsarrangemangen kan också inbegripa andra förfarandegarantier, såsom en skyldighet att underrätta föremålet för informationsinhämtningen om underrättelseverksamheten, individens möjlighet att använda tillräckliga rättsmedel och en skyldighet att dokumentera utövandet av befogenheter att inhämta information liksom även begränsningar av användningen av information som erhållits genom underrättelseverksamhet samt begränsningar som faller tillbaka på andra grundläggande fri- och rättigheter, som t.ex. tryggandet av källskyddet.

Kraven på att rättskyddsarrangemangen och tillsynen ska vara effektiva och behöriga framhävs i synnerhet i underrättelseverksamheten jämfört med hur den nuvarande regleringen möjliggör begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden. Detta beror inte bara på att den föreslagna ändringen gör det möjligt att genom lag föreskriva om nya myndighetsbefogenheter utan även på att de befogenheter som ändringsförslaget möjliggör på grund av särdragen hos underrättelseverksamheten kan avvika från t.ex. de nuvarande metoderna för inhämtning av hemlig information som baserar sig på brott. Även människorättsförpliktelserna och Europeiska unionens rättsordning förutsätter att tillsynen över utövandet av befogenheter som ingriper i skyddet för hemligheten för förtroliga meddelanden ska vara effektiv och oberoende. När det föreskrivs om nya befogenheter måste man sörja för en tillräcklig parlamentarisk kontroll och en effektiv och oberoende laglighetskontroll. Laglighetskontrollen måste ges starka befogenheter att vid behov ingripa i underrättelsemyndigheternas verksamhet för att skydda individens rättsliga ställning och de grundläggande fri- och rättigheterna samt för att säkerställa att verksamheten är lagenlig.

## 2 Ikraftträdande

Lagen föreslås träda i kraft så snart som möjligt med beaktande av dess lagstiftningsordning.

## 3 Lagstiftningsordning

Propositionen gäller en ändring av grundlagen. Den ska därför behandlas i den ordning som föreskrivs i 73 § i grundlagen.

Grundlagsutskottet har med tanke på grundlagens relativa beständighet och statsrättsliga status ansett att det är det viktigt att ändringarna i grundlagen behandlas enligt huvudregeln i normal grundlagsordning enligt 73 § 1 mom. Förfarandet enligt 73 § 2 mom. där förslaget förklaras brådskande bör enligt utskottet inte användas, om inte det finns ett exceptionellt trängande behov av att snabbt ändra grundlagens lydelse (GrUB 5/2005 rd, s. 5). Enligt grundlagsutskottet

är det mycket viktigt att den försnabbade behandlingsordningen inte utnyttjas annat än i tvingande situationer och att behandlingen av grundlagsändringar sker i normal ordning också i praktiken (GrUB 10/2006 rd, s. 6).

I de regeringspropositioner som gäller lagstiftningen om civil och militär underrättelseverksamhet har aspekter i anslutning till den försvagade och allt mer komplexa säkerhetssituationen i Finland utretts ingående. Förändringen i säkerhetssituationen i Finland är en följd bl.a. av den ökade militära aktiviteten och de ökade militära spänningarna i våra närområden. De allvarligaste hoten mot den nationella säkerheten har numera mycket ofta internationellt ursprung eller internationella kopplingar och är därför svårare att hantera. Dessutom har den snabba utvecklingen inom kommunikationstekniken effektiviserat och underlättat kontakterna och nätverksbildandet mellan de aktörer som hotar Finland och gjort det svårare att identifiera de aktörer som står bakom hoten. Utvecklingen på det tekniska området har också gjort det möjligt att förbereda och genomföra handlingar som hotar den nationella säkerheten på kortare tid än tidigare. När hoten har realiserats har effekterna samtidigt blivit mera omfattande och mångfacetterade och farligare än tidigare med tanke på enskilda och samhället i stort.

Den försvagade säkerhetssituationen i Finland och behovet av att bereda sig på verksamhet som hotar Finlands nationella säkerhet utgör enligt regeringens uppfattning en sådan exceptionell situation där det föreligger ett nödvändigt behov att snabbt ändra grundlagen.

I de regeringspropositioner som gäller civil och militär underrättelseverksamhet föreslås nya befogenheter för underrättelsemyndigheterna. De befogenheter som ingriper i skyddet för hemligheten i fråga om förtroliga meddelanden förutsätter en ändring av 10 § 3 mom. i grundlagen. Om den nu föreslagna grundlagsändringen behandlas i normal grundlagsordning kan bestämmelserna om dessa befogenheter träda i kraft kanske först i början av 2020. Om brådskande grundlagsordning tillämpas kan bestämmelserna träda i kraft tidigare, eventuellt redan i slutet av 2018, beroende på behandlingen av propositionerna i riksdagen. Om behandlingen av propositionerna i riksdagen pågår ända till slutet av denna valperiod minskar behovet av ett brådskande förfarande.

På basis av ovan nämnda aspekter föreslår regeringen att förslaget till ändring av grundlagen ska behandlas i brådskande grundlagsordning i riksdagen.

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

*Lagförslag*

# Lag

**om ändring av 10 § i Finlands grundlag**

I enlighet med riksdagens beslut, tillkommet på det sätt som föreskrivs i 73 § i grundlagen,
*ändras* i Finlands grundlag 10 § 3 mom. och
*fogas* till 10 § ett nytt 4 mom. som följer:

10 §

*Skydd för privatlivet*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Genom lag kan föreskrivas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna skall kunna tryggas eller för att brott skall kunna utredas.

Genom lag kan föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid bekämpning 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.

———

Denna lag träder i kraft den 20 .

———

Helsingfors den 25 januari 2018

**Statsminister**

**Juha Sipilä**

Justitieminister Antti Häkkänen

*Bilaga*
*Parallelltext*

# Lag

**om ändring av 10 § i Finlands grundlag**

I enlighet med riksdagens beslut, tillkommet på det sätt som föreskrivs i 73 § i grundlagen, *ändras* i Finlands grundlag 10 § 3 mom. och
*fogas* till 10 § ett nytt 4 mom. som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 10 § | 10 § |
| *Skydd för privatlivet* | *Skydd för privatlivet* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| Genom lag kan bestämmas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna skall kunna tryggas eller för att brott skall kunna utredas. Genom lag kan *också* bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande. | Genom lag kan *föreskrivas* om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna skall kunna tryggas eller för att brott skall kunna utredas. |
| (*ett nytt 4 mom.*) | Genom lag kan *föreskrivas* om sådana begränsningar i meddelandehemligheten som är nödvändiga vid *bekämpning* 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*. |
| | ———— |
| | *Denna lag träder i kraft den 20 .* |
| | ———— |